Ville Kangas

Langattoman lähiverkon tietoturva ja laadunhallinta

7signal-laadunhallintajärjestelmä

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikka
Insinöörityö
15.4.2012

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Ville Kangas Langattoman lähiverkon tietoturva ja laadunhallinta, 7signal-laadunhallintajärjestelmä 36 sivua 15.4.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Jukka Louhelainen

Tässä insinöörityössä käsitellään langattomia verkkoja ja niiden tekniikoita, tietoturvaa ja laadunhallintaa. Työn tavoitteena oli konfiguroida 7signal Sapphire -järjestelmä Metropolian langattomille verkoille, raportoida järjestelmä, kertoa tuloksista ja tietoturvasta. Insinöörityö tehtiin Metropolia Ammattikorkeakoululle.

Insinöörityössä esitellään ja testataan suomalaisen 7signal Oy:n Sapphire-järjestelmää, joka on tällä hetkellä ainoa WLAN-verkon automaattinen laadunhallintajärjestelmä, esitellään Metropolian 7signal Sapphire -järjestelmää, langattoman lähiverkon tietoturvaa sekä laadunhallintaa.

Ympäristö, johon 7signal-laadunhallintajärjestelmä oli rakennettu, koostui kolmesta langattomasta verkosta ja yli kymmenestä tukiasemasta.

Langattomat verkot tuli kartoittaa ja konfiguroida järjestelmään. Myös testiprofiili tuli konfiguroida langattomille verkoille sopivaksi. Etäyhteys konfiguroitiin myös järjestelmään.

Työn tuloksena valmistui raportti Metropolian 7signal-laadunhallintajärjestelmästä ja tietoturvasta.

Avainsanat	WLAN, 7signal, laadunhallinta, tietoturva, 802.11

Metropolia

Abstract

Author(s) Title Number of Pages Date	Ville Kangas Security and monitoring of WLAN network, 7signal Wireless Quality Assurance solution 36 15 April 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Jukka Louhelainen, Senior Lecturer

This thesis deals with wireless networks and its technologies, data security and quality assurance. The purpose was to configure the 7signal Sapphire system to Metropolia wireless networks, report the system, tell about the results and data security. Thesis was made to Metropolia University of Applied Sciences.

In this thesis is presented and tested Finnish 7signal Ltd's Wireless Quality Assurance solution. 7Signal WQA solution is currently the only automatic WLAN quality control system. This thesis also presents Metropolia's 7signal Sapphire system, WLAN security and quality assurance.

Environment where 7signal Quality Asssurance solution was built consisted of three wireless networks and over ten access points.

Wireless networks were identified and configured to the system. Test profile was also configured for wireless networks. Remote access was also configured to the system.

The result of this project was report of Metropolia's 7signal Quality Assurance solution and data security.

Keywords	WLAN, 7signal, quality assurance, data security, 802.11

Sisällys

Termistö

Termistö

Autentikointi	Kontekstissa käyttäjän identiteetin varmistaminen eli todennus.
CCK	Complementary Code Keying, modulaatiokaava.
CentOS	Linux-distribuutio.
Deautentikointi	Vastakkainen tapahtuma autentikoinnille eli käyttäjän todennuksen purku.
EAP	Extensible Authentication Protocol, langattomissa verkoissa käytettävä autentikointiprotokolla.
FTP	File Transfer Protocol, tiedostojensiirtoprotokolla.
HTML	HyperText Markup Language, WWW-sivujen pää merkintäkieli.
HTTP	Hypertext Transfer Protocol, selainten ja WWW-palvelinten tiedonsiirtoon käyttämä protokolla.
HTTPS	Hypertext Transfer Protocol Secure, SSL/TLS-prokollan yhdistelmä salattuun selainten ja WWW-palvelinten tiedonsiirtoon.
ICMP	Internet Control Message Protocol, viestienlähetysprotokolla.
IEEE	Institute of Electrical and Electronics Engineers, standardointijärjestö.
IP-osoite	Internet Protocol-osoite, numeroista ja pisteistä koostuva osoite, joka annetaan jokaiselle verkossa olevalle laitteelle, joka käyttää Internet Protokollaa.

Javascript	Prototyyppipohjainen ohjelmointikieli, käytetään esimerkiksi WWW-sivuissa.
KPI	Key Performance Indicator, suorituskykyilmaisin.
MAC-osoite	Media Access Control-osoite, yksilöi verkkosovittimen ethernet-verkossa.
MIMO	Multiple-Input Multiple-Output, tietoliikennetekniikka, jossa lähetykseen ja vastaanottoon käytetään useampaa antennia samanaikaisesti.
OFDM	Orthogonal frequency division multiplexing, DMT-modulointi.
PEAP	Protected Extensible Authentication Protocol, langattomissa verkoissa käytettävä salattu autentikointiprotokolla.
POC	Proof Of Concept, demonstraatio toimintaperiaatteesta.
Päätelaite	Verkossa oleva käyttäjälaite, esimerkiksi älypuhelin tai kannettava tietokone.
RADIUS	Remote Authentication Dial In User Service, protokolla, jolla käyttäjät tai laitteet voidaan autentikoida keskitetystä järjestelmästä.
RDP	Remote Desktop Protocol, Microsoftin graafinen etäkäyttöprotokolla.
RSA	Rivest Shamir Adleman, julkiseen avaimeen perustuva salausalgoritmi.
SNR	Signal to Noise Ratio, signaali-kohinasuhde.

SSH	Secure Shell, protokolla turvalliseen kommunikointiin ja datan siirtoon.
SSID	Service Set Identifier, langattoman lähiverkon verkkotunnus.
SSL	Secure Sockets Layer, TLS:ää edeltävä kryptografinen protokolla joka mahdollistaa turvallisen kommunikoinnin Internetin yli.
TCP	Transmission Control Protocol, yhteydellinen kuljetusprotokolla.
TLS	Transport Layer Security, kryptografinen protokolla, joka turvallisen kommunikoinnin Internetin yli.
Ubuntu	Linux-distribuutio.
UDP	User Datagram Protocol, yhteydetön kuljetusprotokolla.
VoIP	Voice over IP, protokolla äänen ja multimedian välitykseen IP-verkkojen yli.
VNC	Virtual Network Computing, graafisen käyttöliittymän etäkäyttöprotokolla.
WEP	Wired Equivalent Privacy, langattoman verkon salaustekniikka.
WIDS	Wireless Intrusion Detection System, langattoman verkon tunkeutumisen tunnistusjärjestelmä.
WIPS	Wireless Intrusion Prevention System, langattoman verkon tunkeutumisen estojärjestelmä.
WLAN	Wireless Local Area Network, langaton lähiverkko.

WPA	Wi-Fi Protected Access, langattoman verkon salaustekniikka.
WPA2	Wi-Fi Protected Access, langattoman verkon salaustekniikka.
WPS	Wi-Fi Protected Setup, protokolla, joka mahdollistaa helpon yhteyden turvalliseen tukiasemaan.
WQA	Wireless Quality Assurance, langaton laadunhallinta.

1 Johdanto

Tämän insinöörityön tavoitteena on konfiguroida Metropolian 7signal Sapphire-laadunhallintajärjestelmä koulun langattomille verkoille ja raportoida järjestelmä. Kartoitan myös Metropolian Bulevardin toimipisteen langattomien verkkojen tietoturvan ja kerron 802.11-standardeista ja langattomien verkkojen tietoturvasta.

Langattomat verkot ovat yleistyneet huomattavasti muutaman viime vuoden aikana. 802.11n-standardi on kehitetty 2,4 GHz:n ja 5 GHz:n taajuuksille auttamaan 2,4 GHz-taajuusalueen ruuhkautuneisuudessa ja lisänopeuden tarpeessa. 802.11b/g 2,4 GHz-verkkoja on niin paljon käytössä, että vapaita taajuuksia eli WLAN-kanavia on jo vaikeaa löytää. 802.11n-standardin 5 GHz-taajuusalue ei ole yhtä ruuhkainen tällä hetkellä, jolloin se ei ole myöskään niin häiriöaltis kuin 2,4 GHz:n taajuusalue.

Langattomat verkot on monessa mielessä kätevämpiä kuin langalliset verkot, vaikka niissä on enemmän riskejä. Langattomat verkot ovat käteviä varsinkin, jos tarvitaan liikkuvuutta ja verkkoyhteyttä monelle laitteelle, esimerkiksi älypuhelimelle tai kannettavalle tietokoneelle. Tällöin kaapeleiden vetäminen ei ole mielekästä eikä välttämättä mahdollistakaan.

Langattomien verkkojen hallinta on kuitenkin haaste. Monitorointi on aikaa vievää ja vaikeaa tai jopa mahdotonta. Vikojen tunnistus perustuu useimmiten loppukäyttäjän raportointiin. Uudet sovellukset ja tekniikat kuten esimerkiksi VoIP langattomassa verkossa asettavat tiukat vaatimukset verkon laadulle. Useat systeemit samalla taajuusalueella voivat häiritä toisiaan ja aiheuttaa häiriöitä järjestelmissä. [1, s. 3.]

2 Langattomien verkkojen tekniikat ja taajuudet

2.1 IEEE 802.11a

IEEE 802.11a on julkaistu vuonna 1999. A-standardi toi 5 GHz:n alueelle 54 Mbit/s nopeuden. 5 GHz:n alueelle siirryttiin 802.11-standardin 2,4 GHz:n alueesta lisäkaistan saamiseksi, jotta verkkoyhteyksien nopeuksia pystyttäisiin nostamaan. A-standardissa siirryttiin tiedonsiirtotekniikkana OFDM-tekniikkaan. Tämä tekniikka perustuu pienempiin alasignaaleihin, joihin signaali on jaettu. Nämä signaalit siirretään samanaikaisesti käyttäen eri taajuuksia. Näiden muutosten avulla saavutettiin 54 Mbit/s:n nopeus. Teoreettinen nopeus on 6-54 Mbit/s. [2.]

2.2 IEEE 802.11b

IEEE 802.11b on vuonna 1999 julkaistu standardi, jonka tarkoituksena oli tuoda 5,5 Mbit/s:n nopeus ja 11 Mbit/s:n nopeus uusina nopeuksina langattomille verkoille. 802.11b toimii 2,4 GHz:n alueella ja käyttää CCK-tekniikkaa tiedonsiirrossa. Tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. Jokaisella koodisanalla on oma matemaattinen merkityksensä sarjamuodossa. B-standardi ei ole yhteensopiva A-standardin kanssa. B-standardin teoreettiset nopeudet ovat 1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s ja 11 Mbit/s. [2.]

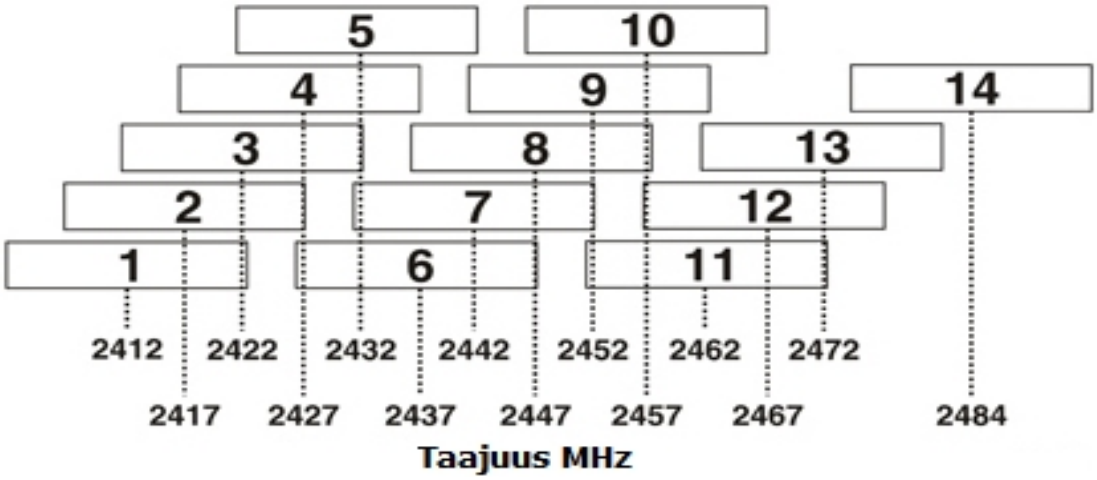
2.3 IEEE 802.11g

IEEE 802.11g on uudempi standardi, joka on julkaistu 2003. Nykyään 802.11g-standardi on syrjäyttänyt 802.11b-standardin yleisesti. 802.11b mahdollistaa 2,4 GHz:n alueella 802.11a-standardin tapaan 54 Mbit/s:n nopeuden. G-standardi on yhteensopiva B-standardin kanssa. Teoreettinen nopeus on 1-54 Mbit/s. [2.]

2.4 IEEE 802.11n

IEEE 802.11n on uusin laajasti käytössä oleva IEEE 802.11-verkkostandardi. Se on standardoitu vuonna 2009 IEEE:n toimesta. N-standardi parantaa suorituskykyä aikaisempiin 802.11-standardeihin verrattuna. 802.11n-standardi käyttää MIMO-tekniikkaa, jolloin useammalla antennilla saadaan parempi kantama ja signaaliyhteys päätelaitteelle. N-standardi on yhteensopiva B -ja G-standardien kanssa. B -tai G-standardia käytettäessä yhteyden nopeuden määrittää vanhempi standardi. N-standardi toimii 2,4 GHz:n ja 5 GHz:n alueella. Kanavat ovat 20 tai 40 Mhz:n välein. N-standardin teoreettinen maksiminopeus on 600 Mbit/s, joka todellisuudessa vastaa 100-200 Mbit/s eli yleistä 100 Mbit/s Ethernet-kaapelia. [2.]

2.5 2,4 GHz:n taajuusalue



Kuva 1: 2,4 GHz-taajuusalueen kanavat

2,4 GHz:n taajuusalueella on käytössä 13 kanavaa Euroopassa. Kanavien leveyksillä on eroa 20 MHz ja keskitaajuuksilla 5 MHz. Kanava 14 on käytössä vain Japanissa. Euroopassa on 4 vähähäiriöistä kanavaa, joilla taajuudet eivät mene päällekkäin. Nämä kanavat ovat 1, 5, 9 ja 13, 20 MHz:n välein. [2.]

3 7signal Sapphire -järjestelmä

3.1 Yleistä

7signalin Sapphire -laadunhallintajärjestelmä on tarkoitettu yritysten langattomien verkkojen monitorointiin ja langattomaan laadunvarmistukseen. Sillä voidaan automaattisesti tai manuaalisesti tarkkailla yrityksen langattomia verkkoja ja ympäröivää radiotaajuusympäristöä yhtäjaksoisesti. Järjestelmällä voidaan suorittaa automaattisia tai manuaalisia testejä, joilla selvitetään verkon ruuhkautuneisuus mm. vasteaikojen avulla. Järjestelmällä voidaan muuntaa testien raportit PDF-muotoon, jolloin ne voidaan lähettää viikoittain sähköpostilla tarkistettavaksi. [3, s. 1.]

7signalin Sapphire -laadunhallintajärjestelmässä verkon suorituskyky voidaan testata Sonar-palvelinta vastaan. Interaktiiviset testit, monitorointiasemat ja parametrit automaattisiin hallinnoidaan keskitetyllä Sapphire Carat -hallintatyökalulla. Testien tulokset tallennetaan tietokantaan ja ne raportoidaan Sapphire Loupe -rapotointityökalulla. [3, s. 1.]

