TAMPEREEN
AMMATTIKORKEAKOULU

TUTKINTOTYÖRAPORTTI

LANGATTOMAN LÄHIVERKON SUUNNITTELU POLIISIKOULUN OPISKELIJA-ASUNTOLAAN

Marko Kauppinen

Tietojenkäsittelyn koulutusohjelma
joulukuu 2005
Työn ohjaaja: Rami Lehtinen

TAMPERE 2005

Tampereen
ammattikorkeakoulu

Tekijä Marko Kauppinen

Koulutusohjelma Tietojenkäsittely

Tutkintotyön nimi Langattoman lähiverkon suunnittelu Poliisikoulun opiskelija-asuntolaan

Työn valmistumis-kuukausi ja -vuosi Joulukuu 2005

Työn ohjaaja Rami Lehtinen **Sivumäärä:** 68

TIIVISTELMÄ

Lisätäkseen opiskelijoiden mielenkiintoa oppilaitosta kohtaan Poliisikoulun tietohallinto on suunnitellut langattoman lähiverkon toteuttamista Poliisikoulun opiskelija-asuntolaan. Verkon tarkoituksena on tarjota opiskelijoille langattomat yhteydet Internetiin niin opiskeluun liittyvässä tiedonhaussa kuin vapaa-ajan käytössäkin.

Tämän opinnäytetyön tarkoituksena oli suunnitella langaton lähiverkko Poliisikoulun opiskelija-asuntolaan. Lisäksi on tarkoitus tuottaa kirjallinen selvitys langattoman lähiverkon toteuttamisesta koulun tietohallinnon käyttöön.

Opinnäytetyön lopputuloksena saatiin tieto tukiasemien paikoista ja määristä. Lisäksi tutkittiin eri kanavien vaikutusta tukiaseman signaalin kuuluvuuteen. Opinnäytetyön tuloksena saatiin myös kerättyä tausta- ja teoriatietoa langattomasta lähiverkosta myöhempää käyttöä varten.

Opinnäytetyö on sellaisenaan hyödynnettävissä rakennettaessa langatonta lähiverkkoa Poliisikoulun opiskelija-asuntoloihin. Työssä otetaan kantaa tukiasemien lopulliseen määrään, sijoituspaikkoihin ja niissä käytettäviin kanaviin. Työtä voidaan käyttää pohjana suunniteltaessa lopullista verkon toteutusta. Työtä voidaan hyödyntää myös verkon suunnitteluvaiheessa, sillä se tarjoaa koottua tausta- ja teoriatietoa langattomista lähiverkoista ja niihin liittyvistä käsitteistä.

Opinnäytetyön alussa on johdanto. Opinnäytetyön toisessa osassa selvitetään työhön liittyvää taustaa ja toimintatapoja sekä välineitä. Sen jälkeen käydään läpi langattoman lähiverkon standardit mukaan lukien uusimmat standardit. Neljännessä osassa selvitetään langattomiin lähiverkkoihin liittyvät teoriat. Tässä kohden perehdytään muun muassa signaaliin ja sen laadun vaihteluihin eri tiedonsiirtonopeuksilla. Langattomiin lähiverkkoihin liittyvää tietoturvaa käsitellään viidennessä luvussa, jossa esitellään salausprotokollien lisäksi autentikontimenetelmät ja muuta tietoturvaan liittyvää. Kuudennessa osassa kerrotaan kuuluvuusmittauksista ja niiden toteutuksista opiskelija-asuntolataloissa. Kuuluvuusmittausten tulokset ja niiden avulla selvitetyt tukiasemien paikat ja kanavat esitellään luvussa seitsemän. Arviointiosassa kahdeksannessa luvussa otetaan kantaa verkon toteuttamiseen ja hallintaan. Johtopäätökset on esitetty yhdeksännessä luvussa. Lähteet ja luettelot muodostavat kymmenennen ja viimeisen luvun.

Avainsanat WLAN 802.11 langaton lähiverkko tietoturva autentikointi

Tampere
Polytechnic

Author	Marko Kauppinen
Degree Programme	Business Information Systems
Title	Planning a Wireless Local Area Network for the students' residential accommodation at the National Police School of Finland
Month and year	December 2005
Supervisor	Rami Lehtinen

Pages: 68

ABSTRACT

In order to enhance the interest of prospective students for the National Police School of Finland itself the data administration of the school has planned wireless local area network for the students' residential accommodation at the National Police School of Finland. The purpose of this WLAN is to provide wireless Internet connections for students to be used in study and in recreational use.

The purpose of this final thesis was two folded. One aim was to produce a plan in order to construct a wireless local area network for the students' residential accommodation at the National Police School of Finland. The second aim was to produce a written source of information regarding implementation of WLAN to the National Police School of Finland.

As the result of this final thesis two things were accomplished. First of all, the placement of access points as well as the required amount of them was found out. Secondly, theory and background information concerning implementation of WLAN was gathered for later use.

This final thesis can be used as such when building WLAN for the students' residential accommodation. It helps to determine the required number and placement of access points. Also information regarding the use of channels in access points can be found in this final thesis. This final thesis can be used as a baseline when planning final implementation of WLAN because it offers wide information source with relation to WLAN's.

The second part of the final thesis covers background, methods, and tools with relation to work which has been done. In the third part can be found the latest information concerning WLAN standards. The fourth part deals with WLAN theory e.g. signal strength and its effect to data transmission speed. Data security is the main issue in the fifth part which presents for instance data encryption protocols and user authentication methods. The sixth part deals with the signal strength measurements and how they were done during this work. Results of the signal strength measurements are presented in the seventh part including the placement of access points. How to proceed in the future with this WLAN is dealt with in the eighth part. Conclusion is presented in the ninth part. Source material and list of figures, graphics, and tables can be found in the tenth and last part.

Keywords WLAN 802.11 wireless network data security authentication

Sisällysluettelo

1 Johdanto

Suoritin opintoihini liittyvän työharjoittelun Poliisikoulun tietohallinnossa 14.2.–15.7.2005 välisenä aikana. Työharjoitteluni aikana ilmeni, että Poliisikoululla on kiinnostusta langattoman lähiverkon toteuttamiseksi Poliisikoulun opiskelija-asuntoloihin. Sovimme tietohallinnon esimiehen kanssa, että tekisin opinnäytetyöni kyseisestä aiheesta.

Rajasimme aiheen koskemaan langattoman lähiverkon suunnittelua opiskelija-asuntoloihin. Suunnittelu käsitti alustavat kuuluvuusmittaukset, joissa tutkittaisiin mm. tukiasemien paikkoja ja eri kanavien vaikutusta kuuluvuuteen. Myös toteuttamisesta oli alustavasti puhetta, mutta se päätettiin lopulta rajata opinnäytetyöni ulkopuolelle. Lisäksi tavoitteena oli tausta- ja teoriatiedon kerääminen Poliisikoulun tietohallinnon käyttöön mahdollisen myöhemmän toteutuksen tueksi.

Kuuluvuusmittaukset suoritettiin C- ja D-taloissa, sillä ne molemmat edustavat kumpaakin opiskelija-asuntolatyyppiä, joita Poliisikoulun alueella on. Lisäksi yksi kerros C-talosta on varattu henkilökunnan työtiloiksi, joten kuuluvuusmittaukset olisi helpompi tehdä sieltä käsin. Työpisteeni siirtyi ennen kuuluvuusmittausten aloittamista päätalosta C-taloon tehtäväni helpottamiseksi. D-talo valittiin kuuluvuusmittausten kohdetaloksi siksi, että se olisi tyhjänä mittausten ajankohtana heinäkuussa 2005.

Tämän opinnäytetyön tavoitteena oli langattoman lähiverkon suunnittelu Poliisikoulun opiskelija-asuntoloihin sekä tausta- ja teoriatiedon kerääminen langattomista lähiverkoista.

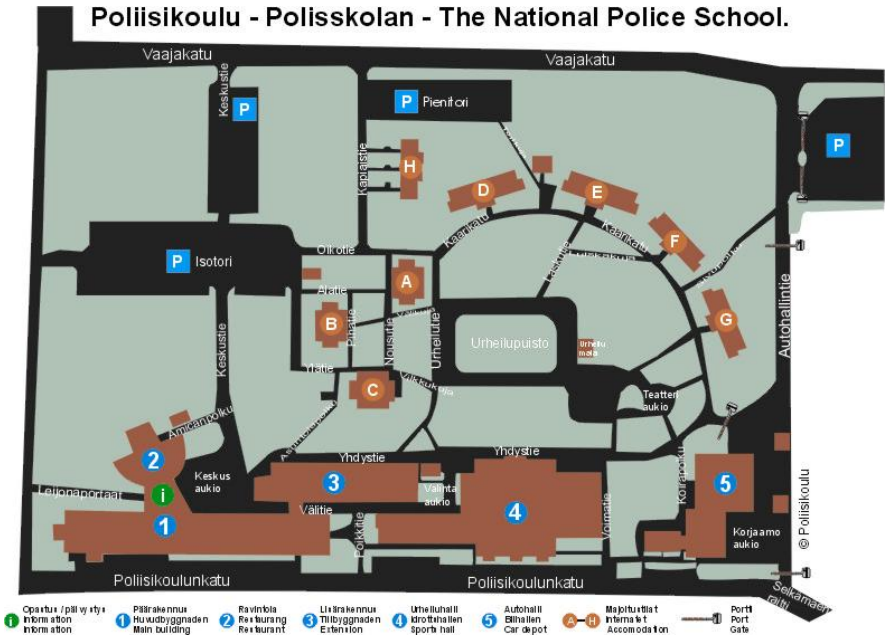
2 Taustat

2.1 Poliisikoulu

Poliisikoulu on toiminut vuodesta 1993 Tampereen Hervannassa. Poliisikoulu vastaa opiskelijoiden rekrytoinnista, opiskelijavalinnoista, poliisin perustutkinto- ja alipäällystökoulutuksesta sekä toimialaansa liittyvästä ammatillisesta erikoistumiskoulutuksesta. Poliisin perustutkinnon suorittaminen kestää kaksi ja puoli vuotta ja koulutukseen kuuluu lähiopintoja ja itseopiskelua. Osa opinnoista suoritetaan poliisin eri yksiköissä tai poliisilaitoksissa. Opiskelijat ovat työharjoittelussa ja kenttätyöjaksolla yhteensä noin vuoden ajan.

Poliisikoulussa opiskelee lähiopintojaksoilla 400 - 500 opiskelijaa. Määrä vaihtelee lähiopetuksessa olevien kurssien ja opintojen vaiheen mukaan. Vuonna 2004 Poliisikoulusta valmistui 362 uutta poliisia seitsemältä suomenkieliseltä ja yhdeltä ruotsinkieliseltä kurssilta. Vuonna 2005 perustutkintokoulutuksen aloituspaikkoja on 408. Syyslukukauden alkaessa 19.8.2005 opiskelijoita Poliisikoulussa oli 909, joista lähiopetuksessa 465 opiskelijaa.

Poliisikoulun alue, jonka yleiskuva on esitetty kuvassa 1, on kokonaisalaltaan noin 21 hehtaaria. Luokka- ja työhuonetilojen lisäksi alueella on opiskelija-asuntolat, ajoharjoittelurata, ajoneuvokoulutustilat, harjoitustalo ja kaksi ampumarataa. Liikuntatiloissa on kuntosali, uimahalli, painisali sekä liikunta- ja palloilusali.



Kuva 1 Yleiskuva Poliisikoulun alueesta

2.1.1 Poliisikoulun kiinnostus langattomaan lähiverkkoon

Lisätäkseen kilpailukykyään opiskelijoiden rekrytointimarkkinoilla Poliisikoulu on kiinnostunut Internet-yhteyksien tarjoamisesta opiskelijoilleen opiskelija-asuntoloissa. Tällä hetkellä opiskelijoilla on mahdollisuus Internetin käyttöön poliisin verkon kautta ainoastaan päätalon luokissa, kirjastossa ja ryhmätyötiloissa. Internetin käyttöä on rajoitettu Sisäministeriön Internet-politiikalla ja esimerkiksi webmail-pohjaiset sähköpostiohjelmat eivät ole käytettävissä koulun koneilta. Näihin voi päästä käsiksi muutamasta poliisin verkosta erillään olevasta Internet-pisteestä.

Opiskelija-asuntoloihin ei ole järkevää toteuttaa normaalia langallista lähiverkkoa. Sen toteuttaminen tulisi suhteellisen kalliiksi, siinä tarvittavien kaapelointitöiden vuoksi. Kaikkiin taloihin johtaa päärakennuksesta kuitukaapeli, joka on kaivettu maahan myöhemmässä vaiheessa. On syytä muistaa, että ensimmäiset kolme asuntolataloa on rakennettu vuonna 1978, jolloin tietokoneet olivat varsin tuntemattomia. Näin ollen langaton lähiverkko on ainoa toteuttamiskelpoinen ratkaisu lähiverkon toteuttamiseksi opiskelija-asuntoloihin.

2.1.2 Poliisikoulun vaatimukset langattoman lähiverkon suhteen

Opiskelija-asuntojen langattoman lähiverkon on täytettävä tietyt vaatimukset. Vaikkakaan verkosta ei ole yhteyttä viranomaisverkkoon, ainoastaan Internetiin, kiinnostaa se silti luvattomia käyttäjiä luonteensa vuoksi. Tärkein vaatimuksista kohdistuu tietoturvaan, sillä verkko ei saa olla luvattoman käyttäjän käytettävissä ja sen liikenne salakuunneltavissa. Näin ollen verkon hallinnassa tulee käyttää uusimpia käyttäjän tunnistusmetodeita ja liikenteen salausprotokollia. Myös laitetason tietoturva tulee ottaa huomioon verkkoa suunniteltaessa ja laitteet eivät saa olla fyysisesti saavutettavissa.

Toinen tärkeä seikka on palvelunlaadun ts. tasaisen yhteysnopeuden turvaaminen kaikille käyttäjille. Tietyt sovellukset, kuten vertaisverkko-ohjelmat (peer-to-peer, P2P), varaavat itselleen normaalia enemmän verkon resursseja ja näin hidastavat verkon toimintaa. Palvelun laatuun liittyy myös verkon käyttäjämäärä, joka voi kasvaa iltaisin suureksi ja näin hidastaa osaltaan verkkoa.

Vaatimuksia kohdistuu myös verkon hallintaan ja käytettävyyteen. Verkon hallinnan tulee olla mahdollisimman yksinkertaista, eikä se saa sitoa liikaa tietohallinnon resursseja. Käyttäjätunnusten ja salasanojen luomisen ja jaon pitää olla mahdollisimman pitkälle automatisoituja. Toisaalta opiskelijoiden kierto lähiopetuksen ja kenttätyöjaksojen välillä asettaa omia erityisvaatimuksia verkon hallinnalle. Käyttäjätunnuksen ja salasanan tulee olla voimassa vain opiskelijan lähiopetusjakson ajan.

Verkkoon liittymisen tulee olla mahdollisimman pitkälle automatisoitu, eikä sen tule vaatia opiskelijalta langattomien lähiverkkojen erityistuntemusta.

2.2 Opiskelijoiden kiinnostus Internet-yhteyttä kohtaan

Opiskelijoiden kiinnostus Internet-yhteyden saamiseksi selvitettiin opiskelijakyselyllä. Kysely kohdistettiin Internet-yhteyksiin yleisesti, sillä tässä vaiheessa ei haluttu vielä tuoda esiin langatonta lähiverkkoa. Kyselyyn vastattiin koulun verkkoympäristöön toteutetulla Paula Palaute-palautejärjestelmällä, jolla opiskelijoilta kerätään palautetta opetuksesta.

Kysely haluttiin pitää lyhyenä ja ytimekkäänä, jotta siihen vastaamista ei olisi koettu vaikeaksi ja aikaa vieväksi. Opiskelijoilta kysyttiin seitsemän aiheeseen liittyvää kysymystä ja lopuksi oli mahdollisuus antaa aiheeseen liittyvää vapaata palautetta. Kysymysten alla on niihin annetut vastausvaihtoehdot.

1) Asutko Poliisikoulun asuntolassa?
    - Kyllä, ei

2) Onko sinulla tietokone käytössäsi?
    - Kyllä, ei

3) Millainen käytössäsi oleva tietokone on?
    - Kannettava, pöytämalli

4) Millainen Internet-yhteys sinulla on käytössäsi?
    - Modeemi, ISDN,

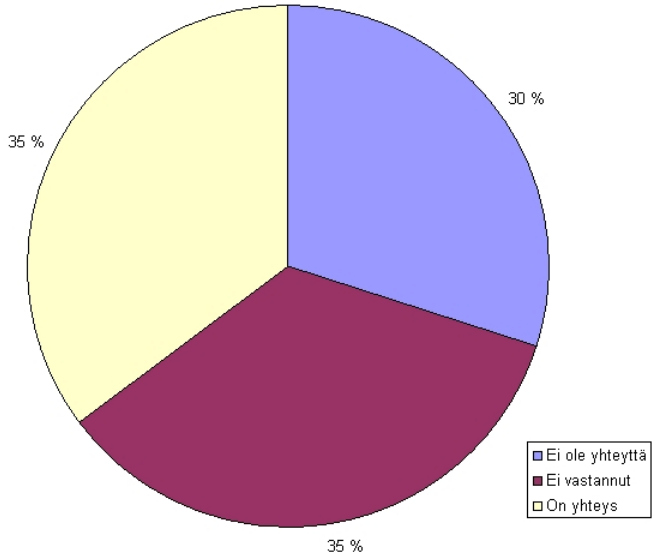
5) Onko koneessasi langattoman yhteyden mahdollistava (WLAN) verkkokortti?
    - Kyllä, ei, en tiedä

6) Oletko kiinnostunut henkilökohtaisesta ADSL-yhteydestä Poliisikoulun asuntolaan omaan huoneeseesi?
    - Kyllä, ei

7) Paljonko olisit valmis maksamaan ADSL-yhteydestä enimmillään kuukaudessa?
    - 5, 10, 15, 20 euroa

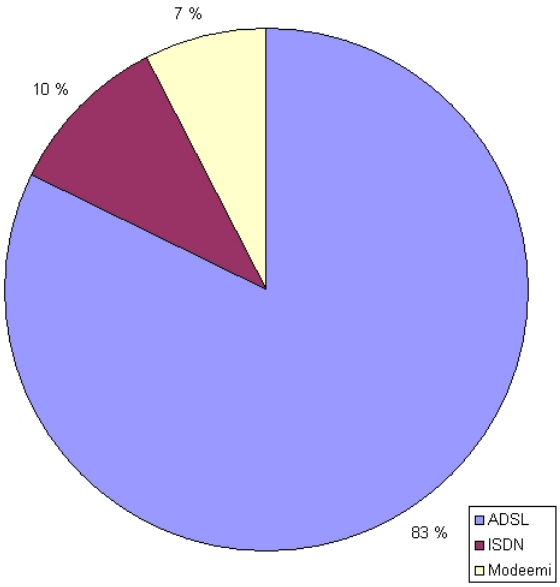
Opiskelijoita oli Poliisikoulussa opiskelijakyselyn aikana 935, joista paikalla oli 520. Työharjoittelussa tai kenttäjaksolla oli 414 opiskelijaa. Kyselyn aikana opiskelija-asuntoloihin oli majoittunut noin 500 opiskelijaa. Vastauksia kyselyyn saatiin kaikkiaan 190 kappaletta. Vastaajista 160 asui koulun opiskelija-asuntoloissa ja 30 asui muualla. 75 vastaajalla ei ollut tietokonetta käytössään, kun taas 115:sta vastaajalla oli.

