Tampereen ammattikorkeakoulu

LANGATTOMAN LÄHIVERKON MITTAUS JA OPTIMOINTI

Joonas Kotajärvi

OPINNÄYTETYÖ
Helmikuu 2020

Tieto- ja viestintätekniikka
Tietoliikennetekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutusohjelma
Tietoliikennetekniikka

KOTAJÄRVI, JOONAS:
Langattoman lähiverkon mittaus ja optimointi

Opinnäytetyö 65 sivua, joista liitteitä 18 sivua
Maaliskuu 2020

Opinnäytetyön taustana oli se, että yritys oli ilmoittanut ja heillä oli havaittu ongelmia langattoman verkon toimivuudessa useassa paikassa heidän rakennustaan. Tarkoituksen oli kartoittaa langattoman lähiverkon kuuluvuus ja tuottaa siitä kunnollinen raportti, jonka pohjalta voitiin tehdä korjaavia muutoksia, jotta langattomasta verkosta saataisiin toimivampi. Tehtävänä oli tutkia, millä laitteistolla tai ohjelmistoilla mittaukset saataisiin suoritettua, sekä minkälaisia erilaisia mittauslaitteistoja ja ohjelmistoja on olemassa. Aikaisempaa kokemusta langattoman verkon mittauksista ei ollut, joten laitteita sekä ohjelmistoja jouduttiin melko tarkkaan tutkimaan. Lopullisen mittausohjelmiston valintaan vaikuttivat tiukka aikataulu, sekä valitun mittalaitteiston hankintahinta. Ongelmana mittauksissa ja mittausraportin tulkitsemisessa oli se, että raportissa oli todella paljon uusia käsitteitä, joita jouduttiin paljon opettelemaan ennen kuin ymmärsi tulokset riittävällä tasolla, jotta tarvittavat verkkoa parantavat muutoksen pystyttiin suorittamaan.

Asiasanat: WLAN, mittausraportti, kuuluvuuskartta, optimointi

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

KOTAJÄRVI JOONAS:
Measuring and Optimising Wireless Network

Bachelor's thesis 65 pages, appendices 18 pages
March 2020

The background to this thesis was that the company had reported that they have problems with the wireless network in several places around their building. The purpose was to measure the wireless network's coverage and produce a proper report that could be used to make corrective changes and make the network more functional. The task was to investigate which measurement hardware or -software could be best for this type of measuring and what kinds of measuring equipment and -software's exist. There was no previous experience with wireless network measurements, so hardware and software had to be studied quite closely. The choice of the final measurement software was selected because we had a tight schedule and the purchase price of the selected measuring equipment was good for us as well as the customer.

From the measurement report we founded that WLAN channels were poorly distributed, meaning that almost all radios were on the same channels at both 2.4 GHz and 5 GHz frequencies. In addition, in the measurement report we found that there were bad encryption algorithms that needed to be disabled to prevent network break-in. The report also showed that the coverage of some of the areas was very low. The customer was advised to acquire new WLAN access points in these places because the old equipment could no longer be upgraded to meet today's standards. Based on the measurements and the measurement report, we were able to improve the performance of the wireless network at that location and the customer was very satisfied with the service they received.

Key words: Wi-Fi, measurement report, heatmap, optimization

SISÄLLYS

LYHENTEET JA TERMIT

WLAN / Wi-Fi	Wireless Local Area Network / Wireless Fidelity – Langaton lähiverkko
OSI-malli	Open Systems Interconnection Reference Model, kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
SSID	Service Set Identifier, Langattoman verkon tunniste, jolla tunnistetaan ja eritellään langattomat verkot
DSSS	Direct Sequence Spread Spectrum, Suorasekventointi
FCC	Federal Communications Commission, Yhdysvaltain telehallintovirasto
MIMO	Multiple-input and multiple-output. WLAN:ssa useamman antennin käyttöä
AES	Advanced Encryption Standard, Lohkosalausmenetelmä langattoman verkon salaukseen
NFC	Near Field Communication, Radiotekniikkaa hyödyntävä laitteiden kättely tekniikka
GPS	Global Positioning System, Satelliittipaikannusjärjestelmä
RSSI	Received signal strength indication, Ilmoittaa vastaanotetun signaalin vahvuuden.
MAC-osoite	Media Access Control. Verkkokortilla oleva oma fyysinen osoite, joka on fyysisesti kirjoitettu laitteen piirille.
BSSID	Basic Service Set Identifier, WLAN-tukiaseman radion tunniste
VLAN	Virtual Local Area Network – virtuaalilähiverkko
WEP	Wired Equivalent Privacy, Langattoman verkon salaustapa
EAP	Extensible Authentication Protocol, autentikointi protokolla, jota 802.1X autentikointi käyttää

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on perehtyä ja tutkia eri WLAN-standardeja, salaustapoja ja siirtotien ominaisuuksia. Tutustua siihen, kuinka WLAN-mittauksia tehdään ja kuinka mittausraportteja tulkitaan. Opinnäytetyö tarkentuu asiakkaan verkon kartoitukseen ja kartoitusdokumentin analysointiin. Lopuksi mittausten pohjalta tehdään tarpeellisia muutoksia, joilla saadaan parannettua asiakkaan langattoman verkon toimivuutta.

Opinnäytetyön tavoitteena on tuottaa asiakkaalle selkeä mittausraportti sekä avata sen käsitteet. Tavoitteena on myös tehdyn mittausraportin pohjalta ymmärtää, kuinka nykyistä langatonta verkkoa voidaan edelleen kehittää, sekä parantaa sen toimivuutta. Opinnäytetyö antaa selvitystä siitä, miten ratkaisut mahdollistavat molemmille osapuolille helpotusta langattoman verkon ylläpidossa sekä nykyisten toimintojen tehokkuuden lisäämistä.

Raportin laadinnassa, käytettiin hyödyksi teknisiä artikkeleita, valmistajien dokumentointia, uutisartikkeleita sekä kirjoittajan omaa alan ammattiosaamista. Kirjoittaja on opinnäytetyötä kirjoittaessaan ollut alan työtehtävissä lähes kuusi vuotta ja tekemisissä eri yrityksien järjestelmä- ja verkkoinfrastruktuurien ylläpito- ja hallintatehtävissä palveluntarjoajan roolissa.

2 LANGATON LÄHIVERKKO

Langattomalla lähiverkolla, WLAN:lla tarkoitetaan langatonta paikallista lähiverkkoa, jossa verkkoon kytketty reititin toimii tukiasemana ja muodostaa yhteyden lähiverkkoon. WLAN on tekniikka, jolla voidaan toteuttaa OSI-mallin mukainen siirtotie verkkolaitteiden välille. Langaton lähiverkko toteutetaan käyttämällä langattomassa reitittimessä olevaa radiolähetintä. WLAN standardeihin on määritetyt radiotaajuudet, joita voidaan käyttää. Taajuusalueet ovat 2,4GHz ja 5GHz. WLAN:in alkuvaiheissa oli käytössä pelkästään 2,4 GHz, ja vuonna 1999 IEEE:n 802.11a -standardin mukana tuli käyttöön myös 5GHz taajuus. (Tutorialspoint. 2019.)

Langaton reititin jakaa SSID:tä, jonka avulla langattomaan verkkoon liitytään. SSID on langattoman verkon tunniste, jonka avulla käyttäjä löytää langattoman verkon omalla tietokoneellaan, tabletilla, puhelimella tai muulla verkkoon liitettävällä laitteella. Tunnisteen avulla käyttäjä voi tietää mihin langattomaan verkkoon hän on yhdistämässä. Tunnisteen lisäksi langattomissa verkoissa on yleensä jonkinlainen salaus. Yleisimpiä WLAN-verkon salaustapoja on salasana sekä radius autentikaatio. Kauppakeskuksissa ja muissa vastaavanlaisissa tiloissa on yleensä myös vieraita varten avoin langaton verkko, jossa ei ole erillistä salausta. Silloin kyseessä on avoin langaton verkko, johon kuka vain voi yhdistää ilman salasanaa tai muuta autentikaatioita.

Langattomat lähiverkot ovat hyvä ratkaisu pienten ja suurten rakennusten verkottamiseen. Nykypäivänä langattomia lähiverkkoja on käytössä lähes joka paikassa, toimistoissa, kodeissa ja julkisilla alueilla. Niiden tietoturva ja suorituskyky on verrattavissa lankaverkkoon. Monet sovellukset tukevat nykypäivänä langatonta verkkoa. Protokollat ovat langattomissa lähiverkoissa itseasiassa hyvin samankaltaisia kuin Ethernet-verkossa. (Geier J 2005, 105)

2.1 Siirtotie

Langattomien ja langallisten verkkojen suurin ero on niiden siirtotiessä. Langallisissa verkoissa käytetään kaapelointia, jossa tieto siirretään sähköjännitteen muodossa. Langattomissa verkoissa data siirretään ilmateitse käyttäen radiotaajuus- eli RF-signaaleja. Radiotaajuus on sähkömagneettinen aalto, jota tietoliikennejärjestelmät käyttävät siirtämään dataa ilmateitse laitteesta toiseen. RF-signaalit etenevät lähettävän ja vastaanottavat laitteen antennien välillä. Antennista lähetettävällä kantoaallolla on yleensä jokin tietty amplitudi, taajuus ja vaihe. Edellä mainitut vaihtelevat ajan suhteen, ja niitä käytetään halutun informaation välittämiseen.

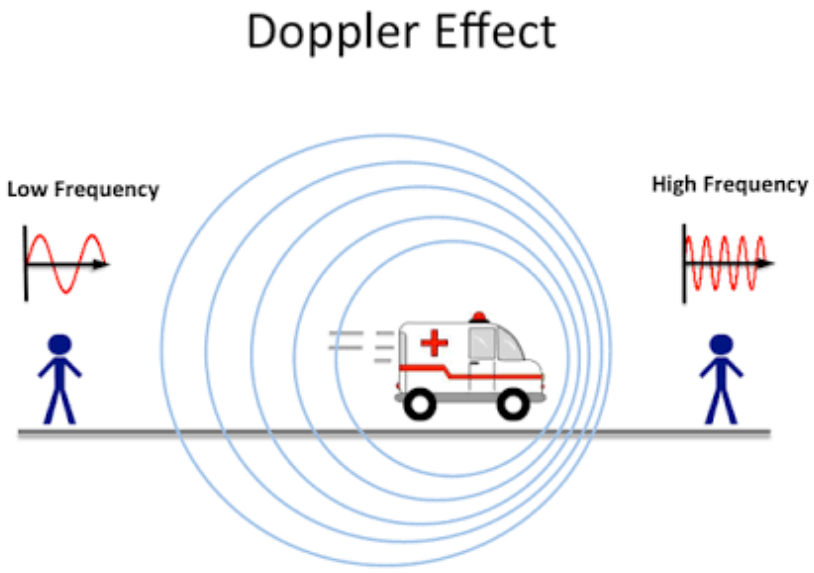
Amplitudia käytetään kertomaan RF-signaalin voimakkuus. Kun radiosignaali etenee ilmatiessä, se menettää amplitudia. Jos lähettäjän ja vastaanottajan välinen etäisyys kasvaa, signaalin amplitudi vähenee eksponentiaalisesti. Avoimessa, esteistä vapaassa tilassa RF-signaaleihin kohdistuu vapaan tilan vaimennus. Ilmakehän vaikutuksesta moduloitu signaali vaimenee eksponentiaalisesti mitä kauemmas se antennista etenee. Siksi signaalilla tulee olla tarpeeksi tehoa, jotta se saavuttaisi halutun etäisyyden tasolla, jota vastaanottaja edellyttää. Vastaanottajan kyky tunnistaa signaali riippuu kuitenkin myös siitä, kuinka paljon lähiympäristössä esiintyy muita langattomia RF-signaaleja. (Geier J 2005, 71)

Langaton siirtotie vaatii kantoaallon signaalin siirtämiseen. Esimerkiksi WLAN-verkko toimii 2,4 GHz:n taajuudella. Taajuus vaikuttaa signaalin kantamaan ja datan siirtonopeuteen. Mitä suurempi kantoaallon taajuus on, sitä enemmän kaistaa on käytettävissä, mikä puolestaan mahdollistaa suuremman tiedonsiirtonopeuden. Taajuuden kasvaessa signaalin kantama pienenee.

Vaihe kertoo signaalin poikkeamaa viitepisteestä. Joka signaalin värähdys kiertää 360 astetta. Signaalin vaihesiirto voi olla vaikka 90 astetta, mikä tarkoittaa, että poikkeama on yksi neljäsosa signaalista. Vaiheen muutos on hyvä tapa tiedon välittämisessä. Signaali voi esimerkiksi edustaa binääristä nollaa, kun vaiheensiirto on 45 astetta ja binääristä ykköstä kun vaiheensiirto on 90 astetta. Hyvä puoli datan esittämisessä vaiheensiirtoa käyttämällä on se, että ilmatiessä

vaikuttavat heikkoudet eivät juuri vaikuta vaiheensiirto tai sen tulkitsemiseen. Ne vaikuttavat yleensä vain amplitudiin ja taajuuteen.

Kun signaalia vastaanottava tai lähettävä laite liikkuu niin silloin langattomassa tiedonsiirrossa, tarvitsee ottaa huomioon dopplerin aiheuttama taajuuden vääristymä. Doppler-ilmiön aiheuttaa se, kun liikutaan tukiasemaa kohti tai siitä poispäin, niin tällöin vastaanotettavan signaalin taajuus hieman vääristyy. Tukiasemaa lähestyessä katoaallon taajuus kasvaa ja kauemmas mentäessä taajuus pienenee. Langattomassa lähiverkossa ei tosin usein liikuta kovin nopeasti niin dopplerin aiheuttama taajuuden vääristymä on melko pientä, vain muutamia hertsejä. Doppler-ilmiötä voidaan kuvata, vaikka sillä kun ambulanssi ajaa sireenit päällä ohi niin kun ambulanssi on tulossa kohti sinua niin ääni kuulostaa korkeammalta, mutta kun ambulanssi on mennyt ohitse niin sireenien ääni kuulostaa matalammalta (kuva 1).



KUVA 1. Doppler-ilmiö (Huawei Technologies Co. 2019)

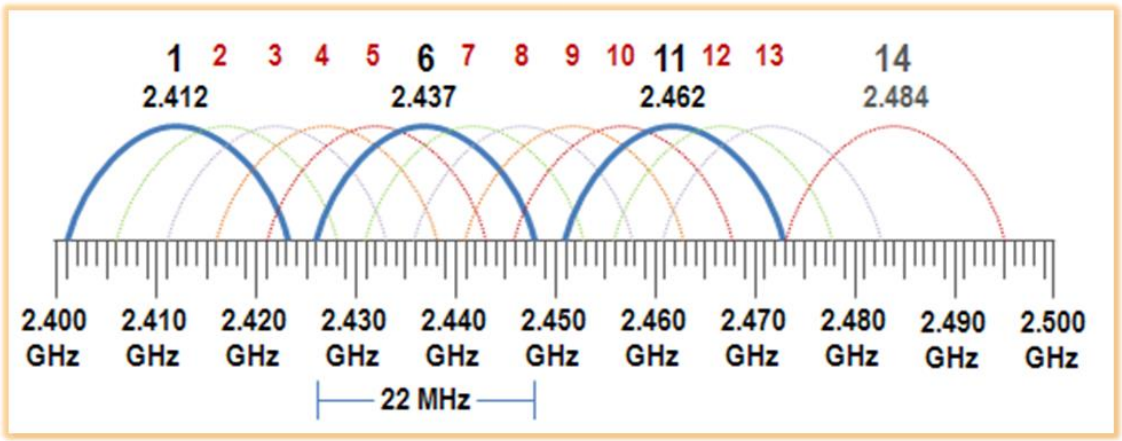
RF-signaalien vahvuuksina ovat suhteellisen pitkä kantama ilman kaapelointia. Kun taajuus kasvaa sade ja sumu vaimentavat signaalia enemmän, mikä puolestaan heikentää vastaanotettavaa signaalia. Heikkouksiin RF-signaaleissa on heikompi datan siirtonopeus, herkkyys muista laitteista aiheutuvasta häiriöstä sekä turvallisuus, koska kuka vain voi niitä kuunnella.

2.2 Taajuudet ja kanavat

WLAN käyttää reitittimessä olevaa radiolähetintä langattoman verkon yhteyden muodostukseen, joten sen tarvitsee käyttää joitain radioverkon taajuuksia signaalien lähettämiseen. WLAN:iin on standardoitu taajuudet 2,4 GHz ja 5 GHz IEEE 802.11-standardien mukaan. Molemmilla taajuuksilla on tiettyjä kanavia, jotka on myös standardisoitu.

2,4 GHz taajuudella on käytössä 14 kanavaa, joista yleisesti käytetään kolmea pääkanavaa. Pääkanavia ovat kanavat 1, 6 ja 11. 2,4 GHz WLAN:in kanavien kaistanleveys on 20 MHz ja yhden kanavan väli on 5 MHz. 2,4 GHz taajuusalue alkaa noin 2,400 GHz:stä ja päättyy noin 2,500 GHz:iin. 2,4 GHz taajuudella on myös mahdollista käyttää 40 MHz kanavaa, jolloin saadaan parempi kaistanleveys ja enemmän nopeutta langattomaan verkkoon, mutta jos käytetään 40 MHz kanavia, niin silloin tulisi käyttää vain kahta kanavaa, jotta ylikuulumista ei tulisi niin paljoa. Esimerkiksi kanavia 3 ja 9.

Kuvassa 2 on kuvattu 2,4 GHz WLAN-kanavien määrä ja niille määritetyt taajuudet. Kuvasta näkee myös sinisellä piirretyt pääkanavat, joita yleisesti tulisi käyttää. Pääkanavien käyttö estää sen, että viereisellä kanavalla olevat WLAN-verkot eivät häiritse toisia WLAN-verkkoja niin paljoa.



KUVA 2. 2,4 GHz WLAN kanavat ja taajuudet (Coleman, D. Extreme Networks. 2012.)

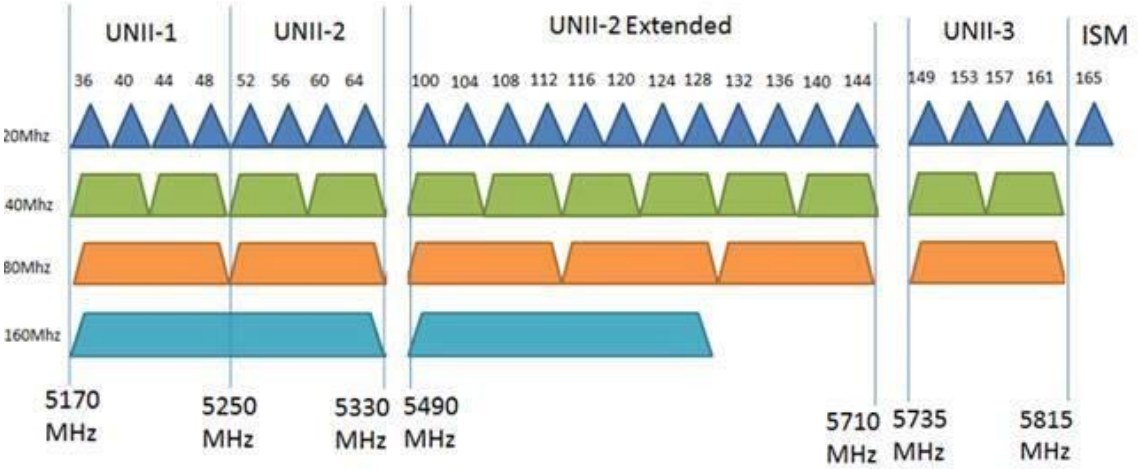
Taajuuksien allokoinnissa on myös hieman eroja ympäri maailmaa ja sääntelyviranomaiset asetettavat erilaisia vaatimuksia, joten kaikkia WLAN-kanavia ei ole saatavana kaikissa maissa tai maanosissa. Alla olevasta taulukosta näkee mitkä 2,4 GHz taajuudet ja kanavat on sallittu missäkin päin maailmaa (taulukko 1).

TAULUKKO 1. 2,4 GHz WLAN:in sallitut kanavat ja taajuudet alueittain. (Electronicsnotes. 2019.)

Kanava numero	Taajuus	Eurooppa	USA ja Kanada	Japani
1	2412 MHz	x	x	x
2	2417 MHz	x	x	x
3	2422 MHz	x	x	x
4	2427 MHz	x	x	x
5	2432 MHz	x	x	x
6	2437 MHz	x	x	x
7	2442 MHz	x	x	x
8	2447 MHz	x	x	x
9	2452 MHz	x	x	x
10	2457 MHz	x	x	x
11	2462 MHz	x	x	x
12	2467 MHz	x		x
13	2472 MHz	x		x
14	2484 MHz			802.11 b ainoastaan

5 GHz taajuudella on huomattavasti enemmän kanavia käytössä, ja siellä voidaan käyttää jopa 80MHz tai 160MHz kanavia, jolloin saadaan kaistaleveyttä vielä huomattavasti enemmän. Toki, kun käytetään suurempaa kaistanleveyttä niin silloin kanavat menevät helpommin päällekkäin, mikä saattaa aiheuttaa ongelmia muilla kanavilla. 5 GHz:lle on myös standardisoitu omat kanavat, joita käytetään, ja ne on esitetty kuvassa 3. Kuvasta voidaan nähdä se, että tällä taajuusalueella kanavien määrä on huomattavasti laajempi, jolloin on enemmän valinnan varaa, eikä tule niin helposti ylikuulumista toisten WLAN-verkkojen kanssa (kuva 3). Yleisesti nykypäivän WLAN-reitittimet ja -tukiasemat osaavat valita kanavansa automaattisesti sen mukaan millä kanavalla on vähiten häiriötä, mutta jois-

sain tapauksissa on hyvä käydä paikan päällä mittaamassa kuinka paljon kanavilla on ruuhkaa, ja sen mukaan valita WLAN-lähettimellä parhaat kanavat käyttöön. 5 GHz:n taajuusalueella käytetään 20 MHz:n jakoa, jolloin käytössä on vain joka neljäs kanava, ja siten voidaan välttää 2,4 GHz:n taajuutta vaivaavat päällekkäisyydet.



