Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Miika Kirves

Langattoman lähiverkon suunnittelu, toteutus ja yhtenäistäminen monikiinteistökohteessa

Insinöörityö 28.5.2010

Ohjaaja: toimitusjohtaja Ilkka Nenonen
Ohjaava opettaja: opettaja Heikki Rahkonen

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä Otsikko Sivumäärä Aika	Miika Kirves Langattoman lähiverkon suunnittelu, toteutus ja yhtenäistäminen monikiinteistökohteessa 55 sivua 28.5.2010
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja Ohjaava opettaja	toimitusjohtaja Ilkka Nenonen opettaja Heikki Rahkonen

Tämä työ käsittelee langattoman lähiverkon suunnittelua, toteutusta ja yhtenäistämistä monikiinteistökohteessa, joka toimii työharjoittelupaikkani asiakasyrityksen tiloissa. Työ tulee keskittymään sekä kolmeen päävaiheeseen alku-, nyky- ja tulevaan tilaan, että WLAN-tekniikan teoriaan.

Langattoman lähiverkon rakentaminen alkoi siitä, kun asiakasyritys oli rakennuttanut kaksi uutta huoneistohotellirakennusta, ja asiakas tarvitsi helppoa lähiverkkoratkaisua kiinteistöihin. Työssä rakennettiin aluksi yhteen monikiinteistökohteeseen langaton verkko ja laadittiin suunnitelma lähiverkon yhtenäistämiseksi.

Verkon rakentaminen alkoi suunnittelulla ja mittaamisella. Varhaisessa suunnitteluvaiheessa suoritettiin mittauksia käyttöön hankituilla laitteilla, jotta voitiin varmistaa laitteiden sopivuus ympäristöönsä sekä varmistaa vahvistuslaskennat käytännössä.

Rakennusvaihe oli kaksiosainen, ensimmäinen osa sisälsi ainoastaan isomman huoneistohotellirakennuksen toteutuksen ja jälkimmäinen osa sisälsi pienemmän rakennuksen toteutuksen. Toteutuksen kaksivaiheisuus mahdollisti todellisten käyttökokemusten keräämisen vuoden ajalta.

Verkon yhtenäistäminen on laadittu valmiiksi suunnitelmaksi, jonka toteutus on vielä keskeneräinen laitetasolla. Yhtenäistämisen toteuttamiseen tarvittaisiin enemmän verkkolaitteita kuin pelkästään langattomia tukiasemia.

Suunnitelman ongelmakohdiksi muodostui väkisinkin useassa eri vaiheissa rakennetut kiinteistöt, joista varsinaisia ongelmien aiheuttajia olivat eriävät rakenneratkaisut. Näitä rakenneratkaisuja oli mm. paloturvallisten materiaalien käyttö rakennushetken ajanhengen mukaisesti.

Hakusanat	wlan, kiinteistö, lähiverkon suunnittelu, laitepohdinta

Helsinki Metropolia University of Applied Sciences **Abstract**

Author	Miika Kirves
Title	Design, implementation and harmonization of a wireless LAN in a multi-building environment
Number of Pages	55
Date	28.5.2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor	Ilkka Nenonen, CEO of Datainfo Getafix
Supervisor	Heikki Rahkonen, Lecturer

This thesis deals with designing, implementing and harmonizing a wireless LAN in a multi-building environment located on the premises of the work placement company's customer. The main focus of this work is on three main states: initial, present and future. The work also contains a theory part of WLAN technology

The building of the wireless LAN began when the customer built two new apartment buildings and needed an ease of use network solution in these buildings. First a wireless LAN for a one of these buildings was built and a plan for the harmonization of the LAN was created in the thesis project.

The building took place in two phases, the first part included the bigger apartment building and the second the smaller one. Those two phases made it possible to collect actual user excperience over a period of one year.

The harmonization of the networks is comprised in a completed plan, the implementation of which is still incomplete at equipment level. To complete the harmonization more network equipment than only wireless access points will be needed.

Problematic issues were encountered on the customer's premises which were built in several different phases and specifically with buildings that had different kinds of structural solutions. An example of such structural solutions was the use of fire safe materials to be applied in agreement with the spirit of the building era.

Keywords	wlan, building, planning LAN, device reflection

Sisällys

Lyhenteet

802.11

Standardi, joka koskee tietokoneiden WLAN-liikennettä.

802.11e

WLAN QoS Extension. Langattoman lähiverkon palvelunlaatulaajennus 802.11-standardiin. Tällä tekniikalla voidaan määrittää, mikä liikenne pääsee nopeammin liikkeelle, muun muuassa lyhyemmän odotusajan takia.

802.11g

802.11-standardin parannus, jolla nostettiin yhteysnopeutta 54 Mbp:iin. Kyseessä on toinen parannus kyseiseen standardiin, ensimmäinen parannus oli 802.11b.

802.11i

Uusin tietoturvaratkaisu langattomiin lähiverkkoihin kykenee myös WPA2:n myötä AES-salaukseen.

802.11n

802.11g-standardin parannus, jonka avulla voidaan nostaa yhteysnopeutta 600 Mbp:iin. Tämä standardi voi hyödyntää myös 40 MHz:n kaistanleveyttä 2,4 GHz:n kantataajuudella sekä pystyy käyttämään molempia tunnettuja kantataajuuksia, jotka ovat 2,4 GHz ja 5,0 GHz.

AES

Advanced Encryption Standard. Salausmenetelmä, joka kykenee erimittaisiin salausavaimiin. AES on suunniteltu korvaamaan vanha DES ja 3DES.

AP

Access Point. Langaton tukiasema, joka ei toimi reitittävässä tilassa, vaan jakaa muualla lähiverkossa olemassa olevasta DHCP-palvelimesta IP-osoitteita. Yhdistää langattomat päätelaitteet verkkoon.

ASCII

American Standard Code for Information Interchange. Normaalit kirjoitusmerkit.

Bluetooth

Standardi, jota matkapuhelinvalmistaja Ericsson alkoi tutkia ja kehittää yhdistääkseen matkapuhelimia ja niiden oheislaitteita keskenään.

CCK

Complementary Code Keying. Täydentävän koodin modulaatio. Keino, jota on käytetty jo 802.11b-standardin aikaisessa toteutuksessa. Tämä modulaatio valittiin käyttöön, koska se käyttää suunnilleen saman verran kaistaa sekä samankaltaista johdanto-osaa (preamble) että otsaketta (header) kuin aiemmin käytetty Barker-koodi. CCK mahdollisti nopeuksien 5,5 Mbps ja 11 Mbps käytön. Hitaammilla nopeuksilla käytetään Barker-koodia.

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. Langattomien lähiverkkojen tulevaisuuden salaus.

CoS

Class of Service. OSI-kerroksen 2 laitteiden mahdollisuus merkitä liikennettä, jotta palvelunlaatumäärittelyt toimisivat jo mahdollisimman varhaisessa vaiheessa.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance. Langattoman lähiverkon median varausmenetelmä, jolla vältetään kahden tai useamman aseman yhtäaikainen lähettäminen. Järjestelmä käyttää infrastruktuurimuodossa tukiasemaa lähetysajan jakelijana. Toimii ohjauskehyksillä.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection. Langallisen lähiverkon median varausjärjestelmä, jolla vältetään kahden tai useamman aseman yhtäaikainen lähettäminen. Järjestelmä tarkastelee verkkosegmenttinsä jännitetasoja ja siten päättää lähetysaikansa itse.

DHCP

Dynamic Host Configuration Protocol. IP-osoitteiden jakeluprotokolla. Toimittaa asiakaskoneelle tiedon myös oletusyhdyskäytävästä (Default Gateway) ja nimipalvelimista (DNS).

IP-osoite

Internet Protocol Address. IP-osoite, jonka avulla Internet toimii. IP-osoite jaetaan MAC-osoitteen perusteella tai määritetään staattiseksi. IP:stä on olemassa kolme versiota: IPv4, IPv6 ja IPv9.

IPv4

Vanha IP-osoiteversio, joka on edelleen runsaassa käytössä. Tyypillisesti nähtävä sisäverkon osoite on esimerkiksi: 192.168.1.1.

IPv6

Uusi IP-osoiteversio, joka ei ole vielä vahvassa markkina-asemassa. Käyttöönoton hitauden syiksi voidaan sanoa esimerkiksi ammattitaitoisten henkilöiden vähäinen määrä verrattuna vanhan ip-osoiteversion ammattilaisiin ja IPv6 ymmärtävien laitteiden vähäinen määrä maailmanlaajuisesti.

IPv9

Kiinan oma versio uudesta IPv6-osoitteistusmenetelmästä.

MAC

Media Access Control. MAC huolehtii pakettien pääsystä fyysiselle kuljetuskerrokselle. Jokaisella verkkolaitteella on yksilöllinen MAC-osoite.

MIC

Message Intecrity Code. Viestin eheyden tarkistusmenetelmä. MIC itsessään ei ole salattu, joten turvakeinot täytyvät toteuttaa muilla keinoin.

MIMO

Multiple Input Multiple Output. Moniantennitekniikka, jota käytetään tiedonsiirtoon. Antennien avulla voidaan nostaa verkkonopeutta tai kuuluvuusaluetta käyttötarkoituksista riippuen.

NTP

Network Time Protocol. Verkkoaikaprotokolla eli tietoliikenneverkossa toimiva kellojärjestelmä, joka mahdollistaa tarkan kellon asettamisen helposti jokaiselle laitteelle, koska laitteet hakevat itse aikansa NTP-masterkoneelta.

NTP-master

Verkkoaikaprotokollan palvelulaite, joka on tietyn matkan päässä Stratum1:stä.

OFDM

Orthogonal Frequency Division Multiplexing. Keino, jota käytetään limittämällä diskreettejä monitaajuuksia, mitkä eivät häiritse toisiaan käytössä. OFDM:n käyttö ei ole rajattu ainoastaan langattoman lähiverkon käyttöön vaan sitä käytetään myös langallisissa verkoissa, kuten ADSL-laajakaistaliittymissä sekä monissa muissa vastaavissa.

PAN

Personal Area Network. Henkilökohtainen lähiverkko eli matkapuhelimille ja niiden oheislaitteiden välille tarkoitettu keskusteluverkko, joka käyttää Bluetooth-standardia.

PDA

Personal Digital Assistant. Henkilökohtainen kämmentietokone. Kämmentietokonetta voidaan käyttää sähköisenä kalenterina ja yleisesti niitä voidaan päivittää langattoman lähiverkon kautta.

QoS

Quality of Service. Palvelunlaatu. Menetelmä, joka on suunniteltu pakettikohtaisen liikenteen parantamiseksi. Se on toteutettu antamalla joillekin paketeille lyhyempi jonotusaika ennen käsittelyä sekä eteenpäin toimittamista.

SOHO

Small Office Home Office. Pientoimistokäyttöön suunnattuja tuotteita.

SSID

Service Set ID. Tunniste, joka näkyy käyttäjille langattoman verkon nimenä. Voi olla enimmillään 32 merkkiä pitkä merkkijono, jossa isot ja pienet kirjaimet ovat eri asia.

Stratum1

On ryhmä tietokoneita, jotka on liitetty suoraan erittäin tarkkoihin kelloihin, kuten atomikelloihin. Ne jakavat kellon aikaa erittäin tarkasti suurempiin verkkoihin erillisten NTP-palvelinryhmien kautta, joita nimetään stratumeiksi. Mitä kauemmaksi mennään loogisessa topologiassa, stratum-numero kasvaa ja sitä suuremmaksi kellojen välinen aikavirhe kasvaa.

TKIP

Temporal Key Integrity Protocol. Langattoman lähiverkon turvaamiseen ja salaukseen kehitetty menetelmä, joka omaa automaattisen avaimen uusimisen. Sisältää WEP-salauksen pohjan yhdistettynä MIC:n ominaisuuksilla.

VOIP

Voice Over Internet Protocol. Internetprotokollan avulla siirrettävä ääni, joka on kokoelma tekniikoita äänen reaaliaikaiseen siirtämiseen.

VPN

Virtual Private Network. Näennäislähiverkko, joka on keino yhdistää joko yksittäinen kone tai kokonainen lähiverkko toiseen lähiverkkoon julkisen verkon kautta.

WEP

Wired Equivalent Privacy. 802.11-standardin ensimmäinen salausmenetelmä.

WLAN

Wireless Local Area Network. Langaton lähiverkko.

WPA

WiFi Protected Access. WEP-salauksen korvaaja, suunniteltiin WEP:n puutteiden takia.

1 Johdanto

WLAN eli langattomat lähiverkot ovat yleistyneet viime vuosina nopeasti, varsinkin 802.11g standardin valmistuttua vuonna 2003 sekä standardia tukevien laitteiden ilmestyessä. Langattomien lähiverkkojen etuja ovat helppo jaettavuus verrattuna kaapeloituun lähiverkkoon.

Viime vuosina kannettavien tietokoneiden, kämmentietokoneiden ja älypuhelinten lisääntyessä on ihmisille tullut tarpeita hyödyntää mukana olevia laitteitaan tiedon etsintään ja sähköpostin käyttöön. Kannettavan tietokoneen kanssa tämä on onnistunut muutenkin liittämällä tietokone LANiin, eli langalliseen lähiverkkoon, mutta tällöin on aina jouduttu karsimaan liikkuvuutta langallisen lähiverkon fyysisten rajoitusten vuoksi.

Tässä insinöörityössä on tarkoitus tutustua langattoman lähiverkon suunnitteluun, toteutukseen ja yhtenäistämiseen monikiinteistökohteessa teorian ja käytännön tasolla. Työ ei ole ainoa vaihtoehto jokaisen käyttöön, mutta se antaa pohjustusta omille pohdinnoille laitehankintoihin tai laitetarpeisiin.

Eikä myöskään tule unohtaa langattoman verkon haittapuolia, joita on esimerkiksi tietoturvan heikentyminen puutteellisen toteutuksen myötä. Tästä syystä langattoman verkon toteutusta muualle kuin omaan kotikäyttöön tulisi aina käyttää tietoliikenneammattilaista tai muuten erittäin valveutunutta dataverkkoihin perehtynyttä tietokonetukihenkilöä. Moni ihminen osaa asentaa langattoman lähiverkon käyttöönsä, mutta kuinka moni osaa ottaa huomioon liikenteen salauksen tai mahdollisen radiotiehäirinnän käyttämällä langatontalähiverkkoa.

