LÄHIVERKON LAITTEIDEN ETÄHALLINTA

Case: Akaan kaupunki

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, kevät 2016

Petteri Lehtonen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Visamäki
Tietojenkäsittely

TIIVISTELMÄ

Tekijä Petteri Lehtonen **Vuosi** 2016

Työn nimi Lähiverkon laitteiden etähallinta

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli löytää sopiva ratkaisu Akaan kaupungin verkonhallintaan. Toimeksiantaja työssä oli Akaan kaupungin tietohallintopalvelut. Ennestään Akaalla ei ollut toimivaa verkonhallintajärjestelmää. Työssä tutustuttiin lähiverkkojen ja verkonhallinnan sisältämiin protokolliin ja toimintamalleihin.

Käytännön osuudessa tutustuttiin kahteen verkonhallintajärjestelmään nimeltään Lansweeper ja OpenNMS sekä niiden asennukseen ja käyttöön. Järjestelmiin tutustuttiin myös yhdessä toimeksiantajan kanssa, minkä jälkeen päädyttiin hankkimaan Lansweeper-ohjelmistoon lisenssi.

Järjestelmiä tutkittaessa kävi ilmi, että järjestelmät toimivat eri periaatteilla: Lansweeper on kaupallinen ja suunniteltu erityisesti työasemien hallintaan. OpenNMS taas on avoimen lähdekoodin ohjelma, josta täytyy itse muokata omiin tarpeisiin soveltuva ohjelma. Toimeksiantaja arvosti enemmän helppokäyttöisyyttä kuin muokattavuutta.

Teoriaosuuden tietopohja perustui suurimmilta osin lähiverkkoja käsitteleviin kirjoihin. Käytännönosuudessa hyödynnettiin verkosta löytyviä ohjemateriaaleja.

Työn pohjalta kaupunki sai käyttöönsä valmiiksi määritellyn verkonhallintajärjestelmän, jota voidaan tarpeen vaatiessa laajentaa tukemaan suurempaa määrää laitteita. Järjestelmä on hyvin laajennettavissa ja tarvittaessa siihen voidaan liittää esimerkiksi työasemia, tulostimia ja muita laitteita kytkinten lisäksi.

Avainsanat verkonhallinta, tietoliikenne, protokollat

Sivut 27 s.

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Visamäki
Business Information Technology

Author Petteri Lehtonen **Year** 2016

Subject of Bachelor's thesis Remote controlling of network devices

ABSTRACT

The goal of this thesis was to find a network management software suitable for a mid-size network. The main use of the software was to manage mainly switches. The client was the town of Akaa. The thesis discusses the protocols and frameworks of network management as well as the basics of local area networks or LANs.

The practical part of this thesis covers the installation and configuration of two network management softwares called Lansweeper and OpenNMS. This was done in co-operation with the client. In the end the decision was to buy a license for Lansweeper –software.

When examining the two solutions many differences were spotted regarding their purposed use. Lansweeper is a closed source software with emphasis on workstation management. OpenNMS is, as the name suggests, a open-source software. OpenNMS requires more time to spend in configuration and maintenance. With unlimited resources it would have been the optimal choice. However, the client favored ease of use over customization.

The theoretical part of the thesis is based on several books discussing networks as well as articles and news found on the internet. The practical part used several online guides and white papers.

Based on this work the town of Akaa was left with a functional, ready to use network management software. The scalability of the software enables future expansions for example including workstation management and deployment of software.

Keywords network managament, network communications, protocols

Pages 27 p.

SISÄLLYS

KÄSITELUETTELO

LAN

Lähiverkko. Tietoliikenneverkko, joka toimii rajatulla maantieteellisellä alueella. Lähiverkot muodostavat yhdessä isompia verkkoja, isoimpana internet.

OSI-malli

Verkkomalli, joka kuvaa verkon arkkitehtuuria kerroksittain. Käytetään viitattaessa protokollien toiminta-tasoon. Vähemmän suosittu kuin TCP/IP-malli.

TCP/IP-malli

Samankaltainen verkkomalli kuin OSI-malli, mutta jakaa verkon toiminnan eri tavalla. Noussut OSI-mallin ohi yleisyydessä.

IETF

Internet Engineering Task Force. Kehittää ja ylläpitää Internetin standardeja.

RFC

Request for Comment. Dokumentti, jossa esitellään protokollan tai standardin toiminta. Protokollia ja standardeja ei haluta määrätä liian tarkasti ja siksi niitä kutsutaan nimellä RFC (Kommentin pyyntö).

ITU

International Telecommunication Union, kansainvälinen televiestintäverkkoja koordinoiva järjestö.

ITU-T

ITU Telecommunication Standardization Sector, ITU:n televiestintäsektori

TMN

Telecommunications management network, ITU-T:n määrittelemä verkonhallinnan standardi.

FCAPS

Lyhenne sanoista fault, configuration, accounting, performance ja security. ITU-T:n suositus verkonhallinnan tehtävistä.

SNMP

Simple Network Management Protocol. Sovelluskerroksen protokolla, jolla kerätään tietoa verkon laitteista.

UDP

User Datagram Protocol, kuljetuskerroksen protokolla, joka ei vaadi yhteyttä laitteiden välille. Pakettien perille saapumista ei siis varmisteta.

Agentti

Hallittavalla laitteella oleva ohjelma, joka vastaa hallinta-aseman pyyntöihin ja hakee tietoja laitteesta

MIB

Management information base. Tietokanta, joka sisältää tietoja laitteen kunnosta. Laitteessa oleva agentti välittää MIB-tietokannasta tietoja eteenpäin hallinta-asemalle

ASN.1

Abstract Syntax Notation One. Kieli, jolla kuvataan tietokannan tietoja.

BER

Basic Encoding Rules. Sääntö, jolla ASN.1 koodataan biteiksi alempia kerroksia varten.

SSH

Secure Shell. Salattu tietoliikenne protokolla, joka toimii TCP/IP –mallin sovellustasolla. Käytetään yhteyden muodostamiseksi laitteisiin, kuten kytkimiin ja palvelimiin.

Telnet

Tietoliikenne protokolla, joka toimii TCP/IP –mallin sovellustasolla. Käytetään SSH-protokollan tavoin etäyhteyden muodostamiseen. Sisältää tietoturvariskin, jonka vuoksi SSH on syrjäyttämässä sitä.

UPS

Uninterruptible power supply. Varavirtalähde, joka suojaa laitteita sähkökatkojen tai virtapiikkien aiheuttamilta ongelmilta.

VLAN

Virtual Local Area Network, virtuaalinen lähiverkko. Fyysinen lähiverkko voidaan jakaa virtuaalisesti loogisiin osiin.

RIP

Routing Information Protocol. Yleisin käytetty reititysprotokolla. Laskee nopeimman mahdollisen reitin hyppyjen eli välissä olevien reitittimen lukumäärän perusteella.

DHCP

Dynamic Host Configuration Protocol. Protokolla, joka jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille. Toimii sovelluskerroksella.

IPv4

Internet Protocol version 4. Verkkokerroksella toimiva protokolla, joka huolehtii tietoliikennepakettien perille toimittamisesta IP-osoitteiden perusteella.

IPv6

Internet Protocol version 6. IPv4-protokollan seuraaja. Tärkeimpänä ominaisuutena osoiteavaruuden laajentuminen verrattuna IPv4-protokollaan.

NAT

Network address translation. Tekniikka, jolla useita sisäverkon IP-osoitteita yhdistetään ja joilla on yksi yhteinen julkinen IP-osoite.

1 JOHDANTO

Opinnäytetyön tarkoituksena on löytää sopiva ohjelmisto, jolla hallita suurehkoa lähiverkkoa. Työn toimeksiantajana on Akaan kaupunki. Kaupungilla on tarve saada verkon laitteet, erityisesti kytkimet, etähallinnan piiriin ja saada niistä hälytykset ulos. Näin säästetään työtunteja, kun ongelmiin voidaan puuttua jo ennen kuin niitä ilmenee ja niihin voidaan puuttua ilman tarvetta käydä paikan päällä korjaamassa vikaa.

Työssä keskitytään kahteen verkonhallinnan osa-alueeseen: virheidenhallintaan ja verkon konfiguraation sekä muutosten hallintaan. Työ on hyvin työelämäläheinen. Toimeksiantaja Akaan kaupunki on noin 17 000 asukkaan kaupunki Etelä-Pirkanmaalla ja käsittää entisten Toijalan, Viialan ja Kylmäkosken kunnat.

Aihe on hyvin käytännönläheinen. Opinnäytetyöaihetta selvitettäessä kävi ilmi, että Akaan kaupungilla ei ole käytössään toimivaa verkonhallintajärjestelmää, ja sellaisen hankkiminen olisi ajankohtaista. Työssä syvennytään verkonhallinnan protokolliin ja periaatteisiin sekä tietoliikenneverkkojen perustoimintaan.

Teoriaosuus käsittelee yleisesti lähiverkkoja, niiden rakennetta ja arkkitehtuuria. Lähiverkkoja käsitellään hyvin yksinkertaisesti ja pelkistetysti. Tämän lisäksi työ käsittelee lähiverkkojen historiaa sekä viimeisimpiä kehitysvaiheita. Lähiverkon lisäksi verkonhallinnan protokollat ja periaatteet käydään läpi. Tässä työssä keskitytään erityisesti hallintaprotokolla SNMP:n käsittelyyn.

Näihin tietoihin pohjautuen Akaan kaupungille otetaan käyttöön verkonhallintajärjestelmä. Järjestelmälle on asetettu tarkat kriteerit ja näiden pohjalta valikoitui kaksi järjestelmää, Lansweeper ja OpenNMS. Näiden kahden järjestelmän toimintaa käydään läpi ja suoritetaan vertailua, jonka jälkeen toinen niistä otetaan käyttöön.

Työssä haetaan vastauksia seuraaviin kysymyksiin: Minkälaisia protokollia, suosituksia ja standardeja verkonhallintaan on? Mikä on paras tapa saada laajahkon verkon laitteista virhehälytyksiä? Miten verkon laitteita, pääasiassa kytkimiä, voidaan hallita? Millä järjestelmällä/järjestelmillä virheenhallinta ja konfiguraationhallinta on paras tehdä?

2 LÄHIVERKKOJEN PERUSTEET

Tietoliikenneverkot voidaan jakaa maantieteellisen kokonsa perusteella lähi-, alue- ja etäverkkoihin. Tällainen jako maantieteellisiin alueisiin on hieman keinotekoista, mutta se auttaa hahmottamaan verkkojen toimintaperiaatteet ja tarkoitukset. (Jaakkohuhta 2005, 5.)

Lähiverkolla (LAN) on tarkoitettu saman yrityksen tai organisaation tietoliikenneverkkoa. Nimensä mukaisesti lähiverkko käsittää lähellä toisiaan olevat laitteet. (Puska 2000, 12.) Lähiverkkoa voitaisiin kuvata taloksi, jossa on useita huoneita. Jokainen huone on osa taloa ja jokaisesta huoneesta pääsee liikkumaan toiseen. Lähiverkossa jokaisella laitteella on oma IP-osoitteensa, jonka avulla samassa verkossa olevat laitteet tunnistavat toisensa. IP-osoite kuitenkin usein vaihtuu siirryttäessä lähiverkosta alue- tai etäverkkoon. Esimerkiksi kodin sisäisessä, eli yksityisessä verkossa käytetään tiettyjä IP-osoitealueita, jotka IETF on määritellyt RFC-1918-dokumentissa. (RFC-1918 1996, 3.)

Alueverkko (MAN) käsittää laajemman alueen kuin lähiverkko. Alueverkko yhdistää yleensä useamman lähiverkon yhteen isommaksi kaupunki- tai kampusalueen dataverkoksi. (Puska 2000, 12.) Alueverkkoa voitaisiin niin ikään verrata kaupungiksi, joka koostuu useasta yksittäisestä talosta.

Etäverkot (WAN) tarkoittavat julkisten teleoperaattoreiden maanlaajuisia tai kansainvälisiä verkkopalveluja. (Puska 2000, 12.) Suurimpana etäverkkona voidaan pitää internetiä, joka koostuu useista lähiverkoista ja alueverkoista. Etäverkko on kuin valtio, jonka kaupungit on liitetty toisiinsa maanteillä. Tällä hetkellä Suomen etäverkkojen liikenne Manner-Eurooppaan ja eteenpäin länteen kulkee Ruotsin kautta (Submarine Cable Map 2016). Tulevaisuudessa Suomen lähi-, alue- ja etäverkot voidaan yhdistää myös suoraan Manner-Eurooppaan ja sieltä eteenpäin C-Lion-merikaapelilla (kuva 1), joka kulkee Helsingin Santahaminasta Saksan Rostockiin (Dahl 2015).

