

Simo Turunen

# Pk-yrityksen sisäverkon dokumentointi, vianselvitys ja seuranta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

11.11.2015

Tekijä(t) Otsikko	Simo Turunen Pk-yrityksen sisäverkon dokumentointi, vianselvitys ja seuranta
Sivumäärä Aika	72 sivua + 9 liitettä 11.11.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Osaamisaluepäällikkö Janne Salonen
<p>Tässä työssä kartoitetaan ja dokumentoidaan pk-yrityksen sisäverkko, tarkastetaan sen kriittisimmät osat vikojen varalta sekä otetaan käyttöön järjestelmä verkon ja palvelimien tilan seuraamiseen. Kartoitus toteutettiin käyttäen ladattavia ilmaisohjelmia Advanced IP Scanner ja Tera Term, Microsoft Windows 8.1:n mukana tulevia työkaluja sekä tarkastellen laitteita fyysisesti paikan päällä. Dokumentointi rakennettiin Microsoft Officen sekä Microsoft Vision avulla.</p> <p>Vianselvitykseen käytettiin niin ikään Tera Termiä ja Microsoft Windows 8.1:n työkaluja sekä Syslog Watcher -nimistä tapahtumarekisterien seurantaohjelmaa. Vianselvityksessä keskityttiin verkon toimintaan ja vikasietoisuuteen. Tarkasteltavia laitteita olivat muun muassa yrityksen L2-kytkimet, WLAN-kontrolleri ja langattomat tukiasemat sekä domain controllereina toimivat palvelimet.</p> <p>Verkon ja palvelimien tilan seuranta varten asennettiin eräälle yrityksen palvelimelle PRTG Network Monitor. Ohjelman ilmaislisenssin avulla voidaan ottaa käyttöön sata laitteiden tilaa seuraavaa sensoria. Kaikkia seurantaan valittuja laitteita seurataan ohjelman avulla ping-komennoilla, sekä tiettyjä kriittisiä osia niistä erikoistuneilla sensoreilla.</p>	
Avainsanat	Sisäverkko, dokumentointi, vianselvitys, seuranta

Author(s) Title Number of Pages Date	Simo Turunen Documenting, troubleshooting and monitoring of an SME's internal network 72 pages + 9 appendices 11 November 2015
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data networks
Instructor(s)	Janne Salonen, Head of Department
<p>This study focuses on the mapping and documenting of an SME's internal network. The aim is to check the network for errors and misconfigurations and set up a system for monitoring the status of the network and the enterprise's servers. The mapping was done with the help of two publicly available free software, namely Advanced IP Scanner and Tera Term, and tools that come built in with Microsoft Windows 8.1 and also by physically checking the network devices. The documentation was created with Microsoft Office and Microsoft Visio.</p> <p>Troubleshooting the network was also done with the help of Tera Term and the built in tools of Microsoft Windows 8.1 and also a publicly available free software called Syslog Watcher. In this troubleshooting the focus was on reliable operation and fault tolerance of the network. The devices checked were mainly the enterprise's L2 switches, WLAN controller and access points, and the servers functioning as domain controllers.</p> <p>For monitoring the status of the enterprise's network and servers, a program called PRTG Network Monitor was installed on a server in the enterprise. The program's free license includes one hundred sensors for monitoring the status of the devices. All devices selected to be monitored with the program were monitored with a sensor utilizing ping-commands and certain critical parts of them with specialized sensors.</p>	
Keywords	Internal network, documenting, troubleshooting, monitoring

## Sisällys

### Lyhenteet

1 Johdanto.....	1
2 Dokumentointi.....	2
2.1 Alkutilanne.....	2
2.2 Dokumentoinnin rajausta.....	3
2.3 Dokumentoinnin toteutus.....	3
2.4 Helsingin toimipiste.....	5
2.4.1 Helsingin toimipisteen verkkoinfrastruktuuri.....	5
2.4.2 Helsingin toimipisteen palvelimet.....	15
2.5 Vantaan toimipiste.....	16
2.6 Espoon toimipiste.....	16
2.7 Verkkotulostimet.....	17
2.8 Konesali.....	19
2.9 Dokumentaation yhteenveto.....	21
3 Vianselvitys.....	21
3.1 Vianselvityksen rajausta ja tavoitteet.....	21
3.2 Vianselvityksen toteutus.....	22
3.3 Kytkimet.....	22
3.3.1 VLAN:it.....	23
3.3.2 Tapatumarekisteripalvelin.....	24
3.3.3 Aikapalvelu ja aikapalvelin.....	26
3.3.4 Spanning tree.....	29
3.4 WLAN-kontrolleri ja WLAN-tukiasemat.....	33
3.5 Domain controllerit.....	38
3.5.1 DHCP-palvelimien asetukset.....	40
3.5.2 DNS-palvelimien asetukset.....	45
4 Verkon tilan ja palvelimien seuranta.....	48
4.1 Seurannan rajausta ja tavoitteet.....	48
4.2 Seurannan toteutus.....	49
4.3 PRTG Network Monitorin yleiskatsaus.....	50

4.4 PRTG Network Monitorin konfigurointi.....	51
4.4.1 Ryhmien ja laitteiden asetukset.....	51
4.4.2 Sensorit.....	55
4.4.3 Kartat.....	63
5 Yhteenveto.....	68

Liite 1. Internetpalveluntarjoajan verkkodokumentti

Liite 2. Palvelimet

Liite 3. Tulostimet

Liite 4. IP-kamerat

Liite 5. Vantaan toimiston IP-osoitteet

Liite 6. Verkkoinfrastruktuuri

Liite 7. Kytkinten portit

Liite 8. Kysely verkon toiminnan ongelmista

Liite 9. Yrityksen verkon kuva

## Lyhenteet

MPLS	Multiprotocol Label Switching on runkoverkon tiedonsiirtomenetelmä, jolla voidaan ohjata liikenne nopeasti ennaltamäärättyjä reittejä pitkin ilman reititystä.
DNS	Domain Name System on internetin nimipalvelujärjestelmä, joka muuntaa verkkonimet IP-osoitteiksi ja toisinpäin. Mahdollistaa muun muassa internetselaimien käytön.
L2	Layer 2 on OSI-mallin toinen kerros, siirtokerros.
OSI	Open Systems Interconnection (Reference Model) on internetprotokollien seitsemänkerroksinen malli.
VLAN	Virtual Local Area Network on virtuaalinen lähiverkko, teknologia joka mahdollistaa fyysisesti eri paikoissa sijaitsevien laitteiden yhdistämisen samaan loogiseen aliverkkoon sekä laitteiden eristämisen omaan verkkoonsa.
DHCP	Dynamic Host Configuration Protocol on OSI-mallin sovelluskerroksen protokolla, joka jakaa laitteille IP-asetukset (muun muassa IP-osoitteen määrätystä osoiteavaruudesta).
WLAN	Wireless Local Area Network on langaton lähiverkko, tekniikka jolla laitteet voidaan yhdistää langattomasti määrättyyn lähiverkkoon.
NAS	Network-attached Storage on tiedostopalvelin, jossa on RAID-tekniikalla yhdistettyjä levyjä sulautetun palvelimen hallinnoimana. Mahdollistaa tietojen helpon tallennuksen verkon yli.
RAID	Redundant Array of Independent Disks on tekniikka, jolla yhdistetään useita fyysisiä kiintolevyjä loogiseksi levyksi, jolla on paranneltu vikasietoisuus, suorituskyky ja tallennuskapasiteetti käytetystä versiosta riippuen.

IP	Internet Protocol on OSI-mallin kolmannessa kerroksessa toimiva protokolla, joka mahdollistaa tietoliikennepakettien toimituksesta pakettikytkentäisessä verkossa.
MAC	Media access control eli MAC-osoite joka tunnetaan myös fyysisenä osoitteena on heksadesimaalimuotoinen laitteen tai verkkokortin uniikki osoite.
USB	Universal Serial Bus on yleisesti käytetty sarjaväyläarkkitehtuuri oheis laitteiden liittämiseen tietokoneisiin. Esimerkiksi lähes kaikki hiiret ja näppäimistöt liitetään nykyään USB-väylään.
DE-9	9-pinninen D:n muotoinen sarjaportti. USB:n edeltäjä, joka on nykyään harvoin käytössä kuluttajalaitteissa.
SCCM	System Center Configuration Manager on Microsoftin hallintaohjelmisto, jolla voidaan suorittaa lukuisia yritysverkon laitteiden hallintaan liittyviä toimintoja.
WSUS	Windows Server Update Services on ohjelma, joka mahdollistaa Windows-päivitysten keskitetyn hallinnan ja latauksen paikalliselta palvelimelta päätelaitteille ulkopuolisen Microsoftin palvelimen sijaan.
SEPM	Symantec Endpoint Protection Manager on Symantecin virustorjunnan keskitetty hallinta. Mahdollistaa yrityksen kaikkien Windows-laitteiden virustorjunnan hallinnan yhdestä paikasta.
NTP	Network Time Protocol on UDP-protokollaan pohjautuva protokolla ajan välittämiseksi tietokoneiden välillä.
VSC	Virtual Service Community on kokoelma asetuksia, jonka WLAN-kontrolleri jakaa hallituille tukiasemille. Yksi VSC voi määrittää esimerkiksi yhden nimetyn WLAN:n kaikki asetukset.

- NAT Network Address Translation on teknologia, jolla voidaan antaa laitteelle erikseen sisäinen ja ulkoinen IP-osoite. NAT:n ulkopuoliset laitteet näkevät laitteesta vain ulkoisen osoitteen. Tämä mahdollistaa yhden julkisen IP-osoitteen käytön usealla laitteella ja parantaa laitteiden tietoturvalisua.
- WPA2 WPA2 eli IEEE 802.11i on langattomien verkkojen tietoturvastandardi. Sen kanssa pystytään käyttämään CCMP:tä salaukseen.
- CCMP Counter Mode with CBC-MAC Protocol on langattomien verkkojen salausjärjestelmä, joka on luotettavampi kuin WEP ja TKIP.
- WMI Windows Management Instrumentation on infrastruktuuri hallintadatalle ja toimintojen suorittamiselle Windows-pohjaisille laitteille.
- ICMP Internet Control Message Protocol on OSI-mallin verkkokerroksen protokolla, jolla suoritetaan muun muassa ping-työkalu.
- IIS Internet Information Services on Microsoftin web-palvelinohjelmisto, jonka päälle voidaan rakentaa verkkosivuja käytettäväksi Windows-palvelimilla.



## 1 Johdanto

Tämä työ aloitettiin alun perin tarkoituksena uusien erään pk-yrityksen verkkoyhteydet internetpalveluntarjoajan vaihdon yhteydessä. Yrityksen voimassaoleva internetpalveluntarjoaja teki kuitenkin kilpailutuksen loppuvaiheessa ylivoimaisesti parhaan tarjouksen ”hintapäivityksen” muodossa, eli mitään verkkoja ei tulaisikaan uusimaan. Tässä vaiheessa yrityksen verkon dokumentointi oltiin kuitenkin jo aloitettu verkon uusintaan valmistautuessa, joten työn tavoitteet päivitettiin vastaamaan muuttunutta tilannetta. Päädyttiin jatkamaan dokumentointi loppuun asti ja lisäksi etsimään mahdolliset vikat kohdat yrityksen sisäverkosta ja selvittämään tai kirjaamaan ne ylös myöhempää selvitystä varten sekä rakentamaan järjestelmä yrityksen sisäverkon tilan ja tiettyjen palveluiden seuraamiselle.

Työlle muodostui aihe muutoksen jälkeen kolme edellä mainittua tavoitetta. Ensimmäisenä on saada yrityksen IT-osaston käyttöön selkeä ja kattava kuva yrityksen verkon rakenteesta ja toiminnasta. Toisena on etsiä verkon toimintaa haittaavat viat ja mahdollisesti korjata ne. Kolmantena tavoitteena on ottaa käyttöön järjestelmä verkon ja tiettyjen yrityksen toiminnan kannalta kriittisten palvelujen seuraamiseen. Tämän järjestelmän tulee olla koko IT-osaston käytössä milloin vain ja yhtä aikaa.

Työ tehtiin yrityksen IT-osaston tilauksesta IT-osaston sisäiseen käyttöön. Kaikki yrityksen helpon tunnistamisen mahdollistavat tiedot on poistettu tästä työstä. Sensuroimat versiot työstä sen ja liitteistä toimitetaan yritykselle itselleen sisäiseen käyttöön. Työn sisällön ymmärtäminen vaatii vahvaa perustason IT-tietojen ymmärrystä, kuten IP- ja MAC-osoitteiden tuntemista.

## 2 Dokumentointi

### 2.1 Alkutilanne

Yrityksellä on kolme toimipistettä pääkaupunkiseudun alueella, joiden välisen sisäisen verkon dokumentointi on vanhentunut lukuisten laitepäivitysten ja eri ulkoisten laitetoimittajien asennusten jäljiltä. Yrityksellä ei ole selkeää kuvaa sisäverkkonsa rakenteesta ja toiminnasta. Verkon tilaa ei seurata millään tavalla, vaan viat näkyvät lähinnä ohjelmien tai yhteyksien toiminnan huononemisena tai katkeamisena. Lähes kaikkien verkkolaitteiden asennuksesta on huolehtinut joku ulkoinen taho. Yrityksen verkon edellinen dokumentaatio on vuodelta 2009 ja pitää vain etäisesti paikkansa.

Yrityksellä on käytössään yksi sisäinen toimialue, johon on liitetty kaikki yrityksen käyttäjien päätelaitteet. Yrityksen kolmen eri toimiston laitteet pystyvät kommunikoimaan keskenään internetpalveluntarjoajan reitityksen ansiosta. Yrityksellä on käytössään kaksi fyysistä palvelinta ja 21 virtuaalipalvelinta konesalipalveluntarjoajan tiloissa. Palvelimista suurin osa on liitetty sisäiseen toimialueeseen. Päätelaitteita ja palvelimia on yhteensä noin 100 kappaletta.

Dokumentoinnin tavoitteena on saada aikaiseksi kattava ja selkeä kokonaisuus, jonka avulla yrityksen IT-osasto voi helposti hahmottaa yrityksen sisäverkkoon kuuluvat laitteet ja hallita niitä.

## 2.2 Dokumentoinnin rajaus

Dokumentoinnin laajuus ja tarkkuus rajattiin palvelemaan yrityksen IT-osaston tarpeita jokapäiväisessä toiminnassa sekä mahdollisissa tulevilla muutoksissa. Verkon rakenteesta jätettiin dokumentoimatta muun muassa kaapeloinnit, sillä yritys ei itse vastaa niistä, vaan ne on tilattu ja tullaan tilaamaan ulkoiselta toimittajalta. Samankaltaisesti dokumentoitiin vain pintapuolisesti niiden laitteiden tiedot, joita yritys ei omista ja joiden ylläpidosta yritys ei vastaa, koska ne saattavat muuttua yrityksen tietämättä, eikä niiden hallintaa tarvitse ottaa huomioon. Lisäksi sekä yrityksen internetpalveluntarjoaja, että konesalipalveluiden tarjoaja luovuttivat heidän puoleisista osista yrityksen verkkoa tietoa erittäin nihkeästi, joten heidän puolisensa verkon osat käydään läpi vain pintakatsauksena. Yrityksellä on lisäksi valmiiksi käytössä toimiva laiterekisteri, joka listaa käyttäjien tietokoneet ja mobiililaitteet, joten näiden tietoja ei myöskään dokumentointiin sisällytetty.

Dokumentoitaviin asioihin otettiin mukaan näin ollen

- yrityksen käytössä olevat palvelimet
- sisäverkon infrastruktuuri
- verkkotulostimet, IP-kamerat ja muut sisäverkossa olevat erikoislaitteet.

## 2.3 Dokumentoinnin toteutus

Dokumentointi aloitettiin olemalla yhteydessä yrityksen internetpalveluntarjoajaan ja konesalipalveluiden tarjoajaan ja pyydettiin heiltä tietoja yrityksen heidän puoleisen verkon rakenteesta.

Internetpalveluntarjoaja toimitti kuvan (liite 1), josta selviää yritykselle varatut aliverkot sekä yrityksen toimipisteiden ja konesalin välillä toimivan verkon nopeusrajoitukset ja rakenne – MPLS. Konesalipalveluiden tarjoaja ei toimittanut käytännössä mitään työn kannalta hyödyllistä, mutta keskusteluista heidän kanssaan selvisi, että kaikki yrityksen sisäverkon ulkopuolinen verkkoliikenne kulkee heidän kauttaan.

Yrityksen edellisiä dokumentointeja tutkittaessa huomattiin nopeasti, ettei niitä voi hyödyntää millään lailla, sillä niissä oli vääriä IP-osoitteita ja palvelimia ja muita laitteita, joita ei ole enää olemassa. Yrityksen Vantaan ja Espoon toimipisteiden verkot ovat sen verran kompakteja, että niiden rakenne selvisi paikan päällä käymällä laitteet läpi ja ottamalla niiden tiedot ylös. Helsingin toimipisteen verkon sisältämät laitteet selvitettiin tutkimalla verkkoa verkon skannausohjelmalla ja käymällä kytkentäkaapit läpi selvittäen niiden sisältämät laitteet ja kytkennät. Lisäksi tarkistettiin yrityksen itse hallitsemien laitteiden asetukset ja otettiin ne ylös osana dokumentointia. Lista yrityksen käytössä olevista virtuaalipalvelimista saatiin yrityksen DNS-tietueista ja IT-päälliköltä, jonka jälkeen niiden palvelut ja riippuvuudet tarkistettiin ja dokumentoitiin.

Yritys käyttää kahden palveluntarjoajan palveluita. Internetpalveluntarjoaja tarjoaa toimipisteiden ja konesalin välisen verkon sekä toimipisteiden reitittimet. Konesalipalveluiden tarjoaja tarjoaa virtuaalipalvelimet ja ulospäin kulkevan verkkoyhteyden sekä palomuuripalvelun. Yrityksellä on käytössään sisäinen toimialue, jota hallinnoi kaksi domain controlleria, palvelimet TOIMISTO ja file1. Yrityksen päätoimipisteessä Helsingissä on kahdeksan yrityksen omistamaa L2-kytkintä ja yksi operaattorin reititin. Vantaan toimipisteessä on yksi kuluttajatason kytkin, joka on kytketty käytettyihin päätelaitteisiin ja palveluntarjoajan reitittimeen. Espoon toimipisteen verkkoa hallinnoi internetpalveluntarjoaja. Yrityksellä on lisäksi kaksi fyysistä palvelinta Helsingin toimipisteessä ja 21 virtuaalipalvelinta konesalipalveluiden tarjoajan toimitiloissa.

Toimipisteiden ja konesalin välinen verkko on toteutettu internetpalveluntarjoajan MPLS-verkkona. Helsingin toimipisteessä sijaitsevat päätelaitteet ja palvelimet ovat samassa sisäisessä VLAN:ssa. Vantaan toimipistettä lukuun ottamatta kaikki päätelaitteet saavat osoitteensa DHCP:n kautta.

## 2.4 Helsingin toimipiste

Helsingin toimipiste on yrityksen päätoimipiste. Helsingin toimipisteen verkkoon kuuluu viisi kytkentäkaappia laitteineen, sekä varasto, jossa on kaksi fyysistä palvelinta, kahdeksan L2-kytkintä, WLAN-controlleri sekä sen kautta hallitut yksitoista langatonta tukiasemaa, seitsemän IP-valvontakameraa ja NAS niiden tallenteille sekä viisi verkkotulostinta ja niiden hallintalaite. Toimiston verkkoyhteydet ulospäin kulkevat internetpalveluntarjoajan reitittimen kautta, joka on yhdistetty valokuidulla root-kytkimeen.

### 2.4.1 Helsingin toimipisteen verkkoinfrastruktuuri

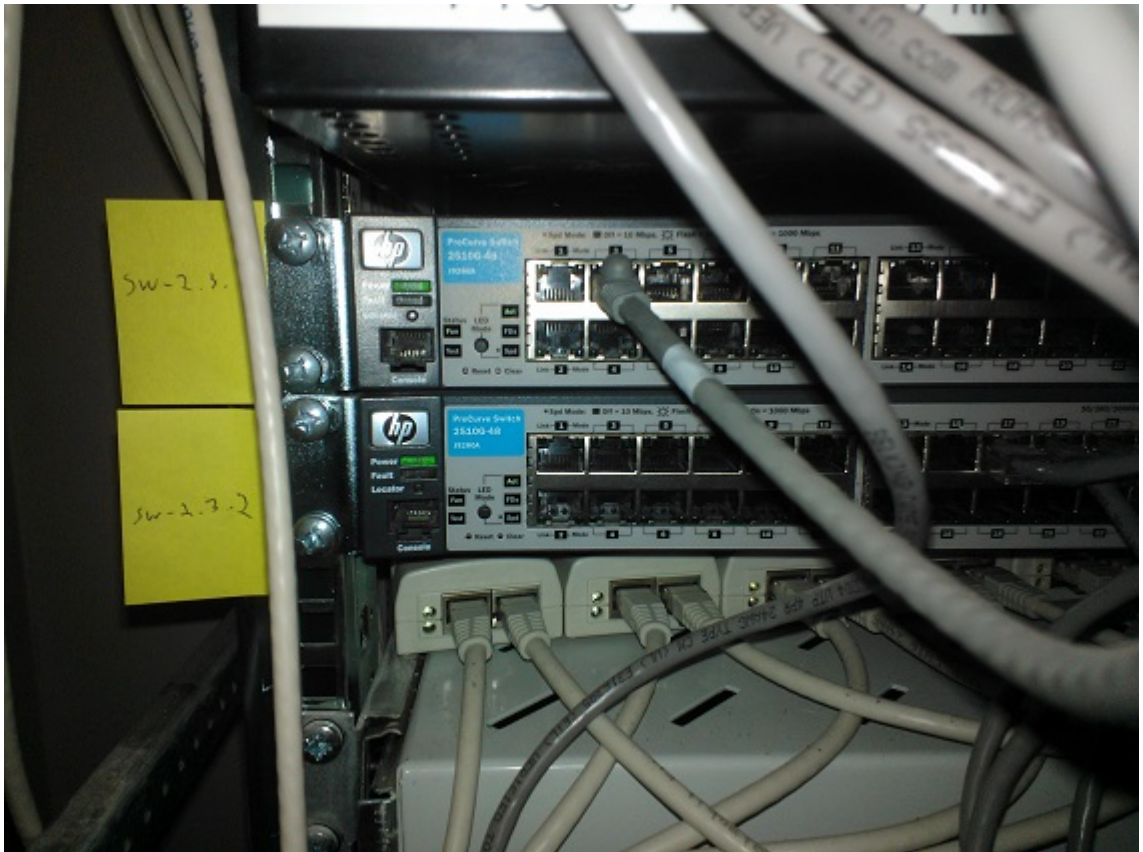
Laitteiden selvitys aloitettiin skannaamalla internetpalveluntarjoajan kertomat Helsingin toimipisteen aliverkot (liite 1) verkko Advanced IP Scannerilla. Ohjelma on haettavissa osoitteesta <http://www.advanced-ip-scanner.com/>. Tämä erittäin yksinkertaisesti käytettävä ilmainen ohjelma etsii verkosta kaikki laitteet, jotka vastaavat vähintään ICMP ping-paketteihin. [1.] Ohjelma listasi kaikista löytämistään laitteista verkkonimen, IP-osoitteen, valmistajan ja MAC-osoitteen.

Status	Name	IP	Manufacturer	MAC address
	172.16.40.1	172.16.40.1	CISCO SYSTEMS, INC.	D0:57:4C:13:53:C0
	172.16.40.135	172.16.40.135		
	172.16.40.142	172.16.40.142		
	172.16.40.146	172.16.40.146		
	172.16.40.147	172.16.40.147		
	172.16.40.154	172.16.40.154		
	172.16.40.181	172.16.40.181	ProCurve Networking by HP	00:24:A8:86:69:30
	172.16.40.200	172.16.40.200	Overland Storage, Inc.	00:C0:B6:22:D4:82
	172.16.40.201	172.16.40.201	Mobotix AG	00:03:C5:08:D8:51
	172.16.40.202	172.16.40.202	Mobotix AG	00:03:C5:08:B8:5F
	172.16.40.203	172.16.40.203	Mobotix AG	00:03:C5:08:D9:09
	172.16.40.204	172.16.40.204	Mobotix AG	00:03:C5:08:D8:4E
	172.16.40.205	172.16.40.205	Mobotix AG	00:03:C5:08:D9:13
	172.16.40.206	172.16.40.206	Mobotix AG	00:03:C5:08:CB:22
	172.16.40.207	172.16.40.207	Mobotix AG	00:03:C5:08:B6:C7
	172.16.40.51	172.16.40.51	ProCurve Networking by HP	00:24:A8:1A:0A:3C
	172.16.40.56	172.16.40.56	ProCurve Networking by HP	00:24:A8:1A:2D:70
	172.16.40.75	172.16.40.75	ProCurve Networking by HP	00:24:A8:1A:2D:8E
	172.16.40.76	172.16.40.76	ProCurve Networking by HP	00:24:A8:1A:02:20
	194.241.70.1	194.241.70.1		

Kuva 1. Advanced IP Scannerin tulokset Helsingin toimiston aliverkoissa.

Valmistajan perusteella pääteltiin, mitä laitteet olivat, ja asia varmistettiin myöhemmin kytkinten hallintakonsolin kautta. Esimerkiksi ”Mobotix AG” -valmistajan laitteiden tiedettiin olevan erittäin todennäköisesti yrityksen IP-valvontakameroita, sillä ne olivat ai-noat tiedossa olevat Mobotixin laitteet verkossa.