KUVA 3. 5 GHz WLAN-kanavat ja -taajuudet (Zak, R. Maketecheasier. 2017.)

3 LANGATOMAN LÄHIVERKON TEKNOLOGIAT – IEEE 802.11

IEEE 802.11 viittaa standardisarjaan, joka määrittelee tiedonsiirron langattomille lähiverkoille. Toisin sanoen IEEE 802.11 on joukko teknisiä ohjeita langattoman verkon toteuttamiseksi. Tuotteiden myyntiä tällä tavaramerkillä valvoo teollisuuden ammattijärjestö nimeltään Wi-Fi Alliance. Ensimmäinen standardi julkaistiin virallisesti vuonna 1997, mutta langattomat verkot alkoivat yleistyä laajemmin vasta vuonna 2001, jolloin hinnat putosivat dramaattisesti. Alkuperäinen standardi nimettiin IEEE 802.11-1997, ja se on nykyään vanhentunut standardi, eikä sitä ole oikein missään käytössä. On tavallista kuulla, että ihmiset viittaavat 802.11-standardeihin tai 802.11-standardien perheeseen. Tarkemmin sanottuna on olemassa vain yksi standardi IEEE 802.11-2007, mutta monia muutoksia. Yleisesti tunnettuihin muutoksiin kuuluvat 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac ja 802.11ax.

Taulukosta 2 näkyy tunnetuimpien muutosten käyttämät taajuudet, teoreettiset maksimi datanopeudet ja tukeeko protokolla moniantennikäyttöä eli MIMO:a. Taulukosta voimme nähdä, että teoreettiset maksimi nopeudet ja kaistanleveydet ovat kasvaneet alkuajoista huomattavasti ja voimme nähdä myös sen, että useamman kuin yhden antennin käyttö on tuonut verkkoon huomattavasti lisää nopeutta (taulukko 2).

Taulukko 2. IEEE 802.11 -protokollan yhteenveto. (Intel Corporation. 2019.)

Protokolla	Taajuus	Kaistanleveys	MIMO	Maksimi nopeus (teoreettinen)
802.11ax	2.4 tai 5GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	14 Gbps
802.11ac wave2	5 GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	2,34 Gbps
802.11ac wave1	5 GHz	20, 40, 80MHz	Single User (SU-MIMO)	1,3 Gbps
802.11n	2.4 tai 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps
802.11g	2.4 GHz	20 MHz	-	54 Mbps
802.11a	5 GHz	20 MHz	-	54 Mbps
802.11b	2.4 GHz	20 MHz	-	11 Mbps
802.11-1997	2.4 GHz	20 MHz	-	2 Mbps

802.11-standardi määrittelee MAC-kerroksen, joka tarjoaa useita 802.11-pohjaisten langattomien lähiverkkojen toimintaa tukevia toimintoja. MAC-kerros ylläpitää ja hallinnoi verkkokorttien ja tukiasemien välisiä yhteyksiä koordinoimalla jaetun ilmatien varausta. 802.11:n MAC -kerrosta pidetään usein verkon aivoina. Se ohjaa jotakin tiettyä fyysistä 802.11-kerrosta, kuten 802.11a, 802.11b tai 802.11g, suorittamaan eri tehtäviä, kuten lähetystä, siirtotien tunnustelua ja kehysten vastaanottaminen. (Geier, J. 2005. 118)

Ennen kuin tukiasema lähettää kehyksiä, sen tarvitsee varata siirtotie, joka on asemien keskenään jakama radiokanava. 802.11-standardin määrittelee kaksi siirtotien varausmuotoa, distributed coordinated function eli DCF ja point coodination function eli PCF. DCF on pakollinen ja se estää kilpavarauksen aiheuttamat törmäykset. DCF:ssä tukiasemat kilpailevat siirtotien varauksesta ja yrittävät lähettää kehyksiä aina kuin siirtotie on vapaa. Jos joku toinen asema on lähettämässä kehystä, muut asemat odottavat, kunnes kanava on vapaa. Siirtotiehen varauksen ehtona MAC-kerros tarkistaa NAV- eli network allocation vectorinsa

arvon. Se on kaikissa tukiasemissa oleva laskuri, joka kertoo, missä ajassa edellinen kehys on lähetettävä. NAV-arvon on oltava 0, ennen kuin asema voi yrittää kehyksen lähettämistä. (Geier, J. 2005. 118-119)

3.1 IEEE 802.11b – 2.4GHz

IEEE standardisoi 802.11b:n vuonna 1999. Se on alkuperäisellä 2,4 GHz kaistalla toimiva suorasekvenssistandardin suuremman tiedonsiirtonopeuden mahdollistava laajennus. Sen suurin mahdollinen datansiirtonopeus on 11 Mbps. 802.1b:n haittana on se, että käytettävissä on ainoastaan kolme ei-päällekkäistä kanavaa 2,4 GHz:n kaistalla. Tämä rajoittaa 802.11b:n kapasiteettiä, jonka vuoksi se soveltuu parhaiten keskiverto suorituskyvyn sovelluksille, kuten sähköpostille ja kevyelle nettisurffailulle.

Toinen 802.11b:n haitta on muiden radiolaitteiden madollinen RF-interferenssi. Esimerkiksi 2,4 GHz:n langaton puhelin häiritsee langatonta 802.11b lähiverkkoa. Mikroaaltouunit ja muut 2,4 GHz taajuudella toimivat laitteet voivat samoin aiheuttaa interferenssiä ja häiriötä toimivuudessa. (Geier, J. 2005. 126)

802.11b käyttää DSSS:ää hajauttaakseen datasignaalin 22 MHz osuudelle 2,4 GHz taajuuskaistasta. Kapeakaistaiseen signalointiin verrattuna tämä tarjoaa paremman vastustuskyvyn RF-häiriöille, jonka vuoksi FCC on ilmoittanut, että hajaspektrijärjestelmät eivät tarvitse lisenssiä. 802.11b muuntaa hajautetun binäärisen signaalin analogiseen aaltomuotoon eri modulaatiomenetelmin, riippuen tiedonsiirtonopeuden valinnasta. Esimerkiksi 1 Mbps nopeudella laitteet käyttävät differentiaalista binääristä vaiheavainnusta (DBPSK). Tekniikka ei ole niin monimutkainen kuin miltä se kuulostaa. Modulaattori vain siirtää keskisiirtotaajuuden vaihetta siten, että binäärinen 0 ja binäärinen 1 pystytään erottamaan toisistaan. 2 Mbps nopeudella laite käyttää differentiaalista kvadraalivaiheavainnusta (DQPSK), joka muistuttaa DBSK:ta, mutta siinä on neljä eri vaihtoehtoa vaihesiirtymään, jotka edustavat aina kahta databittiä. Tämän on kekseliään prosessin

ansiosta datavuo voidaan lähettää 2 Mbps nopeudella käyttäen yhtä paljon kaistaa kuin 1 Mbps nopeudella lähettäessä. Modulaattori käyttää samantapaisia menetelmiä suuremmilla 5,5 Mbps ja 11 Mbps nopeuksilla. (Geier, J. 2005, 127)

3.2 IEEE 802.11a – 5GHz

IEEE standardisoi 802.11b:n kanssa saman aikaisesti myös 802.11a:n vuonna 1999, joka toimii 5 GHz taajuudella käyttäen OFDM:ää 54 Mbps maksiminopeudella. 802.11a on siis huomattavasti nopeampi kuin 2,4 GHz taajuudella toimiva 802.11b. 802.11a:n maksimikantama voi olla 30 metriä riippuen todellisesta tiedonsiirtonopeudesta ja ympäristöstä.

802.11a:n merkittävä etu on se, että se tarjoaa suuremman kapasiteetin kuin 802.1b, koska se toimii usealla ei-päällekkäisellä kanavalla. 802.11a-järjestelmät ovat tehokkaampia kuin 802.11b, ja niiden kapasiteetti on suurempi kuin 802.11g:n. Toinen 802.11a:n etu on se, että se toimii 5 GHz taajuudella, jossa on huomattavasti enemmän kanavia, jolloin käyttäjille voidaan tarjota parempaa suorituskykyä. Useimmat häiriötä aiheuttavat laitteet toimivat myös toisilla taajuuksilla, joten niistäkään ei ole niin paljoa haittaa. 802.11a:n heikkoutena on sen huono kantama johtuen lähinnä sen korkeammasta taajuudesta. Eli siis suuren alueen peittämiseen tarvitaan huomattavasti enemmän tukiasemia kuin 802.11b:llä. (Geier, J. 2005, 124-125)

3.3 IEEE 802.11g – 2.4GHz

IEEE standardisoi 802.11g:n vuonna 2003. Se on yhteensopiva 802.11b:n kanssa ja nostaa suorituskyvyn jopa 54 Mbps asti 2,4 GHz taajuudella OFDM:ää käyttäen. Sen merkittävin etu onkin se, että se on taaksepäin yhteensopiva 802.11b:n kanssa. Yritykset, joilla oli käytössä 802.11b-verkkoja saattoivat siis vain päivittää tukiasemiensa laiteohjelmiston ja saivat käyttöönsä huomattavasti nopeamman 802.11g:n.

802.11b:n haitat, kuten alttius RF-häiriöille ja kolmen kanavan rajoitus koskevat edelleen myös 802.11g:tä, koska se toimii yhtä lailla 2,4 GHz taajuusalueella. Siksi kapasiteetti onkin heikompi kuin 802.11a:ssa (Geier, J. 2005, 127)

3.4 IEEE 802.11n – 2.4GHz / 5GHz

IEEE standardisoi 802.11n:n vuonna 2009. Se on yhteensopiva sekä 802.11g, 802.11b ja 802.11a:n kanssa. 802.11n käyttää taajuusalueinaan molempia sekä 2,4 GHz:n ja 5 GHz:n taajuusalueita, jonka ansiosta se on siis yhteensopiva kaikkien aiempien standardien kanssa. 802.11n:n suurin teoreettinen nopeus 450 Mbps, mikä on taas huomattavasti edeltäjiään suurempi. 802.11n käyttää SU-MIMO-teknologiaa (single-user multiple-input multiple-output), joka mahdollistaa useamman kuin yhden antennin käytön lähetys ja vastaanotto päässä, sekä useamman kanavan saman aikaisen käytön. 802.11n käyttää aiempien standardien mukaisesti OFDM:ää.

802.11n:ää koskevat samat häiriöt kuin aiempiinkin versioihinsa eli 2,4 GHz:llä käytettäessä käytössä on vain kolme ei-päällekkäistä kanavaa ja häiriöt muista laitteista on suurempia. 5 GHz:llä kantama huononee kasvavan taajuuden takia, mikä siis tarkoitti langattoman verkon kantaman pienentymistä.

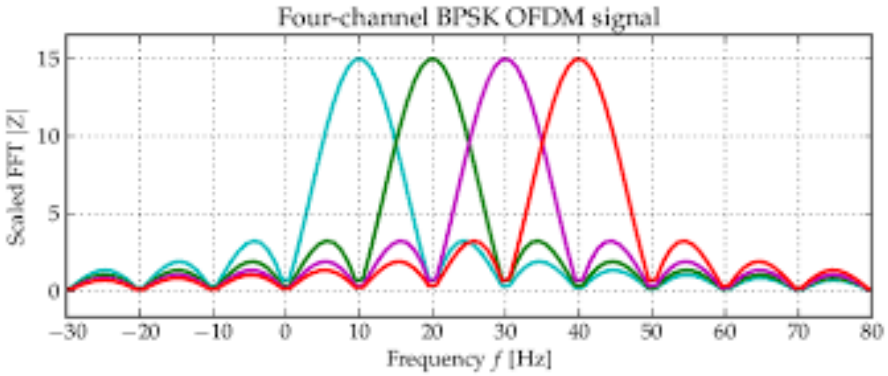
3.5 IEEE 802.11ac – 5GHz

IEEE standardisoi 802.11ac wave 1:n vuonna 2013. 802.11ac on nopeampi ja skaalautuvampi versio 802.11n:stä. Se yhdistää langattoman verkon vapauden Gigabit Ethernetin -ominaisuuksien avulla. WLAN paranee huomattavasti, tukiasemien tukemien laitteiden määrää kasvaa, käyttäjät saavat paremman kokemuksen ja käytettävissä olevaa kaistanleveyttä on tarjolla suuremmalle määrälle. Laitteiden akun käyttöikä pidentyy, koska laitteen WLAN-käyttöliittymä voi herätä, vaihtaa tietoja tukiaseman kanssa ja palata siten lepo tilaan paljon nopeammin.

802.11ac käyttää 5 GHz taajuuskanavaa ja siitä on julkaistu kaksi eri versiota, 802.11ac wave 1 ja 802.11ac wave 2. Wave 2, joka viittaa vuonna 2016 esiteltyihin tuotteisiin ja se tarjoaa suuremman läpäisykyvyn kuin vanhat wave 1 -tuotteet, jotka otettiin käyttöön vuodesta 2013. Maksiminen teoreettinen nopeus wave 1:lle on 1,3 Gbps, kun taas Wave 2 voi nousta 2,34 Gbps. Wave 2 voi siis saavuttaa 1 Gbps, vaikka reaalimaailman suorituskyky osoittautuisi vain puoleksi teoreettisesta nopeudesta. Wave 2 tukee myös suurempaa määrää kytkettyjä laitteita. Wave 1 käyttää 802.11n:n tapaan SU-MIMO tekniikkaa, kun taas uudempi wave 2 käyttää MU-MIMO-tekniikkaa. Wave 1:n suurin kaistanleveys on 80 MHz ja wave 2:ssa suurin kaistanleveys on 160 MHz. Nykypäivän tukiasemat käyttävät ja tukevat 802.11ac wave 2:sta ja sitä olisi suositeltavaa käyttää. (Cisco Systems, 2018.)

3.5.1 OFDM - Monikantoaaltomodulointi

OFDM on 802.11a -standardissa ensimmäistä kertaa käytetty modulointitekniikka, jota käytettään kaikissa sitä uudemmissa 802.11-standardeissa. OFDM jakaa taajuus- tai vaiheavainnuksella tai QAM-modulaatiolla moduloidun signaalin useiden, tietyn kanavan omaavien alikantoaaltojen kesken. OFDM siis jakaa siirrettävän datan alikantoaalloille ja näin käyttää yhden kanavan spektrin tehokkaammin. OFDM:ssä alikantoaallot ovat jopa hieman päällekkäin, mutta eivät juuri häiritse toisiaan, koska aina kun tietyn alikantoaallon huippukohta saavutetaan niin viereisten alikantoaaltojen amplitudit ovat nollassa (kuva 4). Vanhassa DSSS-moduloinnissa yhdellä kanavalla voitiin lähettää vain yksi data purske kerralla, kun taas OFDM:ssä voidaan lähettää useita viestejä samalla kanavalla. OFDM käyttää useita alikantoaaltoja, joista kukin kuljettaa hitaalla bittinopeuden dataa, mikä tarkoittaa, että se on erittäin joustava häipymiselle, häiriöille ja monireittiefektille, ja tarjoaa myös suuren spektritehokkuuden. OFDM on hyvin tehokas, joten se minimoi heijastumisen aiheuttamat ongelmat ja mahdollistaa suuret siirtonopeudet. (Geier, J. 2005, 85)



KUVA 4. OFDM-moduloitu signaali. (StackExchange. 2015.)

OFDM kasvattaa suosiotaan nopeissa yhteyksissä. Se on osa langattomia lähiverkkoja 802.11a:sta 802.11ax-standardeihin ja muodostaa perustan langattomien lähiverkkojen standardille.

3.5.2 SU-MIMO ja MU-MIMO

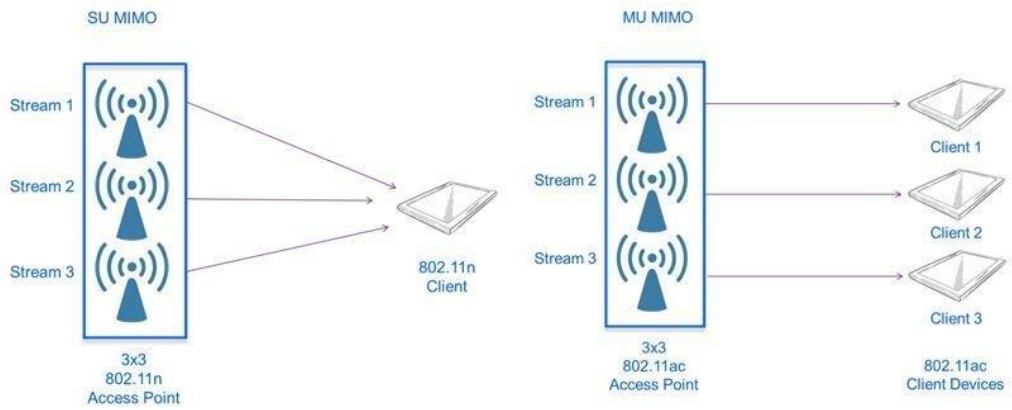
Radioaallot eroavat huomattavasti Ethernet-kaapeloinnista. Yksi suurimmista eroista on se, että Ethernet-kaapeli voi olla kaksisuuntainen, eli se voi lähettää ja vastaanottaa dataa jatkuvasti, kun taas langattomat verkot pystyvät vain lähettämään tai vastaanottamaan. Langattomissa verkoissa ei voida siis lähettää ja vastaanottaa dataa saman aikaisesti samalla antennilla, vaan lähetysten pitää vuorotella. MIMO-teknologian (multiple-input multiple-output) kanssa, asiat muuttuvat.

MIMO-teknologia tuli 802.11n-standardin mukana. Se mahdollisti useiden datavirtojen samanaikaisen lähettämisen tai vastaanottamisen kahden WLAN-laitteen välillä käyttämällä useita antenneja ja säteenmuodostustekniikkaa. Se auttoi nopeuttamaan tiedonsiirtoa kahden WLAN-laitteen välillä. SU-MIMO:n heikkous on se, että useita datavirtoja on lähetettävä tai vastaanotettava vain yhden laitteen välillä kerrallaan. Miinuksia on kuitenkin myös enemmän. Esimerkiksi SU-MIMO vaatii sekä lähettävän, että vastaanottavan WLAN-radion tukemaan MIMO-tekniikkaa yhdessä usean antennin kanssa. Useat antennit lisäävät kustannuksia, painoa ja kokoa WLAN-laitteisiin, ja MIMO-signaalien käsittely vaatii

myös enemmän resursseja. Nämä näkyvät erityisen selvästi pienemmissä laitteissa, kuten älypuhelimissa ja tablet-laitteissa.

Multi user MIMO (MU-MIMO), julkaistiin 802.11ac-standardin toisella julkaisulla. Se parantaa MIMO-tekniikkaa mahdollistamalla WLAN-tiedonsiirron samanaikaisesti useille säteille eri WLAN-laitteille, vain yhden laitteen sijaan, kuten vanhemmassa versiossa. Jos esimerkiksi sanotaan, että tukiasema pystyy lähettämään neljä tietovirtaa samanaikaisesti, se voisi lähettää kaikki neljä laitteeseen, joka voi hyväksyä neljä. Vaihtoehtoisesti se voisi lähettää kaksi virtaa yhdelle laitteelle ja kaksi muuta virtaa kahdelle eri laitteelle. Kaiken kaikkiaan kolme erilaista laitetta vastaanottaisi tiedot samanaikaisesti. Kuvassa 5 on kuvattu SU-MIMO:n ja MU-MIMO:n eroja vielä kuvan muodossa.

MU-MIMO:n selvin hyöty on se, että näitä useita datavirtoja voidaan lähettää tai vastaanottaa eri laitteille tai eri laitteilla, mikä lisää verkon mahdollista kapasiteettia. Kuitenkin on myös paljon muita etuja. Esimerkiksi MU-MIMO:n kanssa, yhtä MIMO-datavirtaa vastaanottavissa WLAN-laitteissa ei tarvitse olla useita antenneja. Vastaanottavien WLAN-laitteiden on tuettava monen käyttäjän MIMO-tekniikkaa, mutta jos antenneja on vain yksi, se voi silti vastaanottaa yhden useista datavirroista langattomalta reitittimeltä tai tukiasemalta. Lisäksi langaton reititin tai tukiasema on laite, joka käsittelee MIMO-signaaleja raskaasti, joten se verottaa vähemmän WLAN-laitteiden prosessoreita. Tämä kaikki tarkoittaa sitä, että MIMO-tekniikkaa tukevissa laitteissa voidaan säästää kustannuksissa, painossa ja koossa. (TechGenix. 2015.)



KUVA 5. SU-MIMO:n ja MU-MIMO:n erot (ResearchGate. 2016.)

3.6 IEEE 802.11ax – 2.4GHz / 5GHz

IEEE standardisoi 802.11ax:n vuonna 2018. 802.11ax:stä käytetään myös nimitystä WIFI 6. Nimi tulee siitä, että se on kuudes standardisoitu WLAN-standardi. WIFI 6, käyttää taajuuksinaan sekä 2,4 GHz:iä, että 5 GHz:iä. Se käyttää myös 802.11ac wave 2 tapaan MU-MIMO:a. Standardi perustuu 802.11ac: n vahvuuksiin lisäten samalla tehokkuutta, joustavuutta ja skaalautuvuutta, mikä mahdollistaa uusien ja olemassa olevien verkkojen nopeuden ja kapasiteetin lisäämisen seuraavan sukupolven sovellusten kanssa. 802.11ax:n teoreettinen maksiminopeus on käyttäen 4x4 MIMO:a on 14 Gbps, eli siis käyttäen neljää antennia molemmissa päissä. Yhdellä antennilla päästään 3,5 Gbps mikä on sekin jo todella paljon. 802.11ax:ssä on myös saatu pudotettua latenssia huomattavasti 802.11ac:sta (ExtremeTech. 2015).

