LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

LANGATTOMAN LÄHIVERKON KUULUVUUSKARTOITUS

Bring your own device -verkko

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Henri Asikainen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

ASIKAINEN, HENRI: Langattoman lähiverkon kuuluvuuskartoitus
Bring your own device -verkko

Tietoliikennetekniikan opinnäytetyö, 51 sivua, 4 sivua liitteitä

Kevät 2015

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli laatia langattoman lähiverkon parantamiseksi suunnitelma Tekniikan alalle. Suunnitelman pohjalta Lahden ammattikorkeakoulu toteuttaa tarvittavat muutokset verkon suorituskyvyn parantamiseksi. Suunnitelmassa otetaan huomioon syksyllä 2015 alkava uusi käytäntö, jossa opiskelijat voivat kirjautua koulun verkkoon omilla päätelaitteillaan.

Bring your own device -käytännön tarkoituksena on tarjota opiskelijoille mahdollisuus liittyä oppilaitoksen langattomaan lähiverkkoon omilla kannettavilla tietokoneilla, tableteilla ja puhelimilla. Tästä syystä langattoman lähiverkon on oltava suorituskyvyltään riittävä useiden satojen opiskelijoiden päivittäiseen yhtäaikaiseen käyttöön. Verkon pitää kattaa tilat, joissa opiskelijat oleilevat.

Ennen suunnitelman tekemistä täytyi kartoittaa nykyisen verkon kuuluvuus, suorituskyky ja alueella käytetyt radiotaajuus kanavat. Verkon kuuluvuutta mitattiin Ekahau site survey -ohjelmalla, joka mittaa alueen kaikkien langattomien verkkojen kuuluvuudet. Suorituskykyä mitattiin nopeustestillä ja kanavat mitattiin Fluken aircheck -testerillä. Lisäksi kartoitettiin teorialuokista pistorasioiden määrä. Pistorasioita täytyy olla riittävä määrä opiskelijoiden omille laitteille. Mittaustuloksien pohjalta alettiin parantamaan langattoman verkon kuuluvuutta ja suorituskykyä. Kuuluvuuskartoitus paljasti verkon kuuluvuudessa pieniä puutteita, jotka muutamalla uudella tukiasemalla voidaan korjata. Nopeustestit tukivat kuuluvuuskartoituksen osoittamia puutteita. Kanavamittaukset toimivat apuna määriteltäessä mille kanavalle uusia tukiasemia voidaan sijoittaa.

Ekahau site survey -ohjelmalla voidaan lisätä uusia simuloituja tukiasemia nykyiselle verkolle. Tämän avulla uuden sijoitetun tukiaseman vaikutus nähdään välittömästi rakennuksen pohjakuvassa. Ohjelma lisää automaattisesti tukiasemat parhaisiin katsomiin paikkoihin tiettyjen syötettyjen parametrien pohjalta. Lisättyjä tukiasemia voidaan itse siirtää sopivimmille paikoille ja vaikutus nähdään samantien pohjakuvassa.

Suunnitelman pohjalta tietohallinto toteuttaa parannukset verkkoon kevään ja kesän 2015 aikana.

Asiasanat: WLAN, WLAN-suunnitelma, kuuluvuuskartoitus, nopeustesti, BYOD

Lahti University of Applied Sciences
Degree Programme in Information Technology

ASIKAINEN, HENRI:

Site survey of a wireless local area network
Bring your own device -network

Bachelor's thesis in Information Technology, 51 pages, 4 pages of appendices

Spring 2015

ABSTRACT

The aim of the thesis was to make an improvement plan for the wireless local area network at the Faculty of Technology at Lahti University of Applied Sciences. Lahti University of Applied Sciences would then make improvements to the network based upon the plan. The plan will into account a new "bring your own device" policy that will start in fall 2015. Students will be able to log in to a wireless network with their own devices and access their own files.

The bring your own device policy allows students to log into the school's wireless network with their own devices such as phones, tablets and laptops. For this reason, the wireless network must perform at a high level for hundreds of users at the same time. The coverage of the wireless network also has to be sufficient.

Before making the plan, it was required to measure the coverage, speed and channels of the current WLAN. The coverage of the WLAN was measured with the Ekahau site survey program. The performance of the WLAN was measured with the Ookla speed test and the radio frequency channels used were measured with the Fluke aircheck tester. The number of power sockets was counted from theory classes. There has to be enough power sockets for all the students. All the measured results were used as a basis for planning. The site survey revealed minor weaknesses in the WLAN coverage, which can be repaired with a few new access points. The speed test supported the claim that there indeed was a need for new access points. The measurements of radio frequency channels were used to determine which channels the new access points can use.

New simulated access points can be added to the current wireless network with a program called Ekahau site survey. With this option it is possible to see the difference that a new access point makes in the school's floor plan. The software automatically adds a sufficient number of new access points to the best possible locations, based on some parameters that are filled in. It is possible to move these simulated access points to better locations. The difference is showed on the screen in real time.

The Faculty of Technology will make the improvements to the network during spring and summer 2015.

Key words: WLAN, WLAN-plan, site survey, speed test, BYOD

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, authorization ja accounting, voidaan tunnistaa toinen osapuoli tietoverkossa.
ACK	Acknowledgement, signaali, joka läheteään kuittaukseksi onnistuneesta lähetyksestä.
AD HOC	Verkko ilman keskitettyä hallinnointia.
AD	Active directory, Windows-toimialueen käyttäjätietokanta.
AES	Advanced encryption standard, lokosalausmentelmä.
BSS	Basic service set, tapa, jolla tietokoneet voivat liittyä toisiinsa langattomasti.
BYOD	Bring your own device, käytäntö, jossa verkkoon liitetään laitteita, joita organisaatio ei hallinnoi.
CCK	Complementary code keying, modulaatio, jota käytetään langattomissa verkoissa.
CRC	Cyclic redundancy check, vian tunnistamismenetelmä.
CSMA/CA	Carrier sense multiple access witch collision avoidance, WLAN -verkossa käytettävä tekniikka, jolla vältetään törmäyksiä tietoliikenneväylillä.
CSMA/CD	Carrier sense multiple access with collision detection, Ethernet -verkossa käytettävä tekniikka, jolla tunnistetaan törmäyksiä tietoliikenneväylillä.
DHCP	Dynamic host configuration protocol, verkkoprotokolla.

DRS	Dynamic rate switching, kaistanleveyden muuttaminen signaalin voimakkuuden mukaisesti
DS	Distribution system, infrastruktuuri, jolla kaksi tai useampi tukiasema voidaan yhdistää toisiinsa.
DSSS	Direct-sequence spread spectrum, suorasekventointi -modulointi.
ESS	Extended service set, yhdistää kaksi tai useampaa BSS:ää yhteen.
FHSS	Frequency-hopping spread spectrum, taajuushyppely -modulointi.
HTTP	Hypertext Transfer Protocol, protokolla, jonka avulla liikennöidään internetissä.
IDS	Intrusion detection system, voidaan havaita verkkoon tapahtuvat hyökkäykset.
IEEE	Institute of electrical and electronics engineers, yhdistys, joka kehittää teknologiaa.
IP	Internet protocol, tietojen lähettämiseen verkosta toiseen käytettävä protokolla.
IPS	Intrusion prevention system, voidaan estää verkkoon tapahtuvat hyökkäykset.
ISO	International organization for standardization, kansainvälinen organisaatio, joka asettaa standardeja.
IV	Initializing vector, alustusvektori.
LAN	Local area network, lähiverkko.

MAC	Media access control address, osoite, joka on verkkoliitännän fyysinen osoite.
MIMO	Multiple-in, multiple-out, tekniikka, joka mahdollistaa useampien antennien käytön samassa tukiasemassa.
NAT	Network address translation, osoitteenmuunnos -tekniikka.
OFDM	Orthogonal Frequency Division Multiplexing, modulointitekniikka.
OSI	Open systems interconnection, standardi tietokoneverkkojen kommunikointiin.
POE	Power over Ethernet, käyttöjännitteen syöttäminen parikaapelin avulla.
RC4	Rivest cipher 4, salausalgoritmi.
SSID	Service set identifier, langattoman lähiverkon nimi.
TKIP	Temporal key integrity protocol, tietoturvaprotokolla.
WDS	Wireless distribution system, WDS:n avulla langattomat tukiasemat voivat yhdistyä toisiinsa langattomasti.
WEP	Wired equivalent privacy, salausmenetelmä.
WI-FI	Markkinallinen termi WLANille. Laitteet saavat Wi-Fi -merkinnän, jos noudattavat tiettyjä asetuksia.
WLAN	Wireless local area network, langaton lähiverkko.

VOIP	Voice over IP, tekniikka, jonka avulla ääntä voidaan lähettää ip-tekniikan ylitse.
WPA	Wi-fi protected access, salausmenetelmä.
WPA2	Wi-fi protected access, salausmenetelmän uudempi versio.
VPN	Virtual private network, virtuaalinen lähiverkko.

1 JOHDANTO

Opinnäytetyön tavoitteena on Lahden ammattikorkeakoulun omistaman Tekniikan alan oppilaitoksen langattoman lähiverkon mittaaminen ja suunnitelman luominen langattoman lähiverkon parantamiseksi. Suunnitelman perusteella tietohallinto päivittää verkon ajantasalle vastaamaan syksyllä 2015 käyttöön otettavaa BYOD (Bring Your Own Device) -käytäntöä.

Opinnäytetyö tehdään Lahden ammattikorkeakoululle. Mittaukset suoritetaan Ståhlberginkatu 10:ssä Tekniikan alan oppilaitoksella. Oppilaitos tarjoaa kaikki työkalut opinnäytetyön suorittamiseen. Työssä käytettävät työkalut ovat entuudestaan tuttuja aikaisemmilta opinnoilta.

Opinnäytetyössä keskitytään mittaamaan huolellisesti oppilaitoksen langattoman lähiverkon kuuluvuus kaikilla alueilla, joihin opiskelijoilla on pääsy. Mittaustulosten perusteella laaditaan suunnitelma verkon parantamiseksi. Mittauksiin käytetään kuuluvuuskartoitusohjelmaa, nopeustestiä ja kanavamittauslaitetta. Suunnitelman tekemiseen käytetään kuuluvuuskartoitusohjelman suunnitteluominaisuutta ja nopeustestien sekä kanavamittauksien tuloksia.

Teoriaosuudessa käydään ensiksi läpi tietoverkkoja yleisesti, minkä jälkeen syvennytään langattoman lähiverkon ominaisuuksiin. Viimeiseksi kerrotaan Bring Your Own Device -käytännön tuomista eduista ja haasteista. Tutustuessaan näihin aiheisiin lukija saa käsityksen langattoman lähiverkon toiminnasta ja BYOD:n ominaisuuksista. Teoriaosuuden lähteinä on käytetty internetistä löytyviä artikkeleita ja kirjoja.

Lahden ammattikorkeakoulun Tekniikan ala järjestää koulutusta konetekniikassa, prosessi- ja materiaalitekniikassa, tieto- ja viestintätekniikassa ja energia- ja ympäristötekniikassa. Opintoja voidaan suorittaa kokopäiväisesti tai joustavina monimuoto-opintoina.

2 TIETOVERKKO

Tietokoneita yhdistetään verkkoon samasta syystä, kuin ihmiset yhdistyvät sosiaalisiin piireihin, jotta saadaan aikaan yhdessä jotain, mitä ei itsekseen saa aikaiseksi. Tietokoneita alettiin yhdistää toisiin tietokoneisiin, jotta hyödynnettäisi useiden tietokoneiden laskentatehoa yhtenäisesti samassa verkossa. Verkot kasvoivat pienistä lähiverkoista pieniin kampusverkkoihin, joista ne kasvoivat kaupunkien välisiksi verkoiksi ja lopulta globaaleiksi verkoiksi. (Silviu 2010, 5.)

Tietoverkko on joukko tietokoneita, jotka yhdistetään keskenään, jotta mahdollistetaan kommunikointi toisten tietokoneiden kanssa. Tietokoneet yhdistetään joko langallisesti tai langattomasti. Kommunikointia ohjaavat tietokoneiden tai verkkolaitteiden verkkosovellukset. Verkkolaitteita ovat laitteet, jotka voivat olla kahden yhdistetyn tietokoneen välissä. Verkkolaitteita ovat muun muuassa kytkimet, hubit, reitittimet, toistajat ja palomuurit. Päätelaitteita ovat kaikki laitteet, jotka kytkeytyvät käyttääkseen verkkoa. Päätelaitteita ovat esimerkiksi tietokoneet, palvelimet, työasemat, tabletit, älypuhelimet ja kannettavat tietokoneet. (Silviu 2010, 6.)

Verkkoa voidaan hyödyntää moneen käyttötarkoitukseen:

- HTTP
- sähköposti
- tiedostojen jakaminen
- etäyhteys
- VoiP
- rinnakkaisprosessointi.

Nämä ovat vain yleisimpiä verkon käyttötarkoituksia, lisäksi on vielä monia muita sovelluksia ja käyttötarkoituksia. (Silviu 2010, 7.)

2.1 Osoitteet

Verkossa liikennöimiseen tarvitaan osoitteita, joiden avulla voidaan suunnistaa paikasta toiseen. IP-osoitteella (Internet protocol) luodaan yhteys ylemmän tason verkkoprotokolliin ja sovelluksiin. IP-osoite on numeroista koostuva sarja, joka on muotoa 192.168.100.101. MAC-osoitteen (Media access control address) avulla luodaan yhteys verkkokorttien välillä. MAC-osoitteet ovat heksadesimaalisia ja ovat muotoa 1A:2B:4C:67:89:FE. (Silviu 2010, 7 – 8.)

IP-osoitteet on jaettu 5 luokkaan, joiden mukaan Internetin runkoverkon liikenteen reititys tapahtuu. Nykyään taulukossa näkyvistä luokista on luovuttu jo, mutta liikennöinti pohjautuu näihin luokkiin edelleen. Ongelmana osoiteluokissa oli se, että toiset luokat olivat liian isoja ja toiset taas olivat liian pieniä. (TAULUKKO 1.) (Wikipedia 2013a.)

TAULUKKO 1. Osoiteluokat (Wikipedia 2013a)

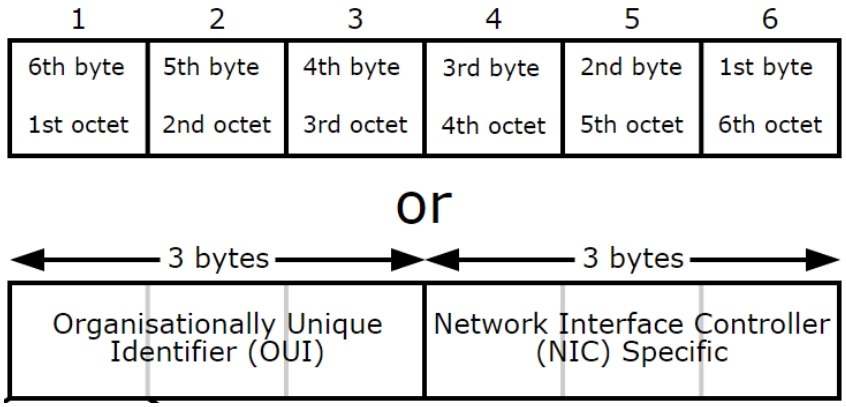
Verkon luokka	Verkon peite	Verkon osoite
A	255.0.0.0	1.0.0.0 – 126.255.255.255
B	255.255.0.0	128.0.0.0 – 191.255.255.255
C	255.255.255.0	192.0.0.0 - 223.255.255.255
D	255.255.255.0	224.0.0.0 – 239.255.255.255
E	-	240.0.0.0 – 255.255.255.255

TAULUKKO 2. Yksityisosoitteet (Wikipedia 2013a)

Verkon osoite	Verkon peite
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

Yksityisosoitteita on kolme ryhmää, jotka on varattu yksityiskäyttöön. Standardin mukaan niitä ei reititetä internetissä. Jos näitä osoitteita halutaan käyttää sisäverkossa ja halutaan kytkeä laite internetiin, on käytettävä osoitteet muuntavaa reititintä. Yksityisosoitteet on varattu ”kotikäyttöön”, jotta ne asetettaisiin sisäverkkojen osoitteiksi. (TAULUKKO 2.) (Wikipedia 2013a.)

MAC-osoitteet ovat verkkosovittimen yksilöiviä osoitteita, jotka on kirjoitettu fyysisesti verkkokortteihin. MAC-osoitetta on mahdollista myös vaihtaa käyttöjärjestelmästä riippuen. MAC-osoite koostuu kuudesta kaksinumeroisesta heksadesimaalisesta luvusta. Kolme ensimmäistä lukuparia on valmistajan käytössä tunnistamiseen ja kolme jälkimmäistä lukuparia on verkkosovittimen yksilöivä sarjanumero. MAC-osoitteita voidaan muuntaa IP-osoitteiksi reverse address resolution -protokollan avulla. IP-osoitteita voidaan myös muuntaa MAC-osoitteiksi address resolution -protokollan avulla. (KUVIO 1.) (Wikipedia 2015b.)



KUVIO 1. MAC-osoitteen rakenne (Wikipedia 2015b)

2.2 OSI-malli

OSI-malli (Open systems interconnection) on tiedonsiirtoprotokollien referenssimalli, joka on ISO:n (International organization for standardization) määrittelemä kansainvälinen standardi. OSI-mallissa on 7 kerrosta, joista jokaisella on tiedonsiirrossa oma merkittävä rooli. (KUVIO 2.) (Silviu 2010, 15.)