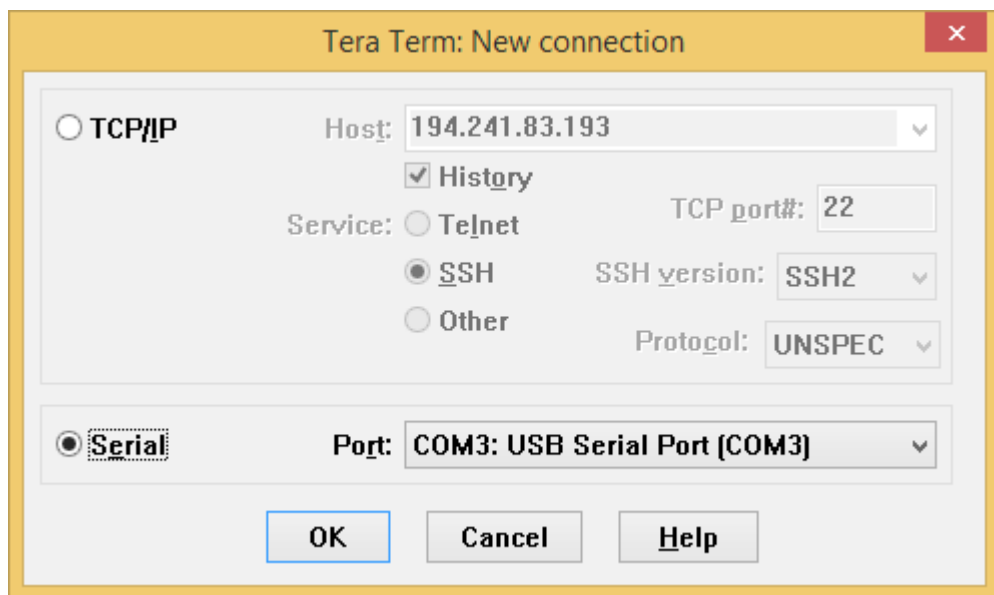
Tämän jälkeen tutkittiin kytkentäkaappien sisältö. Niistä otettiin ylös fyysisten laitteiden merkit, mallit ja käytössä olevat verkkoportit. Nämä tiedot kirjattiin Excel-taulukoihin (liit-teet 6 ja 7). Kytkettyjä seinäpistokkeita ei otettu ylös, sillä ne vaihtuvat kohtalaisen useasti ja dokumentaation ajan tasalla pysyminen olisi epätodennäköistä.



Kuva 2. Kytöntäkaappi Helsingin toimistolla. Kytöntien nimet merkattiin väliaikaisesti Posti-it-lapuille selkeyden vuoksi.

Viimeisimmästä kytkinasennuksesta jääneen dokumentaation mukaan kaikkiin kytkimiin oli asetettu sama salasana hallintaa varten. Tämä pitikin yhtä laitetta lukuun ottamatta paikkansa. Kannettavan tietokoneen USB-porttiin liitettiin adapteri USB-sarjaportti (USB-A to DE-9), johon liitettiin adapteri sarjaportti-ethernet (DE-9 to RJ45). Viimeisen adapterin RJ45-liitäntä kytkettiin kytkimen konsoliporttiin. Tämän jälkeen kytkimiin otettiin yhteys Tera Term -ohjelmalla. Tera Term on hyvin kytkinten hallintaan soveltuva ilmainen terminaalimulaattori. Tera Term on haettavissa osoitteesta <https://ttssh2.osdn.jp/index.html.en>. Tera Termistä valittiin serial adapteri "USB Serial Port" konsoliyhteyttä varten. Kytkimistä otettiin talteen konfiguraatiodokumenttien sisältö tulostamalla se esille "show run" -komennolla ja kopioimalla kannettavalle tietokoneelle txt-tiedostoihin. Komento tulostaa terminaaliin kytkimessä sillä hetkellä käytössä olevan konfiguraation. [5; 6.] Kytöntien verkkonimet merkattiin näkyville kytöntäkaappeihin.

Ainoastaan kytkimeen 5.2.1 ei pystytty kirjautumaan sisään annetulla salasanalla. Sen salasanan vaihto oli ilmeisesti unohtunut asentajilta. Asiaa heiltä sähköpostitse tiedusteltaessa he tyytyivät toteamaan, että kytkimeen pääsisi käsiksi resetoimalla koko laitteen tehdasasetuksille. Laitteen etupaneelissa oli kuitenkin "Clear"-nappi jota painamalla salasanojen resetointi onnistui ilman konfiguraation menetystä. Salasanat resetoitiin tätä toimintoa hyödyntämällä vianselvitysvaiheessa.



Kuva 3. Yhteyden ottaminen sarjaporttiadapterin kautta Tera Termilla.

Kytkinten konfiguraatitiedostoista näkyi välittömästi, että konfiguraatiot ovat minimalistiset ja vaativat todennäköisesti muutoksia myöhemmin. Kytkimiin oli konfiguroitu kolme tai neljä eri porttipohjaista VLAN:ia riippuen kytkimestä:



Taulukko 1. VLAN:ien tiedot

VLAN:in nimi	VLAN ID	Portit
DEFAULT_VLAN	1	Kaikki
”Sisäinen VLAN”	2	Kaikki paitsi portti 1 ja WLAN-controllerin portti
Hallinta	66	1
Vieras	99	*

\* Vieras-VLAN on konfiguroitu ainoastaan kytkimen SW-5.1.1 porttiin 43, joka oli yhteydessä WLAN-kontrolleriin.

VLAN eli Virtual Local Area Network on teknologia, jonka avulla voidaan fyysisesti eri paikoissa sijaitsevat laitteet liittää samaan virtuaaliseen lähiverkkoon, tai eristää fyysisesti samassa paikassa sijaitsevat laitteet omiin virtuaalisiin lähiverkkoihinsa. VLAN:it eivät oikein konfiguroituna näy päätelaitteille, vaan ne luulevat olevansa samassa fyysisessä lähiverkossa. Yrityksen kytkimissä käytetään porttipohjaisia VLAN:eja.

Porttipohjaista VLAN:ia konfiguroitaessa täytyy määrittää, mitkä kytkimen portit ovat VLAN:ssa sijaitseville päätelaitteille ja mistä porteista halutaan VLAN:in jatkuvan toisille kytkimille. Päätelaitteiden porttien kohdalla kytkimeen määritetään VLAN:n asetuksiin portin olevan ”untagged”. Tämä tarkoittaa, että portti kuuluu määritettyyn VLAN:iin, mutta yhdistetylle laitteelle ei lähde pakettien mukana VLAN-tagia, jota se ei välttämättä pystyisi käsittelemään. Tällöin laitteelle saapuva liikenne ei näy tulevan VLAN:sta. Portit, joihin on kytketty toinen kytkin, tai reititin, joiden halutaan osallistuvan VLAN:iin, määritetään VLAN:n asetuksista ”tagged”-porteiksi. Tagged-porttiin kytketty laite vastaanottaa paketeissa VLAN-tagin, joka kertoo, mihin VLAN:iin paketti kuuluu. Tällä perusteella se osaa ohjata sen edelleen ainoastaan kyseiseen VLAN:iin kuuluviin portteihin. Tagged-portti voi myös olla osallisena useissa VLAN:eissa, mutta untagged portti voi osallistua vain yhteen. [2; 3; 4.]

Hallinta-VLAN on tarkoitettu kytkinten etähallintaan. Mistä tahansa tähän VLAN:iin liitetyistä laitteesta saa yhteyden kaikkiin kytkimiin. Ainoastaan Hallinta-VLAN:illa oli IP-osoite jokaisessa kytkimessä. Se oli kaikilla aliverkossa 10.255.255.1/24. Tämä tieto mahdollistaisi kytkinten myöhemmän etähallinnan, joten hallintaosoitteet kirjattiin ylös erikseen.

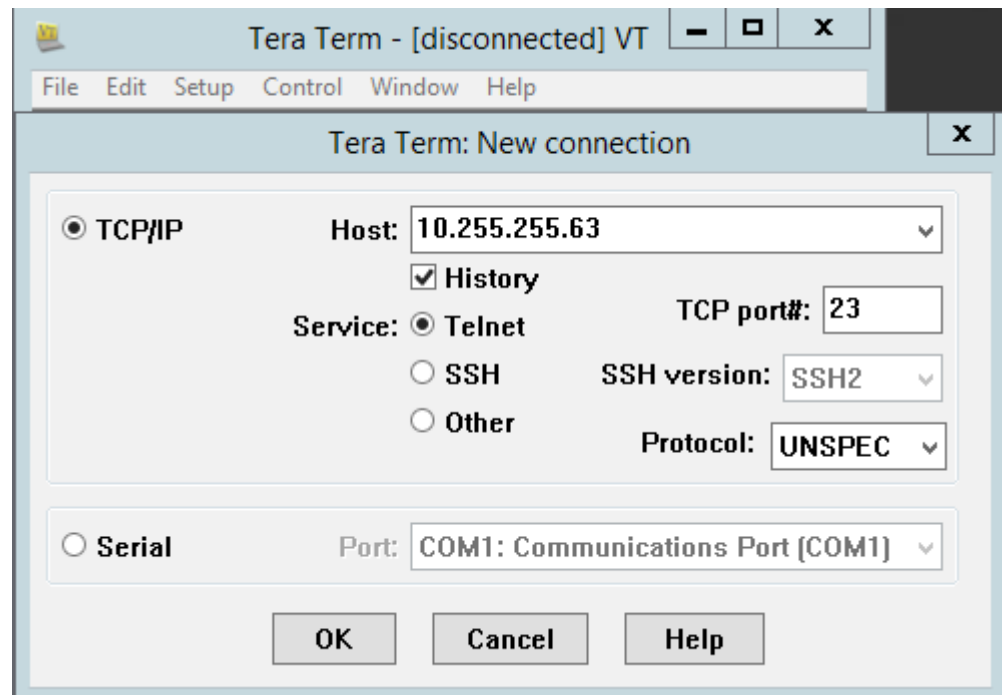
## Taulukko 2. Kytkinten tiedot

Kytkimen verkkonimi	Hallintaosoite	Sijainti
SW-5.1.1	10.255.255.51	5.krs kytkentäkaappi 1
SW-5.1.2	10.255.255.52	5.krs kytkentäkaappi 1
SW-5.2.1	10.255.255.53**	5.krs kytkentäkaappi 2
SW-2.1.1	10.255.255.21*	2.krs kytkentäkaappi 1
SW-2.1.2	10.255.255.63*	2.krs kytkentäkaappi 1
SW-2.2.1	10.255.255.62	2.krs kytkentäkaappi 2
SW-2.3.1	10.255.255.60	2.krs kytkentäkaappi 3
SW-2.3.2	10.255.255.61	2.krs kytkentäkaappi 3

\* Näiden kytkinten VLAN 66 (Hallinta) oli nimetty väärin, eivätkä ne olleet etähallittavissa. Nämä korjattiin vianselvitysvaiheessa.

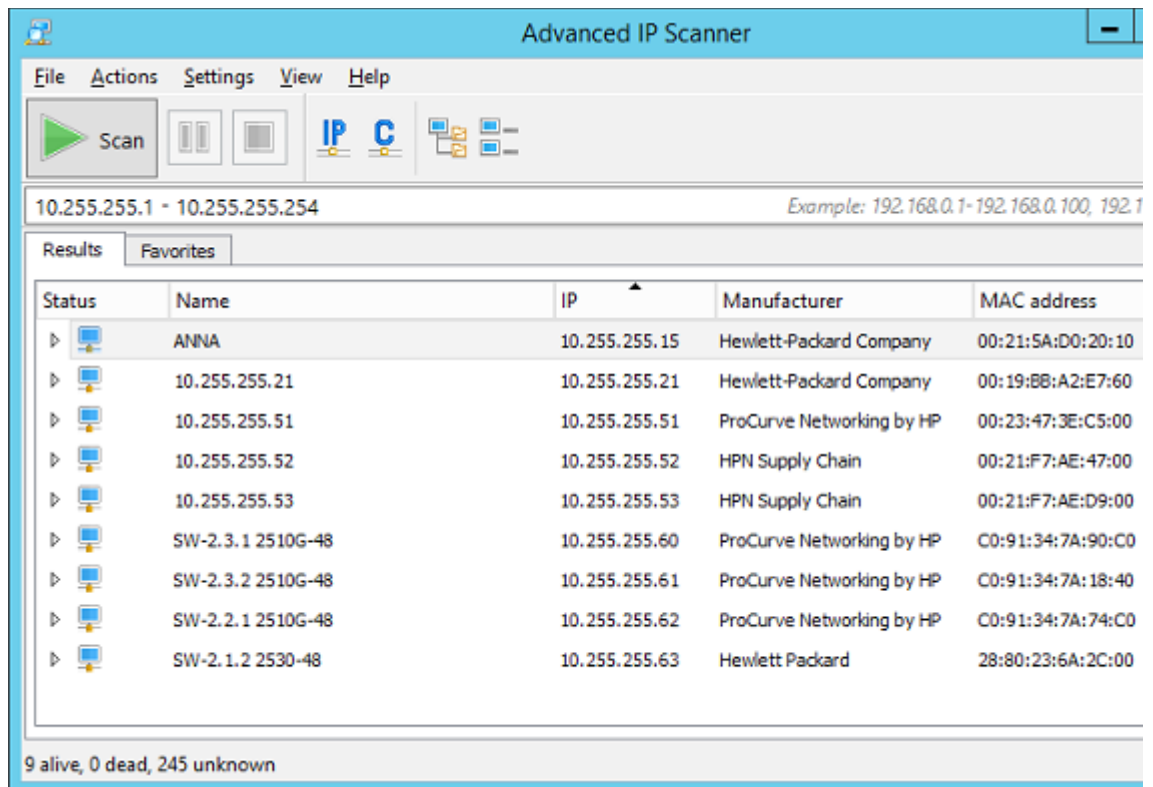
\*\* Kytkimen SW-5.2.1 IP-osoite selvitettiin ajamalla IP-skanneri ANNA:lla osoite-avaruudelle 10.255.255.1/24.

Kytkimen 5.1.2 verkkoportti 1, joka on hallinta-VLAN:ssa, yhdistettiin varastossa sijaitsevan palvelimen ANNA toiseen verkkokorttiin, johon konfiguroitiin IP-osoite 10.255.255.15, joka sijaitsee hallinta-VLAN:in osoiteavaruudessa. Tämän jälkeen kytkimiä voitiin tarkastella helposti etäyhteydellä palvelimen kautta. Kytkinten tarkastelussa käytettiin Tera Term -ohjelmaa. Yhteys otettiin kytkinten hallinta-VLAN -osoitteen avulla, jotka otettiin ylös aiemmin konfiguraatioiden mukana. Yhteystyyppinä käytettiin telnet:iä ja verkkoporttia 23.



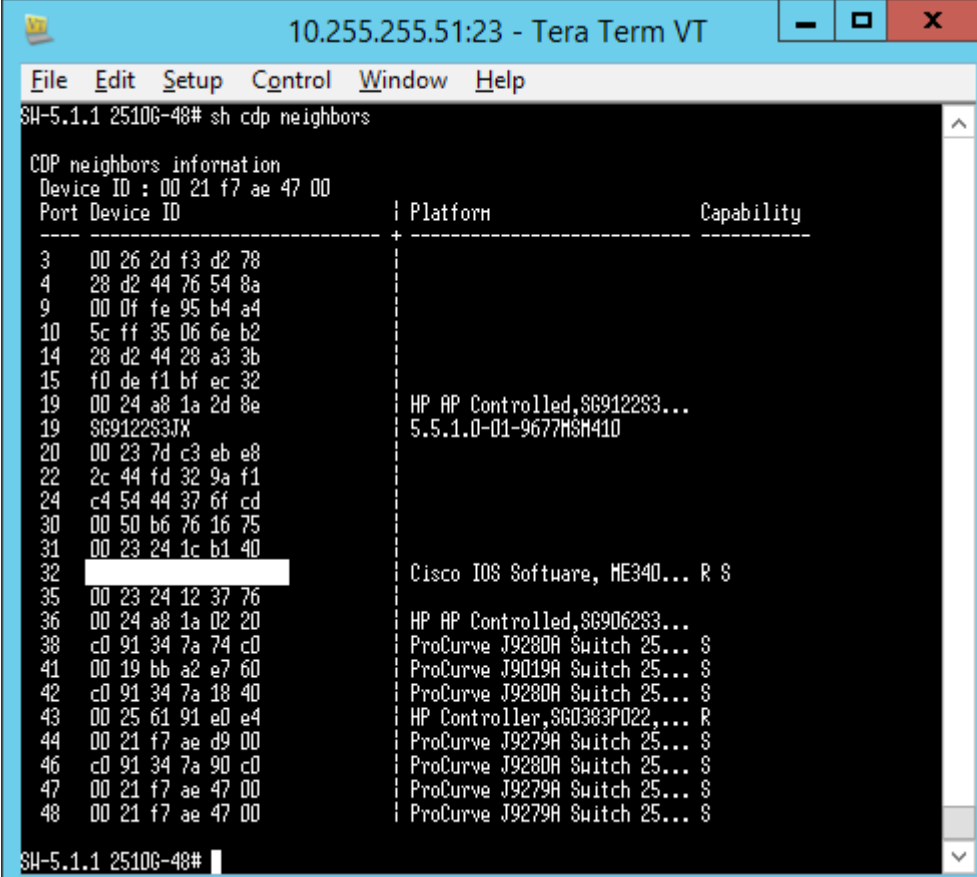
Kuva 4. Tera Term ANNA-palvelimella.

Kytkimen SW-5.2.1 IP-osoite selvitettiin ajamalla IP-skanneri ANNA:lla osoiteavaruudelle 10.255.255.1/24. Osoite oli ainoa, jota ei oltu aiemmin kirjattu ylös, eli 10.255.255.53.



Kuva 5. Advanced IP Scanner ANNA-palvelimella, kytkinten hallinta-aliverkossa.

Kytkinten väliset fyysiset liitännät selvitetiin komennolla "show cdp neighbors detail". Komento näyttää kytkimeen kytketyt laitteet, jotka tukevat Cisco Discovery Protocol:aa ja listaa niistä useita tietoja. [5; 6.]. Tämä komento ajettiin jokaisella kytkimellä ja kirjattiin ylös, mitä mihinkin porttiin oli kytketty. Käyttäjien päätteitä ei kirjattu ylös, sillä monella on käytössä kannettava tietokone eikä voida varmuudella sanoa, että käyttäjä käyttää laitettaan vain tähän tiettyyn kaapeliin kytkettynä. Lisäksi käyttäjien laitteita päivitetään uusiin, ja käyttäjät vaihtavat työpisteidensä sijaintia kohtalaisen usein, joten dokumentaation ajan tasalla pysyminen tällä tarkkuudella olisi käytännössä mahdotonta. Tyydyttiin kirjaamaan, että portti on käyttäjän päätelaitteen käytössä. Kytkennöistä tehtiin Excel-taulukko (liite 7) ja Visio-piirros (liite 9) helpompaa hahmottamista varten.



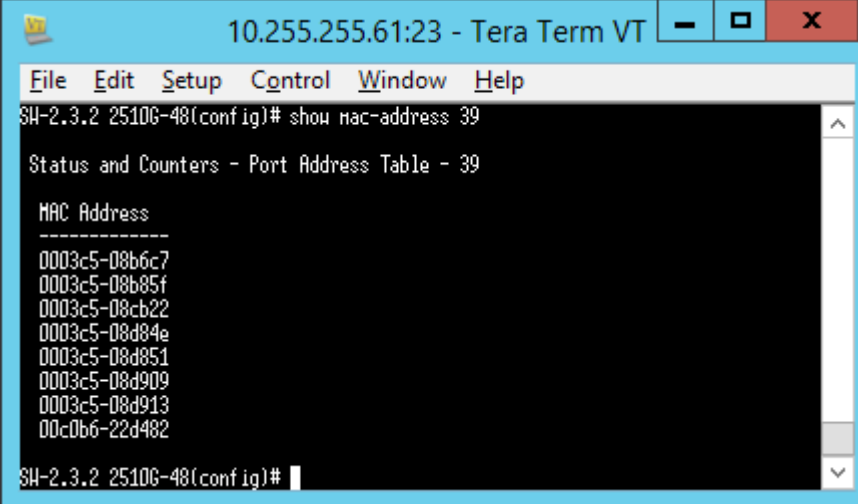
```

10.255.255.51:23 - Tera Term VT
File Edit Setup Control Window Help
SW-5.1.1 25106-48# sh cdp neighbors
CDP neighbors information
Device ID : 00 21 f7 ae 47 00
Port Device ID | Platform | Capability
-----|-----|-----
3 00 26 2d f3 d2 78 | | 
4 28 d2 44 76 54 8a | | 
9 00 0f fe 95 b4 a4 | | 
10 5c ff 35 06 6e b2 | | 
14 28 d2 44 28 a3 3b | | 
15 f0 de f1 bf ec 32 | | 
19 00 24 a8 1a 2d 8e | HP AP Controlled,SG912283...
19 SG912283JX | 5.5.1.0-01-9677MSM410
20 00 23 7d c3 eb e8 | | 
22 2c 44 fd 32 9a f1 | | 
24 c4 54 44 37 6f cd | | 
30 00 50 b6 76 16 75 | | 
31 00 23 24 1c b1 40 | | 
32 | | 
35 00 23 24 12 37 76 | Cisco IOS Software, ME340... R S
36 00 24 a8 1a 02 20 | HP AP Controlled,SG906283...
38 c0 91 34 7a 74 c0 | ProCurve J9280A Switch 25... S
41 00 19 bb a2 e7 60 | ProCurve J9019A Switch 25... S
42 c0 91 34 7a 18 40 | ProCurve J9280A Switch 25... S
43 00 25 61 91 e0 e4 | HP Controller,SG0383P022,... R
44 00 21 f7 ae d9 00 | ProCurve J9279A Switch 25... S
46 c0 91 34 7a 90 c0 | ProCurve J9280A Switch 25... S
47 00 21 f7 ae 47 00 | ProCurve J9279A Switch 25... S
48 00 21 f7 ae 47 00 | ProCurve J9279A Switch 25... S
SW-5.1.1 25106-48#

```

Kuva 6. Show cdp neighbors -komento kytkimellä SW-5.1.1. Lisäämällä komennon perään "details" näkyy kytketyistä laitteista paljon enemmän tietoa.

Tietyt laitteet (muun muassa IP-kamerat ja niiden NAS) oli kytketty ylimääräisen automaattisella konfiguraatiolla toimivan kuluttajaluokan kytkimen taakse. Selvitettyä kytkentäkaappeja tutkimalla mihin kytkinten portteihin oli kytketty ylimääräiset kuluttajataso-son kytkimet, voitiin kuluttajataso-son kytkimiin kytketyt laitteet selvittää komennoilla "show mac-address" ja "show-mac address interface <yksittäinen portti>". Nämä komennot listaavat joko kaikkien kytkimeen yhteydessä olevien laitteiden tai yksittäiseen porttiin yhteydessä olevien laitteiden MAC-osoitteet. [5; 6.] Näitä verrattiin IP-skannerin antamiin MAC-osoitteisiin, verkkonimiin ja valmistajiin laitteiden tunnistamiseksi.



```
10.255.255.61:23 - Tera Term VT
File Edit Setup Control Window Help
SW-2.3.2 2510G-48(config)# show mac-address 39
Status and Counters - Port Address Table - 39
MAC Address
-----
0003c5-08b6c7
0003c5-08b85f
0003c5-08cb22
0003c5-08d84e
0003c5-08d851
0003c5-08d909
0003c5-08d913
00c0b6-22d482
SW-2.3.2 2510G-48(config)#
```

Kuva 7. Show mac-address -komento kytkimellä SW-2.3.2. Kuvassa komennon perään on lisätty portin numero "39", jolloin komento listaa vain kyseiseen porttiin kytkettyjen laitteiden MAC-osoitteet. Kuvassa näkyvät MAC-osoitteet kuuluvat IP-kameroille ja niiden tallennus NAS:lle.

Kuvassa selvitetään kytkimen 2.3.2 porttiin 39 kytketyn kytkimen takana sijaitsevat laitteet. Vertaamalla näitä IP-skannerin tuloksiin saatiin selville, että tähän porttiin on kytketty kaikki IP-kamerat ja niiden tallennus-NAS. Jos yhteys kameroihin tai tallennuspalvelimeen katkeaisi, dokumentaatiosta selviäisi nyt helposti, mihin laitteet on kytketty. Tiedot kirjattiin ylös "Kytkinten portit" Excel-taulukkoon (liite 7).

## 2.4.2 Helsingin toimipisteen palvelimet

Helsingin toimipisteen varastossa sijaitsevat yrityksen ainoat fyysiset palvelimet ANNA ja TOIMISTO. Palvelimien toiminnot olivat jo pääasiassa IT-osaston tiedossa, joten nämä lähinnä varmistettiin tarkastelemalla palvelimia Windowsin etähallintatyökalun avulla (mstsc.exe). Annalla sijaitsee SCCM 2012, jota käytetään lähinnä laitteiden uudelleenasetukseen räätälöidyn imagen avulla, sekä tarvittaessa käyttäjien laitteiden hallintaan etäyhteystyökalun avulla. ANNA on lisäksi yrityksen IT-osaston epävirallinen testipalvelin, sillä se ei ole kriittinen yrityksen toiminnalle joitain IT-osaston toimintoja lukuun ottamatta. Annan käyttöjärjestelmänä on Windows Server 2012 R2. TOIMISTO on yrityksen kriittisin palvelin. Se toimii koko yrityksen verkon toissijaisena domain controllerina, koko yrityksen verkon ensisijaisena DNS-palvelimena ja ainoana WSUS-palvelimena, sekä Helsingin toimipisteen DHCP-palvelimena. TOIMISTO:n kautta asennetaan lisäksi kaikki yrityksen verkkotulostimet käyttäjien laitteille ja jaetulla verkkolevyllä sijaitsee yrityksessä käytettyjen ohjelmistojen asennustiedostot. Tämän lisäksi TOIMISTO:lle on asennettu Esmikko-kulunvalvontajärjestelmän palvelinsovellus, joka vastaa Helsingin toimipisteen kulunvalvonnasta ja hälytysjärjestelmästä, sekä SEPM-virustorjunnan hallintaa varten. Palvelimet sijaitsevat ilmastoidussa varastossa ja niitä käytetään pääasiassa Windowsin etäyhteystyökalun kautta (mstsc.exe).

Taulukko 3. Fyysisten palvelinten laitetiedot

Nimi	Käyttöjärjestelmä	Suoritin	Muisti	Kiinto-levytila	Verkkokortit
ANNA	Win. Server 2012 R2	E5405 @ 2.00GHz	4 GB	1,3 TB	2x 1Gbps
TOIMISTO	Win. Server 2008 R2	E5-2620 @ 2.00GHz	12 GB	3,4 TB	2x 1Gbps

Lisäksi selvitettiin, mihin kytkimiin ja portteihin palvelimet oli kytketty kohdassa 2.4.1 mainitulla tavalla: IP-skannerin ja kytkimillä suoritettavan "show mac-address" -komenton avulla. Jos laitteen MAC-osoite löytyi toiseen hallittuun kytkimeen kytketyn portin takaa, otettiin yhteys tähän toiseen kytkimeen ja ajettiin komento "show mac-address" uudestaan. Tämä toistettiin, kunnes löydettiin varsinainen portti, johon laite oli kytketty. Tiedot kirjattiin ylös "Kytkinten portit" Excel-taulukkoon (liite 7).

