SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

LANGATTOMAN VERKON LAADUNVALVONTA

TEKIJÄ/T: Sami Laakso

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Sami Laakso	
Työn nimi Langattoman verkon laadunvalvonta	
Päiväys 10.12.2017	Sivumäärä/Liitteet 30/0
Ohjaaja(t) laboratorioinsinööri Pekka Vedenpää / Savonia-ammattikorkeakoulu	
Toimeksiantaja/Yhteistyökumppani(t) Istekki Oy / Järjestelmäasiantuntija Saku Kärkkäinen	

Tiivistelmä

Opinnäytetyössä tarkasteltiin langattomien verkkojen laadunvalvontaa ja suunnittelua Istekin asiakkaalle. Teoria-osuudessa paneuduttiin langattomien verkkojen tekniikkaan, uhkiin ja hallitsemiseen.

Kuuluvuus- ja häiriömittaukset tehtiin Jynkän koululla Kuopiossa. Jynkän koulu on uudiskohde, jonne tarvittiin kattava ja tehokas langaton verkko. Tukiasemien sijoittelusuunnittelun jälkeen käytiin tekemässä alustava mittaus verkon kuuluvuudesta. Viimeisenä koulun käyttöönottamisen jälkeen koululla käytiin tekemässä häiriömittaus. Mittauksissa käytettiin Ekahau Site Survey ohjelmiston standard-versiota. Mittaustulokset dokumentoitiin ja opinnäytetyössä avattiin niistä tärkeimpiä tuloksia.

Lopputuloksena Jynkän koululle saatiin rakennettua toimiva langaton verkko, josta saatiin myös kattava mittausraportti Istekin tietoliikenneryhmälle. Koululle asennetut tukiasemat liitettiin WLAN-kontrolleriin, jonka avulla niitä voidaan hallita ja monitoroida. Monitoroinnin avulla on helppoa selvittää ja paikantaa vikoja.

Avainsanat
langaton, ekahau, WLAN,

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Sami Laakso			
Title of Thesis Wireless Netwok Quality Control			
Date	10 December 2017	Pages/Appendices	30/0
Supervisor(s) Mr. Pekka Vedenpää, Laboratory Engineer			
Client Organisation /Partners Istekki / Mr. Saku Kärkkäinen, Information Systems Specialist			

Abstract

The purpose of this thesis was to study the quality control and planning of a wireless network for one of Istekki's customers. The theoretical part of the thesis focused on the technique, threats and controlling of a wireless network.

Coverage and interference measurements were made at Jynkkä primary school in Kuopio. Jynkkä primary school is a new building where an extensive coverage and an efficient wireless network was wanted. After designing locations for the access points, an initial measurement about the wireless network coverage was made. Lastly, an interference measurement was made when the school was in service. Ekahau Site Survey program's standard version was used for measuring. The results of the measurement were documented to Istekki and the most important ones were explained in this thesis.

As a result, Jynkkä primary school was built up with a workable wireless network and for the Istekki's networking group an extensive measurement report was drawn up. The access points were connected to a WLAN controller with which they can be controlled and monitored. It is easy to sort out and locate faults with monitoring.

Keywords
wireless, measurement, Ekahau, WLAN

SISÄLTÖ

TYÖSSÄ KÄYTETYT LYHENTEET JA TERMIT

AAA	Authentication (todentaminen/autentikointi), Authorization (valtuutus) ja Accounting (tilastointi).
AES	Advanced Encryption Standard, lohkosalausmenetelmä.
AP	Access Point, langattoman verkon tukiasema.
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, tietoliikenteen siirtotien varausmenetelmä, vuoronvaraus.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, tietoliikenteen siirtotien varausmenetelmä, kilpavaraus.
dBm	Desibelimilliwatti, desibelinmäärä suhteessa milliwattiin.
DCF	CSMA/CA protokollaan perustuva siirtotien varausmenetelmä.
DHCP	Verkkoprotokolla, joka jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille.
DoS	Palvelunestohyökkäys, jossa pyritään estämään verkkosivuston käyttöä kuormittamalla sitä ylimääräisellä verkkoliikenteellä.
FHSS	Taajuushyppely, jossa lähettäjä vaihtaa lähetystaajuutta tietyn algoritmin mukaisesti.
IEEE	Kansainvälinen tekniikan alan järjestö.
IP	TCP/IP-mallin Internet-kerroksen protokolla. IP-protokollan tehtävänä on toimittaa IP-tietoliikennepaketit perille pakettikytkentäisessä Internet-verkossa.
MAC	Verkkosovittimen Ethernet-verkossa yksilöivä osoite.
NAT	Osoitteenmuutos tekniikka, jossa julkinen IP-osoite piilotetaan tai säästetään.
NAV	Verkon varausvektori.
PCF	Siirtotien varausmenetelmä.
PSK	Pre-Shared Key, ennalta määritetty salasana tukiasemalle kirjautuessa.

RADIUS	Remote Authentication Dial In User Service on tunnistusprotokolla, jota käytetään RADIUS-palvelimella kytkimien ja tukiasemien yhteyteen. RADIUS-palvelin voi myös säilyttää käyttäjänimiä ja salasanoja tietokannassaan.
RAM	Keskusmuisti, johon latautuu ohjelmien ja sovellusten tarvitsemia tietoja.
RF-signaali	Radiotaajuus
SNMP	Simple Network Management Protocol, sovelluskerroksen tietoliikenneprotokolla, jonka avulla verkossa oleva laite voi itsenäisesti antaa hälytyksiä.
SNR	Signal to Noise Ratio eli signaali-kohinasuhde. Sillä tarkoitetaan verkkolaitteiden signaalissa esiintyvän hyötysignaalin ja kohinasignaalin tehojen suhdetta.
VLAN	Virtual Local Area Network eli virtuaalilähiverkolla tietoliikenneverkko voidaan jakaa logiisiin osiin.
WEP	Wired Equivalent Privacy, tietoliikenteen salausmenetelmä. Suojauksen tarkoitus on salata langatonta verkkoa luvattomilta käyttäjiltä ja salakuuntelulta.
WPA	Wi-Fi Protected Access on salausmenetelmä, joka on kehittyneempi versio WEP-salauksesta.

1 JOHDANTO

Langattomat WLAN-verkot valtaavat alaa langallisilta verkoilta. Uutta tekniikkaa kehitetään jatkuvasti nopeiden ja toimintavarmojen verkkojen kysynnän kasvaessa. Langaton verkko mahdollistaa liikkuvuuden, helppokäyttöisyyden ja hyvän tietoturvan. Yritykset haluavat laajentaa langattomia verkkojaan mahdollistaakseen helpon ja tehokkaan työskentelytavan eri puolille rakennusta. Kaupungit ja kunnat ottavat käyttöön ilmaisia avoimia verkkoja ulko- ja sisätiloihin helpottaakseen ja edistääkseen asukkaiden verkonkäyttömahdollisuuksia. Kouluilla oppilaat pääsevät opiskelemaan tableteilta ja kannettavilta tietokoneilta kaikkialla rakennuksessa.

Päätelaitteiden nopea yleistyminen on lisännyt langattomien verkkojen kysyntää. Langatonta verkkoa käytetään matkapuhelimilla, tableteilla, kannettavilla tietokoneilla ja useilla viihdelaitteilla. Sillä saadaan vakaampi verkkoyhteys kuin 3G- tai 4G-verkkojen avulla. Lisäksi monet mobiililaitteet vaativat langatonta verkkoa tehdäkseen ohjelmistopäivityksiä sen toimintavarmuuden vuoksi.

Tämän opinnäytetyön tarkoituksena on tarkastella langattoman verkon tekniikkaa ja olla mukana suunnittelussa Jynkän koululle. Mittauksia tehtiin kahdesti. Molemmista mittauksista tehtiin raportit, joista saatiin opinnäytetyöhön tuloksia esille. Raporteista on otettu esille oleellisimpia langattoman verkon suunnittelussa tarvittavia tuloksia.

Opinnäytetyössä käsitellään aluksi langattoman verkon tekniikkaa, laitteita, tietoturvaa ja uhkia. Lopuksi esitellään työssä käytettyjä laitteita, mittausohjelmaa ja mittauksista saatuja tuloksia.

2 WLAN-VERKKO TEKNIIKKA

Langattoman verkon avulla ihmiset voivat käyttää verkkoa ilman, että päätelaite pitää olla kytkettynä fyysisesti tietoverkkoon. Se mahdollistaa liikkuvuuden vapauden, kun sähköpostia, Internettiä ja sovelluksia voidaan käyttää missä puolella vain rakennusta. Langattoman verkon laitteet käyttävät langatonta verkkokorttia, jota kutsutaan myös sovittimeksi. Langattoman lähiverkon (WLAN) tiedonsiirto tapahtuu radiosignaaleiden avulla, joka käyttää siirtotienään ilmaa. IEEE 802.11 on langattomien lähiverkkojen standardi ja se voi käyttää 2,4GHz ja 5 GHz taajuuskaistoja. (Geier 2005, 3-9.)

MAC-kerroksen vuoronvaraus tapoja on kaksi, joista CSMA/CA langattomien lähiverkkojen ja CSMA/CD langallisten lähiverkkojen varausmenelmä. Radioteitä kulkevassa liikenteessä langattomat tukiasemat kuulevat toisensa, mutta päätelaitteiden etäisyyden vuoksi vastaanotettu signaali vaimenee liikaa. (Puska 2005, 29.)

CSMA/CD-protokolla toimii ethernet-verkossa, jonka vuoronvarausmenetelmä tapahtuu välttämällä törmäyksiä. (Puska 2005, 105.) Tässä menetelmässä vuoron saa ensimmäisenä se, joka ehtii ensimmäisenä lähettämään kehyksensä. Kahden tai useamman koneen lähettäessä kehyksiä samanaikaisesti tapahtuu ns. törmäys (collision). Törmäyksessä kehysten signaalit sekoittuvat keskenään, joka aiheuttaa jännitetason nousua kaapelissa. Päätelaitteiden verkkokortit huomaavat tällöin törmäyksen tapahtuneen ja sitten yrittävät lähettää kehyksiä uudelleen. Verkkokortti kuuntelee, että havaitseeko se jännitettä vielä kaapelissa, jos ei niin kaapelin uskotaan olevan vapaa ja kehys voidaan lähettää. Tämän jälkeen kehys etenee väylässä lähettäjältä molempiin suuntiin ja alkaa keräämään vastaanottajan tietoja. (Hakala, M. ja Vainio, M 2005, 75-76.)

