

VAASAN AMMATTIKORKEAKOULU

Joni Ranta-Eskola

WLANIN RAKENTAMINEN

Liiketalous ja matkailu
2003

ALKUSANAT

Tämä opinnäytetyö on suoritettu Vaasan ammattikorkeakoulussa tietojenkäsittelyn koulutusohjelmassa. Työ on ollut osa Vaasan ammattikorkeakoulun WLAN-projektia. Kiitän projektissa mukana olleita henkilöitä sekä opinnäytetyöni ohjajaa Antti Mäkitaloa.

Vaasassa 04.12.2003

Joni Ranta-Eskola

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Joni Ranta-Eskola
Opinnäytetyön nimi	WLANin rakentaminen
Vuosi	2003
Kieli	Suomi
Sivumäärä	62
Ohjaaja	Antti Mäkitalo

Opinnäytetyön tarkoituksena on ollut tutustua langattoman lähiverkon rakentamiseen ja suunnitteluun. Työssä pyrittiin löytämään ratkaisut tutkimusongelmiin, joita olivat WLAN-verkon edut kaapeliverkkoon nähden sekä langattoman verkon tietoturva.

Tutkimuksessa on käytetty lähdeaineina alan kirjallisuutta, Internet-julkaisuja sekä aiheeseen liittyviä lehtiartikkeleita. Työssä tutustuttiin aiheeseen käytännössä, kun Vaasan ammattikorkeakouluun rakennettiin WLAN-verkko.

Työn tuloksena selvisivät WLAN-verkon tietoturvan toteuttaminen sekä langattomuuden mukanaan tuomat edut. Teorian lisäksi työstä ilmenee esimerkki käytännön toteutuksesta.

Asiasanat WLAN, Langaton lähiverkko

VAASAN POLYTECHNIC

Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Joni Ranta-Eskola
Name of thesis	Building a WLAN
Year	2003
Language	Finnish
Number of pages	62
Instructor	Antti Mäkitalo

This thesis focuses on examining the structure and design of a wireless network.

Main target areas have been to find out solutions for research problems, which were the benefits of a WLAN compared to a cable network, and also the security of a wireless network.

In this study I have used WLAN literature and articles found from the Internet and technical publications. The practical point of view was found when WLAN network was built to Vaasa Polytechnic.

With this work we were able to find out the benefits arrived to with the use of WLAN. Both the theoretical and the practical point of view can be found from the realization of this work.

Keywords WLAN, Wireless Local Area Network

SISÄLLYS

ALKUSANAT	2
TIIVISTELMÄ	3
ABSTRACT	4
SISÄLLYS	5
KUVAT	8
1. JOHDANTO	9
2. TUTKIMUSONGELMAT	10
3. MIKÄ ON WLAN?	11
3.1 Ennakkokäsitykset ja yleinen mielipide langattomasta lähiverkosta	11
3.2 Määrittely	11
3.3 WLAN-verkon edut	12
3.4 WLAN-verkon haittapuolia	13
3.4.1 Radiosignaalista johtuvat ongelmat	13
3.4.2 Signaalin fyysiset esteet	14
3.4.3 Virran kulutus ja kaapelointi	14
3.4.4 Yhteensopivuusongelmat	15
3.5 Standardit	15
3.5.1 Standardi 802.11b	16
3.5.2 Standardi 802.11a	16
3.5.3 Standardit 802.11h ja 802.11d	17
3.5.4 Standardi 802.11g	18
3.5.5 Standardi 802.11i	18
3.5.6 Standardit 802.11e ja 802.11f	18
4. WLAN-VERKKOJEN RAKENNE	20

4.1 Roaming	21
4.2 Osi-malli.....	23
4.3 Topologiat	24
4.3.1 IBSS-verkko	24
4.3.2 Infrastruktuuriverkko BSS	25
4.3.3 Infrastruktuuriverkko ESS	25
4.4 Kanavien varaaminen.....	27
4.4.1 Kanavat AdHoc- ja BSS-verkoissa	28
4.4.2 Kanavat ESS-verkoissa	28
4.4.3 Tiedonsiirto	28
5. WLAN-VERKON SUUNNITTELU	30
5.1 Taustatietoa	30
5.2 Asennusympäristön tutkiminen.....	30
5.3 Antennien valinta	31
5.4 Tukiasemien sijoittelu	31
5.5 Tukiasemien kanavien valinta.....	34
5.5.1 Ympäristön muutokset	35
5.6 Dokumentointi.....	35
6. WLAN-VERKON TIETOTURVA	37
6.1 Langattoman lähiverkon keskeisiä tietoturva-aukkoja.....	37
6.2 Keskeisimmät suojauskeinot.....	38
6.3 Verkon suojaus.....	39
6.4 WEP (Wired Equivalent Privacy)	39
6.5 Autentikointi	41
6.6 Standardi 802.1x	41
6.7 Autentikointipalvelimet.....	41
6.8 WPA	42
6.9 Standardi 802.11i	43
6.10 VPN.....	44

7. WLAN-PROJEKTI VAASAN AMMATTIKORKEAKOULUSSA	45
7.1 Hankkeen taustaa	45
7.2 Hankkeen merkitys alueellisen innovaatiojärjestelmän edistämisessä	45
7.3 Hankkeen toteuttaminen korkeakoulujen yhteistyönä	45
7.4 Mitä hyötyä WLAN-verkko tuo?	46
7.5 Hankkeen aloittaminen.....	46
7.6 Asennukset	47
7.6.1 Tukiasemien sijoittelu	48
7.7 Kuuluvuusmittaukset.....	51
7.8 Tukiasemien kanavointi	52
7.8.1 Kanavien konfigurointi tukiasemiin.....	53
7.9 Tietoturva Vaasan AMK:ssa	54
7.9.1 Oasis.....	54
7.9.2 Tino (This is not oasis).....	55
7.9.2 WLAN yhteyden avaaminen.....	56
7.9.3 VPN.....	56
7.10 Valmis WLAN-verkko.....	57
7.11 WLAN – onnistunut projekti?.....	58
8. YHTEENVETO	59
LÄHTEET	61

KUVAT

Kuva 1. WLAN-verkon tuomia etuja ulkotiloissa.	13
Kuva 2. WLAN-standardit ja niiden tärkeimmät ominaisuudet.	19
Kuva 3. GSM-verkko (Seppänen).....	20
Kuva 4. WLAN-verkko (Seppänen).	21
Kuva 5. Roamingin aiheuttama ongelma.	22
Kuva 6. WLAN OSI-mallin erot verrattuna muihin vastaaviin (Seppänen).....	23
Kuva 7. IBSS/AdHoc-verkko (Seppänen).	24
Kuva 8. Infrastruktuuriverkko, BSS (Seppänen).	26
Kuva 9. Infrastruktuuriverkko, ESS (Seppänen).....	26
Kuva 10. Spektrin periaatekuva, kanavat 1,7 ja 13 (Seppänen).....	27
Kuva 11. Spektrin periaatekuva, kanavat 1,5,9 ja 13 (Seppänen).....	27
Kuva 12. D-link DWL-900 AP+ -tukiasema.	48
Kuva 13. Linksysin WAP54G –tukiasema.	48
Kuva 14. Tukiasema kattorakenteiden yläpuolella.	49
Kuva 15. Tukiasema lampun kuvun sisällä.....	49
Kuva 16 Orinocon WLAN-kortti.....	50
Kuva 17. Netstumbler-ohjelmanäkymä.	52
Kuva 18. Karkea 3-ulotteinen malli koulusta ja tukiasemista.....	53
Kuva 19. D-linkin hallintaohjelma.....	54
Kuva 20. Tinon toiminta.	56
Kuva 21. Vaasan kampus-alueen WLAN-verkko.....	57

1. JOHDANTO

WLAN (Wireless Local Area Network) tarkoittaa langatonta lähiverkkoa. Siinä tietoliikenne kulkee normaalin kaapeloinnin sijasta radiotaajuuksia käyttämällä. Langattomalla lähiverkolla on omat etunsa sekä myös haittansa verrattuna normaaliin langalliseen verkkoon.

Tärkein langattomuuteen liittyvä etu on mahdollisuus liikkua ilman katkoksia lähiverkon alueella. Langattomuus vähentää myös kustannuksia, kun kuparikaapeloinnista voidaan luopua. Samalla helpottuu tietoliikenneyhteyksien saaminen paikkoihin, joihin maantieteellisten tai esteettisten syiden takia tämä on ollut aikaisemmin mahdotonta.

WLAN-verkkoon kuuluvat keskeisesti erilaiset standardit. Yleisin standardi on 802.11b, joka määrittelee käytettävän taajuusalueen (2,4GHz) sekä tiedonsiirtonopeuden (11Mbps). Työssä esitellään myös muut standardit erilaisine ominaisuuksineen. Lisäksi käydään läpi langattoman lähiverkon suunnittelun eri vaiheita.

Opinnäytetyössäni selvitän, kuinka WLAN-verkko tulisi suojata. Ensimmäinen suojaustoimenpide on verkon piilottaminen estämällä verkkotunnusten lähettäminen tukiasemilta. Kovennetulla WEP-salauksella saadaan usein jo tarvittava tietoturva. VPN-tekniikalla ja autentikointipalvelimella päästään jo huipputurvalliseen suojauksen tasoon.

Työssä käsitellään langattoman lähiverkon ja sen suunnittelun teorian lisäksi myös WLAN-verkon käytännön toteutusta. Kesällä 2003 Vaasan ammattikorkeakoululle rakennettiin langaton lähiverkko. Työssäni käyn läpi projektin eri vaiheet sekä tekniset ratkaisut.

2. TUTKIMUSONGELMAT

Mitä sellaista WLAN-verkko tarjoaa, jota kaapeliverkko ei kykene tarjoamaan? Yksi opinnäytetyöni tutkimusongelmista oli selvittää ne edut, joita WLAN-verkko voi tarjota. Tavoitteena oli tutkia, missä tilanteissa WLAN-verkko on kannattavampi ratkaisu kuin kaapeliverkko.

Miten WLAN:ssa toteutetaan tietoturva? Toinen opinnäytetyöni tutkimusongelmista liittyi WLAN-verkon tietoturvaan. Työssä tuli selvittää, voidaanko WLAN:n tietoturva saada kaapeliverkon tietoturvan veroiseksi. Tavoitteena oli tuoda esiin ne keinot, joilla langattoman verkon suojausta voidaan parantaa.

3. MIKÄ ON WLAN?

3.1 Ennakkokäsitykset ja yleinen mielipide langattomasta lähiverkosta

Matkapuhelin on ollut ensimmäinen langattomuutta hyväksikäyttävä laite, joka näkyy jokapäiväisessä elämässä. Matkapuhelimen myötä on tullut ihmisille ajatus langattomuuden tuomasta vapaudesta ja helppoudesta.

Langatonta lähiverkkoa pidetään helppona rakentaa, koska kaapelointia ei tarvitse suorittaa. WLAN-verkossa tieto lähetetään ja vastaanotetaan langattomasti. Tästä johtuen ajatellaan, että tietoturva ei voi olla kovin hyvä. Pystytäänhän GSM-puheluitakin kuuntelemaan. Langattomuuden johdosta myös verkkoyhteyden toimintavarmuutta saatetaan epäillä. Valmistajan ilmoittamiin tiedonsiirtonopeuksiin ei arvella langattomilla yhteyksillä päästävän yhtä tehokkaasti kuin kaapeloidulla verkolla. Langattomien verkkotuotteiden hintojen arvellaan olevan korkeammalla kuin normaalien.

3.2 Määrittely

Langattomassa lähiverkossa (Wireless Local Area Network, WLAN), tietoliikenne kulkee perinteisen kuparikaapeloinnin sijasta radioaaltoja hyväksikäyttäen. WLAN-verkko voidaan rakentaa esimerkiksi paikkaan, johon normaalin langallisen verkon rakentaminen ei ole järkevää. Tällaisia paikkoja voisivat olla historiallisesti tärkeät paikat, laajat ulkoalueet tai messuhallit. Kustannukset ovat kohtuullisen edulliset, koska runkoverkon lisäksi ei tarvita muuta kuin tukiasemia, joilla verkon kattavuus luodaan. Päätelaitteessa täytyy olla langaton verkkokortti (WLAN-kortti) sekä käyttöjärjestelmä, joka tukee korttia.

IEEE 802.11 WLAN -laitteet täyttävät Federal Communications Commissions (FCC) määräykset 2.4GHz:n ISM -kaistan (Industrial, Scientific ja Medical) käytöstä. Tämän taajuuskaistan käyttöön ei tarvita erikseen lisenssiä. (Seppänen)

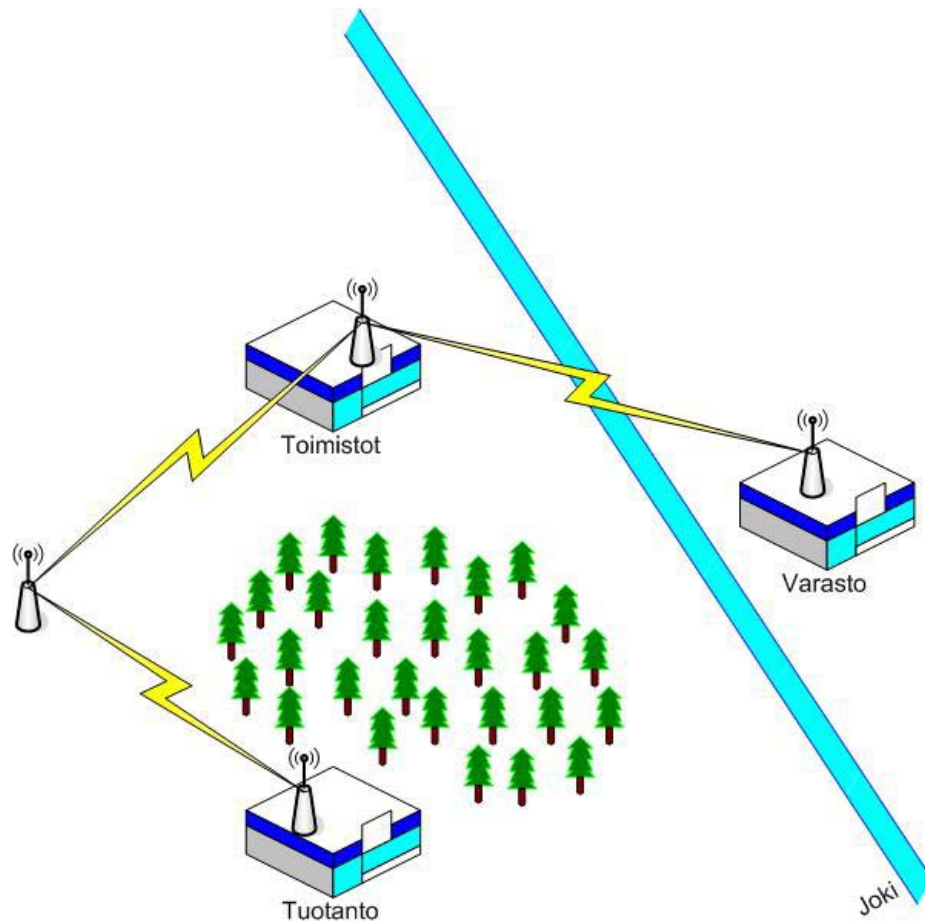
3.3 WLAN-verkon edut

WLAN on viime vuosina kasvattanut suosiotaan kiihtyvällä vauhdilla. Alkuaikoina kasvun esteenä on saattanut olla pelko siitä, ettei WLAN-ratkaisu pysty tarjoamaan tarpeeksi laadukasta tietoturva. Myös tiedon siirron luotettavuutta on saatettu epäillä.

Langattomuus tuo mahdollisuuksia, joita kaapeliverkko ei kykene tarjoamaan. Ehkä tärkein niistä on mahdollisuus liikkuvuuteen ilman yhteydessä tapahtuvia katkoksia. langattoman verkon kuuluvuusalueella. Kun joku verkon käyttäjä tekee palvelimelle muutoksia, ovat uudet päivitettyt tiedot kaikkien verkon käyttäjien nähtävissä välittömästi. Tämä avaa uusia mahdollisuuksia mm. sairaanhoitoalalla ja kaupoissa. Esimerkiksi sairaalassa lääkäri voi ottaa kämmenmikron mukaansa kierrokselle. Potilaan mahdolliset lääkityksen tai tilan muutokset ovat koko hoitohenkilökunnan saatavilla heti, eikä tietoja tarvitse odottaa siihen saakka, kun lääkäri palaa kierrokseltaan. Kaupassa hinnoittelija syöttää kämmentietokoneeseensa uudet hinnat. Kun uusi hintalappu on vaihdettu, tietokantaan tehdyt muutokset ovat heti kassoilla havaittavissa. (Huopalainen ym. 2001; Geier 1999: 8,14)

Toteuttamalla WLAN-verkko voidaan vähentää verkon rakentamisesta johtuvia kustannuksia tuntuvasti. Runkoverkon ja virransyötön lisäksi ei tarvita muuta kuin tukiasemia sekä vastaanottopäihin WLAN-kortit. Tämä ratkaisu on tietoliikennekaapelien vetämistä joustavampi ja halvempi vaihtoehto. Esimerkiksi messujen järjestäminen messuhalliin tai liikuntasaliin on helppoa. Kaapelien vetäminen olisi tällaisiin paikkoihin työlästä ja joskus jopa mahdotonta. Samoilla perusteilla historiallisesti tärkeät paikat saataisiin tarvittaessa verkotettua.