Käytössä olevat tietokoneet jakautuivat siten, että kannettava tietokone oli 73 vastaajalla, pöytämallinen tietokone 43 vastaajalla. Kysymykseen jätti vastaamatta 74 vastaajaa, mikä on noin 39 % kyselyyn vastanneista.



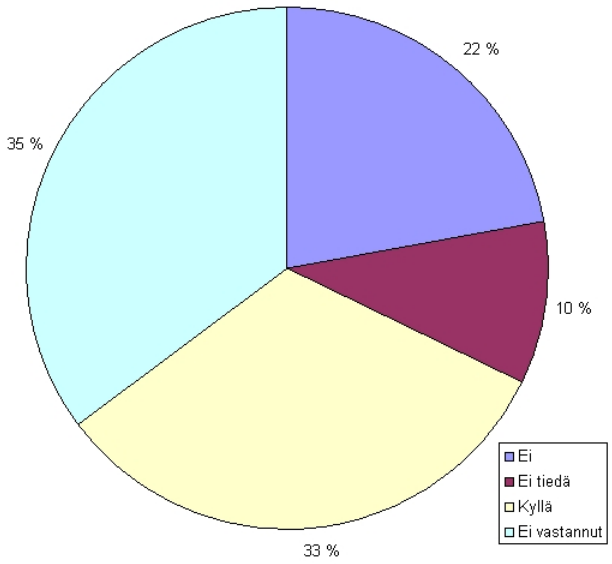
Kuvio 1 Internet-yhteys käytössä

Kuten kuviosta 1 ilmenee, vastaajista 67:llä oli jo käytössään Internet-yhteys, 57:llä ei ollut yhteyttä ja 66 vastaajaa ei vastannut kysymykseen.



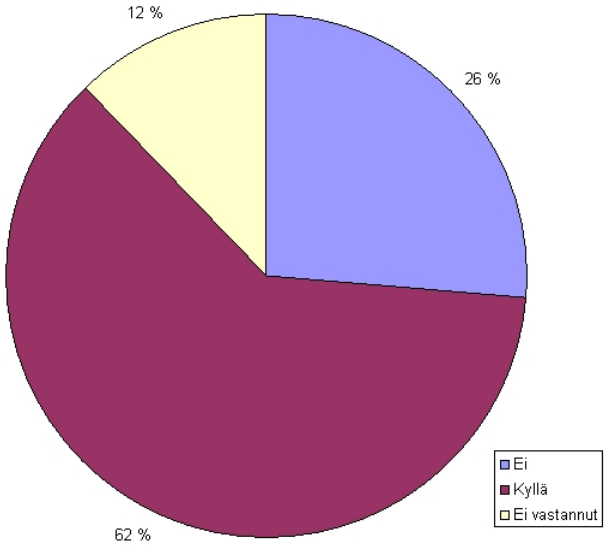
Kuvio 2 Käytössä olevan Internet-yhteyden tyyppi

Kuviosta 2 puolestaan ilmenee, että 83 % niistä, joilla oli jo Internet-yhteys käytössään, yhteys oli ADSL-yhteys. ISDN-yhteyksiä oli 10 % vastaajista ja modeemi yhteys oli 7 % vastaajista.



Kuvio 3 WLAN-kortti tietokoneessa

Vastaajista 62:lla (33 %) oli tietokoneessaan langattoman verkkoyhteyden mahdollistava verkkokortti. 42 (22 %) vastaajalla ei ollut ko. verkkokorttia koneessaan, kun puolestaan 19 (10 %) vastaajaa ei tiennyt onko hänen tietokoneessaan sellaista. Vastaajista 35 % eli 67 vastaajaa jätti vastaamatta kysymykseen. Kuviossa 3 on esitetty WLAN-korttien vastaajakohtainen tilanne.



Kuvio 4 ADSL-yhteydestä kiinnostuneet opiskelijat

Kuviossa 4 puolestaan selvitetään ADSL-yhteydestä kiinnostuneiden jakaumaa. Kyselyyn vastanneista 117 (62 %) vastaajaa oli kiinnostunut henkilökohtaisesta ADSL-yhteydestä asuntolaan omaan huoneeseensa. 50 (26 %) vastaajaa ei ollut kiinnostunut yhteydestä ja 23 (12 %) vastaajaa jätti vastaamatta kysymykseen.

Lopuksi kysyttiin vielä miten suurta kuukausimaksua vastaajat olisivat valmiita maksamaan Internet-yhteydestä. Taulukosta 1 selviää maksamishalukkuus suhteessa maksun suuruuteen. 29 % vastanneista jätti vastaamatta tähän kysymykseen.

Taulukko 1 Kuukausimaksun suuruus

Maksun suuruus (€)	**% vastanneista**
5	19
10	29
15	14
20	9

Kyselyssä ei eritelty miten opiskelijoiden käyttöön mahdollisesti tuleva Internet-yhteys olisi toteutettu, sillä kyselyä ei haluttu yksilöidä liikaa langattoman lähiverkon suuntaan. Syynä tähän oli se, että langattoman lähiverkon suunnittelu on vielä alkutekijöissään, eikä keskeneräisistä asioista haluttu tehdä sen suurempaa numeroa.

Kyselyn tuloksista voidaan päätellä, että suurin osa vastanneista (62 %) on halukas saamaan käyttöönsä Internet-yhteyden Poliisikoulun opiskelija-asuntolaan omaan henkilökohtaiseen käyttöönsä. Valmius langattoman lähiverkon käyttöön on 33 % vastaajista, joilla siis on tietokoneessaan

WLAN verkkokortti. 71 % vastaajista on valmis maksamaan yhteydestä. Opiskelijoilla on siis halukkuutta Internet-yhteyden saamiseksi Poliisikoulun opiskelija-asuntoloihin ja kolmasosalla vastanneista on jo valmius langattomaan lähiverkon käyttämiseksi.

2.3 Opiskelija-asuntolat

Lähiopintojaksojen aikana opiskelijat majoittuvat Poliisikoulun asuntoloissa Hervannassa. Opiskelija-asuntolataloja on alueella seitsemän, ja niissä on vuodepaikkoja yhteensä 776. Asuntolatalot on rakennettu kolmessa eri vaiheessa. Ensimmäisinä rakennettiin A-, B- ja C-talot vuonna 1978. Vuonna 1991 rakennettiin E- ja F-talot. Uusinta rakennuskantaa ovat D- ja G-talot, jotka on rakennettu vuonna 1999.

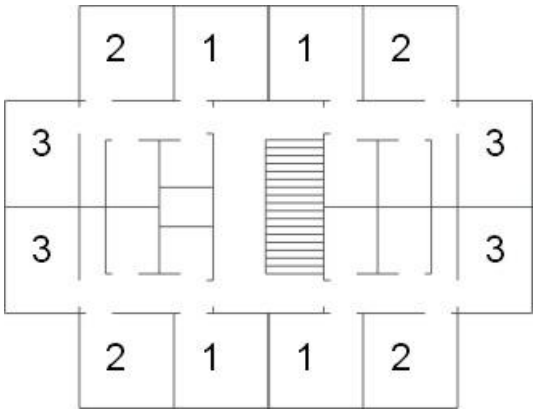
A, B ja C-talot ovat kuusikerroksisia ja kussakin kerroksessa on neljä asuntoa, joissa kaikissa on kolme huonetta. D-, E-, F- ja G-taloissa on viisi asuinkerrosta, joissa ensimmäisissä kerroksissa on yhdeksän asuntoa ja muissa kymmenen asuntoa. Kuvassa 2 etualalla näkyvät A-, B- ja C-talot ja vasemmalla ja taka-alalla D-, E-, F- ja G-talot.

Kuva 2 Yleiskuva Poliisikoulun opiskelija-asuntoloista

Tässä yhteydessä esitellään C- ja D-talot, sillä niissä toteutettiin myöhemmin tässä työssä esiteltävät kuuluvuusmittaukset. C-talo valittiin siksi, että siellä on myös henkilökunnan työtiloja. Näin ollen sinne oli vapaampi pääsy kuin A- tai B-taloon. D-talo valittiin puolestaan siksi, että se oli tyhjänä opiskelijoista kuuluvuusmittausten aikana.

2.3.1 C-talo

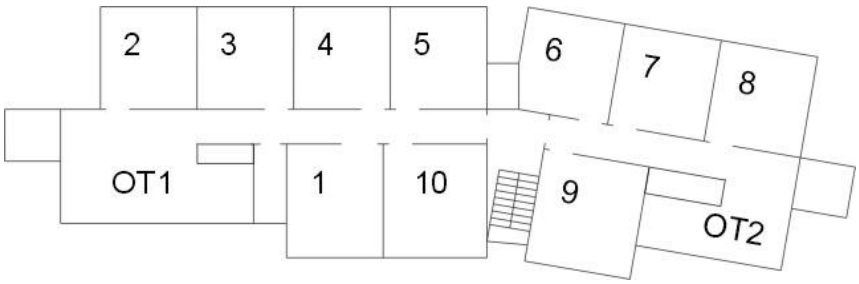
C-talo on vanhempaa rakennuskantaa ja on ensimmäisiä Hervantaan rakennettuja poliisiopiskelijoille tarkoitettuja taloja. C-talosta osa on varattu henkilökunnan työtiloiksi. Asunnoissa on kolme huonetta, joissa jokaisessa on kaksi vuodepaikkaa. Kuten kuvasta 3 käy ilmi, porraskäytävä sijaitsee keskellä taloa ja asunnot ovat sen ympärillä. Rapun ja asuntojen ulko-ovet on lukittu.



Kuva 3 A-, B- ja C-talon toisen kerroksen pohjaratkaisu

2.3.2 D-talo

D-talo on uudempaa rakennuskantaa kuin A-, B- ja C-talot. D-talo on pohjaratkaisultaan samanlainen kuin E-, F- ja G-talot. Porraskäytävä on keskellä taloa. Siitä johtaa ovet eteiskäytäviin, jonka varrelle asunnot on sijoitettu. Vasemmassa siivessä on kuusi asuntoa ja oikeassa siivessä neljä. Kuvassa 4 on kuvattu D-, E-, F- ja G-talojen toisen kerroksen pohjaratkaisut. Eteiskäytävien päissä ovat oleskelutilat. Talon ja asuntojen ulko-ovet on lukittu, mutta ei eteiskäytäviin johtavia ovia.



Kuva 4 D-, E-, F- ja G-talojen toisen kerroksen pohjaratkaisu

2.4 Toimintatavat ja välineet

Kuuluvuusmittauksissa käytetty langattoman lähiverkon tukiasema oli ZyXEL Prestige 660H-61 palomuuri ADSL-modeemi. Tukiasema on

tarkoitettu koti- ja pienyrityskäyttöön. Tukiasema tukee 802.11g-standardia.

Kuuluvuusmittauksissa käytetty kannettava tietokone oli Fujitsu-Siemens Amilo A1630. Tietokoneessa on AMD Athlon 64 3400+-prosessori. Käyttöjärjestelmä on Windows XP. Langattomana verkkokorttina tietokoneessa on Ralink RT2500-kortti, joka tukee standardeja 802.11b ja g.

Kuuluvuusmittauksissa käytetty ohjelma oli NetStumbler. Ohjelma on tarkoitettu 802.11a, b ja g-standardien mukaisten langattomien lähiverkkojen etsimiseen. NetStumbler on langattoman verkon löytämiseen tarkoitettu ohjelma, jonka saa ilmaiseksi ladattua Internetistä. Ohjelma kertoo käyttäjälle tarvittavat tiedot verkon langattomista asetuksista. NetStumbler-ohjelman toiminta perustuu majakkapakettien kuuntelemiseen, joita tukiasemat säännöllisesti lähettävät. Majakkapaketeilla tukiasemat. mainostavat itseään päätelaitteille ja kertovat muille tukiasemille itsestään. Majakkapaketeissa kerrotaan tiedot verkon asetuksista siihen liittymistä varten.

3 Langattoman lähiverkon standardit

Langattomien lähiverkkojen standardeja kehittävät kaksi organisaatiota. Institute of Electrical and Electronics Engineers (IEEE) on kansainvälinen organisaatio, joka edistää sähköteknisiä tieteitä muun muassa valmistelemalla ja julkaisemalla standardeja. Kun puhutaan yleisesti WLAN-standardeista (Wireless Local Area Network), tarkoitetaan juuri IEEE:n 802.11 standardeja (Juutilainen 2004).

The European Telecommunications Standards Institute (ETSI) on eurooppalainen organisaatio, joka on julkistanut oman HiperLAN-standardinsa (High Performance Radio Local Area Network). HiperLAN-standardi on käytössä vain Euroopassa, kun 802.11 on käytössä maailmanlaajuisesti. WLAN ja HiperLAN eivät ole yhteensopivia keskenään (Juutinen 2004).

Syy siihen miksi IEEE:n esittämä standardi on levinnyt maailmanlaajuisesti, on se, että IEEE sai oman standardinsa aikaisemmin valmiiksi kuin ETSI. Kyse ei ole siis tekniikoiden tai laitteiden laadusta (Suominen 2005).

3.1 IEEE 802.11-standardisarja

Langattomien lähiverkkojen tekniikan määrittelee IEEE:n 802.11 standardisarja (Puska 2005:230–231). WLAN-standardin perässä oleva kirjain kertoo IEEE:n työtyhmän nimen (Seppänen 2000). On huomattava, etteivät kirjaimet etene loogisessa järjestyksessä, sillä työryhmät saavat työnsä valmiiksi eri aikoihin.

3.1.1 802.11

IEEE:n suosituksen ensimmäinen versio, 802.11, hyväksyttiin vuonna 1997. Sen taajuusalue oli 2,4 GHz ja siirtonopeus 1 Mbps ja 2 Mbps. Standardin puutteena oli kuitenkin, ettei se taannut verkoille keskinäistä yhteensopivuutta, sillä standardi määritteli verkoille monia vaihtoehtoisia toteutuksia. Tämä puolestaan vähensi niin laitevalmistajien kuin kuluttajienkin kiinnostusta (Ranta-Eskola 2003).

3.1.2 802.11b

Paranneltu version IEEE:n 802.11 standardista, 802.11b, julkaistiin vuonna 1999. Taajuusalue oli sama kuin aiemmassa standardissa (2,4 GHz), mutta tiedonsiirtonopeus oli 11 Mbps. 802.11b on suosituin WLAN standardi. (Juutilainen 2004).

3.1.3 802.11a

802.11a julkaistiin vuonna 2001 ja on myös paranneltu versio alkuperäisestä standardista. Se tukee 54 Mbps siirtonopeuksia 5 GHz:n alueella (Granlund 2001: 230). On huomattava, että 802.11a on sallittu Euroopassa vain sisätiloissa (Juutilainen 2004).

3.1.4 802.11g

Standardin seuraava laajennus oli 802.11g, joka julkaistiin vuonna 2003. Se toimii taajuusalueella 2,4 GHz ja tukee 54 Mbps tiedonsiirtonopeutta. 802.11g on yhteensopiva 802.11b standardin kanssa (Juutilainen 2004).

3.1.5 802.11i

802.11i standardi julkaistiin heinäkuussa 2004 ja se parantaa WLAN-verkkojen tietoturvaa. Siinä määritellään todennus- ja avaintenhallintakäytäntö sekä parannetut menetelmät tiedon salaukseen. Suurin muutos uudessa standardissa koskee salausalgoritmia, joka vaihtuu RC4:stä AES-salaukseen (Juutilainen 2004, Griffith 2004).

3.1.6 Muut sarjan 802.11 standardit

Muiden IEEE 802.11 työryhmien osalta kehitystyö on vielä kesken, joten standardit ovat vielä työn alla.

802.11d työryhmän tarkoituksena on sovittaa 80211b muille taajuusalueille.

802.11e käsittelee multimediaan ja palvelunlaatuun (Quality of Service, QoS) liittyviä ratkaisuja. On todennäköisesti seuraavan hyväksyttävä standardi (Griffith 2004).

802.11f käsittelee WLAN roaming-ominaisuuksien parantamista (Juutilainen 2004) ja eri valmistajien laitteiden keskinäistä yhteensopivuutta (Kuokka 2002:14).

802.11h pyrkii sovittamaan 802.11a:n tehon ja kanavien käytön Eurooppaan sopivaksi.

802.11j pyrkii mahdollistamaan 802.11a:n ja HiperLAN/2 toiminnan samalla alueella (Juutilainen 2004).

802.11n pyrkii kasvattamaan tiedonsiirtonopeuden 100 Mbps (Griffith, 2004).

802.11r työryhmän tarkoituksena on kehittää nopeampi roaming-toiminto tukiasemien välillä (Griffith 2004).

802.11s työryhmän tarkoituksena on mahdollistaa WLAN-tukiasemien liittäminen suureksi silmukkaverkoksi (Griffith 2004).

3.2 ETSI HiperLAN

ETSI alkoi kehittää omaa standardiaan 1990-luvun alussa ja sai sen (EN 300 652) valmiiksi vuonna 1998. ETSI:n HiperLAN toimii 5 GHz:n (5,15 - 5,30 GHz) ISM-taajuuksilla. Tuolla taajuusalueella toimii viisi kaistaa, joista kaksi viimeistä saa käyttöönsä, jos maan hallitus niin sallii. Tämä oli yksi syy siihen, miksei kyseinen standardi saavuttanut yleisön suosiota (Suominen 2005).

HiperLAN-standardit tarjoavat etuja 802.11-standardeihin verrattuna tarjoamalla mm paremman palvelun tason (Quality Of Service, QoS), paremman tietoturvatason (DES, 3DES) ja yhteensopivuuden muiden tekniikoiden (IP, ATM, UMTS) kanssa. HiperLAN-standardien varjopuolia ovat vapaan taajuuskaistan puute ja käytetystä taajuusalueesta johtuva lyhyt kantomatka (Juutilainen 2004).

3.2.1 HiperLAN/1

HiperLAN/1 toimii 5 GHz:n ISM-taajuuksilla. Sen tiedonsiirtonopeus on 22 Mbps. HiperLAN1 ei saavuttanut kovin suurta kiinnostusta ja sen jatko on epävarmaa (Särkimäki 2004).

3.2.2 HiperLAN/2

HiperLAN/2 toimii myös 5 GHz:n ISM-taajuuksilla, mutta sen tiedonsiirtonopeus on maksimissaan 54 Mbps. HiperLAN2 on jatkokehitetty teknologia ja sen tulevaisuus on vielä avoin (Särkimäki 2004).

3.2.3 Muut sarjan ETSI:n standardit

ETSI:llä on vielä kaksi muuta standardia, jotka ovat työn alla.

HiperAccess-standardin tarkoitus on määritellä nopea ja langaton taajuusalueella 40,5 - 43,5 GHz ja point-to-multipoint-periaatteella toimiva laajakaistayhteys koteihin. HiperAccess tunnetaan myös nimellä HiperLAN/3 (Vaaranmaa 2003).

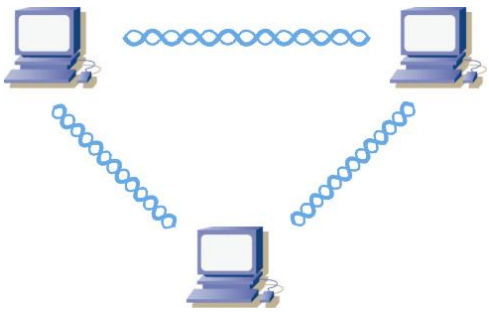
HiperLink-standardi tarjoaa lyhyen kantaman yhteyden HiperLAN/2- ja HiperLAN/3–verkojen välille. Tiedonsiirtonopeus olisi maksimissaan 155 Mbps taajuusalueen ollessa 17 GHz (Vaaranmaa 2003).

