SAVONIA

Langattoman lähiverkon uudistaminen ja dokumentointi

Juho Nurminen

Opinnäytetyö

19.3.2013 Kuopio

Ammattikorkeakoulututkinto

SAVONIA-AMMATTIKORKEAKOULU
OPINNÄYTETYÖ

Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Juho Nurminen	
Työn nimi Langattoman lähiverkon uudistaminen ja dokumentointi	
Päiväys 20.2.2013	Sivumäärä/Liitteet 49
Ohjaaja(t) yrityskouluttaja Reijo Tenhunen	
Toimeksiantaja/Yhteistyökumppani(t) Siilinjärven Kunta / Tietotekniikkapalvelut	

Tiivistelmä

Tämä opinnäytetyö käsittelee Siilinjärven kunnan langattoman lähiverkon uudistamista. Tehtävänä oli dokumentoida kunnan uudistuksessa oleva WLAN-verkko sekä suunnitella tukiasemien käyttöönotto kunnantalon tiloissa. Dokumentointi on hyödyllinen, kun langatonta verkkoa kehitetään tai uudistetaan tulevaisuudessa. Tukiasemien käyttöönoton suunnittelussa mietitään käytännön tasolla tarvittavia ratkaisuja, jotta verkosta tulisi mahdollisimman kattava ja käyttäjän tarpeet huomioiva.

Opinnäytetyö sisältää kaksi osiota: Toinen tarkastelee teoriassa langattomia lähiverkkoja, toinen käsittää raportin tehdystä työstä. Teoriaosuus tarjoaa tietoa langattomien lähiverkkojen toiminnasta ja antaa käsityksen siitä, mitä nämä ovat. Dokumentointi ja suunnittelu mahdollistavat tutustumisen olemassa olevaan ja rakentuvaan nykyaikaiseen langattomaan verkkoon.

Siilinjärven kunta sai työstä dokumentoinnin uudistetusta verkosta sekä suunnitelman tukiasemien sijoittamiselle kunnantalon tiloissa. Dokumentoinnista löytyy yksityiskohtaiset tiedot verkosta. Se käsittää tiedot tietoturvasta, IP-osoitteista ja VLAN:sta.

Avainsanat
WLAN, langaton lähiverkko

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Computer Science			
Author(s) Juho Nurminen			
Title of Thesis Wireless local area network modernization and documentation			
Date	20.2.2013	Pages/Appendices	49
Supervisor(s) Enterprise Instructor Reijo Tenhunen			
Client Organisation/Partners Siilinjärven Kunta / Tietotekniikkapalvelut			

Abstract

This thesis comprises with the municipality of Siilinjärvi wireless local area network modernization. The task was to document the municipal reform of the WLAN base stations, as well as to design a take-up Town Hall premises. Documentation is useful when wireless networks are being developed or revised in the future. Support for the introduction of the design of the stations considering the practical solutions necessary to enable the network should be as comprehensive as possible, and the user's needs into consideration.

The thesis consists of two parts: The second examines theory, wireless LANs, one for a report on their work. The theoretical part provides information about the operation of wireless local area networks, and gives you an idea of what these are. Documentation and design an opportunity to visit existing and modern-based wireless network.

Siilinjärvi municipality received documentation of the work plan, as well as a renewed network of base stations deployment of Town Hall premises. Documentation includes detailed information on the network. It includes information about security, IP addresses and VLAN to.

Keywords
WLAN, Wireless Local area network

SISÄLTÖ

LYHENNELUETTELO 7
1 JOHDANTO 9
2 LANGATON LÄHIVERKKO 11
2.1 Langattomat lähiverkot nykypäivänä 11
2.2 Langattoman lähiverkon signaalit 12
2.3 ISM-kanavat ja taajuusalueet 15
2.4 OSI-malli 16
2.5 WLAN-standardit 18
2.5.1 IEEE 802.11 18
2.5.2 802.11b 18
2.5.3 802.11a 19
2.5.4 802.11g 19
2.5.5 802.11n 20
2.5.6 Muut 802.11-standardilaajennukset 20
2.5.7 HiperLAN 22
2.6 WLAN-topologiat 22
2.6.1 ESS, Extended Service Set 22
2.6.2 BSS, Basic Service set 23
2.6.3 IBSS, Independent Basic Service Set 24
2.7 WLAN-verkkolaitteet 25
2.7.1 Verkkokortit 25
2.7.2 Tukiasemat 26
2.7.3 WLAN-kytkin 27
2.8 Kontrolleripohjaiset verkot 28
2.8.1 Varmistaminen 28
2.8.2 Tietoturva kontrollereilla 29
3 LANGATTOMAN LÄHIVERKON TIETOTURVA 30
3.1 Langaton tietoturva 30
3.1.1 Palvelunesto (Dos) 30
3.1.2 Välistävetohyökkäys 30
3.2 Suojautumistekniikat 31
3.2.1 WEP-salaus 31

3.2.2 WPA/WPA2-salaus 31
3.2.3 TKIP 32
3.2.4 AES 32
3.2.5 MAC-suodatus 32
3.2.6 802.1x-todennus 33
3.3 802.1x-todennus RADIUS-palvelimella 33
3.4 Tunnistusmenetelmät 34
3.5 Langattomiin verkkoihin kirjautuminen, annetut oikeudet ja vierailijaverkot .. 35
3.5.1 Kirjautuminen 35
3.5.2 Oikeudet 35
3.5.3 Vierailijaverkot 35
4 SIILINJÄRVEN KUNNAN WLAN-TEKNIIKAN UUDISTAMINEN 37
4.1 Lähtötilanne 37
4.2 Uudistettu langaton lähiverkko 38
4.2.1 Suunnitelma 38
4.2.2 Toteutus 40
4.3 Dokumentointi 42
4.4 Tukiasemien käyttöönoton suunnittelu 43
5 YHTEENVETO 46
LÄHTEET 48

LYHENNELUETTELO

AES	Advanced Encryption Standard, salausalgoritmi
AP	Access Point, tukiasema
BSS	Basic Service Set, peruspalveluverkko
CCK	Complementary Code Keying, modulaatiotekniikka
CSMA	Carrier Sense Multiple Access, siirtotien varausmenetelmä
CSMA/CA	CSMA with Collision Avoidance, vuoronvaraus, törmäysten välttäminen
CSMA/CD	CSMA with Collision Detection, kilpavaraus, törmäysten havaitseminen
DHCP	Dynamic Host Configuration Protocol, IP-osoitteenjakoprotokolla
DNS	Domain Name System, nimipalvelujärjestelmä
DoS	Denial of Service, palvelunestohyökkäys
EAP	Extensible Authentication Protocol, tunnistusprotokolla
HiperLAN	High Performance Radio LAN
IBSS	Independent Basic Service Set, itsenäinen palveluverkko
IEEE	the Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
IP	Internet Protocol, internetprotokolla
ISM	Industrial, Scientific & Medical, vapaasti käytettävä taajuusalue
LAN	Local Area Network, lähiverkko

MAC	Media Access Control, pääsykerros siirtotielle
MIC	Message Integrity Control, eheystarkistus
MIMO	Multiple-input multiple-output, monilähetintekniikka
MPDU	MAC Protocol Data Unit, MAC-tietosähke
OFDM	Orthogonal Frequency-Division Multiplexing, kantoaaltomodulointi
PoE	Power over Ethernet, käyttöjännitteen syöttäminen parikaapelin avulla
PSK	Pre-Shared Key, ennalta määritelty salasana
QoS	Quality of Service, tietoliikenteen luokittelu ja priorisointitekniikka
SNR	Signal-to-noise ratio, signaali-kohinasuhde
SSID	Service Set Identifier, WLAN-verkon muunnettavissa oleva tunnus
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla
WEP	Wired Equivalent Protocol, salausmenetelmä
Wi-Fi	Wireless Fidelity, langaton lähiverkko
WLC	Wireless LAN Controller, langattoman verkon hallintalaite
WPA	Wi-Fi Protected Access, salausmenetelmä
WPA2	Wi-Fi Protected Access 2, salausmenetelmä
WPA-PSK	WPA-Pre Shared Key, jaettu avain
WLAN	Wireless Local Area Network, langaton lähiverkko

1 JOHDANTO

Langattomat lähiverkot ovat yleistyneet 2000-luvun aikana. Kaupunkialueille on tullut paljon langattomia liityntäpisteitä, jotka tarjoavat langattomia verkkoja nykypäivän laitteille. Internetiin pääsee yhä useammin kaupungin eri paikoista. Langattomia lähiverkkoja tarjotaan kuluttajille niin hotelleissa kuin kahviloissa. Niillä on kuitenkin rajansa, sillä tekniikka ei vielä täysin tue kaiken kattavaa langatonta verkostoa. Ongelmia ovat mm. päällekkäiset kanavat, häiriöitä aiheuttavat laitteet ja pitkät kantomatkat.

Nykypäivänä yhä useampia laitteita saadaan toimimaan langattomien lähiverkkojen kautta. Matkapuhelimet, kannettavat tietokoneet ja eri viihdelaitteet hyödyntävät niitä jo tehokkaasti. Verkkojen kautta onnistuu tiedonsiirto ja päivittymiset. Uusinta ovat televisiot, jotka pystyvät tiedonsiirtoon ja Internet-yhteyteen langattoman verkon kautta. Lisäksi esimerkiksi televisiota pystytään jo hallitsemaan matkapuhelimen kautta wlan-verkkoja hyödyntäen. On vain ajan kysymys, koska kodinkoneiden hallinta yleistyy esim. matkapuhelimen tai muun käyttöliittymän kautta. Kannettavat tietokoneet suunnitellaan hyödyntämään langattomia verkkoja paremmin. Kehityskohteena ovat langattomat verkkokortit.

Yhä useammissa yrityksissä työntekijöille tarjotaan langatonta verkkoa työskentelyyn sekä vierailijoille pääsyä Internetiin. Kannettavien ja muiden liikuteltavien laitteiden yleistyessä työskentelyä voidaan tehostaa näiden avulla eikä työskentely ole paikasta riippuvainen.

Tässä opinnäytetyössä tutkitaan langattomien lähiverkkojen teoriaa ja tekniikkaa. Työssä käsitellään Siilinjärven kunnan langattoman lähiverkon uudistamista. Uudistuksesta tehdään dokumentointi kunnan tietotekniikkapalveluun. Kunnassa on olemassa oleva verkko, jonka laitteet uudistetaan sekä parannetaan tietoturvaa ja tekniikkaa. Osa verkoista on suojattuja ja osa asiakkaille suunnattu vierailijaverkko, jota ei ole suojattu.

Lähdemateriaalina on käytetty kirjallisuutena langattomia lähiverkkoja sekä Internetistä saatua tietoa. Tekniikka on viime vuosina kehittynyt nopeaa vauhtia, minkä vuoksi uutta kirjallisuutta ei ole saatavilla.

Tämä työ on jaettu kahteen osaan: teoriaosuuteen ja Siilinjärven kunnan langattoman verkon uudistamisen tarkasteluun. Teoriaosuudessa käsitellään yleisesti langattomia verkkoja ja eri tekniikoita. Työssä on tarkoituksena kertoa, mitä langattomat lähiverkot ovat ja kuinka ne toimivat. Teoriassa käsitellään tekniikkaa ja tietoturvaa. Tietoturva on tärkeää nykyään, koska iso osa eri tiedoista on sähköisessä muodossa. Uudistamisen tarkastelussa käsitellään dokumentointia, verkon suunnittelua ja pystyttämistä.

2 LANGATON LÄHIVERKKO

Langattomien lähiverkkojen (WLAN) historia juontaa 1980-luvun puolivälistä. Motorola julkaisi silloin Altair-tuotteen, joka oli WLAN-tekniikan (Wireless Local Area Network) ensimmäinen versio. IEEE-järjestön standardointiryhmä alkoi myöhemmin kehittää langattoman lähiverkon standardeja ja vuonna 1997 julkaistiin 802.11-standardin ensimmäinen versio. Tällä päästiin 1 ja 2 Mbit-nopeuksiin. Kehitystä jatkettiin edelleen ja vuonna 1999 julkaistiin 802.11b-standardi, jolla päästiin 11 Mbit-nopeuksiin. Tämän jälkeen on syntynyt kolme laajennusta, jotka ovat 802.11a-, 802.11g- ja 802.11n-standardit. (Puska 2005, 3.)