Suurimmat säästöt saavutetaan suurilla ulkoalueilla. Siellä kaapelien vetäminen saattaisi tulla huomattavan kalliiksi, esimerkiksi jos yhteyspisteiden välillä on joki, rautatie tai autotie. Langattomissa vaihtoehtoisissa tarvitaan vain tukiasemia riittävä määrä. Mikäli tukiasemien välillä on korkeampi läpikulun este, tarvitaan yksi ylimääräinen tukiasema sen kiertämiseen. (Geier 1999: 9,11)



Kuva 1. WLAN-verkon tuomia etuja ulkotiloissa.

3.4 WLAN-verkon haittapuolia

WLAN-verkkojen tarjoamat edut ovat tervetulleita yrityksiin ja yhteisöihin. Vaikka edut ovatkin huomattavat, WLAN-verkot saattavat aiheuttaa päänvaivaa ylläpidolle ja käyttäjille. Verkko saattaa nopean tiedonsiirron sijaan tarjota hitaat yhteydet ja huonon yhteensopivuuden olemassa olevien laitteistojen ja ohjelmistojen kanssa.

3.4.1 Radiosignaalista johtuvat ongelmat

Radiosignaalia käytetään tiedon lähettämiseen ja vastaanottamiseen. Tämä tekee langattomista verkoista haavoittuvaisen. Tiedon siirtoa häiritsee kaikki samalla taajuudella toimivat laitteet. Esimerkiksi mikroaaltouuni käyttää samaa 2,4 GHz:n taajuutta kuin langattomat verkotkin. Mikäli WLAN-verkon kuuluvuusalueella

toimii mikroaaltouuni tai jokin muu liikennettä häiritsevä laite, aiheutuu tästä liikenteelle viivettä tai jopa lähetyksvirheitä. Tällaiset laitteet saattavat rajata mahdollisuutta laajentaa langatonta verkkoa.

Vaikka WLAN-liikennettä häiritseviä laitteita on aika paljon (mikroaaltouunit, bluetooth-laitteet, palohälyttimet, jne.), eivät ne häiritse langatonta verkkoa niin merkittävästi, etteikö verkkoa voitaisi toteuttaa. Tämä johtuu siitä, että yleensä häiritsevien laitteiden käyttämä kaista on kapea verrattuna WLAN-verkon käyttämään. Ilmatietä pitkin WLAN-verkon lähettämä tieto löytää suurimmaksi osaksi perille, eikä viive kasva kovinkaan suureksi. (Geier 1999: 21)

3.4.2 Signaalin fyysiset esteet

Mikäli langaton verkko halutaan yhteen isoon tilaan, jossa ei ole väliseiniä, toimii WLAN-ratkaisu yleensä hyvin. Mikäli kyseessä on rakennus, jossa täytyy saada katetuksi useita kerroksia ja kerroksissa on paksuja seiniä, saattaa tulla ongelmia. Tällaiset ongelmat ovat yleensä havaittavissa yleensä jo alustavissa kuuluvuusmittauksissa. Vaikka signaali kuuluisikin väliseinän läpi, se saattaa heikentyä niin voimakkaasti, ettei WLAN-ratkaisu välttämättä ole paras vaihtoehto.

3.4.3 Virran kulutus ja kaapelointi

WLAN-päätelaitteet, kuten kannettavat tietokoneet tai kämmenmikrot, saavat tarvittavan virran akuista. Mikäli päätelaitteeseen lisätään uusia komponentteja, virrankulutus kasvaa. Esimerkiksi kannettaviin tietokoneisiin tarvitaan WLAN-kortti, jotta voitaisiin lähettää ja vastaanottaa tietoa langattomassa verkossa. Tämä lisälaite kuluttaa kannettavan akkua. Virrankulutus ei kuitenkaan ole kovin huomattavaa. Kiinteissä päätelaitteissa ylimääräisestä virrankulutuksesta ei ole haittaa, koska virtaa syötetään kokoajan verkkovirrasta.

WLAN tukiasemat tarvitsevat toimiakseen sekä verkkovirtakaapelin että verkko-kaapelin (Ethernet). Mikäli valmista kaapelointia WLAN-verkkoa varten ei ole olemassa, joudutaan kaapelointi suorittamaan. Tämä aiheuttaa lisäkustannuksia sekä huomattavan määrän työtä. Tukiasemien sijaintia suunniteltaessa kannattaa-

kin ottaa huomioon jo valmiina olevat kaapeloinnit. Tällä tavoin voidaan säästää huomattava summa rahaa sekä aikaa. (Geier 1999: 23-24)

3.4.4 Yhteensopivuusongelmat

Jotta langattomat verkkolaitteet saataisiin toimimaan, täytyy järjestelmistä löytyä tuki niille. Vanhimmat käyttöjärjestelmät eivät välttämättä ymmärrä WLAN-kortteja. Käyttöjärjestelmän päivityksenkin jälkeen toiminta saattaa olla epävarmaa. Uusimmissa käyttöjärjestelmissä on tuki lähes kaikille uusille langattomille verkkokorteille. Tukiasemat eivät sinänsä tarvitse käyttöjärjestelmältä tukea, koska ne toimivat itsenäisesti verkon jatkeena. Mikäli on tiedossa ohjelmia tai laitteita, joiden kanssa saattaisi tulla ongelmia langattoman verkkotekniikan kanssa, kannattaa asia testata, ennen kuin alkaa toteuttaa WLAN-hanketta. (Geier 1999: 24)

3.5 Standardit

Institute of Electrical And Electronics Engineers (IEEE) on tietoliikennealan kattojärjestö, joka vastaa monien muiden standardien ohella myös langattomissa lähiverkoissa toimivasta 802.11-standardiperheestä.

IEEE 802.11 -suosituksen tehtävänä on määritellä toiminta sellaisessa langattomassa lähiverkossa, jossa kanavavaraukseton päätöksenteko on yksittäisillä työasemilla tai keskitetysti tukiasemalla.

IEEE 802.11 -suosituksen ensimmäinen versio hyväksyttiin vuonna 1997. Alkuperäinen siirtonopeus oli yksi ja kaksi megabittiä sekunnissa. Standardi sisälsi verkoille monia vaihtoehtoisia toteutuksia eikä taannut keskinäistä yhteensopivuutta, mikä vähensi niin laitevalmistajien kuin kuluttajienkin suosiota. Paranneltu versio julkaistiin vuonna 1999, ja se toi mukanaan kaksi laajennusta: IEEE 802.11a, joka tukee 54Mbps siirtonopeuksia 5GHz ISM-alueella ja IEEE 802.11b, joka tukee 11Mbps siirtonopeuksia 2,4 GHz:n ISM -alueella. (Granlund 2001: 230)

Standardointia tehdään, jotta saataisiin selvemmat pelisäännöt. Mikäli standardointia ei olisi, saattaisi syntyä tahtomattakin eri tekniikoiden välille kilpailua. Esimerkiksi WLAN:lle voidaan katsoa potentiaaliseksi uhaksi bluetooth, joka käyttää samaa 2,4GHz:n taajuuskaistaa. Näiden uhkien poistoon tarvitaan standardointia. (Seppänen)

3.5.1 Standardi 802.11b

Alkuperäisen 802.11-standardin nopeus (1 ja 2 Mbps) ei riittänyt vastaamaan kaapeliverkon nopeuksia. IEEE reagoi tarpeeseen määrittelemällä suuremman siirtonopeuden multimediapalveluja silmällä pitäen. Syyskuussa 1999 IEEE 802.11 ”High rate” -lisäys hyväksyttiin. Siinä määriteltiin tiedonsiirtonopeudet 5,5 ja 11 Mbps sekä parempi yhteyden laatu. Suurempaa tiedonsiirtonopeutta varten valittiin suorasekvenssi.

802.11b-järjestelmät toimivat 1 ja 2 Mbps 802.11 DSSS-järjestelmien (Direct Sequence Spread Spectrum) kanssa. Koodaustekniikka Complementary Code Avaining (CKK) kehitettiin 802.11-standardin nopeuden lisäämiseksi (Seppänen)

802.11b on tällä hetkellä yleisin käytettävistä standardeista. Sen liikennöinti tapahtuu 2,4-2,4835 GHz välisellä vapaalla ISM-taajuusalueella. Samaa taajuutta käyttävät muunmuassa bluetooth-laitteet. Vapaan taajuusalueen ansiosta jokainen voi pystyttää verkon mihin tahansa ilman radiolupaa. 802.11b ylittää teoriassa 11Mbps:n nopeuteen. Samalla taajuusalueella toimivat laitteet sekä erilaiset esteet tekevät mahdottomaksi kuitenkin tällaisiin nopeuksiin yltämisen. Todellinen nopeus jää välille 5-7 Mbps. (Juutilainen; Oraskari 2003: 62)

3.5.2 Standardi 802.11a

Standardi julkistettiin samaan aikaan kuin 802.11b. A-version nopeus ylittää teoriassa 54 Mbps:n nopeuteen. Se on nopeutensa ansiosta hyvä valinta silloin, kun tarvitaan runsaasti kaistaa, esimerkiksi reaaliaikaisen videon välittämisessä. 802.11a toimii reilun viiden gigahertsin taajuudella, jonka käytöstä ei ole maailmanlaajuisesti hyväksyttyä sopimusta.

Euroopassa käytetään taajuuksia 5,15 - 5,35 ja 5,470 - 5,725 GHz. 802.11a saa käyttää Usa:ssa taajuuksia 5,15 - 5,35 ja 5,725 - 5,825 GHz ja Japanissa 5,15 - 5,25 GHz. Nämä samat taajuusalueet ovat valmiiksi jo käytössä. Euroopan taajuusalueita käyttävät esimerkiksi satelliitit, tutkat ja erilaiset navigointijärjestelmät. Näiden päällekkäisyyksien takia taajuuskaistoilla tapahtuvalle tietoliikenteelle on säädetty lakeja.

Alempi taajuusalue on tarkoitettu käytettäväksi ainoastaan sisätiloihin ja suurin lähetysteho on rajoitettu 200 milliwattiin. Ylemmällä taajuusalueella lähetysteho saa olla 1 wattia ja se on tarkoitettu myös ulkokäyttöön. Suomessa ulkokäyttö ei kuitenkaan ole sallittua. Lähetystehon voi määritellä helposti itsekin, eikä 802.11a-laitteiden käyttö siihen kaadu. Laitteiden käytön hyväksymisen edellytyksenä on kuitenkin vielä kahden muun kriteerin täytyminen: dynaaminen kanavalinta sekä automaattinen tehonsäätö.

Dynaaminen kanavan valinta tarkoittaa sitä, että tietoliikenne osaa siirtyä automaattisesti toiselle kanavalle, mikäli samalla kanavalla on monta laitetta. Automaattisella tehonsäädöllä taas tarkoitetaan sitä, että tehoa säädetään alaspäin automaattisesti, siten että kauimmainen päätelaite pystyy liikennöimään tukiaseman kanssa. Näiden rajoitusten tarkoituksena on estää langatonta verkkoa häiritsemästä samalla taajuudella tapahtuvaa muuta liikennettä. 802.11a ei toteuta näitä ehtoja. Näin ollen 802.11a:n mukaisten laitteiden käyttö on kiellettyä Suomessa. Viestintäviraston mukaan laitteita ei tulla sallimaan, ennen kuin ehdot saadaan täytetyksi. (Kuokka 2002: 10-12)

3.5.3 Standardit 802.11h ja 802.11d

Koska 802.11a:ssa on tiettyjä puutteita, on kehittelyn alla 802.11h, joka lisäisi a-versiosta puuttuneet ominaisuudet: dynaamisen kanavan vaihdon sekä automaattisen tehonsäädön. 802.11d liittyy kehitteillä olevaan h-standardiin kiinteästi. Se antaa laitteille mahdollisuuden neuvotella käytettävät taajuuskaistat sopiviksi jokaiselle maalle erikseen. Se tarkoittaisi sitä, että WLAN-kortti osaisi automaatti-

sesti virittäytyä kunkin maan tarjoamille taajuuksille. WLAN-kortti osaisi lukea tiedot suoraan siltä tukiasemalta, mihin se ottaa yhteyden. (Kuokka 2002: 13; The wireless lan association 2002)

3.5.4 Standardi 802.11g

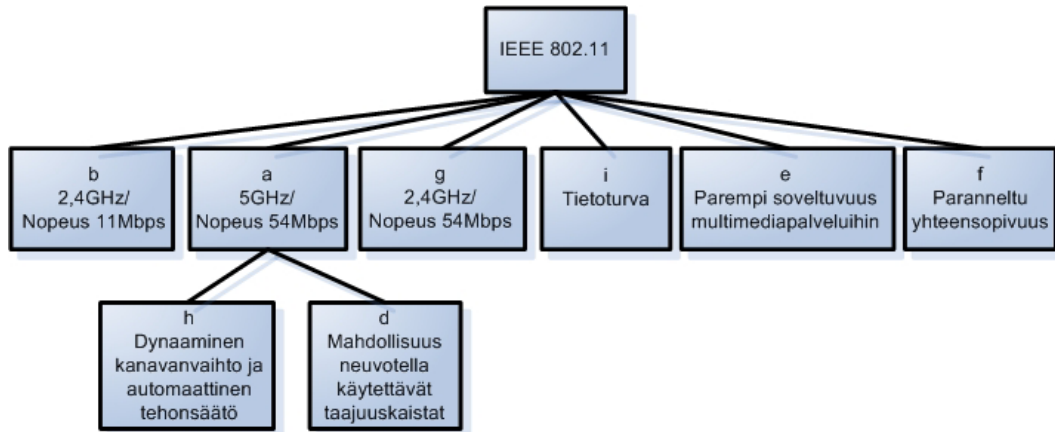
Tämän standardin mukaiset laitteet toimivat a-version tapaan 54Mbps:n nopeudella, mutta 2,4GHz:n taajuudella. Lisäksi se on täysin yhteensopiva aikaisemman 802.11b-standardin kanssa. A-versio ei tukenut b-standardia. 802.11g-laitteet sopivat paikkoihin, joissa vaaditaan suurta kaistaa, esimerkiksi messuhalleihin tai auditorioihin. (Kuokka 2002: 13; The wireless lan association 2002)

3.5.5 Standardi 802.11i

802.11i valmistuu vuoden 2004 alkupuolella. I-versio keskittyy tietoturvan parantamiseen. Suurin muutos uudessa standardissa koskee salausalgoritmia, joka vaihtuu RC4:stä AES-salaukseen. AES-salaus on ajateltu hoitaa kokonaan sille tarkoitettulla prosessorilla, jolloin tiedonsiirron teho paranee. Kappaleessa tietoturva on kerrottu 802.11i-standardista enemmän. (Kuokka 2002: 13; The wireless lan association 2002)

3.5.6 Standardit 802.11e ja 802.11f

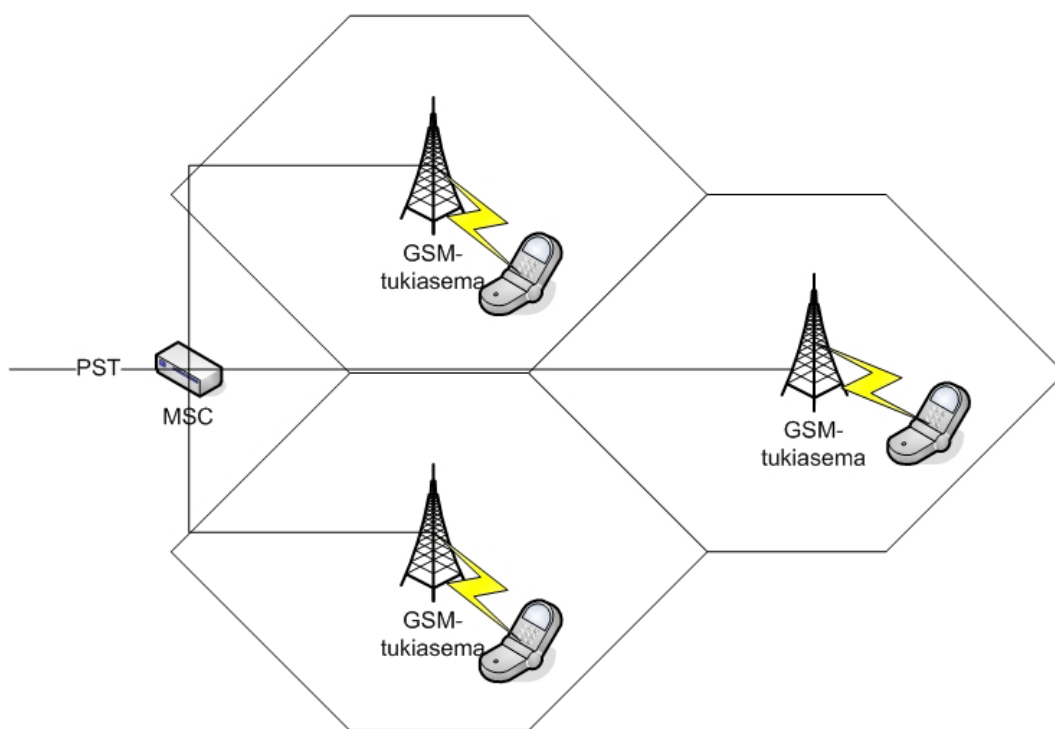
Uudet standardit ovat usein keskittyneet parantamaan nopeutta tai tietoturvaa. E- ja f-versiot parantavat kuitenkin laitteiden ominaisuuksia. 802.11e pyrkii parantamaan WLAN-verkon soveltuvuutta multimediapalveluihin. F-version pyrkimyksenä on parantaa eri valmistajien välistä yhteensopivuutta. (Kuokka 2002: 13-14; The wireless lan association 2002)



Kuva 2. WLAN-standardit ja niiden tärkeimmät ominaisuudet.

