TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Tutkintotyö

Petri Leskinen

SULJETTU WLAN TIETOLIIKENNELABORATORIOON

Tutkintotyö, joka on jätetty opinnäytteenä tarkastettavaksi Petri Leskisen insinöörintutkintoa varten Tampereella 2.5.2007.

Työn valvoja: Ari Rantala
Tampere 2007

TAMPEREEN AMMATTIKORKEAKOULU

Tekijä: Petri Leskinen
Työn nimi: Suljettu WLAN tietoliikennelaboratorioon

Päivämäärä: 2.5.2007
Sivumäärä: 38 sivua ja 6 liitesivua
Hakusanat wlan, langaton, IEEE 802.11, Wi-Fi
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: Lehtori Ari Rantala

TIIVISTELMÄ

Langattomat lähiverkot (WLAN) ovat lisääntyneet huomattavasti joko itsenäisinä verkkoina tai perinteisten, kaapeloitujen verkkojen jatkeina. Langattomuus mahdollistaa laitteiden liikuteltavuuden ja tietoliikenneyhteydet paikkoihin, mihin kaapelointia ei mahdollisesti saada vedettyä.

Langattomat verkot perustuvat IEEE 802.11-standardiin. Alkuperäinen standardi sertifioitiin vuonna 1997. Standardia on paranneltu useilla lisäyksillä, joilla on pyritty parantamaan siirtonopeuksia ja tietoturvaa. Tuleva standardi, 802.11n, pystyy jo teoreettiseen 250+ Mb/s bittinopeuteen.

Tässä työssä on pyritty tutkimaan langattomuuden perusominaisuuksia ja lähiverkon konfigurointia. Langattomuus voidaan toteuttaa joko radiotaajuus- tai infrapunatekniikkaa käyttäen. Tässä työssä perehdytään vain radiotaajuustekniikkaan.

Työn tarkoituksena on ollut langattoman lähiverkon suunnittelu ja rakentaminen Tampereen ammattikorkeakoulun tietoliikennelaboratorioon. Laboratoriosta puuttuu mahdollisuus tutkia langattoman lähiverkon tietoliikennettä, joten lähiverkkoa tullaan käyttämään opetuskäytössä.

Langattomuus on tulevaisuutta, joten opetuspistettä tullaan kehittämään jatkossa: tutkittavaksi voidaan ottaa mm. bluetooth- ja infrapunatekniikat sekä uuden sukupolven matkapuhelimia.

TAMPERE POLYTECHNIC - UNIVERSITY OF APPLIED SCIENCES

Author:	Petri Leskinen
Name of the thesis:	Restricted WLAN to telecommunications laboratory
Date:	2.5.2007
Number of pages:	38 pages and 6 appendices
Keywords:	wlan, wireless, IEEE 802.11, Wi-Fi
Degree programme:	Computer systems engineering
Specialisation:	Telecommunication engineering
Supervisor:	Senior lecturer Ari Rantala

ABSTRACT

Wireless LANs (WLAN) have become hugely popular as an extension or as an alternative to a traditional, wired LAN. Wireless enables the possibility of freely movable devices and they can work where cabling is not possible.

Wireless LANs are part of IEEE's 802.11 standard. The original version of the standard was released in 1997, and nowadays there are several amendments to the original standard, which have improved security and data rates. The upcoming standard, 802.11n, will offer theoretical data rate of 250+ Mb/s.

In this thesis, there is knowledge about the basic properties of WLAN and its configuration. WLAN devices use radiofrequency techniques or infrared. In this case, only radiofrequency techniques have been used.

The main purpose of this thesis is to design and build a wireless LAN in to the telecommunications laboratory of Tampere Polytechnic. There has not been a place to examine wireless telecommunications regarding WLANs, so it will be used to educational purpose.

Wireless is the future, so education space will be developed: there can be an extension for bluetooth, infrared or for 3G-mobile phones.

ALKUSANAT

Työ on tehty kevään 2007 aikana Tampereen ammattikorkeakoulun tietoliikennelaboratorioon. Kiitän perhettäni tuesta sekä Ari Rantalaa ja Jorma Punjua ohjauksesta opintojen aikana.

Tampereella 2. toukokuuta 2007

Petri Leskinen

KÄYTETYT LYHENTEET

AES	Advanced Encryption Standard, lohkosalausmenetelmä
AP	Access Point, tukiasema
BPSK	Binary Phase Shift Keying
CCK	Complement Code Keying
DSSS	Direct-sequence spread spectrum, suorasekvenssi (hajaspektri)
FHSS	Frequency-hopping spread spectrum, taajuushyppely (hajaspektri)
HR/DSSS	High Rate Direct-sequence spread spectrum
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical, lisenssivapaa taajuusalue
LAN	Local Area Network, lähiverkko
MAC	Media Access Control
MIC	Message Integrity Control
OFDM	Orthogonal frequency-division multiplexing, ortogonaalinen taajuusjakoinen kanavointi
OSI	Open Systems Interconnection
PSK	Pre-shared Key
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wireless Fidelity Protected Access

SISÄLLYSLUETTELO

1 JOHDANTO

Tässä työssä on tutkittu langatonta lähiverkkoa (Wireless LAN, WLAN) ja sen ominaisuuksia. Työ on tehty Tampereen ammattikorkeakoulun tietoliikennelaboratorioon kevään 2007 aikana. Työn rakenne seurailee Tampereen ammattikorkeakoulun tekniikan ja metsätalouden koulutusohjelmien tutkintotyöohjetta.

Johdannon jälkeisessä luvussa käsitellään langattoman verkon tekniikoita ja ominaisuuksia. Kolmannessa luvussa perehdytään IEEE:n historiaan ja standardeihin. Neljännessä luvussa tarkastellaan verkon salausta ja tietoturvaa yleisellä tasolla. Viidennessä luvussa tutustutaan itse verkon rakentamiseen ja konfigurointiin. Lopuksi pohditaan tuloksia ja mahdollisia parannusvaihtoehtoja.

1.1 Toimeksianto

Tietoliikennetekniikan koulutusohjelman vastaava, Ari Rantala, määritteli minulle aiheen tietoliikennelaboratorion tarpeiden mukaan. Laboratoriotiloista puuttui mahdollisuus tutustua langattomaan lähiverkkoon, joten tutkintotyönäni minun tuli rakentaa ja kuvata opetustarkoitukseen tarkoitettu suljettu, neljän koneen langaton lähiverkko. Työssä tutkin myös langattomuuden tietoturvaa ja verkon muita ominaisuuksia. Tarvittavan laitteiston - tietokoneet, verkkokortit ja tukiaseman - määrittelin ja tilasin itse.

1.2 Tavoitteet

Tutkintotyön tavoitteena on tutustua langattoman verkon tekniikoihin ja rakentaa toimiva lähiverkko. Päätavoitteena on määritellä ja toteuttaa tietoliikennelaboratorion vaateita vastaava opetuspiste, missä opiskelijat voivat tutustua langattomuuden ominaisuuksiin. Opetuspisteen mahdolliset laajennukset on otettava huomioon.

2 LANGATTOMUUDEN OMINAISUUDET

Langattomuus on yleistynyt viime aikoina huomattavasti. Laitteiden hinnat, tekniikat ja tietoturva ovat parantuneet, joten langattomuus haastaa perinteisen kaapeloidun tietoliikenteen. WLANit toimivat jatkeena tai vaihtoehtona perinteiselle, langalliselle lähiverkolle. WLAN lähettää ja vastaanottaa dataa joko infrapuna- tai radiotaajuustekniikkaa käyttäen. Tässä työssä keskitytään radiotaajuustekniikkaan.

2.1 ISM-taajuusalue

ISM-taajuusalue (Industrial, Scientific and Medical) on lisenssivapaa radiotaajuuskaista. Sitä käyttävät yleisesti useat laitteet ja radiotekniikat, kuten mikroaaltouuni, bluetooth ja osa satelliiteista. ISM-kaistoja on kolme, joista WLAN käyttää kahta aluetta: 2,4 GHz:n ja 5 GHz:n. Taulukossa 1 on esitelty tarkemmin WLANin käyttämiä ISM-taajuuksia. Euroopassa on myös maiden välillä pieniä eroja taajuusalueiden käytössä.

Taulukko 1 ISM-taajuusalueet vaihtelevat hieman maanosittain

Eurooppa	USA	Japani
2,4 - 2,4835 GHz	2,4 - 2,4835 GHz	2,4 - 2,4835 GHz
5,15 - 5,35 GHz	5,15 - 5,35 GHz	5,15 - 5,25 GHz
5,470 - 5,725 GHz	5,725 - 5,825 GHz	-

ISM-taajuusalueella signaalin maksimikantomatka on yritetty rajoittaa lähetystehoilla 100 metriin, mutta käytännössä ylityksiä tapahtuu. Normaalisti ilmassa oleva vesi (sumu) absorboi radioaaltoja, mutta ilman ollessa erittäin kuivaa signaalin kantama pitenee. Taulukossa 2 on esitelty Suomen kansalliset määräykset 802.11-laitteille.

Taulukko 2 Suomen kansalliset määräykset 802.11-standardin laitteille /3/

WLAN-standardi	Taajuusalue	Kanavat	EIRP-teho	Käyttökohteet
802.11	2,4 GHz	1…13	100 mW	sisä- ja ulkotiloissa
802.11b	2,4 GHz	1…13	100 mW	sisä- ja ulkotiloissa
802.11g	2,4 GHz	1...13	100 mW	sisä- ja ulkotiloissa
802.11a	5,15 - 5,25 GHz	36, 40, 44, 48	200 mW	vain sisätiloissa
802.11a	5,25 - 5,35 GHz	52, 56, 60, 64	200 mW	vain sisätiloissa

EIRP-teho lasketaan seuraavan kaavan mukaisesti:

EIRP = (lähetysteho – siirtolinjahäviö) + (antennivahvistus)

Tässä tapauksessa tehot on ilmoitettu watteina, mutta yleisesti ne ilmoitetaan desibelisinä arvoina. Muutos voidaan laskea seuraavan kaavan mukaisesti:

$$P\,[\mathrm{dBm}] = 10\log_{10}\frac{P_{EIRP}}{1\,\mathrm{mW}}$$

2.2 Signaaliin vaikuttavat tekijät

Langattomat lähiverkot käyttävät tiedonsiirrossa radiotaajuustekniikkaa, ts. informaatio kulkee signaalina ilmoitse. Tästä syystä WLAN on alttiimpi häiriölle kuin perinteinen kaapeloitu lähiverkko. Signaali kärsii mm. vaimennuksesta, monitie-etenemisestä ja heijastuksesta. Myös muut langattomat verkot ja ISM-taajuusalueen laitteet voivat häiritä signaalia.

Vaimennus

Signaali vaimenee edetessään ilmassa tai muussa väliaineessa. Vaimennus pienentää signaalin amplitudia ja tehoa. Vaimennukseen vaikuttavat signaalin taajuus, väliaineen ominaisuudet ja etäisyys. Vapaan tilan vaimennus voidaan laskea kaavasta:

$$L[\mathrm{dB}] = 92{,}45 + 20\log_{10}(f\,[\mathrm{GHz}]) + 20\log_{10}(d[\mathrm{km}])$$

missä f on taajuus gigahertseinä ja d etäisyys kilometreinä.

Vapaan tilan vaimennuksen kaavaa voidaan käyttää vain, jos lähettimen ja vastaanottimen välissä on esteetön näkyvyys. Yleisesti signaalin etenemiseen vaikuttavat kaikki tilassa olevat objektit mukaan luettuna ihmiset. Taulukossa 3 on esitelty muutamien tunnettujen väliaineiden vaimennuksia.

