# Avoin kaupunki-WLAN käyttäjän näkökulmasta

MASTONETin käyttäjäkokemukset ja kehitysehdotukset

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2012
Simo Viinikka

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

VIINIKKA, SIMO:

Avoin kaupunki-WLAN käyttäjän näkökulmasta
Mastonetin käyttäjäkokemukset ja kehitysehdotukset

Tietoliikennetekniikan opinnäytetyö, 36 sivua

Kevät 2012

TIIVISTELMÄ

---

Langattoman lähiverkon standardiperhe 802.11 syntyi jo vuonna 1991. Ensimmäiset käytännölliset tekniikat saatiin käyttöön 1997. Tämän jälkeen kehitystahti on ollut nopeaa ja uusia nopeampia ja turvallisempia tekniikoita on tullut saataville.

Avoimia WLAN-verkkoja on maailmalla satoja, Suomessa laajempia verkkoja löytyy muutamasta kaupungista, joista Lahden MASTONET on yksi laajimmista. Avoimia langattomia lähiverkkojen käyttäjinä ovat kaupunkien asukkaiden lisäksi työmatkalaiset ja turistit, joille verkko on tarpeen sähköpostin ja uutisten seuraamista varten.

Tämän opinnäytetyön tavoitteena oli tutkia käyttäjien mielipiteitä MASTONETin toiminnasta ja siitä kuinka verkkoa tulisi käyttäjien mielestä kehittää. Verkon toimivuuteen oltiin tyytyväisiä, kuten myös tukipalveluihin, joita Lahden ammattikorkeakoulu tarjoaa verkon käyttäjille. Kehitysehdotuksina esiin nousi verkon nopeuden kasvattaminen ja kuuluvuusalueen laajentaminen. Lisäksi toivottiin Lahden kaupungin palveluiden ja tapahtumien helppoa saatavuutta MASTONETin välityksellä.

Avainsanat: MASTONET, WLAN, langaton lähiverkko, 802.11, käyttökokemukset, kehitysehdotukset

Lahti University of Applied Sciences
Degree Programme in Information Technology

VIINIKKA, SIMO

Avoin kaupunki-WLAN käyttäjän näkökulmasta
Mastonetin käyttäjäkokemukset ja kehitysehdotukset

Bachelor's Thesis in telecommunications 36 pages

Spring 2012

ABSTRACT

---

Standard family for wireless local area network was started in 1991, but first practical technologies were standardized in 1997. After first launch of WLAN development of the wireless networking has been fast and new faster and safer technologies have been standardized within the 802.11 standard family.

There are hundreds of open wireless local area networks around the world. In Finland there are few widespread open WLANs, which the MASTONET is one of the largest. Open WLANs provide services not only for citizens of town, but also tourists and commuters. Usual uses of open wireless local area networks are e-mail and news services.

The goal of this thesis was to survey opinions of users of the MASTONET about how the MASTONET is working and what improvements users would want for the network to have. The MASTONET is working well in the areas it has coverage, and helpdesk services were praised especially after Lahti University of Applied Sciences took the duty of maintaining the MASTONET. Improvements suggested for the MASTONET consists of faster speed for the network and greater coverage. Also users wanted services and events of town of Lahti to be easier to use and get to via the MASTONET.

Key words: MASTONET, WLAN, Wireless local area network, 802.11, user experiences, improvement suggestions.

SISÄLLYS

LYHENNELUETTELO

AES Advanced Encryption Standard, salausmenetelmä

ASCII American Standard Code for Information Interchange, tietokoneen merkistö

BPSK Binary Phase Shift Keying, kaksivaiheinen vaiheavainnus, modulaatiomenetelmä

BSSID basic service set identifier, MAC-osoitetta käyttävä WLANin verkkotunnus

CCK Complement code keying, tiedonsiirtomenetelmä

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance, WLANin käyttämä siirtotien varausmenetelmä

CTS Clear-to-Send viesti, jolla laitteelle annetaan lupa lähettää

DSP Digital signaling processor

DSSS Direct Sequence Spread Spectrum, suorasekvensointi

FHSS Frequency Hopping Spread Spectrum, taajuushyppely

IEEE Institute of Electrical and Electronics Engineers järjestö, jonka toimintaa tietotekniikan standardoiminen on

IP-osoite Internet Protocol osoite, Internetissä tietokoneen tunnistamiseen käytettävä numero

ISM Industrial, Scientific and Medical, taajuusalue, jonka käyttö ei vaadi lupaa.

LAN Local Area Network, lähiverkko

MAC Media Access Control, verkossa liikennöintiin käytetty järjestelmä, myös laitteen verkkosovittimen yksilöivä numero

Mbit/s Megabittiä sekunnissa

MHz Megahertsi, taajuudenyksikkö

MIMO Multiple input, multiple output

MISO Multiple input, single output

NAT Network address transform, IP-osoitteen muuntomenetelmä

OFDM Orthogonal frequency-division multiplexing, yleinen modulointitekniikka

OSI-malli Open Systems Interconnection Reference Model, tiedonsiirtoprotokollien kuvaamiseen käytetty 7-kerroksinen malli

PN-koodi Pseudorandom Noise -koodi

PSK  Pre-shared key, salausmetodi

PSK Phase Shift Keying, vaiheavainnus, modulaatiomenetelmä

QAM Quadrature Amplitude Modulation, vaihe- ja amplitudimodulaatiomenetelmä

QPSK Quadrature Phase Shift Keying, nelivaiheinen vaiheavainnus, modulaatio-menetelmä

RTS Ready-to-Send viesti, jolla laite ilmoittaa olevansa valmis lähettämään

SIMO Single input, multiple input

SSID service set identifier, WLANin verkkotunnus

TKIP Temporal Key Integrity Protocol, WLANin tietoturvaprotokolla

WEP Wired equivalent privacy, WLANin salausmenetelmä

WLAN Wireless Local Area Network, langaton lähiverkko

WPA Wireless protected access, WLANin salausmenetelmä

VTT Valtion teknologian tutkimuskeskus

# 1 JOHDANTO

WLAN-tekniikka on nykyisin laajalti käytössä. 802.11-standardiperheen kehitys alkoi jo vuonna 1991 ja ensimmäiset käytännölliset ratkaisut hyväksyttiin standardiksi vuonna 1997. Tämän jälkeen kehitystahti on ollut kiivasta, ja nykyisin WLANilla saavutetaan jopa 600 Mbit/s nopeuksia. Verkkojen turvallisuus on parantunut vuosien mittaan paljon.

Avoimia langattomia lähiverkkoja löytyy ympäri maailmaa, mutta kaupunkien laajuiset verkot ovat harvinaisia. Lahden MASTONET on yksi Suomen laajimmista langattomista lähiverkoista, ja sitä ylläpitää Lahden ammattikorkeakoulu Lahden kaupungin rahoituksen turvin. Avoimien WLAN-verkkojen tarve kasvaa, kun uudet älypuhelimet ja tablettitietokoneet yleistyvät. Ihmiset liikkuvat enemmän ja hakevat enemmän tietoa tietoverkoista.

Tämän opinnäytetyön tavoitteena oli tutkia käyttäjien kokemuksia MASTONETin toiminnasta ja mielipiteitä siitä kuinka verkkoa tulisi kehittää.
MASTONETin käyttäjille lähetettiin kysely, jossa pyydettiin vastaamaan verkon toimintaan liittyviin kysymyksiin. Lisäksi kyseltiin käyttäjien mielipiteitä, kuinka MASTONETiä tulisi heidän mielestään kehittää ja millaisilla laitteilla he verkkoa käyttävät. Kysely lähetettiin MASTONETin käyttäjätukeen yhteydessä olleille käyttäjille.

# 2 LANGATTOMAN LÄHIVERKON HISTORIA

Maailman ensimmäinen langaton lähiverkko rakennettiin jo 1970-luvulla Hawajin yliopistossa. Tämä verkko koostui seitsemästä tietokoneesta neljällä eri saarella (Johns Hopkins School of Public Health 2007). Verkko oli nimeltään ALOHAnet, joka oli kokeellinen verkko, jossa käytettiin halpoja käsiradioita. Tämä oli ensimmäinen toimiva langaton dataverkko. (Wikipedia 2010.)

Vuonna 1979 Geller ja Bapst julkaisi tutkimuksen, jossa käytettiin infrapunaa tiedonsiirrossa tietokoneiden välillä. Hieman myöhemmin julkaistiin ensimmäiset raportit hajaspektritekniikan käytöstä testiolosuhteissa. Vuonna 1984 IEEE julkaisi tutkimuksen infrapunaa ja radiotietä käyttävien tekniikoiden toimivuudesta toimistoympäristössä. Seuraavana vuonna otettiin käyttöön ISM-taajuudet, joilla testattiin ensimmäisiä käytännön sovelluksia hajaspektritekniikassa. (IEEE 1996.)

Ensimmäiset WLAN (Wireless Local Area Network, eli langaton lähiverkko) 802.11-standardit julkaistiin vuonna 1997, mutta ensimmäiset luonnokset tekniikan standardoinnista löytyvät jo vuodelta 1991 (IEEE 2012). 802.11-standardia kutsutaan nimillä langaton Ethernet (wireless Ethernet), WLAN sekä Wi-Fi, viimeisin näistä on markkinointinimi, jota käyttää Wi-Fi konsortio, joka on perustettu standardin luoneen työryhmän päälle (Gast 2002, 16). Lisäksi Suomessa on yleistynyt termi langaton lähiverkko.

# 3 802.11 STANDARDIPERHE

## 3.1 802.11

802.11-standardi julkaistiin vuonna 1997 ja se määritteli käytännössä koko langattoman lähiverkon tulevaisuuden tekniikan OSI-mallin fyysisen kerroksen sekä siirtokerroksen toiminnan. Välitystekniikoita standardissa on radiotie sekä infrapuna, joista jälkimmäinen on sittemmin unohdettu lähes tyystin eikä infrapunalle perustuvia käytännön sovelluksia ole juurikaan tehty. Radiotaajuuksille välitystekniikoiksi valittiin suorasekvenssihajaspektri- (DSSS) sekä taajuushyppelyhajaspektri- (FHSS) tekniikat taajuusalueen ollessa 2,4 GHz. Kaistanleveydeksi on määritelty 20 MHz, jota käytetään myös 802.11a-, 802.11g- ja 802.11n-standardeissa.

Verkon käytännön jakaminen toteutetaan CSMA/CA:lla (Carrier Sense Multiple Access/Collision Avoidance), jonka avulla laitteet kommunikoivat verkossa välttäen törmäyksiä lähettäen verkon varaustiedon ennen varsinaista tiedonsiirtoa. Tämä tapahtuu käytännössä niin, että kaikki verkossa olevat laitteet kuuntelevat jatkuvasti verkkoa ja siellä tapahtuvaa liikennöintiä, ja kun laite haluaa lähettää tietoa, lähettää laite verkkoon RTS (request-to-send, pyyntö lähettää) paketin, jolla se pyrkii varaamaan verkon käyttöönsä. Tämän jälkeen muut laitteet hiljenevät, kun lähetystä odottava laite saa CTS (clear-to-send, vapaa lähettämään) paketin verkon tukiasemalta. CSMA/CA on käytössä kaikissa WLAN-stardardin versioissa.

802.11-standardilla saavutettiin yhden-kahden megabitin nopeuksia. Tekniikan tarjoama verkon kantama ei ollut vielä kovin käytännöllinen, maksimin ollessa sisätiloissa noin kaksikymmentä metriä ja käytännössä vielä pienempi. 802.11-standardi ei myöskään tarjonnut kovin suuria nopeuksia, vaan standardin määrittelemä suurin nopeus on kaksi megabittiä sekunnissa, johon kuuluu kaikki verkon liikenne. Näin itse datan siirrolle jää maksimissaan noin puolet kaistasta.