3.3 WLAN topologiat

IEEE (Institute of Electrical And Electronics Engineers) 802.11-suosituksen mukainen langaton lähiverkko sallii kolme tapaa kytkeä verkon laiteita toisiinsa (Granlund 2001:230).

3.3.1 IBSS

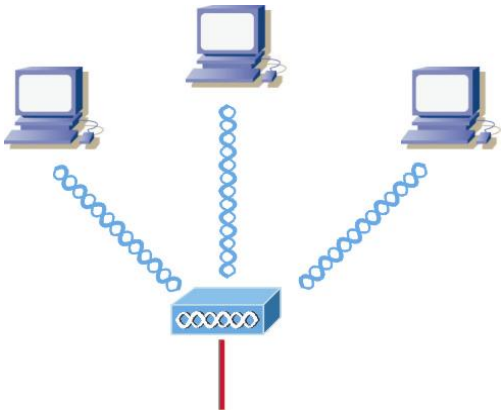
Kun laitteet (esim. kannettavat tietokoneet) muodostavat keskenään tilapäisen verkon, josta ei ole pääsyä kiinteään verkkoon, käytetään tästä verkosta nimitystä IBSS (Independent Basic Service Set). Verkon topologia on esitetty kuvassa 5. Tällainen verkko on yleensä käytössä tilapäisen tarpeen täyttämiseksi esimerkiksi neuvottelu- tai kokoustilanteissa ja se puretaan tarpeen päättyessä. Laitteen siis keskustelevat keskenään langattoman yhteyden yli tietyn hetken ajan. Tästä verkosta käytetään myös nimeä Ad-Hoc-verkko (Granlund 2001:231).



Kuva 5 IBSS-verkko

3.3.2 BSS

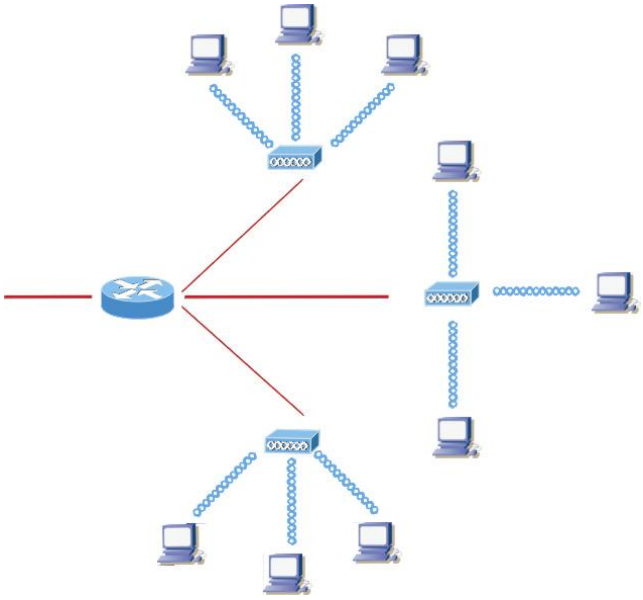
Basic Service Set (BSS), joka on esitetty kuvassa 6, on verkko, joka muodostuu kiinteästä tukiasemasta ja siihen loogisesti liitetyistä laitteista. Tässä verkossa kaikki keskustelu laitteiden välillä käydään tukiaseman kautta. Verkon topologia muistuttaa kytkimiin perustuvaa kiinteää lähiverkkoa (Granlund 2001:231).



Kuva 6 BSS-verkko

3.3.3 ESS

Extended Service Set (ESS) on laajennettu BSS-verkko. ESS on esitelty kuvassa 7. Siinä käytetään useampia tukiasemia, jotka kaikki on kytketty runkoverkkoon. ESS on yleisin tapa muodostaa langattomia lähiverkkoja, sillä kattavuus ei rajoitu yhteen kerrokseen ja ratkaisulla voidaan kiertää laitteiden pienestä kantavuudesta aiheutuvat ongelmat (Granlund 2001:231).



Kuva 7 ESS-verkko

4 Langattomien lähiverkkojen toiminta

Langattomat lähiverkot (WLAN) toimivat 2,4 GHz:n ISM-taajuuksilla (Industrial, Scientific, Medical). ISM-taajuuksien käyttö on vapaata, eikä siihen tarvita lupaa. Näin ollen kuka tahansa voi pystyttää samalla taajuudella toimivan verkon. Samalla taajuudella toimivat mm. mikroaaltouunit ja Bluetooth-laitteet.

4.1 WLAN kanavat

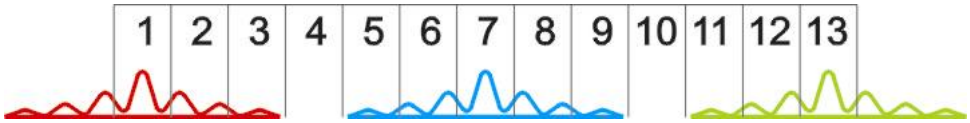
Kanavat ovat taajuuksia, joilla tukiasemat kommunikoivat päätelaitteiden kanssa. Mikäli samalla kanavalla toimii useampi tukiasema, häiriintyy tukiasemien toiminta. Näin ollen tukiasemien kanavat tulisi valita niin, että ne ovat mahdollisimman etäällä toisistaan. Toisin sanoen niiden käyttämien taajuuksien ero tulisi olla mahdollisimman suuri (Oraskari 2003:64).

Langattomien lähiverkkojen standardi 802.11b määrittelee taajuusalueelle 2,4–2,4835 GHz 14 kanavaa. Kanavat on sijoiteltu viiden megahertsin välein. EU:n alueella käytetään pääsääntöisesti käytössä 13 alinta kanavaa, mutta poikkeuksiakin löytyy (Hämäläinen 2003:59.) Suomessa on käytössä kuitenkin kyseiset 13 kanavaa. Taulukossa 2 on esitetty maakohtaiset taajuudet ja käytössä olevat kanavat.

Taulukko 2 Maakohtainen kanavatilanne

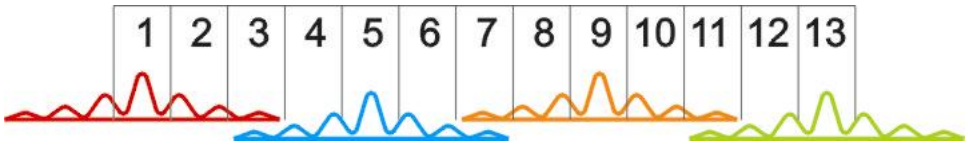
Alue	**Taajuusalue (GHz)**	**Kanavat**
USA	2,4000 – 2,4835	11
Eurooppa	2,4000 – 2,4835	13
Japani	2,4710 – 2,4970	14
Ranska	2,4465 – 2,4835	10 - 13
Espanja	2,4450 – 2,4750	10 - 11

Signaali varaa taajuusalueelta 16–25 MHz:n levyisen kaistan, joka aiheuttaa ylikuulumista muille kanaville ja rajoittaa kanavien valintaa. Näin ollen samalla taajuusalueelle voidaan pystyttää täysin häiriöittä vain kolme rinnakkaista lähiverkkoa (Hämäläinen 2003:59). Kuten kuvassa 8 on esitetty, nämä kanavat ovat 1, 7 ja 13.



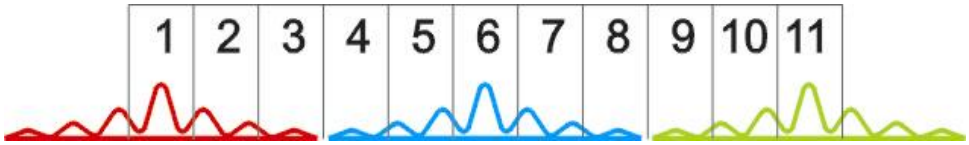
Kuva 8 Kanavajako 3/13 kanavalla

Käytettäessä neljää kanavaa (1, 5, 9 ja 13) saadaan käyttöön useampi kanava, mutta myös jonkin verran häiriötä kohinan muodossa. Kuvasta 9 nähdään, että kanavat menevät hieman toistensa päälle. Käytännössä tästä ei ole sanottavaa haittaa ja saavutettu etu yhden lisäkanavan muodossa on tärkeämpi kuin vähäinen häiriö (Seppänen 2000).

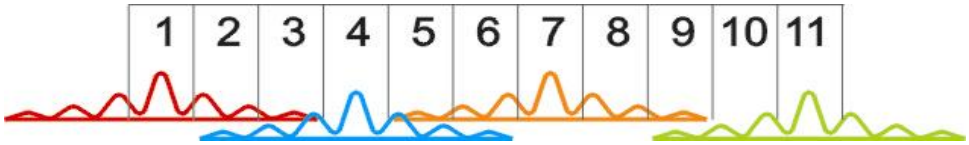


Kuva 9 Kanavajako 4/13 kanavalla

Kaikki PCMCIA-kortit eivät tue kanavia 12 ja 13 ja ne tulisi jättää käyttämättä. Näin ollen käytettävissä olevat kanavat ovat kolmen kanavan mallissa 1, 6 ja 11 (kuva 10) ja neljän kanavan mallissa 1, 4, 7 ja 11 (kuva 11) (Oraskari 2003:64).



Kuva 10 Kanavajako 3/11 kanavalla



Kuva 11 Kanavajako 4/11 kanavalla

4.2 Signaalin mittayksikkö

Teho ilmoitetaan yleensä watteina (W). Langattomien lähiverkkojen yhteydessä watti on kuitenkin liian suuri mittayksikkö, sillä 802.11b laitteiden suurimmaksi lähetystehoksi Euroopassa on määritetty 100 milliwattia (mW) (Puska 2005:51). Milliwatti ei ole kuitenkaan käytännöllinen mittayksikkö mitattaessa langattoman lähiverkon signaalin voimakkuutta, sillä se on lineaarinen mittayksikkö. Signaalin voimakkuus ei häviä lineaarisesti, vaan pikemminkin käänteisesti etäisyyden neliönä. Toisin sanoen etäisyyden kasvaessa tukiasemasta kaksinkertaiseksi, signaali heikkenee yhteen neljäsosaan aiemmasta. (Bardwell 2002).

Langattoman lähiverkon säteilyn teho esitetään yleensä desibelimilliwateissa (dBm) ja esimerkiksi 100 mW on 20 dBm. (Puska 2005:51). Desibelimilliwatti on desibeli yksikkö, jolla mitataan tehoa. Desibelimilliwatti on sopivampi yksikkö signaalin voimakkuuden mittaamiseen, sillä se lo-

garitminen. Milliwatit voidaan kääntää desibelimilliwateiksi ja päinvastoin (Bardwell 2002).

Milliwatit muutetaan desibelimilliwateiksi seuraavalla kaavalla:

$$dBm = \log(mW) * 10$$

Vastaavasti desibelimilliwatit muutetaan milliwateiksi seuraavalla kaavalla:

$$mW = 10 \wedge (dBm / 10)$$

Teho on tässä yhteydessä aina positiivinen suure, sillä negatiivista tehoa ei voi olla. Näin ollen teho ei ole koskaan milliwatteina nollaa pienempi, vaan aina nollan ja ykkösen välillä. Milliwatteina voidaan esittää myös pieniä tehoja, mutta luvut olisivat pitkiä desimaalilukuja. 802.11 standardin mukainen langattoman lähiverkon verkkokortin pienin vastaanottoherkkyys on noin -96 dBm. Milliwatteina tämä luku olisi 0,0000000002511 mW ja olisi vaikeampi hahmottaa (Bardwell 2002).

On helppo ymmärtää luvut 100 mW ja 20 dBm, sillä molemmat luvut on esitetty helpossa muodossa. Hankalampaa on hahmottaa luku 0,0000000002511 mW. On yksinkertaisempaa käyttää lukua –96 dBm, joka on 0,0000000002511 mW desibelimilliwateissa ilmaistuna. Käytettäessä desibelimilliwatteja tehon ilmaisemiseen milliwattien sijaan langattomien lähiverkkojen yhteydessä haetaan kahta asiaa:

1) käyttömukavuutta
2) ymmärtämisen helppoutta (Bardwell 2002).

4.3 Signaalin eteneminen ja vaimeneminen

Radioaalto on sähkömagneettista säteilyä, joka etenee suoraviivaisesti ja vaimentumatta ainoastaan tyhjiössä. Todellisuudessa väliaine (ilma) ja esteet (esim. rakennusmateriaalit, ihmiset) vaikuttavat signaalin etenemiseen (Puska 2005:56). Taulukossa 3 on esitetty yleisimpien rakennusmateriaalien aiheuttamat signaalin vaimenemiset (Juutilainen 2004, Simplify…2005).

Taulukko 3 Eri materiaalien vaikutus signaalin vaimenemiseen

Este	**Vaimennus (dB)**
Kerros	30
Ikkunallinen tiiliseinä	2
Tiiliseinän metalliovi	12,4
Metallioven vieressä oleva tiiliseinä	3
Konttoriseinä	6

Konttoriseinän metalliovi	6
Kevytharkkoseinä	4
Puuovi	3
Kuivamuurattu seinä	4
Marmori	5
Tiiliseinä	8
Betoniseinä	10 - 15

Sisätiloissa radioaaltojen etenemiseen vaikuttavat:

1) vaimeneminen
2) heijastukset
3) monitie-eteneminen

Ulkoilmassa edellisten lisäksi etenemiseen voivat vaikuttaa:

3) taipuminen
4) sironta (Puska 2005:51).

4.3.1 Vaimeneminen

Vaimeneminen on ilmiö, jossa on kyse signaalin tehon vähenemisestä. Tehon pieneneminen riippuu taajuudesta, väliaineen ominaisuudesta ja matkasta (Puska 2005:56). Osa signaalin tehosta muuttuu signaalin vastustuksesta johtuen johtimessa lämmöksi, joten signaali vaimenee. Vaimeneminen vaihtelee riippuen käytetystä siirtotiestä ja taajuudesta. (Granlund 2001:13).

Myös etäisyys aiheuttaa signaalin vaimenemista. Nyrkkisääntönä voidaan pitää, että jokainen etäisyyden lisäys (tai vähentäminen) tukiasemaan nähden pienentää (tai lisää) signaalin kuuluvuutta 6 dB (Young 2004)

4.3.2 Heijastukset

Heijastumista tapahtuu radioaallon osuessa kahden väliaineen pintaan sopivassa kulmassa. Toinen aine on usein ilma, josta säteily heijastuu ikään kuin valo peilistä. Säteen tulokulman ollessa suuri vain osa säteilystä heijastuu ja osa taittuu toisen aineen sisään (Puska 2005:57).

4.3.3 Monitie-eteneminen

Radiosignaali saattaa matkallaan heijastua ympäristössä olevista esineistä ja kulkea jopa kaksinkertaisen matkan verrattuna lyhyempään reittiin. Heijastuva signaali saavuttaa määränpäänsä väärään aikaan ja lisäksi se on menettänyt osan tehostaan heijastuksen yhteydessä (Granlund 2001:

16). Langattomissa lähiverkoissa käytetty hajaspektri- ja kaksiantennitekniikka pystyy kompensoimaan jonkin verran monitie-etenemisen häipymistä (Puska 2005:58).

4.3.4 Taipuminen

Yleisesti ottaen radioaallot etenevät suoraviivaisesti, mutta koska radioaallot ovat sähkömagneettista säteilyä, on sillä myös hiukkasluonne. Taipuminen tapahtuu pienten alkeishiukkasten vaikuttaessa säteilyyn. Tällaisia pieniä hiukkasia on ilmassa ja ilmakehän ylemmissä kerroksissa (Puska 2005:57).

4.3.5 Sironta

Sironnalla tarkoitetaan tilannetta, jossa säteily hajaantuu erisuuntaisten aaltorintamien kimpuksi osuessaan pieneen partikkeliin. Sironnalla on merkitystä lähinnä ilmakehässä (Puska 2005:58)

4.4 Etäisyyden vaikutus signaalin laatuun

Kuten edellä on esitetty, signaalin laatu heikkenee mm. matkan kasvaessa. Tukiasema kuuluu yleensä maksimissaan noin 30 - 100 metrin päähän (Seppänen 2000). Yhdellä tukiasemalla voidaan kattaa noin 280 - 650 m^2 alue (Simplify…2005). Langattoman lähiverkon kantama on pieni lukuun ottamatta tilanteita, joissa tukiaseman ja päätelaitteen välissä ei ole esteitä. Absoluuttista ohjetta on vaikea antaa, koska suorituskykyyn vaikuttaa moni asia. Taulukon 5 arvoja voi käyttää jonkinlaisina ohjearvoina (Granlund 2001:257).

Taulukko 4 Etäisyyden vaikutus tiedonsiirtonopeuteen sisätiloissa

Tiedonsiirtonopeus (Mbps)	**Kantama sisätilassa (m)**
1	50
2	40
5,5	35
11	25

Huomattava on myös, että samalla taajuusalueella toimivat mikroaaltouunit, Bluetooth-laitteet, langattomat puhelimet ja muut WLAN-verkot saattavat heikentää signaalin laatua. Varsinaista lukkiutumista ei tapahdu, vaan häiriö näkyy yhteyden hidastumisena (Granlund 2001:258, Juutilainen 2004).

4.5 Signaalin voimakkuuden vaikutus tiedonsiirtonopeuteen

Mitä voimakkaampi signaali on, sitä parempi on langattoman lähiverkon tiedonsiirtonopeus. Kun signaali heikkenee, putoaa myös tiedonsiirtonopeus. Ylläpitääkseen yhteyden, 802.11 standardin mukaiset laitteet pudottavat automaattisesti tiedonsiirtonopeuttaan (Phifer 2005). Toisaalta jos käyttäjä tyytyy vaatimattomampaan tiedonsiirtonopeuteen, sitä kauempana käyttäjä voi olla tukiasemasta.

Nimellinen ja todellinen tiedonsiirtonopeus ovat kaksi eri asiaa. Siirtovirheiden ja uudelleenlähetysten vuoksi lopullinen siirtonopeus jää usein hieman yli 40 prosenttiin todellisesta. Esimerkiksi 11 Mbps nopeus on todellisuudessa vain 5 Mbps (Oraskari 2003). Jos tukiaseman on yhteydessä yksi laite, se saa käyttöönsä kaiken kapasiteetin. Useamman laitteen ollessa kyseessä signaali jakaantuu niiden kesken (Seppänen 2000).

Tyypillisesti 802.11b standardin mukaiset WLAN verkkokortit edellyttävät –83 dBm signaalia ylläpitääkseen 11 Mbps tiedonsiirron (Young 2004). Vertailun vuoksi taulukossa 5 on esitetty 802.11g standardin mukaisen WLAN verkkokortin arvot (Piscitello 2005).

Taulukko 5 WLAN-verkkokortin tiedonsiirtonopeuden ja signaalin voimakkuuden suhde

Tiedonsiirtonopeus (Mbps)	**Signaalin voimakkuus (dBm)**
54	-68
48	-68
36	-75
24	-79
18	-82
12	-84
11	-82
9	-87
6	-88
5,5	-85
2	-86
1	-89

Taulukosta ilmenee, että mitä pienempi negatiivinen arvo signaalin voimakkuudella on, sitä parempi on sen laatu ja sitä suurempi on sen tiedonsiirtonopeus.