4. WLAN-VERKKOJEN RAKENNE

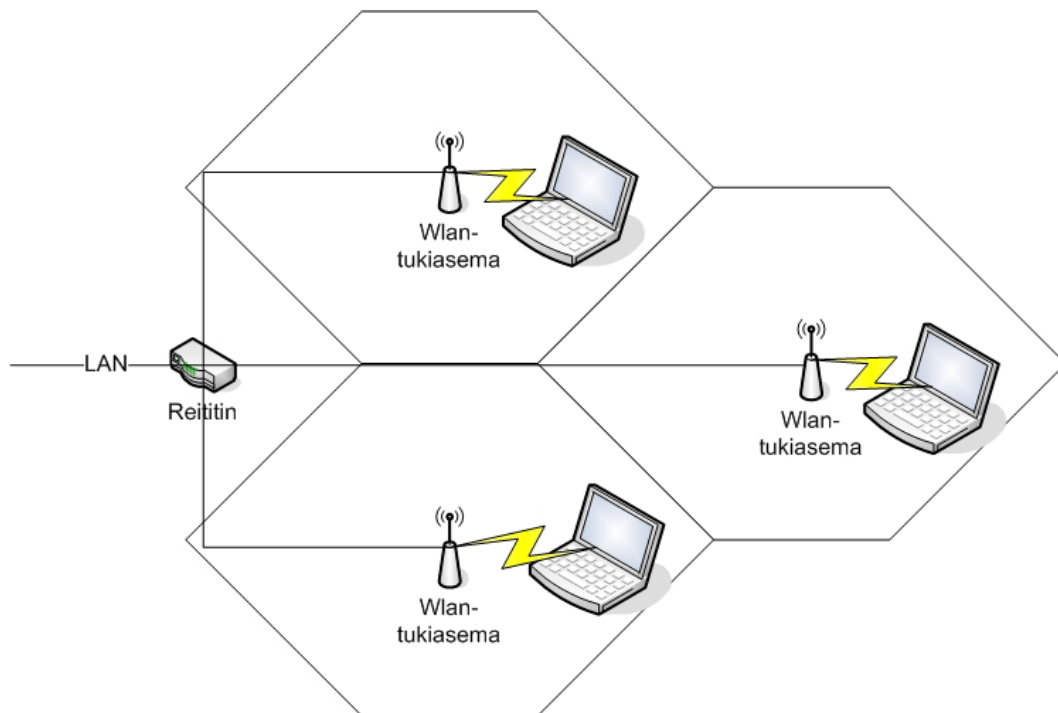
WLAN-verkkojen arkkitehtuurissa käytetään GSM-verkosta tuttua solurakennetta. Siinä jokaisella solulla on oma taajuusalueensa, jolla kommunikoidaan tietyn solun vaikutusalueen sisällä. Jotta solut eivät häiritsisi toistensa toimintaa, on tärkeää, ettei vierekkäiset solut käytä samaa taajuusaluetta. WLAN-verkossa solun liikennettä hallitsee WLAN-tukiasema. Tukiasemat pitävät keskenään yhteyttä runkoverkon välityksellä. Päätelaitteet, kuten käsipuhelimet GSM-verkossa ja kannettavat tietokoneet WLAN-verkossa, ovat yhteydessä tukiasemiin radiorajapinnan välityksellä. (Seppänen)



Kuva 3. GSM-verkko (Seppänen).

WLAN-verkossa tukiasema toimii keskittimenä. Tukiasemat ovat yhteydessä runkoverkkoon ja sitä kautta toisiinsa. Tukiasemiin otetaan yhteys päätelaitteella, jossa on langaton verkkokortti. WLAN-kortissa on lähetin ja vastaanotin, joiden avulla se keskustelee solun muodostavan tukiaseman kanssa. Langattoman verkkokortin avulla voidaan olla yhteydessä tukiasemiin verkon kaikissa soluissa. Li-

kuttaessa WLAN-kortti osaa automaattisesti vaihtaa tukiasemaa (roaming), eikä verkkoyhteys välillä katkea. (Seppänen)



Kuva 4. WLAN-verkko (Seppänen).

4.1 Roaming

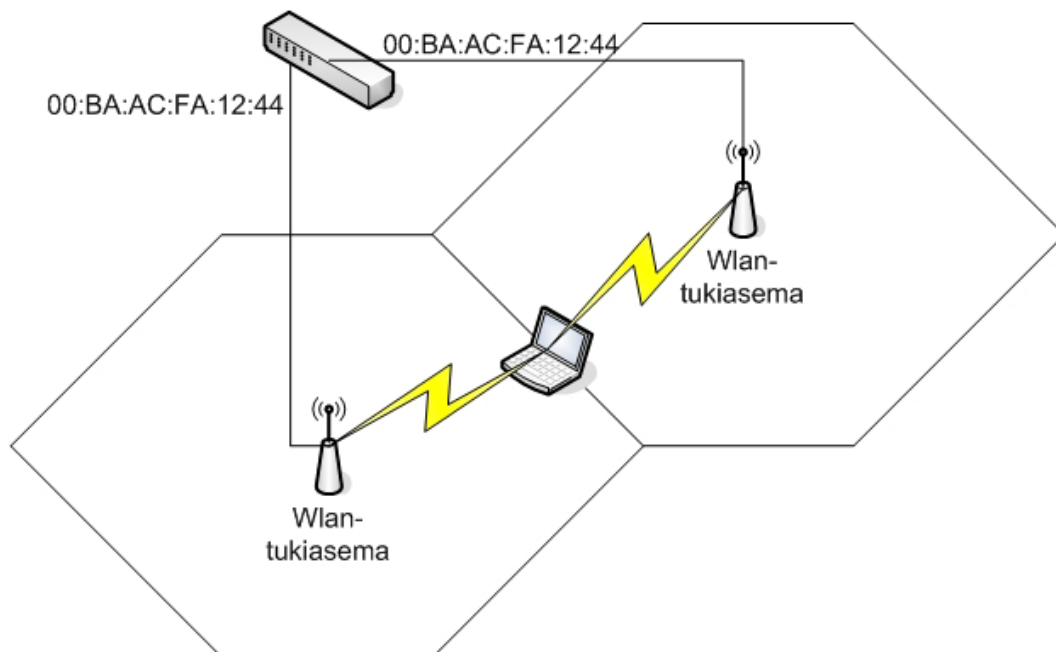
Kun tietoliikenneyhteyden täytyy olla koko ajan auki riippumatta siitä, miten liikutaan langattoman verkon alueella, tarvitaan ominaisuutta, joka pystyy siirtämään kommunikoinnin tukiasemalta toiselle yhteyden katkeamatta. Tämän ominaisuuden nimi on roaming. Käytännössä tämä on monimutkainen tapahtumasarja ja vaatii tukiasemien ja päätelaitteen yhteistoimintaa.

Kun kuuluvuus tukiasemaan heikkenee, alkaa päätelaitteen langaton verkkokortti etsiä paremmin kuuluvaa tukiasemaa. Mikäli tällainen löytyy, lähetetään yhteydenmuodostuspyyntö löydetylle tukiasemalle. Jos pyyntö hyväksytään, siirretään liikenne kulkemaan voimakkaammin kuuluvan tukiaseman kautta. Tästä muutok-

sesta ilmoitetaan kiinteälle verkolle, joka purkaa vanhan yhteyden aiempaan tukiasemaan.

Roaming-ominaisuutta käytettäessä tarvitaan kaapeliverkkoa. Tukiasemien välinen yhteys on toteutettu kiinteän verkon välityksellä, eikä ole WLAN-standardien piirissä. Standardit määrittelevät osittain roamingia koskevia säännöksiä, jotka kaapeliverkon täytyy toteuttaa. Tukiasemien välistä protokollaa kehitetään valmistajien voimin. Protokollan nimi on Inter-Access Point Protocol, IAPP.

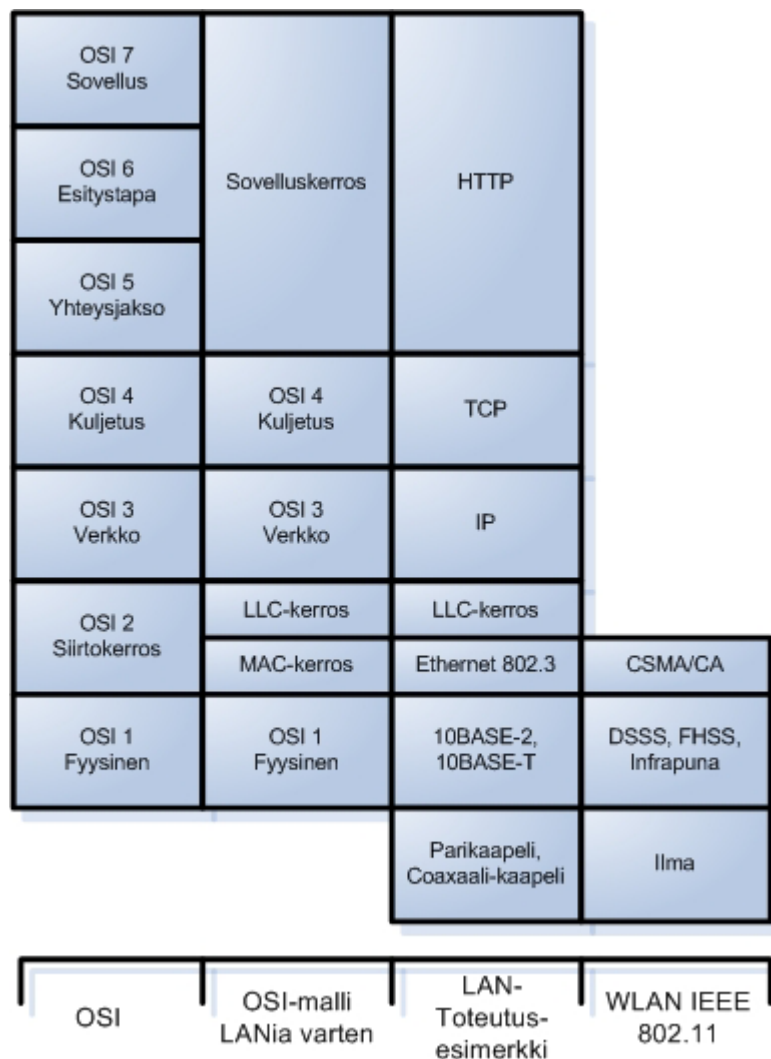
Roaming saattaa aiheuttaa myös ongelmia runkoverkossa. Jos samaan kytkimeen on kytketty kaksi tukiasemaa ja kyseiset tukiasemat sattuvat olemaan vierekkäisissä soluissa, voi muodostua ongelma. Kytkimellä on tiettyssä portissa tieto siitä, mikä fyysinen osoite (MAC) on sitä kautta yhteydessä. Kun siirrytään viereiseen soluun, niin WLAN-kortti vaihtaa paremmin kuuluvaan tukiasemaan. Koska edellistä yhteyttä ei ole purettu, kytkin ymmärtää, että kahden eri portin kautta kulkee liikennettä samasta MAC-osoitteesta (Kuva 5) (Juutilainen; Seppänen).



Kuva 5. Roamingin aiheuttama ongelma.

4.2 Osi-malli

IEEE 802.11 -protokolla määrittelee OSI-mallin toisen kerroksen siirtoyhteyserroksen protokollan (Medium Access Control-kerros MAC), joka on yhteydessä kolmeen eri fyysiseen kerrokseen (Physical layer, PHY). MAC-alikerros huolehtii radiotaajuisesta yhteydestä riippumattomasta yhteyuskäytännöstä. Fyysinen taso yhdistää MAC-alikerroksen varsinaisiin radiotaajuisiin siirtoyhteyksiin. Fyysinen taso on erotettu siirtokerroksesta, jotta jatkossa siirtyminen uusille taajuuskaistoille ja modulaarimenetelmiin on mahdollista. Kuva 6 näyttää IEEE 802.11:n protokollakerrokset verrattuna vastaaviin pinoihin.



Kuva 6. WLAN OSI-mallin erot verrattuna muihin vastaaviin (Seppänen).

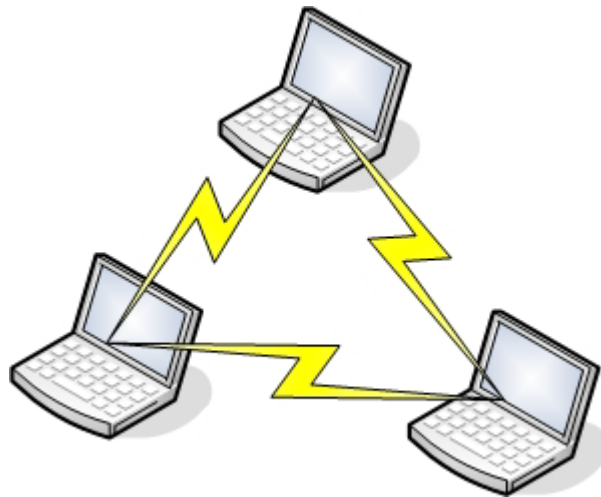
4.3 Topologiat

WLAN-verkko perustuu soluarkkitehtuuriin. Jokaista solua valvoo tukiasema. 802.11 WLAN:iin on olemassa kolmea erilaista soluarkkitehtuuria. Nämä ovat AdHoc sekä kaksi erilaista infrastruktuuriverkkoa. (Seppänen)

4.3.1 IBSS-verkko

Jos laitteiden muodostama verkko ei kytkeydy kiinteään verkkoon (esim. 802.3), verkosta käytetään nimitystä IBSS (Independent Basic Service Set). IBSS-verkko on yleensä lyhytikäinen ratkaisu, jossa verkko muodostetaan johonkin tiettyyn tarpeeseen, ja se purkautuu tarpeen päättyessä. Tyypillinen tilanne voisi olla esimerkiksi neuvottelu- tai kokouksitilanne, jossa osallistujat tuovat mukanaan omia laitteita, ja laitteet keskustelevat langattoman verkon yli kokouksen tai opetuksen ajan. Tämän ominaisuuden takia IBSS-verkosta käytetään myös nimeä Ad-Hoc-network

AdHoc-verkossa asiakaskoneet keskustelevat keskenään omassa lähiverkossa. Lähettiminä ja vastaanottiminä toimivat langattomat verkkokortit. Kommunikaatioon käytetään tukiasemaverkon tavoin radioyhteyttä.



Kuva 7. IBSS/AdHoc-verkko (Seppänen).