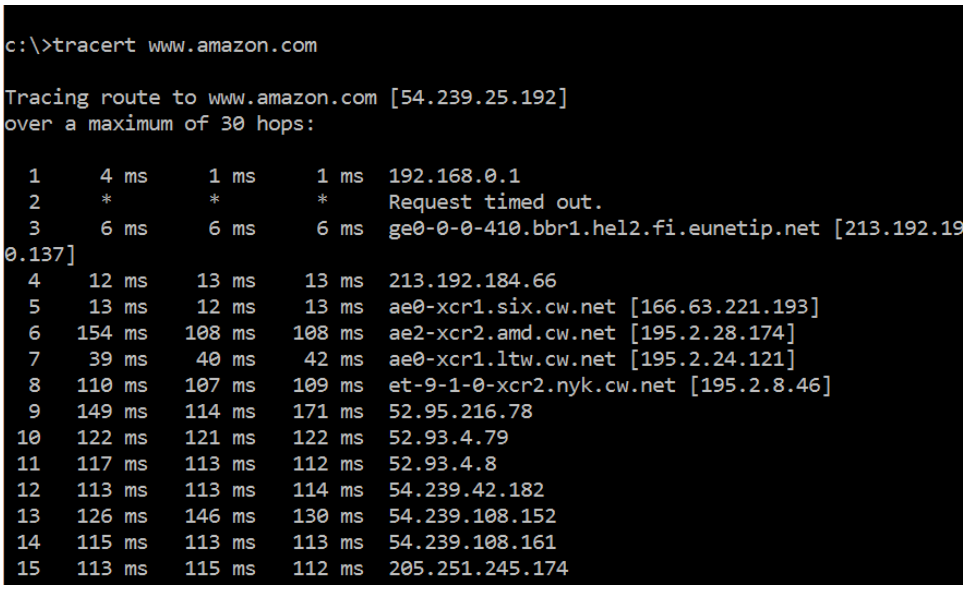
Kuva 1. Suomesta lähtevät merikaapelit yhdistävät Suomen internetiin. Harmaalla uusi C-Lion –merikaapeli. (Primetrica, 2016.)

2.1 Tiedon kulku verkossa

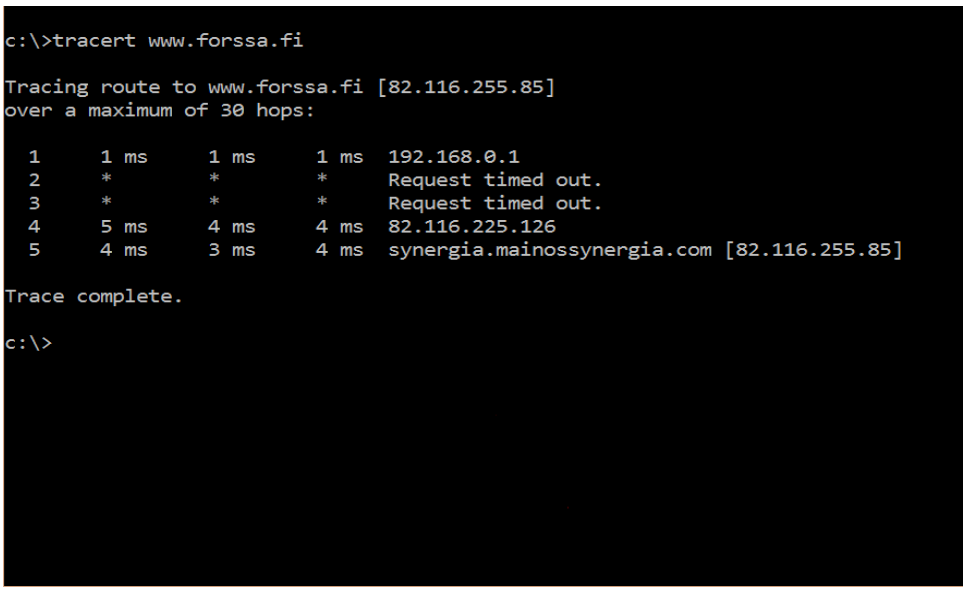
Jotta jokainen tietokone osaisi viestiä verkossa, tarvitaan IP-osoitteita. Lähiverkossa tästä tehtävästä huolehtii yleensä DHCP-palvelin, joka jakaa IP-osoitteita laitteille. Kotikäytössä reititin toimii yleensä DHCP-palvelimena. Jokaisella laitteella on myös MAC-osoite, joka on sidottu fyysiseen verkkokorttiin ja joka ei muutu, toisin kuin IP-osoite (Kaario 2002, 36).

Kun otetaan yhteyttä laitteeseen, joka ei ole samassa verkossa tarvitaan reitittimiä. Reititin liikuttaa dataa kahden eri verkon välillä. Mikäli kohde, johon halutaan yhteys, sijaitsee fyysisesti kaukana, voi välissä olla monta eri verkkoa ja reititintä. Tästä johtuen vasteaika, joka kuluu paketin lähettämisestä sen vastaanottamiseen kasvaa, mitä kauemmaksi se joutuu matkustamaan. Vasteaika ja paketin kulkema reitti voidaan helposti selvittää Traceroute-työkalulla. Työkalun avulla voidaan selvittää paketin kulkema reitti. Windows käyttöjärjestelmässä Traceroute-työkalu lähettää ICMP-sanoman.

Traceroute-komentoa käyttäessä on kuitenkin muistettava, että kaikki verkon laitteet eivät välttämättä vastaa ICMP-sanomiin. Tämä protokolla on monesti poistettu käytöstä tietoturvan takia (Kaario 2002, 259). Kuvassa kaksi näkyy, kuinka paketti siirtyy reitittimeltä toiselle kulkien Ruotsin, Alankomaiden ja Ranskan kautta Yhdysvaltoihin. Vasteajat ovat kohtalaisen suuria. Kuvassa kolme taas paketti ei juurikaan joudu käymään pitemmällä.



Kuva 2. Paketin matka amazon.com -palvelimelle Yhdysvaltoihin



Kuva 3. Lähellä olevaan palvelimeen on lyhyempi matka.

Nykyisten dataverkkojen kasvaneet nopeudet tarkoittavat käytännössä sitä, että siirtymää eri verkkojen välillä ei käytännössä huomaa. Yhdysvalloissa sijaitseva uutissivu aukeaa yhtä nopeasti kuin kotimainenkin, vaikka data joutuu kiertämään monen pisteen kautta ja pitkän matkan.

2.2 IPv4 ja IPv6

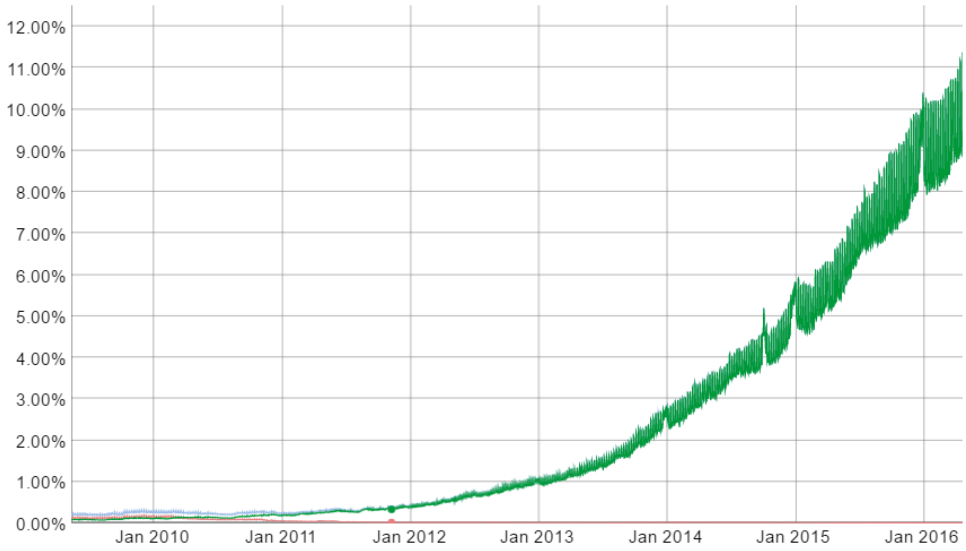
Dataverkkojen kasvu on myös johtanut osoitepulaan. Nykyisin yleisimmin käytetty IPv4-protokolla on ollut käytössä jo yli 30 vuotta, ja syyskuussa 2012 Euroopan IPv4-osoitteita hallinoiva RIPE ilmoitti IPv4-osoitteiden loppuneen (Vänskä 2012). Myös muiden maanosien IPv4-osoitteita hallinnoivien järjestöjen varastot ovat tyhjät. APNIC, Aasiaan IPv4-osoitteita jakeleva taho käytti ensimmäisenä loppuun omat IPv4-varastonsa huhtikuussa 2011 (Korhonen 2011). Kesäkuussa 2014 IPv4-osoitteet loppuivat Etelä-Amerikassa ja Karibialla (Fiveash 2014). ARIN, Pohjois-Amerikan IPv4-osoitteista vastaavat taho ilmoitti syyskuussa 2015, että sen varastot ovat myös loppuneet (Hogg, 2015). Ainoa taho, jolla on vielä IPv4-osoitteita varastossa, on Afrikan osoitteista vastaava AFRINIC (IPv4 Statistics n.d). Vanhoja, kertaalleen jaettuja IP-osoitteita kuitenkin vapautuu vielä jonkin verran käyttöön.

Vaikka osoitteet loppuvat, ei se ole juurikaan näkynyt tavalliselle internetin käyttäjälle. IP-osoitteiden loppuminen koskettaa eniten verkko-operaattoreita. Monet operaattorit ovatkin varanneet omiin varastoihinsa paljon IP-osoitteita, joita voidaan edelleen jakaa asiakkaille. Silti yhä useammat operaattorit ovat siirtyneet käyttämään NAT-menettelyä IP-osoitteiden säästämiseksi. NAT-menettelyssä sisäverkon, eli esimerkiksi operaattorin asiakkailleen jakamat IP-osoitteet, muunnetaan virallisiksi RIPEn myöntämiksi IP-osoitteiksi. Muutoksessa voidaan niputtaa useamman sisäverkon laitteen IP-osoitteet yhdeksi julkiseksi, viralliseksi IP-osoitteeksi (Jaakkohuhta 2005, 196). Esimerkiksi useimmissa mobiili-liittymissä ei ole omaa virallista IP-osoitetta, vaan IP-osoite jaetaan useamman laitteen kanssa. Tästä syystä esimerkiksi oman palvelimen nostaminen julkiseen verkkoon on mahdotonta, mikäli internet-palveluntarjoaja ei tarjoa julkista IP-osoitetta liittymään (Mobiililaajakaistan IP-osoitteet – NAT tai Julkinen IP-osoite n.d). NAT voi myös haitata esimerkiksi verkkopelaamista ja VoIP –ohjelmistoja.

NAT ei kuitenkaan pysty kokonaan vastaamaan IPv4-osoitteiden loppumisesta koituviin haasteisiin monien ongelmiensa takia. Pysyvämmäksi ratkaisuksi on suunniteltu IPv6-protokolla. IPv4-protokollan seuraajaa alettiin suunnitella jo vuonna 1991 ja vuonna 1998 IPv6 protokolla standardisoitiin. (Kaario 2002, 109.) Tärkeimpänä IPv6-protokollan ominaisuutena on osoiteavaruuden kasvaminen. Yhä useammat laitteet käyttävät internetiä, joten IP-osoitteiden tarve kasvaa nopeasti. IPv6-osoitteet ilmaistaan 128 bitillä, jolloin, yhden bitin ollessa joko 1 tai 0, osoitteita on tarjolla käytettäväksi 2^{128}. Tällainen määrä riittäisi hyvin turvaamaan IP-osoitteiden riittävyyden. Vertailun vuoksi, IPv4-osoite koostuu 32 bitistä, joten erilaisia mahdollisia IP-osoitteita on 2^{32}.