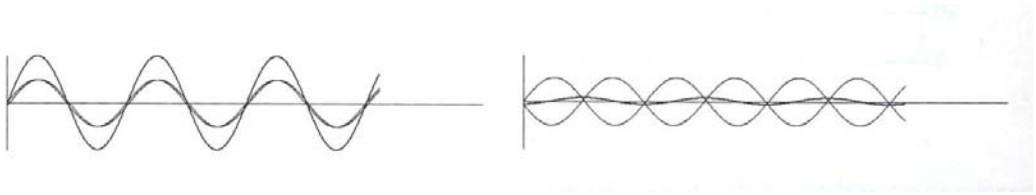
Taulukko 3 Väliaine vaikuttaa signaalin vaimenemiseen /10/

Materiaali	Vaimennus
Betoni 25cm (isot ikkunat)	4 dB
Betoni 25cm (ei ikkunoita)	11 dB
Betoni 10cm (väliseinä)	6 dB
Lasi	2 dB
Lasi (metallivahvisteinen)	8 dB

Etäisyys päätelaitteen ja tukiaseman välillä vaikuttaa maksimisiirtonopeuteen: mitä pitempi etäisyys, sitä matalampi bittinopeus. Vaimennus lisää virheitä ja tästä syystä suuret siirtonopeudet eivät ole mahdollisia, jos etäisyys on suuri. Kappaleessa 5.3 on käsitelty aihetta enemmän.

Kahden aallon interferenssi

Samantaajuiset aallot voivat vaikuttaa toisiinsa. Jos signaalit ovat lähes samanvaiheisia, ne voivat vahvistaa toisiaan, kuten kuvan 1 vasemmanpuoleisessa esimerkissä. Jos taas signaalit ovat erivaiheisia, kuten kuvan 1 oikeanpuoleisessa esimerkissä, on niiden summa-aalto hyvin pieni. Tätä tapahtumaa kutsutaan häipymiseksi. /3/

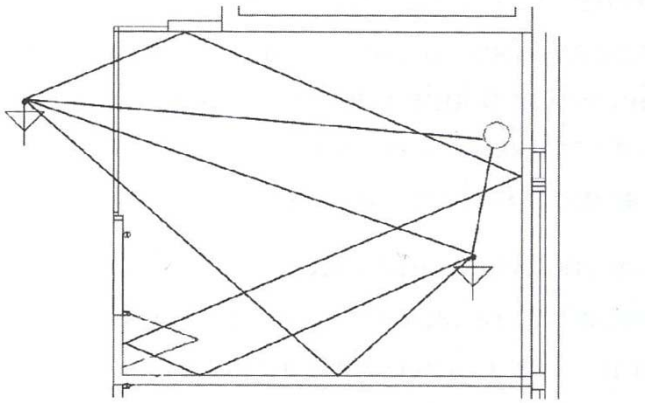


Kuva 1 Kahden signaalin vaikutus toisiinsa /3/

Heijastus ja monitie-eteneminen

Heijastuminen tarkoittaa signaalin etenemissuunnan muutosta. Sen voivat aiheuttaa joko maanpinnan muutokset tai ihmisen tekemät esteet, kuten seinät. Heijastuminen tapahtuu signaalin osuessa sopivassa kulmassa väliaineeseen. Väliaineen rakenne ja signaalin tulokulma määrittelevät heijastuksen määrän ja siitä syntyvän vaimennuksen. Osa signaalista voi tunkeutua väliaineeseen, osa taittua takaisin ilmaan. /3/

Monitie-etenemisessä signaali kulkee useita eri reittejä lähettimen ja vastaanottimen välillä, kuten kuvassa 2 on esitetty. Hajaspektritekniikka on melkein immuuni monitie-etenemiselle.



Kuva 2 Monitie-etenemisessä signaali kulkee useita reittejä laitteiden välillä /3/

2.3 Siirtotekniikat

Tässä kappaleessa käydään läpi langattomien lähiverkkojen käyttämiä modulaatio- ja lähetystekniikoita sekä koodaustapoja. Eri standardit käyttävät eri tekniikoita, joten kaikki langattomat verkot eivät ole yhteensopivia. Standardit käsitellään kappaleessa 3.

Hajaspektri

Hajaspektritekniikka kehitettiin alun perin sotilaskäyttöön, luotettavaan ja turvalliseen kommunikointiin. Lähetys vaatii enemmän kaistanleveyttä kuin perinteinen kapeakaistainen tekniikka, mutta tuloksena on signaali, joka on itse asiassa voimakkaampi ja helpompi havaita edellyttäen, että käytetyn hajaspektrin parametrit ovat tiedossa. Muuten hajaspektrilähetys kuulostaa ja vaikuttaa kohinalta ulkopuolisesta kuulijasta. Tekniikan hyviä puolia ovat luotettava siirto monitiekanavassa, viestin selektiivinen osoittaminen ja hyvä häiriönsietokyky. /7/ /8/

Taajuushyppely-tekniikka, FHSS

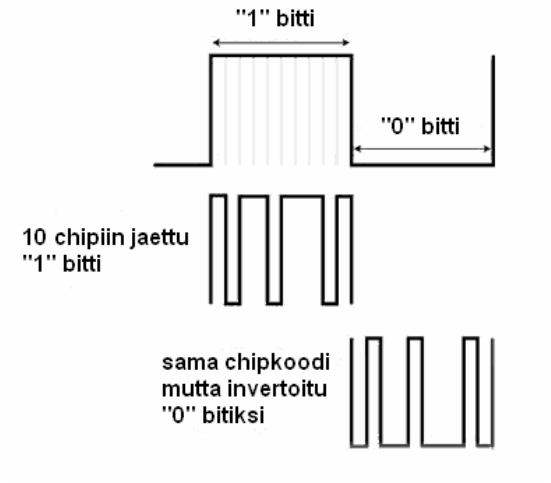
Taajuushyppely-tekniikassa käytössä oleva taajuuskaista jaetaan useisiin kapeisiin taajuuskanaviin. Lähetettävä data jaetaan pieniin osiin ja lähetetään aikavälein eri kanaville. Lähetystaajuutta vaihdetaan tietyn algoritmin perusteella, joka voi olla aivan satunnainen, kunhan se on lähettäjän ja vastaanottajan tiedossa. Kuuntelija, joka ei tiedä hyppelyalgoritmia, ei pysty tulkitsemaan liikennettä. Tekniikka käyttää pitkällä aikavälillä hyväkseen koko taajuusalueen, joka sillä on käytössä.

Taajuushyppely voidaan toteuttaa joko hitaalla tai nopealla hyppelyllä: hitaassa lähetetään useita bittejä yhdellä aikavälillä, kun taas nopeassa lähetetään yksi bitti usealla aikavälillä. Jos jollain kanavalla on häiriötä, voidaan kyseinen taajuus jättää käyttämättä. Hyppelyväli saa olla maksimissaan 400 ms ja samaa kanavaa ei saa käyttää kuin 30 s:n välein. 2,4 GHz:n kaistalla lähetteen pitää hyppiä 75 kanavan läpi hypyn ollessa minimissään 6 MHz. Nämä WLANia koskevat säännöt vähentävät pakettien törmäysmahdollisuutta, jos samassa tilassa on usea verkko. /2/

Erilaiset taajuushyppelyalgoritmit mahdollistavat useiden verkkojen toimimisen samalla taajuusalueella samanaikaisesti. Tekniikka on halpa ja yksinkertainen, mutta huomattavasti hitaampi kuin DSSS-tekniikalla toteutettu verkko.

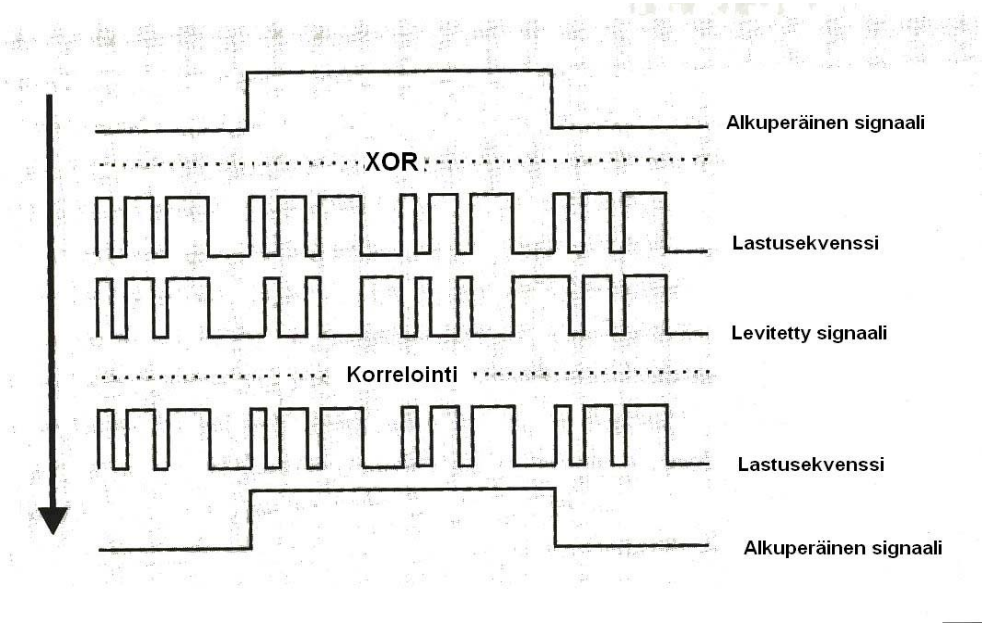
Suorasekvenssi-tekniikka, DSSS

Suorasekvenssi-tekniikassa data jaetaan leveälle kaistalle, 802.11b-standardissa 22 MHz:n leveydelle. Jokainen lähetteen bitti jaetaan useaan ”lastuun” (chip), kuten kuvan 3 esimerkissä, ja lähetetään koko taajuusalueella yhtenä signaalina. Lähetettävä signaali sekoitetaan kohinalta vaikuttavaan kantoaaltoon ja lähetetään käyttäen leveää kaistaa. Vastaanottajan on tiedettävä ns. hajotuskoodi (spreading code) saadakseen lähetteen purettua. Hajotuskoodi määrää järjestelmän kaistanleveyden.



Kuva 3 Bittien jako chipkoodeiksi /7/

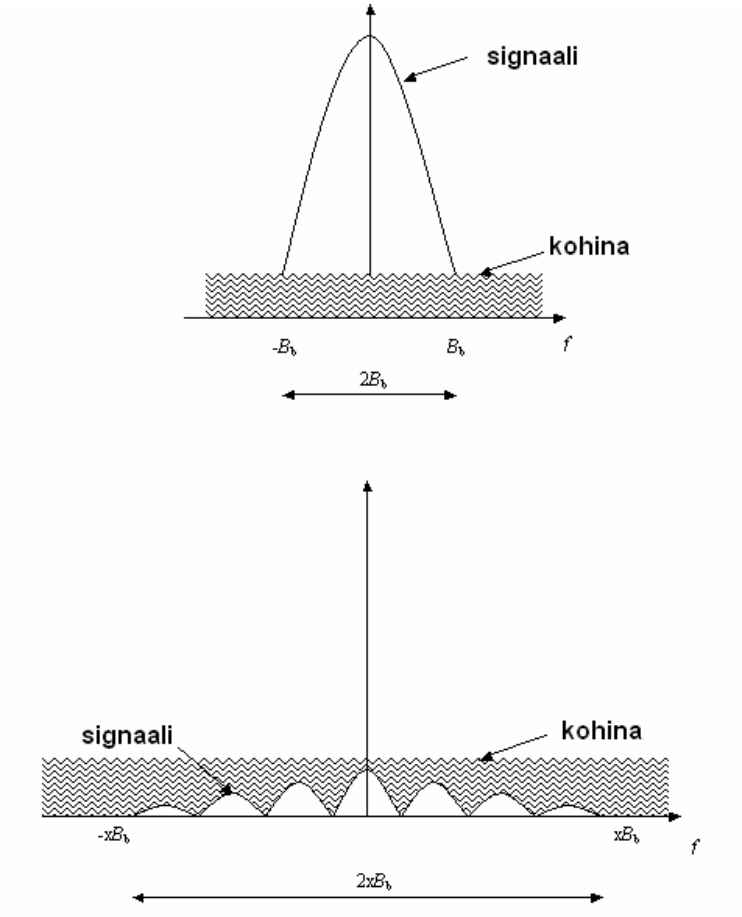
Langattoman lähiverkon standardit käyttävät joko Barker- tai CCK-koodia hajotukseen. Barker-hajotus käyttää 11 -bittistä sekvenssiä {+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1}. Hajotustoimenpide on esitetty kuvassa 4.