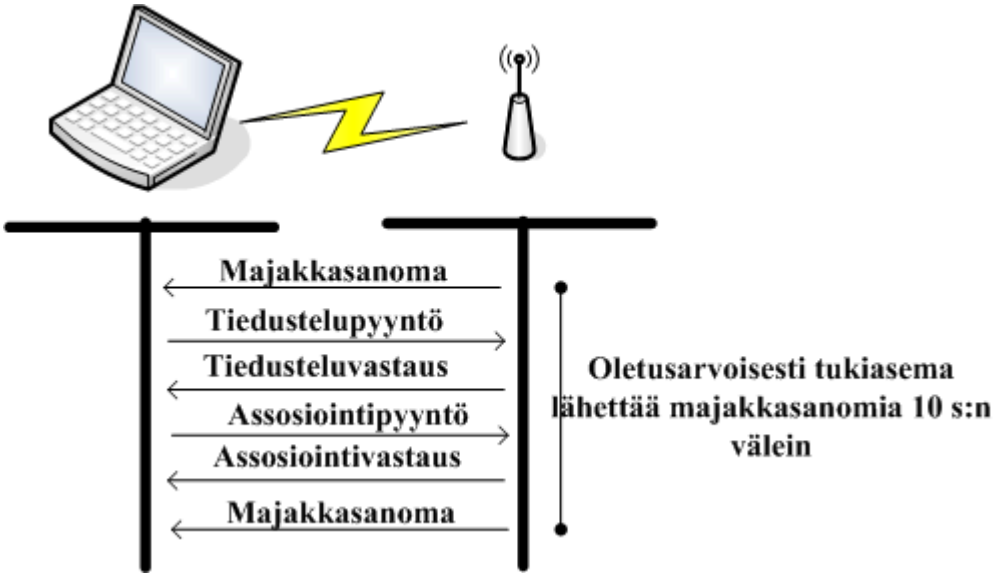
2 Langattoman lähiverkon ja 802.11g+n-standardien teoriaa

Vuonna 1999 IEEE:n (Institute of Electrical and Electroniccs Engineers) 802.11-komitea sai tehtäväksi kehittää jatkoa jo vanhentuneeseen ja hitaaseen 802.11b-standardiin. Uudistuksen tuli käyttää samaa vapaata 2,4 GHz:n aluetta, kuin 802.11b:kin oli käyttänyt. Täten varmistettiin yhteensopivuus vanhempaan standardiin, mikä on hyvä asia, koska kaikkialla ei ole välttämättä aina saatavilla uudemman standardin verkkoa.

802.11g-verkko voi toimia kahdessa tilassa, joita ovat yleisempi infrastruktuuri ja vähemmän käytössä oleva ad-hoc. Ad-hoc-tila jakaa langatonta lähiverkkoa ainoastaan langattomien päätelaitteiden kesken, jolloin ei tarvita erillistä langatonta tukiasemaa. Ad-hoc-tilan etuina on, että ilman langattoman lähiverkon läsnäoloa voi jakaa tietoa tietokoneiden välillä. Yleisempi infrastruktuuritila tarvitsee aina langattoman tukiaseman, joka myös voi toimia kahdessa eri tilassa, jotka ovat toistin (AP) ja reititin. Liitteessä 1 on kuva molempien tilojen toimintamallista.

802.11g-standardille on annettu teoreettiseksi maksimilinjanopeudeksi 54 Mbps ja käytännössä on maksimisiirtonopeudeksi saatu 22 Mbps, eli hieman alle puolet teoreettisesta maksimista. Langattoman lähiverkon siirtonopeus on hitaampi kuin langallisella vastineellaan. Tämän aiheuttavat useat osatekijät, joita ovat esimerkiksi: kapea radiokanava, varoajan suuruus ja muut vastaavat tekijät.

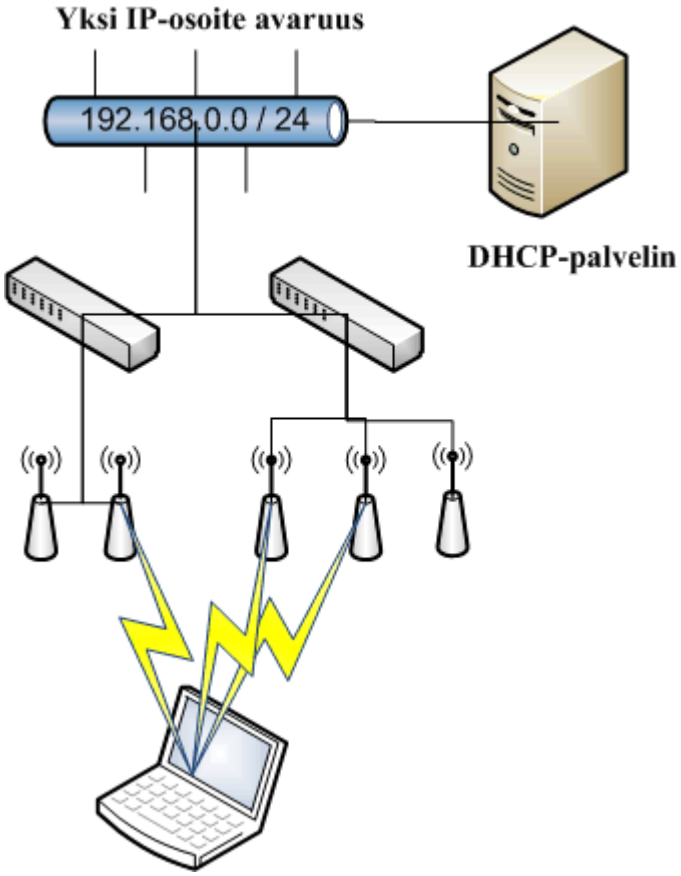
Langattoman lähiverkon tukiasemat toimivat erilaisilla ip-pakettien kehystyypeillä. Näitä kehystyyppejä on muun muuassa hallinta-, ohjaus- ja kuormakehykset. Hallintakehyksistä kannattanee mainita seuraavat: todennus-, todennuksenpoisto-, assosiointipyyntö-, assosiointivastaus-, uudelleenassosiointipyyntö-, uudelleenassosiointivastaus-, assosioinninpurku-, majakka- (beacon), tiedustelupyyntö- (probe request) ja tiedusteluvastauskehys. Kuvassa 1 on esimerkki langattoman yhteyden alustamisesta.



Kuva 1: Yhteyden muodostaminen ilman salausta

Ohjauskehyksistä on hyvä tietää seuraavat: lähetyslupakysely- (Request to Send), lähetyslupa- (Clear to Send) ja kuittauskehys (Acknowledgement). Kuormakehykset ovat varsinaista tietoliikennettä, jota langattomassa lähiverkossa kuljetetaan.

802.11g-verkon laajentamiseksi täytyi käyttää useampia kanavia, joista jokainen sijaitsi omilla tukiasemillaan. Kanavilla voidaan laajentaa saman SSID:n omaavaa verkkoa, kun jokainen tukiasema jakaa omalla kanavallaan verkkoa. Tällöin langaton verkko ei ole rajoitettu vain yhden tukiaseman kuuluvuusalueelle. Tämä mahdollistaa myös kulkemisen eri tukiasemien välillä verkkoyhteyksien katkeamatta, mikäli tukiasemien kuuluvuusalueet ovat päällekkäiset ja jakavat samaa IP-osoite avaruutta. (Kuva 2.) Tähän tarkoitukseen käytetään assosiointi- ja uudelleenassosiointikehyksiä pyyntöineen sekä vastauksineen.

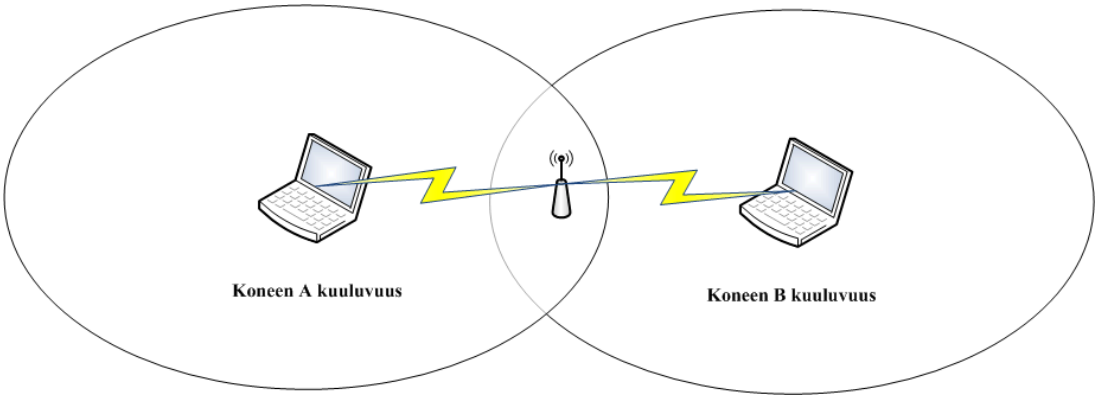


Kuva 2: Insinöörityössä käytetty roaming-tyyppi

Verkkovierailuille on olemassa monta erilaista totetutustapaa, esimerkkeinä voidaan ottaa luovutustavat, joita on kaksi, ja sopimustapa. Luovutustavoista ensimmäinen on horisontaalinen, joka toimii siten, että kaksi saman standardin laitetta voi kommunikoida päätelaitteen kanssa, tätä toimintatapaa käytettiin tässä työssä. Toinen luovutustapa on vertikaalinen, jossa tukiasemat voivat käyttää eri standardeja, kuten 802.11a:ta ja 802.11g:tä. Sopimistapa on operaattoreiden välinen toimintamalli, jossa operaattorin A asiakas voi käyttää operaattorin B infrastruktuuria, kuten matkapuhelimet kotimaassa tai ulkomailla. (1.)

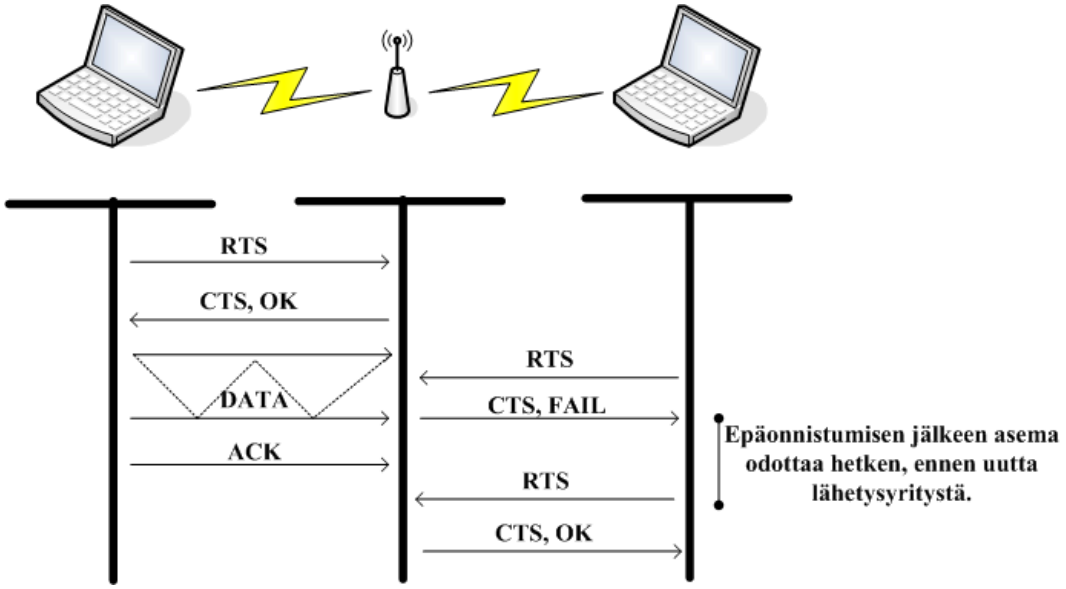
Langattoman lähiverkon mediana toimiva ilmatie on myös aiheuttanut uusien toimintojen kehittämiselle tarvetta, koska langallisessa verkossa toimiva CSMA/CD ei toimi ilmateitse. Tämä toimimattomuus ilmenee siitä, että kaksi eri lähettävää asemaa voivat olla saman tukiaseman kantavuusalueen eri päissä, jolloin ne eivät havaitse

toisiaan eikä CSMA/CD voi toimia. Kuvassa 3 esitetään CSMA/CD:n toimintatapa, mikäli sitä käytettäisiin langattomassa lähiverkossa.



Kuva 3: CSMA/CD langattomassa lähiverkossa

CSMA/CA, joka on luotu CSMA/CD:n tilalle, ei tarkastelekaan jännitetasoja, vaan lähettävä kone pyytää tukiasemalta lupaa lähettää dataa tietyn ajan, jolloin tukiasema vastaa myöntävästi tai kieltävästi. Myönteisen vastauksen jälkeen lähettävä asema lähettää datansa ja kuittaa ajan käytetyksi. Kielteisen päätöksen jälkeen lähettävä asema odottaa tietyn ajan verran ja pyytää uudelleen lähetyslupaa. Mikäli langattomaan lähiverkkoon on otettu käyttöön palvelunlaatumäärittelyt, tässä vaiheessa tukiasemat tekevät palvelunlaatuun liittyvät jonojen ajoitukset. Kuvassa 4 on CSMA/CA:n toimintamalli.(2 s.5.)