KUVIO 2. OSI-malli (Wikipedia 2015c)

OSI-mallin ylimmän kerroksen, sovelluskerroksen tehtävänä on hoitaa sovelluksien näyttäminen käyttäjälle. Sovelluskerroksessa tapahtuu

esimerkiksi internetin selaaminen, sähköpostin käyttäminen ja tiedostojen siirtäminen (FTP, NFS). Sovelluskerros toimii rajapintana käyttäjälle. (Silviu 2010, 16.)

Esitystapakerroksen tehtävänä on muokata data sopivaan muotoon sovelluskerrokselle ja kuljetuskerrokselle. Esitystapakerroksen ansiosta kuvat, sähköpostit ja muut tiedostot näkyvät samanlaisina kaikilla käyttäjillä. (Silviu 2010, 17.)

Istuntokerroksen vastuulla on avata yhteyksiä ja kanavia, joilla viestintä voi tapahtua kahden tai useamman osallistujan välillä. Istuntokerroksen vastuulla on myös tunnistautuminen. Jotkin sovellukset vaativat tunnistautumisen ennen kuin istunto voidaan avata etäisen päätelaitteen kanssa. (Silviu 2010, 17.)

Kuljetuskerroksen tehtävä on muodostaa kuljetettava data sopivanlaiseen muotoon kuljetettavaksi verkossa. Data voi kulkea verkossa eri reittiä päätepisteeseen, joten data saattaa saapua eri järjestyksessä perille, kuin lähetettäessä. Kuljetuskerroksen tehtävänä on järjestää saapuva data oikeaan järjestykseen ja kasata se taas yhteen muotoon. (Silviu 2010, 18)

Verkkokerroksella datapaketeille valitaan paras mahdollinen reitti päämäärään. Verkkokerros asettaa lähde- ja kohde IP-osoitteet datapaketille. IP-, IPX-, AppleTalk- ja SNA-protokollat operoivat verkkokerroksella. Reititin on verkkokerroksella operoiva fyysinen laite. (Silviu 2010, 18.)

Siirtokerroksella data asetetaan siirtotielle. Siirtokerroksella käytetään MAC-osoitteita reitittämiseen. Siirtokerroksen vastuulla on reitittää data paikallisesti. Lähiverkon sisällä datapaketit liikkuvat MAC-osoitteita käyttäen. Siirtokerros saa verkkokerrokselta datapaketit, jotka se asettaa kehyksiin, joissa on paikalliset osoitetiedot. Lopuksi data siirretään fyysiselle kerrokselle siirtämistä varten. Kytkimet ovat siirtokerroksen laitteita. (Silviu 2010, 19.)

Fyysinen kerros on vastuussa datan siirtämisestä lähettäjän ja vastaanottajan välillä joko optisesti, sähköisesti tai radiotaajuuksia käyttäen. Fyysisellä kerroksella oleva data liikkuu aina bitteinä, eli 1:nä ja 0:na. Hubit ja toistajat (repeaters) ovat fyysisen kerroksen laitteita. Hubit vahvistavat signaalia, joten ne toimivat samalla myös toistajina. (Silviu 2010, 19.)

3 WLAN

WLAN (Wireless local area network) tulee sanoista wireless local area network, joka tarkoittaa suomeksi langatonta lähiverkkoa. WLANin avulla voidaan yhdistää laitteita verkkoon ilman kaapeleita. WLAN:lla tarkoitetaan yleensä IEEE 802.11 -standardia (Institute of electrical and electronics engineers), mutta myös muita langattoman lähiverkon standardeja on olemassa. (Wikipedia 2015d.)

WLAN:a kutsutaan joskus virheellisesti myös nimellä Wi-Fi. Wi-Fi on tavaramerkki, jota laitevalmistajat käyttävät laatutason symbolina IEEE 802.11 -standardin tuotteille. (Wikipedia 2015d.)

3.1 WLAN-arkkitehtuuri

WLAN-arkkitehtuurilla tarkoitetaan, millä tavalla langattomassa lähiverkossa eri komponentit toimivat keskenään. Arkkitehtuuri sisältää erilaisia tapoja verkon luomiseen. (Wikipedia 2015d.)

Asemiksi kutsutaan kaikkia laitteita, jotka kykenevät kytkeytymään langattomaan lähiverkkoon. Arkkitehtuurit määrittävät, miten asemat kytkeytyvät toisiinsa. Basic service setistä (BSS) on kaksi versiota, joissa toisessa asemat kytkeytyvät toisiinsa ilman tukiasemaa ja toisessa versiossa laitteet kytkeytyvät tukiaseman kautta. Extended service set (ESS) on joukko yhdistyneitä BSS:jä. Distribution system (DS) yhdistää tukiasemat ESS:ään. (Wikipedia 2015d.)

3.1.1 WLAN-asemat

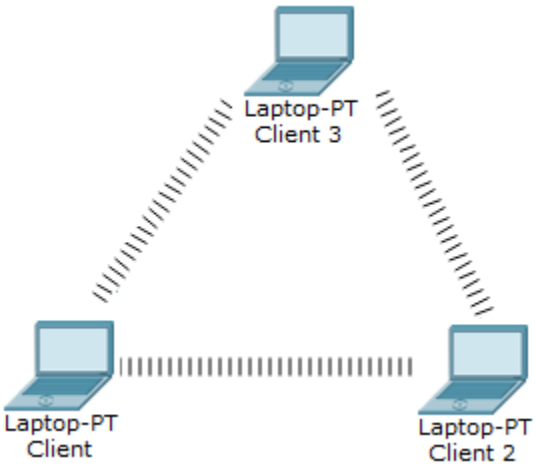
Puhuttaessa IEEE 802.11 -standardista asemaksi kutsutaan jokaista tietokonetta, mobiililaitetta tai muuta laitetta, joka pystyy yhdistymään langattomaan lähiverkkoon. Liikutettavan (mobile) ja siirrettävän (portable) aseman ero on, että liikutettava asema on yhteydessä lähiverkkoon liikkeessä ja siirrettävä asema on yhteydessä vain paikallaan ollessaan. Asemia voi olla kahdenlaisia: asiakkaita (client) tai tukiasemia (access

point). Asiakkaat voivat olla kannettavia tietokoneita, puhelimia tai tabletteja Tukiasemia ovat langattomat reitittimet. Tukiasemat lähettävät ja vastaanottavat radiotaajuuksia mahdollistaen kommunikaation muiden langattomien laitteiden kanssa. (Tutorial-Reports 2013.)

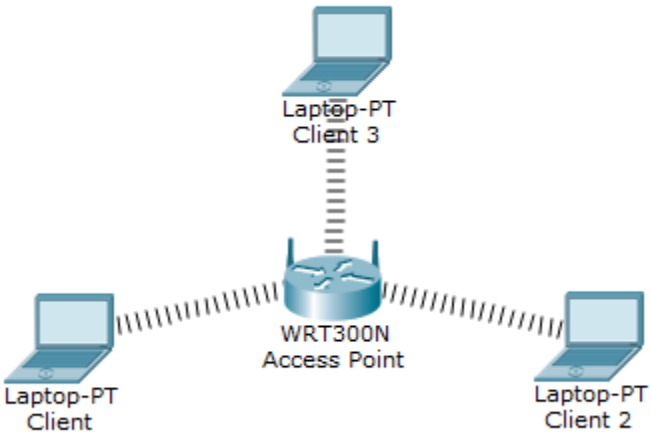
3.1.2 Basic service set

BSS:ä (Basic service set) on kaksi eri versiota: Independent BSS ja infrastructure BSS. Independent BSS:ssä asemat yhdistyvät toisiinsa ilman tukiasemaa muduostaen Ad hoc-verkon. (KUVIO 3.) (Tutorial-Reports 2013.)

Infrastructure BSS:ssä asemat yhdistyvät tukiaseman kautta toisiinsa, muodostaen infrastruktuuriverkon. Infrastructure BSS:ssä kaikki päätelaitteet keskustelevat tukiaseman kautta. (KUVIO 4.) (Tutorial-Reports 2013.)



KUVIO 3. Independent BSS (Tutorial-Reports 2013)

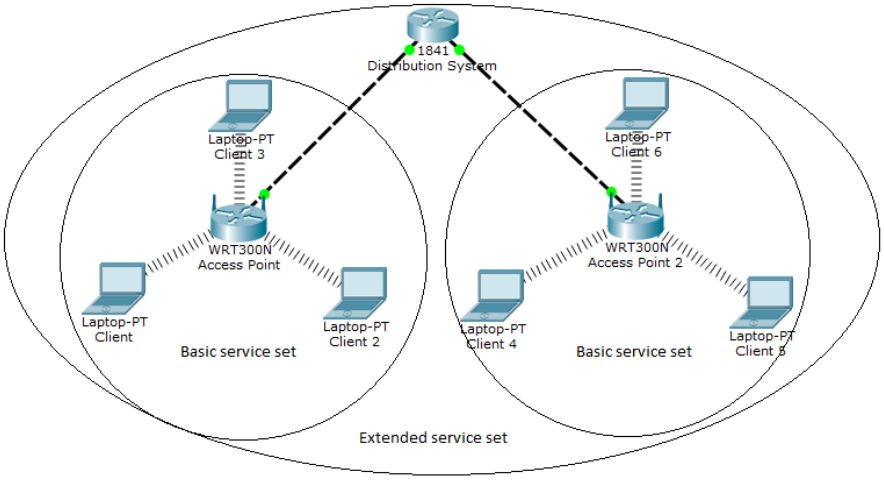


KUVIO 4. Infrastructure BSS (Tutorial-Reports 2013)

3.1.3 Extended service set

ESS (Extended service set) koostuu useammasta infrastructure BSS:stä. ESS:t yhdistää joko langaton tai langallinen Distribution System. (KUVIO 5.) (Tutorial-Reports 2013.)

ESS:n avulla saadaan verkko kattamaan suuria alueita, mikä mahdollistaa esimerkiksi langattoman lähiverkon kuuluvuuden suurissa rakennuksissa. Päätelaitteet voivat liikkua ESS:n sisällä infrastructure BSS:stä toiseen. (KUVIO 5.) (Tutorial-Reports 2013.)

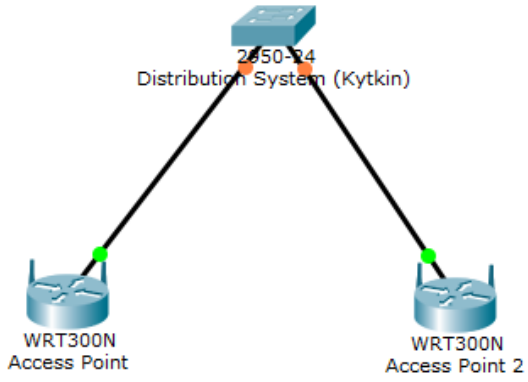


KUVIO 5. Extended service set (Tutorial-Reports 2013)

3.1.4 Distribution system

DS (Distribution system) on infrastruktuuri, jolla kaksi tai useampi tukiasemaa voidaan yhdistää toisiinsa. DS:n avulla voidaan laajentaa verkon kuuluvuutta hyödyntäen roamingia tukiasemasta toiseen. Käytetyimmät DS:t ovat WDS (Wireless distribution system) ja mesh. (Wikipedia 2015d.)

Distribution system on yleensä kytkin, mikäli käytetään langallista DS:ä (KUVIO 6). Langaton DS muodostuu WDS:stä, jossa tukiasemat yhdistyvät toisiinsa käyttäen samoja salausavaimia ja radiokanavia. SSID:kin (Service set identifier) on yleensä sama, mutta se ei ole pakollinen. WDS:ää käytetään yleensä point-to-point- ja point-to-multi -yhteyksiin. Toinen langaton DS on mesh-verkko, jossa 1 tukiasema toimii gatewayna langalliseen verkkoon. Tätä tukiasemaa kutsutaan isäntä -tukiasemaksi. Tämän tukiaseman tehtävä on lähettää SSID:tä muille tukiasemille ja toimia yhdyskäytävänä langalliseen verkkoon. (KUVIO 7.) (Wikipedia 2015d.)



KUVIO 6. Langallinen DS. (Wikipedia 2015d)

KUVIO 7. Langaton DS. (Wikipedia 2015d)

3.2 WLAN-tyypit

IEEE 802.11 standardin määrittelemällä langattomalla lähiverkolla on kaksi tapaa, jolla se voi operoida: ad hoc- ja infrastruktuuri. Ad hocia käytetään pääasiassa tilapäisen verkon luomiseen, kun taas infrastruktuurilla toteutetaan pysyvämpi verkko. (Wikipedia 2015d)

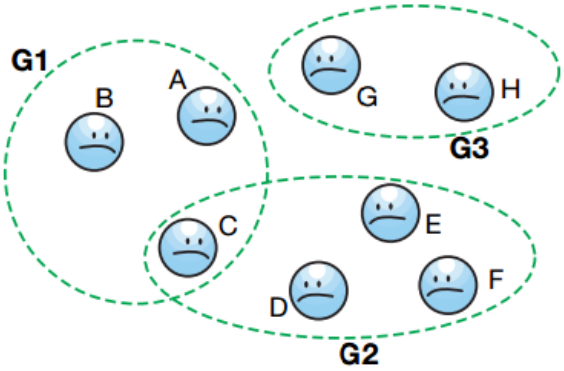
Ad hocia käytettäessä laitteet kommunikoivat peer-to-peer -tyyliin. Infrastruktuuria käytettäessä laitteet keskustelevat tukiaseman kautta, joka toimii siltana toisiin verkkoihin. (Wikipedia 2015d)

3.2.1 Ad hoc

Ad hoc -verkko on ilman keskitettyä hallinnointia toteutettu verkko, joka koostuu solmuista (nodes), jotka käyttävät langatonta sovitinta lähettääkseen paketteja. Solmut toimivat samalla myös reitittiminä toisilleen. Solmut lähettävät paketteja toisilleen, mutta myös reitittävät muilta saamiaan paketteja eteenpäin. (Frodigh, Johansson & Larsson 2000.)

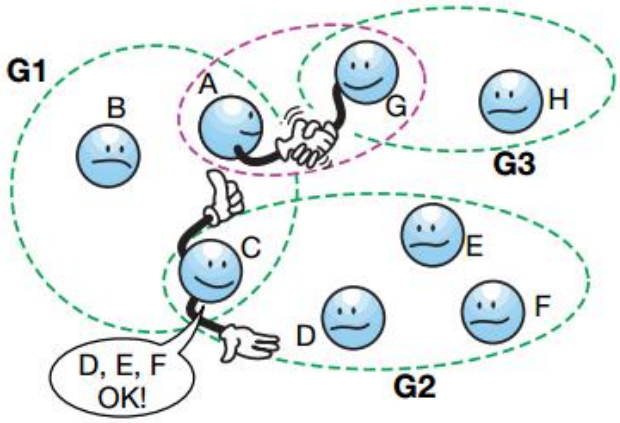
Ad hoc -verkot muodostuvat, kun solmut ovat fyysisesti lähellä toisiaan. Kaikki solmut eivät luota toisiinsa automaattisesti, vaan tätä varten on kehitetty julkinen avain, jota jaetaan luottamuksien syntyessä. Solmut voivat myös jakaa omia luotuja yhteyksiä eteenpäin muille ryhmän sisällä oleville solmuille. Ad hoc -verkot voivat kasvaa suuriksi nopeastikin. (Frodigh, Johansson & Larsson 2000.)

Kuvataan tilanne, miten ad hoc -verkko muodostuu. Alkutilanteessa on ryhmät G1, G2 ja G3, jotka sisältävät solmut A, B, C, D, E, F, G ja H. Solmu C kuuluu sekä G1- , että G2 -ryhmään. Ryhmien välistä kommunikointia ei tapahdu, kuin solmun C kautta ryhmien G1 ja G2 välillä. Ryhmä G3 ei kommunikoi minkään ryhmän kanssa. (KUVIO 8.)



KUVIO 8. Ad hoc -verkon alkutilanne (Frodigh, Johansson & Larsson 2000)

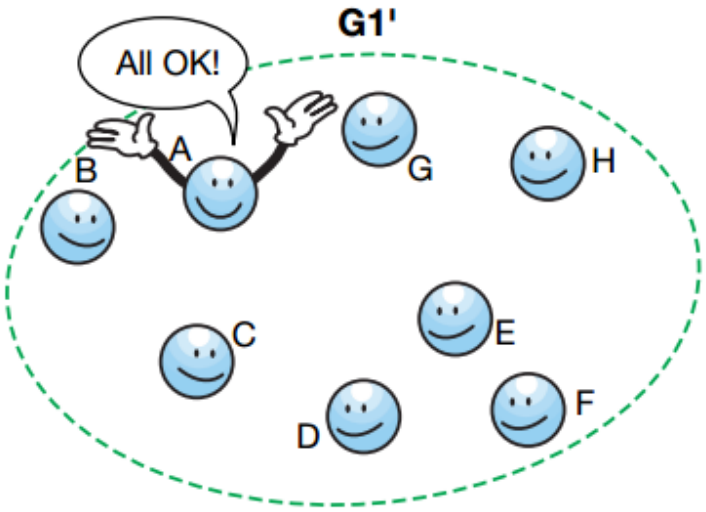
Solmu C jakaa solmuilta D, E ja F saamansa julkiset avaimet isäntäsolmulle A. Solmu A muodostaa manuaalisesti uuden luotettavan yhteyden solmun G kanssa, jolloin ryhmä G1 voi epäsuorasti kommunikoida ryhmän G3 kanssa, solmujen A-G kautta. Isäntäsolmu A lähettää julkiset avaimet kaikille ryhmäläisille, jolloin ne lisätään myös muille solmuille. Kommunikointia tapahtuu nyt useamman solmun ja useamman ryhmän välillä. (KUVIO 9.)