Vaikka IPv6 onkin jo ollut olemassa jonkin aikaa, ei se vieläkään ole levinnyt kovin laajalle. Yksi syy tähän ovat NAT-menettelyn käyttö. Tavalliselle verkonkäyttäjälle ei ole väliä, onko tällä oma julkinen IP-osoite vai ei. IPv6-osoitteiden käyttöönotto on myös melko kallista, sillä IPv6-osoitteet eivät ole yhteensopivia IPv4-osoitteiden kanssa. Jotta IPv6-osoitteella voidaan ottaa yhteyttä IPv4-osoitteeseen, täytyy osoite muuttaa joka tapauksessa IPv4-muotoon. IPv6-osoitteiden visuaalinen muoto ei myöskään lisää innostusta sen käyttöönottoon. IPv6 osoite esitetään muodossa x:x:x:x:x:x:x:x, missä jokainen x on 16-bittinen heksadesimaaliluku. Esimerkiksi 2001:db8::1420:57ab voisi olla IPv6-osoite. Tällainen osoite on huomattavasti vaikeampi muistaa kuin esimerkiksi IPv4-muotoa oleva osoite 192.168.1.1.

Tästä johtuen IPv6-osoitteiden käyttöönotto on ollut melko hidasta. Käyttöönottoa jouduttamaan järjestettiin 6.6.2012 Kansainvälinen IPv6-päivä, jolloin verkko-operaattoreita kannustettiin IPv6-osoitteiden käyttöönottoon. Suurimmat yhtiöt, kuten Microsoft, Google ja Cisco ovatkin jo siirtyneet IPv6-tekniikkaan (IPV6 is the new normal nd.). Google ylläpitää omaa taulukkoaan (Kuva 4), josta näkyy IPv6-tekniikan käyttäjien osuus Googlen palvelujen kaikista käyttäjistä.



Kuva 4. IPv6-käyttäjien osuus kaikista Googlen palvelujen käyttäjistä (Google, n.d.).

Viestintävirasto järjesti Suomessa 9.6.2015 kansallisen IPv6:n käyttöönottopäivän. Päivään osallistui monia suurimpia laajakaistapalveluntarjoajia kuten Elisa, Dna, Sonera ja Ålcom. Tällä hetkellä Suomessa noin 5 miljoonalla laajakaistakäyttäjällä on mahdollisuus ottaa IPv6-osoite käyttöön. (Viestintävirasto 2015.) Usein asiakkaan täytyy kuitenkin erikseen tilata IPv6-osoite laajakaistaoperaattoriltaan (Valokaista palvelukuvaus 2016, 3).

2.3 Lähiverkon arkkitehtuuri

Elävässä elämässä ihminen toimii, yleensä tiedostamattaan, erilaisten sääntöjen mukaan. Esimerkiksi liikenteeseen lähdettäessä on noudatettava liikennesääntöjä, jotka määrittelevät kuka väistää ketä, kenellä on etuajoikeus, onko katu yksisuuntainen, miten toimitaan kolaritilanteessa jne. Tietoliikenteessä näitä liikennesääntöjä kutsutaan protokolliksi. Kaksi samaa protokollaa noudattavaa osapuolta voivat kommunikoida keskenään ja suorittaa niille määritellyn tehtävän (Kaario 2002, 14). Protokollat määrittelevät miten data liikkuu verkossa ja mitä tapahtuu, kun datapaketit törmäävät tai jättävät saapumatta kohteeseen.

Liikenteessä pätevät eri säännöt riippuen liikutaanko kävellen, polkupyörällä vai autolla. Samoin tietoliikenteessä noudatetaan eri protokollia riippuen siitä, minkälaista dataa verkossa halutaan siirtää.

Tietoliikenteen toiminta saattaa vaikuttaa tavalliselle käyttäjälle hyvinkin monimutkaiselta. Tätä monimutkaisuutta varten tietoliikenne voidaan kuvata kerrosmallina. Jokaisessa kerroksessa on omat protokollansa, joiden mukaan data liikkuu. Esimerkiksi edellä mainittu autolla ajaminen voidaan kuvata kerrosmallina, jossa jokaisessa kerroksessa on omat protokollansa, sääntönsä, joiden mukaan toimitaan. Auton moottoria ja tekniikkaa voidaan kuvailla ”pohjakerrokseksi”. Jotta auto liikkuu eteenpäin, moottorin täytyy tuottaa voimaa, joka siirretään pyörille. Kuski käyttää autoa hallintalaitteiden avulla, jotka toimivat omien sääntöjensä mukaan, mutta kuuluvat silti samaan kerrokseen. Lopulta kuski noudattaa liikennesääntöjä, jotka kuuluvat päällimmäiseen kerrokseen. Tietoliikenteessä kaksi yleisintä mallintamistapaa ovat OSI-malli ja TCP/IP-malli.

2.4 OSI-malli

OSI-malli syntyi 1980-luvulla ja sen tavoitteena oli luoda yhdenmukainen verkkomalli laitevalmistajille ja käyttäjille, jonka laitteet pystyisivät kommunikoimaan keskenään. OSI-malli ei kuitenkaan ole saavuttanut suosiota käytännön verkkototeutuksissa, vaan useimmat tietokoneet käyttävät TCP/IP -mallia. OSI-mallin vaikutusta tietoliikenteen kerrosajatteluun ei voida kuitenkaan kiistää ja edelleen käytössä olevissa verkkomalleissa käytetään OSI-mallin terminologiaa (Odom 2005, 58). OSI-malli jakaa verkon seitsemään kerrokseen.

2.4.1 Fyysinen kerros

Fyysinen kerros huolehtii bittivirran fyysisestä siirtämisestä. Se ottaa kantaa muun muassa siihen, minkälaista kaapelia käytetään tai minkälaisia liittimiä käytetään. Fyysinen kerros on poikkeava siinä mielessä, että se joutuu ottamaan huomioon fyysiset ilmiöt. Muut kerrokset ovat lähinnä ohjelmistollisia (Kaario 2002, 19). Fyysinen kerros ei millään tavalla tarkista dataa, vaan jättää sen muiden, ylempien kerrosten tehtäväksi.

2.4.2 Siirtokerros

Siirtokerroksen tehtävä on huolehtia bittivirran siirtämisestä siirtotietä pitkin. Se poimii fyysisestä signaalista datan, tutkii sen siirtovirheiden varalta ja lähettää sen eteenpäin määrämuotoisissa kehyksissä fyysiselle kerrokselle. Mikäli kehyksessä havaitaan virheitä, paketti voidaan joko tuhota tai pyytää uudelleenlähetettäväksi. Esimerkiksi videon suoratoistossa on tärkeämpää, että data liikkuu katkeamatta, kun taas tiedostonlatauksessa datan eheys on tärkeintä. Siirtokerros tarjoaa ylemmälle kerrokselle, verkkokerrokselle, siirtoyhteyden. (Kaario 2002, 20.) Siirtokerros voi myös rajoittaa fyysiselle kerrokselle lähetettävän datan määrää, tai määritellä päätelaitteille oikeuksia fyysisen kerroksen käyttöön. Siirtokerros voi myös muodostaa useamman kuin yhden fyysisen yhteyden kahden laitteen välillä. Tällä tavoin yhteyden laatuvaatimukset saadaan täytettyä. Useamman fyysisen yhteyden takia myös kuljetuskerroksen merkitys korostuu, koska pakettien on tultava perille oikeassa järjestyksessä.

2.4.3 Verkkokerros

Verkkokerroksen tehtävänä on reitittää datapaketit verkon yli tietokoneiden välillä. (Kaario 2002, 20.) Verkkokerros jakaa kuljetuskerroksen lähettämän tiedon paketteihin ja reitittää ne oikeaan paikkaan osoitteen perusteella. Reitittämiseen käytetään reititystauluja, eräänlaisia tienviittoja. Reitittimet vaihtavat tietoja käyttämällä erilaisia reititysprotokollia, tunnetuimpana näistä RIP.

2.4.4 Kuljetuskerros

Huolehtii siitä, että datapaketit tulevat perille oikeassa järjestyksessä. Toimii linkkinä ylempien kerroksien ja varsinaisen tietoliikenneverkon kanssa. (Kaario 2002, 20.) Kuljetuskerroksesta ylemmät kerrokset eivät siis varsinaisesti ole kosketuksissa tietoliikenneverkkoon. Kuljetuskerros myös muodostaa varsinaisen yhteyden kahden laitteen välillä. Tämä yhteys voi olla joko yhteydellinen tai yhteydetön. Yhteydellisissä protokollissa, kuten TCP:ssä pakettien saapuminen varmistetaan. Yhteydettömissä protokolissa, kuten UDP:ssä, pakettien perille saapumista taas ei varmisteta millään tavalla.

2.4.5 Istuntokerros

Huolehtii yhteyden muodostumisesta kahden osapuolen välillä (Kaario 2002, 21.) Vastaavasti istuntokerros huolehtii myös yhteyksien katkaisemisesta. Kerros myös tahdistaa datavirran, jonka tarpeellisuus käy ilmi esimerkiksi videoneuvottelussa. Äänen ja kuvan on tultava samaan tahtiin. Istuntokerros pystyy myös tekemään merkkejä kahden osapuolen keskusteluun. Mikäli osapuolien keskustelu keskeytyy jostain syystä, istuntokerroksen avulla keskustelua voidaan jatkaa merkistä.

2.4.6 Esitystapakerros

Nimensä mukaisesti huolehtii siirron aikana käytettävästä esitystavasta, esimerkiksi merkistökoodauksesta (Kaario 2002, 21). Huolehtii että kohteilla on yhteinen esitystapa. Esimerkiksi verkonhallinnassa käytettävä ASN.1-kieli sijoittuu esitystapakerrokselle. Muita tavanomaisia esitystapakerroksen käyttämiä muotoja ovat esimerkiksi gif-kuvat, xml-tiedostot ja olio-pohjaisessa ohjelmoinnissa käytettävät oliot. Ideana on, että sovelluskerroksen ei tarvitse välittää datan tyypistä. Kryptaus, eli salaaminen, ja enkryptaus, eli salauksen purku, tapahtuvat myös esitystapakerroksella.

2.4.7 Sovelluskerros

Toimii varsinaisena rajapintana sovelluksen ja tiedonsiirron välillä. Käyttäjälle näkyvä sovellus, kuten sähköpostiohjelma, käyttää sovelluskerroksen protokollia siirtäessään tietoa alaspäin kerroksissa. (Kaario 2002, 21.) Sovellus ei siis käytä muita kerroksia, vaan sovelluskerros huolehtii tiedon siirtämistä alaspäin kerroksittain.

2.5 TCP/IP-malli

TCP/IP–malli kehitettiin alun perin ARPANETin, nykyisen internetin edeltäjän, tarpeisiin. Mallista käytetään joskus myös nimeä DoD-malli, ARPANETiä rahoittaneen Yhdysvaltain puolustusministeriön mukaan. (Puska 2000, 143.)

Siinä missä OSI-mallia ei käytetä juurikaan käytännöntoteutuksissa vaan terminologiassa, TCP/IP-mallilla asia on lähes päinvastoin. TCP/IP-malli sisältää neljä kerrosta. Alinta kerrosta, joka sisältää OSI-mallia vastaavat siirto- ja fyysisen kerroksen, ei yleensä kuitenkaan lueta mukaan, sillä TCP/IP-malli ei ota kantaa siihen, minkälaisia protokollia kyseisillä kerroksilla käytetään. (Odom 2005, 57.) Periaatteessa TCP/IP-verkossa voidaan siirto- ja fyysisillä kerroksilla käyttää mitä tahansa tekniikkaa (Kaario 2002, 22).

Taulukko 1. TCP/IP-malli suhteessa OSI-malliin

TCP/IP-malli	**OSI-malli**
Sovelluskerros	Sovelluskerros
	Esitystapakerros
	Istuntokerros
Kuljetuskerros	Kuljetuskerros
Verkkokerros	Verkkokerros
Siirto- ja fyysinen kerros	Siirtokerros
	Fyysinen kerros

2.6 Verkkoprotokollat

Jokaisella verkon tasolla on siis omat ”liikennesääntönsä”, eli verkkoprotokollat. Näitä protokollia säätää ja hallinnoi IETF-organisaatio. Protokollat määritellään RFC (Request for Comment) -dokumentissa, joiden historia ulottuu Internetiä edeltävään Arpanetin aikaan 60- ja 70 luvuille. Nimensä mukaisesti ensimmäiset RFC-dokumentit olivat tyyliltään vapaamuotoisia ja niiden tarkoitus oli esitellä ideoita ja herättää keskustelua, ei niinkään julistaa tietty protokolla säännöksi.

