Langattoman lähiverkon suunnittelu ja toteutus yritykselle

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Hämeen Ammattikorkeakoulu Riihimäki, kevät 2017

Petteri Hakomäki

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Tietotekniikka
Tietoliikenneverkot

Tekijä Petteri Hakomäki **Vuosi** 2017

Työn nimi Langattoman lähiverkon suunnittelu ja toteutus yritykselle

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa Polttimo Oy:n Lahden toimipisteelle uusi langaton lähiverkko. Vanha WLAN-verkko koostui erillisistä langattomista reitittimistä, jotka lähettivät jokainen omaa verkkoaan. Tämän tilalle haluttiin saada laajempi, tietoturvallisempi ja keskitetysti hallittu langaton lähiverkko, lähinnä kokouksia ja vieraita ajatellen.

Verkon suunnittelussa sekä tukiasemien ja langattomien reitittimien signaalivoimakkuuksia mitattaessa käytetiin Ekahaun Site Survey -ohjelmaa. Mittauksia toteutettiin sekä vanhan että uuden verkon laajuuden kartoittamiseksi sekä tukiasemien paikkojen valinnassa.

Työssä käydään läpi langattomien verkkojen perusteet: eri käsitteitä, termistöä ja tietoturvaa sekä tutustutaan suunnittelusääntöihin. Myös uuden verkon rakenne sekä valitun verkkoratkaisun eri ominaisuudet ja hallinta käydään läpi.

Lopuksi pohditaan, millä tavalla rakennettua verkkoa voisi edelleen kehittää ja mitä suunnittelu- ja toteutusvaiheessa olisi voinut tehdä paremmin. Tämän lisäksi katsotaan miten tästä opinnäytetyöstä voisi tehdä jatkotutkimusta.

Avainsanat langattomat lähiverkot, wifi, Aruba, tukiasema

Sivut 27 s. + liitteet 0 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Information Technology

Author Petteri Hakomäki **Year** 2017

Subject of Bachelor's thesis Designing and implementing a wireless LAN for a company

ABSTRACT

The aim of this thesis was to design and implement a new wireless local network for Polttimo Oy in Lahti. The old WLAN consisted of separate wireless routers which advertised their own separate networks. A wider, more secure network and a centralized control environment was required by the commissioner, mainly for meetings and guest use.

Planning software Site Survey by Ekahau was used in planning the new network and for determining the signal strength of the access points and routers. The measurements were done on both the old network and the new one. The locations for the new access points were determined in the project as well.

The thesis examines the fundamentals of WLAN. The different concepts, terminology and security are studied here as well as the design of the new network, different elements and managing the control environment.

Finally, this thesis reviews how the new wireless network could still be improved and what could have been done better in the design and implementation stages. In addition to this it analyzes how someone could conduct further research and expand this topic.

Keywords WLAN, wifi, Aruba, access point

Pages 27 p. + appendices 0 p.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli parantaa Lahden Polttimo Oy:n langattoman lähiverkon toimivuutta suunnittelemalla ja toteuttamalla se uudelleen alusta loppuun. Oli käynyt ilmi useampaan otteeseen, että yrityksen senaikainen langaton lähiverkko ei aina kyennyt toimimaan odotetulla tehokkuudella. Verkon uudistuksesta saatiin molempia osapuolia hyödyttävä aihe opinnäytetyötä varten.

Polttimo Oy on maltaita ja mallasuutteita valmistava konserni, johon kuuluvat myös Senson Oy ja Viking Malt Oy. IT-osasto hoitaa kaikki paikallisesti tehtävät työt, kuten uusien työasemien asennukset, korjaukset sekä tarjoaa lähitukea muille työntekijöille. Alue koostuu konttorirakennuksista, varastosta, siilostosta sekä tehtaasta.

Opinnäytetyössä tavoitteena oli löytää hyvä, helposti hallittava ja kustannustehokas langaton lähiverkkoratkaisu tietoturvaa unohtamatta. Mahdollinen myöhemmin tehtävä verkon laajennus otettiin huomioon verkkoratkaisua valittaessa.

Koululta lainaksi saatuja laitteita ja ohjelmistoja käytettiin langattoman verkon mittauksissa ja suunnittelussa. Ohjelmistona toimi Ekahaun Site Survey, joka mahdollisti täyden raportointi-, suunnittelu- sekä testausmahdollisuuden langattomille verkoille. Tämän avulla tehtiin mittauksia vanhasta ja uudesta verkosta sekä haettiin uusille laitteille mahdollisia paikkoja mittaamalla lainassa olevan tukiaseman signaalivoimakkuutta. Tämä ei tietenkään anna täysin tarkkaa kuvaa kuuluvuusalueista, mutta sillä saatiin suuntaa antavaa tietoa. Inmics Oy:ltä käyneeltä konsultilta saatiin vinkkejä tukiasemien kiinnityspaikkoihin sekä yleiseen suunnitteluun.

Konttorirakennusten sisä- ja ulkomateriaaleilla oli vaikutusta signaalin kulkemisen kannalta. Koska eri rakennusmateriaalien signaalin läpäisykyky vaihtelee, sitä käytettiin hyväksi tukiasemien paikkoja suunniteltaessa. Myös laitteiden määrällä ja peitettävän alueen suuruudella oli suuri vaikutus suunnittelun ja toteutuksen kannalta.

Verkko saatiin käyttövalmiiksi juurin ennen Viking Malt Oy:n vuosittaista tapaamista, jolloin useista eri toimipisteistä kokoontui työntekijöitä Lahteen pitämään palavereja. Tällä saatiin hyvin stressitestattua tukiasemat ja verkko.

2 PERUSTEET LANGATTOMISTA LÄHIVERKOISTA

Langattomilla lähiverkoilla (WLAN) tarkoitetaan pienen alueen sisällä tapahtuvaa langatonta tiedonsiirtoa. Yleisessä käytössä on lyhenne Wi-Fi. Termillä tarkoitetaan laitteita, jotka täyttävät Wi-Fi Alliancen määrittelemät yhteensopivuusehdot ja toimivat silloin muiden sertifikaatin saaneiden laitteiden kanssa. Poiketen tavallisesta tiedonsiirrosta, jossa data liikkuu johtoa pitkin laitteesta laitteeseen, langattomissa verkoissa tämä tapahtuu radioaaltoja hyväksi käyttäen. Infrapunavaloa on käytetty, mutta sen kehi-

tys loppui nopeasti ensimmäisen standardin jälkeen. (Geier 2005, 4.; Hovatta 2005, 12.)

Langattomille lähiverkoille aloitettiin standardikehitys vuonna 1990 ja vuonna 1997 IEEE sai valmiiksi 802.11 standardin. Vaikka 802.11:ssa oli suorituskyky- ja taajuuskäyttölupaongelmia, se antoi hyvän pohjan, jonka päälle voitiin rakentaa entistä tehokkaampia ratkaisuja. Tällä hetkellä on kehitteillä standardi 802.11ay. (Puska 2005, 15.)

Langattomat lähiverkot tuovat omat haasteensa ja uhkansa tietoliikenteeseen, mutta tarjoavat silti kätevän tavan pysyä yhteydessä internettiin periaatteessa missä tahansa. Yritykset käyttävät langattomia lähiverkkoja tarjotakseen vieraille mahdollisuuden kytkeytyä internettiin esimerkiksi kokousten ajaksi tai kahvilat voivat tarjota ilmaisen WLANin houkutellakseen asiakkaita. Tietoturva aiheuttaa kuitenkin jatkuvasti haasteita. Avoimet langattomat verkot ovat suuri tietoturva-aukko. Yhteydet eivät myöskään ole aina luotettavasti saatavilla ja lisäksi suorituskyky jää jälkeen fyysisesti kytkettyjen verkkojen rinnalla.

2.1 Infrastruktuuri ja toiminta

Infrastruktuuriverkossa langattomat päätelaitteet liittyvät yhteyspisteeseen, joka toimii siltana fyysisen lähiverkon ja WLAN-verkon välillä. Yhteyspisteillä tarkoitetaan laitteita, joilla käyttäjä saa yhteyden langattomaan verkkoon, esimerkiksi tukiasemat (AP) ja langatonta signaalia lähettävät reitittimet. Yhteyspisteet lähettävät ympärilleen majakkasanomaa, jolla ne ilmoittavat olemassaolostaan ja parametreistaan käyttäjien laitteille. Tärkein parametri on SSID-tunnus, jolla verkko yleensä tunnistetaan. WLAN-verkon hallinnoija voi halutessaan jättää SSID-mainostuksen pois. Kun käyttäjän laite liittyy verkkoon, se määrittelee verkkokorttiinsa yhteyspisteen parametrit sen lähettämän majakkasanoman mukaisiksi. Majakkasanoma sisältää kaikki tiedot verkosta, kuten aikasynkronoinnin, salausmenetelmän, bittinopeudet ja edellä mainitun SSID:n. Parametrien määrittelyn jälkeen, jos verkko on suojattu salasanalla, verkkoon liittyvä laite ja yhteyspiste käyvät läpi tunnistautumisen, jonka jälkeen käyttäjä voi liittyä verkkoon. Kun tunnistus on hoidettu, verkkoon liittynyt laite lähettää omat tietonsa yhteyspisteelle, joka rekisteröi tiedot ja lähettää takaisin liityntätunnuksen. (Puska 2005, 132.; Puska 2005, 137.)

Jos langattoman lähiverkon peittävyystarve ei ole suuri, yksi yhteyspiste yleensä riittää kattamaan alueen. Laajemmissa ratkaisuissa tarvitaan monta laitetta, jolloin niiden lähettämät radiosignaalit saattavat mennä osittain päällekkäin, mikä taas heikentää verkon suorituskykyä. Tätä voi verrata kahden ihmisen välillä käytävään keskusteluun meluisassa kahvilassa. Alueiden päällekkäisyyksistä aiheutuvaa haittaa hoidetaan eri radiokanavilla, jotta data voi kulkea vapaasti laitteiden välillä.

2.1.1 WLAN-verkkojen yleisimmät taajuudet

Tällä hetkellä yleisimmät taajuudet WLAN-verkoissa ovat 2,4 GHz ja 5 GHz. Molemmilla on omat hyvät ja huonot puolensa. 2,4 GHz:n kaista on edelleen yleisempi ja tukee vanhempia päätelaitteita. Sen taajuudella toimiva signaali kuuluu laajemmalle alueelle ja se pääsee paremmin etenemään esteiden läpi. 2,4 GHz:n kaista on 80 MHz:n levyinen, minkä takia sillä on käytössään ainoastaan kolmesta neljään ei-päällekkäistä kanavaa. Tämä mahdollistaa maksimissaan neljän tukiaseman häiriöttömän toiminnan samalla alueella. (Geier 2005, 128.)

5 GHz:n taajuudella jokainen kanava toimii 20 MHz:n leveydellä, mikä mahdollistaa jopa 19 ei-päällekkäistä kanavaa. Tällöin taajuusalue ei ole niin ruuhkainen, jolloin yhteyden suorituskyky on parempi verrattuna pitempään kaistanleveyteen. 5 GHz:n kaistanleveyden takia, sen signaali ei kanna yhtä kauas kuin 2,4 GHz:n. Tarjolla myös on reitittimiä ja tukiasemia, jotka pystyvät lähettämään molemmilla taajuusalueilla signaalia samanaikaisesti. Tämä mahdollistaa entistä tehokkaammat ja laajemmat yhteydet. (Geier 2005, 128.)