## 2.5 Vantaan toimipiste

Vantaan toimipisteen verkko dokumentoitiin käymällä paikan päällä selvittämässä siellä sijaitsevat laitteet ja kytkennät. Toimipisteen verkko on osa ulkopuolisen yrityspalvelukeskuksen verkkoa eivätkä laitteet saa IP-asetuksiaan DHCP:n kautta, vaan ne on määritetty manuaalisesti. Verkkoon kuuluu internetpalveluntarjoajan reititin, kuluttajatason kytkin, verkkotulostin ja kolme päätelaitetta. Vantaan toimipisteellä ei ole omaa WLAN-verkkoa. Käyttäjien laitteista otettiin ylös manuaaliset IP-asetukset, jotta välttyäisiin IP-osoite-konflikteilta, eli päällekkäisiltä IP-osoitteilta mahdollisten laitelisäysten yhteydessä. Osoitteet kirjattiin internetpalveluntarjoajan antaman aliverkon kanssa "Vantaan toimiston IP-osoitteet" Excel-taulukkoon (liite 5).

## 2.6 Espoon toimipiste

Espoon toimipisteen verkko on internetpalveluntarjoajan hallinnoima ja sen sisältöön ei tarvinnut tässä työssä perehtyä. Paikan päällä käytäessä selvisi kuitenkin, että palveluntarjoajan laitteiden lisäksi Espoon toimistoon on asetettu WLAN-verkko kuluttajatason WLAN-reittimen avulla. Se ei kuitenkaan ole etähallittavissa, joten ongelmien esiintyessä on toimistolla käytävä fyysisesti. Espoon laitteet saavat osoitteensa file1-palvelimelta DHCP:n kautta. Espoon toimipisteen laitteet löytyivät osana kaikkiin yrityksen aliverkkoihin tehtyä IP-osoitteiden skannausta, ja ne dokumentoitiin osana Visio-piirrosta yrityksen verkon rakenteesta (liite 9).

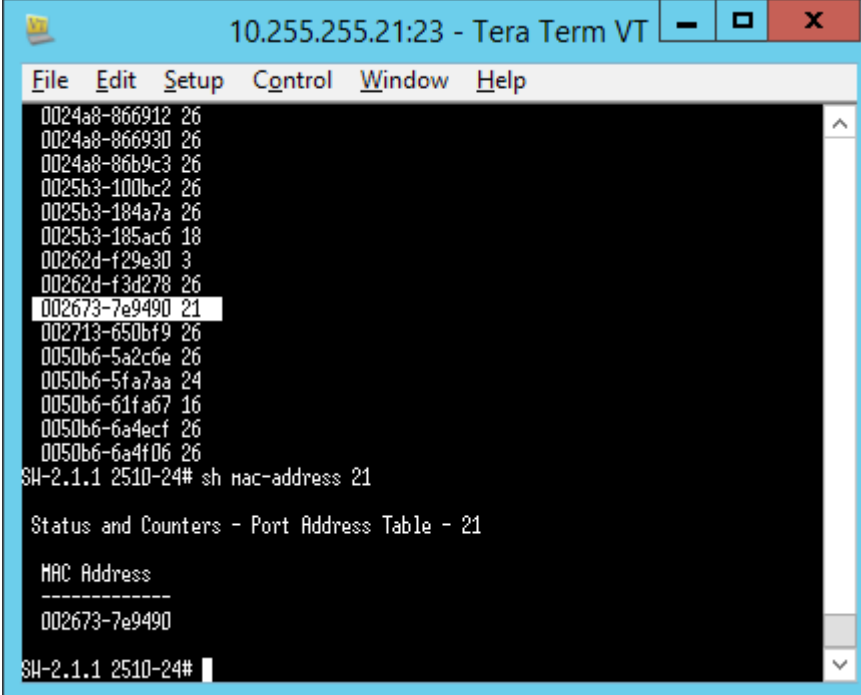


## 2.7 Verkkotulostimet

Yrityksellä on käytössä seitsemän julkista verkkotulostinta, joista kuusi on Ricohin monitoimilaitteita ja yksi on Hewlett Packardin (tästä eteenpäin HP) LaserJet asiakirjojen mustavalkotulostukseen. Laitteista viisi sijaitsee Helsingin toimipisteessä, jossa on lisäksi Ricoh-laitteiden hallintalaite, joka välittää tulostimien huoltotietoja Ricohille. Espoon ja Vantaan toimistoilla on molemmissa yksi Ricohin monitoimilaite. Kaikkien tulostimien ajurit on asennettu TOIMISTO-palvelimelle, jonka kautta käyttäjille on helppo asentaa heidän käyttämänsä laitteet.

TOIMISTO-palvelimen juuresta, osoitteesta "\\TOIMISTO" löytyneiden tulostimien ominaisuuksista otettiin ylös tulostimien IP-osoitteet ja nimet. Kaikissa tulostimissa on hallintamahdollisuus verkkoselaimen kautta, mutta tulostimien osoitteita ei ole kerätty mihinkään helposti saatavilla olevaan paikkaan, joten niiden hallintaa varten on aina jouduttu etsimään laitteen IP-osoite erikseen. IP-osoitteet kirjattiin "Tulostimet" Excel-taulukkoon (liite 3).

Lisäksi selvitettiin, mihin kytkimiin ja portteihin tulostimet oli kytketty kohdassa 2.4.2 mainitulla tavalla käyttämällä kytkimillä komentoa "show mac-address". Tulostimien kytkentöjen tiedot kirjattiin ylös "Kytöntien portit" Excel-taulukkoon (liite 7).



```
10.255.255.21:23 - Tera Term VT
File Edit Setup Control Window Help
0024a8-866912 26
0024a8-866930 26
0024a8-86b9c3 26
0025b3-100bc2 26
0025b3-184a7a 26
0025b3-185ac6 18
00262d-f29e30 3
00262d-f3d278 26
002673-7e9490 21
002713-650bf9 26
0050b6-5a2c6e 26
0050b6-5fa7aa 24
0050b6-61fa67 16
0050b6-6a4ecf 26
0050b6-6a4f06 26
SH-2.1.1 2510-24# sh mac-address 21

Status and Counters - Port Address Table - 21

MAC Address
-----
002673-7e9490

SH-2.1.1 2510-24#
```

Kuva 8. Ricoh-tulostimen etsiminen MAC-osoitteen perusteella komennoilla "show mac address" ja "sh mac-address 21".

Kuvassa 8 näkyy erään verkkotulostimen MAC-osoite kytkimellä komennon "show mac-address" jälkeen. Laite on kytketty porttiin 21, joka ei ole yhteydessä toiseen kytkimeen.



Kuva 9. Ricoh-tulostimen MAC-osoite internetselaimen kautta hallintakäyttöliittymällä tarkasteltuna.

Tulostimen MAC-osoitteen paikkansa pitävyys varmistettiin sen hallintakäyttöliittymästä, johon pääsi käsiksi internetselaimen kautta laitteen IP-osoitteella.

## 2.8 Konesali

Yrityksen konesalipalveluntarjoajan tiloissa sijaitsee 21 virtuaalipalvelinta sekä palomuu-ri, jota yritys ei itse hallinnoi. Lisäksi kaikki yrityksen sisäverkosta poistuva liikenne kulkee konesalipalveluntarjoajan reitittimen kautta. Palvelimiin lukeutuu muun muassa ensisijainen domain controller, sähköpostipalvelin, Microsoft Dynamics CRM -palvelin, M-files dokumenttipalvelin ja Sonet-laskunhallintapalvelin. Listaus yrityksen palvelimista löytyi osittain IT-osastolta, ja loput selvisivät domain controllerien, jotka toimivat myös DNS-palvelimina, DNS-tietueista. Domain controllerilla avattiin DNS-hallinta ja tarkasteltiin konesalipalveluntarjoajan verkon alla olevia tietueita, tarkemmin kohdassa 3.5.2 läpikäydyltä tavalla. Täältä löytyivät lähes kaikki yrityksen käytössä olevat ja jo käytöstä poistuneet palvelimet.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[186], toimisto ██████████ hostmaster ██████████	static
(same as parent folder)	Name Server (NS)	file1 ██████████	static
(same as parent folder)	Name Server (NS)	toimisto ██████████	static
10.250.40.10	Pointer (PTR)	hskk6 ██████████	static
10.250.40.11	Pointer (PTR)	hskk6 ██████████	3/20/2013 3:00:00 PM
10.250.40.12	Pointer (PTR)	data ██████████	static
10.250.40.13	Pointer (PTR)	crm ██████████	9/29/2010 10:00:00 AM
10.250.40.2	Pointer (PTR)	hskk2 ██████████	1/21/2010 11:00:00 PM
10.250.40.21	Pointer (PTR)	file1 ██████████	3/25/2012 2:00:00 PM
10.250.40.22	Pointer (PTR)	posti ██████████	7/26/2013 4:00:00 PM
10.250.40.23	Pointer (PTR)	talous ██████████	10/11/2013 10:00:00 PM
10.250.40.24	Pointer (PTR)	kanta ██████████	9/9/2010 4:00:00 AM
10.250.40.25	Pointer (PTR)	asennus ██████████	11/16/2010 7:00:00 AM
10.250.40.26	Pointer (PTR)	file2 ██████████	2/22/2012 10:00:00 AM
10.250.40.27	Pointer (PTR)	extkanta ██████████	6/8/2012 1:00:00 PM
10.250.40.4	Pointer (PTR)	hskk4 ██████████	9/6/2010 10:00:00 PM
10.250.40.40	Pointer (PTR)	dev-kanta ██████████	10/11/2010 11:00:00 AM
10.250.40.41	Pointer (PTR)	dev-crm ██████████	10/11/2010 11:00:00 AM
10.250.40.42	Pointer (PTR)	sqltest ██████████	2/18/2014 12:00:00 PM
10.250.40.43	Pointer (PTR)	sql ██████████	9/21/2015 10:00:00 AM
10.250.40.5	Pointer (PTR)	hskk5 ██████████	9/1/2011 12:00:00 PM

Kuva 10. TOIMISTO-palvelimen DNS-palvelimen hallinnan konesalipalveluntarjoajan aliverkon reverse lookup zone ennen korjauksia.

Kun lista kaikista palvelimista oli valmis, siitä ensin poistettiin käytöstä poistuneet palvelimet tarkistamalla, ovatko ne kytkettyinä verkkoon Windowsin komentokehotteen (cmd.exe) ping-komennolla, esimerkiksi ”ping 10.250.40.5”. Laitteet, jotka eivät vastanneet pingiin, merkittiin erikseen ja varmistettiin yrityksen IT-päälliköltä, etteivät ne ole enää käytössä. Tämän jälkeen laitteet poistettiin dokumentaatiosta, ja vianselvitysvaiheessa myös DNS-ohjauksista. Jäljelle jääneisiin palvelimiin kirjauduttiin etäyhteyden avulla ja tarkistettiin niissä toimivat palvelut ja niiden väliset riippuvuudet. Linux-palvelimien ominaisuudet selvitettiin yrityksen IT-päälliköltä. Tuloksista tehtiin Excel-taulukko helppoa tarkastelua varten. Lista palvelimista ja niiden ominaisuuksista löytyy liitteistä (liite 3).

## 2.9 Dokumentaation yhteenveto

Tässä vaiheessa dokumentaatio kattoi kaiken yrityksen kannalta oleellisen, eli verkon infrastruktuurin, verkkoon liitetyt laitteet käyttäjien päätelaitteita lukuun ottamatta ja tärkeimmät tiedot palvelimista, joten mietittäväksi jäi, missä muodossa dokumentaatio olisi helppoiten tarkasteltavissa ja tarpeen tullen muokattavissa. Päädyttiin Excel-taulukoihin (liitteet 2-7), jotka kokoavat kaikki hallintaa vaativat laitteet yhteen tiedostoon, sekä sitä havainnollistavaan Visio-piirrokseen (liite 9). Näin kaikki hallintaa mahdollisesti vaativien laitteiden tiedot löytyisivät yhdestä paikasta, eikä koskaan tarvitsisi enää miettiä, minkä dokumentin etsii, kun tarvitsee tietoa näistä laitteista. Excel-taulukon eri välilehdille on koottu kaikki IT-osaston useimmin tarvitsemat tiedot kustakin laitteesta. Visio-piirros havainnollistaa verkon rakennetta ja helpottaa tietyn laitteen etsimistä tarvittaessa.

## 3 Vianselvitys

### 3.1 Vianselvityksen rajausta ja tavoitteet

Vianselvityksen laajuus rajattiin yrityksen itse hallinnoimiin verkkolaitteisiin sekä domain controllereihin, sillä muut mahdollisesti vianselvitystä tarvitsevat kohteet ovat ulkopuolisten tahojen vastuulla. Näin ollen tarkastelun kohteeksi jäivät kahdeksan HP:n Procurve L2-kytkintä, HP:n WLAN-kontrolleri, yksitoista HP:n WLAN-tukiasemaa, yksi fyysinen palvelin – TOIMISTO sekä yksi virtuaalipalvelin – file1. Verkkolaitteista tulisi selvittää koko konfiguraation toimivuus ja domain controllereista lähinnä DNS- ja DHCP-palveluiden toimivuus.

Vianselvityksen tavoitteena on käydä kaikkien edellä mainittujen laitteiden toiminta yrityksen verkon osana läpi ja paikantaa virheet ja riskit konfiguraatioissa mahdollisimman tarkasti sekä korjata ne tai kirjata ylös myöhempää korjausta varten.

### 3.2 Vianselvityksen toteutus

Vianselvitystä varten kaikille yrityksen työntekijöille lähetettiin kysely verkon ongelmista (liite 8). Vastauksena kyselyyn ei tullut mitään, mikä viittaisi verkon ongelmiin. Tämä viittaisi siihen, että verkossa ei ole kriittisiä ongelmia.

Vianselvitys toteutettiin katsomalla läpi kytkimistä konfiguraatiodokumentit, ottamalla käyttöön kytkimille ulkoisen lokipalvelimen ja seuraamalla saapuvia lokitapahtumia. Kytkinten konfiguraatioita muutettiin vastaan tulleiden ongelmien myötä, kunnes niiden toimivuuteen oltiin tyytyväisiä. WLAN-controllerin asetukset tarkastettiin hallintakäyttöliittymän kautta ja yrityksen WLAN:ien toimivuutta testattiin liittymällä niihin kannettavalla tietokoneella. Domain controllereista, jotka molemmat toimivat DNS- ja DHCP-palvelimina, tarkastettiin DNS:n ja DHCP:n asetukset verraten niitä Microsoftin suosituksiin ja yrityksen verkon toivottuun toimintaan sekä poistamalla vanhentuneita tietoja.

### 3.3 Kytkimet

Yrityksen Helsingin toimipisteen kytkimet ovat malleiltaan eriäviä, ja osa on asennettu eri aikaan eri asentajien toimesta. Tästä seurasi, että niiden konfiguraatiot eivät olleet samanlaiset ja vaativat jonkinäköistä yhtenäistämistä. Kytkinten konfiguroinnissa hyödynnettiin kohdassa 2.3.2 mainittua kytkimen SW-5.2.1 hallinta-VLAN:iin liitettyä porttia, joka oli kytketty palvelimeen ANNA ja mahdollisti kaikkien kytkinten hallinnan etäyhteyden kautta Tera Term -ohjelmalla.

### 3.3.1 VLAN:it

Viimeisimpänä asennettujen kytkinten SW-2.1.1 ja SW-2.1.2 hallinta-VLAN (VLAN ID 66), oli ilmeisesti jäänyt vakioasetuksille, sillä sen nimenä oli "Management", eikä "Hallinta" kuten muissa kytkimissä. Tämä väärin konfiguroitu VLAN aiheutti sen, ettei kyseisiä kytkimiä voinut etähallita. Kytkimiin otettiin yhteys konsoliportin kautta kohdassa 2.4.1 mainitulla tavalla. Samalla selvisi ettei kytkimiin oltu asetettu salasanoja. Kytkimillä siirryttiin globaaliin konfigurointitilaan komennolla "conf t". Väärin nimetty VLAN poistettiin komennolla: "no vlan 66". "No"-etuliitteellä ajatut komennot poistuvat käytössä olevasta konfiguraatiosta. Tämän jälkeen se luotiin uudelleen komennolla "vlan 66 name "Hallinta"". Luonnin jälkeen siirryttiin hallinta-VLAN:n konfigurointitilaan komennolla "vlan 66". Tämän jälkeen VLAN 66 liitettiin kytkinten verkkoporttiin 1 komennolla "untagged 1" ja runkoportteihin jotka olivat yhteydessä toisiin kytkimiin komennolla "tagged <portti, joka on yhteydessä toiseen kytkimeen>". Molempien kytkinten hallinta-VLAN:iin lisättiin myös hallintaosoitteet – samat kuin väärinnimetyissä VLAN:eissa oli ollut. Tämä tapahtui komennolla "ip address <hallintaosoite> 255.255.255.0". [3.]

Näiden muutosten jälkeen VLAN 66:n nimi oli sama kuin muissa kytkimissä ja sen IP-osoite oli samassa osoitevaruudessa muiden kytkinten kanssa. Kytkimiä pystyi nyt etähallitsemaan normaalisti. Samalla kytkimiin asetettiin samat hallinta- ja tarkastelusalasanat kuin muihinkin kytkimiin globaalista konfigurointitilasta komennolla "password manager" ja "password operator". Samoilla komennolla asetettiin salasanat myös kytkimeen SW-5.2.1 jonka salasanat resetoitiin etupaneelin "Clear"-nappia painamalla. [5; 6]

```

10.255.255.21:23 - Tera Term VT
File Edit Setup Control Window Help
SW-2.1.1 2510-24(config)# sh run
Running configuration:
; J9019A Configuration Editor; Created on release #Q.11.17
hostname "SW-2.1.1 2510-24"
snmp-server contact [REDACTED]
snmp-server location [REDACTED] 2. Krs"
max-vlans 64
interface 26
  name "to_rk5.1.1-TEMP"
exit
ip default-gateway 10.255.255.254
ntp server 193.229.2.70 1
ip ttime manual 193.229.0.118
logging 10.255.255.15
snmp-server community [REDACTED] Unrestricted
snmp-server host 194.241.70.114 "public"
vlan 1
  name "DEFAULT_VLAN"
  no ip address
  no untagged 1-26
  exit
vlan 2
  name [REDACTED]
  untagged 2-26
  no ip address
  exit
vlan 66
  name "Hallinta"
  untagged 1
  ip address 10.255.255.21 255.255.255.0
  tagged 25-26
  exit
qos type-of-service ip-precedence
spanning-tree
SW-2.1.1 2510-24(config)#

```

Kuva 11. Etäyhteys Tera Term -ohjelman avulla uudelleenkonfiguroituun kytkimeen SW-2.1.1.

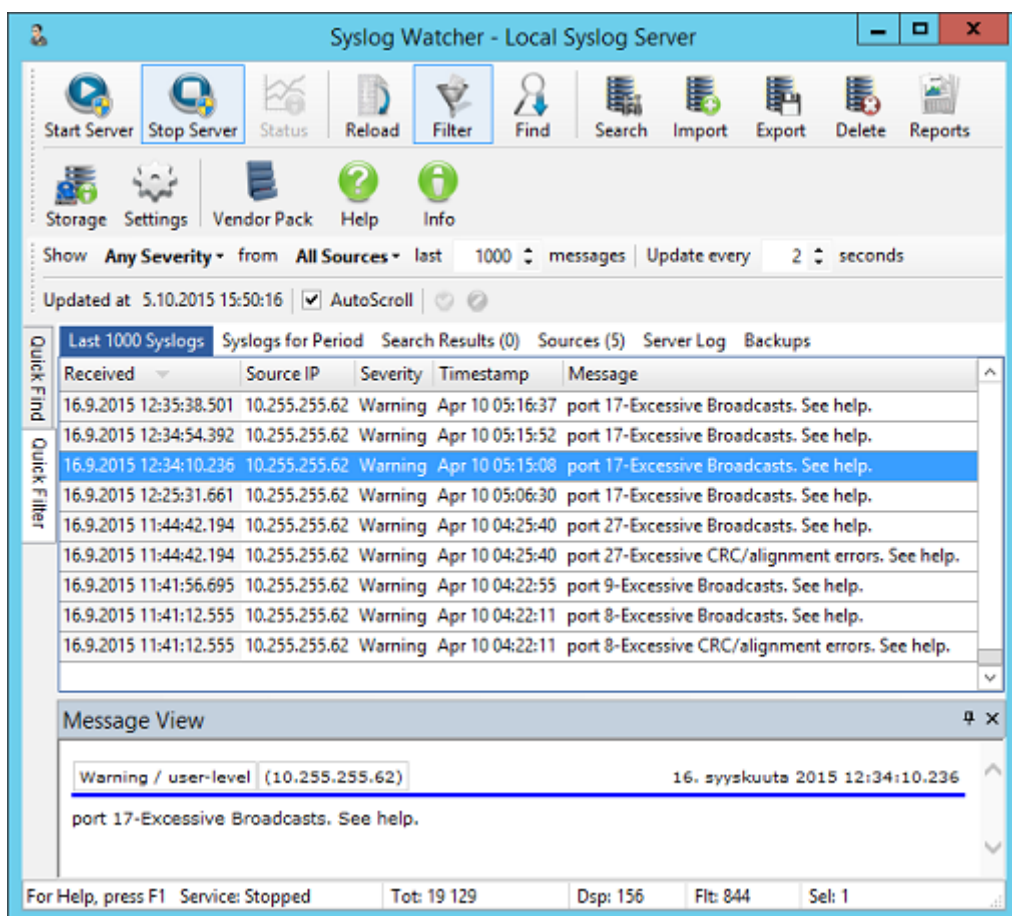
### 3.3.2 Tapahtumarekisteripalvelin

Vikaselvitystä varten kaikki kytkimet konfiguroitiin lähettämään lokitapahtumat ANNA-palvelimen hallinta-VLAN:in aliverkossa (10.255.255.1/24) sijaitsevaan verkkokorttiin, jonka osoitteeksi oli aiemmin asetettu 10.255.255.15. Tämä tapahtui ajamalla kaikissa kytkimissä komento "logging 10.255.255.15" globaalissa konfiguraatiotilassa. [5; 6.]



Palvelimelle ANNA asennettiin väliaikaisesti lokien lukemista varten Syslog Watcher -nimisen lokien lukuohjelman ilmaisversio. Ohjelman voi noutaa osoitteesta <http://www.snmpsoft.com/syslogwatcher/syslog-server.html>.

Syslog Watcher on SnmpSoft'in syslog-tapahtumalokien vastaanottamiseen, lukemiseen ja tallentamiseen tarkoitettu ohjelma. Ohjelman ilmaisversio on rajoitettu vastaanottamaan lokitapahtumia maksimissaan viideltä laitteelta kerrallaan. Tämä aiheutti ongelmia seurattavia laitteita ollessa seitsemän, jolloin joiltain laitteilta täytyi lokien lähetys pysäyttää tehdäkseen tilaa vuorostaan toisille laitteille. Myöhemmin, tämän työn seuranta-vaiheessa siirryttiin käyttämään rajoittamatonta lokien seurantaohjelmaa.



Kuva 12. Syslog Watcher ANNA-palvelimella. Kuvassa näkyvät myös kytkinten toimimattomista ajan synkronointiasetuksista johtuvat aikaleimojen virheet. Ajan synkronointi kytkimille korjattiin vianselvitysvaiheessa.

Lokeja seurattiin noin viikon ajan. Lokeihin ei ilmestynyt mitään erityisen huolestuttavaa.

”Excessive Broadcasts” ja ”Excessive CRC/alignment errors” -viestit tulivat yleensä käyttäjien tietokoneen verkkoon liittymisen yhteydessä ja kestivät muutaman sekunnin.

Tämä on HP:n foorumeiden käyttäjien kommenttien mukaan normaalia toimintaa ja sen voi jättää huomiotta jos se ei jatku muutamaa sekuntia pidempään. [7; 8.] Näin myös tapahtui, ja nämä varoitusviestit jätettiin huomioimatta. Viestejä seurattiin kuitenkin tarkasti, että voitiin varmuudella sanoa niiden kestävän vain muutaman sekunnin.

### 3.3.3 Aikapalvelu ja aikapalvelin

Lokitapahtumien aikaleimat eivät näyttäneet pitävän paikkaansa minkään kytkimen kohdalla, joten päätettiin asettaa kaikille kytkimille uusi aikapalvelin. Palvelimelle ANNA otettiin käyttöön NTP-palvelu ajan synkronoimiseen kytkimille.

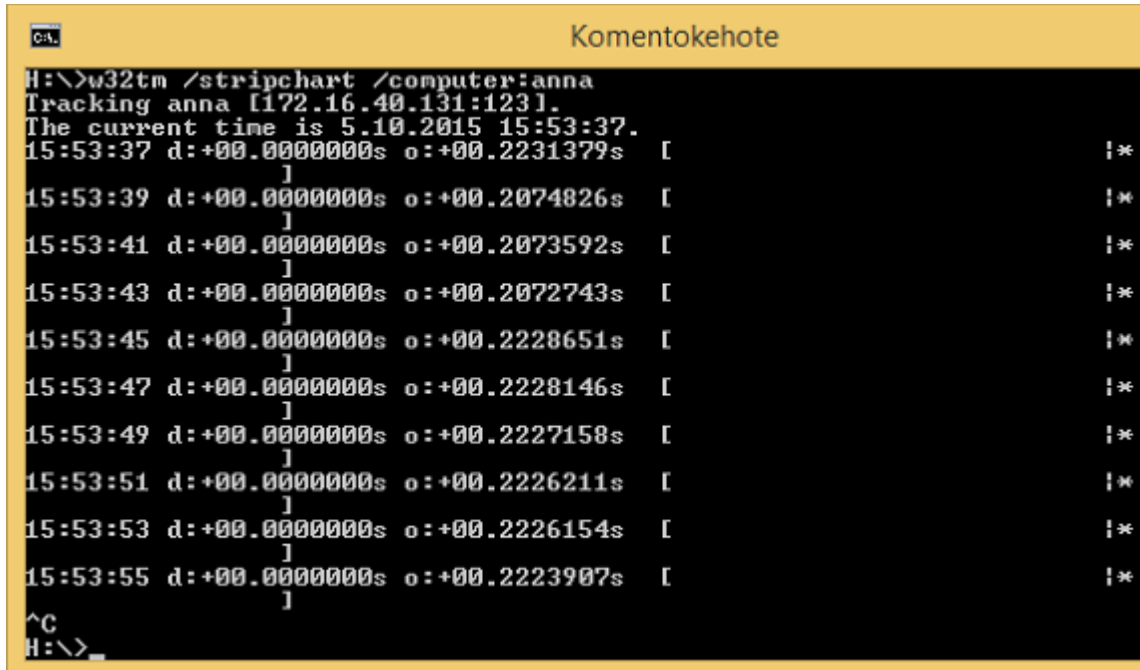
NTP eli Network Time Protocol mahdollistaa ajan synkronoimisen erilaisille verkkoon kytketyille laitteille NTP-palvelimen kautta. NTP-palvelimena tässä työssä käytettiin ANNA-palvelinta, jossa on Windows Server 2012 R2 -käyttöjärjestelmä. Helpoin tapa konfiguroida NTP-palvelin on asettaa se vastaanottamaan aika valmiiksi konfiguroiduilta ja yleisesti luotetuilta palvelimilta, esimerkiksi osoitteesta pool.ntp.org. Pool.ntp.org on omien sanojensa mukaan:

”Suuri virtuaalinen klusteri aikapalvelimia, joka tarjoaa luotettavan ja helppokäyttöisen NTP-palvelun miljoonille käyttäjille. Pooli on käytössä miljoonilla tai kymmenillä miljoonilla järjestelmillä ympäri maailman. Se on vakio- ”aikapalvelin” useimmille merkittävälle Linux distribuutioille ja monille verkossa oleville laitteille.” [9.]