Sapphire Eye eli valvontasilmä monitoroi jatkuvasti valittuja WLAN-kanavia passiivisesti, jolloin se ei vaikuta verkon suorituskykyyn. Silmä voi myös emuloida päätelaitetta kohdeverkossa ja silloin käyttää verkkoa ja palveluita sen kautta. Analysoimalla mittausten ja testien tuloksia voidaan mitata verkon suorituskyky ja palvelunlaatu eli QoS. WQA-ratkaisu voi tuottaa muuttuvaa statiikkaa tietyn käyttäjän näkökulmasta verkon suorituskyvystä. Tämä mahdollistaa verkon kapasiteetin lisäämisen ennen kuin verkossa tapahtuu huomattavaa suorituskyvyn menetystä. [3, s. 1.]

Käyttäjä-emulaatiotesteissä eli aktiivitesteissä silmä yhdistää Sonar-testiserverille langattoman verkon kautta ja käyttää sitä kuin tavallista tuotantopalvelinta. Tämä voi tarkoittaa suuria tiedostonsiirtoja, selaimen latauksia, langattomia VoIP-puheluita tai vaikkapa yhteyttä toiseen tuotantopalvelimeen. Sapphire-järjestelmä testaa loppukäyttäjän käyttökokemusta tutkimalla koko dataketjua asiakkaalta tuotantopalvelimelle. Aktiivitestit voivat monitoroida verkkoa, vaikka siellä ei ole käyttäjiä. Tämä tekee mahdolliseksi ennakoida suorituskykyongelmia ja suorittaa korjaavia toimenpiteitä ennen kuin palvelunlaatu kärsii. Aktiivitestit kertovat palveluiden laadun

ja saatavuuden verkossa ja auttavat järjestelmän ylläpitäjiä havaitsemaan miksi jotkut ohjelmat eivät toimi toivotulla tavalla tietyssä verkkosegmentissä. Ongelmien ilmetessä aktiivitestit voidaan suunnata ongelmalliseen verkko-osioon. [3, s. 1.]

7signal Sapphiren -järjestelmän avainhyödyt ovat käyttäjäemulointi, laaja kuuluvuus-alue, jatkuva monitorointi ja verkon tilan näkyvyys. Kilpailevat ratkaisut perustuvat usein tukiasemien valvontaan, jolloin ne eivät anna mitään indikaatiota käyttäjän koke-masta palvelunlaadusta. Tällaisissa rajoitetuissa ratkaisuissa palvelunlaatuparametrit on mitattu samalla tavalla kuin langallisissakin verkoissa. Sapphire tarjoaa kattavan kuvan radioyhteyden laadusta, missä viiveet, uudelleenlähetykset ja pakettien katoamiset otetaan huomioon muiden yleisten mittaustulosten lisäksi. [3, s. 1.]

3.2 Toiminta

7signal Sapphire-järjestelmän ohjelmistot on toteutettu Javalla laskematta mukaan selaimella toimivaa Loupea, joka on toteutettu Javascriptillä ja HTML:llä.

3.2.1 Sapphire Eye -valvontasilmä

Sapphire Eye eli valvontasilmä on monitorointiasema WLAN-ympäristöille. Valvontasilmä käyttää edistynyttä laajakaista-antenniteknologiaa, jolla saadaan laaja peittoalue. Tämä mahdollistaa useamman tukiaseman monitoroinnin, vaikka ne olisivat eri kanavilla. Silmä on IP55 -tai IP65-hyväksytty jolloin se voidaan sijoittaa ulos ja pölyisiin olosuhteisiin. Silmä toimii palvelimena Sapphire Carat -hallintatyökalulle. Caratin ja silmän välinen liikenne on salattu vahvasti 7signalin omalla hallinnointiprotokollalla [4, s. 3.]

Valvontasilmässä on kovat lähetystehot, joten säteily ylittää terveelliset raja-arvot. Laitetta ei saa mennä 20 cm:ä lähemmäs, jos laite on päällä. [4, s. 1]

Silmän tekniset tiedot:

- mekaaniset osat valettu polykarbonaattimuovista
- Linux-tietokone, 1GB Flash-muisti
- WLAN-radiomoduuli, 802.11 a/b/g/n tuki (2,4 GHz, 4.9 GHz-5.8 GHz)
- laajennuskorteille paikkoja silmän sisällä: 1 Mini-PCI ja 1 PCI-E
- Micro SD -korttipaikka silmän sisällä
- taajuusanalysointikomponentti
- 6-sektoroitua tehokasta antennia, jotka kattavat 360-astetta vaakatasossa, 1-sektoroitu tehokas antenni pystysuunnassa
- radiotaajuus-levy antennin säteen kohdistusmahdollisuudella ja vähäkohinaisilla vahvistimilla vastaanottoketjussa
- akku
- lämmityselementti
- elektroninen kompassi
- GPS-vastaanotin
- Reset-nappula
- Virtaledi. [3, s. 3.]

3.2.2 Sapphire Carat -hallintatyökalu

Carat on hallintatyökalu, jolla voidaan hallita silmää. Sillä voidaan suorittaa ja konfiguroida interaktiivisia ja reaaliaikaisia mittauksia ja myös generoida raportteja tuloksista. Raportit havainnollistavat hyvin kaavioiden ja taulukkojen avulla tuloksia. Carat tallentaa käytetyt profiilit ja verkko-oikeuksien tiedot monitoroitavan verkon automaattisessa testauksessa. Caratia voidaan käyttää interaktiivisesti useilla alueilla verkossa tai se voidaan jättää taustalle suorittamaan testejä. [4, s. 5.]

3.2.3 Sapphire Sonar -testipalvelin

Sonar on testipalvelin, jonka tarkoitus on emuloida yrityksen tuotantopalvelinta. Sapphire Eye yhdistää Sonar-palvelimeen mitatakseen verkon palvelunlaatua (QoS). Mittaukset tehdään molempiin suuntiin eli käytössä ns. fullduplex-yhteys. Uplink-liikenne tarkoittaa liikennettä esimerkiksi silmältä verkkoon Sonar-palvelimelle. Downlink-iikenne tarkoittaa liikennettä verkosta päätelaitteelle. [4, s. 6.]

Sonar-palvelin voi palvella useita Sapphire-valvontasilmiä, joihin on IP-tason yhteys. Yhtä Sonar-palvelinta voidaan tällöin käyttää testipisteenä monelle tietoverkolle. Sonar-palvelin voi sijaita fyysisesti missä vain Internetissä, jolloin se voidaan sijoittaa keskitettyyn datakeskukseen. [4, s. 6.]

3.2.4 Sapphire Loupe -raportointityökalu

Loupe on selaimella toimiva raportointityökalu tulosten havainnointiin ja tallennukseen langattomalle laadunhallintaratkaisulle. Carat kerää datan tietokantaan erilaisista testeistä Loupen käyttöön. Loupella voidaan analysoida saatuja tuloksia ja tehdä vertailuja laitteiden välillä. Loupesta voidaan valita ”Topology”-kohdasta esimerkiksi tukiasemat, joiden tuloksia näytetään. Loupella ei voi kontrolloida testejä ja mittauksia itsessään, vaan tämä tapahtuu Caratilla. [4, s. 7.]

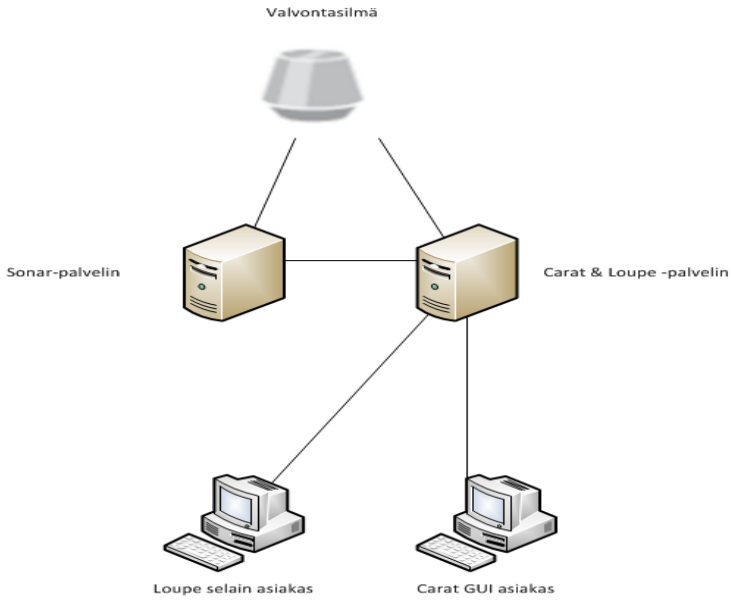
Loupen avulla saadaan tieto verkon tilanteessa KPI-testien kautta silmäyksellä tai yksityiskohtaisesti tietyllä aikavälillä. Loupe näyttää tulokset selainpohjaisesti eli tunnistautuneet käyttäjät voivat käyttää sitä eri selaimilla. Testien tulokset voidaan tallentaa myös tavallisena tekstinä CSV-tiedostoihin tai PDF-tiedostoihin säilyttäen tekstin formatointi. [4, s. 7.]

4 Metropolian 7signal Sapphire -järjestelmä

4.1 Kuvaus järjestelmästä

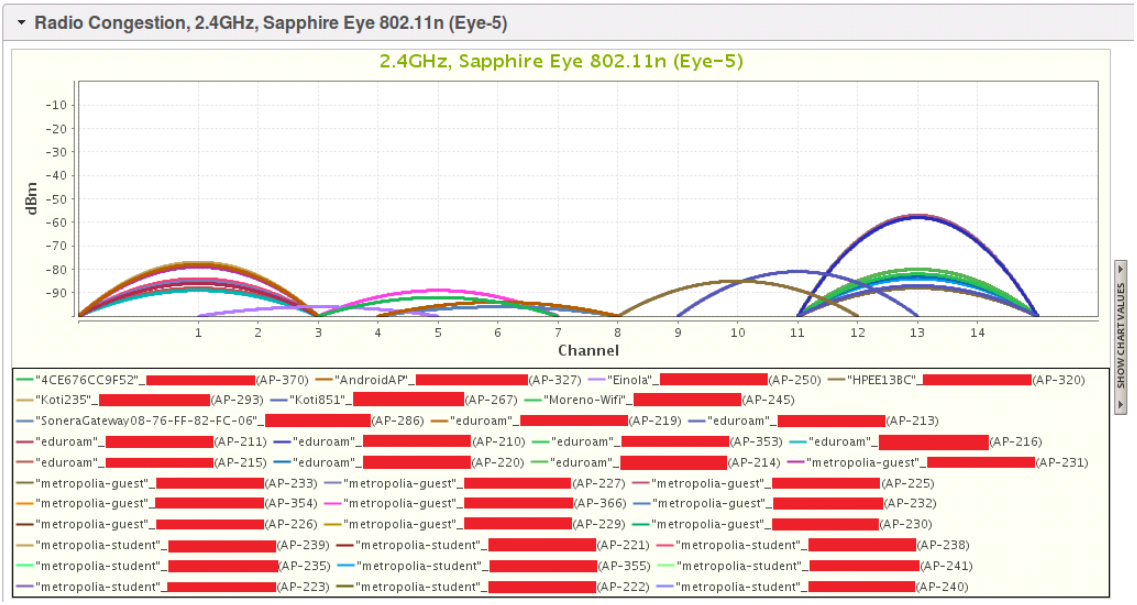
Metropolialla on useita langattomia tukiasemia ja langattomia verkkoja. Niiden monitorointi, laadunhallinta ja tietoturva asettavat tietynlaisia haasteita. Tähän ratkaisuksi on hankittu 7signal-laadunhallintajärjestelmä, jolla ylläpidetään Metropolian Bulevardin toimipisteen langattomien verkkojen laatua ja tietoturvaa.

Bulevardin toimipisteen Sapphire-järjestelmään kuuluvat Sonar-testipalvelin, Carat--hallintatyökalu, Loupe-raportointityökalu ja 802.11a/b/g/n-standardeja tukeva Eye-valvontasilmä.



Kuva 2: 7signal-järjestelmän looginen kartta

Metropolian Bulevardin toimipisteessä valvontasilmä sijaitsee luokassa laitekaapin päällä. Sonar, Carat ja Loupe on asennettu omille virtuaalisille CentOS-palvelimilleen. Caratin graafinen käyttöliittymä on asennettu virtuaaliselle Ubuntu-palvelimelle. Caratin graafisen käyttöliittymän Windows-versiot on myös asennettu parille tietokoneelle kahteen eri luokkaan.



Kuva 3: Langattomat verkot ja kanavat Loupessa

Kuvassa 2 näkyy silmän havaitsemat langattomat verkot. 2,4 GHz:n alueella on paljon langattomia verkkoja. Metropolian langattomia verkkoja ovat eduroam, metropolia-guest ja metropolia-student. Loupessa oli myös toinen kaavio, 5 GHz:n alueesta, joka jäi tyhjäksi, koska lähellä ei ole 5 GHz:n alueen langattomia verkkoja.

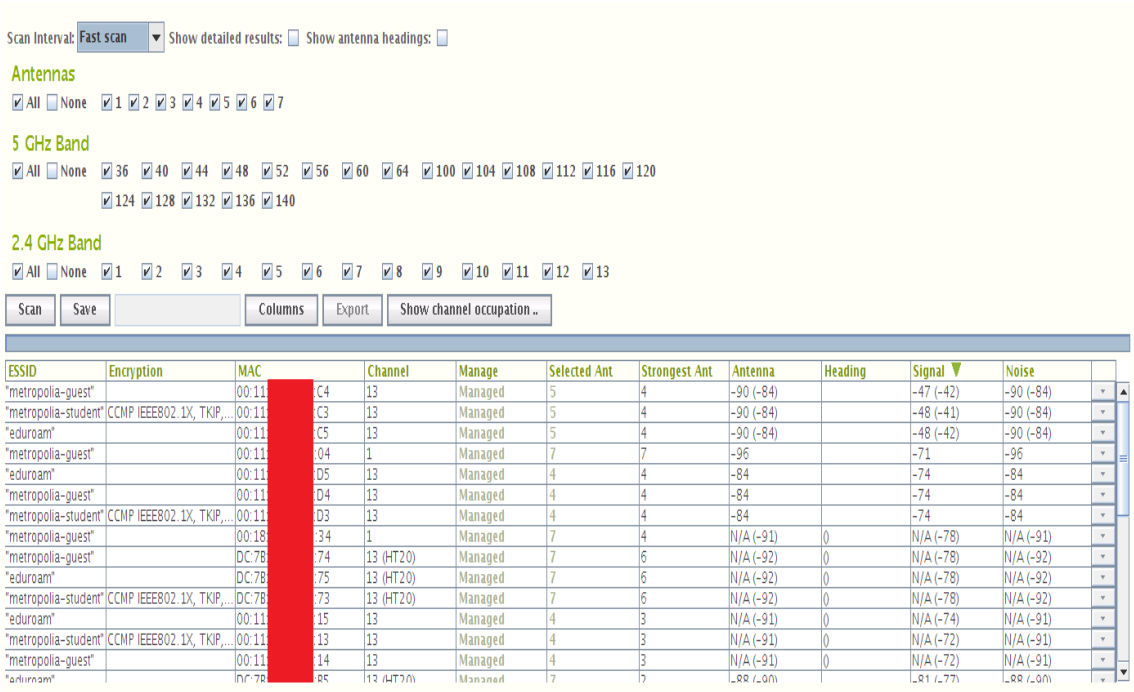
Kuva 4: Valvontasilmä laitekaapin päällä

Kuva 5: Käytössä oleva Ciscon 1121G-tukiasema

Metropolialla on käytössä muun muassa Ciscon 1121G-tukiasemia. Nämä tukiasemat ovat 802.11g-standardia eli tukevat vain 2,4 GHz:n taajuutta ja maksimissaan 54 Mbit/s:n nopeusluokkaa.