## 3.2 802.11a

802.11a julkaistiin alun perin 1997 lisäyksenä 802.11-standardiin. Vuonna 2007 802.11a lisättiin 802.11-standardin osaksi. 802.11a:n tärkeimpinä määrityksinä on 54 Mbps nopeus käyttäen 5 GHz:n taajuusaluetta. Taajuusalueiksi on määritelty 5.15–5.35 ja 5.725–5.825 GHz, mutta käytössä olevat taajuusalueet vaihtelevat eri maissa lainsäädännön ja muiden samaa taajuusaluetta käyttävien palveluiden takia. Taajuusalue on jaettu 200 kanavaan, joiden keskitaajuus saadaan kaavalla keskitaajuus=5000 + 5 x $n_{kanava}$, jossa $n_{kanava}$ on 0,1…200. Näin taajuusalue 5-6 GHz saadaan jaettua uniikeiksi kanaviksi, mutta samalla saadaan joustavuutta kanavoinnille eri maissa. (IEEE-SA Standards Board 2003.)

Taajuusalue nostettiin 5 GHz, jotta kaistanleveyttä ja samalla verkon maksiminopeutta saatiin kasvatettua. Taajuusalueen nosto vaikuttaa verkon kantoalueeseen ja seinien ja muiden esteiden läpäisykykyyn alentavasti. Käytössä on OFDM (Orthogonal frequency-division multiplexing) modulaatio. Käytössä on 52 lomittaista alakanavaa, joita moduloidaan käyttäen BPSK- tai QPSK-modulaatiota ja nopeammille datanopeuksille käytössä on QAM-16- tai QAM-64-modulaatiot. Nämä 300 kHz leveät kaistat yhdistetään niin, että saadaan 20 MHz:in kaista tiedonsiirtoa varten (Aspinwall 2003, 7).

Virheenkorjaus toteutetaan 802.11a:ssa käyttäen konvoluutiokoodausta. Standardin mukaisten laitteiden on tuettava lähetyksessä ja vastaanotossa nopeuksia 6, 12 ja 24 Mbit/s. Kuitenkin käytännössä kaikki laitteet tukevat myös nopeuksia 9, 18, 36, 48 ja 54 Mbit/s. Nämä nopeusluokat ovat teoreettisia maksiminopeuksia siirtotielle, ja käytännön nopeudet jäävät usein alle puoleen tästä, käytännön maksimin ollessa puolet teoreettisesta maksiminopeudesta.

### 3.3 802.11b

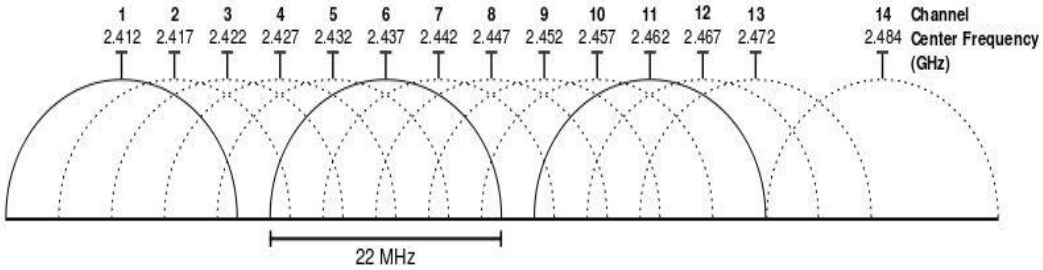
Samalla kun 802.11-standardia selkeytettiin ja julkaistiin lopullisesti vuonna 1999, hyväksyttiin myös lisäys 802.11b, joka määritteli ensimmäisen laajasti käyttöön levinneen WLAN-tekniikan. 802.11b toimii 2.4 GHz:n taajuusalueella, joka kuuluu ISM (industrial, scientific and medical) taajuusalueisiin, jotka ovat vapaasti käytettävissä teollisuuden, tieteen ja lääketieteen tarpeisiin. Koska tämä 2,4 GHz:n taajuusalue on vapaasti käytössä, voi tällä taajuudella toteutettu WLAN-verkko kärsiä erilaisista häiriötekijöistä, esimerkiksi mikroaaltouuneista tai Bluetooth-laitteista, jotka voivat häiritä 802.11b verkon signaaleja.

802.11b käyttää jo alkuperäisessä standardissa ollutta DSSS suorasekvenssihajaspektri-tekniikkaa tiedonsiirtoon, FHSS unohdettiin tyystin. 802.11b-standardi toi WLAN:iin myös uuden modulaatiotekniikan CCK:n. Kuten samoihin aikoihin julkaistu 802.11a, käyttää 802.11b-standardi OFDM-modulointia käyttäen Euroopassa 13 lomittaista kanavaa. Yhdysvalloissa on käytössä 11 kanavaa ja Japanissa 14. Kaistanleveydeksi on määritelty 22 MHz. Yksi 802.11b kanava varaa 25 MHz-laajuisen taajuuskaistan. Kanavan varaaman taajuusalueen ala- ja yläpäässä on molemmissa 1 MHz:n suoja-alue. Japanissa käytettyä kanavanumero 14:ää lukuun ottamatta kanavat sijaitsevat 5 MHz:n päässä toisistaan taajuusalueella, joten toisiaan häiritsemättömiä kanavia on Euroopassa kolme. (IEEE-SA Standards Board 2003.)

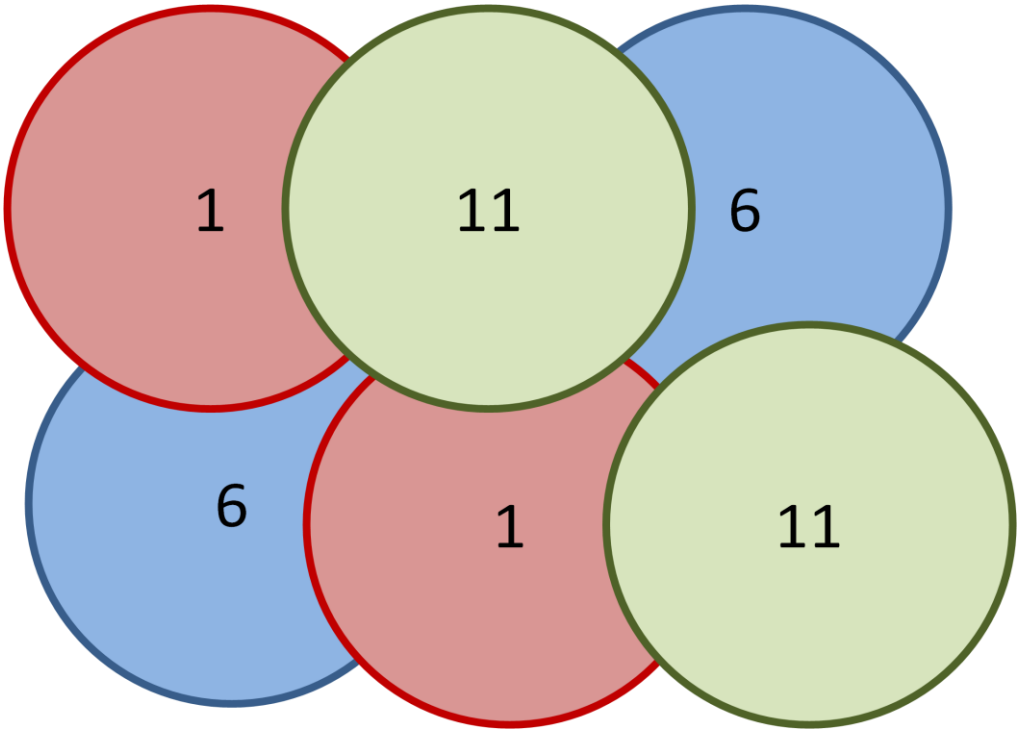
Koska b-lisäys toimii alemmalla taajuusalueella ja pienemmillä kaistanleveyksillä kuin 802.11a, 802.11b:n teoreettinen maksiminopeus on huomattavasti pienempi kuin 802.11a:n tarjoama 54 Mbit/s maksimi. 802.11b:n teoreettinen maksiminopeus on standardin mukaan 11 Mbit/s, ja kuten a-lisäyksen kanssa, käytännön nopeus on noin puolet tästä. Toisaalta verkon kantoalue on suurempi pienemmän taajuuden ansiosta. Lisäksi verkon kuuluvuus esteiden läpi paranee, kun taajuusalue on alempi.

## 3.4 802.11g

Muutaman vuoden päästä 802.11b:n käyttöönoton jälkeen valmistui kolmas lisäys WLAN-standardijoukkoon, 802.11g, joka toi 802.11a-standardista tutun 54 Mbit/s nopeuden 2.4 GHz taajuusalueelle. Standardi hyväksyttiin vuonna 2003. Koska taajuusalue on sama kuin edeltäjässä 802.11b-standardissa, on uusi 802.11g yhteensopiva edeltäjänsä kanssa, eli laitteet, jotka tukevat vain 802.11b-standardia, voivat liikennöidä 802.11g-standardin varaan rakennetussa verkossa. Toisaalta myös 802.11g laitteet voivat käyttää 802.11b-standardin verkkoja. 802.11g verkossa voidaan 802.11b-standardin tavoin käyttämällä kolmea riittävällä taajuuserolla erotettua taajuuskanavaa (kuvio 1) toteuttaa alueen täysin kattava verkko (kuvio 2), sillä oletuksella, ettei verkon kantoalueen sisällä ole juurikaan muita häiriötekijöitä kuten seiniä, niin etteivät viereiset tukiasemat häiritse toisiaan. (IEEE-SA Standards Board 2003.)




KUVIO 1. 802.11g kanavajako (Wikipedia 2012)




KUVIO 2. Kolmella kanavalla toteutettu WLAN-verkko, jossa vierekkäiset tukiasemat eivät häiritse toisiaan.

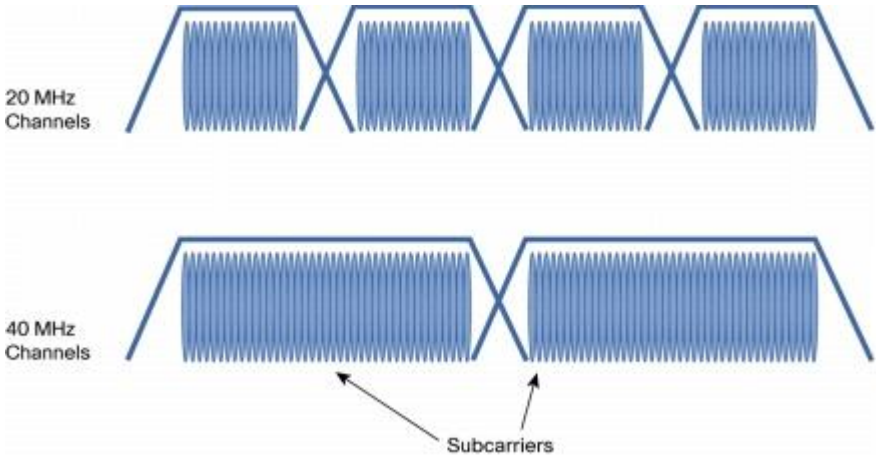
802.11g:ssä on otettu käyttöön 802.11a:sta tuttu OFDM-modulaatiomenetelmä, jolla saavutetaan 54 Mbit/s teoreettinen maksiminopeus. Toisaalta, koska standardi haluttiin yhteensopivaksi 802.11b-standardin kanssa, on 802.11g-standardiin jätetty 802.11b-standardista tutut CCK-modulaatiomenetelmä sekä tiedonsiirtomenetelmä DSSS. 802.11g käyttää myös samaa kokonaiskaistanleveyttä 25 MHz, vaikka itse tiedonsiirtoon käytetäänkin 20 MHz kaistanleveyttä. Kuten 802.11-standardissa, 2,4 GHz taajuusalueen käyttö voi aiheuttaa ongelmia verkon toiminnalle. Lisäksi ongelmia aiheuttaa WLAN-verkkojen määrä, joka aiheuttaa ylikuulumista, jossa viereisillä kanavilla toimivat WLAN-verkot häiritsevät toisiaan. (Gast 2012, 16.)