Kuva 4: CSMA/CA langattomassa lähiverkossa

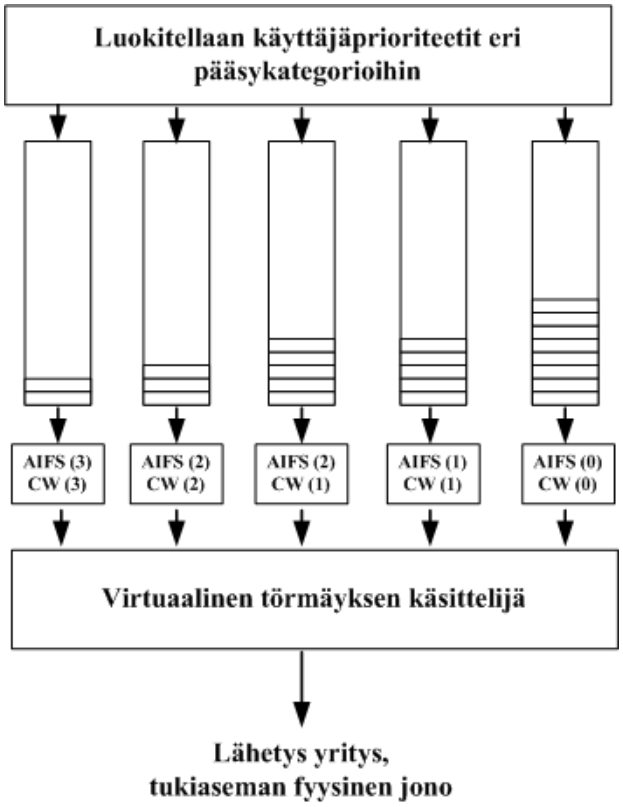
Palvelunlaatu langattomassa lähiverkossa

Alun perin langattoman lähiverkon palvelunlaatumäärittelyitä oli kahta eri mallia, joista ensimmäinen on kilpailullinen DCF (Distributed Coordination Function) ja toinen kilpailuton PCF (Point Coordination Function). Kilpailullisessa mallissa tukiasema toimii palvelunlaadun ohjaajana ja määrää tiedon liikkumisesta. DCF toimii siten, että tukiasema lähettää majakkaviestin, jossa on ajanvaraus ja sen jälkeen tukiasema joko alkaa kysyä päätelaitteilta lähetettävää dataa. Mikäli sellaista ei ole, vuoro menee seuraavalle, tai tukiasema lähettää päätelaitteelle dataa ja antaa vuoron seuraavalle. Mikäli kaikkea kilpailullista aikaa ole ei käytetty, lähettää tukiasema korjaussanoman, jossa vapautetaan ilmatie. (3, s.120–122.)

Tässä työssä käytettävä palvelunlaatumäärittely on standardin 802.11e:n mukainen, ja se on toteutettu MAC-laajennuksilla. Standardin hyviä puolia on, että voidaan käyttää samankaltaista palvelunlaatumäärittelyä kuin langallisenkin verkon puolella. Huonona puolena on vaatimus, että tukiasemat ja päätelaitteet tukevat tätä laajennusta. Ilman laajennusta päätelaitteet käyttäytyvät DCF-mallin mukaan. 802.11e on määritellyt toimintamallit sekä Diff-serv- että Int-serv-malleille. Tässä työssä keskitytään Diff-serv-malliin, joka on nimeltään EDCA. EDCA:n toiminta alkaa sillä, että päätelaite lähettää assosiointivaateen tukiasemalle, joka sisältää 802.11e:n mukaiset määrittelyt.

Tukiasema voi joko hyväksyä tai hylätä assosioinnin. Hyväksymistilanteessa tukiasema lähettää päätelaitteelle omat vastaavat määrittelyt. Koska 802.11e toimii MAC-laajennoksena ja Diff-serv toimii IP-paketissa, ja ovat siksi eri OSI-kerroksilla, täytyy niiden jotenkin kommunikoida. Tähän käyttöön on suunniteltu ja toteutettu ADDTS-primitiivit, jotka välittävät tiedon sekä tukiaseman ja päätelaitteen välillä että MAC-kerrokselta ylemmille kerroksille, jossa tieto käsitellään. (3, s.124–127.)

802.11e toimii käytännössä siten, että on olemassa jopa kahdeksan erilaista käyttäjäprioriteettia (User Priority, UP), joista jokainen kartoitetaan pääsykategorioihin (Access Category, AC), joista jokaisella on oma DCF-yksikkö. Nämä DCF-yksiköt toimivat yksilöinä toisistaan tietämättä ja yrittävät tyhjentää omaa AC:ta. AC antaa erilaisia parametreja DCF:lle, kuten AIFS:n (arbitration inter frame space, säädettävä kehysten välinen aika), joka määrää pakettien lähetysyrityksen välisiä aikoja. DCF:n käsittelyn jälkeen vuorossa on virtuaalinen törmäyksen käsittelijä (Virtual Collision Handler), jonka jälkeen paketit menevät fyysiseen lähetysjonoon. Kuva 5 havainnollistaa kyseistä toimintamallia.



Kuva 5: 802.11e EDCA:n toimintamalli

2.1 802.11g-standardi

802.11g-standardia kutsuttiin aikoinaan sekastandardiksi, koska se yhdisti kaksi erillistä standardia yhteen 802.11a ja 802.11b, tarkemmin mainittuna 802.11g-standardi yhdisti b-standardin CCK-modulaation ja a-standardin OFDM-modulaation.

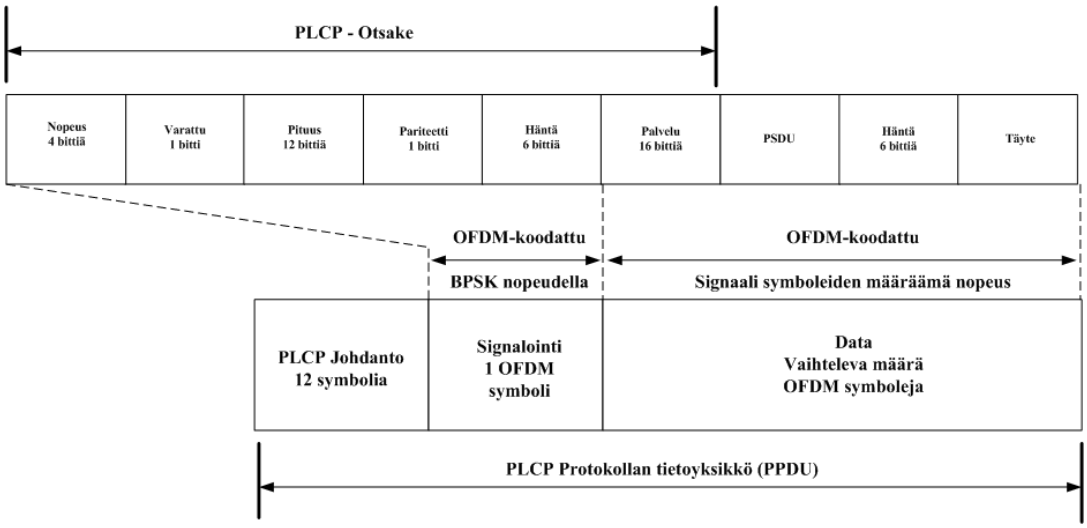
CCK-modulaatiota käytettiin 802.11b-standardin aikana muodostamaan nopeuksia 5,5- ja 11 Mbps, CCK toimii ainoastaan DSSS (Direct Sequence Spread Spectrum, suorasekventointi) tekniikalla, ei taajuushyppelysekvennoinnilla (FHSS). DSSS toimii siten, että lähetettävä data jaetaan pieniksi tiedon paloiksi ja palat lähetetään taajuuksille koko kaistanleveydeltään. Lähetettävä data lisätään itse luodun kohinakantoaallon päälle ja lähetetään vastaanottajalle. Vastaanottaja osaa purkaa kohinan pois datasta, koska se tietää käytettävän sekvenssin. Tästä tulee hyötyinä seuraavat:

- Radiohäirinnän sietokyky on parempi, joko tarkoituksellisen tai tarkoituksettoman häirinnän
- Yhden kanavan voi jakaa useammalle käyttäjälle
- Parempi signaali-kohinasuhde
- pystytään määrittelemään relatiivinen ajoitus tukiaseman ja päätelaitteen välillä
- CCK hyödyntää DQPSK modulointia, jolla voidaan kääntää kantoaaltoa neljään eri kulmaan sen perusetenemiseen nähden.

OFDM-modulaatiota käytetään sekä 802.11a-standardilla että 802.11g-standardilla. OFDM:n avulla voidaan jakaa saatavilla olevat 13 kanavaa, joista jokaisen leveys on 22 MHz, 52 alikanavaan, joista vain 48 on käytettävissä. Ne neljä alikanavaa, joita kutsutaan pilottikanaviksi, on valittu kuuntelemaan muiden alikanavien ylivuotoja ja lähettämään kiinteää bittikuviota, joka ei ole varsinaista dataa. Alikanavat ovat 0,3125 MHz:n päässä toisistaan. Nopeimmillaan 802.11g-verkko toimii 54 Mbps:n nopeudella, minkä voi todeta seuraavasta. 64QAM-modulaatio kykenee toimittamaan 6 bittiä/kantoaalto. 48 alikanavaa joita käytetään kantoaaltoina. Virheenkorjausbitit vievät neljänneksen lopullisesta lopputuloksesta jää jäljelle 6 symbolia/kantoaalto · 48 kantoaalto/sekunti · ¾ hyötykuormalle = 216 symboli/sekunti. Kun tähän kerrotaan

jokaisen alikanavan symbolinopeus, joka on 250 000 bittiä/symboli, saadaan lopputulokseksi 54 Mbps. (3, s. 40–44.)

802.11g-standardin laitteilla voidaan käyttää kahta eri johdanto-osaa, lyhyempää ja pidempää. Mikäli ei ole tarvetta tukea 802.11b-standardin hitaampia laitteita, voidaan käyttää lyhyempää johdantoa. OFDM:n käyttämä johdanto-osa on 12 symbolia pitkä ja kokonaisen johdanto-osan lähettämiseen menee 20 µs. CCK:n käyttämä johdanto-osan lähettäminen kestää 72 µs, eikä pidä myöskään unohtaa synkronointibittien viemää aikaa, jotka voi olla 192 µs tai 96 µs (3, s. 34). Kuva 6 esittää OFDM:n käyttämästä fyysisen ja loogisen tason konvergenssitavasta.



Kuva 6: OFDM:n keino yhdistää looginen ja fyysinen taso (3, s. 42; 4, s. 28)

Kuvan lyhenne PLCP, tarkoittaa fyysisen kerroksen konvergenssiproseduuria (Physical Layer Convergence Procedure). Kuvassa ylempi osio on loogisella tasolla ja alempi fyysisella tasolla. Signaalitasojen takia alkuun lähetetään hidas johdanto- ja signalointiosa ja vasta niiden jälkeen lähetetään signalointia vastaavalla nopeudella dataa. Kuvan alemmassa osassa oleva PLCP-johdanto lähettää ensin kymmenen lyhyttä ja kaksi pitkää OFDM-symbolia joiden tarkoituksena on säätää vastaanottavan aseman AGC:ta (Automatic Gain Control, Automaattinen vahvistuksen säätö). PLCP-johdanto-osan lähettämiseen menee 16 µs ja otsakeosuudelle jää 4 µs aikaa. Johdanto-osan jälkeen lähetetään PLCP-otsakeosuus, johon otetaan loogiselta tasolta seuraavat mukaan nopeus, varattu, pituus, pariteetti, häntä ja palvelu. Huomioitavaa on se, että varattu

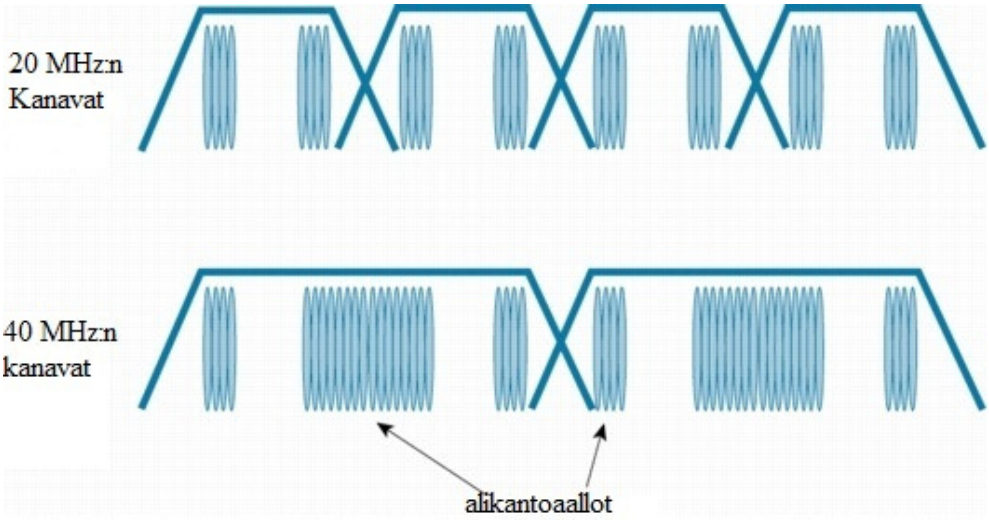
kenttä on aina looginen nolla ja palvelukentän ensimmäiset seitsemän bittiä ovat nollia, ja loput on varattu tulevaisuuden käyttöön (4, s. 28–29).

802.11g-standardilla on samat heikkoudet kuin 802.11b-standardilla. Ne johtuvat enimmäkseen 2,4 GHz:n kantataajuudesta, jolla voidaan radioaaltojen voimin lämmittää vettä, kuten mikroaaltouunin toimintatapaan kuuluu, ja jotka ovat vapaita useamman eri käyttötarkoitukseen suunnatun laitteen käyttöön. Tästä esimerkkinä ovat aiemmin mainitun mikroaaltouunin tapaan myös Bluetooth-standardin PAN-laitteet.

802.11g-standardin mukaisella 2,4 GHz:n kantataajuudella on omat vahvuutensa ja heikkoutensa verraten 802.11a-standardin mukaiseen 5,0 GHz:n kantataajuudella toimivaan versioon. Vahvuuksiin kuuluvat muun muassa yleisempi standardi, jota useat valmistajat tukevat, halvemmat antennin valmistuskulut ja pidemmän matkan kuuluvuus johtuen ilman vaimennuksesta. 5,0 GHz:n kantataajuudella toimivilla lähiverkkolaitteilla on myös etuja, kuten vähemmän häiritsevä radioliikenne, useampi toisiaan häiritsemätön radiokanava, ja suuremmasta kantataajuudesta johtuen radiokaistaa on enemmän käytössä. Samaisesta kantataajuudesta johtuen ei aiheudu distortioita veden molekyylien kanssa.

2.2 802.11n-standardi

802.11n-standardi sai alkunsa vuonna 2007 alkaneesta standardivedoksesta. Standardi lupaa jopa 600 Mbps:n nopeudet, mutta käytännössä nopeudet eivät ole ylittäneet 200 Mbps:aa montaa kertaa hyvissäkään olosuhteissa. Tämän standardin langattomat tukiasemat pystyvät käyttämään molempia käytössä olevia kantataajuuksia, jotka ovat 2,4 GHz ja 5,0 GHz. Keinoja, joilla verkon yhteyttä voidaan nopeuttaa, ovat kaistanleveyden kasvattaminen ja antennien lukumääräinen lisääminen. Alkuperäinen kaistanleveys 802.11b/g-standardeilla on 20 MHz. 802.11n-standardivedoksella on kaksi eri kaistanleveyttä: 20 MHz ja 40 MHz. 20 MHz:n käyttäminen 802.11n-standardin laitteilla antaa taaksepäin yhteensopivuuden vanhempiin langattoman lähiverkon asiakaslaitteisiin (5, s.10–11). Kuvasta 7 käy ilmi eri kaistanleveyksien ero. Leveämmille kanaville mahtuu enemmän dataa, koska alikantoaallotkin ovat leveämpiä.



