STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

WLAN JA LOGISTIIKKA-ALA

Työn tekijä: Mikko Hämäläinen
Työn valvoja: Antti Koivumäki
Työn ohjaaja: Jyri Junkkari

Työ hyväksytty: __. __. 2007

Antti Koivumäki
yliopettaja

ALKULAUSE

Tämä insinöörityö tehtiin Digix Oy:n langattomien lähiverkojen yksikölle. Haluan kiittää työn ohjauksesta johtaja Jyri Junkkaria, yliopettaja Antti Koivumäkeä työn valvonnasta, avovaimoani Maiju Nykästä henkisestä tuesta ja kaikkia muita projektissa avustaneita henkilöitä. Lisäksi haluan kiittää kahta suurta logistiikka-alan yritystä, joiden WLAN-ratkaisujen suunnittelu ja toteutus mahdollistivat insinöörityöni.

Käytin insinöörityöhöni aikaa kaksi vuotta, jotta minulla oli mahdollisuus ottaa mukaan teoreettisen tiedon lisäksi kokemukseen perustuvaa tietoa. Toivon, että työni nähdään hyödylliseksi, niin aloittelijoiden kuin ammattilaisten parissa.

Helsingissä 21.9.2007

Mikko Hämäläinen

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Mikko Hämäläinen	
Työn nimi: WLAN ja logistiikka-ala	
Päivämäärä: 21.9.2007	Sivumäärä: 96 + liite
Koulutusohjelma: Tietotekniikka	Suuntautumisvaihtoehto: Tietoliikennetekniikka
Työn valvoja: yliopettaja Antti Koivumäki Työn ohjaaja: johtaja Jyri Junkkari	

Tästä insinöörityöstä pyrittiin luomaan käytännönläheinen opas logistiikka-alan yritysten WLAN-ratkaisujen suunnittelusta ja toteutuksesta. Insinöörityössä on tiivistetty käytännössä parhaiksi todetut metodit ja teoreettinen tieto langattomista verkoista. Työn tarkoituksena oli kehittää ja parantaa yrityksen langattomien lähiverkkojen yksikön toimintaa ja luoda kattava opas yksikköön saapuville työntekijöille.

Logistiikka-alalla WLAN-tekniikka on mahdollistanut varastoissa langattoman työskentelyn, joka on näkynyt nopeudessa ja kustannustehokkuudessa. Logistiset varastot ovat haasteellinen ympäristö WLAN-verkoille, mutta koko ajan kehittyvän tekniikan ansiosta varastoihin on mahdollista luoda nopea ja luotettava langaton lähiverkko.

Insinöörityön teoreettisessa osiossa käsitellään muun muassa WLAN-tekniikan historiaa, standardeja ja yleisesti WLAN-tekniikkaa. Työssä tutustutaan myös WLAN-antenneihin, laitteistoihin ja tietoturvallisuuteen.

Käytännön tutkimustyö toteutettiin kahden vuoden aikana WLAN-verkkojen ylläpidon, suunnittelun ja toteutuksen muodossa. Näiden vuosien aikana onnistuttiin kehittämään käytettyjä menetelmiä ja luomaan uusia lähestymistapoja, sekä toteuttamaan useita onnistuneita WLAN-verkkoja. Työssä esitellään teoreettisen suunnittelun lisäksi kaksi kappaletta onnistuneesti toteutuneita WLAN-ratkaisuja.

Avainsanat: WLAN, logistiikka-ala, tukiasema, Ekahau, signaalinvoimakkuus, 802.11

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name: Mikko Hämäläinen

Title: WLAN in the Fields of Logistics

Date: 21 Sept 2007 Number of pages: 96 + appendix

Degree Programme: Information Technology Specialization: Telecommunications

Instructor: Antti Koivumäki, Principal Lecturer

Supervisor: Jyri Junkkari, Director

This final creates a practical guide of how to design and carry out WLAN solutions in the field of logistics. The project examines and summarizes the best practical methods and theoretical information of wireless networks. One of the purposes of the project is to evolve and improve the operation of the company wireless networks and making the guide for newcomers.

WLAN technology has been very remarkable in the field of logistics because it has enabled wireless working that improves working speed and makes it more cost effective. Logistic warehouses are very challenging environments for WLAN networks but with new technology, it is possible to build fast and reliable wireless local area network in warehouses.

The technical part of the project deals with history of WLAN, standards and WLAN technology in general. WLAN antennas, devices and network security are also covered in the project.

The practical part of the project was carried out within two years in the form of maintenance, designing and construction of wireless networks. During these years, it was possible to improve used methods and develop new ones while making successful WLAN networks. The project introduces theoretical designing of WLAN networks but also two successfully carried out WLAN solutions.

Keywords: WLAN, logistics, access point, Ekahau, signal strength, 802.11

SISÄLLYS

LYHENNELUETTELO

ACK	Acknowledgement code; Tiedonsiirrossa käytettävä merkinantokoodi
AES	Advanced Encryption Standard; Tehokas salausalgoritmi
AP	Access Point; Tukiasema
ARP	Address Resolution Protocol; MAC-osoitteen löytämiseen käytetty protokolla
BBS	Basic Service Set; Yhden tukiaseman infrastruktuuriverkko
BPSK	Binary Phase Shift Keying; Tiedonsiirrossa käytettävä modulaatio-tekniikka
BSS	Basic Service Set; Yhden tukiaseman peittoalue
CCK	Complementary Code Keying; Tiedonsiirrossa käytettävä koodaustekniikka
CFP	Contention Free Period; Aika joka käytetään keskitettyyn hallintaan
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; MAC-osakerroksen protokolla langattomassa tiedonsiirrossa
CSMA/CD	Carrier Sense Multiple Access with Collision Detection; MAC-osakerroksen protokolla langallisessa verkossa
CTS	Clear to Send; Merkinanto tiedonsiirrolle
CDMA	Code Division Multiple Access; Koodijakokanavointi
dBi	Antennivahvistus desibeleinä
dB	Dimensioton yksikkö, joka vertailee suureiden suhteita logaritmisella asteikolla
dBm	Desibelimäärä suhteessa milliwattiin
DCF	Distributed Coordination Function; Langattoman tiedonsiirron toimintatapa
DES	Data Encryption Standard; Salausalgoritmi
DIFS	Interframe Space; Aikaviive
DoS	Denial of Service; Palvelunestohyökkäys
DBPSK	Differential Bipolar Phase Shift Keying; Modulointitekniikka
DQPSK	Differential Quatrature Phase Shift Keying; Modulointitekniikka
DSSS	Direct Sequence Spread Spectrum; Suorasekvenssihajaspektri

EAP	Extensible Authentication Protocol; Käyttäjän ja laitteen tunnistukseen tarkoitettu autentikointipalvelu
EIFS	Extended InterFrame Space; Pisin WLAN-laitteiden käyttämä viive
EIRP	Equivalent isotropically radiated power; Isotrooppinen lähetysteho
ESS	Extended Service Set; yksi tai useampi yhdistettyä tukiasemaa (BSS) / integroitu LAN, joka näkyy yhtenä tukiasemana (BSS)
ETSI	The European Telecommunications Standards Institute; Eurooppalainen standardointijärjestö
FHSS	Frequency Hopping Spread Spectrum; Frequency-hopping Spread Spectrum; Taajushyppelyhajaspektri
LEAP	Lightweight Extensible Authentication Protocol; Tunnistusprotokolla
HIPERLAN	High Performance Radio Local Area Network; ETSIn määrittelemä standardi langattomalle lähiverkolle
IAPP	Inter Access-Point Protocol; tukiasemien yhteensopivuutta parantava protokolla.
IEEE	The Institute of Electrical and Electronics Engineers; kansainvälinen sähköinsinööriliitto.
IR	Infrared; Infrapunavalo
IETF	Internet Engineering Task Force; Internet protokollien standardointijärjestelmä
ISM	Industrial, Scientific and Medical; Vapaa taajuusalue
ISO	International Standards Organization; Kansainvälinen standardisoimisjärjestö
LWAPP	Light Weight Access Point Protocol; Hallittavien tukiasemien ja kontrollereiden välillä käytettävä protokolla
MAC	Media Access Control address; Päätelaitteen fyysinen osoite
MAC	Media Access Control layer; OSI-mallin tiedonsiirtokerroksen osakerros

MIMO	Multiple-input multiple-output; 802.11n lanseerattava tekniikka, joka mahdollistaa useiden lähettimen ja vastaanottimien yhtä aikaisen käytön
OSI	Open Systems Interconnection; Tiedonsiirtoprotokkollia kuvaava taulukko
OFDM	Orthogonal Frequency Division Multiplexing; Ortogonaalinen taajuusjakomultipleksointi
PCF	Point Coordination Function; Langattoman tiedonsiirron toimintatapa
PIFS	Point Coordination InterFrame Space; Tukiasemien käyttämä viive
PoE	Power over Ethernet; Ethernet-kaapeloinnin avulla toteutettu virransyöttö
QAM	Quadrature Amplitude Modulation; Amplitudimodulaatiotekniikka
QPSK	Quadrature Phase Shift Keying; Tiedonsiirrossa käytettävä modulaatiotekniikka
RADIUS	Remote Access Dial-In User Service; Käyttäjätunnistusmenetelmä ja -protokolla
RC4	Rivest Cipher 4; Salausalgoritmi
RF	Radio Frequency; Radioaalto
RTS	Request to Send; Merkinanto tiedonsiirrossa
SARP	Secure Address Resolution Protocol; Suojattu ARP-protokolla
SIFS	Short InterFrame Space; Odotusaika tiedonsiirrossa
SSID	Service Set Identifier; Langattoman verkon tunnus
SSH	Secure Shell; Tiedonsiirtojärjestelmä
SHA	Secure Hash Algoritm; Eheyden varmistavan tiivisteen laskentamenetelmä
TCP	Transmission Control Protocol; Yhteydellinen kuljetusprotokolla
IP	Internet Protocol; Internet protokolla
TLS	Transport Layer Security; Kuljetuskerroksen salausmenetelmä
WiMAX	Worldwide Interoperability for Microwave Access; Laajakaistainen radiotekniikka kaupunkiverkkoihin
TDMA	Time Division Multiple Access; Aikajakokanavointitekniikka
TKIP	Temporal Key Integrity Protocol; Langattoman lähiverkon salaustekniikka

VLAN	Virtual Local Area Network; Virtuaalinen lähiverkko
VoIP	Voice over Internet Protocol; IP-verkon yli oleva puheliikenne
WEP	Wired Equivalent Privacy; Langattoman lähiverkon salaustekniikka
WPA	Wi-Fi Protected Access; Langattoman lähiverkon salaustekniikka
WPA2	Wi-Fi Protected Access 2; Langattoman lähiverkon salaustekniikka
WLAN	Wireless Local Area Network; Langaton lähiverkko
Wi-Fi	Wireless Fidelity; Langattomien verkkolaitteiden standardointiliitto
PBCC	Packet Binary Convolutional Coding; Modulointitapa
QoS	Quality of Service; Tietoliikenteen luokitteluun ja priorisointiin tarkoitettu termi
RLAN	Radio Local Area Networks; Vaihtoehtoinen termi WLANille
3DES	Triple Data Encryption; Salausmenetelmä
AAA	Authentication, Authorization, Accounting; Käyttäjien tunnistus, valtuutus ja tapahtumien kirjaaminen
AD	Active Directory; Aktiivihakemisto, Microsoftin hakemistoratkaisu käyttäjä- ja resurssitietojen järjestelyyn
EDGE	Enchanced Data rates for Global Evolution; Pakettidatatekniikka
WES	Wireless EDGE Services; Radioporttijärjestelmä
WCS	Wireless Control System; Ciscon langattomien laitteiden hallintajärjestelmä
HTTP	Hypertext Transfer Protocol; Sovelluskerroksen Web-protokolla
HTTPS	Secure HTTP; Turvattu sovelluskerroksen Web-protokolla
IPS	Intrusion Prevention System; Tunkeutumisen havaitsemisjärjestelmä
UDP	User Datagram Protocol; Yhteydetön kuljetusprotokolla
DHCP	Dynamic Host Configuration Protocol; IP-parametrien jako
CAPWAP	Control and Provisioning of Wireless Access Points; Langattomien tukiasemien keskitetyn hallinnan standardiluonnos
WiCoP	Wireless LAN Control Protocol; Langattomien tukiasemien keskitetyn hallinnan protokolla

CTP	CAPWAP Tunneling Protocol; Langattomien tukiasemien keskitetyn hallinnan protokolla
SLAPP	Secure Light Access Point Protocol; Langattomien tukiasemien keskitetyn hallinnan protokolla
EAP-FAST	Flexible Authentication via Secure Tunneling; Autentikointimenetelmä
PEAP	Protected EAP; Autentikointimenetelmä
EAP-TTLS	EAP-Tunneled Transport Layer Security; Autentikointimenetelmä
EAP-TLS	EAP-Transport Layer Security; Autentikointimenetelmä
CCMP	Counter Mode with CBC-MAC Data Origin Authenticity Protocol; Autentikointimenetelmä

1 JOHDANTO

Tämä insinöörityö tehtiin kahden vuoden aikana osana normaalia WLAN-verkkojen suunnittelua ja toteutusta, tarkoituksena tehostaa ja kehittää työskentelyä. Tutkimustyön tarkoituksena oli löytää käyttökelpoisimmat ja tehokkaimmat apuohjelmat ja menetelmät, joiden avulla voidaan suunnitella ja toteuttaa mahdollisimman toimiva WLAN-verkko.

Insinöörityössä esitellään kaksi WLAN-verkon toteutusta, jotka on toteutettu suurille logistiikka-alan yrityksille. Yhtenä lähtökohtana oli toteutuksen kustannusten minimointi tehokkuudesta tinkimättä. Logististen varastojen langattoman lähiverkon suunnittelusta ja toteutuksesta on tehty kattava teoreettinen osio, josta on hyötyä niin aloittelijoille kuin ammattilaisille. Työssä käsitellään myös oleelliselta osalta WLAN-tekniikkaan liittyvä teoria.

Toisessa esitellyssä käytännön esimerkissä käytettiin WLAN-verkon suunnittelun apuna Ekahaun Site Survey-ohjelmaa. Kuuluvuusmittaukset toteutettiin suunnitteluvaiheessa sekä verkon valmistuttua. Suunnitteluvaiheen mittauksissa käytettiin liikuteltavaa, itse rakennettua tukiasemajärjestelmää, jonka kuuluvuutta mitattiin kannettavalla tietokoneella.

WLAN-verkon suunnittelun ja toteutuksen teoreettisen osion kokoaminen alkoi Digix Oy:n langattomien lähiverkkojen yksikön toimintatapojen sisäistämisellä. Kahden vuoden aikana löydettiin uusia tapoja toteuttaa asioita ja opittuja metodeja sovellettiin toimivaksi kokonaisuudeksi. Teoreettisen WLAN-tekniikan sisäistäminen todettiin välttämättömyydeksi toimivan WLAN-verkon toteuttamisen kannalta.

2 WLAN JA LOGISTIIKKA-ALA

Nykyään logistiikka on yksi tärkeimmistä tekijöistä kaupan alalla. Tehokas logistiikka on tärkeää kilpailukyvyn ja työllisyyden kannalta. Bruttokansantuotteesta lähes 40 prosenttia saadaan ulkomaanviennistä ja logistiikka-ala työllistää Suomessa noin 95 000 ihmistä. Yritysten liikevaihdosta yli 10 prosentin ollessa teollisuuden ja kaupan logistiikkakustannuksia, on kustannustehokkuudella suuri merkitys logistiikka-alalla. [5.]

Logistiikasta saatujen tulojen määrä on täysin riippuvainen toimivasta logistiikasta. Nykyään toimivan ja tehokkaan logistiikan edellytyksenä ovat toimivat tietoliikenneratkaisut. Tietoliikenteen merkitys toiminnan kannalta on kriittinen globaalisella tasolla, mutta kustannustehokkuutta tarkasteltaessa varastotason ratkaisut ovat nykyään entistä tärkeämmässä roolissa. [5.]

Varastotasolla on saavutettu langattoman lähiverkon ansiosta huomattavia etuja käsittelyn nopeudessa ja käytön helppoudessa. Langattomuuden ansiosta kerääjät voivat suorittaa muutokset tietokantaan riippumatta siitä, missä päin varastoa he työskentelevät. Langattomuudella saavutetaan lähes rajoittamaton työskentely-alue, mutta tällaisen järjestelmän rakentaminen vaatii tarkkaa suunnittelua ja oikeita välineitä. Varastotilojen haasteellinen ympäristö aiheuttaa monia ongelmia suunniteltaessa toimivaa, mutta yksinkertaista WLAN-verkkoa. Nykyään tietoturvan merkitys on suuri ja se vaikuttaa merkittävästi tuotevalintoihin ja kokonaisratkaisuun.

Logistiset varastot ovat usein isoja ja korkeita tiloja, joissa on paljon esteitä. Tällaiset tilat eivät ole ideaalisia WLAN-verkon toiminnalle, koska vaimentavia tekijöitä on paljon ja suuri yhtenäinen alue rajoittaa tukiasemien määrää ylikuulumisen vuoksi. Varastotilojen haasteellinen ympäristö aiheuttaa myös rajoitteita tukiasemien sijoitteluun ja työasemalaitteiden hankintaan. LAN-kaapelointi on saatava vedettyä tukiasemille, eikä veto saa olla ylimittainen. Työasemalaitteiden on oltava riittävän tehokkaita, mutta myös kestäviä. Varastojen pölyisyys ja muut mahdolliset lisätekijät, kuten kylmyys aiheuttavat usein päänvaivaa. Varasto-olosuhteet ovat hyvin vaihtelevia ja haasteellisia, mutta oikealla suunnittelulla niihinkin on mahdollista rakentaa toimiva WLAN-verkko ominaisuuksista tinkimättä.

3 WLAN OSANA YRITYKSEN LÄHIVERKKOA

Tässä insinöörityössä käsitellään logistiikka-alan WLAN-ratkaisuja, jotka ovat osa yritysten lähiverkkoa. Nykyään uutta lähiverkkoa rakennettaessa on otettava huomioon teknisten vaatimusten lisäksi ratkaisujen integrointitarpeet, joita yhä useammin ovat langattoman lähiverkon sulauttaminen lähiverkkoon. Lähiverkon tekniikan ja rakenteen tunteminen on langattoman lähiverkon suunnittelun ja toteutuksen perusteita.

Yleisin logistiikka-alan lähiverkkoratkaisu nykyään on Ethernet. Topologiana käytetään useimmiten tähteä ja fyysisenä siirtotienä parikaapelia ja optista kuitua. Siirtonopeudet vaihtelevat välillä 10 Mbit/s - 10 Gbit/s. Tällä hetkellä käytetyin Ethernet-tekniikka on Fast-Ethernet, joka sisältää kaikki 100 Mbit/s nopeuteen kykenevät standardit. Nämä tekniikat käyttävät tähtitopologiaa ja fyysisenä siirtotienä kierrettyä parikaapelia. 10BaseT (10 Mbit/s) on vieläkin paljon käytetty tekniikka, mutta nopeutensa puolesta sillä ei ole enää tulevaisuutta.

Logistiikka-ala on vaativa tietoliikenteen suhteen, joten se pyrkii pysymään teknologian kehityksen mukana. Näin ollen 90-luvun alkupuolella suosittua standardia 10base2 (Ohut Ethernet) ei enää poikkeuksia lukuun ottamatta tavata. Päätelaitteiden määrän ja nopeusvaatimusten kasvettua, väylätopologia ja koaksiaalikaapelin käyttö fyysisenä siirtotienä ei ole enää käytännössä edes mahdollista. Vuodesta 2002 alkaen Suomessa yleisin asennettavista kaapelointistandardeista on Cat6, jonka kaistanleveys on 250 Mhz. Nopeuksien kasvaessa ja testausstandardien tiukentuessa ei ole enää järkevää asentaa Cat6:tta aikaisempaa standardia.

Varastoissa on paljon erilaisia häiriötekijöitä, jotka aiheuttavat magneettikenttiä. Näiltä häiriötekijöiltä voidaan suojautua käyttämällä suojattua kierrettyä paria. On suositeltavaa, että käytetään vähintään F/UTP (Foiled Twisted Pair) parikaapelityyppiä, jossa kierretyt parit on suojattu foliolla. Suunniteltaessa lähiverkon kaapelointia suunnitellessa logistisiin varastoihin on nykyään välttämätöntä ottaa huomioon langattomien tukiasemien vaatima kaapelointi. Tämä aiheuttaa usein rajoitteita tukiaseman sijoittelun suhteen, koska matka ristikytkentään on rajallinen.

4 WLANIN HISTORIAA

Hajaspektritekniikkaan perustuvan langattoman tiedonsiirron historialliset juuret ovat militääriset toisen maailmansodan ajoilta. Yhdysvaltojen armeijan tarkoituksena oli kehittää tietoturvallinen tiedonsiirtomenetelmä, joka ei ole altis sähkömagneettiselle säteilylle. Ainutlaatuinen tekniikka oli tietoturvallista sillä hetkellä ja pysyi vuosikymmeniä vain sotilaskäytössä.

Samaiseen tekniikkaan perustuva WLAN (Wireless Local Area Network) -tekniikka eli langaton lähiverkko on nykyään nopeasti kehittyvä tekniikka, jonka kehitys alkoi vuonna 1990 IEEE:n (Institute of Electrical and Electronics Engineers) standardointiryhmän toimesta. Seitsemän vuotta myöhemmin ryhmä julkaisi valmiin 802.11-standardin, joka loi puutteistaan huolimatta perustan tuleville määrittelyille.

802.11-standardi käyttää siirtotienä radioaaltoja ja infrapunavaloa, jota ei enää tueta myöhemmissä standardin laajennuksissa siirtonopeuden kasvettua. Ensimmäinen standardi käytti FHSS-taajuushyppelyä (Frequency Hopping Spread Spectrum) ja DSSS-suorasekvenssihajaspektritekniikkaa (Direct Sequence Spread Spectrum), mutta FHSS-tekniikasta luovuttiin jo ensimmäisessä laajennuksessa.

Langaton laitteisto on loppujen lopuksi vain yksi sovellus normaalissa lähiverkossa. Lähiverkkoon liitetään laite, joka tarvitsee verkkoyhteyttä varten sekä virtaa että kaapeloinnin. Langattomien laitteiden valmistajia on nykyään useita, mutta toisin kuin alkuaikoina laitteiden yhteensopivuus on hyvä. Yhteensopivuudesta huolehtimaan onkin perustettu Wi-Fi Alliance, joka toimii yhteistyössä IEEE 802.11 komitean kanssa. [2.]

Wi-Fi Alliance

Vuonna 1999 perustettu Wi-Fi Alliance -järjestön tarkoituksena oli pyrkiä luomaan yksi maailmanlaajuinen standardi nopealle langattomalle lähiverkolle. Järjestöä perustamassa oli vain muutamia teollisuuden johtajia, mutta nykyään siihen kuuluu yli 250 jäsentä ja määrä kasvaa koko ajan. Langattomien verkkojen yleistyessä kotikäytössä, yrityksissä ja julkisissa tiloissa, on yhteensopivuus hyvin tärkeää. Tällä hetkellä järjestö on sertifioinut yhteensopivaksi yli 3000 laitetta. [2.]

Järjestö ei kuitenkaan keskity pelkästään laitteiden yhteensopivuuden testaamiseen ja sertifiointiin. Järjestön toimenkuvaan kuuluu myös antaa tarvittaessa tietoa langattomista järjestelmistä, niin yksityisille kuin yrityksille. Järjestön toiminnan ansiosta kuluttajilla on mahdollisuus tuoreeseen tietoon ja standardoinnin ansiosta edullisiin ja toimiviin laitteisiin. [2.]

5 WLAN-TEKNIIKKA

WLAN-tekniikan avulla voidaan muodostaa langaton verkkoyhteys laitteiden välille tai liittää laite langattomasti lähiverkkoon. Langattomalla verkkoyhteydellä on samat ominaisuudet ja hyödyt kuin normaalillakin lähiverkkoyhteydellä, mutta ilman kaapeleita ja johtoja. Langattomuus on tuonut yrityksille ja etenkin logistiikka-alalle aivan uudenlaisia mahdollisuuksia tehostaa ja helpottaa työskentelyä. Tämän ansiosta WLAN-tekniikka on yleistynyt hyvin nopeasti ja sitä pyritään kehittämään koko ajan lisää. Langattoman lähiverkon muodostamiseen tarvitaan kuitenkin edelleen fyysinen kaapelointi, jonka kautta signaali voidaan lähettää langattomasti. Signaalin lähettämiseen tarvitaan sitä varten suunniteltu tukiasema (Access Point) tai silta (Wireless Bridge), joka lähettää signaalin radioaaltojen avulla. [1.]

5.1 Radioaallot

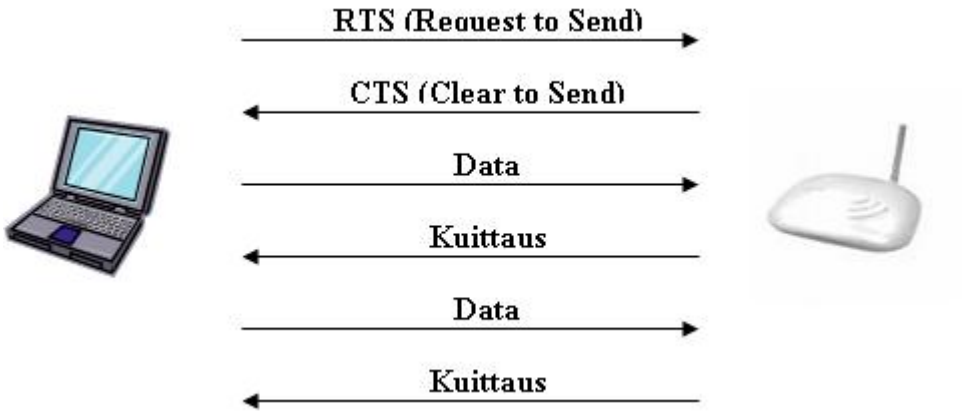
Yleisimmin langattomissa verkkoyhteyksissä tiedonsiirtoon käytetään radioaaltoja. Verrattuna infrapunaan radioaallot kantavat pidemmälle ja niillä on suurempi kaistanleveys (pystytään siirtämään nopeammin dataa). WLAN-verkot käyttävät 2.4 GHz:n ja 5 GHz:n taajuusalueita, jotka ovat varattuja lisensoimattomille laitteille melkein koko maailmassa. WLAN-laitteiden käyttö 2.4 GHz:n avoimella taajuusalueella ei vaadi lupaa, mutta 5 GHz:n taajuusaluetta ei saa poikkeuksellisesti käyttää kuin sisätiloissa. Suuremmalla taajuudella toimivilla laitteilla on huomattavasti huonompi kantomatka, joten 2.4 GHz:n taajuudella toimivat laitteet ovatkin eniten käytetty malli. [2; 1.]

Radiotaajuuksilla käytetään tiedonsiirtoon sekä modulaatiotekniikkaa että hajaspektritekniikka. Näiden ero on se, että hajaspektritekniikassa informaatio jaetaan montaa eri kanavaa pitkin ja modulaatiotekniikassa informaatio moduloidaan jokaisen kanavan yli. Kumpaakin näistä tekniikoista käytetään WLAN-tiedonsiirtoon.