2.1 Langattomat lähiverkot nykypäivänä

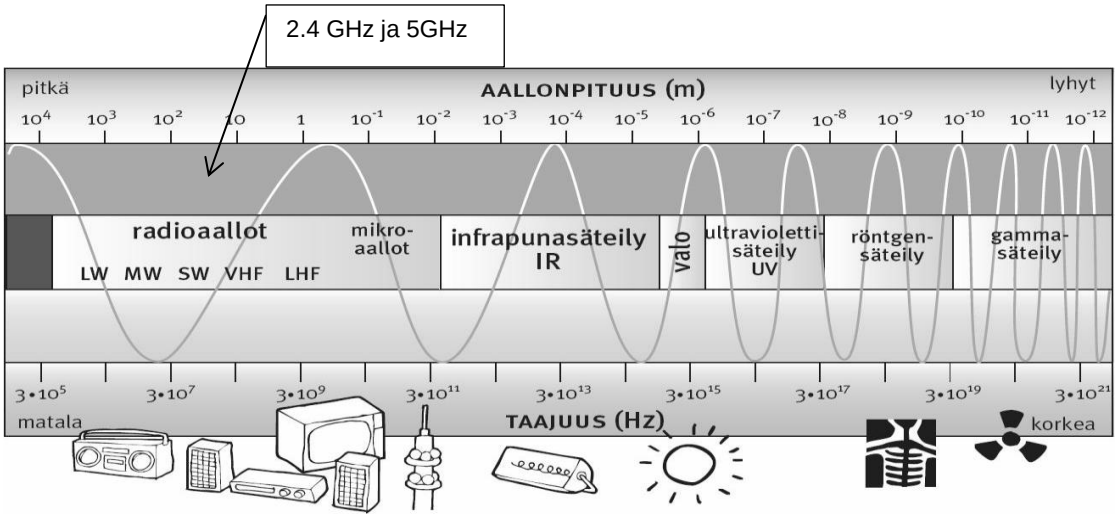
Langattomat verkot ovat nykypäivänä erittäin yleistä tekniikkaa. Tietotekniset laitteet kykenevät hyödyntämään langattomia verkkoja. Arkipäivän toiminnassa käytettäviä laitteita ovat matkapuhelimet, PC:t, kannettavat tietokoneet, tabletit yms., jotka pystyvät käyttämään langatonta verkkoa Internetin käyttöön ja muuhun kommunikointiin. Langaton lähiverkko on yleistynyt viime vuosina, sillä sitä käyttävien laitteiden tuotanto on kasvanut. Nykyään langattomia lähiverkkoja on käytössä yrityksissä ja kotitalouksissa. Useammat laitteet pystyvät hyödyntämään näitä verkkoja. Tekniikan vielä kehittyessä kotitalouksien kodinkoneita pystytään mm. hallitsemaan langattoman verkon kautta. Langattomien järjestelmien tekniikat ovat kehittyneet vuosien saatossa ja nykyään pystytään jo riittäviin nopeuksiin verkossa. Niillä ei kuitenkaan toteuteta täysin kotien tai yrityksien lähiverkkoja, vaan WLAN on nykyään vaihtoehtoinen yhteys lähiverkkoon ja Internetiin. WLAN:a voidaan nykyään kutsua myös termillä Wi-Fi (Wireless Fidelity). Wi-Fi ei ole aivan synonyymi WLAN:lle, mutta sitä käytetään usein tarkoittamaan WLAN:a (Puska 2005, 15.)

Langattoman lähiverkon hyöty on, että kaapeloinnin tarve on erittäin vähäinen. Langattomassa lähiverkossa riittää, että kaapelointi ja verkko tuodaan langatonta lähiverkkoa kaiuttavalle tukiasemalle. Tukiasemilla voidaan muodostaa tietty peitto-alue eikä käyttäjä ole näin sidottu tiettyyn työskentelypaikkaan, vaan langattomassa verkossa voidaan työskennellä peitto-alueen sisällä. (Geier 2005, 8.)

2.2 Langattoman lähiverkon signaalit

Tiedonlähetys perustuu langattomissa lähiverkoissa sähkömagneettisiin signaaleihin eli radioaaltoihin. Tiedonsiirtoon käytetään radiotaajuuksia. Siirretty tieto voi olla sähköposteja, tiedostoja, ääntä tai videota. Sähkömagneettisen säteilyn spektri näyttää langattoman verkon käyttämät radioaallot. Radioaaltojen mittayksikkö on hertsi (Hz) Kuviossa 1 nähdään, että langattomat verkot käyttävät 2,4 GHz ja 5 GHz radioaaltoja. Radioaallot ovat osa analogisia signaaleja, koska niiden amplitudi vaihtelee jatkuvasti ajan suhteen. Amplitudi on signaalin värähdysliikkeen laajuus.

Tietokoneissa käytetään tiedonvälittämiseen digitaalisia signaaleja. Ne sisältävät binäärilukuja, joten lähetettävä tieto vahvistetaan ja sen jälkeen muunnetaan analogiseen muotoon. Vastaanottaessa tehdään toisin päin ja demuloidaan tieto digitaaliseksi. (Puska 2005, 56.)

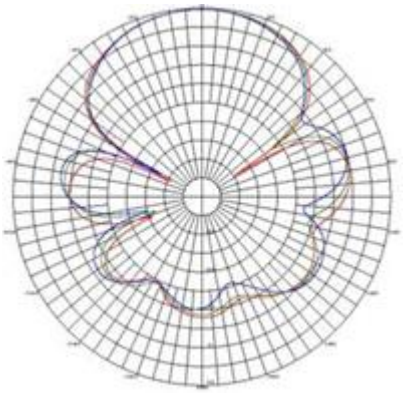


KUVIO 1. Sähkömagneettinen signaali (soveltaen Juutilainen)

Antennien avulla pystytään lähettämään signaalia. Niiden toiminta perustuu siihen, että sähköenergia muunnetaan sähkömagneettiseksi säteilyksi. Signaali voi olla erimuotoinen pysty- tai vaakasuunnassa. Antennin tyyppi vaikuttaa siihen, missä muodossa signaali säteilee. Antennityyppejä on olemassa monenlaisia, kuten suuntaantenni, ympärisäteilevät antennit (kuva 1), sektoriantennit, lautasantennit ja laitteiden sisäiset antennit. Eri antennityyppejä käytetään eri tarkoituksiin. Sisätilan WLANtoteutuksissa käytetään usein laitteiden sisäistä tai ympärisäteilevää antennia. Ulkotiloissa käytetään sektori- ja lautasantennia. Suunta-antenni sopii parhaiten pitkien matkojen signaalin säteilyyn. Kuviossa 2 nähdään suunta-antennin signaali ylhäältä-

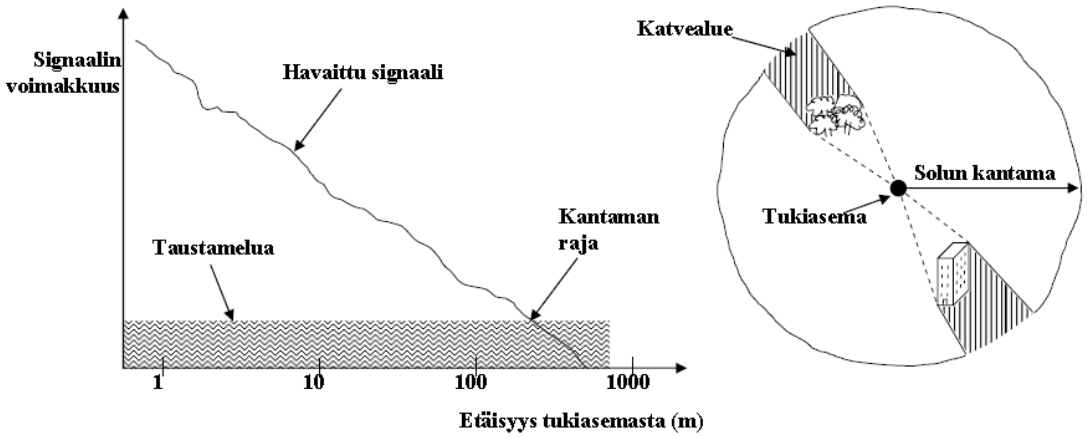
päin. Antennissa aallot summautuvat (interferenssi) ja vastaanottoja näkee yhden signaalin.

KUVA 1. Ympärisäteilevä antenni (Siptune)



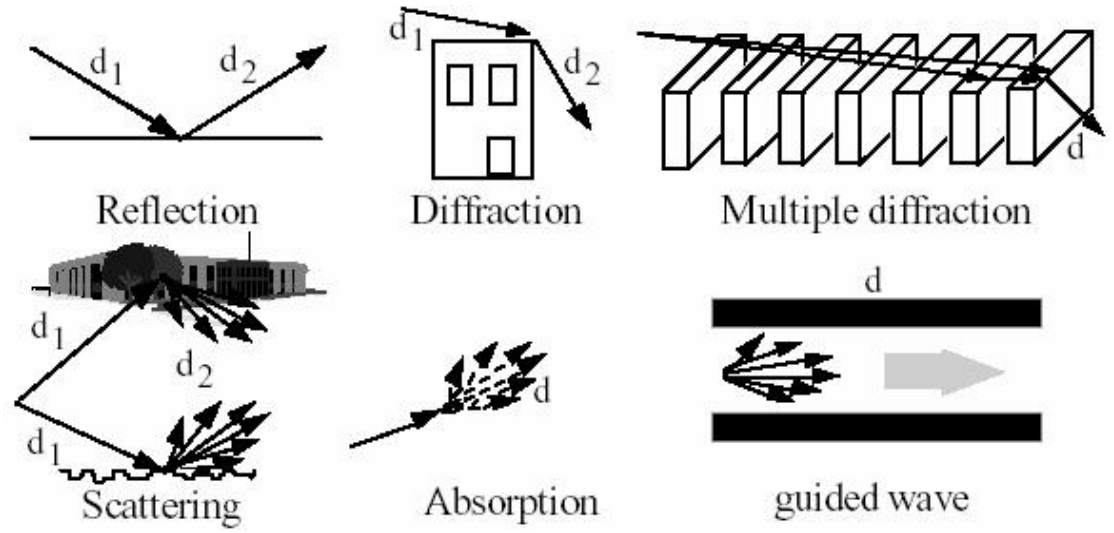
KUVIO 2. Suunta-antennin signaali ylhäältäpäin (Juutilainen)

Signaalit heikkenevät, kun välimatka vastaanottavien laitteiden välillä kasvaa. Kuviossa 3 on havainnollistettu signaalin etenemistä ja vaimenemista. Langattomien verkojen signaalin vaimenemissuhdetta tarkasteluun käytetään vapaata tilaa, jossa voidaan selvittää signaalin vaimeneminen. (Geier 2005, 54–69.)



KUVIO 3. Signaalin kantama ja vaimeneminen (Juutilainen)

Signaalin etenemiseen ja tehoon vaikuttavat monet eri tekijät. Sisätiloissa vaikuttavat rakennuksessa käytetyt materiaalit, hissikuilut, porraskäytävät, huoneiden korkeus, ikkunoiden lukumäärä ja huoneistojen kalusteet. Ulkotiloissa vesi, lumi, sumu, kuiva tai kostea ilma, vuodenajat, kasvillisuus, kaupunki tai maaseutuympäristö. Kuviossa 4 on kuvattu eri tekijöitä etenemiselle. Yksi tekijä on Heijastuminen (Reflection), jossa signaali heijastuu osuessaan esteeseen, joka on tasainen suhteessa signaalin aallonpituuteen. Tulo- ja heijastuskulmat ovat yhtä suuret. Sironta (Scattering) tapahtuu, kun signaali osuu epätasaiseen esteeseen. Tämä tarkoittaa sitä, että signaalin energiasta osa synnyttää uutta signaalia eri suuntiin. Sironnassa signaali heikkenee. Taipumisessa (Diffraction) signaali taipuu ja leviää esteeseen osuessaan. Taipumista tapahtuu tasaisten esteissä. Häipyminen (Fading) johtuu vastaanottajan tai lähettäjän liikkumisesta ja aiheuttaa signaalintason heikkenemistä. Tästä syystä liikkuessa signaali heikkenee langattomassa verkossa työskenneltäessä. Siihen vaikuttajana ovat monet seikat, eikä siltä voi välttyä, vaan se tulee huomioida signaalin etenemistä suunniteltaessa. (Puska 2005, 57–58.)

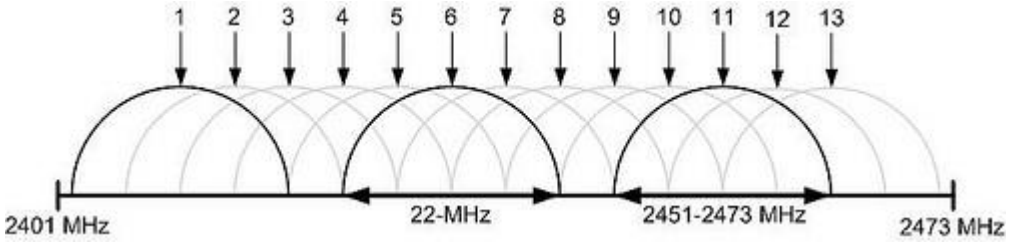


KUVIO 4. Etenemismenetelmät (Juutilainen)

2.3 ISM-kanavat ja taajuusalueet

ISM-taajuusalue on maailmanlaajuinen radiotaajuuskaista. Taajuusalueen käyttö ei vaadi erillisiä lupia. Tietoliikenteessä käytetään näitä ISM-alueita langattomaan tiedonsiirtoon. Langattomilla lähiverkoilla on käytössä ennalta määritellyt taajuusalueet 2,4 GHz ja 5 GHz sekä sovitut kaistanleveydet. Kaista on jaettu myös määritettyihin kanaviin, joita käytetään viestintään. Käytön vapaus aiheuttaakin häiriöitä tietoliikennekäytössä, koska esimerkiksi mikroaaltouuni ja Bluetooth-laitteet toimivat 2,4 GHz:n taajuudella.

Yleisin langattomissa lähiverkoissa käytettävä taajuusalue on 2,4 GHz. Eri mailla on eri kaistan leveydet ja taajuusalueet. Taajuusalueita on euroopassa13 kanavaa, joista jokainen on 22 MHz leveydellinen. Kanavat 1, 7 ja 13 ovat täysin eri taajuusalueella. Käytännössä kanavien valinnassa toimiva ratkaisu on, jos kanavien välillä pidetään kahden käyttämättömän kanavan väli. Eli kanavat 1, 5, 9 ja 13 ovat käyttökelpoisia. Kanavilla 1, 4, 7, 10 ja 13 voi vielä rakentaa toimivan taajuusalueen, kun tukiasemat sijoitetaan hyvin. Kuviossa 5 nähdään kanavien päällekkäisyydet ja että kanavat 1, 7 ja 13 ovat häiritsemättömiä.



KUVIO 5. IEEE 802.11 2,4 GHz taajuusalueen kanavat (soveltaen Puska 2005, 39)

5 GHz:n taajuusalueella on 12 häiritsemätöntä kanavaa, joiden kaistan leveys on 20 MHz. Tämän alueen yhteys onkin sen vuoksi parempi, koska taajuusalueet eivät mene päällekkäin. 5 GHz:n taajuusalueella saavutetaan melkein häiriötön verkko. Muut laitteet eivät pääse häiritsemään signaalia. Korkeamman taajuuden heikkouksia ovat sen signaalin kantavuuden heikkeneminen. (Geier 2005, 128–129.)