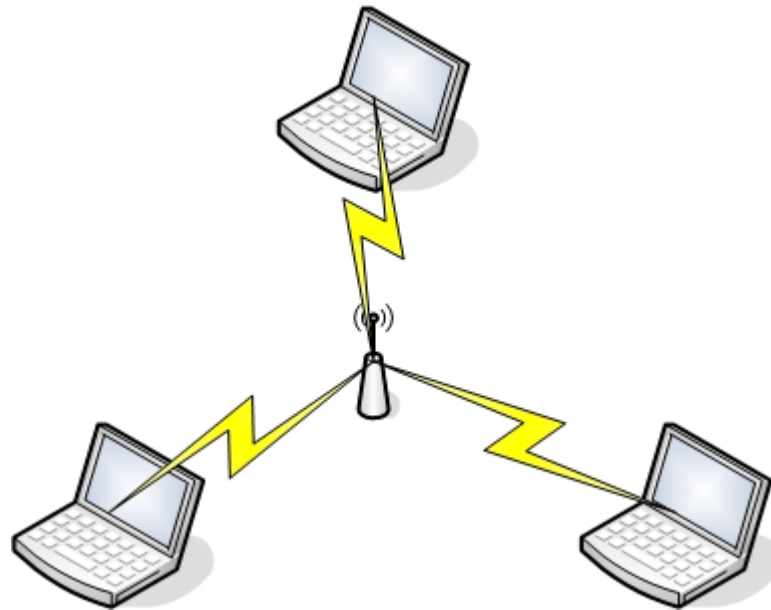
4.3.2 Infrastruktuuriverkko BSS

Infrastruktuuriverkossa on ainakin yksi tukiasema, jonka välityksellä päätelaitteet keskustelevat keskenään. Tätä kutsutaan nimellä Basic Service Set (BSS). Topologia muistuttaa keskittimiin perustuvia kiinteitä lähiverkkoja. IBSS:ään verrattuna, tiedonsiirtoon laitteelta toiselle, käytetään kaksinkertainen kapasiteetti, koska sanoma on ensin siirrettävä tukiasemalle ja vasta tämän jälkeen toiselle työasemalle. (Granlund 2001: 231-232; Seppänen)

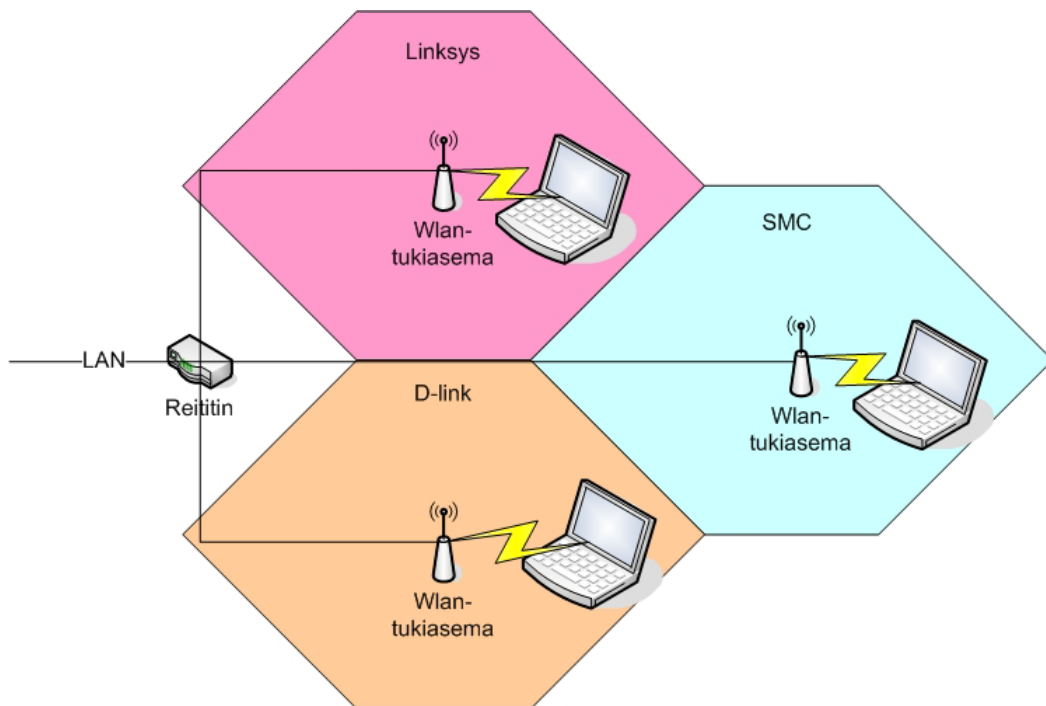
4.3.3 Infrastruktuuriverkko ESS

Laajempi kokonaisuus saadaan, kun rakennetaan useita BSS:illä muodostettuja aliverkkoja. Yleensä laajennettu palvelu Extended Service Set (ESS) on yhdistetty kiinteään runkoverkkoon, josta on myös yhteys Internetiin. Päätelaitteet keskustelevat tässä tyypissä tukiasemien kautta, ja ne edelleen runkoverkon kautta. Runkoverkosta käytetään tässä nimitystä Distribution System (DS). ESS-tyyppisen verkon eri solut voivat olla eri valmistajien tukiasemien muodostamia.

Koko yhteenliitetty WLAN soluineen ja tukiasemineen nähdään yhtenä 802-verkkona ylemmille kerroksille OSI-mallissa. Yleensä kaikki vähänkin suuremmat WLAN-asennukset ovat ESS-tyyppisiä. Yhteen tukiasemaan voi liittyä maksimissaan 254 laitetta, mutta käytännön suositus on 20 - 60 päätelaitetta tukiasemaa kohti. (Granlund 2001: 232; Seppänen)



Kuva 8. Infrastruktuuriverkko, BSS (Seppänen).

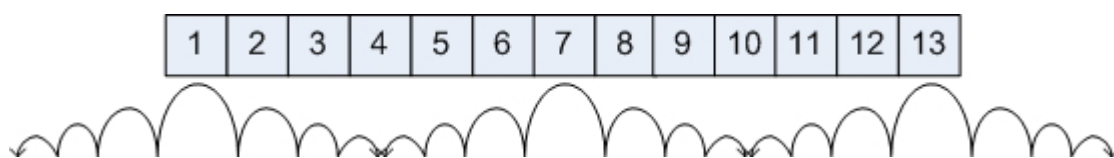


Kuva 9. Infrastruktuuriverkko, ESS (Seppänen).

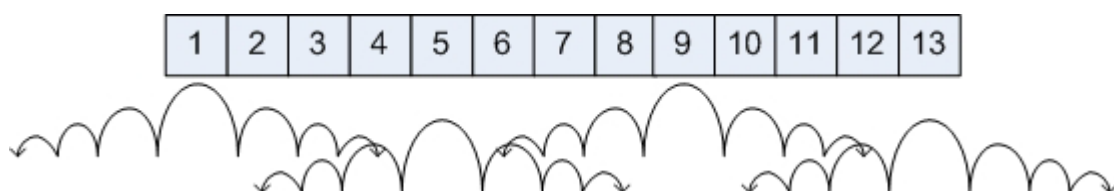
4.4 Kanavien varaaminen

Kanavat ovat taajuuksia, joilla tukiasemat lähettävät ja vastaanottavat tietoa. Mikäli samaan soluun kuuluu samalla kanavalla lähetettävää keskustelua toisen tukiaseman kanssa, häiriintyy kummankin tukiaseman liikenne. Siksi WLAN-verkkoja rakennettaessa tulee suunnitella vierekkäisten solujen kanavat mahdollisimman kauaksi toisistaan. (Oraskari 2003: 64)

Euroopassa 802.11 WLAN -verkossa on eri kanavia käytössä 1 - 13 kappaletta. Kanavien taajuudet menevät kuitenkin osittain päällekkäin. Euroopassa kaikki 13 kanavaa ovat sallittuja, mutta ainoastaan 1, 7 ja 13 ovat kanavia, jotka eivät häiritse toisiaan (kuva 10). Jos halutaan hieman enemmän vaihtoehtoja kanavointiin, voidaan ottaa käyttöön malli, jossa käytetään kanavia 1, 5, 9 ja 13. Näillä kanavilla taajuudet menevät hieman päällekkäin (kuva 11). Häiriö, joka esiintyy kohinaa, ei kuitenkaan ole niin merkityksellinen, koska valitut kanavat ovat melko kaukana toisistaan. Lisäksi tällä ratkaisulla saavutetaan yksi lisäkanava, mikä voi olla hyvin tärkeää suuria kokonaisuuksia suunniteltaessa. (Seppänen)



Kuva 10. Spektrin periaatekuva, kanavat 1,7 ja 13 (Seppänen).



Kuva 11. Spektrin periaatekuva, kanavat 1,5,9 ja 13 (Seppänen).

4.4.1 Kanavat AdHoc- ja BSS-verkoissa

AdHoc-verkoissa ei käytetä tukiasemia, joten kanavavalintaan ei tarvitse kiinnittää huomiota. Päätelaitteet seuraavat kaikkea AdHoc-verkossa tapahtuvaa liikennettä. BSS-verkoissa käytetään tukiasemaa, mutta koska niitä on vain yksi kappale, ei sen liikennettä pääse häiritsemään minkään muun tukiaseman liikenne. Tämän yhden tukiaseman käyttöön voidaan määritellä mikä tahansa 13 kanavasta.

Yleisesti ottaen kanavointiin ei tarvitse kiinnittää huomiota muuta kuin laajennetun palvelun verkoissa tukiasemakohtaisiksi. (Seppänen)

4.4.2 Kanavat ESS-verkoissa

Kun WLAN-verkko on useiden tukiasemien muodostama, kasvaa kanavoinnin merkitys. Tukiasemien kanavat on valittava siten, ettei vierekkäisten solujen käyttämä taajuus mene päällekkäin. Minimisääntönä voidaan pitää sitä, että vierekkäisten tukiasemien solujen väliin jätetään ainakin kaksi käyttämätöntä kanavaa. Mikäli tukiasemat ovat toistensa kuulumattomissa, kanavat voivat olla samatkin, koska tällöin ne eivät pääse häiritsemään toisiaan. (Seppänen; Oraskari 2003: 64)

4.4.3 Tiedonsiirto

Tiedonsiirtonopeus pysyy yleensä vakiona kaapeliverkossa. WLAN-verkossa tilanne on toisin. Langattoman verkon toimintaan vaikuttaa tukiaseman ja päätelaitteen välisen etäisyyden lisäksi erilaiset välillä olevat esteet. Monet asiat rakennuksissa, kuten seinät, palkit, metalli ja jopa ihmiset, voivat vaikuttaa radioaalloilla tapahtuvaan liikenteeseen ja näin järjestelmän kantavuuteen. Tavallisesti tukiasema ja päätelaite voivat kuulla toisensa 30 - 100 metrin etäisyydellä toisistaan.

Mikäli etäisyys on lyhyt vastaanottimen ja lähettimen välillä, kohtaa signaali vain vähän interferenssiä ja vääristymiä ympäristöstä. Näin virheentarkastuksen tarve pienenee. Käyttäjät voivat olla paikallaan tai liikkua kävelyvauhtia. Suuremmissa verkoissa vauhti voi olla suurempikin, jolloin signaalin on mahdollista vääristyä ns. Rayleighin häipymisenä. Kaikki nämä tekijät vaikuttavat siirtonopeuteen.

Lyhyt etäisyys tuottaa paremman signaali-kohinasuhteen, jolloin saavutetaan myös paras siirtonopeus.

Tiedonsiirtonopeuteen vaikuttaa myös tukiaseman solussa liikennöivien asiakkaiden määrä. Mikäli liikennöiviä päätelaitteita on vain yksi, tämä saa kaiken tukiaseman tarjoaman siirtonopeuden käyttöönsä. Yleensä teoreettinen nopeus on 11 Mbps, mutta käytännössä jäädyään 5 - 7 Mbps:n siirtonopeuteen. Mikäli useita käyttäjiä on yhteydessä saman tukiaseman kautta, jaetaan tarjottava tiedonsiirtonopeus käyttäjien kesken.

Tiedonsiirto rakennuksien välillä voidaan toteuttaa esimerkiksi suuntaavilla antennilla. Puhutaan ns. WLAN point-to-point -tyyppisistä lähiverkkojen välisistä silloista. Tällainen yhteys kannattaa toteuttaa esimerkiksi kahden eri rakennuksen välille, joita erottaa tie. Vaatimuksena on ainoastaan näköyhteys paikkojen välillä. (Seppänen; Oraskari 2003: 62)

5. WLAN-VERKON SUUNNITTELU

5.1 Taustatietoa

Kun WLAN-verkkoa lähdetään suunnittelemaan, tulee ennen varsinaisia asennustöitä ottaa huomioon useita verkon toimintaan vaikuttavia asioita. Tulevan WLAN-verkon käyttäjien kanssa tulee selvittää verkon käyttötarkoitus. Eli esimerkiksi, millaisia sovelluksia verkossa käytetään, ja onko verkkoyhteys kaikilla käyttäjillä katkonaista vai jatkuvaa. Myös oletetut käyttäjämäärät tulee selvittää etukäteen.

Yhtäaikaisten käyttäjien määrä voi kasvaa verkossa suureksi, esimerkiksi kirjastoissa, luokkahuoneissa ja auditorioissa. Tällaisissa paikoissa tulee jo suunnitteluvaiheessa varautua siihen, että näillä alueilla tarjotaan suurempaa kaistaa. B-standardi tarjoaa 11 megabitin siirtonopeuden. Siirtovirheistä sekä uudelleenlähetyksestä johtuen, todellinen siirtonopeus saattaa jäädä noin 40 prosenttiin tästä. Todelliseksi siirtonopeudeksi jää tällöin vain noin 5 megabittiä sekunnissa. Tämä nopeus vielä jaetaan yhtäaikaisten käyttäjien kesken. Kun käytetään toimistosovelluksia, on arvioitu, että 11 megabitin verkon yhden kanavan riittävän 20 - 60 yhtäaikaiselle käyttäjälle. (Seppänen; Oraskari 2003: 62)

5.2 Asennusympäristön tutkiminen

WLAN-verkkoa suunniteltaessa tulee ottaa huomioon ympäristö, johon tukiasemien asennukset tehdään. Ennen asennuksia pitää huomioida ympäristön asettamat erityisvaatimukset, kuten erilaiset seinätyypit sekä häiriölähteet. Samalla tulee kartoittaa pistorasioiden sekä verkkoliitäntöjen paikat.

Erilaisissa seinämateriaaleissa on suuriakin eroja, kun ajatellaan tukiasemien kantavuutta. Yleisenä sääntönä voidaan pitää, että yhden tukiaseman signaali läpäisee ainakin yhden seinän, lattian ja katon. Signaalin kulkua rajoittavat seinämateriaalit, ja sen teho laskee suhteessa etäisyyteen tukiasemasta. Materiaaleista puu,

muovi ja lasi vaimentavat radiosignaalia vähän. Tiiliseinät ja betoniseinät haittaavat jo selvästi enemmän, ja metalliesteet ovat lähes läpitunkematon este.

Erilaisia häiriölähteitä voi olla useita erilaisia. WLAN-verkon taajuusalueita jakavat kaikki 2,4 gigahertsin laitteet. Tällaisia ovat esimerkiksi bluetooth-laitteet, murto- ja palohälyttimet, mikroaaltouunit sekä sisäpuhelimet. Mikä tahansa näistä laitteista voi aiheuttaa häiriötä rakennettavalle WLAN-verkolle. Näiden sijainti sekä käyttö tulee selvittää ennen verkon käyttöönottoa. (Geier 1999: 258; Oraskari 2003: 62)

5.3 Antennien valinta

Antennien valinnalla ja sijoittelulla on merkitystä WLAN-verkon toimivuuteen. Jos käytetään tavallista ympäristöilevää antennia, tulisi se sijoittaa mahdollisimman avaraan paikkaan, jotta sen lähellä olevat erilaiset esteet eivät rajoittaisi sen kuuluvuutta. Lisäksi lähekkäisten tukiasemien antennien välimatkan tulisi olla vähintään 2 - 3 metriä. Rakennusten väliseen liikenteeseen käytettäviä suuntaavia antennia suunniteltaessa ei välimatka ole niin tärkeä, koska tämä antennityyppi ei ole niin herkkä.

Tekniset rajoitukset eivät ole ainoita huomioon otettavia asioita suunniteltaessa WLAN-verkkoa. Tietyissä kiinteistöissä saattaa olla esteettisyysrajoituksia, jotka tulee ottaa huomioon tukiasemien sekä antennien sijoittelussa. Julkisivuon ei välttämättä voi asentaa ulkoasua muuttavaa antenniratkaisua tai tukiasemaa. (Oraskari 2003: 63)

5.4 Tukiasemien sijoittelu

Kun on kartoitettu käyttäjien tarpeet ja määrä sekä hahmoteltu verkon rakentamista rajoittavat tekijät, voidaan alkaa suunnitella tukiasemien mahdollisia paikkoja. Tukiasemien sijainti kannattaa aluksi hahmotella karkealla tasolla.

Ensimmäinen tukiasema tulisi sijoittaa paikkaan, jossa oletetaan verkon käytön olevan kaikkein vilkkainta. Muut tukiasemat sijoitellaan tämän tukiaseman ympär-

rille siten, että saadaan verkolle riittävä peitto. Tukiasemat asetellaan mahdollisimman kauas toisistaan kuitenkin siten, että verkko kattaa halutun alueen/rakennuksen. Näin minimoidaan tukiasemien toisilleen aiheuttamat häiriöt sekä asennus- ja laitekulut.

Kun tukiasemia asennetaan useampiin kerroksiin, niiden sijoittelu tulee suunnitella kolmiulotteisesti, koska tukiasemat säteilevät niin alas, ylös kuin sivuillekin. Eri kerroksissa olevat tukiasemat häiritsevät toisiaan, jos ne ovat liian lähekkäin.

Suunnitteluvaiheen tuloksena voidaan piirtää karkea kartta tukiasemien sijainnista rakennuksen pohjapiirustuksen päälle. Kartalle merkitään tukiasemat suunnitelluille paikoille ja piirretään niiden kuuluvuusalue karkeasti ympyröillä. Tällöin ei oteta huomioon seinien ja muiden häiriötekijöiden vaikutusta. Eri taajuusalueet voidaan hahmotella esimerkiksi eri väreillä. Signaalin voimakkuus voidaan merkitä värin eri voimakkuuksilla.