5.2 Vuoronvaraus

WLAN-verkoissa käytetään CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) -siirtotien varausmenetelmää, jonka avulla samaa siirtotietä voidaan käyttää useampaan lähetykseen. Se on samanlainen kuin Ethernet-verkoissa käytetty CSMA/CD-varausmenetelmä, mutta törmäykset havaitaan etukäteen lähettämällä siirtotien varaava signaali ennen varsinaista datan lähetystä. [6, s. 29]

CSMA/CA mahdollistaa virtuaalisen kantoaallon kuuntelun (Virtual Carrier Sense) WLAN-tukiasemissa. Tiedon lähetys on kontrolloitua ja siinä käytetään RTS/CTS-kättelyä (kuva 1). Kättelyssä työasema pyytää lähetyslupaa RTS-sanomalla, johon tukiasema vastaa CTS-viestillä lähetystien ollessa vapaa. Tiedonlähetys tapahtuu yhdessä tai useammassa kehyksessä, jotka tukiasema kuittaa. Tiedonsiirto voidaan suorittaa myös ilman kanavanvarausta, mutta se on käytännöllistä vain pienissä verkoissa, joissa ei ole paljon törmäyksiä. [6, s. 29.]



Kuva 1. RTS/CTS-kättely [6, s .29]

Fyysisen kantoaallon kuuntelulla tukiasema varmistaa, että kanava on vapaa ennen lähetystä. Tukiasema varaa kanavan itselleen NAV (Network Allocation Vector) verkonvarausvektorilla, joka välittyy kaikille verkon solun tukiasemille. Tukiasema arvioi kehyksen lähettämiseen ja kuittaamisen tarvittavan ajan ja sijoittaa varausajan MPDU-kehyksen kestokenttään. Kehyksien lähetys ei tapahdu peräkkäin, vaan niiden välillä on viiveitä [6, s. 30]:

- SIFS (Short InterFrame Space) on lyhyin viive, jota käytetään liittyvien kehysten välillä.
- PIFS (Point Coordination InterFrame Space) -viivettä käytetään kehyksen ennenaikaiseen lähetykseen.
- DIFS (Distributed InterFrame Space) on viive, jota ennen tukiasema ei voi lähettää sanomaa.
- EIFS (Extended InterFrame Space) -viivettä käytetään estämään työaseman lähetys, mikäli tukiasema ei kykene tulkitsemaan verkon sanomaa.

6 WLAN-STANDARDIT JA SIIRTOTEKNIIKAT

Langattoman lähiverkon yleistyttyä laitteiden standardoinnin lisäksi oli kehitettävä standardit myös protokollille. Standardoidut protokollat määrittelevät ISO-järjestön OSI-kerrosmallin fyysisen kerroksen ja siirtokerroksen toimintatavat. Langaton lähiverkko on standardoitu kahden järjestön toimesta. Yleisin on IEEE:n standardi IEEE 802.11, jota on ajan myötä laajennettu alistandardeilla. ETSI:n standardi tunnetaan nimellä HIPERLAN, josta löytyy tällä hetkellä kaksi eri versiota. [9, s. 230.]

IEEE (The Institute of Electrical and Electronics Engineers) on kansainvälinen sähköinsinööriliitto, johon kuuluu jäseniä yli 160 maasta. Liiton toimenkuva on monipuolinen ja yksi sen tärkeimmistä tehtävistä on standardien määrittäminen.

6.1 IEEE 802.11

IEEE 802.11-standardin kehitys alkoi vuonna 1990 esitellystä versiosta, josta ehdittiin tekemään kuusi versiopäivitystä ennen kuin 26.7.1997 IEEE julkaisi virallisen standardin IEEE 802.11. Standardi määrittelee OSI-mallin fyysisen kerroksen ja siirtokerroksen alemman osan (MAC). Standardi käyttää siirtotienä radiotaajuuksia alueella 2,4 - 2,4835 GHz (ISM-taajuusalue) ja toimii nopeuksilla 1 Mbit/s ja 2 Mbit/s. Standardi tukee siirtotienä myös infrapunasäteilyä aallonpituuksilla 850 - 950 nm. Radiotaajuuksilla IEEE 802.11 käyttää koodijakokanavointia (CDMA). [6; 9, s. 230 - 235.]

6.1.1 CDMA

CDMA eli koodijakokanavointi on yksi radiotien kanavanvaraustekniikoista, joka voidaan toteuttaa kahdella eri metodilla: suorasekvenssihajaspektri- (DSSS) ja taajuushyppelyhajaspektritekniikkaalla (FHSS). CDMA soveltuu hyvin WLAN-käyttöön, koska siinä taajuuskaista on kaikilla käyttäjillä kokonaan käytössä lähetettäessä ja vastaanotettaessa. Käyttäjien tunnistus tapahtuu yksilöllisillä koodeilla, minkä ansiosta samaa taajuusaluetta voi käyttää useampi käyttäjä yhtä aikaa. [7, s. 397; 8.]

6.1.2 DSSS (Direct Sequence Spread Spectrum)

DSSS-tekniikassa data jaetaan pieniin osiin, mutta lähetys tapahtuu kantoaallossa yhtenäisenä signaalina käyttäen koko käytettävissä olevaa taajuusaluetta. Nykyisin DSSS-tekniikkaa käytetään enemmän, koska se on vikasietoisempi. [8.]

6.1.3 FHSS (Frequency Hopping Spread Spectrum)

FHSS-tekniikassa lähetystaajuutta vaihdellaan algoritmin mukaisesti. Siinä data pilkotaan pieniin osiin, jotka lähetetään omaa kapeaa kanavaa pitkin.

6.1.4 ISM-taajuusalue

ISM-taajuusalue (Industrial, Scientific and Medical) on vapaassa käytössä oleva maailmanlaajuinen radiotaajuuskaista. ISM-kaistoja on kolme ja niistä kahta käytetään langattomissa lähiverkoissa. Suomessa on sallittu vain 2,4 GHz:n (2,4 - 2,4835 GHz) ISM-taajuusalue, mutta Yhdysvalloissa on sallittua käyttää myös 5 GHz:n (5.728 - 5.850 GHz) aluetta. [1, s. 16.]

6.2 IEEE 802.11b

Verkkosovellusten kehittyessä ja langattoman lähiverkon suosion kasvaessa 802.11-standardin määrittämät nopeudet alkoivat käydä pieneksi. IEEE julkaisi vuonna 1999 kehittyneemmän standardin 802.11b, joka tunnetaan myös nimellä 802.11hr (high rate). Standardi mahdollistaa nopeudet 5,5 Mbit/s ja 11 Mbit/s käyttäen taajuutta 2,4 GHz. Standardi käyttää edelleen suorasekvenssitekniikkaa ja lisäksi CCK-modulointia (Complementary Code Keying). 802.11b on yhteensopiva aikaisemman standardin kanssa, joten huonoissa olosuhteissa datasiirtonopeus voidaan pudottaa myös 1 ja 2 Mbit/s nopeuksiin. [10, s. 118 - 119; 6.]

CCK-modulointi

> ”Suorasekvenssitekniikassa lähetettävä bittijono hajautetaan laajemmalle taajuusalueelle ja lähetetään samanaikaisesti matemaattisten funktioiden perusteella” [6, s. 36].

Hajautus sisältää toistettua tietoa, jonka avulla alkuperäinen tieto voidaan toistaa, vaikka puolet alikanavien tiedoista muuttuisi. CCK-hajautusta käytetään 802.11b-standardin nopeuksilla 5,5 ja 11 Mbit/s. Pienemmillä nopeuksilla käytetään Barker-hajautusta. [6, s. 36 - 37.]

6.3 IEEE 802.11a

Syksyllä vuonna 1999 IEEE julkaisi 802.11a-standardin, joka käyttää siirtotienä 5 GHz:n (51,5 - 5,35 GHz) taajuusaluetta. Standardissa käytetään CSMA/CA-kanavanvaraustekniikkaa ja OFDM-modulointia, joka suuremman taajuuden kanssa mahdollistaa 54 Mbit/s siirtonopeuden. 802.11a-standardista ei ole tullut yhtä yleistä, kuin 802.11b:stä, koska korkeampi taajuus rajoittaa kantamaa verrattuna 2,4 GHz:n taajuudella toimiviin laitteisiin. [6, s. 45.]

OFDM (Orthogonal frequency-division multiplexing)

OFDM eli DTM-modulointi (Discrete Multitone) on monikantoaaltomodulointimenetelmä, jossa tieto siirretään useaa rinnakkain lähettävää osakanavaa pitkin. 802.11b, -a, -g-standardeissa on kolme ei-päällekkäistä kanavaa ja jokaisella kanavalla on 52 ortogonaalista alikanavaa 0,3125 MHz:n välein. 802.11a-standardilla on 12 toisiinsa vaikuttamatonta kanavaa ja jokaisella kanavalla on 52 alikanavaa. [6, s. 40 - 45.]

802.11a- ja -g WLAN-standardeissa tekniikka käyttää 52 osakanavaa, joiden spektrit ovat toisistaan riippumattomia ortogonaalisia funktioita. Signaali muodostetaan osakanavista käyttämällä nopeaa Fourier-käänteismuunnosta taajuustasosta aikatasoon. Vastaanotettaessa alikanavien amplitudit lasketaan aikatasosta taajuustasoon. [6, s. 40 - 45.]

6.4 IEEE 802.11g

802.11g-standardin kehitys aloitettiin vuonna 2000 ja se saatiin valmiiksi vuonna 2003. Standardi toimii 2,4 GHz:n ISM-taajuusalueella ja kykenee 54 Mbit/s siirtonopeuteen. 802.11g käyttää CCK-hajautusta ja OFDM-modulointia, mutta mahdollistaa myös PBCC-moduloinnin käytön tiedonsiirrossa. Standardi käyttää aikaisempien standardien parhaita ominaisuuksia ja on yhteensopiva 802.11b-standardin kanssa. Tällä hetkellä 802.11g on käytetyin standardi langattomissa lähiverkoissa. [13; 12.]

6.5 IEEE 802.11n

Radiolähiverkkojen lisääntyessä ja kasvaessa, samalla kun niitä hyödynnetään yhä useammalla eri alalla, on väistämätöntä, että nykyisten langattomien yhteyksien nopeudet ja luotettavuus eivät enää riitä. 802.11n-standardi tulee parantamaan sekä nopeutta että stabiilisuutta, mutta sitä ei ole vielä julkaistu. Sen kehitys aloitettiin vuonna 2003, ja julkaisun on tarkoitus tapahtua vuoden 2008 lokakuussa. [14; 6, s. 127.]

IEEE:n tavoitteena on saada standardi tukemaan vähintään 100Mbit/s maksimisiirtonopeutta, mutta teoreettisesti on mahdollisuus saavuttaa jopa 600 Mbit/s siirtonopeus. Jotta näihin nopeuksiin päästään, tulee sekä fyysinen että MAC-kerroksen toteutus muuttumaan aikaisemmista standardeista. Standardi tulee tukemaan myös uutta MIMO-tekniikka, jonka avulla voidaan hyödyntää useampaa antennia ja kanavaa samanaikaisesti. [14; 6, s. 127.]

MIMO

MIMO eli Multiple-input multiple-output on tekniikka, jonka avulla tukiasemissa voidaan käyttää yhtäaikaisesti montaa antennia ja kanavaa. Tämän tekniikan ansiosta tukiasemat voivat käyttää useampaa antennia sekä vastaanottoon että lähetykseen. Nykyään tukiasema joko lähettää tai vastaanottaa, vaikka tukiasemassa olisi 2 antennia. Vastaanottimien on mahdollista kerätä dataa eri signaaleista ja yhdistää se lopuksi yhdeksi kokonaisuudeksi. Koska tukiasema voi MIMO-tekniikan avulla käyttää myös useampaa kanavaa yhtaikaa, parantaa se huomattavasti langattoman verkon vikasietoisuutta. MIMO-tekniikkaa on käytetty jo 802.11g-laitteissa, mutta virallisesti se tulee käyttöön 802.11n-standardin mukana. [15.]

6.6 IEEE 802.11-standardien laajennuksia

Edellä mainittujen standardien lisäksi IEEE on julkaissut seuraavat standardien laajennukset.

- 802.11e, sisältää palvelunlaatua (QoS) ja suorituskykyä parantavia laajennuksia. Tukiasemille voidaan antaa eri kiireellisyysasteita, jolloin uudelleenlähetyksen odotusaika pienenee vähentäen verkkoviivettä kyseisessä tukiasemassa. [6, s. 47.]

- 802.11f, määrittelee liityntäpisteiden välisen liikennöinnin IAPP (Inter Access-Point Protocol) -protokollan avulla. Laajennuksen tarkoitus on parantaa samassa verkossa olevien eri valmistajien tukiasemien yhteensopivuutta. Tulevaisuudessa 802.11f korvataan 802.11k- ja 802.11r-laajennuksilla. [6, s. 47.]

- 802.11h, sisältää 5 GHz:n taajuusalueen lisämääritykset Euroopassa. Laajennus tukee lisäksi älykkäämpää taajuusalueen vaihtoa ja parantaa laitteiden virransäästöominaisuuksia. [6, s. 47.]

- 802.11d, parantaa tukiasemien sijaintimaan informaation lähetyksen ominaisuuksia. Laajennuksen avulla langaton laite osaa käyttää oikeaa taajuuskaistaa maasta riippumatta. [16.]

- 802.11i, merkittävä laajennus, joka parantaa tietoturvaominaisuuksia. Laajennus lisää TKIP-avainnuksen ja muita WEP-parannuksia. 802.11i sisältää myös liikenteen salaukseen käytettyä avainten hallintaa, joka perustuu avainparien käyttöön. Laajennus lisää myös CCMP -lohkosalauksen, joka on toteutettu AES -salauksella. 802.11i laajennus tukee myös esitunnistusta ja siirtymistä tukiasemasta toiseen ilman erillistä käyttäjän uudelleentunnistusta. Lisäksi mukana on muita määrittelyjä ja laajennuksia, kuten PEAP -tunnistus. Salausmenetelmistä lisää kappaleessa 5 WLAN Tietoturvallisuus. [6, s. 83 - 84.]

- 802.11j, sisältää Japania koskevia laajennuksia. [6, s. 47.]

Julkaisemattomat standardien laajennukset

IEEE kehittää jatkuvasti uusia laajennuksia, jotta standardit vastaisivat nykypäivän tarpeita. Seuraavat laajennukset ovat vielä julkaisemattomia, eikä niille ole varmaa ilmestymispäivämäärää.

- 802.11s, laajennuksen tarkoituksena on tukea niin sanottua mesh-verkkoja. Päämääränä on luoda järjestelmä, jossa langattomat laitteet voivat yhdistyä ja luoda Ad-Hoc-verkon. Tulevaisuudessa tätä tekniikkaa tullaan käyttämään kaupunkiverkoissa. [17.]
- 802.11p, kulkuneuvojen ja niiden välillä toimivan langattoman yhteyden laajennusprotokolla.
- 802.11k, tulee parantamaan yhteyden laadun ja suorituskyvyn määrittämistä [19].
- 802.11r, tarkoituksena parantaa BSS:ään (Basic Service Set) siirtymistä ESS:ssä (Extended Service Set) ja saada esimerkiksi VoIP-sovellukset toimimaan reaaliajassa ilman viiveitä. Pyrkimyksenä siis poistaa tukiaseman vaihdosta johtuvaa viivettä.
- 802.11.2, tarkoituksena standardoida langattoman yhteyden määrittämiseen tarvittavat määreet, mittaustavat ja testiympäristöt. Mahdollistaa realistisen laitteiden ja verkkojen vertailun, joka on riippumaton käytetystä laitemerkistä. [21.]
- 802.11u, lisää ominaisuuksia ulkoisiin verkkoihin liittymiseen ja mahdollistaa verkkoon liittymisen ilman autentikointia. Sovellusta tullaan käyttämään julkisilla paikoilla, jossa ihmiset voivat liittyä verkkoon ilman autentikointia. [22.]
- 802.11v, mahdollistaa laitteiden keskitetyn monitoroinnin ja hallinnan siirtokerroksen kautta. Nykyään hallintaan käytetään SNMP-protokollaa. [23.]
- 802.11w, tietoturvalaajennus MAC-kerrokselle. Tarkoituksen parantaa tiedon yhtenäisyyttä, tiedon alkuperän varmistusta, replay-suojausta ja tiedon luotettavuutta tietyillä hallintakehyksillä. [24.]
- 802.11y, laajentaa 802.11-laitteiden käytön 3,65 - 3,7 GHz:n taajuusalueelle Yhdysvalloissa. [25.]

6.7 ETSI (HIPERLAN)

Eurooppalainen standardointiorganisaatio ETSI (European Telecommunications Standars Institute) on telealan standardisoimisjärjestö, joka on perustettu CEPT:n toimesta vuonna 1988. Järjestö on nykyään laajentanut toimintaansa myös langattomien lähiverkkostandardien standardoimiseen. ETSI on määritellyt HIPERLAN (High Performance Radio LAN) standardiperheen, joka koostuu kahdesta eri versiosta. [26; 6, s. 47 - 48.]

6.7.1 HIPERLAN/1

HIPERLAN/1 standardin kehitystyö alkoi vuonna 1991 ja se julkaistiin vuonna 1998. Standardi käyttää 5 GHz:n (5,15 - 5,35 GHz) taajuusaluetta ja kykenee maksimissaan 23,5 Mbit/s tiedonsiirtonopeuteen. HIPERLANin käytössä on viisi kanavaa, joista kolme on vapaassa käytössä ja kahdesta päättää jokaisen valtion radiotaajuuksista vastaava järjestö. Standardi käyttää MAC-tasolla kanavankäyttökontrollia (CAC), joka on toteutettu EY-NPMA:n (Elimination-Yield Non-Preemptive Multiple Access mechanism) avulla. [26; 6, s. 47 - 48.]

CAC ja EY-NPMA

CAC:n eli kanavankäyttökontrollin tehtävä on hallita kanavankäyttöpyyntöjä kanavan sen hetkisen tilan ja pyyntöjen prioriteetin perusteella. Kanavankäyttökontrolli käyttää EY-NPMA-mekanismia, joka lähettää tiedon prioriteetista ja funktioista siirtokaistalle ennen data-pakettia. EY-NPMA:n avulla verkko saadaan toimimaan mahdollisimman vähäisillä pakettien yhteentörmäyksillä, vaikka verkossa on paljon käyttäjiä. [26; 6, s. 47 - 48.]

6.7.2 HIPERLAN/2

ETSI julkaisi HIPERLAN/2-standardin vuonna 2000. Standardi käyttää edelleen 5 GHz:n taajuusaluetta, mutta maksimi tiedonsiirtonopeutta on nostettu 54:ään Mbit/s. Standardi käyttää dynaamista TDMA aikajakokanavointia ja tietoturvaominaisuudet ovat paljon kehittyneemmät kuin ensimmäisessä versiossa. Tiedon salaukseen käytetään DES- ja 3DES-algoritmejä. [26; 6, s. 47 - 48.]

TDMA (Time Division Multiple Access)

TDMA eli aikajakokanavointi on kanavanvaraustekniikka, joka perustuu eri signaalien jakamiseen ajan suhteen. Lähetys tapahtuu osissa, jotka lähetetään tietyin aikavälein. Aikavälien täyttyessä yhteyden muodostaminen ei ole mahdollista ja tekniikka on herkkä monitie-etenemishäiriölle. Dynaaminen TDMA varaa dynaamisesti aikavälejä eri nopeuksille liikenteen mukaan. [26; 6, s. 47 - 48.]

6.8 HOMERF (Shared Wireless Access Protocol-SWAP)

HomeRF tekniikka kehitettiin kotikäyttöön tiedonjakoa varten. Tekniikan kehitys lakkautettiin vuonna 2003, koska 802.11b-standardi levisi kotikäyttöön ja Microsoft alkoi tukea käyttöjärjestelmissään bluetooth-standardia. HOMERF käytti FHSS-hajaspektritekniikkaa ja 2,4 GHz:n taajuusaluetta. Standardin teoreettinen maksiminopeus oli 10 Mbit/s, mutta käytännössä laitteet tukivat vain 1,6 Mbit/s nopeuksia.

6.9 WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX on IEEE:n langattoman alueverkon 802.16-standardin laajennus 802.16a, joka julkaistiin vuonna 2003. WiMAX-tekniikkaa kehittää WiMAX Forum -valmistajaliittouma. WiMAX-tekniikan pääasiallinen tehtävä on tarjota langatonta laajakaistaa, jonka kantama on noin 20 - 50 km, käytännössä päästään vain 20 kilometrin etäisyyksiin. [55.]

WiMAX käyttää 2 - 6 GHz:n taajuusaluetta ja Suomessa käytetty taajuus on 3,5 GHz. Yhdellä tukiasemalla voidaan tarjota 75 Mbit/s siirtonopeus, joka jaetaan solussa olevien käyttäjien kesken. Standardi käyttää dynaamista modulaatiota, joka valitsee modulointitekniikan (QPSK, QAM-16, QAM-64) tarpeen mukaan. 802.16a-standardi ei tue päätelaitteen siirtymistä tukiasemasta toiseen, mutta helmikuussa 2006 julkaistussa 802.16e-standardissa tämä ominaisuus on tuettu. [55.]

6.10 Yhteenveto standardeista

WLAN-standardeja on ehtinyt kertyä 10 vuoden aikana useita ja kehitys jatkuu koko ajan. Taulukossa 1 on esitelty yleisimmät standardit ja joitakin peruselementtejä niistä. Taulukon avulla voi saada peruskuvan standardien kehityksestä ja käytetyistä tekniikoista.

Taulukko 1. WLAN-standardien vertailua

Standardi	Julkaistu	Siirtotie	Teoreettinen bittinopeus	Taajuusalue	Kanavia
802.11	1997	RF / IR	1, 2 Mbit/s	IRDA / 2,4 GHz	13
802.11b	1999	RF	1, 2, 5,5, 11 Mbit/s	2,4 GHz	13
802.11g	2003	RF	1-54 Mbit/s	2,4 GHz	13
802.11a	1999	RF	6-54 Mbit/s	5 GHz	12
802.11n	Ei julkaistu	RF	250+ Mbit/s	2,4 GHz / 5 GHz	?
HiperLAN	1998	RF	20 Mbit/s	5 GHz	5
HiperLAN v2	2000	RF	54 Mbit/s	5 GHz	5
802.16 (WiMAX)	2001	RF	2, 4, 8, 10, 12+ Mbit/s	10-66 GHz	-
WiMAX (802.16a)	2003	RF	2, 4, 8, 10, 12+ Mbit/s	3,5 GHz* (2-11 GHz)	-
WiMAX (802.16e)	2006	RF	2, 4, 8, 10, 12+ Mbit/s	3,5 GHz* (2-6 GHz)	-
HomeRF	2001	RF	1,6 Mbit/s** (10 Mbit/s)	2,4 GHz	-

	EIRP-teho	Hajotus / koodaus	Hajaspektri-tekniikka	Modulointi	Kantama
802.11	100 mW	Barker	FHSS / DSSS	DBPSK	25-75m
802.11b	100 mW	Barker / CCK	DSSS	DBPSK / DQPSK	45-100m
802.11g	100 mW	Konvoluutio / CCK	OFDM	BPSK / QPSK/ 16-QAM / 64-QAM	40-95m
802.11a	200 mW	Konvoluutio / CCK	OFDM	BPSK / QPSK / 16-QAM / 64-QAM	25-75m
802.11n	?	?	?	?	70-160m
HiperLAN	200 mW	Space-time	OFDM	FSK / GMSK	50m
HiperLAN v2	200 mW	Space-time	OFDM	BPSK / QPSK/ 16-QAM / 64-QAM	50m
802.16 (WiMAX)	-	-	OFDM	Dynaaminen ***	20-50 km
WiMAX (802.16a)	-	-	OFDM	Dynaaminen ***	20-50 km
WiMAX (802.16e)	-	-	SOFDMA	Dynaaminen ***	20-50 km
HomeRF	100 mW	-	FHSS	-	50m

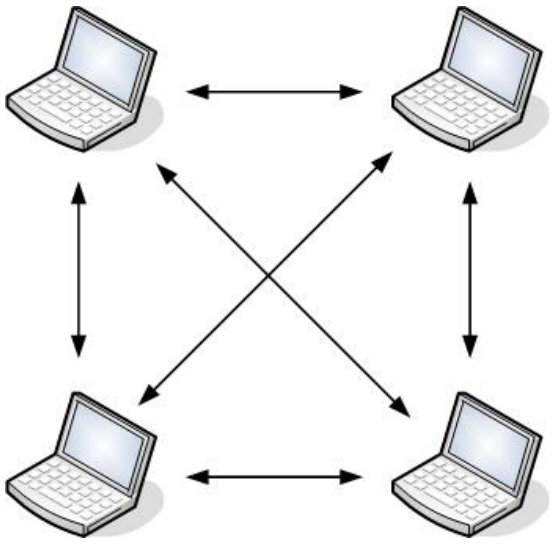
* Suomessa käytössä oleva WiMAX taajuusalue
** Käytetyt HomeRF laitteet tukivat tätä nopeutta
*** Dynaaminen modulointi (64 QAM, 16 QAM, QPSK)

7 VERKKOARKKITEHTUURIT

Langaton verkko voidaan muodostaa kahdella eri tavalla. Ensimmäisessä tavassa on pelkkiä client-päätteitä (verkkokortteja), jolloin kyseessä on Ad-Hoc-tyyppinen verkko. Toinen mahdollisuus on lisätä kokoonpanoon tukiasema, jolloin syntyy niin sanottu infrastruktuuriverkko.

7.1 Ad-Hoc-verkkomalli

Ad-Hoc-verkko (kuva 2) eli Mobile Ad-Hoc Network (MANET) on verkkomalli, jonka muodostavat kaksi tai useampi päätelaitetta (ei tukiasema). Järjestelmän etuna on se, että tukiasemaa ei tarvita, asennus on nopeaa ja kustannukset ovat edulliset. Haittapuolina ovat verkon lyhyt kantama ja huono hallittavuus. Järjestelmä on tarkoitettu lähinnä muutamien koneiden yhdistämiseen ja niiden väliseen tiedonsiirtoon, koska muuten verkon tehokkuus kärsii liiallisesta datapakettien törmäilystä. Internetyhteyden muodostamiseksi jonkin päätelaiteen pitää olla kytkettynä Internetiin, jonka jälkeen se jaetaan muiden käyttöön. Ominaisuus ei palvele kovinkaan monen päätelaitteen Ad-Hoc-verkkoa. [31.]