4.2 Manuaalisia testejä radiotaajuusympäristössä

Silmällä voi suorittaa 5 erilaista testiä manuaalisesti, jotka kertovat radiotaajuusympäristöstä. Manuaaliset testit voidaan suorittaa samanaikaisesti automaattisten testien kanssa. Sapphire-järjestelmä suorittaa kesken olevan automaattisen testin ensiksi ja vasta sen jälkeen käyttäjän määrittelemän manuaalisen testin. Automaattista testiä jatketaan heti, kun manuaalinen testi on saatu suoritettua. Manuaalisia testejä ei tallenneta tietokantaan, vaan ne näytetään vain Carat-järjestelmässä.

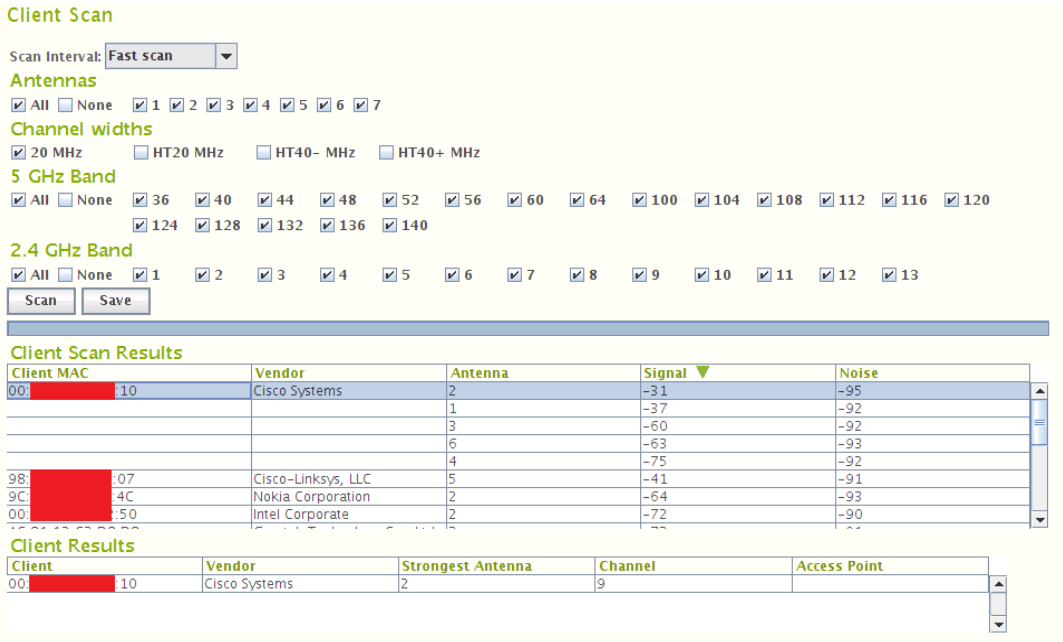


Kuva 6: Langattomien verkkojen skannaus

Ensimmäinen testi on Network Scan eli verkon skannaus, joka kertoo silmän lähellä olevista langattomista verkoista. Testissä valitsin pikaskannauksen, kaikki antennit ja kaikki kanavat 2,4 GHz:n ja 5 GHz:n alueelta.

Tuloksessa näkyy langattoman verkon nimi eli SSID, käytettävissä olevat salausvaihtoehdot, verkon tukiaseman MAC-osoite, verkon kanava ja signaalin vahvuus ja kohina.

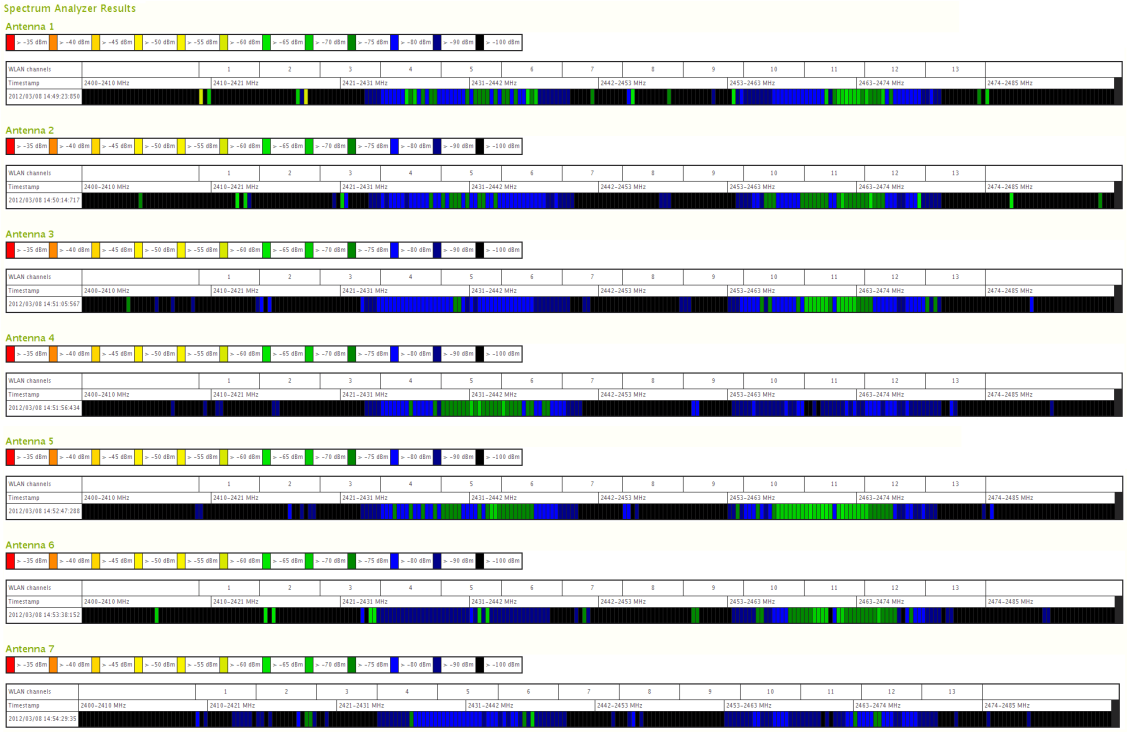
Skannauksella löytyi 14 metropolia-guest SSID:tä, 12 metropolia-student SSID:tä ja 11 eduroam SSID:tä 2,4 GHz:n alueelta. Fyysisiä tukiasemia ei ole kuitenkaan yhteensä 37, kuten SSID:tä vaan 14, koska yhdessä tukiasemassa on noin 3 eri SSID:tä. 5 GHz:n alueelta ei löytynyt yhtään langatonta verkkoa.



Kuva 7: Asiakaslaitteiden skannaus

Toisena testinä silmässä on Client Scan eli asiakaslaitteiden skannaus. Tämä testi näyttää silmää lähellä olevat päätelaitteet, esim. kannettavat tietokoneet ja älypuhelimet.

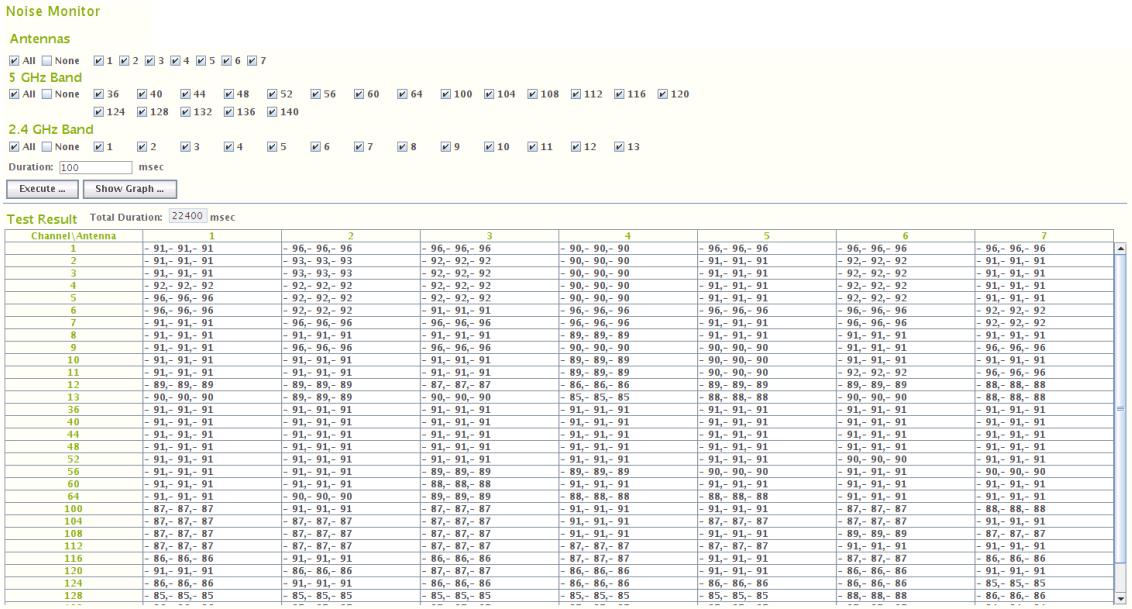
Tässä kuvassa on esitetty silmää lähellä olevat clientit eli asiakaslaitteet. Päätelaitteita löytyi skannaushetkellä 11 kpl. Lähimpänä on Ciscon valmistama WLAN-adapteri, jossa on myös pienin kohina.



Kuva 8: Spektrianalyysitesti

Kolmas testi silmässä on Spectrum Analysis eli spektrianalyysi. Tämä testi näyttää antennikohtaisesti taajuusalueiden käytön. Kuvassa näkyy WLAN-verkon kanavat ja signaalinvahvuus kyseisellä kanavalla. Signaali on vahvimmillaan kanavilla 5 ja 11. Testissä näkyy tulokset vain 2,4 GHz:n alueelta, jolloin 5 GHz:n alueella ei ole radioliikennettä.

Neljäs testi silmässä on Noise Monitor eli kohinan mittaus WLAN-verkossa. Radiotaajuushäiriöt voivat johtua monesta asiasta. Tärkeimpiä on toinen tukiasema samalla kanavalla ja muut 2,4 GHz:n alueella toimivat laitteet, kuten langattomat itkuhälyttimet, autojen hälytyslaitteet ja mikroaaltouuni. Mikroaaltouuni voi häiritä huomattavasti WLAN-signaalia. [5.]



Noise Monitor

Antennas

All None 1 2 3 4 5 6 7

5 GHz Band

All None 36 40 44 48 52 56 60 64 100 104 108 112 116 120
124 128 132 136 140

2.4 GHz Band

All None 1 2 3 4 5 6 7 8 9 10 11 12 13

Duration: 100 msec

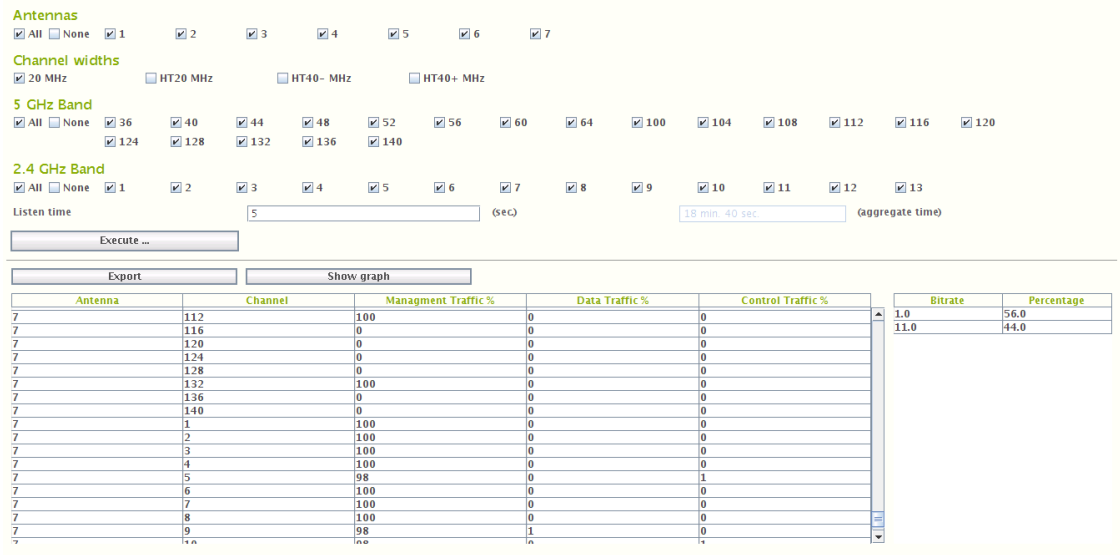
Execute ... Show Graph ...

Test Result Total Duration: 22400 msec

Channel\Antenna	1	2	3	4	5	6	7
1	-91,-91,-91	-96,-96,-96	-96,-96,-96	-90,-90,-90	-96,-96,-96	-96,-96,-96	-96,-96,-96
2	-91,-91,-91	-93,-93,-93	-92,-92,-92	-90,-90,-90	-91,-91,-91	-92,-92,-92	-91,-91,-91
3	-91,-91,-91	-93,-93,-93	-92,-92,-92	-90,-90,-90	-91,-91,-91	-92,-92,-92	-91,-91,-91
4	-92,-92,-92	-92,-92,-92	-92,-92,-92	-90,-90,-90	-91,-91,-91	-92,-92,-92	-91,-91,-91
5	-96,-96,-96	-92,-92,-92	-92,-92,-92	-90,-90,-90	-91,-91,-91	-92,-92,-92	-91,-91,-91
6	-96,-96,-96	-92,-92,-92	-91,-91,-91	-96,-96,-96	-96,-96,-96	-96,-96,-96	-92,-92,-92
7	-91,-91,-91	-96,-96,-96	-96,-96,-96	-96,-96,-96	-91,-91,-91	-96,-96,-96	-92,-92,-92
8	-91,-91,-91	-91,-91,-91	-91,-91,-91	-89,-89,-89	-91,-91,-91	-91,-91,-91	-91,-91,-91
9	-91,-91,-91	-96,-96,-96	-96,-96,-96	-90,-90,-90	-90,-90,-90	-91,-91,-91	-96,-96,-96
10	-91,-91,-91	-91,-91,-91	-91,-91,-91	-89,-89,-89	-90,-90,-90	-91,-91,-91	-91,-91,-91
11	-91,-91,-91	-91,-91,-91	-91,-91,-91	-89,-89,-89	-90,-90,-90	-92,-92,-92	-96,-96,-96
12	-89,-89,-89	-89,-89,-89	-87,-87,-87	-86,-86,-86	-89,-89,-89	-89,-89,-89	-88,-88,-88
13	-90,-90,-90	-89,-89,-89	-90,-90,-90	-85,-85,-85	-88,-88,-88	-90,-90,-90	-88,-88,-88
36	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91
40	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91
44	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91
48	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91
52	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91	-90,-90,-90	-91,-91,-91
56	-91,-91,-91	-91,-91,-91	-89,-89,-89	-89,-89,-89	-90,-90,-90	-91,-91,-91	-90,-90,-90
60	-91,-91,-91	-91,-91,-91	-88,-88,-88	-91,-91,-91	-91,-91,-91	-91,-91,-91	-91,-91,-91
64	-91,-91,-91	-90,-90,-90	-89,-89,-89	-88,-88,-88	-88,-88,-88	-91,-91,-91	-91,-91,-91
100	-87,-87,-87	-91,-91,-91	-87,-87,-87	-91,-91,-91	-91,-91,-91	-87,-87,-87	-88,-88,-88
104	-87,-87,-87	-87,-87,-87	-87,-87,-87	-91,-91,-91	-87,-87,-87	-87,-87,-87	-91,-91,-91
108	-87,-87,-87	-87,-87,-87	-87,-87,-87	-91,-91,-91	-91,-91,-91	-89,-89,-89	-87,-87,-87
112	-87,-87,-87	-87,-87,-87	-87,-87,-87	-87,-87,-87	-87,-87,-87	-91,-91,-91	-91,-91,-91
116	-86,-86,-86	-91,-91,-91	-86,-86,-86	-87,-87,-87	-91,-91,-91	-87,-87,-87	-86,-86,-86
120	-91,-91,-91	-86,-86,-86	-87,-87,-87	-86,-86,-86	-91,-91,-91	-86,-86,-86	-91,-91,-91
124	-86,-86,-86	-91,-91,-91	-86,-86,-86	-86,-86,-86	-86,-86,-86	-86,-86,-86	-85,-85,-85
128	-85,-85,-85	-85,-85,-85	-85,-85,-85	-85,-85,-85	-85,-85,-85	-88,-88,-88	-86,-86,-86