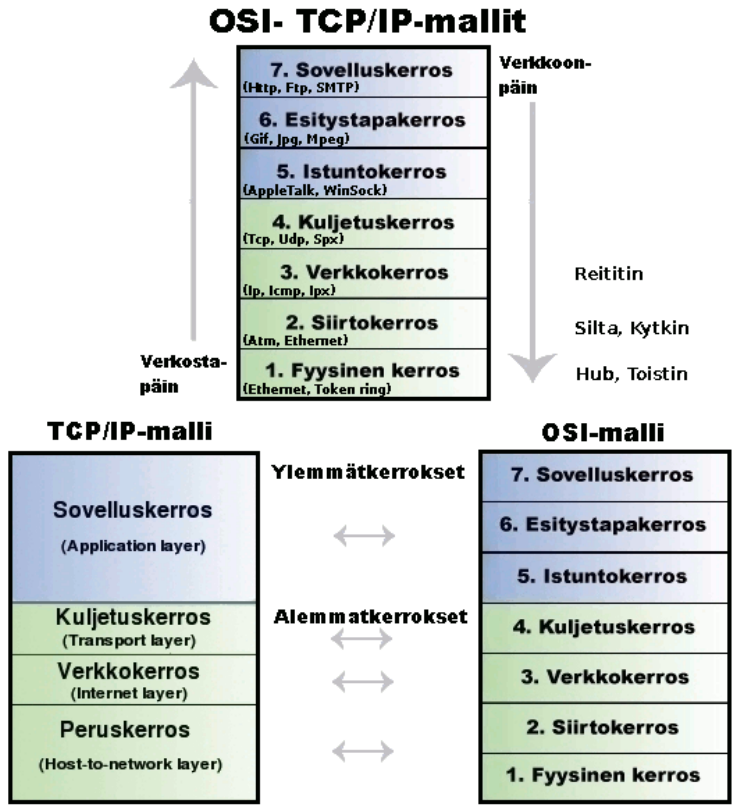
Kanavat voidaan wlan-verkoissa määritellä automaattisesti tai manuaalisesti. Automaattinen toiminta on auto-channel -toiminto, jonka avulla tukiasemat kommunikoivat toisilleen, selvittävät ympärillä olevien signaalien taajuudet ja valitsevat näin parhaan mahdollisen kanavan. Auto-channel -toiminto on kehittynyt ja kehittyy edelleen, mutta aina se ei ole täysin toimiva vaihtoehto. Kanavien vaihtuvuus aiheuttaa vaihtuvuutta signaaliin vahvuuteen ja tämä heikentää yhteyttä. Manuaalisessa kanavan valinnassa kannattaa tukiasemien kanavointi miettiä siten, että ne ovat mahdollisimman kaukana toistensa alueista eli vierekkäisiä tukiasemia ei aseteta vierekkäisille kanaville. (Puska 2005, 39.)

2.4 OSI-malli

ISO-järjestö (International Standards Organization) kehitti 1980-luvun alussa OSI-mallin (Open Systems Interconnect), joka jakaa tietoliikenneverkon tehtävät seitsemään eri kerrokseen. Tätä ennen verkkotekniikoita oli kehitetty 1960-luvulta lähtien. Kehittäjinä pääasiassa tietokonevalmistajat IBM (International Business Machines) ja DEC (Digital Equipment Corporation). IBM:llä oli oma kehitetty verkko-malli SNA-verkko (Systems Network Architecture) ja DEC:llä oma DECnetti. Näissä verkkomalleissa ongelmaksi muodostuivat verkkojen yhteensopivuusongelmat. (Geier 2005, 52–54.)

Yhteensopivuudet toivat niin paljon ongelmia, että kaikki suurimmat tietotekniikkayritykset päättivät luopua valmistajakohtaisista standarteista. Täydellistä yhteensopivuutta ei voitu varmistaa valmistajakohtaisille malleille. Nykyään melkein kaikki verkkolaitteet käyttävät standardia TCP/IP (Transmission Control Protocol/Internet Protocol). Kuviosta 6 nähdään TCP/IP-mallin kerrokset. (Puska 2005.)

OSI-malli on kuitenkin parhain malleista. Malli on seitsemänkerroksinen ja siinä on kuvattu lähiverkon toiminta omina kerroksinaan. Langattoman verkon toimintaa on helppo tarkastella OSI-mallista. Siinä jokainen kerros tukee yläpuolellaan olevaa kerrosta. Kuviossa 6 nähdään OSI-Mallin kerrokset ja vertaukset TCP/IP mallin kerroksiin. (Granlund 2007, 10.)



KUVIO 6. OSI ja TCP/IP mallit (Krimaka.net)

OSI-mallin ensimmäinen kerros on fyysinen kerros (Physical Layer). Kerros käsittää laitteistojen fyysisen kaapeloinnin ja signaalin siirtymisen. Se sisältää tietoa signaalin siirtymisestä. Fyysiseen kerrokseen kuuluu esimerkiksi kaapelityypit, signaalin jännitetasot, vaimennus ja liitintyypit. Esimerkkeinä sen standardeista ja protokoloista mainittakoon Ethernet, Wi-Fi, Bluetooth. (Puska 2000)

Toinen kerros OSI-mallissa on siirtotieyhteys (Data Link Layer). Tämä kerros käsittää tekniikat, jotka liittyvät tietoverkojen datan lähetykseen, esimerkiksi kehysten muodostamisen ja lähettämisen. Laitteista siihen kuuluvat kytkimet, sillat, tukiasemat sekä verkkokortit. Tähän kerrokseen myös kuuluvat 802.11-standardit. (Puska 2000)

Kolmas kerros on verkkokerros (Network Layer), joka sisältää eri reitityksetja IP-osoitteet . Neljäs kerros on kuljetuskerros (Transport Layer), jonka tehtävänä on huolehtia kuljetusprotokolasta.. Viides kerros on istuntokerros (Session Layer), johon kuuluvat käyttöoikeudet ja suojaukset. Kuudes kerros on esitystapakerros (Presentation Layer), johon kuuluu tiedonsiirto palvelimien välillä. Seitsemäs kerros on sovelluskerros (Application Layer). Se sisältää sovellusten ja käyttöjärjestelmien osat. Kuviossa 6 nähdään, että kerrokset on yhdistetty yhdeksi suuremmaksi ohjelmakokonaisuudeksi. (Puska 2000.)

OSI-mallin toiminta alkaa ylimmästä kerroksesta (kuvio 6). Kerrosten välillä toimivat palvelupyynnöt. Palvelupyynnöt muutetaan aina sopivaan muotoon kerrosten välillä. (Puska 2000.)

2.5 WLAN-standardit

2.5.1 IEEE 802.11

Suomessa voi käyttää vapaasti taajuuksilla 2,4 GHz ja 5 GHz toimivia langattomia verkkoja, jos laitteet täyttävät standardien määräykset eikä lähetystehoja ylitetä. Langattomien laitteiden valmistaja tai maahantuoja huolehtii testauksesta ja vastaa, että laitteet ovat standardien mukaiset. Langattomilla verkoilla on useita standardeja. Yleisin on kuitenkin IEEE:n (Institute of Electrical and Electronics Engineers) 802.11-standardista. Standardin maksiminopeus on 2 Mbps. Kuuluvuus on olosuhteista riippuen sisätiloissa 50–180 m ja ulkotiloissa yli 300 m. Samalla alueella pystyy toimimaan 15 tukiasemaa. (Geier 2005, 118; Puska 2005, 15.)

2.5.2 802.11b

802.11b on vuonna 1999 hyväksytty laajennus 802.11-standardiin. Siinä on neljä nopeusluokkaa, ja huonoissa olosuhteissa nopeutta voidaan pudottaa alkuperäisen standardin nopeusluokkiin. Standardin nopeusluokat ovat 1, 2, 5,5, 11 Mbps. 802.11b

toimii 2,4 GHz taajuusalueella. Todellinen nopeus on kuitenkin noin 5 Mbps. Tämän standardin etu on suuri kantama, haitta kanavien päällekkäisyys. Taajuusalueella 2,4 GHz on vain kolme toisiaan häiritsemätöntä kanavaa. Taajuus-alueella on myös yleisesti käytössä olevia muita laitteita. Nämä laitteet, kuten mikro-aaltouuni ja langattomat puhelimet, käyttävät tätä taajuutta ja aiheuttavat näin häiriötä. (Geier 2005, 125–127.)

2.5.3 802.11a

Myös 802.11a-standardi laajennus julkaistiin vuonna 1999. Standardi sisältää kahdeksan nopeusluokkaa ja käyttää 5 GHz taajuusaluetta. Standardin enimmäisnopeus on 54 Mbps. Se käyttää kolmea 100 MHz:n taajuuskaistaa. Jokaisessa taajuuskaistassa on käytössä neljä vapaasti valittavaa kanavaa. Todellisuudessa lähetysnopeus on noin 32 Mbps ja maksiminopeus 54 Mbps on vain teoreettinen lähetysnopeus. (Geier 2005, 125–127.)

Tässä tekniikassa on hyviä ja huonoja puolia. Tiedonsiirto on nopeampaa 5 GHz taajuusalueella. Muut laitteet, kuten mikroaaltouunit, eivät aiheuta häiriötä tällä taajuusalueella. Kanavien kaista on leveämpi 5 GHz:n alueella. Standardin päällekkäisten kanavien häiriö on pieni. Huonona puolena on, ettei taajuutta käyttäviä laitteita ole saatavilla ja laitteiden hinnat ovat kalliita. Standardilla on pieni kuuluvuus ja yhteyden nopeus putoaa nopeasti, kun kuuluvuusalueen reunaa kohti mennään. 802.11b- ja 802.11g-verkoihin nähden eri taajuusalue aiheuttaa myös yhteensopivuusongelmia. (Geier 2005, 125-127.)

2.5.4 802.11g

802.11g-standardi laajennus julkaistiin kesäkuussa 2003, ja se käyttää 2,4 GHz taajuusaluetta. Se sisältää kaksitoista eri nopeusluokkaa. Luokille 1, 2, 5,5 ja 11 Mbps käytetään CCK-modulointia ja luokille 6, 9, 12, 18, 24, 36, 48 ja 54 Mbps käytetään OFDM-modulointia. Todellinen nopeus tiedonsiirrossa on kuitenkin noin 20 Mbps. Yhteensopivuus 802.11b-standardin kanssa saavutetaan käyttämällä CCK-modulointia. 802.11g on samanlainen 802.11a-standardin kanssa. Sen huonoja puolia on, että nopeus laskee jos verkossa on yksikin laite, joka ei tue 802.11g standardia. Tämän aiheuttaa modulointiteknikoiden erot eri standardien välillä. (Geier 2005, 125–127.)

2.5.5 802.11n

802.11n-standardi julkaistiin syyskuussa vuonna 2009. Se sisältää useita parannuksia fyysiseen ja MAC-kerrokseen. Parannus määrittää suurimmaksi bruttonopeudeksi 600 Mbps. Todellisuudessa nopeus on noin 100–200 Mbps luokkaa. Isoin lisäys on MIMO-tekniikka (Multiple Input Multiple Output), joka lisää nopeutta ja luotettavuutta. MIMO-tekniikka hyödyntää signaalien monimuotoisuutta ja päällekkäisyyksiä käyttämällä useaa lähetys- ja vastaanottoantennia samanaikaisesti. Tekniikka siis käyttää useaa antennia, jossa jokainen antennipari käsittelee omaa lähetettään.

Toinen parannuksista on vierekkäiset kanavat yhteen sitova 40 MHz toiminto, joka mahdollistaa yli kaksinkertaisen tiedonsiirtonopeuden. Kaistanleveysvaihtoehtoina on 20 tai 40 MHz. Lisäksi parannuksena on kehysten yhdistäminen, jolla saadaan suoritustehoa, kun yhdistetään useita paketteja. 802.11n-standardi kehitettiin vähentämään häiriöitä, optimoimaan tiedonsiirtoväyliä ja parantamaan langattomien laitteiden herkkyyttä. Standardi pystyy käyttämään 2,4 GHz:n ja 5 GHz:n taajuusalueita ja on yhteensopiva vanhempien standardien kanssa. Yhteensopivuudella mahdollistetaan liukuva siirto uuteen standardiin. (Geier 2005, 125–127.)

2.5.6 Muut 802.11-standardilaajennukset

802.11e-laajennus julkaistiin vuonna 2005, ja se sisältää toimintoja verkon palvelulaadun (Qos) kehittämiseksi. 802.11e-verkossa voidaan merkitä tukiasemille korkeamman kiireellisyysasteen liikennettä. Tämä standardi on enemmän suunnattu multimedialiikenteelle.

802.11f-laajennus on vuonna 2006 julkaistu suositus eri valmistajien laitteiden yhteensopivuuden parantamiseksi. Kun verkossa on eri laitevalmistajien tukiasemia, niin laajennus parantaa yhteensopivuuksia. Tämä laajennus ei ole enää käytössä. 802.11d-laajennus on julkaistu vuonna 2001, ja se sisältää uusia kenttiä sille, että tukiasema kertoo laitteen sijaintimaan. Ajatuksena on, että langaton laite osaa valita oikean taajuuskaistan. Laajennus on hyödyllinen paljon matkustaville ihmisille. 802.11h on vuonna 2004 julkaistu laajennus, ja se sisältää muutoksia 5 GHz:n taajuusalueella toimiville langattomille laitteille Euroopassa. 802.11i-laajennus parantaa valmistajakohtaisia tietoturvaominaisuuksia. Taulukossa 1 on nähtävissä lisää standardilaajennuksista. (Geier 2005, 125–127.)