Kuva 7: 20 MHz:n ja 40 MHz:n välinen ero (6)

802.11n-standardin tukiasemat käyttävät montaa eri keinoa nostaa yhteysnopeutta. Näitä ovat:

- suorituskykyisempi virheenkorjaus, eli on parempi hyötykuormasuhde virheenkorjausbitteihin verrattuna
- lyhyempi varoaika
- enemmän OFDM-alikantoaaltoja, kuin 802.11g-standardin lähitukiasemilla
- moniantennitekniikka, joka antennilla summataan yhteysnopeutta suuremmaksi
- leveämmät kaistat, joka mahdollistaa datakantoaaltojen määrän kasvun. (5, s.18–19.)

2.3 Tietoturva ja salausmenetelmät

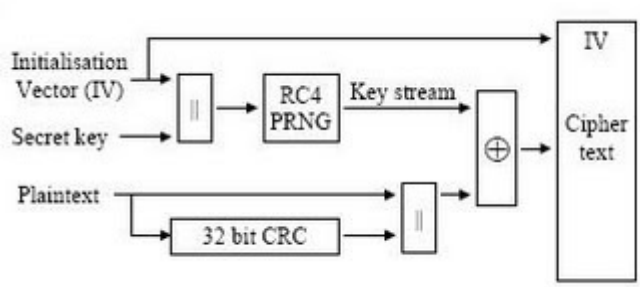
SSID:n salaaminen

On olemassa helppo keino salata langaton verkko, joka on ottaa verkon SSID pois näkyviltä. Tällöin ei tarvitse myöskään kiinnittää huomiota helppoon ja kuvaavaan nimen esittämiseen. Päinvastoin tällöin voi hyödyntää mahdollisimman hankalaa langattoman lähiverkon SSID-nimeä, jolloin se ei ole arvattavissa. Tämä keino on vain

hidaste, koska aina liityttäessä langattomaan lähiverkkoon lähetetään yhteydenmuodostusviestit salaamattomana. Tämä muodostaa mahdollisen riskin, jolloin ei-lähettävässä tilassa oleva langattomaan lähiverkkoyhteyteen kykenevä laite voi kuunnella liikennettä ja napata SSID-tiedon kenenkään tietämättä.

WEP

WEP on ensimmäinen 802.11-standardin salausmenetelmä. WEP-salaus käyttää RC4-salausta luottamuksellisuuden varmistamiseksi ja CRC-32-tarkistussummaa eheyden varmistamiseen. Kuva 8 havainnollistaa WEP-salauksen toimintaperiaatteen.



Kuva 8: WEP-salauksen toimintaperiaate (7)

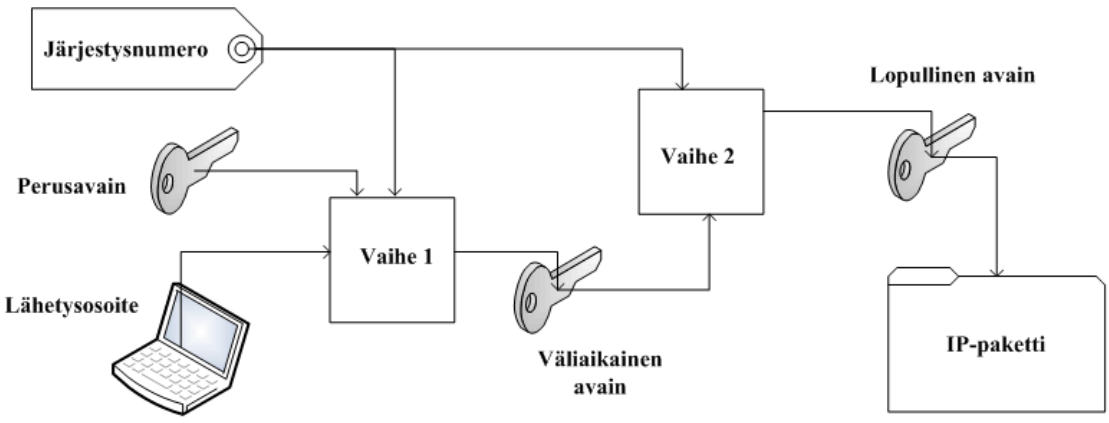
Luottamuksellisuus tarkoittaa sitä, että tiedetään viestin lähettäjä ja vastaanottaja varmasti. Eheys puolestaan tarkoittaa sitä, että tiedetään viestin sisältö muuttumattomaksi. Salaus toteutetaan yksinkertaisella laskennalla, jossa yhdistetään alustusvektorit, salausavain saadaan laskemalla RC4-salaus, joka XOR-laskennalla yhdistetään normaaliin salaamattomaan viestiin. Jotta vastaanottaja pystyy purkamaan salauksen, WEP-salaus lähettää alustusvektorit salaamattomana jokaisen paketin alussa. Alustuksen salaamattomuus muodostaa WEP-salaukseen suuren heikkouden.

WEP-salauksen hyviä puolia on se, että myös vanhemmat langattomat laitteet tukevat sen käyttöä. Huonoksi puoleksi tulee laskea se, että WEP-salauksen voi purkaa myös kotikonstein.

Pelkän WEP-salauksen käyttöä ei voi suositella missään langattomassa verkossa yksittäin. Jos joka tapauksessa haluaa käyttää WEP-salausta, niin sen kanssa olisi hyvä myös hyödyntää MAC-listausta. Sallittujen langattomien verkkokorttien MAC-osoitteet asetetaan luvallisten MAC-osoitteiden listalle, tosin tämäkin keino on pelkkä hidaste, koska MAC-osoitetta voidaan vaihtaa hallintaohjelmilla.

WPA-TKIP

Wpa-tkip luotiin aiemmin tehdyn WEP-salauksen korvaajaksi, koska WEP-salaus ei koskaan ollut vahva salausmenetelmä. WPA-TKIP-salausmenetelmä poisti staattisen neljänkymmenen (40) bitin salauksen tarpeen, jolloin voi laittaa kahdeksasta (8) kolmeenkymmeneenkahteen (32) merkkiä pitkiä salausavaimia, joita kutsutaan perusavaimiksi. Muuttuneiden salausavainten pituuksilla oli se etu, että ennalta-arvattavuus katosi. WPA-TKIP ei käytä suoraan perusavainta, eikä ensimmäisen vaiheen jälkeistä väliaikaista avainta. WPA-TKIP käyttää salaukseen avainta, joka luodaan jokaiselle IP-paketille yksilöllisesti. Kuvasta 9 näkee TKIP-avaimen luontivaiheet. (3, s. 82.)



Kuva 9: TKIP-salausavaimen luonti (3, s.83)

Samalla WPA-TKIP esitteli MIC:n, jonka avulla verkon tietoturva kasvoi entisestään. MIC tarkistaa pakettien eheyttä laskennallisin menetelmin ja virheellisen paketin havaittaessaan se pistää kaikkien kyseisen tukiaseman asiakkaiden todentamisen uusiksi ja estää uusien asiakkaiden liittämisen minuutin ajaksi.

MIC ei itsessään sisällä mitään salausta, vaan MIC:ä tulisi käyttää salatun yhteyden kautta. TKIP käyttää pohjanaan vanhaa RC4-salausta, kuten WEP, joten TKIP on yhtä haavoittuvainen hyökkäyksille, mutta TKIP:n etuna on vaihtaa avainta automaattisesti hyökkäyksiä havaittaessa. TKIP hyödyntää MIC:ä havaitakseen hyökkäyksiä ja pakottaa asiakkaitaan vaihtamaan salausavainta, jolloin hyökkääjä joutuu jälleen aloittamaan alusta. MIC voi myös estää yhteyden muodostumisen liiallisten epäonnistumisten vuoksi.

WPA2-PSK

PSK on WPA2:n ennalta jaetun salausavaimen versio. Tätä salausta voidaan hyödyntää kotona, mikäli omistaa tarpeeksi uuden tukiaseman ja tietokoneen, jossa on tuki WPA2-PSK-salaukselle. Jokainen tietoliikennepaketti salataan 256-bittisellä avaimella, joka muodostetaan itse määrittämästä sanasta, jonka pituus voi vaihdella kahdeksasta (8) kuuteenkymmeneenkolmeen (63) merkkiin. Merkkien tulee olla ASCII-merkkejä, jotka voivat sisältää erikoismerkkejä.

Ennalta jaetun avaimen heikkouksia on alkuperäisen salausavaimen staattisuus, elleivät käyttäjät itse vaihda kovin usein salausavaintaan. Toinen heikkous on, jos käyttää turhan lyhyttä salausavainta. Suosituksien mukaan ei kannata käyttää alle kolmetoista (13) merkkiä pitkiä salausavaimia eikä salausavaimen kannata olla mikään sana, koska sanakirjoista haetaan ensin mahdollisia salausavaimia.

WPA2-AES

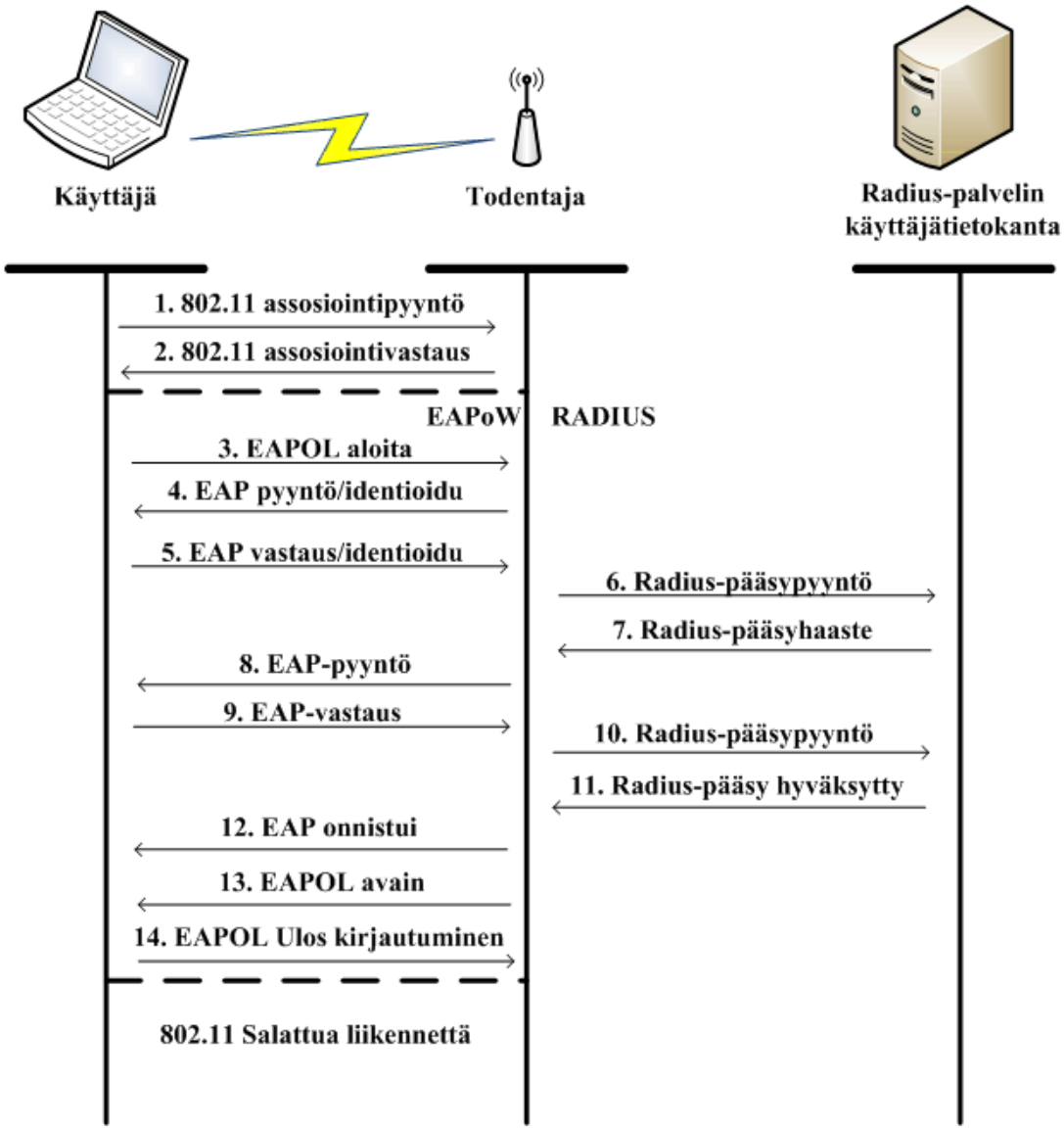
Käytännössä WPA2-AES-salaus on päivitys WPA-salaukseen. Päivityksessä otettiin huomioon myös 802.11i-standardin vaateet ja se hyödyntää myös CCMP-salausprotokollaa. WPA2-standardin päivitys sai alkunsa vuonna 2004.

IEEE 802.1x

IEEE 802.1x on alun perin suunniteltu siten, että verkko todentaa käyttäjät, eli LAN:a ei pystynyt käyttämään ilman kirjautumista, jonka jälkeen sai luvan käyttää verkkoa ja sen suomia palveluita. Tämä ominaisuus on siis varsin hyvä lähtökohta langattoman lähiverkon turvaamiseen. IEEE 802.1x tukee sekä paikallista että etäkäyttäjätietokantaa. Kummatkin on hyvä olla olemassa. Koska etätietokannassa on hyvä pitää verkon käyttäjät, ja mikäli verkko menee syystä tai toisesta vikatilaan, voidaan paikallisesta tietokannasta hakea hallinnointikäyttäjätunnukset.

