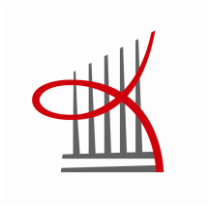


SÄRKÄNNIEMEN WLAN-VERKON KEHITTÄMINEN

Leevi Leppälä

Opinnäytetyö
Toukokuu 2014
Tietojenkäsittelyn ko.
Tietoverkkopalvelut

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelujen suuntautumisvaihtoehto

LEPPÄLÄ, LEEVI:
Särkänniemen WLAN-verkon kehittäminen

Opinnäytetyö 42 sivua, joista liitteitä 2 sivua
Toukokuu 2014

Opinnäytetyön tavoitteena oli kehittää Tampereen Särkänniemi Oy:n huvipuiston tarjoamaa langatonta verkkoa, joka aiemmin oli pelkästään yrityksen sisäisessä käytössä. Työn tarkoituksena oli laajentaa verkkoa uusilla langattomilla tukiasemilla kattamaan koko huvipuiston alue ja avata verkko asiakkaiden käyttöön. Työssä käytettiin perustana toimeksiantajan olemassaolevaa verkkoa, jota laajennettiin tarpeiden mukaan.

Työssä tarkastellaan langattomien lähiverkkojen teoriaa niin radiotekniikan, standardien, laitteiden kuin tietoturvankin osalta. Tapaustutkimuksessa käsitellään Tampereen Särkänniemi Oy:n aiempaa verkkoinfrastruktuuria, toimeksiantajalle myös suunnitellaan ja toteutetaan avoin WLAN-verkko sekä tutkitaan valmiin verkon suorituskykyä.

Lopputuloksena syntyi puiston tärkeimmät alueet kattava WLAN-verkko, jonka avulla asiakkaat voivat muodostaa Internet-yhteyden omilla päätelaitteillaan 802.11-protokollia käyttäen. Puistoon jäi kuitenkin työn jälkeen myös katvealueita, joita on myöhemmin helppo täydentää uusilla tukiasemilla. Myös lisäominaisuuksia, kuten yksittäisen käyttäjän kaistanleveyden hallinta, voidaan ottaa myöhemmin käyttöön.

Tietoturvasyistä työssä ei esitellä yksittäisten aktiivilaitteiden tarkempia konfiguraatiotietoja tai todellisia IP-osoiteavaruuksia.

Asiasanat: langaton lähiverkko, WLAN, Wi-Fi, 802.11

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Network Services

LEPPÄLÄ, LEEVI:
Developing Särkänniemi WLAN

Bachelor's thesis 42 pages, appendices 2 pages
May 2014

The objective of this thesis was to develop the wireless network offered by amusement park Tampereen Särkänniemi Oy. The network has previously been accessible only for the park personnel. The purpose of the thesis was to expand the network with new wireless access points to cover most of the amusement park grounds and to open the network for visitors. The existing infrastructure was exploited with necessary improvements.

In the report following topics are discussed: data transmission over radio frequencies, standards regarding WLAN technology, devices used in wireless networks and security. As this was a case study, the existing network infrastructure in Särkänniemi amusement park was studied and an open wireless network for visitors was designed, implemented and benchmarked.

As a result, an open WLAN covering all the essential areas of the park was completed. Visitors may access the Internet using their own 802.11-compatible devices over the network. The coverage is not perfect throughout the park, but additional access points are easy to install later to further improve the network. Additional features may also be later implemented, like managing the bandwidth of a single user.

For security reasons no detailed configuration settings of network devices are discussed in the thesis, nor are the real IP addressing schemes displayed.

Key words: wireless local area network, WLAN, Wi-Fi, 802.11

SISÄLLYS

LYHENTEET JA TERMIT

DHCP	Dynamic Host Configuration Protocol, protokolla laitteiden automaattista verkkoasetusten konfigurointia varten
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö, johtava standardien määrittelijä IT-alalla
IDS	Intrusion Detection System, tunkeilijan havaitsemisjärjestelmä
IP	Internet Protocol
ISP	Internet Service Provider, palveluntarjoaja
LAN	Local Area Network, lähiverkko
NAT	Network Address Translation, osoitteenmuunnostekniikka
OFDM	Orthogonal Frequency Division Multiplexing, eräs modulaatiotekniikka
OSI-malli	Open Systems Interconnection Reference Model, kuvaa tiedonsiirtoprotokollien suhteita kerroksittain
PAT	Port and Address Translation, osoitteenmuunnostekniikka
QoS	Quality of Service, käytetään erilaisen liikenteen priorisoinnin yhteydessä
RADIUS	Remote Authentication Dial In User Service, eräs käyttäjäntodennusprotokolla
SSH	Secure Shell, salattu etäyhteysprotokolla
SSID	Service Set Identifier, yhteyspisteen nimi kuvataan SSID:llä
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko. Käytetään liikenteen erotteluun loogisella tasolla
VSC	Virtual Service Community, Hewlett-Packardin oma termi langattoman verkon asetuskokonaisuudelle
WAN	Wide Area Network, laajan alueen verkko
WEP	Wired Equivalent Privacy, liikenteen salaustekniikka
Wi-Fi	synonyymi WLANille, Wi-Fi Alliancen hallitsema tavaramerkki ja sertifikaatti
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA/WPA2	Wi-Fi Protected Access, liikenteen salaustekniikka

1 JOHDANTO

Tilastokeskuksen (Tilastokeskus, Tieto- ja viestintätekniikan käyttö -tutkimus 2011) mukaan 42 prosentilla suomalaisista oli älypuhelin vuonna 2011 ja niiden määrä tuskin on viime vuosina ainakaan laskenut. Lisäksi erilaiset tabletit ja muut älylaitteet ovat yleistyneet räjähdysmäisesti. Tyypillisesti nämä mobiililaitteet pystyvät hyödyntämään matkapuhelinverkkojen lisäksi tai niiden sijaan langattomia lähiverkkoja 802.11-protokollien avulla.

Opinnäytetyöni toimeksiantaja Tampereen Särkänniemi Oy ylläpitää Suomen toiseksi suurinta huvipuistoa. Seurauksena puiston alueelle pakkautuu tiiviisti tuhansia asiakkaita kesäpäivisin. Eri operaattoreiden matkapuhelinverkkojen tiedonsiirto-kapasiteetti alueella ei riitä loputtomiin, vaan ruuhkaisina päivinä datayhteydet asiakkaiden mobiililaitteisiin saattavat hidastua paikallisesti paljonkin. Erityisesti ongelmia voisi tulla kesäkaudella 2014, kun Elämyspuiston pakollinen sisäänpääsy-maksu poistetaan (Tampereen Särkänniemi Oy 2014). Tämä saattaa lisätä alueella liik-kuvien ihmisten määrää huomattavasti.

Ongelman minimoimiseksi on yrityksessä päätetty rakentaa avoin langaton internetyhteys asiakkaiden käyttöön WLAN-tekniikan avulla aiemman, vain yrityksen sisäisessä käytössä olleen, verkon rinnalle. Opinnäytetyöni tavoite on kehittää tuota Tampereen Särkänniemi Oy:n tarjoamaa langatonta verkkoa. Työn tarkoituksena on laajentaa verkkoa uusilla tukiasemilla kattamaan lähes koko huvipuiston alue ja avata verkko suojaamattomana asiakkaiden käyttöön.

Tietoturvasyistä työssä ei esitellä yksittäisten aktiivilaitteiden tarkempia konfiguraatiotietoja tai todellisia verkon IP-osoiteavaruuksia. Esimerkissä on käytetty osoiteavaruutta 172.16.0.0 aliverkon maskilla 255.255.248.0.

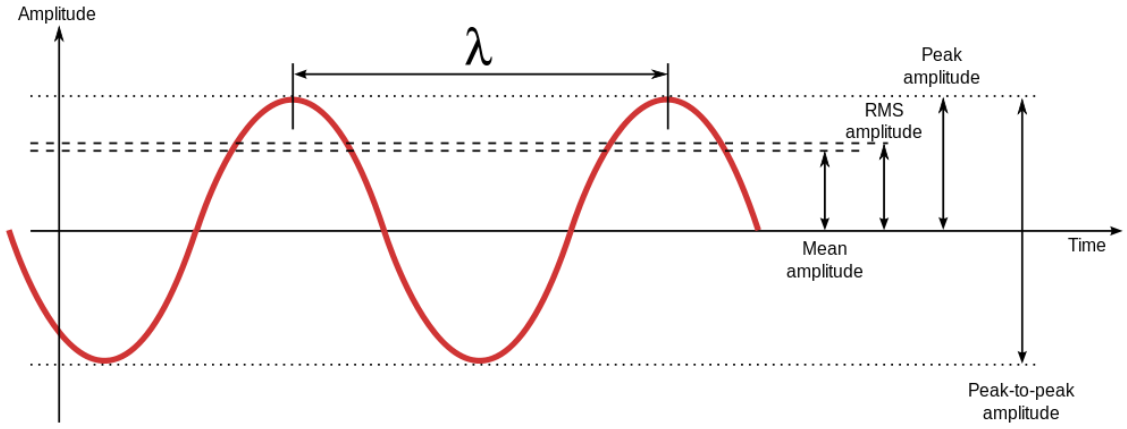
2 LANGATTOMAN LÄHIVERKON TEORIAA

2.1 Tiedonsiirto radioteitse

Langaton tiedonsiirto perustuu sähkömagneettiseen aaltoliikkeeseen. Tietoa siirretään käytännön toteutuksissa joko infrapuna- tai radiotaajuuksilla. Koska käytännön sovelluksissa langattomat lähiverkot toteutetaan aina radiotaajuuksilla, ei tässä työssä käsitellä tiedonsiirtoa infrapunasäteilyn avulla. Merkille pantavaa on kuitenkin, että alkuperäisessä 802.11-standardissa on määritelty tiedonsiirto myös infrapuna-taajuuksilla, joskaan tätä tukevia laitteita ei ole koskaan ollut markkinoilla. (Geier 2005.)

2.1.1 Sähkömagneettinen aaltoliike

Eräitä radioaallon perusominaisuuksia ovat amplitudi (värähdyslaajuus), taajuus ja vaihe. Amplitudi (kuvassa 1 ”Peak amplitude”) kuvaa signaalin voimakkuutta, aaltoliikkeen suurinta poikkeamaa. Signaalin sanotaan heikkenevän, kun sen amplitudi vähenee. Taajuus puolestaan kertoo, montako kertaa signaali värähtelee aikayksikössä. Signaalin heikkeneminen tietyllä matkalla riippuu värähtelytaajuudesta: mitä korkeampi taajuus, sitä enemmän signaali heikkenee. Vaihe taas kuvaa signaalin poikkeamaa viitepisteestä. Vaiheensiirto ilmoitetaan asteina tai radiaaneina, koska yksittäinen signaalin värähdys tekee täyden 360° kierroksen. (Geier 2005.)

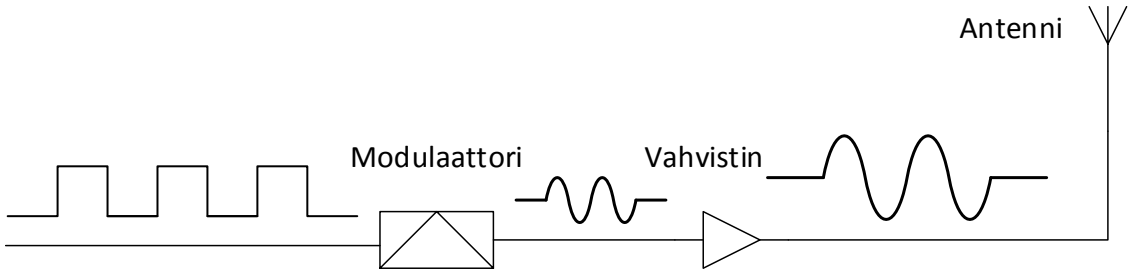


KUVA 1. Sähkömagneettinen aalto (http://fi.wikipedia.org/wiki/Amplitudi)

2.1.2 Digitaalinen signaali analogiseksi: modulaatio

Digitaalinen tieto esitetään binäärimuodossa ja tiedon mittana käytetään bittiä. Bitti voi olla arvoltaan joko 0 tai 1 ja kaikki tieto pystytään esittämään bittien jonoina. Sähkömagneettisessa aaltoliikkeessä bitin arvo voidaan esittää monella eri tavalla, esimerkiksi amplitudin, taajuuden tai vaiheen muutoksena tai näiden kaikkien yhdistelmänä. (Geier 2005.)

Jotta digitaalinen signaali voitaisiin lähettää langattomasti radiotaajuuksilla, se pitää ensin muuntaa analogiseksi signaaliksi, joka sitten antennilla muutetaan langattomaksi sähkömagneettiseksi säteilyksi (kuva 2). Tätä säteilyä kutsutaan kantoaalloksi, koska tieto kulkee kantoaallon ”päällä”. Modulaatioksi kutsutaan sitä prosessia, jossa kantoaaltoa muokataan sopivaksi edustamaan sen välitettäväksi annettavia bittejä (Geier 2005). Nykyiset modulaatiotekniikat yhdistelevät kolmea perusmodulaatiota, jotka perustuvat signaalin taajuuden, vaiheen ja amplitudin muutokseen.