IETF määrittelee jokaiselle RFC:lle luokituksen. Kun RFC-dokumentti ensi kerran julkaistaan, se luokitellaan informational-kategoriaan. Informational-luokituksen saaneet dokumentit ovat standardoimisen alussa, eivätkä välttämättä pääse koskaan eteenpäin prosessissa. Tähän luokkaan kuuluvat myös aprillipiloina julkaistut RFC-dokumentit, kuten RFC 7511, jossa kuvaillaan, miten paketit voisivat liikkua maisemareittejä pitkin tietoverkossa.

RFC-dokumentti voi nousta experimental-luokitukseen, joka tarkoittaa, että protokollan toimivuudesta ja suosiosta ei voida olla varmoja. Mikäli jokin ehdotus saa tarpeeksi suosiota ja se osoittautuu toimivaksi, IETF voi määrittää sen standardiksi tai suositelluksi tavaksi. RFC-dokumentti kuitenkin säilyttää numeronsa vielä standardoimisen jälkeen ja ne ovat kaikille avoimina tarkastelua varten. Esimerkkinä mainittakoon TCP-protokolla, joka on määritelty RFC-793 dokumentissa (Crocker 2009).

3 VERKONHALLINTA

Lähiverkkojen määrä ja laajuus ovat kasvaneet viime vuosina suuresti. Monesti yritysten ja organisaatioiden toimintakyky riippuu lähiverkosta. Siksi onkin erittäin tärkeää, että verkko on saavutettavissa ja käyttökatkokset ovat mahdollisimman harvinaisia ja lyhyitä. (Puska 2000, 306.)

Verkonhallinnan osa-alueet on määritelty ITU-T:n TMN-protokollamallissa. Tässä yhteydessä puhutaan usein FCAPS-mallissa, joka on lyhenne sanoista Vika (Fault), Määrittely (Configuration), Laskutus (Accounting), Suorituskyky (Performance) ja Turvallisuus (Security). (ITU-T M.3400)

Tämä määrittely kattaa kaikki verkot: niin puhelinverkot kuin tietoliikenneverkotkin. Verkonhallinnan osa-alueilla painotetaan eri asioita, puhelinverkossa laskutuksen hallinnalla on suuri osa, tietoliikenneverkossa ei niinkään. (Puska 2000, 307.) Kaikki verkonkäyttö tietenkin maksaa, joten laskutuksen hallinnan tärkeys määräytyy sen mukaan, laskutetaanko verkon käytöstä esimerkiksi datan tai ajan mukaan, vai ovatko maksut aina samat kiinteät. Laskutuksen hallinta onkin kaikista tärkeintä verkko-operaattoreille. Datan lisäksi laskutuksen hallinnalla voidaan tarkkailla myös muita käyttäjän kuluttamia resursseja. Esimerkiksi useat pilvipalvelut laskuttavat virtuaalikoneista käytön mukaan, eli sen mukaan kuinka pitkään virtuaalikone on ollut päällä, kuinka paljon se on käyttänyt levytilaa jne. FCAPS-mallin A-kirjain voi myös tarkoittaa hallintaa (administration), joka sisältää esimerkiksi käyttöoikeuksien hallinnan.

Vikatilanteiden hallinnassa pyritään havaitsemaan ja ilmoittamaan vikatilanteista mahdollisimman nopeasti ja ennen kuin vika aiheuttaa käyttökatkosta verkkoon tai näkyy verkon käyttäjälle (Puska 2000, 306). Määrittelyn hallinnassa seurataan verkon määrittelytietoja ja kokoonpanoja. Usein tässä yhteydessä puhutaan myös muutoksen hallinnasta, jolla tarkoitetaan verkon määritysten muutoksia. Se käsittää niin fyysiset kuin loogisetkin oliot. (Jaakkohuhta 2005, 310.)

Suorituskyvyn hallinta seuraa verkon kapasiteettia ja kuormitusta. Sen avulla voidaan havaita mahdolliset pullonkaulat. Verkon suorituskyky pyritään pitämään hyväksyttävällä tasolla. (Puska 2000, 307.) Laskutuksen hallinnalla seurataan verkon käyttöä, jotta sen käyttäjiä voidaan tarpeen vaatiessa laskuttaa käytön mukaan, tai mahdollisesti asettaa käyttökattoja. (Puska 2000, 307.)

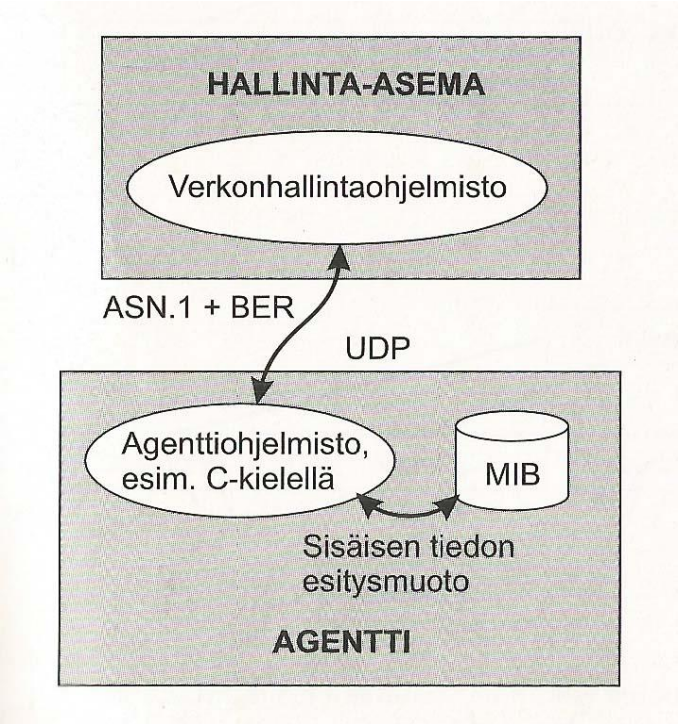
Turvallisuuden hallinta valvoo käyttäjäoikeuksia, sitä kenellä on pääsy mihinkin laitteisiin ja tietoihin. Suurin osa turvallisuuden hallinnasta koostuu lokitietojen keräämisestä ja analysoinnista. Näin mahdolliset oikeusrikkomukset saadaan esille. Turvallisuuden hallinta määritellään yrityksen turvallisuuspolitiikassa. (Jaakkohuhta 2005, 311.)

3.1 SNMP-hallintaprotokollat

Verkon hallinnassa käytetyin protokolla on SNMP, Simple Network Management Protocol. Se toimii TCP/IP-mallin sovelluskerroksella. (Jaakkohuhta 2005, 312.) SNMP:n historia alkaa vuodesta 1988 ja ajan mittaan siitä on julkaistu useita versioita. Kuten muutkin protokollat, SNMP on määritelty RFC-dokumenteissa. Ensimmäinen versio SNMPv1 on vuodelta 1990 ja se on määritelty RFC-dokumenteissa 1065-67. SNMPv2 on vuodelta 1993 ja se on määritelty RFC-dokumenteissa 1441-1450 ja 1452. Tuorein versio, SNMPv3 on vuodelta 2002, jonka määritykset ovat RFC-dokumenteissa 3411-18. IETF on luokitellut SNMPv3-protokollan standardiksi, joka korvaa sen edeltävät versiot SNMPv1 ja SNMPv2. (RFC Search Detail: Standards Track snmpv2 RFCs 2016.)

Yksinkertaisuudessaan SNMP-käyttöympäristö koostuu hallinta-asemasta, hallittavista laitteista ja näissä olevista tietokannoista. Hallinta-asema lähettää hallittavalle laitteelle kyselyn, johon vastaa hallittavassa laitteessa sijaitseva agentti. Hallittava laite säilyttää hallittavia tietoja pienessä tietokannassa, MIB:ssä. MIB:in tietorakenne noudattaa SMI-määrittelyä, jotta tiedon rakenne ja tiedon tunnistaminen olisi mahdollista. (Kaario 2002, 270.) MIB sisältää objekteja, jotka keräävät tietoa esimerkiksi lähetettyjen ja vastaanotettujen pakettien määrästä. Objektit säilyttävät näitä tietoja ja hallittavalla laitteella oleva agentti lähettää ne hallinta-asemalle. (Kuva 5.)

Jotta SNMP:n kautta kulkevat viestit voidaan tulkita oikein, MIB-tietokannat on kuvattu samalla kielellä, ASN.1-kielellä. ASN.1-kielellä kuvatut muuttujat ja tietorakenteet koodataan edelleen binäärimuotoisiksi käyttämällä BER-koodaussääntöjä. (Kaario 2002, 280.)



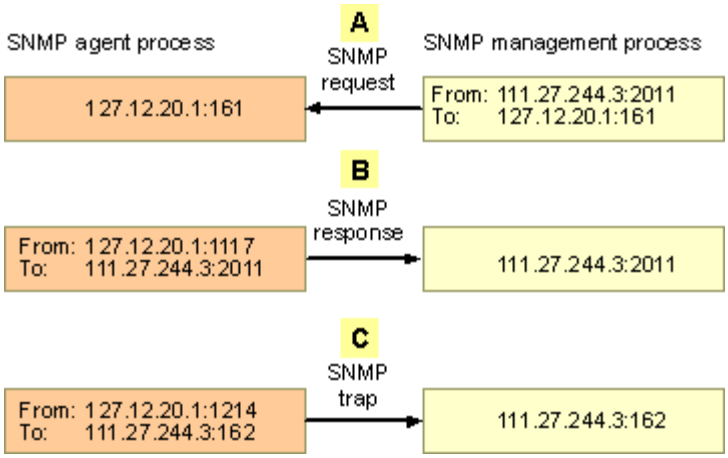
Kuva 5. SNMP -protokollan toiminta (Kaario 2002, 273).

3.2 SNMP-sanomat

SNMP on pyyntö/vastausprotokolla joka toimii UDP-protokollan päällä, joten se toimii ruuhkaisessakin verkossa. Yksinkertaistettuna SNMP käyttää kolmenlaisia operaatioita kyselyihin ja vastauksiin: Get, Set ja Trap. Get-operaatiolla hallinta-asema pyytää agentilta tietyn objektin arvon. (Puska 2000, 311.)

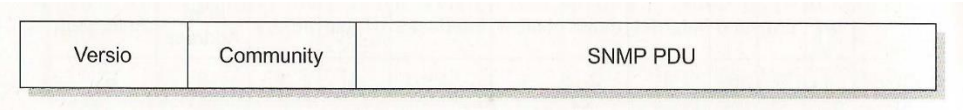
Get-operaatiota on kolmea eri tyyppiä: Get Request, jolla hallinta-asema pyytää MIB-tietokannasta muuttujan arvoa, Get Next Request, jolla hallinta-asema pyytää taulukon seuraavaa muuttujaa ja, SNMP v2 -versiosta eteenpäin, Get Bulk Request, jolla voidaan kerralla kysellä useamman muuttujan arvoa. (Kaario 2002, 277.) Set Request -operaatiolla hallinta-asema voi asettaa muuttujalle tietyn arvon (Puska 2000, 311). Kyselyissä käytetään usein ajastimia, koska ei ole mielekästä lähettää kyselyjä koko ajan.

Hallittavan laitteen agentti vastaa näihin pyyntöihin Get Response -operaatioilla tai uudemmissa SNMP-versioissa Response-operaatioilla. Agentti voi myös tarvittaessa lähettää itsenäisesti ilman kyselyä hallinta-asemalle Trap-sanoman. Trap-sanomaan liittyy yleensä tietyn raja-arvon ylittyminen ja hälytyksen aktivoiminen, esimerkiksi PC-laitteen levytilan ollessa lopussa. (Kaario 2002, 278.) Tätä viestiketjua havainnollistaa kuva 6.



Kuva 6. SNMP -operaatiot. Vasemmalla hallittava laite ja oikealla hallinta-asema. (Microsoft, 2006.)