### 3.5 802.11n

Jo ennen kuin 802.11g-standardi oli hyväksytty, oli aloitettu uuden, nopeamman standardin kehittäminen. Uuden standardin nimeksi tuli 802.11n, jonka tärkein uusi ominaisuus on moninkertaistunut teoreettinen maksiminopeus, jopa 600 Mbit/s, joka saavutetaan käyttäen MIMO-tekniikkaa ja suurempaa kaistanleveyttä 40 MHz. 802.11n-standardissa on määritelty kaksi taajuusaluetta. 802.11a-standardissa käytössä oleva 5 GHz, sekä 802.11b- ja g-standardeissa käytetty 2,4 GHz taajuusalueet. Samalla 802.11n-standardi on täysin taaksepäin yhteensopiva aiempien standardien kanssa.

Standardin toisen vedosversion (draft 2.0) mukaisia laitteita alettiin sertifioida vuonna 2007. Sertifiointi varmisti eri valmistajien laitteiden toimimisen muiden valmistajien laiteiden kanssa, samalla sertifioitujen laitteiden ominaisuudet saatiin samalle vähimmäistasolle. Vähimmäistasolla vaatimuksiin kuului tuki sekä 5 GHz:n että 2,4 GHz:n taajuusalueille käyttäen 20 MHz:n ja 40 MHz:n kaistanleveyttä (kuvio 3).

802.11n-standardin mukaiset suuret siirtonopeudet toteutetaan käyttämällä 40 MHz:n kaistanleveyttä ja jopa neljää kanavaa yhtä aikaa. Tämä aiheuttaa 2,4 GHz taajuusaluetta käytettäessä ongelmia, jos verkon kuuluvuusalueella on muita samaa taajuusaluetta käyttäviä verkkoja, koska 4 yhtäaikaisen kanavan käyttäminen vie suuren osan vapaasti käytössä olevalta 2,4 GHz taajuusalueelta.



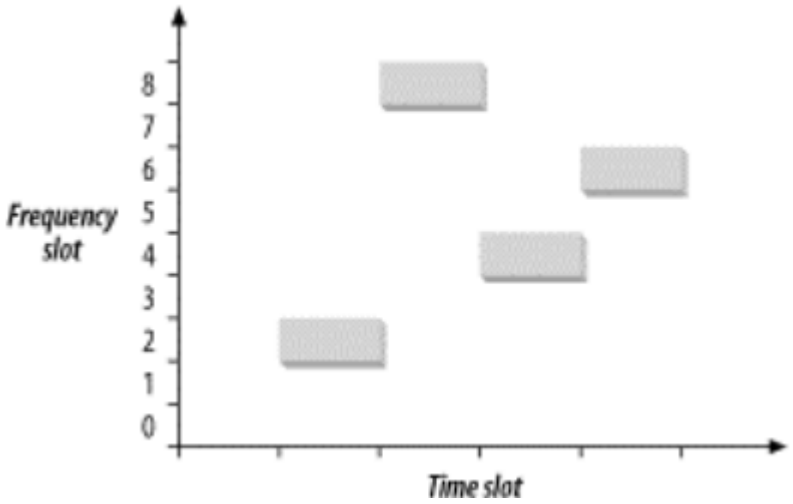

KUVIO 3. 40 MHz:n kaistanleveys verrattuna 20 MHz:n kaistanleveyteen. Saha-aalto kuvaa OFDM-alikantoaaltoja (Cisco Inc. 2012.)

# 4 WLAN-TEKNIIKAT

## 4.1 FHSS

FHSS eli taajuushyppely oli mukana jo vuonna 1997 julkaistussa 802.11-standardissa ja oli ensimmäinen modulaatiotekniikka, joka oli laajemmin käytössä. Suurin hyöty taajuushyppelyn käytöstä on mahdollisuus saada useat verkot toimimaan samalla alueella samalla taajuuskanavalla toimimaan samanaikaisesti. FHSS:ää ei enää WLAN-tekniikassa käytetä, sillä taajuushyppely oli käytössä vain ensimmäisessä 802.11-perheen standardissa. FHSS:n tarvitsema teknologia oli halpaa jo WLAN-tekniikan alkuaikoina. FHSS käyttää myös vähemmän virtaa absoluuttisesti katsottuna kuin DSSS tai uudemmat modulaatiomenetelmät. Lähetettyä databittiä kohden virrankulutus on pienentynyt uusissa tekniikoissa. (Gast 2012, 170 – 175.)

Taajuushyppely toimii nimensä mukaisesti taajuushyppelyllä. Käytetty taajuuskaista jaetaan tasaisiin taajuusväleihin. Aikavälit ovat ortogonaalisia ja kestoltaan 40 millisekuntia. Aikavälejä on 802.11-standardissa käytössä 390 kappaletta. Jokaista taajuusväliä voidaan käyttää samanaikaisesti, mutta samalla aikavälillä ei voida liikennöidä samalla taajuusvälillä (kuvio 4). Toisaalta myös useampi eri verkko voi liikennöidä käyttäen samaa taajuusaluetta, kunhan huolehditaan, että jokainen verkko käyttää samalla aikavälillä eri taajuuksia liikennöintiin. (Gast 2012, 170 – 175.)



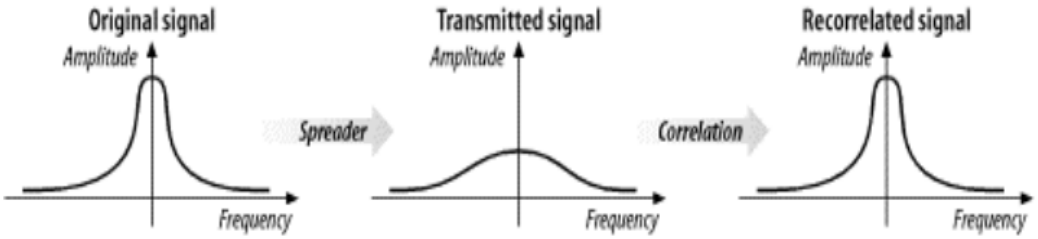

KUVIO 4. Taajuushyppely esitettynä koordinaatistossa: pystyakselilla taajuusväli, vaaka-akselilla aikaväli (Gast 2012, 171)

## 4.2 DSSS, PSK ja CCK

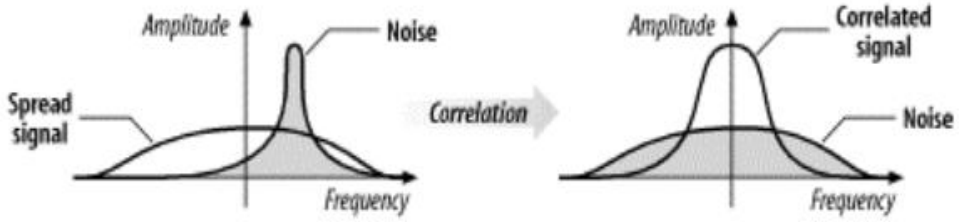
DSSS eli suorasekvensoinnilla tarkoitetaan tekniikkaa, jossa lähetettävä sanoma jaetaan osiin ja lähetetään yhtenä signaalina käyttäen koko taajuusaluetta. Tiedonsiirto tapahtuu sekoittamalla lähetettävä pieninopeuksinen datasignaali kohinan kaltaiseen suurinopeuksiseen kantoaaltoon. Tämä kohina tunnetaan englannin kielessä termillä chiping stream ja myös lyhenteellä PN-koodi (pseudorandom noise, näennäissatunnainen kohina). Vastaanotin tunnistaa satunnaisen kohinan, jonka jälkeen viestin poimiminen kohinan seasta on helppoa, sillä lähetettävä viesti voidaan tulkita, vaikka lähetettävän viestin voimakkuus olisi 10 dB kohinaa vaimeampi. (Gast 2012, 181 – 186.)

Datasignaali luodaan levittämällä lähetettävä kapea datasignaali laajalle taajuuskaistalle, vastaanotin näkee tämän matalatasoisena kohinana. Ideana tässä on laajan taajuuskaistan valvonta, mitä jokainen vastaanotin tekee. Vastaanotin havaitsee signaalissa tapahtuvan laajakaistaisen muutoksen. Kun vastaanotin poimii tämän koko laajalle kaistalle levitetyn signaalin ja tiivistää signaalin, saadaan aikaan alkuperäinen lähetetty datasignaali (kuvio 5). Suurinopeuksinen ja kapeakaistainen kohina, jota signaalissa esiintyy, levitetään vastaanottimessa laajalle kaistalle, jotta saatu datasignaali saadaan paremmin esille (kuvio 6). Signaalinkä-

sittely, jossa siis datasignaali levitetään tiedonsiirtoa varten ja kohina levitetään vastaanottimessa, lisää suuresti DSSS:n häiriönsietokykyä.
(Gast 2012, 181 – 186.)




KUVIO 5. Vasemmalla lähetettävä tieto signaalimuodossa. Keskellä lähetetty signaali ja oikealla vastaanotettu signaali. (Gast 2012.)




KUVIO 6. Vasemmalla kuvattu signaali siirtotiellä, tummennettu käyrä on kohinaa. Oikealla korjattu signaali, josta lähetetty viesti on poimittavissa. (Gast 2012.)

DSSS käyttää Barker-koodausta 11 MHz:n ajoitustaajuudella PN-koodin luomiseen. PN-koodi on itse asiassa binäärinen bitti, jota käytetään datasignaalin levitykseen. Nimitystä PN-koodi käytetään merkitsemään ohjausbittejä, jotta ohjausbittejä ei sotkettaisi databitteihin. PN-koodi lähetetään suurella bittinopeudella ja jokaista tietobittiä varten lähetetään kaksi PN-koodia. Yhdistetyt databitti ja kaksi PN-koodia lähetetään siirtotielle suurella bittinopeudella. Vastaanotin vertaa vastaanotettua signaalia samaan PN-koodisekvenssiin selvittääkseen vastaanotetun tietobitin sisällön. DSSS vie laitteilta enemmän virtaa ja kuluttaa enemmän taajuuksia käytettävissä olevalta taajuuskaistalta kuin FHSS saavuttaakseen saman tiedonsiirtonopeuden. (Gast 2012, 181 – 186.)

CCK-modulaatiotekniikka otettiin käyttöön 802.11b-standardissa, jotta yli 2 Mbit/s tiedonsiirtonopeudet olisivat mahdollisia. CCK käyttää ns. Baker-koodausta, tosin käyttäen lyhyempää ja useampaa katkaisusekvenssiä. Käytössä on jopa 64 kappaletta 8-bittisiä sekvenssejä, jolla saavutetaan 802.11b-standardin maksimi 11 Mbit/s nopeus. Alkuperäinen Baker-koodaus käyttää yhtä katkaisusekvenssiä, jonka pituus on 11 bittiä. (Gast 2012, 194.)

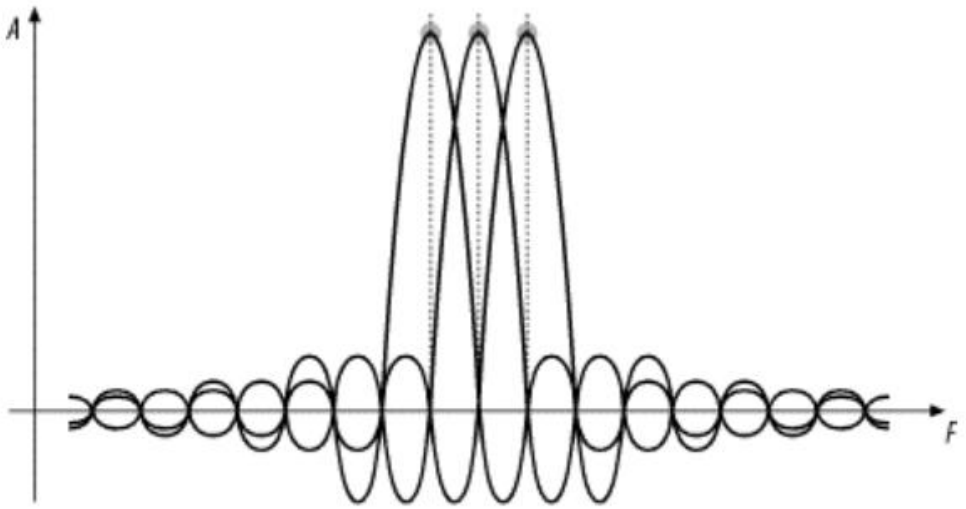
PSK on modulaatiomenetelmä, jossa kantoaallon vaihetta muuttamalla saavutetaan vaihe-eroja, joka merkitsevät tiettyä numeroarvoa. WLAN-tekniikassa on käytössä BPSK sekä QPSK, joista ensimmäisenä mainittu käyttää kahta vaihe-eroa (0 astetta ja 180 astetta) ja jälkimmäinen käyttää neljää vaihe-eroa (0 astetta, 90 astetta, 180 astetta ja 270 astetta). BPSK-moduloinnissa voidaan esittää vain yksi bitti kerrallaan 0 tai 1. QPSK-modulointi on tehokkaampi, ja sillä voidaan esittää kaksi bittiä kerrallaan, joilla saadaan aikaan neljä eri arvoa. (Wikipedia 2012b.)