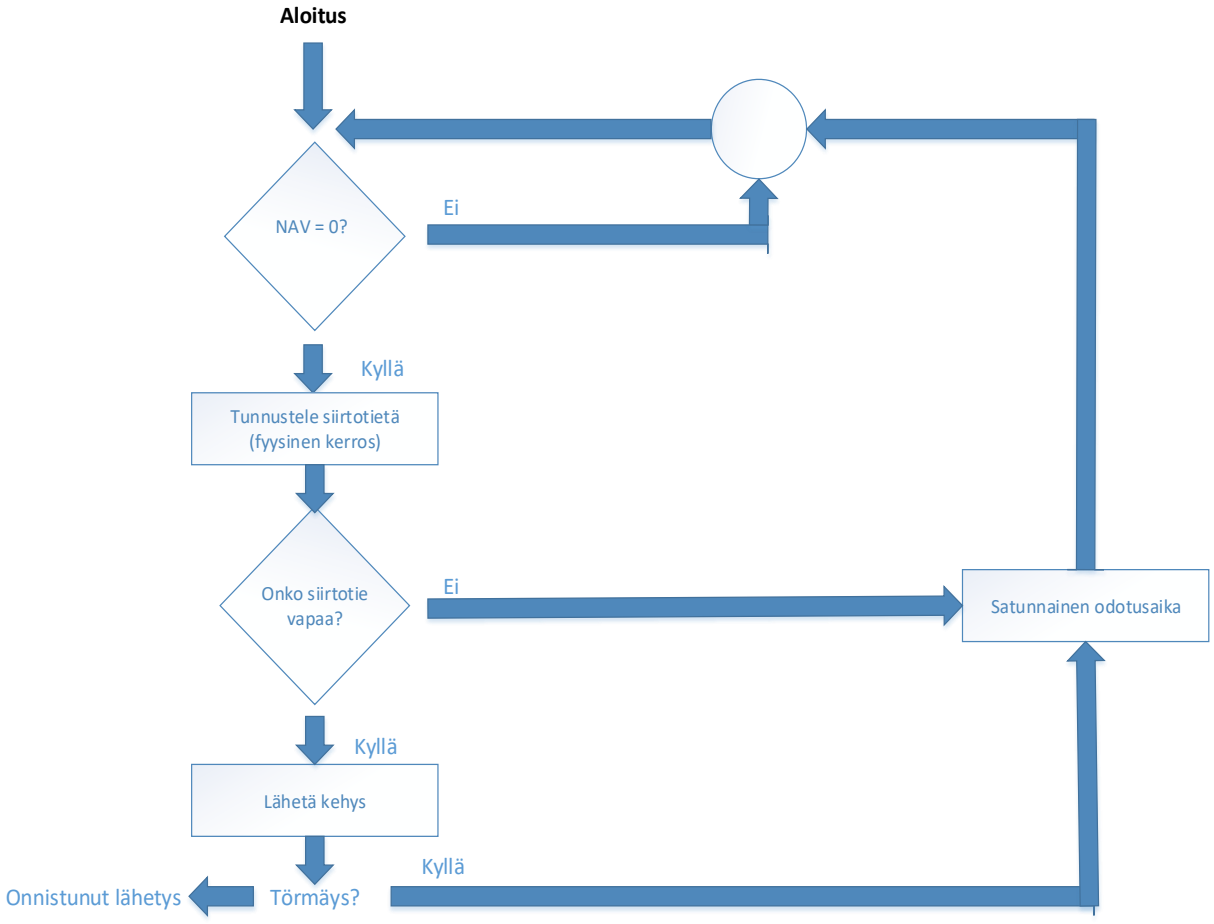
IEEE 802.11 -standardi määrittelee langattomaille lähiverkoille MACin. MAC-kerros pystyy hallinnoimaan ja ylläpitämään radioverkkokorttien ja tukiasemien välistä yhteyttä. 802.11 -standardi pystyy ohjaamaan tiettyjä fyysisiä 802.11-kerroksia, kuten 802.11a, 802.11b tai 802.11g. Kerrosten avulla voidaan suorittaa erilaisia tehtäviä, kuten siirtotien tunnustelua, lähetystä ja 802.11-kehysten vastaanottamista. Läheettääkseen kehyksiä aseman täytyy varata siirtotie, joka on asemien keskenään jakama radiokanava. 802.11 -standardilla on kaksi vaihtoehtoa varata siirtotie DCF ja PCF.

DCF on pakollinen toiminto ja se perustuu langattomissa verkoissa käytettävään CSMA/CA-protokollaan, jonka tarkoituksena on estää kilpavarauksien törmäyksiä. Asemat kilpailevat siirtoteiden varauksista ja pyrkivät lähettämään kehyksiä silloin kun siirtotie on vapaa. Toisen aseman lähettäessä kehystä, muut asemat odottavat, kunnes kanava on vapaa.

NAV on jokaisessa asemassa oleva laskuri, jonka tehtävänä on kertoa missä ajassa edellinen kehys on lähetettävä. MAC-kerros käyttää NAV ominaisuutta saadakseen selville, milloin asema voi yrittää

kehyksen lähettämistä. NAV-arvon ollessa 0, asema aloittaa laskemaan kehyksen lähettämiseen tarvittavaa aikaa perustuen sen pituuteen ja siirtonopeuteen. Asema saa tästä vastaavan arvon kehysotsikon kestokenttään, jota asemat tutkivat ja käyttävät oman NAVin asettamisen perustana. Tällä prosessilla saadaan varattua siirtotie lähettävälle asemalle.

Satunnaisella odotusajastimen avulla asema jää odottamaan satunnaisen ajan, jos kanava on käytössä. Satunnaisen ajan jälkeen asema voi yrittää uudestaan siirtotien varausta. Tämän avulla voidaan estää asemien samanaikainen datan lähetys. Asemat odottavat satunnaisia viiveitä pakettien lähettämisen välillä, jonka avulla vältetään siirtotien tunnustelu samaan aikaan. Odotusajastimella on tärkeä rooli datan lähetyksessä, koska se vähentää merkittävästi pakettien törmäyksiä ja niistä seuraavien uudelleenlähetysten määrää.



KUVA 1. DCF varausmenetelmä. (Laakso 2017-08-15)

PCF toimintoa käytettäessä varaa yksittäiselle asemalle pääsyn siirtotiehen. Varaus tapahtuu tekemällä asemien kiertokyselyitä ruuhkavapaana ajanjaksona. Kehysten lähettäminen ei onnistu ennen kuin asemat ovat tehneet kiertokyselyn.

Radiopohjaisessa lähiverkossa lähettävä asema ei kuuntele törmäyksiä lähettäessään dataa. ACK-kuittauksella vastaanottava asema saa tiedon, ettei virheitä ole vastaanotetussa kehyksessä. Kuittauksen puuttuessa, vastaanottava asema olettaa, että ilmatiessä on tapahtunut RF-interferenssiä tai törmäys ja silloin lähettää kehyksen uudelleen. (Geier 2005, 118-120.)

Radioverkkokortti etsii tukiasemia aktiivisella ja passiivisella skannauksella, joista passiivinen skannaus on pakollinen. Passiivisella skannauksella verkkokortti skannaa lähettyvillä olevia kanavia löytääkseen parhaan tukiasemasignaalin. Valinnaisella aktiivi skannauksella radioverkkokortti lähettää probe-tunnustelukehyksen, johon kaikki kantaman sisäpuolella olevat tukiasemat vastaavat. Tämä skannaus kuitenkin aiheuttaa lisää rasitetta verkkoon.

Beacon-viestin avulla päätelaitteet saavat tietoa tukiasemaa koskevista tiedoista, kuten SSID:n ja tuetut tiedonsiirtonopeudet. Radioverkkokortilla varustettu päätelaite mittaa signaalin voimakkuuden muiden tietojen ohella ja näin valitsee mitä tukiasemaa on parasta käyttää.

Ad hoc-tilassa olevat asemat toimivat independent basic service set-tilassa 802.11 standardissa. Silloin asema lähettää beacon-viestin, jolloin myös muut asemat saavat tiedon verkon olemassaolosta. Asemat lähettävät keskenään beacon-viestejä, ja jos asema ei vastaa beacon-jakson ja satunnaisajan loputtua, niin asema hajauttaa vastuun beacon-viestin lähettämisestä kaikille asemille. (Geier 2005, 120-121.)

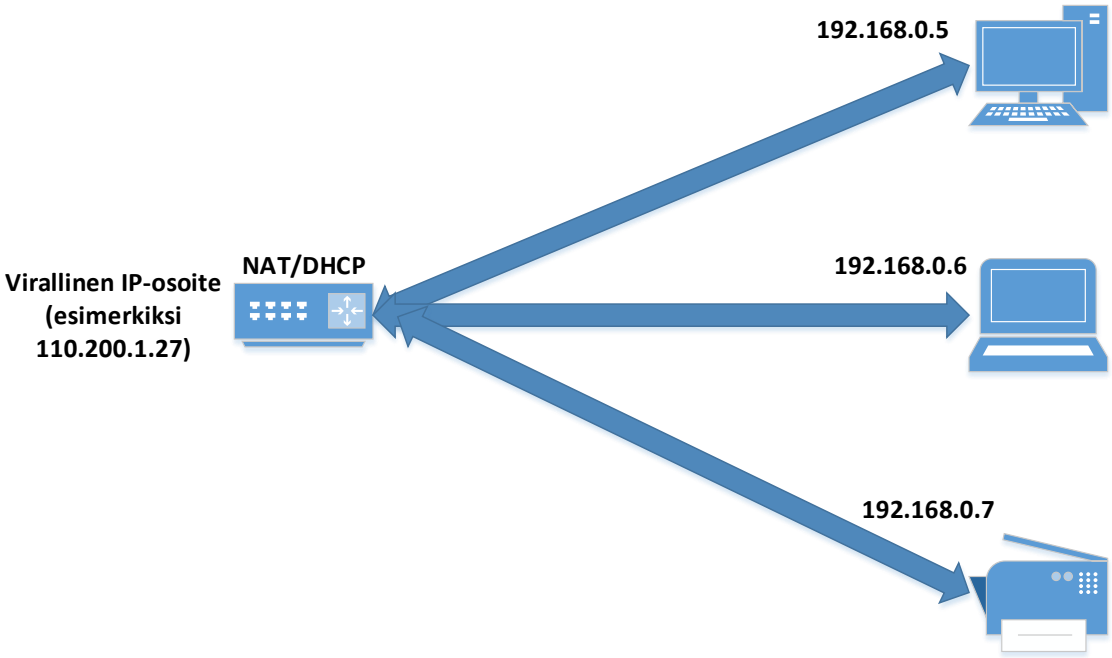
Langattomien lähiverkkoja voidaan käyttää kahdella eri kaistalla 2,4GHz ja 5GHz. Verkkoa suunniteltaessa tulee vertailla näitä kaistoja verkon vaatimuksia määriteltäessä. Suorituskyvyltään 5GHz kaistoilla on suurempi spektri. 5GHz kaistalla on 12 ei-päällekäisellä kanavalla jokaisella on 20MHz kaistanleveys ja 2,4GHz kaista on kokonaisuudessaan 80MHz levyinen ja se mahdollistaa vain kolme ei-päällekäisen kanavaa. 2,4GHz järjestelmien kantama on suurempi ja tukiasemia tarvitaan vähemmän. 5GHz kaistat eivät ole niin herkkiä häiriöille ja niiden kantama on pienempi, joka voi olla tietoturvan kannalta parempi asia. (Geier 2005, 128-129.)

3 WLAN-VERKKOLAITTEET

3.1 Kiinteän verkon aktiivilaitteet

Kytkin on tärkeimpiä verkkolaitteita. Verkot rakennetaan useimmiten tähtiverkoiksi ja kaapelointi tapahtuu parikaapelilla tai valokaapelilla. Verkkoon liitettävät laitteet voidaan liittää suoraan kytkimeen tai ne kytketään keskittimeen. Kytkimen toiminta perustuu MAC-osoitteisiin ja porttien liikenteeseen, jolloin kytkin kerää tietoja liitettyjen laitteiden kehysten lähetyksistä ja laatii ne muistiin. Virtuaalisten lähiverkkojen (VLAN) avulla voidaan rajoittaa kytkimeen tulevan verkon levitysaluetta. Tämän avulla voidaan rajata porteittain mitä verkkoa kytkin syöttää päätelaitteille. (Hakala, M. ja Vainio, M 2005, 84-87.)