Kuva 2. Ad-Hoc verkko

Toimintaperiaate

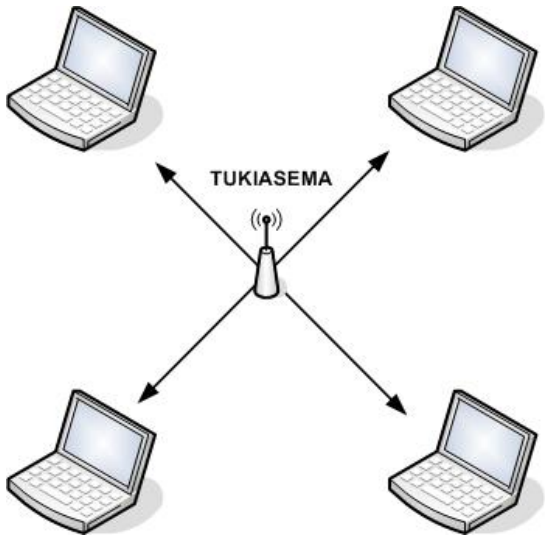
Ad-Hoc-verkon muodostamiseksi ensimmäinen päätelaite muodostaa IBSS:n (Independent Basic Service Set), jonka jälkeen se alkaa lähettää merkkisignaalia, jonka avulla päätelaitteet synkronoituvat. Verkkoon liitytään hyväksymällä merkkisignaalin parametrit. Merkkisignaalien avulla kaikki päätelaitteet tulevat tietoiseksi toisistaan. [32.]

7.2 Infrastruktuuriverkko

Infrastruktuuriverkko sisältää vähintään yhden tukiaseman ja yhden tai useamman päätelaitteen. Yhden tukiaseman infrastruktuuriverkkoa kutsutaan BSS (Basic Service Set) -verkoksi ja useamman tukiaseman järjestelmää ESS (Extended Service Set) -verkoksi.

BSS (Basic Service Set)

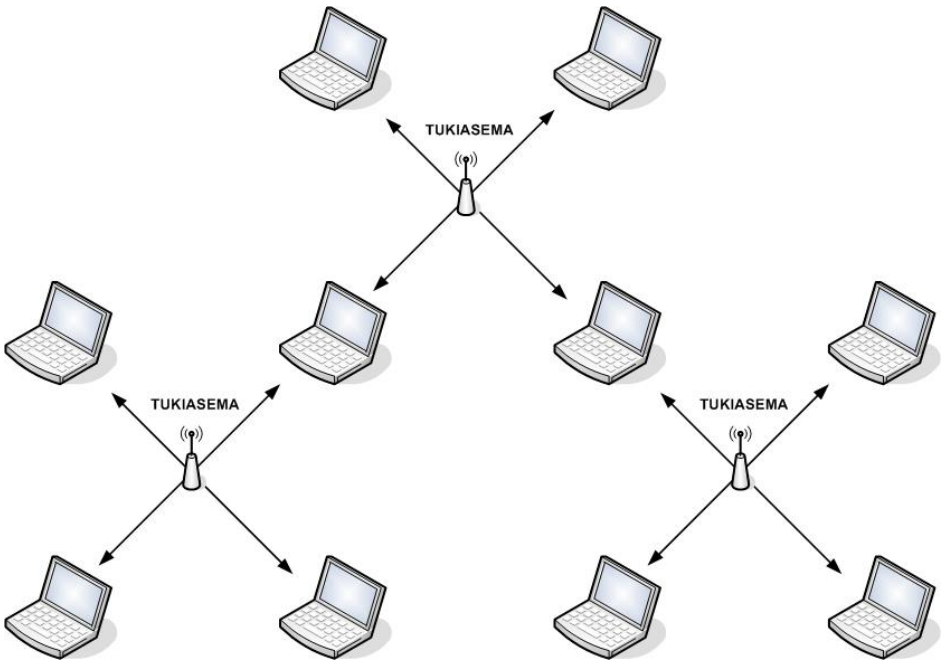
BSS-verkkostruktuuria (kuva 3) käytetään tyypillisimmin kodeissa ja pienissä toimistoissa. BSS-verkon alueellista kokoa rajoittaa tukiaseman signaalin kantavuus. Tukiaseman avulla päätelaitteet voivat liittyä suojatusti lähiverkkoon ja niiden käytössä on myös Internet-yhteys, mikäli tällainen ominaisuus lähiverkosta löytyy. BSS-verkon hallittavuus on helppoa, koska siinä on vain yksi tukiasema. [6, s. 132 - 133.]



Kuva 3. BSS-infrastruktuuriverkko

ESS (Extended Service Set)

ESS-verkkostruktuuri (kuva 4) on käytännössä monien BSS-verkkojen kokonaisuus. ESS-verkossa on useita tukiasemia, jotka ovat samassa aliverkossa. Yleensä kaikki tukiasemat on kytketty langalliseen verkkoon, mutta on myös mahdollista muodostaa tukiasemien välille sillattuyhteys. ESS-verkomallilla saavutetaan se etu, että verkko on käytettävissä laajemmalla alueella ilman katkoksia. Liikkuvuuden mahdollistaa tukiasemien roaming-ominaisuus, jonka ansiosta tukiasemien kuuluvuusalueella on käytännössä yhtenäinen verkko. [6, s. 132 - 133.]



Kuva 4. ESS-infrastruktuuriverkko

7.3 Tulevaisuuden verkkomallit

Tulevaisuudessa tullaan todennäköisesti puhumaan kolmannesta WLAN-arkkitehtuurista nimeltään WMESH (Wireless Mesh) tai MANet (Mobile Ad-Hoc Network)-verkkomallista. Tarkoituksena on luoda reitittävä langaton verkko, joka on vikasietoinen. Käytännössä verkkomallia voitaisiin verrata nykyisiin peer-to-peer-sovelluksiin, joissa kaikki ovat yhteydessä toisiinsa ja yhden yhteyden katkeaminen ei vaikuta omaan yhteyteen. Vielä ei ole varmaa, minkälainen uusi verkkomalli tulee loppujen lopuksi olemaan, mutta se tulee sisältämään Ad-Hoc-verkkomallin ominaisuuksia, jossa tietokoneiden välinen yhteys on osa verkkoa. [33.]

Tekniikkaa tullaan käyttämään lähiverkkoihin, mutta myös mahdollisesti julkisiin Internet-yhteyksiin esimerkiksi kaupungeissa. Tulevaisuudessa on jopa mahdollista luoda GSM-verkon laajuinen langaton verkko, joka kattaa myös Internetin.

8 LÄHETYSTEHO

Suomessa Viestintävirasto määrittää langattomien lähiverkkojen sallitut lähetystehot ja sallitut taajuusalueet. Langattomissa lähiverkoissa käytettävien laitteiden käyttömääräykset ovat julkisia dokumentteja ja löytyvät esimerkiksi Viestintäviraston Internet-sivuilta.

Laitteiden lähetystehoraja koskee antennista lähtevää säteilytehoa, joten antenninvahvistuksen kasvaessa on lähettimen lähetystehoa laskettava. Säteilyteho (EIRP) on riippuvainen lähettimen lähtötehosta, antennikaapelin ja liittimien häviöstä ja antennin vahvistuksesta.

8.1 2,45 GHz:n taajuusalue

2,45 GHz:n taajuusalue eli 2,4 - 2,4835 GHz:n taajuusalue on yhteistaajuusaluetta, jonka käyttö on sallittu kaikille yhtäläisillä oikeuksilla. Suurin sallittu lähetysteho on 100 mW EIRP. [34.]

EIRP

> ”EIRP (Equivalent Isotropically Radiated Power) on lähettimen lähetystehon (dBm tai dBW) ja antennivahvistuksen (dB) summa, ja kertoo, kuinka suuri lähetysteho tarvittaisiin saman kentänvoimakkuuden saavuttamiseksi, jos lähetysantenni olisi isotrooppinen.” [59]

8.2 5 GHz:n taajuusalue

Suomessa Viestintävirasto on rajoittanut 5 GHz:n toimintataajuusalueet eurooppalaisen HIPERLAN-standardin mukaisesti. 802.11a-standardin mukaisia laitteita on sallittua käyttää taajuusalueella 51,5 - 5,35 GHz. Laitteiden käyttö on rajoitettu ainoastaan sisätiloihin ja suurin sallittu lähetysteho on 200 mW (EIRP). [11.]

8.3 Yksiköt

Lähetystehoa laskettaessa, laitehankintojen valinnassa ja kuuluvuusmittauksissa törmää erilaisiin termeihin, jotka liittyvät tehoon, vahvistukseen, vaimennukseen sekä signaalinvoimakkuuteen. Yksiköt menevät helposti sekaisin, joten ne on syytä tuntea, mikäli on aikomus suunnitella ja toteuttaa valmista langatonta verkkoa. Termit dB, dBm, dBi ja mW ovat yleisimmät yksiköt, joihin langattoman verkon yhteydessä törmää.

HF-signaalin voimakkuus

Desibeli (dB) on yksikkö, jota käytetään ilmaisemaan HF (High Frequency) -signaalin eli tässä tapauksessa radioaallon voimakkuutta. Desibeleissä vertaillaan tehojen suhteita logaritmisella asteikolla, jonka ansiosta suurta skaalaa voidaan käsitellä pienellä lukualueella ja laskutoimitukset helpottuvat. [35.]

Antennien signaalinvoimakkuus

Antennien signaalinvoimakkuudesta käytetään merkintää dBm eli tehoa verrataan 1 mW:n tehoon. Käytännössä tämä tarkoittaa sitä, että 0 dBm = 1 mW. Taulukko 2 helpottaa tehon ja signaalinvoimakkuuden suhteiden hahmottamista. [35.]

Valmistajat ilmoittavat usein antennin vahvistuksen dBi-desibeliyksikkönä. 0 dBi:n arvo voidaan rinnastaa isotrooppiseen antenniin, joka teoriassa säteilee samalla voimakkuudella joka suuntaan.

Taulukko 2. Signaalinvoimakkuus taulukot

Antennin vahvistus (dB)	Vahvistuskerroin
-20	0,01
-10	0,1
-3	0,5
0	1
3	2
10	10
20	100
30	1 000
40	10 000
50	100 000

Teho (dBm)	Teho (W)
20	100 mW
10	10 mW
0	1 mW
-10	0,1 mW
-20	0,01 mW
-30	0,001 mW
-60	1 nW
-90	1 pW

Vaimennus

Vaimennukset ilmoitetaan useimmiten dB-arvoina. Esimerkiksi kaapeli voi vaimentaa 0,2 dB / m, jolloin jokainen metri vaimentaa 0,2 desibeliä. [35.]

Teho

Teho ilmoitetaan tutulla watti (W) -yksiköllä ja WLAN-tekniikassa arvot ovat 100 mW tai pienempiä arvoja. Teho voidaan ilmoittaa myös dBm-arvona. Kaavalla 1 voidaan laskea tehojen suhteesta signaalin voimakkuus desibeleissä. [35.]

$$\frac{P_1}{P_2} = 10^{(\frac{A}{10})} \rightarrow A = 10 \cdot \log \frac{P1}{P2} \qquad (1)$$

Kaavassa A = signaalin voimakkuus, P1 ja P2 = tehoja

Ohjelmissa käytetyt arvot

Eri ohjelmissa signaalinvoimakkuutta, signaali/kohinasuhdetta ja muita arvoja saatetaan ilmoittaa eri muodoissa. Signaalin voimakkuutta tarkastellessa käytetään yleensä dBm-yksikköä, jolloin arvot ovat miinusmerkkisiä ja lähempänä nollaa oleva luku on silloin parempi. Signaalin kohinasuhdetta ilmaistaan myös dB-arvolla, mutta siinä luvut ovat positiivisia suuremman luvun ollessa parempi.

Signaalinvoimakkuutta ilmaistaessa vaimennuksen avulla voidaan arvoa -80 dBm pitää rajana milloin signaalinlaatu alkaa olla huono. Signaalin laatua mitattaessa ei kuitenkaan koskaan tyydytä hetkelliseen arvoon, vaan mitataan keskiarvo ja mahdollisesti käytetään apuna muilla tavoin saavutettuja testituloksia.

8.4 Lähetystehon laskeminen

Lähetysteho on syytä tuntea suunniteltaessa langattomia lähiverkkoja, koska tehon alenemiseen vaikuttavat hyvin monet muuttujat. Ensimmäinen huomioonotettava asia on antennin valinta. Tehorajoitusten vuoksi ei voida käyttää aivan mitä tahansa antennia, koska kokonaissäteilyteho ei saa ylittää annettuja rajoja. Lisäksi on tiedettävä kuinka paljon kaapeleilla ja liittimillä on vaikutusta lähetystehoon, mikäli asennusteknisten ongelmien vuoksi joudutaan käyttämään esimerkiksi pidempää kaapelia. Lähetysteho on otettava myös huomioon, kun arvioidaan antennien vahvistusta ja niiden tarvetta kuuluvuuden parantamiseksi.

Lähetystehon laskeminen luvuilla

2,45 GHz:n taajuusalueella laitteesta lähtevä lähetysteho saa olla maksimissaan 100 mW eli 20 dBm, jos antennin vahvistus on yksi eli 0 dB. Jos antennin suuntaavuutta parannetaan, sen lähettämä teho kohdistuu pienemmälle alueelle eli sen lähetysteho vahvistuu. [35.]

> "Jos antennin vahvistus on esim. 20, (eli 13 dB), niin 100 mW:n (eli 20 dBm:n) EIRP toteutuu, kun lähettimen antenniin syöttämä signaaliteho on 100mW/20 = 5 mW (eli 20 dBm - 13 dB = 7 dBm)." [59]

Mikäli tiedetään lähettimen antenniin syöttämä signaaliteho, kaavalla 2 voidaan laskea sallittu antennin vahvistus, jotta käyttöön saadaan lainmukainen 100 mW:n (20 dBm) EIRP maksimikokonaislähetysteho. [35.]

$$A = \frac{100mW}{x-(y+z)} \leftrightarrow A = 20dBm - x - (y+z) \qquad (2)$$

Kaavassa A = antennin vahvistus, x = WLAN-lähettimen antenniin syöttämä teho, y = kaapelin aiheuttama häviö, z = liittimen / muut häviöt (n. 1 dB).

9 ANTENNIT

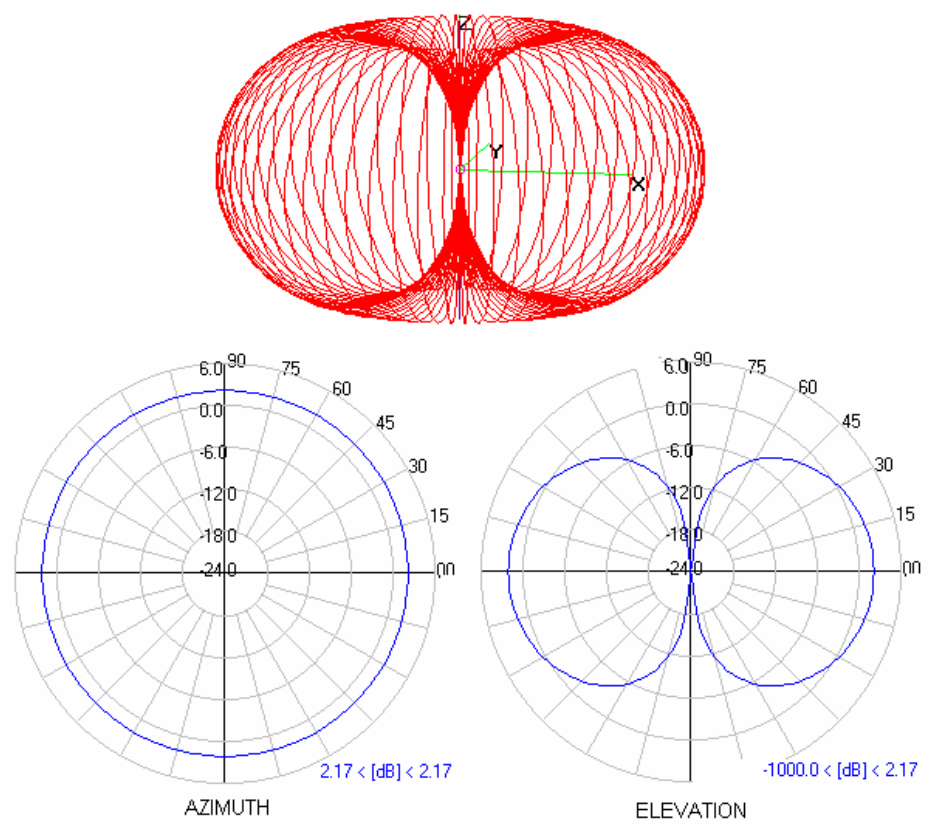
WLAN-antennityyppejä on erilaisia ja kaikkien antennien suuntakuvio on epäsymmetrinen, joten lähetetty teho ei ole koskaan tasainen joka suuntaan. Suunnatuilla antenneilla saadaan suurin lähetysteho haluttuun suuntaan ja ympärisäteilevällä suurin peittoalue. Etäisyyksien kasvaessa tehokkaampien antennien käyttö on välttämätöntä ja esteettömän näköyhteyden merkitys kasvaa. Yli 6 km:n välimatkoilla on alettava ottaa huomioon myös maan kaareutuminen, jonka huomioonottamiseen käytetään Fresnel-ilmiön laskukaavoja. [6, s. 60 - 61.]

Antennityypit

Antennityyppejä on käytännössä kahdenlaisia, suunta-antenneja ja ympärisäteileviä antenneja. Tavallisimmat ympärisäteilevät antennityypit ovat Dipoli-antenni, levyantenni, sauva-antenni ja WLAN-laitteiden sekä sovittimien sisäiset antennit. Suunnattuja antenneja ovat tyypillisesti Yagi ja lautasantennit, mutta myös levyantennia voidaan käyttää suuntaavana, jos se on suunniteltu siihen käyttötarkoitukseen.

Ympärisäteilevät antennit

Tyypillisin antennityyppi logistiikka-alalla on ympärisäteilevä antenni, koska melkein poikkeuksetta pyritään saamaan mahdollisimman kattava kuuluvuusalue. Yksi tyypillisimmistä ympärisäteilevistä antenneista on Dipoli-antenni (kuva 5), jonka pituus on puolen radioaallon pituinen. Varastoissa on usein paljon esteitä, joten siellä on käytettävä jopa 5 dBi:n verran vahvistavia antenneja (kuva 6).

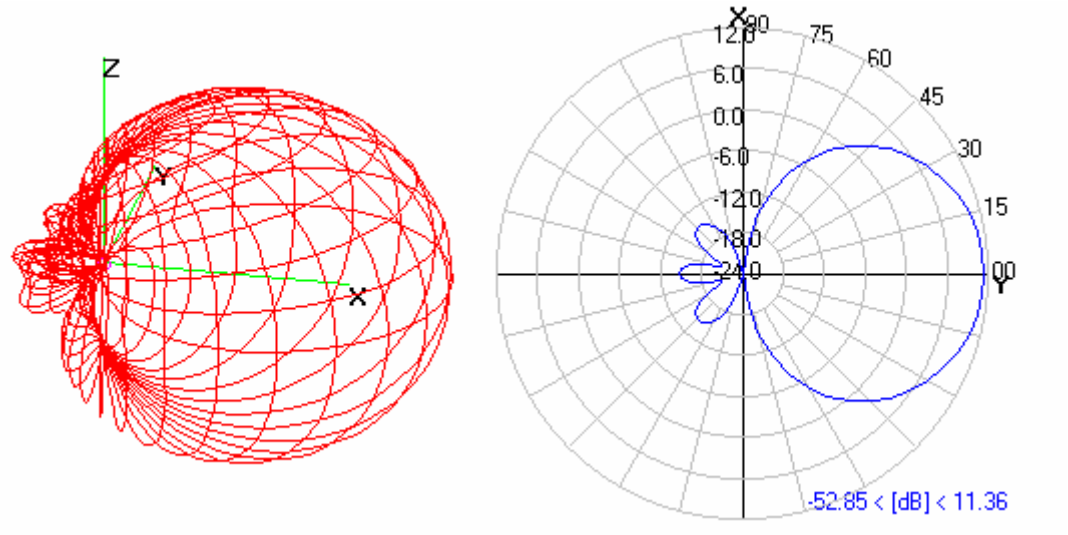


Kuva 5. Tyypillisen Dipoli-antennin (0,5λ) säteilykuviot

Kuva 6. 5 dBi:n ympärisäteilevä antenni [28]

Suunta-antenni

Suunta-antennien (kuva 7, kuva 8) käyttö on tarpeellista, jos kyseessä on käytävä tai halutaan luoda sillattuyhteys tukiasemien välille. Suunta-antennien ”tehokkuus” perustuu niiden suuntaavuuteen eli niiden lähettämä teho kohdistetaan pienemmälle alueelle.



Kuva 7. Suunta-antennin säteilykuviot [28.]

Kuva 8. Suunta-antenneja [29; 30.]

10 WLANIN TIETOTURVALLISUUS

Langattomat lähiverkot ovat yleistyneet huimaa vauhtia, niin yritystasolla kuin kotikäytössäkin. Laitteiden kehityksessä on otettu huomioon myös tietoturvariskit ja langattomien verkko on mahdollista saada turvattua tarpeen mukaan erittäin hyvin. Ongelmana on ihmisten välinpitämättömyys tietoturvaa kohtaa ja mahdollisesti myös tietämättömyys. Etenkin kotikäytössä ihmiset eivät välttämättä ole tietoisia, kuinka paljon helpompaa on murtautua langattomaan verkkoon kuin langalliseen. Langattomissa verkoissa yhteyden saaminen ei vaadi kiinteää liittymistä verkkoon, joten se helpottaa murtautumista huomattavasti.

Kotikäyttäjät ajattelevat usein, ettei heidän koneellaan ole mitään niin tärkeää, että verkkoon murtautumisesta olisi heille haittaa. Ikävä kyllä useat ihmiset säilyttävät kotikoneellaan työhön liittyviä asiakirjoja ja tiedostoja, jotka väärissä käsissä voivat aiheuttaa vakavia seuraamuksia. Langattomissa lähiverkoissa uhkat ovat pääosin samanlaiset kuin langallisissa verkoissa, mutta langattomuus tuo lisää uhkia ja heikkouksia. Tässä kappaleessa käsitellään langattomien lähiverkkojen uhkia sekä niiden ehkäisyä.

10.1 Passiiviset tietoturvauhkat

Passiivisissa hyökkäyksissä ei vaikuteta verkkoon, eikä siihen pyritä tekemään haittaa. Passiivisen tietototurvariskin aiheuttaa salakuuntelu ja verkkoliikenteen analysointi.

Verkkoliikenteen salakuuntelu ja analysointi (sniffing)

Liikenteen salakuuntelu langattomassa lähiverkossa on helppoa, koska tietoliikenne tapahtuu ilmassa ja yleensä ulottuu sisätilojen ulkopuolellekin. Käyttämällä suunta-antenneja salakuuntelu onnistuu kauempaakin, joten fysikaalisesti ulkopuolisilta rajattu alue ei takaa tietoturvaa. Salakuuntelua on kaiken lisäksi mahdotonta havaita ja vaikea estää. [6, s. 69]

Salakuuntelun tarkoituksena on yleensä tiedon kerääminen verkkoon tunkeutumisen helpottamiseksi. Salakuunteluun ei tarvita ammattimaisia taitoja, eikä työkaluja, joten se on erittäin vakava tietoturvaongelma, koska se johtaa yleensä tietoverkkoon tunkeutumiseen. Pahimmassa tapauksessa langatonta lähiverkkoa ei ole lainkaan suojattu ja se lähettää SSID-tunnustaan, jolloin salakuuntelu siihen tarkoitettuun ohjelmalla (kuten AirMagnet) onnistuu vaivatta. Ohjelma kerää langattoman liikenteen datapaketit ja paljastaa niiden sisällöt, jotka voivat olla esimerkiksi luottokorttitietoja, käyttäjätunnuksia ja salasanoja.

Salakuuntelua voidaan, estää tiedon salaamisella (katso 10.5 Salausmenetelmät), mutta nykyään sekin on tehtävä hyvin, koska ohjelmallisesti on mahdollista purkaa salaus, tekniikasta riippuen. Taulukossa 3 on listattu tietoturvaominaisuuksia, jotka on mahdollista purkaa tai kiertää. Lisäksi on mainittu esimerkkiohjelma ja vaikeustaso kyseisen toiminnon suorittamiseen, jotta olisi helpompaa kartoittaa oman tietoverkon tietoturvaa. Ohjelmat ovat ilmaisia ja kaikkien saatavissa, joten on suositeltavaa, että verkonylläpitäjä tutustuu ohjelmiin ja mahdollisesti testaa oman verkkonsa tietoturvaa itse tekemällään hyökkäyksellä.

Taulukko 3. Langattoman verkon murtautumisohjelmia

Ohjelma	Vaikeustaso	Aika*	Toimenpide
Kismet, Network Stumbler	Helppo!	Erittäin lyhyt	Piillotetun SSID:n määrittäminen
Kismet	Helppo!	Lyhyt	Verkon IP-alueen määrittäminen
Kismet, Network Stumbler	Helppo!	Erittäin lyhyt	Valmistajan ja mallin tunnistus
Kismet, Ethereal	Helppo!	Lyhyt	TCP dumbing (pakettien purkaminen/analysointi)
Kismet, Airsnort, Airodump, Aircrack, airreplay, Airodump-ng	Helppo!	Lyhyt	WEP-salauksen purkaminen
Airodump-ng, Aircrack, Kismet	Keskivaikea!	Keskipitkä	WPA \ TKIP -salauksen purkaminen
Airodump-ng	Vaikea!	Pitkä	WPA2-salauksen purkaminen
coWPAtty+Kismet	Vaikea!	Pitkä	WPA-PSK-salauksen purkaminen
???	Erittäin vaikea!	???	WPA-RADIUS-salauksen purkaminen
???	Erittäin vaikea!	???	AES

*Murtamiseen tarvittava aika riippuu yleensä käyttäjä- ja liikennemäärästä

10.2 Aktiiviset tietoturvauhkat

Aktiiviset hyökkäykset ovat tahallista tietoverkkoon vaikuttamista, johon kuuluu datan ja signaalin lähettäminen verkkoon sekä siihen tunkeutuminen. Aktiivinen hyökkäys voi kohdistua pelkästään siirtomediaan eli langattomissa yhteyksissä lähinnä radiotaajuuteen, jota yritetään häiritä tai lamaannuttaa. Radioaalloilla liikkuvaa dataa voidaan muokata niin, että se korruptoituu käyttökelvottomaksi. Suurin uhka on tietoverkkoon murtautuminen, johon on monia eri tapoja.

10.2.1 Palvelunesto (DoS)

Tässä kappaleessa esitellään langattoman verkon palvelunestohyökkäyksiä. Palvelunestohyökkäys voidaan toteuttaa usealla eri tavalla ja käyttäen vain yhtä konetta tai useampaa orjakonetta (zombies) yhteishyökkäyksen muodostamiseksi. Yhteispalvelunestohyökkäystä kutsutaan DDoS (Distrubuted Denial of Service) -hyökkäykseksi. WLAN-verkot ovat alttiita myös samoille DoS hyökkäyksille kuin langalliset verkot, mutta tässä työssä keskitytään langattoman median kautta tapahtuviin hyökkäyksiin. [31, s. 57 - 75.]