5 Langattomien lähiverkkojen tietoturva

Yksi suurimmista langattomia lähiverkkoja koskevista ennakkoluuloista on tietoturva. Langattomat lähiverkot mielletään helposti langallisia lähiverkkoja turvattomimmiksi. Tämä ei kuitenkaan enää pidä paikkaansa, sillä oikeilla toimenpiteillä voidaan langaton lähiverkko suojata langallista vastaavaksi. Tuntemalla tietoturvan tavoitteet, langattomien lähiverkkojen suurimmat turvauhat ja mahdollisuudet langattomien lähiverkkojen tietoturvan parantamiseksi, voi langattoman lähiverkon turvallisuutta parantaa huomattavasti.

5.1 Tietoturvan tavoitteet

Tietoturva voidaan jakaa kuuteen osaan tai tavoitteeseen, joihin toiminnalla pyritään. Kaikki osat koskevat tietoa sen eri muodoissa (Järvinen 2002:22).

1) Luottamuksellisuus
   - Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsee käsiksi vain siihen oikeutettu henkilö.
2) Eheys
   - Eheydellä tarkoitetaan sitä, että kukaan ulkopuolinen ei pysty luvatta muuttamaan tietoa.
3) Saatavuus
   - Saatavuudella tarkoitetaan sitä, että tieto on saatavilla koko ajan.
4) Todentaminen
   - Luottamuksellisuus edellyttää käyttäjän todentamista. Todentamisella varmistetaan käyttäjän oikeus käyttää tietoverkkoa.
5) Pääsynvalvonta
   - Pääsynvalvonta huolehtii todennettujen henkilöiden pääsemisestä järjestelmän tietoihin.
6) Kiistämättömyys
   - Kiistämättömyydellä tarkoitetaan tehtyjen toimien todistamista sitovasti esimerkiksi sähköisessä kaupankäynnissä (Järvinen 2002:22-28).

5.2 Langattomien lähiverkkojen tietoturva uhat

Vaikkakin tietoturvauhat ovat langattomissa lähiverkoissa pääosin samoja kuin langallisissa verkoissa, tuo langattomuus mukanaan uusia puolia. Niitä ovat uudenlaiset murtautumismenetelmät ja murtautumista yrittävät. Pääsy langattomiin verkkoihin on helpompaa, sillä hyökkääjän ei tarvitse ylittää fyysisiä esteitä tai kytkeä päätelaitettaan verkkorasiaan.

Langattomien lähiverkkojen tietoturvauhat voidaan jakaa passiivisiin ja aktiivisiin uhkiin. Passiivisten uhkien ollessa kyseessä verkkoon ei kohdistu suoranaista vahingollista toimintaa. Tilanne on toinen aktiivisen uhan ollessa kyseessä, jolloin tunkeutuja voi lähettää dataa tai signaalia verkkoon.

5.2.1 Passiiviset uhat

Salakuuntelu

Verkon liikennettä voidaan kuunnella rakennuksen sisä- tai ulkopuolelta, jolloin tarkoituksena on kerätä tietoa, joka auttaa verkkoon tunkeutumisessa. Salakuuntelua on vaikea estää ja havaita. Salakuunteluun tarvittavia ohjelmia on saatavilla Internetistä ja ne toimivat perustason tietokoneissa, joissa on langaton verkkokortti.

Liikenteen analysointi

Verkon liikennettä voidaan analysoida tarkoituksena paljastaa luottamuksellista tietoa. Analysointiin ja salakuunteluun saatavilla valmiilla ohjelmilla voidaan saada selville verkon turva-asetukset sekä salausavaimet.

5.2.2 Aktiiviset uhat

Siirtomedian häirintä

Siirtomedian häirinnän tarkoituksena on ylikuormittaa verkkoa, jolloin sen toiminta hidastuu tai katkeaa. Tähän voidaan käyttää vapailla taajuuksilla toimivia radiolähettimiä tai ylikuormittamalla WLAN-tukiasemia turhilla liityntä- tai palvelupyynnöillä (Vesanen 2003).

Datan muokkaaminen

Datan muokkaaminen voi tapahtua tahallisesti tai tahattomasti. Tahaton datan korruptoituminen havaitaan tarkistussummasta ja kehys hylätään virheellisenä. Tahallinen hyökkäys perustuu yhteysosapuolten välissä toimimiseen ja tunnetaan nimellä man-in-the-middle.

Tietojärjestelmään tunkeutuminen

Hyökkääjän lopullinen päämäärä on tietojärjestelmään tunkeutuminen, jolloin muut keinot ovat käytössä päämäärän vuoksi. Langattoman lähiverkon kautta voi hyökkääjä päästä käsiksi yrityksen palvelimiin ja työasemiin (Puska 2005:69)

5.3 Hyökkäykset langattomia lähiverkkoja vastaan

Langattomia lähiverkkoja vastaan tehdyt hyökkäykset tapahtuvat kolmea verkon perusominaisuutta vastaan. Nämä ovat:

1) luottamuksellisuus
2) eheys
3) käytettävyys

Hyökättäessä luottamuksellisuutta vastaan, pyritään kaappaamaan siirrettävää tietoa, purkamaan salausavaimia tai selvittämään tunnistetietoja. Hyökkäyksen tavoitteena on saada haltuun luottamuksellista tietoa tai keinoja sen saamiseen. Eheyttä vastaan hyökätään muuttamalla verkon laitteita tai muuttamalla verkossa siirrettävää tietoa. Pyritään siis luvattomasti saamaan haltuun tietoa, jota muutetaan toiseksi. Tekemällä palvelunestohyökkäyksiä hyökätään käytettävyyttä vastaan.

Hyökkäykset langattomia verkkoja kohtaan alkavat aina verkon etsimisellä. Tähän on saatavana Internetistä ilmaisohjelmia, jotka eivät vaadi suuria laitteistovaatimuksia. Ohjelmat selvittävät esimerkiksi verkon tunnuksen (Service Set Identifier, SSID), käytettävän kanavan ja tukiaseman MAC-osoitteen. Verkkojen etsinnästä käytetään nimitystä "War Driving" (Ahvenainen 2003).

5.3.1 MAC-osoitteen väärentäminen

Pääsyä langattomaan lähiverkkoon voidaan osaltaan rajoittaa MAC-osoitteen perusteella, jolla verkon todennetut laitteet erotellaan todentamattomista. MAC-osoite voidaan kuitenkin vaihtaa toiseksi, jolloin tarkoituksena on huijata tukiasema luulemaan laitetta verkon todennetuksi laitteeksi. Todennetun MAC-osoitteen voi selvittää haistelijaohjelmalla tai generoida ohjelmallisesti eri MAC-osoitteita (Ahvenainen 2003, Keenan 2004).

5.3.2 Palvelunestohyökkäys

Palvelunestohyökkäyksen (Denial of Service, DoS) tarkoituksena on estää laillisia käyttäjiä käyttämästä verkkoa ja sen palveluja. Langattomassa verkossa on käytössä rajallinen määrä taajuuksia, joiden tukkiminen onnistuu esimerkiksi kohinatasoa nostamalla. Hyökkäys voidaan toteuttaa myös muokkaamalla langattoman verkkokortin ohjelmistoa niin, että se pakotetaan jatkuvaan lähetystilaan (Ahvenainen 2003).

5.3.3 Luvaton tukiasema

Luvattomalla tukiasemalla voidaan tarkoittaa kahta tilannetta. Tukiasema voi olla luvallisen käyttäjän luvaton tukiasema, mutta jonka turvallisuusasetukset ovat perustasolla ja joka näin ollen muodostaa tietoturvariskin.

Tukiasema voi olla myös hyökkääjän luvaton tukiasema (Evil Twin). Hyökkääjä konfiguroi oman tukiasemansa vastaamaan luvallista tukiasemaa. Luvaton tukiasema voi olla varustettu suurella lähtöteholla ja suunta-antennilla, jolloin sen signaali on voimakkaampi kuin luvallisen tukiaseman. Verkkoa etsivä päätelaite hakee voimakkainta mahdollista signaalia ja löytää luvattoman tukiaseman. Käyttäjä luulee kirjautuvansa lailliseen tukiasemaan, sillä hänelle ei näy verkosta muuta kuin verkon SSID (Ahvenainen 2003, Keenan 2004).

5.3.4 Man-in-the-middle

Man-in-the-middle-hyökkäyksessä hyökkääjä asettuu yhteyden päätepisteiden väliin, jolloin kaikki tieto kulkee hänen kauttaan. Hyökkääjä voi muokata liikkuvaa tietoa oikeiden käyttäjien huomaamatta. Man-in-the-middle-hyökkäykseen tarvitaan Evil Twin-tukiasema (Ahvenainen 2003).

5.4 Langattoman lähiverkon salausprotokollat

Salaamalla langattoman lähiverkon liikenne pyritään turvaamaan tiedon luottamuksellisuus ja eheys salakuuntelun varalta. Langattoman lähiverkon signaalin salakuuntelua on lähes mahdotonta estää. Signaalin kuulumista voi rajoittaa suuntaavilla antenneilla, mutta nämä eivät kokonaisuudessaan ratkaise ongelmaa. Näin ollen ainoaksi ratkaisuksi jää signaalin sisältämän sanoman salaaminen salakuuntelijoilta.

5.4.1 Staattinen WEP

Wired Equivalent Privacy (WEP) oli 802.11-suosituksen ensimmäinen salausmenetelmä. Sen salaus perustui alun perin 40-bittiseen (myöhemmin 128 bittiä) salaiseen avaimeen. WEP murrettiin muutamassa viikossa ilmestymisensä jälkeen (Keenan 2004). WEP:ssä käytettävässä RSA Securityn RC4-salauksessa ei itsessään ollut vikaa, vaan kyse oli salausalgoritmin yhteydessä käytettävästä alustusvektorista, joka standardin mukaan toteutettuna oli liian heikko (Kotilainen 2003).

5.4.2 Dynaaminen WEP

Staattisen WEP-salauksen ongelmien selvittyä, alkoivat laitevalmistajat korjata ilmenneitä ongelmia. Koska kyse oli alustusvektorin heikkoudesta, eikä itse salauksesta, oli vian korjaaminen helppoa. Näin ollen nykyisissä yrityskäyttöön tarkoitetuissa WLAN-laitteissa ei ole enää staattisen WEP-salauksen heikkouksia (Kotilainen 2003, Enterprise…2003).

5.4.3 WPA (TKIP)

Wi-Fi Protected Access (WPA) seurasi WEP:iä. Se poisti kokonaisuudessaan WEP aiheuttamat ongelmat. WPA:ssa on käytössä Temporal Key Integrity Protocol -salaus (TKIP), parantaa langattoman verkon turvallisuutta huomattavasti ottamalla käyttöön pakettikohtaiset salausavaimet. TKIP käyttää edelleen RSA Securityn RC4-salausta, mutta salausavaimen pituus on 128 bittiä. WPA:n huonona puolena on alttius palvelunestohyökkäyksille, jolloin WPA sulkee verkon kaikilta käyttäjiltä noin minuutiksi hyökkäyksen havaittuaan (Enterprise…2003).

5.4.4 WPA2 (AES)

Wi-Fi Protected Access 2 (WPA2) on määritelty 802.11i-standardissa ja on näin ollen uusin salaustekniikka. Suurin muutos WPA2:ssa on, että siinä on Advanced Encryption Standard-salaus (AES) aiemman RC4-salauksen sijaan (Kotilainen 2003). AES on vahvin mahdollinen siviilikäyttöön tarkoitettu salaus (Enterprise…2003).

5.4.5 VPN

Virtual Private Network-tekniikalla (VPN) on mahdollista luoda suojattu tunneli kahden tietokoneen välille. Tässä ratkaisussa tiedonsiirtoon käytetyn verkon turvallisuudella ei ole merkitystä, sillä paketit salakirjoitetaan IPSec-protokollan avulla. VPN-ratkaisussa tietokoneille asennetaan ohjelma, joka muodostaa salatun tunnelin tietokoneiden välille. Langat-

toman tukiaseman taakse, ennen yrityksen muuta verkkoa, sijoitetaan VPN-yhdyskanava, joka vastaanottaa salatun liikenteen (Kotilainen 2003).

5.5 Langattoman lähiverkon autentikointi

Autentikoimalla eli tunnistamalla verkon käyttäjä tai päätelaite pyritään turvaamaan tiedon todentaminen. Näin varmistutaan siitä, että päätelaitteella tai käyttäjällä on oikeus käyttää tietoverkkoa. Päästäkseen käyttämään langattoman lähiverkon palveluja, on päätelaitteen ensin tunnistauduttava verkon tukiasemalle. 802.11-standardi sisältää yksisuuntaisen laitetunnistuksen, mutta tämä ei ole riittävän turvallinen. Turvalliseen tunnistamiseen tarvitaan kaksisuuntainen tunnistus työaseman ja tukiaseman välille. Tunnistaminen on mahdollista tehdä joko avoimella autentikoinnilla tai jaetun avaimen autentikoinnilla (Puska 2005).

5.5.1 SSID

Avoin autentikointi perustuu palvelutunnisteeseen (Service Set Identification, SSID), joka käytännössä tarkoittaa verkon nimeä. SSID ei ole luotettava tunnistusmenetelmä seuraavista syistä. SSID-tunnukset on tehtaalla asetettu tietyiksi saman valmistajan laitteisiin, joten niiden selvittäminen on helppoa. Tukiasema voi myös hyväksyä päätelaitteen verkkoon liittymisen ilman SSID-tunnusta, joko tyhjällä (Null) tunnuksella tai ANY tunnuksella. Lisäksi tukiasema lähettää SSID-tunnustaan selväkielisenä majakkasanomissa ilmoittaakseen toiminnastaan verkon mahdollisille uusille asiakkaille. (Puska 2005).

5.5.2 MAC

Jokaisella verkkokortilla on oma yksilöllinen MAC-osoitteensa. MAC-tunnistuksessa tukiasemalle luodaan lista niiden päätelaitteiden verkkokorttien MAC-osoitteista, joilla on lupa liittyä verkkoon. MAC-osoitteet ovat kuusitavuisia heksadesimaalilukuja, joten luettelon ylläpitäminen on työlästä ja menetelmä ei sovellu useita päätelaitteita sisältävään ympäristöön (Puska 2005).

5.5.3 WEP

Wired Equivalent Privacy-tunnistus (WEP) perustuu jaetun avaimen menetelmään. Käytetty avain on sama, jota WEP käyttää liikenteen salaamiseen. Riskinä on, että saamalla avaimen haltuunsa saa myös pääsyn WEP:llä salattuihin tietoihin. Menetelmän heikkous on se, että kaikille päätelaitteille pitää määritellä sama avain kuin tukiasemalle. Tosin pääte-

laitteilla voidaan määritellä neljä eri avainta, mikä hieman parantaa asiaa. WEP:n käyttö on vapaaehtoista (Puska 2005).

5.5.4 802.1X

802.1X-standardissa uutta aiempiin verrattuna oli käyttäjien autentikointi. 802.1X-standardi on laadittu niin, että sitä voidaan helposti laajentaa. Näin esimerkiksi oikeuksien valvonta ja avaintenhallinta on helposti toteutettavissa (Niemi 2003).

Käyttäjätunnistuksesta huolehtii autentikointipalvelin, jolle tukiasema toimittaa asiakkaan tunnistetiedot. Asiakkaan tunnistamisessa käytetään Extensible Authentication Protocol -protokollaa (EAP). EAP ei itsessään ole tunnistusmenetelmä, vaan tarjoaa kuljetusalustan tunnistustoteutuksille. Tunnistusmenetelmänä voidaan lähiverkoissa käyttää EAP over LAN. (EAPOL) ja EAP over WLAN-menetelmiä (EAPOW). EAP tunnistaa käyttäjän ja myöntää pääsyn päätelaitteelle, mutta päätelaitteella ei ole mitään keinoa tunnistaa tukiasemaa. (Puska 2005).

5.5.5 EAP/LEAP

Cisco Systems kehitti oman versionsa EAP:stä nimeltään Lightweight EAP (LEAP). Se tarjoaa kahdensuuntaisen tunnistuksen ja mahdollisuuden kirjautua sisään Microsoft 200 ja 2003 Server-järjestelmän aktiivihakemistoon WLAN tunnistautumisen yhteydessä. LEAP toimii vain Cisco Systemsin valmistamien laitteiden kanssa.

5.5.6 EAP/TLS

EAP:n tukema tunnistusmenetelmä on Transport Socket Layer-menetelmä(TLS). TLS mahdollistaa molemminpuolisen tunnistuksen, jossa päätelaite voi tunnistaa tukiaseman ja verkko käyttäjän. Kaksisuuntainen tunnistus ehkäisee salasanojen vakoilun väärennetyn tukiaseman avulla. TLS:n avulla voidaan vaihtaa myös istuntoavaimet turvallisesti. Ongelmana on se, että WLAN-verkkokorteilla ja tukiasemilla on puutteellinen TLS-tuki (Puska 2005).

5.6 Tietoturvan parantaminen langattomissa lähiverkoissa

Kotitason käyttäjälle riittää muutama toimenpide langattoman lähiverkon turvallisuuden parantamiseksi. Tilanne on kuitenkin toinen yritystason langattomassa lähiverkossa sen avoimemman luonteen ja isomman käyttäjämäärän vuoksi.

5.6.1 Fyysinen tietoturva

Fyysisellä tietoturvalla tarkoitetaan tukiasemien asennusta ja suojaamista luvattomilta käyttäjiltä. Fyysinen tietoturva on olennainen osa tietoturvaa, sillä sen laiminlyönnillä aiheutetaan vakava aukko tietoturvaan. Fyysinen tietoturva on syytä ottaa huomioon puhuttaessa tietoturvan parantamisesta langattomissa lähiverkoissa.

Tukiasemien sijoitus

Tukiasemat tulee sijoittaa siten, ettei kukaan ulkopuolinen pääse niihin käsiksi tai löydä niitä helposti. Ne tulee sijoittaa mahdollisimman korkealle tai sen ollessa mahdotonta, suojata ne esimerkiksi lukittavalla muovikotelolla. Yksi mahdollisuus on sijoittaa tukiasemat alaslasketun katon yläpuolelle piiloon, jolloin ne ovat suojassa katseilta.

Tukiasemien konfigurointi

Oleellista on varmistaa, ettei tukiaseman konsoliporttiin pääse kytkemään omaa tietokonetta tai painamaan tukiaseman reset-painiketta tai muita painikkeita. Joissain tukiasemissa on konsoliportti tukiaseman konfigurointiin ja se on syytä ottaa pois käytöstä. Tukiasemat ovat varsin helposti palautettavissa tehdasasetuksiin, jolloin ne nollaavat kaiken tietonsa ja mahdollistavat pääsyn verkkoon. Hyökkääjä voi myös korvata laillisen tukiaseman omalla laittomallaan, jos tukiasemiin pääsee helposti käsiksi.

Kulunvalvonta

Fyysiseen tietoturvaan kuuluu myös kulunvalvonta, jolla estetään luvattomien pääsy alueelle, jossa tukiasemat sijaitsevat (Puska 2005, Seppänen 2000, Geier 2002). Kulunvalvonta voidaan helpoiten toteuttaa lukitsemalla ovet, jotka johtavat tiloihin, jossa langaton lähiverkko kuuluu tai jossa sen tukiasemat sijaitsevat.

Virransaannin rajoittaminen

Yksi mahdollisuus suojata verkko on sulkea tukiasema siksi ajaksi, kun sitä ei käytetä. Tukiaseman virtajohdon fyysinen irrottaminen usean tukiaseman langattomassa lähiverkossa on varsin työlästä. Siksi tulisikin miettiä muita vaihtoehtoja virransaamiseksi jo langattoman lähiverkon suunnitteluvaiheessa. Vaihtoehtona on IEEE:n 802.3af.standardin määrittelemä Power-over-Ethernet (PoE), jossa PoE-tukiasema saa virtansa RJ-

45 verkkoliittimen kautta. PoE tarjoaa keskitettyjä ratkaisuja PoE-tukiasemien virransaannin hallitsemiseksi (Geier 2002).