2.1.2 Tukiasemat, ohjaimet ja hallinta

Langattomien lähiverkkojen ydin on tukiasema (AP). Kotikäytössä puhutaan yleensä reitittimestä, mutta tämä on yleensä tukiasema, joka hoitaa myös reitityksen. Laitteelle voidaan määritellä monia eri parametreja. Näihin kuuluvat mm. laitteen nimi, SSID-tunnus, IP-osoite, aliverkkopeite ja oletusreitittimen osoite. Nykyään suurinta osaa näistä ei välttämättä tarvitse erikseen määritellä, varsinkaan kotioloissa. Tukiasemiin voi asettaa monta eri SSID-tunnusta, joilla on omat parametrinsa. Tällaisia ovat esimerkiksi, onko verkossa tunnistusmenetelmää ja siihen avain, mahdollinen 802.1x -tunnistusprotokolla sekä, lähetetäänkö SSID-tunnusta majakkasanomana vai pidetäänkö se piilotettuna. (Puska 2005, 143.)

Suuremmissa langattomissa verkkojärjestelmissä, joissa on useita tukiasemia eri kohteissa, hallinnointiin tarvitaan yleensä ohjain (controller). Ohjain jakaa muille tukiasemille verkon asetukset, kuten IP-osoitteet sekä hoitaa itsenäisesti kuorman hallinnan ja verkkoon tunnistautumisen. Nykyään on olemassa tukiasemia, jotka eivät tarvitse erillistä ohjainta (IAP). Nämä laitteet voivat toimia sekä tukiasemana että ohjaimena muulle langattomalle verkolle.

Tukiasemia, reitittimiä ja langattoman verkon ohjaimia voidaan hallita usealla eri tavalla. Tietoturvattomia vaihtoehtoja on Telnet-yhteys ja webselaimen kautta otettava HTTP-yhteys. Näissä tieto kulkee salaamattomana verkon yli. Salattuja vaihtoehtoja ovat SSH- ja http-protokollan suojattu versio HTTPS. Konsolikaapeli on näiden lisäksi yksi mahdollisuus yhteyden luomiseen.

2.2 Standardit

IEEE alkoi kehittämään ensimmäistä standardia langattomille verkoille vuonna 1991. Se julkaistiin vasta vuonna 1997 ja siitä on tullut perusstandardi langattomille verkoille. Sen käyttötaajuudeksi valikoitui 2.4 GHz jota käytetään vielä tänäkin päivänä. Käyttönopeuksiksi standardisoitiin 1 ja 2 Mbit/s. 802.11:ssa oli mahdollisuus käyttää infrapunavaloa datan siirtämiseen, mutta sen kehitys lopetettiin tähän. Tässä standardissa esiteltiin kaksi erilaista verkkotopologiaa: ad-hoc-verkko ja infrastruktuuriverkko. Ad-hoc-verkossa jokainen verkkoon liitetty laite lähettää tiedon suoraan toiselle WLAN-verkossa olevalle laitteelle. Infrastruktuuriverkossa sen sijaan on vähintään yksi tukiasema liitettynä langalliseen lähiverkkoon. Suurin osa langattomista verkoista toimii infrastruktuuriperiaatteella. (Hovatta 2005, 11.)

Edellisen standardin siirtonopeuksien katsottiin olevan liian hitaita, joten vuonna 1999 IEEE julkaisi standardin 802.11b. Tässä teoreettiset siirtonopeudet olivat nopeammat kuin paria vuotta aikaisemmassa: 11 Mbit/s. Samana vuonna julkaistiin myös 802.11a. Standardissa tuli käyttöön 5 GHz:n taajuudet ja siirtotekniikaksi vaihtui monikantoaaltomodulaatio (OFDM). Tämä mahdollisti melkein viisinkertaisen teoreettisen maksiminopeuden edelliseen verrattuna. Täytyy muistaa, että teoreettinen tiedonsiirtonopeus ei vastaa käytännön nopeusarvoja. Vaikka a-standardin ja b-standardin teoreettiset nopeudet ovat 54Mbit/s ja 11Mbit/s, käytännössä nopeudet ovat noin puolet tästä. (Hovatta 2005, 12.)

Vuonna 2003 valmistui 802.11g standardi. Se käyttää OFDM siirtotekniikkaa ja teoreettinen maksiminopeus pysyi edelleen samana kuin 802.11b:ssä eli 54 Mbit/s. Tämän standardin mukaiset laitteet toimivat kuitenkin 2,4 GHz:n alueella. G-standardi siis pystyy samaan teoreettiseen maksiminopeuteen kuin a-standardi, mutta pienemmällä taajuusalueella. Tämä mahdollistaa isomman peittoalueen. Laitteet, jotka toimivat g-standardissa, ovat yhteensopivia b-standardia käyttävien laitteiden kanssa.

Standardi 802.11n valmistui vuonna 2009. Se pyrkii nostamaan suorituskykyä usealla antennilla. Tätä kutsutaan MIMO-tekniikaksi (Multiple-Input and Multiple-Output). MIMO mahdollistaa jopa 600 Mbit/s teoreettisen siirtonopeuden käyttämällä kaistanleveyttä 40 MHz. Tammikuussa 2014 valmistunut ac-standardin tarkoituksena on lisätä suorituskykyä n-standardiin verrattuna. Se nostaa antennien enimmäismäärän kahdeksaan ja voi käyttää kaistanleveyksiä 20, 40, 80 ja 160 MHz. Kahdeksalla antennilla ja 160 MHz:n kaistanleveydellä päästäisiin teoriassa yli 6 Gbit/s nopeuksiin. (IEE Std 802.11n™-2009/2009, 247.; IEE Std 802.11n™-2013/2013, 339.)

2.3 Tietoturva

Yksi isoimmista ongelmista langattomissa lähiverkoissa on tietoturvan varmistaminen. Uhat ovat suurimmilta osin samoja kun perinteisissä langallisissa verkoissa, mutta langattomuus tuo niihin omat ulottuvuutensa. Verkon toiminta-aluetta on vaikea rajata tarkasti. Radiosignaalit on myös-

kin helppo napata ilmasta ja salaamattoman viestin voi helposti lukea kuka tahansa. Kaikille avoimet WLAN-verkot luovat tietoturvauhan sen käyttäjille. Vaikka langattomille verkoille on standardikehityksen aikana kehitetty tietoturvaratkaisuja, niiden menestys on ollut vaihtelevaa.

2.3.1 Hyökkäykset

Ilmassa kulkevat, langattomat datapaketit on helppo napata siihen erityisesti tehdyillä ohjelmilla. Jos käyttäjän laitteen ja tukiaseman välillä ei käytetä salausta, kaikki data kulkee selkokielisenä. Tällöin tiedon napannut voi helposti lukea esimerkiksi käyttäjätunnuksia ja salasanoja. (Geier 2005, 172.)

Avoimet ja heikon tunnistautumisen omaavat langattomat verkot ovat vaarallisia, varsinkin yritysmaailmassa. Jos tukiasemaan pääsee käsiksi, se tarkoittaa sitä, että käytössä olevat palvelimet ja käyttäjien tietokoneet saattavat olla vaarassa. Hyökkääjä voi itse myydä firman työntekijälle tai käydä itse asentamassa verkkoon rosvotukiaseman. Tämän avulla hän pääsee helposti koko verkkoon käsiksi. Tästä syystä tietoturvasta vastaavien täytyisi valvoa verkkoon kytkettyjä laitteita ja tutkia epäilyttävät kohteet. (Geier 2005, 176.)

Yksi yleisimmistä hyökkäyksistä on palvelunestohyökkäys, joka tunnetaan nimellä DoS (Denial-of-service). Tämä voi hidastaa verkkoliikennettä huomattavasti tai pahimmassa tapauksessa tehdä koko verkosta käyttökelvottoman. DoS hyökkäyksiä tapahtuu myös tavallisissa, fyysisissä verkoissa. Yleisin hyökkäystapa on lähettää verkkoon valtava määrä paketteja. Tarkoituksena on kuluttaa suurin osa tai kaikki verkon resursseista, jolloin suorituskyky laskee huomattavasti. Koska pakettien määrän tässä hyökkäysmuodossa täytyy olla valtava, hyökkääjä voi käyttää verkon muita tietokoneita lähettäjinä. (Geier 2005, 176.)

Langattomissa verkoissa DoS hyökkäyksen voi suorittaa käyttämällä erittäin voimakasta radiosignaalia, joka hallitsee ilmateitä ja tekee muusta liikenteestä hidasta tai mahdotonta. Palvelunestäminen voi olla tahatonta. Esimerkiksi mikroaaltouunit käyttävät radioaaltoja, jotka voivat häiritä verkon toimintaa. (Geier 2005, 176.)

2.3.2 Suojaus

Alkuperäiseen 802.11 – standardiin kuului WEP-salaus (Wired Equivalent Privacy). Salaus on erittäin heikkolaatuinen, eikä sen käyttö ole suositeltavaa. WEP:n periaatteena on, että langattoman verkon tukiaseman ja käyttäjän laitteen välille luodaan salausavain. Tätä käytetään datapakettien salaukseen ennen radioaalloille lähettämistä ja perillä salauksen purkamiseen ja koskemattomuuden varmistamiseen. Avain voi olla mikä tahansa 13 merkkiä pitkä yhdistelmä. WEP:n heikkous on, että hyökkääjä voi saada salausavaimen selville pelkästään kuuntelemalla ja keräämällä salattua dataa radioaalloilta, sillä sitä ei vaihdeta. (Hovatta 2005, 28.)

Kehittyneempi salausmenelmä on WPA (Wi-Fi Protected Access). Tällä salaustekniikalla pyrittiin paikkamaan WEP-salauksen heikkouksia ja mukaan tuotiin käyttäjän autentikointi. Liikenteen salauksessa käytetään TKIP (Temporal Key Integrity Protocol)-protokollaa. WPA:ssa on salausavaimet edelleen käytössä, mutta ne ovat pidempiä ja pakettikohtaisia. Autentikoinnin tapa riippuu WPA:n versiosta. Personal versio on lähinnä kotikäyttöön tarkoitettu ja käyttää PSK (Pre-shared Key) menetelmää, jossa kaikilla verkon käyttäjillä on tiedossa sama salausavain. Enterprise versio käyttää erillistä tunnistuspalvelinta, jossa voidaan määritellä käyttäjäkohtaiset tunnistetiedot. Palvelimena toimii RADIUS-palvelin, joka voi olla yhteydessä yrityksen Active Directoryyn. Tällöin voidaan käyttää WLAN-verkkoon tunnistautuessa samoja tunnuksia, kun lähiverkon palveluihin. (Hovatta 2005, 29.)

802.11i-standardiin perustuva salausmenetelmä WPA2 on kehittyneempi versio WPA:sta. Vaikka se on suurimmalta osin sama kuin edeltäjänsä, WPA2 käyttää AES (Advanced Encryption Standard) salausta TKIP:n sijaan. Myös tässä uudemmassa on kaksi versiota kuten edeltäjässään: Enterprise ja Personal. Erot versioiden välillä ovat samat. (Hovatta 2005, 30.)

Muita suojausmenetelmiä ovat VPN (Virtual Private Network), jonka voi salata vaikkapa IPSEC-protokollalla, ja MAC-listat. VPN on yleensä käytössä etätyöratkaisuissa ja siihen tarvitaan erillinen ohjelma. MAC-listat tarkoittavat tukiasemille tehtyjä listoja, joihin voidaan määritellä jokaisen yksittäisen laitteen MAC-tunnus. Listalla olevat tietokoneet pääsevät verkkoon käsiksi. Valitettavasti listojen ylläpitäminen on työlästä ja MAC-osoitteen muuttaminen ohjelmallisesti helppoa. (Hovatta 2005, 28.)

Vaikka WPA2 suojauksessa käytettävä AES menetelmä oli ainakin julkaisunsa aikana vahva, nykyaikaisten tietokoneiden laskentatehot ovat kasvaneet paljon. Tämä tekee yksinkertaisista ja lyhyistä salasanoista helposti murrettavan. Salasanaan valittaessa suositellaan käytettävän isoja ja pieniä kirjaimia, numeroita ja symboleita satunnaisessa järjestyksessä. Pituudeksi suositellaan lähteestä riippuen 8-14 merkkiä.