Koska häiriötekijöiden ja erilaisten seinämateriaalien vaikutusta voi olla hankala ennustaa, suunnitelma voidaan alkuvaiheessa tehdä ainoastaan paperilla. Tämän vuoksi kannattaa varmistaa rakennettavan verkon todellinen kuuluvuus mittaamalla se lopullisissa olosuhteissa.

Kuuluvuusmittausten avulla luodaan tarkka kuuluvuusaluekartta sekä hienosäädetään tukiasemien paikat. Mittaustulosten perusteella valitaan kunkin tukiaseman käyttämä liikennöintikanava.

Kannettavat tietokoneet ovat mittaustyössä käteviä, koska ne eivät tarvitse verkovirtaa toimiakseen. Siten pistorasioiden asennus voidaan jättää siihen, kun tiedetään tukiasemien lopulliset paikat. Myös WLAN-kortilla varustettu kämmenmikro sopii mittausten tekemiseen. Se on myös huomattavasti matkamikroa kevyempi kantaa mukana.

Kuuluvuutta voidaan mitata muun muassa Ad-Hoc-verkolla, jossa kaksi kannettavaa tietokonetta keskustelevat keskenään. Toinen sylimikroista asetetaan suunnitellulle tukiaseman paikalle ja toisella kannettavalla mitataan sen kuuluvuutta eri paikoissa. Mikäli tukiasemat on jo hankittu, voidaan ne asettaa ajatelluille paikoille ja mitata niiden kuuluvuutta yhdellä kannettavalla. Tuloksien perusteella asennetaan tukiasemat lopullisille paikoille.

Mittaukset suoritetaan kiinteistössä kävelemällä ympäri suunnitellun verkon kantavuusalueita ja kirjaamalla ylös kuuluvuus- sekä häiriötasot. Käytettävä ohjelmisto on yleensä laitevalmistajan oma. Eri valmistajien ohjelmistojen ominaisuudet vaihtelevat, mutta yleensä ne tarjoavat arvion tukiaseman signaalin voimakkuudelle ja laadulle. Laitevalmistajan oma ohjelmisto on edullinen ratkaisu, mutta sen avulla ei yleensä saa selville häiriötasoja vaan ainoastaan kuuluvuuden. Näin mittauksissa jää huomiotta kuuluvuuteen vaikuttavien muiden laitteiden (mikroaaltouuni, palohälytin) aiheuttama häiriö.

Jos kiinteistöön tarvitsee suorittaa erityisen monta asennusta ja kohteet ovat hankalia, voidaan käyttää kehittyneempiä mittaohjelmia. Tällaiset analysointiohjelmat voivat signaalin voimakkuuden lisäksi tarjota spektrinäyttöä, jossa graafisesti esitetään koko 802.11b-liikenne. Siten saadaan näkyviin samalla taajuusalueella häiritsevät muut radiolähteet.

Tavallisissa WLAN-verkoissa samalla taajuusalueella saa kussakin verkon pisteessä kuulua enimmillään kolme eri kanavalla liikennöivää tukiasemaa. Tämän varmistaminen ei ole erityisen helppoa mutkikkaimmissa verkoissa. Kehittyneemmät verkonanalysointiohjelmat auttavat havaitsemaan päällekkäisyydet. Tämä helpottaa verkon optimointia huomattavasti.

Kehittyneemmät verkon analysointiin tarkoitetut työkalut ovat usein laitteistoriippumattomia. Tällaisia ohjelmistoja valmistaa muun muassa oululainen Wlanbit ja helsinkiläinen Ekahau. Wlanbit Tricycle -ohjelmistoa voidaan käyttää radiokentän voimakkuuden mittauksissa. Se pystyy mittaamaan signaalin laadun ja voimak-

kuuden lisäksi muiden häiriötä aiheuttavien laitteiden häiriötason C/I (Carrier to Interference ratio). Tuloksia voidaan tarkastella Excel-taulukkona tai tekstinä.

Wlanbitin Tricycle-ohjelman tiedot voidaan siirtää saman valmistajan Unicycle-ohjelmistoon, jossa tulokset voidaan esittää itse piirretyllä kartalla tai suoraan rakennuksen pohjapiirustuksella. Koska tulokset saadaan näkymään suoraan kartalla, helpottuu katvealueiden etsintä.

Kuuluvuusmittaukset antavat karkean kuvan verkon ja sen eri tukiasemien kuuluvuudesta ja toiminnasta. Mittauksista ei kuitenkaan voida lukea varmasti verkon kuormituksesta johtuvia ongelmia. Verkon liikennöinnin toimivuutta voidaan simuloida esimerkiksi Opnet-ohjelmalla, mutta simulointi on vain yhtä hyvä kuin siihen käytetty kuormitusmalli. Todellinen verkon toiminta kannattaakin testata oikean testikäytön avulla. Testikäytössä tulisi mitata verkon toimivuutta muuttamalla lähetettävien pakettien kokoa sekä käyttäjämääriä. Verkon hienosäätö toteutetaan näistä tuloksista. (Seppänen; Oraskari 2003: 63-64)

5.5 Tukiasemien kanavien valinta

Tukiasemien käyttämien taajuuksien välinen ero tulee asettaa mahdollisimman suureksi. Näin toisista taajuuksista johtuvat häiriöt saadaan minimoitua. Häiriöiden vähentämiseksi vierekkäisille soluille tulee asettaa käyttämättömiä taajuuksia. Yhden kerroksen verkossa voidaan käyttää taajuuksia 1, 7 ja 13. Useamman kerroksen verkoissa taajuudet voisivat olla 1, 5, 9 ja 13. (Seppänen)

Jotta päätelaitteet saadaan optimoitua nopeaan verkkoliikenteeseen, tulee ne asettaa käyttämään kanavaa, jossa on sillä hetkellä vähiten liikennettä. Mikäli verkossa esiintyy siirtoviivettä, kannattaa pakettien kokoa pienentää, jolloin lyhytkestoinen verkkohäiriö ei aiheuta muuta kuin paketin uudelleenlähettämisen. Paketin eri osilla tulee kuitenkin olla otsaketietonsa. Jos siis paketit pilkotaan liian pieniksi, se lisää liikennemäärää. Pakettiin kannattaa aluksi asettaa arvo 1000. Tämä tarkoittaa sitä, että tämän arvon ylittävät paketit pilkotaan pienemmiksi. Oikean pa-

ketin koon voi arvioida törmäysten (collision) määrästä. Arvosta 1000 aletaan arvoa pudottaa, kunnes toimiva arvo löydetään. (Oraskari 2003: 64)

5.5.1 Ympäristön muutokset

Kun suunnitellaan verkkoa, kannattaa ottaa huomioon mahdolliset ympäristön muutokset. Rakennusten välille saattaa esimerkiksi kasvaa puu, joka estää liikennöinnin rakennusten välillä. Myös muita yllätyksiä saattaa esiintyä verkon jo ollessa valmis.

Tukiasemien sijoittelussa tulee ottaa huomioon se, että toimistotiloissa saattaa väliseinien sekä kaappien paikka vaihdella. Tukiasemat kannattaakin asentaa sellaisille paikoille, joihin tällaiset muutokset eivät helposti vaikuta. Huono paikka on kaapin päällä, kun taas hyvä paikka voisi olla katossa tai korkealla kiinteässä seinässä.

Koska WLAN-verkkojen rakentaminen on vapaata, saattaa naapurikiinteistöön muuttanut uusi yritys rakentaa oman verkkonsa. Heidän verkkonsa sekä sen tukiasemat voivat aiheuttaa häiriötä omaan verkkoomme. Tällaisissa tilanteissa tulisi yhteistyössä sopia tukiasemien paikat ja tehdä mittaukset.

Verkkoja suunniteltaessa kannattaa varautua siihen, että tulevaisuudessa siirrytään nopeampaan verkkotekniikkaan. Tähän voi varautua siten, että rakennusvaiheessa, kun asennetaan uusia sähköpistokkeita ja Ethernet-pistokkeita, rakennetaan myös viereen tyhjät paikat uudempaa tekniikkaa varten. (Oraskari 2003: 64)

5.6 Dokumentointi

Tärkeä osa verkon suunnittelua, rakentamista ja testausta on verkon dokumentointi. Dokumentaatiosta tulee löytyä kuvaus jokaisesta työvaiheesta.

Tukiasemien sijainnit voidaan merkitä rakennuksen pohjapiirustukseen. Mikäli mahdollista, kannattaa rakennuksesta tehdä kolmiulotteinen malli, johon tukiasemien paikat merkitään. Tämä helpottaa sijaintien hahmottamista.

Tukiasemien tarkat merkit ja mallit tulee laittaa myös dokumentointiin. Sen lisäksi tukiasemakohtaiset asetukset dokumentoidaan. IP-numerot, MAC-osoitteet, sarjanumerot ja tukiasemien nimet kirjataan ylös. Projektiin ostettujen laitteiden kuitit tulee säilyttää, jotta takuu korvaa mahdolliset laiteviat.

Käytössä olevat standardit merkitään dokumenttiin. Mikäli tukiasemat toimivat useilla eri standardeilla, tämän tulee ilmetä myös dokumentaatiosta.

Projektin eri vaiheissa tulee varmasti joitain vastoinkäymisiä. Hankaluudet esimerkiksi tukiasemien konfiguraatiossa ja ongelmien ratkaisut on kirjattava muistiin. Dokumentaation perusteella voidaan myöhemmin lisätä uusi tukiasema verkkoon ilman samoja ongelmia. Dokumentaatioon voidaan laittaa tukiasemien peruskonfiguraatio. Tällöin myöhempien asennusten teko nopeutuu, koska dokumentaation perusteella voidaan toimivin asetus tukiasemaan asentaa.

WLAN-verkon kuuluvuusmittauksien jälkeen tukiasemien kuuluvuusalueet merkitään dokumenttiin. Mikäli uusia asennuksia tehdään välillä, merkitään myös niiden kuuluvuusalueet. Dokumentista voidaan lukea verkon katvealueet. Lisäksi voidaan nähdä se, kuinka kauas verkon signaali kuuluu. Mikäli huomataan, että signaali kuuluu kauas ulkoseinistä, voidaan tukiasemien lähetystehoä säätää pienemmäksi. Näin minimoidaan ulkopuolisen uhan mahdollisuus.

Tietoturvaratkaisut dokumentoidaan. Käytettävät tietoturvaratkaisut ja niiden toteutus kirjoitetaan ylös. Koko dokumentointi kannattaa varustaa kuvilla, koska ne yleensä ovat havainnollisimpia kertomaan, mitä tekstissä tarkoitetaan. (Geier:295; Oraskari 2003: 64)

6. WLAN-VERKON TIETOTURVA

Langattomien verkkojen tietoturvaa pidetään yleisesti ottaen riittämättömänä. Lehdistä ja Internetistä on saatu lukea autoilevista hakkereista, jotka löytävät WLAN-kortilla varustetulla kannettavalla kymmeniä suojaamattomia verkkoja. Tämä johtuu useasti siitä, että verkon asennuksen jälkeen suojaus on jätetty tehdasasetuksiin.

Käytännössä WLAN-verkon saa aina turvalliseksi. Aluksi tulee selvittää tarvittava tietoturvan taso. Kovennetulla WEP-salauksella saadaan jo tarvittava tietoturva suurimpaan osaan yrityksistä. VPN-tekniikalla ja autentikointipalvelimella päästään jo huipputurvalliseen suojauksen tasoon.

Epäusko langattoman verkon turvallisuutta kohtaan johtuu siitä, ettei olemassa olevia tietoturvaominaisuuksia ole otettu käyttöön. Jos vain asennetaan WLAN-tukiasema verkkoon ja kytketään se päälle, on tietoturvasta turha haaveilla. Tietoturva yleensä unohtuu, kun on päästy kaapeleista irti ja verkko toimii muuten moitteetta. Kuitenkin seinien ulkopuolellekin säteilevä suojaamaton verkko kerää kutsumattomia vieraita. (Niemi Juha 2003; Kotilainen 2003: 14)

6.1 Langattoman lähiverkon keskeisiä tietoturva-aukkoja

Tietoliikennettä voidaan salakuunnella: Jokin ulkopuolinen taho kuuntelee yrityksen saapuvaa ja lähtevää dataliikennettä. Yleensä sitä tehdään, jos halutaan saada tietoja, joiden avulla yrityksen verkkoon voisi murtautua. Kuuntelua on mahdollista havaita. Myös sen estäminen on erittäin vaikeasti estettävissä

Tukiaseman kautta pääsee sisään verkkoon: Internetissä jaellaan ilmaisia ohjelmistoja, joilla yleisimmät salausprotokollat voi purkaa. Päästyään WLAN-verkon sisälle, murtautujalla on mahdollisuus päästä myös kaapeliverkkoon.

Ulkopuolinen voi katkaista yhteydet: Kun liikennemäärä verkossa kasvaa, huononee käytettävyys ja verkkoyhteydet voivat katkeilla. Koska WLAN-verkko toimii

vapaalla radiotaajuusalueella, on ainakin periaatteessa mahdollista kuormittaa koko taajuusalue siten, että verkossa ei voi enää liikennöidä. Verkkoa on mahdollista kuormittaa myös jatkuvilla palvelupyynnöillä

Kuka tahansa voi pystyttää tukiaseman: Kun verkkoon on tunkeuduttu, voidaan helposti pystyttää oma tukiasema yrityksen verkkoon. Tukiasemassa voidaan käyttää yrityksen IP-avaruutta, jolloin yrityksen asiakkaat tulevat sisään tämän tukiaseman kautta. (Helin ym. 2002)

6.2 Keskeisimmät suojauskeinot

WLAN-verkkoihin kohdistuu monia erilaisia uhkia. Jotta edellä mainittujen kaltaiset tapaukset voitaisiin estää, tulee tietoturvan taso nostaa perusasetuksista paljon korkeammalle. Huomioon tulee ottaa ainakin seuraavat asiat:

- WEP-salauksen käyttöönotto
- aktiivinen avainten vaihtaminen käytössä
- aina päivitettyjen laitteistojen käyttäminen
- järjestelmän nollaus ainoastaan niiden henkilöiden toimesta, joilla siihen on lupa
- sisäänpääsykohtien huolellinen asettaminen
- ei-käytössä olevien sisäänpääsykohtien poistaminen
- vaikeiden salasanojen asettaminen
- SSID-tunnuksen lähettämisen estäminen
- Vakio SSID (tehdasasetus) poistaminen käytöstä
- radioaaltojen vuodon minimointi rakennuksen ulkopuolelle
- sisäänpääsyn tarkastuksen ottaminen käyttöön
- henkilökohtaisten palomuurien ottaminen käyttöön
- IPSec-pohjaisten VPN:n ottaminen käyttöön kaikissa etäkoneissa
- Staattisten IP-numeroiden ottaminen käyttöön etäkoneissa ja palvelimissa
- epämääräisten kirjautumisten valvominen
- koko WLAN-verkon toiminnan valvominen

(Helin ym. 2002)

6.3 Verkon suojaus

WLAN-kortilla varustettu kannettava tietokone tai kämmenlaite havaitsee automaattisesti tukiaseman läheisyydessä olevan verkon. Tämä johtuu siitä, että tukiasema lähettää jatkuvasti SSID-tunnustaan (Service Set Identifier), jolla eri tukiasemien muodostamat verkot erotetaan toisistaan. Kun tunnus havaitaan, osaa esimerkiksi Windows XP ehdottaa verkkoon liittymistä.

Kun halutaan verkko huomaamattomaksi, ensimmäinen toimenpide on estää verkkotunnusten lähettäminen tukiasemilta. Tämä on mahdollista useimmissa WLAN-tukiasemissa. Tällä yksinkertaisella muutoksella tiputetaan suurin osa avointen verkkojen metsästäjistä pois, koska verkko on näkymätön. Signaalinhaittelijaohjelmilla verkon voi edelleen havaita, mutta se vaatii erityisiä ohjelmia sekä normaalia laajempaa tietämystä asiasta.

Kun verkko on piilotettu, kannattaa verkon nimi muuttaa johonkin vaikeasti arvatavaan, koska valmistajien oletusnimet ovat yleisesti tiedossa. Tukiasemien hallintaliittymien salasanat kannattaa ottaa myös käyttöön, jottei asetuksia päästäisi luvatta muuttelemaan. (Kotilainen 2003:15)

6.4 WEP (Wired Equivalent Privacy)

Kun verkko on saatu piilotettua ja salasanat asetettua, tulee keskittyä varsinaisen tietoliikenteen salakirjoittamiseen eli kryptaukseen. WLAN-verkoissa liikenne salataan WEP-salausta käyttäen. Sitä voidaan käyttää kaikissa Wi-Fi-standardin mukaisissa tukiasemissa ja verkkokorteissa. Salauksen käyttö on helppoa. Kryptaus perustuu tukiaseman hallintaohjelman ja asiakaskoneen verkkoasetuksien salanaan. Näiden perusteella liikenne salakirjoitetaan. Yhden tukiaseman muodostamassa aliverkossa kaikki koneet käyttävät samaa salausavainta.