Tukiaseman kuuluvuuden rajoittaminen

Verkon suunnitteluvaiheessa kannattaa tutkia tarkkaan tukiasemien sijoituspaikkaa. Tällä voidaan merkittävästi rajoittaa tukiaseman signaalin kuulumista rakennuksen ulkopuolelle ja näin jo ennalta torjua salakuuntelua. Myös suunta-antennien käytöllä voidaan rajoittaa signaali kuuluumaan vain tietylle alueelle. Salakuuntelun lisäksi kuuluvuuden rajoittaminen estää verkon jumiuttamisen rakennuksen ulkopuolelta (Geier 2002).

5.6.2 Ohjelmallinen tietoturva

Ensimmäinen vaihe ohjelmallisessa tietoturvassa on tukiaseman oletusmääritysten poistaminen. Näihin kuuluvat mm. SSID-tunnukset, käyttäjät ja salasanat.

SSID-tunnus

SSID-tunnuksen vaihtaminen oletusarvoisesta toiseksi on tärkeätä. Yleensä sama valmistaja käyttää samaa tunnusta kaikissa tukiasemissaan. Jos tukiasema lähettää oletusarvoista tunnusta, voi hyökkääjä tästä päätellä tukiaseman muidenkin oletusasetusten olevan voimassa. Tämä kertoo heikosti suojatusta verkosta ja lisää hyökkääjän mielenkiintoa verkkoa kohtaan. Hyökkäyksen ensimmäinen vaihe on kokeilla oletusarvoisia käyttäjätunnuksia ja salasanoja.

Mikäli on mahdollista, tukiaseman SSID-tunnuksen lähettäminen kannattaa poistaa käytöstä tukiaseman hallintaohjelmalla. Tämä tekee verkon näkymättömäksi suurimmalle osalle kuunteluohjelmia ja tekee näin verkon osaltaan näkymättömäksi. SSID-tunnuksen voi kuvitella olevan heikko salasana, joka pysäyttää satunnaisen verkkojen kuuntelijan (Geier 2002).

Käyttäjien tunnistus WLAN-laitteita määriteltäessä

Langattoman lähiverkon tukiasemien laitehallintaa olisi syytä käyttää vain henkilökohtaisia käyttäjätunnuksia ja salasanoja. Tämä vaatii keksitettyä käyttäjätietokantaa ja lokikirjauksia, eikä ole aina mahdollista. Tukiasemien hallintasalasanat ja –tunnukset pitää muuttaa oletusarvoisista vaikeasti arvattaviksi, vahvoiksi salasanoiksi. Salasanaoja pitää myös vaihtaa määräajoin (Puska 2005, Geier 2002).

Laitteiden ohjelmapäivitykset

Langattoman lähiverkon laitteiden ohjelmapäivitykset pitää olla ajan tasalla. Tämä koskee niin tukiasemia kuin myös langattomia verkkokortte-

ja. Parhaiten tiedot päivityksistä saa seuraamalla valmistajien tietoturvatiedotteita. Tukiaseman ohjelmisto kannattaa päivittää ennen kuin sen ottaa käyttöön, sillä valmistajat julkaisevat päivityksiä varsin usein. Jo tukiasemia hankittaessa kannattaa varmistua siitä, että niiden ohjelmistot ovat päivitettävissä. Päivityksistä pitää tehdä jatkuva prosessi (Geier 2002).

Salatut yhteydet tukiaseman etähallintaan

Tukiasemaan etähallintaa tulee käyttää ainoastaan salattua HTTPS-yhteyttä. Telnet- ja HTTP-palvelut pitää poistaa verkkolaitteista, sillä ne lähettävät salasanat selväkielisinä. Hallintayhteydet voi myös rajoittaa tehtäväksi tietyistä IP-osoitteista. Ellei turvallista HTTPS-palvelua voida ottaa käyttöön, tulee etähallinta rajata vain lankaverkosta tapahtuvaksi (Puska 2005).

Verkon tarkkaileminen

Langattoman lähiverkon toimintaa tulee seurata jatkuvasti. Tarkkailulla varmistutaan siitä, että verkossa ei ole luvattomia laitteita. Verkon laitteiden toimintaa ja niiden konfigurointia seurataan käyttöön tarkoitetuilla ohjelmilla. Mikäli verkosta löytyy laite, jonka asetuksia on muutettu, on kyseessä mitä todennäköisimmin luvaton tukiasema tai luvallinen tukiasema, jonka asetuksia on menty luvattomasti muuttamaan. Mikäli tällaisia tukiasemia löytyy, on ryhdyttävä tilanteen vaatimiin korjaaviin toimenpiteisiin (Geier 2002).

Tunnistus- ja salausmenetelmät

Varmista, että tukiasemasi tukee uusimpia tunnistus- ja salausmenetelmiä ja ota ne käyttöön. Tunnistus- ja salausmenetelmät on selvitetty erikseen tässä työssä.

Tarpeettomien palveluiden poistaminen tukiasemista

Tukiasemien palvelut tulee käydä kriittisesti läpi ja poistaa käytöstä kaikki tarpeettomat palvelut. Tietoturvan kannalta erityisen kriittisiä ovat Telnet, TFTP, FTP ja SNMP-versiot 1 ja 2c, mutta kaikki tarpeettomat palvelut kannattaa poistaa (Puska 2005).

6 Kuuluvuusmittaukset

Kuuluvuusmittauksilla haluttiin määritellä tukiasemien paikat C- ja D-taloissa ja tutkia eri kanavien vaikutusta kuuluvuuteen. Kuuluvuusmittaukset tehtiin heinäkuun 2005 aikana. Ensin mitattiin kuuluvuus C-talossa, jonka jälkeen siirryttiin D-taloon. Mittausten tulokset kirjattiin erilliseen mittauspöytäkirjaan, josta tulokset myöhemmin syötettiin Excel-taulukkolaskentaohjelmaan.

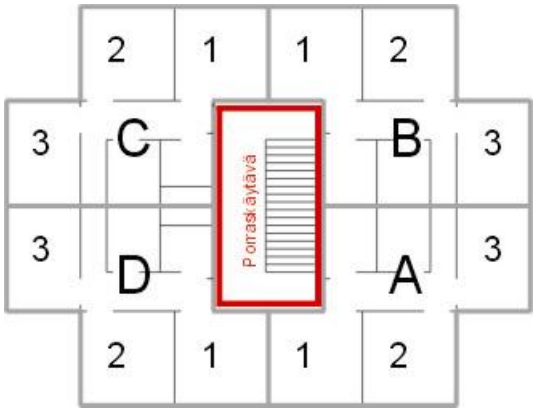
Tukiasemalle etsittiin paikka, joka vastaisi mahdollisimman hyvin lopullista sijoituspaikkaansa. Paikkaa etsittäessä kriteereinä olivat mm. keskeinen sijainti kerrokseen tai siipeen nähden sekä sähköpistokkeen läheisyys. Sijoittamalla tukiasema kerroksen keskelle haluttiin tutkia tilannetta, jossa yhdellä tukiasemalla voitaisiin kattaa yksi kerros. Mittaustilanteita varten tukiasema sijoitettiin väliaikaisesti seinälle ajateltuun lopulliseen sijoituspaikkaansa. Virta tukiasemalle tuotiin jatkojohdolla. Tukiasema konfiguroitiin RJ-45 verkkokaapelin kautta tai mittaustilanteessa langattomasti.

Kuuluvuusmittausten aikana ei ollut mahdollista ottaa langattoman lähiverkon kautta yhteyttä Internetiin tai testata yhteyttä sovellusten käytöllä. Näin ollen ainoaksi kuuluvuuden määrittelyksi jäi tilanne, jossa tukiasema voitiin konfiguroida langattomasti verkon yli. Tämä toimenpide käsitti tukiaseman kanavan vaihdon. Ne tilanteet, joissa kanavan vaihto langattomasti verkon yli ei ollut mahdollista, merkittiin kuuluvuustaulukkoon merkinnällä -.

Kuuluvuusmittauksissa kanavat 12 ja 13 eivät kuuluneet. Tietokonelehdessä 5/2003 julkaistun artikkelin "Katveet peittoon" mukaan kaikki PCMCIA-kortit eivät tue kanavia 12 ja 13. Ralink 2500-verkkokortin on PCI-väylään liitetty kortti, joten ongelman ei pitäisi koskea sitä. Asiaa pyrittiin selvittämään verkkokortin valmistajan kotisivuilta saamatta siihen vastausta. On syytä epäillä, että kyseinen verkkokortti ei tue kanavia 12 ja 13. Tämä siitä huolimatta, että kyseessä on PCI-väyläinen, eikä PCMCIA-kortti.

6.1 Mittaukset C-talossa

Mittauksia varten C-talo jaettiin neljään osaan huonejaon mukaisesti. Osat nimettiin A-, B-, C- ja D-asunnoiksi. Jako on esitetty kuvassa 12. Kaikissa asunnoissa on keittiön lisäksi kolme huonetta.



Kuva 12 C-talon huonejaon mukaiset osat

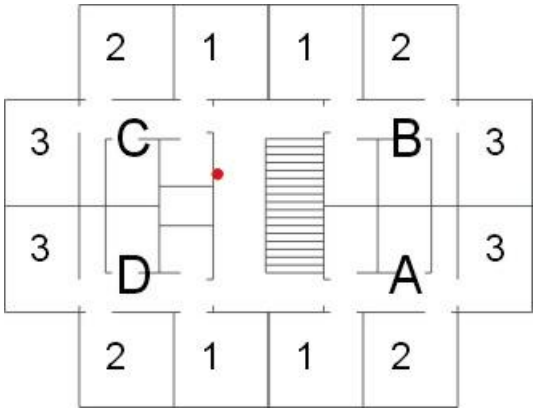
C-talossa tutkittiin ensimmäisenä vaihtoehtoa, jossa yhdellä tukiasemalla katettiin yksi kerros. Jos signaali kantaisi koko kerrokseen, ei toista mittaustilannetta lähdettäisi toteuttamaan. Siinä kahdella tukiasemalla katetaan yksi kerros.

Kuuluvuuden mittaaminen aloitettiin ensimmäisen kerroksen A asunnon huoneesta 3. Sen jälkeen tukiaseman kuuluvuus mitattiin kaikkien asuntojen huoneista. Jos tukiaseman signaali kuului koko kerrokseen, mitattiin kuuluvuus tukiaseman yläpuolella olevasta kerroksesta tarkoituksena kattaa yhdellä tukiasemalla kaksi kerrosta. Ennen varsinaisten mittausten aloittamista suoritettiin mittaus, jossa tutkittiin eri kanavien vaikutusta kuuluvuuteen.

6.1.1 Eri kanavien vaikutus kuuluvuuteen

Tukiaseman ollessa sijoitettuna porraskäytävään tutkittiin kahta seikkaa. Toisaalta haluttiin tutkia tilannetta, jossa yhdellä tukiasemalla voitaisiin kattaa yksi kerros, mutta haluttiin myös tutkia eri kanavien vaikutusta kuuluvuuteen. Tukiaseman paikaksi valittiin näin ollen mahdollisimman keskeinen paikka kerroksessa. Tukiasema sijoitettiin välittömästi hissin oven oikealle puolelle, kuten kuvasta 13 ilmenee. Kuvassa 14 on esitetty tukiaseman paikka C-talon ensimmäisen kerroksen pohjakuvassa.

Kuva 13 Tukiaseman sijoitus C-talon porraskäytävässä



Kuva 14 Tukiaseman sijoitus C-talon ensimmäisen kerroksen pohjakuvassa

Mittauspisteenä oli A-asunnon huone numero 3, sillä se on kauimmaisin huone tukiasemasta. Eri kanavien vaikutus kuuluvuuteen on esitetty taulukossa 6.

Taulukko 6 Eri kanavien kuuluvuus tukiaseman ollessa porraskäytävässä

Kanava	Taajuus (MHz)	Signaali (dBm)
1	2412	-66
2	2417	-68
3	2422	-72
4	2427	-73
5	2432	-71
6	2437	-69
7	2442	-68
8	2448	-69
9	2452	-69
10	2457	-69

11	2462	-72
12	2467	-
13	2472	-

Taulukosta havaitaan, että kanavat 1 – 2 ja 6 - 10 kuuluivat parhaiten. Kuuluvuus oli huonompi kanavilla 3 – 5 ja 11, mutta oli silti riittävä tukiaseman konfigurointiin. Kanavilla 12 ja 13 kuuluvuutta ei olut lainkaan.

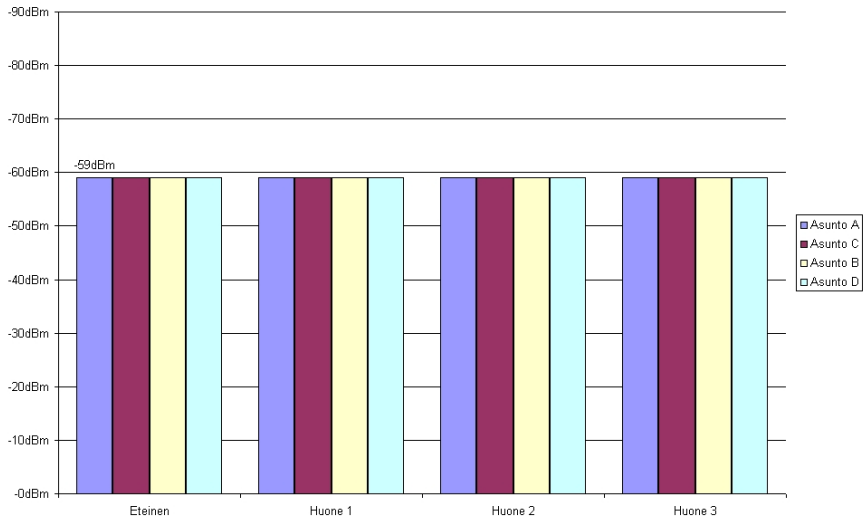
Edellisten mittausten perusteella testikanavaksi päätettiin valita kanava 4, sillä sen kuuluvuus oli ollut mittaustilanteessa heikoin. Ajateltiin, että jos kanava 4 kuuluisi kaikkiin huoneisiin, myös muut kanavat kuuluisivat. Päätettiin siirtyä huonekohtaisiin kuuluvuusmittauksiin.

6.1.2 Huonekohtaiset mittaukset

1. kerros

Huonekohtaisten mittausten alkaessa tukiaseman paikkaa ei vaihdettu, sillä haluttiin tutkia miten keskeisesti sijoitettu tukiasema kuuluisi koko kerrokseen. Tukiaseman kanavaksi oli edellisten mittausten tulosteella valittu kanava 4.

Kuuluvuus mitattiin ensin A asunnon eteisestä. Sen jälkeen mitattiin kuuluvuus huoneista kolme, kaksi ja yksi. Sen jälkeen edettiin aakkosjärjestyksessä muihin asuntoihin. Mittausten ajaksi huoneen ovi suljettiin ja odotettiin hetki ennen mittausten tekemistä. Näin siksi, että tilanne ehtisi normalisoitua ja oven kiinni pitäminen vastaisi mahdollisimman hyvin todellista tilannetta. Mittausten tulokset on esitetty oheisessa kuviossa.

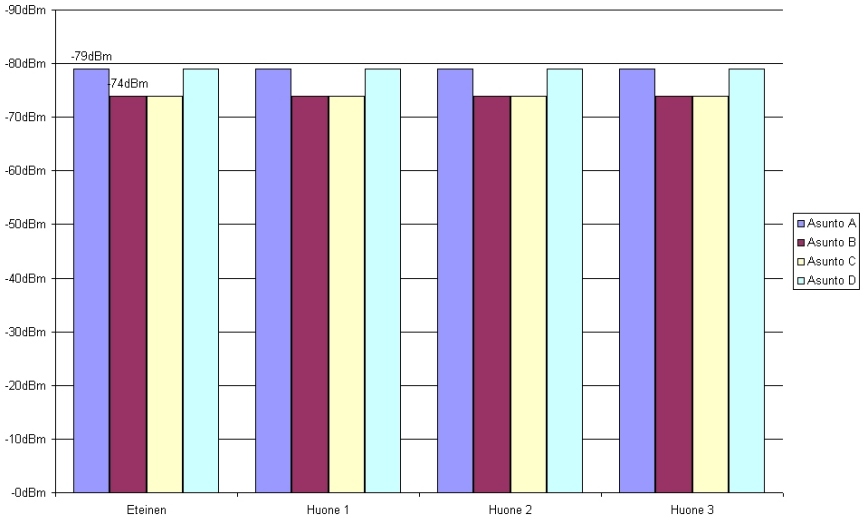


Kuvio 5 C-talo 1. kerros huonekohtainen kuuluvuus

Kuviosta 5 havaitaan, että kaikkien asuntojen kaikkiin huoneisiin signaali kuului tasaisen vahvana. Signaalin tiellä on samanlaiset esteet jokaiseen asuntoon ja jokaiseen huoneeseen, joten suurta eroa signaalin voimakkuuksien välillä ei ole.

2. kerros

Siirryttäessä mittaamaan signaalin kuuluvuutta 2. kerrokseen, ei tukiaseman paikkaa tai kanavaa muutettu. Mittausjärjestelyt olivat samat kuin mitattaessa 1. kerroksesta.



Kuvio 6 C-talo 2. kerros huonekohtainen kuuluvuus

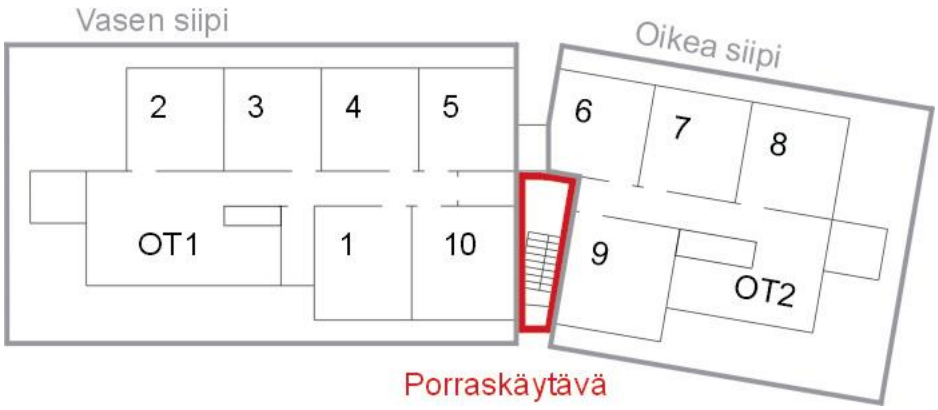
Toiseen kerrokseen signaali kuului vaihtelevasti. Signaalin tiellä on yksi lattia, joten sen vaimeneminen on luonnollista.

Kuviosta 6 nähdään, että asuntoihin A ja D signaali kuului yhtä voimakkaana –79 dBm. Myös asuntoihin B ja C signaali kuului niin ikään samansuuruisena (-74 dBm), mutta hieman paremmin kuin asuntoihin A ja D.