KUVIO 9. Luottamusten luominen (Frodigh, Johansson & Larsson 2000)

Solmu G lähettää solmulta H saamansa julkisen avaimen isäntäsolmulle A. Solmu A lähettää taas julkiset avaimet kaikille, jolloin muodostuu yksi iso ryhmä G1, jossa kaikki solmut voivat kommunikoida keskenään.

Tämän protokollan mukaan muodostetaan uusia luotettuja yhteyksiä ad hoc verkossa. (KUVIO 10.)



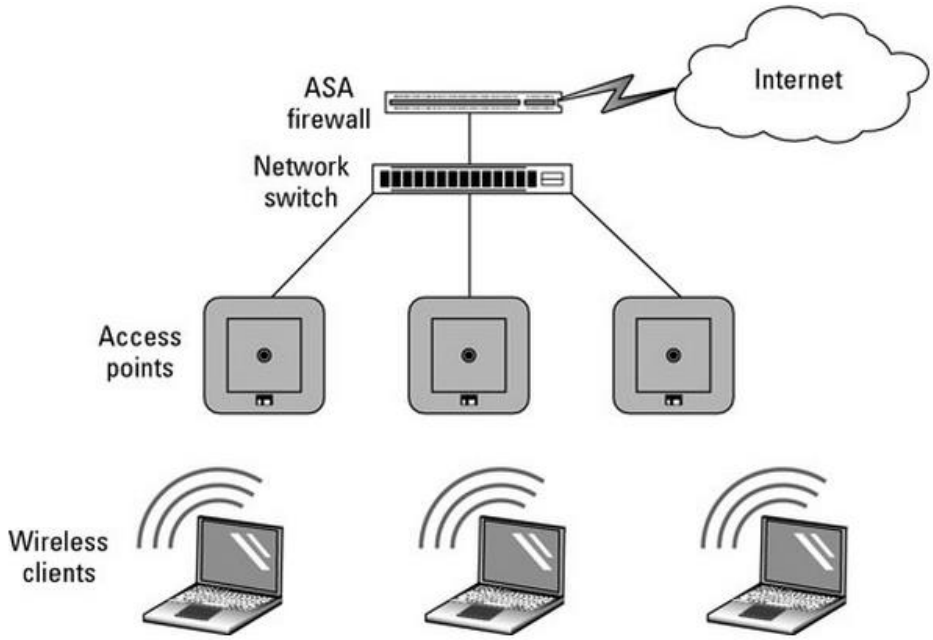
KUVIO 10. Lopputilanne (Frodigh, Johansson & Larsson 2000)

3.2.2 Infrastruktuuri

WLAN -infrastruktuuria käytetään yleensä silloin kun rakennetaan pysyvämpää verkkoratkaisua. Infrastruktuurissa on aina vähintään yksi tukiasema, jonka kautta solmut kommunikoivat keskenään. Lähekkäin olevat solmut eivät kommunikoi suoraan toistensa kanssa, vaan kaikki pakettiliikenne kulkee aina tukiaseman kautta. (Silviu 2010, 679.)

Infrastruktuurin etuna ad hoc -verkkoon on se, että verkkoa on helpompi hallita. Tukiasemia lisäämällä saadaan verkkoon lisää kuuluvuutta. Kaikki säännöt ja asetukset koskevat myös uusia lisättyjä tukiasemia. Tukiasemia voidaan hallinoida keskitetysti. (Silviu 2010, 679.)

Kuvion infrastruktuurissa on palomuuri, joka suojaa verkon liikennettä hyökkäyksiltä ja asiattomalta verkkoliikenteeltä. Palomuuri on kytkettynä kytkimeen jonka kautta jaetaan verkko tukiasemille. Tukiasemat jakavat langatonta verkkoa solmuille. (KUVIO 11.)



KUVIO 11. Infrastruktuuri (Silviu 2010, 680)

3.3 Radiotaajuudet

Radiotaajudet voidaan jakaa kahteen ryhmään: lisensoituihin ja lisensittömiin alueisiin. Lisenssejä radiotaajuuksille myöntää valtio. Lisensoituja radiotaajuuksia ovat esimerkiksi:

- AM -lähetykset
- FM -lähetykset
- matkapuhelinverkko.

Lisensittömiä radiotaajuuksia jaetaan käyttäjille, mutta näiden radiotaajuuksien käyttöön ei tarvita lisenssiä, vaan käytettävän laitteen pitää olla säännösten mukainen. Lisensittömiä radiotaajuuksia ovat esimerkiksi:

- Industryn, Scientificin, Medicalin (ISM) laitteet, jotka käyttävät taajuuksia 900 MHz, 2,4 GHz ja 5 GHz

- Unlicensed National Information Infrastructure (U-NII) määrittää taajuudet langattomille laitteille, kuten tukiasemille ja reitittimille 5 GHz:n taajuudella
- Unlicensed Personal Communications Services (UPCS) määrittää taajuudet laitteille, jotka toimivat 1,9 GHz:n taajuudella.

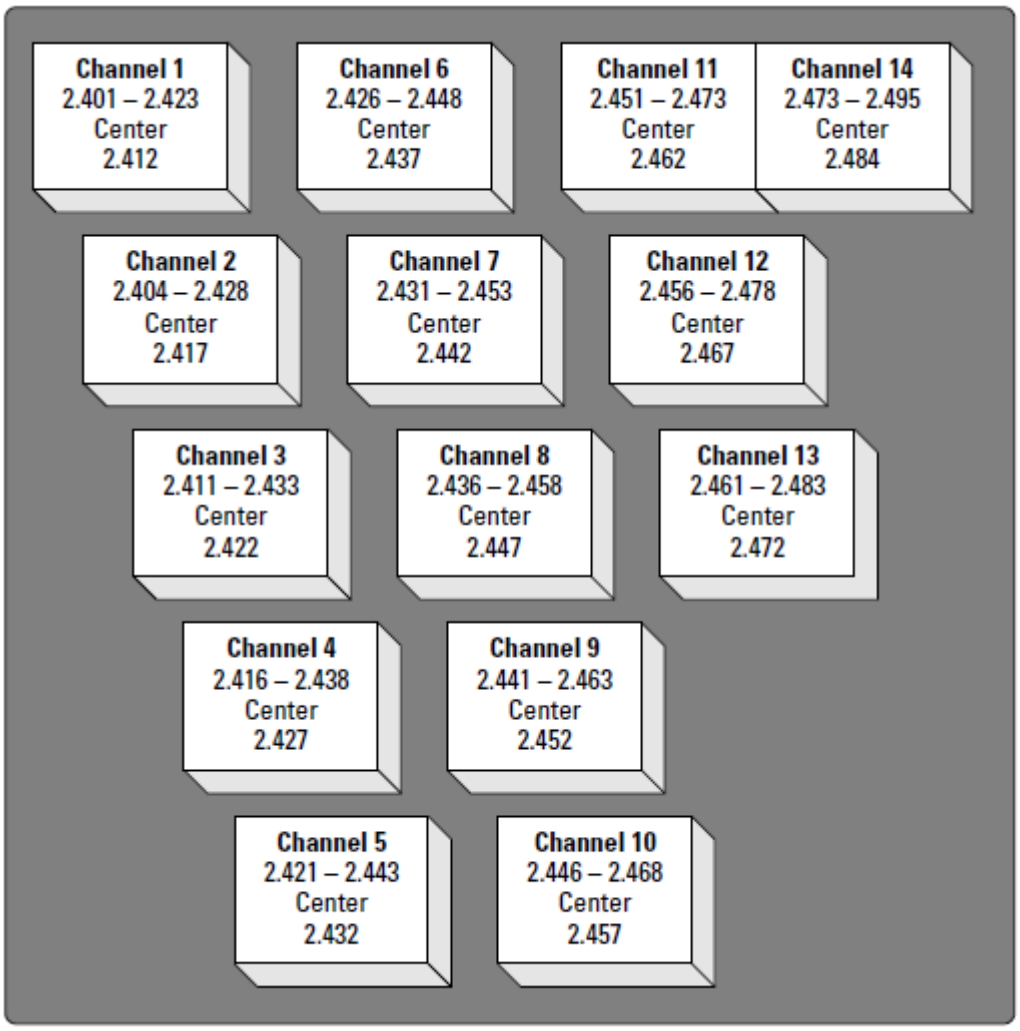
(Silviu 2010, 650 – 651.)

3.3.1 WLAN-radiotaajuudet

Langattomassa lähiverkossa käytettävä 5 GHz:n radiotaajuusalue on 5,170 GHz – 5,835 GHz, ja se jaetaan IEEE 802.11a:ssa 24 kanavaan. Jokainen kanava on 20 MHz leveä. Tämän ansiosta 5 GHz:n taajuusalueella voi toimia 24 tukiasemaa samassa tilassa häiritsemättä toisiaan. (Silviu 2010, 653.)

IEEE 802.11n/ac -standardia käytettäessä on mahdollista vaihtaa kaistanleveyden kokoa 20 MHz:stä 40 MHz:iin tai suurempaan. Kaistanleveyden nostaminen vaikuttaa positiivisesti tiedonsiirtonopeuteen. Tämän takia kanavia on käytössä enää 12. 5 GHz:n radiotaajuusalueen käyttämisen suurimpia etuja on sen omat uniikit kanavat ja radiotaajuusalueen vähäinen käyttö muissa käyttötarkoituksissa. (Silviu 2010, 655.)

2,4 GHz:n taajuusalueella alue on 2.4000 – 2.4835 GHz. Tämä taajuusalue on jaettu 14 kanavaan, joista jokainen on 22MHz:ä leveä, mutta jokaisen kanavan keskusta on vain 5 MHz leveä. Suomessa on käytössä kanavat 1-13. Tämän takia kanavat menevät toistensa päälle aiheuttaen häiriötä viereisille kanaville. 2,4 GHz:n taajuusalueella on siten vain 3 kanavaa, jotka voivat olla käytössä samassa tilassa häiritsemättä toisiaan. Kanavat 1,6 ja 11 voivat toimia samaan aikaan. (KUVIO 12.)



KUVIO 12. 2,4 GHz:n kanavat (Silviu 2010, 654)

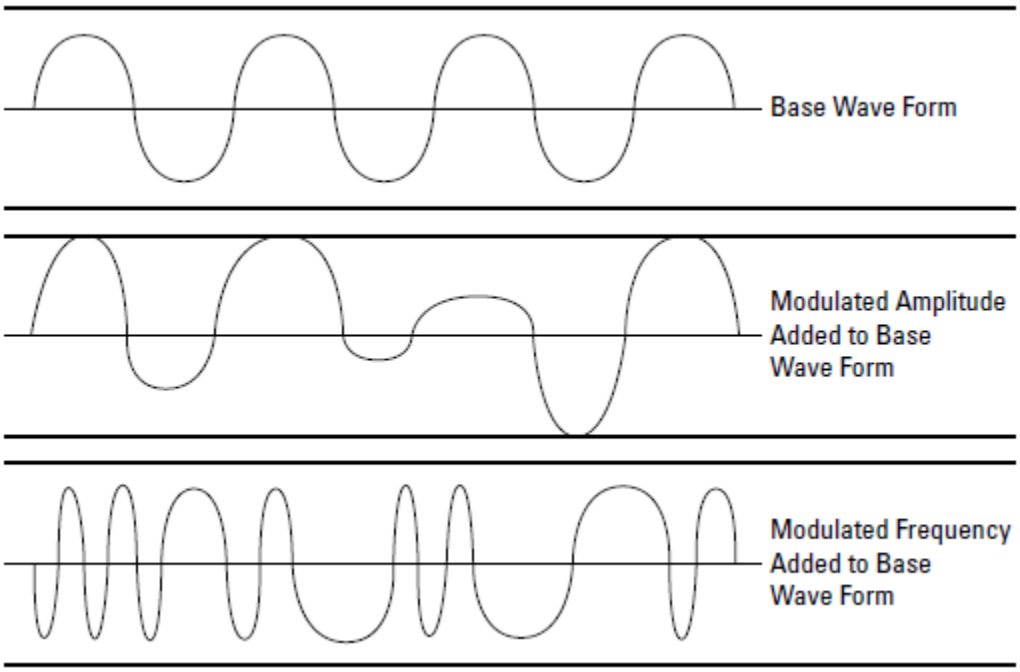
2,4 GHz:n taajuusaluetta käyttää IEEE 802.11 b/g/n -standardien lisäksi myös monet muut laitteet. Tämän takia millä tahansa alueella, jossa käytetään 2,4 GHz:n taajuusaluetta on olemassa vaara ulkoisille häiriöille. (Silviu 2010, 654.)

3.3.2 WLAN-modulointitekniikat

Radiotaajuuksia moduloidaan, jotta aaltomuotoon saadaan lisättyä dataa. Vastaanotettaessa radiotaajuus voidaan demoduloida, jos tiedetään, mitä muutoksia aaltomuotoon on tehty. (Silviu 2010, 652.)

Aaltomuotoa voidaan muokata vaihtamalla huippuarvoa, taajuutta tai signaalin kohtaa. Kuviossa on ylimpänä normaali aaltomuotoinen signaali.

Keskimmäisenä aaltomuotoinen signaali on muokattu vaihtamalla huippuarvoa. Alimmaisena on muokattu signaalin taajuutta. (KUVIO 13.)



KUVIO 13. Aaltomuotoisen signaalin modulointi (Silviu 2010, 653.)

FHSS (Frequency-hopping spread spectrum) -moduloinnissa käytetään kaikkia vapaita kanavia tiedon lähettämiseen ja vastaanottamiseen. Kanavia käytetään vaihtamalla kanavasta toiseen näennäissatunnaisella järjestyksellä. Avain määrää näennäissatunnaisen järjestyksen. Avain, jolla modulaatiota puretaan, on jaettu kaikille tiedonsiirtoon osallistuville. FHSS:ää on erittäin vaikeaa kuunnella, mikäli avainta ei ole tiedossa. (Silviu 2010, 655.)

DSSS -modulointi (Direct-sequence spread spectrum) hyödyntää yhtä kokonaista kanavaa, jonka taajuusväli on 22 MHz kanavaa kohden. Täten lähetys jakautuu koko 22 MHz:n taajuudelle esimerkiksi 2,401 ja 2,423 GHz:n välillä. Samaan aikaan kuin lähetetään dataa, lähetetään nopeammalla vauhdilla ”noise” -signaalia näennäissatunnaisella järjestyksellä. Tämä ”noise” -signaali tiedetään vastaanottimessa, jonka avulla signaali osataan erotella varsinaisesta datasignaalista. Tämän ansiosta samalla kanavalla toimivat muut lähetykset eivät vaikuta

signaaliin häiritsevästi, koska muut lähetykset eivät käytä samaa ”noise” -signaalia. (Silviu 2010, 656.)

OFDM (Orthogonal Frequency Division Multiplexing) -modulointitekniikka hyödyntää multiplexingin mahdollistamia alilähetyksiä (subcarriers), jotka yhdistetään yhdeksi isoksi datavirraksi. Monta pientä datavirtaa lähettävät hitaalla tiedonsiirtonopeudella samaan aikaan, mutta lopputuloksena syntyy yksi iso datavirta, joka lähettää nopealla tiedonsiirtonopeudella. OFDM mahdollistaa nopeammat tiedonsiirtonopeudet kuin DSSS tai FHSS. (Silviu A 2010, 656)

MIMO (Multiple-in, multiple-out) mahdollistaa useampien antennien käytön, kun lähetetään ja vastaanotetaan tietoa. Tekniikan avulla voidaan samalla kanavalla lähettää useita eri lähetyksiä. MIMO:a käytetään yleensä ODFM-tekniikan kanssa parannettaessa tiedonsiirron luotettavuutta. (Silviu A 2010, 656)

3.4 WLAN-standardit

WLAN standardit voidaan jakaa pääosassa kolmeen ryhmään: 2,4 GHz:n, 5 GHz:n ja 2,4 GHz:n sekä 5 GHz:n taajuusalueella toimiviin standardeihin. Ensimmäinen julkaistu standardi oli nimeltään IEEE 802.11-1997 tai IEEE 802.11 Legacy. IEEE 802.11a ja IEEE 802.11b olivat kehitteillä samaan aikaan, ja molemmissa olivat hyvät puolensa. 802.11a:n ja 802.11b:n erotti toisistaan taajuusalue ja modulointitekniikka. Nykyään on olemassa standardeja jotka toimivat sekä 2,4 GHz:n ja 5 GHz:n taajuusalueella. IEEE 802.11n oli ensimmäinen standardi, joka pystyi toimimaan kahdella eri taajuusalueella. 802.11n:n etuna olikin, yhteensopivuus aikaisempien standardien kanssa. (Silviu 2010, 658 – 661.)