SNMP-kehys (kuva 7) koostuu käytettävästä SNMP-versiosta, community-kentästä sekä itse viestistä. Community kenttää voidaan käyttää eräänlaisena suojauksena; hallittavan laitteen agentti vastaa vain sovittuun community-kentän arvoon. SNMPv2-toteuteksessa kentän arvo on oletuksena public, joten agentti vastaa vain SNMP-viesteihin, joiden community-kentän arvo on public. SNMP versiosta kolme lähtien community-tunnus lähetetään kryptattuna, eikä selväkielisenä kuten edellisissä versioissa.



Kuva 7. SNMP-kehyksen rakenne (Kaario 2002, 278)

Kaupungin tapauksessa tietokoneelle asennettu järjestelmä lähetti Get Request -pyynnön laitteille, johon laitteet vastasivat Get Response -operaatiolla. SNMP-sanomien lisäksi verkonhallintajärjestelmät käyttävät muita sovellustason protokollia. Usein SNMP:n lisäksi saatetaan lähettää esimerkiksi ICMP-viesti. Useista laitteista ICMP-sanomiin vastaaminen on kuitenkin poistettu käytöstä, joten pelkkä ICMP ei tarjoaisi luotettavaa verkonhallintaa. Toisaalta myös SNMP voidaan kytkeä laitteesta pois päältä, vaikka tämä onkin harvinaisempaa.

4 CASE: AKAAN KAUPUNKI

Akaan kaupungin tietohallinnolla on tiivis yhteistyö Valkeakosken kaupungin tietohallinnon kanssa. Valkeakosken kaupunki vastaa kuntien tietoverkkojen ylläpidosta ja työasemien hankinnoista. Yhteistyön avulla on volyymimääriä saatu kasvatettua ja kustannuksia laskettua.

Kaupungilla oli toiveena saada käyttöönsä järjestelmä, joka ilmoittaisi häiriöistä ja vioista ennen kuin ne aiheuttavat suurempaa häiriötä kaupungin hallinnolliselle toiminnalle. Järjestelmän käyttö rajoitettaisiin kytkinten sekä UPSien hallintaan, koska kaupunki on itse vastuussa niistä. Järjestelmän avulla tulisi pystyä tunnistamaan vähäpätöiset häiriöt, jotka pystyttäisiin ratkaisemaan jopa käyttäjätasolla. Esimerkkinä tällaisesta häiriöstä mainittakoon UPSista irronnut virtajohto, jonka kuka tahansa pystyy kytkemään takaisin.

Aika ajoin verkon määrityksiä täytyy myös muuttaa. Yleisimpänä muutoskohteena ovat VLAN-määritykset, joita tarvitsee vaihtaa esimerkiksi työntekijän toimipaikan vaihdon yhteydessä.

Verkonhallinnan osa-alueista tässä työssä keskitytään siis vian hallintaan ja kokoonpanon hallintaan. Työssä ei haluttu kuitenkaan valita liian suurta järjestelmää, jonka ylläpito olisi tullut kalliiksi. Ensisijaisina kriteereinä olivat hälytykset, jotka välitettäisiin sähköpostiin sekä hallintapaneeli, josta näkisi yleiskatsauksen laitteen tilasta.

Kaupungin toiveena oli asentaa järjestelmä tavalliselle työasemalle, eikä palvelimelle. Palvelimen hankintaan olisi tarvittu verkkoa hallitsevan Valkeakosken hyväksyntä, joten työssä etsittiin järjestelmiä, jotka toimivat Windows 7 -käyttöjärjestelmässä. Tämä vaatimus rajasi paljon ohjelmia pois. Järjestelmät asennettiin tietokoneelle, joka omistettiin kokonaan verkonhallintaan. Tietokone liitettiin UPSiin, jotta se pysyisi aina päällä, eivätkä trap-sanomat jäisi saamatta. Järjestelmien testikäytön jälkeen tehtiin valinta hankittavasta järjestelmästä.

5 TESTATTAVAT JÄRJESTELMÄT

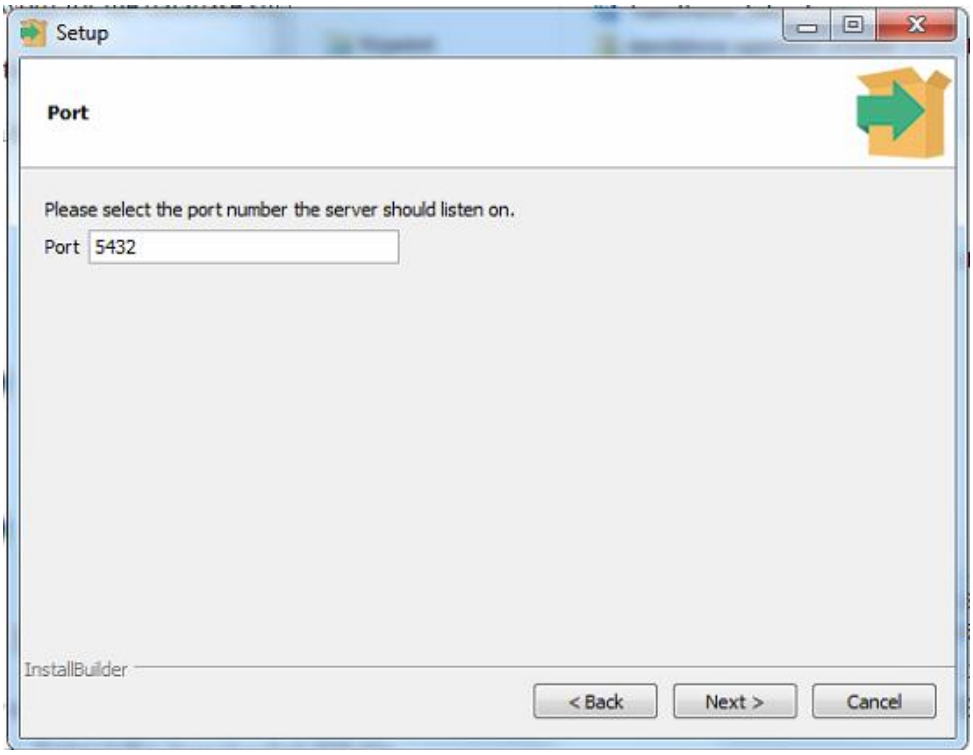
Työssä oli päämääränä hallita noin 100 laitteen verkkoa ja pääasiassa verkon kytkimiä. Järjestelmien oli toimittava työasemalla sekä tuettava Windows 7 –käyttöjärjestelmää. Järjestelmän vaatimusten perusteella valittiin kaksi järjestelmää testattaviksi: OpenNMS sekä Lansweeper.

5.1 OpenNMS

OpenNMS on avoimen lähdekoodin verkonhallintaohjelma. Avoimuutensa vuoksi, sen käyttäminen on ilmaista. Ilmaisuudesta huolimatta, se on suunniteltu valvomaan suuriakin verkkoja. OpenNMS-järjestelmää kehittää The OpenNMS -group sekä The Order of the Green polo -group, jotka tarjoavat myös maksullista koulutusta sekä teknistä tukea järjestelmälle.

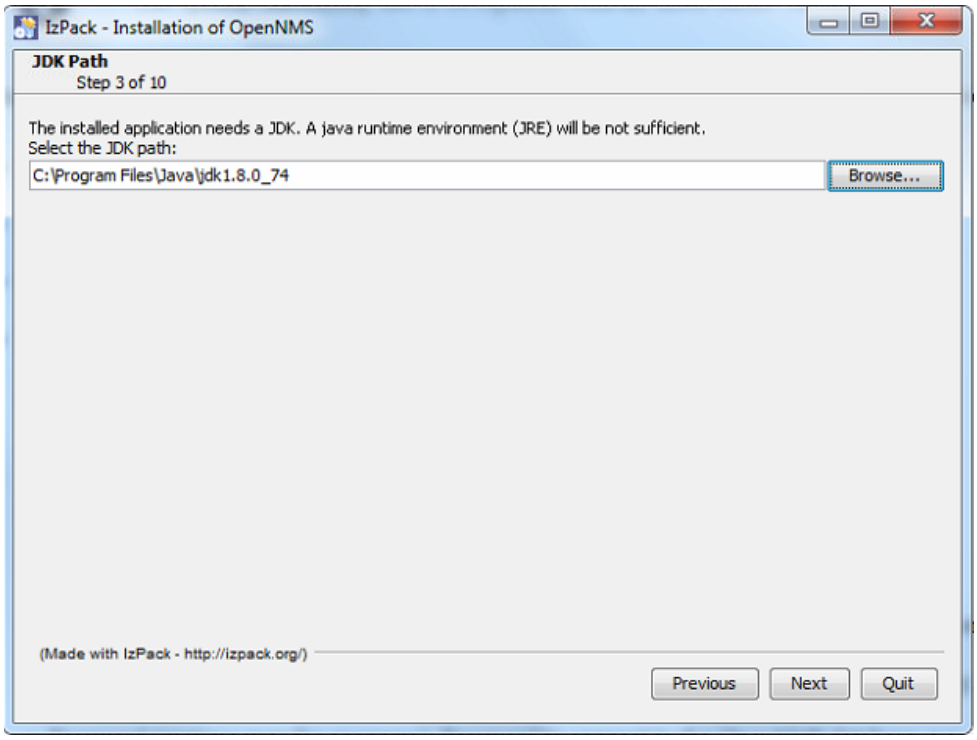
5.1.1 OpenNMS asennus

OpenNMS tukee useimpia Linux jakeluja, Windowsin palvelin- ja työasema käyttöjärjestelmiä sekä Mac OS X-käyttöjärjestelmiä. Asennus koostuu kolmesta osasta: Java Developement Kitin asennus, PostgreSQL-tietokantapalvelimen asennuksesta ja itse OpenNMS-järjestelmän asennuksesta.



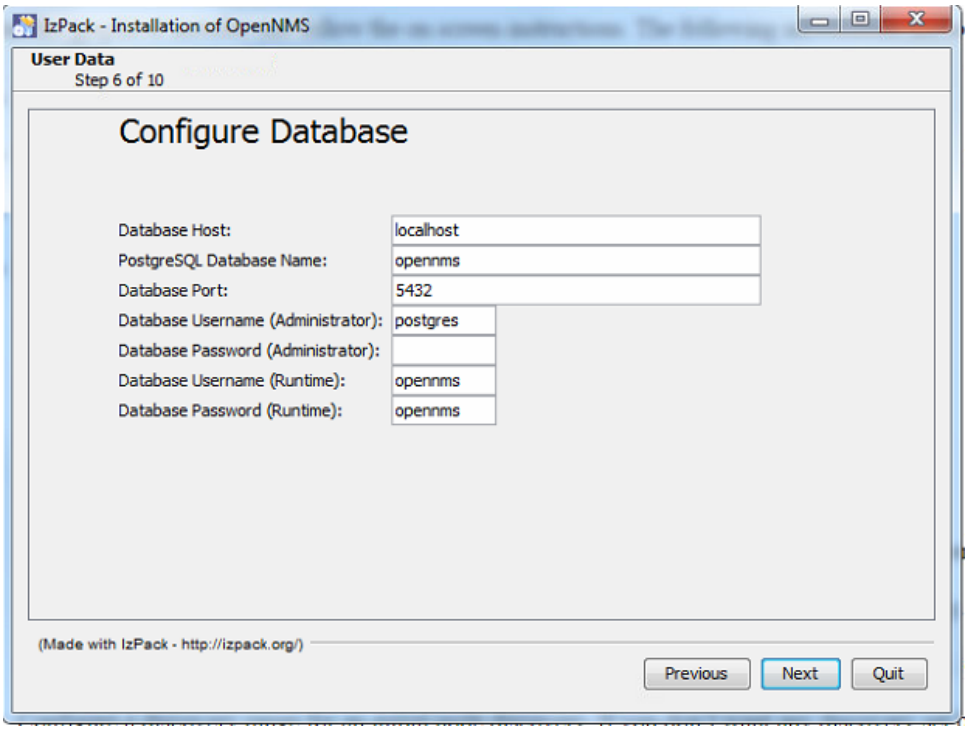
Kuva 8. Määritetään Postgresille kuunneltava portti

Postgres tarvitsee tiedot käyttäjätunnuksesta ja kuunneltavasta portista. (Kuva 8.) Asennuksen jälkeen Postgres käynnistää itsensä automaattisesti palveluna ja määrittää palvelun käynnistymään aina käynnistyksen yhteydessä.