IEEE 802.1x pohjautuu EAP:aan (Extensible Authentication Protocol), joka suunniteltiin PPP:n (Point-to-Point Protocol) käyttöön. Hyvin aikaisessa vaiheessa havaittiin, että EAP on toiminnaltaan todella hyvä todennuskäyttöön ja se standardoitiin. EAP:aa voi käyttää minkä tahansa linkkikerroksen protokollan päällä, joten se on myös joustava protokolla. Langattomassa lähiverkossa käytettävä EAP on tarkennettuna EAPoW (EAP over Wireless). EAP-protokollalla on erilaisia todennusmetodeita, kuten EAP-SIM, jota käytetään enimmäkseen matkapuhelimissa, ja EAP-TLS (Extensible Authentication Protocol – Transport Layer Security), jota käytetään tietoverkkojen siirtokerroksella. EAP-TLS:n suurin etu on, että se osaa molempien osapuolten tunnistuksen ja osaa vaihtaa istuntoavaimet turvallisesti. EAP-TLS:n haittapuolina on vaatimus X.509-sertifikaattiavaimista. Esimerkiksi Microsoftin palvelimet osaavat CA:n (Certificate Authority), jolla myönnetään X.509-sertifikaatteja. EAP:sta on myös valmistajakohtaisia laajennuksia, kuten LEAP (Lightweight EAP), joka on Cisco Systemsin kehittämä menetelmä. (3, s. 77–79.)

IEEE802.1x:n tunnetuin ei-valmistajariippuvainen AAA-protokolla on RADIUS. RADIUSin etuna on myös liitettävyys erilaisiin käyttäjätietokantoihin, kuten Kerberosiin jota Microsoftin aktiivihakemistot käyttävät natiivisti. Kuvasta 10 käy ilmi IEEE802.1x:n mukainen keskustelu todennuksesta.



Kuva 10: 802.1x-todennus Radiusin kanssa (3, s. 77;8)

2.4 Käyttöön valitun tukiaseman soveltuvuus

Tässä insinöörityössä valittiin käyttöön Cisco Systemsin 11240AG-mallin tukiasemat, jotka soveltuvat käyttöympäristöön täysin. Aiemmin esitettyjä salauksia tukiasema tukee ja hyödyntää moitteetta, lukuun ottamatta wpa2-aes-salausta, koska se tulee ilmestymään tulevaisuudessa. Oikeassa käyttöympäristössä turvallisen hallinnan mahdollistavat seuraavat seikat: hallinta-VLANin tulevaisuuden käyttö, SSH- ja hätätapauksessa HTTPS-yhteyksien käyttö. Telnet- ja http-yhteyksiä ei käytetä, koska ne lähettävät käyttäjätunnukset ja salasanat salaamattomana verkossa.

Todennukseen valittu tukiasematyyppi käyttää seuraavia standardeja ja protokollia: wpa, wpa2, Cisco TKIP, Cisco MIC, IEEE 802.11 WEP, EAP-Fast, PEAP-GTC, PEAP-MSCHAP, EAP-TLS, EAP-TTLS, EAP-SIM ja Cisco LEAP.

Salaukseen tukiasema käyttää seuraavia standardeja ja protokollia: AES-CCMP, TKIP(WPA), Cisco TKIP, WPA TKIP, IEEE 802.11 WEP. Tukiasema on varustettu erillisellä AES-salausavustin piirillä, jonka avulla saavutetaan suurempi turvallisuus heikentämättä langattoman lähiverkon suoritusta. (9.)

3 Langattoman verkon suunnittelu monikiinteistökohteessa

Jokainen monikiinteistökohde on erilainen, ja ne voivat olla erilaisia lähtökohdiltaan tai tarpeiltaan. Tämä insinöörityö ei ole ainoa oikea ratkaisu, vaan antaa pohjustusta omille laitehankinnoille ja verkkosuunnitteluille.

3.1 Lähtökohta

Insinöörityön alkutilanne oli seuraavanlainen. Asiakasyritys oli rakennuttanut tontilleen kaksi uutta erikokoista huoneistohotellirakennusta. Asiakasyrityksen mukaan langallisen lähiverkkoyhteyden jakaminen oli sopimaton ratkaisu, koska heidän asiakkaansa joutuisivat näkemään liikaa vaivaa. Tarvittaisiin siis langaton verkko, jonka avulla asiakkaat pääsisivät käyttämään Internet-yhteyttä.

Verkkoratkaisun tuli olla loppukäyttäjille mahdollisimman helppo, heidän ei tarvitse hallita tietotekniikkaa eikä langattoman lähiverkon salausta, ainoastaan valita käytettävissä oleva langaton verkko, joka alueella sattui olemaan. Tekniseltä näkökannalta käytön helppous edellytti DHCP-palvelimen käyttöä, joka tarjoaa IP-osoitteen ja oletusyhdyskäytävän osoitteen, jolloin asiakkaiden ei tarvinnut asettaa IP-osoitetta itse. DHCP-palvelimen käyttöä tukee myös verkkovierailun käyttö. Verkkovierailut edellyttävät tukiasemien pitämistä yhdyspistemuodossa, jolloin tukiasemat jakavat DHCP-palvelimen antamaa IP-avaruutta.

Asiakasyrityksen alueella olevat langattomat tukiasemat ovat kaikki fyysisesti kytkettynä asiakkaille tarkoitettuun lähiverkkoon. Tuotantoverkossa ei ole ensimmäistäkään langatonta tukiasemaa. Henkilökunta kykenee hyödyntämään tätä langatonta lähiverkkoa työasioidensa hoitamiseen, mutta heidän tulee aina ottaa VPN-yhteys työverkkoon, jolloin verkkonopeudet hidastuvat. Syy on infrastruktuurissa. Asiakasverkko on täysin erillinen lähiverkko suhteessa tuotantoverkkoon, jolloin VPN-yhteys yhdistetään aina ISP:n kautta, mikä tarkoittaa ainakin kahden eri modeemin kautta kulkevaa liikennettä.

3.2 Tarpeen määrittely

Loppukesänä 2008 tehty käynti asiakasyrityksen luona selvitti rakennusten fyysiset ratkaisut ja niiden mitat. Päädyin seuraavaan ratkaisuun: sijoitetaan langattomat tukiasemat tekniseen tilaan ja tuodaan ulkotilaan tarkoitetut antennit ulos, laitetaan tukiasemien ja antennien välille hyvin vähän vaimennusta aiheuttava antennikaapeli. Tällöin itse tukiasemat eivät olisi ulkona säiden ja tihutöiden armoilla. Langattoman lähiverkon kattavuudet oli kartoitettu mittaamalla signaalia normaaleilla päätelaitteilla, kuten kannettavalla tietokoneella ja älypuhelimella. Tällä keinolla saatiin varmistettua verkon oikea toimivuus loppukäyttäjienkin laitteilla.

Lähtökohtina oli uusien normien mukaan rakennetut rakennukset, joihin tuli laittaa toimiva langaton lähiverkko. Uudet normit käsittivät paloturvallisia seinä- ja ovirakenteita. Jokaisessa huoneistossa oli myös asiakkaille annettu käyttöön mikroaaltouunit, jotka käyttävät samaa vapaata kantataajuusaluetta kuin käyttöön otettava langaton lähiverkko. Langattomaan lähiverkkoon liittymisen tuli olla helppoa ja vaivatonta loppukäyttäjää ajatellen. Kuvassa 11 esitetään rakennusten ulkoiset rakenteet ja sivuprofiilit.

Kuva 11: Kohderakennusten profiili

Tietoturvapolitiikka

Asiakkaan tietoturvapolitiikka on todella tiukka koskien tuotantoverkkoa, eikä asiakasverkossakaan saa kaikkea tehdä. Tuotantoverkko ja asiakasverkko ovat fyysisesti erotettuja, joten tuotantoverkon tietoturvapolitiikka ei sinällään päde asiakasverkkoon. Asiakasverkossa on sallittu ulosmenevässä ja sisääntulevassa liikenteessä sallittu ainoastaan sähköposti-, HTTP- ja HTTPS-palvelut. Kaikki muu verkkoliikenne jää palomuurin säännöstöihin.

Tuotantoverkossa kirjautuminen tapahtuu Kerberos-palvelimen kautta, ja vain LAN-verkossa olevat koneet muodostavat Kerberos-palvelimeen yhteyden. Yhteys otetaan jo tietokoneelle sisäänkirjautumisvaiheessa, ja liikennöinti palvelimen ja asiakkaan välillä on ESP-suojattua.

Asiakasverkossa ei ole minkäänlaista salausta, koska jokainen loppukäyttäjä on vastuussa omista laitteistaan ja verkonkäytöstään. Ainoastaan verkkopalveluita on karsittu palomuurin avulla, ja kaikki liikenne, mikä ei ole Internet-selaamista, pudotetaan armotta pois. Tämä tosin alkaa vaikuttaa vasta, kun verkkoliikenne menee palomuurin lävitse, eli sisäverkon alueella voidaan käyttää mitä tahansa liikennettä.

3.2.1 Langallisen verkon ulosrajaaminen

Loppukäyttäjiä ajatellen ei ole käytännöllistä antaa heille käyttöön langallista verkkoyhteyttä, johtuen liian suuresta vaivasta käyttöönottovaiheessa. Samalla asiakkaalla on tällä hetkellä täysin toimiva verkkoinfrastruktuuri, joten tämä työ ei tule käsittelemään langallista verkkoa vielä sen enempää. Pelkästään se tieto riittää että langallisen verkon puolella toimii: modeemi, josta on Internet-yhteys ja erillinen palomuurilaite, jossa toimii DHCP-palvelu ja NAT-palvelu. Langallisen verkon puolella on myös erillinen lokien keräyskone NTP-palveluineen.

3.2.2 Langattoman verkon tarpeet

Rakennukset ovat rakenteeltaan luhtityyppisiä. Rakennusten profiilikuvista näkyivät ulkoiset käytävät, joita pitkin huoneistoihin kuljetaan. Käytävät jäävät auttamatta säiden armoille, joten sisätiloihin tarkoitettuja laitteita ei voinut suoraan ottaa käyttöön.

Tein alustavan suunnitelman molempiin rakennuksiin, mutta aluksi vain toiseen rakennuksista suunnitelma toteutettiin testitarkoituksessa. Toteutus tehtiin suurempaan rakennukseen, joka on noin kaksi kertaa suurempi kuin toinen huoneistohotellirakennus.

Rakennusten fyysiset rakenteet eivät mahdollistaneet suoraan normaaleiden sisäkäyttöön suunnattujen langattomien yhdyspisteiden käyttöä, koska rakennuksissa on ulkotilaan avoimet portaikot, jolloin tuli valita osittain ulkotiloihin sopivia laitteita. Alustavat suunnitelmat sisälsivät kanavatopologia-, hallintaosoitteisto- ja rakennusten kohdalla olevan verkkotopologiakaaviot.

Esitin tekniselle myyjälle suunnitelmani, joka sisälsi seuraavat asiat. Suurempi huoneistohotellirakennus tulisi tarvitsemaan kolme tukiasemaa ja kaksikerroksisuuden vuoksi kuusi antennia ja pienempi huoneistohotellirakennus tulisi tarvitsemaan kaksi tukiasemaa ja neljä antennia samaisen kaksikerroksisuuden vuoksi.

Syitä näin lähekkäin sijoitettavien antennien käyttöön ovat uusien paloturvallisuusmääritysten mukaiset rakenteet niin ovissa kuin seinissäkin. Muita syitä lähekkäin sijoitettuihin antenneihin on langattoman verkon saatavuuden varmentaminen, joka saadaan aikaiseksi jakamalla useampaa eri kanavaa rinnakkain, ja vikasietoisuuden lisääminen.

3.3 Tarvittavan laitteiston käytännön testaus

Jotta kannettavalla tietokoneella voi käyttää langatonta verkkoa, tukiaseman antennivahvistuksen tulisi olla pieni, koska ylikuuluvuus voi aiheuttaa langattoman verkon käyttökelvottomuuden.

Antennivahvistuksen kasvaessa ylikuuluvuuden mahdollisuus kasvaa. Ylikuuluvuus tarkoittaa sitä, että vastaanottava asema näkee verkon ja mahdollisesti hyvällä signaalilla, mutta ei pysty lähettämään dataa takaisin liian suuren välimatkan takia. Tämä on ensimmäinen asia, joka kannattaa ottaa huomioon antennivahvistuksia säädettäessä. Toinen asia, joka kuuluu huomioida, on yhteenlaskettu efektiivinen lähetysteho, joka ei saa ylittää Suomessa 100 mW:n rajaa.

Testauslaitteisto

Testausta varten ei hankittu suuria määriä aktiivilaitteita, vaan minimimäärä, jolla testi voitiin suorittaa. Seuraavasta listauksesta selviävät testissä käytetyt laitteet. Testissä käytettävää kannettavaa tietokonetta ei erikseen hankittu, vaan se oli jo valmiina olemassa.

- 1 kpl Cisco Aironet 1240AG- tukiasema
- 2 kpl Air-Ant 2506-antenneja

- 1 kpl 50 metriä pitkä CAT5 ethernet-kaapeli
- 1 kpl HP Mini 2133 kannettava tietokone

Testaus

Testaus suoritettiin käytännössä siten, että langaton verkkolaitteisto oli sijoitettu toiseen päähän rakennusta ja kävelin huoneistoissa kauemmasta päästä läheisempään päähän rakennusta samalla langatonta verkkoa hyödyntäen. Testiin kuului myös käyttää verkkoa välillä huoneiston ovi auki ja välillä kiinni.

Käytävällä ollessani langattoman verkon käyttöä ei häirinnyt mikään, mutta huoneistoon mennessä verkkoyhteys katkesi aina, kunnes tulin tarpeeksi lähelle tukiasemaa olevaan huoneistoon. Tämä huoneisto oli maksimissaan neljäs huoneisto antennista laskettuna, joten radiosignaalia heikentämässä oli maksimissaan kahdeksan seinää.

Havaitsin, että verkkoyhteys toimii tarpeeksi hyvin ja etäisyys olisi sopiva alkuperäisen kolmen tukiaseman verkkoon suunnitelman mukaisesti, näin myös saataisiin yhtenäinen langaton verkko käyttämällä eri tukiasemilla eri kanavia.