Reittimen tehtävänä on siirtää paketteja verkkojen välillä. Se valitsee parhaan mahdollisen reitin paketeille IP-protokollan pakettiotsikoita, reititystauluja ja sisäisiä protokollia käyttäen. NAT-protokollalla (Network Address Translation) avulla verkkolaitteet voivat jakaa samoja Internet-palvelutarjoajan antamia IP-osoitteita. DHCP-protokollalla (Dynamic Host Configuration Protocol) jaetaan yksittäiset IP-osoitteet verkkoon liitetyille laitteille. Näitä protokollia käytettäessä yhdessä, verkkoon liitetyt laitteet voivat jakaa yhteisen Internet IP-osoitteen. (Geier 2005, 108-109.)



KUVA 2. NAT/DHCP yhteiskäyttö. (Laakso 2017-08-19)

3.2 Tukiasemat

WLAN-verkon yksi keskeisimmistä laitteista on tukiasema (access point), joka kannattaa valita sen standardin mukaan mitä suurimmasta osasta päätelaitteista tukee. Tukiasema ja päätelaite ottavat toisiinsa yhteyttä, kun ne tukevat samaa WLAN-standardia. (Hakala, M. ja Vainio, M 2005, 158.) Päätelaitteen verkkokortti ottaa yhteyttä lähimpään tukiasemaan. Liikkuessa rakennuksessa se vaihtaa toiseen tukiasemaan pitääkseen yhteyden luotettavasti yllä. (Geier 2005, 38.)

3.3 Kontrollerit

WLAN-kontrollereiden avulla voidaan ottaa tukiasemista koostuva verkko keskitettyyn hallintaan. Tukiasemien toimintoja on voitu vähentää ja samalla saatu kustannuksia pienemmäksiä, koska kontrolloreillä voidaan hallita tukiasemien toimintaa. Kontrollereiden kautta voidaan päivittää laiteohjelmistot, luoda pääsylistoja ja salauksia kaikille verkon tukiasemille. Tukiaseman rikkoutessa kontrol-

leri lataa tukiasemalle samat konfiguraatiot kuin vanhassakin. Keskitettyyn hallintaan kuuluu useimmiten myös tukiasemien välistä liikkuvuutta kehittäviä ratkaisuja ja radioverkon kanavasuunnittelua automatisoivia toimintoja. (Hovatta 2005, 16-17.)

Kontrollereissa on useimmiten selainkäyttöliittymä, sarjaporttiliitäntä ja telnet- tai SSH-komentoriviyhteys, joiden avulla konfigurointi voidaan suorittaa. Hallintakäyttöliittymää käytettäessä tukiasemilla tulee olla IP-osoite, jotta laitteeseen saadaan hallintayhteys. (Hovatta 2005, 25.)

3.4 Päätelaitteet

Langatonta verkkoa voidaan käyttää ilman kaapeleita monenlaisilla päätelaitteilla, kuten kannettavilla työasemilla ja pöytäkoneilla. (Geier 2015, 105.) Päätelaitteissa (client) tulee olla sisäinen tai ulkoinen langaton-verkkosovitin, joka on vastaava tukiaseman 802.11 -standardin kanssa.

4 HÄIRIÖTEKIJÄT

4.1 RF-signaalin ominaisuudet

Tietoliikennejärjestelmät käyttävät radiotaajuksia- eli RF-signaalia tiedonsiirtoon. Lähettävä ja vastaanottavien asemien antennit käyttävät RF-signaalia hyväkseen. RF-signaalissa on tietty amplitudi, taajuus ja vaihe. Amplitudin voimakkuus laskee, kun radiosignaali etenee ilmatilassa. Signaalin tulee olla voimakas, että se tavoittaa vastaanottavan aseman. Häiriötä asemien välisessä kommunikoinnissa aiheuttavat muut lähistön RF-signaalit. Taajuudet Wlan-verkoissa ovat joko 2,4GHz tai 5GHz, suuremmalla taajuudella signaali värähtelee useammin. Ilmatiessä taajuuteen ei juurikaan ole häiriöitä aiheuttavia vaikutuksia. RF-signaalin vahvuuksia on sen pitkä kantama, joka voi olla jopa 12 kilometriä suoralla näköyhteydellä. Ulkokäytössä signaali etenee hyvin myös sumuisissa olosuhteissa, mutta rankkasade voi huomattavasti heikentää suorituskykyä.

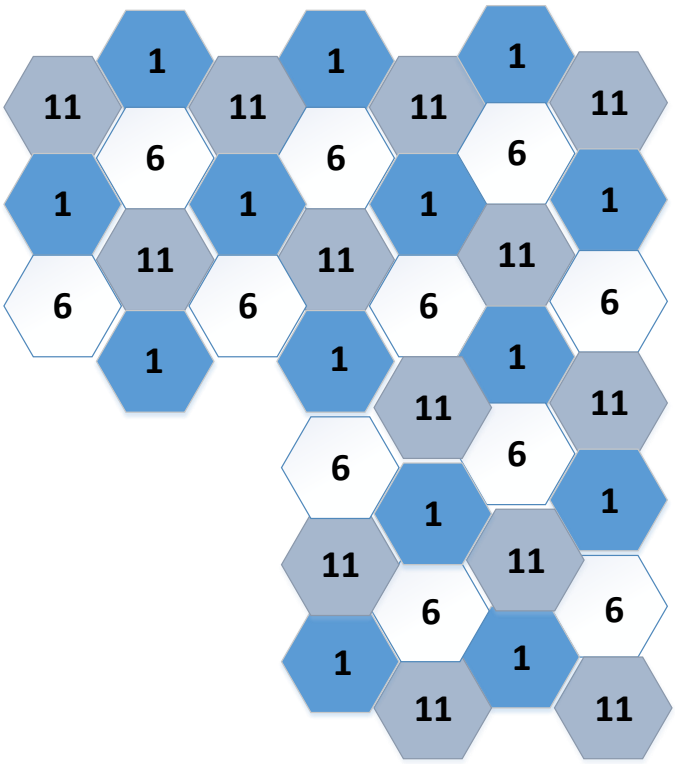
Interferenssi ja heijastuminen heikentävät radiosignaaleja, mikä aiheuttaa suorituskyvyn heikkenemistä ja viiveitä verkon datasiirrossa. Interferenssi syntyy silloin, kun muut asemat käyttävät samaa kaistaa tiedonsiirrossa. Se aiheuttaa virheitä lähetetyissä informaatiobiteissä, mikä aiheuttaa uudelleenlähetyksiä ja näin muodostaa viiveitä verkossa. Signaalin heijastumista muodostuu, kun kantama-alueella on esteitä esimerkiksi suuria huonekaluja. Tällöin vastaanottava asema tekee virheitä moduloidessaan heijasteita sisältävän datan. Vastaanottava asema havaitsee virheet aseman virhetarkastuksessa ja lopulta lähettää datakehyksen uudelleen. Heijastumista voidaan parhaiten ehkäistä toistevastaanottiantennilla, jolloin toiseen antenniin saadaan parempi signaali. Toistevastaanotin tulisi olla fyysisesti eri sijainnissa, kuin vastaanottava asema. (Geier 2005, 70-75.)

4.2 Häiriöitä aiheuttavat esteet

Radiosignaaleiden interferenssit voidaan jakaa sisään- ja ulospäin suuntautuviin lähteisiin. Sisäänpäin suuntautuvalla interferensillä tarkoitetaan, että jostain muusta radiosignaaleja lähettävästä järjestelmästä tulee häiriöitä. Interferenssin lähteitä ovat myös langattomat puhelimet, mikroaaltouunit ja Bluetooth-laitteet. Näiden sijainti vaikuttaa merkittävästä verkon suorituskykyyn ja ne tulee ottaa huomioon verkkoa suunniteltaessa. Ulospäin suuntautuvalla interferenssilä tarkoitetaan tilannetta, jossa langattoman verkon radiosignaalit häiritsevät muita radiosignaaleja käyttäviä järjestelmiä. (Geier 2015, 74.) Mikroaaltouunien aiheuttamaa interferenssiä tapahtuu vain silloin kun mikroaaltouuni on päällä. Osa mikroaaltouuneista käyttää vain yhden kolmasosan 2,4GHz taajuudesta ja loput kokonaista taajuutta. Interferenssiä voidaan kuitenkin estää vaihtamalla kanavaa, jota langaton tukiasema käyttää. Langattomat puhelimet aiheuttavat myös interferenssiä, kun ne käyttävät 2,4GHz ja 5GHz taajuuksia. Useimmat puhelimet valitsevat kanavan vähiten ruuhkautuneen kanavan, mutta useiden puhelinten käyttäessä koko spektriä ne aiheuttavat häiriötä tukiasemissa. Bluetooth laitteet käyttävät kokonaista 2,4GHz taajuutta, mutta ne käyttävät toiminnassaan FHSS (Frequency Hopping Spread Spectrum) taajuushyppelyä. Taajuushyppelyn ansiosta Bluetooth laitteet käyttävät keskimäärin yhtä kolmasosaa 802.11 -standardin 2,4GHz taajuudesta. Bluetooth laitteiden aiheuttamat häiriöt riippuvat kuitenkin niiden suuresta määrästä ja sitä aiheutuu vain, kun Bluetooth ja 802.11 -standardin laite lähettävät dataa samaan aikaan. Esimerkiksi kannettavalta tietokoneelta tulostaminen Bluetoothin avulla häiritsee vain hetken langatonta verkkoa. Suurimmat vaikutukset tulevat ilmi, kun tilassa käytetään laajaa Bluetooth-verkkoa. Silloin lähettävien Bluetooth laitteiden tulee noin 30m säteellä tukiasemasta, että se voisi aiheuttaa merkittävää häiriötä langattomassa verkossa. (Ciscopress 2015.)

4.3 Tukiasemien sijoittaminen rakennuksessa

Langattoman verkon tukiasemissa voidaan käyttää suunnattuja antenneja, joilla voidaan paremmin rajata verkon käyttöalue. Radiosignaaleiden rajaamisella voidaan estää luvattomien käyttäjien pääsyä verkkoon. Antennien tehoa ja suuntausta voidaan muuttaa halutun alueen rajaamiseksi rakennuksen seinien sisäpuolelle. Tukiasemat tulisi aina sijoittaa näkymättömiin tai sellaiseen paikkaan, mistä siihen on hankalampi päästä käsiksi. (Geier 2015, 196-198.) Radiosignaaleihin vaikuttavan rakenteiden vaimennusta voidaan arvioida kaavalla, joka on tarkoitettu 2,4GHz:n taajuudella toimivien verkkojen signaalitason arviointiin. Yhteyden vaimennus (dB) = 40 + 20 log e + ak +bs, jossa e on laitteiden välinen etäisyys, a on kerrosten lukumäärä, b on välissä olevien seinien määrä. Kerroksen aiheuttama vaimennus on k ja seinän vaimennus s. Kaavassa voidaan käyttää tiettyjä oletusarvoja, jossa kerroksen vaimennusarvo (k) on 30 dB. Seinien vaimennuksista (s) ikkunallisen tiiliseinän 2 dB, ikkunaton tiiliseinä 3 dB, harkkoseinä 4 dB, metalliovi 12 dB ja muut väliseinät 6 dB. Todellisuudessa paras tieto vaimennuksista saadaan tekemällä koemittauslaitteella vaimennusmittaus ja suunnitella sen avulla tukiasemien parhaat sijoituspaikat. Vierekkäisten tukiasemien kanavat tulisi valita niin, että välissä olisi kaksi tai kolme tukiasemaa käyttämässä eri kanavaa. Kanavilla 1, 6 ja 11 saadaan parhaita tuloksia ja tukiasemien kanavien suunnitteluun voidaan käyttää ns. hunajakennomallia. (Hakala, M. Vainio, M ja Vuorinen, O 2006, 293-294.)