Taulukko 1. IEEE:n 802.11-standardilaajennukset

Standardi	Ominaisuus
802.11d	Sisältää uusia kenttiä tukiasemien levitysviesteihin, joilla kerrotaan laitteen sijaintimaa.
802.11h	Sisältää muutoksia 5 GHz:n taajuusalueella toimiville langattomille laitteille Euroopassa. Sisältää dynaamisen taajuuden valinnan (DFS) sekä lähetystehon hallinnan (TCP).
802.11e	Verkon suorituskyvyn ja palvelulaadun parantamiseen liittyviä päivityksiä. (Quality of Service, QoS)
802.11i	Parantaa aikaisemmin osittain valmistajakohtaisia tietoturvaominaisuuksia ja määrittelee ne standardin osaksi. Mahdollistaa AES-salauksen käyttämistä sekä 802.1x-autentikointia.
802.11j	Japaniin alueeseen liittyvä aluepäivitys.
802.11k	Mahdollistaa verkon tehokkuuden parantamisen kanavavalintojen, roamingin ja TCP:n kautta.
802.11p	Mahdollistaa liikkuvien autojen välisen kommunikoinnin.
802.11s	Mahdollistavat EES-solmuverkot
802.11u	Lakimuutos fyysiseen ja MAC-tasoon, mahdollistaa tiedonsiirron muiden standardien välillä.
802.11v	Lisää suoritustehoa ja vähentää häiriötä.
802.11w	Datakehysten hallintaa lisäävä tietoturva.

2.5.7 HiperLAN

ETSI:n (European Telecom-muniactions Standards Institute) kehittämä HiperLAN (High Performance Radio LAN) on toinen langattoman lähiverkon standardi. HiperLAN sisälsi ensimmäisessä versiossaan 20 Mbps datasiirtonopeuden 5 GHz:n taajuusalueella . Standardin seuraava versio oli HiperLAN/2, joka toimii samalla taajuusalueella kuin aikaisempi versio, mutta tarjoaa 54 Mbps nopeuden. HiperLANin kolmas versio on HomeRF, joka on tarkoitettu kotikäyttöön. Tätä ei enää ole tarjolla eikä laitteita ei enää valmisteta. (Puska 2005, 47–48.)

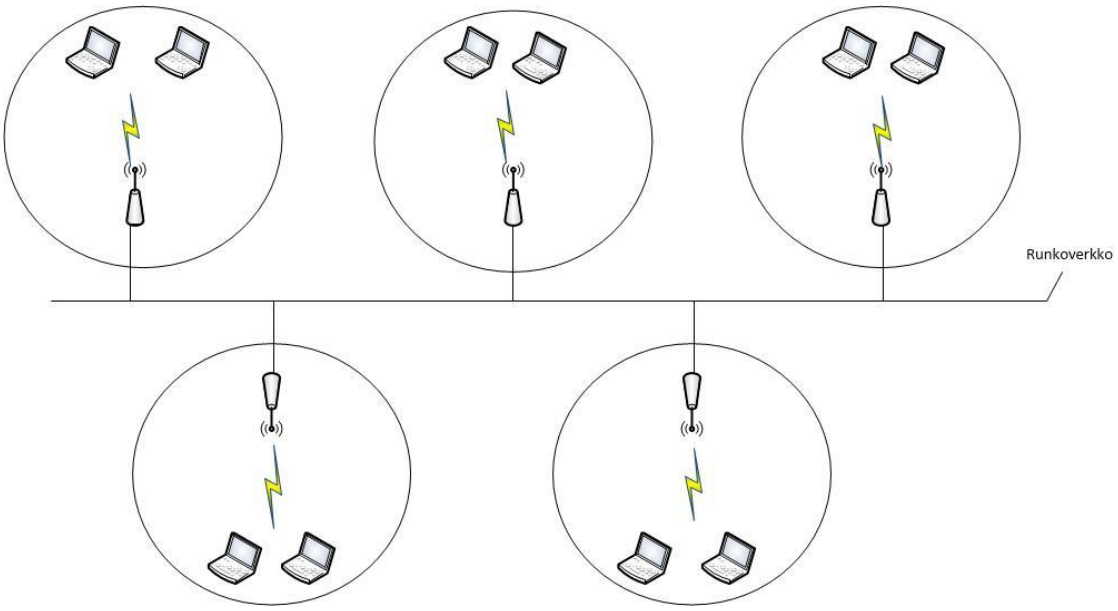
2.6 WLAN-topologiat

Topologiat ovat osa langatonta verkkoa. Topologioihin kuuluvat IBSS, BSS ja ESS. Se mitä langattomalta verkolta halutaan, vaikuttaa siihen mitä topologiaa käytetään. (Granlund 2007, 294–295.)

2.6.1 ESS, Extended Service Set

ESS-verkko (Extended Service Set) on laajennettu palveluryhmä ja se koostuu useasta tukiasemasta, jotka kytketään samaan verkkoon. ESS-verkkoon kuuluvat kaikki kaksi tai useammasta tukiasemasta koostuvat langattomat verkot. DS on lyhenne niiden käyttämästä runkoverkosta. ESS-topologiaa käytetään muodostamaan suuri langaton lähiverkko. Sen tarkoitus on kattaa useita huoneita ja kerroksia. Verkon sisällä voidaan liikkua vapaasti roaming-tekniikan avulla. Kuviossa 7 EES-verkkotopologia havainnollistettuna. (Granlund 2007, 294–296.)

ESS-verkkotopologian runkoverkko (Distribution System, DS) mahdollistaa autentikoinnin työasemille. Tällöin oikeutettu työasema voi liittyä verkkoon tai poistua autentikointitilasta. Autentikoituneiden työasemien liikennettä voidaan seurata siirtotien suojauspalvelun avulla. Tiedonsiirtopalvelu mahdollistaa kahden työaseman välisen tiedonsiirron. (Granlund 2007, 294–295.)



KUVIO 7. ESS-verkkotopologia

2.6.2 BSS, Basic Service set

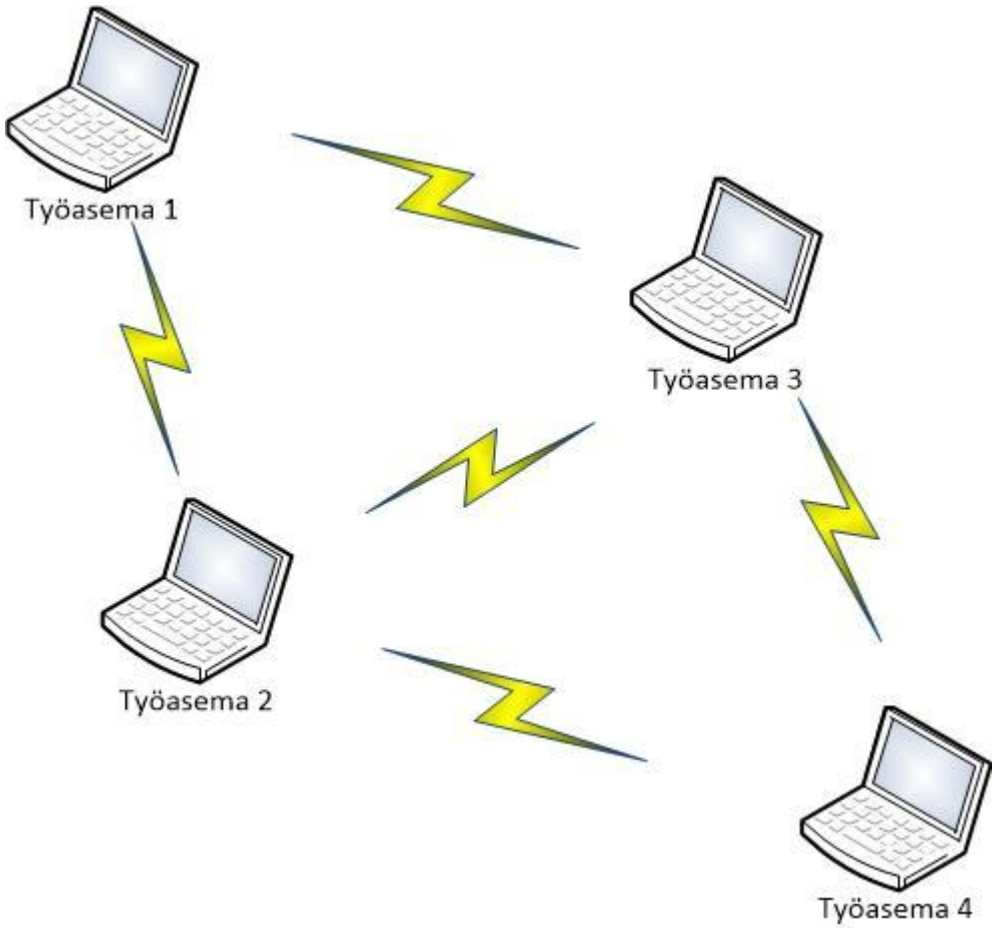
BSS-verkko (Basic Service Set) on peruspalveluryhmä. Se on käytetyin langattoman lähiverkon topologia koti- ja pienyritysverkoissa. BSS-topologiassa verkolla on tukiasemat, jotka ovat liittyneenä pääverkkoon. BSS-verkko vaatii toimiakseen aina tukiaseman. Ilman tukiasemaa yhteys katkeaa ja tällöin verkko ei ole käytettävissä. Kuviossa 8 on BSS-verkkotopologiasta havainnollistava kuva. (Granlund 2007, 294–296.)

KUVIO 8. BSS-verkkotopologia

2.6.3 IBSS, Independent Basic Service Set

IBSS (Independent Basic Service Set) on itsenäinen palveluryhmä. Se toimii laitteiden välisessä kommunikoinnissa. IBSS on yksinkertainen malli. Siinä on paljon katvealueita eikä sen toimivuus ole niin hyvä kuin muissa topologioissa. Kuviossa 9 on yksinkertainen malli IBSS-verkkotopologiasta. (Granlund 2007, 294–296.)

Yhteydet topologian sisällä voivat katketa joissain tapauksissa. Kuviossa 9 on kuvattu kuinka työasema 1 ja 4 eivät pysty yhteyteen toisilleen, koska etäisyys on liian suuri. (Granlund 2007, 294–296.)



KUVIO 9. IBSS-verkkotopologia

.

2.7 WLAN-verkkolaitteet

2.7.1 Verkkokortit

Langattomien verkkojen käyttö vaatii laitteelta, että siinä on verkkokortti. Verkkokortin on oltava oikeanlainen, jotta sillä pystytään käyttämään langattomia verkkoja. Viestintä langattomien verkkojen avulla ei toimi ilman verkkokorttia. Korttien liitäntävaihtoehtoja on useita. Ulkomuodot riippuvat korteilla valmistajasta. Esimerkkinä on kuva 2 PCIe-väylään liitettävä langaton verkkokortti. Pöytätietokoneisiin liitettävissä verkkokorteissa on usein ulkoinen antenni. Nykyaikaisissa laitteissa on yleensä jo sisäiset antennit.

KUVA 2. PCIe-väylään liitettävä langaton verkkokortti (Cisco Lan Controller Modules)

2.7.2 Tukiasemat

Langattomiin verkkoihin yleensä kuuluu tukiasema (Access Point, AP). Tukiasemalla jaetaan haluttu verkko käyttöön ja tukiasemien tulee kuulua langalliseen verkkoon. Tukiasemat voi toimia myös yhdyskäytävänä, jolloin käyttöön saadaan muun muassa reititys, NAT, DHCP ja VPN. Kuvassa 3 nähtävissälangaton tukiasema kahdella antennilla.

KUVA 3. CISCO:n langaton tukiasema kahdella antennilla. (Modattava Wlan tukiasema)

2.7.3 WLAN-kytkin

Wlan-kytkimiä (WLAN Switch, Access Router, WLAN-kontroller) käytetään sellaisissa verkoissa, joissa on satoja tukiasemia. Tukiasemia voi olla useissa kohteissa useita ja niitä voidaan hallita kytkimen avulla keskitetysti. Niiden yksittäinen asentaminen ja konfigurointi on haasteellista ja aikaa vievää. Wlan-kytkiemien avulla voidaan helpottaa asentamista ja hallintaa. Niillä voidaan keskitetysti hallita sekä konfiguroida turvallisuuteen, laadunvalvontaan ja ongelmiin liittyviä asioita.

WLAN-kytkin on hyvä ratkaisu isompiin verkkoihin. Sillä saadaan laitteet myös helposti päivitettyä uusiin versioihin. Kytkimien malleja on erilaisia. Normaaleihin kytkimiin voidaan liittää WLAN kontrolleri, jolloin kytkimen kautta voidaan hallita wlan-verkkoa. Kuvassa 4 kontrolleri moduuli, jonka voi asentaa kytkimeen.

KUVA 4. WLAN kontrolleri moduuli (Cisco Wireless Lan Controller Modules)

2.8 Kontrolleripohjaiset verkot

Kontrolleripohjaisia verkkoja kutsutaan keskitetysti hallittaviksi verkoiksi: Langatonta verkkoa voidaan hallita kontrollerin kautta keskitetysti. Isojen tilojen ja rakennusten langaton verkko vaatii useamman tukiaseman. Jokaisen tukiaseman hallinta olisi työlästä ja aikaa vievää, kun käytössä on esimerkiksi yli kymmenen tukiasemaa. Kontrollerilla voidaan hallita tukiasemia ja määrittää pääsynhallinta ja tietoturva. Lisäksi voidaan määrittää, mikä verkkonimi kuuluu mistäkin tukiasemasta. Kontrollereiden alaisuuteen voidaan liittää satoja tukiasemia. Keskitetty hallinta mahdollistaa asetusten tekemisen yhdestä paikasta. Asetuksista saadaan muokattua niin SSID:n, salauksen ja tunnistamisen kuin muiden palvelujen asetuksia. (Joensuu 2006.)