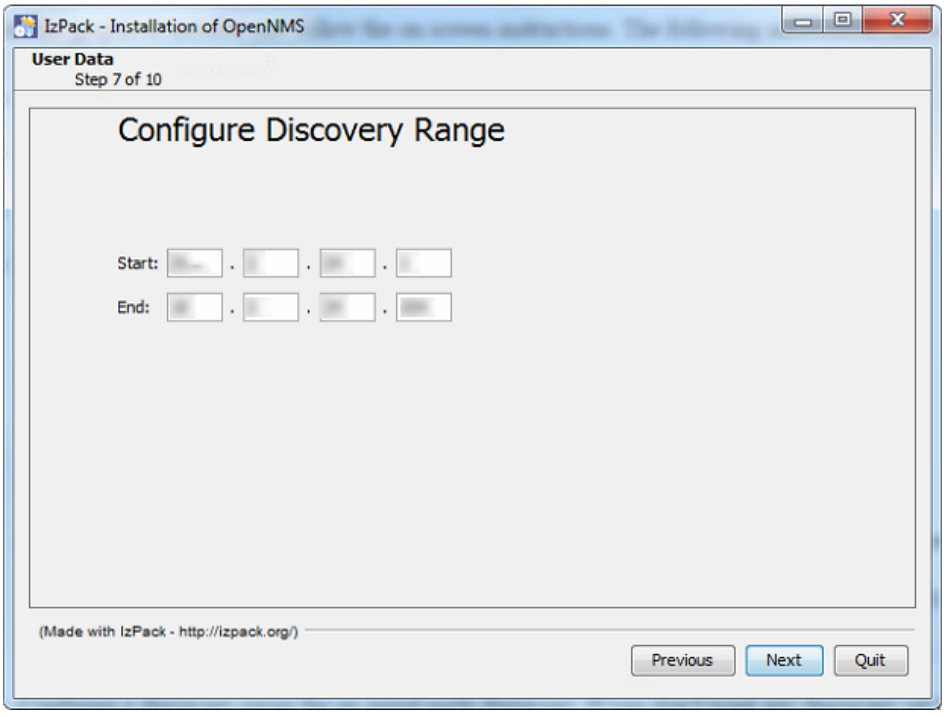
Kuva 9. Osoitetaan OpenNMS asennukselle, mistä JDK löytyy

OpenNMS-asennus onnistuu myös graafisen asennusohjelman kautta. OpenNMS tarvitsee asennukseen tietokantapalvelimen osoitteen, nimen tietokannalle sekä käyttäjätunnukset tietokantaan ja järjestelmään. Asennusohjelmalle osoitetaan myös Java Development Kitin sijainti (kuva 9). Tässä tapauksessa tietokanta asennettiin samalle tietokoneelle kuin OpenNMS, joten osoitteeksi riittää localhost sekä portti, joka annettiin PostgreSQL-tietokannalle. (Kuva 10.) Viimeiseksi asennusohjelmalle annetaan IP-osoitealue, jolta OpenNMS alkaa automaattisesti etsimään laitteita. (Kuva 11).



Kuva 10. OpenNMS tietokantamääritykset

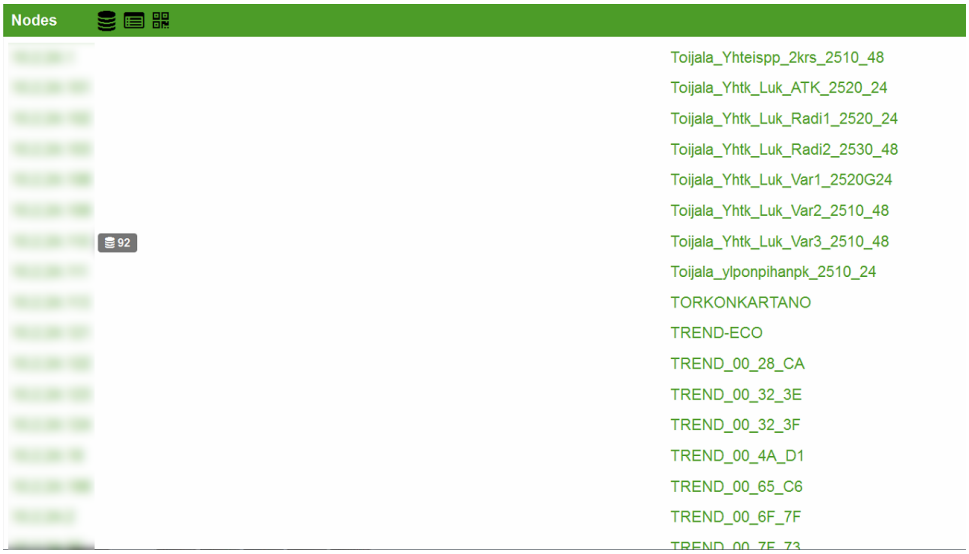
Asennuksen jälkeen järjestelmä käynnistetään ajamalla komentokehote start.bat /OpenNMS/bin-kansiosta. Tämän jälkeen järjestelmään pääsee käsiksi webkäyttöliittymän kautta, joka tässä tapauksessa on localhost:8980/OpenNMS



Kuva 11. OpenNMS etsii automaattisesti laitteet annetulta osoitealueelta

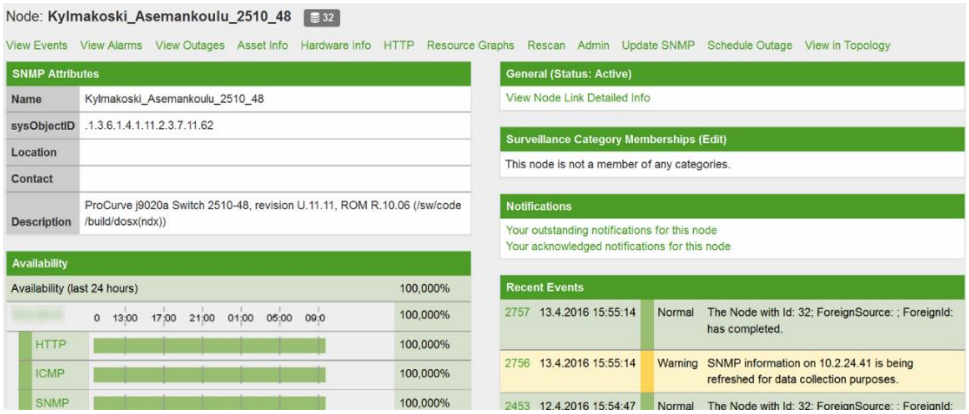
5.1.2 OpenNMS käyttö

OpenNMS ja Lansweeper sisältävät molemmat samankaltaisen aloitusnäytön, joka on muokattavissa tarpeita vastaaviksi. Oletuksena OpenNMS näyttää verkkolaitteiden lukumäärän näiden saatavuuden ja mahdolliset hälytykset.



Kuva 12. OpenNMS yleiskatsaus laitteista

OpenNMS ei näytä laitteita selkeimmällä mahdollisella tavalla, eikä OpenNMS kerro esimerkiksi laitteen tyyppiä. Laitesivulla näkyy laitteen saatavuus protokollan mukaan. Yleiskatsauksessa laitteista näkyy laitteiden nimet sekä IP-osoitteet. (Kuva 12.) Oletuksena laitteeseen ei myöskään voida muodostaa yhteyttä suoraan hallintapaneelista, paitsi http:tä käyttäen. Lansweeper ja OpenNMS molemmat näyttävät laitteen verkkoliitännät. Laitenäkymä ei siis ole yhtä selkeä kuin Lansweeper-ohjelmassa. (Kuva 13.)



Kuva 13. OpenNMS laitenäkymä

Ominaisuuksiltaan OpenNMS on helposti laajennettavissa. Avoimen lähdekoodinsa takia, sille on kehitetty paljon lisäosia. Esimerkiksi asennettaessa OpenNMS-ohjelma palvelinalustalle, voidaan ottaa käyttöön myös mobiilisovellus, joka vastaanottaa hälytyksiä ja jolla päästään tekemään muutoksia ja korjauksia verkkoon. OpenNMS tarjoaa myös hälytysten välittämisen

sähköpostiin. Hälytykset ovat myös muokattavissa, niitä voidaan ottaa pois käytöstä ja valikoida sähköpostiin päätyvät hälytykset.

Suurin osa OpenNMS-ohjeista on wiki-muotoisissa verkkosivustoissa. Koska OpenNMS on hyvin monikäyttöinen ja monipuolinen ohjelma, se ei tarjoa yhtä ainoaa asennusohjeistusta, vaan jokaisella alustalle on omat ohjeensa. Tästä syystä, ohjelman ylläpito ja päivittäminen vaatii enemmän aikaa, kuin kaupalliset vaihtoehdot.

5.2 Lansweeper

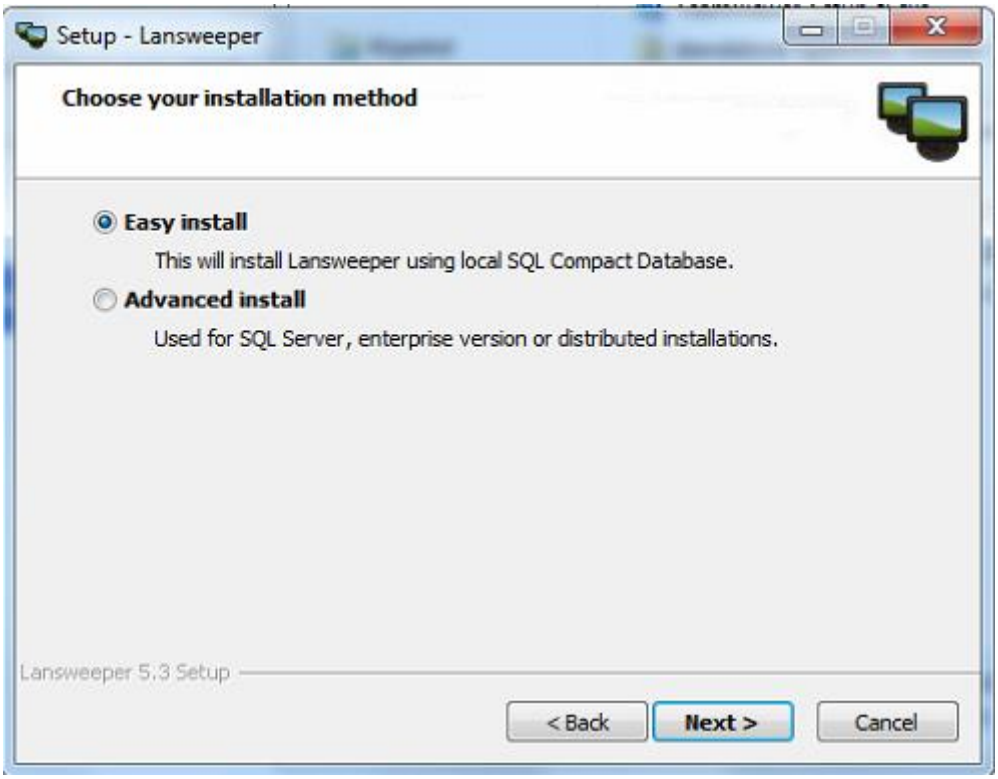
Lansweeper on kaupallinen, Hemoco-yhtiön kehittämä ja ylläpitämä verkonhallintajärjestelmä (Contact N.d). Järjestelmän perusversio sisältää tärkeimmät ominaisuudet verkonhallinnan kannalta, kuten hälytysten lähetyksen sähköpostiin sekä päätelaitteiden skannauksen. Kalliimmat lisenssit sisältävät esimerkiksi mahdollisuuden hallita Vmware ja Hyper-V pohjaisia virtuaalikoneita sekä asentaa keskitetysti ohjelmia työasemiin.

Järjestelmästä tarjotaan myös freeware-versiota, jonka ominaisuuksia ja laitemäärää on kuitenkin rajoitettu. (Freeware and trial limitations N.d). Järjestelmän hinnoittelu määräytyy hallittavien laitteiden määrän sekä ominaisuuksien mukaan. (Kuva 14.)