## 4.3 OFDM

OFDM ei ole uusi menetelmä, vaan tekniikkaa alettiin kehittää jo 1960-luvun loppupuolella ja OFDM patentoitiin jo vuonna 1970. Koska langaton tiedonsiirtoteknologia ei ollut 1970-luvulla vielä kovinkaan kehittynyttä, ei tekniikka mahdollistanut modulointimenetelmän käyttöä. Uudet signaalinkäsittelymenetelmät mahdollistavat OFDM:n nykyisen käytön. (Gast 2012, 204 – 209.)

OFDM-modulaatiomenetelmä käyttää ortogonaalisesti jaettuja taajuusalueita. Käytännössä tämä tarkoittaa signaalin modulointia usealle vierekkäiselle toisiaan häiritsemättömälle kantataajuudelle. OFDM jakaa käytössä olevan laajan taajuuskanavan (esim. 802.11g:ssä kaistanleveys on 22 MHz) pienempiin alikanaviin (kuvio 7). Jokainen alikanava osallistuu tiedonsiirtoon. Alikanavat, joiden kaistanleveys on pieni, ja siten myös tiedonsiirtonopeus on rajallinen, multipleksataan yhdeksi laajakaistaiseksi signaaliksi, jonka bittinopeus on suuri. Kuviossa 7 on nähtävissä alikanavien tarkka ortogonaalinen sijoittelu, sillä vaikka signaalit me-

nevät limittäin, on yhden taajuuden ollessa amplitudin huipussa, muut alikanavat ovat amplitudiltaan nollassa.(Gast 2012, 164.)



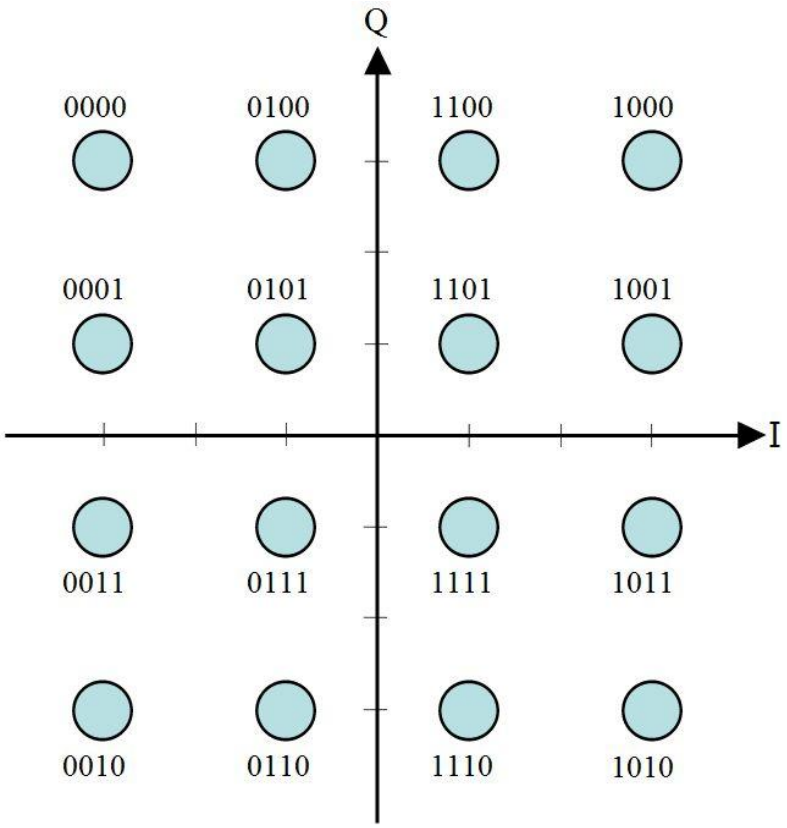

KUVIO 7. OFDM-signaali kolmella alikantoaallolla esitettynä spektrimuodossa. (Gast 2012.)

OFDM-signaali puretaan vastaanottimessa käyttäen käänteistä Fourier-muunnosta. Fourier-muunnos on suhteellisen raskas toimenpide, mutta nykyisille DSP-prosessoreilla varustetuille WLAN-laitteille muunnos ei ole ongelma. OFDM sietää häiriöitä, mutta on herkkä kantoaaltojen väliselle häiriölle (inter-carrier Interference), jossa hyvin lähekkäin olevat alikantoaallot häiritsevät toisiaan, esimerkiksi Dopplerin ilmiön aiheuttaman taajuuden muuttumisen takia. Myös symbolien välinen häiriö (inter-symbol interference) on mahdollista OFDM-moduloidussa signaalissa. Symbolien välinen häiriö johtuu esimerkiksi heijastuneista signaaleista, jotka tulevat vastaanottajalle myöhässä oikeaan signaaliin nähden. Näitä torjutaan käyttämällä suoja-aikoja jokaisen lähetetyn symbolin välissä. Fourier-muunnos suoritetaan vain suoja-aikojen välissä olevalle signaalille. Lisäksi virheitä torjutaan käyttämällä konvoluutiokoodausta. Konvoluutiokoodauksessa jokaista lähetettyä databittiä kohden lähetetään tietty määrä koodibittejä. Lähetettyjen koodibittien suhdetta databitteihin kuvataan yleensä kirjaimella R (esim. R=1/2 tarkoittaa kahden koodibitin lähetystä yhtä databittiä kohden). (Gast 2012, 204 - 209.)

## 4.4 QAM

QAM-modulaatiomenetelmä yhdistää PSK-moduloinnista tutun vaihemodulaation amplitudimodulaatioon. Modulaatiotekniikalla moduloidaan yleensä kahta eri vaihesiirrossa olevaa kantoaaltoa toisistaan riippumatta muokkaamalla sekä signaalin amplitudia että vaihekulmaa. QAM-modulaatio on helpoin käsittää käyttämällä konstellaatiokuvaajaa, jossa arvot kuvataan koordinaatistossa (kuvio 8).

Konstellaatiokuvaajassa amplitudi esitetään etäisyytenä kuvaajan keskipisteestä ja vaihe esitetään kulmana. QAM:ssa on useampia tasoja, joista 4-QAM on käytännössä sama kuin QPSK. Jokaisella tason nostolla saadaan samanaikaisesti moduloitujen symbolien lukumäärää nostettua, jolloin esimerkiksi 64-QAM-moduloinnilla voidaan yhdellä 64-QAM symbolilla välittää 6 bittiä tietoa. (Wikipedia 2012c.)




KUVIO 8. Kuvaajassa esitetty 16-QAM. Kuvaajan vaaka-akselia nimitetään reaaliosaksi ja pystyakselia imaginaariosaksi. (Wikipedia 2012c.)

## 4.5 MIMO

MIMO:lla tarkoitetaan tekniikkaa, jolla verkossa tapahtuvaan liikennöintiin käytetään useampaa kuin yhtä antennia. WLAN-standardeista MIMO-tekniikkaa käytetään vain uusimmassa 802.11n-standardissa, jossa MIMO on valinnainen tekniikka, jolla saavutetaan vanhempia 802.11a/b/g-standardeja nopeampi tiedonsiirtokyky. Teoriassa lähetin- ja vastaanotinantenneja voi olla loputtomasti, käytännössä antennien määrää rajoittaa käytettävissä oleva taajuusalue. (Hall 2009.)

WLANissa on usein käytössä MIMOn menetelmä, jossa tukiasemassa on kaksi antennia, mutta päätelaitteessa on vain yksi. Tätä tilannetta kuvataan useimmiten MISO/SIMO-tilaksi, sen mukaan kumpi laite lähettää ja kumpi ottaa vastaan. On myös mahdollista etteivät tukiaseman molemmat antennit toimi tai muusta syystä ole päätelaitteen käytettävissä, jolloin tukiasema käyttää normaalia yhden antennin tekniikkaa, jossa yksi antenni lähettää sekä vastaanottaa signaalit. (Hall, D. 2009)

## 4.6 Tukiasemat

Langattomat lähiverkot rakennetaan yleensä tähtitopologiaa noudattaen tukiaseman ympärille. Tukiasema vastaa langallisen lähiverkon käyttämää keskitintä (hub). Koska radiotiellä ei voida erikseen määritellä, mille päätelaitteelle viesti lähetetään, viestit lähtevät aina kaikille laitteen kuuluvuusalueella oleville laitteille. Tukiaseman tehtävänä on useimmiten myös liikennöinti WLAN-verkon ulkopuoliseen verkkoon toimien rajapintana WLAN-verkon ja ulkomaailman välillä. (Gast 2002, 22.)

Tukiasematyyppejä on monia. Yleisin malli on kotikäytössä oleva WLAN-reititin, joka toimii samalla ADSL- tai kaapelimodeemina sekä palomuurina ja NAT-laitteena. Laitteet on yleensä valmiiksi määritelty toimimaan WLAN-tukiasemana, mutta toiminto on mahdollista kytkeä pois päältä käyttäjän niin halutessa. Tällainen laite löytyy lähes jokaisesta suomalaisesta kodista (Tilastokeskus 2006).

Toinen tukiasemamalli on käytössä yleensä laajemmissa verkoissa, kuten yrityksien omissa langattomissa lähiverkoissa mutta toisaalta myös esimerkiksi Lahden MASTONET-verkossa. Nämä laitteet toimivat toisella tavalla kuin kotikäytössä olevat WLAN-tukiasemat. Laajoissa verkoissa voidaan käyttää yhtä tai useampaa WLAN-kontrolleria, joka itse asiassa hoitaa liikennöinnin ja verkon ohjaamisen. Kontrolleriin yhdistetään yleensä useita ns. radioita, jotka toimivat tukiasemina, verkon kuuluvuusalueen laajentamiseksi. Tällä tavoin yhden WLAN-verkon toiminta-alue on teoriassa rajaton ja tukiasemien väliset mahdolliset häiriöt voidaan minimoida.

## 4.7 Päätelaitteet

WLAN yhteensopivia päätelaitteita on nykyisin valtavasti. Käytännössä kaikki uudet kannettavat laitteet matkapuhelimet ja musiikkisoittimet tukevat WLAN:a. Lisäksi on saatavilla WLAN-sovittimia muihin laitteisiin, jopa televisioihin ja digitaalisiin järjestelmäkameroihin.

WLANin taaksepäin yhteensopivuus helpottaa vanhempien päätelaitteiden käyttöä uusissakin 802.11n-standardin verkoissa. Toisaalta myös uudet päätelaitteet toimivat vanhaa 802.11-standardia käyttävässä verkossa. Vuonna 2009 maailmassa oli 550 miljoonaa WLAN yhteensopivaa päätelaitetta, ja määrän uskotaan kasvavan 1,7 miljardiin vuoteen 2015 mennessä (Instat 2010).

# 5 SALAUSTEKNIIKAT

## 5.1 WEP

WLAN-verkkojen tietoturvaa voidaan parantaa ottamalla käyttöön jokin tarjolla olevista salausmenetelmistä. Käytettävä salausmenetelmä voi rajoittaa joidenkin päätelaitteiden kykyä yhdistää verkkoon, jos päätelaite ei tue käytettyä salausmenetelmää. Verkon salaaminen on nykyisin hyvin suositeltua, ja on myös suositeltavaa käyttää salaamiseen mahdollisimman uutta salausmetodia, kuten WPA2:ta.