Siirtomedian häirintä (Strong signal jamming)

DoS (Denial of Service) eli palvelunestohyökkäys voi olla radioaaltojen häirintää, joka voi pahimmassa tapauksessa lamauttaa koko yrityksen langattoman verkon. Häirintä voidaan toteuttaa radiolähettimillä, joilla luodaan niin paljon häiriötä langattoman verkon taajuusalueelle, että datan liikkuminen hidastuu merkittävästi tai lakkaa kokonaan datatörmäyksien seurauksena. Tällaisen hyökkäyksen toteuttamiseen tarvitaan usein erittäin tehokas lähetin, joka on sijoitettava fyysisesti lähelle verkkoa. [31, s. 57 - 75.]

Radiotaajuuksien häirintä voi olla myös tahatonta radiotaajuuksien interferenssiä, sillä monet laitteet käyttävät samaa taajuutta kuin WLAN-tukiasemat. Laitteita, jotka operoivat 2,4 GHz:n taajuudella, ovat esimerkiksi mikroaaltouunit ja bluetooth-laitteet. Häirinnän estämiseksi ei ole oikein muuta keinoa kuin vaihtaa radiokanavia tai etsiä häiriön lähde. Häiriönpaikallistamiseen voidaan käyttää verkkoanalysaattoria.

(WPA denial of service)

Häirintä on vakava-ongelma etenkin jos langaton verkko käyttää automaattista törmäystunnistusta, joka sulkee verkkolaitteet vahvemman signaalin vaikuttaessa. Tällainen toiminto on käytössä WPA-salaustekniikassa. [31, s. 57 - 75.]

Yhteyden katkaisu (Disassociate frame attack)

Palvelunestohyökkäys voi kohdistua myös WLAN-tukiasemiin, joita pyritään ylikuormittamaan turhilla liityntä- tai palvelupyynnöillä. Hyökkääjä lähettää tukiasemalle aikaisemmin urkittuja yhteydenkatkaisukehyksiä, pakottaen tukiaseman ja työaseman (client) katkaisemaan yhteyden toistuvasti. Kyseessä on Man in the Middle -tekniikan hyökkäys laajemmassa mittakaavassa, josta enemmän edempänä. [31, s. 57 - 75.]

FakeAP-täyttö (FakeAP flood)

FakeAP on ohjelma, joka on kehitetty murtautujia ja tiedonkalastelijoita vastaan. Ohjelman avulla on mahdollista tehdä jopa tuhansia virtuaalisia tukiasemia, joiden seassa oikea tukiasema sijaitsee. Ohjelman avulla on mahdollista piilottaa tukiasema tehokkaasti, mutta sitä voidaan käyttää myös julkisten WLAN-yhteyksien lamauttamiseen. Kannettavalla tietokoneella ja FakeAP-ohjelmalla voidaan luoda julkiseen WLAN-verkkoon lukuisa määrä valetukiasemia, jotta vierailevat käyttäjät eivät tiedä mitä tukiasemaa käyttää. [31, s. 57 - 75.]

10.2.2 Valetukiasemat (Rogue Access Points)

Valetukiasemien käyttö voidaan käytännössä jakaa kahteen eri tapaukseen. Ensimmäinen tapaus on tukiaseman lisääminen lähiverkkoon ilman lupaa. Tämä tapahtuu yleensä työntekijän toimesta, joka haluaa langattoman verkon käyttöönsä, eikä ole saanut sitä syystä tai toisesta yritykseltä. Tällainen omatoimisuus voi olla erittäin vakava tietoturvallisuusriski yritykselle.

Toinen ja yleisempi valetukiaseman käyttö keskittyy julkisiin WLAN-verkkoihin krakkereiden toimesta. Valetukiaseman tehtävänä on kerätä tietoa, kuten salasanoja, käyttäjänimiä, luottokortin numeroita ja mitä tahansa mistä voi hyötyä. Julkisten WLAN-verkkojen yleistyessä valetukiasemien käytöstä on muodostumassa vakava tietoturvallisuusuhka jopa Suomessa. Valetukiaseman käyttö tietojen kalastelussa perustuu saman SSID-tunnuksen käyttöön jonkin julkisen WLAN-verkon kanssa. SSID-tunnuksellakaan ei välttämättä ole merkitystä, mikäli käyttäjä ei ole tottunut käyttämään jonkin tietyn palveluntarjoajan WLAN-verkkoa. Krakkeri voi myös naamioida kannettavan tietokoneensa tukiasemaksi. [31, s. 57 - 75.]

Tietojen kalastelu on vaivatonta, koska melkein poikkeuksetta käytössä ei ole minkäänlaista salausta. Salauksesta (WPA, WEP) ei kuitenkaan tässä tapauksessa ole hyötyä, koska käyttäjä liittyy tukiasemaan, jonka kummassakin päässä työasemilla on salausavain (encryption key) joiden avulla krakkeri voi purkaa salauksen. Krakkeri voi myös konfiguroida tukiaseman, joka tarjoaa uusille käyttäjille rekisteröitymispalvelun, joka kerää luottokorttien numerot ja henkilökohtaiset tiedot. Rekisteröitymispalvelu on käytössä esimerkiksi monissa hotelleissa, joten huijausta voi olla vaikea epäillä. [31, s. 57 - 75.]

Valetukiasemien ehkäisemiseksi on ikävä kyllä vähän tehtävissä. Valetukiasemia voidaan etsiä skannereilla signaalin perusteella, mutta laitteet tähän ovat kalliita ja ne eivät kerro onko löydetty laite laillinen vai ei. Palveluntarjoajat tietävät mitä tukiasemia heidän järjestelmässään kuuluu olla, mutta järjestelmällinen tarkkailu valetukiasemien varalta ei ole tällä hetkellä mahdollista. Paras ehkäisy on käyttäjien oma varovaisuus, joka perustuu tunnettujen yhteyksien käyttöön ja henkilökohtaisten tietojen varovaiseen käyttöön.

10.2.3 Välistävetohyökkäys (session hijacking)

Välistävetohyökkäys eli yhteyden kaappaus voidaan toteuttaa usealla eri tavalla. Kaikissa tavoissa käytetään hyväksi tietojenkalastelua ja väärentämistä (spoofing). Väärennys kohdistuu yleensä joko IP-osoitteen tai MAC-osoitteen väärentämiseen. Välistävetohyökkäyksessä käytetään niin sanottua Man in the Middle -hyökkäystaktiikkaa, jossa käytetään ARP (Address Resolution Protocol) -protokollan heikkouksia. [31, s. 57 - 75.]

ARP-protokolla

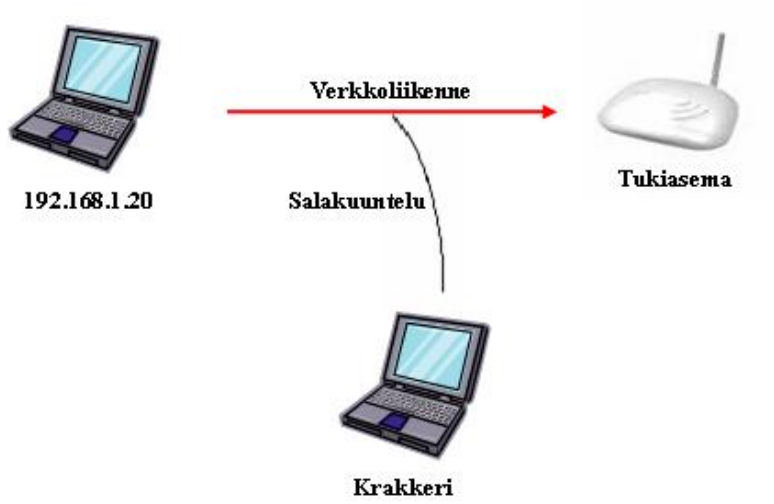
ARP-protokollaa käytetään selvittämään verkkolaitteiden fyysistä eli MAC-osoitetta. Ohjelmat käyttävät IP-osoitetta kohteen selvittämiseksi, mutta verkkokorttien on käytettävä ARP-protokollaa löytääkseen sitä vastaavan MAC-osoitteen. Tämä tapahtuu yleislähettämällä ARP-pyyntöpaketti, joka sisältää kohdeverkkokortin IP-osoitteen. Kaikki verkossa olevat laitteet saavat pyynnön ja IP-osoitetta vastaava laite lähettää vastauksena ARP-paketin, joka sisältää sen MAC- ja IP-osoitteen. Lähettävä laite lisää vastauksen mukana saadun MAC-osoitteen lähetyksen kehyksen kohdeosoitteeksi. Lisäksi laite tallentaa MAC- ja IP-osoitteen ARP-taulukkoon määräajaksi. Krakkerin verkkoon kytkemä laite voi lähettää kysyjälle valheellisen ARP-vastauksen, jonka avulla laite saadaan lähettämään data krakkerin koneelle. Kyseinen tietoturva-aukko voidaan korjata käyttämällä SARP (Secure Address Resolution Protocol) -protokollaa, joka tarjoaa suojatun tunnelin jokaisen työaseman ja tukiaseman välillä. [31, s. 57 - 75.]

Man in the Middle

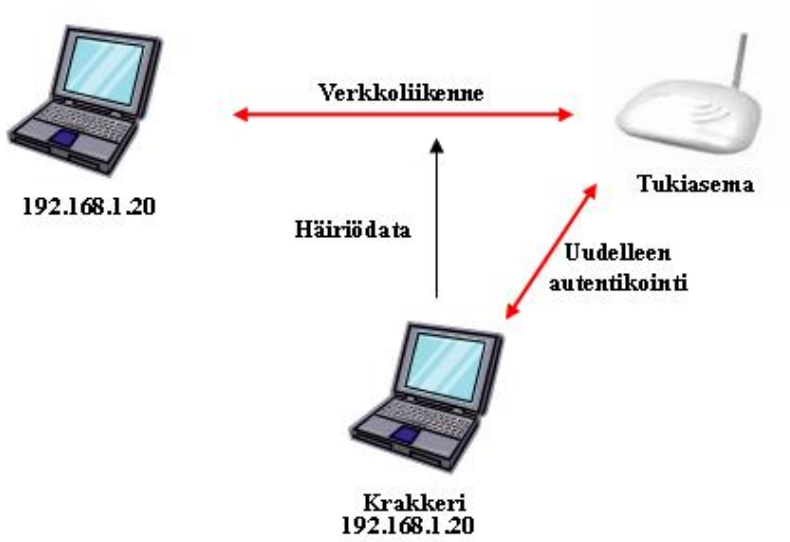
Man in the Middle -hyökkäys voidaan suorittaa esimerkiksi seuraavilla kahdella tavalla:

Tapa 1

Krakkeri hankkii vakoiluohjelman avulla jonkin langattoman verkon työaseman IP-osoitteen ja kirjautumistiedot (kuva 9). Krakkeri käyttää samaa IP-osoitetta kuin työasema ja ujuttaa häiriödataa työaseman yhteyteen saaden tukiaseman uudelleen autentikoimaan käyttäjänsä. Krakkeri autentikoituu työaseman tiedoilla ja ottaa yhteyden hallintaansa (kuva 10). [31, s. 57 - 75.]



Kuva 9. IP-osoitteen ja käyttäjätietojen urkkiminen



Kuva 10. Yhteyden kaappaus uudelleenautentikoinnin avulla

Tapa 2

Krakkeri naamioi kannettavan tietokoneensa langattoman verkon tukiasemaksi käyttäen sen MAC-osoitetta. Krakkeri lähettää asiakkaalle yhteydenkatkaisuviestin, saaden sen uskomaan yhteyden katkenneeksi (kuva 11). Ennen kuin työasema uusii yhteyden, krakkeri naamioituu asiakkaaksi ja kaappaa yhteyden (kuva 12). [31, s. 57 - 75.]

Kuva 11. MAC-osoitteen vakoilu ja yhteyden katkaisu

Kuva 12. Avonaisen yhteyden kaappaus

10.3 Perustietoturvan määrittäminen

Nykyään tietoturva on erittäin tärkeää ja sen määrittäminen vaatii järjestelmällistä suunnittelua. Yrityksen on suositeltavaa laatia tietoturvapolitiikasta kirjallinen suunnitelma, jota käytetään kaikissa yrityksen verkoissa. Etukäteen sovitut tietoturvatavoitteet, turvattavat resurssit, laitteistot ja toimintatavat takaavat yhtenäisen ja turvallisen järjestelmän. Tietoturvan ylläpitämiseksi on syytä testata omatoimisesti sen tasoa ja määritellä seuranta, jolla voidaan monitoroida verkkoon kohdistuvia ulkopuolisia hyökkäyksiä. Testauksesta ja monitoroinnista saatujen tietojen avulla tietoturvaa pyritään kehittämään, jotta se olisi koko ajan tavoitteiden vaatimalla tasolla.

Aina ei kuitenkaan ole mahdollisuutta näin perusteellisen tietoturvapolitiikan määrittelyyn, mutta pitäisi muistaa, että perustietoturvan määrittäminen on nykyään välttämätöntä. Perustietoturvan määrittämien kattaa fyysisen tietoturvan, oletusmääritysten poiston ja etähallinnan rajoittamisen. Nykyään tähän olisi syytä lukea mukaan myös jonkinasteisen salauksen määrittäminen.

10.3.1 Fyysinen tietoturva

Langattomien laitteiden fyysinen tietoturva on ensimmäinen huomioon otettava tietoturvamääritys yritystason WLAN-verkoissa. Laitteiden hallinta ja asetusten muuttaminen konsoliportin kautta voidaan estää oikealla laitteiden sijoittelulla. Tämä voidaan toteuttaa laitteiden sijoittamisella, niin että ne ovat poissa näkyvistä tai muuten hankalasti tavoiteltavissa. Hyvään fyysiseen tietoturvaan kuuluu myös kulunvalvonta. [6, s. 71.]

10.3.2 Oletusmääritysten poistaminen

WLAN-tukiasemien oletusmääritykset on syytä poistaa, koska niitä voidaan käyttää hyväksi hyökkäyksissä. Tukiasemista pitää tarkastaa käyttäjät, salasanat, SNMP-yhteisötunnukset ja SSID-tunnukset. Käyttäjä- sekä hallintatunnukset ja -salasanat tulisi vaihtaa henkilökohtaisiksi ja vaikeasti arvattavaksi. SSID-tunnus kannattaa piilottaa, jolloin se ei näy normaalisti WLAN-verkkoja etsittäessä. Tunnuksen piilottamisella ei kuitenkaan ole tietoturvallisesti juurikaan merkitystä. WLAN-laitteista on syytä poistaa myös kaikki tarpeettomat palvelut. Tärkeimpinä näistä ovat Telnet, TFTP, FTP ja SNMP. [6, s. 71.]

10.3.3 Etähallinta

Fyysisen tietoturvan lisäksi on estettävä tukiasemien etähallinta varmistamalla, että tukiasemissa käytetään vain salattua yhteyttä ja sallimalla hallintayhteydet tietyistä IP-osoitteista. Tämä tarkoittaa Telnet- ja HTTP-palveluiden poistamista käytöstä. Mikäli Web-hallinta halutaan säilyttää, se voidaan korvata HTTPS-palvelulla, mutta se on ainakin syytä rajoittaa ainoastaan lankaverkkoon. [6, s. 71.]

10.4 Päätelaitteen tunnistus

802.11-standardeissa käytetään yksinkertaista yksisuuntaista laitetunnistusta. Tukiasemat tunnistavat päätelaitteen SSID-tunnuksen perusteella ja hyväksyvät yhteyspyynnön vain tunnistetun tunnuksen perusteella. SSID-tunnus on käytännössä salasana, mutta mikäli sitä lähetetään salaamattomana majakkasanomissa, sitä voi käyttää liittymiseen kuka tahansa. Koska SSID-tunnistus ei sisällä minkäänlaista käyttäjätunnistusta ja se käyttää yksisuuntaista liikennettä, ei yhteyspiste pysty tunnistamaan päätelaitetta eikä päätelaite verkkoa luotettavasti. SSID-tunnistuksen puutteiden vuoksi ylimääräisellä yhteyspisteellä voidaan urkkia tietoja, jos käytössä ei ole erillistä salausta tai autentikointia. [6, s. 72 - 73.]

SSID-tunnistuksen puutteita korjaamaan on kehitetty MAC-osoitetunnistus, jonka avulla tukiasemaan voidaan tehdä lista laitteiden MAC-osoitteista, joilla on pääsy verkkoon. Listan ylläpitäminen ja heksadesimaali-osoitteiden syöttäminen on vaivalloista, joten sen käyttö yritystason WLAN-verkoissa on epäkäytännöllistä. Lisäksi MAC-osoitteen vakoilu verkosta ja sen käyttö omassa laitteessa on nykyään helppoa, joten MAC-osoitetunnistus ei ole kovin luotettava tietoturvallisuudenkaan kannalta. [6, s. 73.]

10.5 Salausmenetelmät

Siirtokerroksen (Data Link Layer) salausmenetelmien avulla voidaan suojata langattomien yhteyksien liikenne ja estää luvattomien käyttäjien pääsy verkkoon. Ensimmäiset kehitetyt salausmenetelmät sisälsivät paljon heikkouksia ja niiden murtaminen on helppoa ja nopeaa. Nykyään salausmenetelmiä on useita ja niitä pyritään kehittämään koko ajan lisää. Uusimmat salausmenetelmät ovat lähes murtovarmoja ja yhdessä autentikoinnin kanssa ne muodostavat erittäin turvallisen langattoman siirtoyhteyden. [6, s. 72 - 75.]

10.5.1 WEP (Wired Equivalent Privacy)

WEP-salausmenetelmä oli ensimmäinen 802.11-standardeissa määritelty siirtokerroksen salausmenetelmä. WEP-salaus on symmetrinen eli kaikilla kommunikoivilla laitteilla pitää olla määriteltynä sama avain kuin tukiasemalla. WEP-tunnistus perustuu jaetun avaimen tunnistusmenetelmään, jossa laitteiden välinen tunnistus tapahtuu kuvan 13 mukaisesti. Salausavaimen pituus voi olla 64 (40+24)- tai 128 (104+24)-bittinen, joista 24 bittiä muodostaa alustusvektorin. Salausavain kryptaa lähetetyt paketit käyttämällä RC4-jonosalausta ja pyrkii säilyttämään tiedon eheyden. [6, s. 72 - 75.]

Kuva 13. Jaetun avaimen tunnistusmenetelmä

Avaimen tunnistus (Kuva 13)

- Työasema haluaa liittyä langattomaan verkkoon ja lähettää tukiasemalle autentikointipyynnön (Authentication Request). Viestissään työasema ilmoittaa käyttävänsä jaetun avaimen tunnistusta.

- Tukiasema vastaa pyyntöön lähettämällä haasteen (Challenge), jossa se pyytää jaettua avainta lähettämällä tunnistusalgoritmin ja satunnaisen haastetekstin.

- Työasema lähettää vastauksena saamansa tunnistusalgoritmin ja haastetekstin salaamalla informaation WEP-avaimellaan.

- Tukiasema purkaa saamansa vastauksen omalla WEP-avaimellaan ja vertaa sitä lähettämäänsä haasteeseen. Mikäli haaste on pysynyt samana, tukiasema lähettää vastauksena autentikointivarmistusviestin.

10.5.2 TKIP (Temporal Key Integrity Protocol) (WPA)

WPA (Wireless Fidelity Protected Access) -tietoturvatekniikka kehitettiin korjaamaan WEP-salauksen puutteita. WPA käyttää TKIP (Temporal Key Integrity Protocol) -salausta. TKIP-salaus käyttää henkilökohtaista 128 bitin salausavainta (RC4-algoritmilla) ja 48 bitin vaihdettavaa aloitusvektoria. Näiden ansiosta WEP-salauksessa ilmenneitä avainten uudelleenkäyttöä ja heikkojen alustusvektoreiden ongelmia saatiin parannettua. TKIP mahdollistaa ryhmälähetys- ja levitysviestikehysten salausavaimen kierrätyksen (Broadcast Key Rotation), mutta levitysviestikehysten kierrätys vaatii LEAP- tai EAP-TLS-tunnistusta. TKIP käyttää MIC- (Message Integrity Check) sanoman eheyden tarkistusta, joka on kryptograafisesti paljon vahvempi kuin WEP-salauksessa käytetty sanoman eheytystekniikka. MIC-tekniikka paljastaa myös sanomien väärennysyritykset. [6, s. 82.]

WPA-tekniikasta on olemassa kaksi eri versiota, yrityskäyttöön ja kuluttajakäyttöön. Ominaisuudet kummassakin ovat identtisiä, mutta yrityksille tarkoitetussa versiossa käytetään autentikointipalvelua.

WPA-Enterprise

Enterprise-versiossa on käytettävä autentikointipalvelua, joka voi olla ulkoinen palvelin tai tukiasema, mikäli se tukee paikallista autentikointipalvelua. Autentikointipalvelun lisäksi Enterprise-versiossa on käytettävä porttikohtaista EAP-autentikointia. [38; 40.]

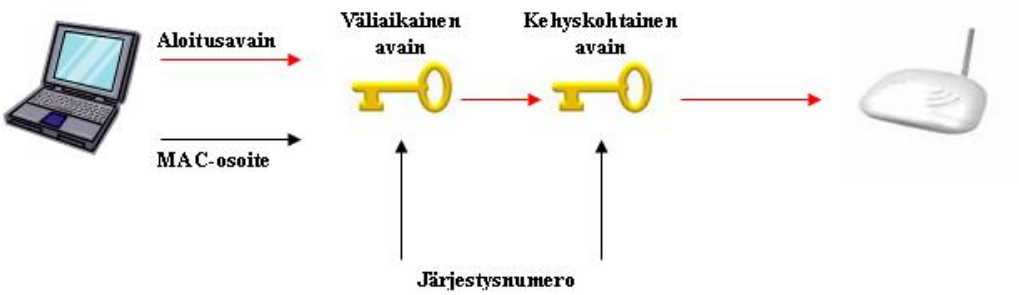
WPA-Standard

Standard-versio eli WPA-PSK (Pre-Shared Key) on kuluttajakäyttöön tarkoitettu versio, joka ei vaadi EAP-autentikointia, eikä autentikointipalvelua. Standard-versiossa kirjautuminen tapahtuu TKIP-salatulla salasanalla. [38; 40.]

TKIP-salausavaimen generointi (Kuva 14)

- Työasema ja tukiasema muodostavat yhteyden 128-bittisellä väliaikaisella avaimella, joka muodostuu aloitusavaimesta, työaseman MAC-osoitteesta ja järjestysnumeron neljästä eniten merkitsevästä bitistä.

- Väliaikainen avain yhdistetään järjestysnumeron kahteen alimpaan bittiin, jolloin saadaan kehyskohtainen avain.



Kuva 14. TKIP-salausavaimen generointi

TKIP-salauksessa jokainen tukiasema käyttää eri istuntokohtaista avainta jokaista työasemaa kohden, joka vaihtuu 10 000 kehyksen välein. Varsinainen salausavain on eri jokaisella lähetetyllä kehyksellä. Kehyksen IV-kenttä on salattu, mikä parantaa alustusvektoreiden suojausta. [6, s. 83.]

TKIP-salauksen vaihtuva istuntokohtainen avain vaikeuttaa krakkereiden salauksen murtamista, koska dataa ei ehdi kerätä tarpeeksi ennen avaimen vaihtumista. WPA-tekniikka puolustautuu verkkohyökkäyksiä vastaan sulkemalla verkon minuutiksi kaikilta käyttäjiltä. Tämä puolustusmekanismi on käytännössä huono ominaisuus, koska palvelunestohyökkäyksellä tukiasema saadaan sulkemaan yhteytensä jatkuvasti, jolloin se estää verkon käytön kokonaan myös sallituilta käyttäjiltä. [6, s. 83.]

10.5.3 CCMP (Counter Mode with CBC-MAC Data Origin Authenticity Protocol) (802.11i / WPA2 / AES)

Kesäkuussa 2004 IEEE:n LMSG-ryhmä määritteli 802.11i-standardin (MAC Enchancements for Enhanced Security), joka tunnetaan myös nimellä WPA2 (Wireless Fidelity Protected Access versio 2). WPA2 sisältää edellä esitellyt WEP-salauksen parannukset, TKIP-salauksen sekä uuden CCMP-lohkosalausmenetelmän. CCMP on tällä hetkellä uusin ja paras salausmenetelmä, eikä sitä ole vielä pystytty murtamaan vahvan AES (Advanced Encryption Standard) -lohkosalauksen ansiosta. WPA2-tekniikkaa on mahdollista käyttää kahdessa eri tilassa, WPA2-Personal ja WPA2-Enterprise tilassa. [6, s. 83; 39.]

WPA2-Enterprise

Enterprise-versio käyttää avaintenhallintaa, joka perustuu avainpareihin. Avaintenhallinta vaatii porttikohtaisen autentikoinnin (EAP) ja autentikointipalvelun käytön. Erillistä autentikointipalvelinta ei kuitenkaan tarvita, jos tukiasema tukee paikallista autentikointipalvelua. Työasemaan ja autentikointipalvelimeen (tukiasema) määritetään uniikki yleisavain, jonka avulla muut tarvittavat avaimet saadaan muodostettua. Työaseman ja tukiaseman liikenne salataan määrä-ajoin vaihtuvalla parittaisella lähetysavaimella. [6, s. 83; 39.]

WPA2-Standard

Standard-versio on suunniteltu kuluttajille ja se käyttää myös AES-algoritmia salaukseen, mutta ei vaadi autentikointipalvelua. Tukiasemiin kirjautuminen tapahtuu käyttämällä pelkästään salasanaa. [39.]

Tukiasemien ja työasemien välistä yhteyttä hallitsee RSN (Robust Security Network) -protokolla. WPA2 tukee esitunnistusta (Pre-authentication) ja mahdollistaa siirtymisen tukiasemasta toiseen ilman uudelleen tunnistusta. Tunnistustiedot välitetään tukiasemille tunnistuspalvelimelta. WPA2 tukee myös PEAP-tunnistusta, josta lisää edempänä. [6, s. 84; 37.]

CCMP-lohkosalaustekniikka käyttää AES-salausta, joka käyttää Rijndael-algoritmiä ja 128, 192 ja 256 bitin salausavainta. AES-salaus on niin vahva, että sen käyttö vaatii erillisen salauspiirin, tai laitteiden suorituskyky laskee huomattavasti. [6, s. 84.]

10.6 Autentikointipalvelimet

Käyttäjän tunnistukseen voidaan käyttää erillistä autentikointipalvelinta (AAA-palvelin), kuten RADIUS (Remote Authentication Dial In User Service) -palvelinta. Autentikointipalvelimia tarvitaan, kun halutaan käyttää AAA (Authentication, Authorization and Accounting) -palvelua. AAA-palvelin sisältää keskitetyn käyttäjätietokannan asiakkaista ja käyttöoikeuksista. Palvelun käyttö vaatii jonkin AAA-protokollan (esimerkiksi RADIUS) käytön, joka vastaa tiedonkulusta palvelimen ja asiakkaan välillä. AAA-protokollan kanssa voidaan käyttää EAP-protokollaa, joka hoitaa autentikointiviesteistä ennen asiakkaan autentikoitumista.