2.4 Suunnittelu

Kaikki tietotekniikkaprojektit pitäisi aloittaa vaatimusmäärittelystä. Tässä kartoitetaan, mitä tarpeita yrityksellä tai organisaatiolla on, esimerkiksi langattoman verkon suhteen, ja tämän perusteella räätälöidään teknisesti hyvä ratkaisu. WLAN-verkon suunnittelussa pitää erityisesti ottaa huomioon peittoalue, käyttäjämäärä, tarvittava verkon suorituskyky ja tietoturva. Tällä saadaan hyvä pohja vankalle ja oikean kokoiselle verkolle, joka tarjoaa tarvittavan turvallisuuden ja suorituskyvyn. (Puska 2005, 220.)

Kun tarvittavat määrittelyt on tehty, tehdään verkkosuunnitelma. Riippuen rakennettavan verkon koosta, verkkosuunnitelmassa määritellään vähintään yhteyspisteiden määrä sekä niille alustavat paikat. Jos verkosta tulee laaja ja jos useat tukiasemat ovat toistensa kuuluvuusalueella, täytyy ottaa huomioon käytettävät radiokanavat ja käyttötaajuus. Huonosti suunniteltuna verkon suorituskyky laskee taajuusalueiden ruuhkautuessa. 5 GHz:n

käyttötaajuus soveltuu hyvin tiheisiin verkkoihin, sillä ei-päällekkäisiä radiokanavia on paljon enemmän kun 2,4 GHz:n taajuudella. (Puska 2005, 220.)

Yhteyspisteiden paikkojen valinnassa täytyy ottaa huomioon materiaalit, joita rakennuksessa on käytetty. Langattoman verkon signaali läpäisee heikommin esimerkiksi betonin kuin kipsilevyn. Erilaisia suunnitteluohjelmia voi käyttää apuna paikkavalintaa tehdessä. Näistä ensimmäisiä oli Ekahau Oy:n ohjelma, joka julkaistiin vuonna 2002. Ohjelmaan tarvitaan pohjakartta rakennuksesta, jonka pohjalta suunnittelu aloitetaan. Jos halutaan simuloimalla etsiä alustavia paikkoja tukiasemille, pohjakarttaan täytyy asettaa seinille ja muille esteille oikeanlaiset materiaalit, jotta signaalin eteneminen olisi mahdollisimman realistinen. (Hovatta 2005, 21.)

Paikkamäärittelyssä voidaan ottaa myös huomioon kaapelointi. Johdot tulisi pyrkiä piilottamaan seinän sisään, jolloin ratkaisusta tulee silmälle esteettinen. Yleensä tukiasemien mukana tulevat virtalähteet vaikeuttavat kaapeloinnin peittämistä huomattavasti. Tästä syystä kannattaa turvautua PoE-tekniikkaan. Tällöin laite saa verkkoyhteyden ja virran yhdestä johdosta, joka on helposti piilotettavissa.

3 POLTTIMON VANHA WLAN JA UUDEN RATKAISUN VALINTA

Vaikka Polttimo Oy:n vanha langaton lähiverkko oli päällisin puolin toimiva, siinä oli paljon kehitettävää. Suorituskyky oli alhainen, laitteita joutui käynnistämään uudelleen sekä saatavuus oli paikoin heikko.

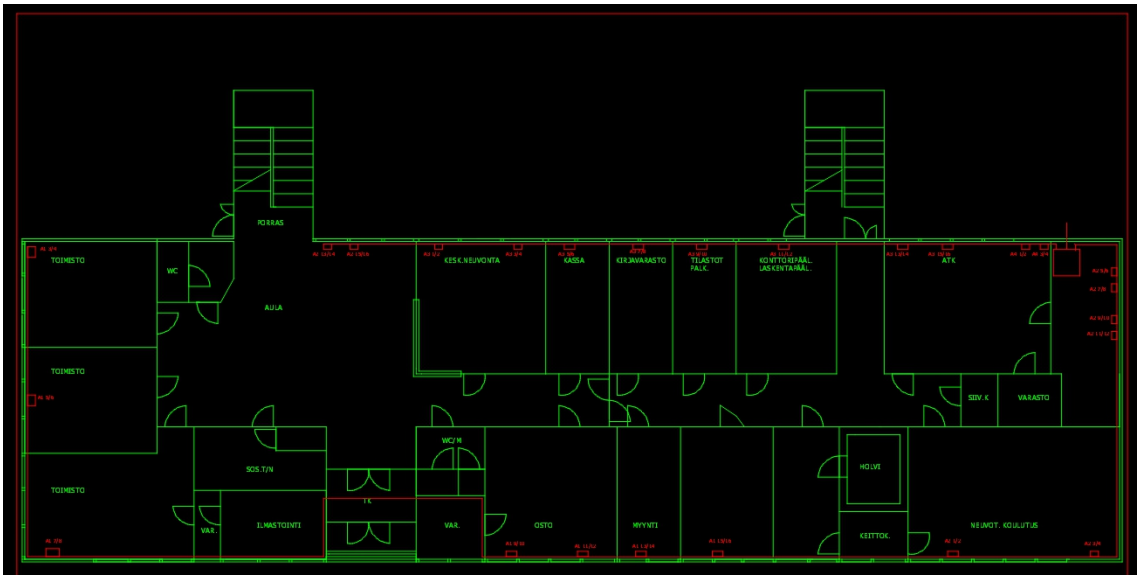
Verkko koostui erillisistä langattomista reitittimistä, jotka lähettivät jokainen omaa verkkoaan. Tämä tarkoittaa sitä, että käyttäjän piti olla kirjautuneena useampaan verkkoon ja hänen täytyi edellisen verkon ulkopuolella etsiä uuden reitittimen verkko. Laitteiden paikoitus ei ollut optimaalinen ja kaapelointi oli jäänyt avoimeksi ja silmään pistäväksi: johdot menivät välillä huoneen poikki tai olivat mytyssä nurkassa. Reitittimien paikat ja lukumäärä rajoittivat merkittävästi signaalin tehokkuutta ja saatavuutta.

Mahdollisuus kytkeytyä langattomaan verkkoon oli rajallinen tai mahdotonta tietyissä paikoissa toimipistettä. Laitteiden signaalit eivät olleet tarpeeksi kantavia, jotta mistä tahansa rakennuksesta olisi voinut kytkeytyä edes johonkin verkkoon. Käyttäjien kanssa käytyjen keskustelujen pohjalta selvisi, että jotkut haluaisivat mahdollisuuden käyttää langatonta verkkoa hyödyksi työtehtävissä.

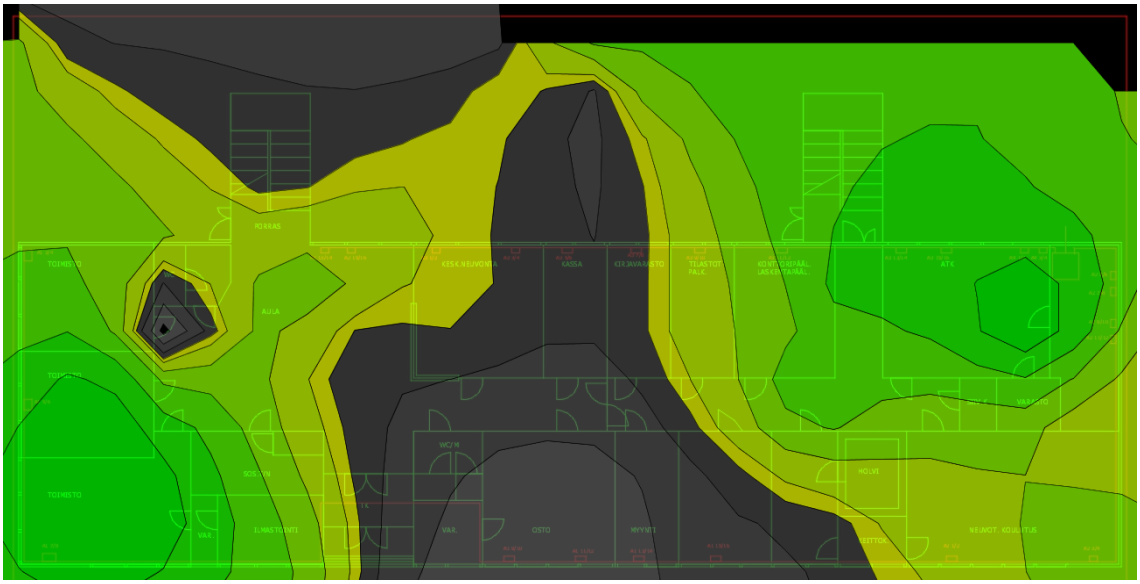
Reitittimillä ei ollut keskitettyä hallintarajapintaa. Jokaiseen laitteeseen piti ottaa yhteys web-selaimella, mikä teki hallinnasta ja verkkojen valvonnasta erittäin vaivalloista ja hankalaa. Reitittimen ja sen myötä koko verkon kaaduttua joutui usein menemään fyysisesti paikalle käynnistämään laitteen uudelleen.

3.1 Katsaus vanhaan verkkoon

Vanhassa verkkoratkaisussa oli mukana kuusi erillistä Buffalon ja Zyxelin langatonta signaalia lähettävää reititintä. Laitteet käyttivät pääasiallisesti 802.11n ja ac-standardeja, mutta mukana oli yksi vanhempaa g-standardia käyttävä laite. Reitittimistä kolme löytyi kokoushuoneista ja kolme muista tiloista. Käytettäviä verkkoja oli saman verran kuin laitteita, eli kuusi kappaletta, ja niiden SSID:t oli nimetty sen mukaan, minkä neuvotteluhuoneeseen signaalit kuuluivat. Paikoituksen ja laitteiston tekniikan vuoksi kuuluvuusalueet olivat jääneet pieniksi. Myös nopeudet ja verkon luotettavuus kärsivät näistä. Kuvissa vihreät alueet merkitsevät hyvää yhteyttä ja harmaat huonoa tai periaatteessa täysin olematonta yhteyttä.