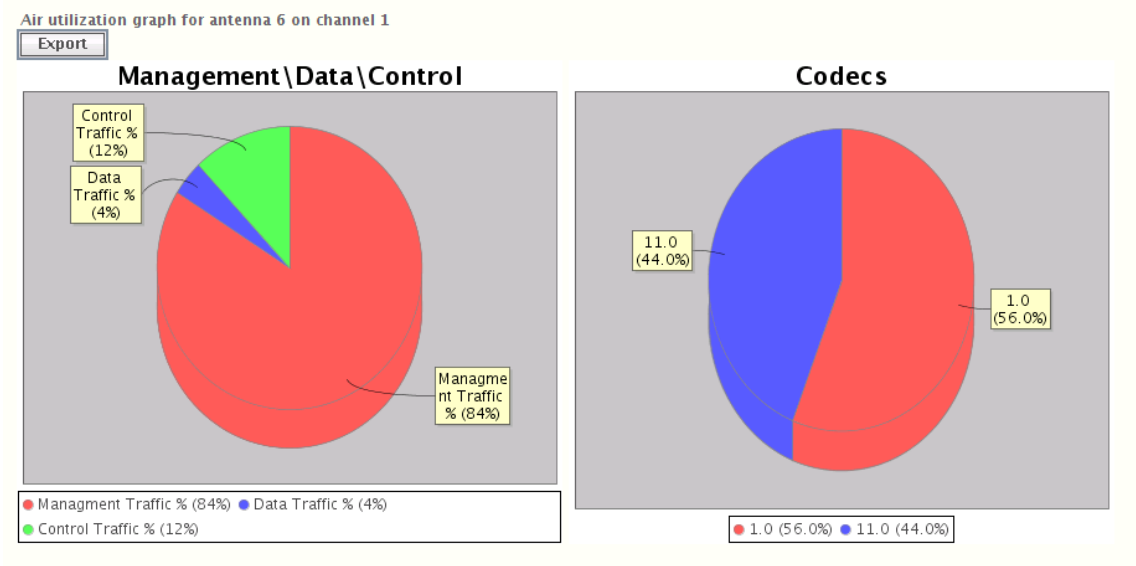
Kuva 9: Kohinan monitorointi -testi

Tämä testi näyttää antennikohtaisesti jokaisen WLAN-kanavan kohinat. Signaali on 2,4 GHz:n alueella -91 ja -86 välissä. 5 GHz:n alueella signaali on parempi eli häiriöttömämpi. Signaali on 5 GHz:lla -91:n ja -85:n välissä. Signaali on tässä tapauksessa sitä parempi mitä lähempänä se on nollaa. 5 GHz:n alueella ei ole niin paljoa kohinaa kuin 2,4 GHz:n alueella.



Kuva 10: Air Utilization -testi

Viimeinen radiotaajuustesti on Air Utilization -testi. Tämä testi auttaa havaitsemaan kanavien raskaita käyttäjiä ja konfigurointivirheitä.



Kuva 11: Liikennetyypin jakautuminen kanavalla 1 antennilla 6

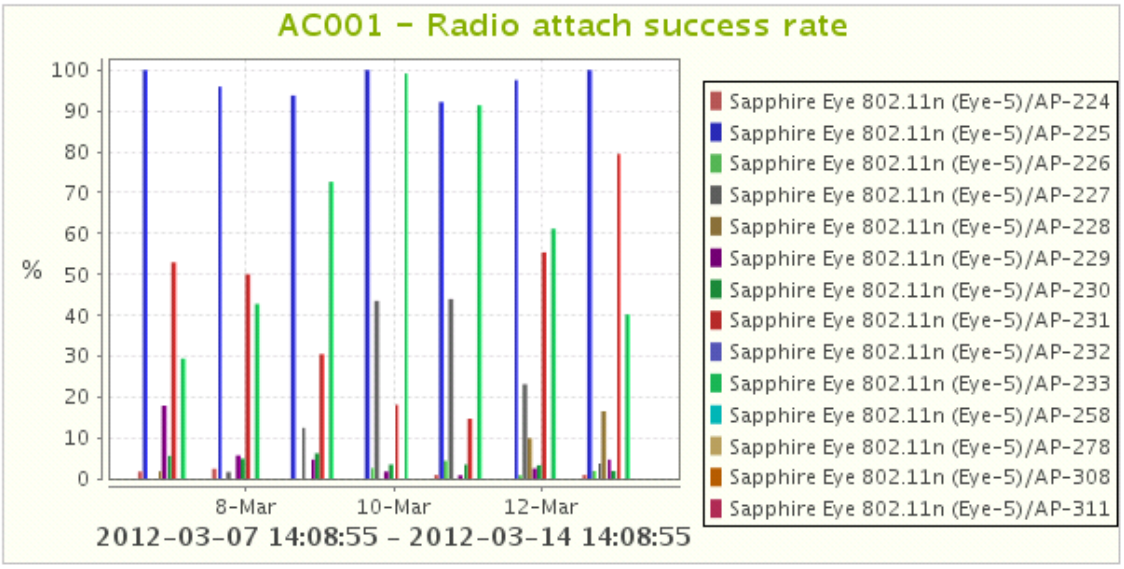
Kuvasta näkyy hallinnointiliikenteen, dataliikenteen ja kontrollointiliikenteen jakautuminen kanavakohtaisesti. Kuvassa hallinnointiliikennettä on 64 %, kontrollointiliikennettä 12 % ja dataliikennettä 4 %. Koodekkia 1.0 käytetään enemmän, 56 % ja koodekkia 11.0 44 %.

4.3 Guest-verkko

Guest-verkko on yksi Metropolian langattomista verkoista. Verkko on avoin, joten siinä ei ole salausta. Guest-verkkoon käyvät samat tunnukset kuin Student-verkkoon. Autentikointi verkkoon tapahtuu selainpohjaisen kirjautumisen kautta. Ilman autentikointia vain DNS-nimen selvitys IP-osoitteeksi onnistuu.

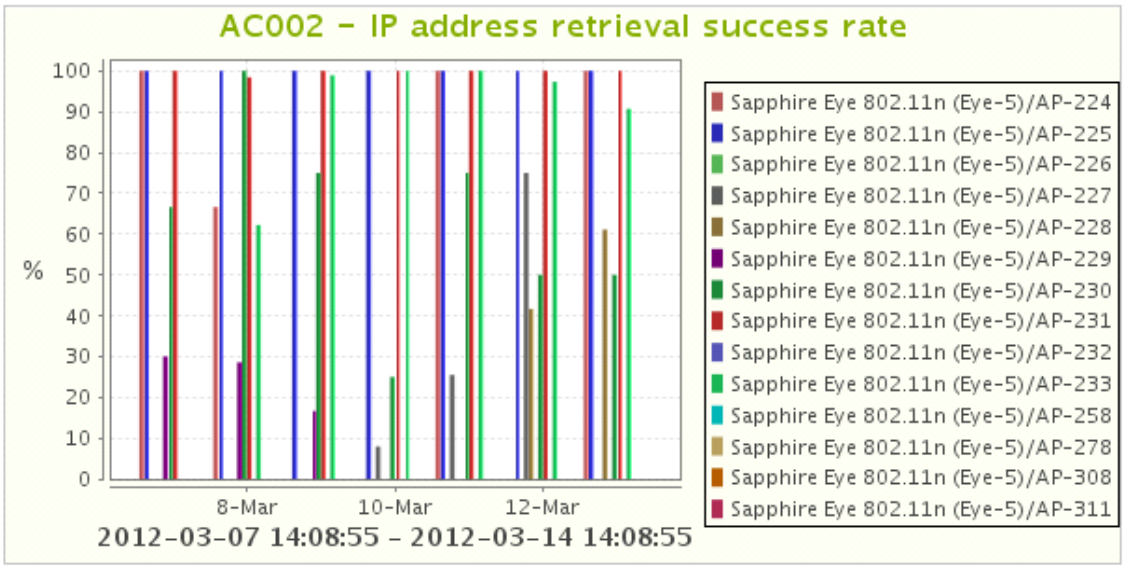
4.3.1 Tulokset

Automaattitestejä olisi ollut valittavissa paljon. Valitsin suositellut testit, koska kaikkien testien valitseminen olisi kuormittanut turhaan järjestelmää ja voinut aiheuttaa häiriöitä ja epästabiiliutta. Testit ovat nimeltään KPI-testejä. KPI eli Key Performance Indicator on suorituskykyilmaisin, jota käytetään havainnollistamaan suorituskykymittauksia. Tulokset ovat Loupesta eri välilehdiltä.



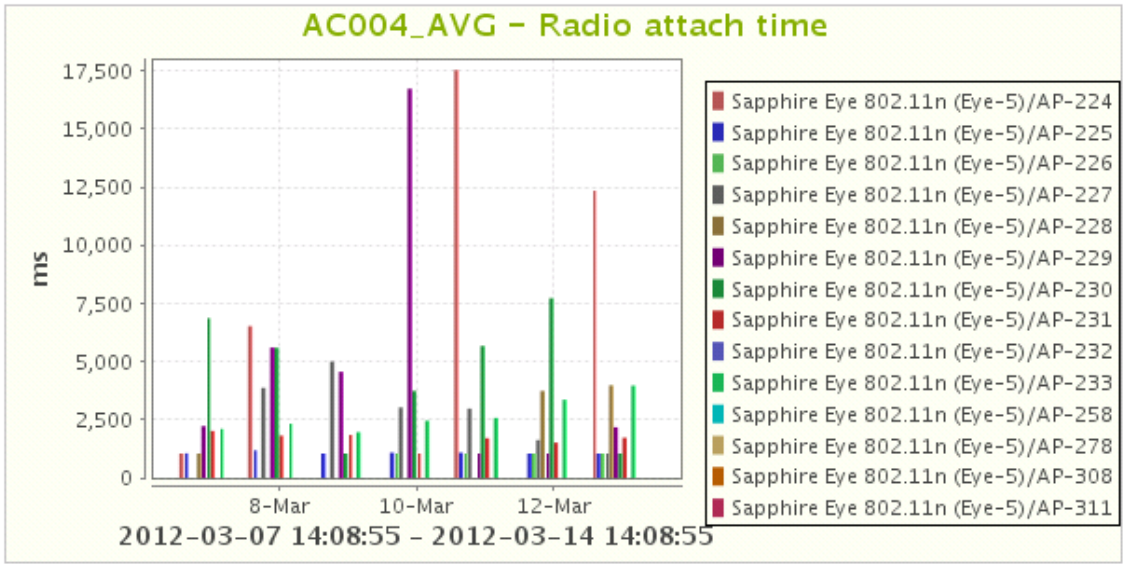
Kuva 12: Tukiasemaan yhdistämisen onnistuminen prosentuaalisesti

Testissä AC001 tukiasemalla 225 on paras onnistumisprosentti. Tämä tukiasema on myös lähimpänä valvontasilmää. Usealla tukiasemalla yhdistämisprosentti on melkein 0 %. Tämä johtuu mahdollisesti huonosta signaalista. Tukiasema 227 oli useamman päivän alhaalla.



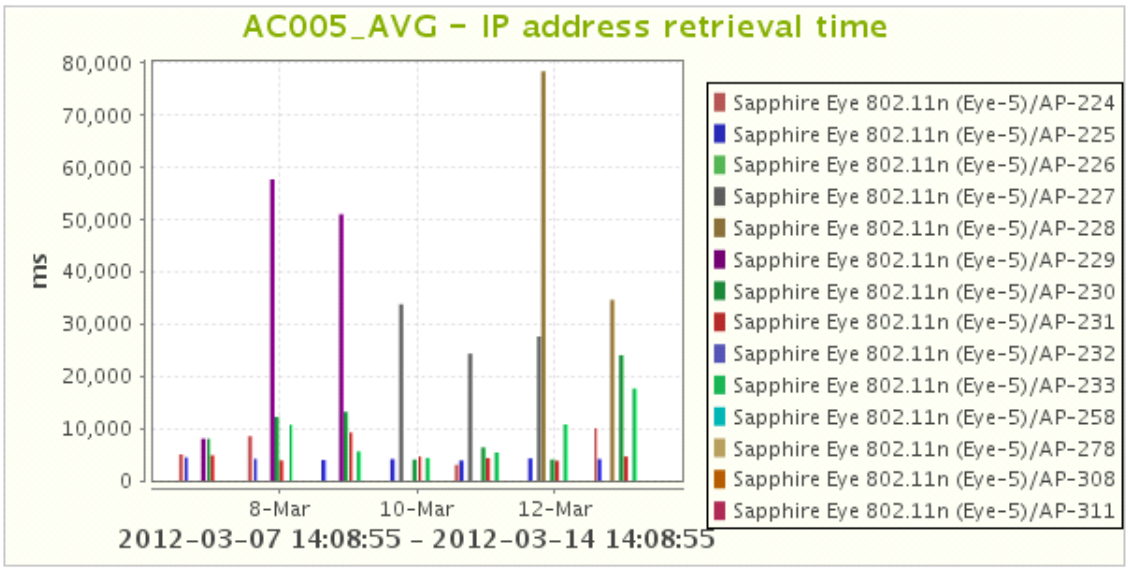
Kuva 13: IP-osoitteen haun onnistumisprosentti

Tämä AC002 -KPI mittaa DHCP-palvelimen onnistumisprosenttia. KPI lasketaan onnistuneiden IP-osoitteiden hakujen ja kaikkien hakukertojen suhteella.