Kuva 4 Barker-koodauksen perusperiaate /4/

CCK on uudempi hajotusmenetelmä kuin Barker. Se käyttää entistä tehokkaammin kaistaa ja tämä takaa mahdollisuuden yhä nopeampiin yhteyksiin. Tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. Sarjamuotoisena kullakin koodisanalla on oma matemaattinen merkityksensä.

Kuvassa 5 on esitetty normaali- ja suorasekvenssilähetteen spektrit. Hajaspektrilähetteessä informaatiosignaali voi olla useita kymmeniä desibelejä kohinatason alapuolella ja silti se saadaan vastaanotettua.



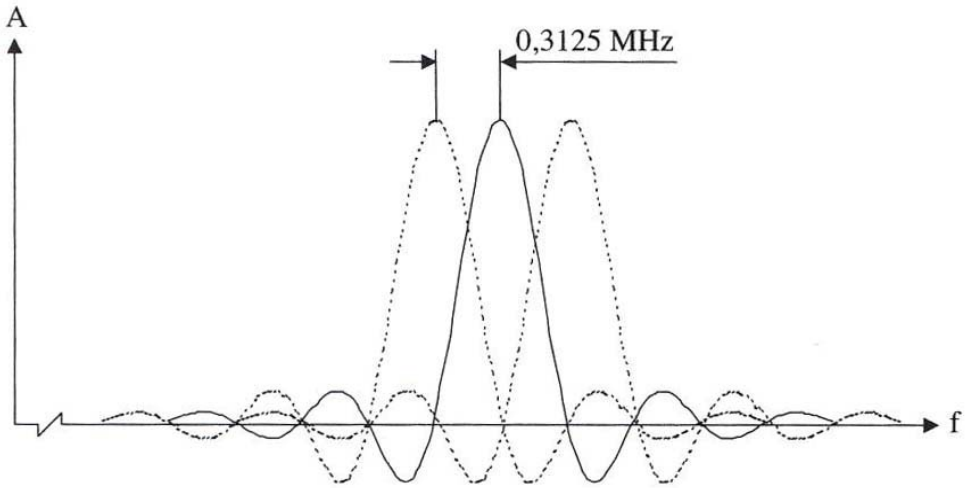
Kuva 5 Signaali levitetään kohinan alapuolelle /7/

Suorasekvenssin etuja ovat hyvä sietokyky virheille ja monitie-etenemiselle sekä nopeammat yhteysmahdollisuudet kuin FHSS-tekniikalla.

OFDM-tekniikka

OFDM-tekniikassa data jaetaan eri taajuuksisiin alikanaviin, joita käytetään rinnakkain. Alikanavien välissä ei ole varokaistaa, koska kanavat on valittu siten, että kanavien keskitaajuudella muiden kanavien spektri on nolla. Kuvassa 6 on kolme vierekkäistä alikanavaa ja siitä nähdään, kuinka kanavien spektrit ovat

riippumattomia eli ortogonaalisia. Lähetyksessä käytetään käänteistä nopeaa Fourier-muunnosta (IFFT) ja vastaanotossa normaalia FFT:tä. /3/



Kuva 6 OFDM-tekniikassa kanavilla ei ole varokaistoja /3/

Taulukossa 4 on yhteenveto IEEE 802.11-standardien käyttämistä hajaspektritekniikoista.

Taulukko 4 Standardien välillä on suuria eroja /3/

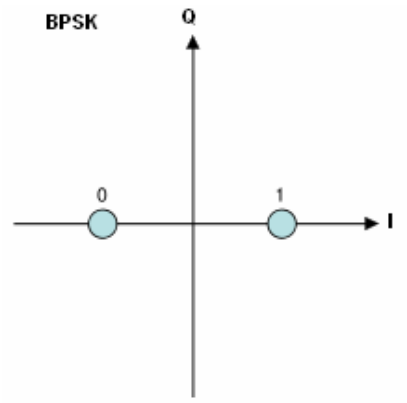
Standardi	Ratifioitu	Mediat	Hajaspektritekniikka	Teoreettinen bittinopeus
802.11	1997	IR, RF	FHSS, DSSS	1 ja Mb/s
802.11b	1999	RF	DSSS	1, 2, 5,5 ja 11 Mb/s
802.11a	1999	RF	OFDM	6 - 54 Mb/s
802.11g	2003	RF	OFDM	1 - 54 Mb/s
802.11n	ei vielä	RF		250+ Mb/s

Modulaatiot

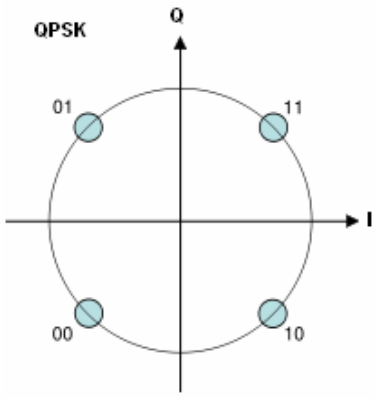
Modulaatiossa sekoitetaan kaksi signaalia, kantoaalto ja lähetettävä datasignaali. Modulaation tarkoitus on muokata lähete siirron kannalta edulliseen muotoon. IEEE 802.11-standardit käyttävät useita erilaisia modulaatioita, mutta periaatteessa: mitä suurempi tiedonsiirtonopeus, sitä monimutkaisempi modulaatio.

Kappaleessa 3.3 on taulukoitu eri standardien ja bittinopeuksien käyttämät modulaatiomenetelmät.

Pienillä nopeuksilla käytössä on hyvin yksinkertainen BPSK-modulaatio. BPSK käyttää kahta kantoaallon vaihetta ilmaisemaan bitin arvon. Sen konstellaatiodiagrammi on esitetty kuvassa 7. QPSK on hieman monimutkaisempi, koska se käyttää neljää eri vaihe-eroa. Se voi ilmaista kahdella bitillä arvot nollasta kolmeen. QPSK-modulaation konstellaatiodiagrammi on esitetty kuvassa 8.

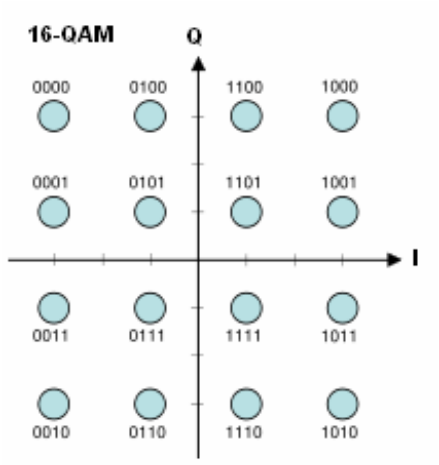


Kuva 7 BPSK-modulaatio



Kuva 8 QPSK-modulaatio

QAM-modulaatio yhdistää PM- ja AM-modulaatiot. Se on spektritehokas modulaatiomenetelmä, koska se hyödyntää signaalin vaiheen sekä amplitudin. Kuvassa 9 on esitetty 16-QAM, joka mahdollistaa neljä amplitudia ja neljä vaihe-eroa.



Kuva 9 16-QAM-modulaatio

Nopeimmat yhteydet käyttävät 64-QAM-modulaatiota. Puska /3/ osoittaa kirjassaan, kuinka 54Mb/s-nopeus saadaan koodaamalla kuusi bittiä yhteen merkkiin ja lähetetään merkkejä rinnan 48 datakanavalla:

$$6 \times 48 = 288 \text{ bittiä}$$

Näistä biteistä ¾ käytetään datalle ja ¼ käytetään virheenkorjaukselle, joten hyötykäyttöön saadaan:

$$¾ \times 288 = 216 \text{ bittiä}$$

Kun jokaisella alikanavalla symbolinopeus on 250 000 symbolia sekunnissa, tulee teoreettiseksi bittinopeudeksi:

$$216 \text{ bittiä} \times 250\,000\ 1/s = 54 \text{ Mb/s}.$$

3 IEEE 802.11-STANDARDIPERHE

Standardointi tähtää siihen, että verkot, laitteet ja tekniikat ovat keskenään yhteensopivia. Standardointi helpottaa laitteiden kehitystyötä ja selventää laitehankintoja kuluttajan osalta. Langattomat lähiverkot on määritelty IEEE 802.11-standardin alle.

3.1 Määritelmät

Langattomat lähiverkot kuuluvat Institute of Electrical and Electronics Engineersin (IEEE) kehittämään 802.11-standardiperheeseen, joka määrittelee protokollan ja rajapinnan langattomalle tiedonsiirrolle. Se kattaa vain kaksi alinta kerrosta OSI-mallista: fyysisen kerroksen ja siirtoyhteyskerroksen alemman osan, joka tunnetaan nimellä MAC (Media Access Control). Fyysinen kerros määrittelee eri standardit, lähetystavat, bittinopeudet, kanavat, bittien hajotuksen alikanaville ja modulaatiotavat, kun taas siirtokerros pitää huolen mm. vuoron varauksesta. Taulukossa 5 on esitetty OSI-mallin kerrokset. /3/

Taulukko 5 802.11-standardi määrittelee alimmat OSI-mallin kerrokset /3/

7	Sovelluskerros		
6	Esitystapakerros		
5	Yhteysjaksokerros		
4	Kuljetuskerros		
3	Verkkokerros		
2	Siirtoyhteyskerros	802.11 MAC	← WLAN-standardien
1	Fyysinen kerros	PLCP, PMD	← määrittelemät kerrokset

802.11 on IEEE:n määrittelemä, alkuperäinen standardi WLAN-lähiverkoille ja sen kehitysversiot on merkitty lisäkirjaimella, kuten 802.11*x*. Standardi määrittelee tiedonsiirtotavaksi radiotaajuus- ja infrapunatekniikan. Nykyisin käytetään myös kaupallista nimitystä Wi-Fi uusimmista WLAN-standardeista.

3.2 Historia

IEEE:n vuonna 1990 aloittama ja seitsemän vuotta myöhemmin, vuonna 1997, valmistunut 802.11 on ensimmäinen langattomiin lähiverkkoihin suuntautuva

standardi. Sen siirtonopeus ja tietoturva eivät vastanneet tarpeisiin, joten kehitysversiot 802.11b ja 802.11a julkaistiin jo vuonna 1999. Vuonna 2003 ratifioitiin 802.11g, joka yhdisti aikaisempien versioiden hyvät puolet yhteen standardiin. Langattomien lähiverkkojen kehitystyö jatkuu edelleen, suurimpina haasteina ovat tiedonsiirtonopeuksien hurja kasvu ja tietoturvan parantaminen. /1/ /2/

3.3 Standardit

IEEE 802.11

802.11 on ensimmäinen langattomien lähiverkkojen standardi. Se julkaistiin vuonna 1997 ja se mahdollistaa tiedonsiirron 1 Mb/s:n ja 2 Mb/s:n nopeuksilla. 802.11 käyttää 2,4 GHz:n ISM-taajuutta.

