KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikka / tietoliikennetekniikka

Juho-Miika Halonen

KESKITETYSTI HALLITTAVAN LANGATTOMAN VERKON SUUNNITTELU

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Elektroniikan koulutusohjelma

HALONEN, JUHO-MIIKA	Keskitetysti hallittavan langattoman verkon suunnittelu
Insinöörityö	48 sivua
Työn ohjaaja	Yliopettaja Martti Kettunen, lehtori Jouko Pahlama
Toimeksiantaja	Cursor Oy
Huhtikuu 2010	
Avainsanat	WLAN, langattomat lähiverkot, DHCP, WLC, lähiverkot, langaton tekniikka

Langattomien verkkojen kehityttyä yhä nopeammiksi ja turvallisemmiksi on niiden hyödyntäminenkin lisääntynyt vuosi vuodelta. Langattomien verkkojen avulla voidaan laajentaa tietoverkkoa suurelle alueelle yhdellä kertaa ja hyödyntää erilaisten päätelaitteiden liikuteltavuutta.

Opinnäytetyön alkuperäisenä tavoitteena oli rakentaa langaton lähiverkko digitaalisen liiketoiminnan keskuksen Datariinan kokous- ja koulutustiloihin. Opinnäytetyön edetessä tavoite muuttui pelkäksi suunnittelutyöksi ja varsinaisen langattoman lähiverkon rakentaminen jäi toteuttamatta.

Työ alkoi Datariinan aiempien langattomien verkkojen kartoituksella, jonka pohjalta suunniteltiin uusien tukiasemien sijoittaminen kartoitetulle alueelle. Kartoitukseen käytettiin kannettavaa tietokonetta, johon oli asennettu NetStumbler-ohjelma.

Suunnittelua ja testausta varten tietoverkkolaboratorioon rakennettiin kytkentä, johon kuuluivat Ciscon WLAN-kontrolleri, Linux-pohjainen DHCP-palvelin ja WLAN-tukiasemat. Laitteiden konfiguroimisessa ja tukiasemien sijoituspaikkojen valinnassa olivat apuna aiheeseen liittyvä kirjallisuus ja internet-sivustojen materiaali. Opinnäytetyön raporttiin sisältyy Ciscon WLAN-kontrollerin ja LAP-tukiasemien vaatiman DHCP-palvelimen käyttöönotto ja asetusten määrittäminen. Mukana ovat myös Datariinan ensimmäisen kerroksen ja kellarikerroksen aiempien langattomien verkkojen kartoituksen tulokset sekä suunnitelma uusien tukiasemien sijoittamisesta. Lisäksi suunniteltiin varsinaiseen toteutukseen käytettäväksi tulevaa laitteistoa ja selvitettiin laitteiston kustannukset.

Opinnäytetyön tuloksena todettiin langattoman verkon rakentaminen toteuttamiskelpoiseksi, mutta ennen hankkeen toteuttamista on vielä tehtävä kuuluvuusmittauksia väliaikaisesti sijoitetuilla tukiasemilla ja tämän jälkeen selvitettävä tarkemmin laitteiston määritykset.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Electronics

HALONEN, JUHO-MIIKA	Plan for a centrally managed wireless network
Bachelor's Thesis	48 pages
Supervisor	Martti Kettunen, Principal Lecturer
	Jouko Pahlama, Senior Lecturer
Commissioned by	Cursor Oy
April 2010	
Keywords	WLAN, DHCP, WLC, wireless technology

As wireless networks develop to be even faster and safer than before, their utilization has increased year after year. With the help of wireless networks you can easily expand a network to cover an extensive area and benefit from data terminal equipment's mobility.

The original aim of this Bachelor's thesis work was to build a wireless network in the conference and education premises of the digital business operation centre Datariina. As the thesis work progressed the aim was changed to merely designing the network and the actual construction was not carried out.

This thesis work started with the mapping of the earlier wireless networks of Datariina, which were used as the basis to decide the places of the access points. The mapping of the wireless networks was carried out with a portable computer and the NetStumbler analysis program.

A network was built for testing purposes in the networking laboratory. It consisted of a Cisco WLAN controller, a Linux based DHCP server and WLAN access points. Subject related literature and various sources on the internet helped the author to configure the DHCP server and map the wireless networks. This thesis includes a report on the implementation and setting up of the DHCP server required by the Cisco WLAN controller and the lightweight access points. The mapping results of the earlier excisting wireless networks of Datariina and a plan for the placement of the new access points are also included. In addition, the hardware for the actual implementation and the hardware costs are given in this paper.

Based on the study results, the construction of the wireless network was found feasible, but coverage measurements with temporarily placed access points will have to be done before the implementation. The results of those measurements will determine the hardware configuration in detail.

SISÄLLYS

LYHENNELUETTELO

AES	Advanced Encryption Standard, salausalgoritmi
ASCII	American Standard Code for Information Interchange, merkistö
AP	Access Point, tukiasema
BPSK	Binary Phase Shift Keying, modulointitekniikka
BSS	Basic Service Set, peruspalveluverkko
CAPWAP	Control and Provisioning of Wireless Access Points protocol, WLC-kontrollerien ja LAP-tukiasemien välisessä kommunikoinnissa käytettävä protokolla
CCK	Complementary Code Keying, modulaatiotekniikka
CRC	Cyclic Redundancy Check, tiivistealgoritmi
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
CTS	Clear to Send, lähetysluvan myöntäminen
DBPSK	Differential Binary Phase Shift Keying, modulointitekniikka
DHCP	Dynamic Host Configuration Protocol, IP-osoitteenjakoprotokolla
DMT	Discrete Multi-Tone, modulointitekniikka
DNS	Domain Name System, nimipalvelujärjestelmä
DoS	Denial of Service, palvelunestohyökkäys