KUVA 2. Digitaalinen signaali moduloidaan, muunnetaan analogiseksi ja vahvistetaan ennen langatonta lähetystä

Vaihtotaajuusavainnus (frequency shift-keying, FSK) muuttaa lähetettävän kantoaallon taajuutta niin, että muutos edustaa joko nollaa tai ykköstä. Positiivinen taajuussiirtymä tarkoittaa kantoaallon siirtymää hiukan korkeammalle taajuudelle ja tämä siirtymä edustaa loogista ykköstä, negatiivisen taajuussiirtymän edustaessa loogista nollaa. Vastaanottaja havaitsee nämä pienet muutokset kantoaallon taajuudessa ja demoduloi ne, jolloin muodostuu bittijono. (Geier 2005.)

Vaiheavainnus (phase shift-keying, PSK) perustuu radiosignaalin vaihekulman muutokseen. Vaiheavainnuksesta on muutamia erilaisia sovelluksia, jotka voivat käyttää kahta, neljää tai kahdeksaa eri vaihetta tiedon esittämiseen. Esimerkiksi kahden eri vai-

heen eli binäärisessä vaiheavainnuksessa käytetään signaalin vaiheita 0° ja 180° kuvaamaan loogisia arvoja 0 ja 1. Käytettäessä neljää vaihetta voidaan esittää neljää arvoa eli kahta bittiä kerralla ja kahdeksalla vaiheella kahdeksaa arvoa eli kolmea bittiä, näin kasvattaen esitettävän datan määrää eksponentiaalisesti samassa ajassa. Toisaalta pienemmät muutokset kantoaallossa on vaikeampi havaita vastaanottopäässä ja häiriöt vaikuttavat herkemmin monimutkaisempaan signaaliin. (Geier 2005.)

Kvadratuuri-amplitudimodulaatio eli QAM on kehittyneempi modulaatiotekniikka, jossa ei muunnella pelkästään yhtä kantoaallon ominaisuutta. Sekä signaalin amplitudia että vaihetta muunnellaan, jolloin niiden yhdistelmänä pystytään esittämään suurempia bittiryhmiä kerralla. Usein moduloidaan kahta eri vaiheessa olevaa kantoaaltoa, joiden summana saadaan QAM-signaali. Erilaisia vaiheen ja amplitudin yhdistelmiä voi olla vaikkapa 256, joista jokainen edustaa kahdeksaa databittiä ($2^8 = 256$).

OFDM-modulaatio (Orthogonal Frequency-division Multiplexing) käyttää joko vaihtotaajus- tai vaiheavainnusta tai QAM-modulaatiota. Moduloitu signaali jaetaan useille toisiaan häiritsemättömille taajuuskanaville samanaikaisesti, jolloin siirtonopeus moninkertaistuu. Nykyään käytetään OFDM:n jatkokehitelmiä, joiden avulla siirtonopeus voidaan moninkertaistaa käyttämällä useita lähettäviä ja vastaanottavia antenneja verrattuna yhtä antennia käyttävään OFDM:ään (Van Nee 2006).

2.1.3 Signaalin häiriöt, heikkeneminen ja interferenssi

Radioaalloilla tapahtuvassa tiedonsiirrossa esiintyy väistämättä häiriöitä, jotka hidastavat datan läpimenoa. Tyypillisiä ongelmia ovat signaalin vaimeneminen, interferenssi ja heijastuminen. Haittojen minimoimiseksi on tärkeää kyetä tunnistamaan erilaiset häiriöt ja niiden aiheuttajat sekä tuntea menetelmät niiden poistamiseen.

Radiosignaalin **vaimeneminen** tarkoittaa amplitudin pienentymistä. Kun signaali on liian vaimentunut, vastaanottaja ei kykene enää erottelemaan sitä taustakohinasta. Vaimenemiseen vaikuttaa eniten signaalin taajuus ja väliaine, jossa signaali etenee. Mitä korkeampi taajuus, sitä nopeammin signaali vaimenee väliaineessa. Toisaalta korkeataajuuksinen signaali kykenee välittämään enemmän dataa, joten langattomissa tekniі-

koissa tehdään kompromisseja näiden kahden ominaisuuden välillä. Väliaineen merkitys puolestaan on olennainen WLAN-tekniikassa: lähettävien ja vastaanottavien antennien sijoitus paksujen seinien ja muiden heikosti läpäistävien materiaalien taakse heikentää signaalin kuuluvuutta. (Juutilainen 2007.)

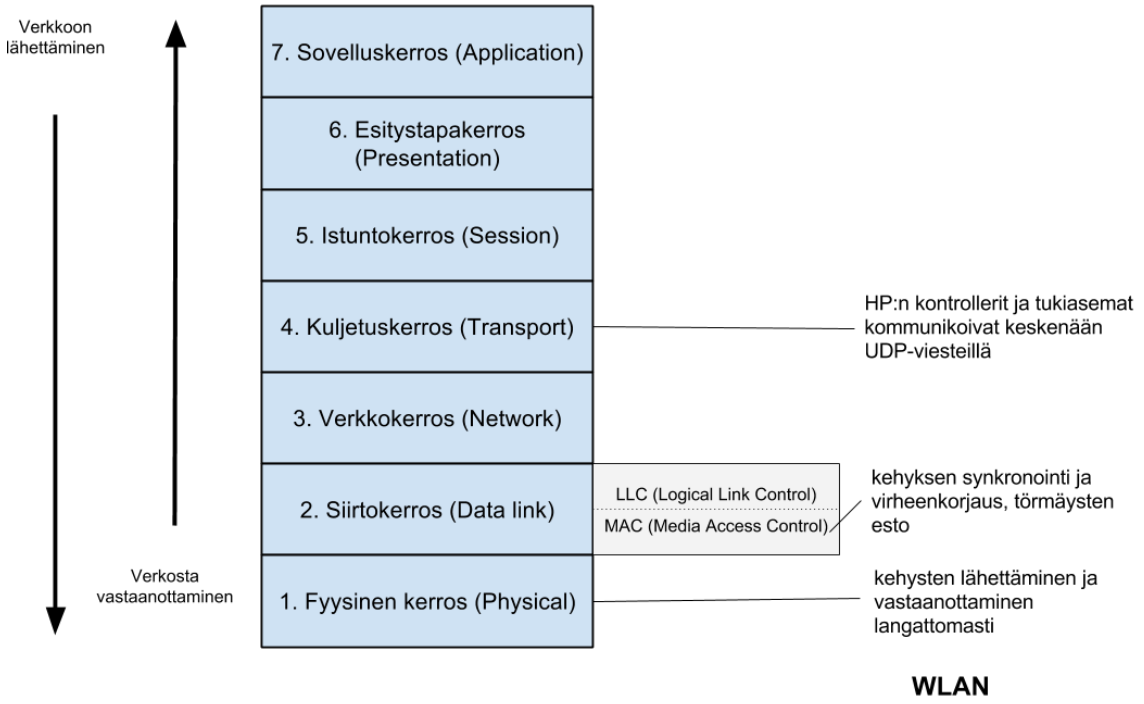
Interferenssi tarkoittaa, että kaksi tai useampia signaaleita, joilla on sama taajuus ja vaihe, saapuvat vastaanottavaan asemaan yhtä aikaa. Tällöin signaalit häiritsevät toisiaan eikä vastaanottaja erota niitä toisistaan. Interferenssin aiheuttaja voi olla esimerkiksi samalla alueella sijaitseva toinen radiojärjestelmä, joka käyttää samaa taajuutta ja modulaatiota. Interferenssin ehkäisemiseksi valtiot valvovat radiotaajuuksia ja niiden käyttö onkin enimmäkseen luvanvaraista. Ongelmia esiintyykin erityisesti lupavapailla taajuuksilla, joilla myös langattomat lähiverkot toimivat. (Geier 2005.)

Signaalin **heijastuminen** tarkoittaa, että osa signaalista kulkee lähettäjältä vastaanottajalle suorinta tietä, kun taas osa heijastuu seinistä ja muista fyysisistä rakenteista. Näin heijastuvat osat kulkevat pidemmän matkan ja viive kasvaa. Vastaanottavan aseman saavuttaa siis sama signaali eri ajanhetkillä, kuitenkin todella lähellä toisiaan. Jos viivettä on liikaa, vastaanottaja tekee virheitä moduloinnissa ja dataa joudutaan lähettämään uudelleen. Tämä hidastaa tiedon läpimenoa. (Geier 2005.)

WLAN-verkoissa on kiinnitettävä huomiota eri taajuuksien ominaisuuksiin. Yleensä käytettävissä ovat taajuuskaistat 2,4 ja 5 GHz alueelta, jotka on vielä jaettu useisiin kanaviin eli kapeisiin taajuusalueisiin. Vierekkäisissä tukiasemissa tulee interferenssin välttämiseksi aina pyrkiä käyttämään kanavia, jotka ovat mahdollisimman kaukana toisistaan. Aina tämä ei ole mahdollista: esimerkiksi kerrostalossa, jossa vierekkäisissä huoneistoissa on WLAN-verkko samalla taajuudella, voi esiintyä interferenssiä eivätkä verkkoja hallinnoivat asukkaat ole välttämättä tietoisia yhteysongelmien aiheuttajasta. Suurissa teollisuuskiinteistöissä, joissa välimatkat ovat pitkiä ja heijastavia pintoja paljon, voi signaalin heijastuminen muodostua todelliseksi ongelmaksi (Geier 2005). Tällöin voidaan laskea tukiasemien lähetystehoa ja lisätä niiden lukumäärää, jolloin heijastuminen vähenee yksittäisen lähettimen ja vastaanottimen välillä ja signaali paranee.

2.2 OSI-malli

OSI-mallia käytetään yleisesti kuvaamaan tiedonsiirtoprotokollia ja niiden suhteita (kuva 3). OSI-mallissa on seitsemän kerrosta, joista ylemmät käyttävät aina alempien kerrosten palveluja omiensa mahdollistamiseksi. Kun tietoa siirretään, se kapseloidaan aina alemman kerroksen protokollien avulla segmentteihin, paketteihin ja kehyksiin ja lopulta fyysisellä kerroksella siirretään sähkövirran, valoimpulssien tai langattomasti sähkömagneettisen säteilyn avulla.



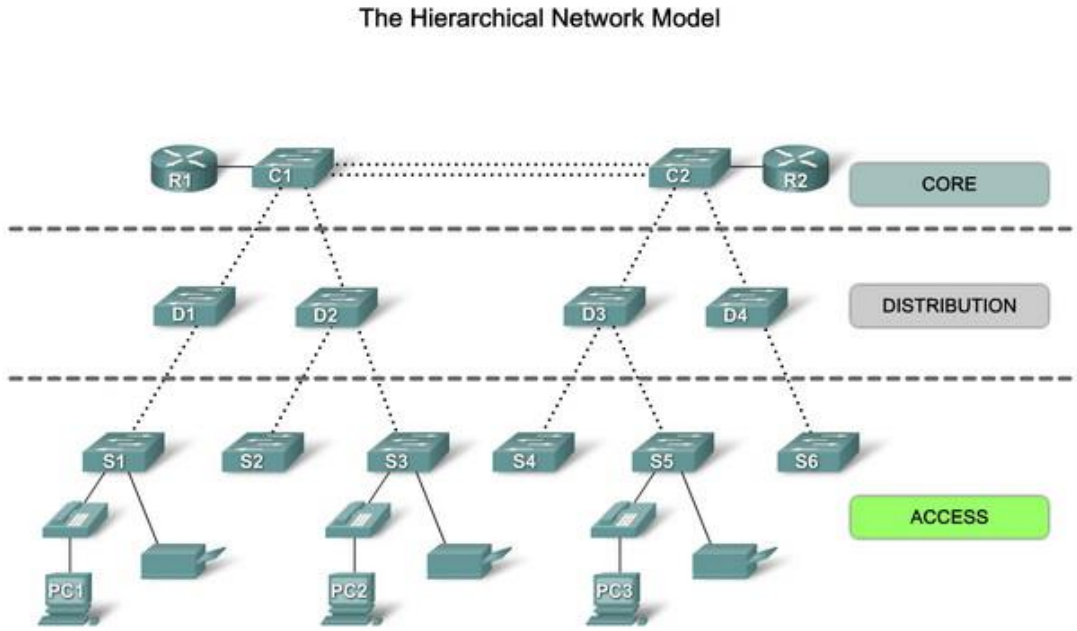
KUVA 3. OSI-malli ja WLAN-tekniikoiden sijainti mallissa

Tässä työssä olennaisimpia ovat OSI-mallin ensimmäinen ja toinen kerros, koska IEEE 802.11-standardit käsittelevät vain niitä. Myös verkko- ja kuljetuskerroksiin otetaan kantaa joissakin yhteyksissä.

2.3 Yleisiä verkon suunnitteluperiaatteita

Lähiverkkojen suunnittelussa kannattaa noudattaa hierarkkisuutta ja modulaarisuutta. Tämä tarkoittaa, että verkkolaitteet on kytketty hierarkkisesti ja eri hierarkiatasoilla on eri tehtävä verkossa. Vikasietoisuutta tulee toteuttaa kahdentamalla laitteita ja niiden välisiä yhteyksiä. Suurille ja keskisuurille verkoille käytetään yleisesti kuvassa 4 esi-

tettyä kolmekerroksista mallia, jota myös suuret laitevalmistajat, kuten Cisco ja Hewlett-Packard, suosittelevat.