Standardi määrittelee kolme tiedonsiirtotekniikkaa ja kaksi verkkotopologiaa: FHSS:n, DSSS:n ja infrapunan sekä ad-hocin ja infrastruktuurisen. Kaikki kehitysversiot pohjautuvat 802.11-standardiin, muuten se on nykyään irrelevantti ja on poistunut käytöstä. /1/ /6/

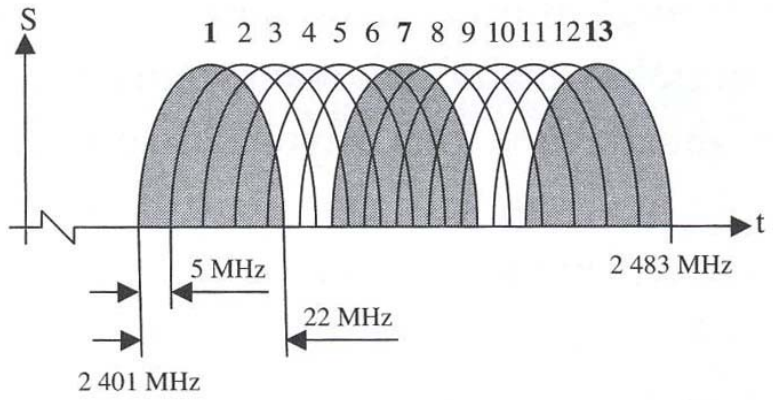
IEEE 802.11b

802.11b on kehitysversioista vanhin – julkaistu vuonna 1999. Se käyttää samaa 2,4 GHz:n taajuusaluetta kuin 802.11 ja määrittelee tiedonsiirtonopeuksiksi 1, 2, 5,5 ja 11 Mb/s. 802.11b toteuttaa tiedonsiirrossa DSSS-tekniikkaa sekä Barker- ja CCK-hajotusta. Siirtonopeudet vaikuttavat hajotus- ja modulaatiotapaan, kuten taulukossa 6 on esitetty.

Taulukko 6 802.11- ja 802.11b-standardien hajotus- ja modulaatiotavat /4/

Standardit	Tekniikka	Bittinopeus	Hajotus	Modulaatio
802.11, 802.11b	DSSS	1 Mb/s	Barker	DBPSK
802.11, 802.11b	DSSS	2 Mb/s	Barker	DQPSK
802.11b	HR/DSSS	5,5 Mb/s	CCK	DQPSK
802.11b	HR/DSSS	11 Mb/s	CCK	DQPSK

Taajuusalue on jaettu kolmeentoista 22 MHz:n kanavaan. Ongelmana on kanavien päällekkäisyys. Kuvasta 7 nähdään, kuinka kanavat 1, 7 ja 13 ovat ainoat kanavat, jotka eivät vaikuta toisiinsa yhtään.



Kuva 10 Kanavien vaikutus toisiinsa /3/

IEEE 802.11a

802.11a julkaistiin samana vuonna kuin 802.11b, suurimpina eroina 5 GHz:n taajuusalue ja pohjautuminen OFDM-tekniikkaan. Sen teoreettinen maksiminopeus on 54 Mb/s. Kanavat ovat 20 MHz:n välein ja menevät hieman päällekkäin, mutta OFDM-tekniikan ansiosta 802.11a tarjoaa 12 toisiinsa vaikuttamatonta kanavaa.

802.11a ei pysty yhtä suuriin peittoalueisiin kuin 802.11b korkeamman taajuuden vuoksi. Samasta syystä se läpäisee myös heikommin eri väliaineita. Modulaatiomenetelmät riippuvat täysin siirtonopeuksista. Taulukossa 7 on esitetty mm. nopeus-modulaatio-suhde. Sama taulukko pätee myös standardin 802.11g kohdalla. /4/

Taulukko 7 802.11a ja 802.11g -standardien modulaatiot /4/

Nopeus	Modulaatio	Bittejä/kantoaalto	Bittejä/symboli	Koodaussuhde
6 Mb/s	BPSK	1	48	1/2
9 Mb/s	BPSK	1	48	3/4
12 Mb/s	QPSK	2	96	1/2
18 Mb/s	QPSK	2	96	3/4
24 Mb/s	16QAM	4	192	1/2
36 Mb/s	16QAM	4	192	3/4
48 Mb/s	64QAM	6	288	2/3
54 Mb/s	64QAM	6	288	3/4

IEEE 802.11g

802.11g on vuonna 2003 julkaistu kehitysversio. Se on yhdistelmä aikaisempien standardien hyvistä puolista ja mahdollistaa siirtonopeudet 54 Mb/s:iin asti. Standardi määrittää radiotaajuustekniikoista DSSS-, HR/DSSS- ja OFDM-tekniikat ja käyttää 2,4 GHz:n taajuusaluetta. Modulaatiot on esitetty 802.11a-standardin yhteydessä taulukossa 7.

802.11g on yhteensopiva samaa taajuutta käyttävän 802.11b-standardin kanssa. /1/

IEEE 802.11*x*-laajennukset

802.11-standardi on saanut useita lisäyksiä vuosien varrella. Osa on parantanut yhteensopivuutta, osa lisännyt tietoturvaa. Seuraavassa on käsitelty lisäyksistä muutama:

- *802.11n* on uusin IEEE 802.11-standardiperheen julkaisuista. Sen virallinen ratifiointi pitäisi tapahtua vuoden 2008 aikana, mutta standardin epävirallisia versioita on jo myynnissä. Suurimpina muutoksina ovat 250+ Mb/s:n teoreettinen siirtonopeus ja entistä parempi peittoalue. Standardi käyttää laitteissa MIMO-tekniikkaa (multiple-input, multiple-output), joka mahdollistaa suuren siirtonopeuden.

- *802.11i* eli WPA2 ei ole periaatteessa standardi vaan lisäys tietoturvaan. Sen tuomat parannukset käsitellään tarkemmin kappaleessa 4.1.

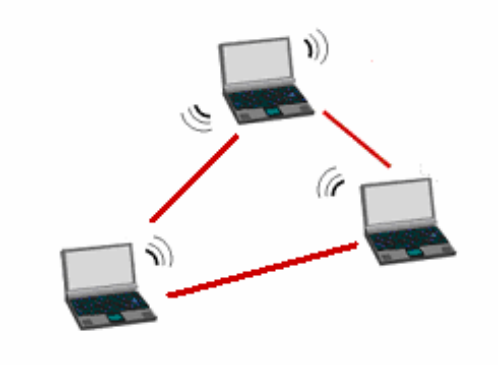
- *802.11e* sisältää palvelun laatuun ja verkon suorituskyvyn parantamiseen liittyviä laajennuksia.

3.4 Topologiat

Langattoman lähiverkon voi rakentaa kahdella eri tavalla: joko ad-hoc WLANilla tai perinteisellä, tukiasemaa käyttävällä, infrastruktuurisella WLANilla, ts. BSS:llä (Basic Service Set). Molempien tapojen konfigurointi ja toimivuus käsitellään kappaleessa 5.2.

Ad-hoc WLAN

Ad-hoc-verkko on erittäin yksinkertainen tapa rakentaa lähiverkko. Ad-hoc-verkossa laitteet keskustelevat suoraan toistensa kanssa (peer-to-peer) eikä tukiasemaa tarvita. Ad-hoc sopii parhaiten pienelle määrälle koneita ja lyhyellä kantamalla. Kuvassa 8 on esitetty ad-hoc-verkon rakennetta.



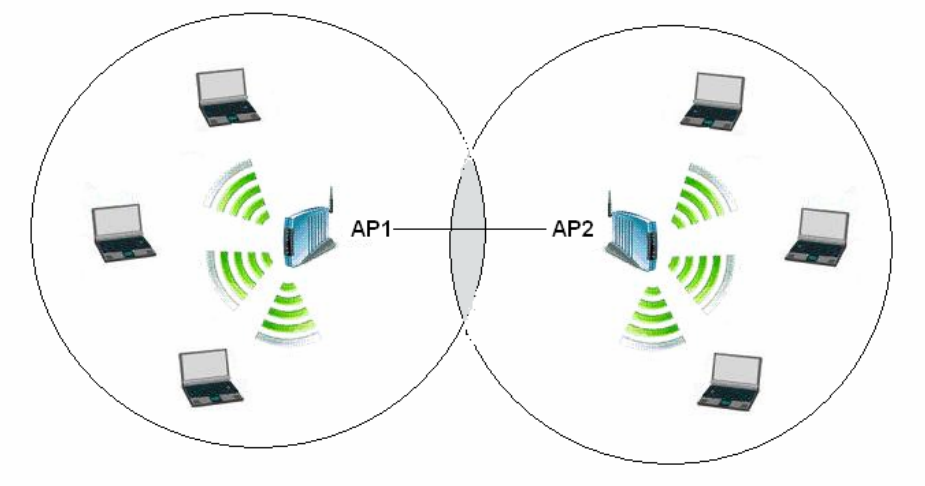
Kuva 11 Ad-hoc-verkossa ei tarvita tukiasemaa

Infrastruktuurinen WLAN (BSS/ESS)

Infrastruktuurisessa WLANissa päätelaitteet ovat yhteydessä koko verkkoon tukiaseman välityksellä, kuten kuvassa 9. BSS on sopiva isojen laitemäärien kanssa ja sen kantama on suurempi kuin ad-hoc-verkolla.

Kuva 12 Tukiasema (AP) hoitaa yhteydet infrastruktuurisessa verkossa

Jos verkko rakentuu useasta tukiasemasta, kutsutaan sitä ESS:ksi (Extended Service Set). Päätelaitetta voi liikuttaa koko verkon alueella: signaalin heikentyessä tukiasemasolun laidoilla päätelaite vaihtaa (roam) tukiasemaan, jota kuulee parhaiten. Kuvassa 10 on kuvattu mahdollista ESS-verkon rakennetta. /3/



Kuva 13 ESS-verkko muodostuu useista soluista

4 TIETOTURVA

Tietoturva nousee helposti esille langattomasta tietoliikenteestä puhuttaessa. Kaapeloinnista poiketen signaalit leviävät lähiympäristöön tehokkaasti, mikä mahdollistaa samalla myös ei-toivottujen henkilöiden mahdollisuuden tarkastella liikennettä. Autentikoimalla käyttäjät ja salaamalla verkkoliikenne saadaan langatonkin verkko turvalliseksi. Salaus on siis hyvin tärkeä osa langattomuutta.

4.1 Verkkoon liittymisen tunnisteet

SSID

Service set identifier (SSID) on keino erottaa langattomat verkot toisistaan. Tunnus, enintään 32 kirjaiminen merkkijono, on lisätty jokaiseen verkossa liikkuvaan pakettiin, jonka avulla paketit kulkevat oikeiden laitteiden ja verkkojen välillä, ts. kaikkien samassa verkossa olevien laitteiden pitää käyttää samaa SSID:tä. SSID-tunnuksen lähetyksen voi kytkeä pois päältä, mutta se ei estä tarkoituksellisia tunkeutujia: uuden laitteen liittyessä verkkoon SSID kulkee salaamattomana laitteen ja tukiaseman välillä, joten tarpeeksi kauan verkkoa kuuntelemalla on mahdollisuus saada SSID selville. On olemassa myös ohjelmia, joilla SSID saadaan melko vaivatta näkyviin.