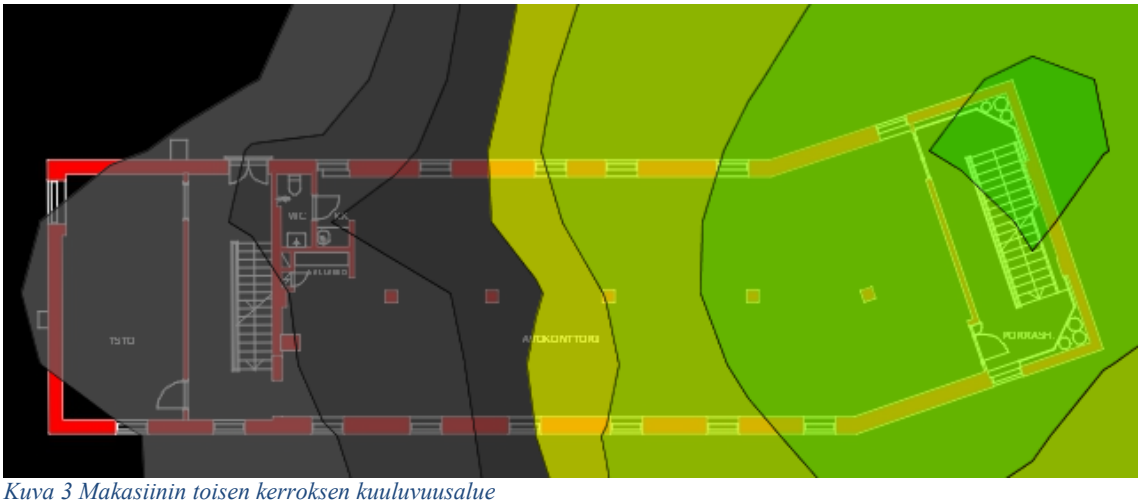
Kuva 1 Polttimon pääkonttorin pohjapiirustus



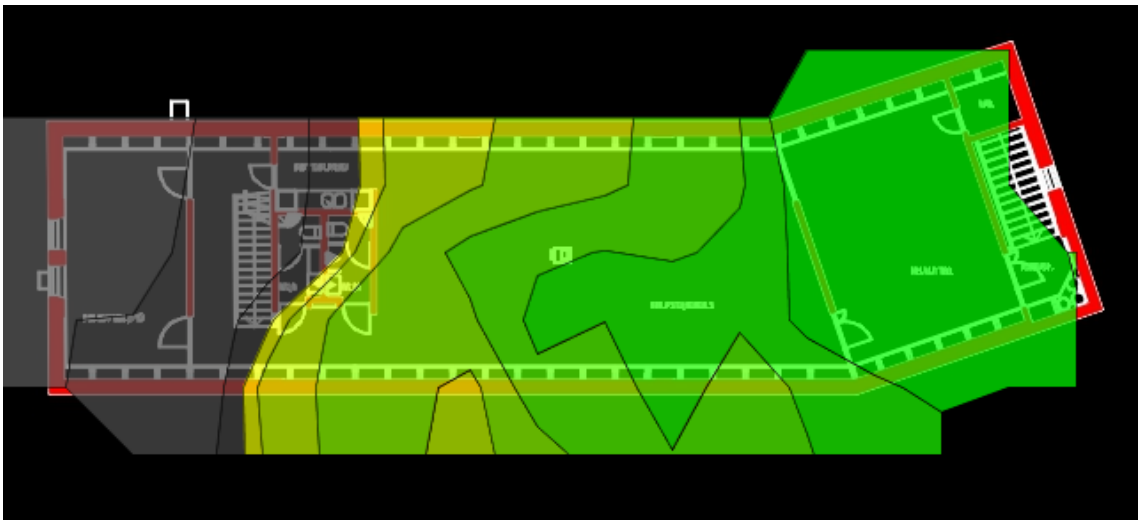
Kuva 2 Vanhan langattoman verkon kuuluvuusalue

Kuvissa 1 ja 2 näkyy pääkonttorin ensimmäinen kerros. Vanha langattoman verkon signaali on hyväksyttävällä tasolla ainoastaan reitittimien läheisyydessä ja yhteys katkeaa kokonaan keskellä.

Makasiinin langaton verkko (kuva 3 ja 4) toimi vain yhdellä tukiasemalla, joka oli kolmannessa kerroksessa kokoushuoneiden yhteydessä. Tämän laitteen signaali ei ollut tarpeeksi hyvä kantaakseen toiseen kerrokseen.

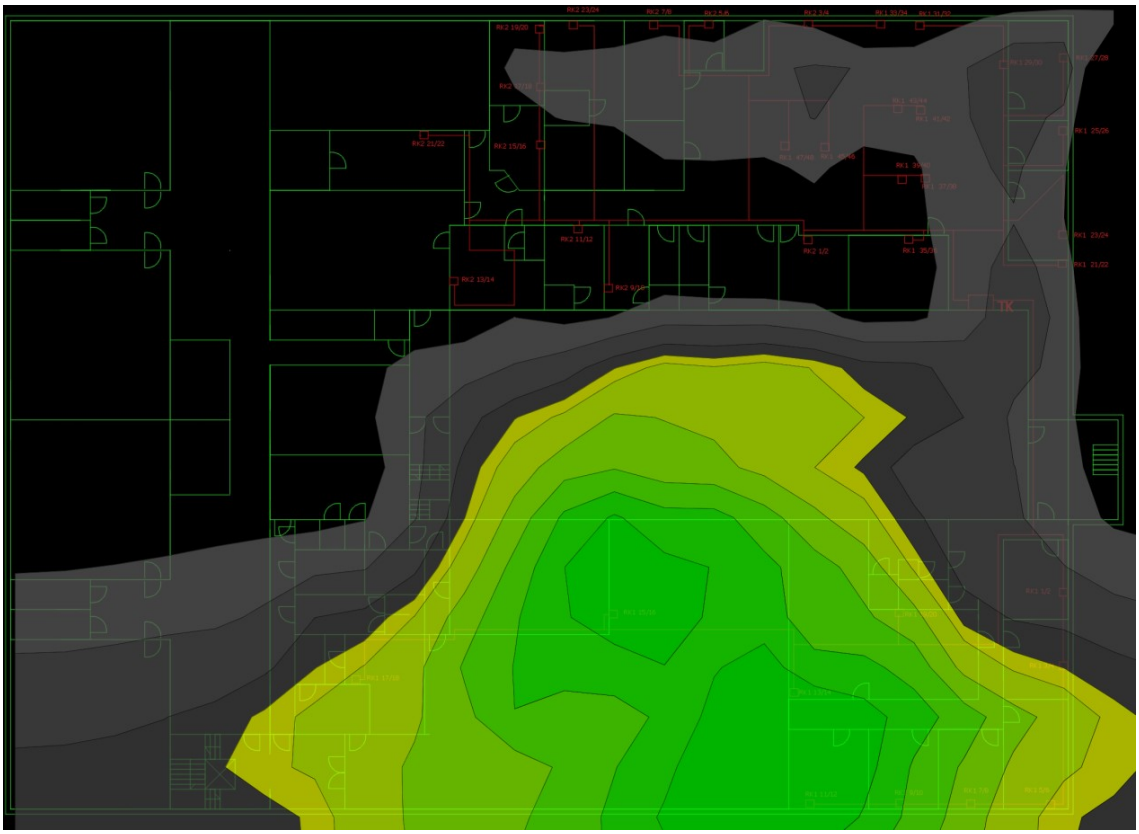


Kuva 3 Makasiinin toisen kerroksen kuuluvuusalue



Kuva 4 Makasiinin kolmannen kerroksen kuuluvuusalue

Teknisessä toimistossa (kuva 5) oli kaksi tukiasemaa, joista toinen oli sijoitettu kokoushuoneeseen ja yksi työntekijän huoneeseen. Vierekkäin olevat kaksi kokoushuonetta käyttivät lähinnä samaa verkkoa keskenään, eikä signaali ollut paras mahdollinen siinä huoneessa, jossa tukiasemaa ei ollut. Ruokalan yhteys oli vakaa, mutta heikko. Laboratoriotiloissa langatonta verkkoa ei ollut käytössä.



Kuva 5 Tekninen toimiston ja laboratorion kuuluvuusalue

3.2 Suunnitelma uudesta verkosta

Polttimon laitehankkijalle jätettiin tarjouspyyntö eri WLAN-ratkaisuista. Tarjous saatiin kahden eri laitevalmistajan laitteistosta: Aruban ja Merun. Aruban tarjouksessa oli mukana kaksi eri laitevaihtoehtoa: 200 - ja 210 sarjan ohjaimettomia tukiasemia. Nämä olivat ainoita laitteita, joita WLAN-ratkaisuun tarvitsi ostaa, mikä halvensi tarjousta huomattavasti Meruun verrattuna. Merun tarjouksessa oli FortiWLC-50D ohjain ja siihen linkitettävät erilliset tukiasemat. Tämän lisäksi tarjouksessa oli mukana ympärivuorokautinen FortiCare -sopimus molemmille laitteille. Ottaen huomioon hinnan, asennuksen, käyttäjäkokemukset sekä Merun laskevan markkinaosuuden päätettiin valita Aruban verkkoratkaisu.

Verkkoa piti laajentaa suuremmalle alueelle, kun se ennestään oli. Vaikka alkuperäisen vaatimusmäärittelyn mukaan langaton lähiverkko oli pääasiallisesti tarkoitettu vain kokoustiloihin, pyrittiin sitä laajentaa työntekijöiden omiin huoneisiin. Muutamat uudet alueet, kuten varasto ja laboratoriotilat, päätettiin liittää langattomaan verkkoon mukaan. Vanhan laitteiston kanssa näissä tiloissa ei ollut mahdollisuutta sen käyttöön.

Ennen laitteiden tilaamista käytiin ulkopuolisen konsultin kanssa läpi alustavasti, mihin paikkoihin tukiasemia kannattaisi harkita. Kierroksen jälkeen päädyttiin noin kymmenestä kahteentoista laitteeseen riippuen siitä miten paljon uutta aluetta haluttiin peittää. Samalla pohdittiin taajuusalueita, autentikointia ja sitä, oliko tarvetta luoda erilliset verkot työntekijöille ja vieraille.

Loppujenlopuksi tukiasemia tilattiin 12 kappaletta. Näin varmistettiin, että langaton verkko ulottuu paikkoihin, joissa sitä ei ennen ollut. Päätettiin käyttää PoE-tekniikkaa antamaan virta ja verkko yhdellä johdolla kaikille laitteille.

4 ARUBA INSTANT WI-FI

Verkkoratkaisuksi valittiin Aruba Instant Wi-Fi. Tämä ratkaisu oli halvin, sillä erillistä ohjainta ei tarvita tukiasemille. Vertailevana tarjouksena oli Merun verkkoratkaisu, joka oli selkeästi kalliimpi tukiasemien ohjaimen takia.

Aruban tapauksessa jokainen tukiasema voi toimia ohjaimena koko verkolle. Jos ohjaimena toimiva tukiasema kaatuu, mikä tahansa muu tukiasema ottaa paikan sen tilalla automaattisesti. Tämä varmistaa, että verkko on käytettävissä ja sitä voi hallita niin kauan kun yksikin tukiasema on toimintakunnossa. (Aruba 2016, 2.)

Aruban oman esitteen mukaan sen laitteista koostuva verkko on korkeilla käyttäjämäärillä 36 % nopeampi kuin kilpailijoiden. Se mainostaa olevansa ainut ohjaimeton Wi-Fi -ratkaisu markkinoilla ja tarjoaa sisäisen RADIUS -palvelimen. Patentoitu ClientMatch -teknologia kerää käyttäjän istunnon aikana suorituskykydataa ja valitsee sen perusteella parhaimman tukiaseman jokaiselle käyttäjälle. Liikkuessa tukiasemat vaihtuvat parempaan katkaisematta yhteyttä. (Aruba 2016, 1.)

Verkkojen luonti ja hallinta tapahtuu keskitetyn hallintaympäristön kautta. Sieltä näkee mm. jokaisen tukiaseman tilan, mikä tukiasema toimii ohjaimena sekä yksityiskohtaista tietoa käyttäjien laitteista, jotka ovat kirjautuneena langattomaan verkkoon. Uusien tukiasemien lisääminen on tehty helpoksi: laite kytketään verkkoon ja se hakee automaattisesti ohjaimelta verkon yhteiset asetukset itselleen ja alkaa automaattisesti toimimaan osana järjestelmää.

4.1 Laitteet

Saadussa Aruban laitteiston tarjouksessa oli mukana kaksi laitevaihtoehtoa: 200-sarjan IAP 205 ja 210-sarjan IAP 215. Ohjainta ei tarjouksessa ollut, koska sitä ei tarvittu. Tukiasemiksi valittiin IAP 215. Tämän lisäksi tarvittiin erikseen seinäänkiinnityspaketti ja PoE-injektori virtaa varten jokaiselle tukiasemalle.