NTP-palvelimen käyttöönotossa käytettiin Windowsin Powershell komentokehotetta (powershell.exe) ja Windowsin rekisterieditoria (regedit.exe). ANNA:n w32time -palvelu konfiguroitiin vastaanottamaan aika pool.ntp.org osoitteesta Powershell-ikkunassa komentamalla ”w32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL”.

Tämän jälkeen rekisteristä muutettiin rekisterieditorilla polusta ”HKLM\system\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer” avaimen ”Enabled” arvo ”DWORD 0”:sta ”DWORD 1”:ksi.

Aikapalvelu vielä käynnistettiin uudelleen komennoilla "Stop-Service w32time" ja "Start-Service w32time". Aikapalvelua testattiin toiselta koneelta komentokehötteen komennon "w32tm /stripchart /computer:anna" avulla. Kuvassa olevista komennon tuloksista näkyy, että paikallinen tietokone saa ajan palvelimelta ANNA ja että saatu aika eroaa noin 0,2 sekuntia paikallisesta ajasta. [10; 11; 12; 13.]



```

CA. Komentokehote
H:\>w32tm /stripchart /computer:anna
Tracking anna [172.16.40.131:123].
The current time is 5.10.2015 15:53:37.
15:53:37 d:+00.00000000s o:+00.2231379s [ |*
    ]
15:53:39 d:+00.00000000s o:+00.2074826s [ |*
    ]
15:53:41 d:+00.00000000s o:+00.2073592s [ |*
    ]
15:53:43 d:+00.00000000s o:+00.2072743s [ |*
    ]
15:53:45 d:+00.00000000s o:+00.2228651s [ |*
    ]
15:53:47 d:+00.00000000s o:+00.2228146s [ |*
    ]
15:53:49 d:+00.00000000s o:+00.2227158s [ |*
    ]
15:53:51 d:+00.00000000s o:+00.2226211s [ |*
    ]
15:53:53 d:+00.00000000s o:+00.2226154s [ |*
    ]
15:53:55 d:+00.00000000s o:+00.2223907s [ |*
    ]
^C
H:\>

```

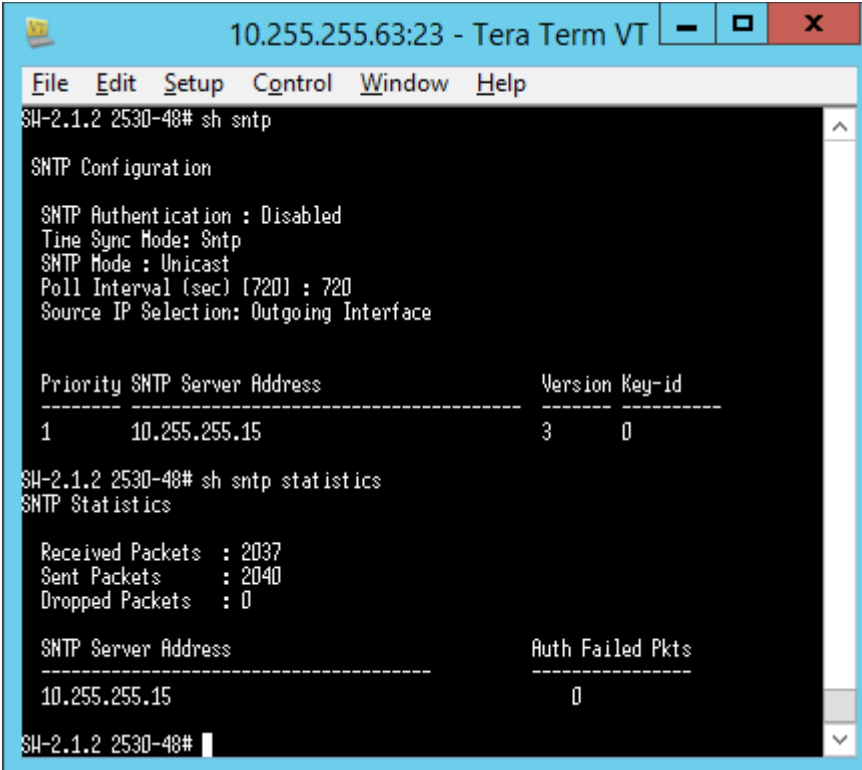
Kuva 13. Aikapalvelun testaus Windowsin komentokehöttelellä.

Kaikista kytkimistä poistettiin sen jälkeen edelliset aikapalvelukonfiguraatiot ajamalla konfiguraatitietojen relevantit rivit läpi globaalissa konfiguraatitilassa "no"-etuliitteellä. Tämän jälkeen kaikkiin kytkimiin ajettiin mallista riippuen joko komennot "timesync sntp", "sntp unicast" ja "sntp server 10.255.255.15" tai "sntp server priority 1 10.255.255.15". Koska aikapalvelu antaa GMT-ajan, täytyi kytkimiin lisäksi konfiguroida aikavyöhyke ja kesäajan muutokset. Aikavyöhyke asetettiin komennolla "time timezone 120", joka lisää aikaan 120 minuuttia, asettaen aikavyöhykkeeksi "GMT+2".

Kesäaikaan siirtyminen automatisoitiin komennolla "time daylight-time-rule western-europe". Lisäksi, koska kytkinten aika erosi oikeasta ajasta vuosilla, täytyi se asettaa manuaalisesti lähemmäksi totuutta, jotta aikapalvelin suostui suorittamaan synkronoinnin.

Tämä tapahtui komennolla "time MM/DD/YYYY HH:MM:SS", jossa ensimmäinen "MM" korvattiin kuukaudella, "DD" päivällä, "YYYY" vuodella, "HH" tunnilla, toinen "MM" minuutilla ja "SS" sekunnilla. Komento ajettiin minuutin tarkkuudella.

Konfiguraatiot testattiin komennoilla "sh sntp" ja "sh sntp statistics", sekä seuraamalla tapahtumarekisteriin ilmestyviä viestejä ajan synkronoinnista. Kytkinten vakio synkronointiaikaväli oli 720 sekuntia, eli 12 minuuttia. Viimeistään tämän ajan kuluttua kaikki kytkimet olivat onnistuneesti synkronoineet aikansa tapahtumarekisterin mukaan. [5; 6; 14; 15.]



```

10.255.255.63:23 - Tera Term VT
File Edit Setup Control Window Help
SH-2.1.2 2530-48# sh sntp
SNTP Configuration
SNTP Authentication : Disabled
Time Sync Mode: Sntp
SNTP Mode : Unicast
Poll Interval (sec) [720] : 720
Source IP Selection: Outgoing Interface

Priority SNTP Server Address          Version Key-id
-----
1        10.255.255.15                 3          0

SH-2.1.2 2530-48# sh sntp statistics
SNTP Statistics
Received Packets : 2037
Sent Packets    : 2040
Dropped Packets : 0

SNTP Server Address          Auth Failed Pkts
-----
10.255.255.15                0

SH-2.1.2 2530-48#

```

Kuva 14. Aikapalvelun toiminnan tarkastelu kytkimellä SW-2.1.2.

### 3.3.4 Spanning tree

STP eli Spanning Tree Protocol on L2-kytkimissä verkon silmukoiden havaitsemiseen ja estämiseen tarkoitettu protokolla.

Sen avulla kytkimet muodostavat jokaisen siihen osallistuvan laitteen välille vain yhden aktiivisen yhteyden ja poistavat vaihtoehtoiset yhteydet käytöstä. Verkon silmukka syntyy, kun kahden L2-verkon pisteen välillä on useampi kuin yksi mahdollinen reitti. Kytkimen lähettäessä broadcast-paketteja kaikista muista kuin tuloportista ulospäin, pääsevät paketit silmukassa lopulta takaisin kytkimeen ja lähtevät edelleen ulos kaikista portsista tuloportista, liikkuen verkossa loputtomasti. Tämä kuormittaa laitteita kohtuuttomasti ja lopulta jopa lopettaa niiden toiminnan. Tätä ongelmatilannetta kutsutaan myös broadcast-myrskyksi. Silmukka muodostuu esimerkiksi kytkemällä yhden kaapelin molemmat päät samaan kytkimeen, tai kytkemällä kahden kytkimen välille kaksi kaapelia ilman erityisiä asetuksia. [16; 17.]

Yrityksen kytkimissä käytetään MSTP:tä (Multiple Spanning Tree Protocol), joka mahdollistaa oman spanning treen määrityksen jokaiselle VLAN:ille. Spanning tree on kuitenkin määritetty vain yleisellä tasolla, koska yrityksen verkossa ei ole tarvetta VLAN-kohtaisille spanning tree -instansseille. Liitteestä 9 näkyy, että kytkin 5.1.1 on verkon "core switch" eli viimeinen kytkin ulospäin suuntautuvalla liikenteelle. Sen halutaan siis olevan myös spanning treen root -kytkin, eli spanning treen lähtöpiste. Tällöin kytkimet etsivät lyhyimmän reitin ulos verkosta, eivätkä satunnaisesti kytkimeen verkossa. Spanning tree päättää automaattisesti root-kytkimen MAC-osoitteen perusteella jos manuaalisia prioriteetteja ei ole asetettu. [18; 19.] Kytkimien konfiguraatiodietoista nähtiin, että manuaalisia prioriteetteja ei ollut asetettu.

Tarkastellessa spanning treen asetuksia kytkimellä 5.1.1 komennolla "sh spanning-tree" nähtiin, että se on asettunut vakioasetuksilla IST:n eli Internal Spanning Treen root-kytkimeksi, mutta ei CST:n, eli Common Spanning Treen. HP:n kytkimissä vakioasetuksilla jokaisella kytkimellä on oma IST-instanssinsa joiden väliset yhteydet määräytyvät CST:n mukaisesti. Vakioasetuksilla CST-instansseja on yksi ja sen root-kytkimeksi asettuu pienimmän MAC-osoitteen omaava kytkin. [20.]

```

10.255.255.51:23 - Tera Term VT
File Edit Setup Control Window Help
SW-5.1.1 2510G-48(config)# sh spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled : Yes
Force Version : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 002347-3ec500
Switch Priority : 32768
Max Age : 20
Max Hops : 20
Forward Delay : 15

Topology Change Count : 1896
Time Since Last Change : 31 days

CST Root MAC Address : 0019bb-a2e760
CST Root Priority : 32768
CST Root Path Cost : 20000
CST Root Port : 41

IST Regional Root MAC Address : 002347-3ec500
IST Regional Root Priority : 32768
IST Regional Root Path Cost : 0
IST Remaining Hops : 20

Root Guard Ports :
TCN Guard Ports :
Protected Ports :
Filtered Ports :

Port Type Cost Priority State Designated Bridge Hello Time PTP Edge
-----+-----+-----+-----+-----+-----+-----+-----+-----
1 100/1000T Auto 128 Disabled
2 100/1000T Auto 128 Disabled
3 100/1000T 20000 128 Forwarding 002347-3ec500 2 Yes Yes

```

Kuva 15. Spanning treen tila kytkimellä SW-5.1.1 ennen muutoksia.

Kytkimestä SW-5.1.1 haluttiin CST:n root-kytkin, joten sille asetettiin manuaalinen spanning tree -prioriteetti globaalista konfiguraatiotilasta komennolla "spanning-tree priority 0". [18] Tarkasteltaessa spanning treen asetuksia uudelleen komennolla "sh spanning-tree" nähdään, että kytkin on nyt root-kytkin myös CST:lle ja sen root-prioriteetti on 0.

```

10.255.255.51:23 - Tera Term VT
File Edit Setup Control Window Help
SW-5.1.1 2510G-48# sh spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled : Yes
Force Version : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 002347-3ec500
Switch Priority : 0
Max Age : 20
Max Hops : 20
Forward Delay : 15

Topology Change Count : 1928
Time Since Last Change : 46 mins

CST Root MAC Address : 002347-3ec500
CST Root Priority : 0
CST Root Path Cost : 0
CST Root Port : This switch is root

IST Regional Root MAC Address : 002347-3ec500
IST Regional Root Priority : 0
IST Regional Root Path Cost : 0
IST Remaining Hops : 20

Root Guard Ports :
TCN Guard Ports :
Protected Ports :
Filtered Ports :

Port Type Cost Priority State Designated Bridge Hello Time PtP Edge
-----+-----+-----+-----+-----+-----+-----+-----+
1 100/1000T Auto 128 Disabled
2 100/1000T 20000 128 Forwarding 002347-3ec500 2 Yes Yes
3 100/1000T 20000 128 Forwarding 002347-3ec500 2 Yes Yes
4 100/1000T Auto 128 Disabled

```

Kuva 16. Spanning treen tila kytkimellä SW-5.1.1 muutosten jälkeen.

Spanning-tree topologian muutos varmistettiin kirjautumalla muillekin kytkimille Tera Termin avulla ja tarkastamalla niiden spanning treen tilanne komennolla "sh spanning-tree". Topologian muutos levisi kaikille kytkimille oikein, ja ne tunnistivat kytkimen SW-5.1.1 uutena CST:n root-kytkimenään.

Kytokinten konfiguraatioiden ollessa valmiit, tallennettiin muutokset komennolla "write memory". Tällöin kytkinten asetukset eivät häviä virtakatkosten tai uudelleenkäynnistysten seurauksena. [5; 6]

The image shows two screenshots of Tera Term VT windows. The top window is titled '10.255.255.63:23 - Tera Term VT' and shows the output of the 'sh spanning-tree' command on switch SW-2.1.2. The bottom window is titled '10.255.255.62:23 - Tera Term VT' and shows the output of the 'sh span' command on switch SW-2.2.1. Both windows display 'Multiple Spanning Tree (MST) Information' with various parameters such as STP Enabled, Force Version, IST Mapped VLANs, Switch MAC Address, Switch Priority, Max Age, Max Hops, Forward Delay, Topology Change Count, Time Since Last Change, CST Root MAC Address, CST Root Priority, CST Root Path Cost, CST Root Port, IST Regional Root MAC Address, IST Regional Root Priority, IST Regional Root Path Cost, IST Remaining Hops, Root Guard Ports, and Loop Guard Ports.

```

10.255.255.63:23 - Tera Term VT
File Edit Setup Control Window Help
SW-2.1.2 2530-48# sh spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled : Yes
Force Version : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 288023-6a2c00
Switch Priority : 32768
Max Age : 20
Max Hops : 20
Forward Delay : 15

Topology Change Count : 1
Time Since Last Change : 360 days

CST Root MAC Address : 002347-3ec500
CST Root Priority : 0
CST Root Path Cost : 40000
CST Root Port : 47

IST Regional Root MAC Address : 288023-6a2c00
IST Regional Root Priority : 32768
IST Regional Root Path Cost : 0
IST Remaining Hops : 20

Root Guard Ports :
Loop Guard Ports :

10.255.255.62:23 - Tera Term VT
File Edit Setup Control Window Help
SW-2.2.1 25106-48# sh span

Multiple Spanning Tree (MST) Information

STP Enabled : Yes
Force Version : MSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : c09134-7a74c0
Switch Priority : 32768
Max Age : 20
Max Hops : 20
Forward Delay : 15

Topology Change Count : 65
Time Since Last Change : 17 days

CST Root MAC Address : 002347-3ec500
CST Root Priority : 0
CST Root Path Cost : 20000
CST Root Port : 48

IST Regional Root MAC Address : c09134-7a74c0
IST Regional Root Priority : 32768
IST Regional Root Path Cost : 0
IST Remaining Hops : 20

Root Guard Ports :
TCN Guard Ports :

```

Kuva 17. Spanning treen tila kytkimillä SW-2.1.2 ja SW-2.2.1 muutosten jälkeen. Kuvasta näkyy myös kytkimien olevan omien IST-instanssiensa root-kytkimet. Aikojen heittälyt johtuvat kellojen aiemmista vääristä ajoista kytkimillä.



### 3.4 WLAN-kontrolleri ja WLAN-tukiasemat

Yrityksen Helsingin toimipisteen tiloissa toimivan langattoman verkon toimintaa ohjaa HP:n MSM760 Controller. Se mahdollistaa kaikkien Helsingin toimipisteen langattomien tukiasemien keskitetyn hallinnan. Helsingin toimipisteessä on käytössä kolme eri WLAN:ia.

Taulukko 4. WLAN:ien tiedot

WLAN ssid	Käyttäjärühmä	Pääsy toimialueeseen
"Vieras"	Ulkoinen/Sisäinen	Ei
"Vieras2"	Ulkoinen/Sisäinen	Ei
"Sisäinen"	Sisäinen	Kyllä

Vierailijoiden käyttöön tarkoitetuissa langattomissa verkoissa "Vieras" ja "Vieras2" on julkisesti saatavilla oleva salasana ja yrityksen sisäisten laitteiden käyttöön tarkoitetun langattoman verkon käyttö vaatii toimialuetunnukset. Sisäinen verkko on myös liitetty toimialueeseen ja siitä on pääsy verkkolevyille, verkkotulostimille ja kaikkeen muuhun, mihin yrityksen langallisesta verkosta normaalisti pääsee. Tietoturvasyistä vierailijoiden käyttöön tarkoitetuista verkoista ei ole pääsyä toimialueeseen. Niiden liikenne on erotettu "Vieras" VLAN:iin, joka on konfiguroitu sekä WLAN-kontrollerille, että kytkimelle SW-5.1.1, johon se on liitetty.

WLAN-kontrollerin hallintakäyttöliittymään pääsee käsiksi sen IP-osoitteella verkkoselaimen kautta. Käyttöliittymästä tarkistettiin VLAN-konfiguraatio, jolla vierasverkkojen liikenne eristetään. Jokaisella WLAN:lla on kontrollerissa oma VSC. Yhden VSC:n asetukset vaikuttavat kaikkien määritettyjen tukiasemien asetuksiin, mahdollistaen helpon keskitetyn hallinnan jokaisen WLAN:n osalta. [21.]

**Add/Edit VLAN**

**General** ?

Port: Internet port

**VLAN** ?

VLAN ID: 99 (Vieras)

**Assign IP address via** ?

DHCP client

Static

IP address: 192.168.1.200

Mask: 255.255.255.0

Gateway: 192.168.1.1

None

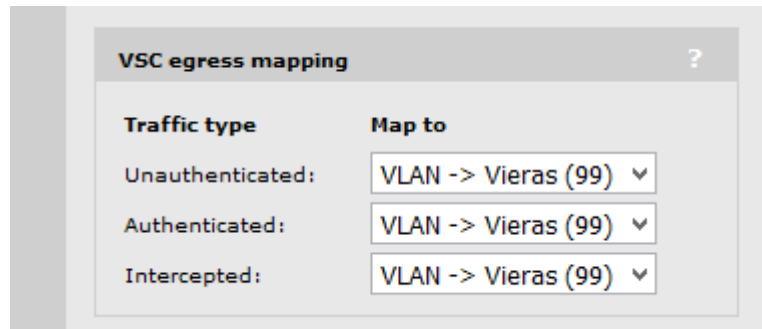
**Network address translation (NAT)** ?

Enabled  Disabled

Cancel Delete Save

Kuva 18. VLAN-asetukset HP:n WLAN-kontrollerin hallintakäyttöliittymässä.

Add/Edit VLAN -ikkunassa näkyy Vieras-VLAN:n asetukset. Se on liitetty "Internet port"-porttiin, joka on yhteydessä kytkimeen SW-5.1.1. Tähän kytkimen porttiin on konfiguroitu myös kytkimellä VLAN "Vieras". VLAN:lle on asetettu manuaaliset IP-asetukset ja NAT on otettu käyttöön. VLAN:lle on oltava määritettynä IP-osoite, jotta sitä voidaan käyttää ulospäin suuntautuvalla liikenteelle (egress mapping). [21.]



Kuva 19. Julkisista WLAN:eista ulospäin suuntautuvan liikenteen siirto Vieras-VLAN:iin HP:n WLAN-kontrollerin hallintakäyttöliittymässä.

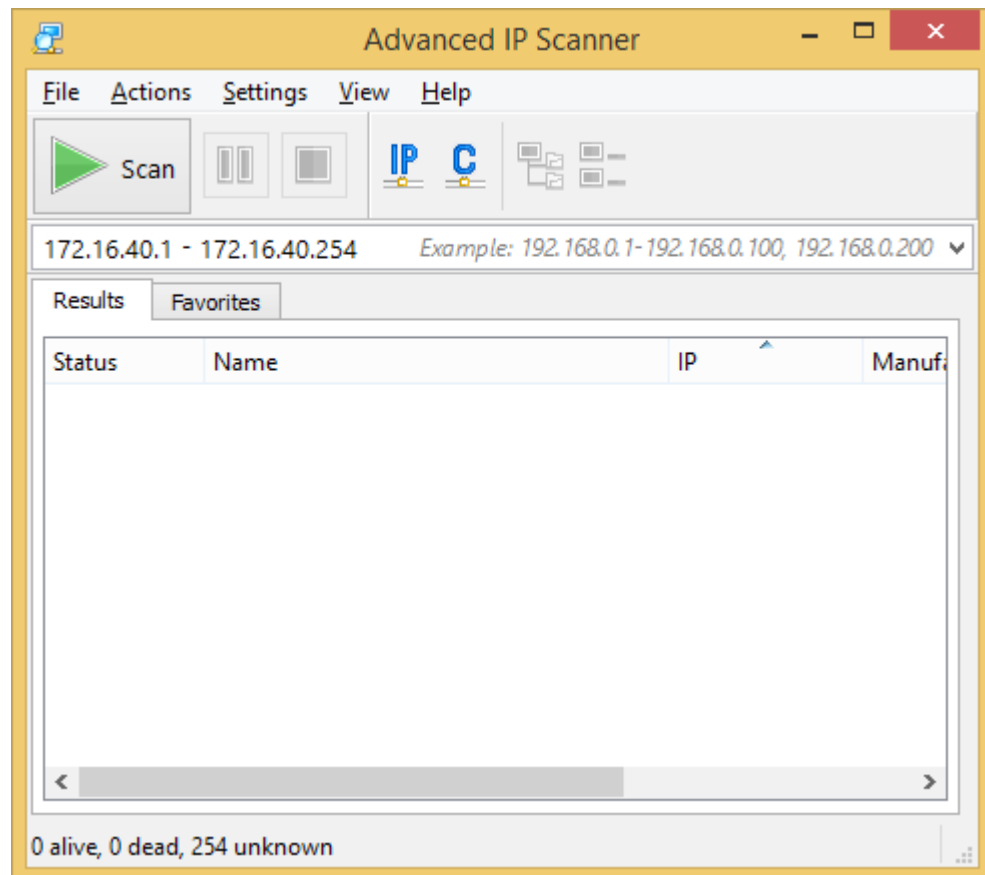
”VSC egress mapping” -kohdasta näkyy, että vierasverkoissa kaikenlaisen ulospäin suuntautuva, eli kaikki käyttäjien liikenne siirretään VLAN:iin ”Vieras” (ID 99). [21.] Tämä VLAN ei ole missään yhteyksissä sisäiseen VLAN:iin.

Myös yrityksen työntekijöiden älypuhelimet käyttävät vierasverkkoa, sillä niiden tietoturvallisuudesta on lähes mahdotonta olla perillä lukuisten mallien ja mahdollisesti käyttäjien asentamien sovellusten seurauksena. Koska WLAN:ien kuuluvuuden ja toimivuuden tiedettiin olevan hyviä, tyydyttiin testaamaan tämän VLAN:illa toteutetun eristyksen toimivuutta ja tarkastamaan WLAN:ien salausasetukset. Kannettavalla tietokoneella liitettiin jokaiseen WLAN:iin vuorotellen ja testattiin Windowsin komentokehotteen ping-komennolla yhteyttä osoitteisiin

- google.fi
- TOIMISTO
- ANNA.

Yhteydet toimivat juuri niin kuin kuuluikin. Sisäisestä WLAN:sta sai yhteyden kaikkiin osoitteisiin ja verkkolevyihin. Vieraskäyttöön tarkoitettuista verkoista ei saanut yhteyttä kumpaankaan sisäiseen palvelimeen, mutta ulospäin suuntautuvat yhteydet (google.fi) toimivat normaalisti. Windows Explorerin ”Verkko”-alue ei myöskään näyttänyt mitään muita laitteita vierasverkoissa. Sisäisessä verkossa näkymässä näkyi kaikki langalliseen sekä langattomaan sisäverkkoon liitetyt käyttäjien tietokoneet sekä ANNA-palvelin. Yhteydet muihinkin sisäisiin palvelimiin toimivat normaalisti.