6.2 Mittaukset D-talossa

Mittauksia varten D-talo jaettiin kahteen siipeen, joiden jakajana porraskäytävä toimi. >Ensimmäisen kerroksen siipiratkaisu on esitetty kuvassa 15 ja toisen kerroksen siipijako kuvassa 16. Vasemmassa siivessä oleskelutilan lisäksi huoneita oli ensimmäisessä kerroksessa viisi ja muissa kerroksissa kuusi. Oikean siiven kaikissa kerroksissa huoneita on neljä ja oleskelutila.

Kuva 15 D-talon ensimmäisen kerroksen siipijako



Kuva 16 D-talon toisen kerroksen siipijako

D-talossa tutkittiin kahta tukiaseman sijoitustilannetta. Ensimmäisessä tilanteessa yhdellä tukiasemalla pyrittiin kattamaan koko kerros. Jos tämä ei toimisi eli tukiasema ei kuuluisi koko kerrokseen, toteutettaisiin toinen mittaustilanne. Siinä kerrosta kohden olisi kaksi tukiasemaa, joilla kummallakin pyrittiin kattamaan yksi siipi.

Mittaustilanteessa kuuluvuuden mittaaminen aloitettiin kauimmaisesta pisteestä tukiasemasta katsottuna, jotka olivat oleskelutiloissa OT1 ja OT2. Mikäli tukiasema kuului sijoituspaikastaan riippuen jompaankumpaan oleskelutilaan, edettiin mittauksissa asuinhuoneisiin. Huoneiden ovi oli suljettuna mittausten ajan. Ennen varsinaisten mittausten aloittamista suoritettiin mittaus, jossa tutkittiin eri kanavien vaikutusta kuuluvuuteen.

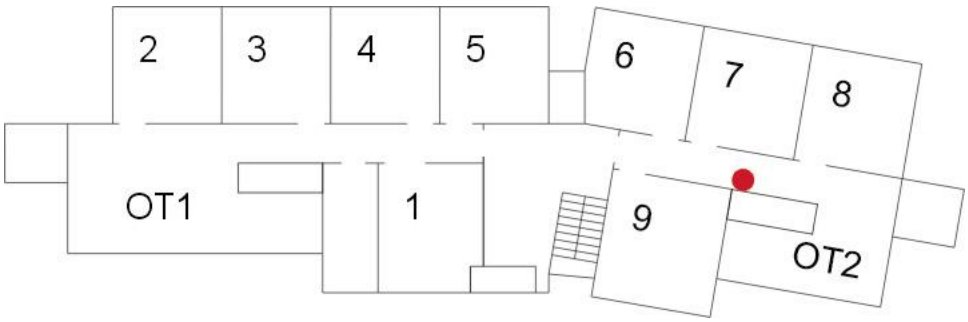
6.2.1 Eri kanavien vaikutus kuuluvuuteen

Aluksi haluttiin tutkia miten eri kanavat vaikuttavat kuuluvuuteen. Tukiasema sijoitettiin paikalleen ajateltuun sijoituspaikkaansa ja sen aloituskanavaksi asetettiin kanava 1. Tämä konfigurointi tehtiin verkkojohdolla. Sen jälkeen siirryttiin varsinaiseen mittauspisteeseen ja aloitettiin mittaukset.

Porraskäytävä – yksi tukiasema kerroksessa

Sijoitettaessa tukiasema porraskäytävään tutkittiin kahta seikkaa. Ensinnäkin haluttiin tutkia eri kanavien kuuluvuutta ja toiseksi haluttiin tutkia voidaanko yhdellä tukiasemalla kattaa koko kerros. Jälkimmäisen tapauksen tutkimiseksi tukiasema sijoitettiin porraskäytävään hissin oven oikealle puolelle (kuvat 17 ja 18).

Kuva 17 Tukiaseman sijoitus D-talon porraskäytävässä



Kuva 18 Tukiaseman sijoitus D-talon ensimmäisen kerroksen pohjakuvassa

Mittaukset aloitettiin vasemman siiven oleskelutilasta, joka on kauimmaisin mahdollinen mittauspiste tukiasemasta katsottuna. Mittauksen tulokset on esitetty taulukossa 7.

Taulukko 7 Eri kanavien kuuluvuus tukiaseman ollessa porraskäytävässä

Kanava	Taajuus (MHz)	Signaali (dBm)

1	2412	-80
2	2417	-77
3	2422	-80
4	2427	-
5	2432	-
6	2437	-
7	2442	-
8	2448	-
9	2452	-
10	2457	-
11	2462	-
12	2467	-
13	2472	

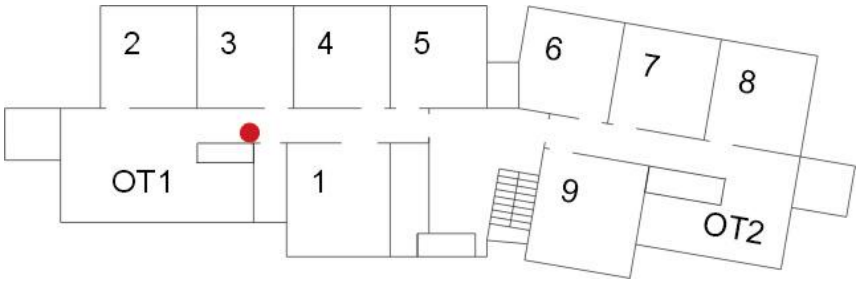
Taulukosta 7 ilmenee, että tukiasema ei kuulunut lainkaan vasemman siiven oleskelutilaan kanavasta neljä lähtien. Tosin aluksi tukiasema kuului heikosti em. kanavalla oleskelutilaan, mutta lakkasi lopulta kokonaan kuulumasta. Yhteys palasi hetkittäin, mutta katkesi taas jonkin ajan kuluttua. Tarkistusmittaus suoritettiin vielä vasemman siiven huoneesta kaksi, mutta sinne tukiasema ei kuulunut lainkaan.

Mittausten perusteella päätettiin hylätä ratkaisu, jossa yhdellä porraskäytävään sijoitetulla tukiasemalla katettaisiin koko kerros. Fyysisen tietoturvan osalta tämän sijoituspaikan haittapuolena olisi ollut tukiaseman sijoitus porraskäytävään varsin matalalle, joten siihen olisi päässyt liian helposti käsiksi.

Vasen siipi – kaksi tukiasemaa kerroksessa

Toisen mittauksen paikaksi valittiin vasen siipi. Valintaa päädyttiin siksi, että vasen siipi on isompi, jolloin tukiaseman signaalin pitää kuulua laajemmalle alueelle. Ajateltiin, että jos tukiasema kuuluisi isommassa siivessä, kuuluisi se myös pienemmässä siivessä. Tukiasema sijoitettiin käytävän keskivaiheille (kuva 19). Tukiaseman sijoitus pohjakuvassa on esitetty kuvassa 20.

Kuva 19 Tukiaseman sijoitus D-talon vasemman siiven käytävässä



Kuva 20 Tukiaseman sijoitus D-talon ensimmäisen kerroksen pohjakuvassa

Kuuluvuus varmistettiin aluksi oleskelutilasta OT1, mutta varsinaiset mittaukset suoritettiin huoneesta numero kaksi. Taulukko 8 kertoo eri kanavien vaikutuksen kuuluvuuteen.

Taulukko 8 Eri kanavien kuuluvuus tukiaseman ollessa vasemmassa siivessä

Kanava	Taajuus (MHz)	Signaali (dBm)
1	2412	-62
2	2417	-60
3	2422	-66
4	2427	-64
5	2432	-65
6	2437	-68
7	2442	-66
8	2448	-66
9	2452	-60
10	2457	-68
11	2462	-72
12	2467	-
13	2472	

Taulukosta 8 havaitaan, että kanavat 3 - 10 kuuluivat parhaiten. Huomattavaa kuitenkin on, että mentäessä korkeammalle taajuusalueelle (2462 MHz, kanava 11) kuuluvuus alkoi huonontua, mutta oli silti riittävä tukiaseman konfigurointiin. Lopulta testattaessa kuuluvuutta kanavilla 12 ja 13 ei sitä ollut lainkaan.

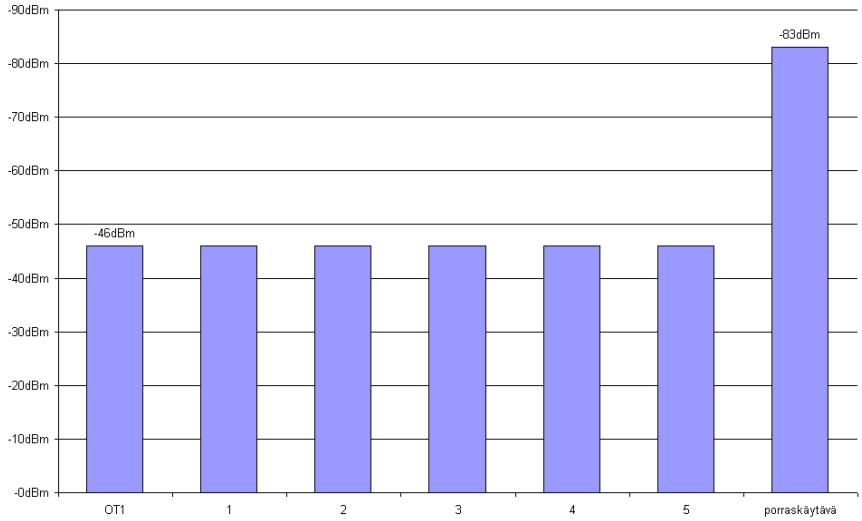
Edellisten mittausten perusteella testikanavaksi päätettiin valita kanava 11, sillä sen kuuluvuus oli ollut mittaustilanteessa heikoin. Ajateltiin, että jos kanava 11 kuuluisi kaikkiin huoneisiin, myös muut kanavat kuuluisivat. Päätettiin siis siirtyä mittauksissa seuraavaan vaiheeseen eli huonekohtaisiin mittauksiin.

6.2.2 Huonekohtaiset mittaukset

Vasen siipi 1. kerros

Huonekohtaisia mittauksia varten tukiasema pidettiin samalla paikalla, kuin mitattaessa eri kanavien vaikutusta vasemmassa siivessä. Huonekohtaisia kuuluvuusmittauksia varten kanavaksi oli edellisten mittausten tulosten perusteella valittu kanava 11.

Kuuluvuus mitattiin aluksi oleskelutilasta OT1, jonka jälkeen edettiin huone kerrallaan ja käytiin läpi koko siipi. Mittausten ajaksi huoneen ovi suljettiin ja odotettiin hetki, jotta tilanne ehtisi normalisoitua. Tämä siksi, että mittaustilanne vastaisi mahdollisimman hyvin todellista käyttötilannetta, jossa huoneen ovi on suljettuna. Mittausten tulokset on esitetty oheisessa kuviossa.

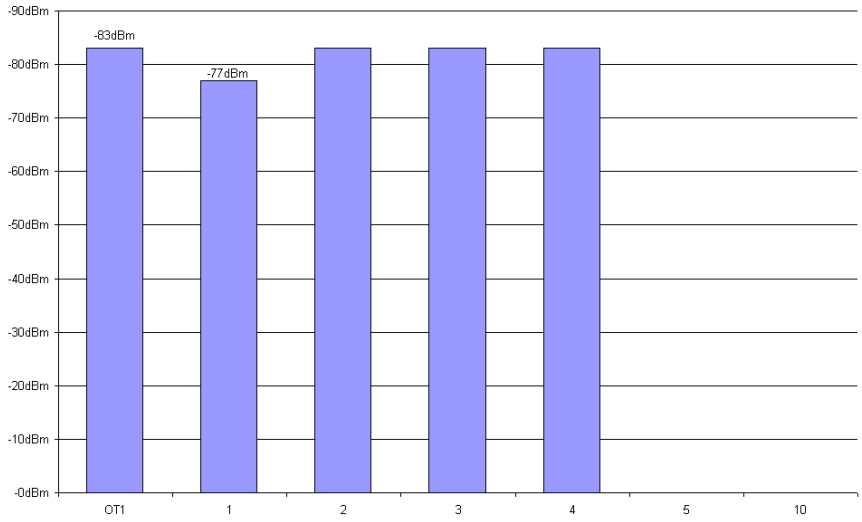


Kuvio 7 D-talo vasen siipi 1. kerros huonekohtainen kuuluvuus

Huoneisiin kuuluva signaali oli voimakkuudeltaan –46 dBm ja porraskäytävään kuuluva signaali oli –83 dBm. Kuviosta 7 nähdään, että huoneisiin kuuluva signaali oli varsin tasainen joka huoneessa, mutta porraskäytävästä mitattaessa signaali heikkeni heikoksi. Huoneista mitattaessa signaalin tiellä ei ollut varsinaisia kuuluvuutta voimakkaasti heikentäviä esteitä. Porraskäytävään kuuluvan signaalin tiellä oli mm. metallinen lasiovi, jossa lasin sisällä on metallikehikko.

Vasen siipi 2. kerros

Suunnitelmien mukaan seuraavat mittaukset tehtiin toisen kerroksen vasemmassa siivessä. Muuten mittausten lähtökohdat pidettiin samoina kuin aiemmassa tapauksessa.



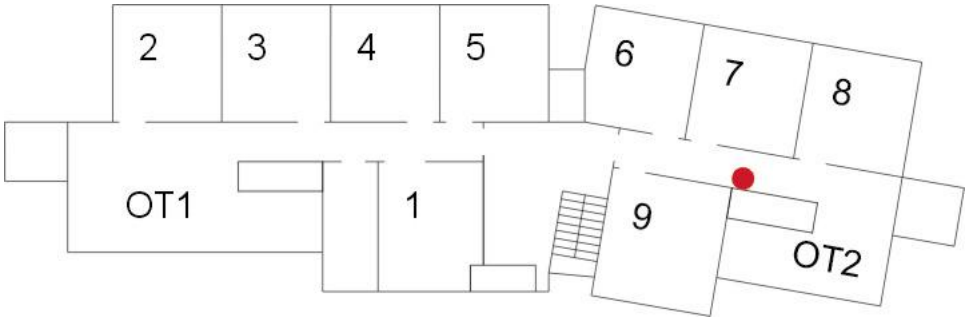
Kuvio 8 D-talo vasen siipi 2. kerros huonekohtainen kuuluvuus

Toisen kerroksen huoneisiin signaali kuului vaihtelevasti. Kuviosta 8 havaitaan, että suoraan tukiaseman yläpuolella oleviin huoneisiin (1, 2, 3 ja 4) signaali kuului. Huoneeseen 1 signaali kuului –77 dBm voimakkuudella, kun taas huoneisiin 2, 3 ja 4 signaali kuului –83 dBm voimakkuudella. Tukiasemasta kauimmaisena oleviin huoneisiin (5 ja 10) kuuluvuutta ei ollut lainkaan.

Oikea siipi 1. kerros

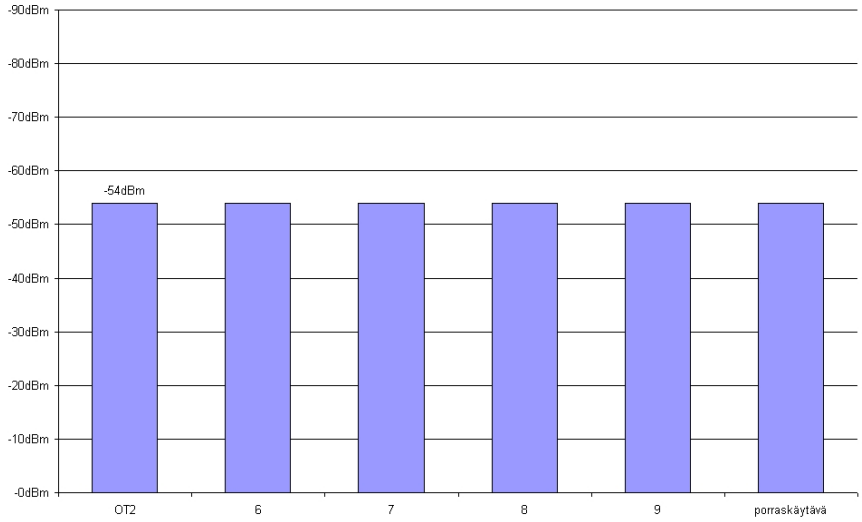
Oikean siiven huonekohtaisia mittauksia varten tukiaseman paikka vaihdettiin oikeaan siipeen vastaavaan paikkaan kuin vasemmassa siivessä (kuvat 21 ja 22). Mittauksia varten tukiasema oli edelleen kanavalla 11. Huoneiden ovet pidettiin mittausten aikana kiinni ja mittaus suoritettiin hetken huoneessa olon jälkeen, jotta tilanne ehtisi normalisoitua.

Kuva 21 Tukiaseman sijoitus D-talon oikean siiven käytävässä



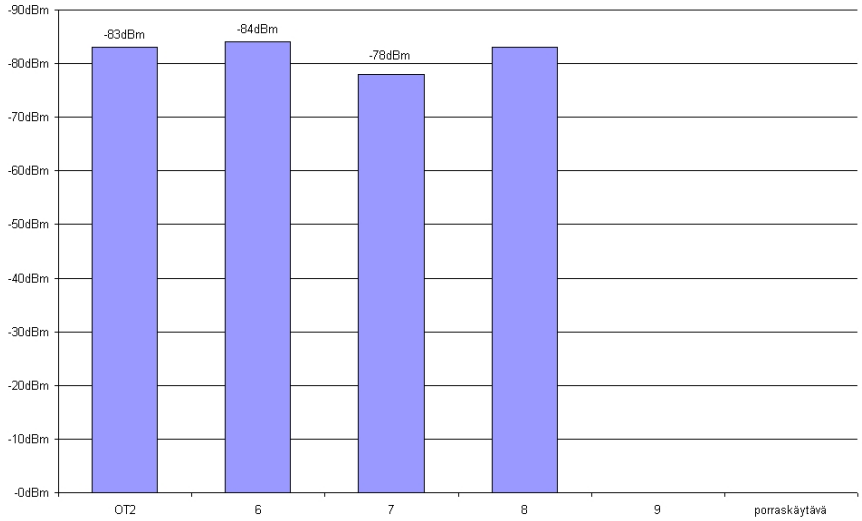
Kuva 22 Tukiaseman sijoitus D-talon ensimmäisen kerroksen pohjakuvassa

Signaali oli voimakkuudeltaan tasainen läpi koko siiven, myös porras-käytävään, vaikka signaalin tiellä oli samanlainen metallinen lasiovi kuin vasemmassa siivessä. Kuviossa 9 on esitetty kuuluvuus pylväsdiagram-mina.



Kuvio 9 D-talo oikea siipi 1. kerros huonekohtainen kuuluvuus

Seuraavaksi mitattiin kuuluvuus toiseen kerrokseen tukiaseman ollessa sijoitettuna samaan paikkaan, kuin aiemmassa mittauksessa. Tulokset on esitetty kuviossa 10. Signaali kuului heikosti (-82 dBm), mutta jatkuvasti ainoastaan oleskelutilaan OT2. Huoneisiin 6,7 ja 8 signaali välillä kuului ja välillä ei. Silloin kun se kuului voimakkuus oli väliltä –78 - -84 dBm. Huoneeseen 9 signaali ei kuulunut lainkaan.