KUVA 3. Tukiasemien kanava suunnittelu. (Laakso 2017-08-15)

5 TIETOTURVA

5.1 Autentikointi ja salaus

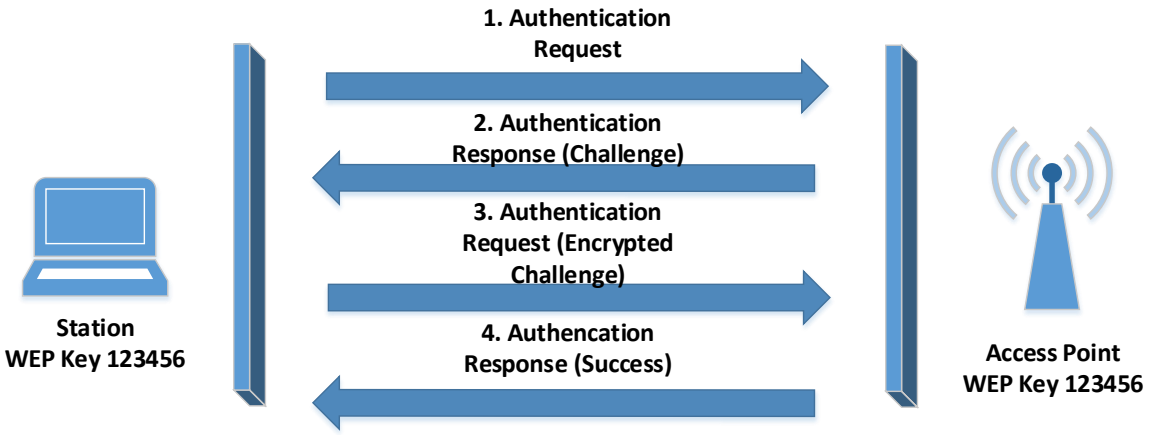
Langaton verkko käyttää tiedonsiirtonaan radioaaltoja, jonka takia sitä on helppoa vakoilla ja myös luvaton verkkoon liittyminen on helpompaa. Suojauskäytäntöjä on kehitetty useita erilaisia, joita käytetään liikenteen salakuuntelun ja luvattoman käytön ehkäisemiseksi. Turvallisuutta on parannettu myös ottamalla käyttöön kiinteistä verkoista tuttuja salaus- ja autentikointiprotokollia. (Hakala, M. ja Vainio, M 2005, 167.)

5.1.1 WEP

WEP-tunnistus perustuu symmetriseen menetelmään, jolloin kaikilla langattomilla asemilla pitää olla määriteltynä sama avain kuin yhteyspisteellä. WEP-suojausta ei pidetä enää nykyään turvallisena, koska se tarjoaa vain kohtuullisen ja yksinkertaisen tunnistusmenetelmän. Suojausavaimina voidaan käyttää 40-bittistä tai 104-bittistä. Suojausavaimiin lisätään vielä 24-bittinen alustusvektori, jolloin useimmiten suojausavaimia kutsutaan 64-bittisiksi tai 128-bittisiksi.

WEP-tunnistautumisessa ensimmäinen vaihe on päätelaitteen autentikointi pyyntö-lähetys yhteyspisteelle. 802.11-standardin hallintakehys pitää yllä sekvenssinumeroa, jolla jokainen lähetys ja vastaanottopyyntö numeroidaan. Seuraavaksi yhteyspiste lähettää takaisin paketin, joka sisältää tunnistusalgometrinä jaetun avaimen tunnistuksen, onnistuneen tilakoodin, haastetekstinä satunnaisesti generoidun merkkijonon ja sekvenssinumeron 2. Päätelaitteen vastaanottaessa tämän paketin, se lähettää vastaavanlaisen takaisin. Päätelaite kuitenkin salaa paketin informaatioelementit WEP-

avaimellaan. Yhteyspisteen vastaanottaessaan tämän se vertaa tietoja omiin lähettämiinsä ja yrittää purkaa informaatioelementtiä. Tietojen vastaessa toisiaan yhteyspiste hyväksyy tunnistuksen ja lähettää kuittauksen. (Puska 2005, 74.)



KUVA 4. WEP autentikointi. (Laakso 2017-08-15)

5.1.2 WPA

WPA on Wi-Fi Alliancen kehittämä protokolla, joka antaa paremman suojauksen kuin WEP. WPA käyttää Temporal Key Intergrity Protocol- eli TKIP- ja 802.1x-mekanismia. Näillä mekanismeilla saadaan luotua dynaanimen avaimen salaus ja kaksisuuntainen todennus. Aluksi päätelaitteen käyttäjä todentaa itsensä tukiaseman kanssa, jonka jälkeen tukiasema voi valtuuttaa päätelaitteen lähettämään itselleen kehyksiä. Seuraavana WPA tekee käyttäjäntason todennuksen 802.1x:llä, jolloin se on yhteydessä todennuspalvelimeen. WPA:ta voi myös käyttää ilman todennuspalvelinta, jolloin todennus tapahtuu käyttämällä etukäteen jaetun avaimen tilaa. WPA-protokollaan on saatavana valinnaisena Advanced Encryption Standard- eli AES. Sen toimiminen kuitenkin vaatii rinnakkaisprosessoria tukiasemassa. Uusimmassa versiossa WPA2:ssa on AES salakirjoitusmenetelmä vakiona. (Geier 2005, 131.)

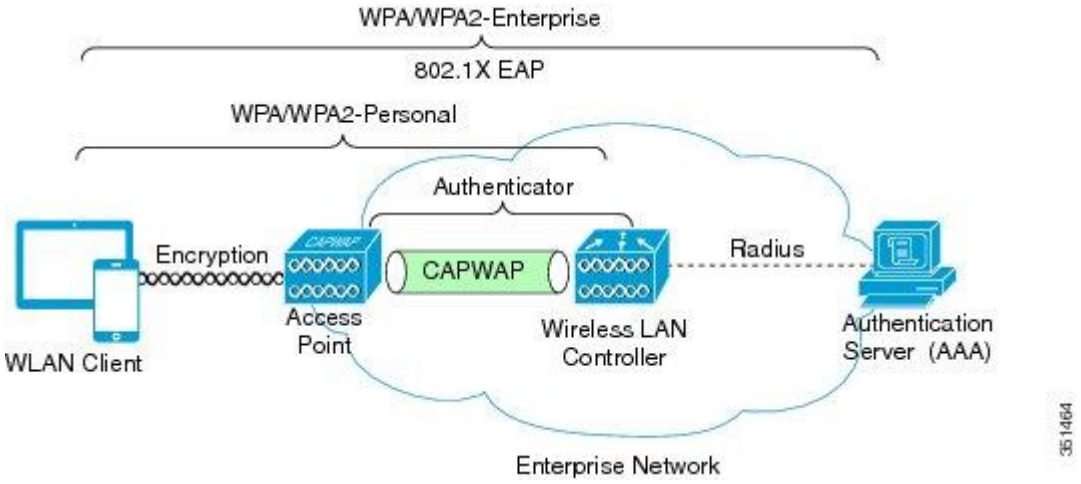
AES on salakirjoitusmenetelmä, jonka on kehittänyt Yhdysvaltojen hallitus. Menetelmä käyttää Rijndael-algoritmia, joka käyttää 128-, 192- tai 256-bittistä avainta ja myös sen lohkot ovat samankokoisia. Algoritmi järjestelee ja jakaa lohkon selväkielisanomia omiin salakirjoitusavaimen taulukkoihinsa. (Hakala, M. Vainio, M ja Vuorinen, O 2006, 382.) AES salakirjoitusmenetelmä on tehokas salausmenetelmä, mutta se voi vaikuttaa alentavasti WLAN suorituskykyyn. (Puska 2005, 118.)

Etukäteen jaettu salausavain eli PSK menetelmässä tukiasemiin ja verkkokortteihin määritellään aloitusavain. Aloitusavaimen avulla laitteet muodostavat toisiinsa yhteyden ja vaihtavat avaimet uusiin aina vähintään 10 000 kehyksen välein. (Hakala, M. Vainio, M ja Vuorinen, O 2006, 297.)

5.1.3 IEEE 802.1X

IEEE 802.1X-todennus määrittelee portin perusteella verkkoon liittymisen, jolloin verkon käyttöä rajoitetaan verkon loogisten porttien ja todennuspalvelimien avulla. Se on suunniteltu käytettäväksi

kaikissa IEEE 802 -lähiverkoissa. Mekanismi rajoittaa verkkoon pääsyä aktiivilaitteiden avulla. RADIUS-palvelimia käytetään todennukseen AAA-protokollan mukaisesti. Protokollaan kuuluu käyttäjän tunnistus (Authentication), käyttäjän oikeuksien määrittely verkon palveluihin (Authorisation) ja verkossa olevien tietokantojen hallinta (Accounting). (Hakala, M. Vainio, M ja Vuorinen, O 2006, 297-298.)



KUVA 5. WPA / WPA2 langattoman verkon topologia. (Cisco 2017)