DS	Distribution System, jakelujärjestelmä, runkoverkko
DSL	Digital Subscriber Line, verkkokytkintekniikka
DSSS	Direct-Sequence Spread Spectrum, modulaatiotekniikka
DQPSK	Differential Quadrature Phase Shift Keying, modulointitekniikka
EAP	Extensible Authentication Protocol, tunnistusprotokolla
ESS	Extended Service Set, laajennettu palveluverkko
FHSS	Frequency-Hopping Spread Spectrum, modulaatiotekniikka
IAPP	Inter Access-Point Protocol, tukiasemien välinen protokolla
IBSS	Independent Basic Service Set, itsenäinen palveluverkko
IEEE	the Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
IETF	Internet Engineering Task Force, internet-protokollien standardoinnista vastaava järjestö
IP	Internet Protocol, internetprotokolla
ISC	Internet Systems Consortium, standardointijärjestö
ISM	Industrial, Scientific & Medical, vapaasti käytettävä taajuusalue
ISO	The International Organization for Standardization, kansainvälinen standardoimisjärjestö
LAN	Local Area Network, lähiverkko
LAP	Lightweight Access Point, tukiasema

LWAPP	Lightweight Access Point Protocol, WLC-kontrollerien ja LAP-tukiasemien välisessä kommunikoinnissa käytettävä protokolla
MAC	Media Access Control, pääsykerros siirtotielle
Mbit/s	Megabits per second, megabittiä sekunnissa
MIC	Message Integrity Control, eheystarkistus
MIMO	Multiple-input multiple-output, monilähetintekniikka
MPDU	MAC Protocol Data Unit, MAC-tietosähke
NSA	National Security Agency, kansallinen turvallisuusvirasto
OFDM	Orthogonal Frequency-Division Multiplexing, kantoaaltomodulointi
OSI	Open Systems Interconnection, tietoliikenteen referenssimalli
OTAP	Over-the-Air Provisioning, LAP-tukiaseman WLC-kontrollerin löytämistekniikka
PMK	Pair-wise Master Key, parittainen pääavainpari
PoE	Power over Ethernet, käyttöjännitteen syöttäminen parikaapelin avulla
PSK	Pre-Shared Key, ennalta määritelty salasana
PHY	Physical Layer, fyysinen kerros
PN	Pseudo-Noise, valesatunnaiskohina
QAM	Quadrature amplitude modulation, modulointitekniikka
QoS	Quality of Service, tietoliikenteen luokittelu ja priorisointitekniikka
QPSK	Quadrature Phase Shift Keying, modulaatiomenetelmä

RC4	Ron’s Code 4, Rivest Cipher 4, jonosalaus
RRM	Radio Resource Management, radiotaajuuksien ja lähetystehojen hallinta
RTS	Request to Send, lähetysluvan anominen
SNR	Signal-to-noise ratio, signaali-kohinasuhde
SSID	Service Set Identifier, WLAN-verkon muunnettavissa oleva tunnus
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla
U-NII	Unlicensed National Information Infrastructure, vapaasti käytettävä taajuusalue
VCI	Vendor Class Identifier, valmistajan/toimittajan tunniste
VM	Virtual Machine, virtuaalitietokone
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

Langattomien verkkojen suurimpana ongelmana on ollut pitkään heikko tietoturva, ja lisäksi siirtotienä käytetään radiokerrosta, joka on fyysisesti avoin kaikille. Edellä mainituista syistä siirtyminen langattomien verkkojen käyttöön yrityksissä on ollut hidasta. Suojauskäytäntöjen kehityttyä ovat myös yritykset siirtyneet käyttämään tätä ratkaisua, vaikka tiedonsiirtonopeudet eivät vedä vertoja perinteiselle kiinteälle verkolle. Monien etujen ansiosta houkutus siirtyä käyttämään langattomia ratkaisuja on kuitenkin suuri. Esimerkiksi kokoustiloissa pääsy verkkoon tai internetiin kannettavalla tietokoneella helpottuu huomattavasti, kun mahdollinen kaapeloinnin puuttuminen ei ole enää esteenä yhteyden muodostamiselle, vaan yhteys voidaan muodostaa langattomasti.

Tässä opinnäytetyössä keskityttiin langattoman lähiverkon rakentamisen suunnitteluun Cursor Oy:lle digitaalisen liiketoiminnan keskuksen Datariinan kokoustiloihin. Suunnittelu tehtiin opinnäytetyönä. Alun perin tavoitteena oli suunnitella ja rakentaa langaton lähiverkko Datariinan kokous- ja koulutustiloihin. Työn edetessä tavoite muuttui pelkäksi suunnittelutyöksi ja varsinaisen langattoman lähiverkon rakentaminen jäi toteuttamatta.

Työ alkoi kartoittamalla Datariinan aiemmat langattomat verkot ja kartoituksen tulosten avulla suunniteltiin uusien tukiasemien sijoittaminen. DHCP-palvelimen testausta varten rakennettiin kytkentä koulun tietoverkkolaboratorioon. Lisäksi suunniteltiin varsinaiseen toteutukseen käytettäväksi tulevaa laitteistoa eri vaihtoehtoineen ja kustannuksineen.