4.1.1 IAP 205

Aruban omista laitteista 200-sarjan IAP 205 on edullisin 802.11ac standardia käyttävä laite. Se antaa parhaimman suorituskyvyn keskikokoisissa ympäristöissä. 205:ssa on kaksi radiota ja se käyttää 5 GHz:n leveydellä 802.11ac standardia. Tällä on mahdollista päästä parhaillaan 867 Mb/s nopeuksiin. 2,4 GHz:n leveydellä käytetään vanhempaa 802.11n standardia,

joka antaa maksimissaan 300 Mb/s siirtonopeuden. Tukiasemaan saa kiinnitettyä yhteensä neljä ympärisäteilevää antennia, joiden käyttö parantaa suorituskykyä. Virransaannin voi halutessaan hoitaa PoE-tekniikalla.
(Aruba 2016, 4.; Aruba 2016, 1)

IAP 205 käyttää Aruban patentoimaa ClientMatch teknologiaa käyttäjän liikkuessa verkon ympäristössä. 200-sarjassa on mukana ACC eli Advanced Cellular Coexistence tekniikka, joka pyrkii minimoimaan mm. 3G ja 4G verkkojen häiriön. Jotkut kommunikaatiosovellukset, kuten Microsoft Lync, voidaan asettaa etusijalle suorituskyvyn suhteen. Videopuhelut, ääni, keskustelu sekä työpöydän jako-ominaisuus toimivat salattuna.

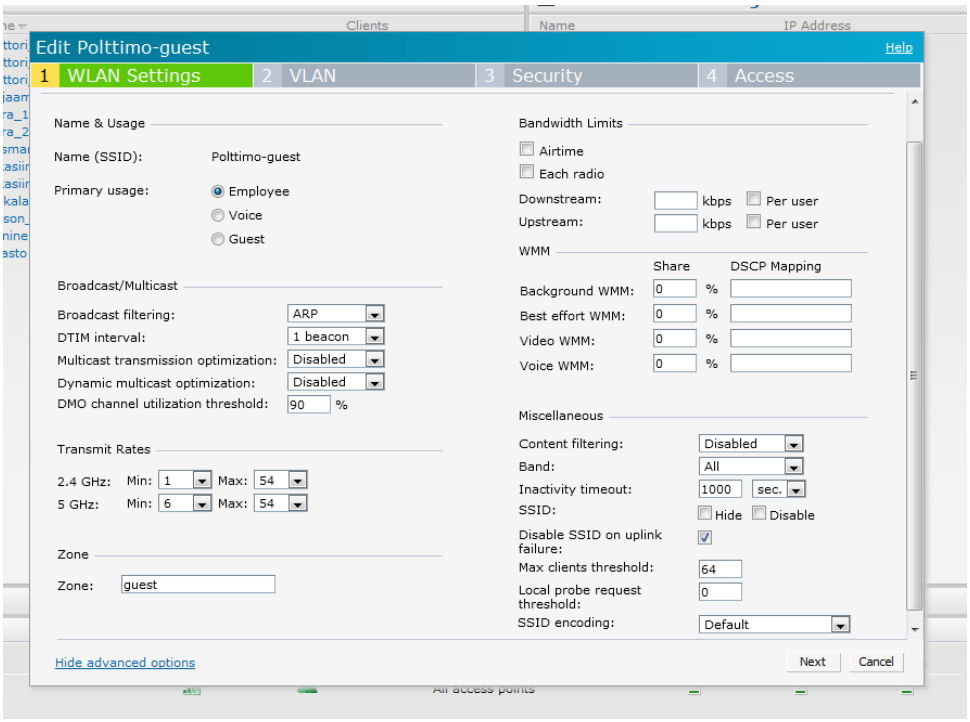
4.1.2 IAP 215

Suosituin Aruban tukiasema, joka käyttää 802.11ac standardia, on IAP215. Se on tarkoitettu keskikokoisille ympäristöille. 2,4 Ghz:n leveydellä käytetään n-standardia, jonka ansiosta maksiminopeus on 450 Mb/s. 5 GHz:n leveydellä ac-standardi mahdollistaa jopa 1.3 GB/s siirtonopeudet. Tukiasemiin saa yhdistettyä enintään kuusi yleissuuntaista antennia. Muut ominaisuudet ovat hyvin samanlaisia 205-malliin verrattuna.
(Aruba 2016, 4.; Aruba 2016, 2.)

4.2 Luonti ja hallinta

Aruban web-käyttöliittymään pääsee käsiksi ottamalla selainyhteyden verkon ohjaimen IP-osoitteeseen ja kirjautumalla sisään. Pääsivulta näkee luodut verkot, tukiasemat ja verkossa olevat käyttäjät. Uusien verkkojen luominen ja asetusten määrittely niin tukiasemiin kuin verkkoihin tehdään pääsivulta.

Uuden verkon luonti tehdään siihen tarkoitetulla ohjatulla työkalulla, joka käynnistetään luotujen verkkojen alta kohdasta ”New”. Tällöin aukeaa kuvan 6 mukainen ikkuna, josta uuden verkon luonti aloitetaan.

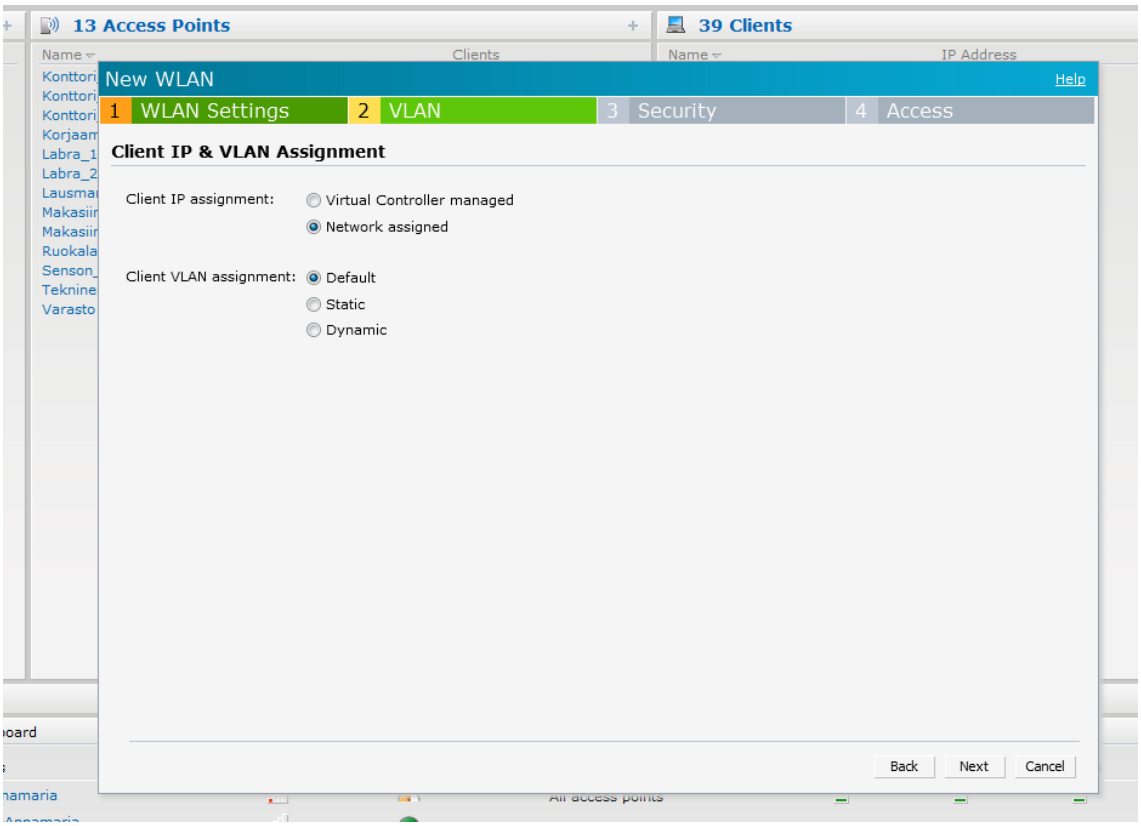


Kuva 6 Uuden WLAN verkon luomiseen käytettävä työkalu

Ensimmäisessä välilehdessä annetaan verkolle SSID-tunnus, jota verkko käyttää siitä lähtien. Verkolle valitaan myös sen pääkäyttötarkoitus (Employee, voice, guest). Jokainen vaihtoehto antaa myöhemmin uusia asetusvaihtoehtoja riippuen siitä minkä valitsee. Alareunasta saa näkyviin lisäasetukset, joista saa asetettua mm. ulos- ja sisääntulonopeudet käyttäjäkohtaisesti tai kokonaisuudessaan.

Seuraavassa välilehdessä (Kuva 7) voidaan määritellä mihin VLAN:iin laitteet kuuluvat ja minkä IP-osoitteen ne saavat verkossa. Jos valitaan että ohjain hoitaa IP-osoitteiden jakamisen, IAP itse saa DHCP-palvelimelta oman osoitteen ja jakaa muille käyttäjille heidän osoitteensa. Käyttäjien osoitteet lähetetään takaisin IAP:lle käyttäen NAT-tekniikkaa.

Jos halutaan, että kiinteä verkko hoitaa osoitteet, valitaan Network Assigned. Default -vaihtoehto antaa käyttäjälle saman IP-osoitteen samasta VLAN:sta kuin IAP on. Static -vaihtoehto antaa mahdollisuuden antaa käyttäjille eri VLAN:sta IP-osoitteen riippuen siitä mihin SSID:hen on kytköksissä. Dynamic -vaihtoehto antaa osoitteet käyttäjille verkon valvojan asettamien sääntöjen mukaisesti.

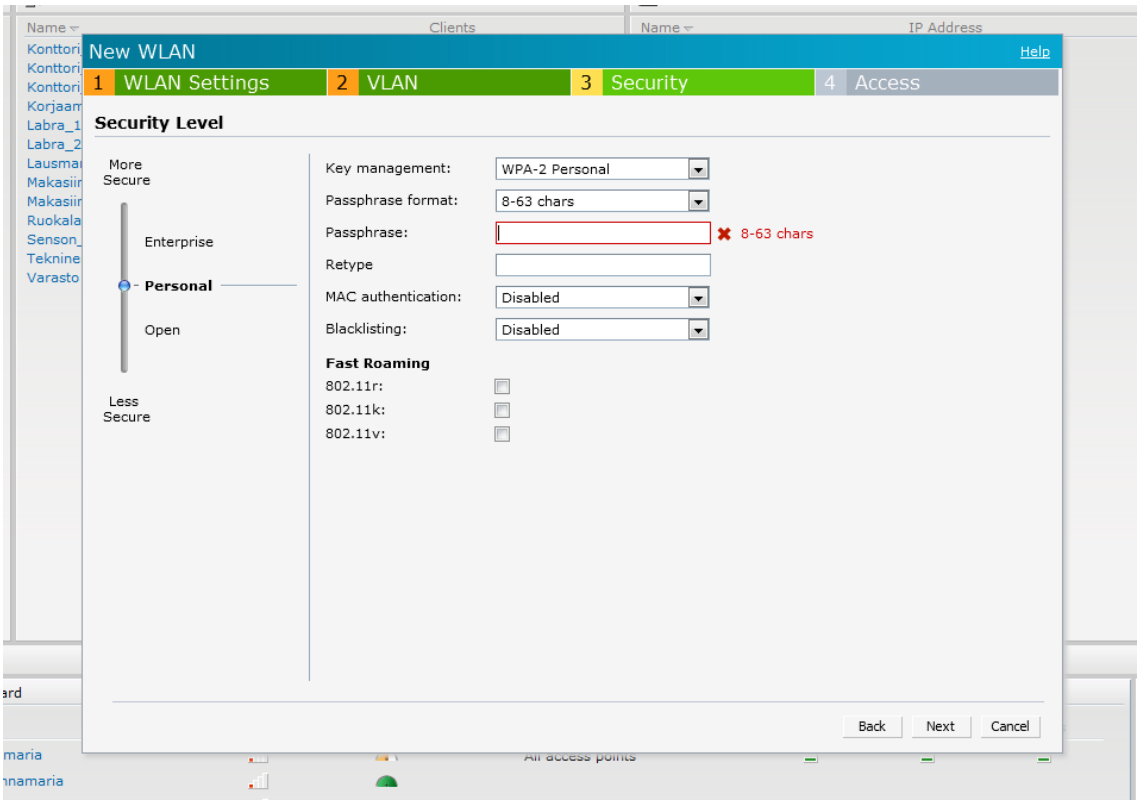


Kuva 7 Asetukset VLAN ja IP osoitteiden määrittelyyn

Security -välilehdellä (kuva 8) määritellään, miten verkkoon kirjaudutaan. Open tasolla SSID:n voi jättää avoimeksi halutessaan, jolloin kuka tahansa voi liittyä langattomaan verkkoon ilman tunnistautumista. Tällä tasolla voi määritellä mm. MAC-tunnistautumisen ja listan laitteista, jotka eivät saa liittyä verkkoon.