IEEE 802.11 standardissa määritellään, että on olemassa kolme fyysisen kerroksen järjestelmää, joita voidaan käyttää. FHSS, joka on taajuushyppely-tekniikka 2,4 GHz:n taajuusalueella. DSSS on suorasekventointi-tekniikka 2,4 GHz:n taajuusalueella. Näiden lisäksi on

myös InfraRed, joka on määritelty standardissa, mutta sitä ei ole koskaan otettu käyttöön. Modulaatiotekniikoiden määrittelyn lisäksi standardissa määritellään tiedonsiirtonopeus, joka on 1 tai 2 Mbps. 802.11 -standardin suurin etu kilpailijoihin nähden oli sen suurempi kantomatka radiotaajuuksien käytön vuoksi. (Silviu 2010, 658.)

Kaikissa 802.11 -standardeissa käytetään CSMA/CA:ta (Carrier sense multiple access witch collision avoidance), joka eroaa ethernetin käyttämästä CSMA/CD –tekniikkaa (Carrier sense multiple access witch collision detection). Molemmissa tekniikoissa CSMA tarkoittaa, että kaikki laitteet voivat tunnistaa, tai nähdä liikenteen ja kaikki laitteet voivat samaan aikaan käyttää siirtotietä, mutta vain yksi laite voi kerrallaan lähettää dataa. Tästä eteenpäin tekniikat ovat kuitenkin erilaisia. LAN:ssa (Local area network) kun tietokone haluaa lähettää kehyksen verkkoon, se käyttää CSMA:ta havaitakseen liikenteen, jonka jälkeen se lähettää kehyksen ethernet -kaapelia pitkin toiseen päähän, josta signaali palautuu lähettäjälle. Kun tietokone saa kehyksen takaisin, se tietää että kehys on lähetetty ehjänä. Jos kehys tulee takaisin puutteellisena, tietokone odottaa epäsäännöllisen ajan, jonka jälkeen prosessi tehdään alusta. CSMA/CA:ssa on käytössä erilainen menetelmä, koska signaalille ei ole olemassa mekanismia palautua takaisin lähettäjälle. Lähetys tapahtuu edelleen kuuntelemalla verkon liikennettä, ja mikäli muita kehyksiä ei havaita verkossa tietyn ajan kuluessa, annetaan lupa lähettää kehys. Vastaanottava asema suorittaa CRC (Cyclic redundancy check) tarkastuksen kehykselle ja lähettää ACK –kehyksen (Acknowledgement) lähettäjälle tiedoksi saapuneesta kehyksestä. Näin lähettäjä saa tiedon kehyksen onnistuneesta lähetyksestä. (Silviu 2010, 658 – 659.)

DRS (Dynamic rate switching) mahdollistaa tukiaseman vaihtamaan pienemmälle kaistanleveydelle, kun signaali heikkenee. Signaalin voimakkuuteen vaikuttaa tukiaseman ja aseman etäisyys toisistaan. Toisin sanoen, mitä kauemmas asema viedään tukiasemasta, sitä hitaampi on tiedonsiirtonopeus tukiaseman ja aseman välillä. (Silviu 2010, 659.)

Ensimmäinen parannus 2,4 GHz:n taajuudella 802.11 -standardille oli nimeltään 802.11b. 802.11b nostaa suurimman mahdollisen tiedonsiirtonopeuden 1-2 Mbps:sta 11 Mbps:n. 802.11b käyttää CCK:ta (Complementary code keying) modulaatiotekniikkana. CCK pohjautuu suorasekventointitekniikkaan. Suurin mahdollinen kantavuus 11 Mbps:n nopeudella on 30 metriä. Vaikka 802.11b:n nopeus on hitaampi kuin 802.11a:n, niin 802.11b:stä tuli suositumpi standardi. (Silviu 2010, 659.)

802.11g on seuraaja 802.11b:lle, joka nostaa tiedonsiirtonopeuden 54 Mbps:n. 802.11g käyttää pääsääntöisesti OFDM:ää modulointitekniikkana. CCK:ta ja suorasekvensointia käytetään lisäksi kun nopeudet ovat pienemmät. Standardi oli yhteensopiva 802.11b:n kanssa, mahdollistaen kommunikoinnin hitaammilla tiedonsiirtonopeuksilla 802.11b:tä käyttävien laitteiden kanssa. Tukiasema kuitenkin voi käyttää vain yhtä standardia lähetintä kohden, joten jos verkossa on 802.11b:tä käyttäviä laitteita, koko verkko hidastuu sille tasolle. Varustamalla tukiasema kahdella radiolähettimellä pystytään samaan aikaan toimimaan sekä 802.11g- että 802.11b -standardeilla. (Silviu 2010, 660.)

802.11a -standardin parhaita ominaisuuksia olivat toimiminen 5 GHz:n taajuusalueella, joka ei ollut niin käytetty taajuusalue kuin 2,4 GHz:n taajuusalue. 802.11a:n suurin siirtonopeus on 54 Mbps, joka on paljon nopeampi kuin 802.11b. 802.11a käyttää OFDM:ää modulaatiotekniikkana. Standardin suurin heikkous on sen yhteensopimattomuus 802.11b/g standardien laitteiden kanssa. (Silviu 2010, 660.)

802.11n on standardi, joka yhdisti 2,4 GHz:n ja 5 GHz:n radiotaajuudet yhden standardin alle. Standardin suurin yksittäinen ominaisuus on sen yhteensopivuus kaikkien aikaisempien IEEE 802.11 -standardien kanssa. 802.11n käyttää modulointitekniikkana ODFM:ää sekä MIMO:a. Kantomatkat 802.11:n:ssä ovat samaa tasoa aikaisempienkin standardien kanssa, mutta tiedonsiirtonopeudet kasvoivat suuremmiksi. Käyttämällä neljää MIMO virtaa, voidaan saavuttaa 600 Mbps:n tiedonsiirtonopeus. Yhdellä virralla voidaan saavuttaa 150 Mbps:n tiedonsiirtonopeus.

Standardilla voidaan käyttää myös 40 MHz:n kaistanleveyttä. (Silviu 2010, 661.)

802.11ac -standardi toimii pelkästään 5 GHz:n taajuudella. Standardissa on nostettu kaistanleveys jopa 160 MHz:n asti. Tämä mahdollistaa tiedonsiirtonopeuksien nousevan jopa 6.93 Gbps asti. Modulointina standardissa käytetään OFDM:ää. Myös MIMO:n määrää on nostettu 802.11n -standardin neljästä kahdeksaan kappaleeseen. (Aeroflex 2012)

Kuviossa on esitelty standardien eroavaisuuksia keskenään vielä tarkemmin. Jokaisen uuden standardin myötä on tiedonsiirtonopeus kasvanut. Taajuuskaista on ollut joko 2,4 GHz, 5 GHz tai molemmat. 2,4 GHz:n taajuuskaistan etuna on kantaman pituus, mutta 5 GHz:n taajuuskaistalla saadaan kaistanleveyttä suuremmaksi, joka nostaa tiedonsiirtonopeuksia. Uusia standardeja kehitellään jatkuvasti ja ne tuovat myös muita uusia ominaisuuksia mukanaan. (KUVIO 14.)

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

KUVIO 14. IEEE 802.11 standardit (Aeroflex 2012)

3.5 WLAN-tietoturva

Langattoman verkon turvaaminen on tärkeä toimenpide, joka tulee suorittaa huolellisesti niin kotiverkossa kuin yritysverkossakin. Langattoman verkon suojaaminen tehdään, jotta tiedot ja tiedostot pysyvät yksityisinä. Langattoman ja langallisen verkon suojaamisessa on yksi suuri ero - langattomassa verkossa käyttäjät voivat olla fyysisesti missä vain verkon kantaman alueella. (Silviu A 2010, 665)

Langattoman verkon turvaamiseen on olemassa neljä tapaa, joita noudattamalla verkosta saa turvallisen:

- autentikointi ja tietojen salaaminen
- MAC -osoitteiden suodattaminen
- hyökkäyksien tunnistus ja hyökkäyksien estäminen
- SSID:n piilottaminen.

Kaikkia näitä toimenpiteitä ei ole mahdollista aina suorittaa, mutta mitä useampaa kohtaa noudattaa, sitä turvallisempi langaton verkko on.

Näiden toimenpiteiden lisäksi on syytä vaihtaa oletussalasanat. Oletussalasanat, SSID, käyttäjien ja pääkäyttäjätunnuksien salasanat on vaihdettava heti käyttöön oton yhteydessä, sillä kaikki nämä tiedot on dokumentoitu laitteen ohjekirjassa. Näin ollen nämä tiedot ovat kaikkien saatavilla. (Silviu 2010, 671.)

3.5.1 Autentikointi ja tietojen salaaminen

RF-signaalien (Radio frequency) salaamiseen käytetään salausmenetelmiä, joista ensimmäinen oli WEP (Wired equivalent privacy). WEP:n tarkoitus oli luoda saman tasoista turvaa langattomalle verkolle, kuin langalliselle verkolle. Salaus perustuu kahteen osaan: Tunnistautumiseen ennen verkkoon liittymistä ja kaikkien verkossa liikkuvan tiedon salaamiseen. WEP:n heikkous salausmenetelmänä on sen helppo murrettavuus. WEP:n pystyy murtamaan minuuteissa. WEP koostuu joko 64- tai 128-bittisestä salausavaimesta. 128 -bittinen salausavain koostuu 104bitin salausavaimesta, johon liitetään 24 -bitin IV (Initializing vector). Näistä kahdesta osasta muodostuu RC4 koodi. IV:n pitää olla uniikki jokaiselle lähetetylle paketille, jonka takia se voi alkaa toistaa itseään jo 5000 lähetetyn paketin jälkeen. (Silviu 2010, 667.)

WPA (Wi-fi protected access) kehitettiin paikkaamaan WEP:n heikkouksia. WPA noudattaa suurinta osaa IEEE 802.11i standardissa määriteltyjä tietoturvapykäliä. Myöhemmin julkaistiin WPA2, joka noudattaa kaikkia IEEE 802.11i -standardissa määriteltyjä

tietoturvapykäliä. WPA käyttää TKIP:tä (Temporal key integrity protocol) staattisen salausavaimen sijaan, jota käytettiin WEP:ssä. Selkokielisen IV -osan sijaan, IV:hen sijoitetaan salainen juuriavain. Protokolla tuo uutena ominaisuutena sekvenssilaskurin, jotta kaikki paketit saapuvat tukiasemalle oikeassa järjestyksessä, tai muutoin paketit hylätään. Protokolla tuo myös lisänään menetelmän salausavaimen uudelleen asettamiseksi tai päivittämiseksi neutralisoidakseen mahdollisen salausavaimen murtamisen. (Silviu 2010, 668.)

TKIP:ta käyttävään WPA -salaukseen on mahdollista kuitenkin murtautua, joskin huomattavasti hankalampaa kuin WEP:iin. Tätä varten kehitettiin AES (Advanced encryption standard) -salaus. AES:ia pidetään tälläkin hetkellä markkinoiden turvallisimpana salausmenetelmänä. AES käyttää joko sertifikaattipohjaista tunnistautumista tai jaettua salausta. Jaettua salausta käytetään WPA2:n personal -moodissa. Sertifikaattipohjaista tunnistautumista käytetään WPA2:n enterprise -moodissa. WPA2 enterprise tarjoaa vahvemman turvan. (Silviu 2010, 668.)

3.5.2 MAC-osoitteiden suodattaminen

Autentikoinnin ja salauksen lisäksi langatonta verkkoa voidaan suojata suodattamalla verkkoon pääsyä laitteiden MAC-osoitteilla. MAC-osoitteita voidaan suodattaa joko tukiasema kerrallaan, keskitetysti tunnistautumispalvelusta, tai AAA (Authentication, authorization ja accounting) palvelimelta omasta verkostasi. MAC-osoitteiden avulla voidaan rajata verkkoon pääsy tietylle ryhmälle asettamalla MAC-osoitteet whitelistille, tai vaihtoehtoisesti estää pääsy tietyiltä MAC-osoitteilta asettamalla ne blacklistille. (Silviu 2010, 670.)

Koska monet käyttöjärjestelmät mahdollistavat MAC-osoitteen vaihtamisen verkkokorttiin, MAC-osoitteilla suodattaminen on heikko tapa suojata verkkoa. Suodattaminen tuo kuitenkin lisää turvaa muiden suojaamiskeinojen lisänä. (Silviu 2010, 670.)

3.5.3 Hyökkäyksien tunnistus ja hyökkäyksien estäminen

IDS- (Intrusion detection systemp) ja IPS (Intrusion prevention system) -järjestelmät seuraavat verkon liikennettä ja liikennöivät järjestelmiin löytääkseen verkosta laitteita, jotka mahdollisesti koittavat tunkeutua verkkoon. Kun hyökkääjä yrittää tunkeutua verkkoon, hyökkääjä ajaa ohjelmia, jotka skannaavat verkosta haavoittuvuuksia. Nämä ohjelmat jättävät jälkiä liikenteeseen, jotka IDS- ja IPS- järjestelmät havaitsevat.

IDS:n avulla voidaan paikallistaa hyökkääjän sijainti ja estää hänen aikeet. Kun puhutaan järjestelmästä, joka tunnistaa hyökkäyksen ja reagoi siihen automaattisesti estämällä sen, viitataan yleensä IPS:ään. IDS- ja IPS-järjestelmät sijaisevat yleensä verkon oletusyhdyskäytävässä tai verkon sisällä. (Silviu 2010, 671.)

3.5.4 SSID:n piilottaminen

Kaikki WLAN-tukiasemat lähettävät säännöllisiä broadcast lähetyksiä, jotka sisältävät verkon nimen. SSID:tä käytetään erottamaan verkot toisistaan. SSID:n avulla avulla liitytään langattomaan lähiverkkoon.

Tukiasemista on mahdollista ottaa pois käytöstä ominaisuus, jolla SSID:tä mainostetaan. SSID:n mainostamisen lopettaminen ei kuitenkaan estä ketään liittymästä verkkoon. Tämän takia SSID:n piilottaminen ei suojaa todellisilta uhkilta. SSID on myös mahdollista saada selville ammattiohjelmistojen avulla kuuntelemalla radiotaajuuksia. (Silviu 2010, 670.)

4 BRING YOUR OWN DEVICE

Älypuhelimien ja tablettien yleistyttyä on kasvanut myös kyseisten laitteiden lukumäärät työpaikoilla. Työntekijöiden omia laitteita voidaan käyttää hyödyksi yrityksessä, jolloin säästetään laitehankinnoissa. On otettava huomioon, että laitteiden kirjo on suurempi, kuin yrityksen itse hankkiessa tietyt mobiililaitteet. Tuettavien laitteiden määrä saattaa olla suuri, joka aiheuttaa tietoturvalle haasteita. Tätä ilmiötä kutsutaan nimellä BYOD (Bring Your Own Device). (PCWorld 2011a.)

Yrityksen on helpompi ottaa käyttöön BYOD -käytäntö aikaisessa vaiheessa, kuin antaa työntekijöiden käyttää hallitsemattomasti yrityksen tietoja omilla laitteillaan. Kun noudatetaan tiettyjä sääntöjä, on tietovuotojen tapahtuminen ennaltaehkäistävää. (ITPRO 2013.)

BYODilla tarkoitetaan yleensä puhelimia ja tabletteja, mutta myös kannettavat tietokoneet kuuluvat tähän kategoriaan. Mobiililaitteiden ja kannettavien tietokoneiden tietoturva hoidetaan kuitenkin yleensä eri tavalla. Mobiililaitteita ja kannettavia tietokoneita yhdistää se, että kumpaankin tehdään suojattu VPN (Virtual Private Network) -yhteys ja tiedostojen salaus. Mobiililaitteita suojataan enemmän varastamiselta, jolloin käytetään lukitsemis ominaisuutta ja gps-seurantaa. Kannettavia tietokoneita suojataan enemmän haittaohjelmilta ja hyökkäyksiltä. (PCWorld 2011a.)

Yritykset, jotka hyödyntävät BYOD -käytäntöä, ovat pienessä etulyöntiasemassa kilpailijoihin nähden. Laitehankinnat siirtyvät käytännössä yritykseltä työntekijälle. Työntekijät ovat myös tyytyväisempiä, kun saavat käyttää omia laitteitaan työssä. Käyttäjät hankkivat laitteen yleensä omien tarpeiden ja mukavuuden mukaan. Työntekijät käyttävät mieluiten laitteita, jotka ovat itse hankkineet, kuin laitteita jotka yrityksen IT-osasto hankkii tietystä valikoimasta. Käyttäjät uusivat laitteitaan useammin kuin yritykset, jolloin voidaan käyttää uusimpia ominaisuuksia käyttäjien laitteissa. (PCWorld 2011b.)