5.2 Verkonhallinta

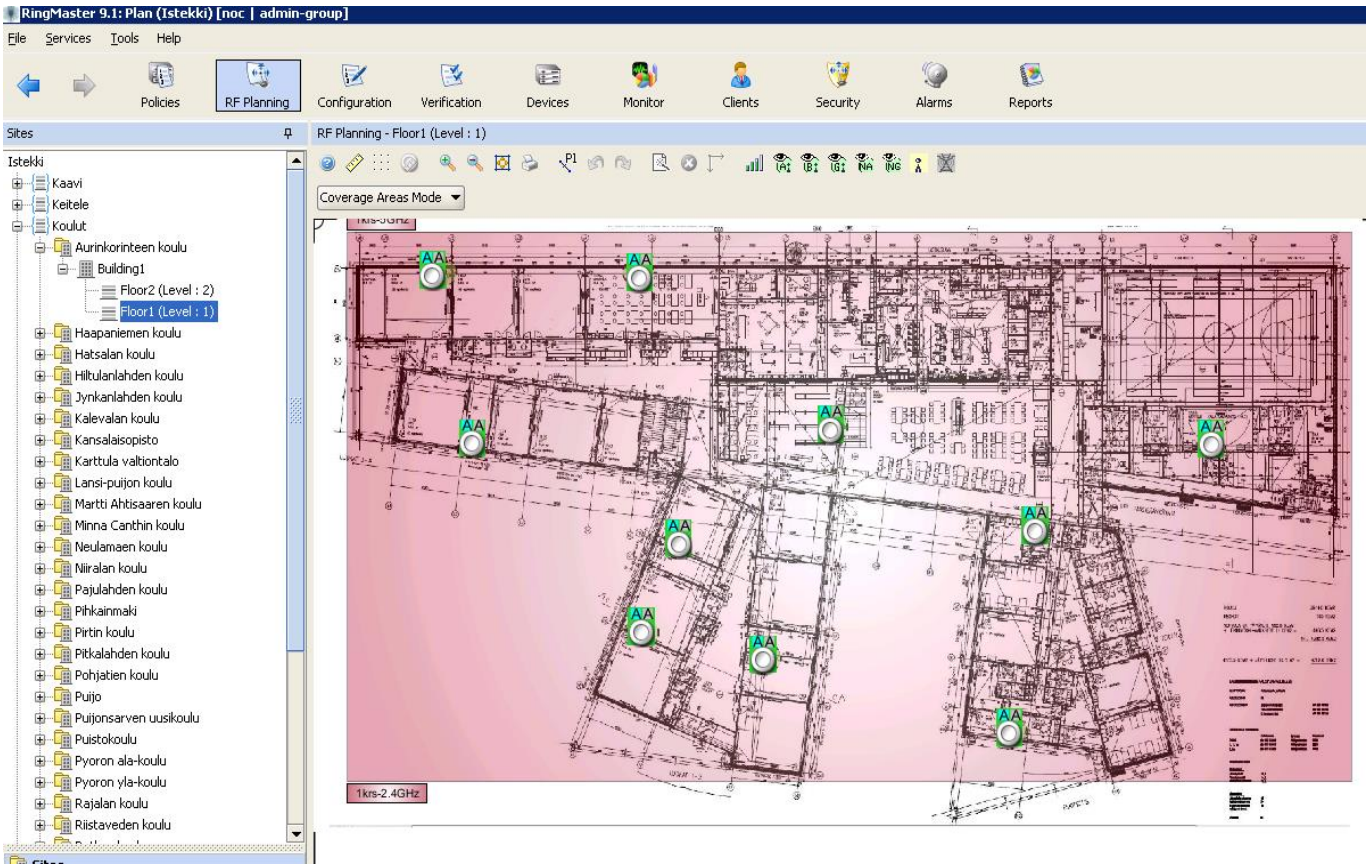
Verkonhallintatyökalujen tarkoitus on ylläpitää verkkoa ja löytää mahdollsia vikatilanteita. Lokikirjauksista saadaan tietoa sisäänkirjatumisyrityksistä, laitteiden uudelleenkäynnistyksistä ja tunnistustapahtumista. Lokikirjauksia varten on oltava aikapalvelin, jolla saadaan aikaleima tapahtumista. Tietoturvan kannalta on tärkeää tarkastella yhteyspisteiden MAC-osoitteita, ettei epävirallisia yhteyispisteitä pääse liittymään verkkoon. (Puska 2005, 231.)

Vikatilanteiden ennakointi on yksi tärkeimpiä WLAN-verkon parannustoimenpiteistä. Suunnitteluvaiheessa tehdyt ratkaisut ovat tärkeitä verkon toimivuuden kannalta, kuten verkkotopologia, luotettavat laitteet ja niiden toimintaympäristö. Ennakointiin kuuluu myös hyvä verkon dokumentointi, varalaitteet ja ylläpitohenkilökunnan työjärjestelyt. (Puska 2005, 233-234.)

SNMP-järjestelmillä (Simple Network Management Protocol) hoidetaan verkonhallintaa, johon useimmat verkonhallintatyökalut perustuvat. Järjestelmä toimii kiertokyselyllä, jos jokin asema ei vastaa kyselyn aikana niin järjestelmä merkkaa sen vikatilaan. SNMP-järjestelmä myös seuraa verkon tapahtumia kokonaisvaltaisesti, kuten verkon tilastoinnin. (Puska 2005, 236.)

5.2.1 Juniper Ringmaster

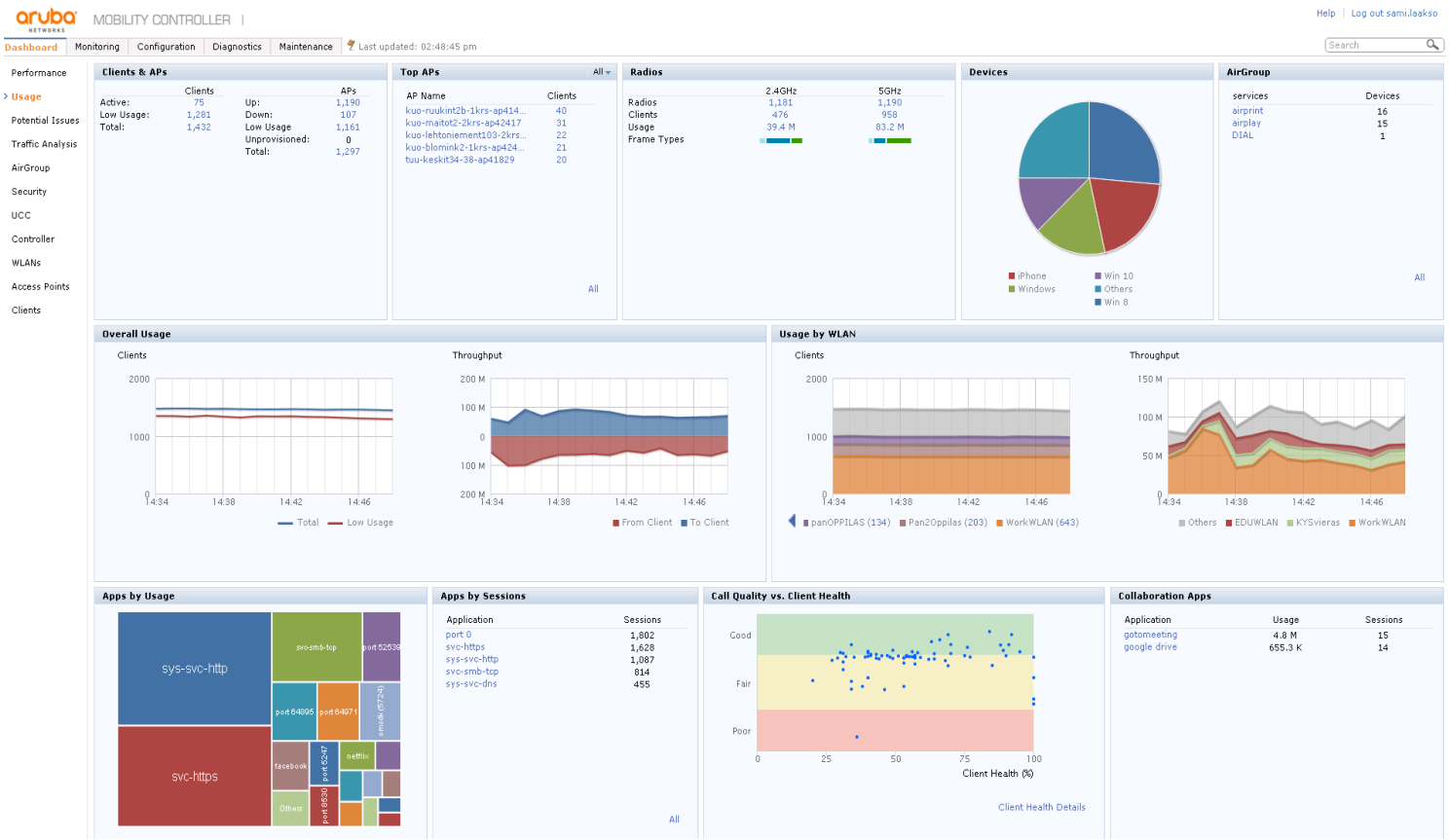
Juniper Ringmaster verkonhallintatyökalulla voidaan suunnitella, konfiguroida ja monitoroida langattomia verkkoja. Verkonhallintatyökalulla nähdään verkossa toimivien tukiasemien tilat ja mitkä laitteet ovat niihin liittyneet. Työkalulla on helppo paikantaa vikoja ja saada niistä kustomoituja raportteja. (Juniper 2017.)



KUVA 6. Juniper Ringmaster verkonhallintatyökalun käyttöliittymä. (Laakso 2017-10-01)

5.2.2 Aruba Airwave

Aruba Airwave verkonhallintatyökalulla voidaan selvittää verkkovikoja, monitoroida ja suunnitella langattomia verkkoja. VisualRF-työkalun avulla saadaan monipuolisesti tietoa verkon signaalin peittoalueesta. Verkonhallintatyökalua voidaan käyttää myös langallisen verkon hallintaan ja se tukee useita eri laitevalmistajia. (Arubanetworks 2017.)



KUVA 7. Aruba Airwave verkonhallintatyökalun käyttöliittymä. (Laakso 2017-10-01)

5.3 Uhkat

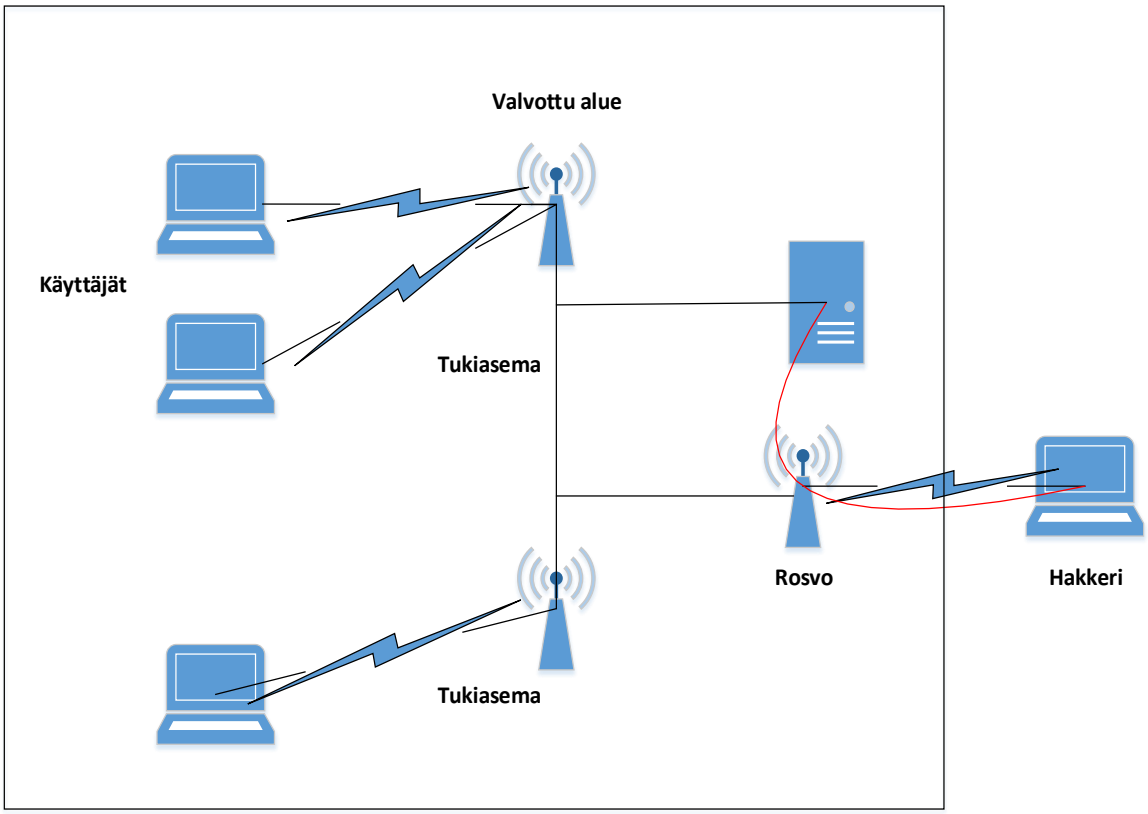
Langattomiin verkkoihin liittyy monenlaisia tietoturvauhkia. On elintärkeää tiedostaa verkkoihin kohdistuvista uhkista, koska hakkereiden päästäessä verkkoon ne voivat varastaa yrityksen tietoja tai rajoittaa/estää verkon toimintaa. Langattoman verkon tietoturvauhkat voidaan jakaa kolmeen alueeseen, jotka ovat passiivinen tarkkailu, luvaton pääsy ja palvelunestohyökkäys.