10.7 Porttikohtainen autentikointi (EAP)

EAP (Extensible Authentication Protocol) -protokolla kehitettiin PPP-protokollan yhteydessä käyttäjientunnistusprotokollaksi. EAP osoittautui käyttökelpoiseksi, joten IEEE sovitti sen toimimaan 802.1x (Port Based Authentication) -standardin kanssa. 802.1x-standardin eli porttikohtaisen autentikoinnin tarkoituksena on estää luvattomien laitteiden kommunikointi lähiverkon liityntäpisteen kautta ja langattomissa verkoissa loogisen portin kautta. EAP-tekniikkaa käytetään WPA- ja WPA2-salausmenetelmien kanssa. EAP ei kuitenkaan ole autentikointitapa vaan autentikointiprotokollan runko, jonka avulla autentikointi valitaan. EAP-tekniikoita on olemassa noin 40 erilaista, mutta tässä kappaleessa esitellään yleisimmät WLAN-tekniikkaan soveltuvat EAP-autentikointimenetelmät.

10.7.1 LEAP (Lightweight Extensible Authentication Protocol)

LEAP on Cisco Systemsin kehittämä autentikointimenetelmä, joka kehitettiin korjaamaan EAP:n puutteita. LEAP tarjoaa kaksisuuntaisen tunnistuksen ja mahdollisuuden käyttää Microsoftin aktiivihakemistoa (Active Directory) WLAN-tunnistuksen yhteydessä. Vaihtuvaa WEP-avainnusta käytettäessä on käytettävä TKIP-protokollaa huolehtimaan avainten vaihdosta. Alun perin LEAPin käyttö edellytti Ciscon sovittimien ja ohjelmistojen käyttöä, mutta nykyään LEAPia voidaan käyttää myös muiden valmistajien sovittimilla ja ohjelmistoilla. Todellisuudessa LEAP kärsii heikosta käyttäjien autentikoinnista, joka toteutetaan muokatun MS-CHAPv2-autentikointiprotokollan avulla. Joshua Wright on kehittänyt ohjelman Asleap, jolla on mahdollista kaapata LEAP- ja PPTP-salasanoja. [6, s. 78; 54.]

10.7.2 EAP-TLS (EAP-Transport Layer Security)

EAP-TLS parantaa EAP-salausmenetelmää mahdollistamalla molemminpuoleisen tunnistuksen, turvallisen istuntoavainten vaihdon ja Microsoft 200x Server- ja LDAP-järjestelmään (Lightweight Directory Access Protocol) kirjautumisen. TLS-tunnistusta tuetaan laajalti, mutta se käyttää digitaalisia X.509-sertifikaatteja, joten sen käyttöönotto on hankalaa. EAP-TLS on yksi turvallisimmista EAP-salausmenetelmistä. [6, s. 79.]

10.7.3 EAP-TTLS (EAP-Tunneled Transport Layer Security)

EAP-TTLS on TLS-salauksen seuraaja, joka helpottaa sertifikaattikäytäntöä ja ottaa käyttöön suojatun yhteyden (secure connection tunnel) käyttäjän autentikoinnin ajaksi. Suojatun ”tunnelin” ansiosta EAP-TTLS antaa suojan salakuuntelulle ja välistävetohyökkäyksille. [56.]

10.7.4 PEAP (Protected EAP)

Cisco Systemsin, Microsoftin ja RSA Securityn kehittämä PEAP muistuttaa EAP-TTLS-salausta. PEAP muodostaa suojatun yhteyden työaseman ja autentikointipalvelimen välille, mutta se ei salaa lainkaan liikennettä niin kuin muut EAP-tekniikat. [57.]

10.7.5 EAP-FAST (Flexible Authentication via Secure Tunneling)

Cisco Systems kehitti EAP-FAST-protokollan korvaamaan LEAPia ja sen puutteita. Palvelintason sertifikaattien käyttö ei ole pakollista EAP-FASTssa. Se käyttää PACia (Protected Access Credential) muodostaakseen TLS-tunnelin käyttäjätunnistusta varten. [58.]

11 KESKITETTY TUKIASEMIEN HALLINTA

Keskitetysti hallittu WLAN-verkko on koko ajan yleistyvä tekniikka, joka mahdollistaa entistä tehokkaamman, vikasietoisemman, monipuolisemman ja helposti hallittavan langattoman järjestelmän. Tällä hetkellä järjestelmän hankintakustannukset rajoittavat asiakaskuntaa, mutta tekniikan kehittyessä ja kulutuksen lisääntyessä on mahdollista, että hinnat laskevat. Tällä hetkellä keskitetystä hallinnasta ei ole ratifioitu yleistä standardia, mutta IETF (Internet Engineering Task Force) on kehitellyt protokollaluonnoksen CAPWAP (Control And Proviosing of WIRELESS APS), jota käytetään langattomien tukiasemien keskitettyyn hallintaan. Projekti on jäänyt luonnosasteelle, mutta monet eri tahot ovat kehittäneet omia protokollia tukiasemien keskitettyä hallintaa varten. [41; 42.]

Normaaleissa WLAN-verkoissa tukiasemat vastaavat liikenteen jakamisesta, radiotien varaamisesta, tietoturvasta, käyttäjien ja laitteiden autentikoinnista ja monista muista toiminnoista. Mikäli kyseessä on iso WLAN-verkko, järjestelmän ylläpito on kustannuksiltaan kallista ja vaatii paljon henkilöstöä. Tietoturvahyökkäyksien havaitseminen ja estäminen ilman keskitettyä hallintaa on melkeinpä mahdotonta.

Split-MAC

Keskitetty hallinta perustuu split-MAC tekniikkaan, joka erottaa reaaliaikaiset piirteet hallinnollisista piirteistä. Tekniikka siirtää autentikoinnin sekä tietoturvan- ja liikkuvuudenhallinnan WLAN-kontrollereihin ja jättää reaaliaikaisten datakehysten vaihdon ja erinäisten MAC-osoitteiden hallinnan tukiasemille.

11.1 Protokollat

Tekniikan kehittyessä ja uusien laitteiden ilmestyessä on tarve luoda yhteinen standardi laitteille, jotka käyttävät keskitettyä hallintaa. Kuluttajien kannalta ikävää on, että vielä ei ole määritelty yhtä tiettyä mallia, jota valmistajat käyttäisivät. Seuraavaksi esitellään protokollamalleja, jotka tukevat keskitettyä hallintaa ja ovat ehdolla yleiseksi standardiksi, jota IETF pyrkii muodostamaan. Kaikilla keskitetyn hallinnan protokollamalleilla on peruspiirteiltään samanlainen laitteisto, joka muodostuu WLAN-kontrollerista ja keskitettyä hallintaa tukevista tukiasemista. Jotkut laitteistot vaativat lisäksi erillisen WLAN-kontrolleria tukevan kytkimen. Tässä työssä esitellään tarkemmin Cisco Systemsin LWAPP-protokolla ja Hewlet-Packardin WESM-protokolla laitteineen.

11.1.1 SLAPP (Secure Light Access Point Protocol)

Trapeze Networks on kehittänyt SLAPP-tekniikan, joka määrittelee kuinka tukiasema keskustelee kontrollerin (access controller) kanssa. SLAPP käsittää tällä hetkellä tarvittavat protokollat tukiasemien hallintaan ja tulevaisuuden standardien tukiasemien hallintaan. SLAPP tarjoaa tuen eri valmistajien tukiasemille toimia yhdessä kontrollerin kanssa. [42.]

11.1.2 CTP (CAPWAP Tunneling Protocol)

Chantry Networks ja Progate ovat kehittäneet keskitetylle tukiasemien hallinnalle CTP-protokollan. CTP toimii tasolla 3 ja tarjoaa lyhyet tukiasemien vaihtoajat. CTP-tekniikan avulla VoIP-palveluiden käyttö on mahdollista WLAN-verkoissa. Tekniikan on tarkoitus tukea eri valmistajien laitteita tarjoten universaalin WLAN-laitteiden hallinnan. [49; 50.]

11.1.3 WiCoP (Wireless LAN Control Protocol)

WiCoP käyttää tekniikkaa, joka mahdollistaa yleisimpien WLAN-arkkitehtuurien käytön erilaisilla laitteilla. WiCoP tukee eri valmistajien laitteita ja mahdollistaa näin ollen edullisen tavan päivittää WLAN-verkko keskitetysti hallittavaksi. Tekniikka mahdollistaa myös tulevaisuuden laitteiden integroimisen järjestelmään. [51.]

11.1.4 LWAPP (Light weight Access Point Protocol)

Ensimmäinen CAPWAP-protokollaan perustuva LWAPP-protokolla julkaistiin Airespacen, D-Linkin, NTT Docomon ja Ciscon toimesta. LWAPP-tekniikka perustuu Lighweight-tukiasemiin, joita hallitsee WLAN-kontrolleri. Kontrollerin tehtävänä on hoitaa tukiasemien normaalisti toteuttamat tehtävät kuten pääsynhallinta, tietoturva ja liikenteen hallinta (Quality of Service [QoS]). LWAPP-tekniikan avulla voidaan hallita keskitetysti koko järjestelmän radiotaajuutta. Tämä mahdollistaa kanavien varauksen, lähetystehon määrittämisen ja liikenteen rajoittamisen keskitetysti. LWAPP mahdollistaa lisäksi automaattisen tukiasemien ohjelmiston päivityksen kontrollerin kautta. [43.]

LWAPP-protokollaa voidaan käyttää kahdella eri OSI-mallin tasolla. Tasolla 2 (ethernet-kehyksessä) kontrollerin ja tukiaseman tulee sijaita samassa aliverkossa tai olla suoraan kytkettyinä. Tasolla 2 toimiva LWAPP lupaa tukiasemien siirtymisajaksi (handoff) alle 14 ms. Tasolla 3 (UDP/IP-kehyksessä) kontrolleri ja tukiasema voivat olla kytkettyinä myös eri aliverkkoihin. Tasolla 3 toimiessa tukiasemat saavat IP-osoitteen DHCP-palvelimelta. Tukiasemien siirtymisajaksi luvataan alle 30ms. [43.]

Tukiasemia, jotka toimivat itsenäisesti ja lightweight-tukiasemina, ovat esimerkiksi Cisco Aironet 1130AG ja Cisco Aironet 1240AG -tukiasemat. Cisco 1000-sarjan Lightweight-tukiasemat (kuva 15) on suunniteltu pelkästään keskitetyn WLAN-verkon tukiasemiksi. Eräitä sarjan tukiasemien ominaisuuksia ovat seuraavat [52.]:

- Tuki 802.11a/b/g/h -standardeille
- Tuki LWAPP-protokollalle, Zero-Touch-konfiguroinnille ja keskitettylle hallinnalle
- Datapalvelun ja ilmatien samanaikainen tarkkailu
- Reaaliaikainen radiotaajuuksien hallinta
- Sisäinen antenni, liitäntä ulkoiselle antennille
- Laadunvalvonta (QoS) ja langaton tunkeutumisen esto IPS (Intrusion Prevention System).
- Uusimmat salausmenetelmät
- Tason 2 ja 3 roaming

Kuva 15. Cisco Aironet 1000 series

WLAN-kontrollerit ovat hallitun WLAN-verkon perusta. Cisco Systems tarjoaa tällä hetkellä kolme eri vaihtoehtoista WLAN-kontrolleria (kuva 16). Cisco 2106, 4402 ja 4404 Wireless LAN Controller tarjoavat samat perusominaisuudet, mutta eroavat liitännöiltään ja liitettävien tukiasemien määrältä. Kontrollereiden tärkeimmät ominaisuudet ovat seuraavat:

- Tuki 802.11a/b/g/d/h -standardeja
- Tuki uusimmille salaus- ja autentikointimenetelmille
- Useita eri hallinnointimahdollisuuksia (HTTP/HTTPS/Telnet/SSH)
- Lightweight tukiasemien maksimimäärä
  - 6 kpl (Cisco 2106)
  - 12/25/50 kpl (Cisco 4402)
  - 100 kpl (Cisco 4404)
- Lukuisia liitäntöjä mallista riippuen

Kuva 16. Cisco Wireless LAN Controllers

Cisco tarjoaa lisävarusteena langattoman kontrollointijärjestelmän (WCS), joka tarjoaa suurille WLAN-järjestelmille kattavan hallintajärjestelmän. WCS (Wireless Control System) toimii yhdessä WLAN-kontrollereiden kanssa. WCS tarjoaa seuraavanlaisia ominaisuuksia: [53.]

- Satojen WLAN-kontrollereiden ja tuhansien tukiasemien hallinta
- Mahdollisuus hallita eri verkkojen laitteita konsernin laajuisesti
- WLAN-verkkojen suunnittelu ja toteutustyökalut (vertaa Ekahau)
- Visuaalinen verkonhallinta ja vikaselvitys
- Muokattava käyttäjien hallinta (vierailijat/työntekijät)
- WLAN-päätteiden seuranta
- Monipuolinen tietoturvapolitiikka

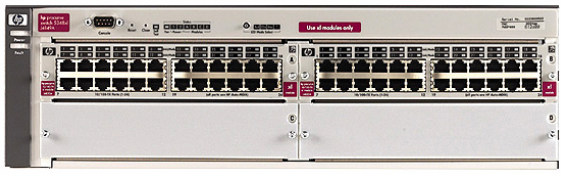
11.1.5 WES (Wireless Edge Services)

Hewlett Packard on kehittänyt WES-radioporttijärjestelmän, joka perustuu EDGE (Enchanced Data rates for Global Evolution) -pakettidatatekniikkaan. Tekniikka perustuu radioporttitukiasemiin (kuva 18) (vrt. lightweight-tukiasemat), joita hallitaan WES-moduulilla (kuva 17). Moduulin avulla voidaan hallita keskitetysti laitteita ja käyttäjiä riippumatta käytetystä yhteystekniikasta. Mainitsemisen arvoista on myös, että laitteella on elinikäinen takuu. [27] [46]

Kuva 17. ProCurve Wireless EDGE Services xl module [46]

Kuva 18. ProCurve Radio Port 220 [47]

WES-moduuli kytketään 5300xl-sarjan kytkimeen (kuva 19), johon radioporttitukiasemien LAN-kaapelointi kytketään. WES-moduuli tukee 12 tukiasemaa ja siihen on mahdollista ostaa lisää lisenssejä kaksi 12 kappaleen pakettia. Maksimissaan moduuli voi hallita siis 36 tukiasemaa. Kytkimiin on mahdollista liittää 2 moduulia, joten yksi kytkin voi hallita 72 tukiasemaa. [46.]



Kuva 19. ProCurve Networking Switch 5348xl [45.]

WES-moduulia voidaan hallita ProCurve Manager Plus-ohjelmalla, joka on tarkoitettu kaikkien ProCurve-laitteiden hallintaan. Lisäksi on mahdollisuus hankkia ProCurve Identity Driven Manager (IDM), joka laajentaa Manager Plus-ohjelmaa. IDM:n avulla voidaan oikeuksia hallita erittäin laajasti ja monipuolisesti. Ohjelman avulla voidaan rajoittaa käyttäjien oikeuksia ja yhteyden nopeutta sekä käyttää eri virtuaaliverkkoja (VLAN) eri käyttäjille. WES-järjestelmään on myös mahdollista liittää erillinen autentikointi-palvelin (kuva 20) (vrt. RADIUS), joka on optimoitu ProCurve-laitteilla toteutetun verkon pääsynhallintaan.

Kuva 20. ProCurve Wireless Network Access Control Server 745wl [44.]

Kolmas hallintaohjelma on ProCurve Mobility Manager, jolla voidaan keskitetysti hallita tärkeimpiä WLAN-laitteiden ominaisuuksia. Mobility Manager mahdollistaa tukiasemien päivitykset, valvonnan ja vikaselvityksen. Ohjelmalla voidaan valvoa myös verkon tietoturvaa, asetuksia ja langattomien verkkoon liittyviä laitteita.

WES-radioporttijärjestelmän käyttö tuo paljon etuja normaalin WLAN-verkkoon verrattuna. Lyhyesti esiteltynä tärkeimmät radioporttijärjestelmän edut ovat seuraavat:

- Radioporttitukiaseman vikaantuessa viereisten tukiasemien lähetysteho-jen säätyminen automaattisesti
- Kanavien automaattinen säätö häiriöiden perusteella
- Mahdollisuus varamoduulin liittämiseen, joka voi ottaa vikatilanteessa ver-kon hallintaan lennosta
- Tukiasemien keskitetty konfigurointi ja päivitys
- Nykyaikaiset tietoturva-asetukset
- Ylivoimaiset hallintaominaisuudet

12 LOGISTIIKKA-ALAN WLAN-VERKON SUUNNITTELU JA TOTEUTUS

Digix Oy suunnittelee WLAN-ratkaisuja painottuen logistiikka-alan yrityksiin. Tässä insinöörityössä esitellään kaksi erilaista WLAN-toteutusta, jotka eroavat toisistaan, niin laitteellisesti, kuin toteutustavaltakin. Molemmat työt on toteutettu suurille logistiikka-alan yritykselle ja tietoturvallisista syistä joitakin asioita on jätetty julkaisematta tai tietoja on muutettu.

Tässä luvussa esitellään logistiikka-alan WLAN-verkkojen suunnittelua ja toteutusvaiheita. Esitetyt tavat eivät ole ainoat oikeat, mutta niiden avulla on helppo päästä sisälle logistiikka-alan WLAN-verkon suunnitteluun. Työssä esitellään myös menetelmiä ja näkökulmia, jotka eivät välttämättä ole yleisesti käytössä. Käytännön kautta todettujen tekniikoiden on todettu edistävän verkon suunnittelua ja toteutusta. Kappaletta täydentää kappaleissa 14 ja 15 esitetyt käytännönläheisemmät esimerkit.

Työssä käsitellään 2,4 GHz:n taajuusalueella rakennettuja verkkoja, koska tämän taajuusalueen käyttö nykyään on yleisintä ja Digix Oy:n asiakkaiden verkot käyttävät 2,4 GHz:n laitteita. Työssä esitetyt menetelmät soveltuvat osittain myös 5 GHz:n taajuusalueella toteutettuihin WLAN-verkkoihin, mutta esimerkiksi laitevalinnoissa ja tukiasemien sijoittelussa on eroja. Periaatteet säilyvät kuitenkin, riippumatta siitä kumpaa taajuusaluetta käytetään.

Verkon suunnittelu ja toteutus yksinkertaistettuna sisältävät seuraavat toimenpiteet toteutusjärjestyksessä:

- Verkkoarkkitehtuurin valitseminen verkon koon ja tarpeen mukaan
- Verkon suunnittelu teoriassa
- Laitteiston valitseminen
- Testimittaukset
- Laitteiston konfigurointi ja asennus (kaapelointi, yms.)
- Verkon testaus ja optimointi
- Raportointi
- Valvonta ja ylläpito

12.1 Keskitetty hallinta vai ESS-verkko

Aivan ensimmäinen asia langattoman verkon suunnittelussa on verkkomallin valinta. Kohdepaikkaan tutustuminen on lähes välttämätöntä ja pohjapiirustuksesta on huomattavaa etua. Keskitetysti hallittu WLAN-verkko on melkein aina parempi ratkaisu laadultaan kuin normaali ESS-verkko, mutta kokonaisuus ratkaisee. Pitää miettiä mikä on välttämätöntä, jotta saavutetaan hyvä lopputulos. Mikäli toteutettava kohde on suuri ja se vaatii lukuisia tukiasemia, on kustannustehokasta rakentaa keskitetysti hallittu WLAN-järjestelmä. Verkon ylläpitokustannukset on siis otettava huomioon jo verkon suunnitteluvaiheessa.

12.2 Teoreettinen suunnittelu

Verkkoarkkitehtuurin valinnan jälkeen alkaa teoreettinen verkon suunnittelu. Suunnittelu pitää sisällään kirjallisen dokumentaation toteutettavasta verkosta ja siitä miten se toteutetaan. Esimerkiksi testimittaukset on suunniteltava huolella, jotta saadaan selville mahdolliset yllätyselementit ennen verkon asentamista. Nykyään ehkä tärkein vaihe verkon suunnittelussa on verkkotietoturvan määrittäminen.

Ensimmäiseksi kannattaa aloittaa tukiasemien sijoittamisella kartalle. Tässä vaiheessa on viimeistään syytä käydä paikan päällä katsomassa kohdetilaa, koska kaikkea huomioonotettavaa ei voi millään merkitä pohjapiirustuksiin. Tukiasemien esisijoittamisessa on kolme vaihetta:

- Tukiasemien sijoittaminen arvioitujen kuuluvuuksien perusteella
- Asennusteknisten seikkojen huomioonottaminen
- Kanavoinnin huomioonottaminen

Tukiasemien sijoittaminen kartalle

Ensimmäisessä vaiheessa tukiasemien kuuluvuudet arvioidaan niin, että koko tarvittava alue saavuttaa halutun kuuluvuustason. Tässä vaiheessa pitää ottaa huomioon materiaalivaimennukset ja häiriölähteet, joista lisää myöhemmin. Tukiasemia ei voida sijoittaa liian lähekkäin, jotta ne eivät häiritse liikaa toisiaan.

Asennustekniset seikat

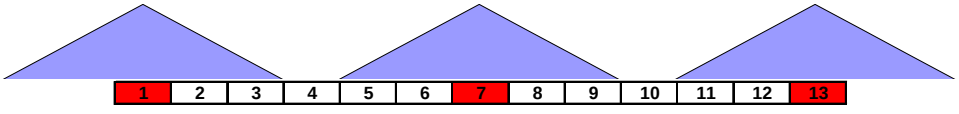
Kun tukiasemat on saatu sijoitettua kartalle, on tarkistettava, että niiden asennus kyseisille paikoille on mahdollista ja järkevää. Ensimmäiseksi tarkastetaan, että tukiasemalle on mahdollista asentaa LAN-kaapelointi pituusrajoituksen (100 m ristikytkentään) puitteissa. Toiseksi varmistetaan, että tukiaseman ja mahdollisen antennin asentaminen on mahdollista. Tukiasema on syytä sijoittaa käytävälle tai muuten avoimeen tilaan. Viimeiseksi katsotaan, että tukiaseman paikka on asennettuna sellaisessa tilassa, että se ei ole vaarassa rikkoutua esimerkiksi trukkien nostaessa tavaraa ylähyllyille. Tukiasemien kotelointia on myös syytä harkita, mikäli tila on erittäin pölyinen tai muuten olosuhteiltaan vaativa.

Kylmävarastot

Työssä keskitytään logistisiin varastoihin suunniteltaviin varastoihin, joten säätila ei vaikuta laitteistojen toimintaan. Varastot voivat kuitenkin olla myös kylmävarastoja, jolloin lämpötilan vaihtelut voivat vaikuttaa laitteiden toimintakykyyn. Kylmävarastoissa on syytä käyttää kotelointia, johon on mahdollista asentaa termostaatti ja vastus lämmittämään tukiasemaa. Esimerkiksi suomalainen Fibox Oy valmistaa sähkölaitteille suojakoteloita, jotka soveltuvat erinomaisesti myös tukiasemien kotelointiin.

Kanavointi

Kanavoinnin huomioonottaminen tässä vaiheessa voi tuntua liian aikaiselta, mutta se on todellisuudessa erittäin hyödyllistä. Kanavoinnin suunnittelussa selviää, mikäli tukiasemia on sijoitettu liian tiheään. Aina pitäisi pyrkiä siihen, että kanavointi tapahtuisi niin, että mikään kanava ei kuulu toisten yli, mutta logistisissa varastoissa tämä on harvoin mahdollista. Paras mahdollinen tilanne on, kun tukiasemien kanavien välissä on vähintään viisi kanavaa (kuva 21).



Kuva 21. Kanavien ylikuuluminen

Tukiasemissa on yleensä myös mahdollisuus asettaa kanavointi automaattiseen tilaan, jolloin käytössä pitäisi olla aina parhaiten kuuluva kanava. Kokemuksien mukaan tämä ei kuitenkaan toimi oikein ja se aiheuttaa toiminnallisia ongelmia, kuten tukiasemaan liittymisongelmia. Keskitetysti hallitut tukiasemat käyttävät myös automaattista kanavointia, mutta siinä toteutus on erilainen, joten se myös toimii. Keskitetysti hallituissa järjestelmissä on myös mahdollisuus käyttää vain yhtä kanavaa, jolloin tukiasemista muodostetaan yksi yhtenäinen tukiasema (katso kappale 12).

Vaimentavat materiaalit

Rakennettaessa langatonta lähiverkkoa rakennettaessa logistiseen varastoon, hyvin tärkeitä ovat vaimentavat materiaalit eli kaikki tavara mitä hyllyissä varastoidaan. Varastot ovat usein isoja ja korkeita, joten pinta-ala aiheuttaa jo itsessään ongelmia hyvän WLAN-verkon rakentamiselle. Melkein poikkeuksetta koko varaston tulee kuulua langattoman lähiverkon piiriin, joten tukiasemia voi joutua sijoittamaan lukuisia kappaleita esteistä riippuen. Tukiasemien määrää rajoittaa kuitenkin kanavien ylikuuluminen, jos vierekkäisiä kanavia tulee liikaa tiheän tukiasemasijoittelun vuoksi.

Varastotiloissa ei ole juuri lainkaan seiniä, vaan tilat ovat täynnä varastohyllyjä, jotka saattavat ylettyä katonrajaan saakka, jopa 8 m:n korkeuteen. Erilaisten materiaalien vaimennusarvot (kuva 22) on hyvä tietää ennen kuin suunnitellaan tukiasemien sijoittelua. Varastoissa on myös yleistä, että tietyt alueet rajataan metallisilla verkkoseinillä, jolloin syntyy Faradayn häkki. Faradayn häkki estää radioaaltojen liikkumisen melkein kokonaan, joten sitä voidaan käsitellä paksuna seinänä.

Materiaalien vaimennuksia

Kirjahylly	2 dB	Lasi + neste (lava)	6 dB
Koppi	1 dB	Paperi (lava, rulla)	6 dB
Ohut-ovi	2 dB	Muovi + neste (lava)	4 dB
Hissi	30 dB	Metalliosia (lava)	3 dB
Tiiliseinä	10 dB	Hylly + metalliosia	3 dB
Kiinteä seinä	12 dB	Puumateriaali	2 dB
Kipsilevyseinä	3 dB	Kivimateriaali	5 dB
Ikkuna	1 dB	Metallihäkki	30 dB
Paksu ikkuna	3 dB		

Kuva 22. Materiaalien keskimääräisiä vaimennuksia

Erilaiset materiaalit vaimentavat eri tavoin, mutta suurin tekijä on kuitenkin kuinka tiheässä ne ovat. Uuden varastohallin WLAN-verkon suunnittelu voi olla haastavaa, mikäli se pitää rakentaa valmiiksi ennen kuin varastohyllyissä on tavaraa. Kokemuksesta on siis etua, jotta osaa arvioida materiaalin vaimennuksen, mikäli sitä ei voida arvioida mittaamalla. Tällaisessa tapauksessa langatonta verkkoa voidaan joutua vahvistamaan jälkikäteen ylimääräisillä tukiasemilla.

Konkreettisia tuloksia ei kuitenkaan kannata sivuuttaa, vaan testimittaukset ennen tukiasemien asennuksia on syytä suorittaa. Testimittaukset suoritetaan yleensä yhdellä tukiasemalla, jonka paikkaa vaihdellaan etukäteen valittujen paikkojen mukaan. Materiaalivaimennuksen huomioon ottaminen suunnitteluvaiheessa voi siis helpottaa testimittauksia huomattavasti ja todennäköisesti säästää turhalta vaivalta, kun testimittaukset tukevat suoraan suunniteltua tukiasemasijoittelua.