Työn kuluessa tutustuttiin langattoman verkon toimintaan ja standardiin sekä Cisco LAP -tukiasemia tukevan DHCP-palvelimen konfiguroimiseen. DHCP-palvelimen konfiguraatiota tehtäessä suurimmat ongelmat olivat Linuxin käytön vaikeus aloittelijalle sekä option 43- ja 60 -vaihtoehtojen konfiguroiminen toimivaksi kokonaisuudeksi. Lisäksi tukiasemien kanavasuunnittelu osoittautui haastavaksi tehtäväksi.

2 LANGATTOMAT LÄHIVERKOT

Langattomien lähiverkkojen historia alkoi 1980-luvun puolivälissä, kun Motorola esitteli Altair-nimisen tuotteensa. Kuten kaikki muutkin 80- ja 90-lukujen tuotteet oli myös Altair valmistajakohtainen, joten tekniikan käyttäjät joutuivat sitoutumaan yhteen toimittajaan. IEEE-järjestön standardointiryhmä aloitti langattoman lähiverkon standardin kehittämisen vuonna 1990 ja vuonna 1997 julkaistiin 802.11-standardin ensimmäinen versio, joka tuki nopeuksia 1 ja 2 Mbit/s. Parannettu 802.11b-standardi julkaistiin vuonna 1999 ja se nosti bittinopeuden 11 Mbit/s asti. Näitä ovat seuranneet vielä kolme muuta laajennusta: IEEE 802.11a-, IEEE 802.11g- ja IEEE 802.11n -standardit. [1] [2]

2.1 Langattomien lähiverkkojen edut

Langattomien lähiverkkojen kaapeloinnin tarve on vähäisempi langalliseen verkkoon verrattuna. Se pienentää käyttöönoton kustannuksia sekä helpottaa verkon rakentamista ja laajentamista. Käyttäjät voivat muodostaa yhteyden koko langattoman verkon alueella, eikä yksittäinen käyttäjä ole sidottu samaan paikkaan kuten langallisissa verkoissa. Kannettavalle tietokoneelle voidaan tarjota pääsy langattoman verkon kautta samoihin palveluihin kuin kiinteän työpisteen tietokoneelle. Erilaisissa kohteissa, kuten varastoissa ja sairaaloissa, voidaan kirjata tietoja langattomasti niitä ylläpitävälle palvelimelle. Jos tukiasemien peittoalueet on rakennettu osittain päällekkäisiksi, käyttäjät voivat liikkua roaming-tekniikan avulla langattoman verkon alueella vapaasti ilman yhteyden katkeamista. [1] [3] [4]

2.2 IEEE 802.11 -standardit

Suomessa saa käyttää vapaasti taajuuksilla 2,4 GHz ja 5 GHz toimivia langattomia verkkoja, jos laitteet täyttävät standardien määräykset eikä sallittuja lähetystehoja ylitetä. Langattomien laitteiden valmistaja tai maahantuoja huolehtii testauksesta ja vastaa, että laitteet ovat standardien mukaisia. [1]

Taulukko1. IEEE 802.11 -standardit [1]

Standardi	Ratifioitu	Hajaspektri-tekniikka	Teoreettinen bittinopeus	Taajuusalue	Kanavia yhteensä	Ei-päällek. kanavia
802.11	1997	FHSS, DSSS	1 ja 2 Mbit/s	2,4 GHz	14	3
802.11b	1999	DSSS	1, 2, 5,5 ja 11 Mbit/s	2,4 GHz	14	3
802.11a	1999	OFDM	6-54 Mbit/s	5 GHz	12	12
802.11g	2003	OFDM	1-54 Mbit/s	2,4 GHz	12	3
802.11n			250+ Mbit/s	5 ja 2,4 GHz		

2.2.1 802.11-standardi

802.11 on alkuperäinen IEEE:n kehittämä ja vuonna 1997 hyväksytty WLAN -standardi, joka aloitti langattomien verkkojen nopean tuotekehityksen. 802.11-standardi määritteli OSI-mallin fyysisen kerroksen ja siirtoyhteyskerroksella sijaitsevan MAC-tason. Nimelliset siirtonopeudet ovat 1 Mbit/s DBPSK-moduloinnilla ja 2 Mbit/s DQPSK-moduloinnilla 2,4 GHz ISM -alueella. Kuuluvuus on olosuhteista riippuen sisätiloissa noin 50 – 180 metriä ja ulkotiloissa jopa yli 300 metriä. [2] [3]

2.2.2 802.11b-standardi

802.11b on vuonna 1999 hyväksytty laajennus 802.11-standardiin. Se sisältää neljä nopeusluokkaa ja huonoissa olosuhteissa nopeutta voidaan pudottaa alkuperäisen standardin nopeusluokkiin 1 ja 2 Mbit/s, joissa käytetään DBPSK- ja DQPSK-modulointia. Nämä nopeusluokat yhdessä taajuuden 2,4 GHz kanssa mahdollistavat yhteensopivuuden alkuperäisen standardin kanssa. Korkeammille nopeusluokille 5,5

ja 11 Mbit/s käytetään CCK-modulointia. Kuuluvuus sisätiloissa on noin 50 – 180 metriä, sekä ulkotiloissa jopa yli 300 metriä. [2] [3]

2.2.3 802.11a-standardi

Vuonna 1999 julkaistiin fyysisellä kerroksella tapahtuva laajennus 802.11-standardiin, eli 802.11a-standardi. Standardi sisältää kahdeksan eri nopeusluokkaa ja käyttää 5 GHz U-NII -aluetta. BPSK-modulointia käytetään nopeuksien 6 ja 9 Mbit/s ja QPSK-modulointia nopeuksien 12 ja 18 Mbit/s hyötykuormalle. 16QAM-modulointia käytetään nopeuksien 24 ja 36 Mbit/s ja 64QAM-modulointia nopeuksien 48 ja 54Mbit/s hyötykuormalle. Standardin heikkoutena on ollut pieni, noin 80 metrin kuuluvuus, jonka alueella yhteyden nopeus putoaa alueen reunaa kohti mentäessä. Yhteensopivuuden kannalta haittapuolena on eri taajuusalue kuin 802.11b- ja 802.11g-verkoissa. [2] [3] [5]