5.3.1 Liikenteen tarkkailu

Luvattomalla verkkoliikenteen tarkkailulla tarkoitetaan tilannetta, jossa hakkeri tarkkailee verkossa kulkevia datapaketteja hakkerointityökalulla. Hakkerointityökalulla voidaan selvittää datapakettien sisältöjä, joista voidaan saada selville esimerkiksi käyttäjätunnuksia, salasanoja ja luottokorttinumeroita. Hyvällä verkon salausmekanismilla voidaan estää hakkereiden nuuskinta ja se turvaa datan yksityisyyden.

5.3.2 Luvaton pääsy

Peräti 30% keskivertokaupungin langattomista verkoista on suojaamattomia. Niin sanotussa war driver -tekniikassa hakkeri kiertää autolla ja etsii suojaamattomia verkkoja. Kun tietoturva ei ole riittävällä tasolla voi hakkeri päästä yrityksen verkossa oleviin palvelimiin ja sovelluksiin kiinni. Rosvotukiasemalla tarkoitetaan avointa porttia verkon käyttöön. Rosvotukiasema voi olla hakkerin tai jopa työntekijän asentama tukiasema, jonka suojaus ei ole riittävällä tasolla. Sitä kautta verkon luvaton käyttö on hakkereille helppoa. Tämän vuoksi yrityksen tulisi tarkkailla jatkuvasti verkkoon liitettyjä laitteita.



KUVA 8. Verkkoon hyökkääminen rosvotukiaseman avulla. (Laakso 2017-09-30)

5.3.3 Palvelunestohyökkäys

Palvelunestolla (DoS) tarkoitetaan tilannetta, jossa hakkeri rajoittaa tai kaataa langattoman verkon toiminnan. Hyökkäys voidaan tehdä väsytyshyökkäyksenä, jolloin verkkoon tulvitetaan runsas määrä paketteja. Runsaan liikenteen vuoksi verkko lamaantuu, koska liikenne ylittää kaikki sen resurssit. Tämä voidaan toteuttaa, kun hakkeri pääsee yrityksen verkkoon liitetylle työasemalle lähettämään hyödyttömiä paketteja palvelimelle. Voimakkaita radiosignaaleita lähettämällä voidaan tukiasemista ja radiokorteista tehdä käyttökelvottomia. Tämä menetelmä on kuitenkin hakkerille melko riskialtis, koska lähettimen täytyy olla todella lähellä langatonta verkkoa. Palvelunestohyökkäyksiin on hyvä keino suojautua vahvalla tietoturvasuojalla, palomuurilla ja salauksella. Kaikista paras keino on kuitenkin kytkeä laite pois verkosta, kun sitä ei käytetä. Etenkin laitteet jotka sisältävät hyvin salaista tietoa. Palvelunestohyökkäyksen laajuus riippuu siitä, mitä verkolla ohjataan tai käytetään. Hyökkäys voi aiheuttaa yritykselle suuria taloudellisia tappioita. (Geier 2005, 171-177.)

6 EKAHAU SITE SURVEY

Ekahau Site Survey -ohjelmalla voidaan mitata verkon suorituskykyä, kattavuutta ja useita muita ominaisuuksia. Ohjelma tukee WLAN standardeja 802.11a/b/g/n/ac. Sillä voidaan selvittää langattoman verkon vikatilanteita ja tehdä lämpökarttoja verkon kantamasta. Mittauksia varten kannettavaan täytyy asentaa ulkoinen WLAN-adapteri Ekahau NIC-300-USB ja sisäinen verkkokortti end-to-end-mittausten suorittamiseen. Järjestelmävaatimuksina on Windows 10, 8.1, 8 tai Windows 7 käyttöjärjestelmä. Muistia minimissään 4GB RAM, suosituksena yli 8GB RAM ja suurempiin projekteihin suositellaan 16GB RAM. (Ekahau 2017.)

Mittausta varten tarvitaan aina kohteen pohjakuva. Pohjakuvaan valitaan oma sijainti, jonka jälkeen vedetään suora viiva seuraavaan päätepisteeseen. Käännöksiä tehdessä pitää aina pysähtyä ja vetää uusi viiva seuraavaan pisteeseen. Kävelyvauhdin tulee olla tasaista ja hidasta. Mittauslaitteisto kerää dataa jatkuvasti, vaikkei mittausreittejä olisikaan pohjakuvaan vedetty. Mittaukset suositellaan tekemään osissa. Esimerkiksi yksi tai kaksi huonetta kerrallaan. Mittauksen jälkeen ohjelmasta saa mittausraportin. Tuloksissa on erilaisia tietoja langattoman verkon kuuluvuudesta ja häiriötekijöistä. Tuloksia voidaan rajata ja valita ainoastaan tärkeimmät tiedot mittausraportille.
(Istekki wiki 2017.)

KUVA 9. Mittausreitit. (Ekahau raportti 2017.)

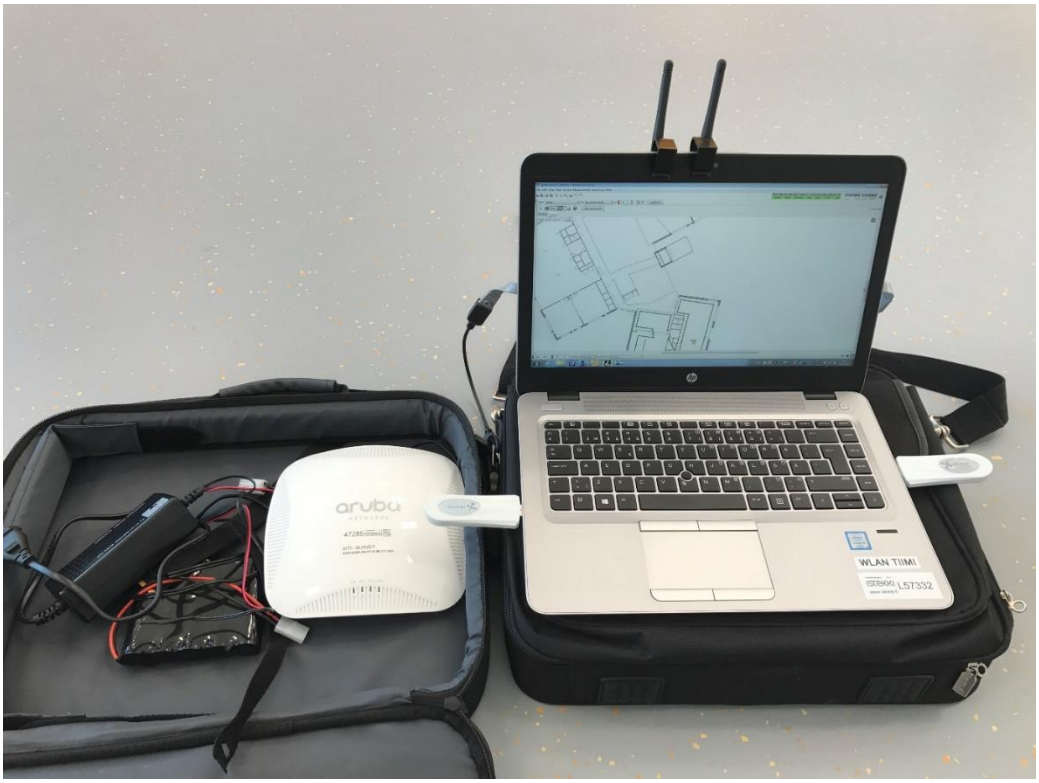
7 LANGATTOMAN VERKON MITTAUKSET

7.1 Jynkän koulun mittaukset

Kuopion Leväselle valmistui uusi koulu, jonne tarvittiin langaton verkko. Langatonta verkkoa käytetään tableteilla, puhelimilla ja kannettavilla tietokoneilla niin opettajat kuin oppilaatkin. Langattoman verkon tulisi täyttää sellaiset vaatimukset, että päätelaitteiden käyttö verkossa olisi nopeaa ja sujuvaa. Nykyään alakouluissakin opetusmateriaali siirtyy jatkuvasti enemmän verkkoon, jonka vuoksi verkon käyttäminen ei saisi rajoittua vain tiettyihin tiloihin rakennuksessa. Työnteon ei pitäisi katketa työskentelypaikkaa vaihdettaessa.

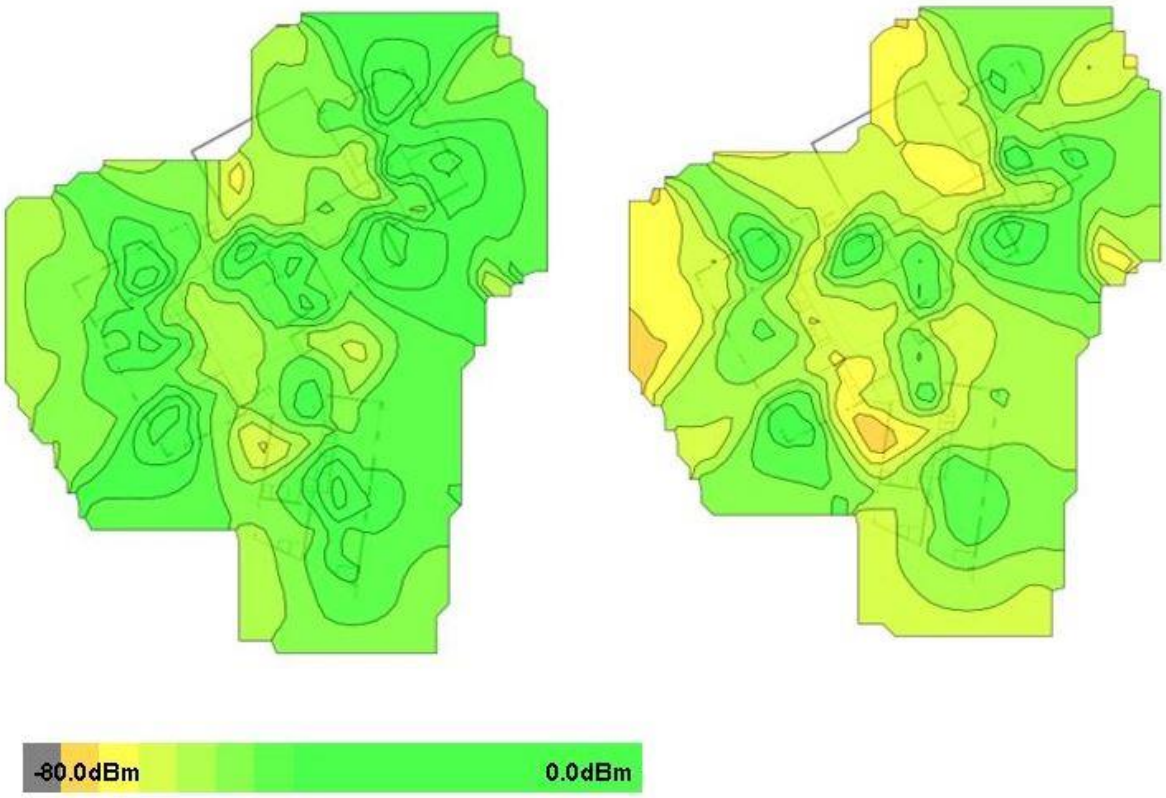
Jynkän koululle tukiasemien sijannit oltiin suunniteltu langattoman verkon oletettujen käyttöasteiden perusteella. Luokkahuoneiden alueelle oli luonnollisesti suunniteltu useampia tukiasemia lähistölle. Käytäville ja aulatiloihin oli suunniteltu yksittäisiä tukiasemia kattamaan alueen. Näissä tiloissa langattoman verkon kantama on parempi, koska esimerkiksi signaalia häiritseviä seiniä ja kalusteita on vähemmän.