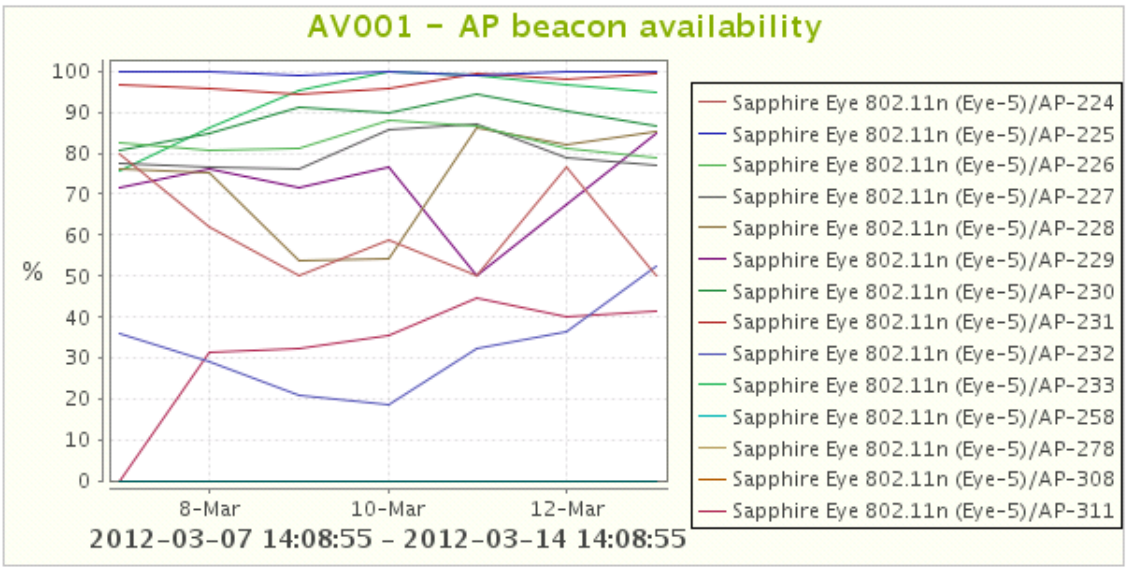
Kuva 14: Tukiasemaan yhdistämiseen kulunut aika

AC004 -KPI mittaa valvontasilmän ja tukiaseman yhdistämisaikaa millisekunteina, kunnes yhdistyminen on valmis.



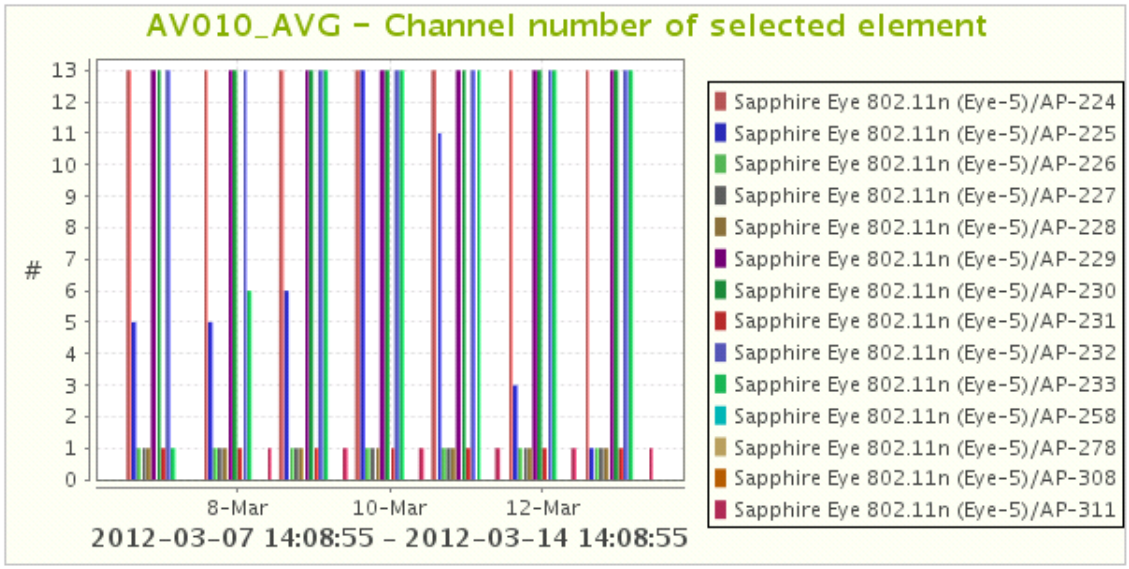
Kuva 15: IP-osoitteen hakuaika

AC005 -KPI mittaa aikaa millisekunteina, kuinka kauan valvontasilmällä kestää hakea IP-osoite tukiasemalta.



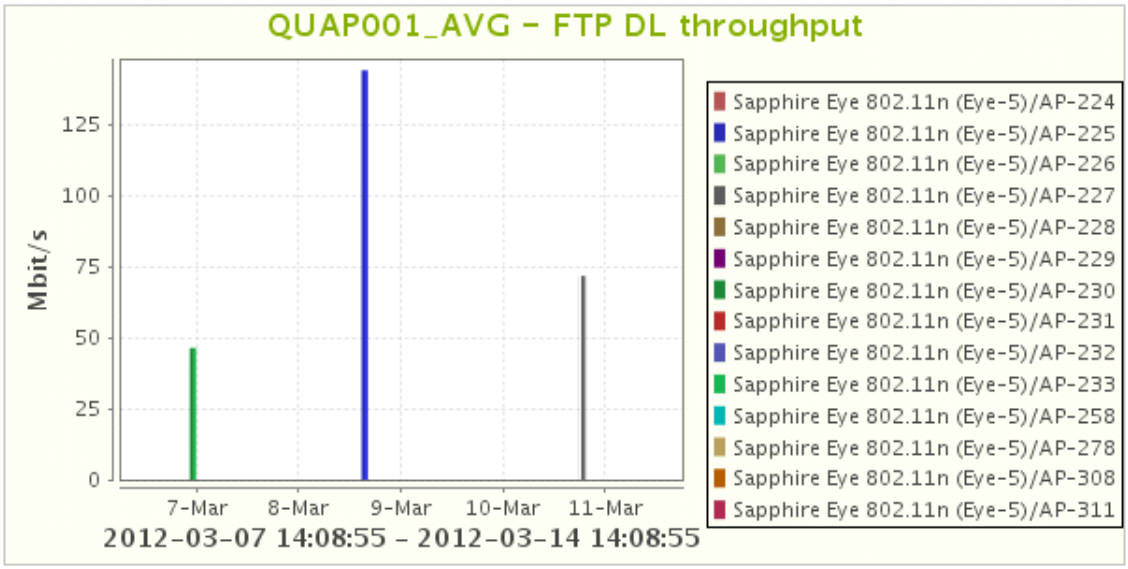
Kuva 16: Tukiaseman saatavuus

AV001 eli ”AP Beacon availability” -testi kertoo, miten tukiasemat ovat olleet aktiivisina ja käytettävissä kyseisellä aikavälillä. 11 tukiasemaa 14 tukiasemasta on ollut käytettävissä.



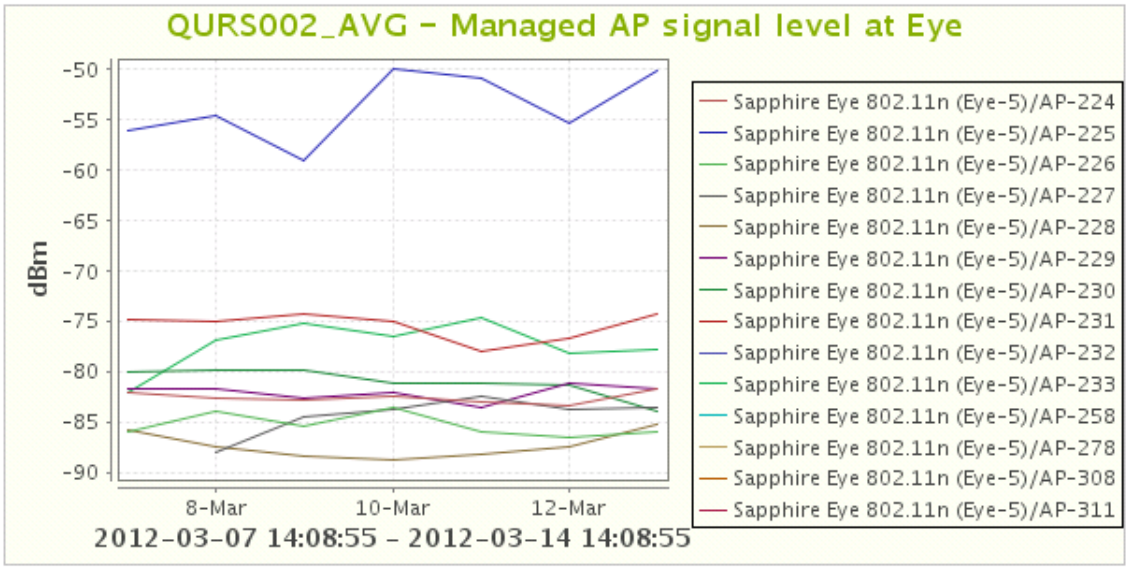
Kuva 17: Tukiaseman kanava

AV010 -KPI näyttää, millä kanavalla kyseinen tukiasema on ollut minäkin päivänä. Esimerkkinä on tukiasema 225, joka on ollut 7.3.2012 kanavalla 5 ja 10.3.2012 kanavalla 13. Tukiasemissa vaikuttaa siis olevan päällä automaattinen kanavan valinta, jolloin käytetään vähiten ruuhkaisinta kanavaa.



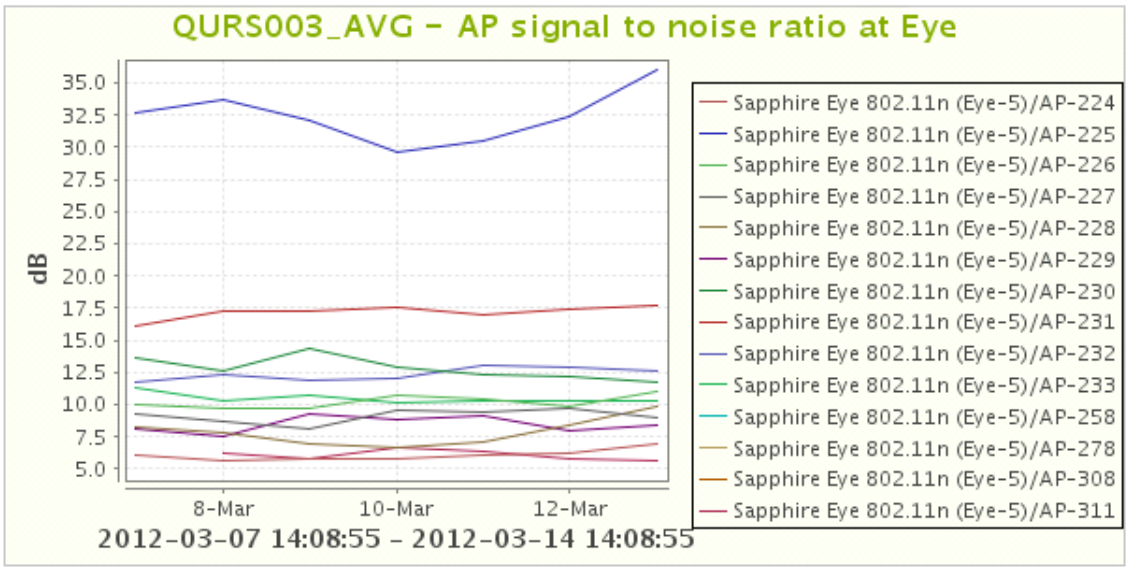
Kuva 18: FTP-latauksen läpisyöttö

QUAP001 mittaa latauksen läpisyöttötehoa FTP-latauksen aikana. Tukiasema 225 ylsi testissä 8.3.2012 reiluun 140 Mbit/s:n nopeuteen.



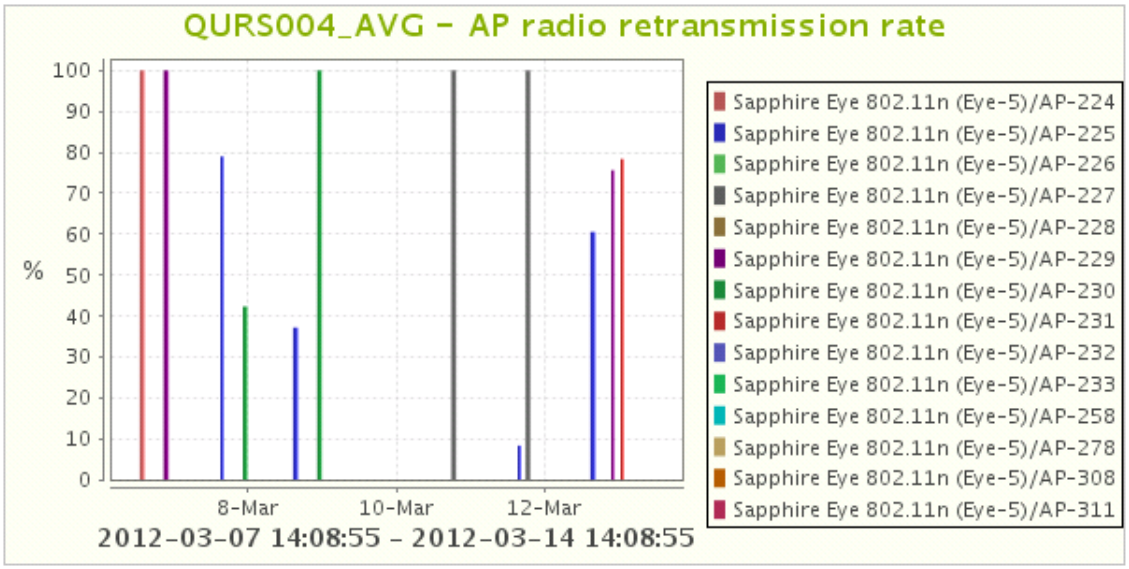
Kuva 19: Hallinnoidun tukiaseman signaalin taso valvontasilmällä

QURS002 mittaa tukiaseman lähettämän radioaallon tehon vahvuuden desibelimäärän suhteessa milliwattiin, valvontasilmästä mitattuna.



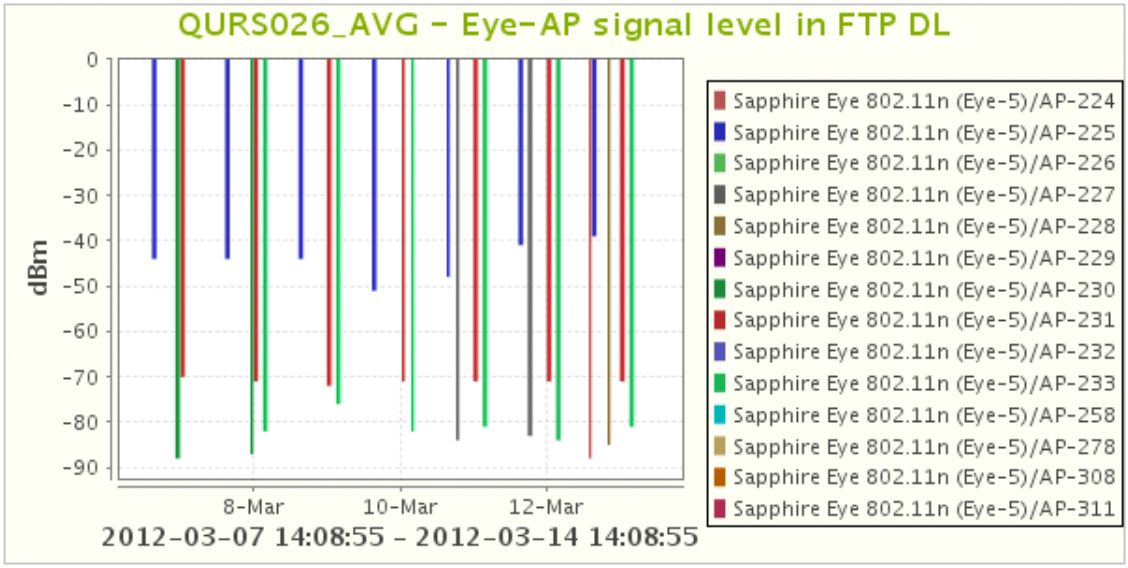
Kuva 20: Tukiaseman SNR-arvo valvontasilmästä mitattuna

GURS003 mittaa desibeleissä tukiaseman lähettämän radiosignaalin voimakkuutta suhteessa häiriöihin, joita valvontasilmä vastaanottaa. Tukiasema 225 suoriutui testistä parhaiten muiden tukiasemien jäädessä alle 20 desibelin.