Alkuperäisenä ajatuksena oli, että WEP-salaus olisi nimensä mukaisesti yhtä turvallinen tietoturvaltaan kuin kaapeliverkkokin. Toteutukseen jäi kuitenkin hieman puutteita. WEP-salauksesta löytyi vakava tietoturva-aukko, joka altisti sen murtamiselle.

WEP:ssä käytetään RC4-salausta, joka on pituudeltaan 64- tai 128-bittistä. Tässä ei itsessään ole vikaa, vaan ongelma on salausalgoritmin yhteydessä käytettävässä aloitusvektorissa. Tämä on standardin mukaan toteutettuna liian heikko. Tietyn tyyppiset aloitusvektorit antavat vihjeitä salausavaimesta. Kun liikennettä seuraa tarpeeksi kauan, voi salausavaimen yksinkertaisesti laskea. Kun WEP-salauksen tietoturva-aukko oli yleisessä tiedossa, ilmestyi Internetiin ilmaisia ohjelmia, jotka automaattisesti suorittivat tämän laskutoimituksen ja antoivat käyttäjälle salausavaimen valmiina.

Salauksen murtaminen ei kuitenkaan ole ihan helppoa. Liikennettä täytyy kerätä yleensä vähintään satoja megatavuja. Tähän saattaa kulua useita viikkoja, mikäli verkkoliikenne ei ole kovin vilkasta. Jos salausavain vaihtuu prosessin aikana, joudutaan kerääminen aloittamaan alusta. Joissakin laitteissa on mahdollista määrittellä useampia WEP-avaimia, jotka vaihtuvat automaattisesti tietyin väliajoin.

Laitevalmistajat alkoivat heti WEP-salauksen aukon paljastuttua korjaamaan ongelmaa. Korjaaminen oli kohtuullisen helppoa, koska se johtui tietyistä aloitusvektoreista, eikä itse salakirjoituksesta. Langattomien laitteiden ohjelmien tai ajureiden salausalgoritmia hieman muutettiin, jolloin heikkojen aloitusvektoreiden syntyminen ehkäistiin kokonaan.

Tiedonsiirron salauksen vahvuus riippuu WLAN-verkossa lähetettävästä laitteesta. Mikäli joukossa on vanhempia sylimikroihin yhdistettyjä verkkokortteja, joissa salausta ei ole, vaikuttaa se vain niiden lähettämään tietoon. Salakuuntelijan työ on erittäin hidasta korjatulla WEP:llä suojatussa verkossa, vaikka joukossa olisivatkin suojaamattomia laitteita. Kun salausavain vielä vaihtuu tietyin väliajoin, voidaan sanoa, että verkko on käytännössä turvallinen. (Niemi Juha 2003; Kotilainen 2003: 15-16)

6.5 Autentikointi

Avoin autentikointi perustuu palvelutunnisteeseen (Service Set Identification). Siinä täytyy päätelaitteella sekä tukiasemalla olla sama palvelutunniste, jotta yhteys voidaan muodostaa. Tässä ei kuitenkaan voida puhua tietoturvasta, koska tukiasema lähettää kokoajan SSID:tä selväkielisenä.

Jaetun avaimen autentikointi on jo turvallisempi. Avainta ei lähetetä selväkielisenä. Siinä käytetään ns. haastemetodia. Tukiasema pyytää asiakaslaitetta salaamaan lähettämänsä viestin, joka tukiasemapäässä sitten puretaan. Mikäli tukiasema huomaa salatussa viestissä olevan palvelutunnisteen olevan saman kuin itsellään, voidaan yhteys muodostaa. (Niemi 2003)

6.6 Standardi 802.1x

Uusi tietoturvaa huomattavasti parantava standardi julkaistiin vuonna 2001. 802.11:een verrattuna suurin edistysaskel oli autentikointi. 802.1x oli toteutettu siten, että uusien ominaisuuksien laajentaminen oli helppoa. Pian siihen lisättiinkin parempi oikeuksien valvonta sekä avainten hallinta.

EAP (Extensible Authentication Protocol) on protokolla, jota käytetään 802.1x:ssä asiakkaan tunnistamiseen. EAP-protokolla tukee radiusta, jossa esimerkiksi avaintenjakoa voidaan suorittaa keskitetysti.

6.7 Autentikointipalvelimet

Suurissa kokonaisuuksissa ongelmaksi saattaa muodostua salausavainten säännöllinen vaihto. Kun vaihdettavia kohteita on vähän, onnistuu salausavainten vaihto käsin. Kun työasemien määrä nousee useisiin kymmeneen, kasvaa ylläpidon työllä liian suureksi. Tähän ongelmaan on ratkaisu 802.1x sekä autentikointipalvelin. Siinä autentikointipalvelin tarkastaa käyttäjätiedot, ennen kuin päästää sallittuihin resursseihin. Todennuksen eli autentikoinnin voi suorittaa esimerkiksi Windowsissa toimiva radius-palvelin (remote authentication dial-in user service), joka tarkastaa käyttäjän tiedot salasanan tai kulkukortin perusteella.

802.1x-standardiin tehtiin laajennus WLAN-verkoille. Siinä WEP-avaimet jaetaan automaattisesti verkkoon kirjautumisen yhteydessä. Mikäli autentikointipalvelin ei tunnista uutta käyttäjää, ei pääsyä resursseihin tule eikä langattomaan verkkoon ole asiaa. Tällainen ratkaisu helpottaa työtä huomattavasti, koska avainten hallinta tapahtuu keskitetysti yhdessä palvelimessa. Lisäksi tietoturva paranee, koska avaimia voidaan helposti vaihtaa huomattavasti useammin. 802.1x:n ongelma on se, ettei sitä suunniteltu alunperin WLAN-perheeseen. Siitä kertoo sen numeroin-
tikin, joka ei ole 802.11-alkuinen. Koska verkkoliikenne on kenen tahansa kuun-
neltavissa, todennusprosessi voidaan kaapata kesken kaiken, jolloin murtautuja
pääsee toisen henkilön varjossa sisään.

802.1x-tekniikalle on tuki suoraan Windows XP:ssä mutta Windows 2000:lle jou-
dutaan ominaisuus asentamaan erikseen. (Yritys-IT 4B/2003: 16-17)

6.8 WPA

Koska WEP-salaus oli joutunut huonoon valoon siinä paljastuneen tietoturva-
aukon takia, joutui Wi-Fi-järjestö kehittämään korvaavaa tekniikkaa. Kehitteillä
oli aivan uusi standardi (802.11i), mutta sen valmistumista ei ollut aikaa odottaa.
Wi-Fi päätti rakentaa välivaiheen standardin, johon sisällytettiin kaikki 802.11i:n
valmiit ja vakaat osat. WPA (Wi-Fi Protected Access) valmistui vuoden 2002
lopulla. WPA on yhteensopiva eteen- ja taaksepäin, eli se toimii hyvin nykyisten
ja tulevien laitteiden kanssa.

WPA on tuotu niin yrityksiin kuin kotienkin ulottuville. Yritysversio perustuu
autentikointipalvelimeen, joka tunnistaa verkon käyttäjän ja jakaa tietokoneille
omat salausavaimet automaattisesti. WPA:ssa ei ole käytössä yhteisiä avaimia,
vaan jokaisella verkon käyttäjällä on käytössään istuntokohtainen salausavain.
Tämä parantaa turvallisuutta huomattavasti. WPA:ssa on käytössä TKIP-salaus
(Temporal Key Integrity Protocol), joka salaa liikenteen RC4-algoritmilla. WEP-
salausavaimien heikot aloitusvektorit on korjattu ja lisäksi salausavainta vaihdetaan
automaattisesti 10 000 paketin välein. Kodeissa ja pienyrityksissä autentikointi-

palvelimen hankkiminen saattaa olla liian suuri investointi. WPA-salausta voidaan kuitenkin käyttää, kun tukiasemalle ja verkkokortille annetaan salasana, joka avaa pääsyn verkkoon. Muilta osin kotiversio on yritysversion veroinen. (Geier 2003; Yritys-IT 4B/2003: 18)

6.9 Standardi 802.11i

WPA oli välivaiheen standardi, jossa oli vain osa 802.11i:n tarjoamia ominaisuuksia. Poisjäänyt ominaisuus on muun muassa RNS (Robust Security Network). Siinä on kaksi avaintenjakomallia; TKIP (Temporal Key Integrity Protocol), joka on suunniteltu jo olemassa olevia järjestelmiä ajatellen sekä CCMP (Counter Mode with CBC-MAC Protocol), jota päästään hyödyntämään vasta tulevaisuissa järjestelmissä. Näiden 802.11i-standardin kahden alemman kerroksen päällä on 802.1x, joka on käsitelty tässä kappaleessa.

Suurin muutos uudessa standardissa koskee salausalgoritmia, joka vaihtuu RC4:stä AES-salaukseen (Advanced Encryption Standard). AES-salausta hoidetaan sille tarkoitettulla prosessorilla, jolloin tiedonsiirron teho paranee. 802.11i:ssä on myös parannettu vertaisverkkojen salausta ja vähennetty verkossa liikkuvaa puhetta sekä videokuvaa haittaavia viiveitä. 802.1x:n ongelma, jossa yhteys saadaan kaapattua, on 802.11i:ssä korjattu. Yhteyden aikana toimii automaattinen avainten vaihto, ja kättelyprosessi tehdään salatusti. Tällöin yhteyden kaappaaminen ei ole mahdollista.

802.1x ja 802.11i eivät yksinään olisi riittävän turvallisia. Niiden yhdistämisen myötä mahdollistetaan vahva salausavainten ja käyttäjätunnusten jako.

Koska uudet 802.11i-standardin laitteet sisältävät uusia rautapuolen ratkaisuja, laitteita on päivitettävä, mikäli haluaa nauttia 802.11i:n tarjoamista parannuksista. Jotkut valmistajat ovat olleet kaukaa viisaita ja tehneet laitteisiinsa mahdollisuuden päivittää vanhat laitteensa uuden standardin mukaiseksi. Käytännössä se tarkoittaa lisäkortin liittämistä vanhoihin laitteisiin sekä ohjelmiston päivitystä.

802.11i valmistuu vuoden 2003 loppupuolella. (Niemi 2003, Yritys-IT 4B/2003: 18)

6.10 VPN

VPN (Virtual Private Network) on erittäin joustava ja turvallinen tapa suojata tietoliikenne. Lähettävässä päässä muodostetaan suojattu tunneli vastaanottavaan päähän julkisen verkon läpi, ja paketit salakirjoitetaan esimerkiksi IPSec-protokollalla (IP Security Protocol). Jotta suojattu tunneli voidaan muodostaa, tulee olla VPN-ohjelmisto. Vastaanottopäähän, ennen yrityksen muuta verkkoa, sijoitetaan VPN-yhdyskäytävä, joka vastaanottaa työasemien salatun liikenteen. VPN-ohjelmistot toimivat lähes kaikkien tietoliikennemuotojen yli, mikä tekee VPN-tekniikasta entistä joustavamman suojaamiseen tarkoitettua tekniikkaa. (Yritys-IT 4B/2003: 18)

7. WLAN-PROJEKTI VAASAN AMMATTIKORKEAKOULUSSA

7.1 Hankkeen taustaa

Palosaaren kampusalueella olevien korkeakoulujen - Vaasan ammattikorkeakoulun, Svenska Yrkeshögskolanin ja Vaasan yliopiston - toimesta on useissa eri yhteyksissä esitetty tarpeita langattoman julkisen verkon toteuttamisesta WLAN-tekniikalla. Vastaavasti Vaasan korkeakoulujen yhteistahot ja sidosryhmät ovat ilmaisseet kiinnostuksensa WLAN-verkon käytölle.

Vastaavasta järjestelmästä voidaan mainita esimerkkinä ammattikorkeakoulun yhteistyökumppanina olevan Fachhochschule Kielin toteuttamana WLAN-verkko Kielin keskustassa. Myös useimmat kampukset Yhdysvalloissa ovat ottaneet langattomat, kannettavat tietokoneet ja PDA-laitteet uusiksi opetusvälineiksi. (Vaasan AMK 2003)

7.2 Hankkeen merkitys alueellisen innovaatiojärjestelmän edistämisessä

Korkeakoulujen alueellisen kehittämisen työryhmän toimenpide-ehdotuksiin sisältyy mm. ehdotuksia Vaasan ammattikorkeakoulujen yhteistyön ja yhteisen koulutarjonnan lisäämisestä. Esitetyllä verkkohankkeella luodaan pohjaa erilaisille käytännön toteutuksille sekä opetusyhteistyön että tutkimuksen ja kehitystyö alueilla. Oleellista on, että uutta yhteyttä Internetiin (tai ISP -palvelua) ei olla hankkimassa, vaan tarkoituksena on muodostaa yhteinen langaton mobiiliverkko, jonka puitteissa Vaasassa toimivien korkeakoulujen opetusta ja tutkimusta, eri yksiköiden yhteistoimintaa sekä virtuaaliyliopiston ja virtuaaliammattikorkeakoulun toimintaa voidaan voimakkaasti vahvistaa lähivuosina. (Vaasan AMK 2003)

7.3 Hankkeen toteuttaminen korkeakoulujen yhteistyönä

Tavoitteena on, että ensimmäisessä vaiheessa Palosaaren kampus-alueella toteutetaan yhteisvoimin kattava ja kaikille osapuolille avoin WLAN-verkko, joka mahdollistaa joustavan työskentelyn koko kampusalueella. Vaihtoehtoisessa tilantees-

sa kaikki eri yksiköt tekevät omia toteutuksiaan, joka koordinoimattomana voi tarkoittaa jopa sitä, että erilliset WLAN-verkot häiritsevät toistensa toimintaa. (Vaasan AMK 2003)

7.4 Mitä hyötyä WLAN-verkko tuo?

Langattomien verkkojen hyötyjä on kerrottu aikaisemmissa kappaleissa. Korkeakouluyhteisössä tilanne on kuitenkin hieman toinen, kun ei haeta rahallisia säästöjä, vaan etsitään niitä keinoja, joilla pystytään parantamaan opetusmetodeja sekä olemaan alan kiihtyvässä kehityksessä mukana.

WLAN-verkko Palosaaren kampus-alueella on omiaan herättämään niin opettajien kuin oppilaidenkin kiinnostusta asiaa kohtaan. On ymmärretty se, että koko ajan ollaan menossa langattomuutta kohden. Myös opetusmetodeille luodaan tähän langattomat toteutusmahdollisuudet. Voidaan puhua ns. mobiilista opiskelusta. Tietokoneilla, jotka ovat kiinteästi kaapeliverkossa, voidaan osallistua opetukseen, mutta langattomuus antaa vapauden liikkua. Ruokala, auditoriot ja muut kaapeli-verkkoa vailla olevat alueet olisivat WLAN-verkon myötä yhtä potentiaalisia opiskelupaikkoja kuin atk-luokatkin. Lisäksi työt voisi viedä mukanaan kannettavan kiintolevyllä. Pienimpiin asioihin, kuten lukujärjestyksen, ruokalistan tai vaikka Winha Willen tarkastamiseen, kävisi myös WLAN-yhteyksillä varustettu PDA-laite.

Tämä kaikki tarkoittaa sitä, että WLAN-yhteyksiä käytettäessä opiskelijoilla itsellään pitäisi olla omat laitteet: kannettava tietokone ja WLAN-kortti. Lähitulevaisuudessa tästä tuskin tulee estettä, koska jo nyt kannettavat ovat kasvattaneet suosiotaan. Nykyisellä suorituskyvyllä niillä voi korvata normaalin käyttäjän pöytäkoneen. Kannettavien ja pöytäkoneiden hinnat ovat lisäksi lähentyneet huomattavasti, joten hintakaan ei ole enää kannettavan tietokoneen hankinnan tiellä.

7.5 Hankkeen aloittaminen

Idea hankkeelle saatiin Tampereelta. Tampereella oli käytössä open-source-toteutus, ja Vaasa päätti ottaa myös käyttöönsä Tampereen tavan.

Hanketta alettiin suunnitella jo vuoden 2002 syksyllä. Vuoden 2003 alkupuolella päätettiin, että WLAN-hanketta aletaan toteuttaa. Projekti oli tarkoitus toteuttaa yhteistyönä Vaasan suomen- ja ruotsinkielisen ammattikorkeakoulun sekä Vaasan yliopiston kanssa. Pedagoginen tiimi suunnitteli langattomalle verkolle käyttötarpeet. Hanke esitettiin opetusministeriölle, joka hyväksyi hankkeen ja alkoi rahoittajaksi.

Ennen teknistä toteutusta tarvittiin tietoa siitä, kuinka helposti langaton lähiverkko on toteutettavissa Palosaaren kampus-alueelle. Päätettiin, että ainakaan alkuvaiheessa ei lähdetä kattamaan verkolla ulkoalueita, vaan keskitytään pelkästään sisätiloihin. Jokainen oppilaitos huolehtisi itse omista asennuksistaan sekä muusta toteutuksesta. Kaikki tieto olisi yhteistä ja projektin eri osapuolten käytettävissä. Projektin edistymistä pohdittiin kaikkien osapuolten yhteisissä kokouksissa.