WIFI 6 on alun perin rakennettu vastaamaan kasvavaa laitteiden määrään maailmassa. Jos omistaa VR-laitteen, useita älylaitteita tai on vain suuri määrä laitteita taloudessa, WIFI 6 -reititin saattaa olla juuri paras WLAN-reititin. WIFI 6 tukevia tukiasemia on vasta alkanut 2019 Q4:llä tulemaan markkinoille ja niiden hinnat ovat vielä melko korkealla. Halvimmat kotikäyttöiset reitittimet ovat noin 200€:n hintaisia. Yritys käyttöön tarkoitettujen tukiasemat ovat halvimmillaan noin 400€:n hintaisia ja vaikka tukiasemat tukisivat WIFI 6:ta niin suurin osa laitteista ei vielä tue kyseistä protokollaa.

4 WLAN-VERKON SALAUSTAVAT

WLAN-verkoissa käytettään erilaisia salauksia ja salausalgoritmeja, joilla saadaan estettyä ei toivottujen henkilöiden tai laitteiden pääsy langattomaan verkkoon. Langattoman lähiverkon tietoturva koostuu menetelmistä, joiden tarkoituksena on lisätä tiedonsiirron ja kirjautumisen turvallisuutta WLAN-verkoissa. Menetelmät koostuvat yksinkertaisista verkkoon pääsyn ja autentikoinnin ratkaisuista sekä moninkertaisesta tiedon salaamisesta. Langattomat verkot lähettävät viestejä radion avulla, joten ne ovat salakuunteluherkempiä kuin langalliset verkot. Tämän takia langattoman verkon salaus on tärkeä asia, jos halutaan että kuka vain ei pääse kytkeytymään verkkoon.

Ulkopuolisten tahojen pääsyä langattomaan voidaan estää erilaisilla pääsylistoilla, joissa voidaan määritellä, että vain tietyillä MAC-osoitteella olevat laitteet päästetään verkkoon. Tässä tavassa on huonoa se, että ylläpitäjä joutuu jatkuvasti päivittämään listoja sitä mukaan, kun halutaan uusia laitteita verkkoon. MAC-osoitteen mukaan tehdyt pääsy listat ovat muutenkin vähän huonoja, koska MAC-osoitteet näkyvät selkokielisenä ja niitä pystyy tietokoneelle manuaalisesti vaihtamaan, jolloin hyökkäykset tällaisiin verkkoihin ovat helppo suorittaa.

4.1 WEP

WEP on vanhentunut algoritmi langattomien IEEE802.11-verkkojen suojaamiseksi. WEP protokolla käyttää salaus algoritmina RC4:ää ja CRC-32:n tarkistussummaa. Kun WEP otettiin käyttöön vuonna 1999 ja sen oli tarkoitus tarjota turvallisuus, joka on verrattavissa perinteiseen kiinteään verkkoon. Vuonna 2001 analyytikot havaitsivat useita vakavia heikkouksia, joiden seurauksena WEP-yhteys voidaan murtaa helposti saatavilla olevilla ohjelmistoilla muutamassa minuutissa. Muutaman kuukauden kuluessa IEEE perusti uuden 802.11i-työryhmän vastaamaan ongelmista. Vuoteen 2003 mennessä Wi-Fi Alliance ilmoitti, että WEP oli korvattu Wi-Fi Protected Access (WPA) -salauksella, joka oli osa tuolloin tulevaa 802.11i-muutosta. (Wireless LAN Security Interoperability Lab. 2019.)

4.2 WPA, WPA2 ja WPA3

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2 / WPA2 Personal) ja Wi-Fi Protected Access 3 (WPA3) ovat kolme suojausprotokollaa ja turvallisuusvarmennusohjelmaa, jotka Wi-Fi Alliance on kehittänyt turvaamaan langattomat tietokoneverkot. Allianssi määritteli nämä vastauksena vakavaan heikkouteen, jonka tutkijat olivat löytäneet edellisessä järjestelmässä.

WPA-protokolla toteuttaa suuren osan IEEE 802.11i-standardista. Erityisesti Temporal Key Integrity Protocol (TKIP) hyväksyttiin WPA:lle. WEP käytti 64-bittistä tai 128-bittistä salausavainta, joka on annettava manuaalisesti langattomiin tukiasemiin ja laitteisiin eikä muutu. TKIP käyttää pakettiavainta, mikä tarkoittaa, että se luo dynaamisesti uuden 128-bittisen avaimen jokaiselle paketille ja estää siten WEP:n vaarantavien hyökkäysten tyyppejä.

WPA sisältää myös viestin eheyden tarkistuksen, jonka tarkoituksena on estää hyökkääjää muuttamasta ja lähettämästä tietopaketteja. Tämä korvaa syklisen redundanssitarkistuksen (CRC), jota WEP-standardi käytti. CRC:n suurin virhe oli, että se ei taannut riittävän vahvaa tietojen eheyden takuuta käsittelemilleen paketeille. Näiden ongelmien ratkaisemiseksi oli olemassa hyvin testattuja viestin todennuskoodeja, mutta vanhojen verkkokorttien käyttämiseen tarvittiin liian paljon laskentaa. WPA käyttää TKIP-nimistä viestin eheyden tarkistusalgoritmia pakettien eheyden tarkistamiseen. TKIP on paljon vahvempi kuin CRC, mutta ei niin vahva kuin WPA2:ssa käytetty algoritmi AES. Tutkijat ovat sittemmin löytäneet puutteen WPA:ssa, joka vetoaa WEP:n vanhempiin heikkouksiin ja viestin eheyskoodin hash-toiminnon rajoituksiin. (Informa PLC Informa UK Limited. 2018.)

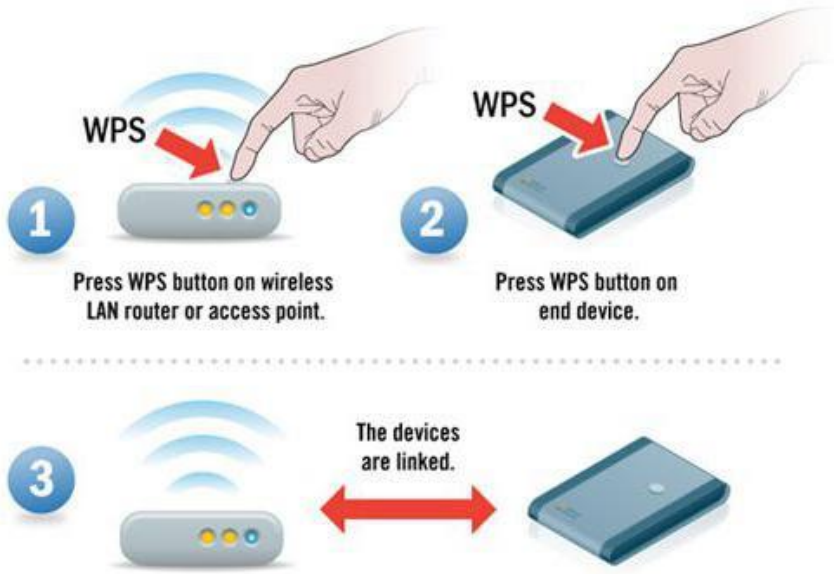
WPA2 korvasi WPA:n. WPA2, joka vaatii Wi-Fi Alliancen testauksen ja sertifioinnin, toteuttaa IEEE 802.11i:n pakolliset elementit. Erityisesti se sisältää pakollisen tuen CCMP:lle, AES-pohjaiselle salausmoodille. Sertifiointi alkoi syyskuussa 2004. Maaliskuusta 2006 alkaen WPA2-sertifiointi on pakollinen kaikille uusille laitteille, joissa on Wi-Fi-tavaramerkki.

Tammikuussa 2018 Wi-Fi Alliance ilmoitti WPA3:n korvaavan WPA2:n. WPA3-standardi korvaa myös esijaetun avaimenvaihdon IEEE 802.11-2016 -määritelmässä määritellyllä samanaikaisella yhtäaikaisella autentikoinnilla, mikä johtaa turvallisempaan alkuavaimen vaihtoon. Wi-Fi Alliance väittää myös, että WPA3 vähentää heikkojen salasanojen aiheuttamia turvallisuusongelmia ja yksinkertaistaa laitteiden asentamisprosessia, joissa ei ole näyttöliittymää. WPA3 on 2019 Q4:llä tullut uusiin WLAN-tukiasemiin vaihtoehdoksi. (Informa PLC Informa UK Limited. 2018.)

4.3 WPS

WPS tulee sanoista Wi-Fi Protected Setup. Se on langattoman verkon suojaustandardi, joka yrittää tehdä yhdistämisestä reitittimen ja langattomien laitteiden välillä nopeaa, helppoa ja suojattua. WPS toimii vain langattomissa verkoissa, jotka käyttävät salasanaa, joka on salattu WPA Personal- tai WPA2 Personal -suojausprotokollalla. WPS ei toimi langattomissa verkoissa, jotka käyttävät vanhentunutta WEP-tietoturvaa, jonka kuka tahansa hakkeri voi helposti murtaa perustyökaluilla ja taidoilla.

WPS:n käyttöön on kolme eri menetelmää, joko PIN-menetelmä, missä laitteella, jolla ollaan ottamassa WLAN:iin yhteyttä painetaan WPS PIN nappia ja näytölle ilmestyy 8 numeroinen koodi, joka syötetään sitten reitittimeen ja näin verkkoyhteys saadaan muodostettua. Toinen vaihtoehto on nappia painamis -vaihtoehto. Siinä pitää painaa reitittimessä olevaa fyysistä tai virtuaalista WPS-painiketta ja samanaikaisesti painaa yhdistettävästä laitteesta WPS-painiketta. Puhelimessa löytyy virtuaalisena tuo painike WLAN-asetuksen takaa. Tietokoneissa ja puhelimissa ei yleensä ole WPS:lle fyysistä painiketta vaan virtuaalinen painike löytyy asetusten takana. Kolmas vaihtoehto, jolla WLAN:iin voidaan WPS:n avulla liittyä on NFC. Tässä tavassa esimerkiksi puhelin voidaan liittää WLAN:iin koskettamalla puhelimella reititintä. Tällöin molempien laitteiden on tuettava NFC:tä. Kuvassa 6 on esitetty vielä, kuinka laitteet saa helposti WPS-painikkeiden avulla yhdistettyä toisiinsa.



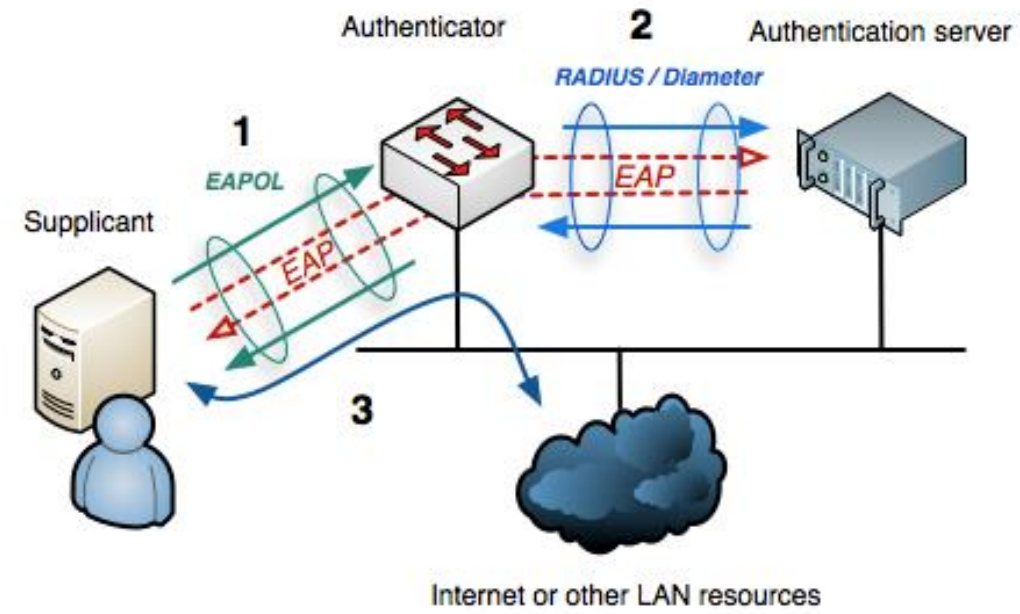
KUVA 6. WPS-salauksella laitteiden yhdistäminen (Girlsgameland. 2019.)

4.4 802.1X – Radius autentikaatio

IEEE 802.1X -standardilla tarkoitetaan verkkoon tunnistautumista käyttäen RADIUS-palvelinta. Radius-palvelin päättää hänelle asetettujen sääntöjen mukaan päästetäänkö laite verkkoon, annetaanko rajoitetut oikeudet verkkoon vai potkikaanko laite pois verkosta. 802.1X on monesti nimetty myös WPA2-Enterprise:ksi. WPA2:sta on siis kaksi versiota, Personal ja Enterprise. Molemmat käyttävät vahvaa AES-CCMP-salausmenetelmää langattoman tiedon salaamiseksi. Tärkein ero näiden turvamoodien välillä on todennusvaiheessa. WPA2 Enterprise käyttää IEEE 802.1X:ää, joka tarjoaa yritystason todennuksen. WPA2 Personal käyttää esijaettuja avaimia (PSK) ja on suunniteltu kotikäyttöön.

802.1X-todentamisessa on mukana kolme osapuolta: ehdottaja (supplicant), todentaja (authenticator) ja todennuspalvelin (authentication server). Ehdottaja on asiakaslaite (kuten kannettava tietokone), joka haluaa liittyä WLAN-verkkoon. Termiä ehdottaja käytetään myös vuorottelevasti viittaamaan asiakkaassa käynnissä olevaan ohjelmistoon, joka tarjoaa todennuksen tunnistetiedot. Todentaja on verkkolaite, joka tarjoaa datayhteyden asiakkaan ja verkon välillä ja voi sallia

tai estää verkkoliikenteen näiden välillä, kuten Ethernet-kytkin tai langaton tukiasema. Todennuspalvelin on tyypillisesti luotettava palvelin, joka voi vastaanottaa ja vastata verkkoon pääsyä koskeviin pyyntöihin, ja voi kertoa todentajalle, onko yhteys sallittava, sekä erilaisista asetuksista, joita tulisi soveltaa kyseiseen yhteyteen tai asetukseen. Todennuspalvelimet yleensä käyttävät ohjelmistoja, jotka tukevat RADIUS- ja EAP-protokollia. Joissakin tapauksissa todennuspalvelinohjelmisto saattaa olla käynnissä todennuslaitteistossa. Kuvassa 7 on kuvattu 802.1X:n liikenne autentikointi tilanteessa. Kuvasta näkee, että ehdottaja ottaa ensin yhteyttä todentajaan (vaihe 1), joka välittää tarpeelliset tiedot autentikointi palvelimelle (vaihe 2), joka palauttaa todentajalle vastauksen mitä oikeuksia kyseiselle ehdottajalle annettaan ja todentaja sitten joko päästää laitteen verkkoon (vaihe 3) tai estää laitteen pääsyn verkkoon. Kuvasta näkee, että autentikointi tapahtuu EAP-protokollaa käyttäen (kuva 7). (Network World. 2010.)

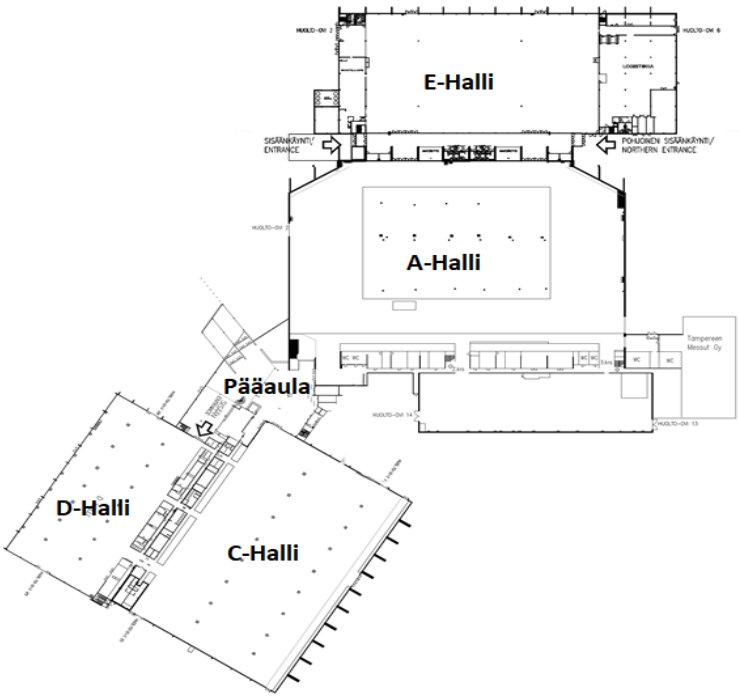


KUVA 7. 802.1X autentikaatio (Wikipedia. 2019.)

5 LANGATTOMAN LÄHIVERKON KUULUVUUDEN MITTAUS

Yrityksellä, jossa WLAN-mittaukset suoritettiin, oli havaittu, että WLAN:in toimivuus ei ole riittävällä tasolla ja se haluttiin mitata ja siten tarkistaa langattoman verkon tilanne. Mittauksia ennen pohjatietona oli useamman vuoden kokemus kyseisestä kohteesta ja tiedettiin tukiasemien sijainnit, merkit ja mallit. Kohteena oli messukeskus, jossa kävijöitä on useita satoja tai jopa tuhansia kerralla, jolloin radioverkot ovat kovalla koetuksella. Lisäksi kyseisessä kohteessa ongelmana on, että useat asiakkaat tuovat sinne omia verkkolaitteitaan, jotka jakavat osastoille verkkoa WLAN:lla. Tämä tarkoittaa sitä, että messutapahtuman aikana radiokanavat ovat kaikki todella tukossa, varsinkin 2,4 GHz:n taajuudella, koska sillä taajuudella on todella vähän kanavia tarjolla.

Mittauksia lähdettiin kuitenkin tekemään aikana, jolloin hallit ovat tyhjillään, jotta nähtiin, onko WLAN:in kuuluvuus ylipäätään riittävällä tasolla, jotta langatonta verkkoa voidaan tarjota varmuudella, että se kattaa koko rakennuksen. Kuvassa 8 on mitattavan kohteen pohjakartta. Rakennuksessa on neljä suurta hallia sekä pääaula ja kahden isoimman hallin (A- ja E-hallin) välissä on myös aula alue, jossa langattoman verkon täytyy myös kuulua riittävällä tasolla.

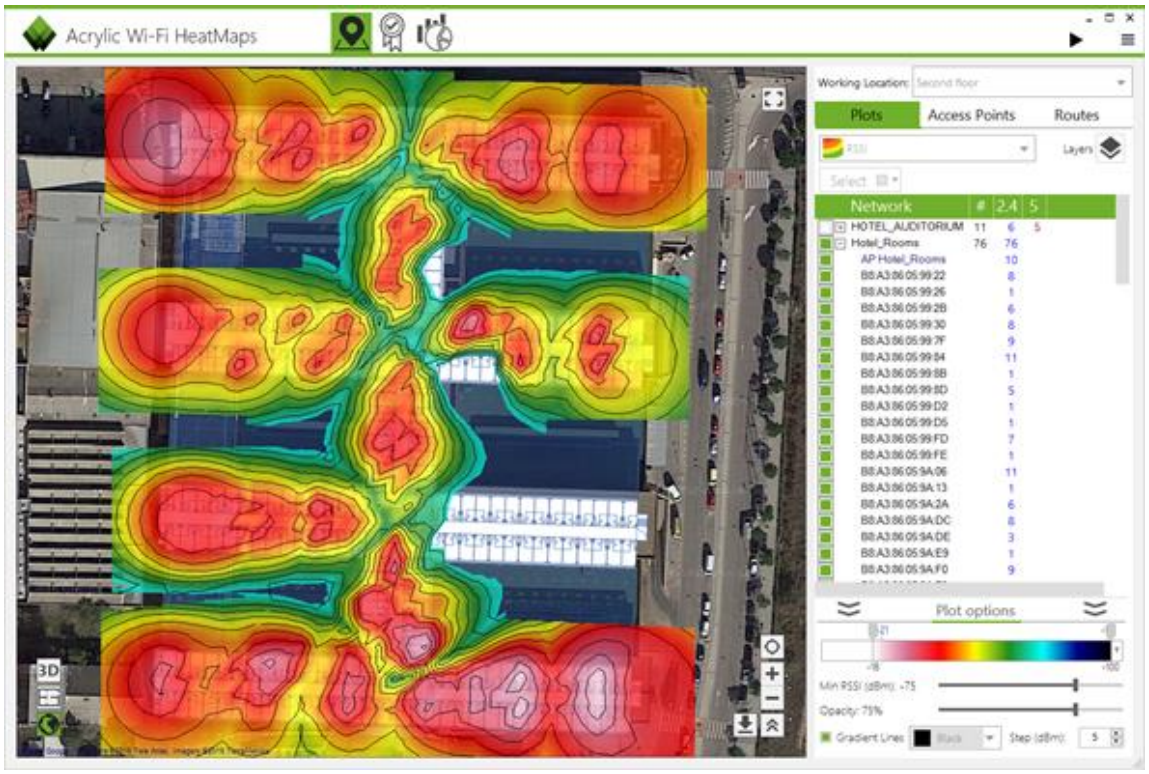


KUVA 8. Pohjakartta mittauskohteesta.