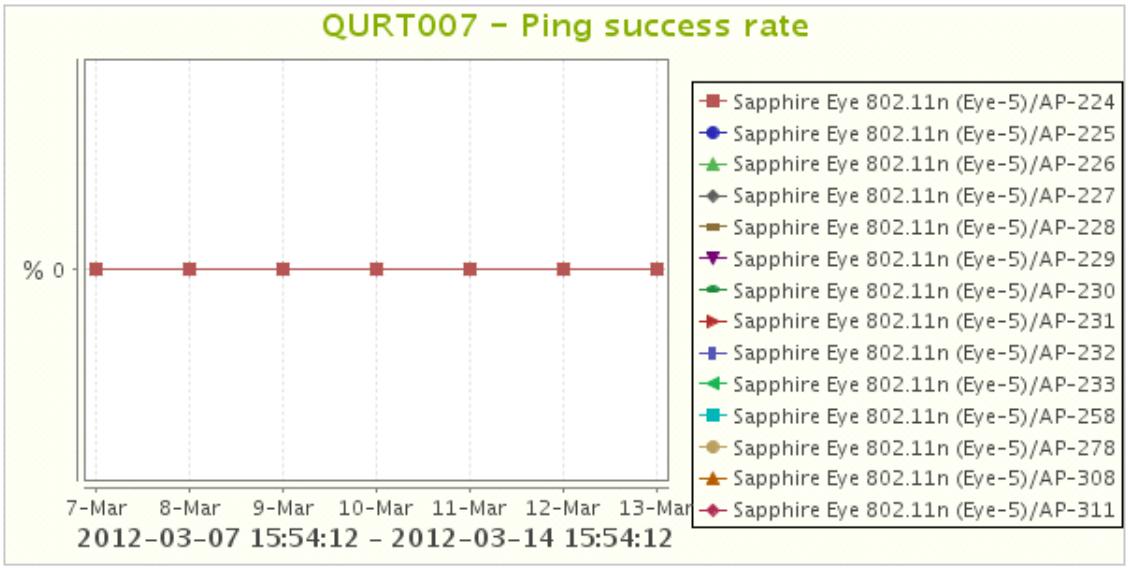
Kuva 21: Tukiaseman uudelleenlähettämissuhde

QURS004-kuva näyttää tukiaseman uudelleenlähettämissuhteen eli uudelleenlähetettyjen kehysten määrän jaettuna kaikilla tukiaseman lähettämillä kehyksillä. 10.3. on ollut häiriöitä, jolloin tuloksia ei ole saatu mistään tukiasemasta.



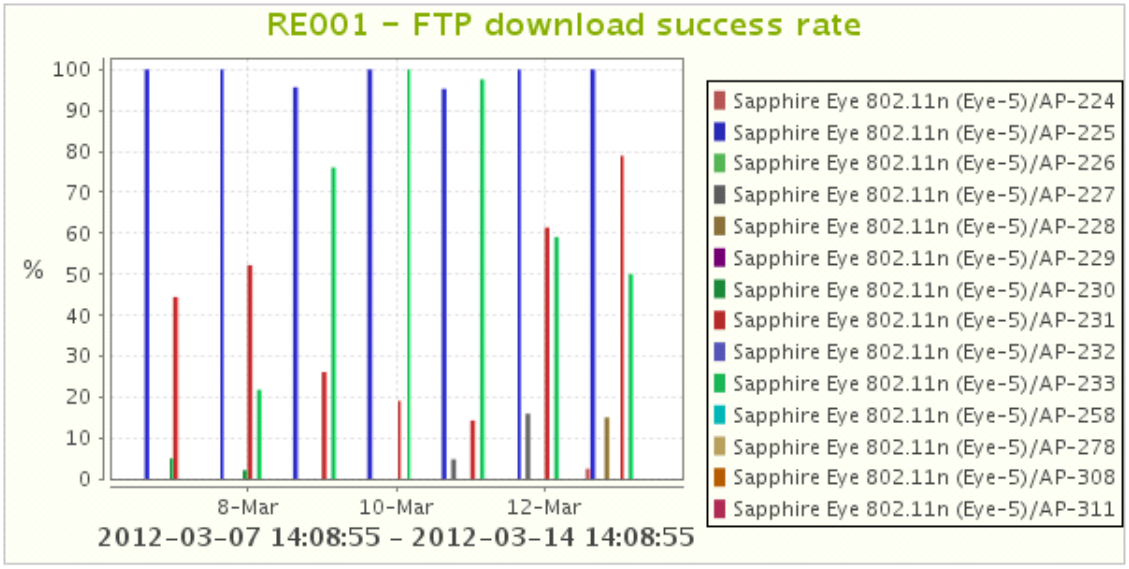
Kuva 22: Silmän ja tukiaseman signaalin voimakkuus FTP-latauksessa

QURS026 näyttää signaalin voimakkuuden tukiaseman ja valvontasilmän välillä FTP-latauksen aikana. Paras signaalinvahvuus on tukiasemalla 225. 7 tukiasemaa 14:sta näkyy testissä.



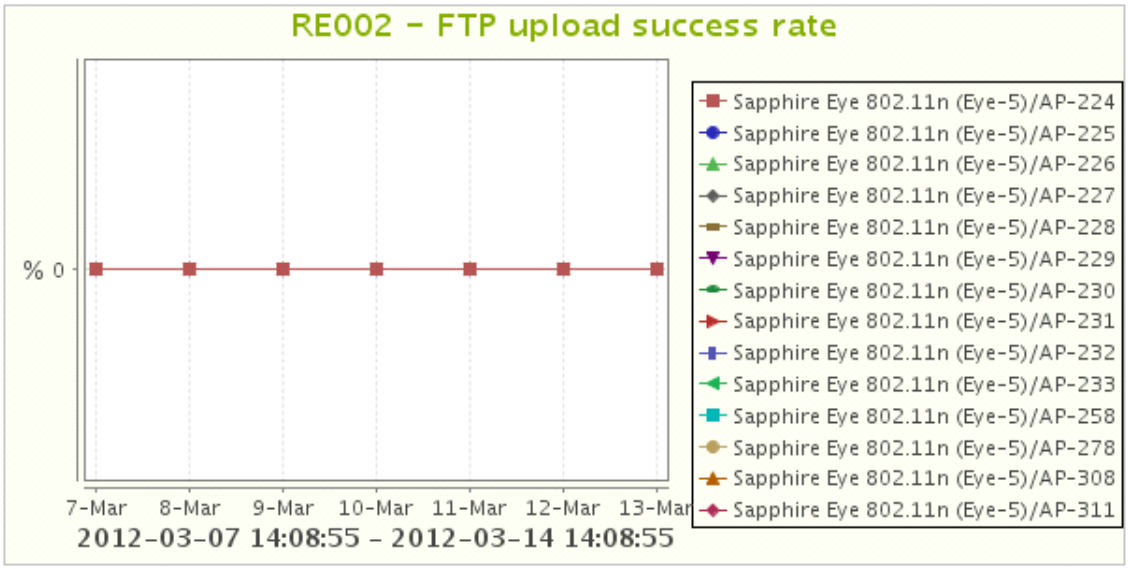
Kuva 23: Pingin onnistumis-suhde

QURT007-kuva näyttää onnistuneet ping-yritykset jaettuna kaikilla ping-yrityksillä eli pingin onnistumisprosentin on 0 %. Testistä päätellen ICMP-liikenne vaikuttaisi estetyltä.



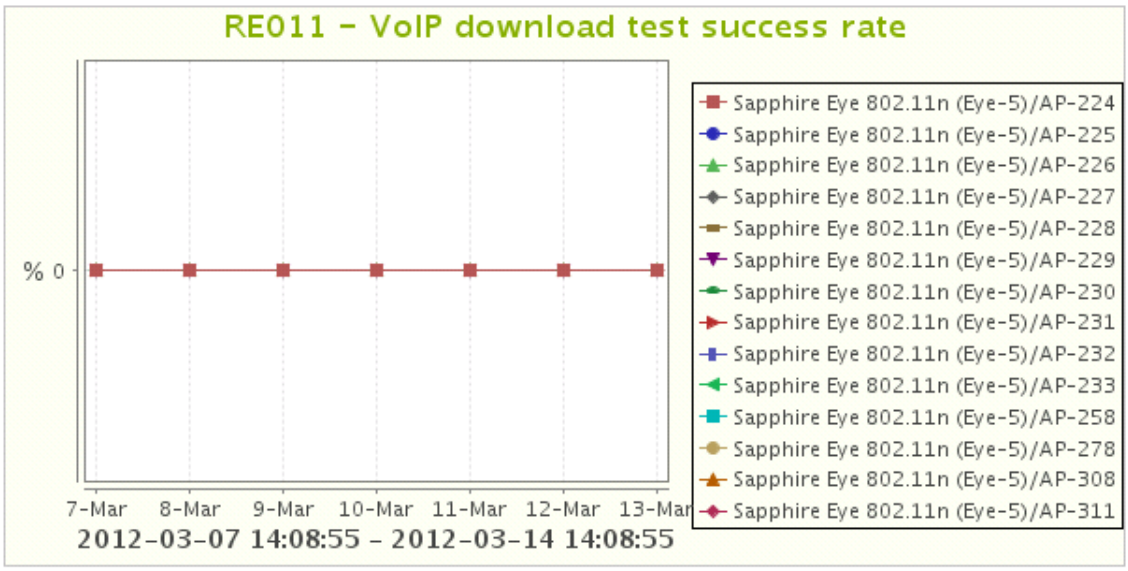
Kuva 24: FTP-latauksen onnistumisprosentti

FTP-lataus onnistui Sonar-palvelimelta parhaiten tukiasemilta 225 ja 226. Tukiasema 225 onnistui testissä melkein sataprosenttisesti joka kerralla.



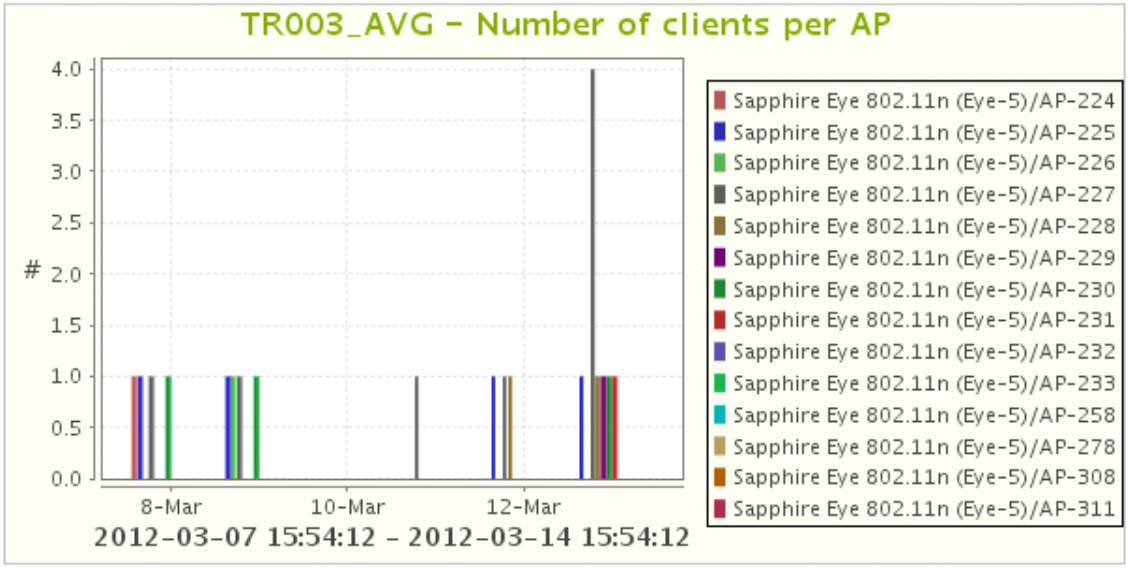
Kuva 25: FTP-lähetyksen onnistumisprosentti

RE002 KPI mittaa FTP-lähetyksen onnistumisprosentin. Tulos yllätti 0 prosentillaan. Tämä johtui luultavimmin estetyistä porteista.



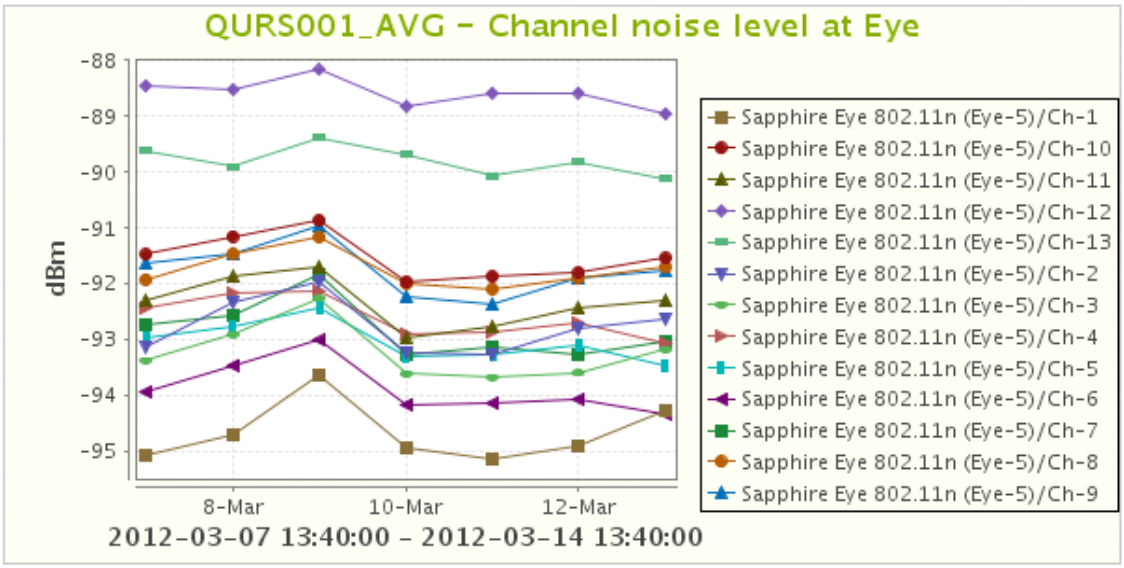
Kuva 26: VOIP-lataustestin onnistumisprosentti

Tämä RE011 KPI-testi ja myös RE012 KPI-testi epäonnistuivat estettyjen porttien vuoksi. VoIP-testi Sonar-palvelimelle olisi tarvinnut UDP-portin 9999 avoimeksi. [3, s. 5].