BYOD tuo myös mukanaan muutamia ongelmia. Kun laitteet eivät ole IT-osaston hallitsemia ja valitsemia, on vaikeampi kontrolloida, mitä ohjelmia käyttäjä saa omassa laitteessaan käyttää. Tärkeää onkin luoda säännöt, joiden avulla määritellään, mitä saa tehdä ja mitä ei. Pitää myös asettaa tietyt minimivaatimukset laitteelle ja käyttöjärjestelmälle. Kun käyttäjä yhdistää laitteensa yrityksen verkkoon, on tietoturvan syytä olla kunnossa käyttäjän laitteessa. Laitteessa oleva data on edelleen yrityksen omistuksessa, vaikka se sijaitseekin käyttäjän omistamalla laitteella. Työntekijän poistuessa yrityksen palkkalistoilta voi olla ongelmallista poistaa data laitteelta. Onkin tärkeää luoda säännöt, joiden mukaan menetellään, kun laitetta ei enää käytetä yrityksen hyväksi. (PCWorld 2011b.)

BYOD -infrastruktuuria määriteltäessä on tärkeää ottaa huomioon, kuinka kovalle rasitukselle verkko joutuu. WLAN-verkon on katettava koko rakennuksen alue, jossa käyttäjät käyttävät verkkoa. Verkkoa on yleensä päivitettävä uusilla tukiasemilla, jotta saadaan rakennettua kaiken kattava verkko. Tietyt rakennuksen alueet ovat suositumpia kuin toiset, joten näihin paikkoihin pitää saada enemmän kaistaa käytettäväksi. (InformationWeek 2012.)

Toinen huomioon otettava seikka on IP-osoitteiden määrä. IP-osoitteiden tarve tulee lisääntymään, kun käyttäjällä saattaa olla useita laitteita, jotka kaikki yhdistyvät verkkoon. IP-osoitteita voidaan jakaa yksityisistä osoiteavaruuksista, NAT:n (network address translation) takaa, jolloin osoitteita saadaan enemmän, mutta se tuo mukanaan omat ongelmat. DHCP:n jakamat osoitelainat pitää myös pitää mahdollisimman lyhyinä, sillä varsinkin oppilaitosympäristössä käyttäjiä on suuri määrä, jolloin osoitteita ei voi jättää varaamaan yksittäisille laitteille pitkäksi aikaa. (InformationWeek 2012.)

5 WLAN-VERKON SUUNNITTELU

5.1 Lähtökohta verkon suunnittelulle

Lahden ammattikorkeakoulu on tilannut WLAN-verkon kuuluvuuskartoituksen Tekniikan alalle. Tietohallinto hyödyntää mittauksia ja sen pohjalta tehtävää suunnitelmaa verkon parantamiseksi syksyllä 2015 käyttöön otettavaa Bring Your Own Device -käytäntöä varten.

Lahden ammattikorkeakoulun tekniikan laitokselle oli suoritettu muutamia WLAN-mittauksia aikaisemminkin, mutta mittaukset päädyttiin tekemään uudestaan, jotta voidaan luottaa oman työn jälkeen, eikä erheitä syntyisi sen takia, että mittaukset eivät ole ajantasalla tai ovat puutteelliset. Mittauksia ei tiedettävästi kuitenkaan ole tehty vastaavassa mittakaavassa, joten ajantasaiset ja kattavat mittaukset ovat aiheelliset.

Mitattava WLAN-verkko on nimeltään ”lamk_students”, joka on oppilaiden käyttöön tarkoitettu langaton verkko. Verkon on tarkoitus kattaa kaikki alueet rakennuksessa, joihin opiskelijoilla on pääsy. Mittaukset tehtiin myös vain niihin alueisiin, joihin opiskelijoilla on pääsy.

WLAN-verkkoon kytkeydytään opiskelijoiden omilla AD-tunnuksilla, minkä jälkeen opiskelijat voivat vapaasti käyttää internetiä laitteessaan. Todentaminen on toteutettu ciscon web -authentikoinnilla. Verkko toimii 802.11n -standardilla, joka mahdollistaa 2,4 GHz:n sekä 5 GHz:n radiotaajuuksien käyttämisen.

Mittauksia tehtäessä käytettiin oppilaitoksen tarjoamia työkaluja, joiden kanssa on työskennelty aikaisempien projektien parissa. Valitut työkalut olivat olleet hyväksi todettuja ja pääasiassa tuttuja, joten aikaa ei kulunut uusien työkalujen opetteluun tai hankkimiseen.

Tarkoituksena oli mitata verkosta sen kattavuus, nopeus ja käytetyt kanavat. Lisäksi kartoitettiin teorialuokkien pistorasioiden riittävyys, jotta opiskelijoilla on mahdollisuus kytkeä omat laitteensa sähköverkkoon kiinni.

Edellämainittujen ominaisuuksien mittaamiseen käytettiin työkaluina seuraavia laitteita ja- tai- ohjelmia: Ekahau site survey –ohjelmalla saatiin mitattua verkon kattavuus ja signaalin voimakkuus. Fluke Aircheck Testerillä saatiin mitattua verkkojen käyttämät kanavat kullakin radiotaajuudella, lisäksi testerillä voitiin paikantaa esimerkiksi tukiasemia tai tehdä testejä, joilla voitiin mitata verkon toimivuutta. Verkon nopeus testattiin Ooklan speedtestillä, joka on selainpohjainen työkalu.

5.2 WLAN-verkon mittaaminen

Mittaaminen suoritettiin kerros kerrallaan ja samalla kierroksella tehtiin kartoitusmittaus, nopeustesti ja kanavien kuormitusmittaus. Teorialuokkien pistorasioista tehtiin samalla kartoitus, paljonko niitä on. Mittaukset suoritettiin saatujen ohjeiden mukaisesti. Mittaukset suoritettiin, kun tilat olivat mahdollisimman tyhjiä, jotta vältyttiin virheiltä tai muilta rasituksilta. Mittauksia suoritettiin useampana ajankohtana, jotta oli mahdollista päästä kaikkiin tiloihin häiritsemättä opetusta ja pääsemällä mahdollisimman tyhjiin tiloihin.

Pistorasiat kartoitettiin tulevaa BYOD -käytäntöä silmälläpitäen. Osaan teorialuokista tarvitaan lisää pistorasioita opiskelijoiden omille päätelaitteille. Pistorasioiden lukumäärä kerättiin ”noin” arvolla, sillä kaikkien kaappien, hyllyjen ja muiden esteiden taakse ei päästy tarkistamaan. Pistorasioiden varsinaisella lukumäärällä ei ollut merkitystä, mikäli niitä teorialuokassa oli vain 2-4, sillä BYOD:a varten pistorasioita tarvittaisiin paljon enemmän. Tietokoneluokkien pistorasiakartoitusta ei koettu tarpeelliseksi.

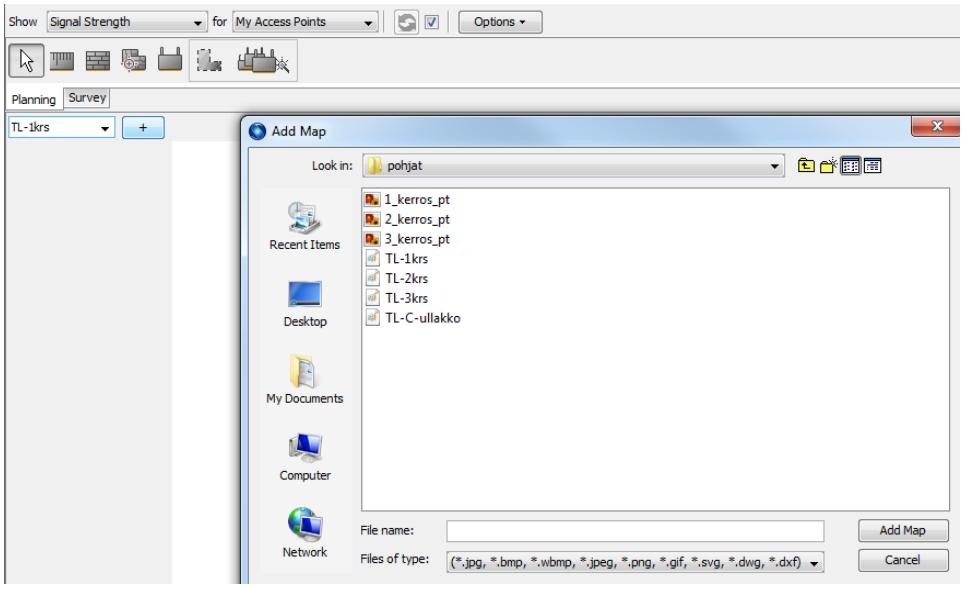
Mittausvaiheessa tarkasteltiin myös mahdollisia uusien tukiasemien sijoituspaikkoja. Sijoituspaikkaan vaikuttaa pääasiassa tarve tukiasemalle, mutta myös sen toteuttamisen mahdollisuus. Tukiasema tarvitsee toimiakseen virtakaapelin ja ethernet -kaapelin tai vaihtoehtoisesti PoE:n (Power over ethernet) avulla pelkän ethernet -kaapelin. Tietoliikennerasian osuminen tukiaseman lähelle vähentää kustannuksia omalta osaltaan, kun vältytään rasian asennuskustannuksilta.

Mittauksissa tärkeintä oli huolellinen ja tarkka työn laatu. Nopeustestejä tehtiin samassa tilassa 3 kertaa, joista valittiin keskiarvo, mikäli tulokset olivat lähellä toisiaan. Jos yhdessä tuloksessa oli huomattavaa eroa kahteen muuhun, niin mitätöitiin kyseinen tulos. Tarvittaessa otettiin lisää mittauksia. Kanavamittauksissa luotettiin mittarin osoittamaan lukemaan, sillä mittari päivitti löytämänsä tukiasemat lähes reaaliajassa. Mittaria pidettiin hetken verran paikallaan, minkä jälkeen lukemat kirjattiin ylös. Site surveylla mitatessa pieniä virheitä saattoi tulla pohjapiirustusta lukiessa ja väärään kohtaan sijainnin merkitsemisessä. Jokaisen mitatun tilan jälkeen tulokset tarkastettiin ja todettiin kuljettu reitti joko oikeaksi tai vääräksi. Väärin merkatut tulokset hylättiin ja mittaus suoritettiin uudelleen.

5.2.1 Site survey

Mittaustyöt aloitettiin lisäämällä pohjapiirrokset Ekahau site survey -ohjelmaan. Pohjapiirroksen täytyi olla tietyssä tiedostomuodossa, jotta ohjelma hyväksyi ne. Saadut pohjapiirrokset olivat .pdf -tiedostoja, joten tiedostojen muuttamiseen käytettiin gimp -kuvankäsittelyohjelmaa, jolla tiedostot muokattiin oikeaan tiedostomuotoon.

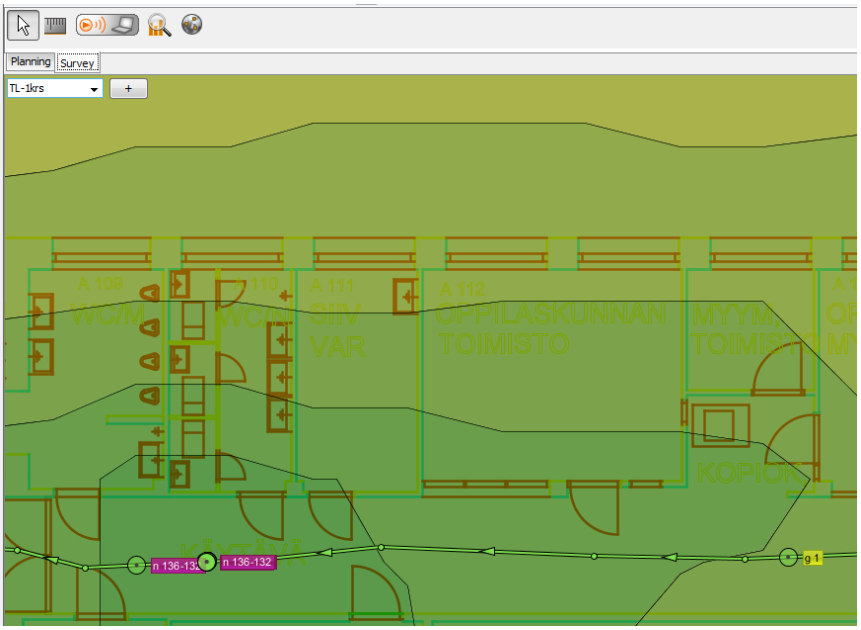
Pohjapiirroksia voitiin samaan tiedostoon lisätä useampia. Samaan tiedostoon lisättiin kaikki kolme pohjapiirrosta, joista jokainen käsittää yhden kerroksen rakennuksesta. Pohjapiirros lisätään valitsemalla vasemmasta reunasta + symbolia painamalla, josta aukeaa valikko mistä voidaan lisätä pohjakuva. + symbolin vasemmalla puolella on dropdown – valikko josta voidaan vaihtaa kerrosta. (KUVIO 15.)



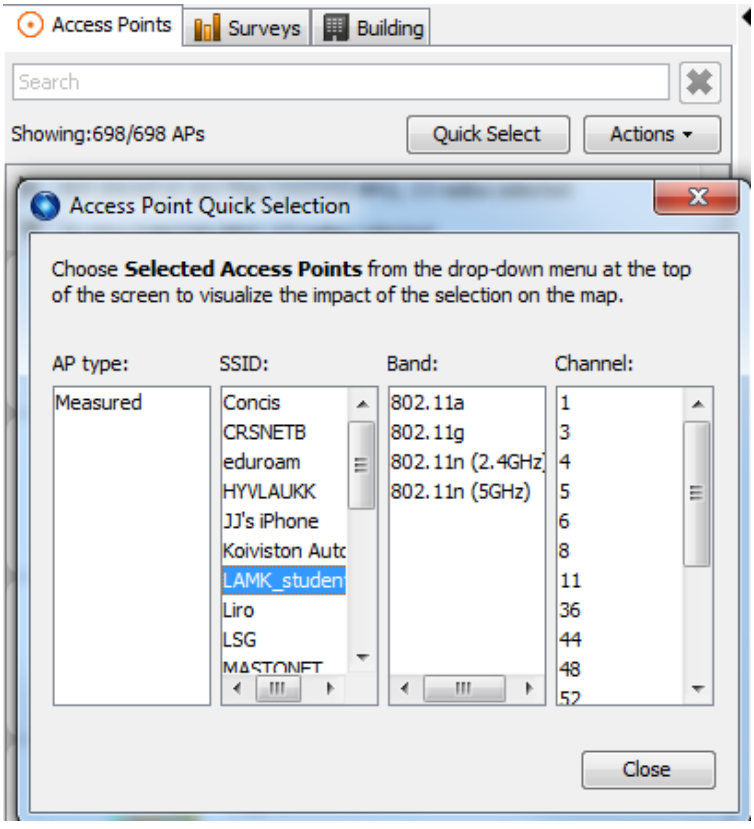
KUVIO 15. Pohjapiirroksen lisääminen

Jokaiseen kerrokseen lisättiin myös skaala. Piirustuksista ei ilmennyt skaalaa, joten mittanauhalla mitattiin seinästä sopiva mitta ja osoitettiin sen pituus ohjelmaan skaalaksi. Skaala asetettiin viivottimen näköistä nappulaa painamalla, minkä jälkeen kartasta painettiin kaksi pistettä, joiden välissä oleva etäisyys merkittiin metreinä ja sentteinä.

Kuuluvuuskartoitus suoritettiin etenemällä pohjapiiroksen mukaan rakennuksessa ja klikkaamalla pohjapiirrokseen sijainti, missä ollaan. Ohjelma ilmoitti kuuluvuuden värikoodattuna. Tummanvihreä väri tarkoitti, että signaali on voimakas, kun taas punainen väri ilmoitti, että signaali on heikko. (KUVIO 16.) Ohjelmaan päivittyi kaikkien alueella olevien verkkojen kuuluvuus oletuksena, joten oli valittava valikosta quick select, jonka jälkeen aukesi uusi ikkuna, josta valittiin lamk_students -verkko. Tämän jälkeen ohjelma näytti kuuluvuuden tietyn verkon mukaisesti. (KUVIO 17.)



KUVIO 16. Kartoitus

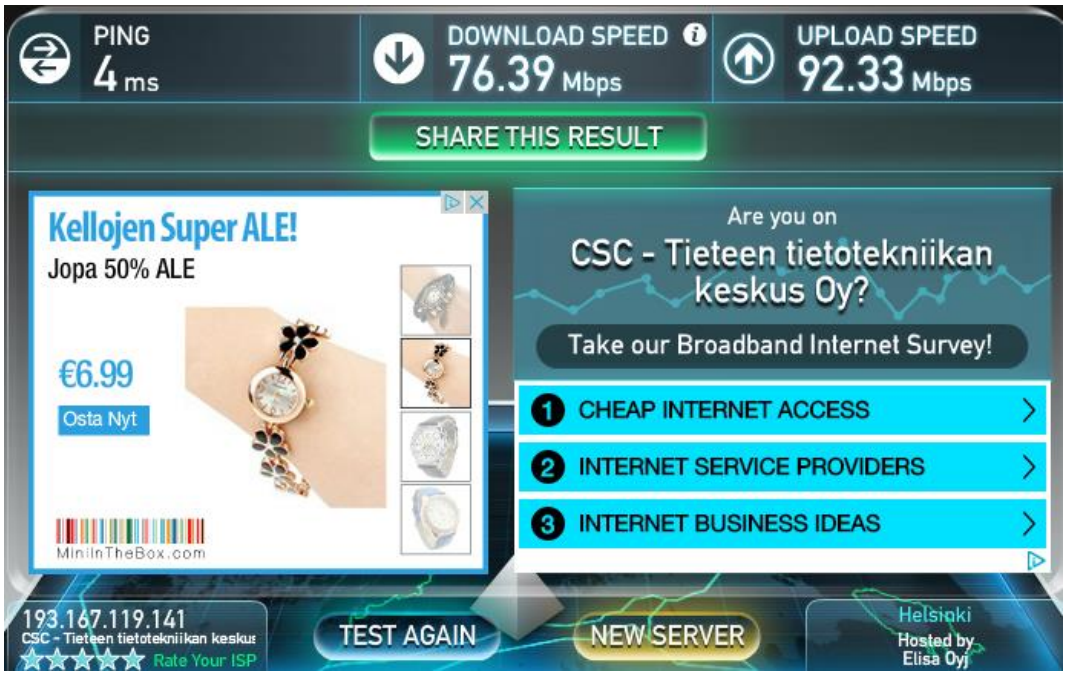


KUVIO 17. Verkon valinta

5.2.2 Nopeustesti

Nopeustestillä testattiin verkon ja tukiaseman suorituskykyä. Mikäli tukiasema oli liian kaukana mittauspisteestä, päätelaitteen tiedonsiirtonopeus putosi. Mittauksissa huomattiin eroja eri tukiasemissa. Signaalin ollessa hyvä, toisissa tukiasemissa nopeudet olivat huomattavasti suurempia.