Ennen tukiasemien asennusta paikoilleen, tehtiin vielä mittaus suunnitelluista tukiasemien sijoittelusta. Mittauslaitteistoon kuului mittauskannettava, johon asennettuna Ekahau Site Survey. Rakennuksen tarkka pohjakuva, jonka perusteella mittausdata saadaan oikealta alueelta. Mittauskannettavaan liitettiin kaksi USB-tikkua, joista toinen mittasi 2,4GHz ja toinen 5GHz taajuuksia. Yksi tukiasema, joka liitettiin telineeseen kiinni. Tukiasemalle oli määritelty IP ja SSID, johon liityttiin mittauskannettavalla. Tukiasemaan saatiin virta pienestä akusta.



KUVA 10. Mittauslaitteisto (Laakso 2017-08-20)

Mittaustuloksista keskeisin arvo on signaalin voimakkuus, joka on lähestulkoon kaikkialla 2,4GHz ja 5GHz taajuuksilla hyvä. Toinen keskeinen arvo on signaali-kohinasuhde, jolla saadaan todellinen tieto verkon käytännön toimivuudesta. Signaali-kohinasuhde vertaa signaalin voimakkuutta interferenssiin, jota koululla voi aiheuttaa esimerkiksi oppilaiden käyttämät bluetooth-laitteet. Päällekkäisistä kanavista saatava tieto on myös tärkeässä osassa. Liian lähekkäin olevat tukiasemat samalla kanavalla aiheuttavat häiriötä keskenään.



KUVA 11. Signaalin voimakkuus (Signal Strength). Vasemmalla 5GHz ja oikealla 2,4GHz taajuus. (Laakso 2017-09-30)

Signaalin voimakkuus (Signal Strength) on yksi perinteisimmistä vaatimuksista langattomalle verkolle. Huono signaali aiheuttaa epäluotettavaa yhteyttä ja hidasta suoritustehoa. Säteilyn teho esitetään yleensä desibelimilliwateissa (dBm). Signaalin voimakkuudet saadaa raportille 2,4Ghz ja 5,0Ghz taajuuksilla. (Puska 2015, 51.)

Signaali-kohinasuhteella (Signal To Noise Ratio, SNR) kerrotaan, kuinka paljon voimakkaampi signaalin voimakkuus on verrattuna kohinaan (interferenssiin). SNR tulee olla suurempi kuin nolla tai datansiirto ei ole mahdollista ja huono SNR aiheuttaa katkoksia yhteydessä. SNR-arvot määritetään dB (desibeli) yksiköllä, jossa raja-arvoina pidetään huonona 5.0dB ja 40dB suurempaa tai yhtä suurta erinomaisena.

KUVA 12. Päällekäiset kanavat (Channel Overlap). Vasemmalla 5GHz ja oikealla 2,4GHz taajuus. (Laakso 2017-09-30)

Päällekkäiset kanavat (Channel Overlapping) aiheuttavat häiriötä ja hidastavat tai katkovat yhteyksiä. Mittari näyttää useiden päällekkäisten kanavien alueet harmaina ja ongelmattomat alueet vihreänä. Tiheään asennettujen tukiasemien lähetystehoa voidaan pienentää, jonka avulla kanavien törmäysalueita saadaan pienennettyä.

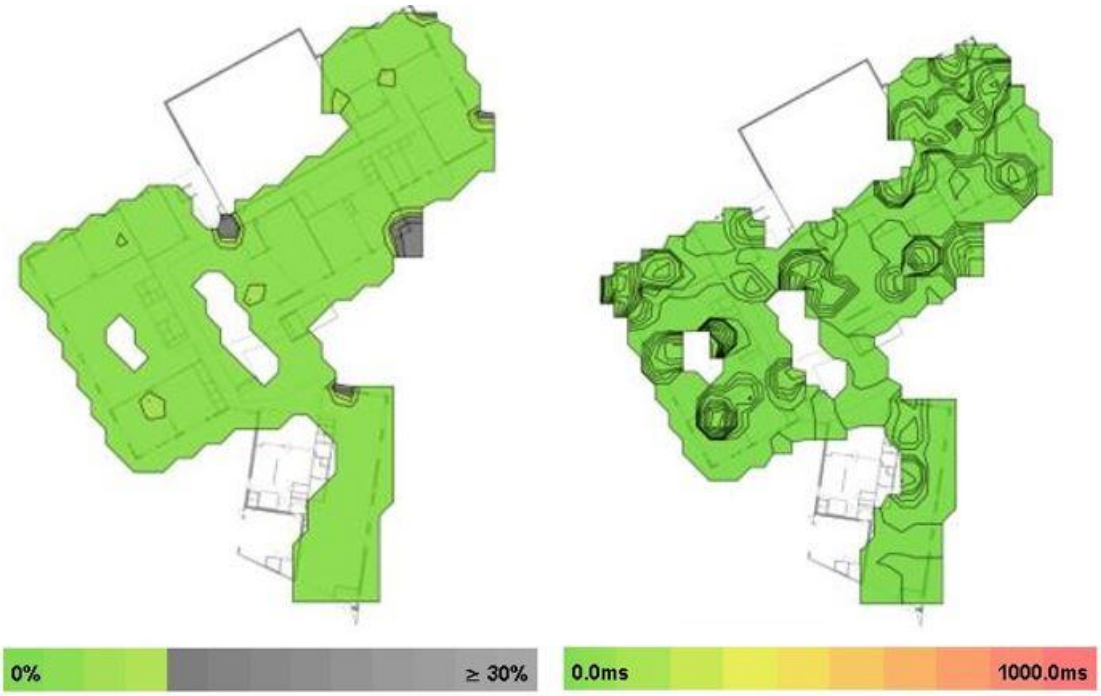
Tukiasemien määrää (Number of APs) voidaan tutkailla paikoittain ja nähdä samalla millä alueella tukiasemia on eniten. Tukiasemien määrää on merkitty väriastekoilla.

Datanopeus (Data Rate) esittää nopeimman mahdollisen lähetysnopeuden, jota langattoman verkon laitteet voivat käyttää. Tavallisesti todellinen lähetysnopeus on joko puolet tästä tai vähemmän. Mittausyksikkönä käytetään megabittiä sekunnissa (Mb/s).

KUVA 13. Tukiasemien määrä (Number of APs) ja datanopeus (Data Rate). (Laakso 2017-09-30)

Suoritusteho (Throughput) esittää enemmän todellista lähetysnopeutta, jolla verkko pystyy onnistuneesti lähettämään dataa vastaanottajalle. Mittausyksikkö on sama kuin datanopeudessa, mutta arvot ovat pienempiä.

Päätelaitteeseen liittyneet tukiasemat (Associated Access Point) näyttää moneenko tukiasemaan päätelaitteella on saatu yhteys mittauksen aikana. Lisäksi se taulukoi kaikkien tukiasemien tiedot.



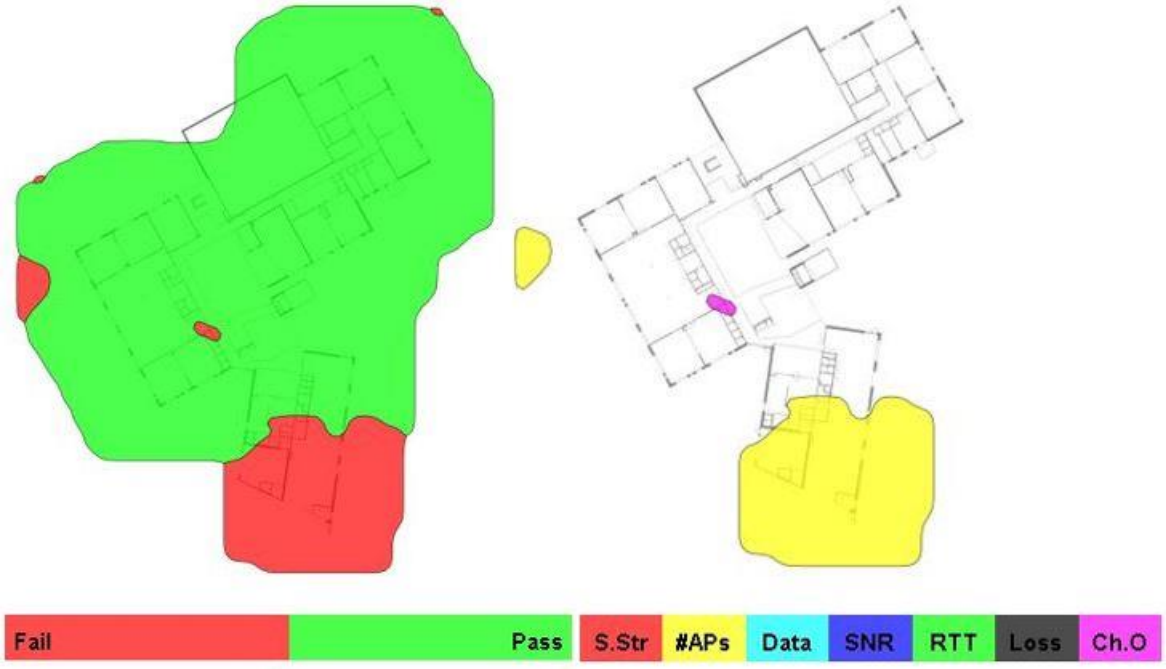
KUVA 14. (Packet Loss) vasemmalla ja (Round-Trip Time) oikealla. (Laakso 2017-10-22)

Datapakettien lähetyskatkoilla (Packet Loss) esitetään moniko lähetetty datapaketti ei mennyt perille. Raportilla tätä esitetään prosentuaalisesti väriasteikoilla vihreästä punaiseen.

Lähetyksen vastausajalla (Round-Trip Time) esitetään aikaa, jolloin paketti on lähetetty tiettyyn kohteeseen ja milloin sen vastaus saapunut takaisin lähettäjälle. Mittausyksikkönä on millisekunnit (ms), jonka astekoilla 0.0ms on hyvä ja 1000.0ms on heikko.