Mittaustulosten varmistaminen laskennalla

Jotta mittauksen tulos voitiin varmistaa tieteellisemmällä näkemyksellä, suoritettiin laskenta laitteistosta saaduista arvoista. Arvoina oli tukiaseman vahvistus, antennin vahvistus, kaapelin vaimennus ja antennikaapeleiden liitoskohtien vaimennus. Lisäksi olin saanut kannettavalla tietokoneella mitattua signaalin, jonka aikana langaton verkko vielä toimi käyttötarkoituksessaan. Mittaustulos oli tietokoneohjelman antamana (-90) dBm, kyseisen tuloksen sain Network Stumbler-ohjelmalta. Kaavan 1 mukaan dBm:t muutettiin mW:ksi.

$$P = 10^{\left(\frac{dBm}{10}\right)} \qquad (1)$$

P on kokonaisteho wateissa

dBm on millidesibelejä

Kokonaisvahvistus on laskettu seuraavasti: tukiaseman lähtöteho + antennivahvistus – kaapelihäviö – signaalin heikkeneminen liitoksissa, jonka kaava on seuraava:

$$dBm = P_{dB} + G_{dBi} - A_{cable} - A_{Connections} \quad (2)$$

dBm on millidesiBelejä

P_{dB} on langattoman tukiaseman lähtöteho desibeleissä

G_{dBi} on antennin vahvistus desibeleissä

A_{cable} on antennikaapelin kokonaisvaimennus desibeleissä

$A_{Connection}$ on antennikaapeleiden liitosten vaimennus desibeleissä

Nyt kun kaavat ovat tiedossa, luvut voidaan sijoittaa lukuja yhtälöihin. Ensimmäiset kaksi kaavaa on pidemmälle kaapelille ja jälkimmäinen lyhyemmälle kaapelille. Käytetyt arvot ovat valmistajan ilmoittamat.

17 dBm + 5,2 dB – 4,4 dB – 1 dB = 16,8 dBm

$$10^{\left(\frac{16,8}{10}\right)} = 47,86 \ mW$$

17 dBm + 5,2 dB – 3,4 dB – 1 dB = 17,8 dBm

$$10^{\left(\frac{17,8}{10}\right)} = 60,26 \ mW$$

En ole käyttänyt liikaa tehoa, koska maksimi sallittu teho vapaalla 2,4 GHz:n alueella on Suomessa 100 mW eli 20 dB (10, s. 14).

4 Langattoman verkon toteutus monikiinteistökohteessa

4.1 Toteutuksen tavoitteet

Langattoman lähiverkon tavoitteina oli olla helposti ja laajasti saatavilla. Tämän varmistamiseksi käytettävän laitteiston tuli olla helposti mukautettavissa ja skaalattavissa isoihin verkkoihin.

Langattoman verkon käyttöönoton tuli olla suunnitelman mukaista eli helppoa ja vaivatonta. Loppukäyttäjän tuli vain käyttää omaa laitettaan, joka tuki langatonta lähiverkkoliitäntää ja kykeni keskustelemaan TCP/IP-pohjaisessa verkossa.

Käyttöä oli hieman rajoitettu. Langattoman lähiverkon suunnitelmaan kuului pelkästään normaali Internetin selausmahdollisuus, eli porteista 80 ja 443 päästettiin liikenne läpi. VOIP-ratkaisua verkon ei tarvinnut tukea lainkaan.

4.2 Laitteisto

Laitteiston valinnassa otettiin huomioon seuraavia asioita:

- asennuspaikan vaatimukset
- laitteiston takuuaika
- ulkoilmaan tarkoitettujen laitteiden saatavuus
- etähallinnan mahdollisuus.

Suunnitelman toteuttamiseksi tarvittiin tukiasemia, joihin oli saatavilla useampia erilaisia antenneja ja mahdollisuus liittää antenni tukiasemaan myös etäältä. Tämä mahdollistaa tukiaseman sijoittamisen lukittuihin sisätiloihin, jossa se on suojassa säältä ja ilkivallalta.

Tukiasemat

Laitteistoksi valittiin Cisco Systemsin Aironet-sarjan tukiasemia, joiden ominaisuudet katsottiin riittäviksi tämän hetken ja tulevaisuuden verkkoratkaisuihin.

Näiden tukiasemien tuli joko olla kokonaisuudessaan ulkona myös Suomen talvessa tai ainakin antennien tuli sijaita ulkona ja kestää samat olosuhteet. Tämän hetken tukiasemiksi valittiin Cisco Aironet 1240AG sarjan tukiasemat, koska niihin pystyi liittämään erilliset antennit ja tukiasemat kykenivät tarvittaessa toimimaan monessa eri toimintatilassa.

1240AG-sarjan tukiasemat saadaan liitettyä myös langattomien tukiasemien ohjainlaitteeseen, jolloin kaikki asetukset saadaan säädettyä yhdestä paikasta. Tämä seikka tullaan huomioimaan myöhemmin. Näissä tukiasemissa on myös liitännät

802.11a-standardin mukaisiin antenneihin eli 5 GHz:n kantataajuudella toimiviin verkkoihin.

Kuvassa 12 näkyvät käyttöön valitut tukiasemat.Siitä käyvät ilmi niiden antenniliitäntämahdollisuudet 2,4 GHz:n ja 5,0 GHz:n antenneille sekä konsoli- ja lähiverkkoliitäntä.

Kuva 12: Cisco Aironet 1240AG (11)

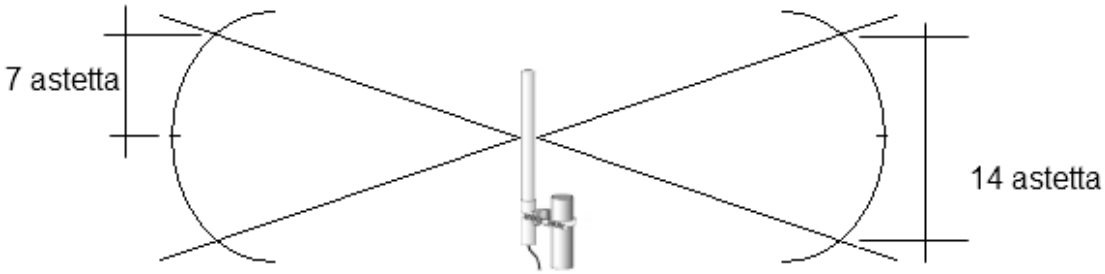
Antennit

Antenneiksi valittiin Cisco Aironet sarjan tukiasemiin yhteensopivat versiot, jotka täyttävät viranomaisten antamat määräykset. Nämä mainitut määreet rajoittivat antennien valmistajaksi ainoastaan Cisco Systemsin.

Antennit ja antennikaapelit ovat Cisco Systemsin valmistamat yhteensopivuuden varmistamiseksi. Antenneiksi valittiin mastokiinnitteiset antennit, jotka ovat pystyakseliinsa nähden ympärisäteileviä ja joiden säteilykeila vaaka-akseliinsa nähden on 14 astetta. Antennikaapelit sitten taas on puolestaan valittu lähimmän sopivan pituuden mukaan ja silloinkin pienimmällä mahdollisella vaimenemisella. Antennien vahvistus on 5,2 dBi (12, taulukko 6 ja 12).

Kuvassa 13 näkyy käyttöön valittu antennimalli ja kuvassa 14 saman antennin säteilykeila.

Kuva 13: Air Ant2506 antennista (13)



Kuva 14: Säteilykeila

Antennikaapelit

Antennikaapeleita valittiin käyttöön kahta eri mittaa, ja kummatkin kaapelit tuli olla mahdollisimman vähän signaalihäviötä aiheuttavia. Koska antennikaapeleiden valmistaja on yhdysvaltalainen, myös niiden mitat on ilmoitettu yhdysvaltalaisittain. Kaapeleiden mitat ovat 50 ja 100 jalkaa. Mitat tulee muuttaa metrijärjestelmään kaavan 3 mukaisesti.

$$l = x \cdot 0{,}3048 \frac{m}{jalkaa} \qquad (3)$$

l on pituus metreissä

x on kerrottavien jalkojen määrä

Muuntokaavan perusteella pystyy kertomaan metrimääräinen pituus antennikaapeleille.

$50 \cdot 0{,}3048$ m = 15,24 m

$100 \cdot 0.3048$ m = 30,48 m

Antennikaapeleille on valmistaja ilmoittanut kokonaisvaimennuksen, joten ei ole tarvetta laskea sitä itse. Kokonaisvaimennus on kuitenkin kaapelinmitasta ja kantataajuus riippuvaisia. Kaapelien tyyppimerkinnät ovat AIR-CAB100ULL-R ja AIR-CAB050LL-R. Vaimenema lyhyemmälle kaapelille on 2,4 GHz:n kantataajuudella 3,4 dB ja pidemmälle kaapelille samalla kantataajuudella 4,4 dB.

LAN-liitokset

Jokainen tukiasema on liitetty langalliseen lähiverkkoon, jotta voidaan varmistaa tukiasemien toimivuus silloinkin, kun yksi tukiasema on väliaikaisesti poissa käytöstä. Langattoman lähiverkon tukiasemat on liitetty OSI-kerroksella 2 toimivaan hallitsemattomaan kytkimeen, josta menee yksi kaapeli valokuitumuuntimeen. Tukiasemat sijaitsevat teknisissä tiloissa, johon ei ole pääsyä sivullisilla, joten ratkaisu oli vähintäänkin hyväksyttävä.

4.3 Laitteiston asennus ja dokumentointi

Langattomiin tukiasemiin asennettiin suunnitelman mukaiset asetukset, jotka sisälsivät täysin avoimen verkkoon liittymisen ja näkyvän SSID:n. Ainoiksi asioiksi, joita piti dokumentoida, olivat laitteiden asetukset, myös ne jotka eivät käyttäjille näy ja, ottaa niistä kopiot tekstitiedostoihin.

Tukiasemien asetuksiin kuuluivat seuraavat asetukset: NTP- ja lokipalvelimet, hallintaosoite, tukiaseman nimi, SSID:n vaihtaminen, alkuperäisten käyttäjätunnusten poisto, uusien käyttäjätunnusten luonti sekä hallintakäyttöön että lokien lukukäyttöön eräänlainen moniantennitekniikan käyttöönotto ja laittaminen liityntäpistetoimintatilaan.

4.4 Mittaaminen ja käyttökokemuksen kerääminen

Koska olosuhteet pakottivat langattoman verkon toteutuksen kahdessa erässä, ensimmäisen osion kanssa oli noin vuosi aikaa hankkia käyttökokemusta langattoman verkon toiminnasta ennen toisen osion asennusta.

Käyttökokemuksen kerääminen

Käyttökokemusten mukaan langattomassa verkossa oli hyvin vähän valittamista koskien saatavuutta tai käyttämistä. Ainoastaan kolme valitusta saapui vuoden testikäytön aikana.

Ensimmäinen valitus johtui sähkökatkoksesta, jossa yksi langaton tukiasema oli mennyt vikatilaan. Kaksi muuta tukiasemaa olivat selviytyneet tilanteesta. Tämän yksittäisen tukiaseman palauttaminen oli helppoa, koska asennusvaiheessa oli otettu valmiit asetustiedot erilliseen tiedostoon, josta ne saattoi helposti ottaa käyttöön.

Toinen tilanne, josta oli tullut valitus langattoman verkon toimimattomuudesta, oli johtunut LAN-verkon puolelta. Yksi rakennusten välisistä kuitumuuntimista oli mennyt rikki.

Kolmas valitus tuli siitä, että aiemmin DHCP-palvelua ja NAT-palvelua pitämä modeemi oli saanut virtapiikin ja mennyt outoon toimintatilaan, jossa NAT ja DHCP olivat pois toiminnasta ja ulkoverkon puolelta oli päässyt suoraan IP-osoitteet sisäverkkoon.

Mittaaminen

Langattoman lähiverkon käyttöönoton jälkeen tehtiin testejä langattomalle lähiverkolle. Kyseiset mittaukset tehtiin yhdellä ohjelmalla, joka on suomalais-yhdysvaltalaisvalmisteinen ilmaisohjelma Ekahau Heat Mapper, joka on langattoman

lähiverkon kattavuuden selvitystyökalu. Heat Mapper kykenee löytämään tukiasemat ja sijoittamaan ne pohjalle, mikäli olet sellaisen luonut. Samalla Heat Mapper etsii seuraavia tietoja tukiasemasta: kanavatiedon, tukiaseman MAC-osoitteen, käytetyn salauksen ja tukiaseman valmistajan mikäli mahdollista.

Heat Mapperin ilmaisversiossa on yksi todella suuri rajoite, maksimimittausaika on 15 minuuttia. Annettu aika on todella lyhyt, jos mitattava alue on laaja. Käytännössä tämä tarkoittaa sitä, että viidentoista minuutin kuluttua ohjelma alkaa poistaa ensimmäisiä mittaustuloksia.

Heat Mapperilla kerättiin tietoa rakennuksista ja niiden lähiympäristöstä. Tiedot saatiin valmiina kuvamuotoon, joten jatkokäsittelyltä vältyttiin. Ekahau Heat Mapper osaa antaa kuuluvuusalueet eri väreillä koodattuina karttapohjalle.

Heat Mapperin aikarajoite pakotti tekemään mittaukset useammassa osassa, jotka oli rajattu seuraavasti:

- pienemmän rakennuksen yläkerta
- pienemmän rakennuksen alakerta ja lähiympäristö
- suuremman rakennuksen yläkerta
- suuremman rakennuksen alakerta ja lähiympäristö.

Heat Mapperilla tehdyistä mittauksista on kuvia liitteessä 2.

5 Langattoman verkon yhtenäistäminen monikiinteistökohteessa

5.1 Yhtenäistämisen suunnitelma

Koska kohde-alue on varsin laaja, ja monissa eri kiinteistöissä tarvitaan samanlaisia palveluita, tulisi alueiden laitteistojen olla täysin samankaltaiset. Kyseessä on koko verkon kattava yhtenäistäminen, jotta langaton lähiverkko saisi paremman saatavuuden ja luotettavuuden kaikkien tämän asiakkaan kiinteistöjen alueella.

Nykyinen fyysinen infrastruktuuri on rakennettu siten, että langaton verkko on tarjottu ainoastaan asiakkaille ja langallinen verkko ainoastaan henkilökunnan käyttöön. Verkot on erotettu toisistaan myös OSI-kerroksella 1. Ongelmaksi muodostuu se, että jokaiseen rakennukseen tulee viedä vähintään kahdet valokuitukaapelit ja jokaiselle valokuitukaapeliparille omat kuitumuuntimet.

Ongelmasta voidaan muodostaa myös koko verkkoinfrastruktuurin vahvuus asentamalla OSI-kerroksilla 2 ja 3 toimivia aktiivilaitteita, jotka asetetaan toimimaan HSRP-tilaan. Käytännössä tämä tarkoittaa sitä, että molemmat rakennuksiin tulevat valokuituparit otetaan käyttöön samaan fyysiseen verkkoon ja vain toista käytetään aktiivisesti. Toinen valokuitupareista olisi silloin passiivisena odottamassa aktiivisen parin rikkoutumista tai muuta toimintaan liittyvää häiriötä ja tulisi silloin itse aktiiviseen tilaan.