2.2.4 802.11g-standardi

Kesäkuussa 2003 julkistettu laajennus 802.11g käyttää 2,4 GHz ISM -aluetta. Sisältää kaksitoista eri nopeusluokkaa, joista nopeusluokille 1, 2, 5,5 ja 11 Mbit/s käytetään CCK-modulointia ja nopeusluokille 6, 9, 12, 18, 24, 36, 48 ja 54 Mbit/s käytetään OFDM-modulointia. Todellinen tiedonsiirtonopeus on kuitenkin noin 20 Mbit/s. CCK-modulointia käytetään taaksepäin yhteensopivuuden kannalta, millä saavutetaan yhteensopivuus 802.11b-standardin kanssa. Kuuluvuus on olosuhteista riippuen sisätiloissa noin 50 – 180 metriä ja ulkotiloissa jopa yli 300 metriä. [3] [5]

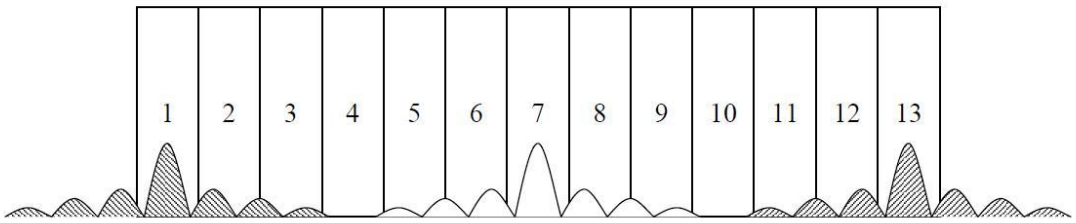
2.2.5 802.11n-standardi

Seitsemän vuotta kehitteillä ollut 802.11n-standardi julkaistiin syyskuussa 2009 ja se sisältää useita parannuksia fyysiseen ja MAC-kerrokseen. Suurin parannusta tuova lisäys on MIMO-tekniikka, joka lisää nopeutta ja luotettavuutta. MIMO-tekniikka hyödyntää signaalien monimuotoisuutta ja päällekkäisyyksiä käyttämällä useaa lähetys- ja vastaanottoantennia samanaikaisesti. Toinen parannus on vierekkäiset kanavat yhteen sitova 40 MHz toiminta, jolla saavutetaan yli kaksinkertainen tiedonsiirtonopeus. Kolmantena on kehysten yhdistäminen, joka lisää suoritustehoa yhdistämällä useita paketteja. 802.11n-standardi kehitettiin minimoimaan häiriöitä, optimoimaan tiedonsiirtoväyliä ja parantamaan langattomien laitteiden herkkyyttä. [6] [7]

Edellisten parannusten ansiosta 802.11n-standardi kykenee todelliseen tiedonsiirtonopeuteen 160 Mbit/s ja 90 metrin päässä tukiasemasta jopa teoreettiseen nopeuteen 70 Mbit/s. 2,4 GHz ISM- ja 5 GHz U-NII -alueita käyttävä 802.11n-standardi on yhteensopiva vanhempien langattomien verkkostandardien kanssa, joka mahdollistaa liukuvan siirtymisen uuteen standardiin. [6] [7]

2.3 ISM-alueen kanavat

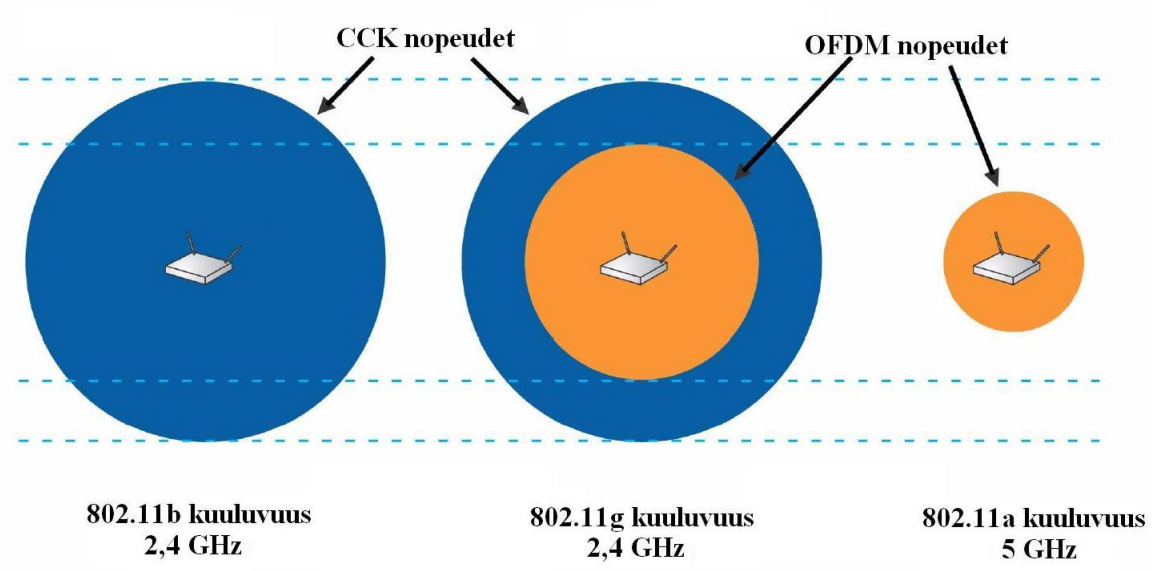
Tiedonsiirrossa käytettävä 2,4 GHz ISM -alue on Euroopassa jaettu 13 kanavaan, jotka menevät osittain päällekkäin. Lähekkäin sijaitsevat ja viereisillä kanavilla tietoa siirtävät tukiasemat häiritsevät toisiaan. Ainoastaan kanavat 1, 7 ja 13 ovat täysin eri taajuusalueella ja toimivat vierekkäin ilman häiriöitä. Käytännössä kuitenkin kaksi käyttämätöntä kanavaa riittää lähekkäin sijaitsevien laitteiden väliin, eli siis kanavat 1, 5, 9 ja 13 sekä jopa kanavat 1, 4, 7, 10 ja 13 ovat käyttökelpoisia, kun tukiasemat on sijoitettu hyvin. [3]