WEP-salaus sisällytettiin ensimmäiseen 802.11-standardiin, tosin vain 40-bittisen salausavaimen kanssa johtuen Yhdysvaltain tiukoista vientimääräyksistä, jotka koskevat laitteita, joissa on käytössä tiedon salaamiseen käytettyjä tekniikoita. WEP käyttää RSA Security-yhtiön kehittämää RC4-salausmenetelmää, joka perustuu symmetriseen salaukseen. Käytännössä lähetettävä tieto salataan RC4-algoritmilla lasketulla salausavaimella ja vastaanottaja purkaa tiedon samalla salausavaimella. (Gast 2012, 96 - 107)

WEP-salauksessa käytetty RC4-salausalgoritmi on havaittu puutteelliseksi ja WEP-salaus on murrettu täysin. Salauksen purkaminen onnistuu helposti jopa ”kotikonstein” käyttämällä yleisesti saatavilla olevia ohjelmistoja. Salauksen murtaminen tapahtuu yksinkertaisesti kuuntelemalla WEP-salausta käyttävää verkkoa ja keräämällä verkossa kulkevia paketteja riittävä määrä; kun tietoa on riittävästi, on kerätyistä paketeista helppo laskea käytössä oleva salausavain. WEP-salauksen ongelmien takia tätä salausmenetelmää ei suositella käytettäväksi kuin pakkotilanteissa. (Gast 2012, 96 - 107.)

## 5.2 WPA

WPA-salaus kehitettiin pikaisesti korjaamaan WEP-salauksessa kohdatut puutteet ja ongelmat. WPA oli eräänlainen väliaikaisratkaisu salausongelmiin WLAN-verkoissa. WEP-salausta kehitettiin edelleen ja käyttöön otettiin TKIP-protokolla, joka käyttää jokaiselle lähetetylle paketille omaa salausavainta, jolloin WEP-salauksen murtoon käytetty pakettien keruuseen perustuva verkkoon murtautuminen ei onnistu. TKIP-avain on 128-bittinen, eli moninkertainen WEP-salauksessa käytettyyn 40-bittiseen verrattuna. Käytössä on WEP-salauksessakin käytetty RC4-salausalgoritmi. TKIP vaatii erillisen autentikointipalvelimen, jolla salausavaimisto tuotetaan. Tästä johtuen TKIP-protokollaan perustuvaa WPA-salausta käytetään useimmiten vain laajoissa verkoissa. (Aspinwall 2003, 276 – 277.)

WPA sisältää myös ilman erillistä salauspalvelinta toimivan salausmetodin, PSKn. Siinä jokainen verkossa liikennöivä laite salaa lähettämänsä tiedon ennalta määrätyllä salausavaimella, jonka pituus on 256 bittiä. Salausavain voi koostua joko 64 heksadesimaalimerkistä tai ASCII muodossa olevista kirjaimista, jolloin avaimen pituus on 8 - 63 merkkiä. (Aspinwall2003, 276 – 277.)

## 5.3 WPA2

WPA2 on WiFi allianssin käyttämä nimitys 802.11i-standardista. WPA2 tuo WPA-salauksesta tuttujen menetelmien lisäksi mahdollisuuden käyttää AES-salausalgoritmia, joka poikkeaa suuresti aiempien salausmenetelmien käyttämästä RC4-salausalgoritmista. AES-algoritmi vaatii sitä tukevalta laitteelta erillisen salauspiirin. AES-salausalgoritmi on vapaasti saatavilla oleva symmetrinen salausmetodi ja on tähän päivään mennessä murtamaton. WPA2:ssa voidaan käyttää AES:in 256-bittistä salausavainta. Toisin kuin RC4, AES-salaus perustuu pakettisalaukseen jossa salattu paketti on aina samankokoinen. (Benton 2010.)

WPA2 käyttää myös uutta kättelymenetelmää, joka on nelivaiheinen. Tämä kättely tapahtuu niin, että tukiasema lähettää kertaluonteisen salatun paketin päätelaitteelle, joka tämän lähetetyn paketin avulla muodostaa uuden salausavaimen, jonka päätelaite lähettää sitten tukiasemalle. Tukiasema muodostaa jälleen uuden salausavaimen, joka muodostetaan käyttäen tukiaseman alkuperäistä viestiä, päätelaitteen lähettämää viestiä, tukiaseman MAC-osoitetta ja päätelaitteen MAC-osoitetta. Tämän jälkeen tukiasema lähettää salausavaimen päätelaitteelle joka hyväksyy salausavaimen ja kuittaa tiedon tukiasemalle. (Benton 2010.)

## 5.4 Avoimet langattomat verkot

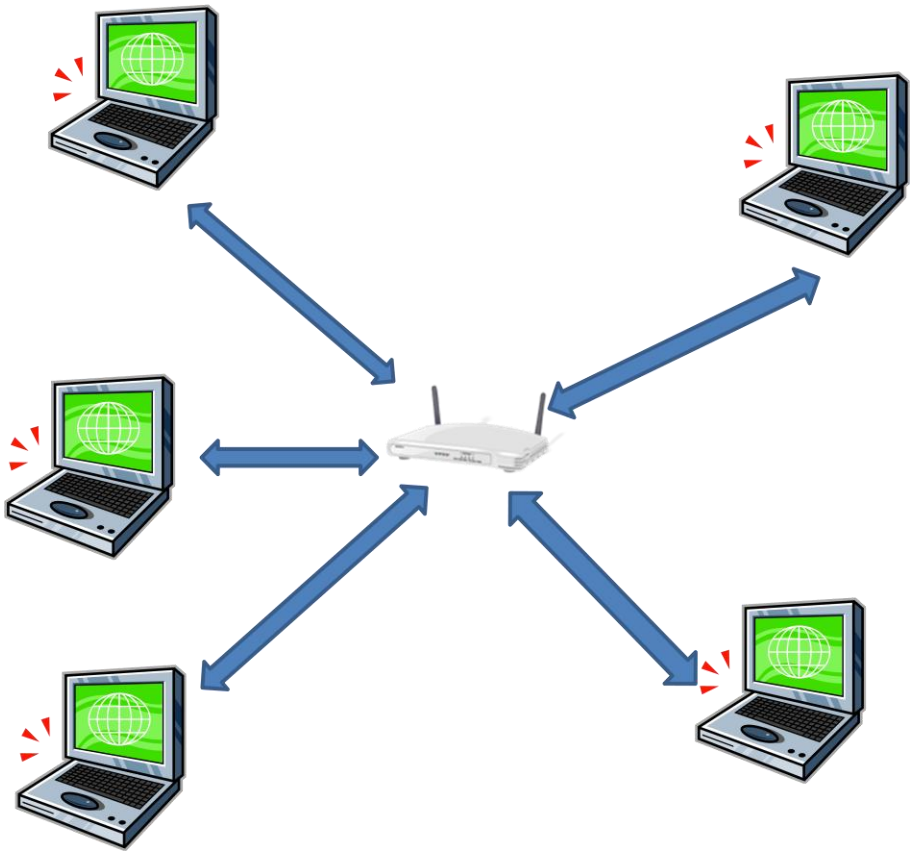
WLAN-verkko voidaan luoda myös täysin avoimeksi, jolloin mitään salausmenetelmiä ei käytetä. Tällöin verkon liikenne on salaamatonta ja siirretty tieto pitää tarvittaessa salata muilla keinoin. Näitä keinoja ovat mm. ssl- ja ssh-salaukset. Ssl-salausta käytetään esimerkiksi kun käytetään verkkopankkia Internet-selaimella. Ssh-salaus on käytössä esimerkiksi turvallisissa terminaaliyhteyksissä. Langattomien lähiverkon salausmenetelmien luonteesta johtuen ei salausta kyetä ottamaan käyttöön täysin avoimissa verkoissa, sillä salaus tapahtuu joko ennaltamäärätyllä salasanalla tai sertifikaatilla. Päätelaite on syytä suojata verkosta tulevilta uhilta palomuurilla ja virustorjuntaohjelmistolla.

Avoimen WLAN-verkon hyötynä on sen saatavuus, kuka tahansa voi käyttää verkkoa koska tahansa. Avoimia langattomia lähiverkkoja on yleensä paikoilla, joissa ihmiset liikkuvat ja oleskelevat, kuten lentokentillä ja hotelleissa matkustajia varten. Avoimet verkot on tarkoitettu tilapäiseen käyttöön, esimerkiksi työmatkalaisille ja turisteille sähköpostin yms. katsomista varten.

# 6 LANGATON LÄHIVERKKO KÄYTÄNNÖSSÄ

## 6.1 WLAN-verkkojen topologiavaihtoehdot

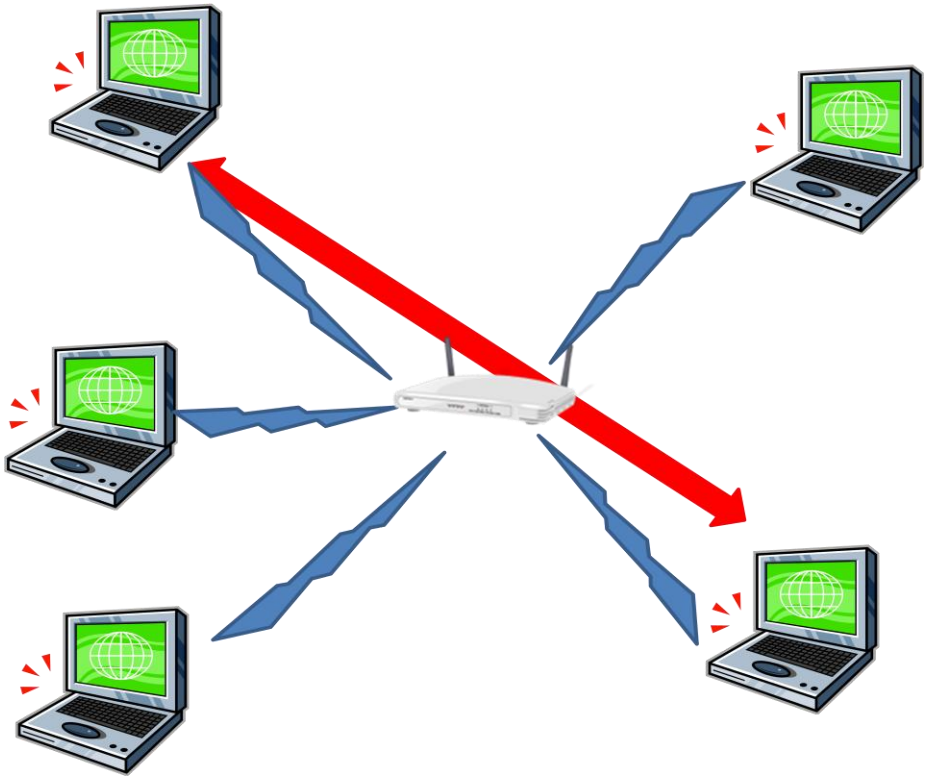
WLAN-verkko voidaan rakentaa periaatteessa kahdella tavalla. Yleisin tapa on käyttää tähtitopologiaa (kuvio 9), jossa päätelaitteet liikennöivät yhden verkon aktiivilaitteen, WLAN-tekniikassa tukiaseman, lävitse. Tähtitopologiasta käytetään myös nimitystä pisteestä useaan pisteeseen (point-to-multipoint).



KUVIO 9. Tähtitopologia

Tähtitopologiaa noudattavat WLAN-verkot vastaavat langallisen verkon puolelta keskitin(hub)-verkkoa, jossa kaikki keskittimelle tuleva tieto jaetaan kaikkien verkossa olijoiden kesken. Tämä johtuu WLAN-verkoissa teknisistä rajoitteista. Radiotaajuuksien suuntaaminen hyvin tarkasti on mahdotonta, joten tilanne on ratkaistu samoin kuten LAN-verkoissa käyttäen tekniikoita estämään samanaikaista viestien lähettämistä verkossa ja näin verkon tukkeutumista.