KUVA 4. Yleisesti käytetty verkon hierarkkinen suunnittelumalli kolmella tasolla (http://www.ciscopath.com/content/61/hier-network-model)

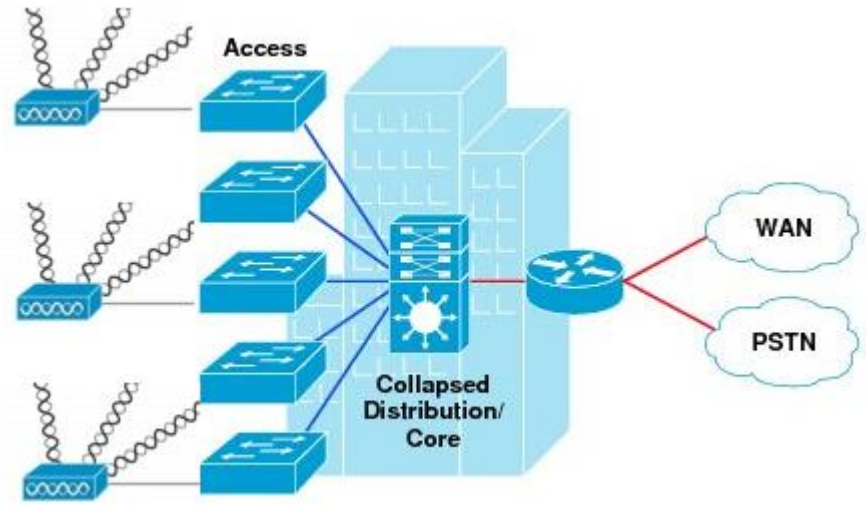
- **Liityntätaso** (Access Layer) sisältää menetelmät, joilla päätelaitteet liittyvät lähiverkkoon. Käytännössä laitteet ovat siis verkkokytkimiä. Myös langattomat tukiasemat liitetään liityntätason kytkimiin. Liityntätasolla alkaa myös liikenteen erottelu virtuaalisiin lähiverkkoihin, VLANeihin (Virtual Local Area Network). Ylläpitäjä määrittää liityntätason kytkinportteihin, mihin virtuaaliseen lähiverkkoon ne kuuluvat. Kytkin lisää päätelaitteelta tuleviin kehyksiin VLAN-tunnuksen, jonka eri tasojen kytkimet tunnistavat ja ohjaavat oikeisiin portteihin. Päätelaitteelle suuntautuvista kehyksistä kytkin taas poistaa VLAN-tunnuksen. Langattomat tukiasemat kykenevät usein myös käsittelemään VLAN-tunnuksia, jolloin tukiaseman kytkinporttiin pitää sallia kaikkia VLANit, joita tukiaseman halutaan tukevan. VLAN-tunnuksia ei tällöin poisteta tukiasemalle menevästä liikenteestä, koska tukiasemat esiintyvät liityntätason laitteina eivätkä päätelaitteina. (Puska 2005.)

- **Jakelutason** (Distribution Layer) laitteet yhdistävät yleensä saman rakennuksen tai muun fyysisen kokonaisuuden liityntäkytkimet. Jakelutason kytkimet on suo-

siteltavaa kahdentaa, jotta yhden kytkimen hajoaminen ei lamaannuttaisi useita siihen kytkettyjä liityntätason kytkimiä. Jakelutasolla toteutetaan myös verkon lisäpalveluja: VLANien välistä reititystä, pääsylistoja, aliverkkojen summausta ja reitityspäivitysten kontrollointia. (Puska 2005.)

- **Ydintaso** (Core Layer) ei sisällä mitään lisäpalveluja, vaan sen ainoa tarkoitus on liittää jakelutason kokonaisuudet toisiinsa mahdollisimman nopeasti ja tehokkaasti. Yrityksen palvelimet kytketään usein suoraan ydintason kytkimiin, jos niiden tarkoitus on palvella koko organisaatiota. Toisaalta paljon liikennettä aiheuttavat palvelimet kannattaa sijoittaa jakelutasolle mahdollisimman lähelle liikenteen aiheuttavaa käyttäjäryhmää, jotta koko yritystä palveleva ydintaso ei kuormittuisi niin paljon. (Puska 2005.)

Pienissä ja keskisuurissa yrityksissä ei usein ole tarkoituksenmukaista rakentaa verkkoa täysin kolmetasoiseksi, vaan jakelu- ja ydintaso voidaan yhdistää (kuva 5). Näin kustannukset ja ylläpidettävien laitteiden lukumäärä pysyy hallinnassa suorituskyvyn kärsimättä. Linkkien kahdentamisesta ja varalaitteista ei kuitenkaan kannata tinkiä, sillä lyhytkin katkos verkon toiminnassa vaikuttaa usein välittömästi yrityksen liiketoimintaan.



KUVA 5. Yhdistetty ydin- ja jakelutaso, liityntätaso ja tukiasemat (Pueblas, Gyurindak, Strika, Kachalia, Hamilton & Tenneti 2010, muokattu)

2.4 IEEE 802.11-standardit

IEEE 802.11 on standardiperhe, joka kuvaa langattoman lähiverkon tiedonsiirron ja radiotekniikat. Standardeissa käsitellään OSI-mallin ensimmäistä ja toista eli fyysistä ja siirtokerrosta. Standardit siis kuvaavat, miten laitteet voivat fyysisellä kerroksella moduloida signaalia ja lähettää sitä radioaalloilla sekä miten siirtokerroksella hallitaan kehysten siirtoa esimerkiksi törmäysteneston ja vuoronvarauksen avulla.

802.11 /a/b/g

Alkuperäinen 802.11-standardi julkaistiin vuonna 1997. 802.11 oli kuitenkin niin väljästi määritelty, että eri valmistajien protokollaa tukevien laitteiden välillä oli vakavia yhteensopivuusongelmia. 802.11 ei yleistynytkään ennen kehittyneempien a- ja b-versioiden julkaisua 1999. Näistä a-versio toimii 2,4 GHz taajusalueella ja b-versio 5 GHz alueella lähes kaksinkertaistaen tiedonsiirtonopeuden mutta toisaalta lyhentäen signaalin kantamaa. Vuonna 2003 standardoitu 802.11g toimii myös 2,4 GHz taajuusalueella ollen näin yhteensopiva 802.11b-laitteiden kanssa. G-version maksimisiirtonopeus on 54 Mb/s.

802.11n

Standardin n-versio julkaistiin 2009. Teoreettinen maksimisiirtonopeus on 600 Mb/s, joka saavutetaan useilla parannuksilla vanhoihin standardeihin. Tärkein niistä on useiden rinnakkaisten lähetysten käyttö eli laitteissa on useampia antenneja (MIMO, Multiple Input Multiple Output). Standardi mahdollistaa jopa neljän antennin käytön. Toinen tärkeä parannus n-versiossa on suurempi lähetyskaistanleveys: 40 MHz levyinen kaista mahdollistaa kaksinkertaisen siirtonopeuden aiempien standardien käyttämään 20 MHz kaistaan nähden. 802.11n voi toimia sekä 2,4 Ghz että 5 Ghz taajuusalueilla ja se onkin taaksepäin yhteensopiva 802.11a/b/g-laitteiden kanssa. (Stanford 2007.)

802.11ac

802.11ac-protokolla moninkertaistaa tiedonsiirtonopeuden n-versioon verrattuna. Käytettävä taajuuskaista on leveämpi: jopa 160MHz kaista on mahdollinen. Lisäksi rinnakkaisia lähetyksiä voi olla maksimissaan kahdeksan. OFDM-modulaatiota on paranneltu uudella MU-MIMO-OFDM-tekniikalla (Multi-User-Multiple Input Multiple Output). Näiden ja muiden parannusten ansiosta 5 GHz taajuusalueella toimiva ac-protokolla kykenee teoriassa jopa 7 Gb/s siirtonopeuteen. Täyttä nopeutta ei kuitenkaan saavuteta missään käytännön sovelluksissa. (Anthony 2013.)

802.11ad

802.11ad toimii täysin uudella taajuusalueella verrattuna aiempiin 802.11-protokolliin. 60 GHz taajuusalue tarkoittaa lyhyempää kuuluvuusaluetta, mutta merkittävästi suurempaa tiedonsiirtonopeutta tukiaseman lähellä. Protokolla on kuitenkin yhteensopiva aiempien standardien kanssa, eli se tukee ainakin kolmea eri taajuusaluetta (2,4 GHz, 5 GHz, 60 GHz) (Ruetsch 2013).

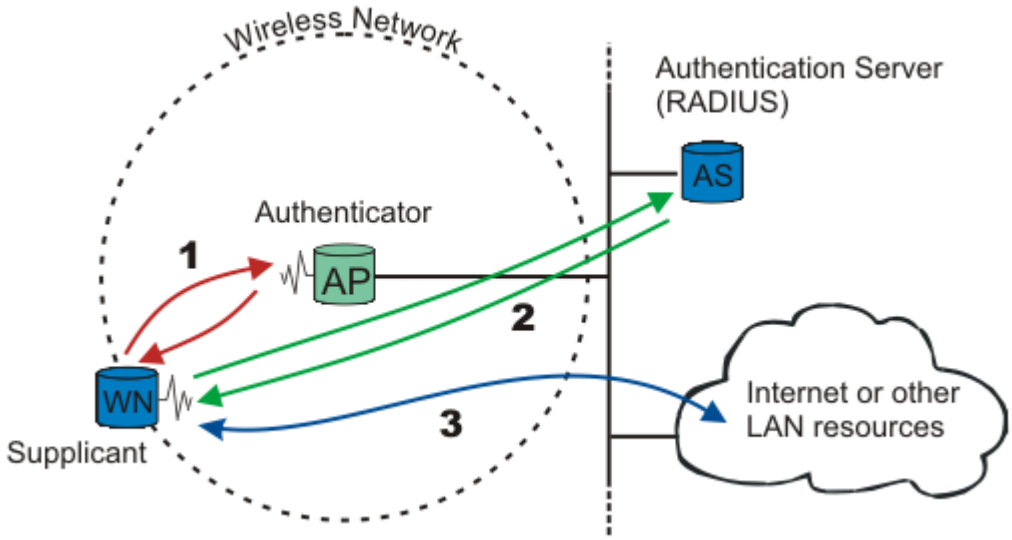
2.5 Tietoturva

Tietoturva on nykyään erittäin keskeinen osa kaikkea tietoverkkojen toimintaa. Langattoman verkon tapauksessa tietoturvan keskeisin haaste on tiedonsiirto radioaalloilla, joiden leviämistä ei voida fyysisesti estää. Näin ollen on lähdettävä oletuksesta, että kuka vain pystyy vastaanottamaan ja lähettämään dataa. Datan tulkitsemista vaikeuttamaan onkin kehitetty useita salausprotokollia ja verkkoihin pääsynvalvontaa.

WEP (Wired Equivalent Privacy) on alkuperäisessä 802.11-standardissa määritelty suojausprotokolla. Sen pääsynvalvonta perustuu etukäteen jaetun salausavaimen menetelmään (PSK, pre-shared key) ja liikenne salataan tällä avaimella ja salaus-algoritmilla. WEPissä käytetty algoritmi on kuitenkin helposti murrettavissa, joten se ei ole enää käyttökelpoinen suojausmenetelmä, joskin parempi kuin ei suojausta lainkaan. (Cam-Winget, Housley, Wagner & Walker 2003.)

IEEE alkoi WEP-protokollan murtumisen jälkeen kehittää uutta suojausprotokollaa langattomille verkoille. Tämä 802.11i-standardi julkaistiin 2004 ja siinä määritelty protokolla tunnetaan yleisesti nimellä **WPA2** (Wi-Fi Protected Access II). Ennen sen julkaisua kehitettiin väliaikasesti **WPA** (Wi-Fi Protected Access), joka ennakoi tulevaa standardia sisältäen monia sen ominaisuuksia. WPA2-suojauksessa on suuria parannuksia WEPiin verrattuna, tärkeimpänä tehokkaammat salausalgoritmit ja monipuoliset vaihtoehdot pääsynvalvontaan pelkän PSK:n sijaan (Benton 2010). WPA2 on edelleen moderni ja käyttökelpoinen suojausprotokolla 802.11-verkkoihin, eikä sitä korvaavaa protokollaa ole vielä kehitetty.

Yritykset jouduvat hallinnoimaan suuria määriä langattomia päätelaitteita. PSK on tällöin raskas ja aikaavievä tapa huolehtia pääsynvalvonnasta. Ratkaisuksi tähän IEEE (Institute of Electrical and Electronics Engineers) integroi yleisen **802.1X**-pääsynvalvontaprotokollan osaksi WPA2-suojausta. 802.1X on porttikohtainen pääsynvalvontamenetelmä, jota käytetään myös langallisissa lähiverkoissa. Porttikohtainen tarkoittaa, että asiakaslaitteen kommunikointi lähiverkossa todennetaan liityntäpisteessä eli esimerkiksi kytkinportissa tai langattomassa tukiasemassa sijaitsevassa loogisessa portissa. Kun uusi asiakaslaite liitetään porttiin (kuva 6, kohta 1), se pyritään todentamaan yleensä ulkoisen todennuspalvelimen avulla (kuva 6, kohta 2). Ennen kuin asiakaslaite on todennettu, ainoastaan todennusprotokollan liikenne sallitaan verkossa. Tyypillisesti todennusprotokollana käytetään RADIUSta (Remote Authentication Dial In User Service) ja asiakaslaite todennetaan käyttäjätunnuksen ja salasanan avulla. Kun asiakaslaite on todennettu, sallitaan asiakaslaitteen liikenne verkossa muutenkin (kuva 6, kohta 3. (Strand 2004.)



KUVA 6. Asiakaslaitteen (Supplicant) todennus portin (Authenticator) ja todennuspalvelimen avulla (Strand 2004)

2.6 Laitteet

Langaton lähiverkko voi suppeimmillaan tarkoittaa vain kahden päätelaitteen välistä langatonta yhteyttä. Tällaista ratkaisua kutsutaan ad-hoc-verkoksi. Yleensä langattoman

verkon tarkoitus on kuitenkin täydentää lankaverkkoa jatkamalla sitä mobiililaitteisiin. Tällöin tarvitaan langallisen verkon peruselementtien, kytkinten ja reitittimien, lisäksi myös **tukiasemia** (AP, Access Point). Laajan, useista tukiasemista koostuvan langattoman verkon hallintaa helpottaa **langattoman verkon kontrolleri**.