Muut häiriötekijät

Vaimentavien materiaalien lisäksi on otettava huomioon myös muut häiriötekijät, jotka vaikuttavat tukiasemiin, kaapelointiin ja työasemiin. Kaikki 2,4 GHz:n radiotaajuusaluetta käyttävät laitteet vaikuttavat WLAN-verkon toimivuuteen. Tällaisia laitteita ovat kaikki mikroaaltouunit, bluetooth laitteet ja jotkut radiopuhelimet. Työasemissa onkin usein bluetooth-sovitin, jota ei kannata pitää päällä ellei sitä käytä. Kaapelointiin vaikuttavat häiriötekijät on syytä ottaa huomioon, koska niiden poistaminen jälkikäteen on yleensä mahdotonta. Kaapeleissa kulkevaan dataan aiheuttavia häiriötekijöitä on muun muassa sähkökaapelit. Varastotiloissa tukiasemien sijoittelu tapahtuu usein katonrajaan, joten asennuspaikka sijaitsee usein lamppukiskossa. LAN-kaapelointi kulkee siis usein sähköjohtojen parissa, joten on suositeltavaa käyttää vähintään foliosuojattua kaapelointia.

12.3 WLAN-laitteisto

WLAN-laitteiston valinta ei ole koskaan helppoa, koska markkinoilla on useita valmistajia ja jokaisella on monia eri tuoteperheitä. On paljon laitteiston valintaan vaikuttavia tekijöitä, jotka rajaavat laitevalintaa. Laitteen valmistajalla on usein suuri merkitys, mutta käytännössä sen voi jättää viimeiseksi valintakriteeriksi.

Laitteiston valintaan vaikuttavia tekijöitä tärkeysjärjestyksessä:

- **BSS, ESS, LWAPP / Radio Port;** ensimmäisenä on tiedettävä kuinka iso alue/tila on saatava langattomaan lähiverkkoon. Toimiston WLAN-ratkaisuksi käy yksi tukiasema, mutta jos kyseessä on kymmeniä tukiasemia vaativa tila, pitää miettiä onko järkevämpää käyttää keskitettyä tukiasemien hallintaa.
- **Tietoturvaominaisuudet**; löytyykö laitteistosta tarvittavat tietoturvaominaisuudet, joita aiotaan käyttää.
- **Suorituskyky / hallinta**; laitteen suorituskyvyn pitää olla riittävä ja hallintamahdollisuudet kattavat käyttötarkoituksesta riippuen.
- **Lisävarusteet**; onko tarvetta antenneille, kirjautumispalvelimelle tai muille lisävarusteille, joiden yhteensopivuus on tarkistettava.
- **Budjetti**; aina on mahdollisuus parempiin laitteisiin, mutta missä kulkee sen hinta/hyötysuhteen raja, jonka työasema on valmis maksamaan.
- **Laatu / suorituskyky**; laitteen suorituskyvyistä voi olla aikaisempia kokemuksia, josta voi olla hyötyä jos itse et ole valitsemassa laitteistoa, mutta voit vaikuttaa siihen. Merkkikohtaisia eroja on, joten ne on syytä ottaa huomioon valinnassa.

Laitteiston valinnassa on usein tehtävä kompromisseja lähinnä kustannusten takia, mutta ominaisuus mistä ei koskaan pitäisi tinkiä, on tietoturva. Mikäli tietoturvaominaisuudet ovat puutteelliset, ei laitteen hankintaa pitäisi edes harkita vaikka sen muut ominaisuudet olisivat hyvät. Tietoturvaominaisuuksien ollessa riittävät on panostettava suorituskykyyn. Laitteistolla, jonka suorituskyky ei riitä toteutettavaan kohteeseen ei ole minkäänlaista arvoa. Hallintaominaisuudet voivat tuntua toisarvoiselta seikalta, mutta kun kyseessä on suuri tila/alue, jossa on kymmeniä tukiasemia, on hallinnalla iso merkitys. Etenkin logistiikka-alalla on usein tarpeellista käyttää lähetysteholtaan suurempia ulkoisia antenneja, jotta kaikki alueet saadaan verkon kantaman sisäpuolelle. Toinen laitteisto voi vaatia ulkoisen antennin, kun taas toinen selviää alkuperäisellä varustuksella vähintään yhtä hyvin. Lisävarusteiden hankinta lisää kustannuksia, joten ne on otettava huomioon jo suunnitteluvaiheessa.

12.4 Teoreettisen WLAN-verkon mittaaminen

Isoissa WLAN-verkoissa on aina syytä toteuttaa testimittaukset ennen verkon toteuttamista, koska virheet tulevat kalliiksi. Testimittauksissa käytetään yleensä yhtä tukiasemaa, jota vaihdetaan paikasta toiseen. Erinäisten ohjelmien avulla saadaan kartoitettua alueittain tukiaseman kuuluvuus mitatuissa pisteissä. Mittauksissa on mahdollisuus käyttää ohjelmistoja, jotka osaavat yhdistää mitatut tiedot ja tehdä niistä graafisen esityksen. Tällaisen ohjelman käyttö on kuitenkin hitaampaa ja monesti turhaa, mikäli kohdealue on pieni.

Testimittauksissa on pyrittävä käyttämään mahdollisimman samanlaista laitteistoa kuin aiotaan käyttää toteutettavassa verkossa. Yhdellä testilaitteistolla mitattaessa on syytä olla tarkkana, mikäli mittaukset eroavat paljon teoreettisista arvoista. Laitteiston toimintahäiriöstä aiheutuneet valheelliset mittaustulokset voivat vesittää WLAN-verkon suunnittelun täysin. Käytännön mittauksista enemmän kappaleessa 13.

12.5 Toteutus ja viimeistely

Testimittausten ja mahdollisten muutosten jälkeen alkaa verkon toimintakuntoon saattaminen. Valmiiksi konfiguroidut laitteet ja selkeät tukiasemien sijoituspaikat kartalla tekevät asennusmiesten työn vaivattomaksi. Asennustyön jälkeen verkko pitää vielä testata ennen käyttöön ottoa. Testauksen tarkoituksena on varmistaa, että teoria vastaa käytäntöä. Samalla tarkistetaan mahdolliset ongelmat ja pyritään optimoimaan verkon toimintakyky.

Käyttöönoton jälkeen verkosta tehdään raportti, joka sisältää seuraavat osiot:

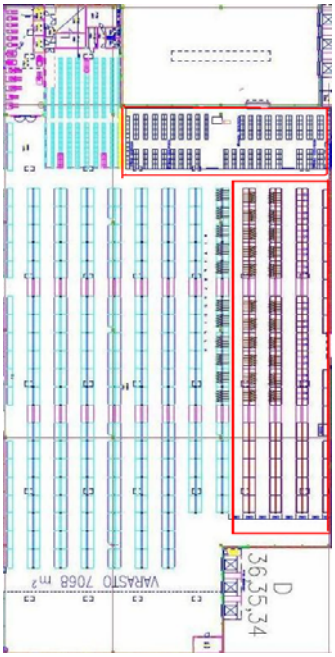
- Kartat, joissa tukiasemien sijoitus ja kanavointi
- Laitteisto ja konfiguraatiot
- Testimittausten tulokset
- Tietoturvapolitiikka
- Toteutetun verkon mittaustulokset
- Parannusehdotukset ja puutteet
- Ylläpidolliset ohjeet

Raportointi on loppujen lopuksi erittäin tärkeä ja hyödyllinen osa verkon suunnittelua, koska siitä on hyötyä myöhemmin. Valmiin verkon ylläpito kattavan dokumentoinnin avulla on paljon helpompaa. Dokumentaatio voi olla myös osa hallinnointiohjelmistoa (Cisco WCS).

13 VARASTOHALLIN WLAN-LAAJENNUS

Työn tarkoituksen oli suunnitella suuren logistiikka-alan yrityksen varastohallin laajennukseen WLAN-verkko, joka toimii yhdessä vanhan varasto-osion kanssa. Kyseinen ratkaisu tulee kuitenkin olemaan vain väliaikainen ratkaisu, joten suunnittelu ei mennyt aivan normikaavan mukaan. Kyseinen halli on yksi useamman hallin kokonaisuutta, jotka ovat yhteydessä toisiinsa. Hallit on erotettu toisistaan betoniseinillä lukuun ottamatta suuria kulkuaukkoja. Hallin WLAN-verkon suunnittelu piti toteuttaa niin, että myöhemmässä vaiheessa halliin tulee käyttöön radioporttijärjestelmä (EDGE), joka otetaan käyttöön myös muissa halleissa. Verkon suunnittelu piti siis toteuttaa radioporttijärjestelmälle, mutta siten, että se toimii väliaikaisesti normaalina ESS-verkkona.

Pohjapiirustukseen (kuva 23) on rajattu punaisella värillä uudet alueet. Ylempi osio oli olemassa osittain aikaisemminkin, mutta sitä jatkettiin ja siihen rakennettiin toinen kerros. Ylempi kerros on pohjapiirustuksen mukaisesti täynnä hyllyjä ja alhaalla on pakkausalue, jossa on enemmän vapaata tilaa. Toinen uusi alue on täynnä varastointihyllyjä, jotka ylettyvät lähes 8 m:n korkeuteen. Pohjapiirustuksen ylälaidassa oleva valkoinen alue on eri yrityksen käytössä ja kyseisessä hallissa on myös käytössä WLAN-verkko. Halli jatkuu vasemmalle, jonne vie neljä eri kulkuaukkoa.



Kuva 23. WLAN-laajennuksen pohjapiirustus

13.1 Laitteiston valitseminen

Kyseisessä hallissa oli olemassa ennestään WLAN-verkko, joka on toteutettu Buffalo AirStation WLAR-L11G-L ja Buffalo AirStation G54-tukiasemilla. Kyseiset tukiasemat eivät sovellu kunnolla yritystason käyttöön heikkojen tietoturvaominaisuuksiensa vuoksi, eivätkä toimintakyvyltään ja kestävyydeltään ole riittäviä varastotason koviin olosuhteisiin. Koska ensimmäinen vaihe (laajennus) on väliaikainen, ei vanhoja tukiasemia vaihdeta uudempiin malleihin kustannussyistä.

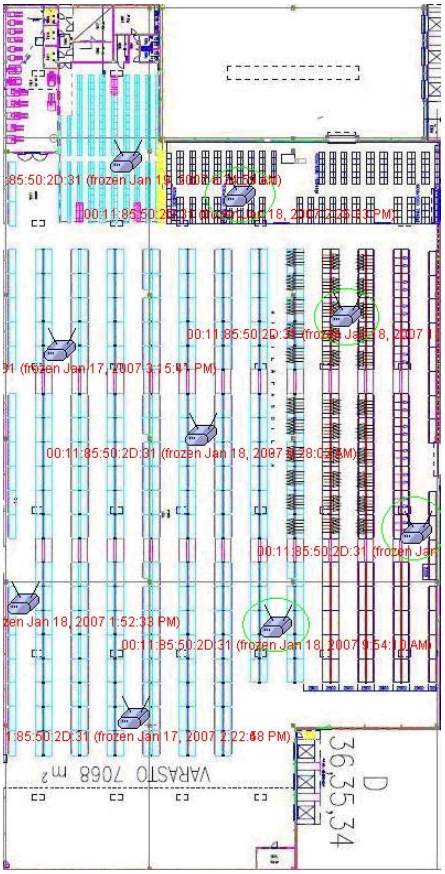
Uudelle alueelle päätettiin asentaa mittauksien mukainen määrä HP ProCurve Access Point 420-tukiasemia (kuva 24), joista on hyötyä pienemmissä kohteissa sen jälkeen, kun radioporttijärjestelmä otetaan käyttöön. Tukiasemiin lisätään myös ulkoiset antennit mallia ProCurve 5 dBi omnidirectional Antenna (kuva 6).

Kuva 24. ProCurve Wireless Acess Point 420

Radioporttijärjestelmäksi on alustavasti suunniteltu/tarjottu Hewlett Packardin järjestelmää. Kyseisessä järjestelmässä radioporttitukiasemia hallinnoisi ProCurve Wireless Edge Services xl Module. Radioporttitukiasemat (ProCurve Radio Port 220) liitetäisiin ProCurve Networking Switch 5348xl kytkimeen, joka on liitetty hallinnointimoduuliin. Radioporttijärjestelmän käyttöönottoon mennessä laitteistoa voidaan joutua muuttamaan tekniikan kehittyessä.

13.2 Ennen mittauksia suoritettavat toimenpiteet

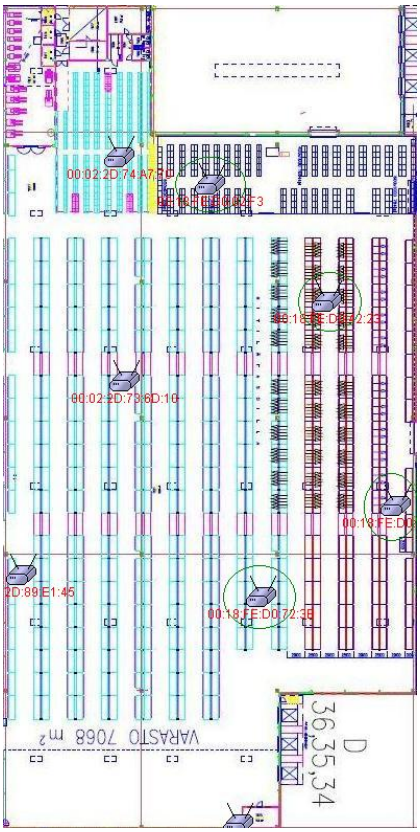
Mittausten valmistelut aloitettiin rajaamalla logistiikkakeskuksen pohjapiirustuksesta kohteena olevan hallin pohjapiirustus Ekahau Site Survey-ohjelmaan sopivaksi. Pohjapiirustuksen pikselikoon avulla ja hallin pinta-alan avulla laskettiin oikeat mittasuhteet ohjelman käyttöä varten. Ennen mittauksien suorittamista on arvioitava, kuinka monta tukiasemaa halliin tarvitaan ja minne ne sijoitetaan. Mittauksilla varmistetaan riittääkö arvioitu tukiasemien määrä ja saadaanko niillä tarvittava kuuluvuus aikaiseksi. Tukiasemien tarpeeksi arvioitiin yhdeksän kappaletta, joka pitäisi olla riittävä radioporttijärjestelmää varten (kuva 25). Uudella kaksikerroksisella alueella tukiasema sijoitetaan alakertaan. Uusien HP ProCurve Wireless Access Point 420-tukiasemien paikat on ympyröity vihreällä.



Kuva 25. Tukiasemien sijoittelu

13.2.1 Vanhojen tukiasemien hyödyntäminen

Vanhat tukiasemat (kuva 26) (uudet tukiasemat ympyröity vihreällä) on otettava huomioon radioporttijärjestelmää suunnitellessa, koska radioporttitukiasematkin tarvitsevat LAN-kaapelin toimiakseen. Vanhojen tukiasemien kaapelointia on mahdollisuus käyttää hyväkseen joko suoraan tai niitä voidaan siirtää mahdollisuuksien mukaan. Vanhojen kaapeleiden siirtäminen toiseen paikkaan on paljon nopeampaa ja helpompaa kuin uusien vetäminen, joten niitä ei kannata jättää huomioimatta WLAN-verkkoa suunnitellessa. Kyseisessä tapauksessa on mahdollisuus käyttää entistä kaapelointia suoraan kahdelle radioporttitukiasemalle ja kolmannelle siirtämällä vanhaa kaapelointia.



Kuva 26. Vanhat tukiasemat

13.2.2 LAN-kaapelointi & kytkimien tarve

Tukiasemien sijoittelussa kartalle pitää ottaa huomioon LAN-kaapelointi, kuten aikaisemmassa luvussa kerrottiin. Jos vanhaa kaapelointia ei voida käyttää edes siirtämällä, on tukiasemille vedettävä uudet kaapelit. Uusien kaapeleiden vedossa on otettava huomioon kaapeleiden asettamat pituusrajat, joten tukiasemia ei voida aina sijoittaa niin kuin halutaan. Kyseisessä laajennuksessa uusia kaapeleita jouduttiin vetämään neljälle tukiasemalle. Radioporttijärjestelmän tullessa käyttöön uudet kaapelit joudutaan vetämään vielä kahdelle radioporttitukiasemalle.

Tukiasemien sijoittelu piti varmistaa paikan päällä, koska ristikytkennästä (RK) tukiasemiin, matkaa saa kertyä maksimissaan 100 metriä. Järkevän tietoliikennepohjaratkaisun ansiosta kyseisessä hallissa on kummassakin hallin päässä RK-pisteet. Kaapelointi oli todettu mahdolliseksi valittuihin paikkoihin, joten enää oli varmistettava, että RK-pisteiden kytkimissä on tarpeeksi vapaata tilaa uusille laitteille. Mikäli mittaukset osoittavat, että suunnitellut paikat ovat hyvät, voivat asennusmiehet aloittaa kaapeloinnin uusia tukiasemia varten.

13.2.3 Tehonsyöttö

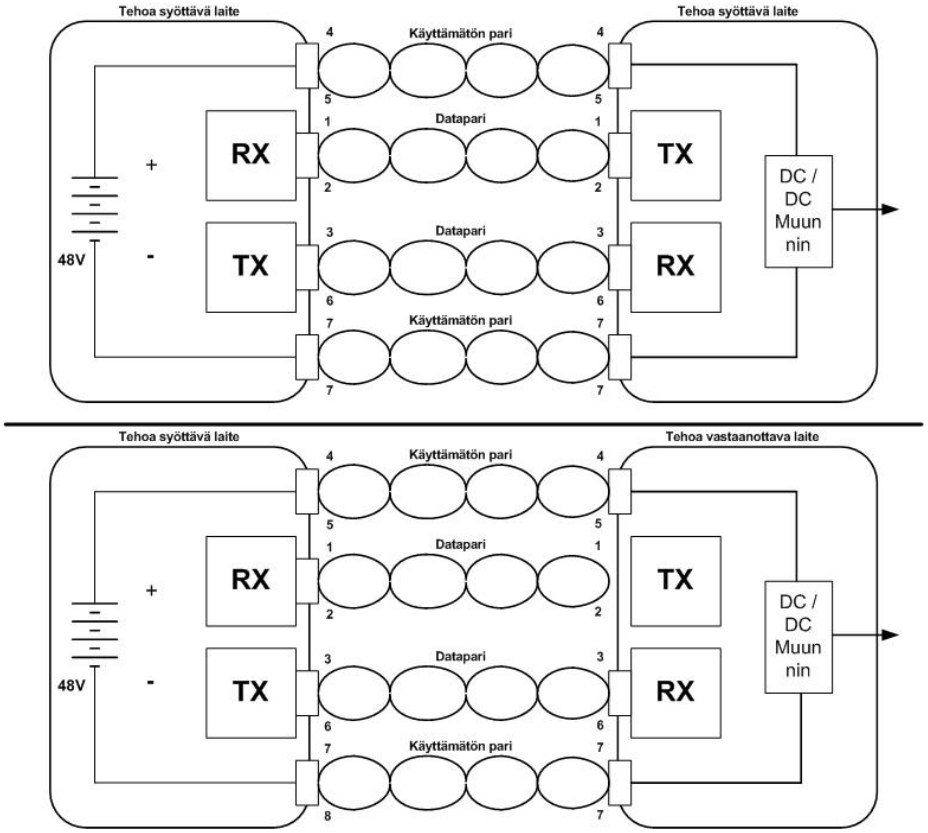
Tukiasemat tarvitsevat lähiverkkoyhteyden lisäksi tehonsyötön. Pienemmissä tiloissa on mahdollista käyttää verkkovirtaa suoraan muuntimen ja virtajohdon avulla, mutta isoissa ratkaisuissa tämä tuottaisi lisäkustannuksia, hidastaisi projektia ja mahdollisesti toisi ongelmia tukiasemien sijoittelun kanssa.

PoE (Power over Ethernet)

Tehonsyötön ratkaisemiseksi ja helpottamiseksi on kehitetty PoE (Power over Ethernet), joka on julkaistu IEEE:n 802.3af-standardin yhteydessä. PoE:ssa tehonsyöttö tapahtuu lähiverkkokaapelointia pitkin. Sovellusta käytetään myös VoIP-puhelimissa ja IP-kameroissa. Tehon siirtäminen tapahtuu joko käyttämättömiä 4&5- ja 7&8-johdinpareja tai aktiivisia johdinpareja (kuva 27). Tekniikkaa ei voida käyttää 1000BaseT Gigabit Ethernet-verkoissa, koska niissä kaikki neljä johdinparia on käytössä. Edellä mainitussa verkkorakenteessa ja isoimmissa kohteissa voidaan käyttää sähköä tuottavia kytkimiä (kuva 28). [6, s. 198 - 199.]

Ilmastointi ja varavirta

PoE-ratkaisua käytettäessä on muistettava, että laitteet tuottavat paljon lämpöä. Riittävän ilmastoinnin toteuttaminen on tärkeää, etenkin jos samassa tilassa on muitakin tietoliikennelaitteita. Katkeamattoman yhteyden takaamiseksi on muistettava lisätä PoE-palikat varavirtalähteeseen (UPS).



Kuva 27. PoE kaapelissa

Kuva 28. Sähköä syöttävä kytkin

13.2.4 Tukiaseman konfiguraatio

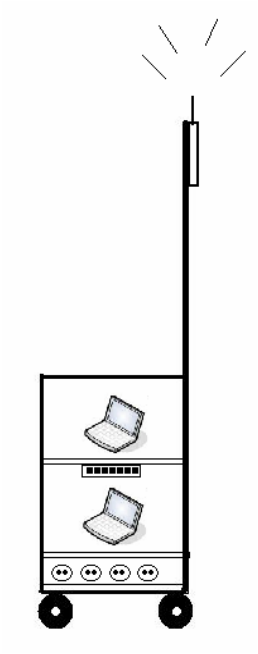
Ennen mittauksia on vielä suunniteltava tukiasemien konfiguraatio ja tietoturvamääritykset. Tukiasema ilman mitään salausta ja autentikointia toimii aivan eri tavalla kuin raskasta salausta käyttävä. Mikäli testituloksista halutaan mahdollisimman paikkaansa pitäviä, on testeissä syytä käyttää samoja laitteita samoilla konfiguraatioilla kuin toteutettavassa verkossa.

Väliaikaisverkon tietoturvaratkaisuja rajoitti tässä tapauksessa vanha laitteisto, joka ei tue samoja salaus- ja autentikointimenetelmiä, kuin uudet HP ProCurve Wireless Access Point 420-tukiasemat. Tietoturvaominaisuuksiin väliaikaisverkossa ei haluttu panostaa asiakkaan toiveesta, joten tukiasemien konfigurointi tuli olemaan hyvin yksinkertainen.

ProCurve Wireless Access Point 420-tukiasemien konfiguraatio (LIITE) ei sisällä minkäänlaista salausta, eikä käyttäjä-autentikointia. Käyttöä rajoitetaan ainoastaan MAC-pääsylistoilla. Tukiasemien kanavointi määritettiin automaattiseksi ja toimintatila 802.11b- ja 802.11g-standardeja tukevaksi. LAN-portin nopeus määritettiin manuaalisesti 100 Mbit/s Full-Dublex tilaan, jotta kytkin ja tukiasema keskustelisivat mahdollisimman nopeasti ja virheettömästi ilman turhia pakettitörmäyksiä. Tukiasemien lähetystehoa ei muutettu, eikä maksimidatanopeutta rajoitettu.

13.3 Testimittaukset

Mittaukset suoritettiin kahdella eri laitteistolla, jotta tuloksista saataisiin realistisempia. Mittauksissa käytettiin omatekoista mittauskärryä (kuva 29). Mittauskärryyn on mahdollista liittää tukiasema, joka voidaan nostaa noin 6 - 8 m:n korkeuteen. Tukiasemaan on mahdollista liittää myös ulkoinen antenni. Tukiasema on sijoitettu ylös, koska aina mittauksissa ei käytetä ulkoista antennia, mikäli suunniteltavassa verkossakaan ei niitä tulla käyttämään. Lisäksi pitkästä kaapeloinnista aiheutuisi turhaa signaalinvoimakkuuden häviötä, mikäli tukiasema sijaitsisi alhaalla kärryssä. Kärryyn on mahdollista sijoittaa kaksi kannettavaa tietokonetta. Kärryssä on myös pieni kytkin ja virtakisko joka on liitetty 50 m:n jatkojohtokelaan.



Kuva 29. Mittauskärry

Testitukiasema sijaitsi pientavara-aluetta lukuun ottamatta noin 5 m:n korkeudella. On odotettavaa, että signaalinvoimakkuus kasvaa hieman korkeuden noustessa tukiasemien sijoituskorkeuteen.

Mittauksien perusteella yhdeksällä tukiasemalla saadaan rakennettua koko hallin kattava WLAN-verkko. Käytännössä koko hallissa signaalinvoimakkuuden pitäisi olla vähintään -70 dBm – -60 dBm (kipurajana voidaan pitää arvoa -80 dBm). Uuden alueen mittaustulokset ovat hieman muuta hallia parempia, koska simuloiduilla vaimennuksilla ei saada realistista kuvaa todellisesta vaimennuksesta.

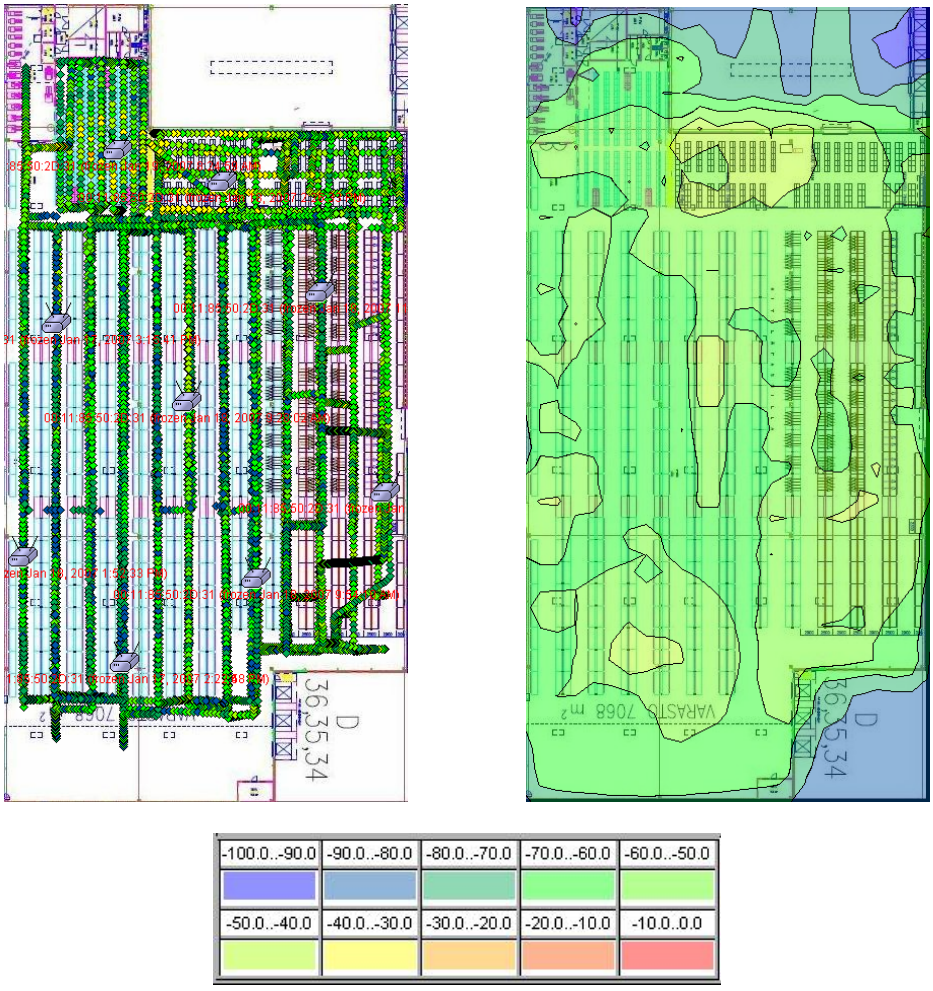
Mittaustulosten perusteella on myös havaittavissa, että työasemassa käytettäessä ulkoista antennia saadaan signaalivoimakkuus pysymään (-50 dBm – -60 dBm) hyvän rajoissa paljon laajemmalla alueella.