2.8.1 Varmistaminen

Varakontrollerilla voidaan varmistaa toimivuus, mikäli ensisijainen kontrolleri rikkoutuu. Se ottaa tarvittaessa automaattisesti tukiasemat kontrolliinsa. Verkon hallinta tapahtuu silloin varakontrollerin kautta eikä tietoliikennekatkoksia pääse syntymään.

Kontrollerit sijoitetaan yleensä moduuleina kytkimiin. Tällöin on huolehdittava myös siitä, että kytkin säilyy ehjänä. Virransyöttö tapahtuu kytkimen kautta, joten varmennus virransyöttöön on tehtävä koko kytkimelle. (Joensuu 2006.)

2.8.2 Tietoturva kontrollereilla

Kontrollereilla voidaan hoitaa myös tietoturvaominaisuudet. Niiden tietoturvaominaisuuksiin kuuluu ACL (Acceess Control List), jolla voidaan suodattaa liikenne pelkkien IP-osoitteiden perusteella. NAT (Network Address Translation) -verkko-osoitteen muunnos saadaan hoidettua sisä- ja ulkoverkon välillä. MAC-osoitteiden suodatus on web-portaalitunnistus, siinä selain pyytää erikseen vielä tunnistuksen verkkoon. Liikenteen salaukset ja tunkeutumisten havaitseminen sekä estäminen voidaan määrittää kontrollereiden avulla. Kontrollerin käyttöliittymä mahdollistaa myös liikenteen seuraamiseen. Kontrollerilta voidaan seurata, mikä laite on liittynyt mihinkin tukiasemaan ja miten paljon se käyttää kaistaa verkosta.

Kontrollereiden käyttöliittymään kirjautuminen voidaan salata erillisellä käyttäjätunnuksella ja salasanalla. Hallintaa voidaan myös rajoittaa siten, ettei niiden hallintaan päästä kirjautumaan kuin tietystä VLAN:sta. Kontrollereiden avulla voidaan myös tukiasemille määrittää useita SSID-verkkonimiä. (Joensuu 2006.)

3 LANGATTOMAN LÄHIVERKON TIETOTURVA

3.1 Langaton tietoturva

Langattomien verkkojen tietoturva on paljon haasteellisempaa, koska sitä ei pystytä hallitsemaan niin helposti kuin kaapeliverkkoa. Uhkana on, että ulkopuolinen voi päästä kiinni dataan, jos tietoturva ei ole riittävän hyvä.

Langattomien lähiverkkojen laitteiden fyysinen tietoturva on tärkeää. Laitteet kannattaa sijoittaa paikkoihin, joihin ulkopuolisten on vaikea päästä. Verkkolaitteiden portteihin ei pitäisi pystyä liittämään ulkopuolisia laitteita. Laitteiden salasanat on vaihdettava. Salasanan olisi hyvä sisältää numeroita ja isoja kirjaimia. Erikoismerkkejä on myös hyvä käyttää, mikäli mahdollista. (Puska 2005, 70.)

3.1.1 Palvelunesto (Dos)

Palvelunestohyökkäyksellä voidaan saada haittaa aikaan langattomassa lähiverkossa. Palvelunestohyökkäyksiä on monia ja yksi niistä on väsytyshyökkäys. Siinä verkko väsytetään lähettämällä isoja määriä turhia paketteja, jolloin verkon resurssit kuluvat loppuun ja verkko lopettaa toimimasta. Toinen keino on käyttää voimakkaita radiosignaaleja, jotka voivat häiritä langatonta verkkoa.

Palvelunesto voi tapahtua myös tarkoittamatta. Jos vaikka mikroaaltouuni lähettää häiritsevän signaalin verkkoon. (Puska 2005, 70.)

3.1.2 Välistävetohyökkäys

Välistävetohyökkäys tapahtuu siten, että verkon välissä on laite joka kaappaa kaiken liikenteen.Välistävetohyökkäys käyttää apunaan TCP/IP-verkosta tuttua ARP-protokollaa, joka selvittää kohdeverkkokortin fyysisen osoitteen.

Välistävetohyökkäyksiä vastaan voidaan suojautua Secure ARP tekniikalla (SARP). SARP muodostaa niin sanotun turvatunnelin tukiaseman ja asiakkaan välille. SARP hylkää kaikki tunnelin ulkopuolelta tulevat pyynnöt, jolloin hyökkäys on mahdoton. (Thomas 2005.)

3.2 Suojautumistekniikat

Suojautuminen eri hyökkäyksiltä langattomia lähiverkkoja kohtaan on vaativaa ja haasteellista. Sitä voitaisiin parantaa rakennuksien eri rakennustekniikoilla ja suunnitelmilla. Tämä on kuitenkin kallista eikä niitä huomioida usein rakennettaessa. Lisäksi jälkikäteen olevat ratkaisut rakennuksiin on haasteellisia toteuttaa. Tämän vuoksi onkin suositeltavaa käyttää tietoteknisiä suojautumismuotoja. (Geier 2005, 177–178.)

3.2.1 WEP-salaus

WEP-salaus (Wired Equivalent Privacy) on 802.11-standardin suojaustekniikka. WEP pyrittiin aikoinaan kehittämään salaustekniikaksi, joka vastaisi kaapeliverkon turvallisuutta. (Granlund 2007, 320.)

WEP-salauksessa kaikilla laitteilla on sama salausavain, jota ilman verkkoon ei pääse liittymään. Salausavaimena voidaan käyttää 64- tai 128-bittistä salausavainta. WEP-salauksessa käytetään RC4-suojausalgoritmia. Datan korruptoituminen estetään CRC-32-tarkistussummalla, jonka avulla paketin vastaanottaja varmistuu tiedon aitoudesta. (Granlund 2007, 320.)

3.2.2 WPA/WPA2-salaus

WPA käyttää salausavainten hallintaan TKIP-tekniikkaa (Temporal Key Integrity Protocol). Sillä on mahdollisuus käyttää 802.1x-autentikointia käyttäen EAP (Extensible Authentication Protocol) -pakettisuodatusta. Toinen vaihtoehto on käyttää PSK (Pre Shared Key) – salausavainta. PSK-salausavainta käytettäessä tukiasema ja asiakas todentavat toisensa, että molemmilla on sama avain. WPA2-versiossa salausavaimen hallintaan liittyvää tietoturvaa lisättiin AES-salauksella (Advanced Encryption Standard). WPA-salaukseen kuuluu myös MIC-toiminto, jonka avulla hallitaan ja tarkistetaan pakettien eheys. (Granlund 2007, 320.)

WPA-salaus on suunniteltu käytettäväksi 802.1x-todennuksen kanssa, joka jakaa jokaiselle käyttäjälle omat avaimet. Salausta voidaan kuitenkin käyttää myös jaetulla avaimella. WPA-PSK on jaetun avaimen todennustekniikka. Tämä on yleisesti kotikäyttöihin suunniteltu todennuspalvelu. (Granlund 2007, 320.)

WPA-salaus suojautuu DoS-hyökkäyksiä vastaan siten, että se sulkee langattoman verkon, kun hyökkäys havaitaan. Tällöin kaikki langattomassa verkossa olevat käyttäjät tipahtavat pois. Tämä on huono puoli WPA-salauksessa, koska tästä voi aiheutua tiedon menetyksiä. Näitä ongelmia on pyritty korjaamaan WPA 2 -versiossa. (Granlund 2007, 320.)

3.2.3 TKIP

TKIP (Temporal Key Integrity Protocol) sisältää algoritmeja, joiden tarkoituksena on korjata WEP-salauksen tietoturvaa erityisesti salasanan muodostamisessa. TKIP salaa liikenteen RC4-algoritmilla ja salausavaimen pituus on 128-bittiä. (Geier 2005, 183.)

TKIP:n salauksen hyviä puolia on kehyskohtaiset avaimet. Tällöin laitteet alkavat salaamaan 128 bittisellä aloitusavaimella (Temporal Key) ja se yhdistetään työaseman MAC-osoitteeseen sekä kehyksen järjestysnumeron neljään eniten merkitsevään bittiin. Väliaikainen avain yhdistetään kahteen alimpaan bittiin, josta syntyy kehyskohtainen avain. Se on jokaisella laitteella omansa. TKIP vaihtaa näitä satunnaisavaimia noin 10000 paketin jälkeen, riippuen vähän tietoturvan vaatimuksista. Salakuuntelijoille ei anneta mahdollisuutta kerätä tarpeeksi dataa, että avain voitaisiin murtaa. (Geier 2005, 183.)

3.2.4 AES

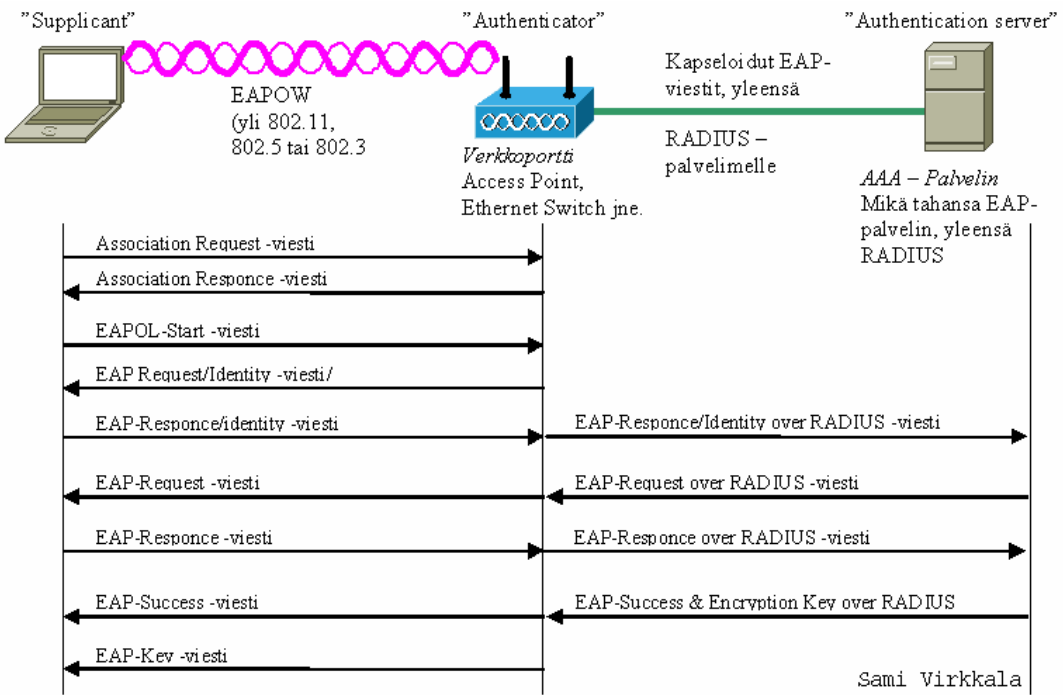
AES (Advanced Encryption Standard) on symmetrinen salausalgoritmi. Symmetrisyys tarkoittaa sitä, että tiedon salaamiseen ja purkamiseen käytetään samaa avainta. AES-salattua tiedostoa on lähes mahdoton purkaa. (Thomas 2005.)

3.2.5 MAC-suodatus

MAC-suodatusta voidaan käyttää langattomissa verkoissa. Tällöin langattoman verkon liikenne rajataan suodattimen avulla siten, että tukiasemaan pääsevät liittymään vain laitteet, joiden MAC-osoite on liitetty suodatuslistalle. MAC-suodatusta käytetään harvoin, koska on työlästä syöttää MAC-osotteita järjestelmään. (Puska 2005, 73.)

3.2.6 802.1x-todennus

802.1x-todennuksen ideana on, että asiakas muodostaa yhteyden langattomaan tukiasemaan. Tukiasema avaa asiakkaalle portin, jossa on sallittua vain EAP-pakettien (Extensible Authentication Protocol) lähettäminen. Asiakkaalle avataan loput portit vasta, kun tunnistaminen on saatu tehtyä. Tällöin http DHCP- ja POP3-pakettien lähettäminen mahdollistuu. 802.1x-todennus on tehokas tapa suojata yrityksissä langatonta lähiverkkoa. Kuviossa 11 on 802.1x todennuksen vaiheet. EAP lähettää aluksi aloitusviestin ja tukiasema vastaa identiteettipyyntöviestillä. Työaseman vastatessa pyyntöön EAP-vastauspaketilla, autentikointipalvelin käyttää todennusalgoritmia asiakkaan identiteetin selvittämiseen. Jos käyttäjä on oikeutettu käyttämään verkkoa, portit avataan ja hylätään, jos käyttäjällä ei ole oikeutta. (Geier 2005, 189–190.)



KUVIO 11. 802.1x todennuksen vaiheet (Sami Virkkala 2005.)

3.3 802.1x-todennus RADIUS-palvelimella

802.1x-todennuksessa voidaan käyttää RADIUS-palvelinta autentikointiin. Palvelin toimii tällöin käyttäjän varmistajana, sallitaanko asiakkaan liittyä tukiasemaan. Se tarkastaa kaikki yhteydenottopyynnöt. Pyynnöt joko hyväksytään tai hylätään.
RADIUS-client, esim. tukiasema välittää käyttäjä- ja yhteysparametrit RADIUS-palvelimelle RADIUS-viestinä. Palvelin suorittaa autentikoinnin ja hyväksynnän pyyn-

töön. Tukiasemassa kiinni olevat laitteet suorittavat myös kommunikointia palvelimen kanssa. Laitteiden, tukiasemien ja palvelimen välinen lähetys-/vastausliikenne on nähtävissä kuviossa 11, että autentikointi tapahtuu 802.1x-todennuksen vaiheiden mukaan. (Seppänen 2006.)