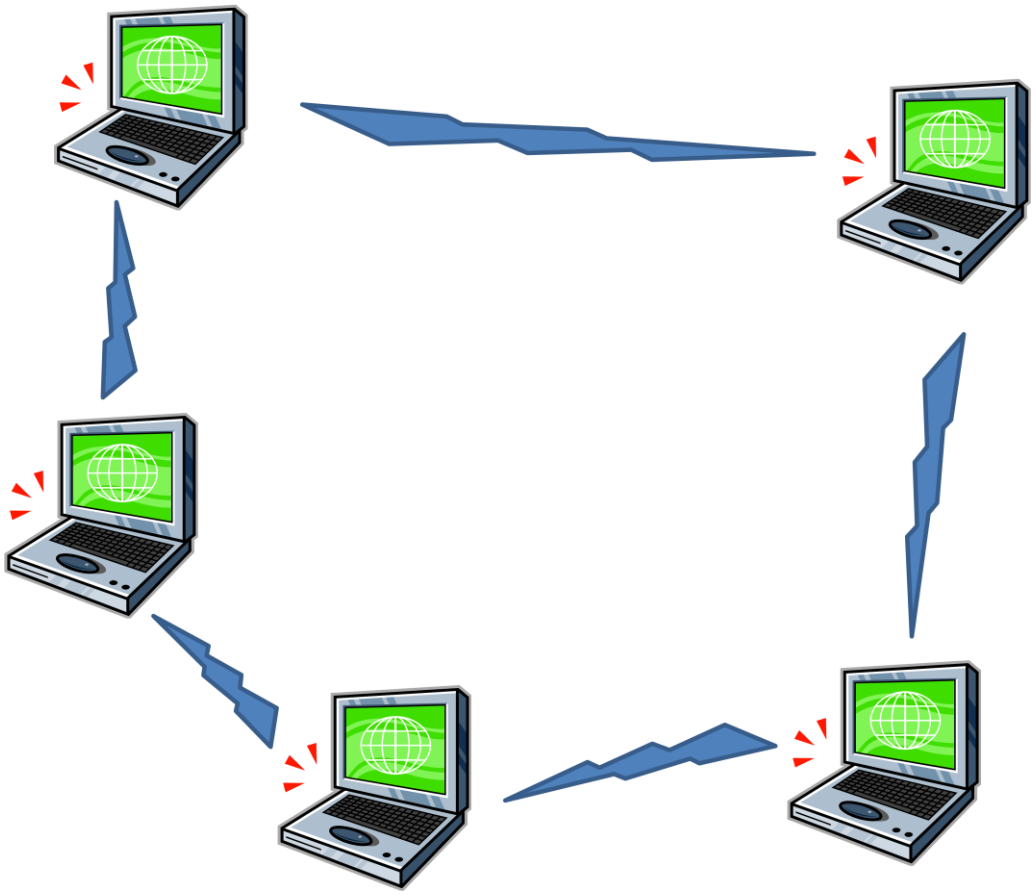
Tähtitopologian suurimpana haittapuolena on, ettei kahden samassa verkossa, ja näin siis saman tukiaseman kanssa liikennöivän, päätelaitteen lähetys- ja vastaanottoteho välttämättä riitä siihen, että kaukana toisistaan sijaitsevat päätelaitteet näkisivät toisensa. Myös tätä piiloasemaongelmaa (hidden node problem) (kuvio 10) pyritään poistamaan käyttämällä törmäyksen ehkäisymenetelmää.



KUVIO 10. Piiloasemaongelma. Kuviossa punaisella nuolella yhdistetyt laitteet eivät havaitse toisiaan.

## 6.2 Ad-Hoc-verkko

Toinen tapa rakentaa langaton lähiverkko on käyttää ad-hoc-yhteystapaa. Ad-hoc-verkossa päätelaitteet muodostavat oman verkkonsa, jossa jokainen päätelaite osallistuu verkossa siirrettävän tiedon ohjaamiseen vastaanottajalle. Toisin kuin tukiasemaan pohjautuvassa verkossa, ad-hoc-verkon kaikki laitteet ovat yhteneväisessä asemassa ja voivat liikennöidä suoraan mille tahansa verkossa olevalle päätelaitteelle. Tämä yhteystapa on topologialtaan rengastyyppinen (ring) (kuvio 11). Toisaalta, koska ad-hoc-verkossa päätelaitteet voivat keskustella useamman kuin kahden viereisen laitteen kanssa, voidaan verkon käsittää myös toimivan verkko (mesh)-topologialla. Yleensä pitäydytään rengastopologiassa.
(De Couto, Lee & Morris 2012.)



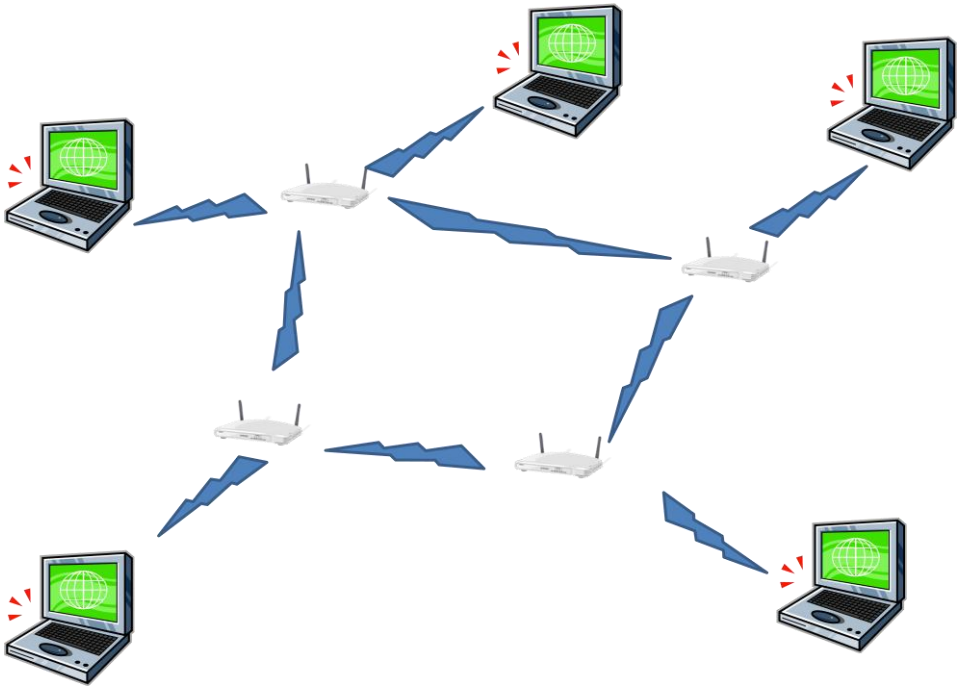
KUVIO 11. Ad-hoc verkko-kuvattuna rengastopologian mukaisesti

Ad-hoc-verkossa ei siis ole tukiasemaa, jos verkkoon tukiasema tai asemia laitetaan, muuttuu verkko silloin topologialtaan mesh-verkoksi. Ad-hoc-verkossa kaikki laitteet ovat samanarvoisia, toisin kuin tukiasemaan perustuvissa verkoissa, joissa tukiasema ohjaa liikennettä ja antaa päätelaitteille luvan liikennöidä. Ad-hoc-verkon aktiivilaitteet pitävät itse yllä reititystaulukkoa, jossa on kaikki ”viereiset” päätelaitteet, joihin päätelaite voi liikennöidä suoraan esimerkiksi etäisyyden salliessa.

## 6.3 Mesh-tekniikka

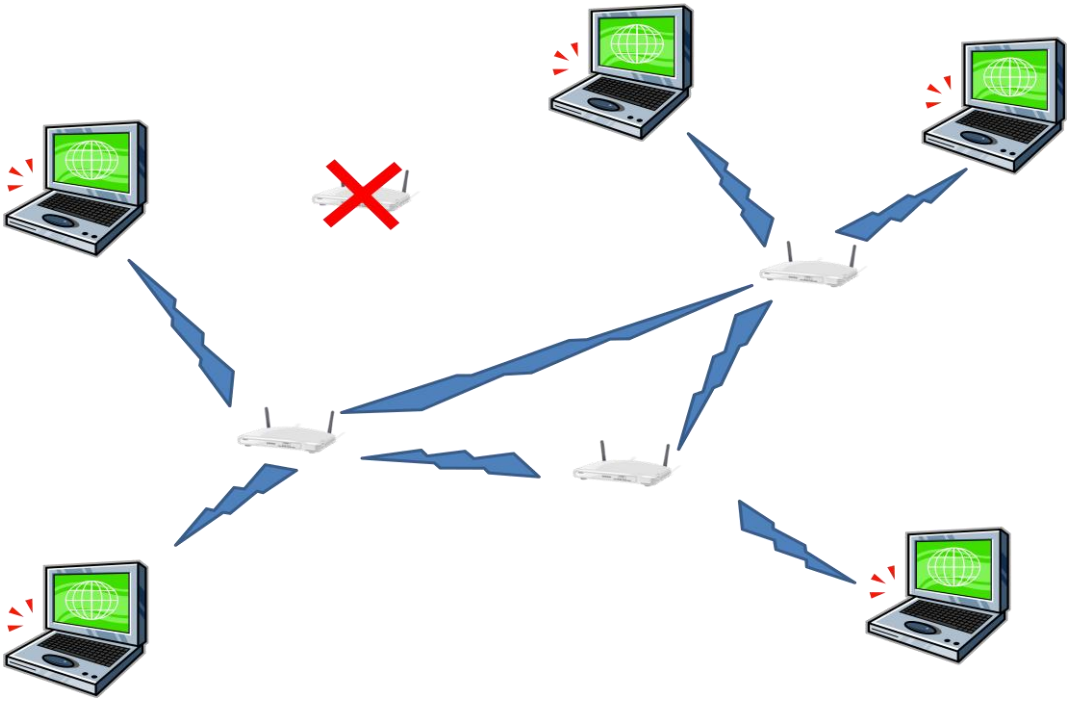
Laajoja WLAN-verkkoja on mahdollista toteuttaa myös käyttäen 802.11s-standardin määrittelemää mesh-tekniikkaa. Mesh-teknologian avulla voidaan WLAN-laitteista luoda verkko (mesh), joka voitaisiin kuvitella vaikkapa kalaverkoksi, jossa jokainen tukiasema liikennöi usean muun laitteen kanssa (kuvio 12). Mesh-verkossa tukiasemia kutsutaan solmuiksi (node).

Mesh-tekniikalla voidaan ottaa käyttöön päätelaitteiden kyky jatkaa verkkoa tukiasemaverkon ulkopuolelle. Lisäksi tukiasemaverkko voidaan rakentaa käyttämään langatonta tiedonsiirtoa toisten tukiasemien välille, jolloin yhteys ulkoverkkoon voidaan hoitaa käyttäen yhtä tukiasemaa, joka on kytketty Internetiin tai muuhun verkkoon. Mesh-verkko voidaan siis käsittää eräänlaisena ad-hoc verkkona. (Roos 2012.)



KUVIO 12. Mesh-verkko

Mesh-verkon hyötynä on verkon vikasietoisuus, jossa yhden tai useamman tukiaseman katoaminen verkosta ei riko koko verkkoa, vaan verkko voidaan rakentaa uudelleen käyttäen edelleen toimivien tukiasemien avulla uudelleen, menettäen toki kadonneiden laitteiden tuoman kuuluvuusalueen. Rikkoutuneen laitteen ”viereiset” tukiasemat automaattisesti tunnistavat vikatilanteen ja alkavat etsiä vaihtoehtoisia reittejä, jotta verkko toimisi taas normaalisti. Rikkoutuneeseen tukiasemaan yhteydessä olleet päätelaitteet alkavat etsiä toista mahdollista verkon tukiasemaa (kuvio 13). Verkon toipuminen vikatilanteesta riippuu myös verkon asetuksista sekä solmutiheydestä, eli siitä kuinka limittäin tukiasemien kuuluvuusalueet ovat. Mitä enemmän tukiasemia verkon tarkoitetulla kuuluvuusalueella on, sitä huomaamattomampi on yhden tukiaseman vikaantuminen verkkoa käyttävän päätelaitteen osalta. (Roos 2012.)