Tietoturvan varmentamiseksi otetaan käyttöön VLANit, joita tarvitaan kuusi erillistä kappaletta, joista yksikään ei ole oletus-VLAN numero yksi. Oletus-VLANin vaihtaminen ykkösestä joksikin toiseksi, estää omien luvattomien aktiivilaitteiden hyödyntämisen tässä tietoliikenneverkossa.

5.2 Nykyiset laitteet muissa kiinteistöissä

Tämän hetken laitteistot muissa tiloissa on hankittu aina kahdella asiakasyrityksen määrittelemällä kriteerillä: kustannustehokkuudella kyseisessä tilanteessa ja mahdollisuudella hankkia samaa tai vastaavaa tavaraa pitkänkin ajan kuluessa.

Edellä mainitut kriteerit ovat aiheuttaneet sen, että jokaisessa kiinteistössä on asennettu tilausajankohdan mukaista ”hyllytavaraa”. Muutenkin aiemmin tilatut langattoman lähiverkon tukiasemat ovat olleet pientoimistokäyttöön tarkoitettuja laitteita, jolloin niissä on ollut heikkouksia esimerkiksi liitettävien laitteiden lukumääräisessä tuessa tai langattoman verkon tehon säädettävyydessä.

SOHO-laitteiden käyttö ei sinällään ole ollut paha ratkaisu aikanaan, mutta nykyään asiakasyrityksessä on paljon enemmän tarvetta langattomalle verkolle. Langattoman lähiverkon kasvun voi selittää sillä, että langatonta verkkoa käyttävien laitteiden määrä on lisääntynyt vuosi vuodelta laitehintojen laskiessa alemmas.

5.3 Laitteiston yhtenäistämisen tarkoitus

Tietoturvan parantamisen keinoiksi otetut VLAN:it on tarkoitus hyödyntää myös useammilla keinoilla. Yhdeksi keinoksi voidaan mainita VLAN-kohtaiset QoS- ja CoS-säännöstöt ja jokaisen VLAN:n omat yhteysoikeutensa riippuen käyttäjäntodentamisesta.

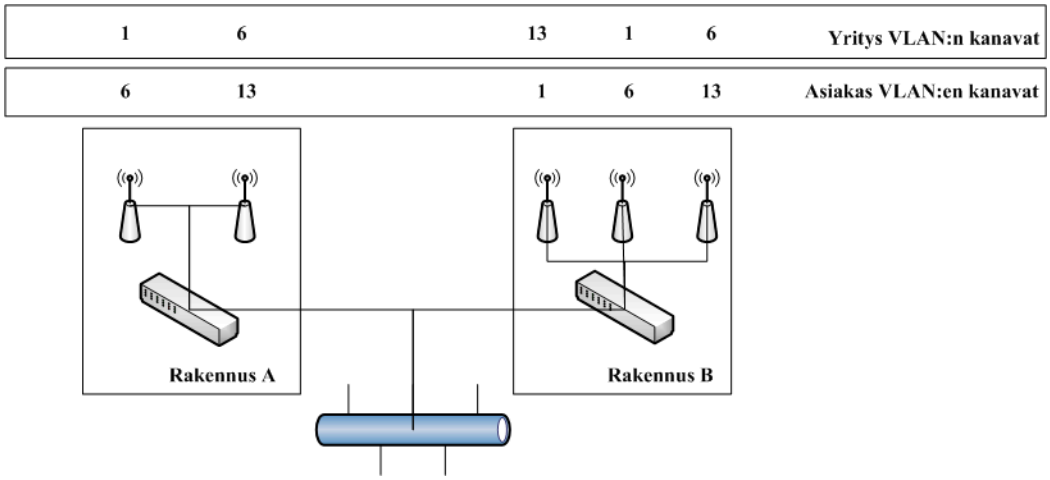
VLAN

Virtuaali-LAN:t ovat IEEE 802.1q-standardin määrittelemä keino jakaa käyttäjiä loogisiin ryhmiin lähiverkossa, eli tietoturva tapahtuu jo aktiivilaitteissa ja voidaan käyttää yhtä aktiivilaitetta useamman sijaan. VLAN:n tietoturva tapahtuu siten, että Tiettyyn ryhmään kuuluva käyttäjä ei pysty näkemään toiseen ryhmään kuluvan käyttäjän verkkoliikennettä, vaikka haluaisi.

VLAN toimii jo OSI-kerroksella 2 eli siirtokerroksella. Näin ollen verkkoliikenteen jako tapahtuu jo varhaisessa vaiheessa ja se voidaan toteuttaa OSI-kerroksella 2 toimivilla laitteilla eli kytkimillä. Tosin jos lähiverkon halutaan ymmärtävän VLAN:n suomia etuja, tulee verkossa olla OSI-kerroksella 3 toimivia laitteita jaottelemassa liikennettä.

Langattoman lähiverkon kohdalla tulee ottaa huomioon seuraava asia. Langaton tukiasema toimii langattoman verkon puolella OSI-kerroksella 2 ja ilmatie itse OSI-kerroksella 1, mistä muodostuu rajoite. Rajoite voidaan kuitenkin kiertää siten, että jaetaan samalla tukiasemalla useampaa eri SSID-verkkoa, ja nämä SSID-verkot olisi jaettu omiin VLAN: nsa. Tähän työhön valitut langattomat tukiasemat kykenevät erottelemaan useita VLAN:ja ja jakamaan samanaikaisesti useampaa SSID-verkkoa.

Kuvassa 15 on nähtävänä esimerkki useamman VLAN:n jakamisesta tukiasemilla. Kuvasta näkyy selvästi, että samoilla tukiasemilla ei ole kahdesti samaa kanavaa eri VLAN:lle. Sekä asiakas, että Yritys VLAN:t jaetaan eri SSID-tunnuksilla olevilla verkoilla.



Kuva 15: Kanavasijoittelu tukiasemilla

VLAN numero 1 on oletus-VLAN jokaisessa OSI-kerroksen 2 laitteissa eikä sitä tule käyttää missään käyttötarkoituksessa tietoturvan takia. Näin ollen VLAN 1 otetaan kokonaan pois käytöstä ja oletus-VLAN:ksi asetetaan VLAN 5. Näin vältetään tilanne, jossa loppukäyttäjä pystyisi lisäämään verkkoon omia kytkimiään, langattomia tukiasemiaan tai toistimiaan luvatta.

VLAN numero 10 annettaisiin todentamatta asiakaskäyttöön, VLAN 10:stä on pelkästään pääsy Internetiin. Kuitenkin tämäkin yhteys kävisi seuraavat toimenpiteet läpi: TCP/IP-palveluista päästettäisiin läpi vain http, https, smtp, ja QoS mahdollistaisi maksimillaan 384 kbps:n yhteyden verkosta ulos.

VLAN numero 20 annettaisiin todennetuille asiakkaille. Todennus pohjautuu 802.1x-standardin mukaiseen RADIUS-todennusmenetelmään. Asiakkaat saavat samat palvelut kuin todentamatta, mutta QoS mahdollistaisi suuremmat nopeudet Internetiin, kuitenkin maksimissaan 2 Mbps.

VLAN numero 30 annettaisiin todentamista vastaan henkilökunnan käyttöön. Tästäkin verkosta on yhteys Internetiin, mutta QoS ei rajoittaisi lainkaan internet-nopeuksia, vaan siirtäisi tämän yhteyden etuoikeutettuun tilaan. Tämä todentaminen toteutettaisiin radius-todentamisen avulla. Tämän VLAN:n radius-todentaminen olisi toteutettu Kerberoksen ja aktiivihakemiston avulla.

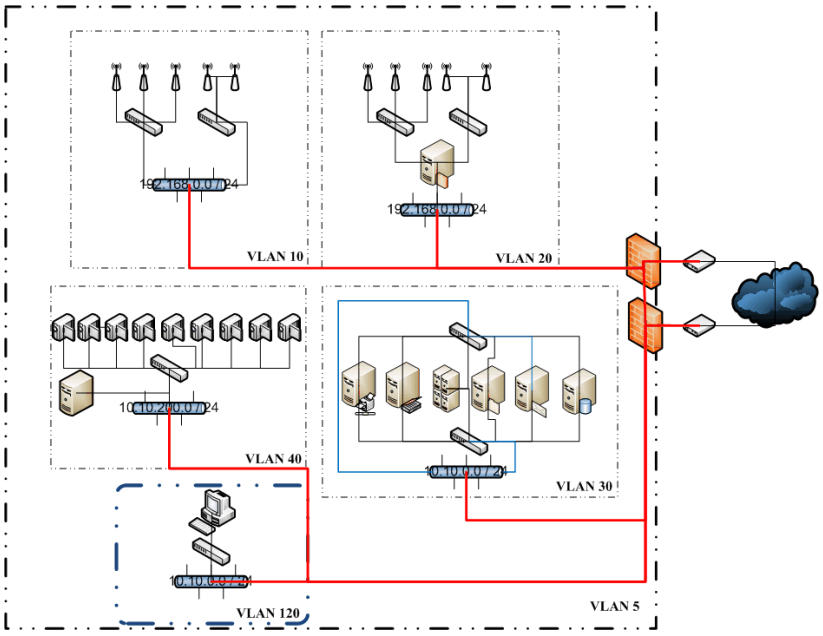
Aktiivihakemiston todentamisen onnistumiseen RADIUSin kautta tarvittaisiin toteutukseen Microsoft Windows Server palvelin, jossa on käyttöönotettuna aktiivihakemisto ja radiuspalvelut. Tämä mahdollistaa sen, että kirjautuessasi toimialueeseen liitettyyn tietokoneeseen, tietokone automaattisesti todentaa Kerberospalvelimelle, jonka säännöstöissä on kerrottu verkkoon liittymiseen tarvittavat tiedot.

VLAN numero 40 olisi puhtaasti kiinteistökäytössä, eli tässä VLAN:ssa toimisivat kameravalvonta- ja oviohjausjärjestelmät ilman muiden laitteiden läsnäoloa tai häirintää. Jotta tämä verkko toimisi normaalisti, verkolle annettaisiin sisäverkon osalta suurin etuoikeus QoS:n puolelta.

VLAN numero 120 annettaisiin pelkästään hallinnointikäyttöön. Verkossa pyörisivät aktiivilaitteiden lokien kerääminen ja muu aktiivilaitteiden hallintaan kuuluvat asiat. Aktiivilaitteiden hallinta annetaan pelkästään verkossa VLAN 120 tapahtuvaksi tai aktiivilaitteen omaan konsoliliitäntään.

VLAN 10 ja 20 tulevat jakamaan saman IP-osoiteavaruuden, jota jakaa jokin aktiivilaite. VLAN 30 saa oman IP-osoiteavaruuden, jota jakaa aktiivihakemistoon liitetty palvelin, jolloin tässä verkossa ei voi olla luvattomia DHCP-palveluita. VLAN 40 tulee jakamaan jälleen omaa IP-osoitealuettaan, tarvittaessa voidaan jokaiselle päätelaitteelle asentaa kiinteät IP-osoitteet.

VLAN 120 saa oman alueensa, jota mahdollisesti jakaa WLAN Controller tai muu siihen kykenevä laite. Kuvassa 16 näkyy VLAN:en loogisesta käytöstä. Kuvasta on isompi versio liitteessä 3.



Kuva 16: VLAN:en looginen kaavio

6 Yhteenveto

Työn tarkoituksena oli konsultoida, suunnitella ja toteuttaa kahden kiinteistön kattava yhtenäinen langaton lähiverkko, testata lähiverkon toimivuutta huoneistoissa molemmissa kerroksissa ja eri antennien alueilla. Langattoman lähiverkon saatavuutta pyrittiin parantamaan asentamalla useampia antenneja päällekkäin kantavuusalueille.

Laskenta ja mittaukset tukivat toisiaan, minkä seurauksen jokaisessa huoneistossa on toimiva langaton lähiverkko.

Ongelmilta tämän työn osalta on tähän mennessä vältytty, lukuun ottamatta pientä asennusongelmaa, mutta ne eivät olleet allekirjoittaneen vastuualueella alkujaankaan. Vuoden mittaisen testikäytön aikana todettiin vain kolme pientä ongelmaa, joista yksikään ei varsinaisesti johtunut suunnittelusta tai toteutuksesta.

Lähteet

1 Roaming and WLAN. (WWW-dokumentti.) Mind Commerce. <http://www.mobilein.com/Perspectives/Authors/zagaWLANRoaming.htm>. Päivitetty 2004. Luettu 12.3.2010.

2 A Technical Tutorial on the IEEE 802.11 Protocol. (WWW-dokumentti.) Breezecom. <http://sss-mag.com/pdf/802_11tut.pdf>. Päivitetty 1997. Luettu 29.3.2010.

3 Puska, Matti. Langattomat lähiverkot. Helsinki: Talentum, 2005.

4 Shaikh, Kamil Mohiuddin. The Performance Evaluation of OFDM Based WLAN (IEEE 802.11a and 802.11g). Dipl. insinöörityö. Blekinge Tekniska Högskola, 2009.

5 Pulkkinen, Jaakko. WLAN 802.11n -standardin suorituskyky. Insinöörityö. Metropolia Ammattikorkeakolulu, 2009.

6 802.11n: The Next Generation of Wireless Performance (WWW-dokumentti.) Cisco Systems. <http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7_ns767_Networking_Solutions_White_Paper.html>. Päivitetty 2010. Luettu 12.3.2010.

7 Kuva WEP-salauksesta (WWW-dokumentti.) blogspot.com. <http://2.bp.blogspot.com/_ifJKmmFgY9k/Su4isDwhdQI/AAAAAAAAAF0/Ua0lvTwz4X8/s400/wep.jpg>. Luettu 12.3.2010.

8 EAPoW. (WWW-dokumentti.) Vocal technologies LTD. <http://www.vocal.com/security/eapow.html>. Päivitetty 2009. Luettu 12.3.2010.

9 Cisco Aironet 1240AG Series 802.11A/B/G Access Point Data Sheet. (WWW-dokumentti.) Cisco Systems. <http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.html>. Luettu 12.3.2010.