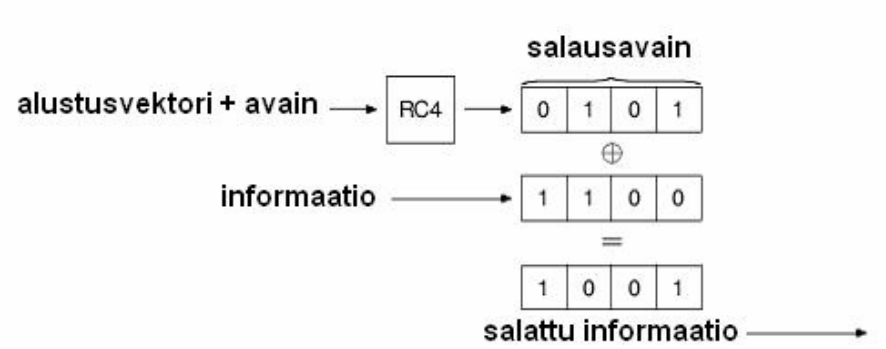
Pääsylistat

Pääsylistoilla voi rajata laitteet, joilla on pääsy verkkoon, määrittelemällä verkon asetuksiin sallittujen laitteiden MAC-osoitteet. Suurten verkkojen pääsylistojen ylläpito on hyvin vaivalloista, joten tämä menetelmä on suositeltava vain kotiverkoissa. Salaustapana pääsylistaa ei voi pitää kovin luotettavana: MAC-osoitteet kulkevat verkossa selväkielisinä paketteina, vaikka niissä itse data olisikin salattu. Salakuuntelijan on siis helppo selvittää sallittu MAC-osoite ja muuttaa oman verkkokorttinsa MAC vastaamaan sitä.

4.2 Salaustavat

WEP

Wired Equivalent Privacy (WEP) on osa alkuperäistä 802.11-standardia. Se käyttää RC4-salausalgoritmia, joka hyödyntää 64 bittiä pitkää salausavainta. Salausavaimen 40 bittiä on käyttäjän päätettävissä, loput 24 alustusvektoribittiä kone generoi jokaisen lähetyksen yhteydessä. Kuvassa 11 on esitetty salauksen perusperiaate.



Kuva 14 WEP-salauksen periaate

Kehittyneempi versio salaa 128 bitillä (104 bittiä + alustusvektori), mutta se ei takaa parempaa turvallisuutta: tunkeutujalla menee vain hetken pitempään salausavaimen selvittämiseen.

WEP on vanhentunut ja helposti kierrettävä salausmenetelmä. Netistä voi ladata ilmaisohjelmia, joiden avulla WEP-suojattuun verkkoon pystyy tunkeutumaan kuuntelemalla verkon liikennettä muutamia minuutteja. Loppujen lopuksi murtautumisaika riippuu liikenteen määrästä.

Matti Puskan teoksen /3/ mukaan, jos liikennemäärä on 30 Mb/s, liikkuu verkossa 15 000 kehystä sekunnissa 250 tavun keskimääräisellä kehyksen koolla. WEP-salaus murrettiin vuonna 2001 kuuntelemalla 5-6 miljoonaa kehystä, joka vastaa noin 6 minuutin liikennemäärä.

WPA (TKIP)

Wireless Fidelity Protected Access (WPA) on huomattavasti parempi salaustapa kuin WEP, vaikka siinäkin on omat murheensa. WPA suunniteltiin paikkaamaan WEP-salauksen puutteet, joten se piti suunnitella yhteensopivaksi vanhojen sekä uusien laitteiden kanssa, mikä taas rajoitti kehitystä. Se kehiteltiin 802.11i-standardin rinnalla ja sisältää sen mukaisia ominaisuuksia.

Suurin parannus on TKIP:n käyttö. TKIP (Temporal Key Integrity Protocol) salaa liikenteen RC4-algoritmilla, käyttäen 128 bittistä salausavainta. Alustusvektorit on muutettu 48 bittiseksi ja salausavain generoidaan kehyskohtaisesti. WPA vaihtaa salausavainta noin 10 000 paketin välein, joten avaimen selvittäminen on käytännössä mahdotonta. TKIP sisältää myös MIC-toiminnon; MIC (Message Integrity Control) tarkkailee paketteja ja se paljastaa sanomien väärennysyritykset, kuten bittien uudelleen järjestelyn ja lähde- tai kohdeosoitteen muuttamisen. Kehys hylätään, jos tiedot eivät vastaa MIC:n tarkistussummaa.

WPA-salaukselle on kaksi tapaa: Personal ja Enterprise. WPA-Personal käyttää PSK-menetelmää (Pre-Shared Key) eli ennalta määrättyä avainta. Uuden laitteen liittyessä verkkoon, tukiasema ja verkkokortti keskustelevat ja vaihtavat avaimia. Jos avaimet täsmäävät, sallitaan pääsy verkkoon. Tästä eteenpäin avaimet vaihtuvat dynaamisesti, toisin kuin WEP-salauksessa, missä samaa avainta käytettään jatkuvasti. WPA-Enterprise-tavassa käytetään ulkoista palvelinta käyttäjien tunnistamiseen. Yksittäistä jaettua avainta ei siis käytetä ja palvelin kontrolloi koko verkkoa. Suuret verkot käyttävät yleisesti Enterprise-tapaa.

WPA:n huono puoli on sen tapa suojautua palvelunestohyökkäyksiltä. Hyökkäyksen tapahtuessa, WPA sulkee koko verkon minuutiksi, joten kaikki verkon laitteet kärsivät. WPA tukee kaikkia 802.11-standardeja.

WPA2 (AES)

WPA2 on uusin kehitysversio, mikä julkaistiin 802.11i-standardina. Se parantaa langattoman lähiverkon tietoturvaa huomattavasti. Se käyttää RC4-algoritmin sijasta AES-lohkosalausalgoritmia (Advanced Encryption Standard). AES käyttää

128-, 192- tai 256-bittistä salausta, joten se vaatii hieman enemmän prosessoritehoa kuin aikaisemmat menetelmät. AES-salausta ei ole tähän päivään mennessä pystytty murtamaan. Muller /2, s.413/ toteaa teoksessaan, että tietokoneella, mikä pystyisi laskemaan 255 salausavainta sekunnissa, kestäisi 149 miljardia vuotta murtaa AES-salaus. /2/ /9/

5 VERKON RAKENNUS

Tässä tapauksessa rakennetaan suljettu WLAN, ts. langaton lähiverkko, mistä ei ole yhteyttä internetiin: neljä konetta on yhteydessä vain toisiinsa. Verkko rakennettiin Tampereen ammattikorkeakoulun tietoliikennelaboratorion tiloihin.

5.1 Laitteisto

Verkko rakentuu neljästä tietokoneesta, joista yksi on kannettava. Kaikissa tietokoneissa on käyttöjärjestelmänä Windows XP™ SP2.

Pöytäkoneiden tiedot:

- Intel Pentium 4 (3 GHz)
- 1 Gt RAM

Kannettavan koneen tiedot:

- Intel Pentium 4 (1,9 GHz)
- 512 Mt RAM

Käytössä olevat verkkokortit:

- Zyxel G-220F USB Adapter MAC-osoite: 00:13:49:6E:6D:83
- Buffalo WLI-PCI-G300N-3 MAC-osoite: 00:16:01:3F:11:A5
- Buffalo WLI-CB-G300N-3 MAC-osoite: 00:16:01:1A:32:A4

Tukiasema:

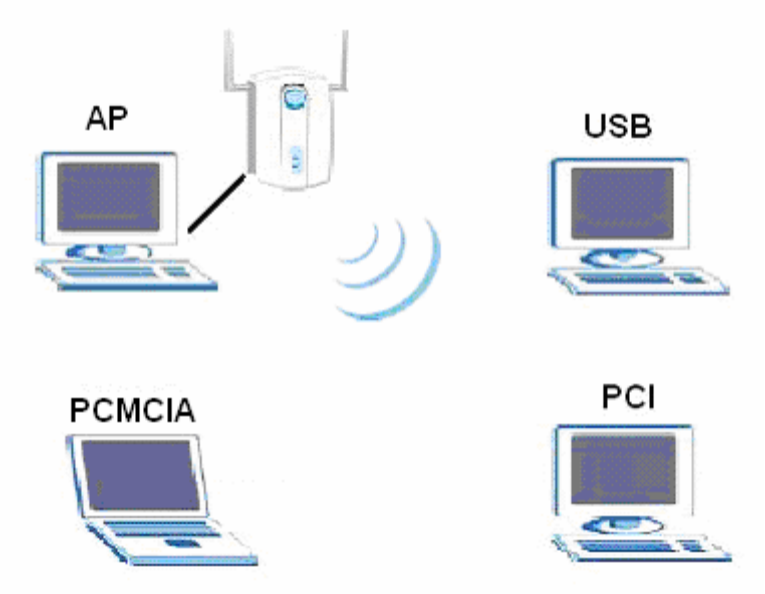
- Linksys WRT54GS IP-osoite: 192.168.1.1
  Käyttäjätunnus: <tyhjä>
  Salasana: admin

Työ tehtiin radiotaajuustekniikoita käyttävillä laitteilla, mitkä tukevat IEEE 802.11-standardeista b:tä ja g:tä. Buffalon laitteet toimivat 802.11n draft 1.0-versiolla, mutta tukevat vanhoja standardeja. Linksys-tukiasema voi toimia myös reitittimenä ja DHCP-palvelimena.

5.2 Konfigurointi

Tässä kappaleessa tutustutaan verkon konfigurointiin ja asetuksiin.

Koneisiin asennettiin Windows XP-käyttöjärjestelmät sekä verkkokorttien ajurit. Koneet nimettiin laboratoriotilan mukaan TA31606-TA31608. Kannettavan nimi on TA316WLAN-L. Kaikkien koneiden käyttäjätunnus on labra ja salasana Tamk2007. Kuvassa 12 on kuvattu laboratoriotilan koneet ja verkkokorttiratkaisut.



Kuva 15 Laboratoriotilan testiverkon rakenne

Tarvittaessa pitää käynnistää Windowsin Wireless Zero Configuration. Sen saa aktivoitua seuraavasti:

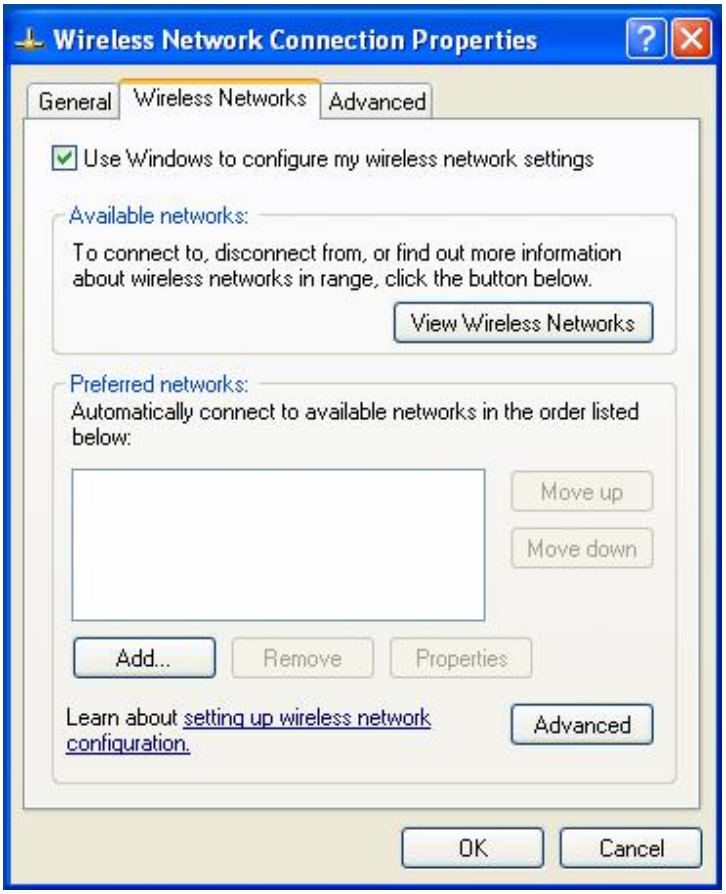
klikataan My computer -kuvaketta oikealla hiirenkorvalla ja valitaan Manage. Sieltä valitaan Services and applications -kohdasta Services ja listan alapäästä käynnistetään Wireless Zero Configuration.