5.1 WLAN-mittaus laitteiston valinta

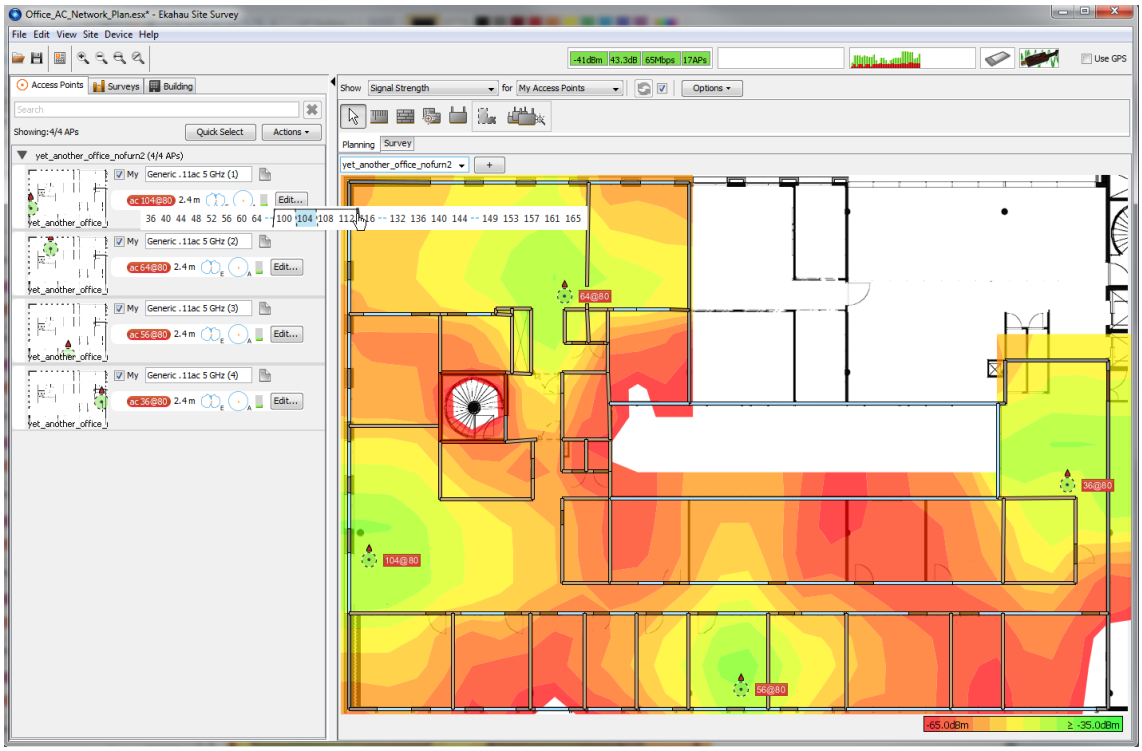
WLAN-mittauksia aloittaessa kannattaa miettiä kuinka paljon mittalaitteistolle on käyttöä ja miten saisi kaikista realistisimpia tuloksia. Jos on tekemässä mittaukset vain yksittäisestä kohteesta niin silloin ei ehkä kannatta hankkia parhaimpia ja kalleimpia lisenssejä, ohjelmistoja ja laiteita, mutta ei myöskään kannata valita ilmaisversioita, koska niissä on yleensä erittäin vähän ominaisuuksia. Toki ilmaisversiota suositellaan käytettäväksi, jos käyttää ensimmäistä kertaa, jolloin pystyy hieman vertailemaan mikä ohjelmisto sopisi itselle parhaiten.

Tässä tapauksessa mittauslaitteistoksi valittiin tavallinen kannettava tietokone (HP Probook 650 G2), jossa WLAN-verkkokortti, joka tukee kaikkia nykyisin käytössä olevia WLAN-standardeja eli 802.11b/a/g/n/ac sekä 5 GHz, että 2,4 GHz taajuutta ja siihen ohjelmistoksi valittiin Acrylic Wifi Heatmaps. Tähän kokopanoon päädyttiin siitä syystä, että käyttöä oli noin viiteen kohteeseen ja kaikki saatiin mitattua kuukauden sisään, joten ei tarvinnut hankkia kuin kuukauden lisenssi. Lisenssille tuli hintaa noin 130€ ,mikä on ihan kohtalainen hinta siihen nähden, että saa tarkat mittausraportin tarvituista kohteista. Acrylicin etuna oli myös se, että siitä on olemassa ilmaisversio, jonka avulla pystyttiin ensin harjoittelemaan käyttöä ja saatiin hieman mallia siitä, mitä kaikkea tuolla kokoonpanolla voidaan mitata ja kuinka laaja raportti mittaustiedolla kyetään toimittamaan. Kuvassa 9 hieman esimerkkiä siitä minkälainen on Acrylicin käyttöliittymä. Mittaukset suoritettiin käyttämällä kannettavassa tietokoneessa olevaa langatonta verkkokorttia, jotta saatiin mahdollisimman realistiset mittaus tulokset. Mahdollista olisi myös ollut käyttää ulkoisia antenneja, mutta tällöin mittaukset eivät olisi vastanneet oikein sitä miltä ne vastaanotetulla laitteella näyttäisi. Ohjelmiston valinnassa vaihtoehtoina olivat Acrylic Wifi Heatmaps, Ekahau Site Survey ja Cape Networks (nykyisin Aruba User Experience Insight).



KUVA 9. Acrylic Wifi Heatmapsin käyttöliittymä. (Acrylic WiFi. 2019.).

Ekahau on lähes samanlainen kuin Acrylic, mutta siinä isona miinuksena on se, että Ekahaulta ei ole mahdollista ostaa vain lyhyen ajan lisenssiä vaan ainoa vaihtoehto on ostaa lisenssi, joka on ikuisesti voimassa. Ekahaun etuna oli kuitenkin se, että mittaus ohjelmiston mukaan sai melko pienellä hinnalla ostettua erilliset verkkokortit, jota ohjelmisto tukee ja sillä olisi voinut tehdä tarkempiakin WLAN-mittauksia. Ekahau:lle olisi tullut hintaa melkein 4500€ euroa, joka on melko paljon siitä, että käyttöä on vain muutamaan kohteeseen. Lisäksi aiemmin mainitun erillisen verkkokorttisarjan hinnaksi olisi tullut 150€. Kokonaishinnaksi tuolle mittausohjelmisto paketilla siis olisi tullut 4650€. Ohjelmana Ekahau on helppokäyttöinen ja mittausdata on helposti luettavissa. Kuvassa 10 on esimerkki dataa, jota Ekahaun ohjelmisto antaa. Siinä näkee selkeästi missä kuuluvuus on hyvää ja missä on parantamisen kohteita. Ekahaun käyttöliittymä on hyvin samanlainen kuin Acrylicin, jos ei jopa hieman selkeämpikin ja yksinkertaisempi.



KUVA 10. Ekahau Site Survey esimerkki kuva mittausdatasta. (Ekahau. 2013.)

Tarjolla oli myös Cape Networks. Cape Networks on mittalaite, joka viedään tilaan, jossa langatonta verkkoa halutaan mitata. Se jätetään paikanpäälle ja se analysoi valittuja WLAN-verkkoja jatkuvasti. Siihen voidaan myös kytkeä langallinen verkko ja siihen voidaan asettaa eri VLAN merkkauksia. Sillä voidaan siis mitata myös useampia eri langallisia ja langattomia verkkoja samanaikaisesti. Siihen voidaan asettaa erilaisia hälytys rajoja, jolloin aina kun WLAN tai LAN ei toimi riittävällä tasolla niin laite ilmoittaa siitä käyttäjälle, että nyt olisi verkossa jotain vikana. Kyseistä laitetta ei voi niinkään käyttää WLAN-kuuluvuuden kartoitukseen, koska laitetta ei mittaushetkellä kuuluu liikuttaa. Tämä laite on enemmänkin tarkoitettu tarkempaan vian selvitykseen, jos esimerkiksi jollain työpisteellä on ongelmia WLAN:in kanssa niin tämä laite voidaan viedä käyttäjän pöydälle ja laite tallentaa langattomasta tai langallisesta verkosta dataa ja mittaa sen toimivuutta jatkuvasti. Se huomaa esimerkiksi, jos verkossa tulee katkoja tai jos verkko on tukossa. Laitteessa on sisään asennettu SIM-kortti, joten vaikka verkko olisi poikki niin se voi lähettää virhedataa netissä olevaan portaaliin. Siitä voidaan ottaa ulos myös dataa .pcap muodossa, jota voi erilaisilla ohjelmilla sitten tutkia paketti tasolla. Esimerkiksi Wireshark on hyvä ohjelma .pcap-tiedostojen analysointiin. Cape Networks -laitteen hinta on noin 700€ ja lisäksi laitteeseen tarvitsee ostaa vuosittain lisenssi, jonka hinta on myös 700€. Eli ensimmäiselle vuodelle

tulisi hintaa 1400€ ja sitä seuraaville 700€ per vuosi. Kuvasta 11 näkee miltä laite itsessään näyttää.

KUVA 11. Cape Networks WLAN:in mittauslaite. (IT Pro. 2017.)

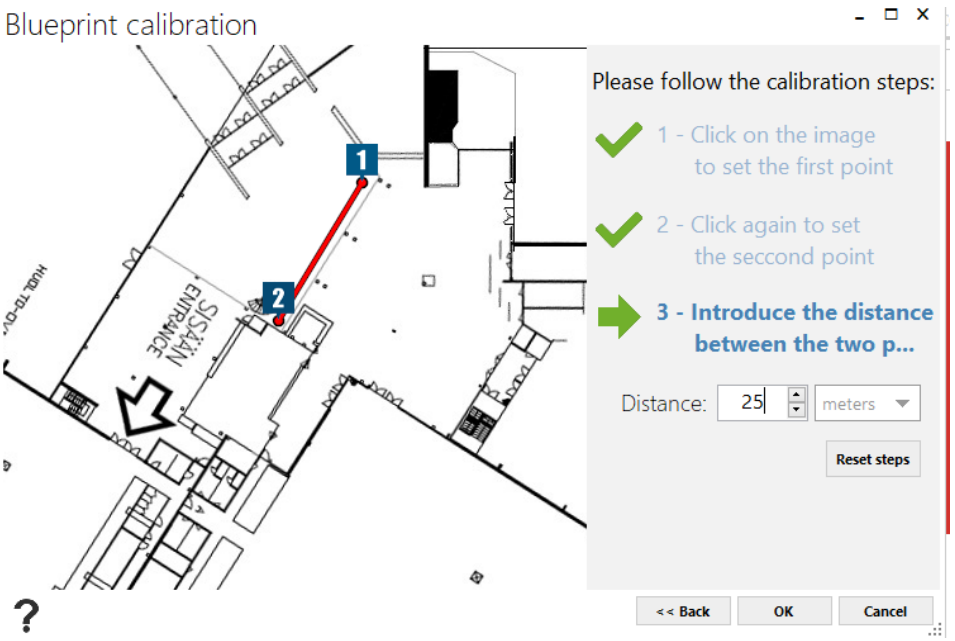
Taulukossa 3 on käyty vielä laitteiden hinnat läpi sekä kunkin mittaus ohjelmiston tai mittauslaitteen plussat ja miinukset ja hinnat läpi. Näistä voidaan tulkita se, että tähän mittaukseen valittu Acrylic Wifi Heatmaps oli vertailussa selvästi paras kyseiseen mittauskohteeseen, niin hinnan kuin ominaisuuksien puolesta.

TAULUKKO 3. Mittausohjelmistojen vertailu.

	Acrylic Wifi Heatmaps	Ekahau Site Survey	Cape Networks (Aruba User Experience Insight)
Hinta	130€/kk tai 2200€ kertamaksu	4500€ kertamaksu	700€/vuosi + 700€/laite
Plussat	Halpa hinta, hyvä ja yksityiskohtainen mittausraportti	Saatavilla kohtuulliseen hintaan lisäverkkokortit. Helppo käyttöliittymä ja hyvä ja selkeä rapotti	Hyvä verkon vikojen diagnosointiin. Saa datan ulos pcap tiedostossa, joka on yhteensopiva muiden ohjelmistojen kanssa
Miinukset	Hieman epäselvä käyttöliittymä	Kallis hankinta hinta	Kallis hinta ja ei sovellu hyvin kuuluvuuden kartoitukseen

5.2 Langattoman verkon mittauksen suorittaminen

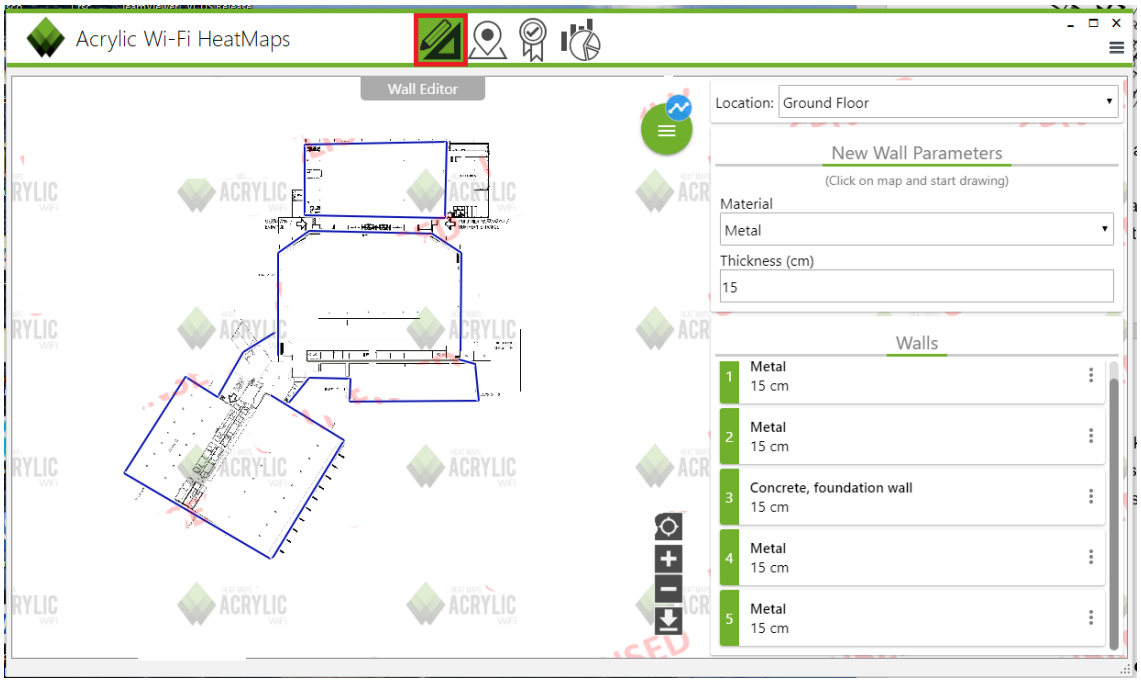
Acrylic Wifi Heatmaps sovelluksen avattua ohjelma kysyy ensimmäiseksi lisenssi tietoja. Syötettyä lisenssin pääsee eteenpäin ohjelman aloitusruutuun. Ohjelma kysyy heti auettuaan, että halutaanko luoda uusi projekti. Seuraavaksi kun luodaan uusi projekti, ohjelma kysyy hieman tietoja kuten projektin nimen, kuvausta projektista, sekä mitattavan kohteen nimen. Ohjelmaan voi myös tässä vaiheessa laittaa oman yrityksen tai asiakasyrityksen logon, jolloin logo tulee myös mittausraportteihin. Lisäksi tässä vaiheessa pitää lisätä pohjakartta mitattavasta kohteesta. Pohjakuvaa lisätessä ohjelma kysyy, että käytetäänkö pohjakartan kalibroinnissa apuna GPS:ää vai valitaanko skaalaus manuaalisesti pohjakartan avulla. Päätimme valita manuaalisen tavan, koska kyseisessä mittauskohteessa on hieman huonot yhteydet GPS:n suhteen, joten mittaustuloksiin saattaisi tulla jonkin verran heittoa. Lisäksi mittauslaitteistomme ei tukenut GPS:ää. Toki manuaalisesti asetetuissa mittauspisteissä on hieman virhettä. Manuaalisessa vaihtoehdossa tarvitsee valita jokin matka metreinä ja piirtää se pohjakarttaan, jotta ohjelma osaa mitata WLAN-kuuluvuuden oikein. Kuvassa 12 on kuvattu kuinka mittaussuhteet kalibroidaan manuaalisesti pohjakartan avulla.



KUVA 12. Mittasuhteiden kalibrointi manuaalisesti Acrylic Wifi Heatmapsissa.

Pohjakuvan asettamisen ja kalibroinnin jälkeen pohjakarttaan tulee lisätä seinät ja niiden materiaalit mahdollisimmat tarkkaan. Seinien lisäys vaikuttaa siihen,

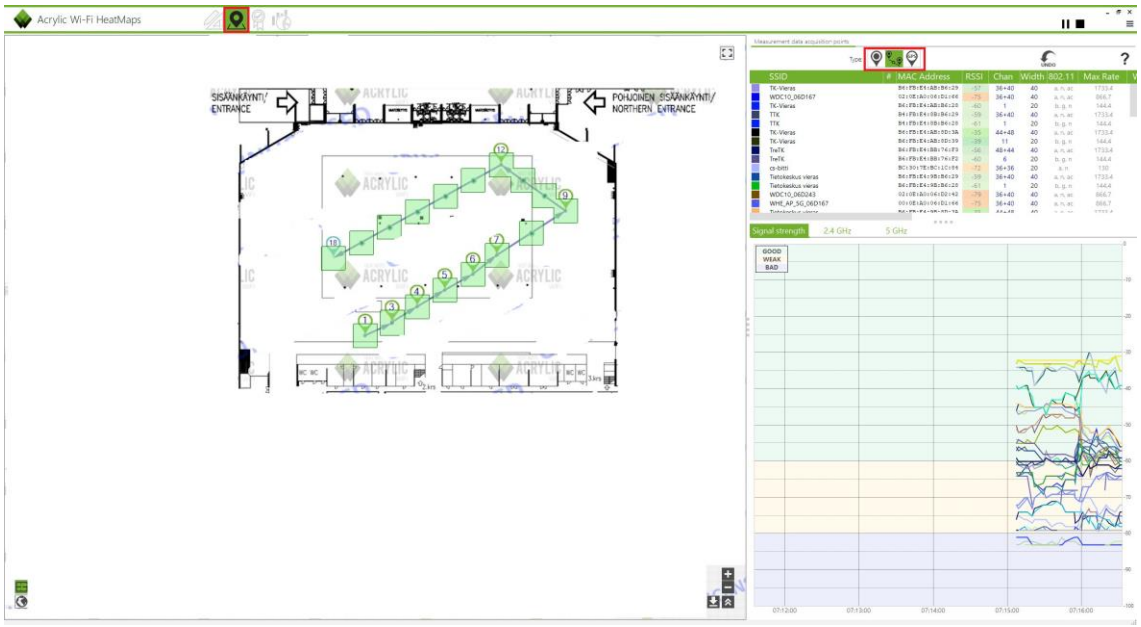
kuinka hyvin kartassa näkyvät kuuluvuuskartat pitävät paikkaansa. Metalliseinän läpi ei mene signaalit kauhean hyvin läpi, niin jos sen vaikka jättää laittamatta niin saattaa tuloksissa olla vääristyneet lukemat. Kuvasta 13 näkee, että seinät saa pohjakarttaan lisättyä ohjelman yläreunassa olevasta wall editor -napista. Tämän jälkeen pitää valita oikeasta reunasta oikea seinän materiaali ja vetää pohjakarttaan seinät. Kun seinät on lisätty, ohjelman oikeassa alareunassa näkyy seinät lisäys järjestyksessä, ja niitä klikkaamalla näkee kartassa korostettuna mikä seinän kohta on valittu.



KUVA 13. Seinien piirtäminen Acrylic Wifi Heatmaps -ohjelmaan.