Nopeustesti tehtiin menemällä keskelle tilaa ja suoritettiin Ooklan speedtest -sovellus. Sovellus antoi tuloksena vasteajan, latausnopeuden ja lähetysnopeuden. (KUVIO 18.)



KUVIO 18. Nopeustesti

5.2.3 Kanavamittaus

Kanavamittauksella saatiin selville, montako tukiasemaa on käytössä kantaman sisällä. Jos kantaman sisällä oli paljon tukiasemia, jotka käyttävät samoja kanavia, verkon suorituskyky laski, sillä radiotaajuudet olivat ruuhkaiset. Kanavamittaus suoritettiin Fluke aircheck -testerillä. Testeri käynnistettiin painamalla vihreää virtanappulaa, minkä jälkeen esiin aukesi aloitusnäkymä. Aloitusnäkymästä valittiin ”Channels” -valinta. (KUVIO 19.) Valinnasta aukesi näkymä, josta nähdään, millä kanavilla tukiasemat toimivat (KUVIO 20).

KUVIO 19. Aloitusnäkymä

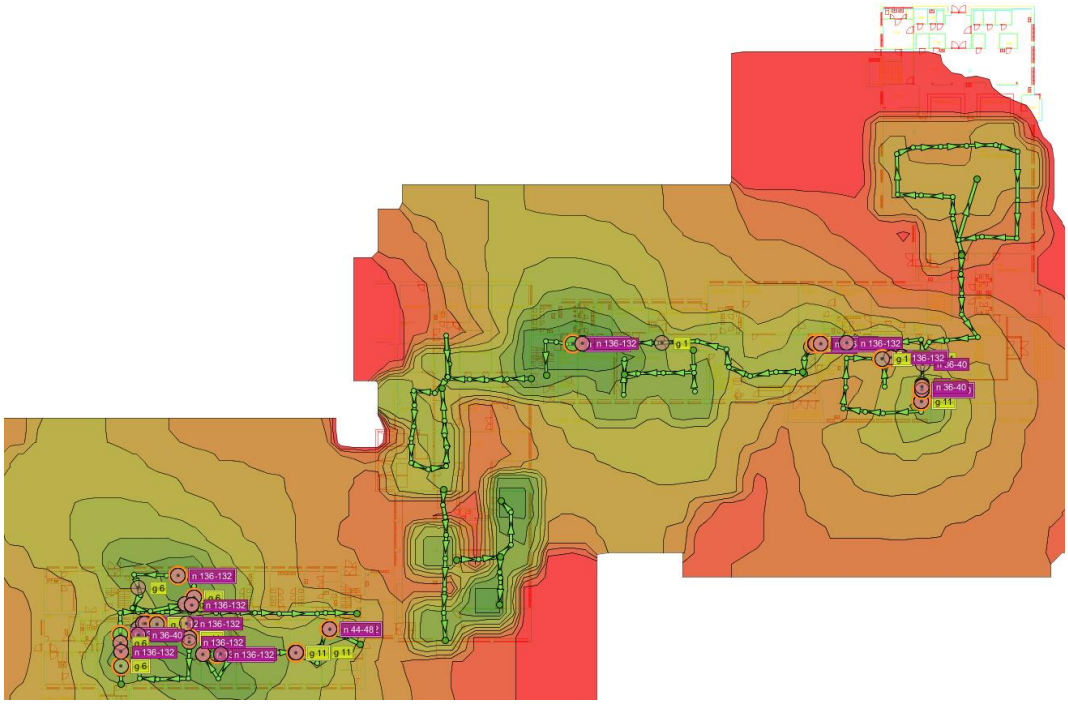
KUVIO 20. Kanavamittaus

Mittari vietiin testattavaan tilaan ja odotettiin hetki, että mittari päivittää tilan arvot. Mittarin näyttämät kanavat kirjattiin ylös, mikäli kanavilla oli paljon ruuhkaa. Testerillä nähtiin, kuinka monta tukiasemaa kullakin kanavalla on käytössä. Ruuhkainen kanava vaikutti suorituskykyyn negatiivisesti. (KUVIO 20.)

5.3 Mittaustulosten tulkitseminen

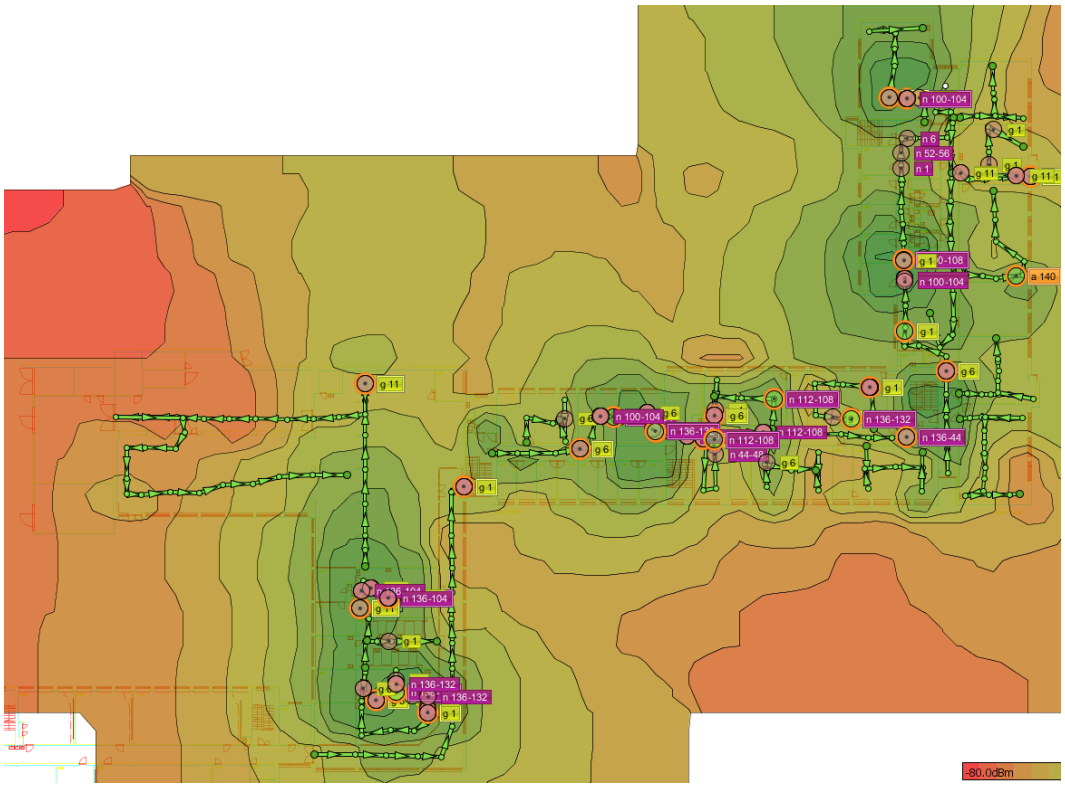
Kuuluvuuskartoituksen avulla saatiin selville, missä rakennuksen osissa on tarvetta uusille tukiasemille. Mittaustuloksia tulkitessa pitää ottaa huomioon vain ne tilat, joihin on tarkoitus saada verkko toimimaan. Verkon tulee toimia tiloissa, joihin opiskelijoilla on pääsy.

Tekniikan alan 1. kerroksen pohjakuvaa tarkasteltaessa on nähtävissä, että suurin tarve tukiasemille on E-siivessä. Sisääntuloaula ja ruokala ovat huonosti kuuluvia alueita, joihin on syytä lisätä tukiasemia. Kanavamittauksista selviää, että ruokalassa ja aulassa ovat raskaimmin käytettyinä 2,4 GHz:n kanavat. Nopeustesteistä selviää, että varsinkin lähetysnopeus on huomattavasti heikompi, kuin verrattuna tiloihin, joissa signaalin voimakkuus on hyvä. (KUVIO 21.) (LIITE 1.)



KUVIO 21. Tekniikan ala 1. kerros

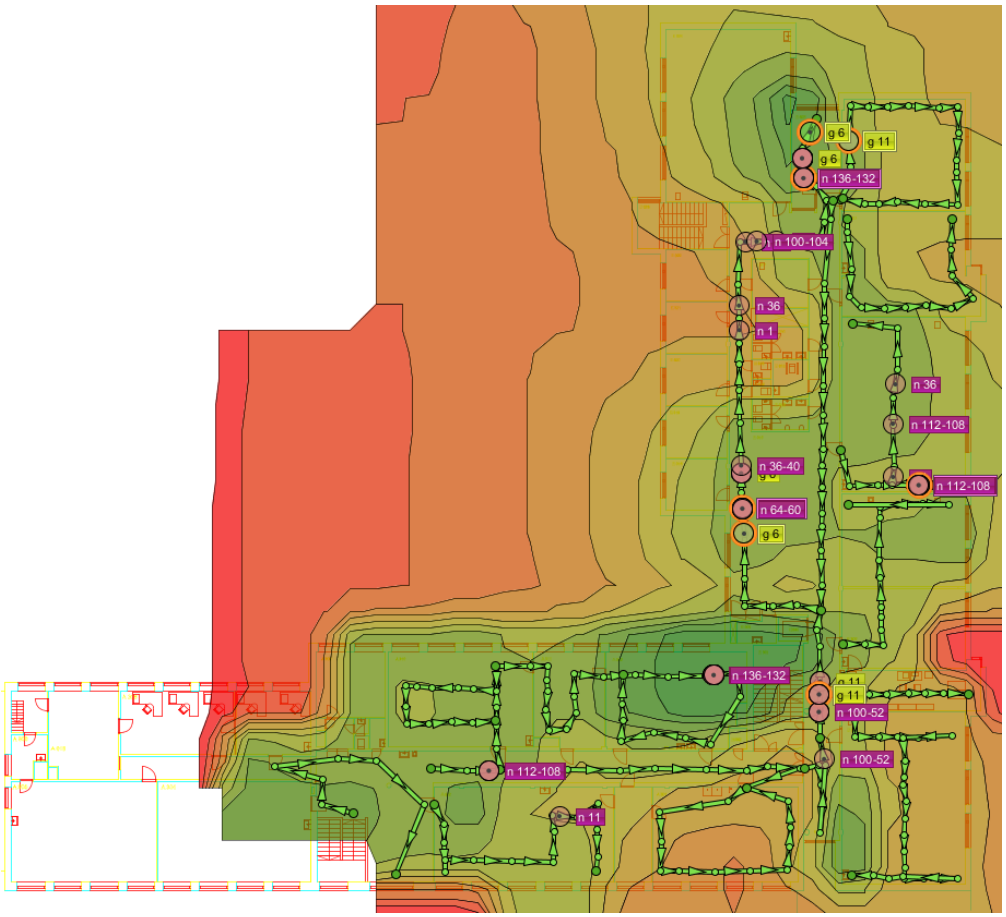
Tekniikan alan 2. kerroksen pohjakuvasta on nähtävissä, että verkko on oleellisilla alueilla varsin hyvin katettu. E-siivessä on taas suurimmat puutteet. Käytävän oikeanpuoleisissa luokissa on parannettavan varaa. Nopeustestien tulokset tukevat tätä, sillä tiedonsiirtonopeudet ovat vain 20Mbps molempiin suuntiin niissä luokissa, joissa signaali on heikompi. Kanavamittauksista selviää, että 2,4 GHz:n kanavat ovat E-siivessä raskaasti käytettyjä. 5 GHz:n alueella tilaa on enemmän uusille tukiasemille. (KUVIO 22.)



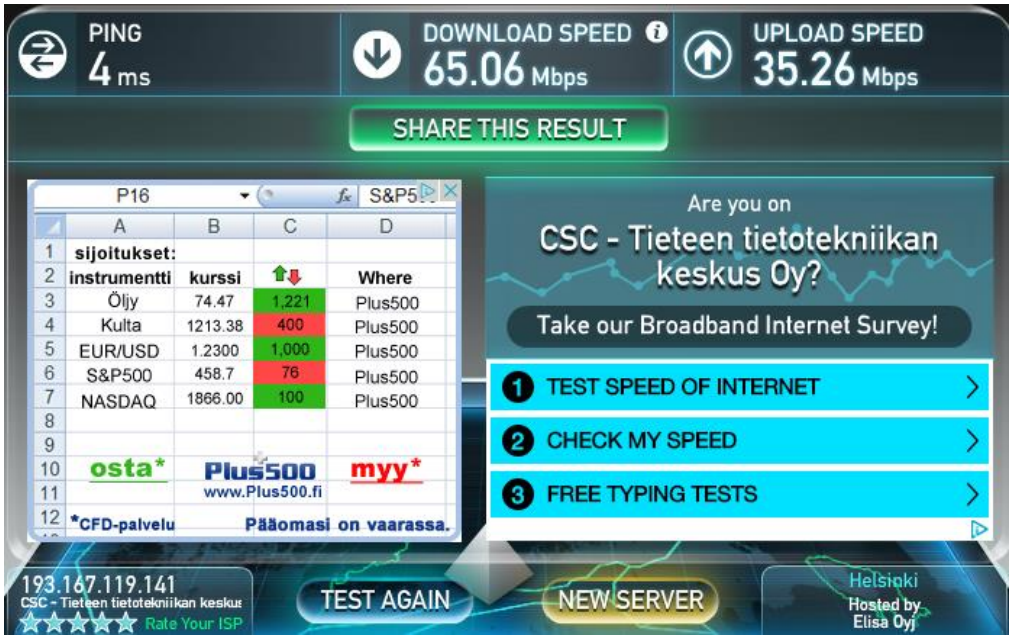
KUVIO 22. Tekniikan ala 2. kerros

Kolmannen kerroksen pohjakuvaa tarkasteltaessa voidaan huomata, että suurimmat puutteet ovat E-siivessä. Käytävän oikeanpuoleiset luokat tarvitsevat uusia tukiasemia. Lisäksi A-siivessä luokassa A301 signaalin voimakkuus on heikko. Nopeustesti tukee tätä, sillä lähetysnopeudessa päästään vain kolmasosaan verkon maksiminopeudesta. Latausnopeudessa jäädään kolmasosa maksiminopeudesta. 2,4 GHz:n

alueella on ruuhkaa näillä alueilla, joten uusia tukiasemia voidaan sijoittaa 5 GHz:n kanaville. (KUVIO 23.) (KUVIO 24.)