Lankaverkon kytkimet ja reitittimet muodostavat selkärangan, joka mahdollistaa WLAN-verkon rakentamisen. Tukiasemat ja kontrollerit kytketään kaapelein lankaverkon kytkimiin.

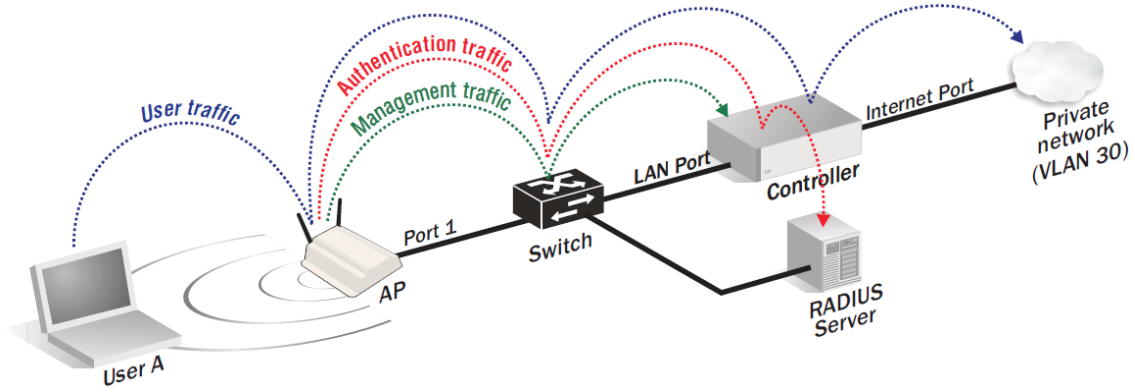
2.6.1 Kontrolleri

Langattoman verkon kontrolleri toimii tukiasemien ”isäntänä” ja tukiasemat ”orjina”, jolloin tukiasemat saavat tarvittavat asetukset ja mainostettavat verkot kontrollerilta. Ylläpitäjän tarvitsee syöttää muutokset ainoastaan kontrolleriin, joka levittää ne langallista lähiverkkoa pitkin tukiasemiin.

Kontrolleriohjattua langatonta verkkoa varten on kehitetty kaksi keskeistä protokollaa: **LWAPP** (Lightweight Access Point Protocol) sekä **CAPWAP** (Control And Provisioning of Wireless Access Points). Protokollien tavoitteena on yhtenäistää kontrollerin ja tukiasemien väliset käytännöt määrittelemällä yleisluontoiset kapselointi- ja kuljetusmekanismit riippumatta OSI-mallin ensimmäisen ja toisen kerroksen tekniikoista, mutta käytännössä niitä käytetään 802.11-verkkojen kanssa niitä varten luoduilla sidonnaisilla. (IETF 2009a, IETF 2009b, IETF 2010.) Suurista alan toimittajista Cisco Systems on ottanut nämä protokollat käyttöön tuotteissaan, mutta esimerkiksi Hewlett-Packard käyttää omaa, UDP-protokollan avulla toimivaa järjestelmäänsä kontrollerin ja tukiaseman väliseen kommunikointiin (Hewlett-Packard Company 2011b). Käytössä on siis monia erilaisia toteutuksia ja usealla OSI-mallin kerroksella.

Yleisesti kontrollerilla voi olla monenlaisia rooleja. Se voi hallita langatonta verkkoa monipuolisesti (kuva 7), jolloin kaikki liikenne kierrätetään kontrollerin kautta ja jopa reititetään siinä. Näin on helppo toteuttaa käyttäjien todennusta ja pääsynvalvontaa, kun muodostetaan tunneli kontrollerin ja jokaisen tukiaseman väliin. Tunnelin liikenne voidaan myös salata. Toisaalta kontrollerin roolina saattaa olla pelkästään hallintako-

mentojen välittäminen tukiasemille. Ylläpitäjän kontrolleriin syöttämät asetukset siirtyvät kaikille tukiasemille, jotka sitten osaavat ohjata liikenteen oikeaan VLANiin itsenäisesti. Tällöin verkon pääsynvalvontaa täytyy suorittaa erikseen jossain muualla kuin kontrollerissa.



KUVA 7. Kontrollerin ja tukiaseman tyypillinen toiminta lähiverkossa (Hewlett-Packard Company 2011b, muokattu)

2.6.2 Tukiasema

Tukiasema toimii rajapintana langallisen ja langattoman verkon välillä. Tukiasema voi olla itsenäinen (standalone) tai kontrollerin ohjaama (lightweight). Itsenäiseen tukiasemaan ylläpitäjän tulee tehdä kaikki asetukset paikallisesti, jolloin suuressa verkossa työn määrä on suuri. Toisaalta itsenäiset tukiasemat ovat halvempia, varsinkin kun otetaan huomioon, että kallista kontrolleria ei tarvita.

Kontrolleriohjatulla tukiasemalla puolestaan on monia etuja. Tällaisessa verkossa keskitetty ylläpito on luonnollisesti helpompaa, mutta myös esimerkiksi päätelaitteiden MAC-osoitetaulua voidaan ylläpitää keskitetysti kontrollerin muistissa, jolloin verkon toiminta on hiukan nopeampaa ja suoritintehoa kuluu vähemmän. Verkon suorituskyky pystytään myös optimoimaan automaattisemmin kontrollerin avulla: kontrolleri voi määrätä tukiasemien käyttämät taajuuskanavat välttääkseen häiriötilanteet, joissa vierekkäiset tukiasemat käyttävät samoja kanavia. (Rajesh 2010.)

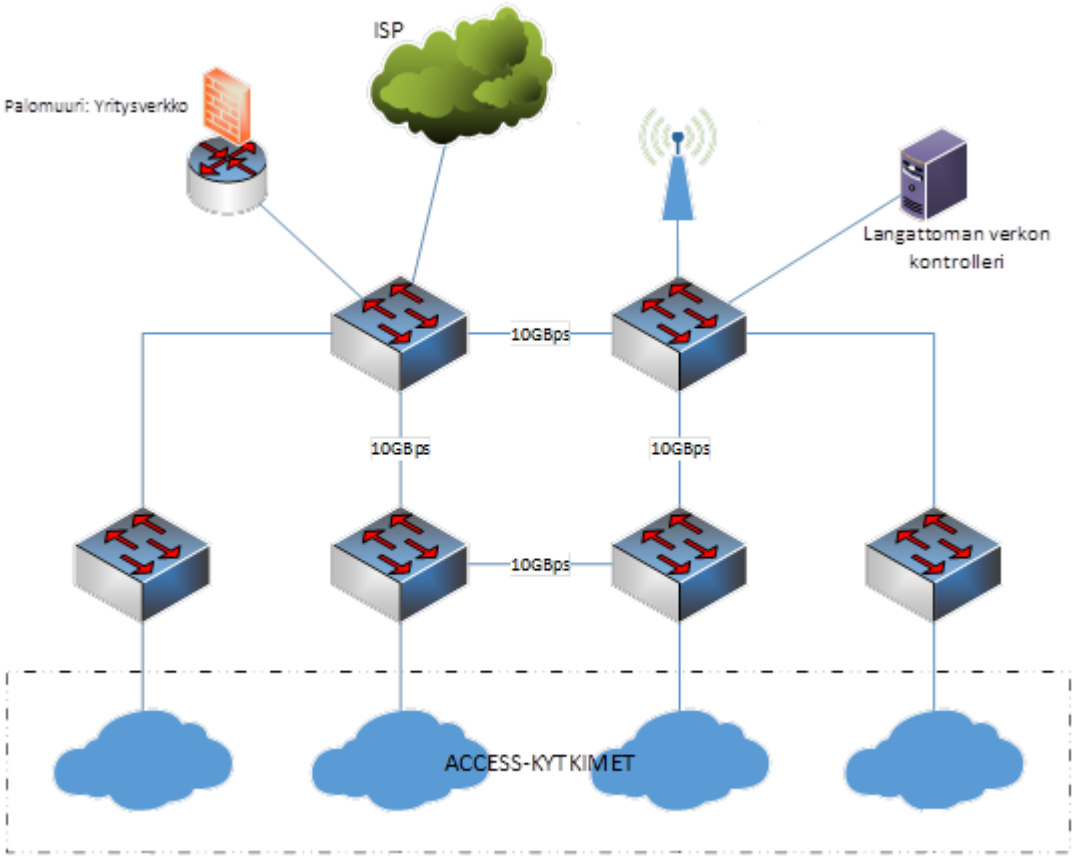
3 CASE SÄRKÄNNIEMI

Tampereen Särkänniemi Oy:ssä on ilmennyt tarve saada langaton verkkoyhteys huvipuistoasiakkaiden käyttöön. Lähes kaikki nykyiset mobiililaitteet älypuhelimista tabletteihin ja kannettaviin tietokoneisiin kykenevät WLAN-yhteyksiin 802.11-protokollia käyttäen. Verkkoyhteys on siis luontevaa toteuttaa näiden standardien avulla. Avoimen yhteyspisteen nimeksi (SSID, Service Set Identifier) annetaan Sarkka Open.

Huvipuisto on pienelle alueelle tiiviisti rakennettu alue, jossa liikkuu kuitenkin todella paljon asiakkaita: parhaina päivinä yli kymmenen tuhatta. Ympäristö siis asettaa monia haasteita langattoman verkon suunnitteluun ja rakentamiseen. Kuinka laaja peittoalue verkolle on järkevää toteuttaa? Mihin tukiasemat sijoitetaan peittoalueen saavuttamiseksi? Kuinka suureen käyttäjämäärään varaudutaan? Näihin kysymyksiin toteutuksessa pyritään vastaamaan.

3.1 Lähtötilanne

Huvipuiston kiinteä langallinen verkko kattaa valmiiksi koko huvipuiston alueen erittäin hyvin. Runkoverkko koostuu kuudesta tehokkaasta keskuskytkimestä, joihin on kytketty liityntätason kytkimet. Näitä liityntätason kytkimiä on lähes joka rakennuksessa ja kioskissa. Verkko noudattaa osittain yleistä verkkojen kerroksellista suunnittelu-filosofiaa, jossa ydin- ja jakelutasot on yhdistetty. Kaikissa kytkimissä tosin on myös liityntätason elementtejä. Verkon rakenne on esitelty kuvassa 8.



KUVA 8. Verkon fyysinen topologia ennen Sarkka Openia

Langattoman verkon kontrolleri on yhdessä kuudesta keskuskytkimestä. Ennestään puistossa on muutaman tukiaseman langaton verkko yrityksen sisäisessä käytössä, joten perusinfrastruktuuri avoimen langattoman verkon rakentamiseen on olemassa. Olemassa olevat langattomat verkot käyttävät käyttäjän todentamista, kun taas Sarkka Open tulee olemaan avoin kaikille ilman todentamista.

Verkossa on muutama VLAN liikenteen erottelua varten. Esimerkiksi työasemat, verkonhallintaliikenne ja kassaliikenne on eroteltu toisistaan. Reititys virtuaalisten lähiverkkojen välillä tapahtuu ns. tikunnokkareitityksenä keskuskytkimeen kytketyssä palomuuri/reitittimessä. Sama laite reitittää yrityksen liikenteen myös palveluntarjoajan suuntaan.

3.2 Tarpeet ja vaatimukset

Lähtökohtana suunnittelussa oli rakentaa verkko, jonka avulla huvipuistoasiakkaat, työntekijät, yritysasiakkaat, kokousvieraat ja muut alueella vierailevat sidosryhmät pääsevät Internetiin omilla langattomilla päätelaitteillaan. Verkossa ei tällöin tarvita pääsynvalvontaa tai liikenteen salausta.