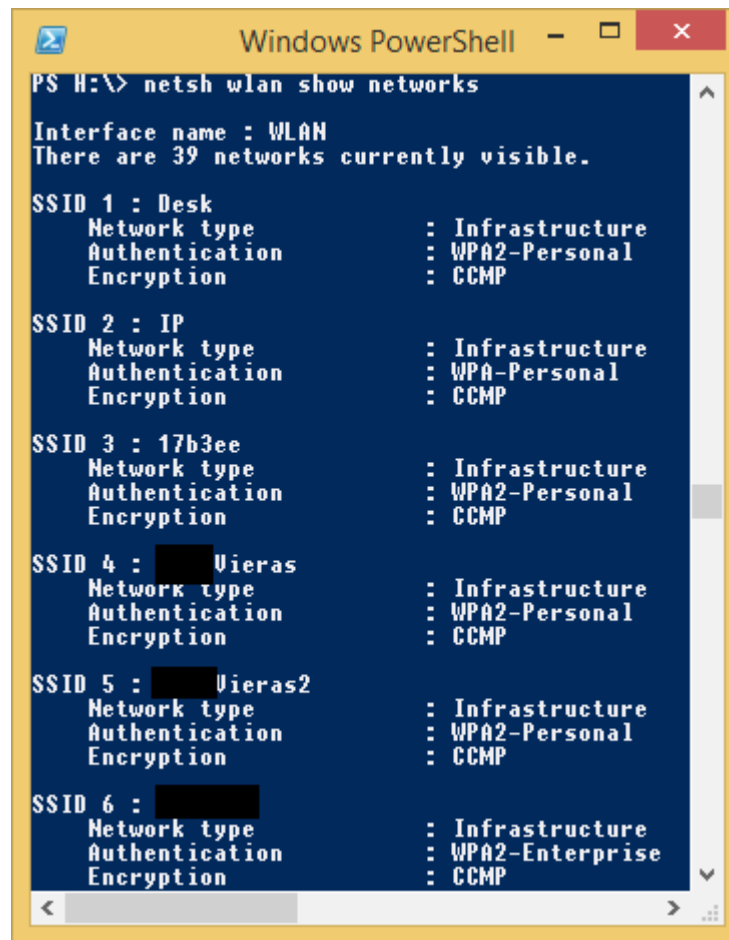
Vierasverkoissa ajettiin myös Advanced IP Scanner Helsingin toimiston päätelaitteiden osoitealueelle (172.16.40.1/24).



Kuva 20. Advanced IP Scanner ajettuna Vieras-WLAN:ssa, Helsingin toimiston käyttäjien laitteille varatulla aliverkossa. Ohjelma ei löytänyt yhtään laitetta.

Skanneri ei löytänyt yhtäkään laitetta sisäverkon osoitealueelta. Näiden testien perusteella voidaan todeta, että VLAN-eristys toimii hyvin eikä vaadi muutoksia.

Tämän jälkeen varmistettiin WLAN:ien salauksien toimivuus tarkastelemalla niiden ominaisuuksia PowerShell-komentokehotteen kautta komennolla "netsh wlan show networks". Tämä komento listaa tietokoneen havaitsemat WLAN-yhteydet ja niiden salaustyyppit. [22.]



```
Windows PowerShell
PS H:\> netsh wlan show networks

Interface name : WLAN
There are 39 networks currently visible.

SSID 1 : Desk
    Network type           : Infrastructure
    Authentication         : WPA2-Personal
    Encryption             : CCMP

SSID 2 : IP
    Network type           : Infrastructure
    Authentication         : WPA-Personal
    Encryption             : CCMP

SSID 3 : 17b3ee
    Network type           : Infrastructure
    Authentication         : WPA2-Personal
    Encryption             : CCMP

SSID 4 : █████ Uieras
    Network type           : Infrastructure
    Authentication         : WPA2-Personal
    Encryption             : CCMP

SSID 5 : █████ Uieras2
    Network type           : Infrastructure
    Authentication         : WPA2-Personal
    Encryption             : CCMP

SSID 6 : █████
    Network type           : Infrastructure
    Authentication         : WPA2-Enterprise
    Encryption             : CCMP
```

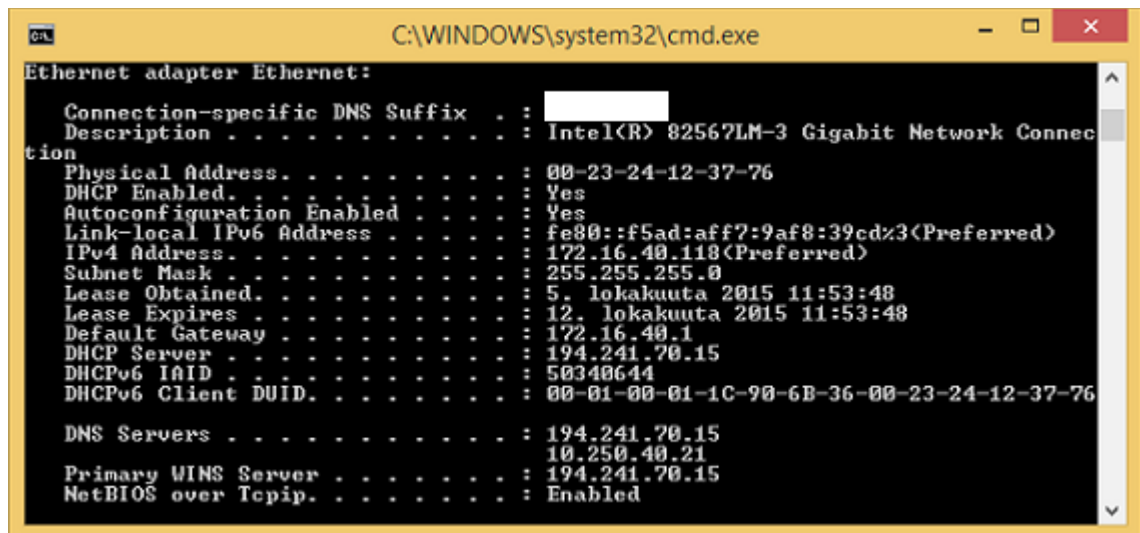
Kuva 21. Langattomien verkkojen tietojen tarkastelu Windowsin PowerShell-komentokehötteen kautta. Yrityksen langattomat verkot ovat kuvassa SSID 4, 5 ja 6.

Langattomat verkot on konfiguroitu käyttämään WPA2-autentikointia CCMP-salauksella. Tämän on yksi vahvimmista yleisesti käytetyistä WLAN:n suojausteknologioista joten tämän vianselvityksen puolesta WLAN:ien toiminta on moitteeton. [23.]

### 3.5 Domain controllerit

Yrityksen kahden domain controllerin (file1 ja TOIMISTO) toiminnan osalta tämän vian-selvityksen rajaukseen sisältyivät DHCP-poolien ja DNS-ohjauksien konfiguraatiot sekä domain controllerien perustason toiminnan tarkistus.

File1:llä ja TOIMISTO:lla on molemmissa käyttöjärjestelminä Windows server 2008 R2. Molempiin palvelimiin on myös asennettu roolit DHCP-palvelin ja DNS-palvelin. Palvelimiin otettiin etäyhteys Windowsin etähallintatyökalulla (mstsc.exe) ja konfiguraatioita verrattiin keskenään, internetpalveluntarjoajan toimittamaan aliverkkodokumenttiin (liite 1), sekä dokumentaatiovaiheessa kerättyihin tietoihin yrityksen palvelimista. Tämän jälkeen konfiguraatioista korjattiin väärät ja vanhentuneet tiedot. Ensiksi varmistettiin, että toimialueeseen liitetty tietokone sai haettua automaattisesti molempien palvelimien tiedot oikein komennolla ”ipconfig /all”



```

C:\WINDOWS\system32\cmd.exe

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
    Physical Address. . . . . : 00-23-24-12-37-76
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f5ad:aff7:9af8:39cd%3(Preferred)
    IPv4 Address. . . . . : 172.16.40.118(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 5. lokakuuta 2015 11:53:48
    Lease Expires . . . . . : 12. lokakuuta 2015 11:53:48
    Default Gateway . . . . . : 172.16.40.1
    DHCP Server . . . . . : 194.241.70.15
    DHCPv6 IAID . . . . . : 50340644
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1C-90-6B-36-00-23-24-12-37-76

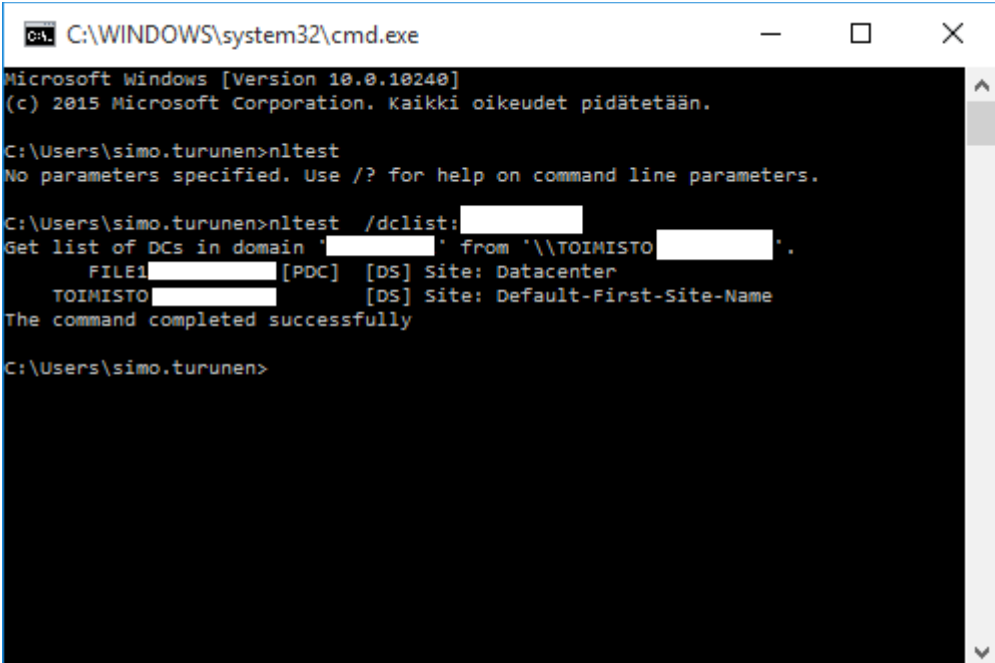
    DNS Servers . . . . . : 194.241.70.15
    . . . . . : 10.250.40.21
    Primary WINS Server . . . . . : 194.241.70.15
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Kuva 22. Komento ”ipconfig /all” Windowsin komentokehotteessa.

DHCP-palvelimen ja ensisijaisen DNS-palvelimen IP-osoite 194.241.70.15 on TOIMISTO-palvelin. Toissijaisen DNS-palvelimen IP-osoite 10.250.40.21 on file1.

Tietokone, jossa konfiguraatiota tarkasteltiin, oli Helsingin toimiston sisäverkossa, joten kaikki osoitteet olivat juuri niin kuin haluttiinkin. Tämän perusteella voitiin olettaa, että asetukset olivat ainakin pääasiallisesti oikein.

Yritykseltä saatujen tietojen perusteella ensisijainen domain controller on file1 ja toissijainen TOIMISTO. Tämä tarkistettiin Windowsin komentokehötteen avulla komennolla "nltest /dclist:<toimialue>". Komento listasi syötetyssä, yrityksen käytössä olevassa toimialueessa havaitut domain controllerit ja merkitsi ensisijaisen domain controllerin [PDC] -tagilla (Primary Domain Controller). [24.]



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. Kaikki oikeudet pidätetään.

C:\Users\simo.turunen>nltest
No parameters specified. Use /? for help on command line parameters.

C:\Users\simo.turunen>nltest /dclist:
Get list of DCs in domain ' ' from '\\TOIMISTO '.
      FILE1 [PDC] [DS] Site: Datacenter
      TOIMISTO [DS] Site: Default-First-Site-Name
The command completed successfully

C:\Users\simo.turunen>
```

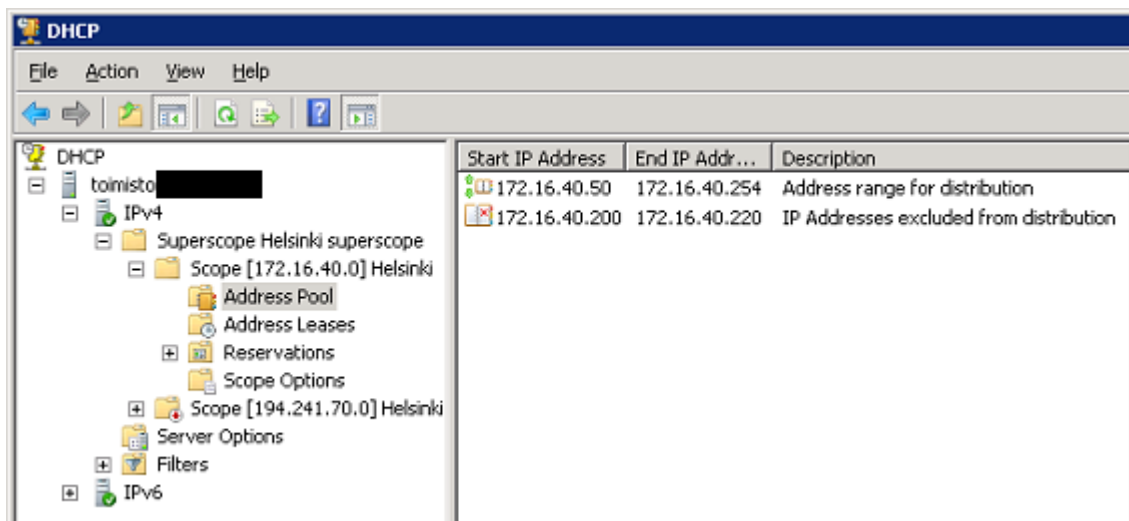
Kuva 23. Komento "nltest /dclist:<toimialue>" Windowsin komentokehötteenä.

Komennon tuloksista näkyi, että ensisijainen domain controller oli file1, kuten kuuluikin.

### 3.5.1 DHCP-palvelimien asetukset

DHCP eli Dynamic Host Configuration Protocol on teknologia päätelaitteiden IP-asetusten automatisointiin. Se koostuu kahdesta komponentista: protokollasta, jolla voidaan toimittaa asetuksia päätelaitteelle, ja mekanismista, joka varaa laitteille verkko-osoitteita ennalta määrättyltä alueelta, niin kutsusta DHCP-poolista. Laitteelle myönnetty osoite on voimassa ennalta määrätyn ajan, joka uusiutuu automaattisesti laitteen ollessa yhteydessä DHCP-palvelimeen. DHCP:n käyttö helpottaa lukuisten laitteiden hallintaa automatisoimalla IP-asetusten konfiguroinnin. Kenties tärkeimmät arvot, jotka DHCP-protokollan kautta päätelaitteille tulevat, ovat laitteen oma IP-osoite, aliverkon peite, oletusyhdyskäytävän osoite ja DNS-palvelimien IP-osoitteet. [25.]

Windows Server 2008 palvelimien DHCP-asetuksia pääsee helposti tarkastelemaan hakemalla niiden käynnistä-valikosta sanalla ”dhcp” ja avaamalla DHCP-nimisen sovelluksen. TOIMISTO:n DHCP-pooliksi oli asetettu 172.16.40.1/24. Aliverkkodokumentin (liite 1) mukaan tämä on yksi Helsingin toimipisteelle verkolle varatuista aliverkoista. Tämä oli oikein konfiguroitu eikä vaadi muutoksia. IPv6-asetuksia ei tässä työssä käyty läpi, sillä ne eivät ole kriittisiä yrityksen toiminnalle tällä hetkellä.



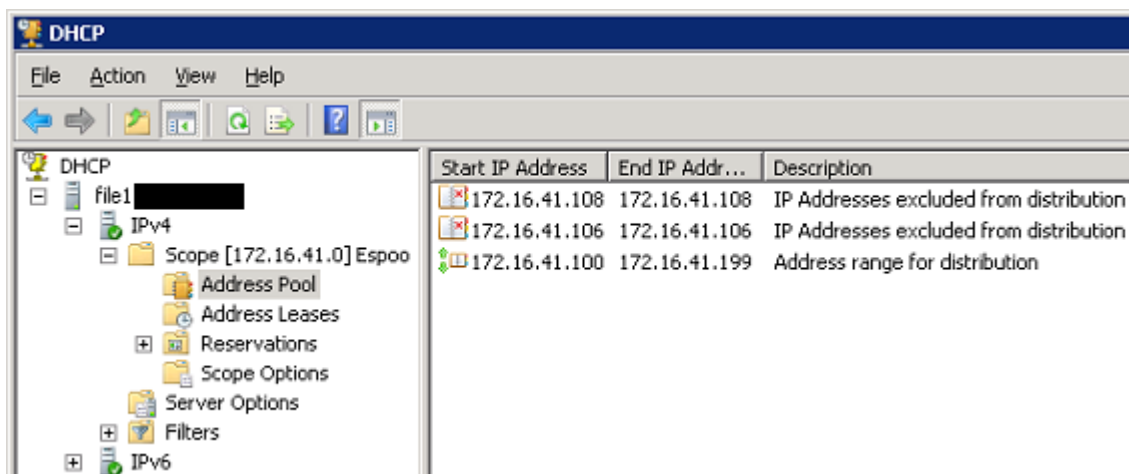
Kuva 24. TOIMISTO-palvelimen DHCP-pool.

TOIMISTO:n DHCP-pooliin oli lisäksi asetettu exclusion range 172.16.40.200 – 172.16.40.220, jonka osoitteita DHCP ei suostu jakamaan laitteille. [26.]



Tällä alueella ovat IP-kamerat ja niiden tallennus-NAS. Niihin on kaikkiin asetettu IP-osoite manuaalisesti eikä haluta, että DHCP-palvelin antaa niiden käytössä olevia IP-osoitteita toisille laitteille, synnyttäen IP-osoiteristiriidan, jossa usealla laitteella on sama IP-osoite. [27.]

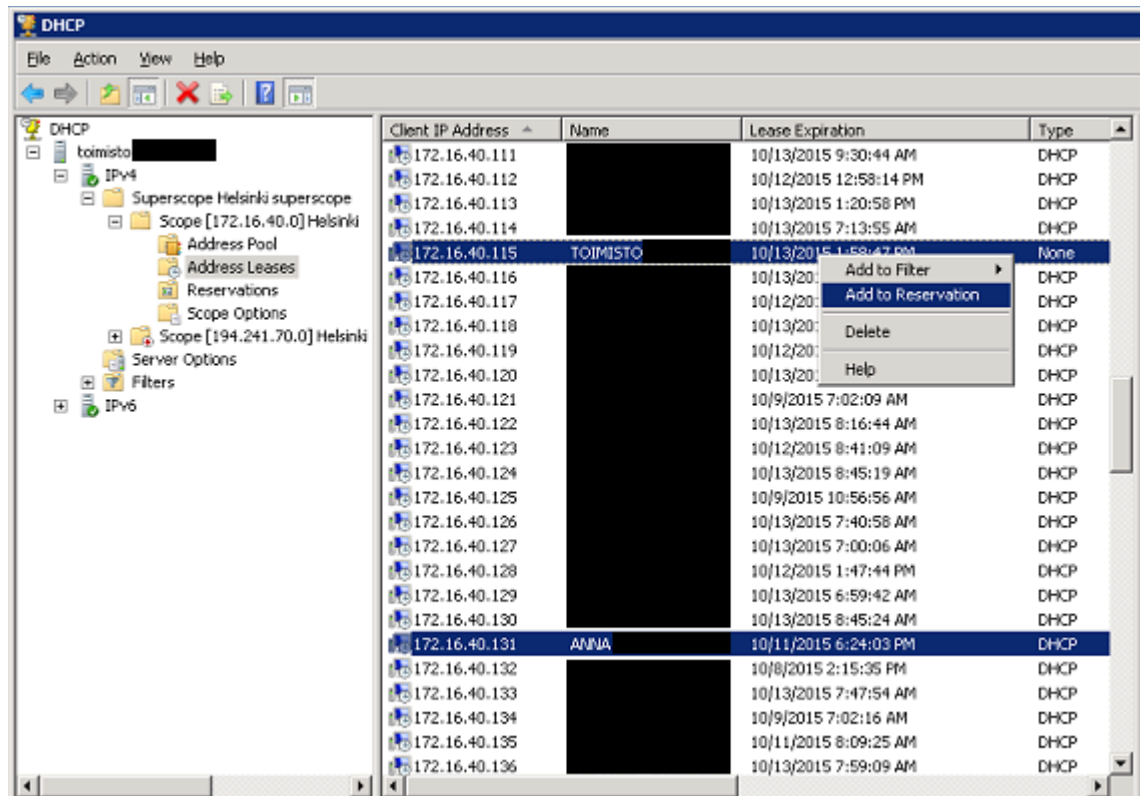
File1:n DHCP-pool on 172.16.41.100 – 172.16.41.199. Tämä on Espoon toimipisteen aliverkko, joka on niin ikään aliverkkodokumentin (liite 1) mukaan oikein. Alueelta on varattu joitain osoitteita internetpalveluntarjoajan hallinnoimien laitteiden käyttöön. Nämä varaukset on määritetty exclude-poleihin seuraavan kuvan mukaisesti.



Kuva 25. File1-palvelimen DHCP-pool.

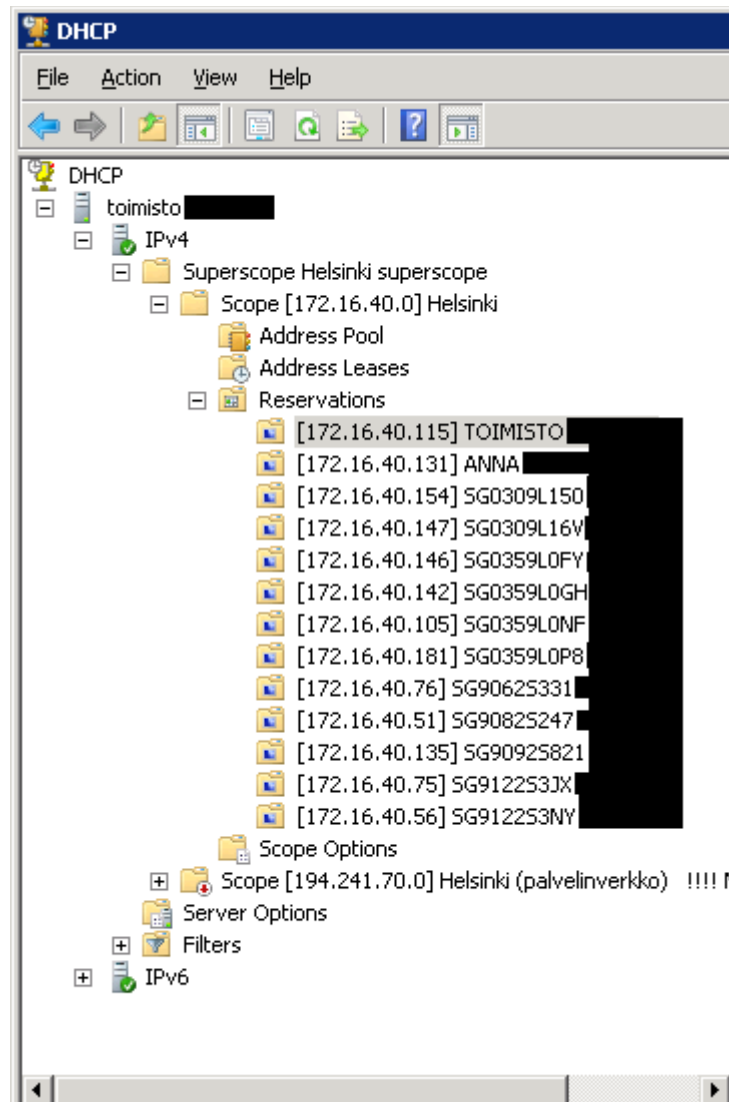
Suurin osa Helsingin toimiston laitteista oli asetettu vastaanottamaan IP-asetuksensa DHCP:n kautta, mukaan lukien palvelimet ANNA ja TOIMISTO, sekä kaikki langattoman verkon tukiasemat. Varsinkin palvelimien kohdalla IP-osoitteen tahaton vaihtuminen esimerkiksi pitkittyneen huollon jälkeen saattaisi aiheuttaa vakavia ongelmia IP-osoitteen perusteella toimivien ohjelmien kadottaessa yhteytensä, ja mahdollisten staattisten DNS-ohjausten ohjatessa palvelimille kohdistuvan liikenteen väärään osoitteeseen. Langattomien tukiasemien kohdalla niiden IP-osoitteen vaihtuminen rikkoi seurantavaiheessa asennetun ohjelmiston toiminnan laitteen osalta, jossa IP-osoite vaihtuu.

Edellä mainittujen riskien takia päätettiin laitteille lisätä DHCP-varaukset. Varattu osoite annetaan vain määritetylle laitteelle. Sen edut manuaalisiin IP-asetuksiin verrattuna ovat, että laite saa tiedot mahdollisista muiden verkkoasetusten muutoksista DHCP-palvelimen kautta, eikä niitä tarvitse syöttää käsin. [28.]



Kuva 26. DHCP-osoitevarauksien lisäys TOIMISTO-palvelimelle.

Laitteet lisättiin DHCP-varauksiin valitsemalla ne "Address Leases" -kohdan listauksesta, jossa näkyvät kaikki laitteet, joille DHCP on antanut IP-osoitteen ja valitsemalla hiiren oikeaa nappia painamalla aukeavasta valikosta "Add to Reservation". Tällä tavalla lisättiin varauksiin palvelimet ANNA ja TOIMISTO sekä kaikki langattomat tukiasemat.



Kuva 27. TOIMISTO-palvelimen DHCP-osoitevaraukset tehtyinä.

File1:n DHCP-poolissa ei ole laitteita, jotka tarvitsisivat välttämättä aina saman IP-osoitteen, joten sille ei määritetty varauksia.

### 3.5.2 DNS-palvelimien asetukset

DNS eli Domain Name System on internetin nimipalvelujärjestelmä, joka muuntaa verkkonimiä IP-osoitteiksi – ja toisin päin. Se mahdollistaa muun muassa verkkoselainten käytön sanamuotoisilla osoitteilla numeromuotoisten IP-osoitteiden sijaan. Yrityksen molemmat domain controllerit toimivat myös DNS-palvelimina. Ne toimivat resolversina ulkoisten osoitteiden selvityksessä ja autoritäärisinä nimipalvelimina yrityksen sisäverkon laitteille. Resolveri on nimipalvelin, joka välittää nimikyselyt eteenpäin juurinimipalvelimille, jotka joko vastaavat kyselyyn tai välittävät kyselyn edelleen eteenpäin. Autoritäärinen nimipalvelin vastaa kyselyyn suoraan, eli sen ei tarvitse välittää kyselyä eteenpäin. [29.] DNS-asetukset on jaettu ”forward lookup zones” ja ”reverse lookup zones” -alueisiin. Forward lookup zonen asetukset vastaavat kyselyihin ”Mikä on tämän nimen laitteen IP-osoite?” ja reverse lookup zonen asetukset kyselyihin ”Mikä on tämän IP-osoitteen verkkonimi?”. [30.]