KUVIO 13. Kuvion 12 verkko, kun yksi tukiasema on pudonnut verkosta ja verkko on toipunut tilanteesta

## 6.4 WLAN-verkon asetukset

WLAN-tekniikka sijoittuu OSI-mallissa fyysiselle kerrokselle ja siirtokerrokselle. Fyysinen kerros käsittää WLANin käyttämän tiedonsiirtomedian, radiotien. Siirtokerroksen osalta WLAN käyttää MAC-osuutta, joka on siirtokerroksen alempi osuus. Laitteiden tunnistaminen ja liikennöinti laitteiden välillä tapahtuu LAN-verkkojen tapaan MAC-osoitteilla.

Jokainen WLAN-verkko on pystyttävä tunnistamaan jollain keinolla. Tätä varten WLAN-verkoille annetaan nimi (SSID), joka on normaalisti päätelaitteiden löydettävissä. WLAN-verkon voi myös piilottaa normaaleilta WLAN-verkkojen etsintämenetelmiltä poistamalla kyseisen verkon SSID. Tämä ei kuitenkaan estä edistyneempien WLAN-skannereiden osalta verkon löytämistä, vaan skannerit tunnistavat verkon tukiaseman MAC-osoitteella. Salatun SSID:n (BSSID) käyttö ei siis ole varsinainen turvatekijä.

SSID:n avulla voidaan luoda ns. roaming-verkkoja. joita on esimerkiksi mesh-verkot tai WLAN-kontrollerin avulla luodut verkot. Roaming-tekniikka mahdollistaa päätelaitteiden liikkumisen verkon eri tukiasemien välillä jopa ilman katkoja verkkoyhteydessä. Ilman roaming-ominaisuutta päätelaite menettää yhteyden verkkoon, kun päätelaite poistuu tukiaseman kuuluvuusalueelta. Jos päätelaite näkee samalla SSIDllä olevan verkon olevan saatavilla, ottaa päätelaite yhteyttä verkkoon, jolloin esimerkiksi päätelaitteen saama IP-osoite saattaa muuttua.

WLAN-verkon pystyttämisen jälkeen käyttäjän on helppo yhdistää päätelaitteensa, oli se sitten tietokone, matkapuhelin tai vaikkapa televisio, WLAN-verkkoon. Yhdistäminen verkkoon tapahtuu etsimällä haluttu SSID, tai vaihtoehtoisesti, esimerkiksi salatun SSIDn ollessa käytössä, yhdistämällä suoraan haluttuun SSID:hen. Kun yhteys tukiasemaan on luotu, käyttäjän päätelaite saa yleensä IP-osoitteen WLAN-verkon kautta. Vaikka liikennöinti WLAN-verkossa tapahtuukin MAC-osoitteiden avulla tarvitaan IP-osoitetta WLAN-verkon ulkopuoliseen liikennöintiin. (Briere, Bruce, Hurley 2003.)

# 7 AVOIMET KAUPUNKIVERKOT

## 7.1 MASTONET

MASTONET-verkko luotiin vuonna 2005 Lahden stadionille Salpausselän kisoja varten. Samaan aikaan Lahdessa oli toinen avoin WLAN-verkko, EduWLAN, joka kattoi alueita Lahden kaupungin koulurakennusten lähistöiltä. EduWLAN oli rakennettu koulujen käytettäväksi. Lisäksi kaupungissa oli Lahti Energian omistaman tytäryhtiö Suomen 4G:n omistama kaupallinen verkko, joka myöhemmin EduWLANin kanssa yhdistettiin osaksi MASTONETiä.

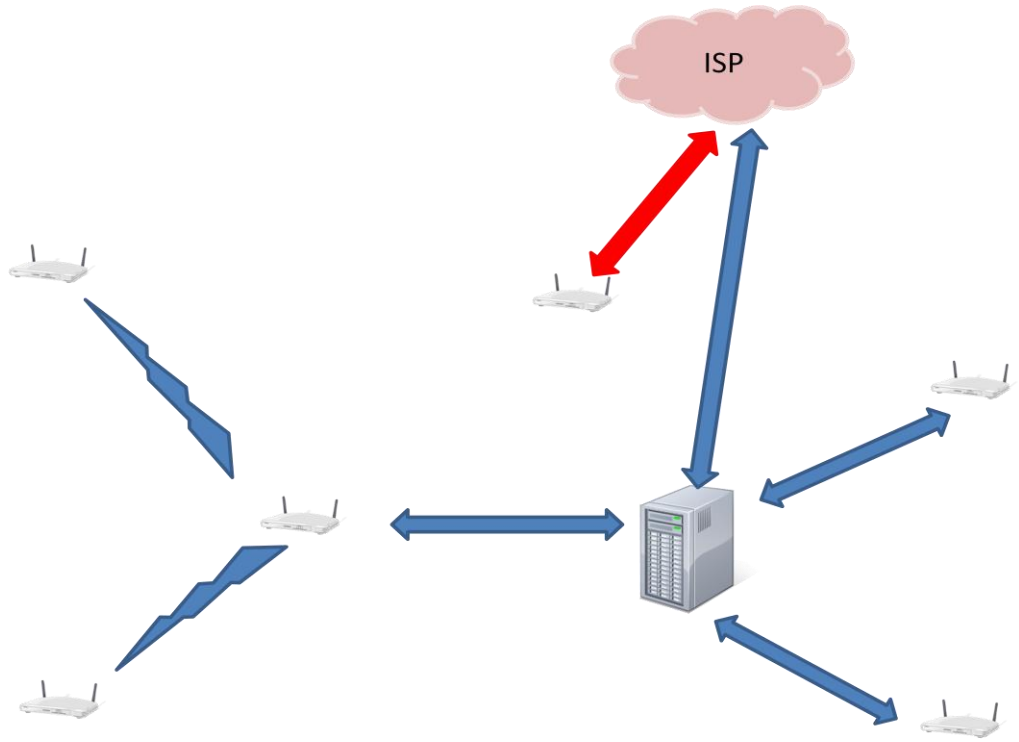
Verkkojen yhdistämisen jälkeen MASTONETiä ylläpiti Lahden sivistystoimen koulutuspalvelukeskus, eikä verkkoon ollut budjetoitu rahaa verkon päivittämiseen. Vuonna 2007 käydyn julkisen keskustelun jälkeen MASTONETiä ylläpiti jonkin aikaa Lahti Energia, kunnes yhtiö myöhemmin irtisanoi sopimuksen.

Vuoden 2009 alusta lähtien verkkoa on ylläpitänyt Lahden ammattikorkeakoulu. Ylläpitoa rahoittaa Lahden kaupunki. Lahden ammattikorkeakoulu on alkanut kehittää verkkoa ns. HotSpot-menetelmällä, jossa verkkoa laajennetaan niihin sijainteihin, joissa ihmiset oleskelevat ja liikkuvat eniten, kuten rautatie- ja linja-autoasemalle, Sibeliustaloon ja sen ympäristöön sataman alueella, sekä kirjastoon.

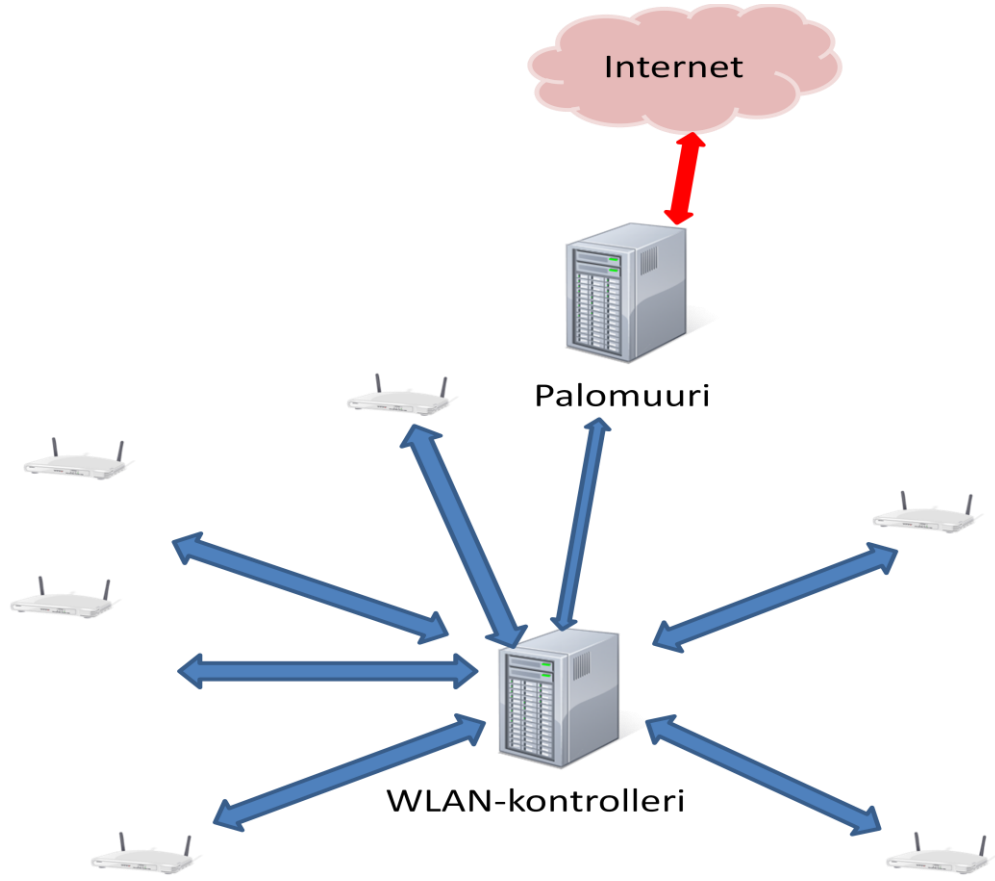
MASTONETin historiasta johtuen käytössä on kirjavaa tekniikkaa. EduWLANin ja Lahti Energian verkkojen tukiasemat ovat useimmiten Orinoco AP1000- tai AP400-mallisia tukiasemia. Etenkin ensin mainitut laitteet ovat erittäin vanhoja ja tukevat vain 802.11b-standardia. Sittemmin Lahden ammattikorkeakoulun alettua ylläpitää ja kehittää verkkoa Lahden kaupungin rahoituksella on käyttöön otettu Ciscon keskitetysti hallittava 4400-sarjan järjestelmä. Runkoyhteys vuonna 2010 oli 10 Mbit/s yhteys.

MASTONET rakentuu historiansa takia hieman epätyypillisesti. MASTONETin vanhat EduWLANin ja Lahti Energian laitteet on kytketty samaan lähiverkkoon, joka taas on yhdistettynä Lahden kaupungin runkoverkkoon. Nämä vanhat tukiasemat on yhdistetty yhteiseen lähiverkkoon käyttäen monenlaisia ratkaisuja. Esimerkiksi Lahden vesitornilta on langaton linkkiyhteys Lahden Lyseon koulurakennukseen, josta on myös langaton linkki Oululainen Oy:n viljasiilon päällä olevaan tukiasemaan. Muita käytössä olevia yhteyksiä on Lahden sisäinen lähiverkko, johon on kytketty lähinnä Lahden koulurakennuksissa olevat tukiasemat, sekä erilaiset vuokrayhteydet, jotka voivat olla esimerkiksi kaupallisilta operaattoreilta hankitut ADSL-yhteydet. (Kuvio 14.)

Verkon uudempi osuus, joka on rakennettu Lahden ammattikorkeakoulun toimesta, on toteutettu käyttäen keskitettyä hallintaa. Verkon varsinainen tukiasema on Ciscon WLAN-kontrolleri, joka hoitaa liikennöinnin verkon sisällä ja myös liikenteen ulkoverkon kanssa palomuurin lävitse. Kontrolleriin on kytketty ”tyhmiä” radioportteja, joiden kautta liikennöinti päätelaitteiden ja kontrollerin välillä tapahtuu. Radioportit ovat omassa virtuaalisessa lähiverkossaan kontrollerin kanssa, eivätkä radioportit näy päätelaitteille, muutoin kuin WLAN-skannerilla, jolla on mahdollista tunnistaa eri radioportit niiden MAC-osoitteiden perusteella. Kontrolleriin pohjautuva verkko ei ole suoraan yhteydessä MASTONETin vanhaan osuuteen, joten loogisessa mielessä MASTONET on kaksi eri WLAN-verkkoa. (Kuvio 15.)