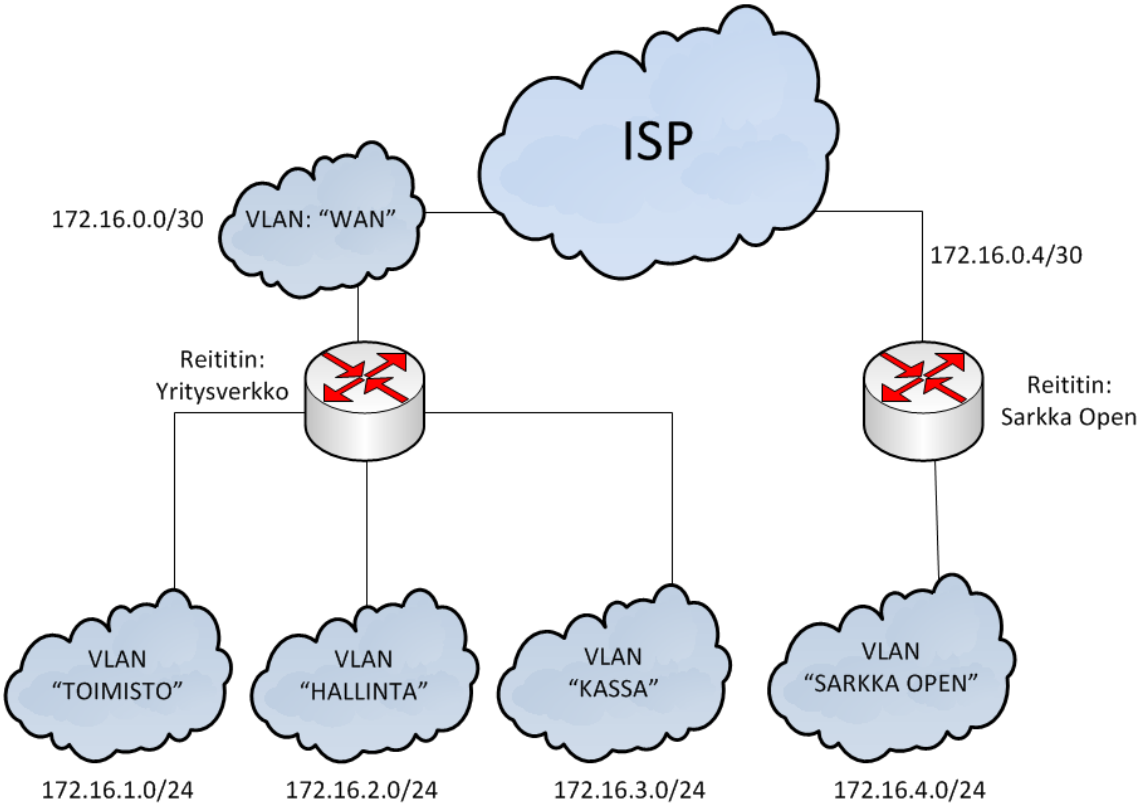
Kaikille avoin langaton verkko on luonnollisesti avoin myös salakuuntelulle, joten käyttäjien on huolehdittava mahdollisesta liikenteen salauksesta itse sovellustasolla. Nykyään voitaneen tosin pitää yleistietona, että langatonta tietoliikennettä voidaan salakuunnella ja esimerkiksi yrityssalaisuuksia käsiteltäessä tämä on yleensä huomioitu asiallisesti. Päätelaitteet voivat myös muodostaa yhteyksiä toisiinsa, sillä ne ovat samassa aliverkossa. Tällöin ne altistuvat hyökkäyksille saman langattoman verkon muiden käyttäjien suunnalta, ellei päätelaitteiden tietoturvasta ole huolehdittu.

Verkon suunnittelu aloitettiin toimeksiantajan toteuttamalla pienimuotoisella kyselyllä verkon tarpeesta. Erityisesti ulkomaalaisilla asiakkailla havaittiin tarve WLAN-verkolle, sillä ulkomailla mobiilidatan käyttö on usein huomattavan kallista verrattuna kotimaahan. Tämä on tuttu ilmiö myös ulkomailla vieraileville suomalaisille, ja usein 3G-yhteydet suljetaankin kokonaan mobiililaitteista ulkomailla matkailtaessa. Tällöin WLAN on käytännössä ainoa keino luoda Internet-yhteys, joten verkko on erittäin hyödyllinen ja tarpeellinen ulkomaisille asiakkaille. Tarpeita tosin on myös yrityksen sisällä: Elämyspuiston alueella on useita kokoustiloja, joita vuokrataan yritysasiakkaille. Lisäksi toimeksiantaja itse järjestää paljon tilaisuuksia, joiden vieraat hyötyvät WLAN-yhteydestä.

Verkolta vaaditaan myös tuki ”roaming”-toiminnolle, jossa päätelaite liikkuu tukiaseman kuuluvuusalueen laidalle ja yhdistää siellä toiseen tukiasemaan verkkoyhteyden katkeamatta.

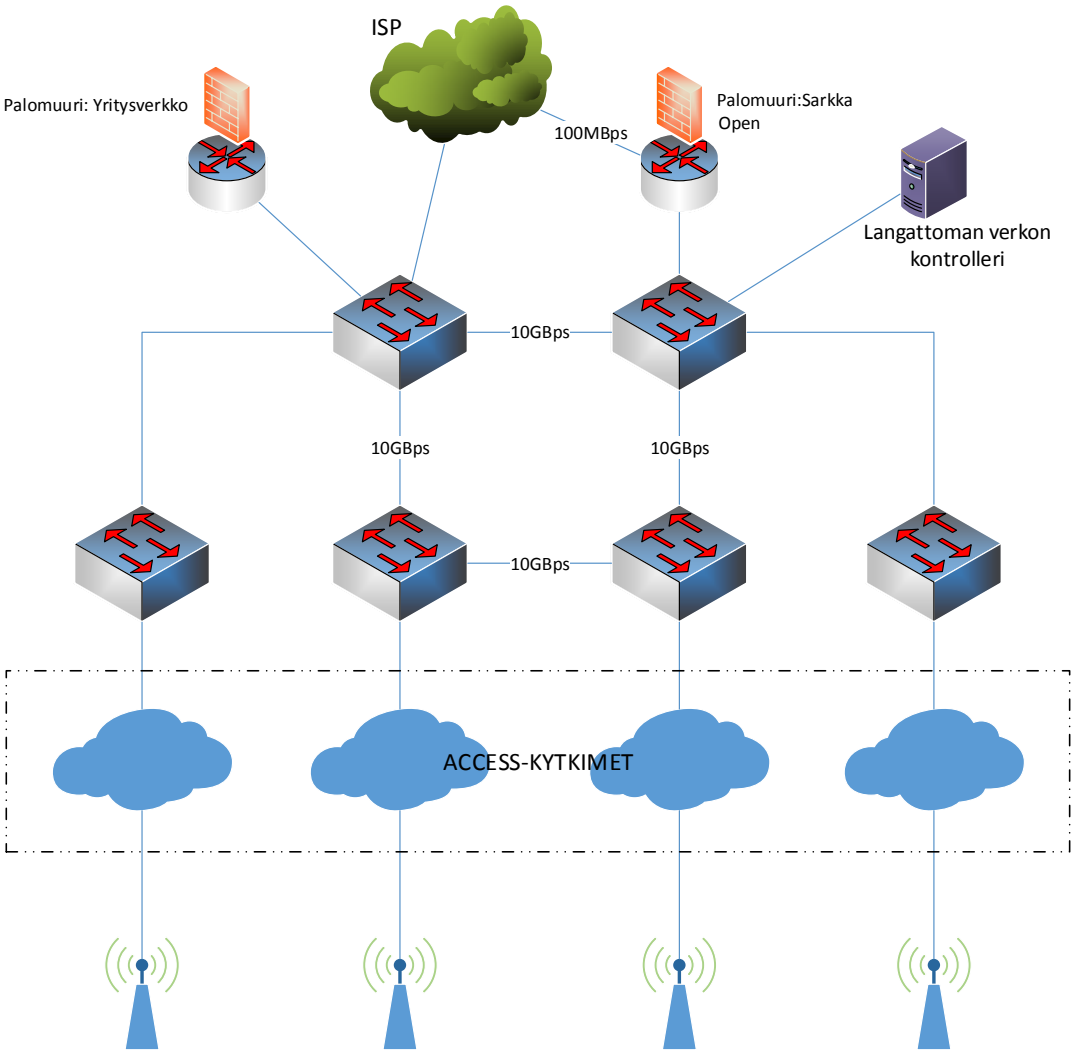
3.3 Verkon suunnittelu

Sarkka Open-verkon liikenne ohjataan omaan aliverkkoonsa ja VLANiin sekä reititetään palomuuri/reitittimen läpi palveluntarjoajalle (ISP, Internet Service Provider). Sarkka Open-verkosta ei pääse yrityksen sisäverkkoon, jonka liikenne reititetään omassa laitteessaan. Näin suojataan yritysverkkoa Sarkka Open-verkon käyttäjiltä ja ulkoisilta hyökkäyksiltä (kuva 9).



KUVA 9. Verkon looginen topologia Sarkka Openin jälkeen.

Kuva 10 kuvaa tulevan verkon fyysisen rakenteen. Vanhaan runkoverkkoon lisätään Sarkka Open-verkon oma palomuuri/reititin. Lisäksi asennetaan tukiasemat liityntätasolle.



KUVA 10. Verkon fyysinen topologia Sarkka Openin jälkeen

3.3.1 Laitteet

Verkon toteuttamiseksi vaaditaan olemassa olevaan verkkoon lisää tukiasemia sekä Sarkka Openin palomuuri/reititin. Langallinen verkko kattaa ennestään puiston alueen niin hyvin, että lähes joka rakennuksessa on kytkin, johon yksittäinen tukiasema voidaan liittää.

Kontrolleri

Langattoman verkon kontrollerina käytetään HP Procurve MSM765zl-moduulia (kuva 11), joka on liitetty HP 5400-sarjan runkokytkimeen. Kontrolleriin ostettu lisenssi mahdollistaa maksimissaan 40 tukiaseman liittämisen, mikä riittää Sarkka Openin toteutta-

miseen: käytettävissä on 23 tukiasemaa. Tämä jättää mahdollisuuden laajentaa verkkoa myöhemmin tukiasemilla.

Kontrollerissa on monipuoliset ominaisuudet: muun muassa DHCP-palvelin, palomuuri, NAT/PAT, tuki ulkoiselle tai sisäiselle todennuspalvelimelle ja liikenteen priorisointi (QoS, Quality of Service). Valtaosaa näistä palveluista ei tarvita Sarkka Openin toteuttamisessa, mutta olemassa olevat langattomat verkot sisäisessä käytössä tarvitsevat esimerkiksi tukea RADIUS-todennuspalvelimelle.

KUVA 11. Kontrollerimoduuli. (Hewlett-Packard Company 2011a)

Kontrolleria hallitaan web-käyttöliittymästä tai komentoriviltä konsoli- tai SSH-yhteydellä. Kontrollerin ehkäpä olennaisin ominaisuus on VSC, Virtual Service Community. VSC on kokoelma asetuksia, jotka kuvaavat kontrollerin ja sen hallitseman tietyn tukiasemajoukon toimintaa. Käytännössä VSC on verkko, jolla on oma SSID ja tyypillisesti myös oma VLAN. VSC liitetään tukiasemaryhmään, jolloin kaikki ryhmään kuuluvat tukiasemat saavat VSC:hen määritetyt asetukset. Kontrolleri tukee maksimissaan 64 ja yksittäinen tukiasema 16 VSC:tä, mikä riittää hyvin useimmissa ympäristöissä. (Hewlett-Packard Company 2011a.)

Tukiasemat

Tukiasemina käytetään HP MSM430-laitteita (kuva 12). Laitteessa on kaksi radiolähetin-vastaanotinta, joilla molemmilla on kolme sisäänrakennettua antennia. Toinen radio toimii 2,4 GHz ja toinen 5 GHz taajuudella. Laite tukee 802.11a/b/g/n protokollia.

KUVA 12. HP MSM430-tukiasema

5 GHz radiolähetin-vastaanotin tukee 802.11a-protokollaa 54Mb/s maksiminopeudella ja 802.11n-protokollaa 300Mb/s maksiminopeudella. 2,4 GHz taajuudella toimiva radio taas tukee 802.11b-protokollaa 11Mb/s nopeudella, 802.11g-protokollaa 54Mb/s nopeudella ja 802.11n-protokollaa 300Mb/s nopeudella. Uudemmat 802.11ac/ad-protokollat eivät siis ole tuettuja. (Hewlett-Packard Company 2013.)

Tukiasemaan ei voi liittää ulkoista virtalähdettä lainkaan, vaan ainoastaan Power over Ethernet-ominaisuus (PoE) on tuettu. Tukiasema saa virtansa verkkokaapelin välityksellä verkkokytkimessä sijaitsevasta tai erillisestä, ulkoisesta PoE-injektorista. Tämä luonnollisesti vaatii kytkimeltä tukea PoE-ominaisuudelle. Särkänniemen verkossa käytetään ainoastaan HP:n PoE-kytkimiä, joten ongelmilta vältytään.

Reititys

Särkänniemen verkon reititys hoidetaan Dell Sonicwall Pro 2040-palomuuri/reitittimillä (kuva 13). Sarkka Open-verkolle on alistettu oma laite tähän tarkoitukseen. Laite, Sonicwall Pro 2040, on pienten ja keskisuurten verkkojen reitityksen ja tietoturvan hoitamiseen suunniteltu keskitetty ratkaisu, joka tarjoaa muun muassa NAT- ja DHCP-palvelut lähiverkkoon (Perry 2004).

KUVA 13. Dell Sonicwall Pro 2040 palomuuri/reititin.

3.3.2 Asennuspaikat

Hyvällä tukiaseman asennuspaikalla on paljon vaatimuksia. Tukiaseman kuuluvuusalueen tulisi olla mahdollisimman laaja, verkkokytkimen pitäisi olla mahdollisimman lähellä pitkien kaapelivetojen välttämiseksi sekä tukiasema pitäisi olla fyysisesti helposti tavoitettavissa mutta kuitenkin asiattomien ulottumattomissa. Tällaisia paikkoja tuli kaiken lisäksi löytää 23 tukiasemalle. Kompromisseja jouduttiin tekemään valmiin ympäristön asettamissa puitteissa.

Koska tukiasemat toimivat PoE-virralla, ainoa tarvittava kaapelointi on verkkokaapeli lähimmältä PoE-kytkimeltä. Tukiasemat eivät sovellu ulkokäyttöön suojauksensa puolesta, joten kaikki asennuspaikat on löydyttävä kuivista sisätiloista.

Näistä lähtökohdista alettiin suunnitella tukiasemien sijoituspaikkoja. Koko huvipuiston laajaa aluetta ei ollut tarkoituksenmukaista peittää täydellisesti: tärkeintä oli peittää alueet, joilla liikkuu eniten ihmisiä ja joissa todennäköisimmin on tarvetta WLAN-yhteydelle.