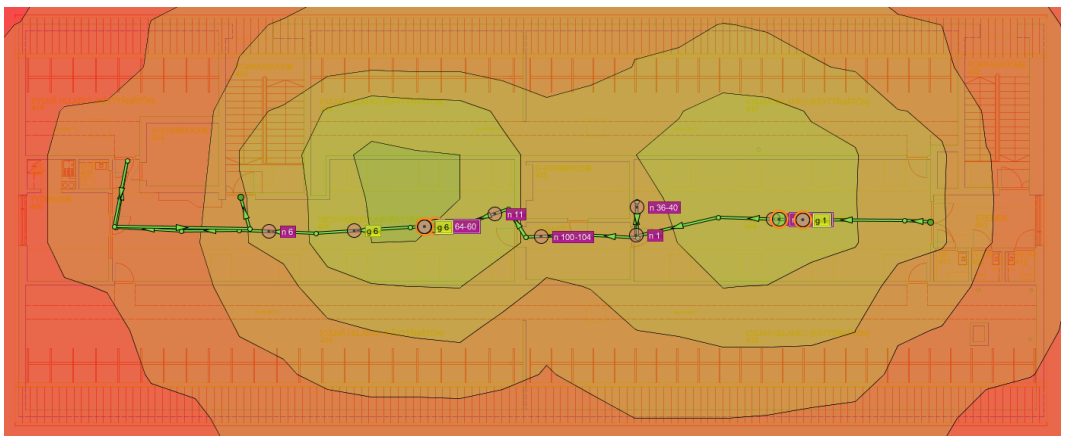


KUVIO 23. Tekniikan ala 3. kerros



KUVIO 24. Nopeustesti A301

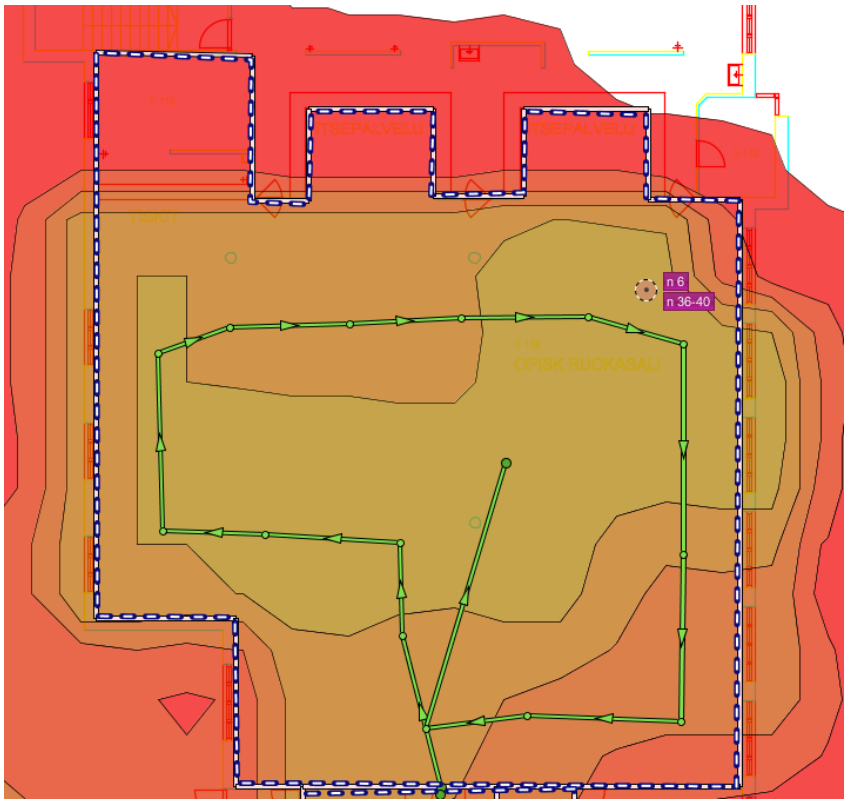
Neljännen kerroksen tietoverkkolaboratorioiden pohjakuvaa tarkasteltaessa huomataan, että signaalin voimakkuus ei ole kovin hyvä. Kyseessä ovat luokat, joissa on tietokoneet käytössä, joten langattomalle verkolle ei välttämättä ole suurta tarvetta. Nopeustestit paljastavat verkon lähetys- ja latausnopeudeksi vain 20 Mbps. 5 GHz:n kanava-alueella on tilaa lisätä uusia tukiasemia. (KUVIO 25.)



KUVIO 25. Tekniikan ala 4. kerros

5.4 WLAN-verkon suunnitelman laatiminen

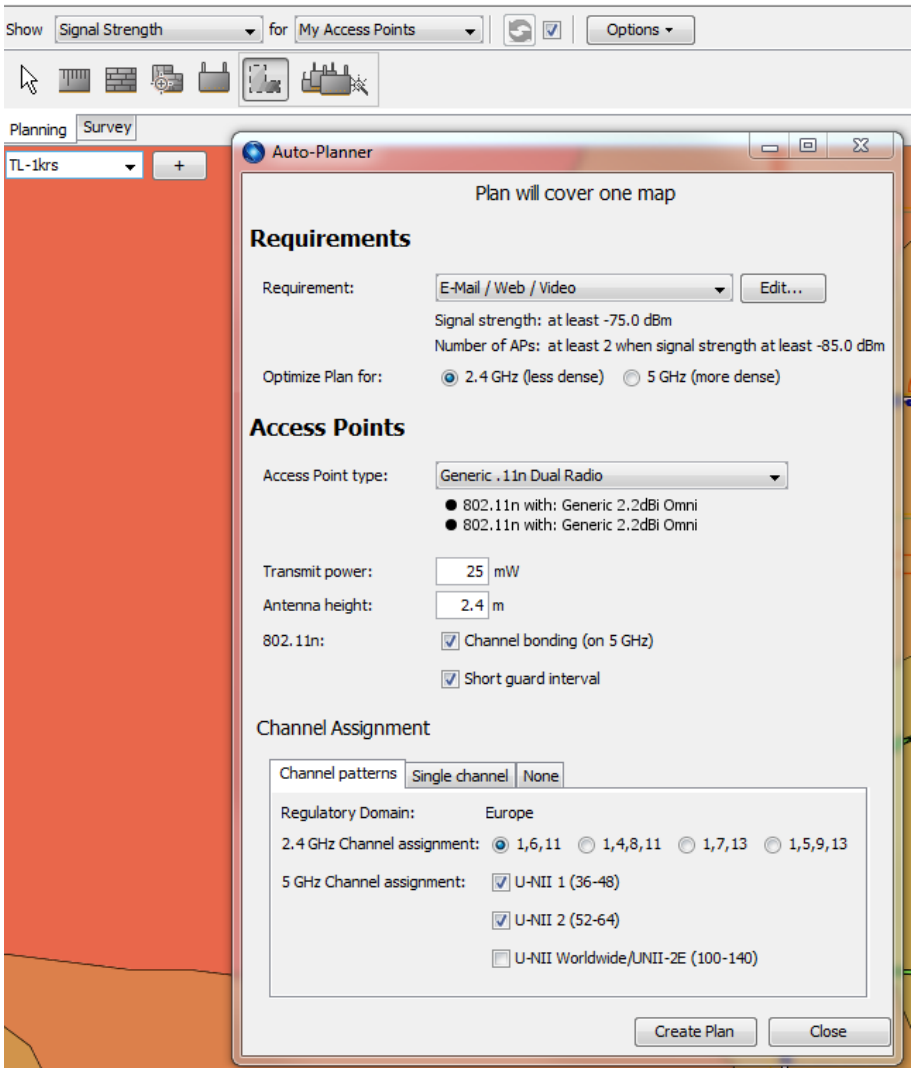
Suunnitelman laatimiseen käytettiin ekahau site survey –ohjelman planning ominaisuutta. Kanavamittauksia ja nopeustestejä käytettiin apuna suunnitelmaa laatiessa. Site surveyn pohjakarttojen päälle voidaan lisätä seinät ja alueet, joille langaton verkko halutaan kuuluvaksi. Seinät asetetaan wall –nimisestä painikkeesta ja osoitetaan pohjapiirrokseen seinien kohdalle hiirellä. Vastaavalla tavalla lisätään coverage -painikkeesta alueet, joihin halutaan verkko kuulumaan. (KUVIO 26.)



KUVIO 26. Planning –ominaisuus

Kun seinät ja coverage-alueet on määritelty, painetaan auto-planner nappulaa, joka avaa valikon, josta voidaan valita eri ominaisuuksia, joita langattomalta verkolta halutaan. Ensin valitaan verkon käyttö: valitaan E-mail/Web/Video, jolloin verkko on normaaliin käyttöön optimoitu. Access Points –kohdasta voidaan valita tukiaseman tyyppi, joka halutaan lisätä. Ohjelma sisältää runsaasti tunnettuja tukiasemia. Simuloinnissa käytetään

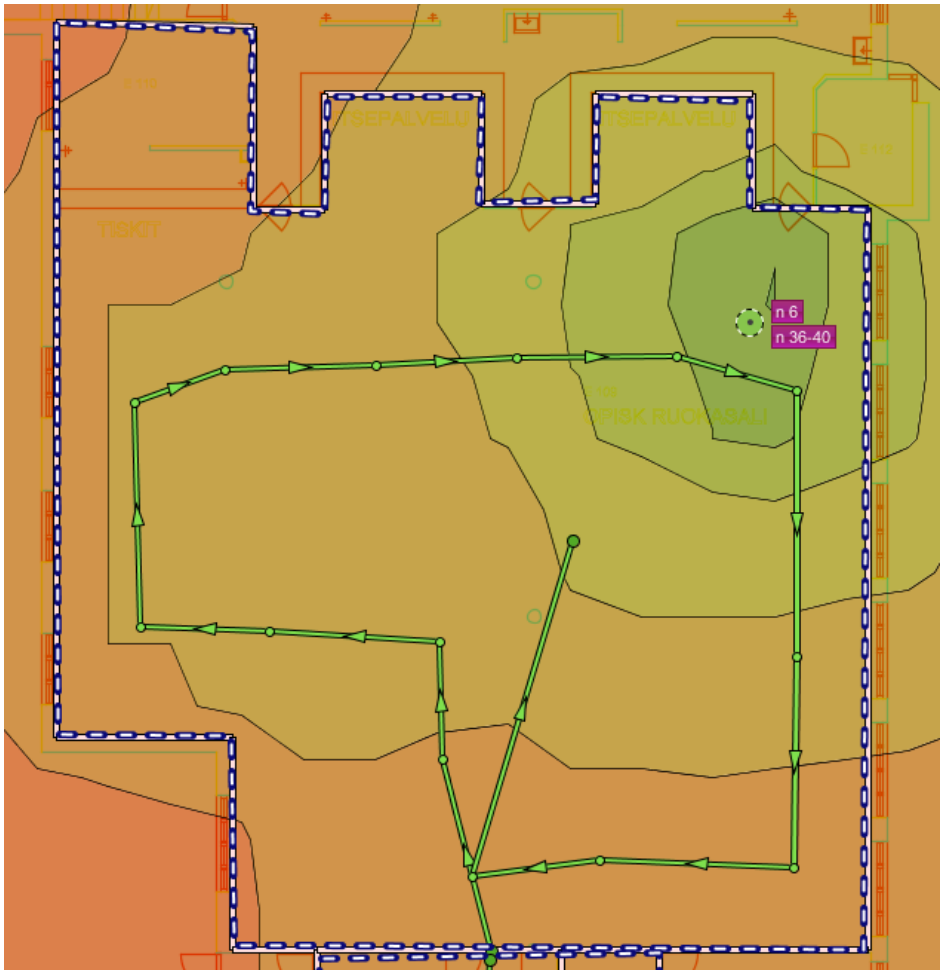
geneeristä 802.11n -standardia käyttävää tukiasemaa, joka on oletuksena. Seuraavaksi voidaan valita, mitä kanavaa tukiasemat käyttävät. Tässä vaiheessa voidaan hyödyntää kanavamittauksien tuloksia ja niiden perusteella valita sopiva kanava käyttöön. Lopuksi painetaan Create Plan, jolloin ohjelma sijoittaa automaattisesti tukiasemat parhaille paikoilleen. (KUVIO 27.)



KUVIO 27. Auto-Planner

Ohjelman saatua suunnitelman valmiiksi, ohjelma päivittää kuuluvuuden pohjakartalle automaattisesti. Ohjelman lisäämiä simuloituja tukiasemia voi liikuttaa eri paikkoihin, jolloin siirtämisen vaikutus nähdään pohjapiirroksessa samantien. Ohjelma saattaa lisätä turhia tukiasemia, joilla ei ole vaikutusta kuuluvuuteen paljoa, joten ylimääräiset tukiasemat

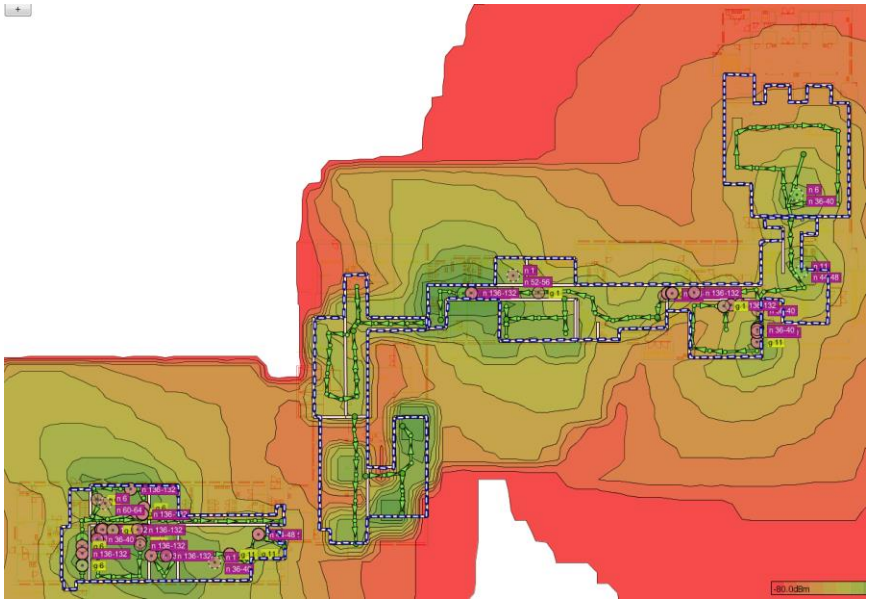
on helppo poistaa vasemmasta sivuvalikosta, jossa on listattuna kaikki tukiasemat.



KUVIO 28. Simuloitu tukiasema

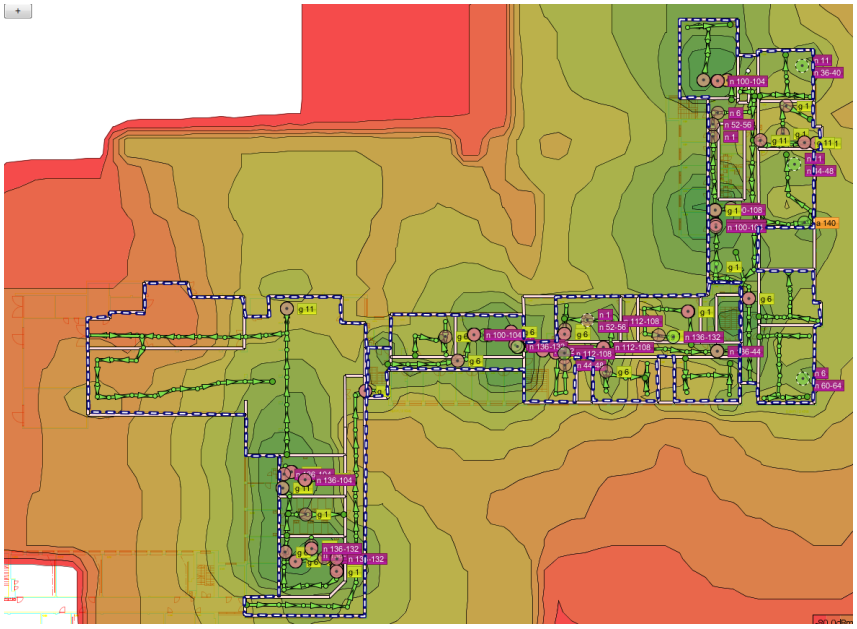
Lisättäessä yksi uusi tukiasema ruokalaan verkon kuuluvuus ja suorituskyky paranevat huomattavasti. Ruokalan lopullinen tukiasema sijoitus voi olla myös toisessa kohtaa, sillä siirrettäessä tukiasemaa, signaalin voimakkuus pysyy samana lähes koko alueella. (KUVIO 28.)

Tekemällä suunnitelman Tekniikan alan 1. kerrokselle ja mukauttamalla hieman tukiasemien sijainteja ja poistamalla ylimääräiset tukiasemat, saadaan varsin toteutuskelpoinen suunnitelma aikaiseksi. Tukiasemia on lisätty ruokalaan ja aulaan lisäämään verkon kattavuutta ja suorituskykyä. (KUVIO 29.)



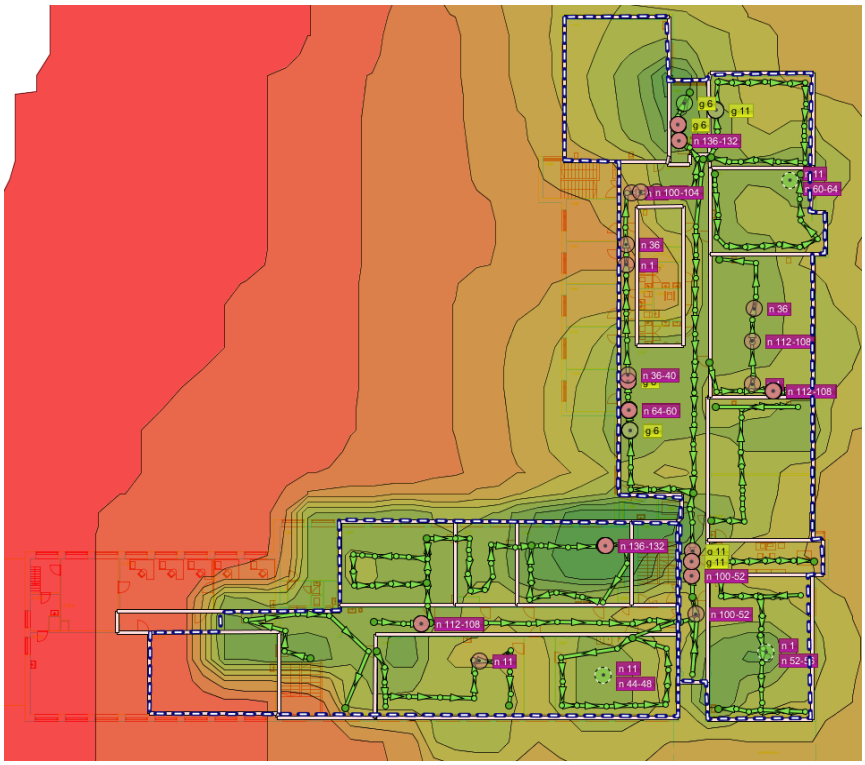
KUVIO 29. Tekniikan ala 1. kerros suunnitelma

Toisen kerroksen suunnitelmassa on lisätty tukiasemia E-siiven luokkiin E203, E206 ja E208. Näiden tukiasemien lisääminen parantaa huomattavasti verkon kuuluvuutta ja suorituskykyä E-siivessä. (KUVIO 30.)