KUVIO 14. MASTONETin ”vanha verkko”




KUVIO 15. MASTONETin ”uusi verkko”, joka pohjautuu WLAN-kontrolleriin

## 7.2 panOULU

Oulun kaupunki teki aloitteen panOULU-verkon rakentamiseksi kaupungin 400-vuotisjuhlien kunniaksi. Tavoite oli luoda kaikille avoin, ilmainen langaton Internet-yhteys. Verkko kasvoi nopeasti seuraavien vuosien aikana, ja jo vuonna 2008 verkossa oli yli tuhat tukiasemaa. Tavoitteena on kattaa kaikki Oulun kaupungin julkiset sekä panOULUn yhteistyökumppanien tilat.

Verkkoa kehittää Oulun yliopisto, Oulun seudun ammattikorkeakoulu ja DNA Oy (entinen Oulun Puhelin Oyj). Yhteistyökumppaneina ovat VTT, Elisa Oyj sekä Netplaza Oy. Verkko koostuu useasta osasta, joista eri tahot vastaavat, KampusWLAN:ista, OuluNET:stä, OukaWLAN:ista sekä RotuaariWLAN:ista. Lisäksi kaupalliset operaattorit myyvät panOULU-liittymiä, jolla yksityishenkilöt sekä yritykset voivat osallistua verkonlaajennukseen. (panOULU 2012b.)

panOULU-verkossa on käytössä neljä erilaista tukiasemamallia, jotka ovat Cisco Systemsin valmistamia. Suurin osa verkosta on toteutettu Cisco Aironet 1100, 1200 tai 1240-mallisilla tukiasemilla. Lisäksi käytössä on Ciscon omistaman Linksysin valmistamia tukiasemia.(panOULU 2012a.)

# 8 MASTONET KÄYTTÄJÄN KANNALTA

## 8.1 Käyttäjäkysely

Käyttäjäkyselyä varten laadittiin lista kysymyksiä. Kysely lähetettiin MASTONETin käyttäjätukeen yhteyttä ottaneiden sähköpostiin. Kyselyn tarkoituksena oli kerätä tietoa, kuinka MASTONETiä käytetään ja miten hyvin MASTONET on käyttäjien kannalta toiminut sekä millaisilla laitteilla käyttäjät MASTONETiä käyttävät. Lisäksi tiedusteltiin, mitä mahdollisia palveluja käyttäjät toivoisivat MASTONETin tarjoavan käyttäjilleen.

Kysymysasettelulla pyrittiin saamaan vapaamuotoisia vastauksia, jotka olisivat hieman pidempiä kuin kyllä/ei-vastaukset. Kysely lähetettiin 10 ihmiselle, joista vain puolet vastasi kyselyyn. Kysely suoritettiin maaliskuussa 2010, ennen kuin MASTONETin laajennusprosessi oli lähtenyt kunnolla käyntiin.

### 8.1.1 Kyselylomake

Käyttäjille lähetettiin seuraavanlainen kyselylomake:

Hei!

Olette olleet yhteydessä MASTONET-verkon käyttäjätukeen. Teemme nyt tutkimusta MASTONETin käyttäjäkokemuksista ja haluaisimme vastauksianne muutamiin kysymyksiin. Tämän kyselyn vastauksia käytetään opinnäytetyön osana, jonka tavoitteena on parantaa MASTONETin käyttäjäkokemusta ja käytettävyyttä. Vastauksia ei julkaista sellaisenaan.

1. Mihin ja miten käytätte verkkoa? (Sähköpostin lukeminen, nettipankkiasiointi jne. Kannettavalla tietokoneella, kännykällä jne.)
2. Käytättekö verkkoa monessa sijainnissa? Jos käytätte, niin missä?
3. Miten arvioisitte verkon toimivuutta? Onko yhteys riittävän vakaa ja nopea?
4. Mihin haluaisitte että verkkoa laajennetaan?
5. Mitä palveluita haluaisitte, että MASTONET tarjoaisi? (Esim. sähköpostipalvelu)
6. Miten arvioisitte käyttäjätuen toimintaa?
7. Muita kommentteja MASTONETista.

Terveisin,
Simo Viinikka
Lahden ammattikorkeakoulu

## 8.2 Käyttäjien kokemukset ja käyttäjien kehitysehdotukset

Palvelun laatu on parantunut viime aikoina. Alkuaikoina verkossa on ilmennyt pätkimistä ja kuuluvuusongelmia, joita on sittemmin korjattu. Verkon toimivuus nykyisin on käyttäjien mielestä hyvä niillä alueilla, joissa verkko ylipäänsä kuuluu. Toisaalta vanhojen EduWLANin aikaisten vikaantuneiden laitteiden korjaamattomuutta moitittiin. Myös verkon ajoittainen ruuhkaisuus on ollut ongelma ja esimerkiksi Internetin videopalvelujen käyttäminen MASTONETin avulla on ollut vaikeaa videoiden pätkimisen takia.

Kyselyyn vastaajat käyttivät MASTONETiä useimmiten vain kotona käyttäen kannettavaa tietokonetta. Myös matkapuhelimen avulla verkkoa on kokeiltu. Vastaajat käyttivät verkkoa sähköpostin lukemiseen, verkkopankkiasiointiin ja tiedonhankintaan.

MASTONETin käyttäjätukeen oltiin tyytyväisiä, etenkin Lahden ammattikorkeakoulun aloitettua käyttäjätukipalvelut. Palvelun ilmaisuutta kehuttiin paljon. Myös verkon kuuluuteen oltiin tyytyväisiä.

Kyselyyn vastaajat toivoivat verkon laajentamista koko Lahden alueelle, ja yhteysnopeuksien nostamista. Lahden kaupungin tarjoamien palveluiden ja tietoa Lahden alueen tapahtumista toivottiin helposti saataville MASTONETin käyttäjille. Verkon ylläpitoon kaivattiin lisäpanosta, jota on nyt saatu Lahden kaupungin budjetoitua rahaa verkon ylläpitoon.

# 9 YHTEENVETO

WLAN-tekniikat ovat reilun kymmenvuotisen olemassaolonsa aikana kehittyneet hurjasti. Alun maksimissaan 2 Mbit/s nopeuksista on noustu aina 600 Mbit/s nopeuksiin. Lisäksi verkkojen tietoturvaa on parannettu erilaisin salausmenetelmin. 802.11-standardiperhe kasvaa joka vuosi uusilla lisäyksillä, joista jokainen vie tekniikkaa eteenpäin.

Avoimet langattomat lähiverkot tarjoavat haasteita niin ylläpidolle kuin myös käyttäjille. Avoimien verkkojen tietoturva on teknisistä syistä rajoittunutta ja verkossa liikennöivän tiedon salaaminen on verkkotekniikan osalta lähes mahdotonta jos langaton lähiverkko halutaan pitää saatavilla kaikille ilman salasanoja. Kaupunkien ja yhteisöjen tarjoamat ilmaiset, avoimet langattomat verkot on otettu hyvin vastaan ja niiden toivotaan lisääntyvän ja laajentuvan uusille alueille. Etenkin uusien mobiilien laitteiden kuten kehittyneiden älypuhelimien ja tablettitietokoneiden yleistymisen myötä tarve langattomille verkoille vain kasvaa.

MASTONETin toimintaan oltiin yleisesti tyytyväisiä. Verkon kehittämiseen suhtauduttiin hyvin ja ehdotuksia, kuinka verkkoa pitäisi käyttäjien mielestä kehittää, tuli muutamia. Verkkoa tulisi laajentaa entisestään ja lisätä yhteysnopeuksia. Toisaalta verkon ylläpitoon toivottiin lisäpanosta.

Verkkoa kehittäessä tulisi ottaa huomioon käyttäjien toiveet verkon tulevaisuuden suhteen. Uusien kannettavien ja hyvin mobiilien älylaitteiden markkinoiden lähes räjähdysmäinen kasvu antaa edellytykset laajentaa verkkoa ja nostaa verkon kapasiteettia kuten käyttäjät toivovat. Lisäksi liikematkalaisia ja turisteja ajatellen MASTONET voisi tarjota jonkinlaista palvelua, johon on koottu tietoa Lahden seudun tapahtumista.

# 10 LÄHTEET

Aspinwall, J. 2003. Installing. Troubleshooting, and Repairing Wireless Networks. McGraw-Hill: Chicago.

Roos, D. 2012. How Wireless Mesh Networks Work [viitattu 9.4.2012]. Saatavissa:
http://www.howstuffworks.com/how-wireless-mesh-networks-work.htm

Gast, M. 2002. 802.11 Wireless Networks: The Definite guide. E-kirja: O'Reilly.

IEEE, 1991. The First IEEE Workshop on Wireless LANs: Preface [viitattu 9.4.2012]. Saatavissa:
http://www.cwins.wpi.edu/wlans91/scripts/preface.html

IEEE. 1996. The Second IEEE Workshop on Wireless LANS: Summary [viitattu 9.4.2012]. Saatavissa:
http://www.cwins.wpi.edu/wlans96/scripts/summary.html

IEEE. 2012. Official IEEE 802.11 Working group project timelines, viitattu 9.4.2012, saatavilla http://www.ieee802.org/11/Reports/802.11_Timelines.htm

IEEE-SA Standards Board. 2003. Supplement to IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical, Layer in the 5 GHz Ban [viitattu 9.4.2012]. Saatavissa:
http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

IEEE-SA Standards Board. 2003. Supplement to IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band [viitattu 9.4.2012]. Saatavissa: http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

IEEE-SA Standards Board. 2003. Supplement to IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band [viitattu 9.4.2012]. Saatavissa: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

Instat, 2010. Wi-Fi Market Overview: Connectivity Becoming Ubiquitous [viitattu 9.4.2012]. Saatavissa: http://www.instat.com/promos/10/IN1005038WHT.pdf

Johns Hopkins School of Public Health. 2007. History of Wireless [viitattu 9.4.2012] Saatavissa: http://web.archive.org/web/20070210131824/www.jhsph.edu/wireless/history.html

Benton, K. 2010. The Evolution of 802.11 Wireless Security [viitattu 9.4.2012]. Saatavissa: http://itffroc.org/pubs/benton_wireless.pdf

Li, J., Blake, C,. De Couto D., Lee, H. I. & Morris, R. Capacity of Ad Hoc Wireless Networks [viitattu 9.4.2012]. Saatavissa: http://pdos.csail.mit.edu/papers/grid:mobicom01/paper.pdf

panOULU. 2012a. Laitteisto [viitattu 9.4.2012]. Saatavissa: http://www.panoulu.net/equipment.shtml.fi

panOULU. 2012b. Verkon esittely [viitattu 9.4.2012]. Saatavilla http://www.panoulu.net/structure.shtml.fi

Tilastokeskus. 2006. Tietotekniikasta tullut osa suomalaisten arkipäivää [viitattu 9.4.2012]. Saatavissa: http://www.stat.fi/ajk/tiedotteet/v2006/tiedote_017_2006-03-08.html

Wikipedia. 2012. IEEE 802.11g-2003 [viitattu 9.4.2012]. Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11g-2003

Wikipedia. 2010. ALOHAnet [viitattu 9.4.2012]. Saatavissa: http://en.wikipedia.org/wiki/ALOHAnet

Wikipedia. 2012a. MIMO [viitattu 9.4.2012]. Saatavissa: http://en.wikipedia.org/wiki/MIMO

Wikipedia. 2012b. Pre-shared key [viitattu 9.4.2012]. Saatavissa: http://en.wikipedia.org/wiki/Pre-shared_key

Wikipedia. 2012c. Quadrature amplitude modulation [viitattu 9.4.2012]. Saatavissa: http://en.wikipedia.org/wiki/Quadrature_amplitude_modulation