Kuva 1. 2,4 GHz ISM -alueen kanavat [3]

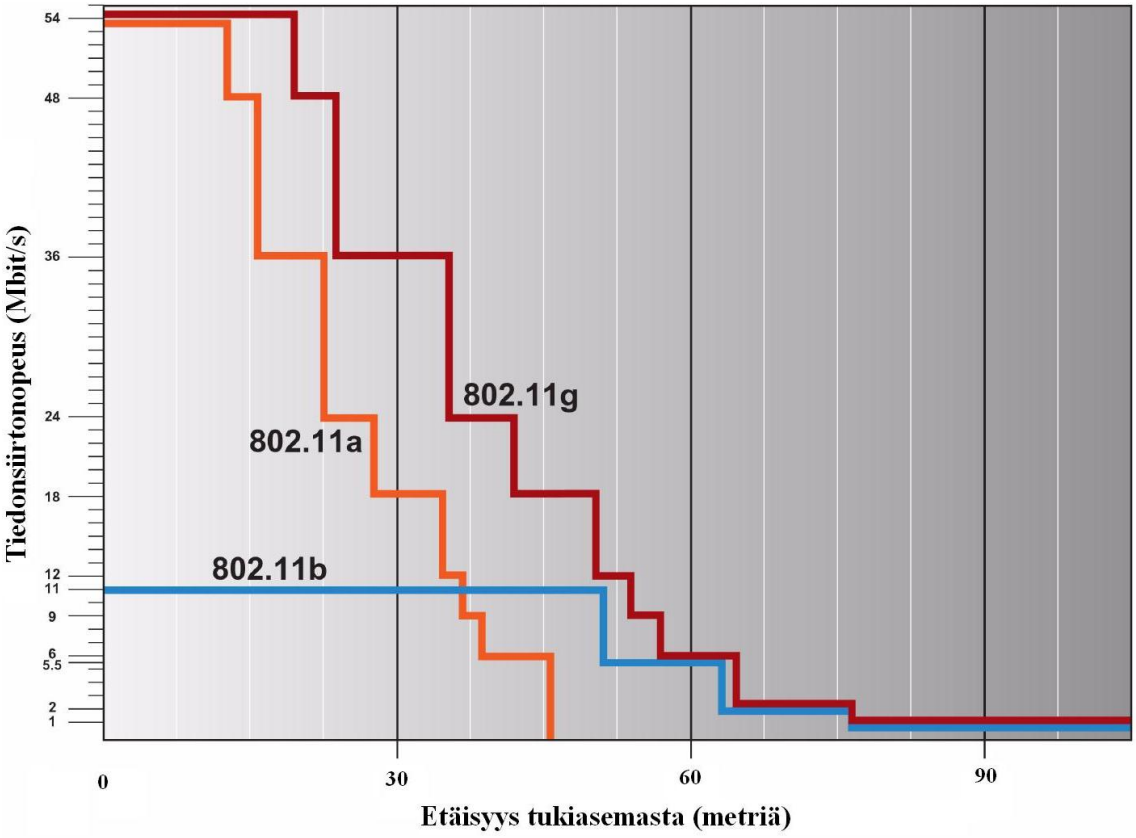
2.4 Kuuluvuus

Kuvassa 2 on esitetty 802.11b-, 802.11g- ja 802.11a-standardien suhteelliset kuuluvuudet. Kuvasta näkee että 2,4 GHz kaistaa käyttävien 802.11b- ja 802.11g-standardien kuuluvuudet ovat samat, kun taas 802.11a-standardin kuuluvuus on korkeammasta taajuudesta johtuen huomattavasti pienempi. Matalamman taajuutensa ansiosta 802.11g-standardi kykenee OFDM-moduloinnilla parempaan kuuluvuuteen kuin 802.11a-standardi. [5]



Kuva 2. 802.11b/g/a-laitteiden suhteelliset kuuluvuudet (muokattu) [5]

Etäisyyden kasvaessa langattoman verkon asiakkaan ja tukiaseman välillä nopeutta pudotetaan yhteyden pysyvyyden takaamiseksi (kuva 3.). Tukiasemasta kauemmas siirryttäessä 802.11g- ja 802.11b-standardit tuottavat lähes saman nopeuden samalla etäisyydellä, mutta lähemmäs mentäessä 802.11g-standardi on huomattavasti nopeampi kuin 802.11b. 802.11a-standardin tuottama kuuluvuus muihin standardeihin verrattuna on suppea ja sen tiedonsiirtonopeus putoaa myös nopeammin. 802.11n-standardi on omassa luokassaan ja se kykenee olosuhteista riippuen jopa nopeuksiin 70 Mbit/s 90 metrin päässä tukiasemasta. [6] [7]