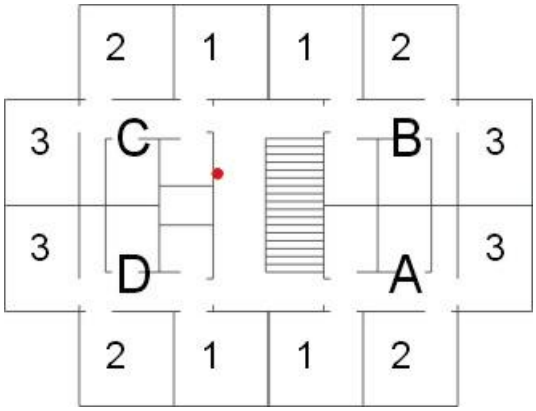


Kuvio 10 D-talo oikea siipi 2. kerros huonekohtainen kuuluvuus

7 Suunnitelma verkon toteuttamisesta

7.1 Tukiasemien määrä ja sijoitus C-talossa

Mittauksissa ilmeni, että yhdellä käytössä olleella keskeisesti sijoitetulla tukiasemalla voidaan kattaa luotettavasti vain yksi kerros. Sen signaali kuuluu riittävällä voimakkuudella koko kerroksen kaikkiin asuntoihin ja huoneisiin. Mittauksiin perustuva ja kaikkialle tasaisen kuuluvuuden takaava sijoituspaikka on esitetty kuvassa 23.



Kuva 23 Tukiaseman paikka C-talossa

Mittauksissa signaalin voimakkuus oli –59 dBm. Taulukon 5 mukaisesti huoneisiin kuuluva signaali on kykenevä 802.11g-standardin mukaiseen maksimitiedonsiirtonopeuteen, joka on 54 Mbps. Tosin tämä on laskennallinen maksiminopeus ja todellinen on siitä noin 40 %. Näin ollen tiedonsiirtonopeus olisi noin 22 Mbps.

Mitattaessa kuuluvuutta toiseen kerrokseen signaalin voimakkuus oli asunnoissa A ja D –79 dBm ja asunnoissa B ja C –74 dBm. Taulukon 5 mukaan laskennalliset tiedonsiirtonopeudet olisivat vastaavasti noin 24 Mbps ja 36 Mbps. Todelliset nopeudet olisivat noin 10 Mbps ja 14 Mbps. Toisen kerroksen tiedonsiirtonopeus olisi noin puolet ensimmäisen kerroksen vastaavasta, joten ajatus siitä, että yhdellä tukiasemalla katetaan kaksi kerrosta, päätettiin hylätä.

7.2 C-talossa käytettävät kanavat

Mittauksissa kävi myös ilmi, ettei alempaan kerrokseen sijoitettu tukiasema kuulu riittävän hyvin ylempään kerrokseen. Näin ollen joka kerrokseen pitää sijoittaa yksi tukiasema. Tukiasemien sijoittelussa pitää ottaa huomioon päällekkäisten kanavien aiheuttamat häiriöt.

Kun muistetaan se seikka, etteivät kaikki langattoman lähiverkon PCMCIA-kortit tue kanavia 12 ja 13, viisainta olisi jättää ne käyttämättä.

Näin ollen käytössä on 11 kanavaa. Jotta kanavien väliin saadaan riittävästi vapaata kaistaa, kolmen kanavan mallissa on käytössä kanavat 1, 6 ja 11. Ensimmäisen kerroksen tukiaseman kanavaksi valitaan kanava 1, toisen kerroksen kanava 6 ja kolmannen kerroksen kanava 11. Neljännessä kerroksessa kierros aloitetaan uudelleen kanavalla 1 jne. Näin samojen kanavien välille saadaan kaksi kerrosta. Kerrokset ja ehdotus niissä käytettäviksi kanaviksi on esitetty taulukossa 9.

Taulukko 9 Kerroskohtainen kanavajako kolmella kanavalla

Kerros	Kanava
1	1
2	6
3	11
4	1
5	6
6	11

Käytettäessä neljää kanavaa kolmen sijaan, saadaan kanavien välille vielä lisää kaistaa ja samalla saadaan lisää kanavia käyttöön. Käytössä on silloin kanavat 1, 4, 7 ja 11. Silloin kanavien välille saadaan kolme kerrosta, jolloin mahdollisuus siihen, että kanavat häiritsisivät toisiaan, pienenee entisestään. Kerrokset ja ehdotus niissä käytettäviksi kanaviksi on esitetty taulukossa 10.

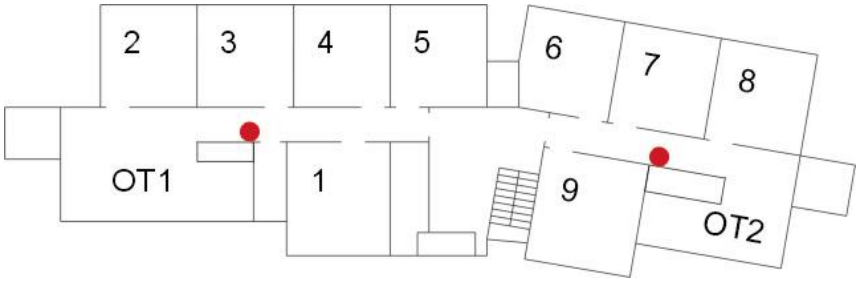
Taulukko 10 Kerroskohtainen kanavajako neljällä kanavalla

Kerros	Kanava
1	1
2	7
3	4
4	11
5	1
6	7

Neljän kanavan ratkaisu on suositeltavin, sillä sen käytöllä saadaan riittävästi kanavia käyttöön, mutta myös tilaa niiden väliin. Luonnollisesti asiasta saadaan täysi varmuus vasta, kun jokaisessa kerroksessa on oma tukiasemansa ja voidaan suorittaa lopullinen mittaus.

7.3 Tukiasemien määrä ja sijoitus D-talossa

Mittauksissa selvisi, ettei yhdellä tukiasemalla voi kattaa luotettavasti yhtä kerrosta D-talossa, vaan se vaatii kaksi tukiasemaa, joiden signaalit kattavat oman sijoitussiipensä. Mittauksiin perustuvat ja tasaisen kuuluvuuden takaavat sijoituspaikat on esitetty kuvassa 24.



Kuva 24 Tukiasemien paikat D-talon 1. kerroksessa

Vasemman siiven huoneisiin kuuluva signaali oli voimakkuudeltaan –46 dBm ja porraskäytävään kuuluva signaali oli –83 dBm. Taulukon 5 mukaisesti huoneissa kuuluva signaali on kykenevä 802.11g-standardin mukaiseen maksimitiedonsiirtonopeuteen eli 54 Mbps. Porraskäytävässä tiedonsiirtonopeus olisi noin 11 – 12 Mbps. On muistettava, että em. arvoista puhuttaessa puhtaan laskennallisista arvoista. Todellinen tiedonsiirtonopeus huoneissa olisi noin 22 Mbps.

Oikean siiven huoneisiin ja porraskäytävään kuuluva signaali oli voimakkuudeltaan tasainen –54 dBm. Laskennallinen tiedonsiirtonopeus oikean siiven huoneissa olisi noin maksimi eli 54 Mbps, mutta todellinen noin 11 – 12 Mbps.

Tukiaseman signaali ei kuulunut kaikkiin toisen kerroksen huoneisiin, joten ajatus yhden tukiaseman kuulumisesta vasemman siiven kahteen kerrokseen päätettiin hylätä. Myös kuuluvuus oikean siiven alemmasta kerroksesta ylempään kerrokseen ei ollut moitteeton. Tukiasema ei kuulunut kaikkiin huoneisiin, joten päätettiin tehdä sama ratkaisu kuin edellä ja hylätä oikean siiven kattaminen yhdellä tukiasemalla.

7.4 D-talossa käytettävät kanavat

D-talo on kanavien suhteen kriittisempi kuin C-talo, sillä kerrosta kohden tarvitaan kaksi tukiasemaa. Ne voivat häiritä toisiaan, ellei niiden välille saada riittävästi kaistaa. Tilannetta mutkistaa edelleen se tosiasia, että käytössä on vain 11 kanavaa 13 kanavan sijaan. Jos päätetään käyttää kolmea kanavaa, joudutaan tilanteeseen, jossa sama kanava on käytössä jo seuraavassa kerroksessa, mutta toki eri siivessä. Tästä voi aiheutua häiriöitä. Taulukossa 11 on esitetty kanavajako kolmea kanavaa käytettäessä.

Taulukko 11 Kerroskohtainen kanavajako kolmella kanavalla

Kerros	Kanava	
	Vasen siipi	Oikea siipi
1	1	11
2	11	6
3	6	1
4	1	11
5	11	6

Neljää kanavaa käytettäessä tilanne paranee ja samojen kanavien väliin saadaan yksi kerros. Tilannetta parantaa vielä se, että jo aiemmin käytetty kanava on eri siivessä. Taulukossa 12 on esitetty kanavajako neljää kanavaa käytettäessä.

Taulukko 12 Kerroskohtainen kanavajako neljällä kanavalla

Kerros	Kanava	
	Vasen siipi	Oikea siipi
1	1	7
2	4	11
3	7	1
4	11	4
5	1	7

D-talon kohdalla suositeltavin ratkaisu on myös neljän kanavan ratkaisusta samoista syistä kuin C-talossa. Kanavien kuuluvuus ja mahdolliset häiriöt pitää varmistaa kun jokaisessa kerroksessa on oma tukiasemansa.

8 Ehdotuksia verkon toteuttamiseksi

Lopullista verkkoa toteutettaessa on otettava huomioon monia eri seikkoja. Tässä luvussa on esitetty oleellisimmat huomioitavat seikat, joista kustakin on esitetty tärkeimmät huomioitavat asiat. Luettelon tarkoituksena on toimia suuntaa-antavana muistilistana lopullista verkkoa suunniteltaessa ja toteutusta mietittäessä.

8.1 Verkon topologia

Verkon topologia tulee olemaan tyypiltään Extended Service Set (ESS), sillä siinä on useita tukiasemia, jotka kaikki on kytketty runkoverkkoon. Kerroksissa olevilta tukiasemilta lähtevät kaapeloinnit kootaan yhteen siihen varatussa tilassa kussakin talossa. Tästä tilasta on yhteys kuitukaapelia pitkin päärakennukseen. Päärakennuksessa tarkoitusta varten varatussa tilassa kootaan yhteen kaikista asuntoloista tulevat kuitukaapelit. Tästä tilasta on yhteys internetpalveluntarjoajan kautta Internetiin.

8.2 Verkon hallinta

Verkon hallinta oppilaitosympäristössä useine ja säännöllisesti vaihtuvine käyttäjineen on jatkuva prosessi. Pahimmillaan se työllistää yhden ihmisen lähes kokopäivätoimisesti, joten verkon hallinnan suunnitteluun on syytä paneutua hyvin jo verkon suunnitteluvaiheessa. Suunnittelussa on pyrittävä siihen, että verkon hallinta on pitkälle automatisoitu prosessi, joka voidaan hoitaa muiden töiden ohella mahdollisimman pienellä vaivalla. Verkon hallinta voidaan hoitaa itsenäisesti tai se voidaan ulkoistaa sopivalle taholle. Molemmissa tapauksissa on hyvät ja huonot puolensa.

Verkon hallinta voidaan jakaa kahteen osaan, jotka ovat käyttäjien hallinta ja verkon laitteiden hallinta. Verkon laitteiden hallinta voidaan puolestaan jakaa vielä kahteen osaan eli tukiasemien hallintaan ja verkkoon liitettävien tietokoneiden hallintaan.

8.2.1 Sisäinen hallinta

Tässä tapauksessa verkko hallitaan sisäisesti Poliisikoulun tietohallinnon toimesta. Tämä vaatii erillisen palvelimen, jossa on hallintaan tarkoitettu sovellus. Koko verkko hallitaan keskitetysti yhdeltä palvelimelta. Palvelimen lisäksi on syytä olla palomuuri, joka torjuu perinteisen verkon kautta tulevat asiattomat käyttäjät. Palomuuri voi olla ohjelmallinen tai se voi olla oma laitteensa.

Paras ratkaisu on se, jossa verkon hallinta hoidetaan itse, sillä silloin tietämys asioista on tietohallinnon henkilökunnalla ja vasteaika ongelmatilanteissa on pienempi, kuin otettaessa hallinta ulkopuoliselta. Lisäksi opiskelijat ovat tietokoneisiin liittyvissä ongelmatilanteissa tottuneet ottamaan yhteyttä tietohallintoon, joten toiminta verkon ongelmatilanteissa ei muuttuisi aiemmista tilanteista.

8.2.2 Ulkoistettu hallinta

Vaihtoehtona on myös verkon hallinnan ulkoistaminen. Eri Internet operaattoreilta todennäköisesti löytyy tähän sopivia vaihtoehtoja, joihin pitää tutustua perinpohjaisesti verkko toteutettaessa. Yksi harkittava vaihtoehto voisi olla ulkoistaa verkon hallinta sellaiseen erikoistuneelle taholle. Esimerkkinä tästä TOASnet, joka hoitaa Tampereen seudun opiskelija-asuntosäätiön (TOAS) opiskelija-asuntoloiden tietoliikenneverkkoa. Tiedossa ei ole tarjoaako TOASnet vastaavia palveluja muille tahoille, mutta asia kannattaa selvittää verkon suunnitteluvaiheessa.

8.2.3 Käyttäjien hallinta

Verkon käyttäjien hallinta on asia, jota tulee pohtia erityisen tarkasti. Mietittäviä asioita ovat mm. käyttäjän lisääminen verkkoon, käyttäjätunnusten ja salasanojen jakaminen, niiden voimassaolo ja salasanapolitiikka.

Verkko on muusta Poliisikoulun verkosta erillään oleva verkko, jonne pitää olla omat käyttäjätunnukset ja salasanat. Missään tapauksessa käyttäjätunnukset eivät saa olla samoja, joilla kirjaudutaan koulun verkkoon. Käyttäjätunnukset ja salasanat pitää kuitenkin luoda jossain keskitetysti ja jakaa verkon käyttäjille. Niiden voimassaolo tulee olla rajattu, sillä opiskelijat vaihtuvat asuntoloissa säännöllisin väliajoin. Käyttäjätunnukset ja salasanat voisivat lakata olemasta voimassa esimerkiksi samana päivänä, kun opiskelija poistuu koulusta.

Toisaalta salasanapolitiikka pitää olla vahva, eikä ns. ”heikkoja” salasanoja saa verkossa hyväksyä. Tämä pakottaa siihen, että salasanat luodaan käyttäjien puolesta, eikä käyttäjä voi muuttaa salasanaa itse. Varsin usein käyttäjä luo itse helpon käyttäjätunnuksen ja salasanan. Jos käyttäjille annetaan mahdollisuus salasanojen muuttamiseen, tulee salasanan täyttää tietyt vaatimukset, eikä vanhoja salasanoja saa toistaa.

Parasta olisi, mikäli käyttäjien hallinta toteutettaisiin ohjelmallisesti mahdollisimman yksinkertaisesti. Ohjelma loisi käyttäjätunnukset ja salasanat automaattisesti ja ne jaettaisiin verkon käyttäjille tarpeen mukaan. Ohjelmassa voitaisiin määrittää vaatimukset salasanoille ja käyttäjätunnuksille.

8.2.4 Verkon laitteiden hallinta

Tukiasemat

Verkon tukiasemien hallintaan on kaksi mahdollisuutta. Ensimmäinen vaihtoehto verkon hallintaan on tehdä hallinta tukiasemien ohjelmien kautta. Tämä on kuitenkin hyvin aikaa vievää, sillä tukiasemia tullee lopullisessa verkossa olemaan kaikkiaan 58 kappaletta. Tämän määrän hallinnointi on lähes kokopäiväistä työtä, sillä tukiasemat pitää hallinnoida yksi kerrallaan, mikä on vaivalloista ja työlästä. Tosin hallinnointi voidaan tehdä etätyönä omalta tietokoneelta, mutta se on silti työlästä.

Toinen mahdollisuus on hallita verkon laitteita keskitetysti tarkoitukseen tehdyllä ohjelmalla. Laitevalmistajilta löytyy tähän tarkoitukseen tehtyjä ohjelmia, joilla voidaan hallita kyseisen valmistajan laitteita keskitetysti. Asiaan pitää ja kannattaa perehtyä tarkemmin tukiasemia valitessa. Huomattava on, että edellä mainitut ohjelmat mahdollistavat ainoastaan tukiasemien keskitetyn hallinnan, eivät esimerkiksi verkkoon liitettävien tietokoneiden hallintaa.

Verkon tietokoneiden hallinta

Toinen varsin mittava työ verkkoon liittyen, on siihen liitettävien tietokoneiden hallinta eli verkkoon liittäminen. Verkko toimii kuitenkin oppilaitosympäristössä, jossa opiskelijat ja tietokoneet vaihtuvat säännöllisin väliajoin. Myös tämä vaihe tulee olla mahdollisimman pitkälle automatisoitu. Suotavaa olisi, että verkon käyttäjä voisi itse liittää laitteensa tietoturvallisesti verkkoon, ilman erityisosaamista. Liittymisen yhteydessä tulisi ottaa automaattisesti käyttöön uusimmat mahdolliset salausprotokollat ja tiukimmat mahdolliset tietoturva-asetukset ilman, että käyttäjän tulee sitä tehdä.

8.3 Verkon hallintaohjelma

Tamperelaisella Atific Oy:llä on valmis ratkaisu verkon keskitettyyn hallintaan ja moneen muuhun tässä esitettyyn ongelmaan. Atific Oy on suunnitellut ja kehittänyt Easy Access WLAN-nimisen ohjelman, joka on tarkoitettu WLAN-verkkojen suunnitteluun ja hallintaan. Ohjelma on varsin monipuolinen ja siinä on monia erilaisia ominaisuuksia. Kaikki ominaisuudet ovat tärkeitä, mutta yksi tärkeimmistä on automatisoidut verkko- ja turvallisuusasetukset. Se ottaa käyttöön vahvan liikenteen salauksen ilman erillistä konfigurointia tai salausavainten manuaalista asettamista.

Atific Oy:n ohjelmassa on mahdollisuus palvelunlaaduntakaamiseen tietyille sovelluksille. Toisin sanoen ohjelmalla voidaan suosia tiettyjä sovelluksia (esim. VoIP-puhelut). Erilaiset sovellukset voidaan siis eriar-

voistaa ja toisille taata isompi osuus käytettävissä olevasta kaistasta. Kaistan määrittelyjä voidaan tehdä paitsi sovelluskohtaisesti myös käyttäjä- tai ryhmäkohtaisesti. Ohjelmassa on myös palomuuri, jolla voidaan estää luvattomien palveluiden käyttö (esim. P2P), sekä haittaohjelmien ja virusten levittäminen.

Lisäksi Atific Oy:n ohjelmassa on keskitetty käyttäjienhallinta, jolla käyttäjätunnukset ja salasanat voidaan luoda automaattisesti. Salasanoille voidaan antaa tiettyjä parametreja, jotka sen on täytettävä ennen kuin se luodaan. Ohjelmassa on myös vahvat salausprotokollat (TKIP, AES, VPN), jolla estetään verkon liikenteen salakuuntelu mahdollisimman hyvin. Ohjelmassa on myös mahdollisuus verkon laitteen autentikointiin uusimmilla tunnistustekniikoilla.

Atific Oy:n ohjelma on hyvä ratkaisu verkon hallintaan, sillä siinä on kaikki ne ominaisuudet, joita verkon hallintaan tarkoitetulle ohjelmalle on asetettu. Verkon suunnitteluvaiheessa Atific Oy:ltä pitää pyytää tarjous ohjelmasta, kunhan heille ensin on selvitetty, mitä vaatimuksia ohjelmaan kohtaan on ja mitä sen tulisi tehdä.

8.4 Verkon laitteet

8.4.1 Palvelin

Mikäli päädytään vaihtoehtoon, jossa verkkoa hallitaan itse erillisellä ohjelmalla, tarvitaan siihen oma palvelimensa. Tämä palvelin ei saa olla mitenkään yhteydessä poliisin verkkoon. Palvelimelle asetettavat vaatimukset tehon ja suorituskyvyn puitteissa tulee selvittää tarkasti verkon suunnitteluvaiheessa.