RADIUS-palvelimen ja clientin välinen liikenne on autentikoitu jaetun avaimen avulla (eng. Shared key). Tämä avain ei koskaan liikennöi verkon yli, vaan se on oltava molempien päiden tiedossa etukäteen. RADIUS-palvelimen saadessa kirjautumispyyntö tukiasemalta, käy palvelin läpi tietokannan ja etsii tarvittavan käyttäjänimen. Pyynnössä voi olla myös muuta informaatiota, millaista yhteyttä käyttäjä haluaa käyttää yhteydenottoon. Radiuksessa autentikaatio ja autorisointi on kytketty samaan viestiin. Käyttäjänimen ja salasanan täsmätessä tietokantaan, palauttaa palvelin vastauksen hyväksymisestä. Tähän kuuluu myös atribuutit siitä, millaisia parametreja käytetään yhteydessä. Näitä parametrejä ovat mm. palvelun tyyppi, protokolla, VLAN, käytettävä Access-lista tai salaustyyppi. RADIUS-palvelimelle voidaan myös esittää konekohtaisia rajoituksia. Tällöin vain tietyt koneet toimialueen sisällä voivat liittyä verkkoon. Yleisesti määritellään kone nimen perusteella.

Jos käyttäjä- tai konenimeä ei löydy tietokannasta palvelin lähettää hylkäysvastauksen. Sama tapahtuu, mikäli syötetään salasana väärin. Tämä viesti voi sisältää myös selityksen sille, miksi hylkäys on tapahtunut. (Seppänen 2006.)

3.4 Tunnistusmenetelmät

Laitteet tunnistavat langattoman verkon SSID verkkonimen perusteella. SSID:t on oltava samanlaiset tietyllä verkolla. Langattomien verkkojen tunnistusmenetelmiä ja liikenteen salausmenetelmiä on useita. Tunnistusmenetelmät voidaan luokitella useammallakin tavalla ja tunnistuksessa voidaan käyttää useampia menetelmiä päällekkäin, esimerkiksi MAC-filteröintiä ja WPA-tunnistusta. Tunnistusmenetelmiin lukeutuvat aikaisemmin selvitetyt 802.1x-todennus, MAC-tunnistus, WEP, WPA ja WPA2. (Airaksinen & Niemelä 2006.)

802.1x on autentikointi, jonka avulla estetään luvattoman laitteen verkkoliikenne tukiaseman kautta. 802.1x kanssa voidaan käyttää myös keskitettyä autentikointipalvelua. RADIUS-palvelimen avulla määritellään keskitetysti laite- tai käyttäjäkohtaisia autentikointitietoja, kuten MAC-osoitteita tai käyttäjätunnuksia ja salasanoja. Tällöin lupa

verkkoliikenteeseen annetaan, jos nämä tiedot löytyvät RADIUS-palvelimelta. (Airaksinen & Niemelä 2006.)

MAC-tunnistus on myös yksi tunnistusmenetelmistä. Jokaisella WLAN-kortilla on oma MAC-osoitteensa, joka on 48 bittinen tunnusluku. Tällä tunnistusmenetelmällä voidaan tämä yksityinen MAC-osoite määrittää, jotta vain tietyt osoitteet pystyvät liikennöimään tukiasemasta. (Airaksinen & Niemelä 2006.)

WEP-, WPA- ja WPA2-salaustunnistukset perustuvat siihen, että käyttäjällä on oltava tiedossa salasana, joka on asetettu tukiasemaan liittymisen ehdoksi. Ilman tätä salasanaa laite ei voi liittyä verkkoon. (Airaksinen & Niemelä 2006.)

3.5 Langattomiin verkkoihin kirjautuminen, annetut oikeudet ja vierailijaverkot

3.5.1 Kirjautuminen

Wlan-verkkoihin kirjautumiseen vaaditaan, että kirjautuva laite omaa wlan-sovittimen ja pystyy näin havaitsemaan langattoman verkon. Laitteet tunnistavat eri verkot verkkonimen (SSID) perusteella. Käyttäjän on itse tiedettävä, mihin verkkoon hänellä on oikeus kirjautua. Avoimiin verkkoihin kirjautuminen tapahtuu ilman tunnistusta ja se on vapaa kirjautumiselle. Verkko voi olla suojattu myös yleisellä salasanalla, jonka laite pyytää päästäkseen kirjautumaan verkkoon. Kolmas ja yrityksissä paljon käytetty todennus eli käyttäjällä on oltava laite, joka on määritelty erikseen hyväksyttäväksi kirjautumiselle. Kirjautumiselle voidaan asettaa myös ehdoksi käyttäjänimi ja salasana.

3.5.2 Oikeudet

Langattomiin verkkoihin voidaan määritellä tiettyjä oikeuksia liikennöintiin verkossa. Avoimiin verkkoihin yleisesti annetaan oikeudet Internet-liikennöintiin. Sisäisissä verkoissa voidaan erikseen määritellä oikeuksia esimerkiksi tiedosto- tai tulostuspalveluihin. Mikäli verkkoon on määritelty oikeudet käyttää tulostuspalvelua verkon kautta, käyttäjä voi tulostaa tällöin verkossa oleviin verkkotulostimiin tätä kautta. Näitä oikeuksia voidaan määritellä esimerkiksi VLAN:n kautta.

3.5.3 Vierailijaverkot

Vierailijaverkot ovat yleinen tapa yrityksissä ja esimerkiksi hotelleissa tarjota Internet-mahdollisuus asiakkaille. Ne ovat yleensä avoimia verkkoja eikä niitä ole erikseen suojattu, vaan liikenne kulkee pääsääntöisesti operaattorin kautta suoraan. Vierailijaverkkoihin pääsyä kuitenkin rajoitetaan erillisten autentikointipalvelimien kautta. Verkkoihin luodaan selainpohjainen kyselyikkuna, jonka kautta kysytään tunnukset verkon käyttöön. Jokaiselle asiakkaalle luodaan tunnukset tietylle aikavälille ja asiakkaan liittyessä verkkoon hän saa IP-osoitteen, mutta kaikki oikeudet verkon käytössä on rajattu. Avattaessa selain niin ohjautuu selain ikkuna automaattisesti kysymään tunnukset verkkoliikennöintiin ja syöttäessä oikeat tunnukset, avautuu oikeus Internet-liikenteelle. (Airaksinen & Niemelä 2006.)

4 SIILINJÄRVEN KUNNAN WLAN-TEKNIIKAN UUDISTAMINEN

Siilinjärven kunta on päättänyt parantaa langatonta lähiverkkoaan uudistamalla sitä. Uudistukseen kuuluu laitteiden uusiminen ja lisääminen. Langattomasta lähiverkosta tulee näin nykyaikainen, mahdollistaen uusien tekniikoiden käytön. Uudesta verkosta tehdään dokumentointi sekä suunnitellaan uusien tukiasemien sijoittamista sekä asennetaan uusia tukiasemia.

Dokumentointi sisältää eri wlan-verkojen verkkokuvat ja selostuksen niiden toiminnasta. Kuviin liitetään verkon yksityiskohtaiset tiedot, joita ei tietoturvan vuoksi esitellä tässä työssä. Työssä ainoastaan näytetään tiedoilta karsittuja kuvia. Lisäksi esitellään uudistamisen eri vaiheita sekä suunnitellaan kunnantalon tukiasemien sijoittelu.

4.1 Lähtötilanne

Siilinjärven kunnalla on olemassa oleva langaton lähiverkko. Langaton lähiverkko kattaa osaksi kunnantalon, kouluja, terveyskeskuksen sekä muita yleisiä kohteita. Tukiasemia on erimallisia ja niiden hallinta tapahtuu kontrollereiden kautta, jotka ovat erillisissä kytkimissä moduuleina.

Siilinjärven langattomassa lähiverkossa on tarjolla verkkoja hallinnolle, kouluille ja terveydenhuollolle sekä omat verkot vierailijoille. Vierailijaverkkoja on kahta mallia: koulujen vierailijat ja muut vierailijat. Hallinnon ja terveydenhuollon langattomiin verkkoihin pääsee liittymään ainoastaan oikeutetut työasemat ja käyttäjät. Vierailijaverkot on toteutettu siten, että vierailijoille luodaan vierailijatunnus, jonka avulla pääsee selaimen kautta Internetin väliseen tiedonsiirtoon. Muuten vierailijaverkko on avoin.

Kunnan langattoman lähiverkon uudistukseen kuuluvat laitteiden uusimista sekä tekniikan mahdollinen parantaminen. Uudelle langattomalle lähiverkolle hankittiin HP:n uudet kontrollerit ja tukiasemat. Uusia HP:n MSM765-kontrollereita on kaksi kappaletta. (Kuva 4). Kontrollerit sijoitetaan erillisiin kytkimiin. Tukiasemina toimivat HP:n MSM430-tukiasematyypit. (Kuva 5.)

KUVA 4. HP MSM765 Mobility Controller (HP.com)

KUVA 5. HP MSM430 Dual Radio 802.11n Access Point (HP.com)

4.2 Uudistettu langaton lähiverkko

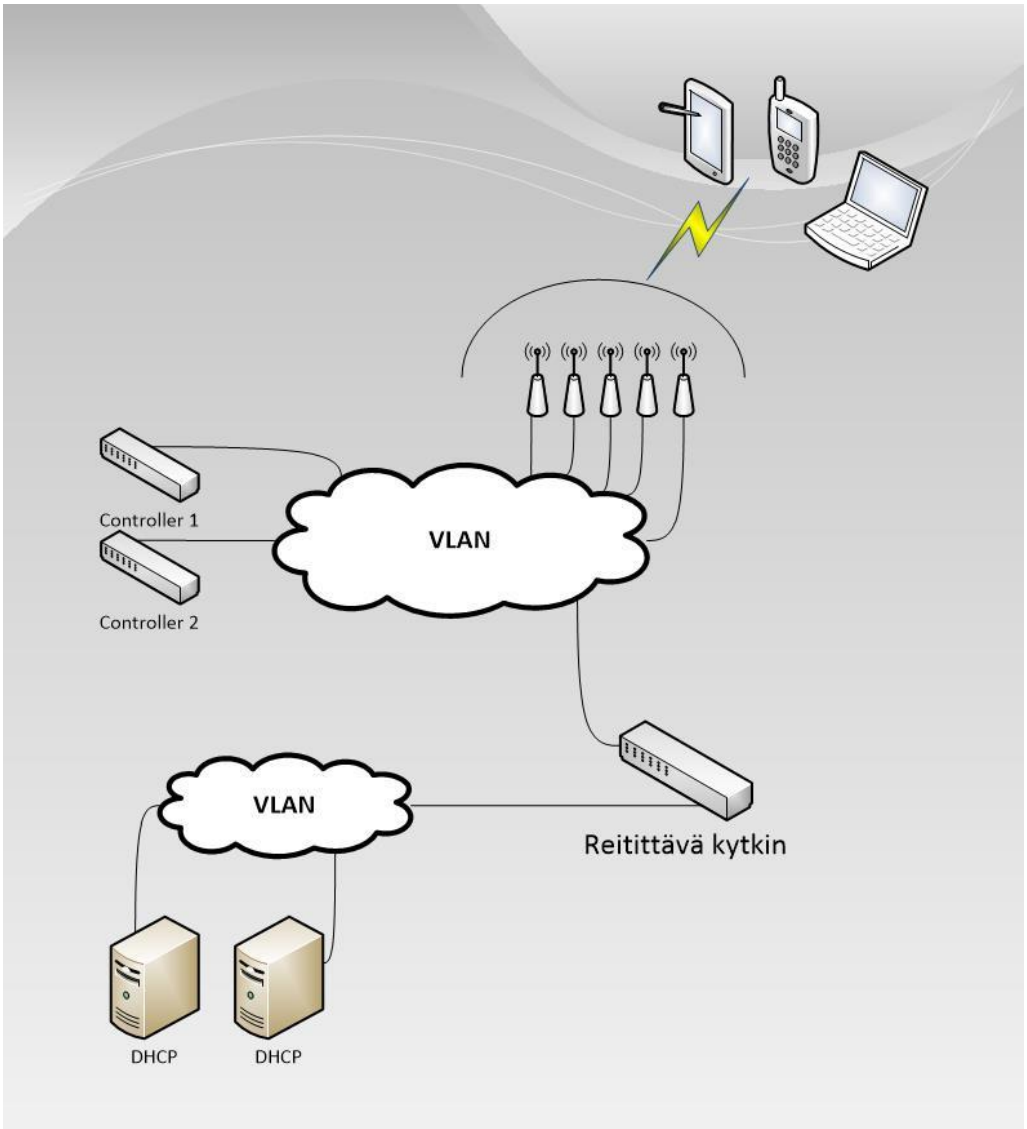
Langattoman lähiverkon uudistaminen pohjautuu uusien laitteiden hankinnalle, niin että uudet laitteet korvaavat vanhemmat. Näin saavutetaan nykyaikaisempi tekniikka. Samalla laitteita lisätään ja pyritään tarjoamaan yhä kattavampi langaton lähiverkko.

4.2.1 Suunnitelma

Uuteen langattomaan lähiverkkoon ei tehdä isoja muutoksia työntekijä- ja asiakastarjontaan, vaan pysytään pieniä muutoksia lukuun ottamatta vanhan verkon tarjonnassa. Työntekijöille ja asiakkaille tarjotaan edelleen viisi eri langatonta lähiverkkoa. Verkkoja on tarjolla hallinnolle, terveydenhuollolle, kouluille, koulujen vierailijoille ja muille vierailijoille. Verkkojen jakaminen tapahtuu VLAN (Virtual Local Area Network) -tekniikalla. VLAN:n tarkoituksena on saada yhden kytkimen toiminto vastaamaan

useamman kytkimen tarjontaa. Tällöin verkkolaitteita ei tarvita niin paljoa. Lisäksi VLAN:n kautta voidaan hallita verkkoa helpommin. VLAN toimii siten, että se asetetaan kytkimen porttiasetuksissa tiettyyn porttiin, joihin kytkettävä laite kytketään.