Huvipuistoalueella on onneksi tiheästi erilaisia rakennuksia. Pari vuotta sitten toteutetun lankaverkon laajennuksen myötä lähes jokaiseen rakennukseen vedettiin valokuituyhteys. Elämyspuiston karttaa tutkimalla selvitettiin, mihin rakennuksiin käytettävissä olevat tukiasemat kannattaa sijoittaa. Valituista rakennuksista etsittiin tukiasemille asennuspaikat, jotka mahdollistavat hyvän kuuluvuuden radiosignaaleille ja helpon asennuksen. Joissakin kohteissa jouduttiin tekemään usean kymmenen metrin kaapelivetoja, mutta näin saatiin tukiasemat korkeisiin paikkoihin ja asiakkaiden lähettyville häiriöi-

den minimoimiseksi. Kuvassa 14 on esimerkki normaalista tukiaseman asennuksesta sisätiloissa, joihin vain työntekijöillä on pääsy.

KUVA 14. Tyypillinen tukiaseman asennuspaikka katonrajassa.

3.4 Toteutus

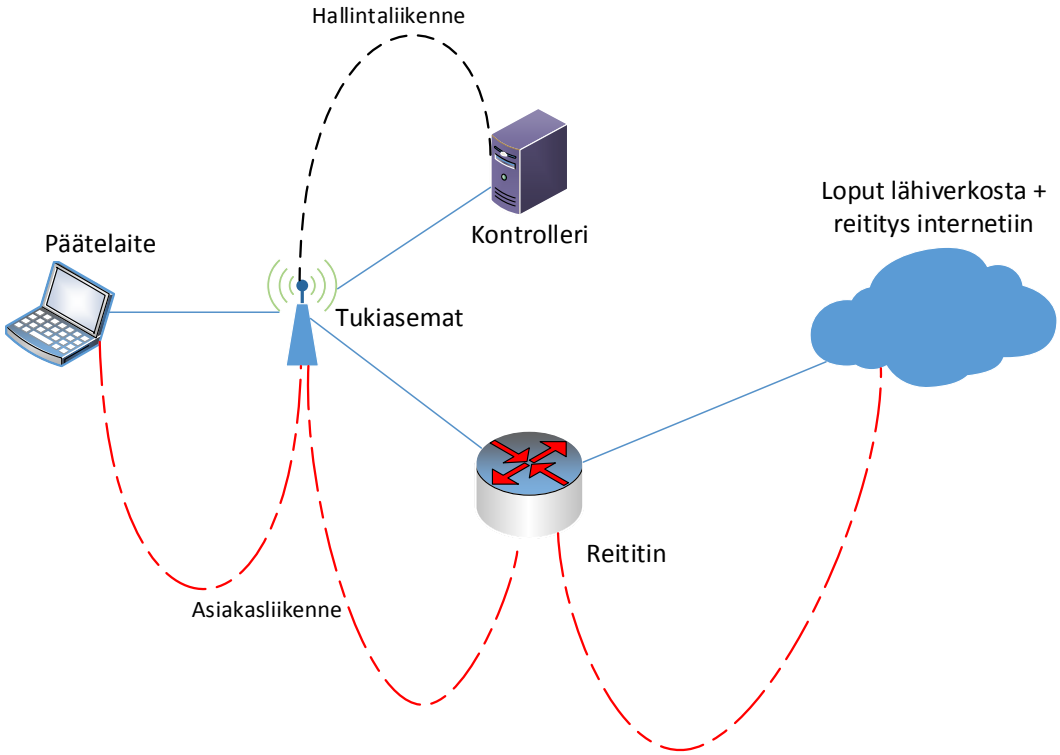
Langattoman verkon varsinainen käytännön toteutus tarkoitti työssä uusien tukiasemien ja palomuuri/reitittimen asennusta ja konfigurointia, asetusmuutosten tekemistä kontrolleriin ja kokonaisuuden testaaminen ja mittaaminen.

3.4.1 Laitteiden asennus

Itse tukiasemien asennus on erittäin suoraviivaista. Aluksi asentamaton tukiasema liitetään samaan aliverkkoon kontrollerin kanssa asennuslaboratoriossa. Tukiasema saa IP-asetukset DHCP-palvelimelta, joka tässä tapauksessa toimii kontrollerissa. Tukiasema alkaa etsiä verkosta kontrolleria UDP-viesteillä, joita kontrolleri kuuntelee. Kontrolleri vastaa tukiaseman kutsuun ja tukiasema yhdistyy kontrolleriin. Kontrolleri tarkistaa tukiaseman ohjelmistoversion ja päivittää sen jos se ei ole ajan tasalla. Kun ohjelmisto on päivitetty, tukiasema käynnistyy uudelleen ja asennusprosessi alkaa alusta. Tällä kertaa kontrolleri kuitenkin toteaa ohjelmiston olevan ajan tasalla ja laitteet muodostavat hallintatunnelin välilleen. Hallintaliikenne kontrollerin ja tukiasemien välillä on salaamatonta UDP-liikennettä. (Hewlett-Packard Company 2011a.)

Kun kontrolleri on saanut tukiaseman hallintaansa, ylläpitäjä asettaa kontrollerin web-hallintapaneelista tukiaseman asetukset kohdilleen. Tukiasemille annetaan nimet ja kiinteät IP-asetukset sekä liitetään tukiasema ryhmään. Ryhmään taas liitetään oikea VSC. Tukiasema viedään lopulliseen asennuspaikkaansa ja kytketään verkkoon. Lopuksi varmistetaan tukiaseman verkkoyhteys ping-komennolla, johon tukiasema vastaa, mikäli yhteys on kunnossa. Kun kaikki tukiasemat on saatu asennettua, otetaan kontrollerin DHCP-palvelin pois käytöstä. Näin estetään esimerkiksi mahdollista hyökkääjää saamasta selville tietoja verkosta kytkemällä oma tukiasemansa verkkoon. Hyökkääjän tukiasema saisi konfiguraatiotiedot kontrollerilta ja saattaisi päästä tutkimaan näitä konsoliyhteyden kautta ja etsimään heikkouksia. Viitteitä tällaisista hyökkäyksistä tai niiden todennäköisyydestä ei löytynyt, mutta riskien minimoimiseksi DHCP-palvelin on järkevää pitää pois käytöstä silloin kun sitä ei tarvita.

Palomuuri/reititin asennettiin samaan laitetilaan palveluntarjoajan rajakytkimen kanssa ja kytkettiin verkkoon kuvan 15 mukaisesti. Laite konfiguroitiin DHCP-palvelimeksi langattomille asiakkaille Sarkka Openin aliverkkoon. Laite myös reitittää verkon liikenteen palveluntarjoajan verkkoon sekä suojaa verkkoa hyökkäyksiltä palomuurilla ja tunkeilijan havaitsemisjärjestelmällä (IDS, Intrusion Detection System).



KUVA 15. Kontrollerin ja tukiaseman suhde Sarkka Openissa

3.4.2 Laitteiden konfigurointi

Kontrollerissa luotiin VSC nimeltä Sarkka Open, joka tarkoittaa käytännössä myös verkon SSID:tä. VSC:lle ei tehty määrityksiä pääsynvalvonnan, liikenteen salauksen tai QoS:n osalta, koska mitään niistä ei otettu käyttöön. Päätelaitteiden maksimimäärä rajattiin 100 asiakkaaseen. Tämä määrä koettiin riittäväksi normaalikäytössä, mutta erityistilanteissa määrää voidaan tietenkin helposti nostaa tai laskea muutamassa minuutissa.

Sarkka Open-verkon asiakkaat saavat IP-asetuksensa palomuuri/reitittimessä olevalta DHCP-palvelimelta. Myös kontrollerissa on DHCP-palvelimen mahdollisuus, mutta tällä menettelyllä vähennetään mahdollisia tapauksia, joissa laiterikon vuoksi verkko lamaantuisi. Jos kontrolleri putoaa verkosta esimerkiksi virtalähteen pettämisen vuoksi, ei verkon toiminta keskeydy uusien asiakkaiden saadessa edelleen IP-asetukset palomuurilta. Tosin tukiasemille ei voida tehdä muutoksia kontrollerin ollessa pois toiminnasta, mutta ainakaan asiakasliikenne ei katkea. Jos taas palomuurissa tapahtuu liikenteen katkaiseva laiterikko, liikenne Internetiin estyy vaikka DHCP-palvelin olisi kont-

rollerissa, koska palomuuri reitittää kaiken Sarkka Open-verkon liikenteen Internetiin palveluntarjoajalta vuokrattua yhteyttä pitkin.

Palomuuri on lisäksi konfiguroitu estämään yhteyden muodostamiset ulkopuolelta Sarkka Open-verkkoon. Näin suojataan asiakkaita ulkopuolisilta hyökkäyksiltä.

Kaikilta verkon aktiivilaitteilta kerätään valvontadataa SNMP-protokollan (Simple Network Management Protocol) avulla. Valvontapalvelu on ostettu yritykseltä, joka valvoo verkkoa ympäri vuorokauden. Kriittisistä vioista valvontajärjestelmä lähettää hälytyksen vastuulliselle ylläpitäjälle, jotta vika tulisi korjattua mahdollisimman pian.

Tukiasemille on asetettu kontrollerista päälle automaattinen kanavien valinta (Hewlett-Packard Company 2011a, 4:25). Näin jokainen tukiasema tarkkailee jatkuvasti radiotaajuuksia ja vaihtaa kanavaa, mikäli havaitsee häiritsevää liikennettä. Manuaalisella kanavien asettamisella jokaiselle tukiasemalle saataisiin kenties vähennettyä häiriöitä hiukan tehokkaammin, mutta ylläpito olisi raskasta ja vaatisi huolellista muutosten dokumentointia. Tukiasemien kuuluvuusalueet eivät mene päällekkäin useamman kuin korkeintaan 2-3 tukiaseman kesken kerrallaan, joten kaikilla tukiasemille on häiriötön kanava käytössä.

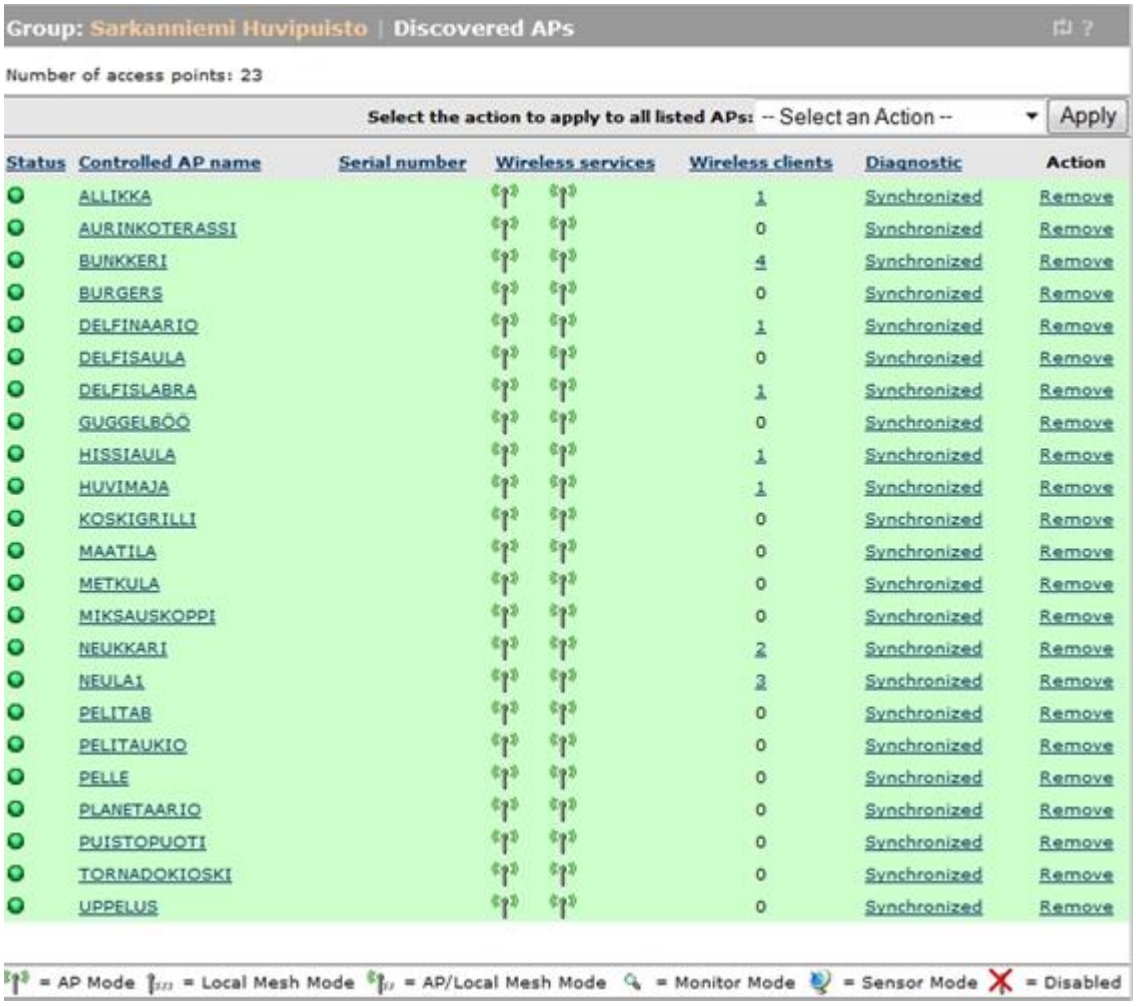
Kontrollerin graafisesta web-käyttöliittymästä voidaan tarkastella tukiaseman havaitsemia muita tukiasemia alueellaan. Ylläpitäjä voi vertailla näiden fyysisiä eli MAC-osoitteita (Media Access Control) omien tukiasemien osoitteisiin ja näin havaita mahdolliset ”rogue”-tukiasemat, joiden avulla hyökkääjä pyrkii ohjaamaan asiakasliikenteen omaan verkkoonsa, joka mainostaa samaa SSID:tä. Tällaista vertailua tulisi suorittaa säännöllisin väliajoin.