Palvelin TOIMISTO toimii toimialueen ensisijaisena nimipalvelimena eikä sen toiminnassa ole ollut yrityksen henkilöstön suullisen kuulemisen, tai yrityksen työntekijöille lähetetyn kyselyn (liite 8) vastausten perusteella mitään ongelmia. Asetuksia tarkastellessa huomattiin kuitenkin nopeasti, että ne olivat täynnä vanhentuneita tietueita. Lukuisia palvelimia, joiden osoitteet löytyivät DNS-palvelimilta, ei ollut enää olemassa. Lisäksi joihinkin palvelimiin viittasi väärä IP-osoite osoitteiden vaihduttua, mutta DNS:n tietueiden päivityksen unohduttua. DNS-palvelimien asetuksia pääsee tarkastelemaan helposti Windows Server 2008 -palvelimella hakemalla käynnistä-valikosta sanalla ”dns” ja avaamalla DNS-nimisen sovelluksen.

Name	Type	Data	Timestamp
[REDACTED]	Host (A)	172.16.40.221	10/5/2015 8:00:00 AM
[REDACTED]	Host (A)	172.16.41.116	10/6/2015 10:00:00 AM
[REDACTED]	Host (A)	172.16.40.168	9/30/2015 7:00:00 AM
[REDACTED]	Host (A)	172.16.40.69	10/4/2015 5:00:00 PM

Administrator: Command Prompt

Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\\_situ [REDACTED] > ping [REDACTED] kauppa

Pinging [REDACTED] 10 [REDACTED] [193.184.244.179] with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 193.184.244.179:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss).

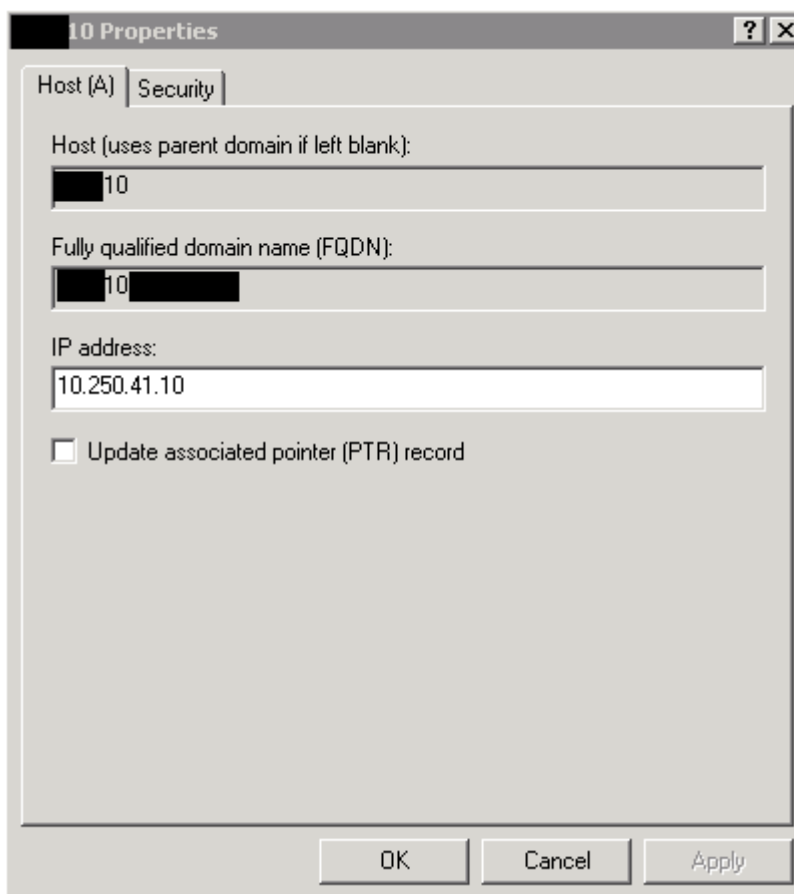
C:\Users\\_situ [REDACTED] > \_

[REDACTED]	10	Host (A)	193.184.244.179	static
[REDACTED]	2	Host (A)	10.250.40.2	3/25/2012 2:00:00 PM
[REDACTED]	4	Host (A)	10.250.40.4	10/6/2015 3:00:00 AM
[REDACTED]	5	Host (A)	10.250.40.5	3/13/2013 7:00:00 AM
[REDACTED]	6	Host (A)	10.250.40.10	10/4/2015 11:00:00 PM
[REDACTED]	5	Host (A)	10.250.40.11	10/4/2015 11:00:00 PM
[REDACTED]	[REDACTED]	Host (A)	172.16.40.150	11/19/2014 1:00:00 PM
[REDACTED]	[REDACTED]	Host (A)	192.168.1.5	1/2/2012 8:00:00 PM
[REDACTED]	[REDACTED]	Host (A)	172.16.40.172	10/25/2011 9:00:00 AM
intranet	[REDACTED]	Alias (CNAME)	[REDACTED]	static
[REDACTED]	[REDACTED]	Host (A)	194.241.70.10	11/28/2013 6:00:00 AM
[REDACTED]	[REDACTED]	IPv6 Host (AAAA)	2002:c2f1:460a:0000:0000:0000:c2f1:460a	11/28/2013 6:00:00 AM
kanta	[REDACTED]	Host (A)	10.250.40.24	2/25/2014 10:00:00 PM
[REDACTED]	kauppa	Alias (CNAME)	[REDACTED] 10 [REDACTED]	static
[REDACTED]	kauppa	Alias (CNAME)	[REDACTED] 10 [REDACTED]	static

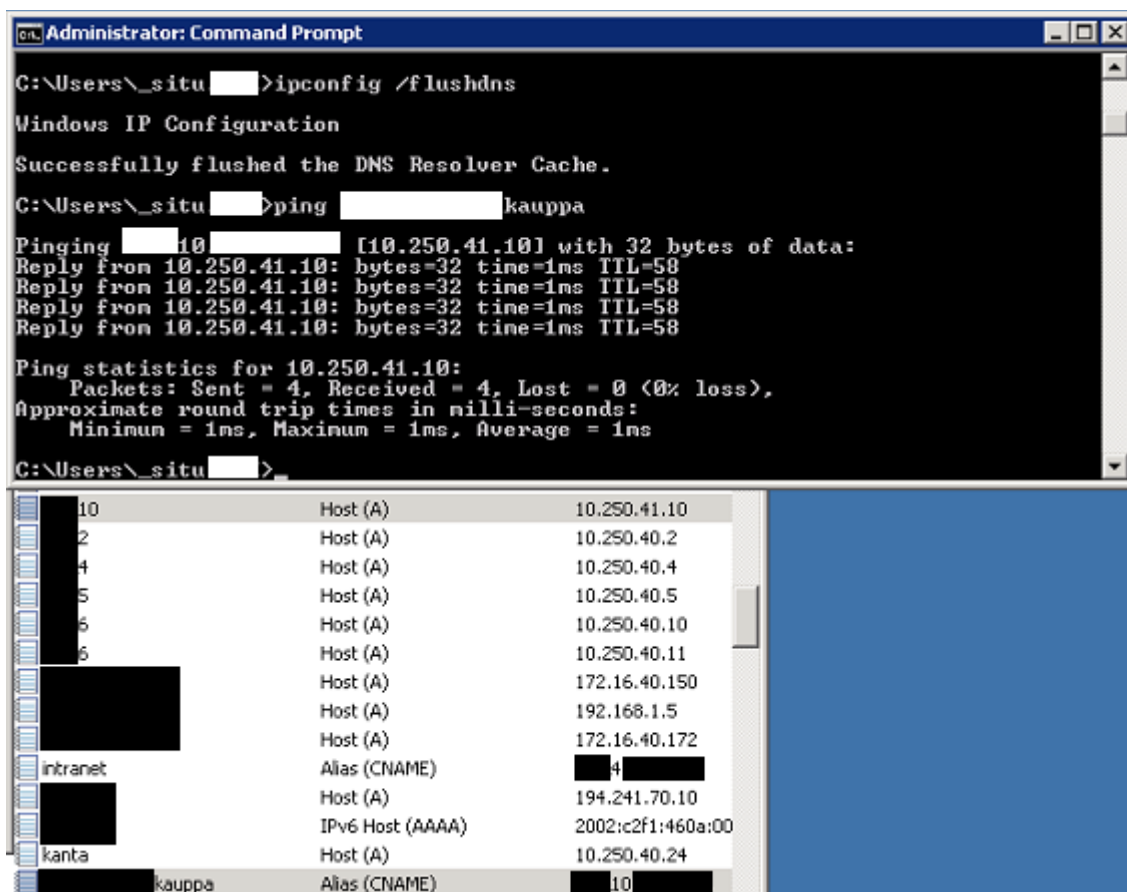
Kuva 28. TOIMISTO-palvelimen DNS:n forward lookup zone. Kuvassa näkyvä ping-komento ei toimi, koska pingattavan palvelimen DNS-tietueessa on väärä IP-osoite.

Asetuksia verrattiin listaan yrityksen käytössä olevista palvelimista. Asetuksista poistettiin käytöstä poistuneet palvelimet ja lisättiin palvelimet, jotka sieltä puuttuivat. Lisäksi korjattiin joitain vääriä IP-osoitteita. Tietueita voi muokata helposti tuplaklikkaamalla niitä. Ohjauksiin lisättiin myös tietueet verkkotulostimille helpomman hallinnan nimen avulla mahdollistamiseksi. Uuden tietueen voi lisätä klikkaamalla hallittavaa "zonea" oikealla hiiren napilla ja valitsemalla avautuvasta menusta "New Host".



Kuva 29. Kuvassa 28 näkyvän vanhentuneen IP-osoitteen korjaus DNS-tietueesta.

Asetusten muutosta testattiin Windowsin komentokehötteen komennoilla "ipconfig /flushdns", joka poistaa tietokoneelle aiemmin tallennetut DNS-ohjaukset, sekä ping-komennon avulla. [31.]



Kuva 30. Korjatun DNS-tietueen testaus. Palvelin vastaa nyt pingiin.

## 4 Verkon tilan ja palvelimien seuranta

### 4.1 Seurannan rajaus ja tavoitteet

Yrityksen työntekijöiden päätelaitteiden tilan keskitetty seuranta ei ole kriittistä yrityksen hyvän sisäisen kommunikaation vuoksi. Päätelaitteiden ongelmat tulevat IT-osaston tietoon lähes välittömästi niiden esiintyessä käyttäjien raportoidessa niistä puhelimitse, Lyncillä, sähköpostilla tai paikan päällä suullisesti.



Päätelaitteiden tilasta seurataan valmiiksi päivitysten tilaa WSUS-palvelimen kautta ja tietoturvan tilaa Symantec Endpoint Protection Managerin (SEPM) avulla.

Yrityksen verkkoinfrastruktuuria tai palvelimien tilaa ei kuitenkaan seurata keskitetysti millään tavalla. Tämä hidastaa ongelmien paikantamista ja tekee niiden ehkäisemisen lähes mahdottomaksi. Tässä työssä keskityttiin juuri näiden laitteiden tilan seurannan keskitetyn hallinnan rakentamiseen. Verkon toimintaan liittyvän ongelman tai palvelimen toimintahäiriön paikallistaminen ilman minkäänkokoista keskitettyä seuranta on tämän työn tekijän IT-tuen parissa vietetyn ajan perusteella aikaa vievää ja hermoja raastavaa toimintaa, joka saattaa johtaa hätiköityihin ratkaisuihin, jos ongelmaa ei pystytä paikantamaan. Jos keskitetty seuranta lyhentää käyttäjien tarvitsemien palveluiden katkoksia edes minuuteilla, on kaikki seurannan rakentamiseen nähty vaiva sen arvoista.

Seurannan tavoite on saada kaikkien määritettyjen laitteiden ja palveluiden saatavuudesta lähes reaaliaikaista tietoa ja tiettyjen kriittisten palveluiden toiminnasta tarkempaa ja tilastoitavaa tietoa. Lisäksi kaiken tämän tiedon pitää olla koko yrityksen IT-osaston helposti saatavissa ja helposti tulkittavassa muodossa, jotta ongelmat voidaan havaita ja niihin reagoida mahdollisimman nopeasti.

## 4.2 Seurannan toteutus

Seurantaohjelmavaihtoehtoja selviteltiin Googlen hakukoneesta hakusanoilla ”network monitor”. Haluttiin vaihtoehto, joka on mahdollisimman monipuolinen, helppokäyttöinen ja ilmainen tai sisältää pitkän kokeiluajan. Eri vaihtoehtoihin tutustuttiin niiden verkkosivuilla olevien ominaisuuksien ja kuvien perusteella. Päädyttiin kokeilemaan PRT Network Monitor (tästä eteenpäin vain PRTG) -nimistä ohjelmistoa. PRTG osoittautui soveltuvan yrityksen verkon seurantaan niin hyvin, että tarvetta muiden ohjelmistojen testaukselle ei ollut.

PRTG asennettiin IT-osaston testipalvelimelle ANNA. Tähän ohjelmistoon päädyttiin sen monipuolisuuden, selkeiden ohjeiden ja käytettävyyden, rajoittamattoman kuukauden kokeiluajan ja ilmaisen lisenssin reiluuden vuoksi.

Samalla ohjelmistolla voidaan seurata kytkinten lokiviestejä, verkkoinfrastruktuurin toimintaa ja palvelinten sekä niiden palveluiden ja ohjelmien toimintaa. Lisäksi ohjelman avulla voidaan seurata yrityksen käytössä olevien verkkosivujen saatavuutta ja niiden latauksen nopeutta.

### 4.3 PRTG Network Monitorin yleiskatsaus

PRTG on Paesslerin kehittämä pääasiassa verkon ja infrastruktuurin seuraamiseen tarkoitettu ohjelma. PRTG:n kokeiluversion voi ladata osoitteesta [https://shop.paessler.com/shop/standalone\\_free\\_license/](https://shop.paessler.com/shop/standalone_free_license/). Kokeilu vaatii rekisteröitymisen sähköpostilla. PRTG Network Monitorin aloituslisenssiin sisältyy 30 päivän kokeiluaika. Tänä aikana ohjelmassa ei ole mitään rajoituksia. 30 päivän jälkeen ohjelman lisenssi muuttuu automaattisesti "Freeware"-lisenssiksi, joka on täysin maksuton, mutta rajoitettu sataan sensoriin. Sensori on PRTG:n perusyksikkö, joka seuraa yhden tietyn laitetiedon tai ohjelman toimintaa. Laajentaakseen PRTG:n seuranta yli sataan sensoriin, täytyisi ostaa maksullinen lisenssi. Tämän työn vaatimaan seuranta kuitenkin sata sensoria oli tois-  
taiseksi riittävä määrä, ja työ toteutettiin ilmaislisenssillä.

PRTG koostuu kahdesta komponentista "Probe":sta ja "Server":stä. Probe on ohjelma, joka lähettää sensoreiden vaatimat kyselyt laitteille ja eteenpäin Serverille. Itse seurattaville laitteille ei asenneta mitään ohjelmia. Joissain tapauksissa ne tosin vaativat joidenkin asetusten muutoksia, jotta Probe saa oikeudet tarkastella tarvittavia tietoja. Näissä tapauksissa sensori ilmoittaa tarvitsevansa kyseiset muutokset ja antaa ohjeet niiden tekemiseen. Server kokoaa ja tallentaa Proben välittämät tiedot sekä esittää ne erilaisissa helposti ymmärrettävissä muodoissa.

Probeja voi PRTG:n asennuksessa olla useita, joka jakaa palvelimelle aiheutuvaa kuormaa ja mahdollistaa eri verkoissa ja toimialueissa olevien laitteiden seurannan. Probe toteuttaa kyselynsä sensorista riippuen monen eri teknologian avulla.

Tässä työssä käytetyt sensorit toimivat pääasiassa WMI-infrastruktuurin ja ICMP-protokollan (ping) avulla.

#### 4.4 PRTG Network Monitorin konfigurointi

PRTG asennettiin ANNA-palvelimelle, joka on liitetty sekä normaaliin toimialueverkkoon ja sisäiseen VLAN:iin, että kytkinten hallintaverkkoon ja VLAN:iin "Hallinta". Tämä mahdollisti yhteyden saamisen kaikkiin yrityksen laitteisiin yhdestä paikasta. Asennus vaati toimialueen järjestelmänvalvoja -tason tunnuksien luovutuksen ohjelmiston käyttöön, jotta WMI:n avulla toimivien sensorien kyselyt hyväksyttäisiin kaikilla toimialueeseen liitetyillä laitteilla. Sekä Probe että Server asennettiin molemmat palvelimelle ANNA. Asennus oli suoraviivainen, Windows-ympäristöstä tuttu, lähinnä "Next"-napin painelua vaativa toimenpide, eikä vaatinut mitään muutoksia palvelimen asetuksiin.

##### 4.4.1 Ryhmien ja laitteiden asetukset

Asennuksen jälkeen luotiin ryhmät seurattaville laitteille. Ryhmät luotiin klikkaamalla "Devices"-osion oikeassa laidassa sijaitsevasta puuhierarkiasta automaattisesti luotua "Local probe" -ryhmää oikealla hiiren napilla, ja valitsemalla aukeavasta valikosta "Add Group...". [32.]

Ryhmistä luotiin puuhierarkia alkaen fyysisestä sijainnista (Helsinki, Espoo tai Vantaa) ja päättyen laitetyyppiin. Näin seurattavien laitteiden hahmottaminen on selkeää, ja tar-

vittaessa tietty laite löytyy loogisesti puuta seuraamalla. Laitteet lisättiin oikeaan ryhmäänsä joko manuaalisesti ryhmää oikealla napilla klikkaamalla ja valitsemalla aukeavasta valikosta "Add Device..." tai ottamalla ryhmälle "autodiscovery" käyttöön. Manuaalisesti laitteen pystyy lisäämään joko IP-osoitteen tai verkkonimen perusteella. Osalle ryhmistä asetettiin "autodiscovery", joka etsii laitteet automaattisesti annetulta IP-osoitealueelta, kun tiedettiin kyseisen ryhmän laitteiden sijaitsevan tietyllä IP-osoitealueella. Näistä esimerkkinä on IP-kamerat, joiden haluttiin kuuluvan samaan ryhmään ja joiden tiedettiin dokumentointivaiheen perusteella sijaitsevan tietyllä IP-osoitevälillä. [33.]

The screenshot shows the PRTG Group Settings interface for a group named 'Kamerat'. The interface includes a navigation bar with tabs for Overview, Live Graph, 2 days, 30 days, 365 days, Alarms, Log, Settings (selected), Notifications, and a menu icon. Below the navigation bar, the 'BASIC GROUP SETTINGS' section includes:
 

- Group Name: Kamerat
- Status: Started (selected), Paused
- Parent Tags: (empty)
- Tags: guru
- Priority: ★★★★★

 The 'GROUP TYPE' section includes:
 

- Sensor Management: Automatic device identification (standard, recommended) (selected), Manual (no auto-discovery), Automatic device identification (detailed, may create many sensors), Automatic sensor creation using specific device template(s)
- Discovery Schedule: Once
- IP Selection Method: Class C base IP with start/end (IPv4) (selected), List of individual IPs and DNS names (IPv4), IP and subnet (IPv4), IP with octet range (IPv4), List of individual IPs and DNS names (IPv6), Use computers from the active directory (maximum 1000 computers)
- IPv4 Base: 172.16.40
- IPv4 Range Start: 200
- IPv4 Range End: 207
- Name Resolution: Use DNS / WMI / SNMP names (recommended) (selected), Use IP addresses
- Device Rescan: Skip auto-discovery for known devices/IPs (recommended) (selected), Perform auto-discovery for known devices/IPs

Kuva 31. Auto-discovery-toiminnallisuuden asetukset PRTG:n hallinnassa ryhmän "Kamerat" kohdalla. Kuvan asetuksilla ohjelma etsii laitteita osoiteväleiltä 172.16.40.200 – 172.16.40.207.

Niiltä osoiteväleiltä, joilla sijaitsee mahdollisesti eri ryhmien laitteita, ei otettu autodiscoveryä käyttöön, vaan laitteiden IP-osoitteet syötettiin ohjelmaan käsin. Tämän jälkeen ohjelman ollessa vielä kokeilulisenssillä ajettiin kaikille laitteille manuaalinen, laitekohmainen discovery, painamalla laitteen pääikkunasta "Recommend Now" -nappia.

Tämä manuaalinen ”discovery” selvittää parhaansa mukaan, minkä tyyppinen laite on kyseessä ja ehdottaa mahdollisesti hyödyllisiä sensoreita laitteelle. Testausta varten otettiin käyttöön lähes kaikki ohjelman ehdottamat sensorit.

Anna (prtgadmin) Local probe (Local Probe) Palvelimet - Datacenter crmtest [redacted]

Device crmtest [redacted] [star] [star] [star] [star] [star]

Overview Live Graph 2 days 30 days 365 days Alarms Log Settings Notifications [icon] [icon]

Status: OK Sensors:  1 (of 1) DNS/IP: 10.250.41.22 Dependency:  crmtest - ping Default Interval: every 60 seconds

crmtest - ping  
OK

Ping Time  
1 msec

0 182 msec

Pos	Sensor	Status	Message	Graph	Priority
1.	<input checked="" type="checkbox"/> crmtest - ping	Up	OK	Ping Time	★★★★★

### RECOMMENDED SENSORS

Priority	Sensors	Total Sensors	Links
★★★★★	1×CPU Load, 1×Memory, 1×Disk Free, 1×Pagefile Usage, 1×Uptime	5	<input type="button" value="Add these sensors"/>
★★★★☆	1×SSL Security Check (Port 443), 1×Network Card, 1×RDP (Remote Desktop), 2×Windows IIS Application, 6×PerfCounter IIS Application Pool	11	<input type="button" value="Add these sensors"/>

**WHAT IS THIS?**  
PRTG can inspect your devices to recommend useful sensor types. Add these sensors to get a much better and more detailed picture about the status of this device in the future.

Kuva 32. Laitekohtainen discovery ja sen tulokset palvelimelle crmtest.

Tällä tavalla saatiin laitteista todella laajasti tietoa seurantaan. Näistä sensoreista kar-sittiin myöhemmin ei-kriittiset pois, jotta pysyttiin ilmaisversion sadan sensorin rajoituk- sessa. Suositeltujen sensorien lisäksi tietyille palvelimille lisättiin sensorit seuraamaan niillä toimivien kriittisten ohjelmistojen tai palveluiden toimintaa. Sensorin lisääminen ta- pahtuu helposti kuvassa 30 näkyvästä ”Add Sensor” -painikkeesta.

Siitä aukeavasta työkalusta voi etsiä erilaisia sensoreita joko tekstihaulla tai rajaamalla sensoreita seurattavan asian, seurattavan laitteen tyyppin ja käytetyn seurantateknologian mukaan. [34.]

#### 4.4.2 Sensorit

PRTG:ssä on erittäin laaja skaala sensoreita, joilla seurataan erilaisten laitteiden ja ohjelmien tietoja. Tässä työssä jokaiselle seurattavalle laitteelle lisättiin ping-sensori, joka nimensä mukaisesti seuraa laitetta ping-komennon avulla, tilastoiden latenssia ja pakettien hävikkiä. Tietyille kriittisille palvelimille lisättiin erikoissensoreita seuraamaan niiden laitteiston tilaa, kuten esimerkiksi prosessorin käyttöä tai tietyn kriittisen ohjelman toimintaa. Ilmaislisenssin sadan sensorin rajoituksen vuoksi ainoastaan kriittisimpiä tietoja pystyttiin seuraamaan toistaiseksi. Jokaisen laitteen kohdalla mietittiin, kuinka kriittinen se on yrityksen toiminnan kannalta ja edelleen, mitkä osat sen toiminnassa ovat kriittisimpiä. Esimerkiksi tietokantapalvelimille lisättiin sensorit prosessorien ja kiintolevyjen käytön seurantaan varten.

Sensoria luodessa sille kannattaa antaa kuvaava nimi, jolla tunnistaa pelkästään sensorin nimen perusteella, minkä laitteen mistä sensorista on kyse, sillä erilaisissa sensorien listauksissa ei välttämättä lue laitetta, jonka tilasta sensori raportoi. Tässä työssä käytettiin formaattia "<laitteen nimi> - <sensorin nimi>", eli esimerkiksi "TOIMISTO – ping". Jokaiselle sensorille kannattaa myös välittömästi säätää skannausväli, eli kuinka usein sensori hakee uudet tiedot kohdelaitteelta.

Tämän voi tehdä joko sensorikohtaisesti, jokaisen sensorin asetuksista, kohdasta "Scanning Interval" tai hakemalla kaikki samanlaiset sensorit PRTG:n ylävalikon "Sensors"-välilehdestä, valitsemalla halutut sensorit ja säätämällä asetukset hiiren oikealla napilla aukeavasta "Configuration"-valikosta. [35] Jotkut sensorit kuormittavat verkkoa tai kohdelaitteita kohtuuttomasti, jos skannausväli on liian tiheä. Sensorin kuormittavuudesta kertova palkki näkyy uutta sensoria lisättäessä.

Mitä pidemmälle palkki on väritetty, sitä kuormittavampi sensori on. Esimerkiksi ”Windows Updates Status (Powershell)” -sensorin skannausväliksi PRTG:n manuaalissa suositellaan 12 tuntia. [36.] Vakiona se on kuitenkin yksi tunti ainakin tämän työn teko- vaiheessa olevassa PRTG:n versiossa. PRTG:tä kuitenkin kehitetään jatkuvasti lähes viikottaisten päivitysten muodossa, joten tämä tulee todennäköisesti muuttumaan.

PRTG:n sensorilla voi olla kahdeksan tilaa, jotka ovat

- Up – kaikki on kunnossa
- Paused – sensori on pysäytetty
- Warning – seurattavan asian tila saattaa johtaa ongelmiin
- Down – mahdollisesti korjausta vaativa ongelma
- Down (Partial) – klusterissa on sekä down-, että up-sensoreita
- Down (Acknowledged) – down tila, joka on manuaalisesti kuitattu hälytyksen lopettamiseksi
- Unusual – tilastollinen poikkeama
- Unknown – sensorilla ei ole tilaa, joko ongelman tai uudelleenkäynnistyksen takia. [37.]