Kuva 3. Odotettavissa olevat tiedonsiirtonopeudet etäisyyden mukaan (muokattu) [5]

3 TIETOTURVA

Tietoturva on ollut langattomien verkkojen heikkous ja hidastanut langattomien toteutusten yleistymistä huomattavasti. Riittävän tietoturvan toteuttaminen ja varmistaminen on jatkuvaa työtä ja tietoturvan toteutus voidaan pilata esimerkiksi heikolla salasanalla tai muulla huonosti valitulla muuttujalla. [1]

Tunnistusta tarvitaan rajaamaan verkkoon pääsyä niin, että asiattomilta on pääsy kokonaan kielletty ja muilla on pääsy vain heille tarpeellisiin verkon palveluihin. Verkon langattomuus tuo uhkiin uusia painotuksia, murtautumiskeinoja ja yrittäjiä, mutta pääosin langattomien lähiverkkojen uhat ovat kuitenkin samoja kuin langallisissa tietoverkoissa. [1]

3.1 Salausmenetelmät

Langattoman lähiverkon tieto kulkee radiosignaaleilla, eikä niiden etenemistä voida rajoittaa ja ilman kunnollista salausta langattoman lähiverkon sisältö on kuultavissa

jopa rakennuksen ulkopuolelta. Jotta langaton verkko ei olisi altis väärinkäytölle, tarvitaan riittävää salausta. [1]

3.1.1 WEP-salaus

WEP-salaus on suunniteltu varmistamaan, ettei langattoman verkon tietoturva ole huonompi kuin lankaverkon. WEP-salaus tarjoaa jonkinasteista suojaa kotikäyttäjälle, jolloin salaus kertoo, että langaton verkko on yksityinen ja että asiaton verkkoon tunkeutuminen on rikos. [4] [8]

Alun perin salaus käytti 40 bitin jaettua avainta, mutta myöhemmin salausavaimen pituutta nostettiin 104 bittiin. Nykyään salausavain on joko 64- tai 128-bittinen ja muodostuu salaisesta avaimesta ja alustusvektorista. Salainen avain on joko 40 tai 104 bittiä ja alustusvektori 24 bittiä. WEP-salauksessa käytetään RC4-suojausalgoritmia salaamaan ja purkamaan langattoman verkon liikennettä. Datan korruptoituminen estetään CRC-32-tarkistussummalla, jonka avulla paketin vastaanottaja voi varmistua tiedon aitoudesta. [4] [8]

Salaus on murrettavissa kuuntelemalla verkon liikennettä ja laskemalla liikenteen perusteella verkon salausavain. Salauksen murtaminen kestää sitä kauemmin, mitä vähemmän liikennettä langattomassa verkossa on, koska siihen tarvitaan useita paketteja. WEP-salaus ei suojaa verkkoa vakavalta murtautujalta, joten parempaa tietoturvatasoa haluttaessa on käytettävä jotain muuta ratkaisua. [3] [4] [8]

3.1.2 WPA-salaus

WPA-salaus kehitettiin parantamaan langattoman verkon tietoturvaa ja se sisältää useita parannuksia tietoturvatasoon. WPA-salauksessa salausavain vaihtuu automaattisesti 10 000 paketin välein. TKIP-protokollaa käytetään salaamaan yhteydet, mikä parantaa huomattavasti tietoturvaa, sillä se käyttää pakettikohtaisia salausavaimia. TKIP-protokollassa on käytössä RC4-salausmenetelmä, mutta sitä on parannettu nostamalla salausavaimen pituus 128 bittiin ja alustusvektorin pituus 48 bittiin. WPA-salausta on myös parannettu WEP-salaukseen verrattuna niin, että se salaa koko paketin tiedot, kun WEP-salaus jättää otsikot salaamatta. WPA-salaus sisältää myös MIC-toiminnon, jonka avulla hallitaan ja tarkistetaan pakettien eheys. MIC-toiminto suori-

tetaan vahvan matemaattisen yhtälön avulla, jossa vastaanottaja ja lähettäjä laskevat toisiinsa verrattavat tarkistesummat, joilla todetaan paketin eheys. [3] [8]

Käyttäjän tunnistautuessa langattomaan verkkoon RADIUS-kirjautumispalvelin tai tukiasema luo ainutlaatuisen PMK-pääavainparin istuntoa varten. TKIP-protokolla antaa käyttäjälle avaimen, sekä luo avainhierarkian ja dynaamisten avainten hallintajärjestelmän. Pakettikohtaiset avaimet luodaan TKIP-protokollalla kyseisen avaimen mukaan. [8]

WPA-salaus on suunniteltu käytettäväksi 802.1x-todennuspalvelimen kanssa, joka jakaa jokaiselle käyttäjälle erilaiset avaimet, mutta salausta voidaan käyttää myös jaetulla avaimella. WPA-PSK, eli jaetun avaimen todennustekniikka on suunniteltu langattomille koti- ja toimistoverkoille, joilla ei ole varaa tai tarvetta 802.1x-todennuspalvelimen laitteistoon, ohjelmistoon ja ylläpitoon. Jaettu avain voi koostua 8 – 64 kappaleesta ASCII- tai heksadesimaalimerkkejä. Kyseisellä tekniikalla tietoturvaa heikentäväksi ongelmaksi muodostuvat käyttäjien luomat heikot avaimet. Onkin suositeltua käyttää ainakin 14 satunnaisesta kirjaimesta koostuvaa avainta. Lisäksi avain pitää vaihtaa aina, kun verkon käyttäjä menettää oikeudet verkon käyttöön ja kun työasema, johon avain on laitettu, häviää. [8]