Spektrin hyödyntäminen (Spectrum Utilization, Spectrum Channel Power) kertovat miten voimakkaasti langaton verkko tai muut radiotaajuuksia käyttävät laitteet käyttävät tiettyä kanavaa alueella. Tehon näkee väriastekoilla vihreästä punaiseen.

Spectrum Channel Power näyttää miten voimakkaasti muutkin kuin langattoman lähiverkon laitteet käyttävät samaa taajuusaluetta. Yleensä taajuusalueen käyttö tulee langattomasta verkosta, mutta muita samalla taajuudella toimiva laitteita voivat olla esimerkiksi Bluetooth-laitteet, A/V tekniikka, tutka, sähkömoottorit ja valaistus. Vihreällä näkyvä alue kertoo, että alueella on myös muita samaa taajuutta käyttäviä laitteita. Silloin olisi suositeltua välttää käytettyjä kanavia minimoidakseen langattoman verkon interferessi.



KUVA 15. Verkon kunto (Network Health) ja verkon ongelmat (Network Issues) 2,4GHz taajuudella. Laakso (2017-10-01)

Verkon kunto kohdasta (Network Health) voi katsoa vastaako mittaustulokset määritettyjä verkon vaatimuksia. Vihreät ovat läpäisseet ja punaiset kohdat eivät (Fail/Pass) .

Verkon ongelmat (Network Issues) kohdasta näkee eriteltynä, mikä ongelma aiheutti verkon vaatimusten hylkäämisen sijainneissa. Värikoodeilla on merkitty mistä ongelma on johtunut.

Coverage Requirement: **High Speed, High Usage**	Signal Strength Min	**-75.0 dBm**
	Signal-to-noise Ratio Min	**10.0 dB**
	Data rate Min	**11 Mbps**
	Number of Access Points Min	**2 at min. -80.0 dBm**
	Channel Overlap Max	**3 at min. -80.0 dBm**
	Round Trip Time (RTT) Max	**300ms**
	Packet Loss Max	**5.0 %**

KUVA 16. Mittaukselle asetetut verkon vaatimukset. (Laakso 2017-10-01)

Verkon kapasiteetin kunto (Capacity Health) kohdasta näkee täyttääkö langaton verkko kapasiteettivaatimukset. Vihreänä näkyvä alue kertoo, että langaton verkko pystyy tukemaan päätelaitteiden toimintaa alueella. Kapasiteetin vaatimukset voidaan itse muokata vastaamaan oletettua verkon käyttöastetta.

Päätelaitteiden määrä tukiasemaa kohden (Capacity: Clients per AP) näyttää väriastekoilla vihreästä punaiseen, missä alueella on eniten kuormitusta yhdelle tukiasemalle tai tukiasemille.

Kanavan kaistanleveys (Channel Bandwidth) kertoo korkeimman mahdollisen kaistanleveyden jokaisella alueella. Kanavan kaistanleveydet ilmoitetaan megahertseinä (MHz).

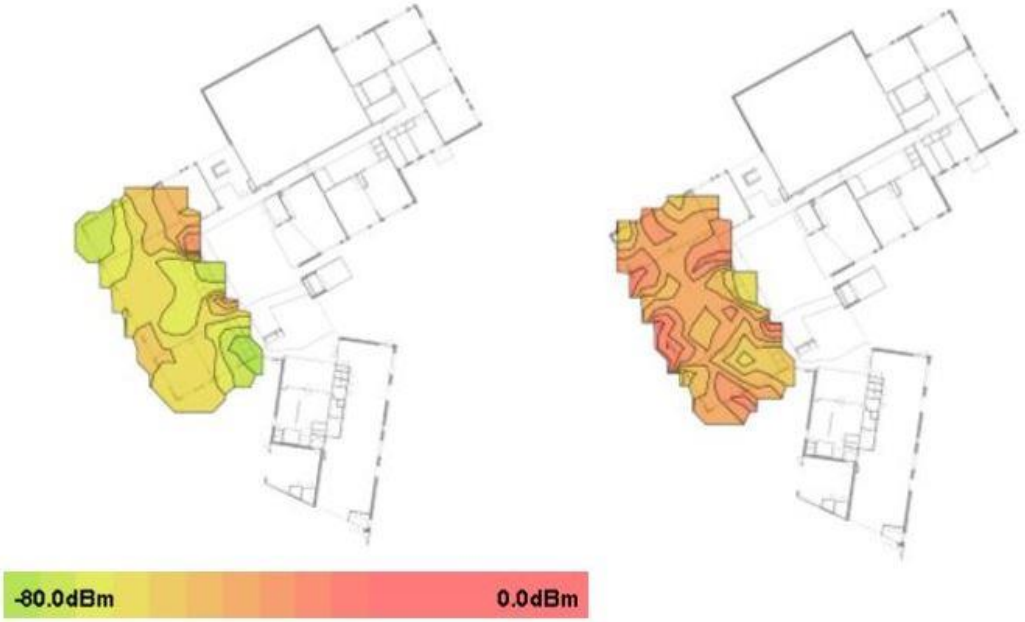
7.2 Häiriömittaukset

Jynkän koululla tehtiin häiriömittaus Ekahaun Site Survey -ohjelmalla. Häiriömittauksella haluttiin selvittää verkon hitauteen ja pätkimiseen vaikuttavia syitä. Mittaukset suoritettiin kahdessa osassa ja ne otettiin alueelta, jossa niitä oli enimmäkseen havaittu. Ensimmäinen mittaus suoritettiin tukiasemat päällä, jolloin nähtiin miten häiriöt vaikuttavat verkkoon. Seuraavaksi tukiasemat sammutettiin ja etsittiin häiriönaiheuttajaa.

KUVA 17. Signaali-kohinasuhde (Signal To Noise Ratio) Jynkän koulun 1.krs 2,4GHz taajuudella. (Laakso 2017-10-22)

KUVA 18. Signaali-kohinasuhde (Signal To Noise Ratio) Jynkän koulun 2.krs 5GHz taajuudella.

Uudessa rakennuksessa seinien rakennusmateriaalit ovat hyvin eristäviä, joten signaali rajoittuu herkemmin. Jynkän koululla havaittiin myös muita radioaaltoja lähettäviä laitteitta, jotka antavat häiriötä langattoman verkon toimintaan. Niiden toimintaan ei kuitenkaan päästä vaikuttamaan. Tulevaisuudessa voitaisiin päästä käyttämään pelkästään 5GHz taajuutta, joka ei ole niin herkkä häiriöille. Kaikki koulun päätelaitteet eivät vielä tue sitä, jonka vuoksi käytetään myös 2,4GHz taajuutta.



KUVA 19. Spektrin hyödyntäminen (Spectrum Channel Power) Jynkän koululla 1.krs luokkatilassa, vasemmalla 2,4GHz ja oikealla 5GHz taajuudella.

Jynkän koululla on automaattivalaistukset luokissa, jotka aiheuttavat hetkellisiä piikkejä kanavan käytössä luokkaan kävellessä. Käytävillä myös huomattiin mobiiliverkon yhteyden vahvistimia, joiden lähettämä signaali on samalla taajuudella kuin langattoman lähiverkon. Mittauskoneen vietyä lähellä vahvistinta antoi se huomattavaa häiriötä. Häiriönaiheuttajia seurataan vielä koululle asennettujen spektritukiasemien avulla, joilla saadaan kerättyä dataa verkon käytöstä. Langattoman verkon toimintahäiriöt voivat myös johtua käyttäjien päätelaitteista, jolloin laitteen verkkokortti ei vastaa kaikki vaatimuksia verkon optimaaliselle hyödyntämiselle.

8 YHTEENVETO

Opinnäytetyön tavoitteena oli suorittaa kuuluvuus- ja häiriömittauksia Jynkän koulun langattomaan verkkoon. Työ oli todella mielenkiintoinen ja opettavainen. Mittausten ohessa pääsi tutustumaan langattoman verkon suunnitteluun, hallintaan ja monitorointiin. Kontrollereiden toiminnasta ei ollut aiemmin tietoa, mutta tämän työn avulla pääsi näkemään, kuinka tehokkaasti ja helposti tukiasemia voidaan hallita. Kontrolleiden toiminta nopeuttaa esimerkiksi tukiasemien käyttöönottoa, tukiasemien kanavasuunnittelua ja verkkoryhmien lisäämistä tukiasema kohtaisesta.

Langattoman verkon tekniikan opiskelu oli todella mielenkiintoista. Opinnäytetyötä kirjoittaessa ja tutustuessa lähteisiin sai hyvän käsityksen langattomien verkkojen toiminnasta. Tietoturvaan ja häiriötekijöihin tutusminen oli avartavaa, koska etenkään erilaisista häiriölähteistä ei ollut niin tarkkaa käsitystä.

Mittauksissa käytetty Ekahaun site survey -ohjelmisto toimi moitteettomasti ja sillä saatiin luotettavia tuloksia. Ohjelmiston käyttäminen alko tulla hiljalleen tutummaksi ja uusia ominaisuuksia löytyi jatkuvasti. Mittaustuloksista saa todella kattavaa tietoa ja tulokset on esitetty hyvin selkeästi.

Tehtyjen mittausten avulla tukiasemien sijoitussuunnitelmat voitiin toteuttaa ja asentaa tukiasemat. Langaton verkko ehdittiin toteuttaa määräaikaan mennessä ennen koulujen alkamista. Koulun joissain luokissa havaitut häiriötekijät ovat vielä selvityksessä ja niihin etsitään ratkaisua.

9 LÄHTEET

LÄHTEET JA TUOTETUT AINEISTOT

GEIER Jim 2005. Langattomat verkot. Helsinki: Edita.

HAKALA, M ja VAINIO, M 2005. Tietoverkon rakentaminen. Porvoo: Docendo.

JUNIPER 2017. WLA522. [Viitattu 2017-5-14.] Saatavissa: http://www.juniper.net/sites/us/en/products-services/wireless/wla-series/wla522/index.page

PUSKA Matti 2005. Langattomat lähiverkot. Helsinki: Talentum.

CISCOPRESS 2017. Cisco Network Security Fundamentals: Wireless Security. [Viitattu 2017-05-22.] Saatavissa: http://www.ciscopress.com/articles/article.asp?p=360065&seqNum=4

HAKALA, M. VAINIO, M JA VUORINEN, O 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo.

CISCO 2017. Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide. [Viitattu 2017-05-25.] Saatavissa: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd/CCVP_BK_R7805F20_00_rtowlan-srnd_chapter_0100.html

JUNIPER 2017. RingMaster Software. [Viitattu 2017-06-03.] Saatavissa: http://www.juniper.net/sites/uk/en/products-services/wireless/ringmaster/index.page

ARUBANETWORKS 2017. Aruba AirWave network management. [Viitattu 2017-06-03.] Saatavissa: http://www.arubanetworks.com/products/networking/management/airwave/

EKAHAU 2017. Documentation – Ekahau Site Survey. [Viitattu 2017-06-03.] Saatavissa: https://support.ekahau.com/hc/en-us/categories/115000762008-Documentation-Ekahau-Site-Survey

CISCOPRESS 2015. Wireless LAN Implication, Problems, and Solutions. [Viitattu 2017-06-26.] Saatavissa: http://www.ciscopress.com/articles/article.asp?p=2351131&seqNum=2

Hovatta, T 2005. WLAN-tekniikat ja -käyttösovellukset toimitilakiinteistössä. Espoo: Sähköinfo Oy.