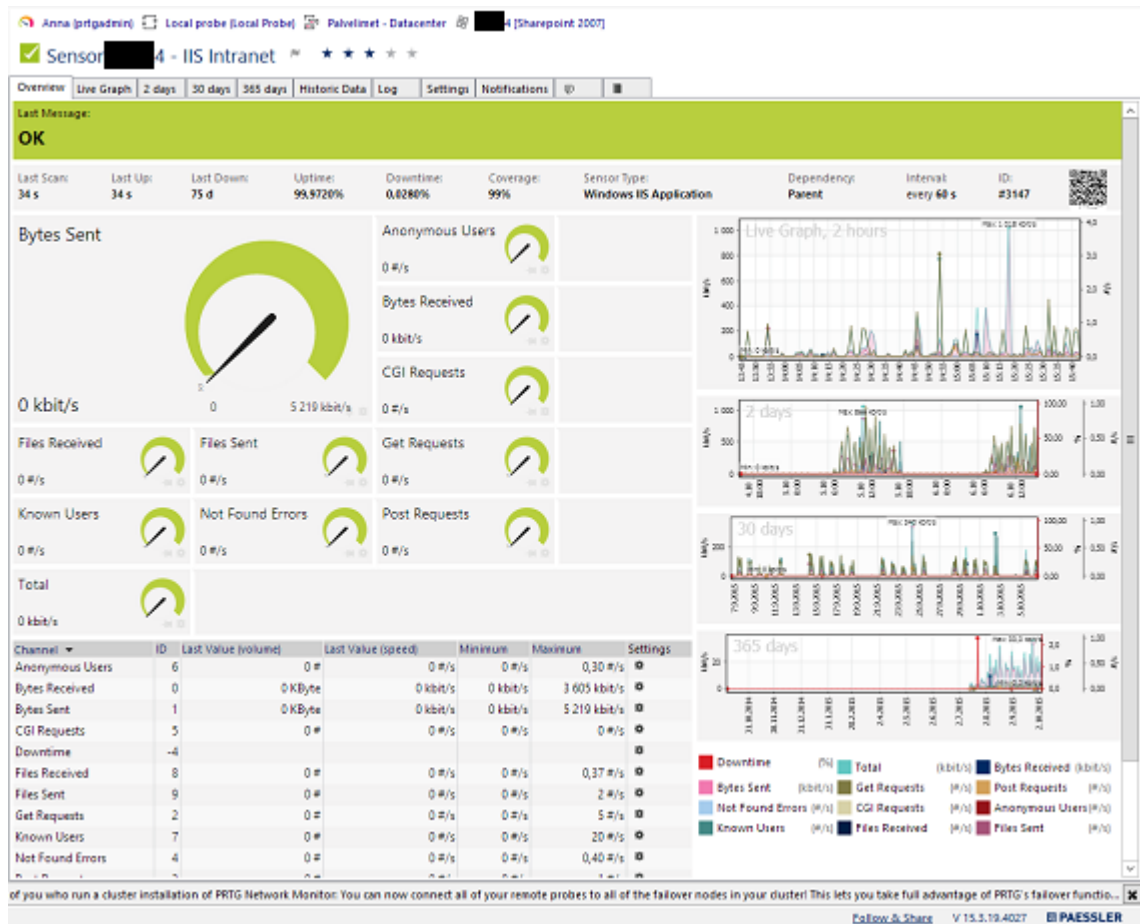
Sensor Name	Status
CRM [CRM]	
CRM - ping	Up
CRM - CPU Load	Up
CRM - Disk Free	Paused
CRM - Memory	Up
CRM - Windows Update	Warning
CRM - IIS CRM	Down

Kuva 33. Sensorien tiloja.

Sensorin siirtyessä Warning-, Down- tai Unusual-tilaan, voidaan PRTG konfiguroida lähettämään erilaisia hälytyksiä, esimerkiksi sähköpostin, tekstiviestin tai ohjelmaan ilmestyvien ilmoitusten muodossa. [38.] Tässä työssä käytetään vain ohjelmaan ilmestyviä ilmoituksia. Jokaiselle sensorille löytyy lukuisia asetuksia, joita ei kaikkia tässä työssä käydä läpi, mutta ne ovat yleensä joko hyvin yksiselitteisiä, tai niistä löytyy selkeää kuvaus PRTG:n verkkosivuilta löytyvästä manuaalista (<http://www.paessler.com/manuals/prtg>).

Laitteessa olevilla sensoreilla on lisäksi riippuvuussuhteita, jotka sensorin siirtyessä Down-tilaan pysäyttävät siitä riippuvaiset sensorit. Esimerkiksi raskaan Windows Update -sensorin suoritus olisi hyvä pysäyttää, jos CPU-sensori menee down-tilaan kovan rasituksen alla. Vakiona kaikissa laitteissa ping-sensori on "master-object" ja sen siirtyessä down-tilaan kaikki muut sensorit pysähtyvät. Riippuvuudet voi asettaa esimerkiksi sensorin omista asetuksista. [39.]

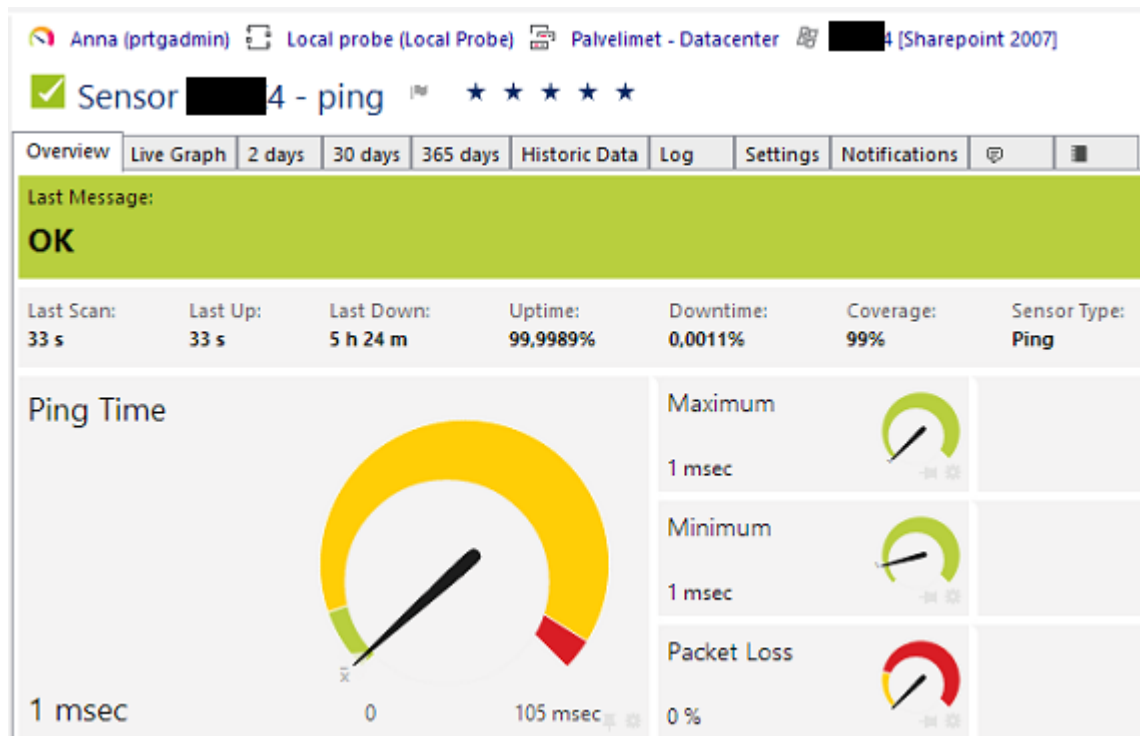
Esimerkkinä erikoissensorista, joka seuraa tiettyä ohjelmistoa tai palvelua, on Sharepoint-palvelimelle lisätty IIS-sensori, joka seuraa palvelimella toimivan Sharepoint 2003 intranet-sivuston toimintaa.



Kuva 34. Intranetin toimintaa seuraava IIS Application -sensori.

Sensori hälyttää, jos IIS tai sen sisältämä intranet-sivusto lakkaa toimimasta. Lisäksi se antaa monta erilaista mittaria intranet-sivuston toiminnalle. Sensorin tilastoista ja sen piirtämistä kuvaajista voidaan tarkastaa esimerkiksi, mihin aikaan päivästä yrityksen intranet-sivustoa käytetään eniten, tai milloin se on mahdollisesti ollut tavoittamattomissa. Sen tärkein ominaisuus on kuitenkin hälytys, jos sivusto lakkaa toimimasta.

Lähes kaikissa sensoreissa on useampi kuin yksi asia, jota seurataan. Nämä ovat sensorin kanavat - "Channels". Kanavilla on kaikilla omat asetuksensa, joista tärkeimmät ovat rajat. Niiden avulla päätetään, millä arvoilla sensori vaihtaa tilaansa. [40.]



Kuva 35. Ping-sensorin kanavat ja niille määritetyt rajat. Keltainen alue on Warning- ja punainen Down-tila.

Jokaiselle kanavalle voi määrittää yleiset tai sensorikohtaiset rajat, jotka määrittävät milloin sensori siirtyy OK-tilasta Warning- tai Down-tilaan. Kaikkiin yrityksen sisäverkon laitteisiin asetettiin vähintään ping-sensori. Ping-sensori lähettää oletuksen viisi ICMP-pakettia kohdelaitteelle ja ilmoittaa ja tilastoi niiden tulokset. Ping-sensori sisältää kanavat "Ping Time", joka näyttää viimeisimmän mittauksen tuloksen keskiarvon, "Maximum", joka näyttää viimeisimmän mittauksen pisimmän viiveen, "Minimum" joka näyttää viimeisimmän mittauksen pienimmän viiveen, sekä "Packet Loss", joka näyttää kadonneiden pakettien suhteen. [41.]

Yrityksen sisäverkon latenssien ollessa hyvin pienet, yleensä noin 1-3 millisekuntia, asetettiin "Ping Time" -sensorin rajoiksi Warning 10 millisekuntia ja Down 100 millisekuntia. Näin sensori varoittaisi heti, jos yhteys johonkin laitteeseen hidastuisi normaalista edes vähän ja hälyttäisi, jos pingin latenssi nousisi yli sataan millisekuntiin, joka normaalisti näin pienillä latensseilla olisi joko merkki erittäin kovasta rasituksesta, tai verkon ongelmista.

Edit Channel	
Line Color	<input checked="" type="radio"/> Automatic <input type="radio"/> Manual
Line Width	1
Data	<input checked="" type="radio"/> Display actual values in msec <input type="radio"/> Display in percent of maximum
Value Mode	<input checked="" type="radio"/> Average <input type="radio"/> Minimum <input type="radio"/> Maximum
Decimal Places	<input checked="" type="radio"/> Automatic <input type="radio"/> All <input type="radio"/> Custom
Spike Filter	<input checked="" type="radio"/> Disable Filtering <input type="radio"/> Enable Filtering
Vertical Axis Scaling	<input checked="" type="radio"/> Automatic Scaling <input type="radio"/> Manual Scaling
Limits	<input type="radio"/> Disable Limits <input checked="" type="radio"/> Enable Limits
Upper Error Limit (msec)	100
Upper Warning Limit (msec)	10
Lower Warning Limit (msec)	
Lower Error Limit (msec)	
Error Limit Message	
Warning Limit Message	

**Help**

Spike filtering is applied to values that are applied to the channel for 5 minutes (see 'B Status page')

Kuva 36. Ping-sensorin Ping Time -kanavan rajat. Sensori siirtyy Warning-tilaan 10 ms kohdalla ja Down-tilaan 100 ms kohdalla.

Kanaville Maximum ja Minimum ei asetettu rajoja, sillä pingin heittely ei välttämättä ole merkki ongelmasta vaan enemmänkin laitteiden rasituksesta. Kanavalle Packet Loss asetettiin Warning-rajaksi 1 % ja Down-rajaksi 21 %. Näin sensori varoittaisi heti, jos yksikin ping-paketti häviää. Jos enemmän kuin yksi viidestä paketista häviää, siirtyy sensori down-tilaan ja hälyttää.

PRTG:ssä on myös sensori syslog-viestien käsittelyyn ja varastointiin. Sensori otettiin käyttöön vakioasetuksilla, ja se alkoi toimia välittömästi. Sen avulla päästiin eroon erillisestä syslog-viestien seuraamisohjelmasta, jossa oli viiden laitteen rajoitus. Sensoriin asetettiin myös rajat, jotka muuttavat sensorin statuksen Warning-tasoon, jos sensori vastaanottaa Warning-tason viestin, tai Down-tasoon error- tai vakavammalla tasolla.

The screenshot shows the PRTG Sensor Syslog Receiver interface. At the top, there are navigation tabs: Overview, Live Graph, 2 days, 30 days, 365 days, Historic Data, Messages (selected), Log, Settings, and Notifications. Below the tabs is the title 'Sensor Syslog Receiver' with a checkmark icon and five stars. The main content area is titled 'SYSLOG MESSAGES' and contains a table of log entries. The table has columns for Source, Message, Hostname, Timestamp (Device), and Severity. The messages are filtered to show 50 items, with a date range of 2015. The messages include status changes for various ports (20, 21, 26, 27, 13) and STP-related events.

Filter	Source	Message	Hostname	Timestamp (Device)	Severity
					Any
Items: 50 Date Range: 2015					
	10.255.255.62	Apr 30 08:23:36 10.255.255.62 ports: port 20 is now on-line			6
	10.255.255.62	Apr 30 08:23:34 10.255.255.62 ports: port 20 is Blocked by STP			6
	10.255.255.62	Apr 30 08:23:31 10.255.255.62 ports: port 20 is now off-line			6
	10.255.255.62	Apr 30 08:16:41 10.255.255.62 ports: port 27 is now off-line			6
	10.255.255.62	Apr 30 08:06:32 10.255.255.62 ports: port 21 is now on-line			6
	10.255.255.62	Apr 30 08:06:29 10.255.255.62 ports: port 21 is Blocked by STP			6
	10.255.255.62	Apr 30 08:06:27 10.255.255.62 ports: port 21 is now off-line			6
	10.255.255.52	May 1 12:18:38 10.255.255.52 ports: port 13 is now off-line			6
	10.255.255.62	Apr 30 07:55:53 10.255.255.62 ports: port 26 is now off-line			6
	10.255.255.52	May 1 12:18:34 10.255.255.52 ports: port 13 is now on-line			6
	10.255.255.52	May 1 12:18:31 10.255.255.52 ports: port 13 is Blocked by STP			6

Kuva 37. Syslog-sensori, joka vastaanottaa syslog-viestejä.

#### 4.4.3 Kartat

Kaikkien ryhmien, laitteiden sekä sensorien ja niiden kanavien ollessa tyydyttävällä tasolla, oli aika miettiä, miten sensorien tilaa voisi havainnollistaa ja seurata helposti. Sähköposti-ilmoituksia tai vastaavia ei haluttu ottaa käyttöön, vaan ohjelman tilan seuraamisen tulisi olla vapaaehtoista. Laitteiston tilan lukemisen tulisi olla selkeää ja helppoa, jolloin se ei tuntuisi askareelta, vaan työtä helpottavalta ja toivotulta asialta, sillä mitä yritys tekisi seurantaohjelmistolla, jota kukaan ei jaksanut seurata. Nämä asiat ratkesivat PRTG:n ”Maps”-ominaisuudella.

Ohjelmistoon voi myös luoda kustomoituja ”karttoja” seurattavista laitteista. Tämä toiminnallisuus on laitteiden seurannan helpon luettavuuden kannalta ylivoimaisesti tärkein. Karttoihin voi lisätä valitsemansa laitteet ja sensorit, piirtää niiden väliset yhteydet, valita laitteille havainnollistavat kuvakkeet sekä lisätä kartoilta taustakuvat. Karttoihin voi lisäksi ottaa mukaan taulukoita ja kuvaajia sensorien tiloista. Kartat voi jakaa toisille käyttäjille http-linkkinä, joka aukaisee selaimen automaattisesti päivittyvän sivun, joka sisältää kartan kaikki toiminnallisuudet muokkausta lukuun ottamatta. Tällä tavalla kartan voi avata milloin vain miltä vain sisäverkkoon liitetyltä koneelta, antaa olla IT-osaston koneilla toisella näytöllä auki, tai jopa laittaa sen näkyville dedikoituun näyttöön yleiselle paikalle IT-osastossa. [42.]

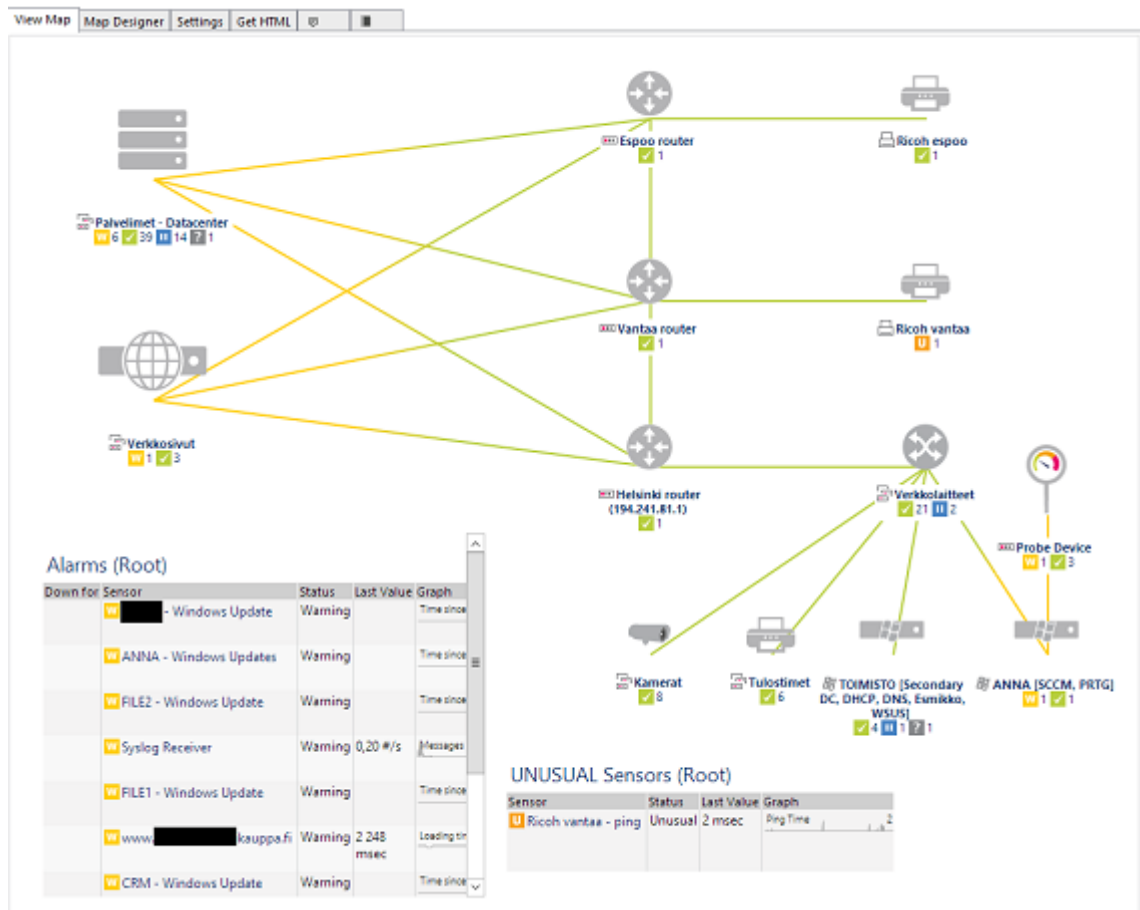
Yrityksen laitteiston helppoa seuranta varten luotiin kaksi karttaa. Kartat luodaan PRTG:n ylävalikon ”Maps”-välilehdellä. Karttojen muokkaus on ”vedä ja pudota” -tyyppistä kartan molemmin puolin sijaitsevista valikoista löytyvien ryhmien ja laitteiden sijoittelua kartalle varatulle alueelle. Ennen kartan luontia on hyvä päättää, minkä kokoisesta kartasta haluaa luoda, esimerkiksi 1024x800 pikseliä. Lisäksi kartalle on hyvä miettiä taustakuva jo etukäteen. Molemmat voi muokata jälkikäteenkin, mutta työmäärä on suurempi.

”Yleiskuva” karttaan otettiin mukaan kaikki seurattavat laitteet ja sensorit. Sensorit ryhmiteltiin laitteiden fyysisten ja loogisten sijaintien mukaisiin ryhmiin. Lisäksi karttaan lisättiin taulukot hälytyksistä, eli Warning- ja Down-statuksen sensoreista, sekä Unusual sensoreista.

Sensorin hälyttäessä, eli siirryessä Down-tilaan muuttuu siitä lähtevien yhteyksien väri punaiseksi, laitteen alle tulee punainen kuvake ja "Alarms (Root)" -taulukkoon tulee ylimmäiseksi hälytyksen aiheuttaneen sensorin tiedot. Taulukosta sensoria klikkaamalla pääsee suoraan sensorin hallintaan.

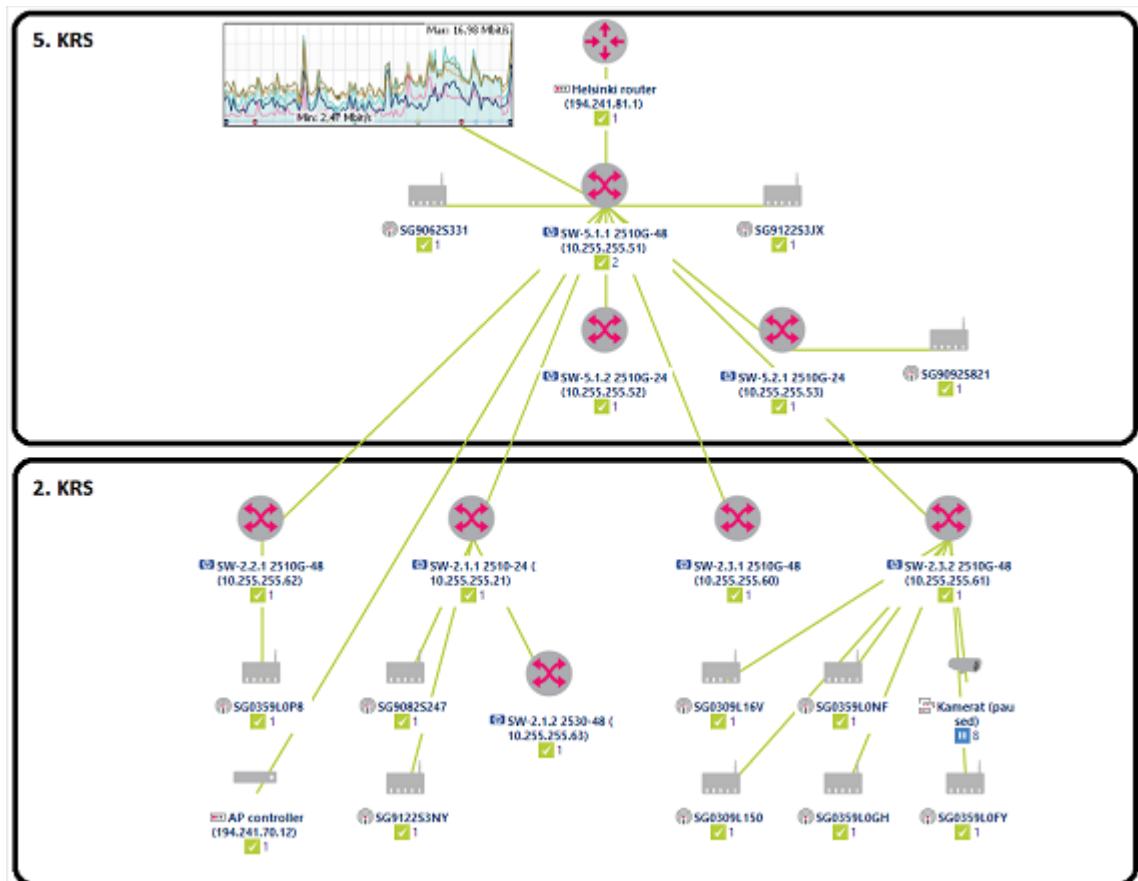
"UNUSUAL Sensors (Root)" -taulukkoon tulee tiedot sensoreista, joiden lukemia PRTG pitää tilastollisesti poikkeavina. Tämän toiminnallisuuden ideana on havaita ongelmat jo ennen niiden syntyä, eli jos jokin laite alkaa käyttäytyä poikkeavasti, saattaa siinä piillä alkava ongelma. [37.] Tämän työn aikana PRTG:n ilmoittamat unusual-tilat ovat kuitenkin olleet kaikki vain seurausta joko pingin heittämisestä eri toimistojen välillä, tai käyttäjien tavallista aktiivisemmasta tai passiivisemmasta toiminnasta palvelimien käytössä. Taulukko kuitenkin jätettiin "Yleiskuva"-karttaan, sillä se ei vie paljoa tilaa, ja se saattaa tulevaisuudessa ilmoittaa lähestyvistä ongelmista.





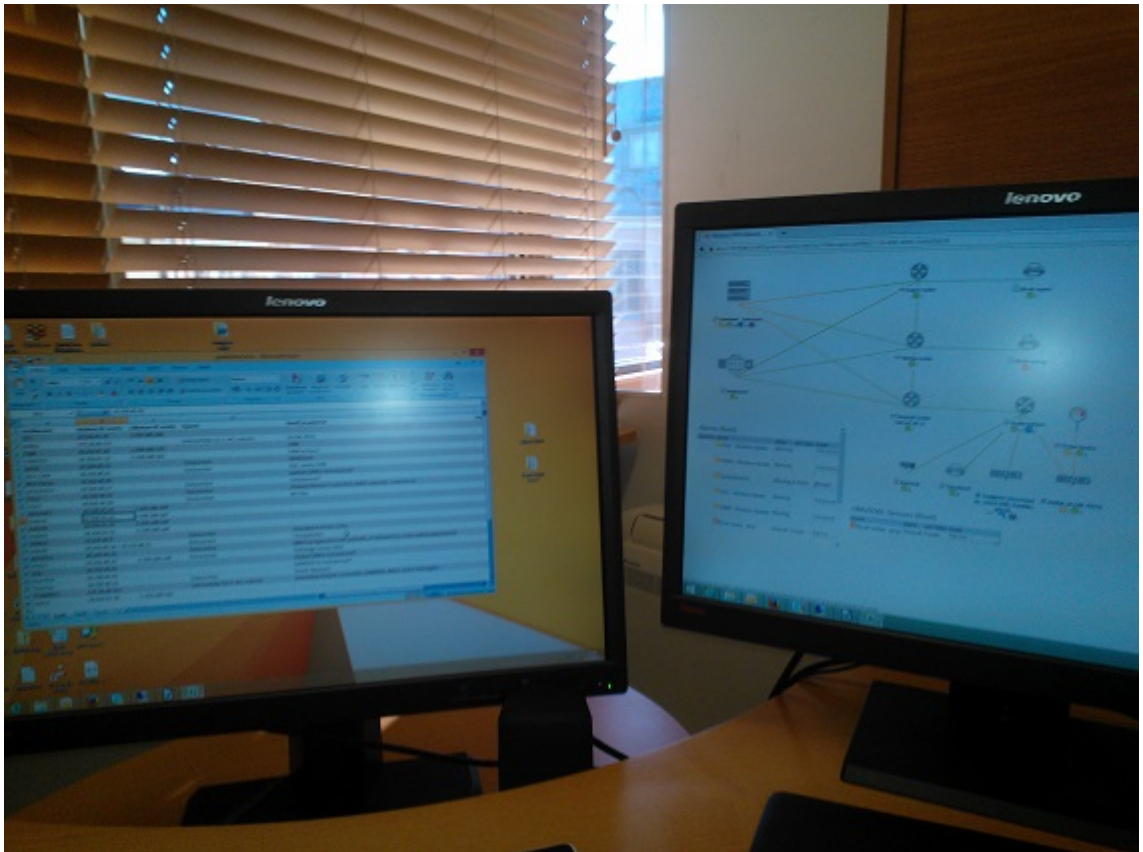
Kuva 38. "Yleiskuva"-kartta. Kartassa näkyvät kaikki seurattavat laitteet joko ryhmään sisällytettyinä tai omana laitteenaan. Lisäksi kaksi taulukkoa listaa Warning- ja Down-, sekä Unusual-statusen sensoreita.