WPA-salauksen tapa suojautua DoS-hyökkäyksiltä sulkee langattoman verkon minuutiksi, kun hyökkäys havaitaan. Tällöin kaikki langattoman verkon käyttäjät menettävät yhteyden, mistä saattaa koitua vahinkoa langattoman verkon hyödyntäjille. WPA-salauksesta on löydetty myös tietoturva-aukko, joka muodostuu, kun tukiasemat lähettävät salausavaimen tietoja. Tietoturva-aukko ei kuitenkaan uhkaa ratkaisuja, joissa on käytössä 802.1x-standardin mukainen järjestely. [8]

3.1.3 WPA2-salaus

WPA2-salausta tehtäessä on pyritty korjaamaan tunnetut tietoturvaongelmat. Siinä on määritelty 802.1x-standardin mukaiset todennuskäytännöt ja dynaamisten avainten hallinnan käytännöt. Salausmenetelmiä on parannettu lisäämällä WPA-salauksen ratkaisujen lisäksi AES-lohkosalausmenetelmä. AES-salausmenetelmä vaatii erojensa takia RC4-salausmenetelmään verrattuna enemmän prosessointitehoa. AES-salausmenetelmä pystyy käyttämään eripituisia avaimia ja vaihtoehtoina ovat 128, 192 ja 256 bitin pituiset avainpituudet. NSA on todennut AES-salausmenetelmän riittävän

turvalliseksi USA:n hallituksen käytettäväksi luokittelemattoman materiaalin salaamiseen. [8]

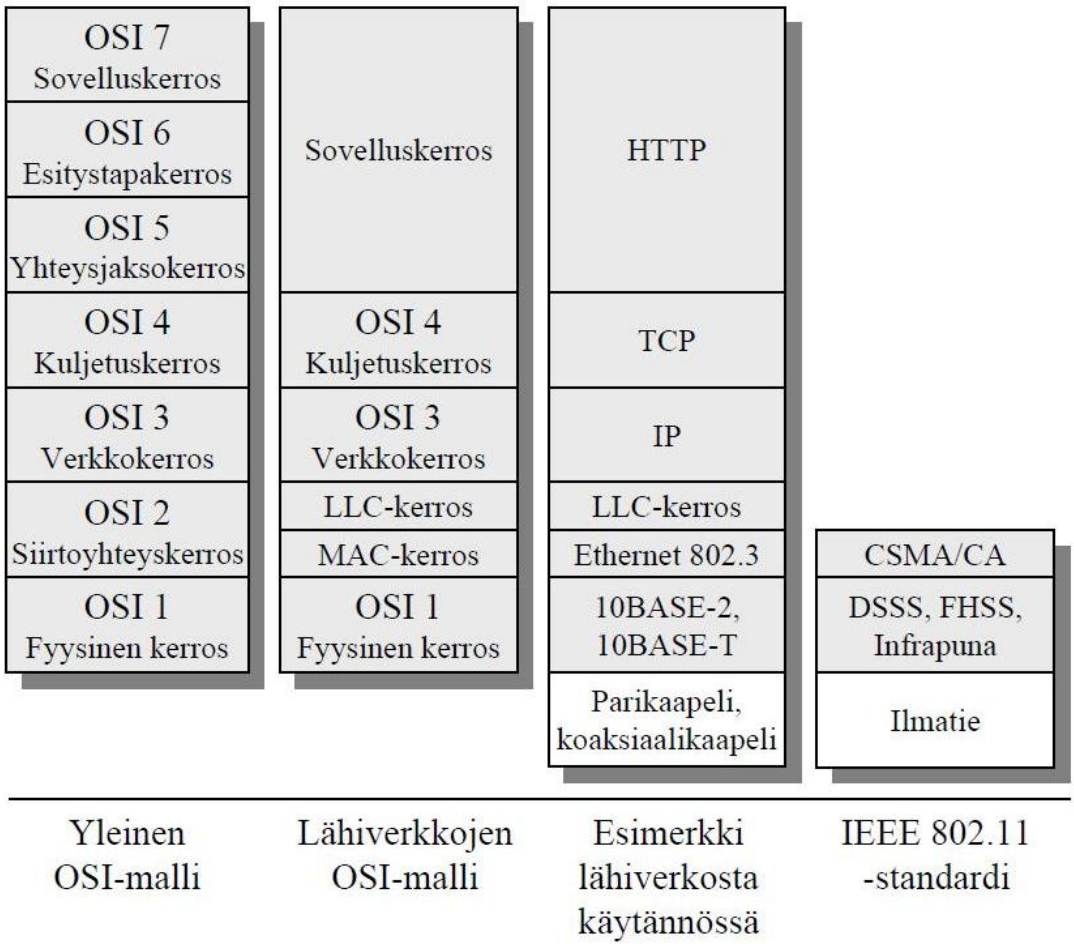
802.1x-standardi on porttipohjainen, LAN-portissa oleville laitteille tunnistuksen tarjoava standardi. Onnistuneen tunnistuksen jälkeen muodostetaan point-to-point-yhteys ja epäonnistuneen tunnistuksen jälkeen yhteys kyseisestä portista estetään. Tämä käytäntö on usein tukiasemissa käytössä ja se perustuu EAP-protokollaan. WPA- ja WPA2-salauksille on virallisesti hyväksytty viisi EAP-tyyppistä tunnistamismenetelmää. 802.1x-standardi käyttää WEP-salausta, mutta tästä huolimatta dynaaminen avainten hallinta vähentää altistumista avainhyökkäyksille ja molemminpuolinen tunnistus varmistaa, että työasemat viestivät tunnettujen verkkojen kanssa, joten langattoman verkon tietoturva lisääntyy huomattavasti. [8]