Mittaukset suoritetaan painamalla ohjelman ylärivistä Site Survey -nappia. Ohjelmaan aukeaa taas sama pohjakartta näkymä. Seuraavaksi painetaan ohjelman oikeasta yläreunasta käynnistys nappia. Painamishetkellä kannattaa tarkastaa, että langaton verkkokortti on toiminnassa eikä se saa olla kytkettynä mihinkään langattomaan verkkoon, ohjelma myös huomauttaa, jos asetukset ovat väärin. Vaihtoehtoja on kolme mittauksen suorittamiseen. Voi kävellä pitkin mitattavaa aluetta ja muutaman metrin välein klikata sijaintinsa karttaan. Aina kun karttaa klikkaa niin ohjelma mittaa siitä kohdasta WLAN:in kuuluvuuden ja muita arvoja. Tämä on työläs tapa varsinkin isoissa kohteissa, koska muutaman metrin välein joutuu pysähtymään ja klikkaamaan sijaintia kartalla. Toinen vaihtoehto on valita

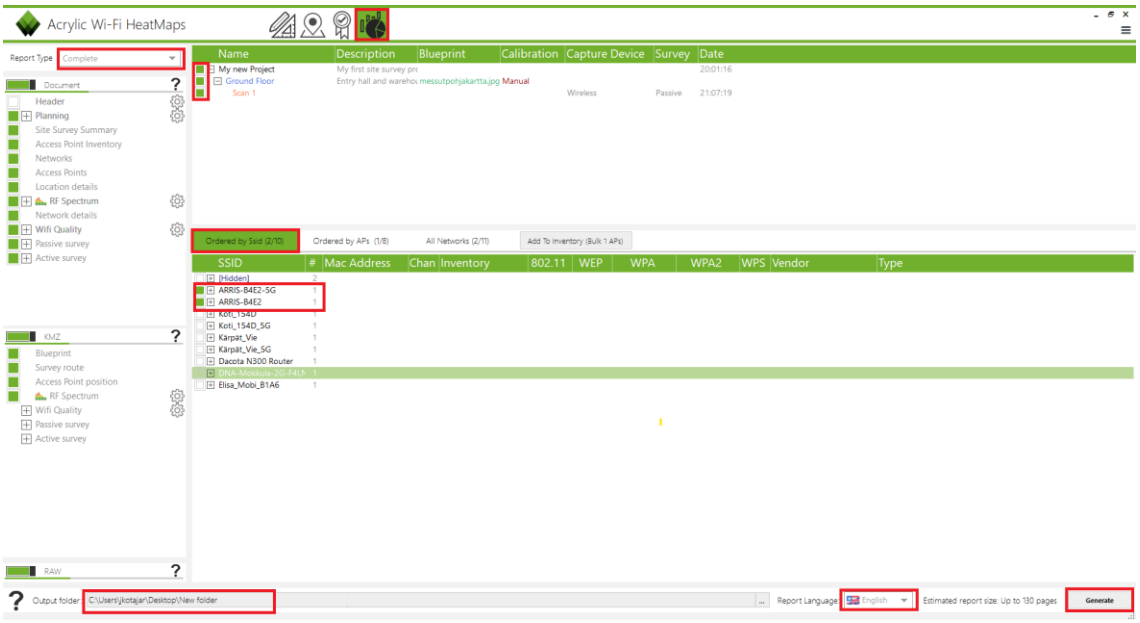
jatkuva mittaus eli painetaan kartasta aloitus piste ja lähdetään kävelemään johonkin suuntaan, kun on päästy haluttuun pisteeseen, niin painetaan lopetussijainti kartasta. Ohjelma ottaa automaattisesti siltä väliltä mittauksia eikä tässä tavassa tarvitse pysähtyä koko aikaa. Itse suosin tätä tapaa. Kolmas vaihtoehto on käyttää GPS:ää. Sekin on hyvä tapa, jos mitattavassa kohteessa on riittävän hyvä GPS-signaali ja mitattava laite tukee GPS:ää. GPS-vaihtoehto on kaikkein helpoin, koska silloin ei tarvitse erikseen karttaan klikkailla sijaintiaan vaan ohjelma tunnistaa GPS-signaalin avulla missä mittalaite menee ja ottaa automaattisesti tietyn välein mittauksia. Skannauksia ei myöskään tarvitse ottaa koko rakennuksesta kerralla vaan mittaukset voi jakaa eri alueiden mukaan osiin. Esimerkiksi omassa mittauksessani tein jokaiselle hallille omat mittausdatat ja pääaulalla oman. Mittaukset saa jaettua osiin painamalla pysäytys nappia oikeasta yläkulmasta ohjelmaa. Uuden alueen saa taas aloitettua painamalla käynnistys nappia siitä vierestä. Kun mittauksia suoritetaan niin ohjelma näyttää oikeassa reunassa havaitut SSID:t, tukiasemat, kanavat ja signaalien vahvuudet (kuva 14). Mittaus hetkellä ohjelma näyttää myös oikeassa alareunassa reaaliaikaista dataa eri radioista.



KUVA 14. Mittauksen suorittaminen ja eri mittaustavat.

Nyt on mittaukset saatu suoritettua ja voidaan alkaa tarkastelemaan mittaustuloksia. Seuraavalta välilehdeltä voi katsella dataa suoraan tästä ohjelmasta,

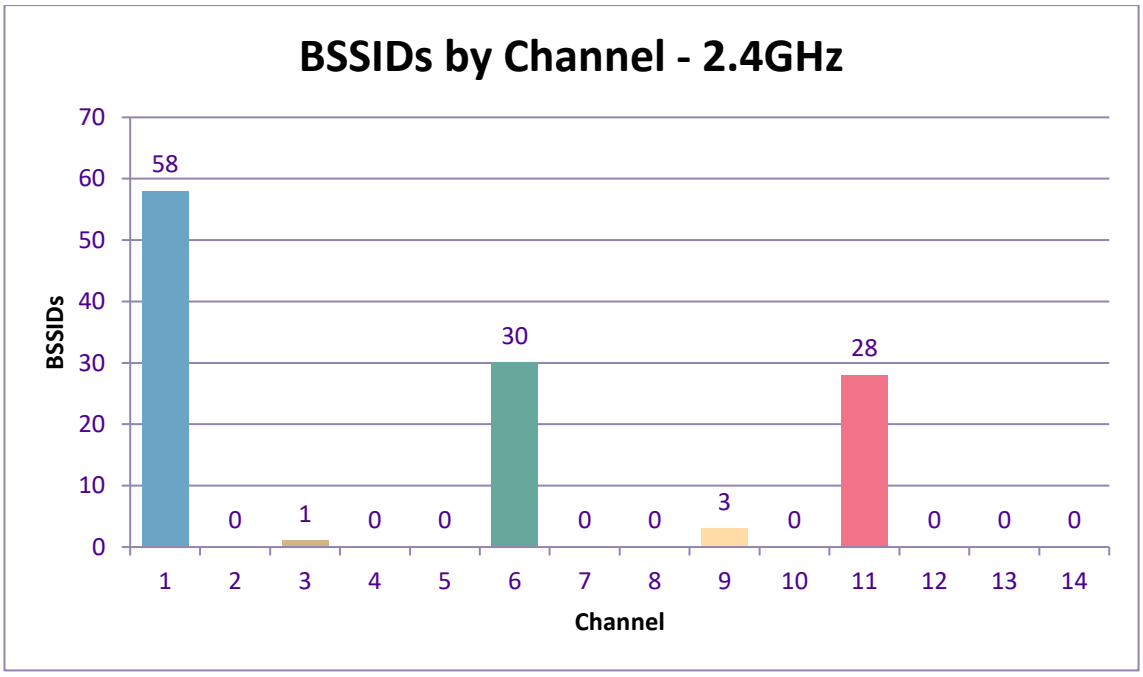
mutta mielestäni se ei ole kauhean selkeä toiminto. Data on siellä jotenkin sekaisin ja vaikeasti ymmärrettävissä. Mielestäni parempi vaihtoehto on mennä suoraan viimeiselle välilehdelle, jossa luodaan mittausdatasta raportti. Raporttia luodessa pitää valita miltä kaikilta osilta haluaa ottaa mittausdatan raporttiin. Voi esimerkiksi jättää yhden alueen pois, joka on mitattu, jos haluaa. Jokaisesta alueesta voi myös luoda oman raportin. Raporttia luodessa pitää myös valita mitkä SSID:t tai mitkä tukiasemat halutaan mittausdataan. Järkevintä on valita mittausdataan SSID:n perusteella, koska silloin saadaan kartta siitä missä mikäkin verkko kuuluu ja omasta mielestä se on kaikista hyödyllisin data. Toki, jos haluaa tietää millä alueella jokin tietty tukiasema kuuluu, niin siitäkin voi luoda oman raporttinsa. Ohjelmasta pitää vielä valita, että kuinka laajan datan raporttiin haluaa. Se tapahtuu ohjelman vasemmasta sivupalkista. Yleensä kannattaa valita kaikki, koska silloin ei ainakaan jää mitään oleellista dataa puuttumaan raportista. Ohjelmasta valitaan vielä alapalkista polku, johon raportti luodaan ja voi myös valita kieleksi englannin, espanjan, saksan tai ranskan. Lopuksi painetaan generate-näppäintä ja ohjelma luo raportin mittauksista (kuva 15).



KUVA 15. Raportin luonti Acrylic Wifi Heatmaps -ohjelmalla.

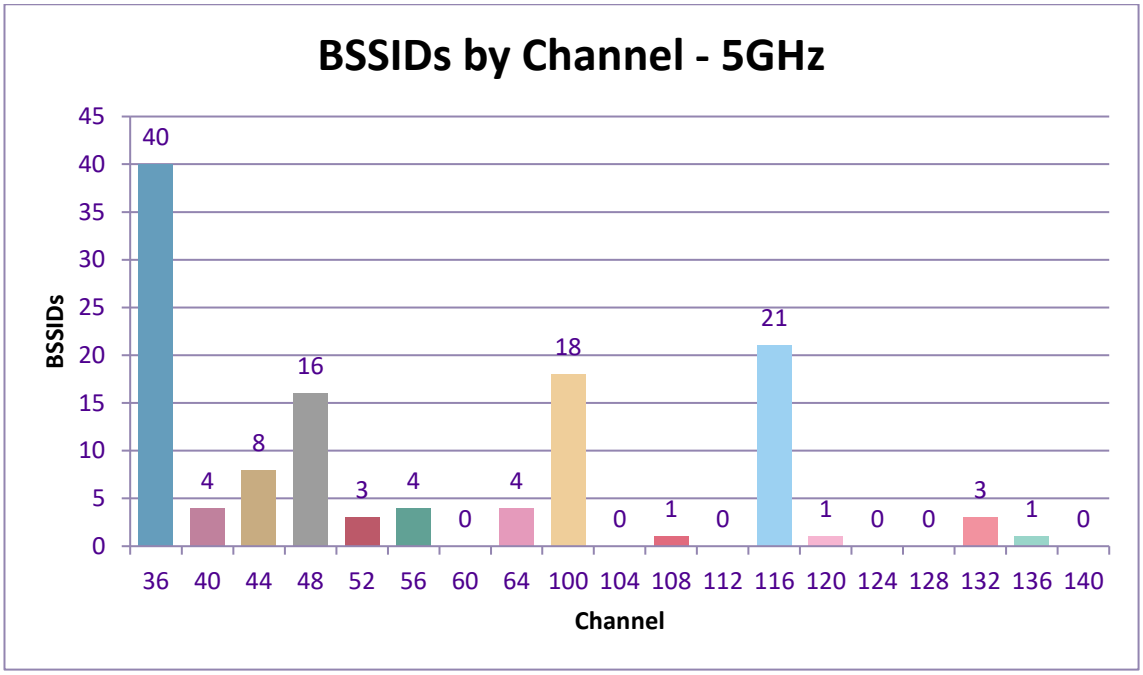
5.3 Mittaustulosten analysointi

Nyt kun mittaukset kohteessa on suoritettu ja saatu raporttina ohjelmasta ulos tarvitsee mittausdataa hieman tutkia. Liitteenä 1 on pätkä oikeasta mittausraportista. Mittausraportissa on muutama ensimmäinen sivua yhteenvetoa mittauksista, mittausten päivämäärä, valittujen skannausten-, tukiasemien- ja tukiasemien radioiden määrä. Seuraavaksi raportissa näkyy tukiasemien radioiden määrä kanavittain. Kuviossa 1 on mittausraportista otettu 2,4 GHz kanavan radioiden määrä. Kuviosta voidaan huomata, että kanavia mitatussa kohteessa voisi jaotella hieman tasaisemmin, koska radiot painottuvat pääasiassa kanavalle 1. Kuviosta voimme myös huomata, kanavat on oikeaoppisesti valittu eli käyttöön on valittu vain sellaiset kanavat, että ei tule päällekkäisyyksiä eli kanavat 1,6 ja 11.



KUVIO 1. 2,4 GHz:n kanava mittausraportista.

Mittausraportissa on myös samantapainen kuvio 5 GHz kanavalle. Siitä voimme myös huomata, että myös 5 GHz taajuus vaatii hieman kanavien tasapainotusta. Lähes puolet kaikista 5 GHz radioista on kanavalla 36 mikä tarkoittaa, että se ruuhkautuu helposti. 5 GHz kanavalla on muutenkin huomattavasti enemmän valinnan varaa kanavien suhteen kuin 2,4 GHz, joten mittaus raportin pohjalta suositeltaisiin kanavien tasapainotusta (kuvio 2).



KUVIO 2. 5 GHz:n kanava mittausraportista.

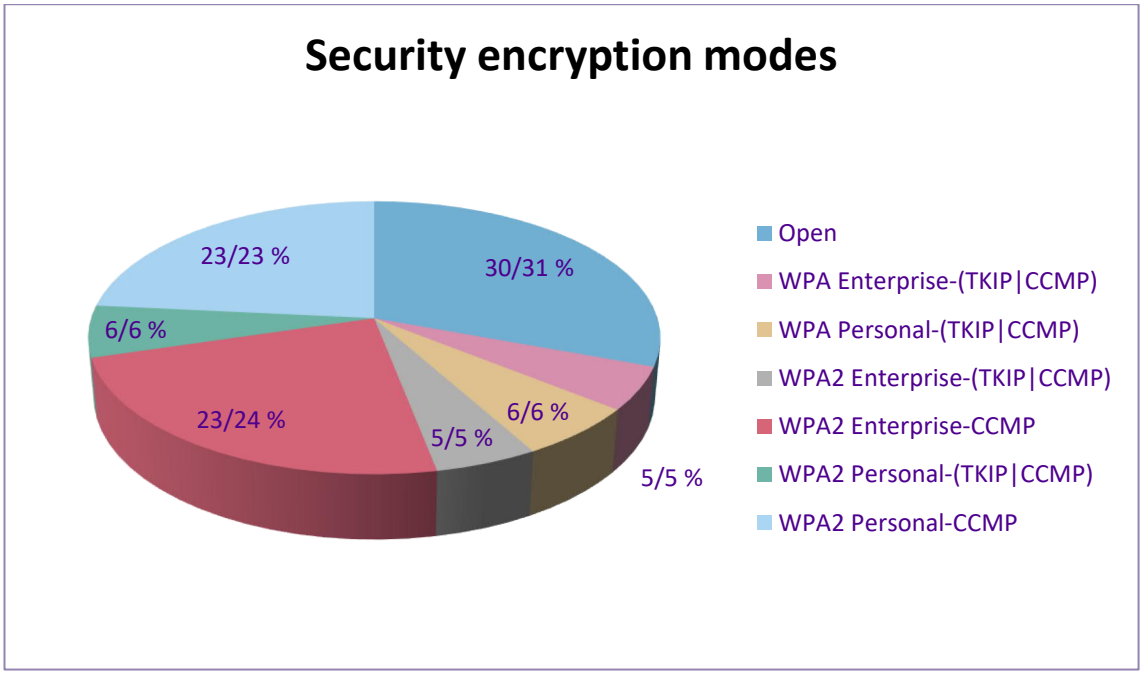
Mittausraportti luetteloi jokaisen mitatun SSID:n (service set identifier) ja jokaisessa SSID:ssä olevan radion. SSID:llä tarkoitetaan jokaisen langattoman verkon tunnistetta, jolla käyttäjä voi tunnistaa mihin verkkoon hän on kytkeytymässä. Mittausraportti kertoo myös jokaisesta tukiasemasta minimi, maksimi ja keskiarvon mitatun signaalin vahvuudesta sekä kanavan, jota kyseinen radio käyttää. Tästä taulukosta voi nähdä, jos jollain tukiasemalla on koko ajan huono signaalin vahvuus niin se on joko suunnattu huonosti, sijoitettu huonosti tai tukiasemassa on jotain vikaa. Taulukosta näkee myös jokaisen SSID:n salaus tavan jokaiselle radiolle. Eri radiolla voi olla erilaiset salaustavat, mutta se ei ole suotavaa ja jos mittausraportista huomaa, että jollain SSID:llä on eri salauksia eri radioissa niin kannattaa tarkastaa kaikki tukiasemat ja vaihtaa kaikkiin radioihin sama salaustapa. Taulukossa 4 on pieni otos edellä mainitusta mittausdatasta. Taulukosta voimme nähdä, että kyseinen SSID ei käytä mitään salausta vaan se on avoin verkko. SSID esimerkissä on WLAN1. Taulukosta voimme myös todeta, että mitä suurempi lukema RSSI kohdassa on niin sitä parempi signaali tukiasemalta tulee. RSSI tarkoittaa signaalin vahvuutta ja se on ilmoitettu dBm-yksikössä. BSSID tarkoittaa tukiaseman radion MAC-osoitetta. MAC-osoite on jokaisella verkkokortilla omansa ja sen avulla verkkolaitteet tunnistavat lähiverkossa toisensa.

BSSID:stä huomaa, että 5 GHz:n radiolla ja 2,4 GHz radioloillakin on eri MAC-osoitteet.

TAULUKKO 4. Radio-kohtaiset mittaustulokset.

SSID	BSSID	CHAN	FREQ	RSSI AVG	RSSI MAX	RSSI MIN	SECU-RITY
WLAN1	00:13:A6:24:A6:E1	36	5180	-62	-45	-85	Open
	00:13:A6:24:A6:F0	1	2412	-56	-43	-82	Open
	00:13:A6:24:A7:41	36	5180	-58	-44	-84	Open
	00:13:A6:24:A7:48	1	2412	-53	-42	-76	Open

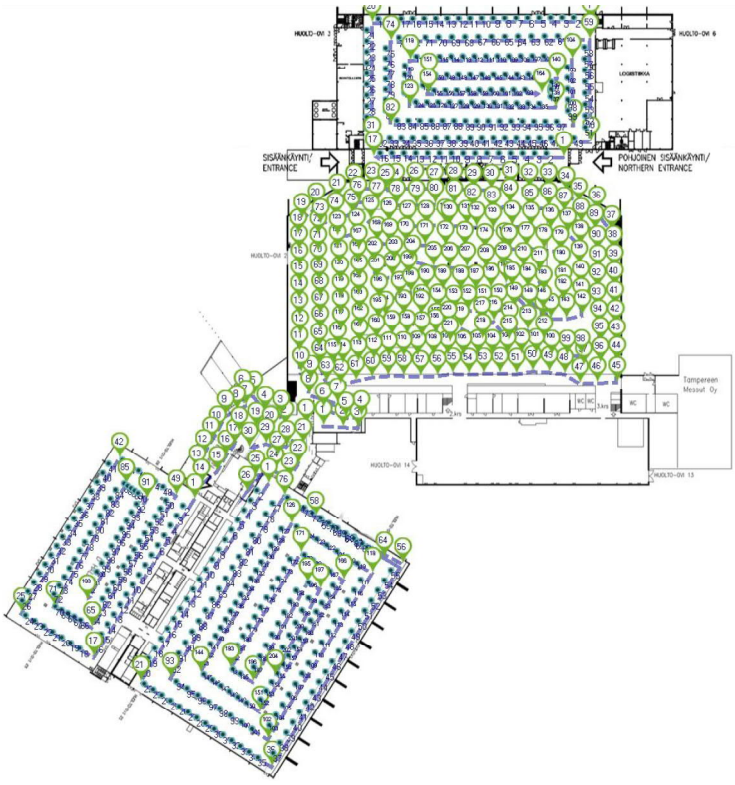
Kuviossa 3 on esitetty eri tukiasemien langattomien verkkojen salaustavat. Kuviosta voimme huomata, että mitatussa kohteessa on melko monia eri salaustapoja käytössä. Suositeltavaa olisi, että jokaisella SSID:llä olisi vain yksi salaustapa, jotta laitteet olisi aina samassa verkossa yhtä hyvin suojattu. Kuviosta voimme huomata, että mitatussa kohteessa on käytössä myös WPA salausta, jota ei olisi enää suotavaa käyttää. Tämäkin asetus tulisi ottaa kaikista tukiasemista pois ja vaihtaa kaikki tukiasemat käyttämään WPA2-salausta. Myös WPA2 TKIP salaus olisi järkevää poistaa käytöstä, koska CCMP/AES on siitä huomattavasti kehittyneempi versio (kuvio 3).



KUVIO 3. Salaustavat ja niiden suhteet.

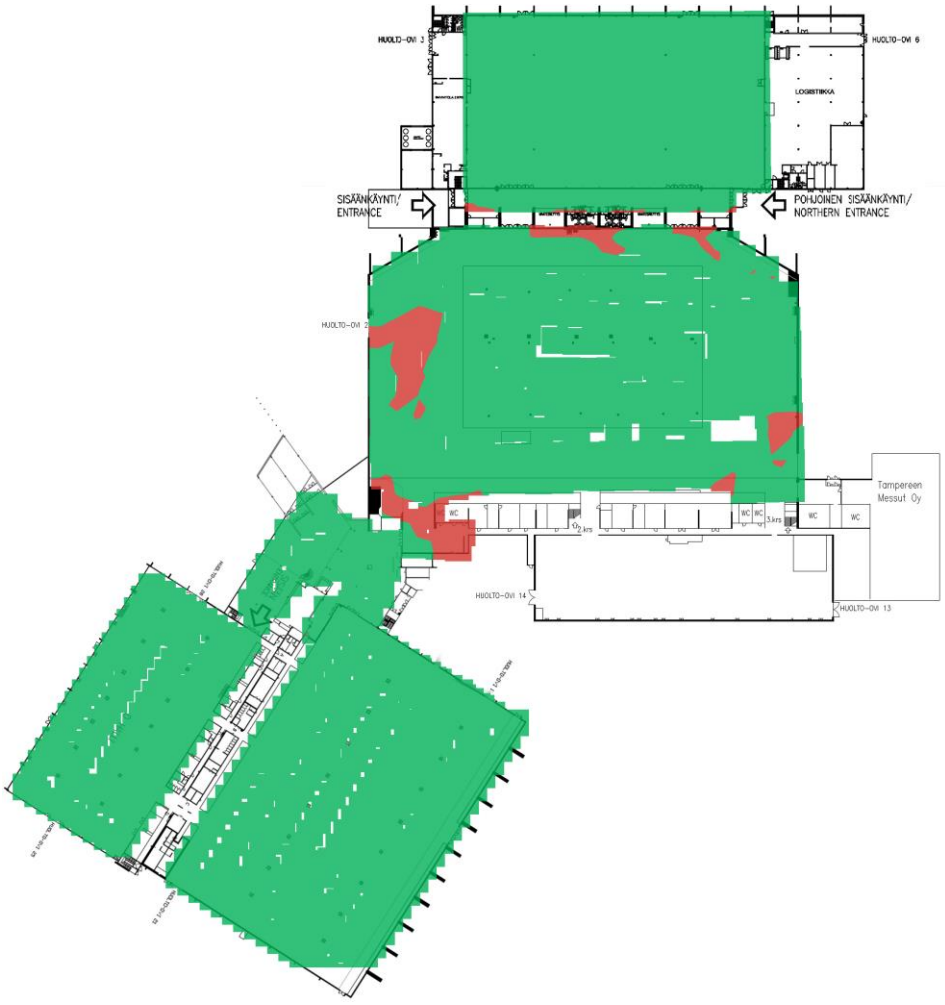
Mittausraportti kertoo myös jokaisen tukiaseman valmistajan, BSSID:n, SSID:n, kanavan, taajuuden ja mitä 802.11-protokollaa mikäkin BSSID käyttää. Näistä tilastoista voimme huomata, jos jokin tukiasemista käyttää vain pelkästään jotain tiettyä vanhentunutta 802.11-standardia, jolloin kyseisen tukiaseman asetukset voidaan käydä tarkistamassa ja vaihtaa uudempiin ja parempiin standardeihin. Toki saattaa olla, että jokin tukiasemista ei tue uusimpia standardeja, mutta yleensä senkin saa ohjelmistopäivityksillä korjattua.