3.4.3 Testaus

Valmis verkko testattiin käytännössä liikkumalla huvipuistossa jokaisen tukiaseman kuuluvuusalueella ja testaamalla verkkoon yhdistämistä älypuhelimella. Kuva 16 näyttää kontrollerin statussivun, jossa ryhmään ”Sarkanniemi Huvipuisto” kuuluvat tu-

kiasemat näkyvät. Tähän ryhmään on sidottu VSC nimeltä Sarkka Open, eli jokainen alla listattu tukiasema mainostaa Sarkka Open-verkkoa.

Suurimpien rakennusten sisätiloissa saavutettiin hyvä verkkoyhteys lähes kaikissa asiakastiloissa. Ulkotilojen kuuluvuus mitattiin erikseen ja tätä mittausta käsitellään seuraavassa kappaleessa tarkemmin. Roaming-toiminnallisuus testattiin toimivaksi siellä missä tukiasemat ovat riittävän lähellä toisiaan. Tukiasemien kuuluvuusalueiden pitää olla riittävästi päällekkäin, jotta verkkoyhteys ei katkea.



KUVA 16. Kaikki tukiasemat ovat toiminnassa.

3.5 Suorituskyvyn mittaus

Toimivan ja testatun verkon suorituskyky voidaan mitata monesta eri näkökulmasta. Voidaan tutkia esimerkiksi verkon kaistanleveyttä, viivettä, yhtäaikaisten yhteyksien määrää ja verkon kuuluvuutta eri paikoissa. Tarkoitukseen on olemassa monia tehokkaita ohjelmistoja, mutta tällaisen ilmaiseksi tarjottavan verkon mittaamiseen ei ollut tarkoituksenmukaista hankkia suurten verkkojen tutkimiseen tarkoitettua verrattain kallista ohjelmistoa. Verkossa ei liiku bisneskriittistä dataa eikä verkon suorituskyky sanottavasti vaikuta toimeksiantajan tulonmuodostukseen.

Verkon peittoalue haluttiin kuitenkin selvittää. Peitolla selviää helposti, mihin paikkoihin tarvitaan mahdollisesti lisää tukiasemia tai onko jossakin turhaan päällekkäisiä tukiasemia.

Mahdollisia käytettäviä laitteita ja ohjelmistoja selvitettiin ja tarkoitukseen sopivimmaksi valikoitui Ekahau Heatmapper-ohjelman ilmaisversio. Ohjelma asennettiin kannettavaan tietokoneeseen Windows-käyttöjärjestelmään ja siihen ladattiin karttapohja. Mitään erikoislaitteistoa ei vaadittu, ainoastaan langattoman verkkokortin tuki testattaville protokollille. Karttapohjan lataamisen jälkeen ohjelmalla aloitettiin mittaus: karttaan merkittiin mittauksen aloituspiste ja käveltiin mitattava alue hitaasti läpi, jatkuvasti merkiten karttaa senhetkinen sijainti. Ohjelma skannasi tarjolla olevia verkkoja ja näytti mittauksen jälkeen yhteisen kuuluvuuskartan kaikille verkoille.

Yhteinen kuuluvuuskartta olisi tuottanut merkittäviä ongelmia, mikäli alueella olisi muitakin tukiasemia kuin Sarkka Open-verkkoa mainostavia. Tällöin nekin olisivat näkyneet kartalla. Nyt kuitenkin kaikki mitatun alueen tukiasemat mainostivat Sarkka Open-verkkoa, joten tältä ongelmalta vältyttiin.

Ekahau Heatmapper-ohjelman ilmaisversio rajoitti yksittäisen mittauksen pituudeksi 15 minuuttia. Tämä oli merkittävä haaste, sillä koko huvipuiston mittaamiseen kului useita tunteja. Ratkaisuna oli alueen mittaaminen useissa 15 minuutin jaksoissa. Mittausten tuloksena syntyneet kuuluvuuskartat piti yhdistää kuvankäsittelyohjelmalla jälkikäteen. Ohjelman generoimat rajat eri kuuluvuusalueille eivät tietenkään osuneet täysin saumattomasti yhteen, joten karttojen yhdistämisessä jouduttiin käyttämään pientä luovaa ekst-

rapolointia siellä, missä alueiden raja ei ollut selvä. Ongelma oli onneksi etukäteen tiedostettu, joten mittausalueen rajat pyrittiin pitämään mahdollisimman kaukana tukiasemista jolloin lähinnä huonoimpien kuuluvuusalueiden rajoilla jouduttiin käsin piirtämään ylimääräisiä rajoja. Vaikka ohjelmakin käytännössä ekstrapoloi kuuluvuusalueiden rajat mittauksen perusteella likimäärin, heikentää tällainen lopputuloksen käsin manipulointi mittauksen toistettavuutta ja luotettavuutta.

Lopputuloksena syntyi kaksi erillistä kuuluvuuskarttaa (liite 1): ensimmäinen kartta kattaa valtaosan Elämyspuiston alueesta ja toinen pelkästään Koiramäen alueen. Tämä johtuu siitä, että mittauksen aikaan ei ollut saatavilla koko suuren alueen kattavaa ajantasaista yleiskaavakuvaa, vaan tuore Koiramäen alue oli omalla kartallaan.

Valmiita karttoja tarkastelemalla havaitaan, että ulkoalueen peitto on hyvä lähinnä tukiasemien välittömässä läheisyydessä eli rakennusten vieressä ja sisällä. Laajoilla ulkoalueilla, mihin tukiasemia ei ole voitu sijoittaa rakennusten puutteen vuoksi, ei verkkoyhteyttä käytännössä ole. Tällaiset alueet ovat tosin elämyspuistossa lähinnä siirtymiä varten, eivätkä asiakkaat neljän Elämyspuistossa viettämäni kesän perusteella vaikuta viihtyvän tällaisilla alueilla kovin pitkään kerrallaan. Viihtyvyyttä voisi toki lisätä nopea WLAN-yhteys, joten alueiden kehittämistä suunnitellessa asiaa kannattaa tuoda esiin.

Tärkeimpinä katettavina voidaan pitää alueita, joilla asiakkaat viettävät paljon aikaa kerrallaan. Tällaisia ovat esimerkiksi terassit, kahvilat ja esiintymislavojen läheisyys. Lähes kaikki tällaiset alueet ovat kartalla vihreällä tai keltaisella alueella. Määritellyn kaltaiset alueet, joissa ei ole hyvää kuuluvuutta, tulisi pikimmiten kattaa uusilla tukiasemilla. Tällainen alue on esimerkiksi Elämyspuiston sisäänkäynnin läheisyys.

Muutama tukiasema sijaitsee rakennuksissa, joiden yksi seinä on metallinen, nostettava sermi. Mittaukset suoritettiin sermien ollessa suljettuna, jolloin radiosignaalien kulku oletettavasti oli heikompaa kuin sermien ollessa auki. Mittaus suoritettiin pahimman tilanteen periaatteella, sillä sermit eivät aina ole auki huvipuiston aukioloaikoinakaan. Erikseen voidaan pohtia, olisiko järkevämpää sijoittaa tukiasemat sermien ulkopuolelle, jotta kuuluvuuteen ei vaikuttaisi niin dramaattisesti sermien asento.

Verkko toteutettiin alussa määriteltyjen tarpeiden ja vaatimusten mukaisesti. Laajentamisen varaa jäi tukiasemien osalta tulevaisuutta varten. Käyttäjämäärään varaudutaan aluksi maltillisesti, mutta määrää voidaan helposti nostaa tulevaisuudessa. Tukiasemille löydettiin hyvät asennuspaikat, jotka mahdollistavat riittävät kuuluvuusalueet ympäri puistoa. Verkon suorituskyky havaittiin mittauksissa tarpeisiin sopivaksi.

4 POHDINTA

Opinnäytteen tavoite oli kehittää Särkänniemen Elämyspuiston asiakkaille tarjoamia tietoteknisiä palveluita yrityksen tarjoaman langattoman verkon kautta. Työn tarkoituksena oli toteuttaa avoin WLAN-verkko, jonka avulla niin asiakkaat kuin yritysvieraatkin voivat muodostaa Internet-yhteyden langattomilla päätelaitteillaan. Työn lopputuloksena todellakin syntyi avoin langaton verkko, jota kuka tahansa alueella liikkuva voi käyttää 802.11-yhteensopivalla päätelaitteellaan. Työstä on hyötyä toimeksiantajalle asiakkaita palvelevan langattoman verkon muodossa. Työn tekijälle kertyi monipuolista ammatillista osaamista oikean työelämälähtöisen projektin muodossa. Kokemus oli arvokas ja lisäsi teknistä osaamista ja valmiuksia langattomien verkkojen rakentamiseen ja ylläpitämiseen tulevalla työuralla.

Työn teoriaosuudessa käsitellyt asiat saivat perustelunsa toteutusosassa, kun teoria vietiin käytäntöön. On tärkeää erottaa OSI-mallin kerrokset toisistaan, kun toteutetaan tällaista monipuolista verkkoa. Radiotekniikka esittää myös perustavanlaatuista osaa käytännön toteutuksessa ja siksi se on käsitelty huolellisesti teoriaosuudessa. Tämä työ ei ole suinkaan ainut ja oikein tapa toteuttaa WLAN-verkkoa, vaan eri teknologioiden, standardien ja laitteiden kirjo oli tärkeää käsitellä teoriaosuudessa, jotta lukijalle muodostuu realistinen käsitys aiheesta.

Työssä haastavinta oli perehtyä ennestään melko tuntemattomaan radiotekniikkaan alkeista lähtien. Myös asennuspaikkojen suunnittelu aiheutti hiukan päänvaivaa, kun tukiasemia oli käytössä rajattu määrä. Kuuluvuusmittauksien suorittaminen oli myös haastavaa lähinnä käytettävän ohjelmiston vuoksi.

Verkko rakennettiin pikku hiljaa kesän 2013 aikana, mutta tällaisen verkon ei oikeastaan voida koskaan sanoa olevan valmis. Kuuluvuusmittauksissa havaittiin, että koko Elämyspuiston alue ei todellakaan ole katettu langattomalla verkolla, vaan paikoitellen on isojakin epäjatkuvuusalueita. Verkon täydentäminen jatkuu mahdollisesti myöhemmin uusilla tukiasemilla. Kaikki kontrollerin lisenssin mahdollistamat 40 tukiasemaa kannattaisi ottaa käyttöön, jotta verkosta tulisi mahdollisimman kattava ja hyvin palveleva.

Sarkka Open-verkossa ei nykyisellään ole käytössä liikenteen priorisointia tai kaistanleveyden hallintaa, jolla voitaisiin estää yksittäistä käyttäjää ”ryöstämästä” koko verkkoyhteyttä itselleen. Tällaisten ominaisuuksien käyttöönoton mahdollisuuksia olisi hyvä selvittää jatkossa, jotta verkko olisi mahdollisimman tehokas ja kaikkien käyttäjien saavutettavissa. Lisäksi verkkoa käyttävät yritysasiakkaat saattaisivat arvostaa mahdollisuutta salattuun langattomaan liikenteeseen salakuuntelun vaikeuttamiseksi. Tällaisen, mahdollisesti Sarkka Open-verkolle rinnakkaisen, salatun yhteyspisteen toteuttamista voisi selvittää tarkemmin tulevaisuudessa.

Avoimen yhteyspisteen tapauksessa on pohdittava myös tarjoajan vastuuta palvelustaan. Onko toimeksiantaja välillisesti vastuussa, mikäli avoimen yhteyspisteen kautta syyllistytään rikoksiin tietoverkoissa tai käyttäjien tietoja varastetaan salaamattoman yhteyden vuoksi? Erityisesti tätä tulee pohtia, koska Sarkka Open-verkon sisällä päätelaitteiden väliset yhteydet on sallittu. Yksityishenkilön tarjoaman yhteyspisteen osalta Suomessa on olemassa ennakkotapaus (Oksanen 2012), jonka perusteella palveluntarjoaja ei ole vastuussa avoimen yhteyspisteen käyttäjien tekemistä tekijänoikeusrikoksista. Tapausta ei kuitenkaan välttämättä voi soveltaa yrityksen tarjoamaan yhteyspisteeseen tai muihin kuin tekijänoikeusrikoksiin, joten asiaa tulisi selvittää lakioppineiden avulla. Yksi usein käytetty ratkaisu on pakottaa käyttäjä hyväksymään palvelun käyttöehdot ja toimeksiantajan vastuuvapautuslauseke ennen verkon käyttöä. Tämä voidaan toteuttaa Internet-selaimeen avautuvalla sivulla, jonka ehdot hyväksyttyään pääsee käyttämään verkkoyhteyttä tiedostettuaan, että yhteys muodostetaan salaamattomana.

Työn luotettavuus perustuu käytännössä kirjallisten lähteiden luotettavuuteen ja niiden oikeaoppiseen käyttöön. Tässä työssä käytetyt langattomia verkkoja käsittelevät kirjallisuuslähteet ovat pääasiassa 5-10 vuotta sitten julkaistuja, joten niissä ei ole kaikkein uusinta tietoa alan kehityksestä. Kuitenkin alkuperäiset 802.11-standardit on luotu vuosituhannen vaihteessa eikä sen jälkeen ole tapahtunut perustavanlaatuisia muutoksia teknologiassa. Voidaan siis perustellusti sanoa, että käytetyt lähteet ovat yhä luotettavia tällaisen käytännön toteutuksen kohdalla. Toki tuorettakin tietoa työssä on käytetty siellä missä sille on erikoisesti ollut tarvetta, kuten käytettyjen laitteiden ja protokollien tarkoissa teknisissä yksityiskohdissa.