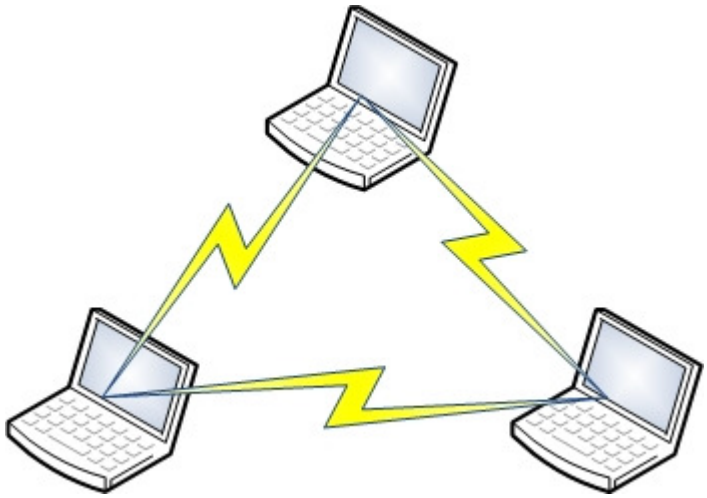
10 Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. Viestintävirasto. Helsinki: 2008.

11 Kuva tukiasemasta. (WWW-dokumentti.) ecrater.com. <http://s.ecrater.com/stores/81517/48e662344647f_81517n.jpg>. Luettu 4.10.2009.

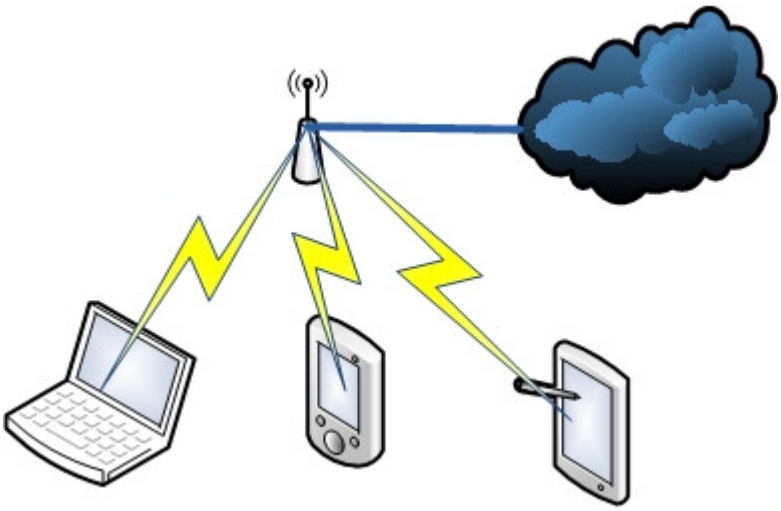
12 Cisco Aironet Antennas and Accessories Reference Guide. (WWW-dokumentti.) Cisco Systems. <http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html>. Luettu 7.10.2010.

13 Kuva antennista. (WWW-dokumentti.) Cisco Systems. <http://www.cisco.com/web/JP/images/product/hs/wireless/airoa/prodlit/ccmigration_09186a008008883b_09186a008069dd97-110.jpg>. Luettu 4.10.2009.

Liite 1: Kuvat langattoman lähiverkon toimintamalleista



Kuvassa nähdään ad-hoc-toimintatilan malli, eli tietokoneet voivat keskustella langattomasti suoraan keskenään.



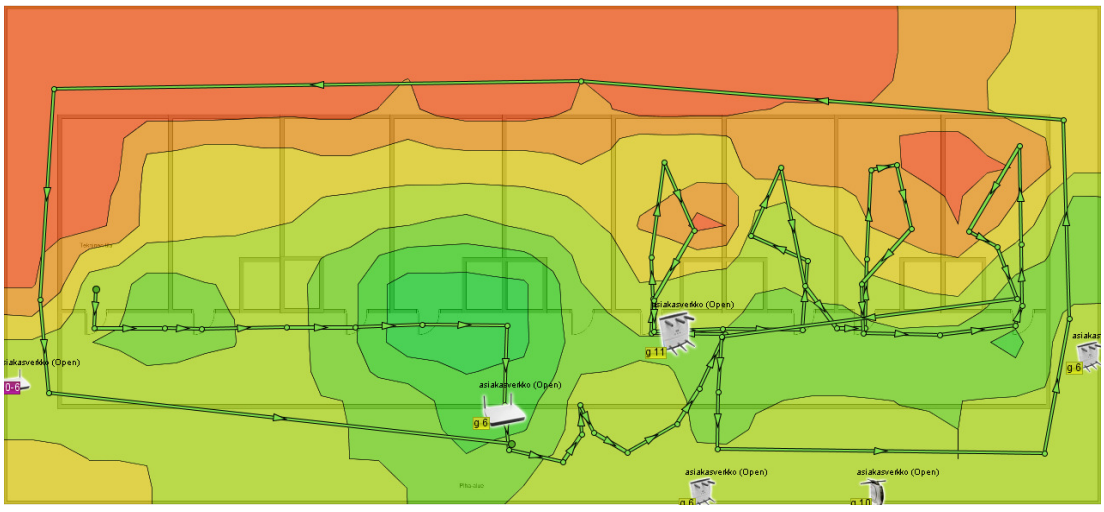
Kuvassa näkyy infrastruktuuritoimintatilan malli. Tämä on yleisin toimintamalli langattomissa lähiverkoissa, eli langaton tukiasema yhdistää päätelaitteet Internetiin.

Liite 2: Heat Mapperilla saatuja mittaustuloksia kuvina ja värien selvitys

värien selitys:

tummanvihreä:		-56...-48 dBm
vihreä:		-64...-56 dBm
keltainen:		-72...-64 dBm
oranssi:	-	-80...-72 dBm
punainen:		-88...-80 dBm
tummanpunainen:		-90...-88 dBm

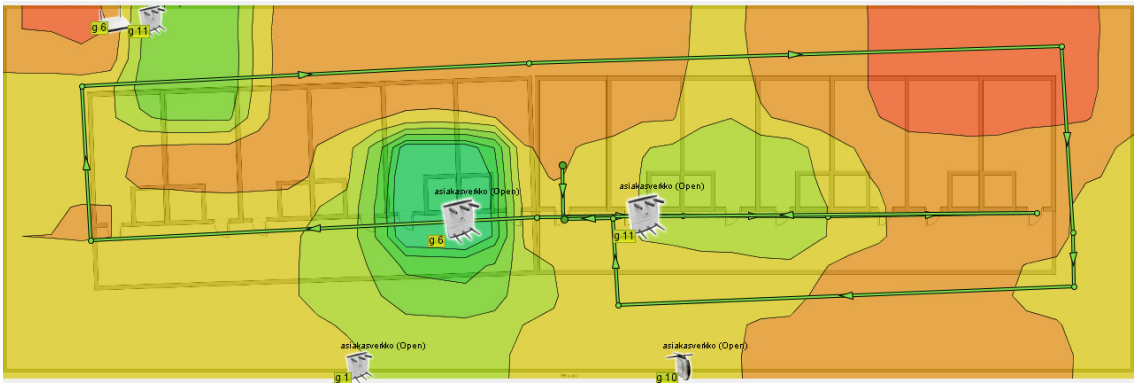
Pienemmän rakennuksen yläkerta



Pienemmän rakennuksen alakerta

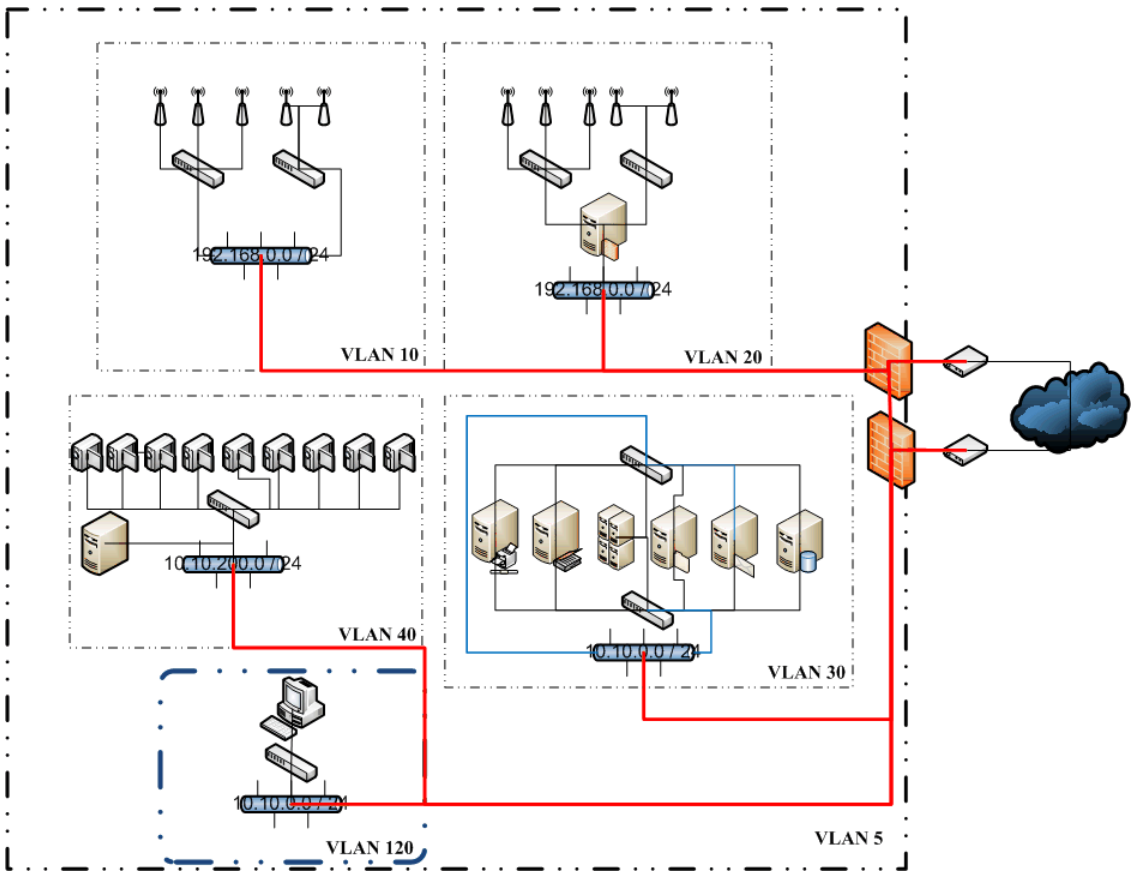
Liite 2: Heat Mapperilla saatuja mittaustuloksia kuvina ja värien selvitys

Isomman rakennuksen yläkerta. Huoneistot olivat käytössä eikä niihin päässyt käymään mittaushetkellä.



Isomman rakennuksen alakerta. Rakennuksen huoneistot olivat käytössä eikä niihin päässyt mittaamaan.

Liite 3: Käytettävien VLAN:en kartta



Kuten kuvasta näkee, siirto-VLAN:na toimiva VLAN 5 ei ylety palomuurin ja modeemin väliselle alueelle, vaan pysyy LAN-alueella.

Liite 4: Laitteiden saatavuussuunnitelma

Asiakkaalla:

1. Tukiasemat sijaitsevat fyysisesti lukitussa tilassa, jonne on elektroninen pääsynvalvonta.
2. Tukiasemat ja niiden välittömässä läheisyydessä olevat kytkimet ja kuitumuuntimet ovat varmistettu katkeamattomalla virransyötöllä.
3. Tukiasemien hallintasalasanat on vaihdettu ja oletuskäyttäjätilit on poistettu.
4. Hallintatunnuksia ei ole luovutettu asiakkaalle.
5. Antennit on sijoitettu siten, että sinne ei ole pääsyä ilman työtasoja.
6. Tukiasemista on otettu asetukset talteen erillisiin tekstitiedostoihin, jotka on nimetty tukiasemien mukaan.
7. Tekstitiedostot sijaitsevat lukitussa palvelinhuoneessa palvelimilla, joissa on sekä RAID 5-, että nauhavarmistus.
8. Tiedostoihin pääsee ainoastaan järjestelmänvalvojan tunnuksin.
9. Järjestelmänvalvojan tunnuksia ei ole asiakkaille myönnetty.

Päämajalla:

1. Tekstitiedostoista on kopiot myös meidän tiedostopalvelimella, jotka on myös RAID5- ja nauhavarmennettu.
2. Tekstitiedostot on myös tulostettu ja tulosteet säilytetään päämajassamme, lukitussa datakaapissa, yli 10 km:n päässä asiakkaasta

Liite 5: Tukiaseman asetukset

Yksilöiviä asetuksia on muokattu tietoturvariskin minimoimiseksi. Lähetystehojen hienosäätö on tehty graafisesti. Muokkaukset on merkattu punaisella.

ka**Muokattu**ne#sh run
Building configuration...

Current configuration : 3397 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ka**Muokattu**ne
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
ip domain name ki**Muokattu**io.fi
!
!
!
dot11 ssid asiakasverkko
  authentication open

Liite 5: Tukiaseman asetukset

```
   guest-mode
!
power inline negotiation prestandard source
!
crypto pki trustpoint TP-self-signed-1888866376
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1888866376
 revocation-check none
 rsakeypair TP-self-signed-1888866376
!
!
crypto pki certificate chain TP-self-signed-1888866376
 certificate self-signed 01
  30820252 308201BB A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
                                **Muokattu**
  B99ED25B C3367C49 3C394C0D 53CB2517 032C69A8 4D288753 20AA9468
B8E2931B
  372C222F C0E2B7F3 9C6019FC 2B79F0AE B159F5E8 2A32899D 82D32B14
C92AB4AD
  4DD70203 010001A3 7A307830 0F060355 1D130101 FF040530 030101FF
30250603
                                **Muokattu**
  6BB18E7C 274A98F2 871BA65D BAA778BC 75C63004 4BFDC9A2 9D9DF912
88A5780C
  7E15F10C 58A5107E B17B7506 61CC2F9F E082D256 0193E5DE A91EF299
ED36D7A3
  F4B30597 433C7A46 833FBFEB CE7F8034 54B611BF 51BF
```

Liite 5: Tukiaseman asetukset

```
 quit
username Luku password 7 1531021F0725
username admin privilege 15 password 7 112248361E47
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid asiakasverkko
 !
 speed  basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel 2412
 station-role root
 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 Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 no dfs band block
 channel dfs
 station-role root
```

Liite 5: Tukiaseman asetukset

```
 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
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address **Muokattu** 255.255.255.0
 no ip route-cache
!
ip default-gateway **Muokattu**
ip http server
ip http authentication aaa
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
bridge 1 route ip
!
!
!
line con 0
```

Liite 5: Tukiaseman asetukset

line vty 5 15

!

end

ka**Muokattu**ne#