Verkkojen ja tukiasemien hallinta tapahtuu uuden kontrollerin kautta. Toinen kontrolleri toimii varalaitteena. Kontrollerilla luodaan verkot ja verkkojen salaukset sekä ohjataan tiettyihin jokaiselle verkolla olevaan omaan VLAN:iin. Niillä määrätään, mikä verkko kuuluu mistäkin tukiasemasta. Kontrollereille ja tukiasemille on oma VLAN, johon langattoman lähiverkon laitteet kuuluvat. Kuviosta 12 nähdään kontrollereiden ja tukiasemien topologia.



KUVIO 12. MSM-topologia

Tukiasemien sijoittelut suunnitellaan eri kohteissa uudelleen ja niillä pyritään mahdollisimman hyvään verkkopeittoon. Kohteissa huomioidaan kuuluvuuden kannalta tärkeimmät kohteet, esimerkkinä kokoustilat.

Vierailijaverkot ovat käytössä siten, että koulujen vierailijaverkkoon pääsevät liittymään oppilaat, joille koulujen henkilöstö voi luoda tunnukset. Verkko on käytössä vain päivällä. Yleinen vierailijaverkko on käytössä ympäri vuorokauden ja siihen tunnuksia luovuttaa tietotekniikkapalvelujen Service desk erillispyynnöstä. IP-osoitteet verkkoihin antaa operaattorin reititin. Muuten ne ovat suojaamattomia. Hallinnon, terveydenhuollon ja koulujen sisäiseen langattomaan verkkoon vaaditaan todennus työasemasta sekä verkkoihin oikeutetut käyttäjätunnukset. Hallinnolla ja kouluilla on omat AD- ja RADIUS-palvelimensa, joissa on kone- ja käyttäjätunnusten määritykset. Nämä verkot käyttävät tiettyä salaustekniikkaa ja kaikki liikenne kulkee palomuurin läpi. IP-osoitteet tulevat erillisiltä DHCP-palvelimilta.

4.2.2 Toteutus

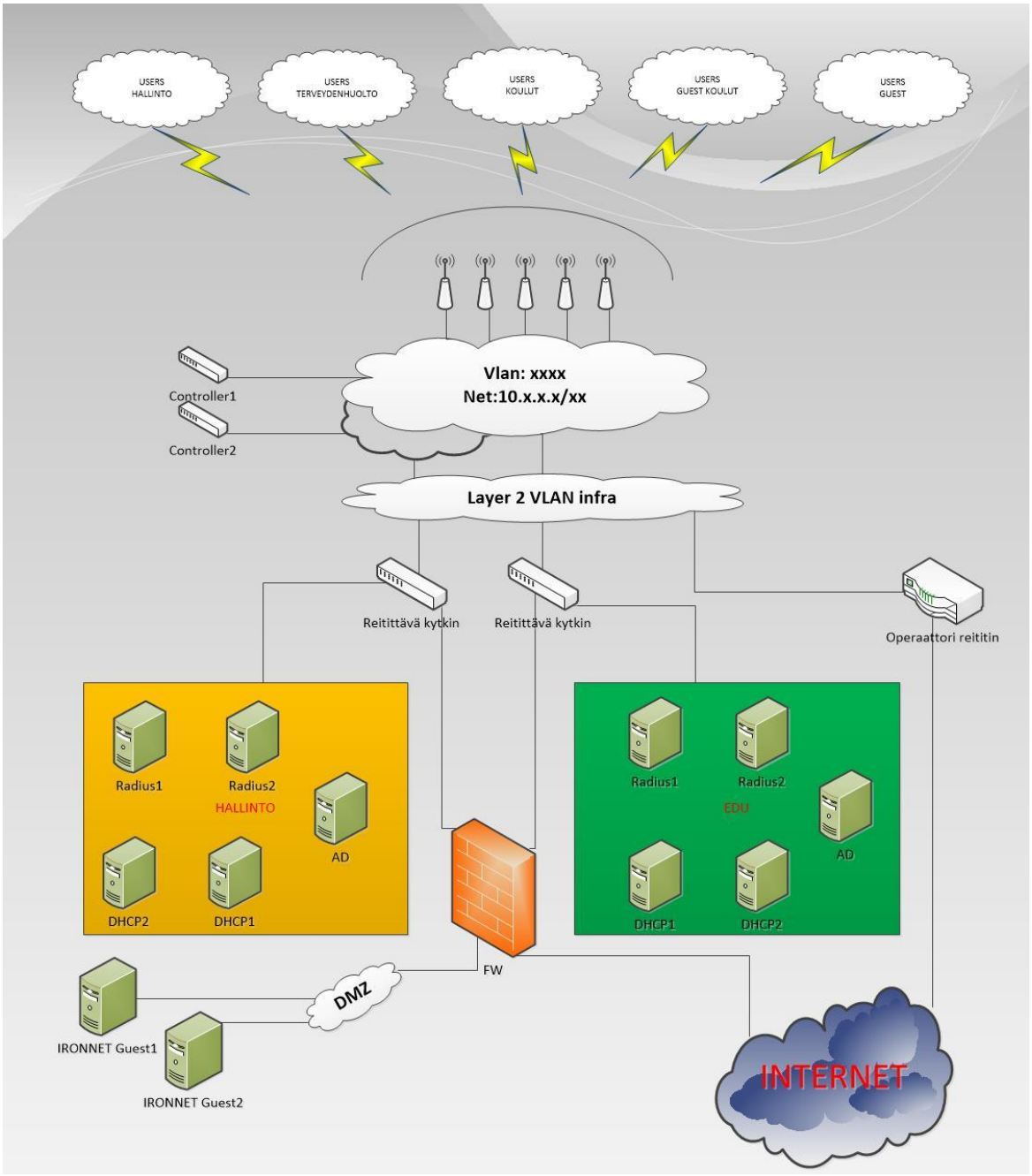
Wlan-verkon toteutuksessa asennettiin alkuun uudet kontrolleri moduulit fyysisesti kytkimiin paikalleen. Kontrollereita ja tukiasemia varten luotiin uusi oma VLAN reitittävälle pääkytkimelle. Kontrolleria käytetään selainpohjaisella käyttöliittymällä. Niiden avulla luotiin verkot, jotka näkyvät kuvion 13 ylälaidassa ja määritettiin jokaiselle verkolle omat VLAN:t, joita käytetään. Langattomat verkot saavat IP-osoitteet näiden VLAN-määritysten mukaan, joilla määritettiin myös käytettävät salaus- ja todennustekniikat.

Langattomia verkkoja on viisi kappaletta. Verkot on suunnattu siten, että tietyille käyttäjäryhmille on omat verkot, jotka ovat hallinnon, terveydenhuollon sekä koulujen käyttäjät, koulujen vierailijat ja muut vierailijat. Hallinnon langaton verkko on suunnattu kunnan työntekijöille, joilla on pääsy Siilinjärven sisäiseen verkkoon. Terveydenhuollon langaton verkko on tarkoitettu kunnan terveydenhuoltohenkilöstölle. Koulujen langaton verkko on koulujen oppilaille ja opettajille sisäiseen verkkoon. Vierailijaverkko on käytössä oppilaiden ja opettajien henkilökohtaisille laitteille. Yleinen vierailijaverkko on käytössä muille kunnan vierailijoille, kuten asiakkaille. Koulujen vierailijaverkko on rajoitettu siten, että se on käytössä vain päivällä.

Jokaisella verkolla on oma VLAN, jonka mukaan DHCP jakaa verkkoon liittyvälle laitteelle IP-osoitteen. Hallinnon ja terveydenhuollon verkot hakevat osoitteet hallinnon DHCP palvelimilta. Koulujen langaton verkko hakee osoitteet omalta DHCP-palvelimeltaan. Vierailijaverkkojen osoite tulee suoraan operaattorilta.

Hallinnon ja terveydenhuollon verkot vaativat, että käytettävä laite kuuluu Siilinjärven kunnan hallinnon toimialueeseen ja käyttäjällä on oltava tunnukset kirjautuakseen koneelle. Jotta voidaan liittyä näihin langattomiin verkkoihin, on laite ja käyttäjätunnus määriteltävä RADIUS-palvelimella, jonka kautta todennetaan oikeus käyttää verkkoa. Autentikointi käyttää 802.1x-todennustekniikkaa. Koulujen sisäiseen verkkoon liityttäessä käytetään muuten samaa tekniikkaa, mutta koulujen verkkoon on oma AD-, DHCP- ja RADIUS-palvelimensa. Näissä verkoissa salauksena käytetään wpa-salausta. Vierailijaverkot ovat avoimia verkkoja joihin kuka tahansa pystyy liittymään. Internetin käyttäminen vaatii kuitenkin tunnukset vierailijaverkkoon, joka todennetaan IRONnet-palvelimen kautta. Web-liikenne avataan, kun tunnukset syötetään selaimelle avautuvaan tunnistukseen. Tunnukset eivät ole sidottuja tiettyyn laitteeseen vaan niitä voidaan käyttää useamman laitteen kautta.

Tukiasemat sijoitetaan rakennuksissa seinille ja laitteet liittyvät aina lähimpään tukiasemaan liittyäkseen verkkoon. Tukiasemat kuuluvat samaan VLAN:n kuin kontrollerit. Tukiasemille määritetään, mikä verkko kuuluu mistäkin tukiasemasta. Ne saavat virtansa PoE:n (Power over Ethernet) kautta ja käyttävät auto-channel-toimintoa, jonka avulla tukiasemat valitsevat itse parhaimman mahdollisen kanavan. Kontrollerilla saman kohteen tukiasemat voidaan sisällyttää ryhmiin, mikä mahdollistaa ryhmiin kuuluvien tukiasemien konfiguroimisen kerralla. Tällä säästetään aikaa, eikä jokaista tukiasemaa tarvitse erikseen konfiguroida.



KUVIO 13. Yleiskuva Wlan-verkosta

4.3 Dokumentointi

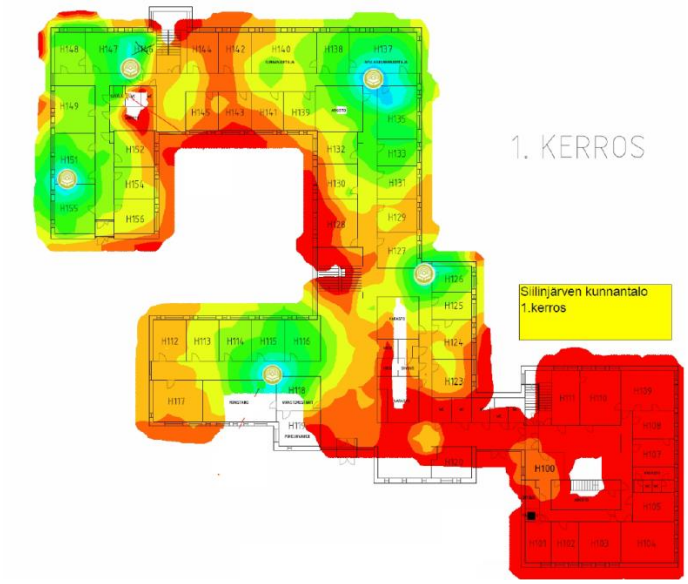
Tehtävänä oli tehdä dokumentoinnit uudesta verkosta. Dokumentointi vaati tutustumisen verkkoon ja sen tekniikkaan. Dokumentointi sisältää seitsemän kuvaa ja dokumentaatio-asiakirjat. Verkkokuvat sisältävät kuvat viidestä eri verkosta, MSM-topologia kuvan (kuvio 12) ja yleiskuvan verkosta (kuvio 13) Kuvat sisältävät yksityiskohtaiset tiedot langattomista verkoista. Kuviin kirjattiin verkkojen SSID:t, VLAN:t, VLAN:n IP-osoitealueet, palvelinten nimet ja osoitteet. Asiakirjoihin on vaihe vaiheelta

kerrottu verkon toiminta. Lisäksi dokumentoitiin todennus- ja salaustekniikat. Salassapidon vuoksi en voi enempää kertoa dokumentointisisältöä ja työssä näkyvät kuvat ovat tiedoiltaan karsittuja kuvia. Dokumentoinnin on tarkoitus toimia tiedon säilytyksenä uudesta verkosta. Dokumentointi on hyödyllinen kun langatonta verkkoa kehitetään tai uudistetaan seuraavan kerran. Henkilöstön vaihtuessa dokumentaatio antaa nopean tavan päästä selville langattomasta lähiverkosta kunnassa. Verkkokuvat piirrettiin Microsoft Visio 2010 – ohjelmalla.

4.4 Tukiasemien käyttöönoton suunnittelu

Tehtävänä oli myös suunnitella tukiasemien sijainnit Siilinjärven kunnantalolle. Suunnittelun pohjalle suoritettiin mittaus olemassa olevasta wlan-verkosta. Tämä toimi pohjana sille, kuinka lähdettäisiin uusia tukiasemia sijoittamaan.

Tukiasemien sijoittelun suunnittelun tueksi mitattiin Tamograph side survey – ohjelmalla olemassa olevan verkon kuuluvuus kunnantalolla. Tamograph side survey -ohjelma mittaa kuuluvuuden alueella, joka sille määritetään. Ohjelmaan syötettiin pohjakuva kunnantalosta ja ohjelman ajoa suoritettaessa käveltiin läpi alue, josta kuuluvuus mitattiin. Kuviossa 14 nähdään 1. kerroksen kuuluvuus. Mittaukset toteutettiin kaikille kerroksille kunnantalolla. 1. kerroksen lisäksi ainoastaan toisen kerroksen yhdessä siivekkeessä oli kaksi tukiasemaa.