7.6 Asennukset

Jokainen rakennus on oma yksilönsä, kun suunnitellaan langatonta verkkoa. Eri-laiset rakennusmateriaalit toimivat esteinä tukiasemien kuuluvuudelle. Lisäksi eri tyyppisillä tukiasemilla ja käytetyillä WLAN-korteilla on eroja. Ennen varsinaisia asennuksia olikin testattava eri valmistajien tuotteita. Testiin valittiin muun muassa Cisco-, Linksys-, Orinoco- sekä D-link-merkkisiä tuotteita. Tarkoituksena oli löytää hinta-laatu-suhteeltaan hyvä ratkaisu.

Loppujen lopuksi päädyttiin D-Linkin AirPlus DWL-900AP+ b-standardin mukaisiin tukiasemiin (kuva 12). Niillä oli tarkoitus tarjota yleistä peittoa WLAN-verkolle. Tämän yleistukiaseman valinnassa perusteina olivat edullisuus, tehokkuus sekä käytännöllinen muotoilu. Lisäksi D-linkin eduksi laskettiin antennin vaihtomahdollisuus. Antenni on irrotettavaa mallia, joten siihen voidaan liittää tehokkaampia antenneja kantamaa parantamaan. Tukiasema tarjoaa monipuoliset siltaominaisuudet, joilla voidaan tehdä point-to-point-, point-to-multipoint- ja client-accesspoint-yhteydet.



Kuva 12. D-link DWL-900 AP+ -tukiasema.



Kuva 13. Linksysin WAP54G -tukiasema.

Niille alueille, joissa arveltiin käyttäjämäärän olevan suurin sekä verkon kuormituksen voimakkainta, valittiin Linksysin WAP54G (kuva 13). Paljon verkko-resursseja syöviä paikkoja arveltiin olevan esimerkiksi ruokalan edusta sekä auditoriot. Linksysin tukiasema on 802.11g-standardin mukainen ja tukee näin ollen jopa 54Mbps-nopeutta. Lisäksi tukiasema toimii 2,4GHz:n taajuudella, ja on täysin yhteensopiva b-standardin laitteiden kanssa.

7.6.1 Tukiasemien sijoittelu

Lähtökohtana on aikaan saada mahdollisimman suuri kattavuusalue tukiasemien sijoittelulla. Koska tukiasemien hinta oli halpa, ei niiden määrässä säästely. Niiden paikkoja oli kuitenkin syytä miettiä, koska tukiasema tarvitsee aina toimiakseen verkkovirtaa, sekä runkoverkkoon liittymiseen mahdollistavan kaapelin (Ethernet). Asennuksissa huomattiin, että suurin osa kuluista ei tule itse tukiasemasta, vaan tarvittavan verkkokaapelin sekä virransyötön vetämisestä haluttuun paikkaan.

Tukiasemien asennuksissa tulee ottaa huomioon tietoturva. Kaikki hyökkäykset eivät tule verkon ylitse, vaan murtautuja saattaa olla myös kiinnostunut pääsemään verkkoon kiinnittämällä päätelaitteensa suoraan tukiasemaan. Vaasan

AMK:ssa tukiasemat sijoitettiin suurimmaksi osaksi suojaan. Ainoastaan tukiaseman antenni saattaa olla esillä. Kuvissa on esitelty muutama huomaamaton asennustapa. Ensimmäisessä kuvassa (14) on tukiasema sijoitettu kattorakenteiden yläpuolelle. Antenni on laitettu näkymään ulos rakenteista.



Kuva 14. Tukiasema kattorakenteiden yläpuolella.



Kuva 15. Tukiasema lampun kuvun sisällä.

Toisessa kuvassa (15) tukiasema on asennettu kattolampun kuvun sisään. Kupu on muovia eikä häiritse antennin toimintaa. Näillä ratkaisuilla estetään tukiasemia herättämästä huomiota. Koska asennukset tehtiin pääsääntöisesti kattoon, ovat tukiasemat kohtuullisessa turvassa ulkopuoliselta fyysiseltä uhalta.

Jotta tukiasemien lähettämää signaalia voitaisiin ottaa vastaan päätelaitteella, tarvitaan WLAN-kortti. Testit osoittivat toimivimmaksi kortiksi Orinocon kortit (kuva 16). Orinocon korttien kalliin hinnan vuoksi Vaasan AMK:lle ostettiin lisäksi D-linkin sekä SMC:n WLAN-kortteja. D-linkin kortit ovat toimivia, mutta kuuluvuusmittauksia tehtäessä mittausohjelmat eivät toimineen D-linkin kanssa.

SMC:n kortit toimivat parhaiten, kun ei olla koko ajan liikkeessä. Niissä tukiaseman vaihtaminen lennosta (roaming) ei toiminut toivotulla tavalla. Kun toinen tukiasema olisi ollut voimakkaammin kuultavissa, SMC:n kortti edelleen yritti pitää yhteyttä alkuperäisen tukiaseman kautta. Orinoccon korteissa ei näitä ongelmia ilmennyt.

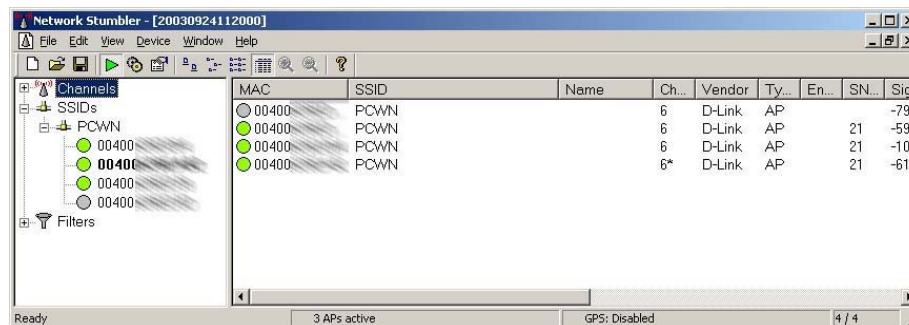


Kuva 16 Orinoccon WLAN-kortti

7.7 Kuuluvuusmittaukset

Olennainen osa tukiasemien sijoittelua on jatkuva kuuluvuuden mittaaminen. Kesän ja syksyn 2003 aikana mittauksia suoritettiin useaan otteeseen. Kesän aikana mittauksilla selvitettiin signaalin kantamaa. Syksyllä, kun kaikki tukiasemat oli asennettu, suoritettiin kattava mittaus. Kuuluvuusmittaus kertoi, tarvittiinko joihinkin paikkoihin lisää tukiasemia vai oliko joissain paikoissa mahdollisesti turhia asennuksia. Asennusten jäljiltä tukiasemat olivat oletuskanavalla 6, joten kuuluvuutta häiritsi myös samalla kanavalla kuuluvat päällekkäiset tukiasemat. Ensimmäisissä mittauksissa tarkasteltiin lähinnä sitä, että tukiasemien signaali kuuluisi joka paikkaan. Sen jälkeen vasta suunniteltaisiin kanavointi. Kanavoinnin tarkoituksena on yhteyden nopeuden optimointi sekä se, että toiset alueella olevat tukiasemat eivät kuuluisi päällekkäin.

Mittauksissa käytettiin kannettavaa tietokonetta, joka oli varustettu Orinocon Silver-kortilla. Se toimi mainiosti mittauksissa käytetyn Netstumbler-ohjelmiston kanssa. Ohjelma kertoi kaikkien kuuluvien tukiasemien käyttämän kanavan sekä signaalin voimakkuuden. Ohjelmasta saattoi myös lukea tukiaseman käyttämän kanavan. Orinocon WLAN-kortin toimivasta roaming-ominaisuudesta johtuen pystyimme kulkemaan taukoamatta ympäri rakennusta, ja lukemaan sillä hetkellä parhaiten kuuluvan tukiaseman voimakkuuden. Mittauksessa selvisi myös tietyssä paikassa yhtäaikaan kuuluvat tukiasemat. Mittauksien tulokset merkittiin rakennuksen pohjapiirustukseen. Tämä tieto helpotti myöhemmin tehtyä tukiasemien kanavointia. Mittauksia tehdessä löytyi myös muutamia paikkoja, joihin signaali ei kuulunut tai kuului niin heikosti, ettei tiedonsiirtonopeus riittänyt tavalliseen työkentelyyn.



Kuva 17. Netstumbler-ohjelmanäkymä.

Vaasan ammattikorkeakoulu koostuu kolmesta osasta. Langattoman verkon tuli kattaa Vaasan AMK:n kaikkien rakennuksien sisätilat. Tulokset merkittiin aluksi kynällä ja luotiin karkea kuva verkon kattavuudesta. Kuvasta ilmeni muutamia katvealueita, jotka korjattiin uusilla asennuksilla. Myöhemmin kuuluvuuskriteerinä pidettiin sitä, että ainakin kaikista luokista piti pystyä muodostamaan VPN-tunneli. VPN-tunnelin muodostaminen tarvitsee erittäin hyvän verkkoyhteyden.

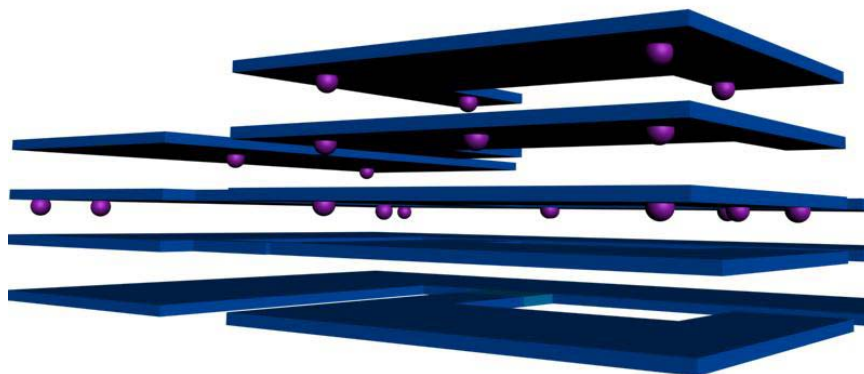
7.8 Tukiasemien kanavointi

Kuuluvuusmittaukset olivat suuntaa antavia. Kuva ei kuitenkaan ollut aivan todellinen, koska kaikki tukiasemat toimivat samalla kanavalla ja häiritsivät toistensa toimintaa. Oli tehtävä suunnitelma tukiasemien kanavoinnista.

Kanavia on Euroopassa käytössä 13. Kun samalla kuuluvuusalueella kuuluu useita tukiasemia, saadaan paras tulos kun käytetään kanavia 1,7 ja 13. Nämä kanavat eivät mene toistensa kanssa päällekkäin. Tukiasemien kanavien väliin tulisi kuitenkin jättää vähintään kaksi tyhjää kanavaa. Tukiasemien kanavien varaamisesta on kerrottu tarkemmin kappaleessa 3.4

Pohjana tukiasemien kanavointiin käytettiin mallia 1,5,9 ja 13. Mittaustuloksien lukeminen oli hankalaa pohjapiirustuksista. Jotta saatiin havainnollisempi kuva tukiasemien sijainnista, tehtiin koulun pohjapiirustuksien perusteella karkea 3-ulotteinen malli koulun kaikista osista. Tukiasemien sijainnit pystyttiin lukemaan kuvasta. Koska tukiasemat kuuluivat lattioiden ja seinien läpi, auttoi 3-ulotteinen malli huomaamaan erittäin pahasti päällekkäin kuuluvat tukiasemat. Apuna käytettiin

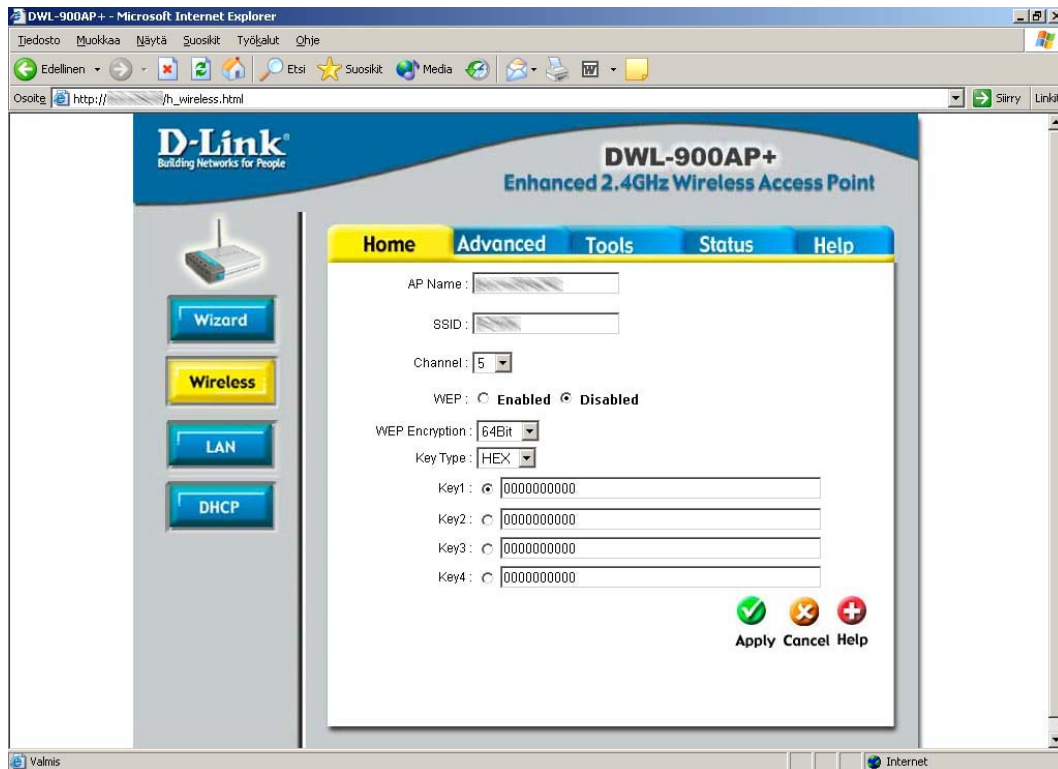
tettiin myös mittauksissa saatuja tuloksia. Koska tukiasemia asennettiin välillä lisää, tehtiin kanavointisuunnittelukin kahteen kertaan.



Kuva 18. Karkea 3-ulotteinen malli koulusta ja tukiasemista.

7.8.1 Kanavien konfigurointi tukiasemiin

Itse uudelleenkanavointi suoritettiin verkon yli. Tukiaseman hallintaohjelmistoon pääsi käsiksi selaimella. Osoiteriville laitettiin tukiaseman IP-numero. Hallintaohjelma kysyi käyttäjätunnuksen ja salasanan, jonka jälkeen oli mahdollisuus muuttaa tukiaseman asetuksia. Kanavanvaihto onnistui helposti alasvetovalikosta, josta valittiin kanava, jota tukiaseman tuli käyttää. Sen jälkeen otettiin käyttöön uudet asetukset. Tukiasema käynnisti itsensä automaattisesti uudestaan ja oli tämän jälkeen toimintakunnossa. Tämä osa kanavoinnista oli erittäin helppo ja nopea toteuttaa.



Kuva 19. D-linkin hallintaohjelma.

7.9 Tietoturva Vaasan AMK:ssa

Vaasassa Palosaaren kampus-alueen WLAN-verkon tietoturva vietiin korkealle tasolle. Kaikille oppilaille annetaan mahdollisuus käyttää Internet-yhteyttä vapaasti omilla tunnuksillaan. Käyttäjät tunnistetaan autentikointipalvelimella, jossa toimii oasis.