Työn reliabiliteettia heikentää erityisesti kuuluvuusalueiden mittauksessa käytetty menetelmä, joka edellytti tulosten manipulointia käsin. Tällaista menetelmää on erittäin vaikea toistaa täysin samalla tavalla. Muuten työ on jokseenkin tavanomainen ”koulu-esimerkki” avoimen langattoman verkon toteutuksesta. Työstä voidaan ottaa mallia vastaavan verkon rakentamisessa ja vaikkapa valmiin verkon tutkimisessa ja kehittämisessä.

LÄHTEET

Anthony, S. 11.7.2013. What is 802.11ac WiFi, and how much faster than 802.11n is it? Luettu 16.4.2014. http://www.extremetech.com/computing/160837-what-is-802-11ac-and-how-much-faster-than-802-11n-is-it

Benton, K. 2010. The Evolution of 802.11 Wireless Security. UNLV School of Informatics. http://itffroc.org/pubs/benton_wireless.pdf

Cam-Winget, N., Housley, R., Wagner, D. & Walker, J. 2003. Security Flaws in 802.11 Data Link Protocols. Communications of the ACM 5/2003, 35-39. http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf

Geier, J. 2005. Langattomat verkot perusteet. Helsinki: IT Press.

Held, G. 2001. Data Over Wireless Networks: Bluetooth, WAP & Wireless LANs. McGraw-Hill.

Hewlett-Packard Company. 2011a. HP MSM765zl Mobility Controller Installation and Getting Started Guide.

Hewlett-Packard Company. 2011b. HP MSM7xx Controllers Management and Configuration Guide. Luettu 7.2.2014. http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c02704528-2.pdf

Hewlett-Packard Company. 2013. HP MSM-802.11n Dual Radio Access Point Series Quickspecs. Luettu 19.2.2014. http://h18000.www1.hp.com/products/quickspecs/13994_div/13994_div.pdf

Internet Engineering Task Force (IETF). 2009a. Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification. http://tools.ietf.org/html/rfc5415

Internet Engineering Task Force (IETF). 2009b. Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11. http://tools.ietf.org/html/rfc5416

Internet Engineering Task Force (IETF). 2010. Lightweight Access Point Protocol. http://tools.ietf.org/html/rfc5412

Juutilainen, M. 2007. Radiotekniikan perusteet: Signaalien eteneminen. Luento. Ti5312600 Siirtyvä tietoliikenne. Luettu 8.4.2014. http://www.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento03.pdf

Oksanen, V. 14.5.2012. Ylivieskan KO: Ei vastuuta WLAN:ista. Luettu 12.5.2014. http://www.turre.com/2012/05/ylivieskan-ko-ei-vastuuta-wlanista/

Perry, D. 2004. Sonicwall technical FAQ: SonicWALL PRO 2040. Luettu 22.2.2014. http://www.sonicwall.com/downloads/SonicWALL_PRO_2040_FAQ_.pdf

Pueblas, M., Gyurindak, S., Strika, J., Kachalia, R., Hamilton D. & Tenneti, S. 2010. Medium Enterprise Design Profile Reference Guide. Cisco Systems Inc. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/MEDP.pdf

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

Rajesh, K. 2010. Why is a Controller required in a wireless network. Luettu 4.1.2014. http://www.excitingip.com/673/features-of-todays-centralized-wireless-wi-fi-networks/

Ruetsch, L. 23.4.2013. What's The Difference Between IEEE 802.11ac And 802.11ad? Luettu 16.4.2014. http://mwrf.com/test-amp-measurement/what-s-difference-between-ieee-80211ac-and-80211ad

Stanford, M. 7.9.2007. How does 802.11n get to 600Mbps? Luettu 16.4.2014. http://www.wirevolution.com/2007/09/07/how-does-80211n-get-to-600mbps/

Strand, L. 18.8.2004. 802.1X Port-Based Authentication HOWTO. Luettu 7.4.2014. http://tldp.org/HOWTO/html_single/8021X-HOWTO/

Tampereen Särkänniemi Oy. 14.1.2014. Särkänniemeen ilmainen sisäänpääsy kesällä 2014. Lehdistötiedote. Luettu 24.2.2014. http://www.sarkanniemi.fi/fi/ajankohtaista/118-sarkanniemeen-ilmainen-sisaanpaasy-kesalla-2014

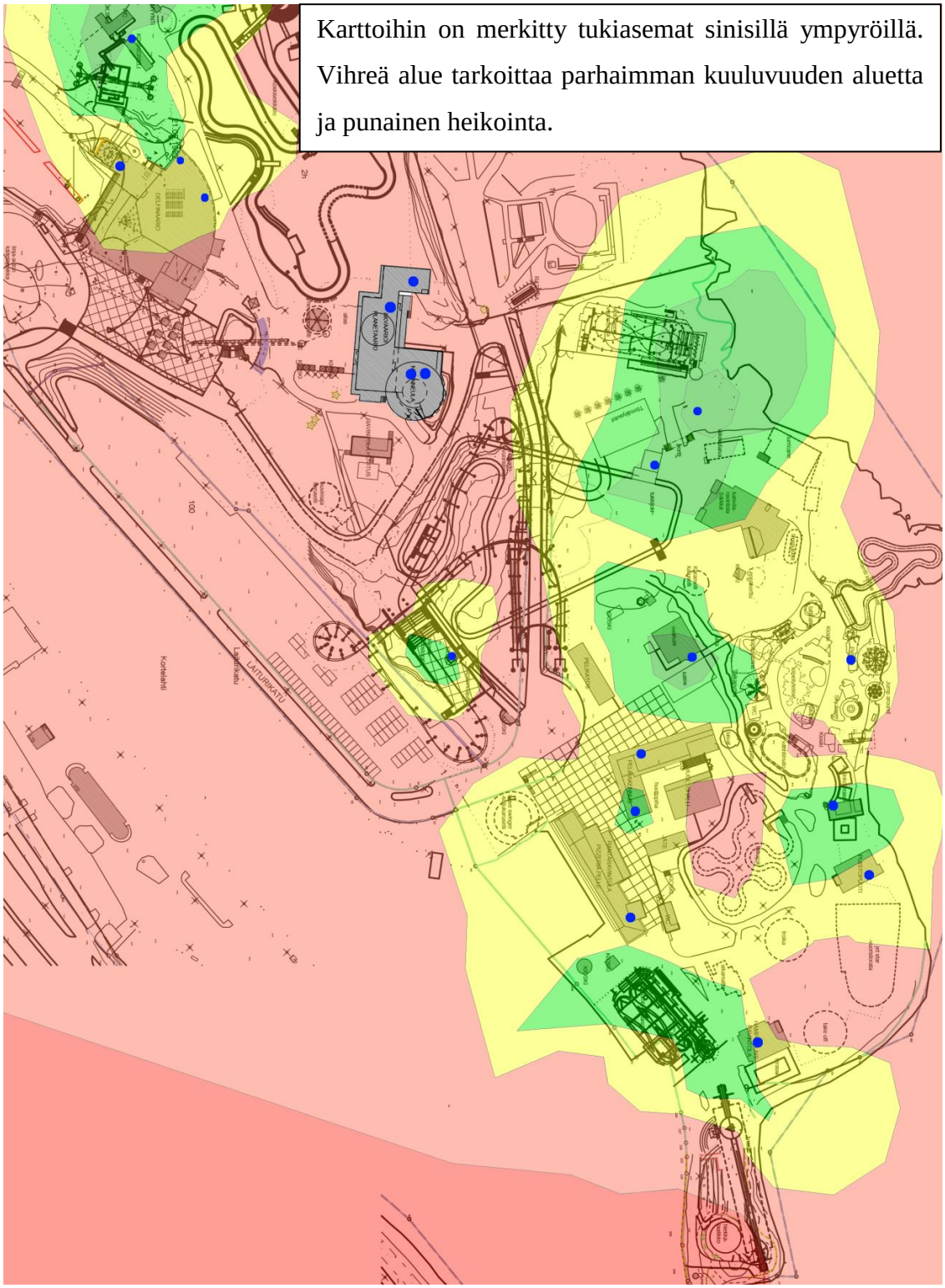
Tilastokeskus. 2012. Tieto- ja viestintätekniikan käyttö -tutkimus 2011. Luettu 7.1.2014. http://www.stat.fi/til/sutivi/2011/sutivi_2011_2011-11-02_fi.pdf

Van Nee, R. 2006. The 802.11n MIMO-OFDM Standard for Wireless LAN and Beyond. Luettu 1.4.2014. http://www.cs.odu.edu/~nadeem/classes/cs795-WNS-S13/papers/11n-006.pdf

LIITTEET

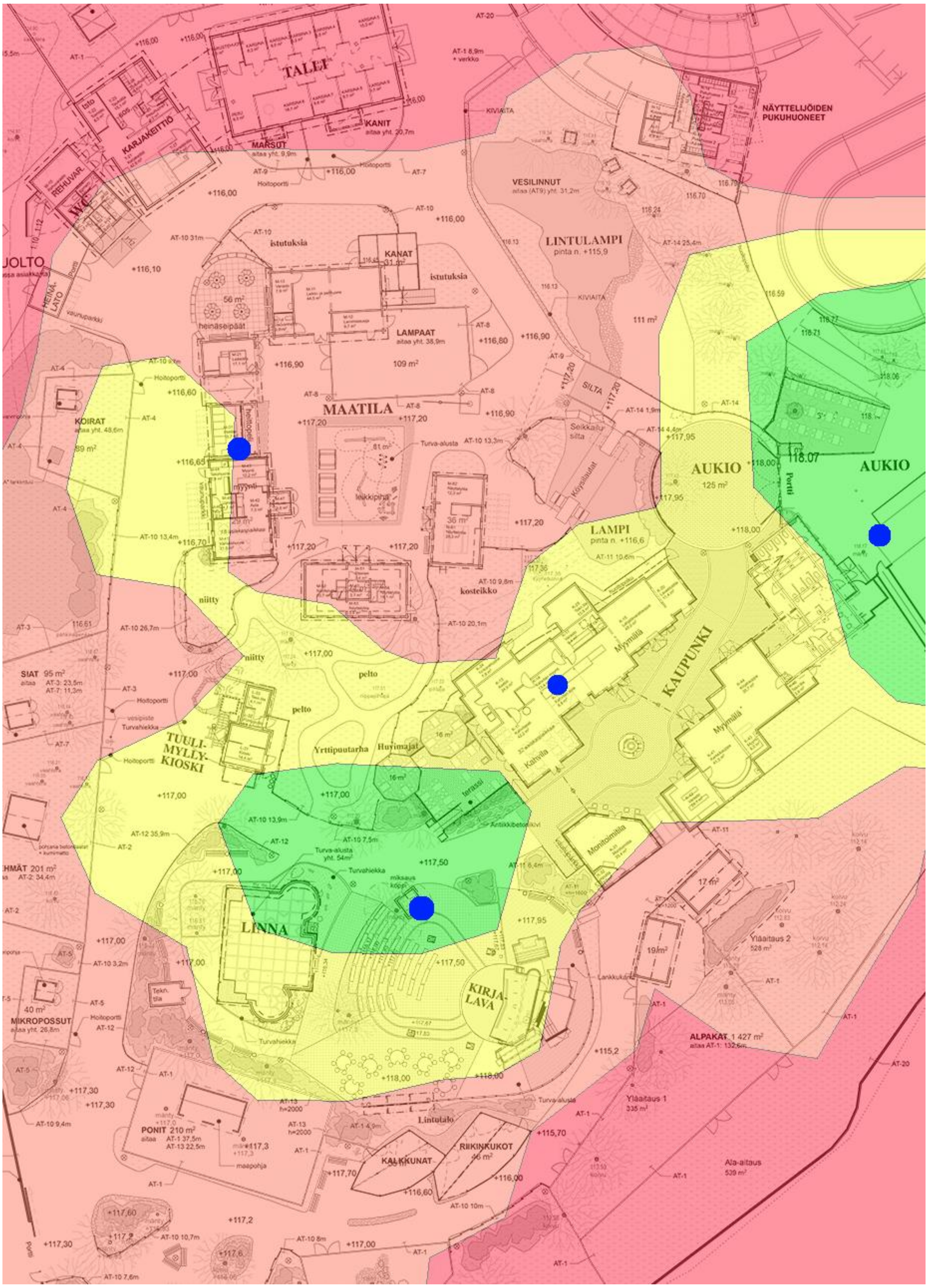
Liite 1. Sarkka Open-verkon peitto: huvilaitealue ja Koiramäki

1 (2)



(jatkuu)

2 (2)


TALLI
KANIT
MARSUT
KARJAKEITTIÖ
REHUVAR.
WC
NÄYTTELIJÖIDEN PUKUHUONEET
VESILINNUT
LINTULAMPI
KANAT
istutuksia
LAMPAAT
MAATILA
KOIRAT
SILTA
AUKIO
AUKIO
LAMPI
KAUPUNKI
leikkipiha
kosteikko
niitty
pelto
SIAT
TUULI-MYLLY-KIOSKI
Yrttipuutarha
Huvimajat
LINNA
KIRJA-LAVA
MIKROPOSSUT
PONIT
Lintutalo
KALKKUNAT
RIIKINKUKOT
ALPAKAT