13.3.1 Testimittaukset (järjestelmä 1)

Mittauksissa käytetty testilaitteisto:

- Verkkokortti: Intel(R) PRO/Wireless 2200BG + ulkoinen antenni
- HP ProCurve Wireless Access Point 420-tukiasema + 5 dBi:n antenni

Mittaus suoritettiin mahdollisimman laajasti, koska kyseisessä hallissa on hyvin tärkeää, että kuuluvuudella ei ole katvealueita. Kuten mittauspistekuvasta (kuva 30) havaitaan, on Ekahau-ohjelmaan saatu erittäin kattava määrä mittapisteitä (vihreät pallot), joiden perusteella ohjelma laskee kuuluvuuden. Kuvan 30 signaalinvoimakkuuskuvasta nähdään, että vastaanotetun signaalin taso on huonoimmillaan -70 dBm, joten teoreettinen tavoite saavutettiin. Mittaustuloksia arvioitaessa on otettava huomioon, että mittaukset tehtiin vanhan langattoman verkon rinnalla. Vanhoista tukiasemista aiheutuu häiriötä ja lisäksi testaukset tehdään yhdellä tukiasemalla. Tukiasemaa siirretään paikasta toiseen ja se ei sijaitse todellisella korkeudella. Mittausten perusteella voidaan huoletta todeta, että arvioidut tukiasemien paikat ja määrät ovat riittävät, koska on odotettavissa, että valmiin verkon kuuluvuus on parempi kuin testatessa.



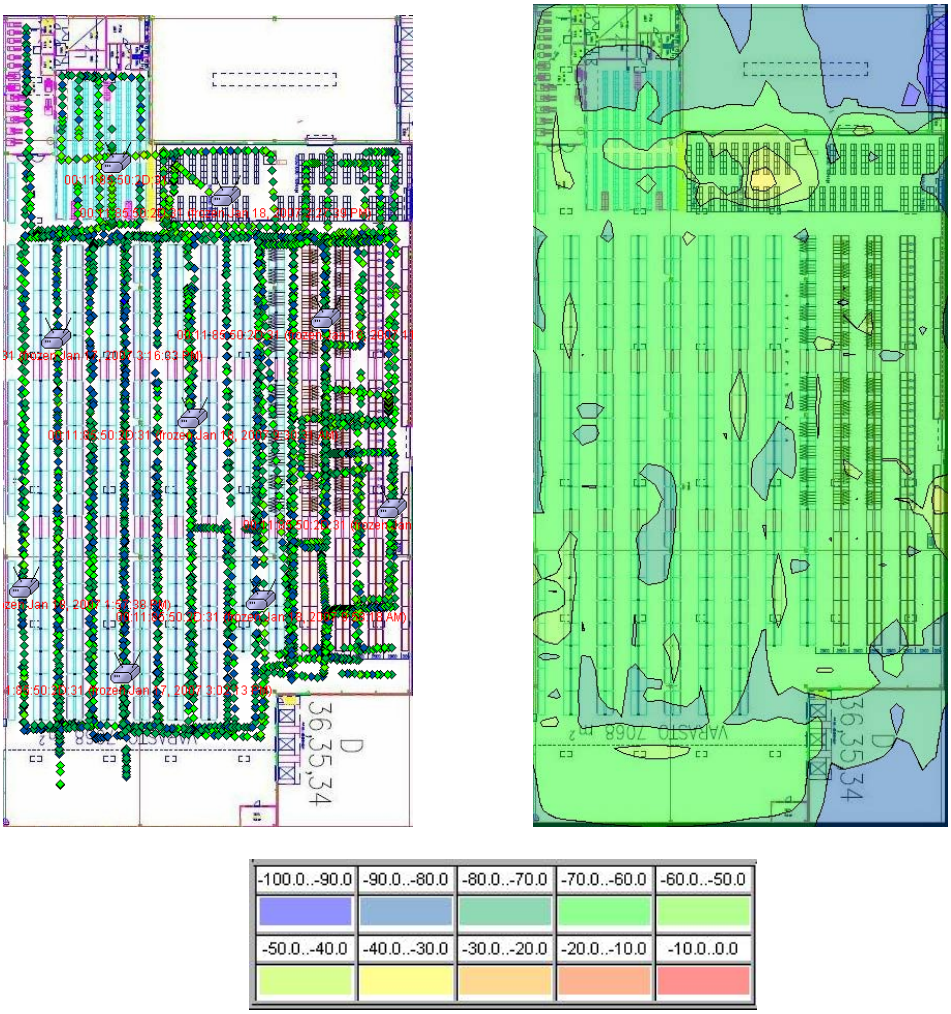
Kuva 30. Radioporttijärjestelmän testimittauksen (järjestelmä 1) mittauspisteet (vasemmalla) ja signaalin voimakkuudet (oikealla) sekä signaalin voimakkuuksien värikoodit (alhaalla) (Mbit/s)

13.3.2 *Testimittaukset (järjestelmä 2)*

Mittauksissa käytetty testilaitteisto:

- Verkkokortti: Cisco Aironet 802.11a/b/g Wireless Adapter
- HP ProCurve Wireless Access Point 420-tukiasema + 5 dBi:n antenni

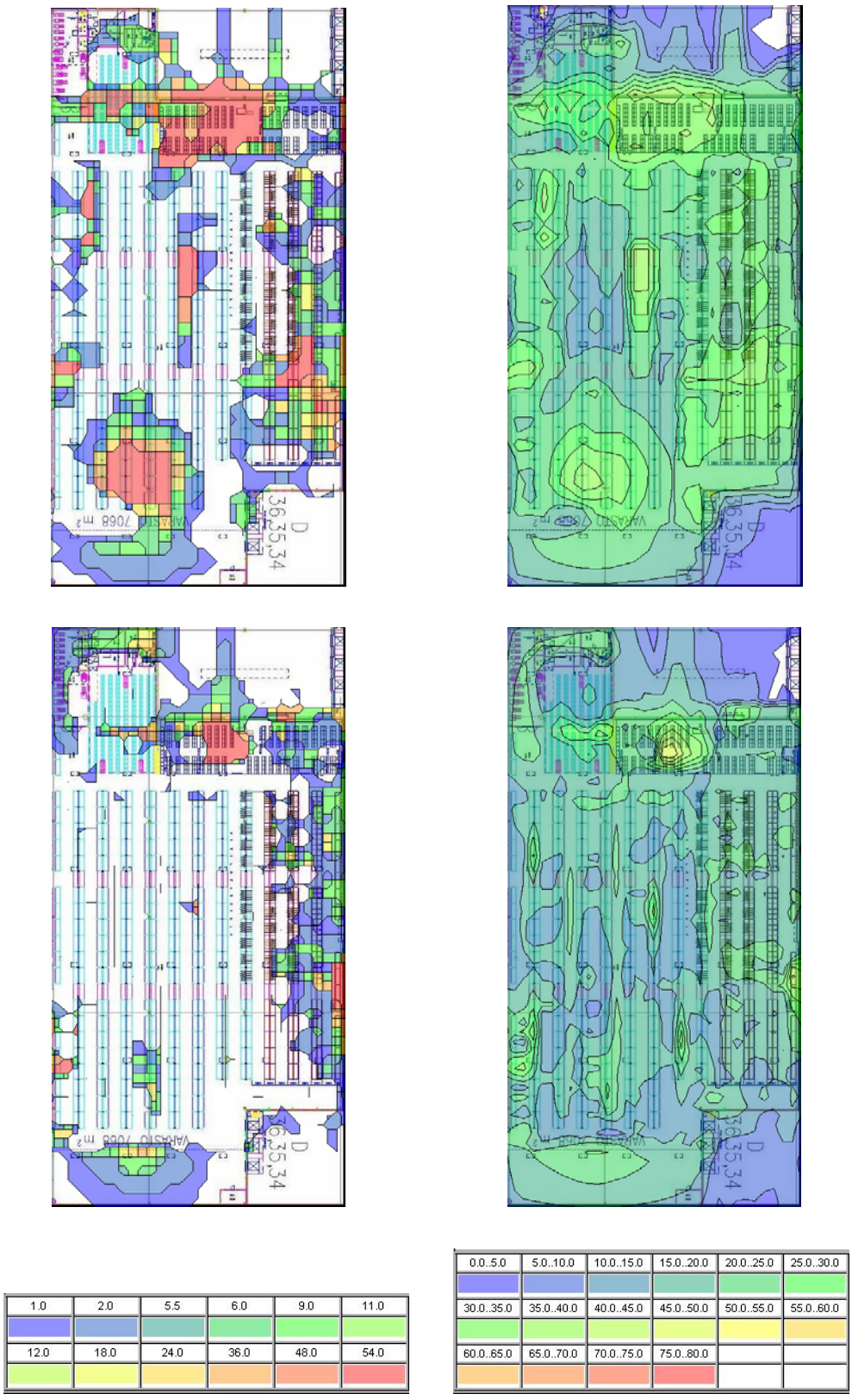
Mittaustulokset järjestelmällä 2 eroavat toisesta järjestelmästä, koska käytössä ei ole ulkoista antennia. Ulkoisesta antennista puhuttaessa, tässä tapauksessa tarkoitetaan myös kannettavien sisällä olevia antenneja. Kuvasta 31 huomataan, että mittauspisteitä on hyvin ja signaalin taso pysyy siedettävissä rajoissa (max. -70 dBm). Mittaustulokset ovat erittäin positiivisia, koska varaston kaikissa laitteissa on käytössä ulkoinen antenni, joten voimme olettaa valmiin verkon kuuluvuuden hyväksi.



Kuva 31. Radioporttijärjestelmän testimittauksen (järjestelmä 2) mittauspisteet (vasemmalla) ja signaalin voimakkuudet (oikealla) sekä signaalin voimakkuuksien värikoodit (alhaalla) (Mbit/s)

Ekahau-ohjelmalla voidaan mitata myös verkon maksimidatanopeutta ja signaalikohinasuhdetta (SNR). Kuvasta 32 kuitenkin nähdään, että kyseisessä testimittausympäristössä ei kyseisiin mittaustuloksiin voida luottaa. Mittaustulokset vääristyvät, koska testimittauksessa käytetään vain yhtä tukiasemaa. Kuvan oikeassa yläkulmassa voidaan kuitenkin havaita, että signaalikohinasuhde on kuitenkin tyydyttävä suurimmalla osaa aluetta, joten näistäkin tuloksista on hyötyä lopullisten tulosten analysoinnissa.

Kummankin testilaitteiston perusteella tukiasemien määrä oli arvioitu oikein ja koko halliin saatiin vähintään tyydyttävä signaalinvoimakkuus. Kokonaisuutena halliin on odotettavissa hyvä kuuluvuus, joka paranee radioporttijärjestelmän käyttöönoton yhteydessä. Testimittaukset onnistuivat hyvin, koska kyseisenä ajankohtana varaston käyttöaste oli korkea ja näin ollen mittauksille saatiin mahdollisimman huono kuuluvuus. Saatujen mittaustulosten perusteella asennusmiehille voitiin antaa lupa toteuttaa suunniteltu verkonlaajennus.



Kuva 32. Värikoodit maksimidatanopeudelle (Mbit/s) (vasemmalla) ja signaaliko-hinasuhteelle (dB) (oikealla)

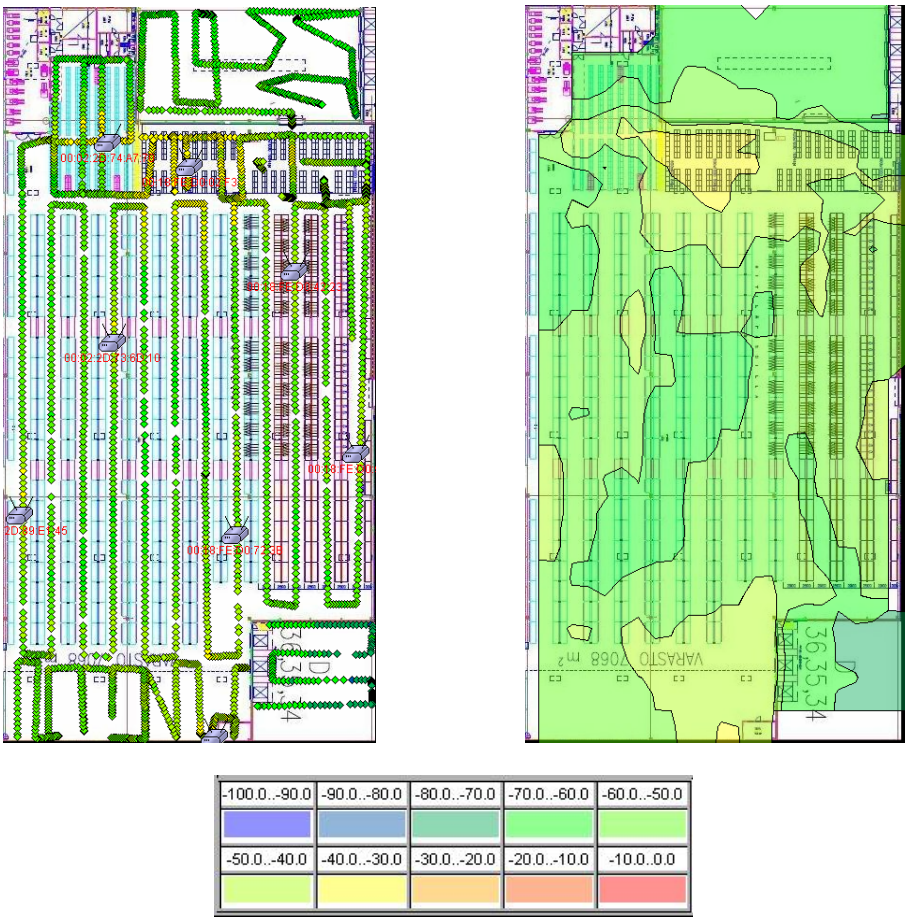
13.4 Väliaikaisverkon mittaaminen

Väliaikaisverkon valmistuttua sille tehtiin kuuluvuusmittaus, jotta saataisiin selville, olivatko testimittaukset osoittautuneet oikeaksi ja onko verkossa parantamisen tarvetta. Valmiin verkon mittaukset suoritettiin ensimmäisen testilaitteiston (kappale 13.3.1) mukaisella laitteistolla, koska se vastasi eniten varastossa käytettyä laitteistoa. Mittauksissa käytettiin apuna Ekahay Site Survey ja Network Stumbler-ohjelmia sekä komentokehotteen ping-käskyä.

13.4.1 Mittaukset (1. kerros)

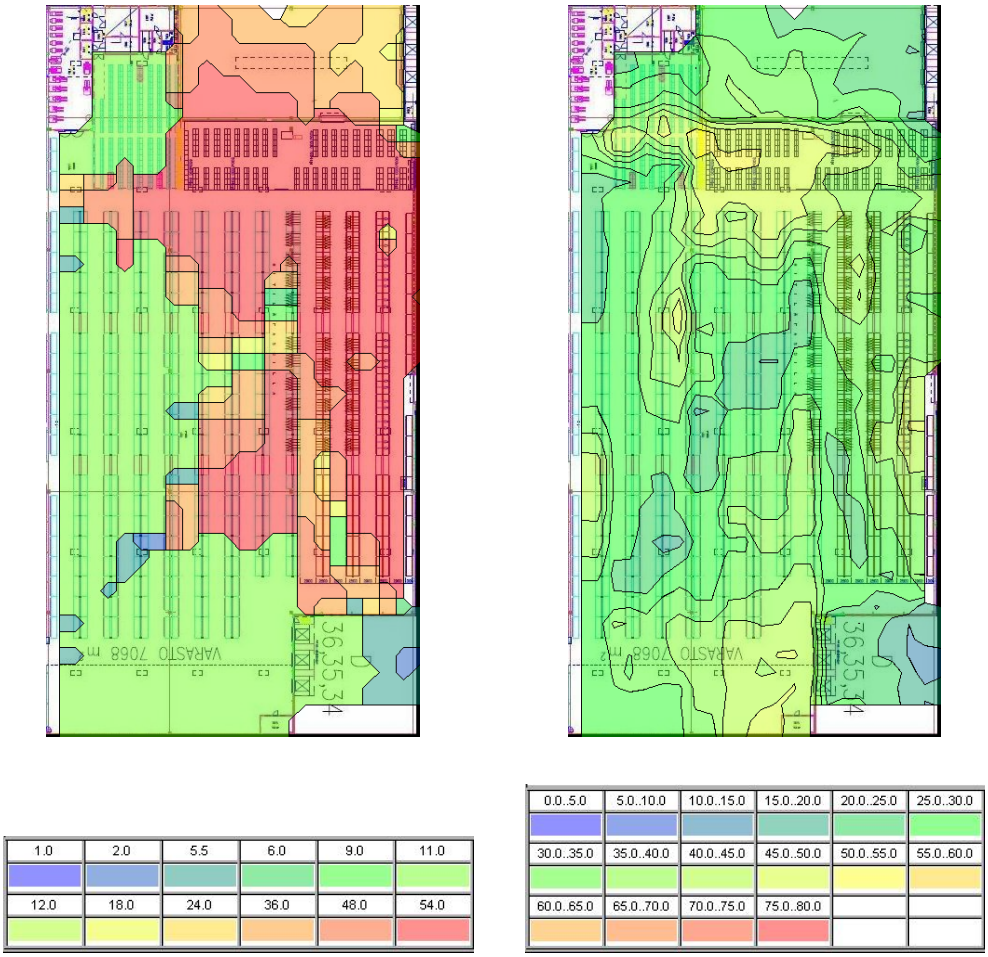
Mittaukset suoritettiin taas mahdollisimman laajasti, jotta mukaan saataisiin kattava mittauspistemäärä (kuva 33). Nyt mittaukset suoritettiin myös toisen yrityksen varastotilojen puolella (ylhäällä oleva valkoinen alue) ja ulkona (oikeassa alakulmassa), jotta nähtäisiin kuinka paljon tukiasemien signaali vuotaa varaston ulkopuolelle.

Mittaustulokset osoittavat välittömästi sen, että testimittauksiin vaikutti merkittävästi valmiin verkon tukiasemien olemassaolo. Väliaikaisverkon signaalinvoimakkuuksista voidaan todeta, että kuuluvuus on hyvä koko varastossa. Signaalinvoimakkuuskuvan 33 mukaan signaalin voimakkuustaso on melkein koko hallissa -50 – -60 tai parempi. Mittaustulokset osoittavat myös, että tukiasemien signaali vuotaa toisen yrityksen puolelle, mutta se oli odotettavissa, koska käytössä on ympärisäteilevät antennit. Ulkotiloissa tilanne oli positiivisesti erilainen, koska signaalin voimakkuus heikkeni huomattavasti ulkopuolelle mentäessä. Tietoturvallisesti signaalin vuotamisesta ulkopuolelle ei siis tarvitse olla huolissaan. Huomioitavaa on myös uusien tukiasemien keskimääräisesti parempi signaalinvoimakkuus vanhoihin tukiasemiin verrattuna, vaikka kaikissa on samat antennit.



Kuva 33. Valmiin väliaikaisverkon mittauspisteet (vasemmalla) ja signaalin voimakkuudet (oikealla) sekä signaalin voimakkuuksien värikoodit (alhaalla) (Mbit/s)

Testimittauksissa maksimidatanopeuden ja signaalin kohinasuhteen tulokset eivät olleet lainkaan todenmukaiset, koska vanhan WLAN-verkon tukiasemat vaikuttivat mittaustuloksiin. Väliaikaisverkon mittaustuloksista huomataan, että testimittauksissa todetut virheelliset mittaustulokset olivat virheellisiä. Kuvasta 34 nähdään, että uusien tukiasemien alueella maksimidatanopeus on 54 Mbit/s ja vanhalla alueella 11 Mbit/s. Signaalin kohinasuhde uudella alueella on selkeästi parempi kuin vanhalla alueella. Kohinasuhde uudella alueella on keskimäärin 30 - 50 dB ja vanhalla alueella 20-35 dB. Signaalin kohinasuhde oli tulosten perusteella hyvä.



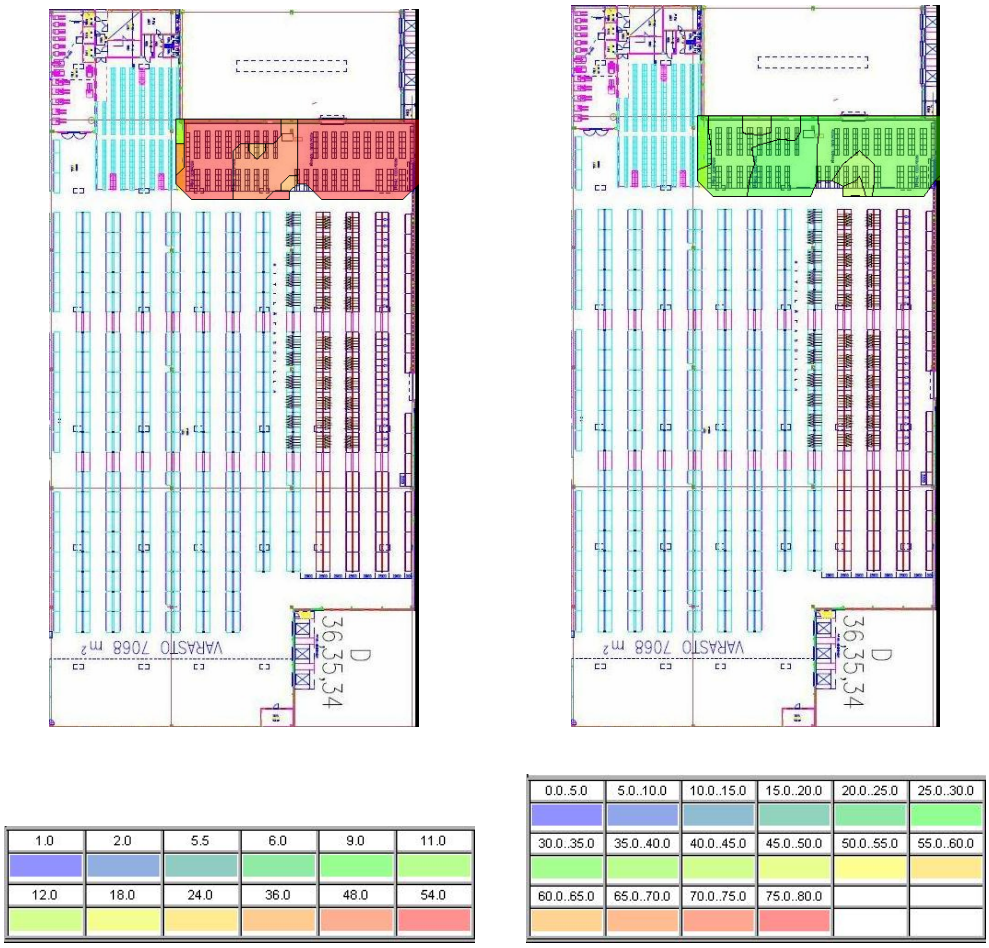
Kuva 34. Valmiin väliaikaisverkon maksimidatanopeudet (vasemmalla ylhäällä) ja signaalin kohinasuhde (oikealla ylhäällä) sekä värikoodit maksimidatanopeudelle (Mbit/s) (vasemmalla alhaalla) ja signaalikohinasuhteelle (dB) (oikealla alhaalla)

13.4.2 Mittaukset (2. kerros)

Mittaukset toteutettiin myös toisen kerroksen tiloissa, jotta varmistutaan siitä, että tukiasemien sijoitus kyseisellä alueella vain alakertaan on riittävä. Vertaamalla signaalinvoimakkuuksien värikoodeja signaalinvoimakkuuskuvaan (kuva 35), signaalin voimakkuustaso yläkerrassa on samaa luokkaa muun hallin kanssa. Tämä signaalin voimakkuustaso kyseisissä olosuhteissa on hyvä ja voidaan olettaa, että laitteiden käytössä ei tule ongelmia.

Kuva 35. Valmiin väliaikaisverkon 2. kerroksen mittauspisteet (vasemmalla) ja signaalinvoimakkuudet (oikealla) sekä signaalin voimakkuuksien värikoodit (alhaalla)

Toisen kerroksen datanopeus ja signaalikohinasuhde (kuva 36) olivat mittauksien perusteella hyvät. Nähdään, että maksimidatanopeus on lähes koko alueella 54 Mbit/s ja signaalikohinasuhde noin 30 - 40 dB.



Kuva 36. Valmiin väliaikaisverkon 2. kerroksen maksimi datanopeus (vasemmalla ylhäällä) ja signaalikohinasuhde (oikealla alhaalla) sekä värikoodit maksimidatanopeudelle (vasemmalla alhaalla) (Mbit/s) ja signaalin kohinasuhteelle (oikealla alhaalla) (dB)

13.5 Mittauksien jälkeen suoritettavat toimenpiteet

Mittausten jälkeen verkko laitetaan tuotantoon ja verkon toimintakyky joutuu realistiseen testiin. Tuotantokäytössä voi ilmetä ongelmia, koska käytössä on paljon erilaisia päätelaitteita, verkon kuormitus on suuri ja asetukset voivat aiheuttaa ristiriitoja. Tuotantokäytön ongelmia ei aina ole mahdollista havaita testauksissa. Tässäkin tapauksessa verkon käyttöönoton jälkeen ilmeni ongelmia. Käyttäjien mukaan uudella alueella yhteys pätki ja signaali oli heikko. Ongelma vaikutti aivan päinvastaiselta kuin mittaustulosten perusteella oli voitu olettaa.

Ongelman vikaselvitys aloitettiin kävelykierroksella kannettavan tietokoneen kanssa, jossa oli aktiivisena NetStumbler-ohjelma ja jatkuva pingaus tukiasemaan. Lyhyen kierroksen jälkeen ongelmaksi selvisi, että työasemat eivät pääse liittymään uusiin tukiasemiin. Tukiasemien asetusten läpikäynti ja MAC-listojen läpikäynti ei tuottanut aluksi tulosta. Loppujen lopuksi selvisi, että uusien tukiasemien automaattikanavointi ei toiminut vanhojen tukiasemien kanssa. Kyseinen tapaus osoitti sen, että automaattikanavointi ei välttämättä ole kannattava vaihtoehto, ellei käytössä ole keskitettyä WLAN-järjestelmää.