Zyxelin USB-verkkokortti toimii vain omalla, ZyAIR Wireless LAN utility, ohjelmistollaan, joten se ei vaadi edellä demonstroitua toimenpidettä.

Ad-hoc WLAN

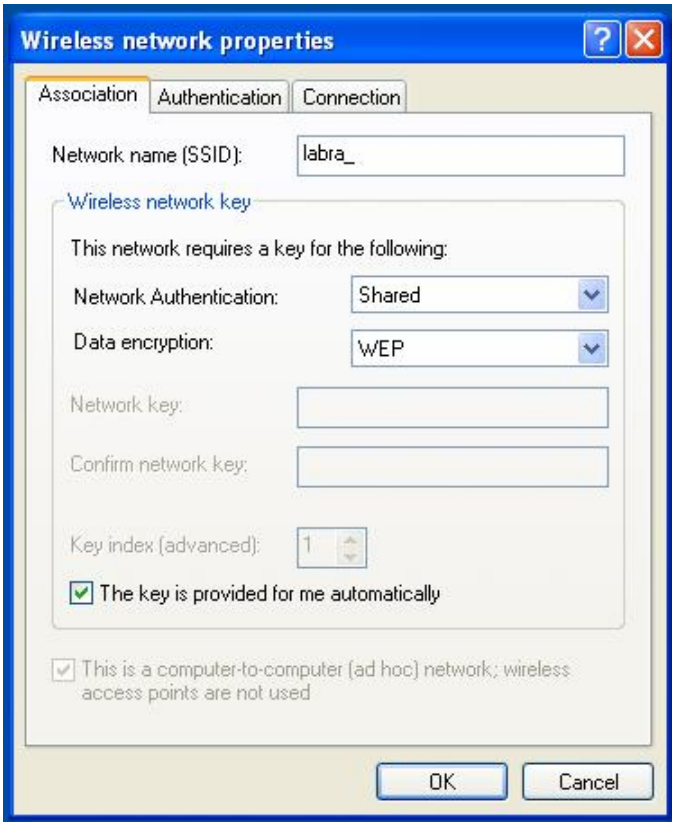
Ad-hoc-verkko konfiguroidaan käyttämällä Windowsin omia työkaluja.

Valitaan Start-valikosta Settings ja Network Connections. Sieltä valitaan Wireless Network connections properties. Avataan välilehti Wireless Networks. Aukeaa kuvan 16 ikkuna.



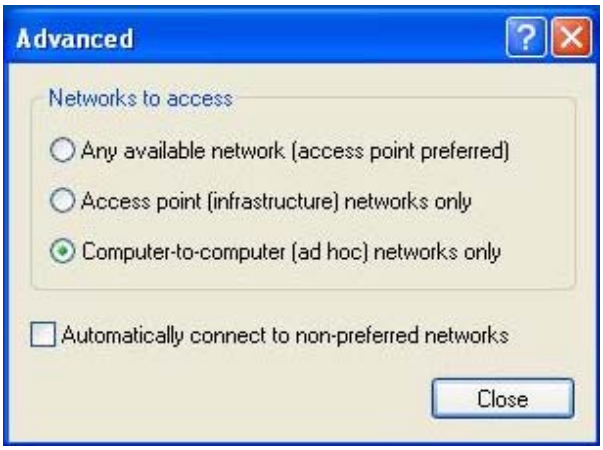
Kuva 16 Verkkoyhteys täytyy lisätä Windowsin verkkoyhteyksiin

Lisätään verkkoyhtyes painamalla Add-painiketta. Aukeaa kuvan 17 näkymä. Annetaan verkolle haluttu SSID-tunnus ja valitaan salausmenetelmä. Tässä tapauksessa SSID on labra_.



Kuva 17 Langattomalle verkolle määritellään SSID ja salaus

Painamalla OK palataan kuvan 16 näkymään, mistä valitaan Advanced. Kuvan 18 näkymästä valitaan computer-to-computer, ts. ad-hoc-topologia.

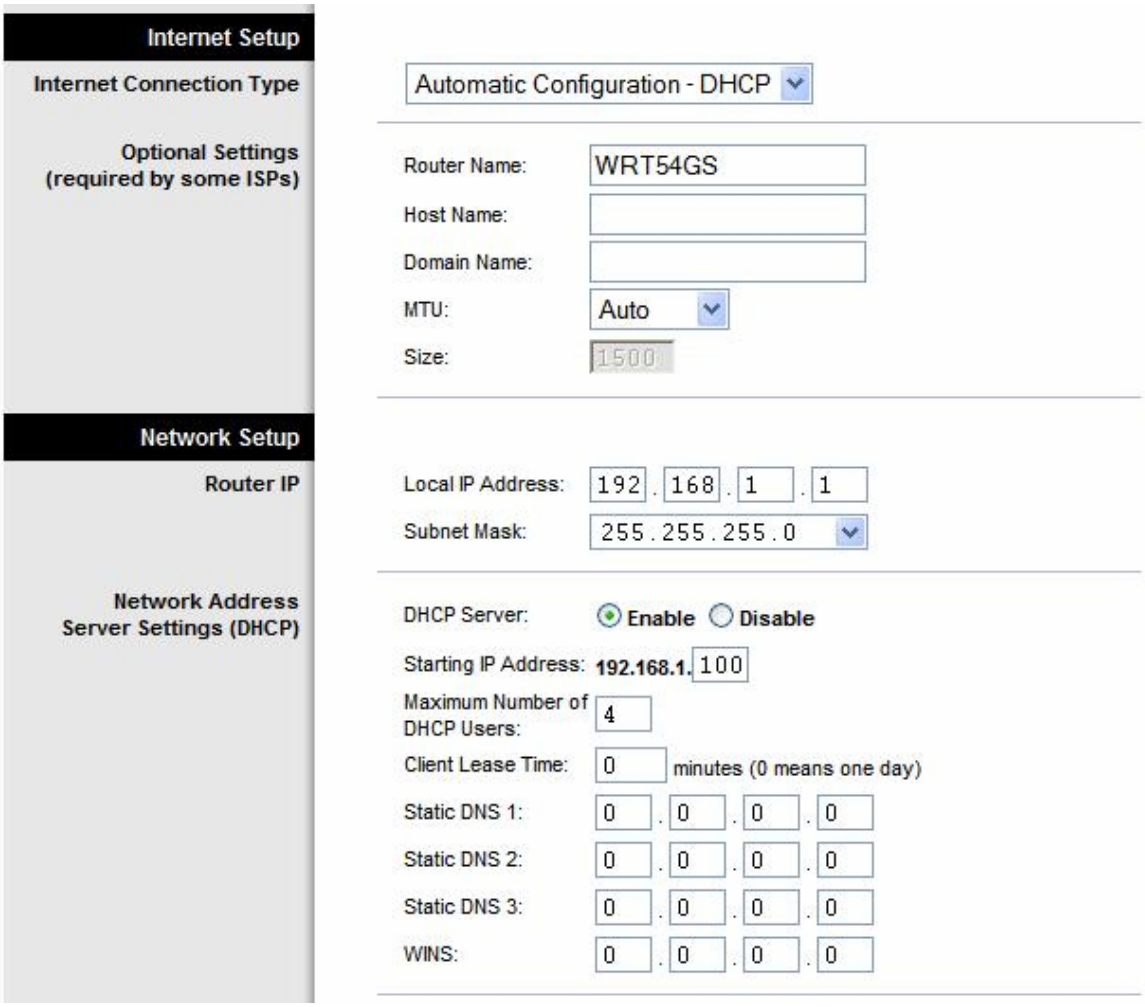


Kuva 18 Liityttävien verkkojen topologiat voi rajata

Tämä toteutetaan kaikille verkon koneille. Salausmekanismin pitää olla kaikilla koneilla sama, kuten myös SSID-tunnuksen. Zyxel-verkkokortti toimii vain omalla konfigurointiohjelmallaan.

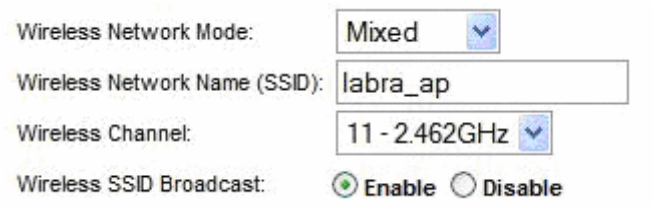
Infrastruktuurinen WLAN eli BSS

Otetaan yhteys verkkoselaimella Linksys-tukiasemaan (IP: 192.168.1.1). Aukeaa kuvan 19 näkymä. Kun reitittimen ja DHCP-palvelimen valinnat on toteutettu, valitaan Wireless-välilehti.



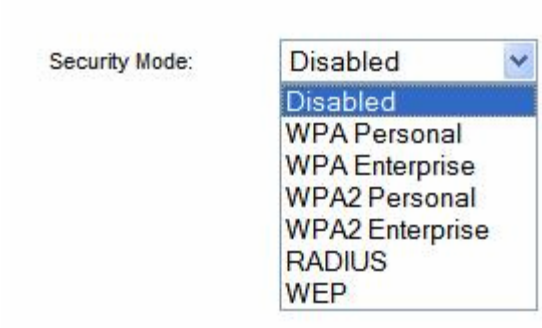
Kuva 19 Reitittimelle määritetään nimi ja DHCP-palvelimen asetukset

Annetaan verkolle SSID-tunnus ja valitaan haluttu taajuuskanava, kuten kuvassa 20 on esitetty. Tässä tapauksessa SSID on labra_ap.



Kuva 20 Verkolle valitaan käytetty standardi, SSID-tunnus ja taajuuskanava

Wireless security-välilehdeltä asetetaan haluttu salaustapa ja sen tarvitsemat parametrit, kuten salausavain. Salaustapoja on käytössä useita, kuten kuvasta 21 nähdään. WPA2 on suojauksista tehokkain, mutta samalla eniten prosessoritehoa vaativa. WPA2 Personal sopii parhaiten pienelle kotiverkolle.



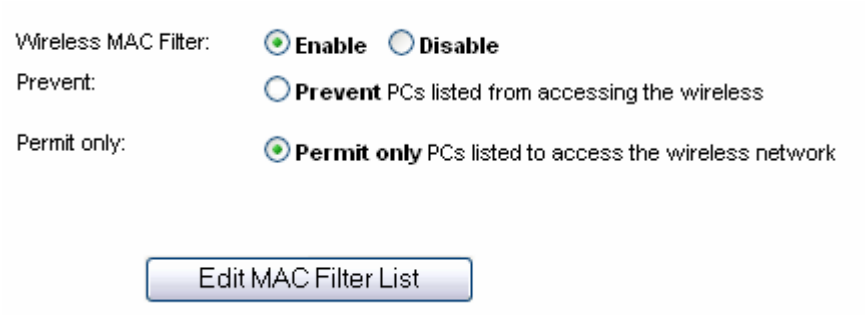
Kuva 21 Tukiasema tukee useaa salaustapaa

Verkkoon voi liittyä lisäämällä verkkoyhteyden Windowsin työkaluilla, kuten ad-hoc-verkon konfiguroinnissa. Computer-to-computer-valinnan tilalle valitaan access point only (kuva 18). SSID-tunnus ja mahdollinen salausavain pitää olla tiedossa.