Toinen luotu kartta avaa hieman Helsingin toimipisteen verkon rakennetta ja näyttää tarkemmin siellä sijaitsevat laitteet. Sen avulla näkee helposti, missä mahdollisesti viallinen laite sijaitsee. Siihen on otettu mukaan kaikki verkkoinfrastruktuuriin liittyvät laitteet ja IP-kamerat sekä niiden tallennus-NAS. Se näyttää, mihin kytkimeen on mikäkin laite kytketty ja missä kerroksessa laitteet sijaitsevat.



Kuva 39. "Verkkolaitteet"-kartta. Kartassa näkyy Helsingin toimiston verkkoinfrastruktuuriin kuuluvat laitteet sekä "Kamerat"-ryhmä. Kuvaaja on sensorista, joka seuraa kytkimen SW-5.1.1 ja reitittimen välistä liikennettä, eli kaikkea Helsingin toimistolta poistuvaa liikennettä.

Näiden karttojen asetuksista säädettiin kartat julkisesti saataviksi, jonka jälkeen niitä pääsee tarkastelemaan verkkoselaimen kautta kartan asetuksista löytyvän linkin avulla. Kartan voi esimerkiksi avata erilliselle näytölle, ja se päivittyy automaattisesti näyttäen lähes välittömästi Warning- tai Down-statusen sensorit. Tämä toiminnallisuus on tarkoitettu yrityksen koko ICT-osaston käyttöön, jolloin joku varmasti huomaa, jos seuraavissa laitteissa esiintyy vikoja.



Kuva 40. "Yleiskuva"-kartta selaimessa työpisteen toisella näytöllä.

Kuvassa 40 näkyy PRTG:n "Yleiskuva"-kartta toisella monitorilla. Aina kun toista näyttöä ei tarvitse, se voi olla näkyvillä ja sivusilmällä havaitsee helposti, jos karttaan ilmestyy keltaisia tai punaisia hälytyksiä. Tulevaisuudessa on tarkoitus ottaa yrityksen IT-osastolle käyttöön dedikoitu TV, joka näyttää vähintään "Yleiskuva"-kartan tilaa jatkuvasti, jolloin karttoja ei tarvitsisi pitää omilla näytöillä PRTG:tä seuratakseen. Eri karttoja voi myös laittaa automaattisesti kiertoon saman linkin kautta, jolloin määritetyn ajan välein karttanäkymä vaihtuu seuraavaan. Tällä tavalla voidaan esimerkiksi dedikoidun näytön kautta seurata kaikkia karttoja ilman, että niitä täytyisi vaihdella manuaalisesti. [42.]

## 5 Yhteenveto

Yrityksen verkon sisältämistä laitteista, niiden konfiguraatioista ja niiden välisistä yhteyksistä tehtiin selkeät dokumentaatiot Excel-taulukoiden muodoissa ja tarkemmat tiedot, kuten kytkinten konfiguraatiot löytyvät erillisistä dokumenteista tarvittaessa. Dokumentaatio laitettiin yrityksen intranet-sivustolle ICT:n osion alle, jossa se olisi tarpeen tullen helposti saatavilla. Dokumentaatiota selkeyttämään piirrettiin laitteiden loogisista ja fyysisistä sijainneista ja niiden välisistä kytkennöistä Visio-piirros. Sen avulla voi esimerkiksi nopeuttaa yrityksen ulkopuolisten asentajien työtä ja paikantaa laitteita.

Yrityksen verkon toiminnasta lähetettiin sähköpostitse kysely yrityksen työntekijöille ongelma-kohtien löytämiseksi. Lisäksi käytiin läpi yrityksen Helsingin toimipisteen kytkimien, WLAN-kontrollerin ja sen hallinnoimien langattomien tukiasemien asetukset, sekä yrityksen domain controllerien DHCP- ja DNS-asetukset. Kriittisiä vikoja ei tullut vastaan missään vaiheessa. Korjatut viat lähinnä paransivat verkon viansietokykyä ja helpottivat hallinnointia.

Yrityksen verkon tilan seuraamiseen asennettiin PRTG Network Monitor, joka ylitti kaikki odotukset ja mahdollisti todella helpon verkon tilan seurannan. Lisäksi ohjelmiston avulla pystytään seuraamaan yrityksen palvelimien ja niissä toimivien kriittisten sovellusten toimintaa. PRTG:n mahdollisuus seurata laitteiden tilannetta verkkoselaimen kautta millä vaan yrityksen tietokoneella ja tulevaisuudessa mahdollisesti erillisen TV:n kautta nostaa ongelmien havaitsemisen nopeuden kiitettävälle tasolle. PRTG:n ilmaisversion rajoitukset vaativat tarkkoja päätöksiä siitä, mitkä seurattavat asiat olivat kriittisimpiä ja mitä vähemmän kriittisiä asioita voidaan jättää seuraamatta.

Tarvittaessa maksulliseen lisenssiin ja laajempaan seurantaan päivittäminen käy kuitenkin hetkessä, sillä sensoreita voi tehdä etukäteen niin paljon kuin haluaa, kunhan jättää ne pysäytettyyn tilaan.

Työn seurauksena yrityksellä on selkeä käsitys sisäverkkonsa toiminnasta ja rakenteesta ja näin ollen helpompi mahdollisuus tehdä muutoksia tulevaisuudessa.

Työtä varten ei hankittu mitään laitteita tai maksullisia ohjelmistoja, vaan kaikki tehtiin yrityksen olemassa olevilla laitteilla ja ohjelmistoilla sekä ilmaisohjelmilla. Myös helpompaa verkon tilan seurantaan varten suunniteltu dedikoitu näyttö ohjauskoneineen ja kaapeleineen löytyvät jo yrityksen varastosta ja odottavat vain asennusta. Työn suoraa taloudellista hyötyä yritykselle on vaikea arvioida, sillä hyödyt tulevat esille lähinnä vikatilanteiden välttämisenä ja vikojen korjauksen nopeutumisena, mutta tarvittaessa vastaavan selvityksen ja seurantaohjelmiston käyttöönotosta pelkästään työtunneista ulkopuolinen toimija laskuttaisi todennäköisesti tuhansia euroja. Tällä oletuksella työ on kokonaisuudessaan sekä taloudellisesti että toiminnallisesti yritykselle hyödyllinen.

## Lähteet

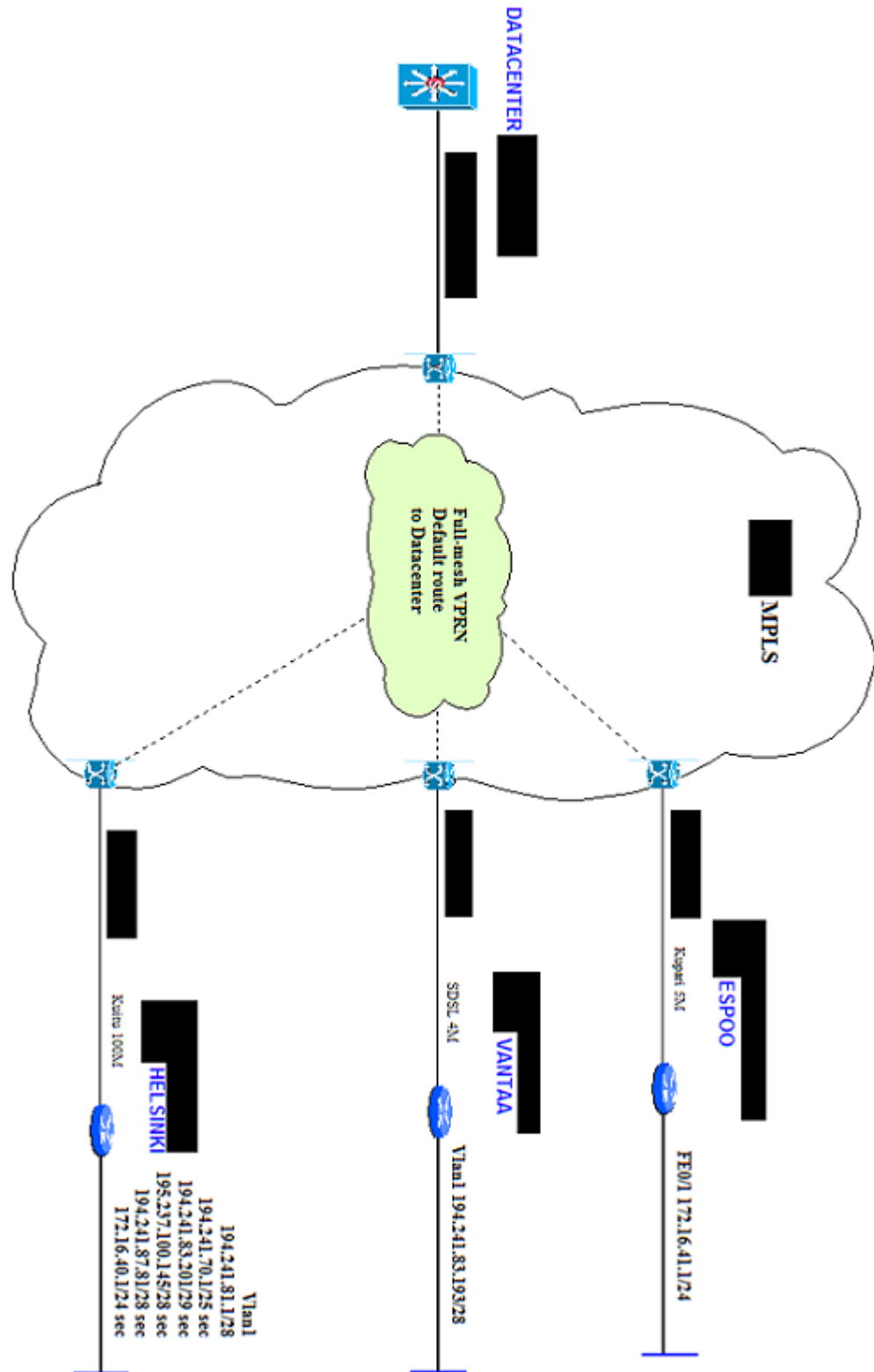
- 1 <http://www.advanced-ip-scanner.com/help/> Luettu 15.10.2015.
- 2 <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html> Luettu 11.10.2015.
- 3 [http://www.skullbox.net/hp\\_procurve\\_vlan.php](http://www.skullbox.net/hp_procurve_vlan.php) Luettu 11.10.2015.
- 4 <http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanmerkint.html> Luettu 12.10.2015.
- 5 <http://cdn.procurve.com/training/Manuals/2510G-MgmtCfg-Jun2008-59923095.pdf> Luettu 18.10.2015.
- 6 [http://h20628.www2.hp.com/km-ext/kmcsdirect/emr\\_na-c03594944-1.pdf](http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c03594944-1.pdf) Luettu 18.10.2015.
- 7 <http://h30499.www3.hp.com/t5/Switches-Hubs-Modems-Legacy-ITRC/What-qualifies-as-quot-excessive-broadcasts-quot/td-p/3525045> Luettu 11.10.2015.
- 8 <http://h30499.www3.hp.com/t5/ProCurve-ProVision-Based/Excessive-broadcasts-and-CRC-Alignment-errors-on-ProCurve-2610A/td-p/5574749> Luettu 11.10.2015.
- 9 <http://www.pool.ntp.org/en/> Luettu 18.10.2015.
- 10 <https://technet.microsoft.com/en-us/library/cc794937%28v=ws.10%29.aspx> Luettu 11.10.2015.
- 11 <http://www.sysadminlab.net/windows/configuring-ntp-on-windows-server-2012> Luettu 11.10.2015.
- 12 <http://blogs.msdn.com/b/w32time/archive/2008/04/02/configuring-a-standalone-time-server.aspx> Luettu 11.10.2015.
- 13 <http://www.windowstimestamp.com/PartIIAdjustmentofSystemTime.pdf> Luettu 12.10.2015.
- 14 <http://www.techieshelp.com/procurve-e-series-how-to-define-sntp-time-server-synchronization/> Luettu 12.10.2015.
- 15 <http://doc.ntp.org/4.2.6p3/ntpd.html> Luettu 12.10.2015.
- 16 [http://www.tlu.ee/~matsak/telecom/lasse/spanning\\_tree\\_algorithm/ieee\\_8021d\\_stp\\_spanning\\_tree\\_protokolla.html](http://www.tlu.ee/~matsak/telecom/lasse/spanning_tree_algorithm/ieee_8021d_stp_spanning_tree_protokolla.html) Luettu 13.10.2015.
- 17 <http://www.dummies.com/how-to/content/spanning-tree-protocol-stp-introduction.html> Luettu 13.10.2015.
- 18 [http://www.hp.com/rnd/support/manuals/pdf/release\\_06628\\_07110/Bk2\\_Ch5\\_STP.pdf](http://www.hp.com/rnd/support/manuals/pdf/release_06628_07110/Bk2_Ch5_STP.pdf) Luettu 11.10.2015.

- 19 [https://community.spiceworks.com/how\\_to/43285-how-to-set-up-stp-on-hp-switches](https://community.spiceworks.com/how_to/43285-how-to-set-up-stp-on-hp-switches) Luettu 11.10.2015.
- 20 <http://www1.hp.com/ctg/Manual/c02571903.pdf> Luettu 18.10.2015.
- 21 <https://cdn.cnetcontent.com/0c/9c/0c9c9003-0f7c-4b04-bc71-eba0ba4d6bbc.pdf> Luettu 19.10.2015.
- 22 [https://technet.microsoft.com/en-us/library/cc755301%28v=ws.10%29.aspx#bkmk\\_wlanShowNetworks](https://technet.microsoft.com/en-us/library/cc755301%28v=ws.10%29.aspx#bkmk_wlanShowNetworks) (Luettu 19.10.2015)
- 23 [https://www.juniper.net/documentation/en\\_US/network-director1.5/topics/concept/wireless-encryption-and-ciphers.html](https://www.juniper.net/documentation/en_US/network-director1.5/topics/concept/wireless-encryption-and-ciphers.html) Luettu 18.10.2015.
- 24 <http://myitforum.com/myitforumwp/2012/07/20/whos-the-primary-find-the-primary-dc/> Luettu 18.10.2015.
- 25 <https://tools.ietf.org/html/rfc2131> Luettu 13.10.2015.
- 26 <https://technet.microsoft.com/en-us/library/cc754471.aspx> Luettu 18.10.2015.
- 27 <https://support.microsoft.com/en-us/kb/133490> Luettu 18.10.2015.
- 28 <https://technet.microsoft.com/en-us/library/cc779507%28v=ws.10%29.aspx> Luettu 18.10.2015.
- 29 <https://technet.microsoft.com/en-us/library/cc775637%28v=ws.10%29.aspx> Luettu 18.10.2015.
- 30 <https://technet.microsoft.com/en-us/library/cc730980.aspx> Luettu 18.10.2015.
- 31 <https://technet.microsoft.com/en-us/library/cc781949%28v=ws.10%29.aspx> Luettu 18.10.2015.
- 32 [https://www.paessler.com/manuals/prtg/context\\_menus](https://www.paessler.com/manuals/prtg/context_menus) (luettu 20.10.2015)
- 33 [https://www.paessler.com/manuals/prtg/auto\\_discovery](https://www.paessler.com/manuals/prtg/auto_discovery) Luettu 18.10.2015.
- 34 [https://www.paessler.com/manuals/prtg/add\\_a\\_sensor](https://www.paessler.com/manuals/prtg/add_a_sensor) (luettu 20.10.2015)
- 35 [https://www.paessler.com/manuals/prtg/multi\\_edit\\_lists](https://www.paessler.com/manuals/prtg/multi_edit_lists) (luettu 20.10.2015)
- 36 [https://www.paessler.com/manuals/prtg/windows\\_update\\_info\\_sensor](https://www.paessler.com/manuals/prtg/windows_update_info_sensor) Luettu 18.10.2015.
- 37 [https://www.paessler.com/manuals/prtg/sensor\\_states](https://www.paessler.com/manuals/prtg/sensor_states) (luettu 20.10.2015)
- 38 <https://www.paessler.com/manuals/prtg/notifications> (luettu 20.10.2015)
- 39 <https://www.paessler.com/manuals/prtg/dependencies> Luettu 18.10.2015.
- 40 [https://www.paessler.com/manuals/prtg/sensor\\_channels\\_settings](https://www.paessler.com/manuals/prtg/sensor_channels_settings) Luettu 18.10.2015.
- 41 [https://www.paessler.com/manuals/prtg/ping\\_sensor](https://www.paessler.com/manuals/prtg/ping_sensor) Luettu 18.10.2015.

42 <https://www.paessler.com/manuals/prtg/maps> Luettu 18.10.2015.



## Internetpalveluntarjoajan verkkodokumentti



Palvelimet

Verkkointimi	Sisäinen IP-osote	Ulkoinen IP-osote	Sijainti	Roolit ja palvelut	Riippuvuudet
0	10.250.40.10		Datacenter		
DATA	10.250.40.12		Datacenter	ClickView	
	10.250.40.20		Datacenter	DMZ:ssä sijaitseva web-palvelin, et-dominissa, Indox julkaisujärjestelmä	
FILE1	10.250.40.21		Datacenter	Primary DC, DHCP Espoole, verkkolevyt	
POSTI	10.250.40.22		Datacenter	Exchange Server 2010	
TALOUS	10.250.40.23		Datacenter	Sonet, Barware, verkkolevyt	
FILE2	10.250.40.26		Datacenter	M-Files	
EXTKANTA	10.250.40.27		Datacenter		
1	10.250.40.4		Datacenter	Sharepoint server 2007, Intranet	DEV-Kanta
DEV-Kanta	10.250.40.40		Datacenter	vanha CRM:n tietokannat	DEV-Kanta
DEV-CRM	10.250.40.41		Datacenter	vanha CRM	
SQLTEST	10.250.40.42		Datacenter	CRMTESTin tietokannat	
SQL	10.250.40.43		Datacenter	Juuden CRM:n tietokannat	
10	10.250.41.10		Datacenter		
	10.250.41.20		Datacenter		
CRMTEST	10.250.41.22		Datacenter	CRM testaus	SQLTEST
ADFS	10.250.41.23		Datacenter		
CRM	10.250.41.24		Datacenter	CRM	ADFS, SQL
wpres	10.250.41.28		Datacenter		
30	10.250.41.30		Datacenter		
	10.250.41.31		Datacenter		
TOIMISTO	172.16.40.115			Secondary DC, ESMIKKO, WSUS, SEPM, verkkotulostimet, DHCP heisingille	
ANNA	172.16.40.131			SCCM, PRIG	

Tulostimet

Laitte	IP-osoite	Sijainti	Muuta
RICOH ESPOO	172.16.41.106	Espoo	
VAIHDE	172.16.40.222	5. krs Vaihde	HP laserjet
RICOH YLEINEN	194.241.70.94	2. krs Aspa	
	194.241.70.86		HP laserjet
RICOH POSTITUSKESKUS	194.241.70.98	5. krs Postituskeskus	
RICOH VANTAA	194.241.83.199	Vantaa	
	194.241.70.96	5. krs ICT	
RICOH KOULUTUS	194.241.70.97	2. krs Palveluliiketoiminta	
Ricoh-lisälaite	194.241.70.14	5. krs ICT-varasto	

## IP-kamerat

Laitte	IP-osoite	Muuta
	172.16.40.201	TOIMISTO:n DHCP:n exclude poolissa
	172.16.40.202	TOIMISTO:n DHCP:n exclude poolissa
	172.16.40.203	TOIMISTO:n DHCP:n exclude poolissa
	172.16.40.204	TOIMISTO:n DHCP:n exclude poolissa
	172.16.40.205	TOIMISTO:n DHCP:n exclude poolissa
	172.16.40.206	TOIMISTO:n DHCP:n exclude poolissa, paikasta ei varmuutta
	172.16.40.207	TOIMISTO:n DHCP:n exclude poolissa
Video NAS	172.16.40.200	TOIMISTO:n DHCP:n exclude poolissa

**Vantaan toimiston IP-osoitteet**

<b>Nimi</b>	<b>Verkkonimi</b>	<b>IP-osoite</b>
	MS-S15-HEL-04	194.241.83.194
	LV-K14-VAN-01	194.241.83.195
Kolmas kone		194.241.83.198
<b>Osoitealue</b>	-	194.241.83.193 - 194.241.83.206

## Verkkoinfrastruktuuri

Laite	Verkkonimi	IP-osoite	Sijainti	Merkki ja malli	itse hallinnoitu
<b>Reititimet</b>					
Helsinki router		194.241.81.1	5.krs, kytkentäkaappi 1	Cisco	ei
Espoo router		172.16.41.1	Espoo		ei
Vantaa router		194.241.83.193	Vantaa		ei
<b>Kytkimet</b>					
5.1.1	SW-5.1.1	10.255.255.51	5.krs, kytkentäkaappi 1	HP Procurve 2510G-48	kyllä
5.1.2	SW-5.1.2	10.255.255.52	5.krs, kytkentäkaappi 1	HP Procurve 2510G-48	kyllä
5.2.1	SW-5.2.1	10.255.255.53	5.krs, kytkentäkaappi 2	HP Procurve 2510G-48	kyllä
2.1.1	SW-2.1.1	10.255.255.21	2.krs, kytkentäkaappi 1	HP Procurve 2510-24	kyllä
2.1.2	SW-2.1.2	10.255.255.63	2.krs, kytkentäkaappi 1	HP Procurve 2530-48G	kyllä
2.2.1	SW-2.2.1	10.255.255.62	2.krs, kytkentäkaappi 2	HP Procurve 2510G-48	kyllä
2.3.1	SW-2.3.1	10.255.255.60	2.krs, kytkentäkaappi 3	HP Procurve 2510G-48	kyllä
2.3.2	SW-2.3.2	10.255.255.61	2.krs, kytkentäkaappi 3	HP Procurve 2510G-48	kyllä
<b>Langaton verkko</b>					
WLAN-kontrolleri		194.241.70.12	2.krs, kytkentäkaappi 2	HP MSM760	kyllä
SG9082S247		172.16.40.51			kyllä, kontrollerin kautta
SG9122S3NY		172.16.40.56			kyllä, kontrollerin kautta
SG9122S3JX		172.16.40.75			kyllä, kontrollerin kautta
SG9062S331		172.16.40.76			kyllä, kontrollerin kautta
SG0359L0NF		172.16.40.105			kyllä, kontrollerin kautta
SG9092S821		172.16.40.135			kyllä, kontrollerin kautta
SG0359L0GH		172.16.40.142			kyllä, kontrollerin kautta
SG0359L0FY		172.16.40.146			kyllä, kontrollerin kautta
SG0309L16V		172.16.40.147			kyllä, kontrollerin kautta
SG0309L150		172.16.40.154			kyllä, kontrollerin kautta
SG0359L0P8		172.16.40.181			kyllä, kontrollerin kautta

Kytkinten portit osa 1

Kytkin / Portti	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
5.1.1																												
5.1.2	ANNA																											
5.2.1								RICOH POSTITUSKESKUS																				
2.1.1												AP 5G9802SNZ																
2.1.2																												
2.2.1																												
2.3.1																												
2.3.2																												
Merkinä	<p>Sellitys palvelu- tai verkkoinfrastruktuurin kuuluva laite</p> <p>088:laiteet</p> <p>Työpa portti</p> <p>Porttia ei ole</p> <p>Langaton tukiasema (Access Point)</p> <p>AP</p>																											





## Kysely kiinteän verkon toimivuudesta

### Kysely kiinteän verkon toimivuudesta [REDACTED] henkilöstölle

Tämän kyselyn tarkoitus on kartoittaa kiinteän (langallisen) verkon toimivuutta käyttäjien näkökulmasta, jotta voidaan paikallistaa mahdolliset ongelmakohdat verkossa – ja korjata ne mahdollisuuksien mukaan. Kyselyyn vastaaminen ei ole pakollista, mutta suositeltavaa. Jos ongelmia ei ole esiintynyt, tai esiintyy vain harvoin, voit jättää vastaamatta kyselyyn. Jos vastaat kyselyyn, tee se huolellisesti niin saadaan kunnollinen kuva ongelmista ilman välittömiä lisäselvityksiä.

Verkko-ongelmia ovat esimerkiksi:

- verkkosivujen hidas aukeneminen ja aukaisun epäonnistuminen
- verkkoa käyttävän ohjelman hidastelu muiden ohjelmien toimiessa normaalisti (esim. lync pätkii)
- kellon vieressä sijaitsevan verkkokuvakkeen päällä keltainen huutomerkki tai punainen ruksi
- tulostus ei onnistu tai verkkotulostinta ei löydy
- verkkolevyihin ei saa yhteyttä tai verkkolevyjen käyttö on hidasta

**Huom!** Yleisessä vikatilanteessa, [REDACTED] tapahtuvista ongelmista ei tarvitse ilmoittaa tässä kyselyssä.

Nimi	
Sähköpostiosoite	
Ongelman esiintymispaikka (osoite, kerros, osasto)	
Verkko-ongelmien esiintymistiheys (esim. 3 kertaa päivässä)	
Verkko-ongelma koskee (ohjelmistot/laitteet joihin ei saa yhteyttä)	
Käytössä oleva laite (pöytäkone/läppäri/tabletti)	
Verkko-ongelmien vakavuus (hidastelu/täysi yhteyden menetys)	
Vapaa kuvaus ongelmista	

Palauta täytetty kysely sähköpostiin [REDACTED]

Henkilötietoja, kuten nimeä ja sähköpostiosoitetta ei tulla julkaisemaan missään.

## Yrityksen verkon kuva