Seuraavana mittausraportissa näkee mittausreitin, jonka on mittaus hetkellä kulkenut. Siitä voi vielä tarkistaa, että mittausdata on tullut ehjänä raportille asti. Kuvassa 16 on otettu kuva liitteestä 1, jossa näkyy, että koko haluttu alue on mitattu. Kuvasta näkee myös, että mittauksissa on käytetty kahta eri tyyliä mittausten tekemiseen eli kuvassa vihreät numeroidut pallot tarkoittavat yksittäisiä mittauksia, jossa jokaisen mittauksen otto hetkellä on pysähdytty mittaamaan. Siniset pisteet tarkoittavat, että on laitettu jatkuva mittaus päälle ja merkitty aloitus ja lopetus pisteet ja ohjelma on automaattisesti tehnyt mittauksi tuolta väliltä tietyin väliajoin.



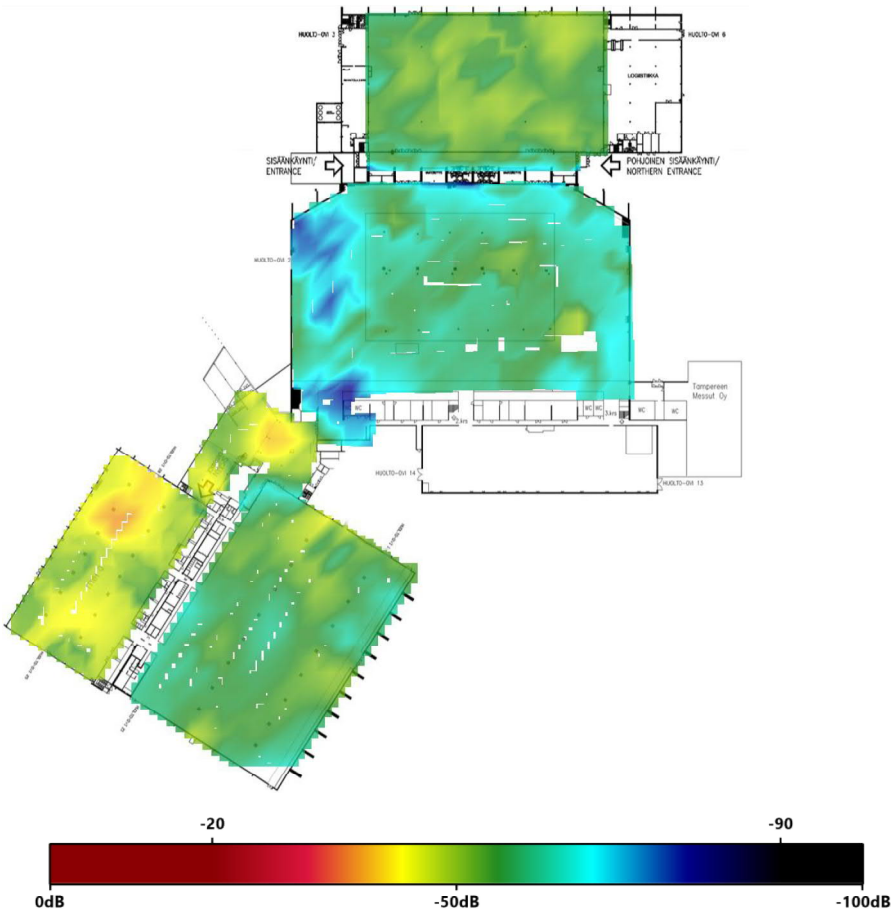
KUVA 16. Mittauspisteet kartalla.

Mittausraportissa on myös RSSI-kuuluvuuskartta (received signal strength indicator), joka laskee kaikkien tukiasemien vastaanotetun signaalin voimakkuuden ja ilmoittaa vihreällä tai punaisella värillä onko RSSI-arvo mitatulla alueella riittävällä tasolla. RSSI kertoo, onko vastaanotetun signaalin vahvuus riittävällä tasolla vertailu lukuun verrattuna. RSSI-arvo mitataan dBm-yksikössä ja vaihteluväli on 0 dBm - (-100) dBm. Hyväksyttävät arvot ovat välillä 0 – (-75) dBm. Riittävää tiedonsiirron tasoa ei voida taata alhaisemmilla signaalinvoimakkuuksilla. Asiakkaalta mitatusta datasta voimme huomata, että isoimmassa hallissa eli A-hallissa on muutamia kohtia, joissa nuo kriteerit eivät täyty ja ne on piirretty kuvaan punaisella (kuva 17). Punaisille alueilla tullisi suunnata WLAN-antenneja paremmin, laittaa laitteisiin enemmän lähetystehoa tai lisätä tukiasemien määrää.



KUVA 17. RSSI-kuuluvuuskartta

Mittausraportissa tärkeimpänä tuloksista on RSSI lämpökartta. Lämpökartta kertoo millä alueilla on minkäkin vahvuista signaalia tarkasti. Kuva on hieman samantapainen kuin aiempi kuva, mutta se kertoo huomattavasti tarkemmin jokaisen kohdan kuuluvuuden. Jos aiempi kuva kertoi, että onko kuuluvuus riittävällä tasolla niin tämä näyttää tarkemmin jokaiselle alueella, että mikä signaalin vahvuus on dBm:nä. Väriskaala kartassa kertoo signaalin vahvuuden. Punainen väri tarkoittaa kaikista vahvinta signaalia ja sininen väri taas tarkoittaa heikkoa signaalia. Kuvasta 18 voimme huomata, että pääaula sekä D-hallin signaalit ovat erittäin hyvällä tasolla. Muissa halleissa signaali on kohtalainen ja A-hallissa signaalin taso on useassa paikassa todella huonolla tasolla. Kuvan perusteella voimme todeta, että A-, C- ja E-hallissa tulisi joko nostaa tukiasemien tehoa tai vaihtaa tukiasemat tehokkaampiin malleihin. D-hallissa ja pääaulassa on 2017 kesällä vaihdettu uudet tukiasemat ja kuvasta voimme todeta, että näillä alueilla signaalin vahvuus on huomattavasti parempi, jolloin voimme olettaa, että myös toimivuus on parempi.



KUVA 18. RSSI-lämpökartta.

Raportissa on myös paljon muita kuvia ja taulukoita, mutta mainitsemani kuusi kohtaa ovat ehkä ne tärkeimmät datat, joita raportista tarvitsee tulkita. Raportista on myös mahdollista saada enemmän irti, mutta se vaati tietyn tyyppisen verkkokortin, joka tukee verkon monitorointia. Verkosta olisi mahdollista saada raporttiin myös esimerkiksi verkon kaistaleveys, verkon viive, roamingin toimivuus, pakettien hukkuminen. Nämä kaikki on tärkeitä ja ne olisi myös hyvä saada mittausdataan, mutta koska tässäkin tapauksessa budjetti oli rajallinen ja aikataulu mittauksille oli melko pieni, niin haluttiin saada edes jotain dataa asiakkaan verkosta ja mielestäni tulokset auttoivat verkon kehittämisessä.

5.4 Langattoman lähiverkon optimointi

Langattoman lähiverkon optimointi on hyvä tehdä sen jälkeen, kun mittausraportti kohteesta on suoritettu. Optimoinnilla tarkoitetaan asetusten muuttamista paremmaksi mittaustulosten perusteella. Esimerkiksi tässä tapauksessa lähdettiin muuttamaan kanavia mittaustulosten perusteella siten, että kanavat olisivat tasaisemmin jaettu. Esimerkiksi 2,4 GHz:n kanavalla 1, oli tasan puolet kaikista radioista. Nyt radiot on muutettu siten, että ne on tasaisesti jaoteltu muille kanaville. 5 GHz kanaville tehtiin sama juttu eli jaoteltiin radiot tasaisemmin kaikille kanaville eikä jätetty lähes kaikkia kanavalle 36.

Mittaamassamme kohteessa muutettiin myös salausalgoritmit siten, että käytössä on enää WPA2-personal, WPA2-enterprise ja avoin verkko. Poistettiin siis kokonaan käytöstä WPA-salaus, koska on tullut jo uudempia salaus algoritmeja käyttöön ja laitteet niitä tukee. Lisäksi poistettiin käytöstä myös TKIP, jonka tilalle laitettiin pelkkä AES. Käytöstä otettiin poistettiin myös vanhimmat 802.11-standardit, koska niissä nopeudet ovat niin huonolla tasolla, että niitä on syytä välttää, vaikka ne jotenkin toimisivatkin. Käytöstä otettiin siis pois 802.11b ja 802.11a.

Tukiasemia myös sijoiteltiin hieman paremmin ja käänneltiin hieman antenneita, jotta saatiin huonoimpien alueiden kuuluvuutta hieman parannettua. D-hallissa ja pääaulassa on käytössä Aruban WLAN-tukiasemat, joissa on toimintona client

match. Client matchin avulla saadaan parannettua sitä, että millekään tukiasemalla ei tulisi liikaa käyttäjiä vaan tukiasemat osaisivat siirtää ruuhkatilanteissa toisille tukiasemille käyttäjiä, jotta kaikki käyttäjät eivät olisi samassa tukiasemassa kiinni. Lisäksi kesällä 2019 vaihdettiin E-halliin tukiasemat, koska vanhat Extricomin tukiasemat olivat jo niin vanhoja eikä niihin saanut enää tukea niin ne vaihdettiin myös Aruba merkkisiksi. Nyt muutaman testi kuukauden jälkeen voidaan sanoa, tukiasemien vaihtaminen kannatti. Kaikissa halleissa on nyt WLAN:in toiminta ollut hyvällä tasolla ja kertaakaan ei ole tullut puolen vuoden aikana ilmoitusta, että kyseisessä hallissa ei toimisi langaton verkko. Toki A-hallin kuuluvuutta voisi vielä parantaa vaihtamalla sinne myös tukiasemat

Langattoman verkon optimoinnissa tulee siis ottaa seuraavat asiat huomioon:

1. Kanavien tasapainoinen valinta, etteivät kanavat ole tukossa
2. Salausalgoritmit samalle tasolle, ei montaa salausalgoritmia samassa SSID:ssä.
3. Vanhentuneet 802.11-standardit pois käytöstä, jotta voidaan tarjota paras nopeus ja toimivuus WLAN:lle.
4. Tukiasemien siirtäminen ja antennien suuntaus.
5. Tukiasemien päivittäminen
6. Tukiasemien vaihtaminen uudempiin ja parempiin malleihin.

POHDINTA

Tässä opinnäytetyössä perehdyin langattoman verkon mittaukseen sekä mittausraportin tulkitsemiseen. Alussa kävin hieman läpi WLAN-teknologioita sekä WLAN-standardeita. Käytiin läpi erilaisia salaustekniikoita sekä mitä salaustekniikoita nykypäivänä tulisi käyttää, jotta langaton verkko olisi suojattu riittävän tehokkaasti hyökkäyksiltä. Tutustuin langattoman verkon mittauslaitteisiin sekä erilaisiin mittausohjelmistoihin. Lopuksi kävin läpi mittaustuloksia, sekä annoin vinkkejä siihen kuinka langattoman verkon toimivuutta saa parannettua käyttäen nykyisiä laitteita.

Mittausraportista saatiin tutkittua, että WLAN-kanavat oli jaoteltu huonosti. Lähes kaikki radiot olivat samoilla kanavilla, sekä 2,4 GHz:n taajuudella, että 5 GHz:n taajuudella. Lisäksi mittausraportista havaittiin, että käytössä oli huonoja salausalgoritmeja, jotka otettiin pois käytöstä, jotta verkon murtautuminen ei olisi niin helppoa. Raportista nähtiin myös, että osassa tiloista kuuluvuus oli erittäin huonolla tasolla. Näihin tiloihin kehotettiin asiakasta hankkimaan uudet tukiasemat, koska vanhaa laitteistoa ei enää saada parannettua nykypäivän standardeja vastaamaan. Lopputulema oli se, että mittausten ja mittausraportin pohjalta saimme parannettua langattoman verkon toimivuutta kyseisessä kohteessa ja asiakas oli tyytyväinen saamaansa palveluun.

Lopuksi voin sano, että mittausten suorittaminen oli erittäin hyödyllistä. Mittausdatasta saatiin paljon vinkkejä siihen kuinka langatonta verkkoa saatiin parannettua mitatussa kohteessa. Mittausraportin avulla havaittiin paljon epäkohtia, kuten kanavien jaottelu, salauksen virheelliset asetukset ja langattoman verkon kuuluvuus ei ollut mitatussa kohteessa riittävällä tasolla. Suurin osa ongelmakohdista on nykyhetkeen saatu korjattua. Ainoastaan isoimmassa hallissa eli A-hallissa on enää käytössä vanhat tukiasemat, mutta niitä on parhaan mukaan mittaustulosten perusteella optimoitu ja siten saatu elvytettyä vielä hieman.

Asiakas on tällä hetkellä tyytyväinen langattoman verkkonsa tilaan ja mittaamisesta oli paljon apua verkon toimivuuden korjaamiseksi. Jatkossa saman tapaisiin mittauksiin on helpompi lähteä, kun on jo valmiiksi kokemusta, miten mittauslaitteet toimivat ja osaa tulkita mittaustuloksia huomattavasti paremmin. Jatkossa ei myöskään enää tarvitse miettiä, että minkälaisella kalustolla lähtee mittaamaan, kun senkin valinnasta on kokemusta. Kaiken kaikkiaan mittauksen olivat onnistuneita ja muutokset, joita saatiin aikaan, olivat hyviä.

LÄHTEET

Acrylic WiFi. 2019. Introduction to Acrylic Wi-Fi Heatmaps. Kuva otettu 10.12.2019. https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wifi-site-survey-software-acrylic-heat-maps/user-manual/

Cisco Systems. 2018. 802.11ac: The Fifth Generation of Wi-Fi. Tulostettu 08.12.2019. https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf

Coleman, D. Extreme Networks. 2012. 2.4 GHz Channel Planning. Luettu 06.12.2019. https://www.extremenetworks.com/extreme-networks-blog/2-4-ghz-channel-planning/

Ekahau. 2013. Ekahau Site Survey 6.0 released! – New and improved version with 802.11ac support. Kuva otettu 10.12.2019. https://www.ekahau.com/blog/2013/03/28/ekahau-site-survey-6-0-released-new-and-improved-version-with-802-11ac-support/

Electronicsnotes. 2019. Wi-Fi Channels, Frequencies, Bands & Bandwidths. Luettu 07.12.2019. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php

ExtremeTech. 2015. What is 802.11ax Wi-Fi, and will it really deliver 10Gbps?. Luettu 09.12.2019. https://www.extremetech.com/computing/184685-what-is-802-11ax-wifi-and-do-you-really-need-a-10gbps-connection-to-your-laptop

Geier, J. 2005. Langattomat verkot: perusteet. EDITA: Edita Publishing Oy.

Girlsgameland. 2019. Mikä on WPS? Kuva otettu 25.2.2020. https://girlsgameland.ru/fi/tehnika/chto-takoe-i-zachem-nuzhen-wps-na-routere-wps-chto-takoe-i-kak-nastroit/

Huawei Technologies Co. 2019. What is the Doppler effect?. Kuva otettu 19.2.2020. https://forum.huawei.com/enterprise/en/what-is-the-doppler-effect/thread/510221-100305

Informa PLC Informa UK Limited. 2018. Wi-Fi Alliance Launches WPA2 Enhancements and Debuts WPA3. Luettu 09.12.2019. https://www.darkreading.com/endpoint/wi-fi-alliance-launches-wpa2-enhancements-and-debuts-wpa3/d/d-id/1330762

Intel Corporation. 2019. Different Wi-Fi Protocols and Data Rates. Luettu 08.12.2019. https://www.intel.com/content/www/us/en/support/articles/000005725/network-and-io/wireless-networking.html

Network World. 2010. What is 802.1X? Everything you need to know about LAN authentication. Luettu 09.12.2019. https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html

IT Pro. 2017. Cape Networks Wireless Sensor. Kuva otettu 10.11.2019. https://www.itpro.co.uk/network-internet/30196/cape-networks-wireless-sensor

ResearchGate. 2016. Figure 1- uploaded by Alessandro Raschellà. Tulostettu 09.12.2019. https://www.researchgate.net/figure/Differences-between-SU-MIMO-and-MU-MIMO_fig1_317889335

StackExchange. 2015. OFDM transmitter bandwidth. Kuva otettu 25.2.2020. https://dsp.stackexchange.com/questions/20132/ofdm-transmitter-bandwidth

TechGenix Ltd. 2015. MU-MIMO vs SU-MIMO Wi-Fi. Luettu 08.12.2019. http://techgenix.com/mu-mimo-vs-su-mimo-wi-fi/

Tutorialspoint. 2019. Wi-Fi - Summary. Luettu 06.12.2019. https://www.tutorialspoint.com/wi-fi/wifi_summary.htm

Wikipedia. 2019. IEEE 802.1X. Kuva otettu 09.12.2019. https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802.1X_wired_protocols.png

Wireless LAN Security Interoperability Lab. 2019. What's Wrong With WEP?. Tulostettu 09.12.2019. http://www.opus1.com/www/whitepapers/whatswrong-withwep.pdf

Zak, R. Maketecheasier. 2017. How to Find the Best WiFi Channel for 5Ghz Frequency. Luettu 07.12.2019. https://www.maketecheasier.com/best-wifi-channel-for-5ghz-frequency/

LIITTEET

Liite 1. WLAN kartoitus dokumentti

Site Survey Summary (1)

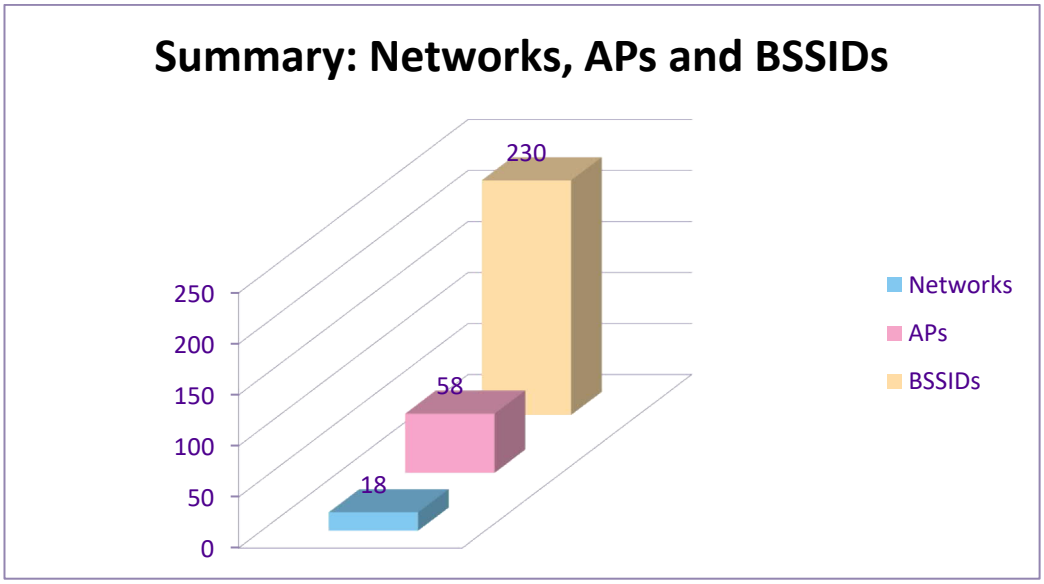
Summary of detected networks

The following table summarizes Networks, MAC addresses and physical APs grating network accesses at different locations:
- Location: Physical area where monitoring takes place.
- Networks: Number of Networks detected.
- Access Points (APs): Number of physical access points.
- BSSIDs: Access points (MAC addresses) granting network access.

The number of BSSIDs can exceed the number of physical APs because a single AP can propagate more than one network by using different MAC addresses.