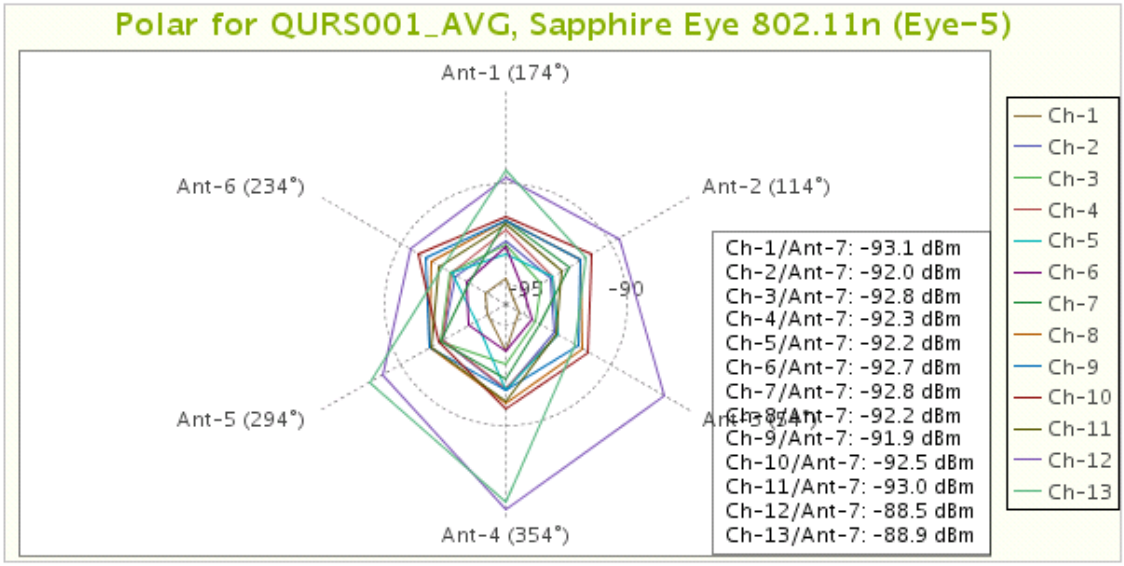
Kuva 27: Asiakaslaitteiden määrä per tukiasema

Tämä TR003 KPI-testi mittaa, kuinka monta asiakasta käyttää tiettyä tukiasemaa testin aikana. Tukiasemalla 227 näytti olevan 4 käyttäjää. Tukiasema oli luultavimmin luokan läheisyydessä, jolloin kävijäpiikki osui jonkun oppitunnin kohdalle.



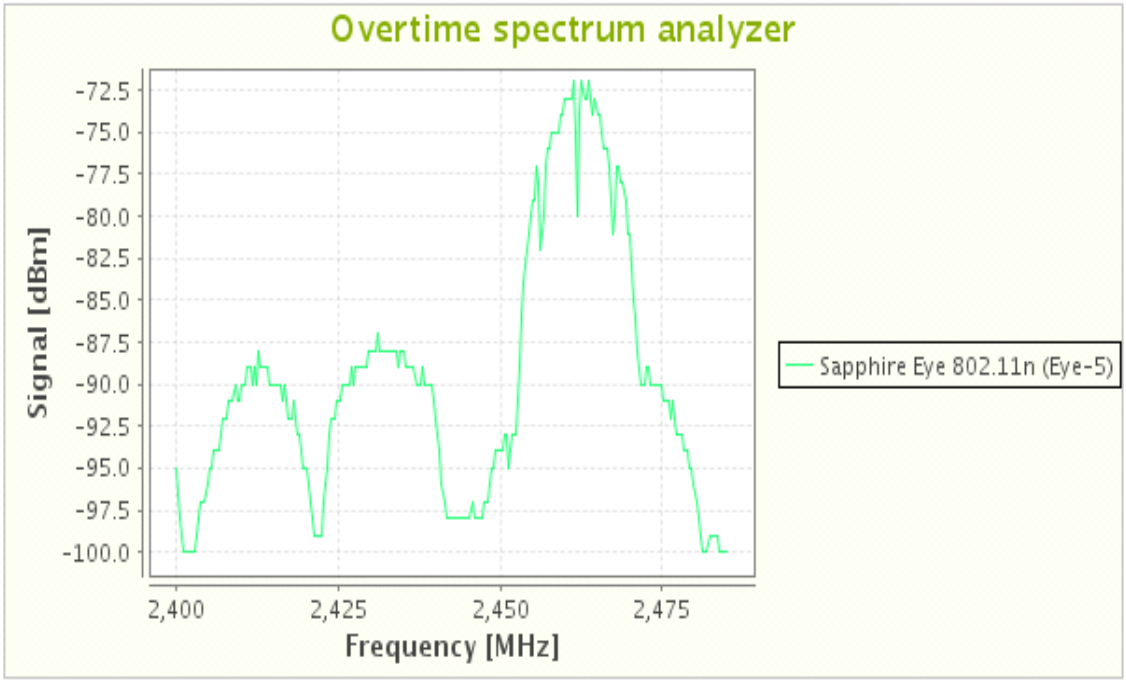
Kuva 28: Kanavien kohinat silmästä mitattuna

Kuvassa 25 näkyy WLAN-kanavien kohinan taso silmästä mitattuna. Kanavilla 12 ja 13 on pienin kohina.



Kuva 29: Kohinan jakautuminen silmän antenneille

Tässä havainnollistavassa kuvassa näkyy, miten kohina jakautuu silmän eri antenneille. Pienin kohina-alue on antennien 4 ja 5 välissä kanavalla 13 antennilla 7.



Kuva 30: Taajuusspektri

Tässä kuvassa näkyy taajuusspektrin jakautuminen. Vahvin signaali on kanavien 10 (2,457 GHz ja 13 (2,472 GHz) välissä.

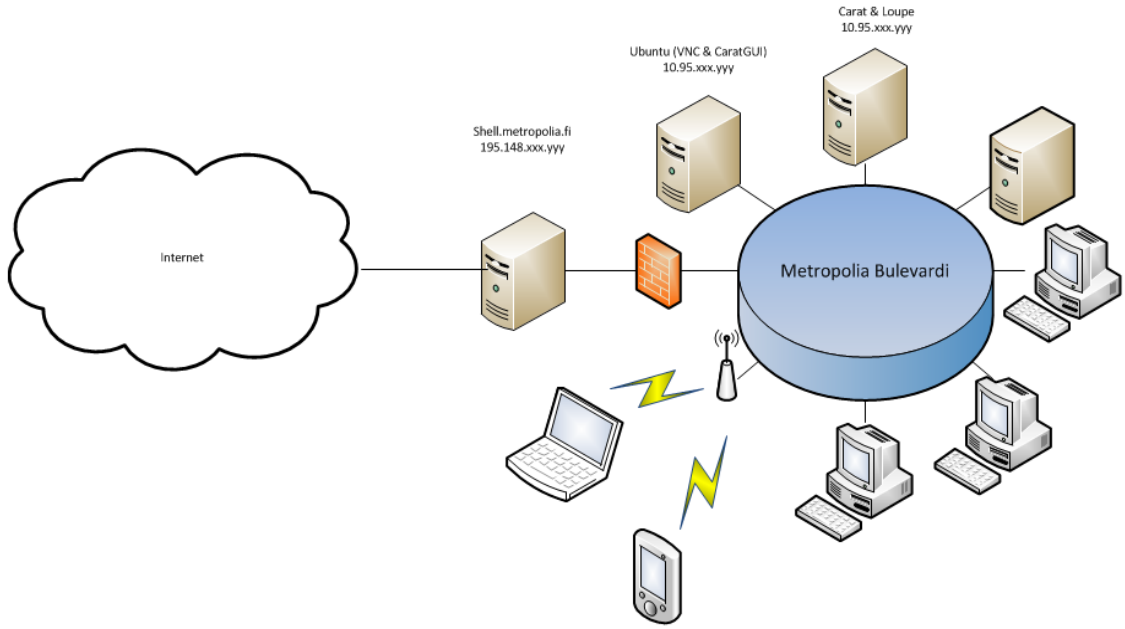
4.3.2 Yhteenveto

Tulokset kertovat valvontasilmän sijoituksesta ja hiukan tietoturvastakin. Silmä ei ole sijoitettu parhaimpaan paikkaan, jonka vuoksi testitulokset ovat puutteellisia. Vain muutamalta tukiasemalta saadaan kunnolla tuloksia, muilta se ei onnistunut häiriöiden ja huonon signaalin vuoksi. Valvontasilmä olisi hyvä sijoittaa uuteen parempaan paikkaan, jotta saataisiin paremmin tuloksia kaikista Metropolian tukiasemista [3, s. 9]. Loupe myös näytti tulokset välillä oudosti. Tulokset olivat esimerkiksi päällekkäin ja epäselviä. Käyttäen erilaisia kaaviovaihtoehtoja sain järkevämpiä tuloksia. Loupessa ja Caratissa pystyi myös selailemaan eri välilehtiä, vaikka kirjautumisistunto oli vanhentunut. Estetyt portit haittasivat myös testejä, jonka takia esimerkiksi VoIP-testit ja FTP-testi eivät onnistuneet.

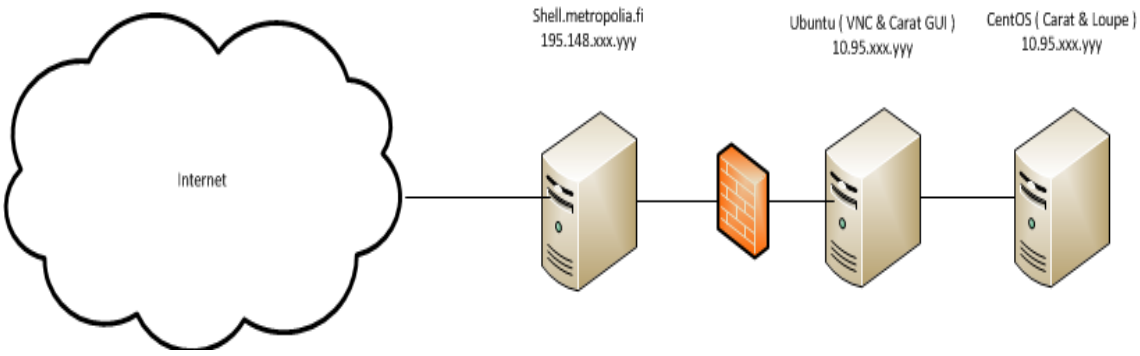
Metropolian Bulevardin toimipisteen alueella on paljon langattomia verkkoja ja 2,4 GHz:n alueella on ruuhkaista (kuva 2). 5 GHz:n alueella on vähemmän kohinaa kuin 2,4 GHz:n alueella (kuva 8), koska siellä ei ole muita langattomia verkkoja eikä laitteita luvun 3.2 neljännen kappaleen ja myös sivun 12 ensimmäisen kappaleen mukaan.

4.4 Etäyhteys

Sapphire-järjestelmään haluttiin etäyhteys koulun verkon ulkopuolelta. Järjestelmässä oli jo valmiina Ubuntu-virtuaalipalvelin, joka helpotti etäyhteyden luomista. Virtuaalipalvelimelle oli asennettu Sapphire Carat GUI -asiakasohjelma. Etäyhteys virtuaalipalvelimen VNC:hen onnistuu kätevästi SSH-tunnelilla koulun shell-palvelimen kautta. VNC:n muutin kuuntelemaan porttiin 3389, joka on RDP:n portti ja yksi harvoista sallituista porteista koulun verkossa. Etäyhteyden tarkoituksena oli pystyä käyttämään Loupea ja Carat GUI-asiakasohjelmaa etäyhteyden avulla.



Kuva 31: SSH-tunnelin fyysinen topologia



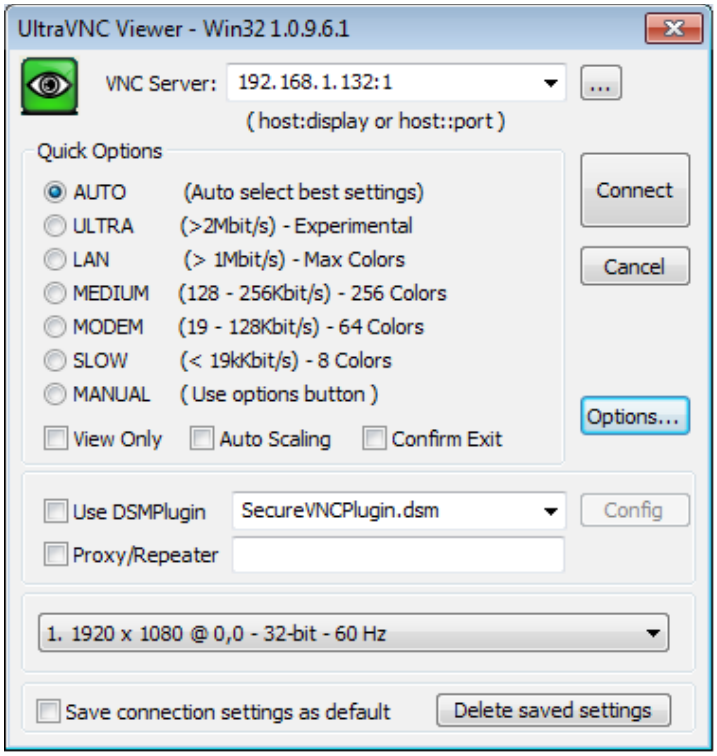
Kuva 32: SSH-tunnelin looginen topologia

4.4.1 Linux

```
ssh -f m0[redacted]@shell.metropolia.fi -L 192.168.1.132:5901:10.[redacted]:3389 -N
```

Kuva 33: SSH-tunnelin luonti Linuxilla

Kuvassa 33 muodostetaan SSH-tunneli koulun shell-palvelimelle omalla käyttäjätunnuksellani. Tunneli laitetaan kuuntelemaan Linux-palvelimen IP-osoitteelle 192.168.1.132 TCP-porttiin 5901. Shell-palvelimelta tunneli ottaa yhteyden koulun verkossa olevaan Ubuntu-palvelimen IP-osoitteeseen 10.95.xxx.yyy. Komennossa vivuilla -f ja -N jätetään tunneli taustalle pyörimään, jolloin ei käytetä SSH-yhteyttä muuhun. Ilman näitä vipuja muodostetaan SSH-tunneli ja voidaan käyttää SSH-yhteyttä normaalisti.