8.4.2 Tukiasemat

Kuuluvuusmittausten aikana käytettävissä ollut tukiasema oli tehty pienyritys – ja kotikäyttöön, eikä näin ollen liene sopiva lopulliseen tarkoitukseen. Lähes kaikilta isoimmilta valmistajilta (Cisco, ZyXEL yms.) on saatavilla myös yrityskäyttöön tarkoitettuja tukiasemia. Verkon suunnitteluvaiheessa tulee valita kultakin valmistajalta tietyt kriteerit täyttävä yrityskäyttöön tarkoitettu tukiasema ja testata sen sopivuus tarkoitukseensa. Kriteereinä tukiasemaa mietittäessä voisi mielestäni pitää mm. seuraavia asioita:

- Fyysinen suojaus
- Power over Ethernet-valmius
- Tuetut autentikointi- ja salausmenetelmät
- Tuetut standardit

- Kestävyys

Muiden ominaisuuksiensa lisäksi yrityskäyttöön tarkoitetut tukiasemat voivat tarjota myös keskitettyä hallintaa, joka helpottaa hallinnasta aiheutuvaa työtä.

8.4.3 Tukiasemien virransaanti

Lopullisten tukiasemien valintavaiheessa yksi tärkeä kriteeri tulee olla tukiaseman valmius virransaantiin RJ-45 verkkoliittimen kautta. Lähes kaikilla valmistajilla alkaa olla valikoimissaan PoE-laitteita (Power over Ethernet). Näitä käytettäessä ei tarvita erillistä sähköpistoketta verkkovirralle muuntajineen, vaan tukiaseman saa virtansa jakamokaapista. Lisäksi PoE tarjoaa keskitettyjä ratkaisuja virranhallintaan, joten tukiasemat voidaan sen kautta sammuttaa tietyiksi ajoiksi. PoE-ratkaisussa säästytään erillisten sähköjohtojen vetämiseltä, mikä tuo osaltaan hieman säästöä verkon työkustannuksiin.

8.4.4 Verkon muut laitteet

Verkkoon tarvitaan palvelimen ja tukiasemien lisäksi muitakin laitteita. Näitä voivat olla esimerkiksi reitittimet, joilla kootaan tukiasemilta tulevat verkkojohdot yhteen. Lisäksi tarvittaneen kuituoptisia laitteita sekä asuntoloihin että päätaloon.

8.5 Verkon toteutus

8.5.1 Talojen kaapelointi

Kaikista taloista johtaa kuitukaapeli päärakennukseen, joten yhteydet päätalosta asuntoloihin ovat kunnossa. Asuntoloissa ei ole kuitenkaan minkäänlaista kaapelointia verkkoa varten, joten tukiasemille tulee järjestää kaapelointi verkkoyhteyksiä varten. Käytännössä tämä tarkoittaa sitä, että tilasta johon verkon muut laitteet sijoitetaan, tulee järjestää kaapelointi eri kerroksiin jokaiselle tukiasemalle. Työ on varsin mittava ja aiheuttaa todennäköisesti ison osan verkon rakennuskustannuksista.

8.5.2 Verkon muiden laitteiden sijoittaminen

Tukiasemien lisäksi langattomaan lähiverkkoon tarvitaan muitakin laitteita. Myös niiden sijoittaminen tulee miettiä verkon suunnitteluvaiheessa. D-talossa ja muissa samantyyppisissä taloissa laitteet voitaneen sijoittaa ensimmäisen kerroksen varastohuoneeseen, jonka oven voi lukita. C-

talossa ja muissa vastaavissa laitteet voitaneen sijoittaa pohjakerroksen kellari- ja varastotiloihin. Molemmissa taloissa laitekaappien tulee olla lukittavia sen lisäksi, että ne ovat lukittujen ovien takana.

8.5.3 Kustannukset

Kustannuksista on tässä yhteydessä vaikea antaa mitään arvioita. Yksistään tukiasemia tarvitaan useita kymmeniä, joten jo ne muodostavat oman kustannuseränsä. Lisänä tulevat vielä esimerkiksi kaapelit, rasiat, jakamokaapit, kotelot tukiasemille ynnä muut sellaiset. Työkustannukset muodostavat oman osansa verkon kustannuksista, joita on lähes mahdoton arvioida ilman erillistä tarjouspyyntöä urakoitsijoilta.

8.5.4 Verkon dokumentointi

Verkko pitää jo suunnitteluvaiheessa dokumentoida hyvin. Tukiasemien paikat tulee merkitä piirustuksiin, jotta ne löydetään helposti tarvittaessa. Niiden asetuksista tulee ottaa tulostukset, joita säilytetään yhdessä verkon muiden dokumenttien kanssa turvallisessa paikassa. Asetukset voi myös tallentaa sähköisesti riippuen tukiaseman ominaisuuksista.

Verkon laitteista pitää myös luoda erillinen lista, josta selviää mm. laitteen tyyppi, käyttötarkoitus, sijoituspaikka, sarjanumero, takuuaika, ostopäivä ja niin edelleen. Laitelistan tarkoituksena on helpottaa verkon laitteiden hallintaa esimerkiksi niiden rikkoontuessa.

8.5.5 Fyysinen tietoturva

Tukiasemat asennetaan julkisiin tiloihin, joihin johtava ovi on lukittu. Toisin sanoen asiattomat eivät pääse näihin tiloihin, ainoastaan opiskelijat ja henkilökunta. Siitäkin huolimatta tukiasemat tulee piilottaa katseilta mahdollisuuksien mukaan.

Valitettavasti kummassakaan talossa ei ole alaslaskettua kattoa, jonka suojiin tukiasemat voisi asentaa. Ainoaksi vaihtoehdoksi jää tukiasemien sijoittaminen lukittavaan tai ainakin hankalasti avattavaan muovikoteloon. Muovikotelo ei estä signaalin kuulumista juurikaan, mutta tarjoaa näkösuojan tukiasemalle. Samalla tukiaseman liittimet ja kytkimet ovat piilossa ja poissa ulottuvilta.

Tukiasemat tulee sijoittaa mahdollisimman ylös maasta, jotta niihin on vaikea päästä käsiksi. Mitään minimikorkeutta on vaikea antaa, mutta tukiaseman muovikoteloineen tulisi sijaita mahdollisimman lähellä katonrajaa ja olla näin vaikeasti saavutettavissa. Verkon johdot joudutaan vetämään pinta-asennuksena, jolloin ne jäävät näkyville. Johdot tulee suoja-

ta esim. johtokouruilla, jolloin ne eivät herätä niin paljoa huomiota, kuin ollessaan paljaina.

Kaikki verkon laitteet tulee sijoittaa lukittuihin tiloihin tai lukittaviin kaappeihin. Ovet tulee pitää lukittuina kaiken aikaa ja avaimia ei ole syytä jakaa tarpeettomasti.

8.5.6 Verkon käyttöönotto

Riippumatta siitä, että toteutetaanko verkko kaikkiin taloihin kerralla vai vain osaan, pitää verkko ottaa käyttöön vaiheittain. Käyttöönottokokeilu voisi tapahtua esimerkiksi C- ja G-taloissa, sillä niiden käyttäjistä osa on henkilökuntaa. Periaatteena on, että ensin testataan verkkoa rajoitetusti pienellä käyttäjäkunnalla, tutkitaan sen toimintaa, kehitetään sitä ja korjataan verkossa havaittuja ongelmia. Verkon testaukseen tarkoitettuja ohjelmia on saatavilla laitevalmistajilta, joilla voidaan myös selvittää verkon todellinen tiedonsiirtokapasiteetti. Lopullinen lanseeraus tehdään perusteellisen testauksen jälkeen.

8.6 Verkon käyttöpolitiikka

Jo suunnitteluvaiheessa on syytä miettiä mitä sallitaan ja mitä ei. Toisin sanoen pitää miettiä sallitaanko vertaisverkko-ohjelmien (peer-to-peer, P2P) käyttö vai ei. Rajusti verkon resursseja varaavien ohjelmien (esimerkiksi P2P) käyttö pitää kieltää, sillä se aiheuttaa verkon tukkoisuutta ja pahimmassa tapauksessa verkon käyttämättömyyden. Verkon käyttäjät ovat eri asemassa, sillä tehokäyttäjä voi omilla toimillaan rajoittaa tavallisen käyttäjän mahdollisuuksia verkon käyttöön. Lisäksi vertaisverkko-ohjelmat eivät luonteensa vuoksi sovi Poliisikoulun opiskelija-asuntoloissa käytettäviksi, sillä niihin liittyy varsin usein piratismi.

9 Johtopäätökset

Opinnäytetyöhön liittyviä tavoitteita oli kaksi. Ensimmäinen oli langattoman lähiverkon suunnittelu Poliisikoulun opiskelija-asuntoloihin, jossa paino oli kuuluvuusmittauksiin perustuvilla tukiasemien paikkojen määrittelyllä ja kanavien vaikutuksella kuuluvuuteen. Toinen tavoite oli tausta- ja teoriatiedon kerääminen Poliisikoulun tietohallinnon käyttöön mahdollisen myöhemmän toteutuksen tueksi.

Tukiasemien paikat määriteltiin kuuluvuusmittausten avulla samoin kuin eri kanavien vaikutus kuuluvuuteen. Kuuluvuusmittausten tulokset ja analyysi tukiasemien määrästä ja paikoista on esitetty opinnäytetyön tässä luvussa. Tulokset eri kanavien vaikutuksesta kuuluvuuteen on esitetty luvussa kuusi, sillä niiden perusteella valittiin kuuluvuusmittauksissa käytetty tukiaseman kanava. Näin ollen voidaan todeta, että tämä opinnäytetyölle asetettu tavoite saavutettiin.

Toista asetettua tavoitetta, tausta- ja teoriatiedon keräämistä edustaa tämä opinnäytetyö. Siinä on esitetty kattavasti verkon suunnitteluun ja toteutukseen liittyviä asioita ja niiden taustaa, joten toisenkin tavoitteen voidaan todeta saavutetun.

10 Lähteet

Ahvenainen, Marko 2003. Langattomien Lähiverkkojen Turvallisuus [online] [viitattu 16.11.2005]. http://keskus.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf

Bardwell, Joe 2002. Converting Signal Strength Percentage to dBm Values [online] [viitattu 12.11.2005]. http://www.brainworks.de/Site/hersteller/wildpackets/dokumente/airopeek_nx/wp%20-%20Converting_Signal_Strength.pdf

Enterprise Wireless LAN Security: Making Sense of the Options 2003. [online] [viitattu 15.11.2005]. http://www.trapezenetworks.com/technology/whitepapers/WLANsecurity.asp

Gast, Matthew 2004. The Top Seven Security Problems Of 802.11 Wireless [online] [viitattu 14.11.2005]. http://www.airmagnet.com/bitpipe/assets/AirMagnet.Security.WhitePaper25.pdf

Geier, Jim 2002. The Guts of WLAN Security Policy [online] [viitattu 17.11.2005]. http://www.wi-fiplanet.com/tutorials/article.php/1499151

Granlund, Kaj 2001. Langaton tiedonsiirto. Jyväskylä: Docendo Finland Oy

Griffith, Eric 2004. 802.11i Security Specification Finalized [online] [viitattu 13.11.2005]. http://www.wi-fiplanet.com/news/article.php/3373441

Helin, Ari, Karttunen, Jussi & Pitkänen, Jussi 2002. Wlan ja tietoturva. [online] [viitattu 15.11.2005]. http://www.tukkk.fi/tjt/OPETUS/TJTS11/Arkisto/wlan.pdf

Hämäläinen, Pertti 2003. Langattomat verkot sopeutuvat. Tietokone 11, 59 - 60.

Juutilainen, Matti 2004. Siirtyvä tietoliikenne, Langaton lähiverkko [online] [viitattu 11.11.2005]. http://www.it.lut.fi/kurssit/04-05/010651000/Luennot/1651_wlan.pdf

Järvinen, Petteri 2002. Tietoturva ja yksityisyys. Jyväskylä: Docendo Finland Oy

Keenan, Kathy 2004. What Hackers Don’t Want You to Know About Your WLAN [online] [viitattu 15.11.2005]. http://www.airmagnet.com/bitpipe/assets/WLAN_Hacker_White_Paper.pdf

Kotilainen, Samuli 2003. Turvaa wlan-verkkosi. Tietokone 4 Yritys-IT, 14 - 19.

Kuokka, Henri 2002. Wlan vyöryy verkkoihin. Tietokone 10, 10 - 19.

Niemi, Juha 2003. WLAN-turvallisuus [online] [viitattu 16.11.2005]. http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf

Oraskari, Jyrki 2003. Katveet peittoon. Tietokone 5, 62 - 64.

Phifer, Lisa 2005. Understanding WLAN signal strength [online] [viitattu 11.11.2005]. http://www.gwec.org/students/resources/Files/Understanding%20WLAN%20signal%20strength.pdf

Piscitello, David 2005. Expanding Your WLAN Reach [online] [viitattu 11.11.2005]. http://www.corecom.com/external/livesecurity/wlanreach.htm

Puska, Matti 2005. Langattomat lähiverkot. Helsinki: Talentum Media Oy

Ranta-Eskola, Joni 2003. WLANin rakentaminen [online] [viitattu 13.11.2005]. http://www.wlan.puv.fi/wlan_lopputyo.pdf

Seppänen, Lasse 2000. WLANProtocols2. [online] [viitattu 9.11.2005]. http://trade.hamk.fi/~lseppane/courses/wlan/doc/WLANProtocols2.htm

Simplify WLAN Planning and Deployment 2005. [online] [viitattu 10.11.2005]. http://www.airespace.com/products/appnote_wlan_planning_design.php

Suominen, Janne 2005. Langattomat lähiverkot [online] [viitattu 13.11.2005]. http://www.it.lut.fi/kurssit/04-05/010626000/seminaarit/

Särkimäki, Ville 2004. Lyhyen kantaman radiolähettimien soveltuvuus sähkökäyttöjen kunnonvalvonnan ja etädiagnostiikan tiedonsiirtotarpeisiin [online] [viitattu 13.11.2005]. https://www.ee.lut.fi/fi/tutkimus/diplomityo_sarkimaki.pdf

Vaaranmaa, Jussi, Luoma, Marko & Tamminen, Jarmo 2003. WLAN Tekniikka. [online] [viitattu 13.11.2005]. http://www.wlan.puv.fi/opiskelija.htm

Vesanen, Ari 2003. Langattomien lähiverkkojen tietoturva [online] [viitattu 14.11.2005]. http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/wlan/Wlan.html

Young, Michael F. Understanding Decibels and Their Use in Radio Systems [online] [viitattu 10.11.2005]. http://www.ydi.com/deployinfo/wp-decibels.php

Kuvaluettelo

Taulukkoluettelo

Kuvioluettelo

Lyhenneluettelo

3DES	Triple Data Encryption Standard: salausmenetelmä
802.1X	Porttikohtainen autentikointi IEEE 802 lähiverkoissa
ADSL	Asymmetric Digital Subscriber Line: modeemitekniikka
AES	Advanced Encryption Standard: salausmenetelmä
ATM	Asynchronous Transfer Mode: asynkroninen tiedonsiirtotapa
BSS	Basic Service Set: langattoman lähiverkon topologia
dB	Desibeli: mittayksikkö
dBm	Desibelimilliwatti: mittayksikkö
DES	Data Encryption Standard: salausmenetelmä
DoS	Denial of Service: palvelunestohyökkäys, tietyn verkkopalvelun lamauttaminen niin, että palvelu ei ole käytettävissä
EAP	Extensible Authentication Protocol: käyttäjien tunnistusprotokolla
EAP/LEAP	Extensible Authentication Protocol/Lightweight EAP: Cisco Systems Oy:n kehittämä käyttäjien tunnistusprotokolla
EAP/TLS	Extensible Authentication Protocol/Transport Layer Security: käyttäjien tunnistusprotokolla
ESS	Extended Service Set: langattoman lähiverkon topologia
ETSI	The European Telecommunications Standards Institute: telealan eurooppalainen standardisoimisjärjestö
FTP	File Transport Protocol: tiedostonsiirtomenetelmä kahden tietokoneen välille
GHz	Gigahertsi: mittayksikkö
HiperLAN	High Performance Radio Local Area Network: ETSI:n standardoima langaton lähiverkko
HTTP	Hyper Text Transfer Protocol: tiedonsiirtoprotokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon
HTTPS	Secure Hypertext Transfer Protocol: HTTP-protokollan salattu versio
IBSS	Independent Basic Service Set: langattoman lähiverkon topologia
IEEE	The Institute of Electrical and Electronics Engineers: yhdysvaltalainen sähkö-, tietokone- ja tietoliikenneinsinöörien yhdistys
IP	Internet Protocol: protokolla: joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa
IP-osoite	Numerosarja, jonka perusteella IP-paketit löytävät perille Internetissä
ISDN	Integrated Services Digital Network: piirikytkentäinen puhelinverkkojärjestelmä, joka on suunniteltu digitaaliseen puheen ja datan siirtoon tavallisissa puhelinlinjoissa
ISM	Industrial, Scientific, and Medical band: taajuusalue, jolla esim. WLAN toimii
MAC	Medium Access Control: IEEE 802-verkoissa verkon varaamisen ja liikennöinnin hoitava järjestelmä
Mbps	Megabits per second: mittayksikkö

MHz	Megahertsi: mittayksikkö
mW	Milliwatti: mittayksikkö
P2P	Peer-to-peer: vertaisverkko, tietokoneverkko, jossa ei ole kiinteitä palvelimia tai asiakkaita, vaan jokainen verkkoon kytketty kone toimii sekä palvelimena että asiakkaana verkon muille koneille
PCI-väylä	Peripheral Component Interconnect: tietokoneväylä lisälaitteiden liittämiseen
PCMCIA	Personal Computer Memory Card International Association: tietokoneen laajennuskorttipaikka
PoE	Power over Ethernet: virransiirtotekniikka verkkolaitteille verkkokaapelia pitkin
QoS	Quality of Service: tietoliikenteen luokittelu ja priorisointi
RC4	Ron's Code 4, Rivest Cipher 4: salausalgoritmi
SNMP	Simple Network Management Protocol: TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla
SSID	Service Set Identifier: langattoman lähiverkon tunnus
Telnet	yhteysprotokolla pääteyhteyksiin Internetin ylitse
TFTP	Trivial File Transfer Protocol: tiedonsiirtoprotokolla
TKIP	Temporal Key Integrity Protocol: tietoturvaprotokolla
UMTS	Universal Mobile Telecommunications System: kolmannen sukupolven matkapuhelinteknologia
WEP	Wired Equivalent Privacy: salausmenetelmä
Wi-Fi	Wireless Fidelity: langattomien verkkolaitteiden valmistajien liittoutuma
WLAN	Wireless Local Area Network: langaton lähiverkko
VoIP	Voice over Internet Protocol: tekniikka, jonka avulla voidaan siirtää ääntä ja videokuvaa reaaliaikaisesti internetin välityksellä
WPA	Wi-Fi Protected Access: tietoturvatekniikka
WPA2	Wi-Fi Protected Access 2: tietoturvatekniikka
VPN	Virtual Private Network: laitteisto- tai ohjelmistototeutuksena tehtävä ratkaisu, jolla organisaation sisäverkko voidaan ulottaa turvallisesti turvattoman julkisen verkon, kuten Internetin yli