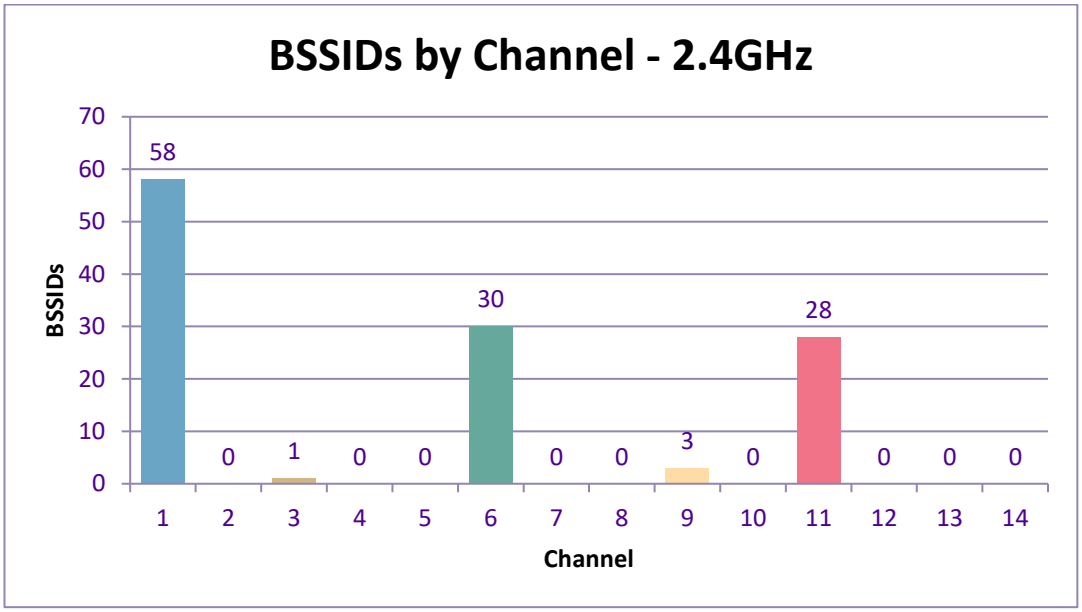
LOCATION	NET-WORKS	APS	BSSIDS
Asiakas A	18	58	230
Total	*18*	*58*	*230*

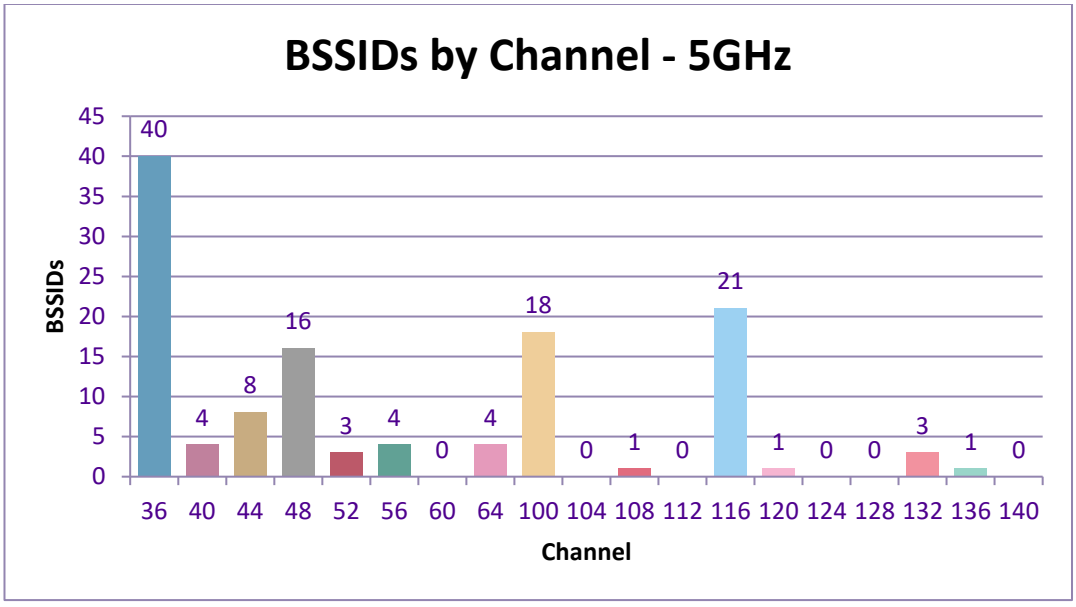
The following graph shows a comparison between the number of networks, physical APs and BSSIDs at each location.



(2)

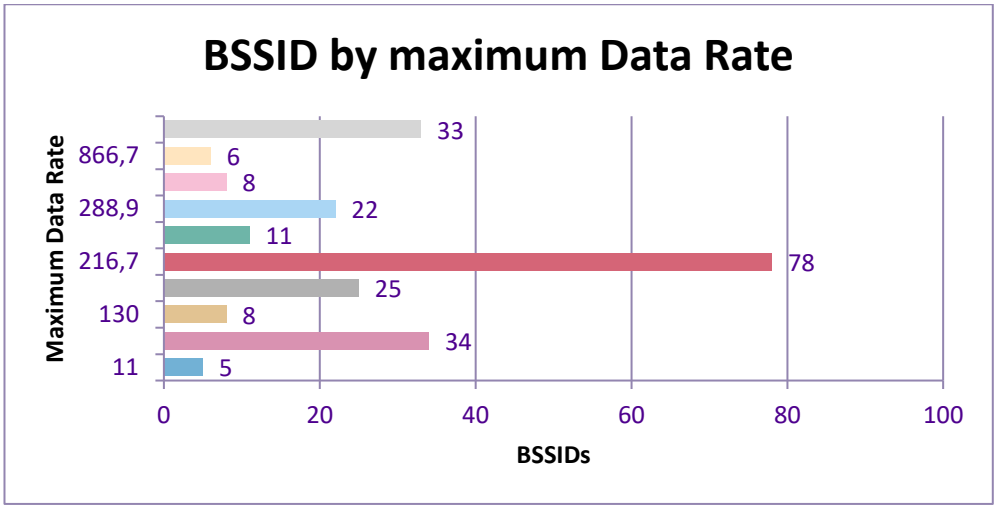
The following two graphs show the number of BSSIDs detected at each Channel, in the 2.4GHz bandwidth and in the 5GHz bandwith respectively.





The following graph shows the number of BSSIDs detected, ordered by maximum Data Rate registered value.

(3)



Networks

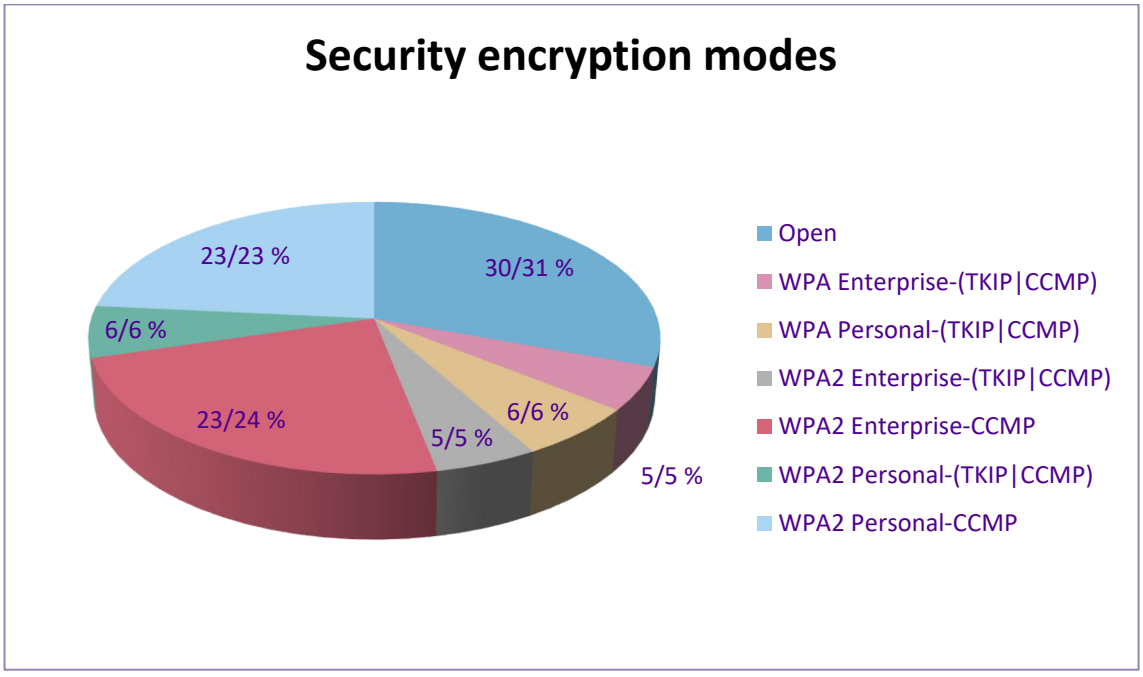
The following table contains relevant information about all the networks detected during the survey:

- SSID: Network identifier offered by the BSSID.
- BSSID: Unique device identifier (Basic Service Set Identifier)
- Channel: Identifier of the frequency on which the network is operating.
- Frequency: Value of frequency in which the network channel is operating, expressed in Mhz.
- Average RSSI: Average Signal Strength detected on each device during the survey.
- Maximum RSSI: Maximum Signal Strength detected on each device during the survey.
- Minimum RSSI: Minimum Signal Strength detected on each device during the survey.
- Security: Types of authentication and encryption supported by the network.

SSID	BSSID	CHAN	FREQ	RSSI AVG	RSSI MAX	RSSI MIN	SECURITY
WLAN1	00:13:A6:24:A6:E1	36	5180	-62	-45	-85	Open
	00:13:A6:24:A6:F0	1	2412	-56	-43	-82	Open
	00:13:A6:24:A7:41	36	5180	-58	-44	-84	Open
	00:13:A6:24:A7:48	1	2412	-53	-42	-76	Open
	00:13:A6:24:A7:50	48	5240	-56	-43	-84	Open
	00:13:A6:24:A8:E1	36	5180	-65	-49	-84	Open
	00:13:A6:24:A8:E9	9	2452	-56	-40	-84	Open
	00:13:A6:24:A8:F1	48	5240	-63	-46	-82	Open
	70:3A:0E:9D:14:A0	1	2412	-71	-47	-86	Open
	70:3A:0E:9D:14:B0	116	5580	-80	-70	-85	Open
	70:3A:0E:9D:16:80	6	2437	-71	-39	-85	Open
WLAN2	00:13:A6:24:A6:E2	36	5180	-62	-45	-84	WPA Personal
							WPA2 Personal
	00:13:A6:24:A6:F1	1	2412	-57	-43	-83	WPA Personal
							WPA2 Personal
	00:13:A6:24:A7:49	1	2412	-53	-42	-82	WPA Personal
							WPA2 Personal
	00:13:A6:24:A7:51	48	5240	-56	-43	-82	WPA Personal
							WPA2 Personal
	00:13:A6:24:A8:E8	9	2452	-56	-40	-84	WPA Personal
							WPA2 Personal
	00:13:A6:24:A8:F0	48	5240	-64	-46	-86	WPA Personal
							WPA2 Personal
	70:3A:0E:9D:14:A1	1	2412	-72	-47	-86	WPA2 Personal
	70:3A:0E:9D:14:B1	116	5580	-80	-70	-87	WPA2 Personal
	70:3A:0E:9D:16:81	6	2437	-71	-40	-85	WPA2 Personal
WLAN3	00:13:A6:24:A6:E3	36	5180	-62	-45	-85	WPA Enterprise
							WPA2 Enterprise
	00:13:A6:24:A7:4A	1	2412	-54	-42	-78	WPA Enterprise

SSID	BSSID	CHAN	FREQ	RSSI AVG	RSSI MAX	RSSI MIN	SECURITY
							WPA2 Enterprise
	00:13:A6:24:A7:52	48	5240	-57	-43	-83	WPA Enterprise
							WPA2 Enterprise
	00:13:A6:24:A8:EA	9	2452	-55	-40	-82	WPA Enterprise
							WPA2 Enterprise
	00:13:A6:24:A8:F2	48	5240	-63	-46	-81	WPA Enterprise
							WPA2 Enterprise
	70:3A:0E:9D:14:A2	1	2412	-73	-44	-86	WPA2 Enterprise
	70:3A:0E:9D:14:B2	116	5580	-81	-70	-86	WPA2 Enterprise
	70:3A:0E:9D:16:82	6	2437	-70	-40	-84	WPA2 Enterprise

The following pie chart provides a comparison between the different encryption modes implemented in the selected Stations.



Access Points

This section shows information about the physical access points detected during a survey, grouping all BSSIDs that are managed by the same physical device, as well as the number of clients connected to each one of them during the survey.

(6)

For each physical access point, its manufacturer is shown, as well as all its managed networks.

For each physical access point:
- BSSID: Associated MAC addresses granting network access.
- SSID: Network identifier offered by the BSSID.
- Channel: Identifier of the frequency associated to the network.
- Frequency: Value of the frequency associated to the network.
- 802.11: Supported standard
- Clients: Number of connected clients (if monitoring is performed on Monitor Mode or Airpcap)

00:13:A6:24:A6:E- / EXTRICOM LTD

BSSID	SSID	CHAN	FREQ	802.11
00:13:A6:24:A6:E1	WLAN1	36	5180	a, n
00:13:A6:24:A6:E2	WLAN2	36	5180	a, n
00:13:A6:24:A6:E3	WLAN3	36	5180	a, n

00:13:A6:24:A6:F- / EXTRICOM LTD

BSSID	SSID	CHAN	FREQ	802.11
00:13:A6:24:A6:F0	WLAN1	1	2412	b, g, n
00:13:A6:24:A6:F1	WLAN2	1	2412	b, g, n

70:3A:0E:9D:14:A- / ARUBA NETWORKS

BSSID	SSID	CHAN	FREQ	802.11
70:3A:0E:9D:14:A0	WLAN1	1	2412	b, g, n
70:3A:0E:9D:14:A1	WLAN2	1	2412	b, g, n
70:3A:0E:9D:14:A2	WLAN3	1	2412	b, g, n

70:3A:0E:9D:14:B- / ARUBA NETWORKS

BSSID	SSID	CHAN	FREQ	802.11
70:3A:0E:9D:14:B0	WLAN1	116	5580	a, n, ac
70:3A:0E:9D:14:B1	WLAN2	116	5580	a, n, ac
70:3A:0E:9D:14:B2	WLAN3	116	5580	a, n, ac

(7)

A8:BD:27:0D:95:A- / Hewlett Packard Enterprise

BSSID	SSID	Chan	Freq	802.11
A8:BD:27:0D:95:A0	WLAN1	11	2462	b, g, n
A8:BD:27:0D:95:A1	WLAN2	11	2462	b, g, n
A8:BD:27:0D:95:A2	WLAN3	11	2462	b, g, n

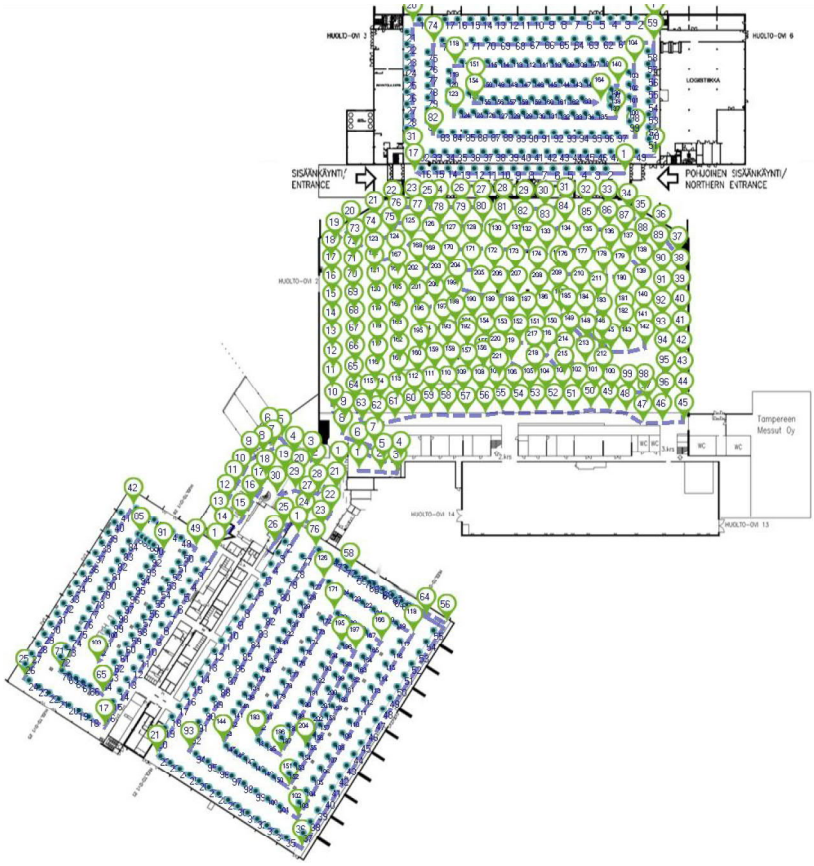
A8:BD:27:0D:95:B- / Hewlett Packard Enterprise

BSSID	SSID	Chan	Freq	802.11
A8:BD:27:0D:95:B0	WLAN1	116	5580	a, n, ac
A8:BD:27:0D:95:B1	WLAN2	116	5580	a, n, ac
A8:BD:27:0D:95:B2	WLAN3	116	5580	a, n, ac

Survey Route

The following image shows the path followed at the **Asiakas A** location during the site survey, which indicates all locations where data was collected to be later analyzed.

(8)



WiFi Quality

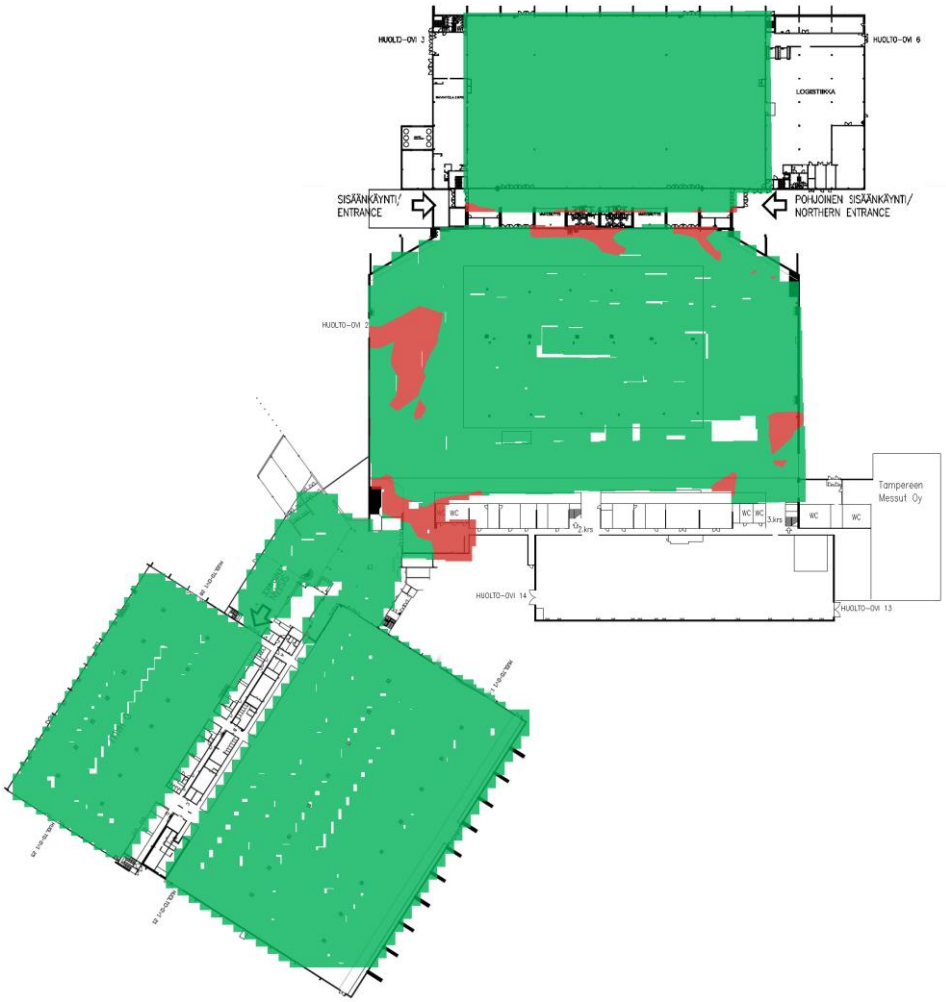
Web Browsing WiFi requirements

ASSESSMENT CONTROL	%	QUALITY
RSSI Coverage	95%	Very Good
Simultaneous RSSI Coverage	95%	Very Good
Channel Overlap	99%	Very Good
Co-Channel Interference	100 %	Excellent
Latency	N/A	N/A
Bandwidth	N/A	N/A
Packet Lost	N/A	N/A
Access Point Roaming	N/A	N/A
OVERALL WIFI QUALITY	97%	VERY GOOD

(9)

RSSI Coverage Web Browsing

The Rssi Coverage control displays those areas where the signal strength received from any of the selected access points falls below the selected threshold value. Signal strength has a significant impact on the quality of communications. Signal strength is measured in dBm, and ranges from 0 dBm (stronger) to -100 dBm (weaker).
Acceptable values range from 0 to -75 dBm. Proper communication cannot be guaranteed with lower signal strength values.