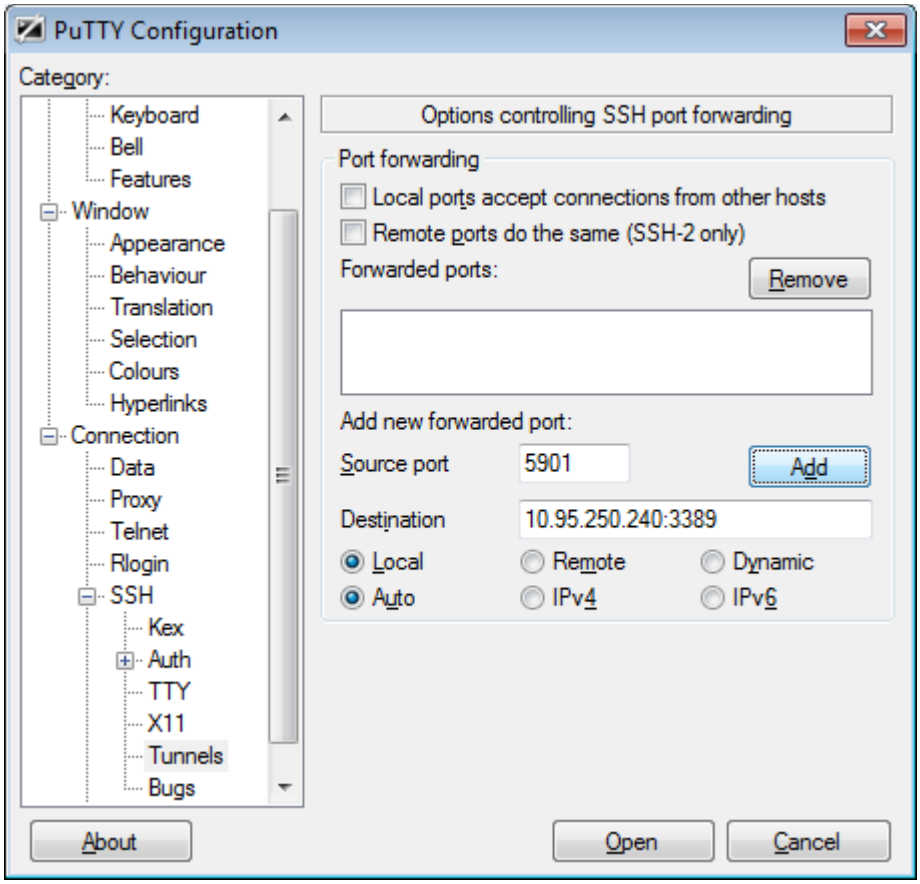


Kuva 34: VNC-yhteyden ottaminen tunnelin kautta Ubuntuun UltraVNC Viewer -ohjelmalla

Kuvassa 34 ":1" tarkoittaa samaa kuin portti 5901. Yhteyden muodostuessa avautuu graafinen etäyhteys Ubuntuun, jolloin voidaan käyttää Sapphire Carat GUI-asiakasohjelmaa ja Sappire Loupea koulun verkon ulkopuolelta. Loupen käyttö onnistuu selaimella sisäverkon IP-osoitteella.

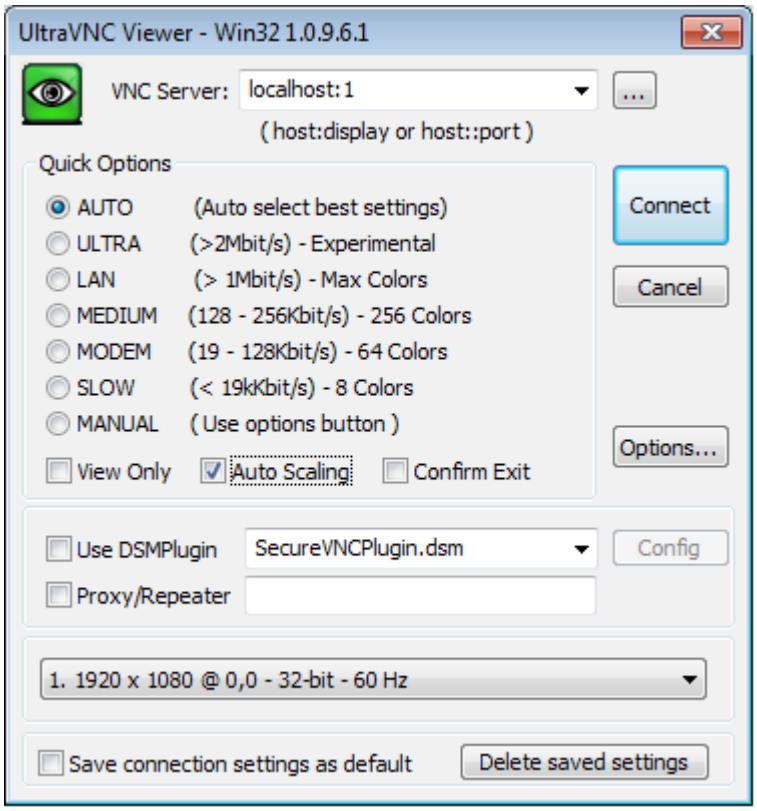
4.4.2 Windows

Windowsilla etäyhteys onnistuu myös SSH-tunnelilla kätevästi. SSH-tunnelin muodostamiseen käytetään Putty Tray -ohjelmaa.



Kuva 35: SSH-tunnelin luonti Putty Tray-ohjelmalla

Kuvassa 35 säädetään portinvälitys kuntoon. ”Source port” on portti, jolle halutaan yhteys SSH-tunneli kuuntelemaan. ”Destination” on yhteyden päämäärä, ja siihen laitetaan kohteen IP-osoite ja portti. Asetuksiin määritellään myös ”Local”, jolloin kuuntelevaksi IP-osoitteeksi määrittyy localhost eli 127.0.0.1. Jos halutaan päästä muiltakin lähiverkon koneilta käyttämään SSH-tunnelia, voidaan ”Source port” -kohtaan määrittää ”0.0.0.0:5901”, jolloin jokaisen verkkokortin 5901-portissa kuunnellaan yhteyttä varten. ”0.0.0.0”-osoitteen tilalle voidaan myös määrittää pelkästään käytettävän verkkokortin IP-osoite. Näiden määrittelyiden jälkeen klikataan ”Add”-nappulaa, jolloin asetus tallentuu. Puttyn ”Session”-kohtaan tulee myös määrittää IP-osoite tai DNS-nimi ja myös portti, jotta yhteys pystytään luomaan.



Kuva 36: VNC-yhteyden luominen tunneliin paikallista osoitetta käytettäessä

VNC-yhteyden muodostamiseksi voidaan käyttää UltraVNC Viewer -ohjelmaa. Jotta yhteys voidaan muodostaa SSH-tunnelin kautta, tulee ”VNC Server”-kohtaan määritellä osoitteeksi ”127.0.0.1:1” tai ”localhost:1”, jos Putty Tray-ohjelmaan on määritelty ”Local” ja TCP-portti 5901 ”Source”-portiksi. UltraVNC Viewer -ohjelmasta kannattaa myös valita ”Auto Scaling”, jolloin ikkuna skaalataan näytölle sopivaksi.

4.5 Tietoturva

Sapphire-laadunhallintaärjestelmä käyttää TLS-ja SSL-protokollia yhteyksien muodostamiseen. Järjestelmä käyttää yksilöllisiä 2048-bittisiä SSL-sertifikaatteja, jolloin jokaisella Sapphire-järjestelmällä on oma sertifikaattinsa. Tämä mahdollistaa liikenteen salauksen tason pysymisen hyvänä. [3, s. 6.]

Loupeen muodostetaan yhteys selaimella HTTPS-session yli, jolloin liikenne Loupen ja asiakkaan välillä on salattua 2048-bittisellä RSA:lla.

Sapphire-järjestelmän palvelimia ja silmää voidaan myös hallita SSH-yhteyden kautta, jolloin yhteys on salattu nykytiedon valossa riittävän hyvin.

VNC-yhteys Internetin yli on salattu SSH-tunnelin avulla, mutta VNC-liikenne koulun verkossa on salaamatonta. Salasanat on salattu, muttei muu VNC-liikenne. [6.] Tämä olisi hyvä vielä suojata, vaikkakin virtuaalipalvelimelta yhteydet Sapphire-järjestelmään ovat salatut. Turvallisempi VNC-ohjelma olisi SSVNC, johon saa SSL ja/tai SSH salauksen. [7.]

Metropolian langattomien verkkojen tietoturvan taso vaikutti hyvältä. Student-ja Eduroam-verkot on suojattu RADIUS-palvelimella ja PEAP-autentikoinnilla käyttäen WPA/WPA2-salausta. Guest-verkon HTTP-autentikointi on myös suojattu SSL:llä ja oikeilla sertifikaateilla. Guest-verkon liikenne liikkuu kuitenkin salaamattomana, jolloin sen kaappaaminen selkokielisenä on mahdollista.

5 Langattomien verkkojen tietoturva

Langattomien verkkojen riskit johtuvat siitä, että data kulkee ilmassa, jolloin kuka vaan voi kaapata ja analysoida sitä. Data on useimmiten salattua sen liikkuessa langattomasti, mutta salaukset ovat murrettavissa.

Langattomien verkkojen salausalgoritmeista WEP on vanhentunut ja turvaton, joten sitä ei pidä enää käyttää. Tällä hetkellä turvallisia salausalgoritmeja ovat WPA ja WPA2, jos salausavain ei ole sanakirjan sana, vaan se on täysin sattumanvarainen ja siinä on erikoismerkkejä, numeroita ja kirjaimia. Salausavaimen tulee olla myös vähintään 13 merkkiä pitkä, jolloin se ei ole helposti murrettavissa. [8.]

Salausavaimen murtaminen tapahtuu käytännössä niin, että käyttäjä on autentikoitunut langattoman tukiaseman kanssa. Tällöin käyttäjä deautentikoidaan, jolloin saadaan kaapattua autentikointi käyttäjän uudelleen autentikoituessa. Tämän jälkeen on enää murrettava salausavain, kun autentikointi on saatu kaapattua. Salausavaimen murtaminen on helppoa, jos se löytyy sanakirjasta. Tällöin se voidaan murtaa helposti dictionary-hyökkäyksellä. Toinen tapa on käyttää bruteforce-hyökkäystä salausavaimen murtamiseen. Tällöin kokeillaan kaikki vaihtoehdot läpi, jolloin jos salasanassa on erikoismerkkejä tai se on pitkä ja monimutkainen, on sen murtaminen hankalampaa.

Lähivuosina näytönohjainten tehot ovat suurentuneet ja niitä pystyy nykyään käyttämään tehokkaasti salasanojan murtamiseen. Esimerkiksi Pyrit-ohjelmalla murtaminen onnistuu käyttäen näytönohjaimia, jolloin näytönohjain-klusterilla monimutkaisemmankin salausavaimen murtaminen on mahdollista.

RADIUS-palvelimen käyttö käyttäjän tunnistaumisessa WLAN-verkkoon lisää turvallisuutta huomattavasti, perinteiseen pelkkään WPA-avaimeen verrattuna. RADIUS-palvelimen EAP-protokollana tulisi käyttää esimerkiksi turvallista PEAP-protokollaa, joka mahdollistaa EAP-protokollan tunneloimisen salatun TLS-tunnelin läpi. [12.]

Kohdistetussa hyökkäyksessä hyökkääjä perustaa oman luvattoman tukiaseman ja RADIUS-palvelimen, ja yrittää sen kautta saada kaapattua käyttäjätunnuksen ja salasanan verkkoon. Hyökkääjä voi muuttaa luvattoman tukiaseman MAC-osoitteen muistutta-

maan oikeaa tukiasemaa tai jopa samaksi, jos saa häirittyä oikeaa tukiasemaa häirintälähettimellä. Yrityksen työntekijä voi myös perustaa luvattoman tukiaseman tuomalla oman tukiaseman yrityksen verkkoon tai vahingossa luomalla ohjelmalla salaamattoman tukiaseman, joka sallii pääsyn yrityksen verkkoon. Luvattomat tukiasemat on mahdollista kuitenkin havaita ja estää WIDS / WIPS-järjestelmällä [11; 10.]

Loppuvuodesta 2011 löytyi WPS-protokollasta haavoittuvuus [9.]. POC:na tehtiin Reaver-ohjelma, jolla saadaan murrettua langattomat tukiasemat, jotka käyttävät WPS-protokollaa. Kotilaitteissa yleisimmin päällä oleva WPS kannattaa poistaa käytöstä haavoittuvuuden vuoksi.

Suojamaton langaton verkko on myös tietoturvariski, koska data siirtyy salaamattomana. Tällöin kuka vaan voi kaapata dataa verkossa ja selvittää salasanoja helposti. Maaliskuussa 2011 tuli voimaan laki, joka sallii avoimien langattomien verkon käytön [13].

6 Yhteenveto

Tässä insinöörityössä perehdyttiin 7signal Sapphire -laadunhallintajärjestelmään, langattomiin lähiverkkoihin ja niiden tietoturvaan. Työn painopisteenä oli Metropolian 7signal Sapphire -järjestelmä. Ensiksi kerrottiin langattomista verkoista ja niiden standardeista. Tämän jälkeen esiteltiin 7signal Sapphire -järjestelmän toimintaa ja komponentteja. Kolmannessa pääkappaleessa kerrottiin Metropolian Bulevardin toimipisteen langattomista verkoista, siellä olevasta Sapphire-järjestelmästä ja erilaisten suorituskykytestien tuloksista ja myös järjestelmän tietoturvasta. Lopuksi kerrottiin yleisesti langattomien verkkojen tietoturvasta. Insinöörityön aikana tehdyt testit Sapphire-järjestelmällä kertovat hyvin radiotaajuusympäristöstä ja myös tukiasemien ja langattoman verkon tilasta.

Jotta 7signal-järjestelmästä saataisiin mahdollisimman suuri hyöty, tulisi silmä sijoittaa uuteen paikkaan, jossa signaali kaukaisempiinkin tukiasemiin olisi riittävä. Myös portteja tulisi avata, jotta kaikki tarvittavat testit pystyttäisiin suorittamaan. Virtuaalipalvelimen VNC-yhteys olisi myös hyvä salata tietoturvasyistä. 5 GHz:n taajuusaluetta olisi myös hyvä hyödyntää tukiasemien salliessa. Tämä mahdollistaisi vähähäiriöisemmät yhteydet.

Alunperin oli tarkoitus raportoida Metropolian Bulevardin toimipisteen kaikista langattomista verkoista. Silmälle ei kuitenkaan tietoturvasyistä saatu salausavaimia Metropolian salattuihin verkkoihin, eikä pyydettyjä portteja auki, jotta kaikki testit olisi saatu suoritettua. Myöskään tukiasemien määrää eikä fyysistä sijaintikarttaa saatu, koska se ei ollut mahdollista oppilaitoksen tietoturvapolitiikan vuoksi.

7 Lähteet

[1] 7signal yleisesittely. PDF-dokumentti. 7Signal Oy.

[2] IEEE 802.11. WWW-dokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/IEEE_802.11>. Luettu 2.2.2012.

[3] 7signal Sapphire Deployment Guide. PDF-dokumentti. 7Signal Oy.

[4] 7signal Carat. PDF-dokumentti. 7Signal Oy.

[5] Electromagnetic interference at 2.4 GHz. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz> .Luettu 3.2.2012.

[6] Virtual Network Computing. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Virtual_Network_Computing>. Luettu 3.3.2012.

[7] SSVNC: SSL/SSH VNC viewer. WWW-dokumentti. <http://www.karlrunge.com/x11vnc/ssvnc.html>. Luettu 13.4.2012.

[8] Wi-Fi Protected Access. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>. Luettu 5.2.2012.

[9] WiFi Protected Setup PIN brute force vulnerability. WWW-dokumentti. <http://www.kb.cert.org/vuls/id/723755>. Luettu 13.3.2012.

[10] Rogue Access Point. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Rogue_access_point>. 14.3.2012.

[11] Wireless Intrusion prevention system. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system>. Luettu 13.4.2012.

[12] Wireless Security. WWW-dokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wireless_security>. Luettu 4.3.2012.

[13] Avoin WLAN nyt vapaata riistaa. WWW-dokumentti. <http://petterijarvinen.puheenvuoro.uusisuomi.fi/65324-avoin-wlan-nyt-vapaata-riistaa>. Luettu 13.4.2012.