KUVIO 14. 1. kerros wlan kuuluvuus

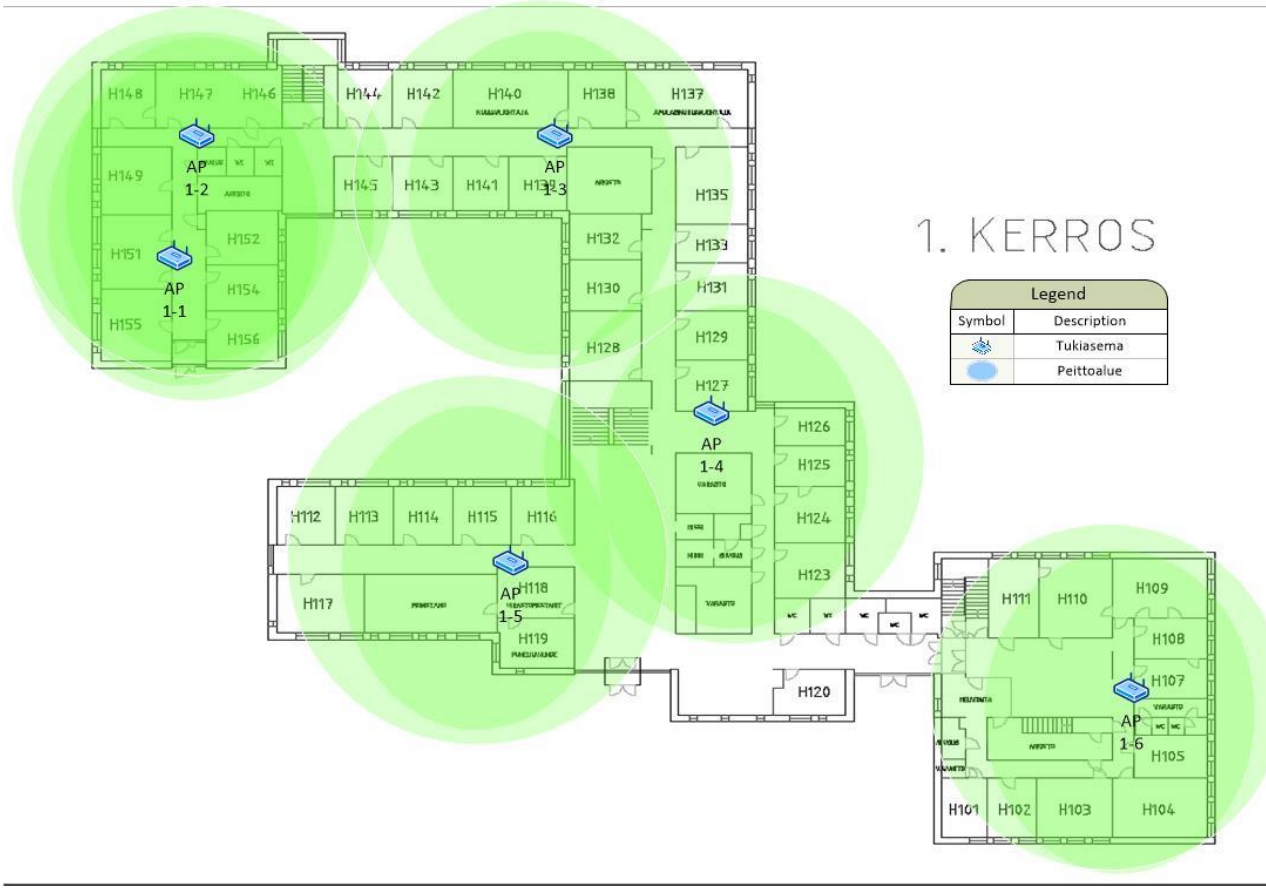
Kunnantalolle oli varattu 15 tukiasemaa verkkoa varten. Kunnantalo on sen verran iso, ettei tällä määrällä tukiasemia saada kokonaan taloa verkon peittoon. Tiettyjä kohteita priorisoitiin rajallisen tukiasema määrän vuoksi.

Pohjakerroksessa sijoitettaisiin yksi tukiasema atk-luokkaan, yksi kattamaan yhdellä käytävällä olevia työhuoneita sekä yksi erilliseen siivekkeeseen.

1. kerros oli yksi tärkeimmistä kohteista. Kerrokseen sijoitettaisiin 6 tukiasemaa. Tärkeimmät kohteet ovat tietotekniikkapalvelujen tilat ja kokoushuone yhdellä käytävällä. Tietotekniikkapalvelujen tilat sisältävät suuremman määrän langatonta verkkoa käyttäviä laitteita, joten sinne huomioitiin kaksi tukiasemaa tuomaan lisää kaistan leveyttä. Muuten kerroksessa olevat käytävät pyrittiin peittämään yhdellä tukiasemalla käytävää kohden.

2. kerroksessa lähdettiin tukiasemien sijoitteleminen samalla periaatteella kuin 1. kerroksessa. Yksi käytäväosuus katettaisiin yhdellä tukiasemalla. Kerroksessa sijaitsi kunnantalon kokoushuoneet yhdessä siivekkeessä, jonne mahdollisesti sijoitettaisiin kaksi tukiasemaa, jotta kaistan leveys on riittävä, kun kokouksia pidetään ja useampia laitteita on liittynyt langattomaan verkkoon. Kokonaisuudessa 2. kerrokseen sijoitettaisiin viisi tukiasemaa

3. kerros oli vähiten tärkein kohde, sillä siellä sijaitsee ainoastaan yksi kokoushuone ja ruokala. Kerrokseen sijoitetaan aivan kokoushuoneen viereen tukiasema, josta on vapaa tila ruokalaan päin. Näin myös ruokalaan saadaan jonkinlainen kuuluvuus langattomalle verkolle. Kuviossa 15 nähdään 1. kerroksen suunnitelma tukiasemien sijoittelusta.



KUVIO 15. 1. kerros tukiasemien suunnitelma

5 YHTEENVETO

Langattomat verkkotekniikat on viime vuosina kehittynyt merkittävästi. Kehitys on tapahtunut verkkostandardeissa, laitteissa ja käytettävyydessä. Nykypäivänä laitteiden liikuteltavuus on myös parantunut. Liikuteltavuus antaa langottomille laitteille käytännöllisyyttä. Langattomat verkot ovat helposti asennettavissa ja hallittavissa. Käyttöönotto on helppoa ja asetusten asettaminen helpottunut huomattavasti esimerkiksi kontrollereiden käyttöliittymillä. Suojausten helpot asettamiset ovat myös tärkeätä verkkojen menestykselle. Edelleen kuitenkin langattomissa verkoissa on heikkouksia ja tietoturvapuutteita, minkä vuoksi langattomat verkot eivät aina ole paras ratkaisu kodin ja yrityksien verkkoratkaisuiksi. Langaton verkko toimii kuitenkin hyvänä tukena langalliselle verkolle.

Tulevaisuus näyttää langattomien verkkojen kannalta lupaavalta. Tekniikoiden vielä kehittyessä päästään yhä parempiin häiriönsietokykyihin ja tiedonsiirtonopeuksiin. Tulevaisuudessa voi kehitys jopa johtaa täysin langattomiin tiedonsiirtoihin. Tällöin säästettäisiin kaapeliratkaisuissa ja langaton ratkaisu vaikuttaisi esimerkiksi rakennusten rakentamiseen.

Matkapuhelimet, kodinkoneet sekä erilaiset muut laitteet kykenevät kommunikoimaan langattomien verkkojen kautta. Niiden hallinta onnistuu jo osittain langatonta verkkoa hyödyntäen.

Työtä varten opiskelin langattomien verkkojen teoriaa, mikä auttoi niiden ymmärtämisessä. Opiskelun pohjalta pystyin tekemään dokumentoinnin langattomasta verkosta. Lähdekirjallisuus sekä Internet tarjosivat tietoa teorioista. Osaksi jouduin myös käyttämään englanninkielistä materiaalia. Siilinjärven kunta siirtyy uudistettuun verkkoon vuoden 2013 aikana.

Työn tekeminen onnistui hyvin. Uudet laitteet olivat toimivia ja asetukset onnistuivat helposti käyttöliittymän avulla. Käyttöönotto tapahtuu uudistetulla verkolla vasta vuoden 2013 aikana eikä tarkempaa ajankohtaa määritelty, joten työssä ei tapahtunut viivästymisiä. Aivan uusimpia tekniikoita ei voida vielä ottaa käyttöön, koska kunnassa on käytössä vanhoja laitteita, jotka eivät tue näitä. Laitteiden uusiutuessa uusiutuu näin ollen myös tekniikka vaiheittain. Laitteet, joilla wlan-verkko tuotetaan, tukevat

kuitenkin nyt uusimpia tekniikoita. Siirtyminen näin ollen on porrastettu useammalle vuodelle.

Alkukäsitykseni langattomista verkoista oli, että verkot toimivat kuin kotiympäristössä. Jälkeenpäin huomasin, että kyse on kuitenkin paljon isommasta verkosta sekä eri toteutuksesta. Kyseessä ei ollutkaan pieni yritysverkko vaan langaton verkko, jota tarjotaan monelle eri taholle. Samalla pääsin tutustumaan tarkemmin kontrollereilla toteutettuun langattomaan verkkoon ja hallintaan sekä, siihen kuinka langattomien verkkojen suojaukset ja tietoturva toteutetaan sisäisessä verkossa. Lopuksi verkon toteutus oli aika yksinkertainen ja helppoa, suuremmilta ongelmilta vältyttiin.

Haasteen työhön toi se, että vanhasta verkosta ei ollut aikaisempaa dokumentaatiota. Kaikki jouduttiin tutkimaan ja suunnittelemaan uudestaan. Tietoturvan merkitys on tärkeää, kun verkkoa luodaan esimerkiksi terveydenhuoltoon, jossa on erittäin arkaluontoista tietoa. On myös tärkeätä suunnitella tukiasemien sijoittamista, jotta oikeanlainen kuuluvuus saadaan oikeisiin paikkoihin, katvealueita ei saisi syntyä. Langaton verkko on hyödyllinen silloin, kun laitteita on liikuteltavana. Langallinen verkko on kuitenkin tällä hetkellä turvallisempi ja vakaampi.

LÄHTEET

Airaksinen, P. & Niemelä, T. 2006 WLAN- Turvallisuus. [verkkodokumentti]. [Viitattu 14.12.2012]. Osoitteessa: http://www2.it.lut.fi/kurssit/06-07/Ti5316800/tyot/WLAN-turvallisuus_Petri_Airakisnen_Teemu_Niemela_dokumentti_v2.pdf

Verkkokauppa.com tuoteluettelo. Asus PCE-N15 Wireless N PCIe -langaton verkkosovitin. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://www.verkkokauppa.com/fi/product/50679/dckrd/Asus-PCE-N15-Wireless-N-PCIe-langaton-verkkosovitin

Hubbert, B. 2010 Freakquency RTS/CTS. [verkkodokumentti]. [Viitattu 8.12.2012]. Osoitteessa: http://freakquency.hubbert.org/2010/12/rtscts-and-you.html

Cisco.com. Cisco Wireless Lan Controller Modules. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps6730/product_data_sheet0900aecd80364432.html

Geier, J. 2005. Langattomat verkot - perusteet. PL 700: Edita Publishing Oy.

Granlund, K. 2001. Langaton tiedonsiirto 1. painos Jyväskylä. Docendo Finland Oy.

Granlund, K. 2007. Tietoliikenne 1. painos Jyväskylä. Docendo Finland Oy

HP.com. HP MSM430 Dual Radio 802.11n Access Point. [verkkokuva] [Viitattu 8.12.2012] Osoitteessa: http://h30094.www3.hp.com/product.aspx?sku=10302420

HP.com. HP MSM765 Mobility Controller. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://h10010.www1.hp.com/wwpc/uk/en/sm/WF06b/12883-12883-1137927-4172286-4172286-3963981-3963980.html?dnr=1

Joensuu, T. 2006 Langattomien verkkojen tarjoamat todentamis/tunnistus-palvelut. Erikoistyö. [verkkodokumentti]. [Viitattu 21.12.2013]. Osoitteessa: *research.jyu.fi/laila/erkka_**joensuu**.doc*

Juutilainen M. Siirtyvä tietoliikenne: Radiotekniikan perusteet. [luentokalvot]. [Viitattu 8.12.2012]. Osoitteessa: http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento03.pdf

Juutilainen, M. Siirtvvä tietoliikenne: Langaton lähiverkko. [luentokalvot]. [Viitattu 8.12.2012]. Osoitteessa: http://www2.it.lut.fi/kurssit/03-04/010651000/luennot/wlan.pdf

Lal Chand Godara, 2002 Handbook of antennas in wireless communications. Boca Raton: CRC Press.

Tietokone.fi. Modattava Wlan tukiasema. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://www.tietokone.fi/lehti/tietokone_9_2009/modattava_wlan_tukiasema_7921

Krimaka.net. OSI ja TCP/IP malli. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://www.krimaka.net/tietotekniikka/verkko-ja-ethernet/osi-ja-tcp-ip-mallit.html

Puska, M. 2000. Lähiverkkojen tekniikka – Pro Training. Helsinki: Talentum.

Puska, M. 2005. Langattomat lähiverkot. Helsinki: Talentum.

Seppänen, K. 2006. Turvallinen kirjautuminen yrityksen WLAN-verkkoon RADIUS-tunnistuksen avulla. [opinnäytetyö]. [Viitattu 22.12.2012]. Osoitteessa: http://publications.theseus.fi/bitstream/handle/10024/11895/2007-04-27-12.pdf?sequence=1

Siptune, ympärisäteilevä antenni. [verkkokuva]. [Viitattu 8.12.2012]. Osoitteessa: http://www.siptune.com/siptune.com/index.php?main_page=index&cPath=38_40

Thomas, 2005. Verkkojen tietoturva. Helsinki. Edita Publishing Oy.