Personal tarjoaa tutuimman kirjautumistavan: salasanan. Verkon hallinnoija valitsee salausavaimeen käytettävän tekniikan ja antaa salasanan verkolle. Personal tasolla voidaan käyttää MAC -tunnistautumista Open tason tavoin.

Enterprise -tasolla käytetään erillistä tunnistautumispalvelinta, esimerkiksi RADIUS -palvelinta. MAC-tunnistautumiseen saa tällä tasolla myös uusia ominaisuuksia: sen voi asettaa tueksi 802.1x autentikoinnille. Salausavaimiin tulee mukaan Enterprise versiot WPA ja WPA2 -tekniikoista.
Verkkoon voi asettaa käyttäjille aikarajan, jonka umpeuduttua heidät pakotetaan kirjautumaan uudelleen verkkoon. Enterprise tasolla verkosta saa erittäin tietoturvallisen, mutta verkon hallinnoijan täytyy olla varovainen, ettei käytettävyys laske liian tiukkojen määrittelyjen seurauksena.



Kuva 8 Security välilehti työkalussa

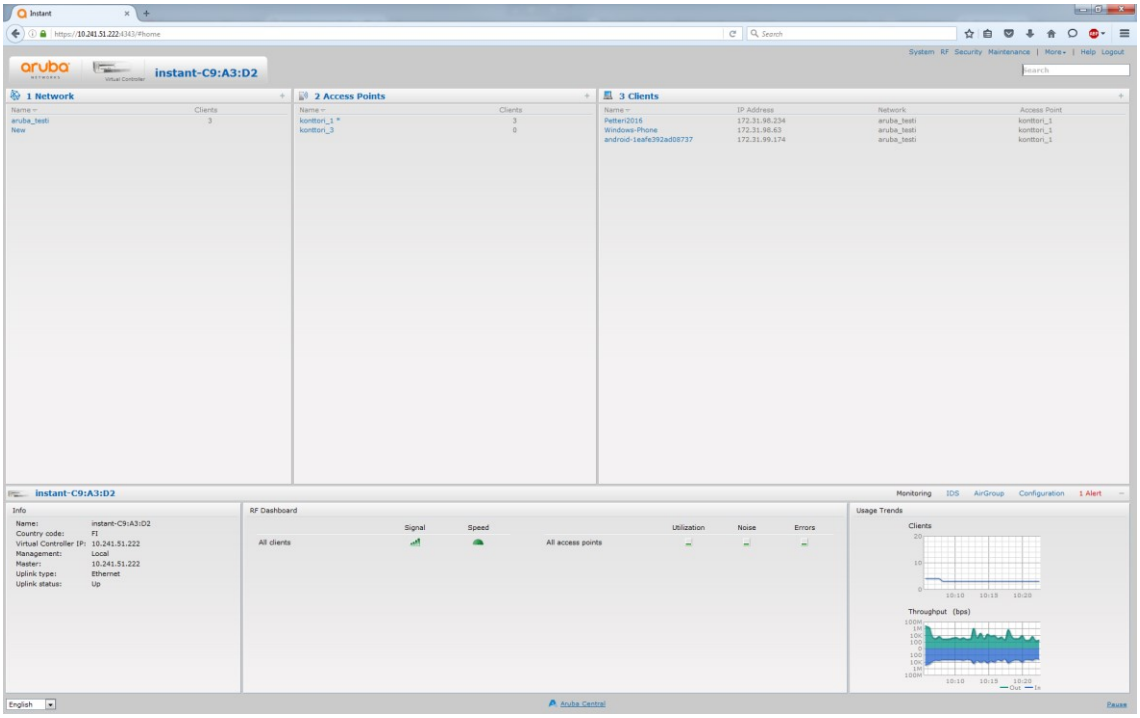
Viimeinen välilehti käsittelee palomuurisääntöjä. Vaihtoehtoja on kolme: Unrestricted, Network-based ja Role-based. Jos valitaan rajoittamaton pääsy, kuka tahansa voi liittyä verkkoon. Verkkoon täytyy kuitenkin tunnistautua normaalisti, jos edellisellä välilehdellä on niin määritelty. Verkkoon pohjautuvat säännöt koskevat tiettyä SSID:tä, jossa säännöt ovat sama. Roolipohjaisessa mallissa sen sijaan määritellään eri rooleja omilla säännöillään ja käyttäjien laitteet liitetään näihin rooleihin. Tähän usein tarvitaan erillinen palvelin.

4.2.1 Hallinta

Aruba Instantin graafisen web-käyttöliittymän pääsivu (Kuva 9) on jaettu neljään eri osaan: verkot, tukiasemat, käyttäjät sekä sivun alareunassa info-osioon. Info-osiosta näkee yksityiskohtaista tietoa joko tukiasemien muodostamasta klusterista, verkoista, tukiasemista tai käyttäjistä.

Jos halutaan saada laajempaa tietoa verkoista, tukiasemista tai käyttäjistä, haluttu osio laajennetaan klikkaamalla sitä. Esimerkiksi, jos halutaan tarkastella käyttäjiä tarkemmin, laajennetaan käyttäjät osio. Tällöin käyttöliittymä näyttää jokaisen käyttäjän IP- ja MAC-osoitteet, laitteen mallin, mihin SSID:hen ja tukiasemaan on yhteydessä, radiokanavan ja tyypin, roolin verkossa sekä nopeuden.

Yksittäistä käyttäjää voi tarkastella valitsemalla käyttäjän. Tällöin käyttöliittymän alareunassa oleva info-osio näyttää valitun käyttäjän tietoja, kuten signaalin voimakkuuksista, suoritustehosta ja kuinka kauan laite on ollut liittyneenä verkkoon.



Kuva 9 Web-käyttöliittymän pääsivu

Käyttöliittymän oikeassa yläreunasta pääsee vaihtamaan itse klusterin (System), radiosignaalin (RF), tietoturvan (Security) asetuksia sekä tekemään etänä huoltotöitä tukiasemille (Maintenance): esimerkiksi käynnistämään niitä uudelleen tai ajamaan uudet päivitykset tukiasemien käyttöjärjestelmille.

5 VALMIIN VERKON TARKASTELU

Tukiasemien testaamisen jälkeen uusi langaton verkko saatiin täysin käyttövalmiiksi ja kaikki vanhat reitittimet ja niiden verkot saatiin poistettua ympäristöstä. Vaihto onnistui pääosin hyvin, eikä vanhojen WLAN:ien puuttuminen haitannut työntekoa. Kaikkia tukiasemia ei saatu asennettua täysin samoille paikoille, kun oli alun perin suunniteltu. Kaikki tilatut laitteet saatiin kiinnitettyä ja kytkettyä, eikä verkon suorituskyky tai laajuus kärsinyt uusista paikoista huolimatta merkittävästi.

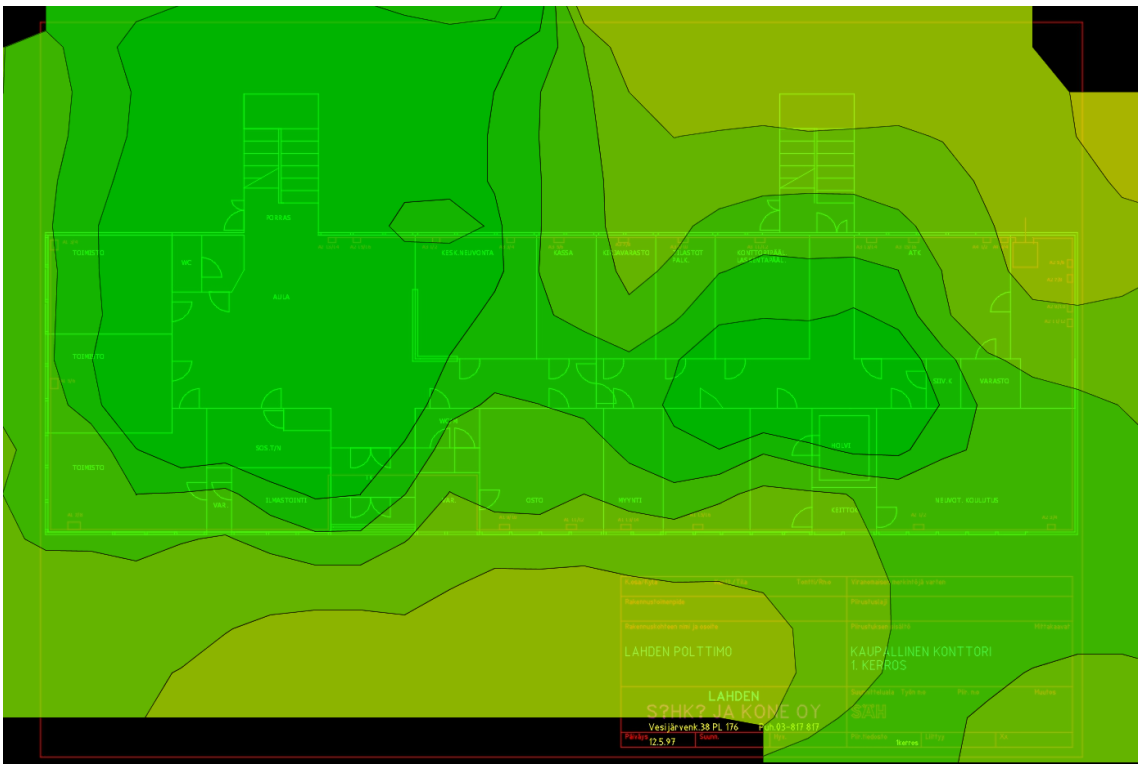
Langatonta lähiverkkoa saatiin stressitestattua Viking Maltin vuosittaisen tapaamisen avulla. Parhaillaan verkossa oli yli 50 eri laitetta. Tukiasemat osasivat jakaa käyttäjien laitteet hyvin parasta yhteyttä silmällä pitäen eikä yksikään kyseisistä tukiasemista kaatunut. Käyttäjien mukaan verkko toimi nopeammin, luotettavammin ja laajemmin kuin ennen.

Myöhemmin verkkoon lisättiin vielä yksi tukiasema lisää. Kuten Aruba oli luvannut, uuden tukiaseman tuominen verkkoon sujui helposti. Heti saatuaan virran laite alkoi etsiä verkolleen ohjainta ja löydettyään sen, WLAN:in mainostus alkoi automaattisesti muutaman minuutin kuluttua.