Kuva 14. Lansweeper hinnoittelu

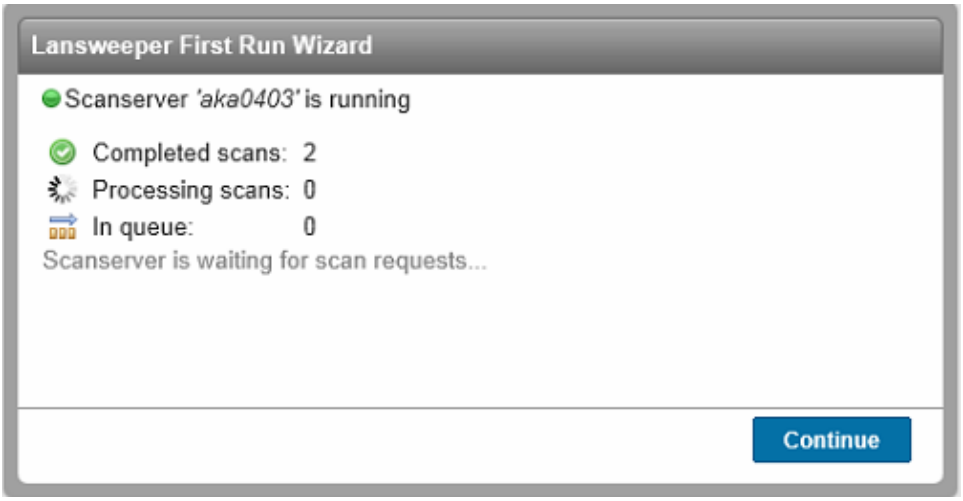
5.2.1 Lansweeper asennus

Lansweeperin asennus on hyvin suoraviivainen ja yksinkertainen. Asennusohjelma osaa asentaa tietokannan itsestään, mutta tarvittaessa tietokannan voi määritellä manuaalisesti, esimerkiksi toiselle palvelimelle. (Kuva 15.) Hallintapaneeli asennetaan käyttämään oletuksena portteja 81 ja 82.



Kuva 15. Lansweeper tietokannan asennus

Lansweeper osaa automaattisesti skannata verkkoa, annetun osoitealueen perusteella. (Kuva 16.) Windows-työasemien sekä Linux- ja Mac –laitteiden skannaus vaatii käyttäjätunnuksien käyttöä. SNMP-laitteille voidaan määritellä myös salaus käyttämällä SNMP-community nimeä.



Kuva 16. Lansweeper skannaa verkkoa

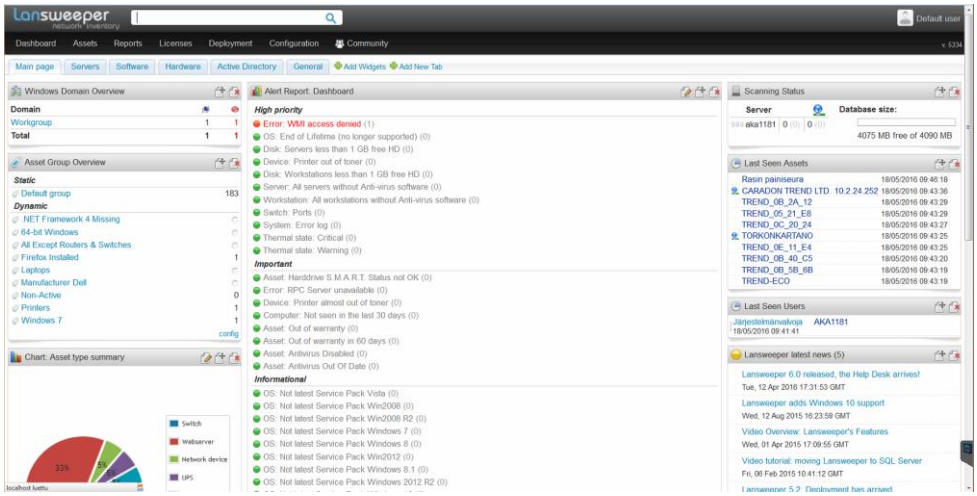
Tarvittaessa Lansweeperin laitetietokantaan voidaan syöttää myös manuaalisesti tietoja. Tämä tapahtuu helposti lataamalla mallipohja hallintapaneelista. Mallipohjaan syötetään tarvittavat tiedot Excel-taulukossa, jonka jälkeen se tallennetaan csv-muotoiseksi ja ajetaan tietokantaan. (Kuva 17.)

Domain	IPAddress	OScode	SP	Description	Assettype	AssetName
	[illegible]			Asemanraitti 168	Switch	Aseman koulu - Kivikoulu
	[illegible]			Asemanraitti 168	Switch	Aseman koulu - Puukoulu

Kuva 17. Tietokantaan voi manuaalisesti syöttää laitteiden tietoja

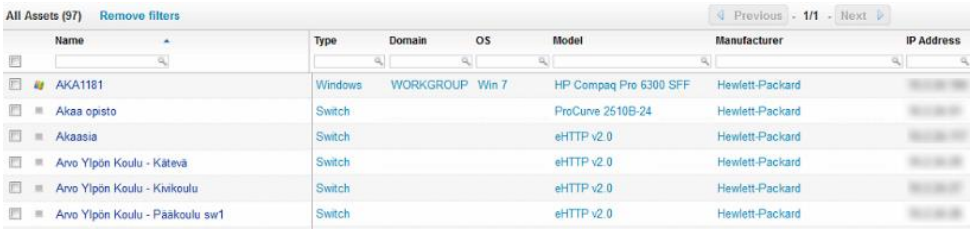
5.2.2 Lansweeperin käyttö

Lansweeperin oletusnäkymä tarjoaa hyvän yleiskatsauksen verkkoon. Tämä aloitusnäkymä on täysin muokattavissa tarpeiden mukaan. Dashboard-näkymään voidaan tuoda hälytykset, kaavio verkon laitteiden tyypeistä ja valmistajista sekä viimeksi skannatuista laitteista. (Kuva 18.)



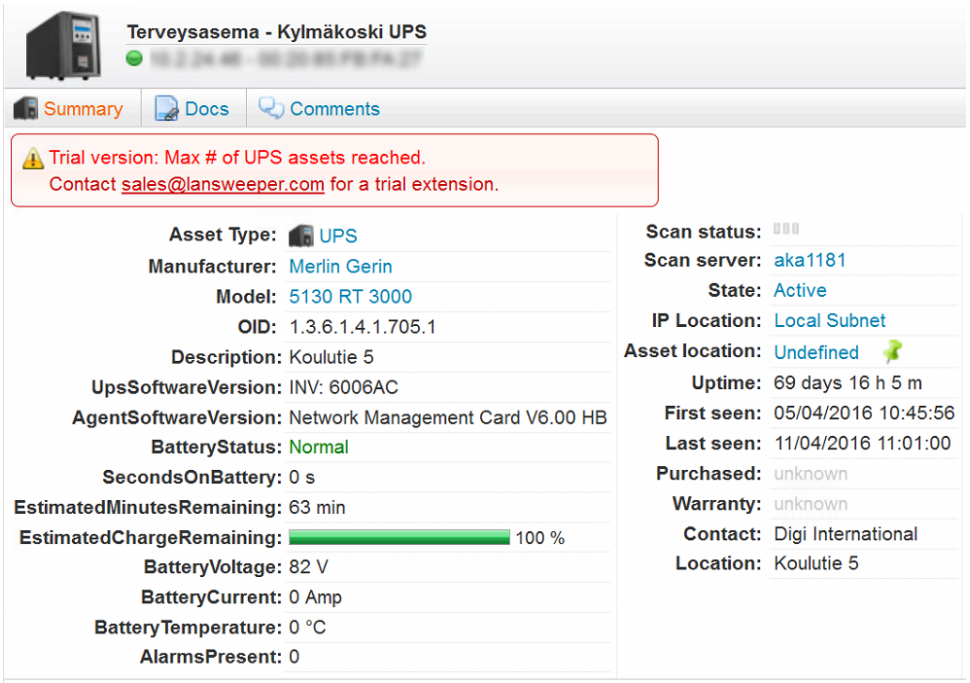
Kuva 18. Lansweeper dashboard

Lansweeper on suunniteltu etupäässä hallitsemaan työasemia, tulostimia ja palvelimia. Ohjelman kautta voidaan levittää ohjelmistoja sekä jakamaan lisenssejä. Kaupungin tapauksessa tällaiset ominaisuudet eivät kuitenkaan ole ensiarvoisen tärkeitä, vaan pääasiallinen tarkoitus oli tarkkailla kytkimiä ja UPSeja. Lansweeper tarjoaa yleisnäkymän kaikista verkon laitteista, jossa näkyy laitteiden IP-osoite, fyysinen osoite, valmistaja sekä aika, jona laite on viimeksi skannattu. (Kuva 19.)



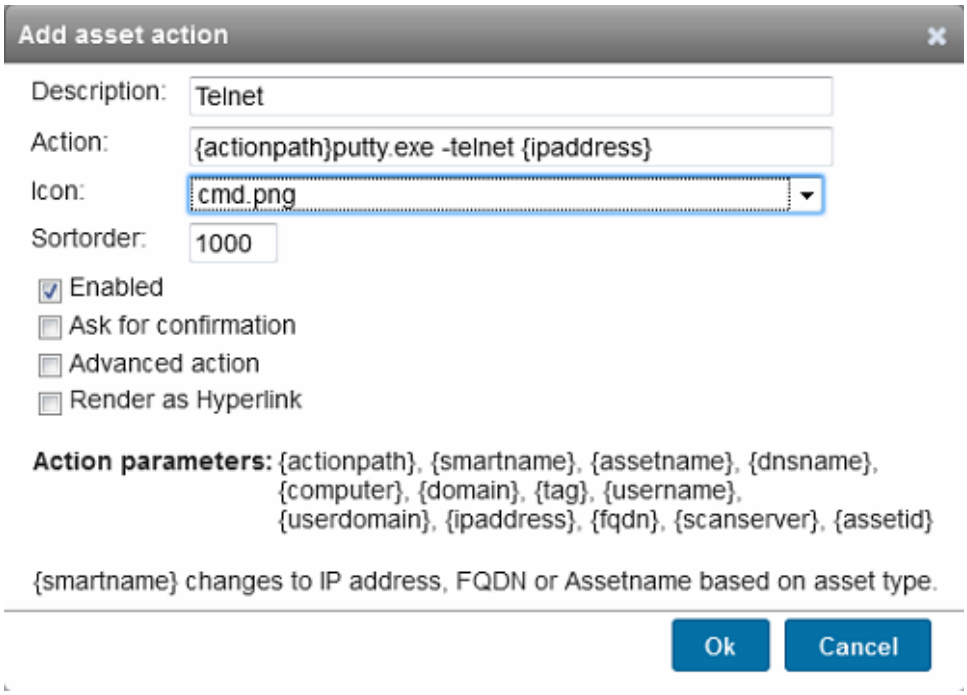
Kuva 19. Asset näkymä

Verkon laitteilla on omat sivunsa, josta näkee laitekohtaisia tietoja. Kytkinten kohdalla tämä tarkoittaa muun muassa verkkoliitäntöjä ja VLAN-määrityksiä. Kuvassa 20 UPS-laitteen kohdalla taas näkyy muun muassa akun varaustaso ja kunto.



Kuva 20. UPS-laitteen sivu

Laitesivulla voidaan myös suorittaa erilaisia toimintoja laitteelle, kuten muodosta SSH-yhteys, lähettää ping tai muodostaa etätyöpöytäyhteys. Toimintoja voidaan myös itse lisätä, poistaa tai muokata. Tässä työssä lisättiin telnet–pikanäppäin toimintoihin. (Kuva 21.)



Kuva 21. Lansweeper toiminnon lisäys

5.3 Järjestelmien erot

Molemmat järjestelmät osoittautuivat erittäin käytännöllisiksi ja hyödyllisiksi. OpenNMS tarjoaa paljon erilaisia ominaisuuksia, kustomointia ja sen takana on vahva yhteisö, jonka puoleen voi kääntyä ongelma-asioissa. OpenNMS vaatii kuitenkin enemmän perehtymistä ja konfigurointia, kuin esimerkiksi Lansweeper. OpenNMS ei myöskään ole kovinkaan käyttäjäystävällinen eikä sen käyttöliittymä ole selkeimmästä päästä. Suurin osa asetuksista tehdään muokkaamalla suoraan config-tiedostoa. Tämän lisäksi OpenNMS pitää oletuksena käynnistää komentojonolla. Vaikka tämän saa automatisoitua ja tarvittaessa OpenNMS voidaan myös suorittaa Windows-palveluna, vaatii ohjelman peruskäyttö huomattavasti enemmän perehtymistä, kuin Lansweeperin käyttö.