5.3 Mittaukset

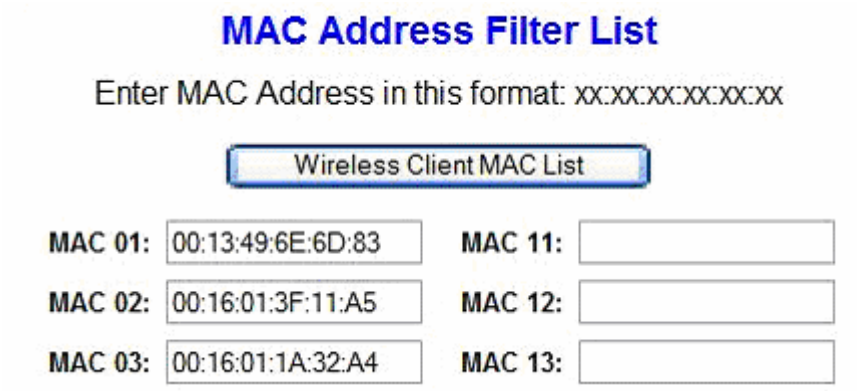
Pääsylistat

Linksys-tukiaseman asetuksista aktivoidaan MAC-suodatus päälle ja muokataan pääsylista vastaamaan verkon laitteita. Kuvassa 22 on pääsylistan aktivointiin tarvittavat valinnat esitelty. Edit MAC Filter list -napin takaa löytyy kuvan 23 lista.



Kuva 22 Pääsylista pitää aktivoida tukiaseman ominaisuuksista

Kuvassa 23 on määritetty MAC-osoitteet pääsylistaan. Vain ko. osoitteilla pääsee liittymään verkkoon.



Kuva 23 MAC-osoitteet määritetään pääsylistaan

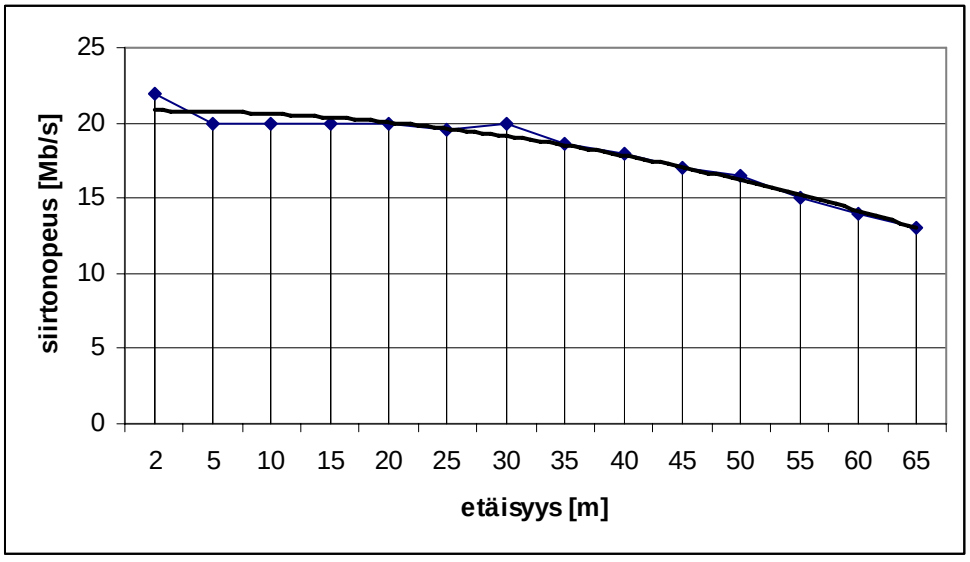
Etäisyyden vaikutus siirtonopeuteen

Tutkittiin etäisyyden vaikutusta siirtonopeuksiin. Mittaus suoritettiin Tampereen ammattikorkakoulun A3-käytävällä. Signaalivoimakkuus oli parhaimmillaan -35 dBm, kun verkkokortit olivat aivan lähekkäin. Taulukossa 8 on esitetty tulokset ja sama graafisesti kuvaajassa 1. Signaalivoimakkuus mitattiin Zyxel-verkkokortin ohjelmistolla.

Taulukko 8 Etäisyys vaikuttaa bittinopeuteen

etäisyys [m]	nopeus [Mb/s]	sign. voimakkuus [dBm]
2	22,0	-44
5	20,0	-49
10	20,0	-60
15	19,9	-60
20	19,9	-62
25	19,5	-66
30	20,0	-67
35	18,6	-70
40	18,0	-73
45	17,0	-73
50	16,5	-73
55	15,0	-76
60	14,0	-77
65	13,0	-79

Mittaustuloksiin vaikuttivat käytävän koko, seinien rakenteet ja pinnat sekä mittalaitteiden välissä ollut avoin lasiovi. Käytävän pituus ei riittänyt yhteyden katkeamiseen, mutta bittinopeudet pienenivät selvästi, kuten kuvaajasta 1 voi nähdä. Ihanteellinen mittauspaikka olisi ollut iso halli tai ulkotila, missä ei olisi ollut esteitä päätelaitteiden välillä.



Kuvaaja 1 Etäisyys vaikuttaa selvästi bittinopeuteen

6 YHTEENVETO

Langattomat lähiverkot ovat kehittyneet huomattavasti viimeisen kymmenen vuoden aikana ja ne tarjoavat varteenotettavan vaihtoehdon perinteisille, langallisille verkoille. Siirtonopeudet ja tietoturva vastaavat nykyisiin tarpeisiin, joten suurimpana ongelmana on sallittujen taajuusalueiden vähäisyys ja siitä johtuen ruuhkaisuus. ISM-taajuutta käyttävät laitteet ovat yleisiä ja häiritsevät samantaajuista langatonta tiedonsiirtoa.

Työtä olisi voinut laajentaa tutkimalla ISM-taajuutta käyttävien eri tekniikoiden ja laitteiden vaikutusta verkon nopeuteen. Myös eri väliaineiden vaimennuksia olisi voinut tutkia.

Opin työn parissa paljon langattomasta tiedonsiirrosta ja varsinkin IEEE 802.11-standardin laitteista. Uskon, että langattomat verkot yleistyvät edelleen ja alan asiantuntijoille on tulevaisuudessa tarvetta, joten opetuspisteestä tulee olemaan hyötyä tulevaisuuden opiskelijoille. Työ onnistui mielestäni hyvin ja tavoitteet täyttyivät.

7 LÄHTEET

1 Briere, Danny - Hurley, Pat, Wireless Network Hacks & Mods for Dummies. Wiley Publishing, Inc. Indiana 2005.

2 Muller, Nathan J., Wireless A to Z. The McGraw-Hill Companies. 2003.

3 Puska, Matti, Langattomat lähiverkot. Talentum. 2005

4 Granlund, Kaj, Langaton tiedonsiirto. Docendo Finland OY. 2001

5 Penttinen, Jyrki, Tietoliikennetekniikka: 3G ja erityisverkot. WSOY. 2006

6 Suomenkielinen wikipedia. [www-sivu]. [viitattu 20.3.2007] Saatavissa: http://fi.wikipedia.org/wiki/802.11

7 Teknillisen korkeakoulun opetusmateriaali. [www-sivu]. [viitattu 22.3.2007] Saatavissa: http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/27/wlan_tekniikka.shtml

8 Rantala, Ari, Hajaspektritekniikka. Tampere. 2001

9 Tuominen, Toni, WLAN Tietoturva [insinöörityö]. Tampereen Ammattikorkeakoulu. 2005

10 Rantala, Ari, Tietoliikenne ja tiedonsiirto. Tampere. 2001

8 LIITTEET

/1/ NET TRAFFIC METER-OHJELMAN ESITTELY

/2/ LANGATON LÄHIVERKKO (WLAN) – Tehtävät

/3/ LANGATON LÄHIVERKKO (WLAN) – Esitehtävien ratkaisut

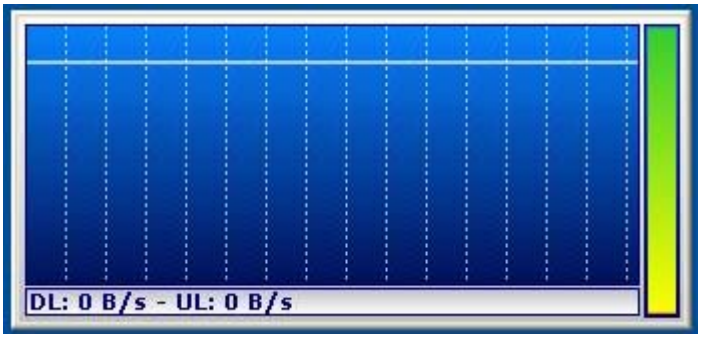
/4/ LANGATON LÄHIVERKKO (WLAN) – Tehtävien ratkaisut osa 1

/5/ LANGATON LÄHIVERKKO (WLAN) – Tehtävien ratkaisut osa 2

/6/ LANGATON LÄHIVERKKO (WLAN) – Työselostuksen laskutehtävän ratkaisu

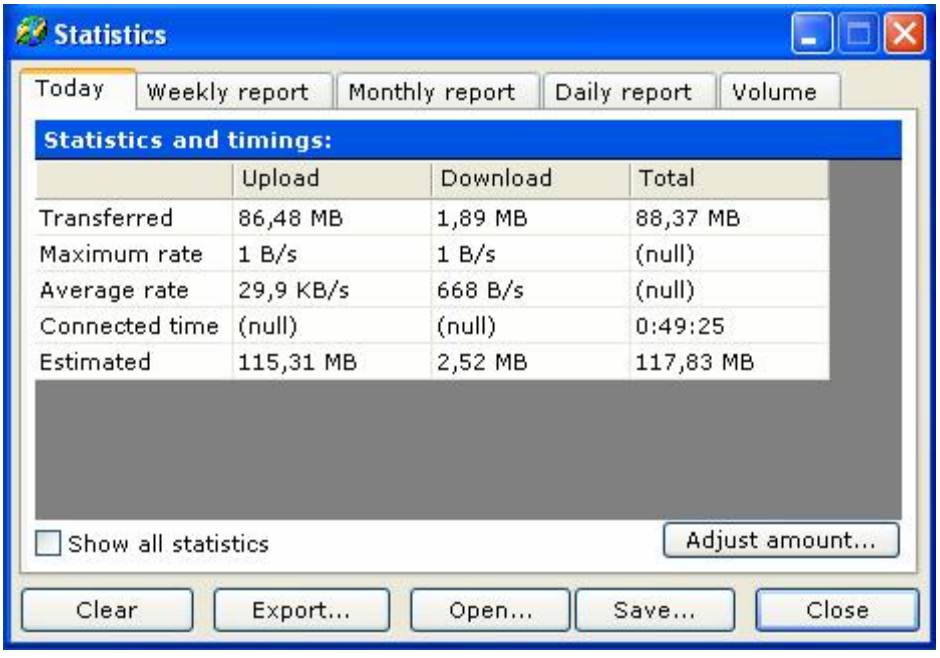
NET TRAFFIC METER-OHJELMAN ESITTELY

Net traffic meter on ilmainen verkkoliikenteen tarkkailuohjelma. Liikennettä voi tarkkailla graafisesti tai tilastoja seuraamalla. Graafinen kuvaaja näyttää liikenteen määrään ulos ja sisään (upload, download) eri värein. Nopeutta voi seurata tavuina tai bitteinä.