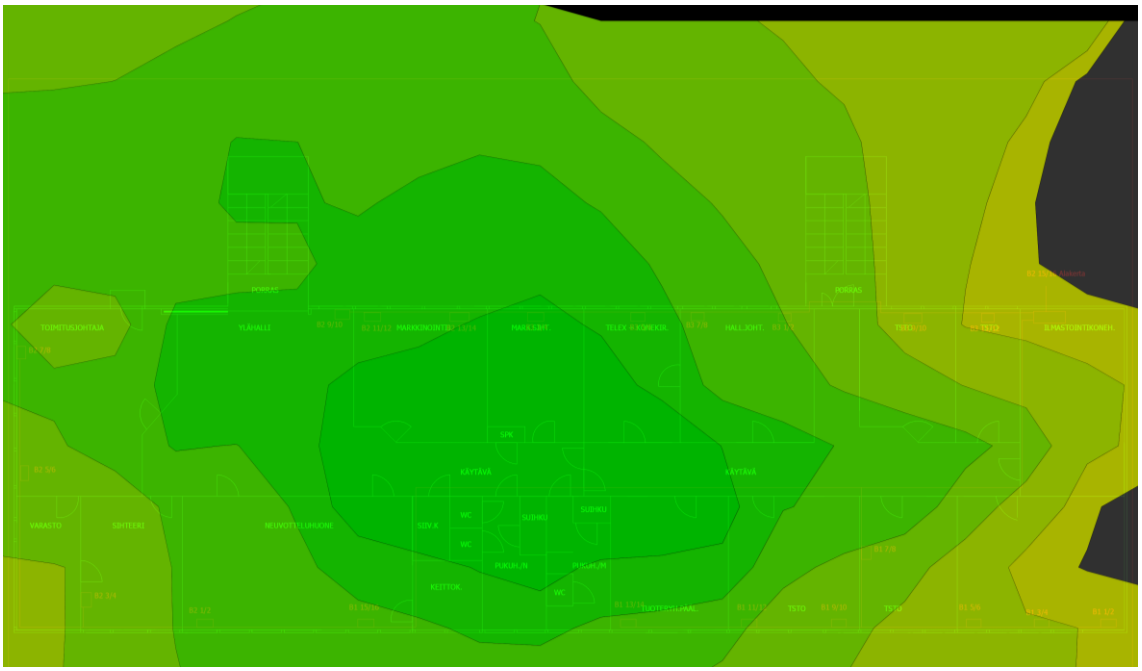
5.1 Verkon esittely

Tukiasemiksi valikoitui Aruban IAP-215, joita tilattiin yhteensä 12 kappaletta. Ne levitettiin tasaisesti ympäri aluetta rakennuksiin, joissa langatonta verkkoa tarvittiin: pääkonttoriin, makasiiniin, korjaamolle, varastolle, tekniseen toimistoon, laboratoriotiloihin ja uutetehtaan kokoustiloihin. Näistä paikoista vain pääkonttorissa, makasiinissa ja teknisessä toimistossa oli ennen pääsy langattomaan verkkoon. Kaikki uudet tukiasemat ovat yhteydessä toisiinsa pääkonttorilla sijaitsevan, ensisijaisen, ohjaimen kautta. Uutetehtaalla tarvittiin langatonta verkkoa pääosin vain yhteen kokoushuoneeseen. Yksi tukiasema sijoitettiin sinne.

Pääkonttori sai kolme tukiasemaa, joista kaksi on ala-kerrassa ja yksi yläkerrassa. Tärkeimmät paikat olivat kokoustilat, joita löytyy molemmista kerroksista. Alustavien mittausten perusteella valittiin paikat, joissa signaali kulkisi ensimmäisestä kerroksesta toiseen vaimentumatta paljon. Tukiasemat pyrittiin kiinnittämään katonrajaan, jotta signaali pääsisi mahdollisimman esteettömästi etenemään tiloissa. Kuvista 10 ja 11 näkyy, että molemmissa kerroksissa saa lähes kaikkialla hyvän signaalin.

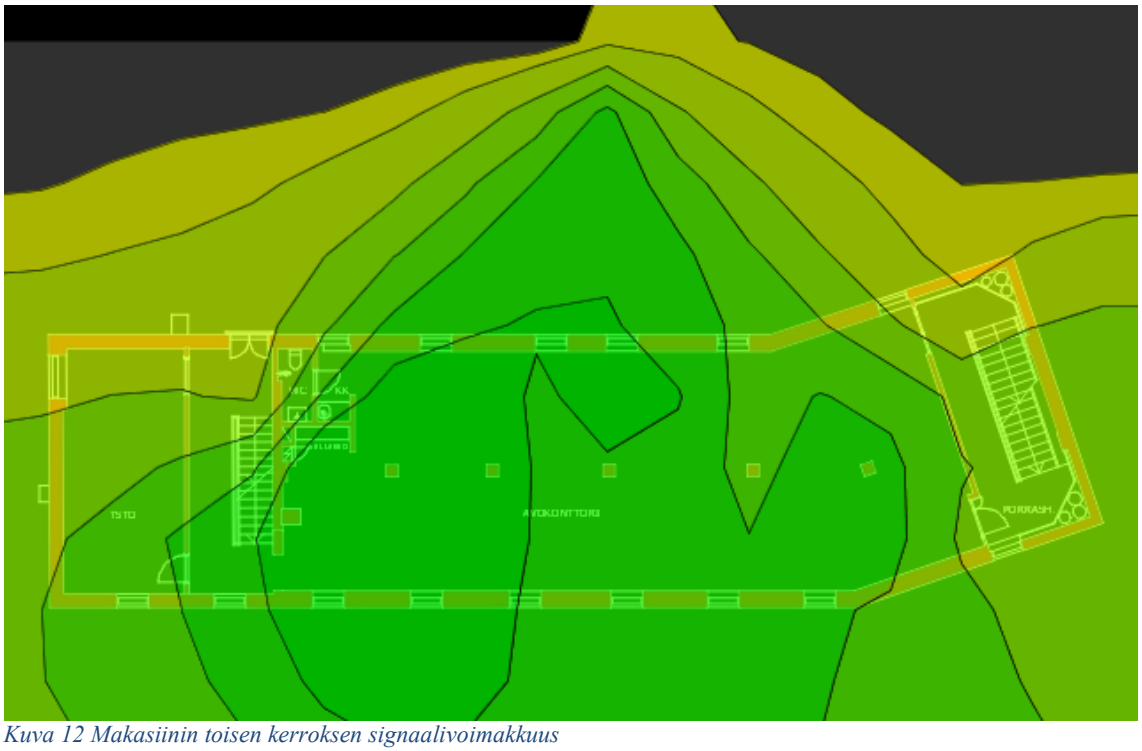


Kuva 10 Pääkonttorin ensimmäisen kerroksen signaalivoimakkuus

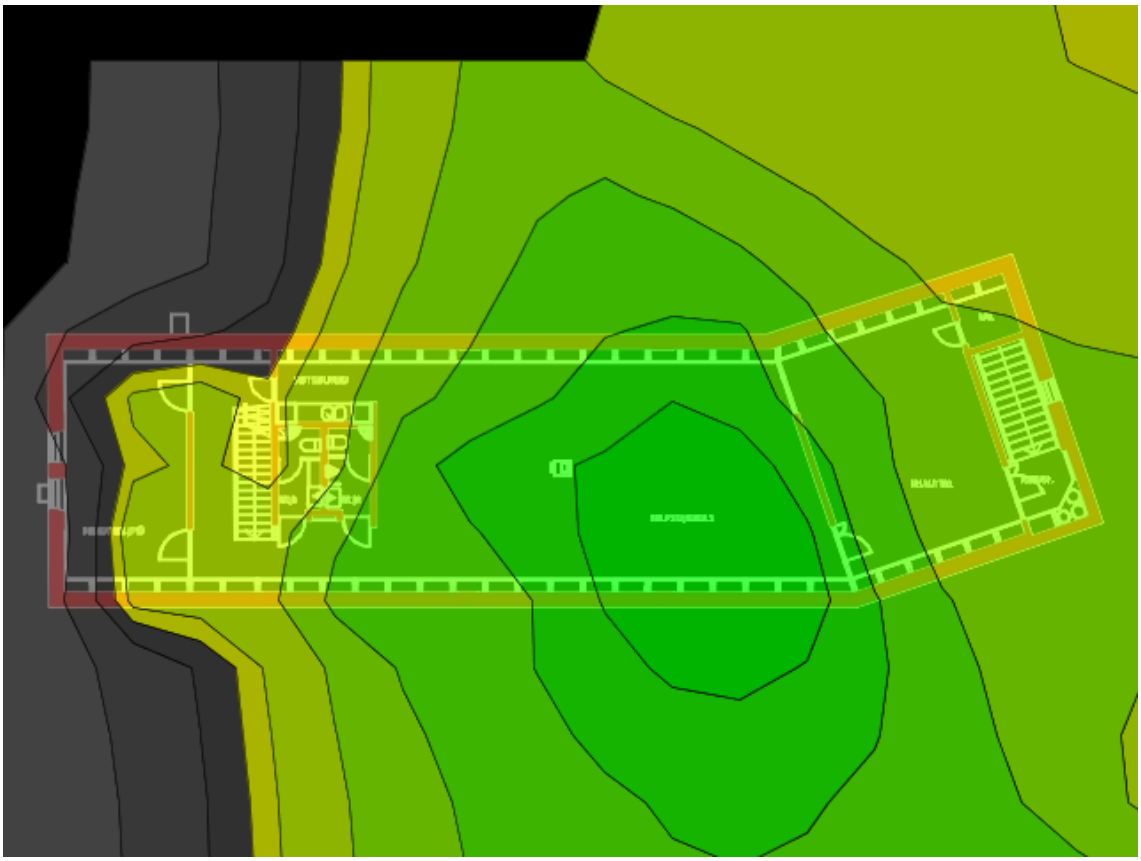


Kuva 11 Pääkonttorin toisen kerroksen signaalivoimakkuus

Makasiini (kuvat 12 ja 13) sai yhteensä kaksi tukiasemaa, jotka sijaitsevat toisessa ja kolmannessa kerroksessa. Kolmannessa kerroksessa oleviin kokoustiloihin oli tärkeää saada hyvä signaali ja siellä tukiasema sijoitettiin kattoon, jotta signaali leviäsi isolle alueelle. Toisessa kerroksessa ei ennen ollut erikseen tukiasemaa ja langaton verkko toimi parhaillaan heikosti kolmannen kerroksen tukiaseman kautta. Signaalin leviämistä vaikeuttivat paksut betoniseinät ja pylväät.