Lansweeperin käyttäminen ja käyttöönotto sujuivat helposti. Ohjelma tarjoaa oletuksena kokeiluversiota, jossa laitteiden määrä on rajoitettu. Tämän kokeilun puitteissa pystyy helposti testaamaan, onko järjestelmä tarkoitukseen sopiva vai ei. Lansweeperin asennus on oletuksena hyvin yksinkertainen. Asennusohjelma asentaa automaattisesti tarvittavan tietokantapohjan ja ohjelma on heti käytettävissä. Tarvittaessa Lansweeper tarjoaa myös edistyneempää asennusvaihtoehtoa, jonka avulla voidaan määritellä esimerkiksi käytettävä tietokanta. Asennuksen yhteydessä Lansweeper kysyy myös kaikki tarvittavat tiedot, joten ohjelma on heti asennuksen jälkeen käytettävissä. Lansweeper painottaa erityisesti työasemien hallintaa.

Lansweeperillä pystytään hallinnoimaan työasemiin asennettuja ohjelmia, lisenssejä ja laitteiden takuuaikoja. Nämä ominaisuudet jäivät kuitenkin testaamatta, koska pääasialliset käyttökohteet olivat kytkimet ja UPSit. Käyttöliittymä on selkeä ja miellyttävä ja sitä saa OpenNMS-ohjelman tapaan

muokattua haluamansa näköiseksi. Lansweeperin lisenssimaksut eivät ole korkeimmasta päästä, monien muiden verkonhallintajärjestelmien lisenssihinnat ovat huomattavasti kalliimmat. Lansweeperistä on tarjolla myös freeware-versio. Lansweeper tarjoaa myös hälytysten lähettämistä sähköpostiin. Näiden ja muiden ominaisuuksien ja asetusten löytäminen kävi helposti ja suurin osa asetuksista tehtiin suoraan käyttöliittymästä.

Lansweeperin helppokäyttöisyyden takia valittiin se käyttöönotettavaksi järjestelmäksi. OpenNMS on erittäin monipuolinen ja muokattavissa tarpeita vaativaksi, mutta sen käyttäminen vaatii liikaa aikaa ja resursseja. OpenNMS tarjoaa ehkä hieman liikaa ominaisuuksia. Verkonhallintajärjestelmän tarkoituksena oli vapauttaa työaikaa ja ennaltaehkäistä virhetilanteita sekä tarjota yleiskatsaus verkon laitteista ja niiden tilasta. OpenNMS teki nämä kaikki, mutta Lansweeperin käyttäjäystävällisyys teki siitä paremman vaihtoehdon. Mikäli verkonhallinnan tarpeet kuitenkin muuttuvat, täytyy myös järjestelmän valintaa tarkastella uudestaan.

6 YHTEENVETO

Työn lopuksi päätettiin hankkia lisenssi Lansweeper-ohjelmistoon. Valintaa puolsivat ohjelman käyttäjäystävällisyys ja selkeys. Ohjelman lisenssi oli myös huomattavasti halvempi verrattuna muihin järjestelmiin. Lisenssi ostettiin yhdeksi vuodeksi. Lisenssin umpeutuessa voidaan harkita joko lisenssin uusimista, tai jonkin vaihtoehtoisen järjestelmän käyttöönottoa, mikäli verkonhallinnan tarpeet ovat muuttuneet. Ohjelmien testikäytön jälkeen tehtiin lyhytmuotoinen vertailu ohjelmista toimeksiantajan kanssa ja perehdytettiin toimeksiantajan edustaja Lansweeper-järjestelmän käyttöön ja ominaisuuksiin. Lansweeperiä pidettiin erittäin sopivana järjestelmänä verkonhallintaan, jollaista kaupungilla ei entuudestaan ole ollut.

Lähiverkoista löytyi paljon erilaista kirjallisuutta, joista saatiin paljon tietoa työhön. Vaikka osa kirjoista oli vanhoja, eivät perusasiat olleet muuttuneet. Verkossa julkaistujen uutisten ja artikkelien avulla pystyttiin täydentämään työtä viimeisimmillä ilmiöillä ja tiedoilla.

Työssä käytiin läpi verkonhallinnan osa-alueet sekä tunnetuimman verkonhallintaprotokolla SNMP. SNMP:stä löytyi myös yleistä tietoa suomeksi lähiverkkoja käsittelevistä kirjoista. Kirjoista löytyvää aineistoa täydennettiin internetistä kerätyn tiedon avulla. Työssä käsiteltiin verkonhallinnan perusteita, eikä siksi syvennytty esimerkiksi ASN.1-kieleen, joka liittyy vahvasti SNMP:hen ja siten verkonhallintaan. Työ ei myöskään käynyt sen enempää läpi MIB-tietokannan rakennetta, joka olisi ollut liian syventävää tietoa opinnäytetyön laajuutta ajatellen. Työssä kuitenkin käydään läpi, minkälaisia protokollia verkonhallinnassa käytetään ja miten ne toimivat.

Projektille oli toimeksiantajan puolesta määritelty selvästi, mitä verkonhallintajärjestelmältä halutaan. Verkonhallinnassa keskityttiin UPS-laitteisiin ja kytkimiin. Lisäksi järjestelmän tulisi toimia Windows 7 –käyttöjärjestelmässä. Näiden vaatimusten perusteella valikoitiin testattavaksi Lansweeper- ja OpenNMS-järjestelmän. Näiden kahden järjestelmän erot olivat hyvin selvät ja melko varhain Lansweeper osoittautui paremmin tarpeisiin sopivaksi järjestelmäksi. Käytännön osuudessa käytiin läpi, kuinka lähiverkon laitteita voidaan hallita esimerkiksi SSH- ja telnet-yhteyksillä. Hälytyksiä laitteiden tilasta voidaan lähettää järjestelmästä suoraan sähköpostiin, mikäli palomuuri sallii liikenteen.

Työ opetti paljon verkonhallinnasta. Samalla kun työ perehtyi verkonhallintaan, kerrattiin myös tietoliikenneverkkojen perusteita. Näiden johdosta työ kehitti myös itsevarmuutta, kun projekti onnistui. Projekti oli ensimmäisiä oikeaan työelämään tehtyjä projekteja. Toimeksiantaja, Akaan kaupungin tietohallinto, antoi melko vapaat kädet työssä, mutta tarvittaessa saatiin myös kommentteja järjestelmään liittyen. Työn yhteydessä selvisi, millaista työskentely julkishallinnon alalla on, ja mitä siihen sisältyy tietohallinnon näkökannalta.

Työstä jäi Akaan kaupungin tietohallinnolle käytettäväksi Lansweeper-verkonhallintajärjestelmä. Projektissa päästiin hyvin tavoitteisiin, jotka olivat

kytkinten etähallinta ja hälytysten valvonta. Toimeksiantaja oli tyytyväinen valittuun järjestelmään. Alkuperäisten tavoitteiden täyttyessä, suunniteltiin toimeksiantajan kanssa myös tulevaisuutta. Järjestelmään suunniteltiin esimerkiksi työasemien ja valvontakameroiden liittämistä. Niiden liittämistä ei kuitenkaan sisällytetty tähän opinnäytetyöhön. Tulevaisuudessa kaupunki tarvitsee mahdollisesti apua järjestelmän ylläpidossa ja laajentamisessa.

LÄHTEET

Contact. Lansweeper. N.d. Viitattu 27.4.2016. Saatavilla http://www.lansweeper.com/contact.aspx

Crocker, D. 2009. How the Internet Got Its Rules. New York Times. Julkaistu 6.4.2016. Viitattu 26.2.2016. Saatavilla http://www.nytimes.com/2009/04/07/opinion/07crocker.html?_r=2&em

Dahl, P. 2015. Merikaapelin lasku Itämereen alkaa – tietoliikenneyhteydet Manner-Eurooppaan nopeutuvat huomattavasti. Yle Uutiset. Julkaistu 12.10.2015. Viitattu 23.2.2016. Saatavilla http://yle.fi/uutiset/merikaapelin_lasku_itamereen_alkaa__tietoliikenneyhteydet_manner-eurooppaan_nopeutuvat_huomattavasti/8373334

Fiveash, K. 2014. IPv4 address now exhausted in Latin America and the Caribbean. The Register. Julkaistu 11.6.2014. Viitattu 21.4.2016. Saatavilla http://www.theregister.co.uk/2014/06/11/IPv4_addresses_depleted_in_latin_america_and_the_caribbean/

Freeware and trial limitations. Lansweeper. N.d.. Viitattu 27.4.2016. Saatavilla http://www.lansweeper.com/kb/154/freeware-and-trial-limitations.html

Google. n.d. IPv6 Adoption. Viitattu 26.4.2016. Saatavilla https://www.google.com/intl/en/IPv6/statistics.html.

Hogg,S. 2015. ARIN Finally Runs Out of IPv4 Addresses. Network World. Julkaistu 22.9.2015. Viitattu 21.4.2016. Saatavilla http://www.networkworld.com/article/2985340/IPv6/arin-finally-runs-out-of-IPv4-addresses.html

IETF, 2015. RFC 7511 Viitattu 26.4.2016 Saatavilla https://tools.ietf.org/html/rfc7511

IPv4 Statistics. N.d. Afrinic. Viitattu 21.4.2016. Saatavilla http://afrinic.net/en/services/statistics/IPv4-exhaustion

IPV6 is the new normal. The Internet Society. N.d. Viitattu 26.4.2016. Saatavilla http://www.worldIPv6launch.org/

ITU-T M.3400. 2001. ITU-T. Viitattu 20.5.2016. Saatavilla https://www.itu.int/rec/T-REC-M.3400-200002-I/en

Jaakkohuhta, H. 2005. Lähiverkot – Ethernet. Helsinki: Edita.

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo.

Korhonen, S. 2011. Vanhat IP-osoitteet loppuivat Aasiassa. Tietoviikko. Julkaistu 18.4.2011. Viitattu 21.4.2016. Saatavilla http://www.tivi.fi/Arkisto/2011-04-18/Vanhat-IP-osoitteet-loppuivat-Aasiassa-3184170.html

Microsoft, 2006. SNMP Operations (Windows CE 5.0). Viitattu 27.4.2016. Saatavilla https://msdn.microsoft.com/en-us/library/ms894624.aspx.

Mobiililaajakaistan IP-osoitteet – NAT tai Julkinen IP-osoite. N.d. Elisa. Viitattu 21.4.2016. Saatavilla http://elisa.fi/asiakaspalvelu/aihe/mobiililaajakaista/ohje/IP-osoitteet/

Odom, W. 2005. Tietoverkot. Helsinki: Edita
.
Puska, M. 2000. Lähiverkkojen tekniikka – Pro Training. Helsinki: Satku – Kauppakaari.

RFC Search Detail: Standards Track snmpv2 RFCs. IETF. 2016. Viitattu 10.3.2016. Saatavilla http://www.rfc-editor.org/search/rfc_search_detail.php?pubstatus%5b%5d=Standards+Track&std_trk=Any&pub_date_type=any&wg_acronym=snmpv2

RFC-1918. 1996. IETF. Viitattu 20.5.2016. Saatavilla https://tools.ietf.org/html/rfc1918#page-4

Submarine Cable Map. 2016. Primetrica. Viitattu 23.2.2016. Saatavilla http://www.submarinecablemap.com/

Valokaista palvelukuvaus. 2016. Lounea. Viitattu 26.4.2016. Saatavissa http://lounea.fi/media/filer_public/2c/83/2c836ec1-0529-46a3-bd36-80a36186f35d/lounea_valokaista_palvelukuvaus_20160219.pdf

Viestintävirasto. 2015. IPv6 on käytettävissä jo 5 miljoonassa liittymässä Suomessa. Julkaistu 10.6.2015. Viitattu 26.4.2016. Saatavilla https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2015/IPv6onkaytettavissajo5miljoonassaliittymassa-suomessa.html

Vänskä, O. 2012. Nyt se sitten kävi: IPv4-osoitteet loppuivat koko Euroopasta. Tietoviikko. Julkaistu 17.9.2012. Viitattu 21.4.2016. Saatavilla http://www.tivi.fi/Uutiset/2012-09-17/Nyt-se-sitten-k%C3%A4vi-IPv4-osoitteet-loppuivat-koko-Euroopasta-3194616.html