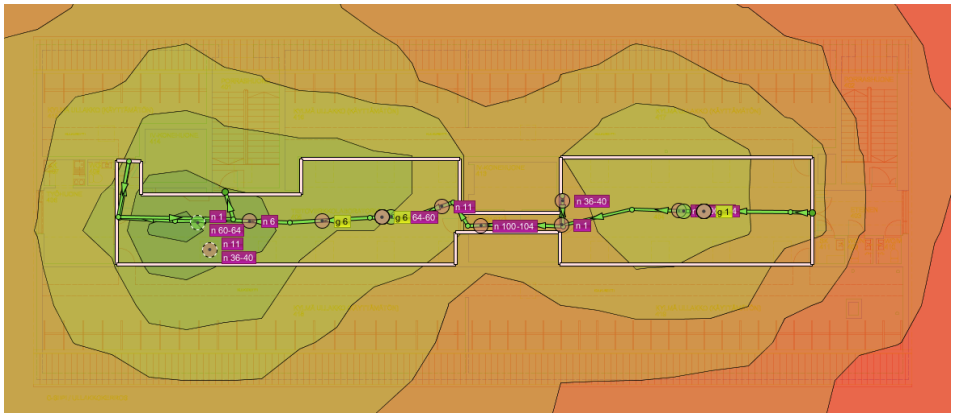
KUVIO 30. Tekniikan ala 2. kerros suunnitelma

Kolmannen kerroksen osalta tukiasemia on tarve lisätä A-siiven luokkaan A301 ja E-siiven luokkiin E303 ja E307. (KUVIO 31.)



KUVIO 31. Tekniikan ala 3. kerros suunnitelma

Neljännen kerroksen tietoverkkolaboratorioihin voi tarvittaessa lisätä yhden tukiaseman C406- tilaan parantamaan tilan langattoman verkon suorituskykyä. Luokat ovat kuitenkin atk-luokkia, joissa on kiinteät yhteydet, joten suurta tarvetta langattomalle verkolle näissä tiloissa ei ole. (KUVIO 32.)



KUVIO 32. Tekniikan ala 4. kerros suunnitelma

Osana suunnitelmaa on myös pistorasioiden kartoitus. Pistorasioita on oltava teorialuokissa riittävä määrä, jotta opiskelijoiden omat laitteet voidaan kytkeä verkkovirtaan. Suurimpaan osaan luokista riittää, että lisätään muutamia jatkojohtoja lisäämään pistorasioiden määrää. Muutamissa luokissa kuitenkin pistorasioiden määrä on pieni, tai pistorasiat on sijoitettu hankalaan paikkaan, josta syystä olisi hyvä asennuttaa muutamia pistorasioita lisää.

Luokat, joissa pistorasioiden määrä on pieni:

- A101 (kaikki pistorasiat edessä)
- A201 3kpl
- A203 6kpl
- A215 4kpl
- A220 3kpl
- A310 3kpl
- E207 8kpl

Muut tilat ovat joko atk-luokkia, joista ei pistorasiamäärää katsottu tarpeelliseksi katsoa, tai tiloja, joissa pistorasioita oli <10.

Ruokalan ja E-siiven aulan tukiasemille on tarve vetää ethernet -kaapeli jostain kauempaa, tai asennuttaa tietoliikennerasia lähettyville. Luokissa C406, E303, E307, E203, E206 ja E208 tukiasemien sijoituspaikoilla oli lähettyvillä tietoliikennerasioita.

Uudet tukiasemat voisivat olla tietohallinnon nykyisen käytännön mukaisesti Cisco -merkkisiä ja malleina Aironet 2700 tai Aironet 3700 – sarjan tukiasemia, jotka ovat Ciscon suosituksien mukaisia BYOD -tukiasemia. Molemmat tukiasemat tukevat 802.11ac -standardia.

5.5 Kokonaissuunnitelma

Taulukkojen ensimmäisellä sarakkeella on kerrottu tilan sijainti, toisella sarakkeella on kerrottu langattoman verkon nykytila ja viimeisellä sarakkeella on parannusehdotus. Sulkujen sisällä on lisätietoja. (TAULUKKO 3.) (TAULUKKO 4.)

Taulukossa 3 on viimeisellä sarakkeella ehdotettu kanavia 2 GHz:n ja 5 GHz:n taajuuksille. Kyseiset kanavat on valittu sen mukaan, miten vähän ruuhkaa kanavilla on ollut mittauksia tehdessä. 2 GHz:n kanavat 1, 6 ja 11 olivat kaikki ruuhkaisia kyseisissä tiloissa, joten on vain valittu vähiten ruuhkaisin kanava. 5 GHz:n alueella vapaita kanavia oli muutamia. (TAULUKKO 3.)

Uusiksi tukiasemiksi suosittelen Cisco Aironet 3700 sarjan tukiasemia. Tietohallinnon nykyiset tukiasemat ovat Cisco -merkkisiä. Aironet 3700 -sarjan tukiasemat tukevat 802.11ac -standardia ja toimivat 2,4G Hz/5 GHz:n taajuudella. 5 GHz:n käyttäminen tuo suurempia tiedonsiirtonopeuksia ja kapasiteettia on enemmän. 5 GHz:n kanavat ovat myös vähemmän käytettyjä tekniikan alalla.

Taulukossa on mainittu, mikäli tilassa ei ole tietoliikennerasiaa lähettyvillä. Näissä tapauksissa on tarve vetää ethernet -kaapeli jostain pidempää tai

asentaa tietoliikennerasia jonnekin tukiaseman lähettyville. (TAULUKKO 4.)

Taulukossa 4 on käyty läpi tilat, joissa on pistorasioita liian vähän. Näihin tiloihin olisi hyvä asennuttaa lisää pistorasioita. Auditorioon A101 olisi hyvä asentaa pistorasioita pöytätasojen alle, jotta opiskelijoiden omat laitteet voitaisiin kytkeä verkkovirtaan. Tällä hetkellä kaikki auditorion pistorasiat sijaitsevat tilan etuosassa. (TAULUKKO 4.)

TAULUKKO 3. Verkon kuuluvuus.

TILA	NYKYTILA	PARANNUSEHDOTUS
- 1. krs E-siipi aula	- kuuluvuus huono - Ei tietoliikenneyhteyttä	- 1 tukiasema (11, 112) - Tietoliikenneyhteys
- 1. krs E-siipi ruokala	- kuuluvuus huono - Ei tietoliikenneyhteyttä	- 1 tukiasema (1, 112) - Tietoliikenneyhteys
- 2. krs E-siipi E203	- kuuluvuus välttävä	- 1 tukiasema (11, 136)
- 2. krs E-siipi E206	- kuuluvuus välttävä	- 1 tukiasema (11, 136)
- 2. krs E-siipi E208	- kuuluvuus välttävä - ATK-tila	- 1 tukiasema (1, 136)
- 3. krs A-siipi A301	- kuuluvuus huono - Ei tietoliikenneyhteyttä	- 1 tukiasema (11, 100) - Tietoliikenneyhteys

- 3. krs E-siipi E303	- kuuluvuus välttävä - ATK-tila	- 1 tukiasema (6, 100)
- 3. krs E-siipi E307	- kuuluvuus välttävä - ATK-tila	- 1 tukiasema (11, 100)
- 4. krs C-siipi C406	- kuuluvuus huono - ATK-tila	- 1 tukiasema (1, 136)

TAULUKKO 4. Pistorasiat.

TILA	NYKYTILA	PARANNUSHEDOTUS
- 1. krs A-siipi A101	- Pistorasiat kaikki tilan etuosassa	- Taakse ja sivuille pistorasioita - Pöytätasojen alle pistorasioita
- 2. krs A-siipi A201	- Pistorasioita 3kpl	- Pistorasioita lisää
- 2. krs A-siipi A203	- Pistorasioita 6kpl	- Pistorasioita lisää
- 2. krs A-siipi A215	- Pistorasioita 4kpl	- Pistorasioita lisää
- 2. krs A-siipi A220	- Pistorasioita 3kpl	- Pistorasioita lisää
- 2. krs E-siipi E207	- Pistorasioita 3kpl	- Pistorasioita lisää
- 3. krs A-siipi A301	- Pistorasioita 8kpl	- Pistorasioita lisää

6 YHTEENVETO

Mittaamalla langattoman lähiverkon signaali, saadaan hyvä käsitys siitä, minkälainen suorituskyky verkolla on. Signaalin ollessa heikko tiedonsiirtonopeudet putoavat. Heikko signaali voi myös johtaa yhteyden katkeamiseen. Signaalin voimakkuuteen voidaan vaikuttaa sijoittamalla lisää tukiasemia rakennukseen. Voimakkuuteen voidaan vaikuttaa myös asettamalla tukiasemia sekä 2,4 GHz:n, että 5 GHz:n radiotaajuuksille. 2,4 GHz:n radiotaajuuksilla päällekkäin toimivia kanavia on useita, joten on suotavaa käyttää kanavia 1,6 ja 11 mahdollisimman paljon, jotka eivät toimi päällekkäin. Nykyään useimmat laitteet tukevat vähintään 802.11n -standardia, joten tukiasemien lisääminen 5 GHz:n radiotaajuudelle, jossa on paljon enemmän tilaa kanaville, ei ole ongelma.

Tekniikan alan langatonta lähiverkkoa voidaan parantaa sijoittamalla uusia tukiasemia alueille, joissa on heikko signaali, ja joissa on käyttöä langattomalle verkolle. Suunnitelmaa tehdessä keskityttiin parantamaan verkon kuuluvuutta niillä alueilla, jossa opiskelijat oleilevat. Suunnitelmassa ei otettu kantaa kustannuksiin, vaan tarkoituksena oli tehdä ”järkevä” ja toteutuskelpoinen parannusehdotus.

Opinnäytetyön tavoitteet tulivat täytettyä. Työn kaksi osaa tukivat toinen toisiaan. Mittaamisella saatiin verkon nykytila tietouteen ja suunnittelulla saatiin parannusehdotukset. Varsinainen tietohallinnolle lähetetty suunnitelma on opinnäytetyöstä karsittu raportti, jossa on keskitytty pelkästään mittaustuloksiin ja suunnitelmaan.

Langatonta lähiverkkoa voidaan parantaa vielä tulevaisuudessa näiden dokumentaatioiden pohjalta. Nykyisiä tukiasemia voidaan parantaa vaihtamalla ne tulevaisuudessa uudempiin, jotka mahdollistavat suurempia tiedonsiirtonopeuksia. 802.11 -standardeja tulee koko ajan lisää, jonka myötä tukiasemien nopeudet paranevat kokoajan.

Langattoman verkon kuuluvuus yrityksissä ja organisaatioissa on tärkeää työntekijöiden ja vierailijoiden kannalta. Työntekijöiden ja vierailijoiden mobiililaitteet voidaan yhdistää verkkoon esimerkiksi neuvottelutiloissa,

jolloin kokousmateriaalit voivat olla kaikkien omilla laitteilla nähtävissä. Langaton verkko mahdollistaa työskentelyn myös muualla kuin omalla työpisteellä.

LÄHTEET

Aeroflex. 2012. Wide bandwith measurement techniques for 802.11ac WLAN devices [viitattu 19.2.2015]. Saatavissa: http://www.mpdigest.com/issue/Articles/2012/Aug/Aeroflex/Default.asp

InformationWeek. 2012. 3 Tips to Keep BYOD from killing your network [viitattu 12.2.2015]. Saatavissa: http://www.networkcomputing.com/3-tips-to-keep-byod-from-killing-your-network/a/d-id/1233902?

ITPRO. 2013. Surge in BYOD sees 7/10 employees using their own devices [viitattu 12.2.2015]. Saatavissa: http://www.itpro.co.uk/mobile/19944/surge-byod-sees-710-employees-using-their-own-devices#ixzz31cNhd9ul

Frodigh M., Johansson P. & Larsson P., 2000. Wireless ad hoc networking – The art of networking without a network [viitattu 19.2.2015]. Saatavissa: http://people.cs.vt.edu/~hamid/Mobile_Computing/papers/frodigh_ericsson00.pdf

PCWorld. 2011a. IT Security's scariest acronym: BYOD [viitattu 12.2.2015]. Saatavissa: http://www.pcworld.com/article/236727/it_securitys_scariest_acronym_byod_bring_your_own_device.html

PCWorld. 2011b. Pros and cons of BYOD [viitattu 12.2.2015]. Saatavissa: http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

Silviu. A. 2010. CCNA Certification ALL-IN-ONE for dummies. Kanada. Wiley Publishing. Inc.

Tutorial-Reports. 2013. IEEE 802.11 Architecture [viitattu 13.2.2015]. Saatavissa: http://www.tutorial-reports.com/wireless/WLANwifi/wifi_architecture.php

Wikipedia. 2015a. IP-osoite [viitattu 5.3.2015]. Saatavissa: http://fi.wikipedia.org/wiki/IP-osoite

Wikipedia. 2015b. MAC-osoite [viitattu 5.3.2015]. Saatavissa: http://fi.wikipedia.org/wiki/MAC-osoite

Wikipedia. 2015c. OSI-malli [viitattu 5.3.2015]. Saatavissa: http://fi.wikipedia.org/wiki/OSI-malli

Wikipedia. 2015d. WLAN [viitattu 12.2.2015]. Saatavissa: http://en.wikipedia.org/wiki/Wireless_LAN

LIITTEET

LIITE 1. NOPEUSTESTIT

TILA	LATAUSNOPEUS	LÄHETYSNOPEUS	VASTEAIKA
1. krs A101	72.67 Mbps	67.83 Mbps	6 ms
1. krs A106	16.86 Mbps	19.13 Mbps	6 ms
1. krs Aula	40.53 Mbps	18.12 Mbps	6 ms
1. krs B104	20.66 Mbps	18.39 Mbps	5 ms
1. krs C101	40.36 Mbps	25.35 Mbps	4 ms
1. krs C103	50.23 Mbps	33.04 Mbps	4 ms
1. krs C104	45.12 Mbps	40.84 Mbps	4 ms
1. krs C105	33.54 Mbps	39.53 Mbps	4 ms
1. krs Muovilab	22.69 Mbps	23.25 Mbps	4 ms
1. krs Ruokala	68.69 Mbps	28.11 Mbps	6 ms
1. krs Ruokala-aula	55.38 Mbps	16.97 Mbps	6 ms
2. krs A201	18.94 Mbps	24.21 Mbps	6 ms
2. krs A203	46.73 Mbps	17.84 Mbps	6 ms

2. krs A215	16.61 Mbps	20.56 Mbps	6 ms
2. krs A216	75.62 Mbps	30.67 Mbps	6 ms
2. krs A218	73.88 Mbps	47.50 Mbps	5 ms
2. krs A220	62.40 Mbps	28.80 Mbps	7 ms
2. krs A-siipi sunset boulevard	11.65 Mbps	18.29 Mbps	6 ms
2. krs A-siiven aula	38.62 Mbps	14.09 Mbps	6 ms
2. krs B202	78.20 Mbps	64.99 Mbps	5 ms
2. krs B205	79.19 Mbps	69.69 Mbps	4 ms
2. krs B209	19.70 Mbps	24.27 Mbps	5 ms
2. krs B211	65.27 Mbps	51.98 Mbps	4 ms
2. krs B-siipi laajakaista	71.80 Mbps	56.95 Mbps	3 ms
2. krs E203	72.10 Mbps	42.93 Mbps	5 ms

2. krs E204	76.39 Mbps	92.33 Mbps	4 ms
2. krs E206	19.89 Mbps	19.24 Mbps	5 ms
2. krs E207	58.18 Mbps	48.25 Mbps	5 ms
2. krs E208	27.69 Mbps	11.95 Mbps	5 ms
2. krs E224	54.37 Mbps	23.11 Mbps	4 ms
2. krs E-siipi käytävä	69.97 Mbps	90.97 Mbps	5 ms
3. krs A301	65.06 Mbps	35.25 Mbps	4 ms
3. krs A310	74.98 Mbps	48.42 Mbps	5 ms
3. krs A312	61.93 Mbps	31.39 Mbps	5 ms
3. krs A-siiven aula	76.30 Mbps	56.59 Mbps	5 ms
3. krs E302	55.83 Mbps	30.26 Mbps	5 ms
3. krs E303	78.24 Mbps	46.25 Mbps	5 ms
3. krs E304	72.39 Mbps	63.12 Mbps	4 ms

3. krs E305	76.06 Mbps	81.33 Mbps	5 ms
3. krs E306	75.09 Mbps	88.89 Mbps	5 ms
3. krs E307-308	75.98 Mbps	69.59 Mbps	5 ms
3. krs E-siiven käytävä	76.30 Mbps	65.30 Mbps	5 ms
4. krs C405	19.22 Mbps	20.94 Mbps	5 ms
4. krs C406	20.54 Mbps	22.71 Mbps	4 ms