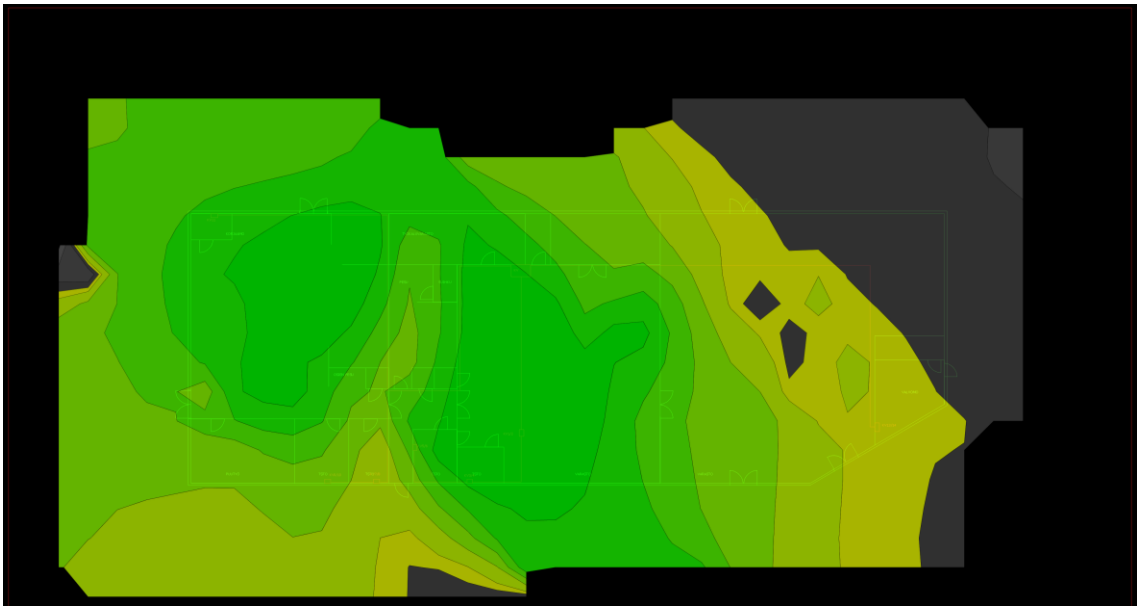


Kuva 12 Makasiinin toisen kerroksen signaalivoimakkuus



Kuva 13 Makasiinin kolmannen kerroksen signaalivoimakkuus

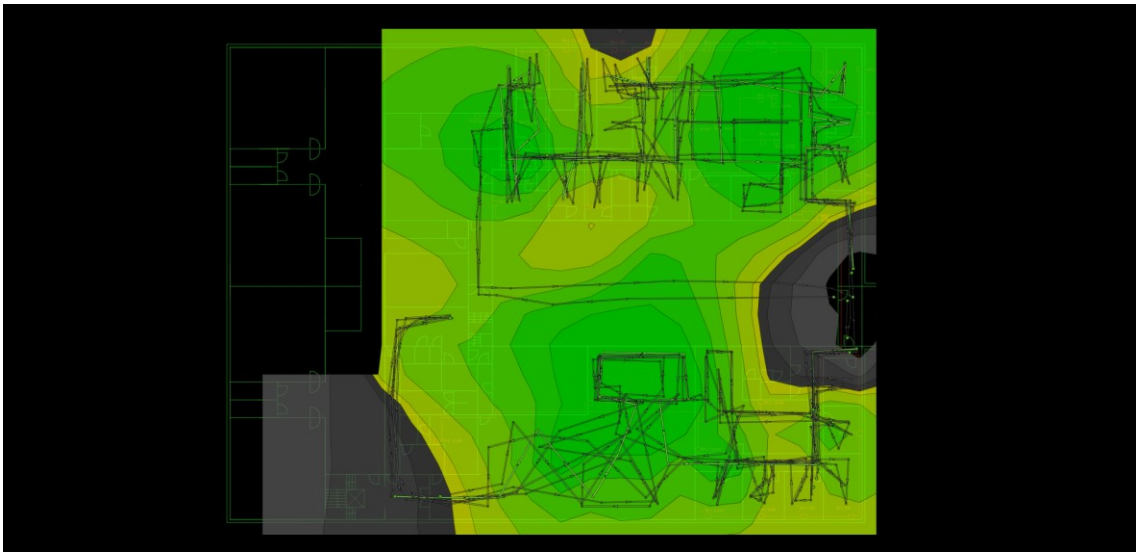
Korjaamolle ja varastolle tuli kaksi uutta tukiasemaa. Aluksi pohdittiin, tarvittiinko sinne ollenkaan langatonta verkkoa, mutta lopulta päädyttiin tekemään kerralla perusteellinen ja kattava verkko. Myös näissä kohteissa töitä tekevät käyttäjät olivat toivoneet saavansa langattoman verkon käyttöönsä. Isot hyllyt ja paksut betoniseinät haittasivat jälleen signaalin kulkua, mikä näkyy selvästi kuvassa 14.



Kuva 14 Korjaamon ja varaston signaalivoimakkuus

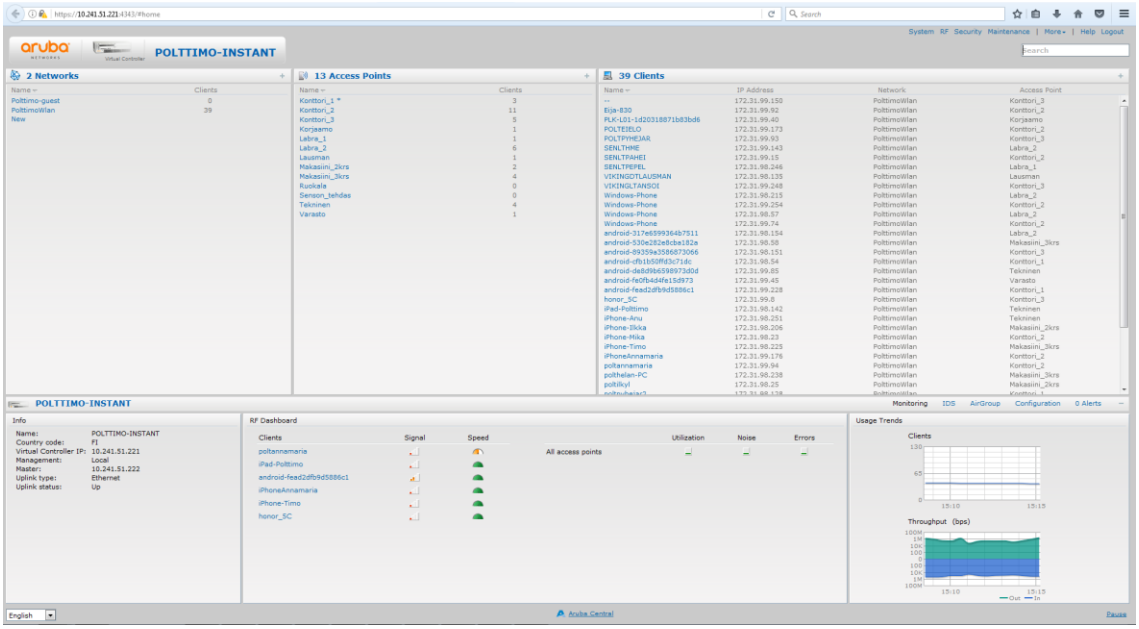
Tekniseen toimistoon tuli kaksi tukiasemaa, jotka sijoitettiin kokoushuoneisiin. Toimiston vieressä olevaan ruokalaan piti myös saada langaton verkko, joten lähemmän kokoushuoneen tukiasema sijoitettiin siten, että sen signaali pääsee helposti ruokalan tiloihin. Toimiston puolella oleva fyysinen arkistointitila haittasi signaalin etenemistä osaan työhuoneista.

Laboratoriotiloihin kytkettiin niin ikään kaksi tukiasemaa: kumpaankin päähän yksi. Näissä tiloissa ei ennen ollut langattomaan verkkoon pääsyä. Betoniseinät haittasivat signaalin etenemistä hieman. Kuvassa 15 näkyy signaalivoimakkuuden lisäksi reitit, joilla langattoman verkon signaalinvoimakkuutta mitattiin teknisen toimiston ja laboratorion tiloissa.



Kuva 15 Teknisen toimiston ja laboratoriotilojen signaalinvoimakkuus

Työntekijöiden ja vieraiden verkon erittelyä ei katsottu tarpeelliseksi opinnäytetyön aikana. Kirjautuminen verkkoon tapahtui samalla tavalla kuin ennen: salasanalla. Kaikille tukiasemille varattiin kiinteät osoitteet fyysisestä verkosta ja DHCP -palvelin jakoi käyttäjille omat IP-osoitteet. Vieraille lisättiin myöhemmin oma verkko, johon he voivat kirjautua. Tämän lisäksi yksi tukiasema lisättiin yhteen valvomoista, mikä nostaa verkon tukiasemien määrän 13:een. Kuvassa 16 näkyy Polttimon valmis verkko Aruban omassa web-käyttöliittymässä.



Kuva 16 Web-käyttöliittymä Polttimon verkossa

6 POHDINTA

Keskitetysti hallittavat WLAN-verkot ovat käytännöllisempiä kuin yksittäisten tukiasemien tarjoamat verkot. Polttimon langattoman verkon käytettävyys, tavoitettavuus ja tietoturva kasvoivat huomattavasti Aruban verkkoratkaisuun siirtymisen jälkeen. Hallinta on helpompaa ja verkon laajentaminen käy yksinkertaisesti.

Vaikka tavoitteisiin päästiin, työssä on kehitettävää. Perusteellinen dokumentaatio verkosta, sen rakenteesta ja hallinnasta, olisi helpottanut kaikkia osapuolia. Raportin kirjoittaminen osoittautui osittain hankalaksi, sillä verkkoon tehtyjä muutoksia ei dokumentoitu laajamittaisesti. Esimerkiksi kuvat kehittyvästä verkosta olisivat auttaneet.

Aikataulullisesti työ saatiin valmiiksi ajoissa. Toisaalta, jos verkko olisi saatu toimintakuntoon aikaisemmin, sen asetusten määrittelyyn ja toimintaan olisi voinut vaikuttaa enemmän. Tietoturvaa olisi voitu parantaa määrittelemällä vieraille ja Polttimon työntekijöille omat verkot ja niihin omat autentikointijärjestelmät. Hallintaa olisi voinut tarkastella paremmin, mikä olisi ollut opiskelijalle, mutta myös verkon uusille hallinnoijille, hyödyllistä. Tässä olisi dokumentointi ollut entistä tärkeämpää.

Tukiasemien paikat olisivat teoriassa voineet olla paremmat. Mittauksiin ei aina voi luottaa, etenkin, kun käyttää testilaitteena eritasoista tukiasemaa, kuin valmiiseen verkkoon on ajateltu. Joka tapauksessa tosiasia on, että paikoituksen optimointia voi tehdä loputtomiin, eikä suorituskyvyltään ja peittävyydeltään paras vaihtoehto ole käytännössä paras tai välttämättä edes mahdollinen.

Käyttäjiltä tulleen palautteen mukaan uusi verkko on toiminut hyvin, eikä ongelmia ole esiintynyt. Nopeus, saatavuus ja luotettavuus ovat paljon parempia kuin ennen ja käyttäjät ovat olleet tyytyväisiä uuteen langattomaan verkkoon. Verkon hallinnoijat ovat tuntuneet olleen tyytyväisiä ja verkon laajentamisessa tai hallinnassa ei ole esiintynyt ongelmia.

Tätä opinnäytetyötä voisi laajentaa ottamalla vertailuun mukaan verkkoratkaisun toiselta valmistajalta. Vertailua voisi tehdä mm. laitteistosta, suorituskyvystä ja hallintajärjestelmästä. Langattoman verkon voi myös toteuttaa eri tavalla eri laitteistolla. Olisi mielenkiintoista nähdä, miten laitteisto ja erilainen suunnittelu verkon suhteen vaikuttavat sen toimivuuteen. Vertailua voisi tehdä siitä, miten paljon yritykset satsaavat langattomaan verkkoon ja käyttävät hyväksi sen tuomia mahdollisuuksia. Ovatko yritykset kallistumassa enemmän keskitettyihin verkkoihin vai luottavatko he edelleen vanhoihin malleihin?

LÄHTEET

Aruba 2016. Aruba 210 Series Data Sheet. Haettu 1.12.2016 osoitteesta http://www.arubanetworks.com/products/networking/access-points/210-series/

Aruba 2016. Aruba 200 Series Data Sheet. Haettu 1.12.2016 osoitteesta http://www.arubanetworks.com/products/networking/access-points/200-series/

Aruba 2016. Solution Overview . Haettu 18.11.2016 osoitteesta http://www.arubanetworks.com/products/networking/aruba-instant/

Geier, J. (2005). *Langattomat lähiverkot: perusteet.* Helsinki: Edita Prima Oy

Hovatta, T. (2005). *Wlan-tekniikat ja – käyttösovellukset toimitilakiinteistossä*. Espoo: Sahköinfo

IEE Std 802.11n™-2009 (2009). Enhancements for Higher Throughput. IEEE Standards Association. 1.12.2016 https://standards.ieee.org/

IEE Std 802.11ac™-2013 (2013). Enhancements for Very High Throughput for Operation in Bands below 6 GHz. IEEE Standards Association. 1.12.2016 https://standards.ieee.org/

Instant Training. Aruba. Haettu 25.1.2016 osoitteesta http://www.arubanetworks.com/products/networking/aruba-instant/training/instant-training/

Puska, M. (2005). *Langattomat lähiverkot*. Helsinki: Talentum Media Oy