Kuva 24 Bittinopeudet esitetään myös graafisesti

Samat asiat näkee myös tilastoituna, monen muun statiikan lisäksi. Ohjelma listaa niin keskiarvot kuin maksimibittinopeudet.



Kuva 25 Ohjelma kerää paljon eri tilastoja

Ohjelma on ladattavissa osoitteesta http://www.kctoolbox.tk.

TAMPEREEN AMMATTIKORKEAKOULU LIITE 2
Tietotekniikka, tietoliikennetekniikka
Petri Leskinen

LANGATON LÄHIVERKKO (WLAN)

ESISELOSTUS

1. Tutustu hajaspektritekniikkaan. Miten FHSS ja DSSS eroavat toisistaan?
2. Selvitä langattomien verkkojen topologiat.
3. Selvitä seuraavien WLANia koskevien termien merkitys: ISM, SSID, OFDM, MIMO.

TYÖ

1. Konfiguroi kahden koneen ad-hoc-verkko. Käytä Windowsin omia työkaluja, lukuun ottamatta Zyxel-verkkokorttia: käytä ZyAIR Wireless LAN utility-ohjelmaa.

   Käyttäjätunnus: labra
   Salasana: Tamk2007

   Kopioi (koneelta TA31608) dataa testi-kansiosta kannettavalle ja tarkkaile siirtonopeuksia. Vaihda toiseksi koneeksi TA31606. Mikä muuttuu ja miksi?

   Tutki etäisyyden vaikutusta bittinopeuteen A3-käytävällä. Arvioi myös signaalin maksimikantamaa. Käytä koneita TA31606 ja TA316WLAN-L.

   Huom: Siirtonopeuksia voi tarkastella NET Traffic Meter-ohjelmalla.

2. Tutustu tukiaseman ominaisuuksiin ja mahdollisuuksiin. Konfiguroi tukiasemaa käyttävä verkko. Jaa koneille IP-osoitteet käyttämällä DHCP-ominaisuutta.

   IP: 192.168.1.1 (salasana: admin)

   Tee pääsylista MAC-osoitteiden perusteella ja kokeile liittyä verkkoon koneella, joka ei ole listalla.

   Huom: Resetoi tukiasema/reititin, kun saat työn valmiiksi! Reset-nappi on takapaneelissa. Poista myös muista koneista konfiguroimasi langattomat verkot!

TYÖSELOSTUS

1. Vastaa kaikkiin työohjeessa esitettyihin kysymyksiin sopivalla tavalla sanallisesti, piirtäen, tulosteiden avulla jne. Kerro tukiaseman ominaisuuksista työselostuksessa.

2. Voisiko ad-hoc-verkkoa käyttäen verkkoyhteyttä hypyttää rajattoman pitkälle? Perustele vastauksesi.

3. 802.11g-standardin tukiasema lähettää 12dBm:n teholla signaalia. Vastaanottavan laitteen herkkyys on -53 dBm. Kuinka kaukana tukiasemasta vastaanottava laite voi olla?

   Oletus: näkyvyys on esteetön.

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka, tietoliikennetekniikka
Petri Leskinen

LANGATON LÄHIVERKKO (WLAN)

RATKAISUT LIITTEEN 1 ESITEHTÄVIIN

ESITEHTÄVÄT

1.

FHSS: Taajuushyppely-tekniikka käyttää pitkällä aikavälillä koko taajuuskaistan. Lähete hyppii lähettäjän ja vastaanottajan tiedossa olevan algoritmin mukaisesti alikanavalta toiselle.

DSSS: Suorasekvenssissä signaali sekoitetaan kohinalta vaikuttavaan kantoaaltoon ja lähetetään käyttäen leveää kaistaa. Jokainen bitti hajotetaan ns. lastuihin (chip).

2.

Ad-hoc WLAN: ilman tukiasemaa toimiva verkko, ts. peer-to-peer

Infrastruktuurinen WLAN: tukiasemaa käyttävä verkko, ts. BSS.

3.

ISM = lisenssivapaa taajuusalue (Industrial, Scientific and Medical)

SSID = Service set identifier eli SSID-tunnus erottaa langattomat verkot toisistaan.

OFDM = OFDM-tekniikassa data jaetaan eri taajuuksisiin alikanaviin, joita käytetään rinnakkain. Alikanavien välissä ei ole varokaistaa, koska kanavat on valittu siten, että kanavien keskitaajuudella muiden kanavien spektri on nolla.

MIMO = Tekniikka (multiple-input, multiple-output), joka mahdollistaa suuret siirtonopeudet. Tekniikka käyttää useita antenneja lähettämiseen ja vastaanottamiseen.

LANGATON LÄHIVERKKO (WLAN)

RATKAISUT LIITTEEN 1 TEHTÄVIIN osa 1

TEHTÄVÄT

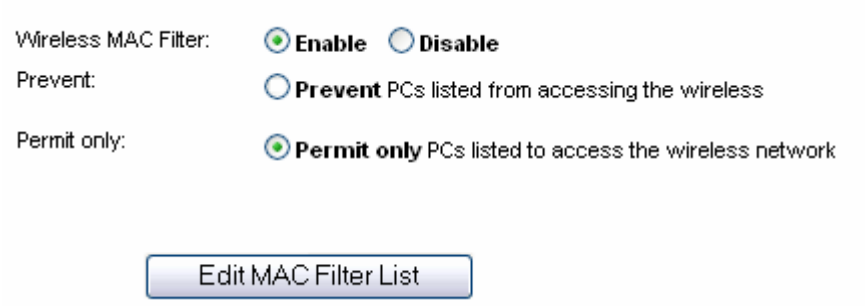
1.

Siirtonopeuksiin vaikuttaa verkkokorttien tekniikat, ts. niiden käyttämät IEEE:n standardit. TA31608 ja kannettava käyttävät 802.11n draft-standardia, joka takaa nopeammat yhteydet kuin koneen TA31606 802.11g-standardi.

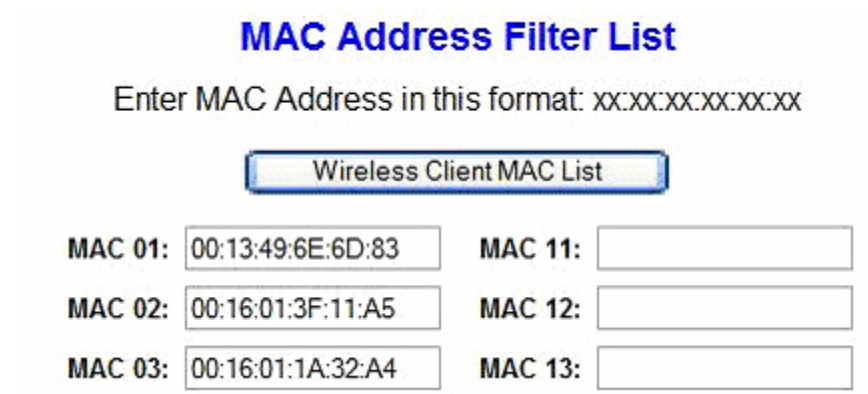
Taulukko 9 Standardien välillä on eroja

Kone	Nopeus	Standardi
TA31608	48 Mb/s	802.11n
TA31606	23 Mb/s	802.11g

MAC-osoitteet määritetään tukiaseman asetuksiin. Vain koneet, joiden osoitteet ovat listattu pääsevät liittymään verkkoon. Seuraavissa kuvissa on esitetty tarvittavat valinnat.



Kuva 26 MAC-pääsylista pitää aktivoida



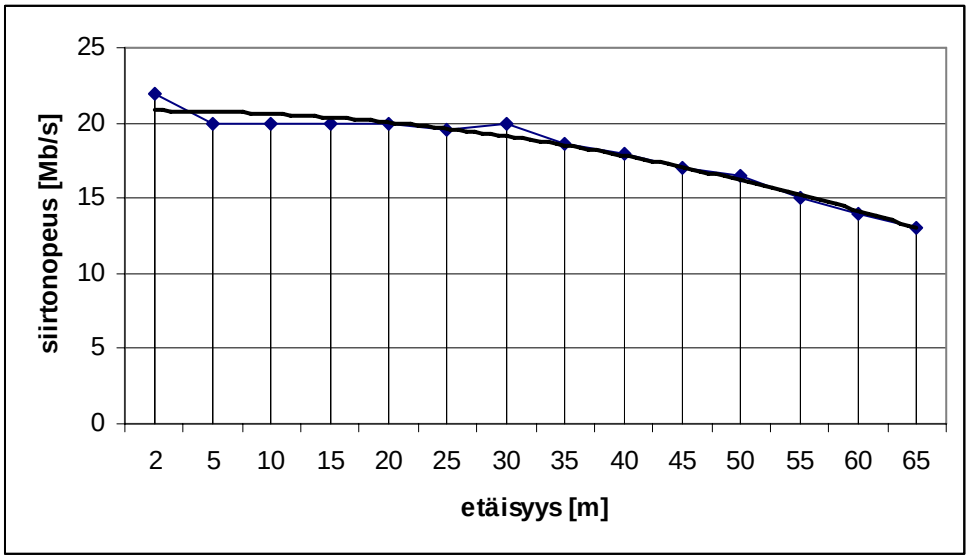
Kuva 27 MAC-osoitteet lisätään pääsylistaan

LANGATON LÄHIVERKKO (WLAN)

RATKAISUT LIITTEEN 1 TEHTÄVIIN osa 2

Etäisyys vaikuttaa siirtonopeuksiin huomattavasti; mitä pitempi etäisyys, sitä hitaammat siirtonopeudet. Maksiminopeudella verkko toimii useiden metrien päässä tukiasemasta, mutta kuuluvuusalueen reunoilla tilanne on toinen.

Pöytäkone sijoitettiin laboratoriotilaan ja kannettavaa liikutettiin Tampereen ammattikorkeakoulun A3-käytävää pitkin. Tilojen välinen lasiovi oli auki.



Kuvaaja 2 Siirtonopeudet pienenevät kun etäisyys kasvaa

Jos tuloksesta haluaisi luotettavamman, pitäisi mittaus suorittaa ulkona tai todella isossa hallissa, missä ei olisi mitään häiriötekijöitä. Käytävän pituus loppui kesken, joten maksimikantamaa ei saatu mitattua. Arvio: noin 90m.

2. Verkkoyhteyden hypyttäminen:

Ei ole mahdollista. Etäisyyden kasvaessa, viive kasvaa ja verkossa alkaa tapahtua liikaa törmäyksiä. Tämä tekee verkkoliikenteen mahdottomaksi. Myös laitemäärien kasvaessa suureksi, kaista ei riitä kaikille laitteille.

LANGATON LÄHIVERKKO (WLAN)

RATKAISU LIITTEEN 1 LASKUTEHTÄVÄÄN

3. Ratkaistaan väliainevaimennus, kun lähetysteho P_{EIRP} = 12 dBm ja päätelaitteen herkkyys on -53 dBm:

$$L_o[\mathrm{dB}] = \left[12 - (-53)\right]\mathrm{dBm} = 65\,\mathrm{dB}$$

Ratkaistaan vapaantilan vaimenemisen kaavasta etäisyys *d*, kun L_o = 65 dB ja taajuus *f* = 2,4 GHz:

$$L_o[\mathrm{dB}] = 92{,}45 + 20\log_{10}(f[\mathrm{GHz}]) + 20\log_{10}(d[\mathrm{km}])$$

$$65\,\mathrm{dB} = 92{,}45 + 20\log_{10}(2{,}4) + 20\log_{10}(d) \rightarrow d = 0{,}0177\ \mathrm{km} = 17{,}7\ \mathrm{m}$$

Vastaus: Etäisyys *d* on noin 17,5 metriä.