Verkon optimointi

Mikäli verkossa ei olisi ollut niin vanhoja laitteita, jotka eivät tue 802.11g-standardia, olisi tukiasemien konfigurointimuutoksilla saatu väliaikaisverkosta paljon toimivampi. Tukiasemien pakottaminen käyttämään pelkästään 802.11g-standardia tekisi verkosta paljon toimivamman ja vikasietoisemman. Verkon kuormitus on suuri, joten lähetystehon parantamiseksi olisi syytä rajoittaa maksimilähetysnopeus 11 Mbit/sekunnissa.

14 VARASTON WLAN-VERKON SUUNNITTELU JA TOTEUTUS

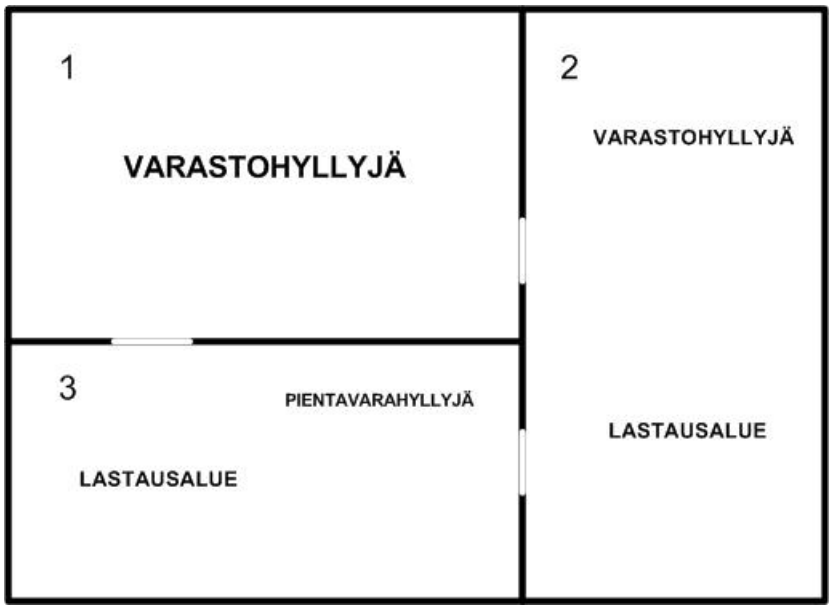
Toisessa käytännön työssä suunnitellaan koko varastoon WLAN-verkko ja toteutetaan se käyttämällä Cisco Systemsin laitteistoa. Tässä varastossa toteutusvaiheen mittauksia ei suoritettu Ekahaun avulla, koska suurin osa varastoa oli uutta ja tyhjää, joten Ekahaun käyttö olisi ollut ajanhukkaa.

Koska kyseessä oli suuri kansainvälinen logistiikka-alan yritys, byrokratian vuoksi laitehankintojen oli mentävä maailmanlaajuisen konseptin mukaisesti. Lisäksi laitteiden asetusten ja käyttäjätodennuksen olisi pitänyt olla konseptin mukaiset, mutta tekniikan kehittyessä ja muuttuessa tämä ei enää ollut mahdollista. Tässä työssä tuli hyvin esiin, kuinka paljon asioita joutuu ottamaan huomioon vaikka kaikki on teoriassa saneltu etukäteen.

Tietoturvasyistä työssä ei ollut lupaa julkaista varaston pohjapiirustuksia, mutta tarvittaessa asioita on havainnollistettu kuvaesimerkein. Kuvat eivät vastaa todellista tilannetta, mutta kyseisillä esimerkeillä voidaan havainnollistaa tilanne tarvittavalla tarkkuudella.

14.1 Teoreettinen suunnittelu

Varasto koostuu käytännössä kolmesta eri tilasta. Kuvan 37 tilassa 1 on pelkästään varastohyllyjä, joten tilaan on helppo sijoittaa tukiasemat. Tilassa 2 on myös varastohyllyjä, mutta osa hyllyistä on metallihäkin sisällä. Tilassa kaksi on myös avoin lastausalue. Tilassa 3 on iso lastausalue ja suljettuja alueita, jotka eivät kuulu langattoman verkon piiriin. Tilassa 3 olevan pientavara-alueen ja alueen kaksi välillä ei käytännössä ole lainkaan seinää.



Kuva 37. Varaston periaatteellinen kuva

14.1.1 Laitteisto ja tietoturvallisuus

Varastoon tuli asentaa konsernin mukaisesti Cisco Systemsin Cisco Aironet 1200 Series-tukiasemia (kuva 38). Tukiasemien kuuluvuus alkuperäisillä antenneilla on kokemuksien mukaan hyvä, joten ulkoisia antenneja ei otettu alustavaan suunnitelmaan mukaan.

Kuva 38. Cisco Aironet 1200 Series-tukiasema

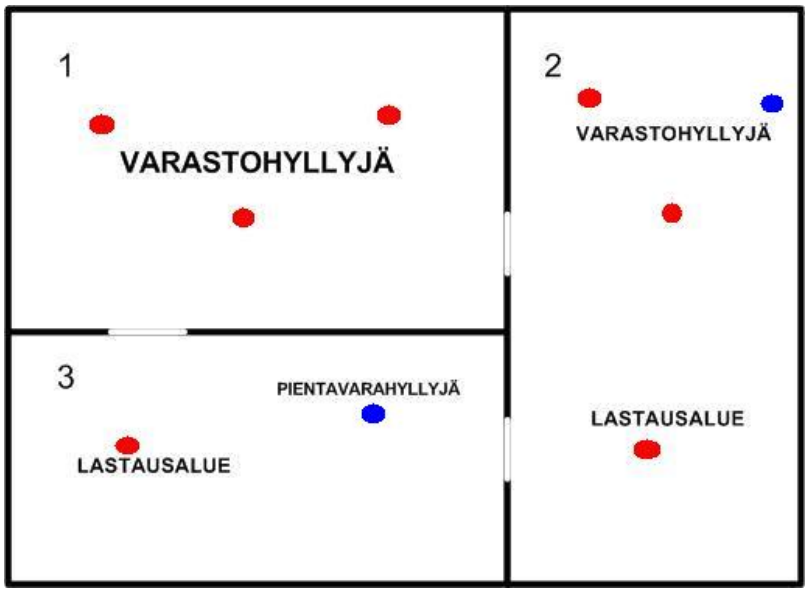
Tiedon salaukseen käytetään TKIP-salausta ja local-RADIUS-käyttäjätodennusta. Tukiasemien asetukset on esiteltynä liitteessä.

14.1.2 Teoreettinen tukiasemien sijoittelu

Tukiasemien sijoittelu oli tässä kohteessa haasteellinen, koska kyseessä oli vanha varasto, jota laajennettiin. Alueelle 3 sijoitettiin vain yksi tukiasema, koska tärkein peittoalue oli lastausalue. Tukiaseman kuuluvuus riittäisi osittain myös pientavarahyllyille. Alueen 2 lastausalueen tukiasema ei sijoitu aivan alueen keskelle, koska sen on tarkoituksena täydentää kolmosalueen pientavarahyllyjen kuuluvuutta. Lastausalueet olivat helppo sijoittaa, koska esteitä ei ollut paljon. Ongelmaksi voi tulla pientavarahyllyjen alue, koska se on kahdessa kerroksessa ja esteitä on paljon.

Alueen 2 varastohyllyalue on pulmallisin, koska siellä sijaitsee alue, joka on rajattu metallihäkillä. Metallihäkin vaimennus voi olla niin suuri, että se vaatii oman tukiaseman, koska se muodostaa Faradayn häkin. Alustavasti alueelle sijoitettiin vain kaksi tukiasemaa, jotka normaalisti riittäisivät kattamaan alueen. Varastoalue 1 on suurin tila ja siellä on pelkästään varastohyllyjä. Alue on tyhjä ja testimittauksista ei ole hyötyä, koska ne joudutaan suorittamaan ennen varaston täyttämistä. Kokemuksen mukaan kyseisen alueen peittämiseen tarvitaan noin kolme tukiasemaa ja sijoittaminen on syytä olla hieman epäsymmetrinen.

Teoreettinen tukiasemien sijoittelu tapahtui kuvan 39 mukaisesti, jossa punaiset pallot ovat todennäköisiä sijoituskohteita ja siniset reservipaikkoja.



Kuva 39. Tukiasemien teoreettinen sijoittelu

14.2 Mittaukset

Testimittaukset suoritettiin kahdella eri laitteistolla, jotta tuloksista saataisiin realistisempia. Mittauksissa käytettiin omatekoista mittauskärryä, joka on esitelty kappaleessa 13.

Mittauksissa käytetty testilaitteisto:

- Verkkokortti: Cisco Aironet 802.11a/b/g Wireless Adapter
- Verkkokortti: Intel(R) PRO/Wireless 2200BG + ulkoinen antenni
- NetStumbler, Ping-komento, Ekahau

Mittaukset aloitettiin sijoittamalla tukiasema alueen 2 ja 3 lastausalueille, jotta kuuluvuus alueen 3 pientavara-alueelle saadaan mitattua. Mittaukset osoittivat, että pientavara-alueelle jää mahdollinen katvealue, jos sinne ei asenneta ylimääräistä tukiasemaa. Alueella ei kuitenkaan ole ainakaan alkuvaiheessa tarvetta WLAN-verkolle, joten siihen ei asenneta tukiasemaa. Alueen mahdollinen katvealue dokumentoitiin ja lisätukiasemalle tehtiin varaus tulevaisuutta varten. Lastausalueiden tukiasemat peittivät muuten suunnitellut alueet.

Alueen 1 mittauksia ei tarvinnut suorittaa, koska alue oli tyhjä. Varaston koon mukaan sinne pitäisi kuitenkin riittää mainiosti kolme tukiasemaa. Tukiasemien sijoittelussa on hieman epäsymmetrisyyttä, josta on kokemuksien mukaan hyötyä kuuluvuudelle. Alueen 2 varastohylly alue oli haastava mittauksien kannalta, koska se on korkea ja aivan täynnä tavaraa. Mittauksien perusteella alueelle tarvitaan ainakin kaksi tukiasemaa, koska hyllyissä varastoitava materiaali on hyvin vaimentavaa. Alueelle mitoitettiin lisäksi reservitukiasema, koska metallinen häkkiseinä saattaa aiheuttaa toisella laidalla signaalin liiallisen heikkenemisen.

Valmiin verkon mittaaminen

Valmiin verkon mittaaminen suoritettiin ennen käyttöönottoa kannettavalla tietokoneella, jossa signaalinvoimakkuutta valvottiin NetStumbler-ohjelmalla. Lisäksi yhteyden eheyttä valvottiin jatkuvalla ping-komennolla. Valmiin verkon mittaustulokset osoittautuivat hyviksi ja havaitut katvealueet pysyivät. Katvealueiden tarkemmaksi määrittämiseksi suoritettiin lisäksi mittaus Ekahaulla. Tulosten perusteella alueen 2 varastohyllyalueelle lisättiin yksi tukiasema sille varatulle paikalle.

15 YHTEENVETO

Langattomat lähiverkot ovat yleistyneet huimasti viime vuosina yrityskäytössä ja ne ovat tuoneet aivan uuden osa-alueen yritysten ICT-hallinnoille. Langattomuus aiheuttaa paljon tietoturvaongelmia, joten asiantuntemus WLAN-verkkoja suunniteltaessa ja toteutettaessa on välttämätöntä.

Tässä insinöörityössä käsiteltiin langattomia lähiverkkoja tutustumalla ensin WLAN-tekniikkaan, sekä langattomissa yhteyksissä käytettyihin laitteisiin. Työssä käsiteltiin myös laajasti tietoturvaa ja siihen liittyviä uhkia. Työn painopiste oli WLAN-verkkojen suunnittelussa ja toteutuksessa logistisiin varastoihin. Työn teoreettinen osio pyrittiin pitämään suppeana, mutta informatiivisena.

WLAN-verkkoja toteutettaessa teorian tuntemisen tärkeyttä ei pidä aliarvioida. Tekniikan tunteminen teoriassa mahdollistaa käytettyjen ratkaisujen ymmärtämisen ja niiden tärkeyden sisäistämisen. WLAN-verkkojen suunnittelijan näkökulmasta on erittäin ikävää seurata yritysten tekemiä päätöksiä, jotka perustuvat tietämättömyyteen. WLAN-verkkojen suurimmaksi huolenaiheeksi on muodostumassa niiden tietoturvallisuus. Suurin osa nykyisistä salausmenetelmistä on helposti murrettavissa, joten tietoturvallisuuteen tulisi suhtautua vakavasti, etenkin kun kyseessä on langaton tiedonsiirto. Insinöörityön teon aikana törmättiin useita kertoja asiakkaan tekemiin päätöksiin, joissa kustannukset menivät tietoturvallisuuden ja käytettävyyden ohitse. Toivottavasti työni ajautuu asiakkaidenkin käsiin, jotta järjettömiä ratkaisuja ei voida perustella tiedon puutteella.

Työssä perehdyttiin myös WLAN-verkkojen hallinnoimiseen keskitetysti. Keskitetyn hallinnan avulla saavutetaan huomattavia parannuksia verkon tehokkuuteen ja vikasietoisuuteen. Lisäksi tukiasemien päivitykset, konfigurointi ja muut toimenpiteet voidaan hoitaa keskitetysti, mikä tuo säästöjä ylläpitokustannuksiin. Hallittavia järjestelmiä on nykyään tarjolla useilta eri valmistajilta, mutta niille ei ole vielä yleistä standardia.

Vuonna 2008 ratifioitavaksi suunniteltu IEEE:n 802.11n-standardiluonnos tulee olemaan seuraava merkittävä uudistus WLAN-tekniikassa. Se tarjoaa huomattavasti nopeamman yhteyden, MIMO-tekniikan, pidemmän kantomatkan ja parannuksia tietoturvaan.

VIITELUETTELO

[1] Cisco Networking Academy, *Fundamentals of Wireless LANs* [verkko-oppimateriaali, viitattu 26.8.2007]. Saatavissa: http://cisco.netacad.net/

[2] Wi-Fi Alliance, *About the Alliance* [verkkodokumentti, viitattu 10.8.2006]. Saatavissa: http://www.wi-fi.org/about_overview.php

[3] Dacco Corporation Oy, *Langaton verkko* [verkkodokumentti, viitattu 10.8.2006]. Saatavissa: http://WLAN.dacco.fi/langaton.htm

[4] MC MCSE Certification Resources, *Hierarchical model* [verkkodokumentti, viitattu 10.8.2006]. Saatavissa: http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

[5] Elinkeinoelämän keskusliitto, *Logistiikka* [verkkodokumentti, viitattu 24.11.2006]. Saatavissa: http://www.ek.fi/ek_suomeksi/kilpailukyky/logistiikka/index.php

[6] Puska, Matti, *Langattomat lähiverkot*. Jyväskylä: Gummerus Oy. 2005.

[7] Dodd, Annabel, *The Essential Guide to Telecommunications (Fourth Edition)*. Indiana Crawfordsville: R.R. Donnelley. 2005.

[8] Kurki, Jouko. Helsingin ammattikorkeakoulu. *WLAN physical and MAC layer* [luentomateriaali, viitattu 10.7.2007]. Saatavissa: http://opetus.stadia.fi/kurki/Courses/WirelessLAN/WLAN_course_2006/WL_6_WLAN_802_11_PHY_MAC_functions.pdf

[9] Granlund, Kaj, *Langaton tiedonsiirto*. 1. painos. Porvoo: Docendo. 2001.

[10] Puska, Matti, *Lähiverkkojen tekniikka*. Jyväskylä: Gummerus Kirjapaino Oy. 2005.

[11] Viestintävirasto, *Langattomat lähiverkot (RLAN) 5 GHz taajuusalueella* [verkkodokumentti, viitattu 11.7.2007]. Saatavissa: http://www.ficora.fi/index/viestintavirasto/työasematiedotteet/radiotaajuudet/2002/P_12.html

[12] Brachkov, Hristo. Tampereen teknillinenkorkeakoulu. *Presentation at Wireless LANs course: 802.11g Physical Layer* [luentomateriaali, viitattu 11.7.2007]. Saatavissa: www.cs.tut.fi/~83180/83180_05_S3a.ppt

[13] Stuart, Kerry ja McCann, Stephen. IEEE. *Official IEEE 802.11 working group project timelines* [verkkodokumentti, viitattu 11.7.2007]. Saatavissa: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

[14] IEEE, *High Throughput* [verkkodokumentti, viitattu 11.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11n.pdf

[15] Computerworld, *Quickstudy: MIMO* [verkkodokumentti, viitattu 11.7.2007]. Saatavissa: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=109410

[16] Winncom Technologies, *IEEE 802.11d Standard* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://www.winncom.com/glossary.aspx?term=63

[17] IEEE, *802.11s* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11s.pdf

[18] IEEE, *802.11p* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11p.pdf

[19] IEEE, *802.11k* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11k.pdf

[20] IEEE, *802.11r* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11r.pdf

[21] IEEE, *802.11.2* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11-2.pdf

[22] IEEE, *802.11u* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11u.pdf

[23] IEEE, *802.11v* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11v.pdf

[24] IEEE, *802.11w* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11w.pdf

[25] IEEE, *802.11y* [verkkodokumentti, viitattu 16.7.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-11y.pdf

[26] ETSI, *Who is ETSI?* [verkkosivusto, viitattu 16.7.2007]. Saatavissa: http://www.etsi.org/about_etsi/5_minutes/home.htm

[27] Hewlett Packard, *ProCurve Wireless Edge Services xl Module* [verkkodokumentti, viitattu 17.7.2007]. Saatavissa: http://www.hp.com/rnd/pdfs/datasheets/ProCurve_Wireless_Edge_Services_xl_Module.pdf

[28] Hewlett Packard, *HP:n langattomat lisävarusteet (J8441A) -tekniset tiedot ja takuu* [verkkokuva, viitattu 24.7.2007]. Saatavissa: http://h10010.www1.hp.com/wwpc/fi/fi/ho/WF06c/A1-1696349-1696425-1696425-1696439-1696439-10845235.html

[29] Hewlett Packard, *HP:n langattomat lisävarusteet (J8443A) -tekniset tiedot ja takuu* [verkkokuva, viitattu 24.7.2007]. Saatavissa: http://h10010.www1.hp.com/wwpc/fi/fi/ho/WF06c/A1-1696349-1696425-1696425-1696439-1696439-10845231.html

[30] Verkkokauppa.com, *Tuote 22692* [tuoteseloste, viitattu 24.7.2007]. Saatavissa: http://www.verkkokauppa.com/popups/prodinfo.php?id=22692

[31] McCullough, Jack, *Caution! Wireless Networking: Preventing a Data Disaster*. Indianapolis Indiana: Wiley Publishing Inc. 2004.

[32] Wi-Fi Planet, *Tutorials: Understanding Ad Hoc Mode* [verkkodokumentti, viitattu 24.7.2007]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/1451421

[33] Wi-FiTechnology.com, *Wi-Fi Mesh Networks, The path to mobile Ad-Hoc* [verkkodokumentti, viitattu 25.7.2007]. Saatavissa: http://www.wi-fitechnology.com/Papers+req-showcontent-id-7.html

[34] Viestintävirasto: *Langattomat lähiverkot (RLAN) 5 GHz taajuusalueella* [verkkodokumentti, viitattu 25.7.2007]. Saatavissa: http://www.ficora.fi/index/viestintavirasto/työasematiedotteet/radiotaajuudet/2002/P.html

[35] Palomäki, Martti, *Suurin sallittu lähetysteho 2.4 GHz WLAN-verkossa* [verkkodokumentti, viitattu 25.7.2007]. Saatavissa: http://www.saunalahti.fi/elepal/wlanout.html

[36] Cisco Systems, *Cisco Aironet 1200 Series* [verkkodokumentti, viitattu 19.8.2007]. Saatavissa: http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html

[37] Tech-FAQ, *What is RSN (Robust Secure Network)* [verkkodokumentti, viitattu 1.8.2007]. Saatavissa: http://www.tech-faq.com/rsn-robust-secure-network.shtml

[38] Wi-Fi Planet, *WPA-PSK: Step-by-Step* [verkkodokumentti, viitattu 3.8.2007]. Saatavissa: http://www.wifiplanet.com/tutorials/article.php/3552826

[39] Wi-Fi Alliance, *WPA2 (Wi-Fi Protected Access 2)* [verkkodokumentti, viitattu 3.8.2007]. Saatavissa: www.wi-fi.org/knowledge_center/wpa2

[40] Wi-Fi Alliance, *WPA (Wi-Fi Protected Access)* [verkkodokumentti, viitattu 3.8.2007]. Saatavissa: www.wi-fi.org/knowledge_center/wpa

[41] Techworld, *What's behind the CAPWAP flap* [verkkodokumentti, viitattu 6.8.2007]. Saatavissa: http://www.techworld.com/mobility/features/index.cfm?featureid=480

[42] LookSmart, *Trapeze Networks Drives New Solution for Access Point Interoperability in IETF CAPWAP Working Group* [verkkodokumentti, viitattu 8.8.2007]. Saatavissa: http://findarticles.com/p/articles/mi_m0EIN/is_2005_April_6/ai_n13561818

[43] Cisco Systems, *Understanding the Lightweight Access Point Protocol (LWAPP)* [verkkodokumentti, viitattu 14.8.2007]. Saatavissa: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_white_paper0900aecd802c18ee.shtml

[44] Hewlett-Packard, *ProCurve Wireless Network Access Point Control Server 745wl* [verkkodokumentti, viitattu 16.8.2007]. Saatavissa: http://www.hp.com/rnd/products/wireless/700wlseries/overview.htm

[45] Hewlett-Packard, *ProCurve Networking Switch 5300xl series* [verkkodokumentti, viitattu 16.8.2007]. Saatavissa: http://www.hp.com/rnd/products/switches/switch5300xlseries/overview.htm

[46] Hewlett-Packard, *ProCurve Wireless EDGE Services xl module* [verkkodokumentti, viitattu 16.8.2007]. Saatavissa: http://www.hp.com/rnd/products/wireless/ProCurve_Wireless_Edge_Services_xl_Module/overview.htm

[47] Hewlett-Packard, *ProCurve Radio Port 220* [verkkodokumentti, viitattu 16.8.2007]. Saatavissa: http://www.hp.com/rnd/products/wireless/ProCurve_Radio_Port_220/overview.htm

[48] Hewlett-Packard, *ProCurve Networking Wireless Access Point 420* [verkkodokumentti, viitattu 16.8.2007]. Saatavissa: http://www.hp.com/rnd/products/wireless/420_series/overview.htm

[49] Techworld, *CTP to break standards deadlock?* [verkkodokumentti, viitattu 17.8.2007]. Saatavissa: http://www.techworld.com/mobility/news/index.cfm?NewsID=1340&Page=1&pagePos=5

[50] Chantry Networks, *Chantry Networks and Propagate Networks Partner to Propose an Alternative Standard to Expired LWAPP Protocol* [verkkodokumentti, viitattu 19.8.2007]. Saatavissa: *http*://chantry.webeditz.com/news/detail.php?ID=36

[51] IETF Tools, *Wireless LAN Control Protocol (WiCoP)* [verkkodokumentti, viitattu 22.8.2007]. Saatavissa: http://tools.ietf.org/html/draft-iino-capwap-wicop-02

[52] Cisco Systems, *Cisco Aironet 1000 Series* [verkkodokumentti, viitattu 25.8.2007]. Saatavissa: http://www.cisco.com/en/US/products/ps6306/index.html

[53] Cisco Systems, *Cisco Wireless Control System (WCS)* [verkkodokumentti, 1.8.2007]. Saatavissa: http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd802570d0.html

[54] Joshua Wright, *Asleap* [verkkodokumentti, viitattu 2.8.2007]. Saatavissa: http://asleap.sourceforge.net/

[55] WiMax.com [verkkodokumentti, viitattu 17.8.2007]. Saatavissa: http://www.wimax.com

[56] Paul Frank, *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)* [verkkodokumentti, viitattu 17.8.2007]. Saatavissa: http://www3.ietf.org/proceedings/02mar/slides/eap-1/index.htm

[57] Microsoft, *Securing Wireless LANs with PEAP and Passwords* [verkkodokumentti, viitattu 19.8.2007]. Saatavissa: http://www.microsoft.com/technet/security/guidance/cryptographyetc/peap_0.mspx

[58] Cisco Systems, *EAP Authentication Protocols for WLANs* [verkkodokumentti, viitattu 19.8.2007]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=369223&seqNum=5&rl=1

[59] Antti, Koivumäki. Helsingin ammattikorkeakoulu [sähköpostikeskustelu, viitattu 20.6.2007].

Cisco Aironet 1200 tukiaseman konfiguraatio

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname xxxxxx
!
enable secret xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
!
ip subnet-zero
no ip domain lookup
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server xxx.xxx.xxx.xxx auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
dot11 ssid xxxx
   authentication network-eap eap_methods
   authentication key-management wpa
   guest-mode
!
dot11 network-map
!
!
username root privilege 15 password xxxxxxxxxxxxxx
!
bridge irb
```

```
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
 !
 broadcast-key change 100 membership-termination capability-change
 !
 !
 ssid 6
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel 2472
 station-role root
 world-mode dot11d country FI both
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 speed 100
 full-duplex
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface BVI1
 ip address xxx.xxx.xxx.xxx 255.255.255.0
 no ip route-cache
!
ip default-gateway xxx.xxx.xxx.xxx
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
snmp-server view dot11view ieee802dot11 included
snmp-server community public view dot11view RO
snmp-server enable traps tty
radius-server local
  no authentication eapfast
  nas xxx.xxx.xxx.xxx key 7
124D5143115F0952297D7C7D30637B4701450152520B0C00035D51
  user xxxxxxxx nthash 7
12495D4F30295B277A79737D10660636574E5024700F7B77025E214D460F007476
```

```
 user xxxxxxxx nthash 7
0528575A0719192B4B564E46522D21787D057C6711733721325225740A7E767058
 user xxxxxxxx nthash 7
072B051E6A5C415746342D2D5D090876091710773153325452070C0B06725A514F
 user xxxxxxxx nthash 7
02535D0B5F2558021919594055433302A2827737F067917130341564F542574080B
 user xxxxxxxx nthash 7
013256250D5B245F766F175C49213344585425730806 0B6B1774465E4727207409
 user root nthash 7
047F5F505C751C1C593B5644405F29517F0977706B61004024475A50007D7C0A02
!
radius-server attribute 32 include-in-access-req format %h
radius-server host xxx.xxx.xxx.xxx auth-port 1812 acct-port 1813 key 7
00504752070F0E500C77141B0A4F5C4314580E572E79707B646670
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
 logging synchronous
line vty 0 4
 logging synchronous
line vty 5 15
 logging synchronous
!
end
```

Punaisella merkityt kohdat on muutettu tietoturvan vuoksi.