7.9.1 Oasis

Oasis on StocholmOpen:in kehittämä ohjelma, joka toimii Linux-ympäristössä. Alkuperäinen oasis jouduttiin koulun omien työntekijöiden toimesta muokkaamaan Vaasan ammattikorkeakoululle sopivaan malliin. Koska kyseessä oli avointa lähdekoodia käyttävä ohjelma, olivat tehdyt muutokset täysin sallittuja ilman erillisiä sopimuksia. Alussa ongelmat olivat järjestelmän kaatuilu. Kun oasisista oltiin muokattu saatiin pahimmat ongelmat korjattua, mutta edelleenkin se ei ollut tyydyttävä ratkaisu. (StockholmOpen.net 2002)

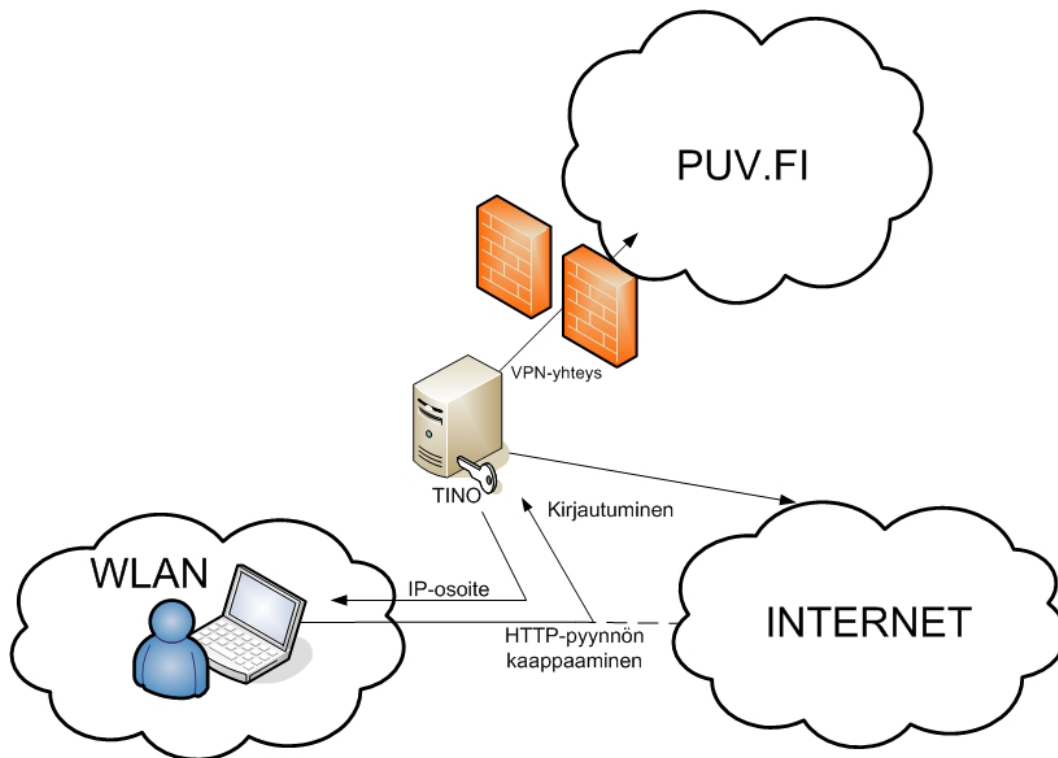
7.9.2 Tino (This is not oasis)

Oasiksen toiminnan osoittauduttua epävakaaksi useiden päivityksien jälkeenkin, päätettiin kirjoittaa oasis kokonaan uudelleen. Haasteen otti vastaan Vaasan ammattikorkeakoulun Hannu Teulahti. Hänen ja Vaasan yliopiston Hannu Hirvosen ideoimana syntyi Tino-niminen (This is not oasis) pääsynvalvonta-palikka. Tino toteuttaa ne osat oasisesta, mitä koulujen WLAN-projektissa tarvitaan ja toimii vakaasti, ilman ongelmia.

Tino tarjoaa web-pohjaisen kirjautumissivun. Se tulee esille, kun käyttäjä tulee WLAN-kuuluvuusalueelle ja lähettää HTTP-pyyntöä. Pyyntö kaapataan ja käyttäjä ohjataan kirjautumissivulle.

Tino hoitaa myös käyttäjien autentikoinnin PAM:ia (Pluggable Authentication Modules) hyväksikäyttäen sekä IP-osoitteiden jakamisen WLAN-asiakkaille DHCP-palvelimen avulla. Tino tallentaa asiakkaiden MAC- eli fyysiset osoitteet levypohjaiseen tiedostojärjestelmään.

Autentikoinnin jälkeen on pääsee Internetiin. Jos halutaan käyttää koulun sisäverkkoa, täytyy muodostaa VPN-tunneli. Mikäli päätelaite ei uusi DHCP-leasiaan 5 minuutin sisällä, suljetaan yhteys. (Pitkäranta 2003, StockholmOpen.net 2002)



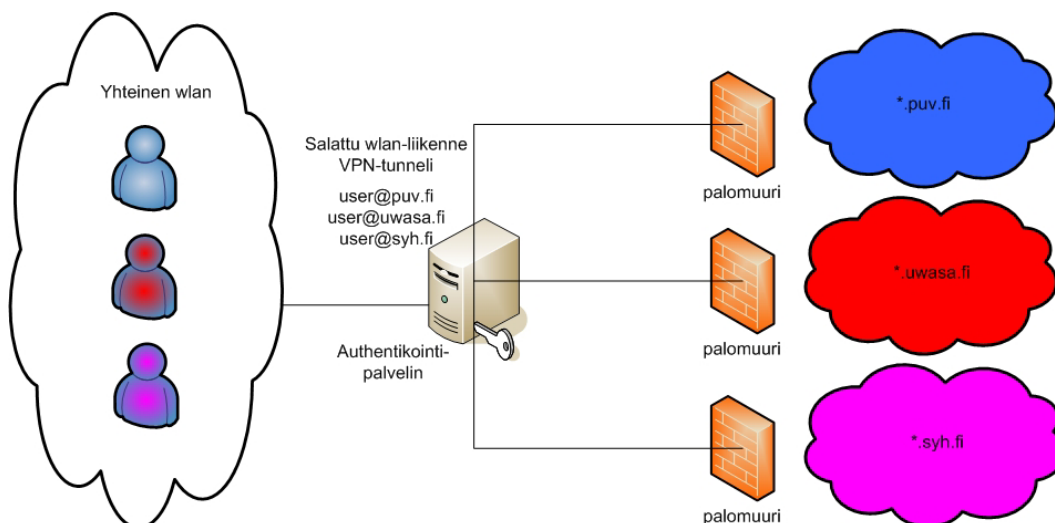
Kuva 20. Tinon toiminta.

7.9.2 WLAN yhteyden avaaminen

Kun käyttäjä tulee Vaasan kampus-alueen WLAN-verkon kuuluvuusalueelle, kaapataan hänen HTTP-pyyntönsä ja käyttäjä ohjataan kirjautumissivulle. Käyttäjä kirjautuu omalla tunnuksellaan, ja sen lisäksi hänen täytyy laittaa @-merkki ja toimialue, johon hän kuuluu. Lisäksi hän tarvitsee salasanan, jotta kirjautuminen onnistuu. Tämän jälkeen Internetin selaaminen on mahdollista.

7.9.3 VPN

Mikäli opiskelija haluaa käyttää koulun intranetiä, tulee hänen muodostaa VPN-tunneli koulun palvelimeen. Yhteyden muodostamiseen Vaasan kampus-alueella suositellaan cison VPN-clienttiä. Käyttäjä ottaa yhteyden osoitteeseen vpn.puv.fi. Tämän jälkeen häneltä kysytään vielä hänen unix-tunnuksensa. Yhteyden muodostamiseen tarvitaan erittäin voimakas verkon kuuluvuus. VPN-tunnelia käytettäessä kaikki liikenne on vahvasti salattua.



Kuva 21. Vaasan kampus-alueen WLAN-verkko.

7.10 Valmis WLAN-verkko

Kun WLAN-verkko oli toteutuksen puolesta valmis, järjestettiin testausviikko. silloin kaikki halukkaat, jotka omistivat sopivan päätelaitteen, pääsivät mukaan testaukseen. Koulu tuki testausta tarjoamalla maksutta WLAN-kortteja. Yhteensä testiin osallistui noin 30 henkilöä. Testi onnistui hyvin. Järjestelmä toimi koko testiviikon ajan. Suurin piikki ajoitettiin 6. päivään lokakuuta, jolloin melkein kaikki 30 henkilöä oli yhteydessä langattomaan verkkoon yhtä aikaa. Silloinkaan ongelmia ei havaittu. Testiin osallistuneille henkilöille lähetettiin palautelomake, johon vastanneet saivat kertoa kokemuksiaan testistä. Kyselyyn merkittiin muun muassa se, mistä yhteys oli testin aikana muodostettu ja oliko verkko toiminut. Pääsääntöisesti vastaukset olivat positiivisia. Yhteys oli saatu muodostetuksi ja yhteyden laatuun oltiin oltu tyytyväisiä.

WLAN-verkko julkistettiin virallisesti 31. lokakuuta, jolloin julkistamistilaisuuteen saapui paikalle myös tiedotusvälineiden edustajia. Tiedotusvälineiden lisäksi paikalla oli muiden vastaavien projektien isäntiä ja teknisiä toteuttajia Tampereelta, Turusta ja Oulusta. Virallisemmän tiedotustilaisuuden jälkeen eri kaupunkien edustajat jatkoivat kokouksen merkeissä tilaisuutta.

Kokouksen pääaiheena oli esitellä muiden kaupunkien WLAN-toteutuksia. Tilaisuudessa jaettiin myös kokemuksia projektien eri vaiheista. Kokouksessa kerrot-

tiin myös erilaisia odotettavissa olevia visioita. Erään vision mukaan WLAN kat-
taa tulevaisuudessa koko maan.

Kokouksessa keskusteltiin paikalla olevien tahojen kanssa mahdollisuudesta
verkkovierailuun. Tämä tarkoittaisi sitä, että esimerkiksi Vaasassa opiskeleva
opiskelija voisi mennä käymään Oulun kampus-alueella ja kirjautua paikalliseen
WLAN-verkkoon omilla tunnuksillaan ilmaiseksi. Tämä kaikki tarkoittaisi ristiin
autentikointia, jolloin voitaisiin yhdistää autentikointipalvelimien tietoja ja vaihtaa
keskenään yhteyksiä eri osapuolten kanssa. Mikäli projektiin saataisiin osallistu-
maan kouluja tarpeeksi, voitaisiin olla minkä oppilaitoksen WLAN-verkon kuulu-
vuusalueella tahansa ja kirjautua järjestelmiin sisään ilman erillisiä verkkovierai-
lusopimuksia.

7.11 WLAN – onnistunut projekti?

Kun projekti on ohi ja verkko toiminnassa on aika tarkastella työn tuloksia. Ko-
konaisuutena voidaan sanoa, että projektissa saavutettiin tavoitteet. WLAN-
verkko toimii kaikissa mukana olleissa yksiköissä. Langaton verkkoyhteys voi-
daan muodostaa koulujen sisätiloissa mistä tahansa. Tietoturvan puolesta projekti
oli myös menestys. Projektin aikana luotu Tino-niminen käyttäjätunnistus on
osoittautunut vakaaksi ja toimivaksi ratkaisuksi. Arvoa lisää entisestään se, että
Tino on koulun voimin luotu. Käyttäjien autentikoinnin lisäksi VPN-tunneli kou-
lun sisäverkkoon toimii.

8. YHTEENVETO

WLAN-ratkaisut ovat kasvattaneet suosiotaan. Tähän on syynä parantunut tietoturva sekä mahdollisuudet, joita WLAN tarjoaa verrattuna tavalliseen kaapeliverkkoon.

Ehkä tärkein WLAN:n tarjoama etu on mahdollisuus liikkuvuuteen ilman katkoksia. Teoriassa tämä kaikki toimii hienosti, mutta todellisuudessa näin ei aina ole. Esimerkiksi eri valmistajien WLAN-korteissa ja tukiasemissa on joitakin yhteensopivuusongelmia, jotka estävät roaming-ominaisuuden toimimisen kunnolla. Tämä todettiin kuuluvuusmittauksia tehdessä Vaasan ammattikorkeakoulussa. Siellä jouduttiin käyttämään tietyn valmistajan WLAN-korttia, jotta yhteys säilyi vaikka liikuimme solusta toiseen kävelynopeudella.

WLAN on tavallista kaapeliverkkoa edullisempi ratkaisu. Säästöt tulevat siitä, ettei yksittäisille tietokoneille tarvitse vetää omaa kaapelia. WLAN-verkkoon tarvitaan tukiasemalle Ethernet-kaapeli sekä virransyöttö. Päätelaitteeseen tarvitaan WLAN-kortti. Tukiasemat ja langattomat verkkokortit ovat halpoja. Suurimmat kustannukset tulevatkin yleensä tukiasemalle vedettävistä Ethernet- ja virtakaapeleista. Koska tukiasemien ja päätelaitteiden välinen liikenne on toteutettu langattomasti, voidaan WLAN-ratkaisu toteuttaa sellaisiin paikkoihin mihin se on aiemmin ollut hankalaa tai jopa mahdotonta.

Vaikka WLAN-verkossa on huonojakin puolia, mikään niistä ei ole ylitsepääsemätön este langattoman verkon toimimiselle. Mikäli laitteet ovat yhteensopivia ja häiriölähteet on huomioitu, toiminnan kannalta WLAN-verkko on hyvä ratkaisu runkoverkon jatkeena.

WLAN-verkon tietoturvaa pidetään yleisesti huonona. Tämä johtuu siitä, ettei kaikkia suojaustoimenpiteitä ole otettu käyttöön. Langattoman verkon tietoliikennettä voidaan salakuunnella ja tätä on lähes mahdoton havaita. Tukiaseman kautta voi kuka tahansa päästä sisään verkkoon tai ulkopuolinen voi katkaista yhteydet.

Mikäli suojaus ei ole kunnossa, mahdollistaa se oman tukiaseman lisäämisen ilman lupaa. Nämä ovat keskeisimmät tietoturva-aukot, jotka suojaustoimenpiteitä suunniteltaessa tulee ottaa huomioon.

Ensimmäinen suojaustoimenpide on verkkotunnusten lähettämisen estäminen. Kovennetulla WPA-salauksella saadaan jo usein tarvittava tietoturva. Jotta avainten jako olisi helpompaa, kannattaa myös autentikointipalvelin (802.1x) ottaa käyttöön. Tietoliikenne saadaan salatuksi, jos vielä käytetään VPN-tekniikkaa.

Vaasan ammattikorkeakoulussa WLAN-verkko on kaikkien opiskelijoiden ja henkilökunnan käytettävissä. Haluttu tietoturva saavutettiin Tino-nimisellä ohjelmistolla ja autentikointipalvelimella. Liikennöinti tapahtuu koko ajan koulun palomuurin ulkopuolella. Mikäli yhteys sisäverkkoon halutaan, muodostetaan VPN-tunneli. Ammattikorkeakoulun tapauksessa tietoturva on saatu halutulle tasolle. Ongelmia ei ollut osiksen uudelleenkirjoittamisen jälkeen. Tämä on erittäin joustava ratkaisu ja esimerkillinen toteutus ajatellen kouluolosuhteita.

Tällä hetkellä tietoturvan taso saadaan korkealle. Kuitenkin joitain aukkoja tietoturvassa on. WPA:ta tulee seuraamaan vuoden 2003 lopussa ilmestytävä 802.11i, jossa on WPA:sta pois jääneet ominaisuudet. 802.11i kokoaa aiempien standardien tietoturvaominaisuudet ja voi olla erittäin merkittävä askel eteenpäin. Tällöin nähdään, saavutetaanko parannuksia langattoman verkon tietoturvassa ja saadaanko aiemmat ongelmat korjatuksi.

LÄHTEET

Geier, Jim 2003. WPA plugs holes in WEP [online]. Network World Fusion. Saatavilla www-muodossa:

<<http://www.nwfusion.com/research/2003/0331wpa.html>>

Geier, Jim 1999. Wireless LANs: Implementing interoperable networks. 1.painos. Macmillan Technical Publishing

Granlund Kaj 2001. Langaton tiedonsiirto. 1.painos. Porvoo. Docendo Finland Oy.

Helin, Karttunen, Pitkänen 2002. WLAN ja tietoturva [online]. Seminaarityö, Turun kauppakorkeakoulu. Saatavilla www-muodossa:

<www.tukkk.fi/tjt/OPETUS/TJTS11/Arkisto/wlan.pdf>

Huopalainen, Kerkelä, Paakki, Salminen 2001. Siirtyvä tietoliikenne: WLAN [online]. Seminaarityö, Lappeenrannan teknillinen korkeakoulu. Saatavilla www-muodossa: <<http://www.it.lut.fi/opetus/00-01/010651000/doc/wlan.pdf>>

Juutilainen, Matti. Siirtyvä Tietoliikenne: Langaton lähiverkko[online].

Saatavilla www-muodossa:

<http://www.it.lut.fi/opetus/0102/010651000/luennot/1651_wlan.pdf>

Kuokka, Henri 2002. WLAN vyöryy verkkoihin. Mobiili-IT 10B/2002 s.10-19. Forssa: Sanoma Magazines Finland Oy.

Pitkäranta, Timo 2003. Mobiilipalvelut-seminaari : Palosaari campus wireless network. Vaasa

Niemi Juha 2003. WLAN-turvallisuus [online]. Seminaarityö, Helsingin yliopisto. Saatavilla www-muodossa:

<http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf>

Seppänen, Lasse. Langaton lähiverkko: Wireless Local Area Network (WLAN) IEEE 802.11 [online]. Saatavilla www-muodossa:

<<http://trade.hamk.fi/~lseppane/courses/wlan/doc/Materiaali.pdf>>

StockholmOpen.net 2002 [online]

<<http://software.stockholmopen.net/>>

Oraskari, Jyrki 2003. Katveet peittoon. Tietokone 5/2003 s.62-64. Forssa. Sanoma Magazines Finland Oy.

Kotilainen, Samuli 2003. Turvaa WLAN-verkkosi. Kotilainen 2003 s,14-19. Forssa Sanoma Magazines Finland Oy.

Vaasan ammattikorkeakoulu 2003 [online].

<<http://www.wlan.puv.fi>>

The wireless lan association 2002. Wireless networking standards and organizations [online]. Saatavana www-muodossa:

<http://www.wlana.org/pdf/wlan_standards_orgs.pdf>