RSSI Coverage for the network WLAN1

Pass	RSSI Required greater than or equal -65 dBm
Fail	

(10)

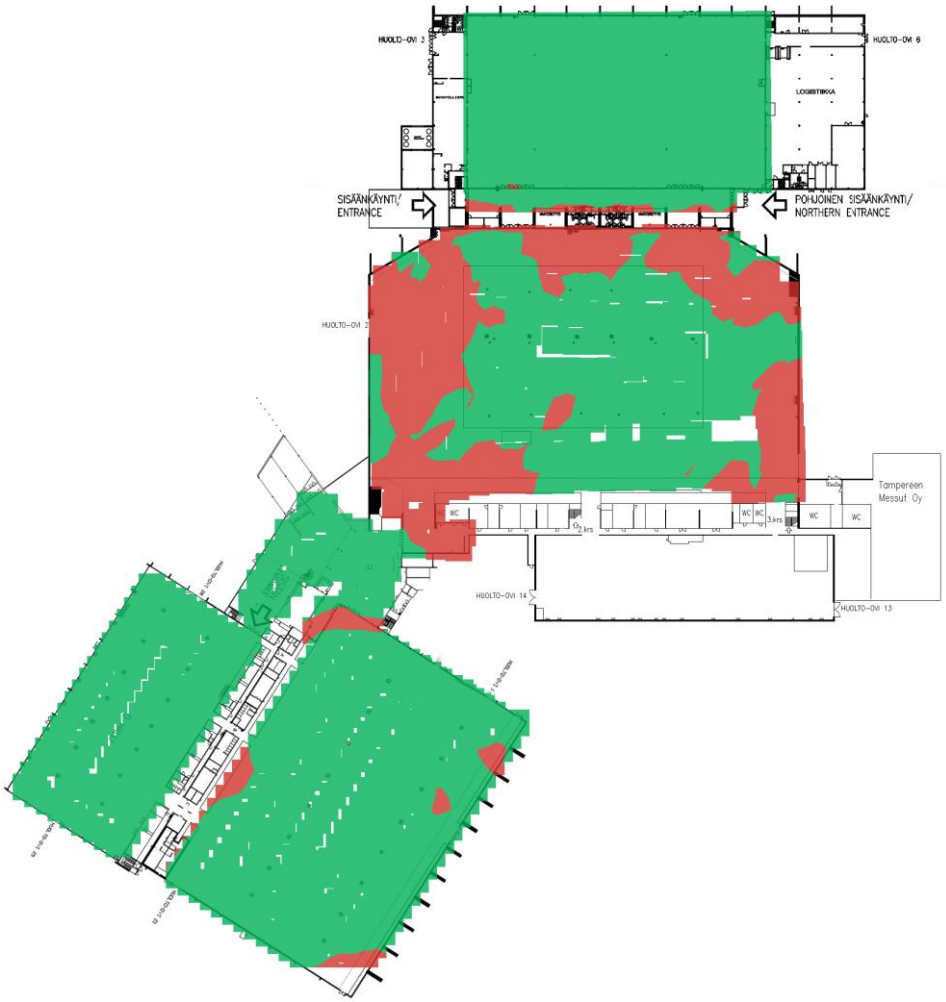
VoIP over WiFi requirements

Assessment Control	%	Quality
RSSI Coverage	80%	Poor
Simultaneous RSSI Coverage	92%	Good
Channel Overlap	99%	Very Good
Co-Channel Interference	100 %	Excellent
Latency	N/A	N/A
Bandwidth	N/A	N/A
Packet Lost	N/A	N/A
Access Point Roaming	N/A	N/A
Overall WiFi Quality	**92%**	**Good**

(11)

RSSI Coverage VOIP

The Rssi Coverage control displays those areas where the signal strength received from any of the selected access points falls below the selected threshold value. Signal strength has a significant impact on the quality of communications. Signal strength is measured in dBm, and ranges from 0 dBm (stronger) to -100 dBm (weaker).
Acceptable values range from 0 to -75 dBm. Proper communication cannot be guaranteed with lower signal strength values.



RSSI Coverage for the network WLAN1

Pass	RSSI Required greater than or equal -60 dBm
Fail	

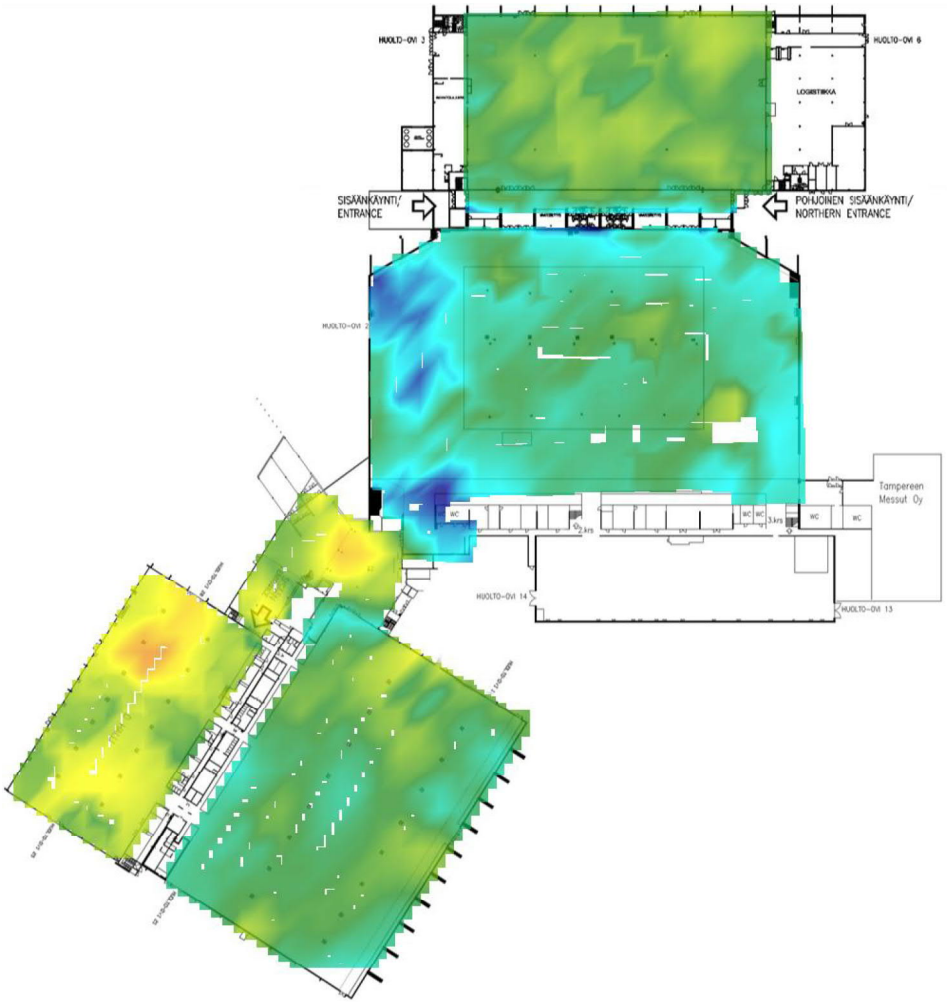
(12)

Survey

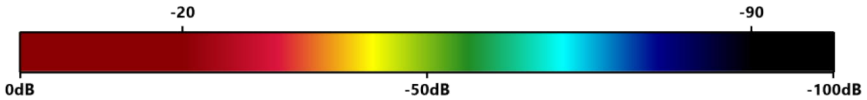
RSSI Heatmap

Signal Strength translates as how efficiently the network is reaching the surveyed area, indicating how the **WLAN1** network is received at each location.

Signal strength values range from 0 db to -100db, being -100db the worse performance. The color scheme is shown below the image.



Signal Strength Heatmap for WLAN1 Network



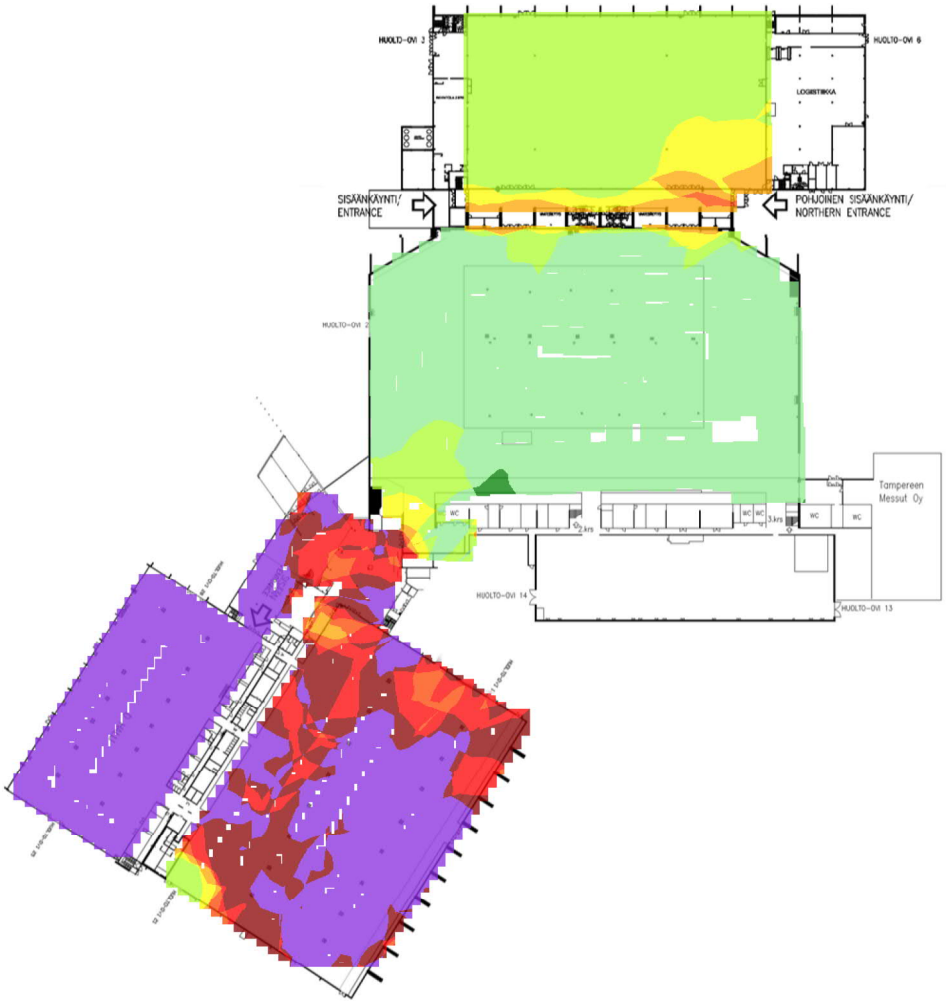
Network coverage area*	34195 m2

*This information indicates the network coverage area at a signal strength of at least:-90

Number of APs (13)

The following image shows the number of access points granting access to the **WLAN1** network that were detected within the surveyed area.

The graph reveals the existing signal overlapping from the different access points granting access to the same network.



Number of APs for WLAN1 Network

Number of APs	1	2	3	4	5	6	7	8	9	10

AP Coverage (14)

The following image shows the color-coded coverage of every AP propagating the **WLAN1** network.

If coverage from two or more channels overlap throughout the surveyed area, then the stronger signal channel is display.

Using this graph, you will be able to analyze the appropriate coverage distribution.

AP Coverage for WLAN1 Network

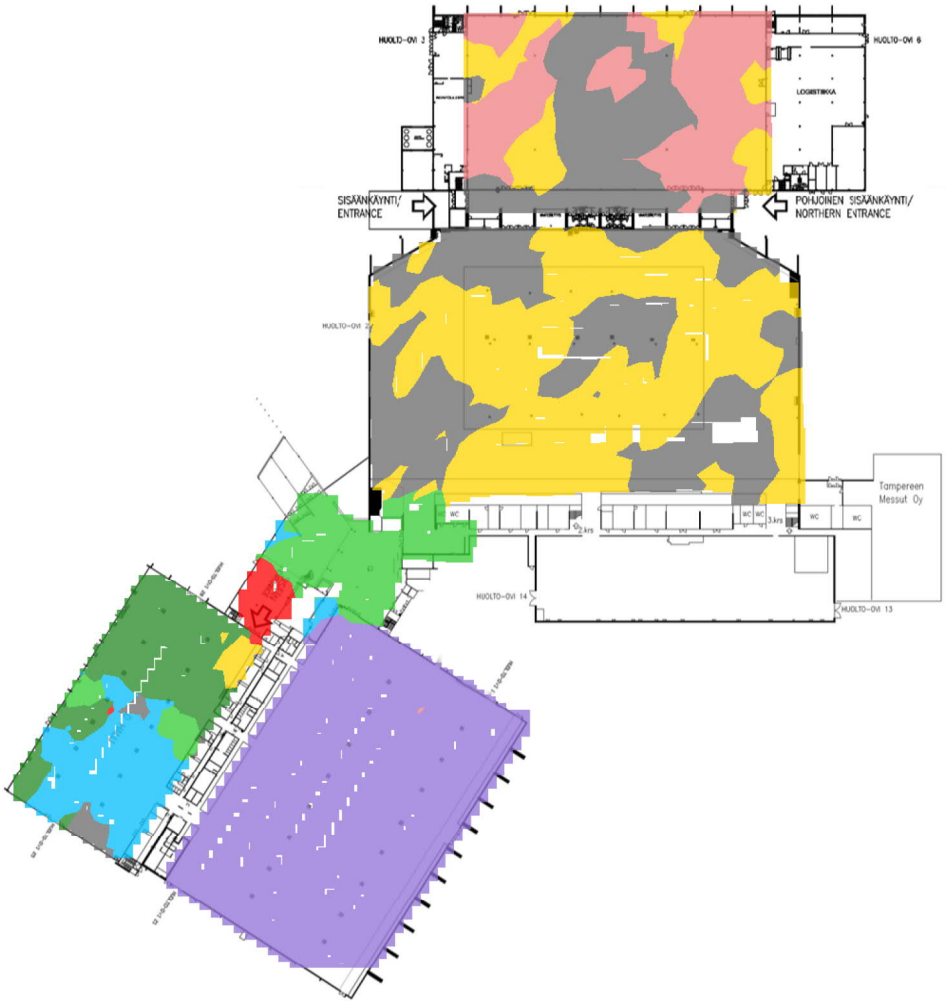
(15)

Access Point	Access Point	Access Point
00:13:A6:24:A6:E1	00:13:A6:24:A6:F0	00:13:A6:24:A7:41
00:13:A6:24:A7:48	00:13:A6:24:A7:50	00:13:A6:24:A8:E1
00:13:A6:24:A8:E9	00:13:A6:24:A8:F1	70:3A:0E:9D:14:A0
70:3A:0E:9D:14:B0	70:3A:0E:9D:16:80	70:3A:0E:9D:16:90
70:3A:0E:9D:23:80	70:3A:0E:9D:23:90	70:3A:0E:9D:35:A0
70:3A:0E:9D:35:B0	A8:BD:27:0D:95:A0	A8:BD:27:0D:95:B0
A8:BD:27:0D:9D:E0	A8:BD:27:0D:9D:F0	B4:5D:50:00:11:40
B4:5D:50:00:1D:20	B4:5D:50:00:1F:A0	B4:5D:50:00:1F:B0
B4:5D:50:00:23:E0	B4:5D:50:00:23:F0	B4:5D:50:00:24:A0
B4:5D:50:00:24:B0	B4:5D:50:00:35:40	B4:5D:50:00:35:50

Channel Coverage (16)

The following image shows the coverage range for every channel in the **WLAN1** network.

If coverage from two or more channels overlap throughout the surveyed area, then the stronger signal channel is display.

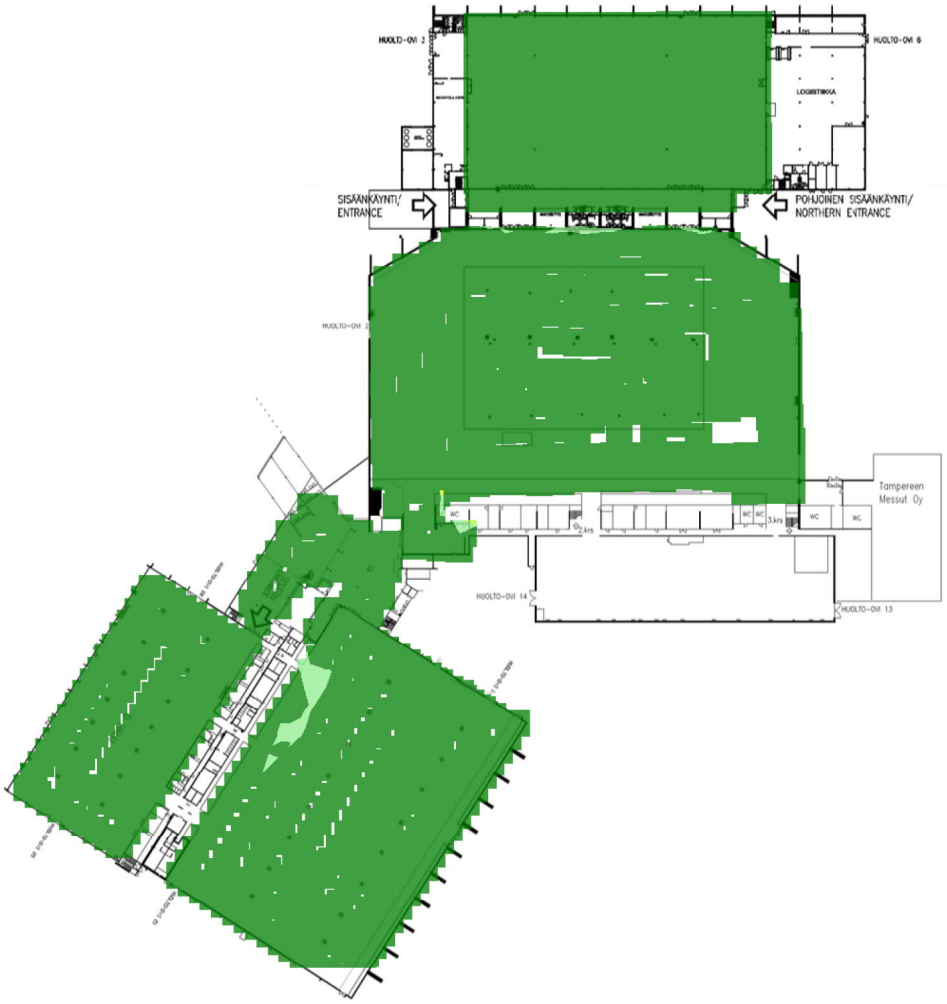


Channel Coverage for WLAN1 Network.

Channel	1	6	9	11	36	48	100	116

Channel Overlap (17)

The following image shows the coverage area for each operative channel on the **WLAN1** network, and the signal overlapping between two or more channels throughout the surveyed area.



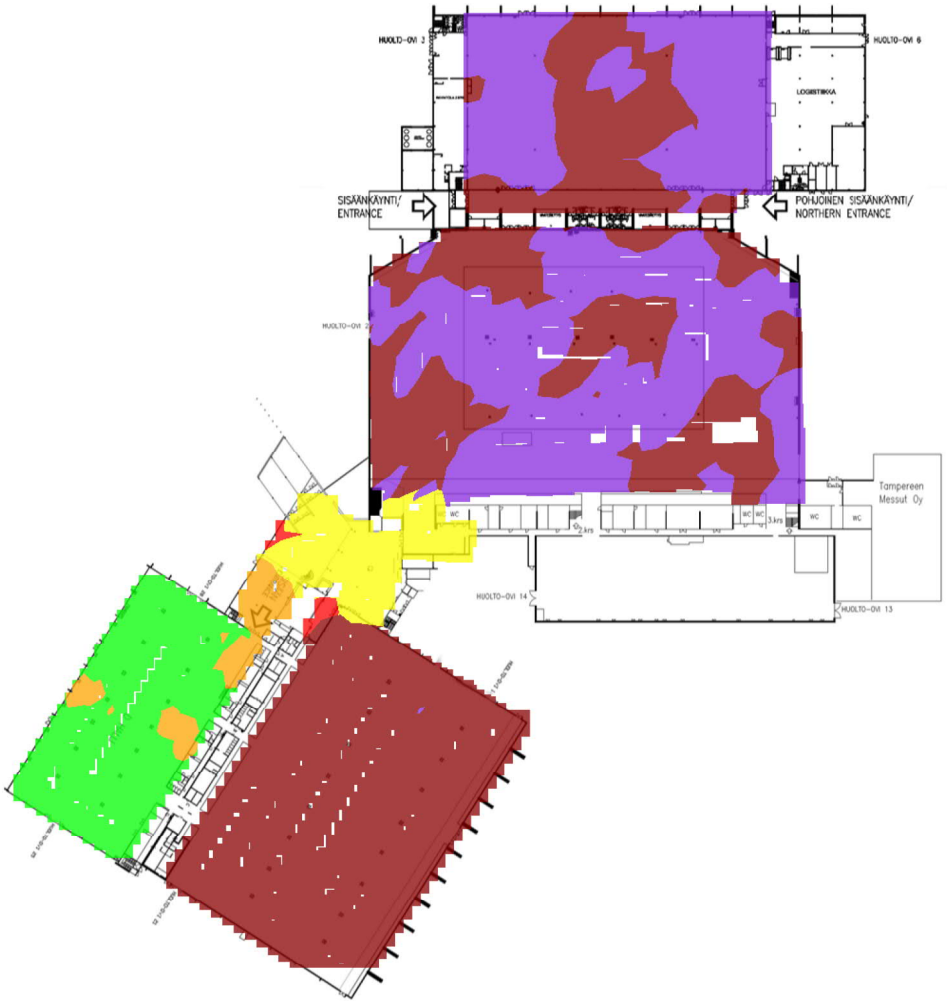
Channel Overlap for WLAN1 Network

Channel	1	2	3	4	5	6	7	8	9	10

Data Rate Heatmap (18)

The following image shows the area covered by the APs based on their data transfer rates for the **WLAN1** network throughout the surveyed area.

Data rate helps determine the maximum data transmission speed among the wireless devices connected to a Wi-Fi network.
This value allows you to establish how consistent a network is when transmitting data across the coverage area, and helps you find those areas where these values greatly differ or the network performance significantly decreases.



Data Rate for WLAN1 Network

Data Rate	Data Rate	Data Rate
130	144,4	270
288,9	866,7	1733,4