4 WLAN-VERKON RAKENNE

Langattomissa lähiverkoissa käytetään GSM-verkoista tuttua solurakennetta, jossa jokaisella solulla on oma taajuusalue, jolla solussa kommunikoidaan. Vierekkäisillä soluilla käytetään eri taajuuksia, jotta solut eivät häiritse toisiaan. Langattomissa lähiverkoissa solun muodostaa tukiasema, joka hallinnoi liikennettä. Langattoman verkkokortin sisältävillä päätelaitteilla otetaan yhteys tukiasemaan, josta liikenne kulkee runkoverkkoa pitkin tavoiteltavaan kohteeseen. [2] [9]

4.1 OSI-malli

ISO-järjestön 1980-luvun alussa kehittämä OSI-malli jakaa tietoliikenneverkon tehtävät seitsemään eri kerrokseen. Kuvassa 4 on vasemmalta oikealle katsottuna yleinen OSI-malli, lähiverkkojen OSI-malli, esimerkki lähiverkosta ja IEEE 802.11 -standardi. IEEE 802.11 -standardiin kuuluu siirtoyhteyskerroksella sijaitseva CSMA/CA-kilpavaraustekniikka ja fyysisen kerroksen toteuttavat tekniikat. [3] [10]



Kuva 4. ISO-järjestön OSI-malli [3]

4.1.1 Fyysinen kerros

OSI-mallin fyysinen kerros tarjoaa ylemmällä kerroksella sijaitsevalle MAC-kerrokselle rajapinnan tiedonsiirtomediaan ja hoitaa varsinaisen verkon yli tapahtuvan signaloinnin. Fyysisen kerroksen toteuttamiseksi langattomissa verkoissa on neljä vaihtoehtoa: DSSS-, FHSS-, OFDM- ja infrapunatekniikka. DSSS- ja FHSS-hajaspektritekniikoissa signaali hajautetaan käytettävälle taajuuskaistalle, millä saavutetaan hyvä tiedonsiirron luotettavuus ja häiriöiden sieto. Hajaspektritekniikan avulla verkon kapasiteetti jakautuu automaattisesti käyttäjien kesken. [3] [9]

Suorasekvenssihajaspektritekniikassa (DSSS) signaali moduloidaan 22 MHz:n kaistalle sopivaksi limittämällä se tarkoitukseen sopivan PN-koodin avulla. Koodi lisää lähetettävien bittien määrää ja vastaanottaja demoduloi signaalin vastaavalla koodilla. Lähetyksessä käytettävä taajuuskaista on jaettu eri taajuuksilla oleviin kanaviin, joita on Euroopassa 13. DSSS-tekniikka tukee suurempia siirtonopeuksia kuin FHSS-tekniikka. [3] [9]

Taajuushyppelyhajaspektritekniikka (FHSS) hyppii sattumanvaraisesti taajuudesta toiseen ja lähettää lyhyen purskeen jokaisella taajuuskanavalla. Euroopassa FHSS-tekniikalla on 2,4 GHz:n kaistalla 79 kanavaa. FHSS-tekniikka on hyvin häiriösietoinen, koska yhdellä kanavalla viivytään vain hetki. Kanavavaihtojen tahdistus ja hyppyjen koordinointi tekevät tekniikasta MAC-kerrokselle vaativan, mistä seuraa, että FHSS-tekniikan hyötysuhde ei ole kovin hyvä ja maksiminopeus on vain 2 Mbit/s. Kolmea useampaa FHSS-tekniikkaa käyttävää järjestelmää ei pidä asentaa lähekkäin, koska silloin kahden järjestelmän hyppyjen taajuudet voivat mennä päällekkäin. [2] [3] [9]

OFDM-tekniikka jakaa datan useaksi analogiseksi signaaliksi ja lähettää signaalia samanaikaisesti usealla taajuuskanavalla. OFDM-tekniikka käyttää taajuuskaistan tehokkaasti hyväkseen sekä sillä on hyvä impulssimuotoisten ja monitie-etenemisestä johtuvien häiriöiden sietokyky. OFDM-tekniikka muistuttaa suurelta osin DSL-modeemeissa käytettävää DMT-tekniikkaa. [3] [9]

4.1.2 Siirtoyhteyskerros

LLC-kerros on osa OSI-mallin siirtoyhteyskerrosta ja sen tehtävä on tarjota palveluja verkkokerrokselle. Palvelut toteutetaan kehystämällä verkkokerroksen IP-paketti LLC-kehykseen, jonka otsikko sisältää protokollatunnukset ja ohjauskentän. [1]

MAC-kerros kuuluu OSI-mallin siirtoyhteyskerrokseen ja se kommunikoi fyysisellä kerroksella sijaitsevien protokollien kanssa. MPDU-kehys eli ns. MAC-tietosähke sisältää kehyksen ohjaustiedot, vuoronvarauksessa käytettävän varauksen keston, uudelleenjärjestelyssä tarvittavan sekvenssitiedon, radiotiellä käytetyt osoitteet ja virheettömyyden varmistavan tarkistussumman. Lisäksi MAC-kerros määrittelee kehysten väliset ajat sekä CSMA/CA-vuoronvarauksen. Kerroksen tehtäviä ovat langattoman siirtomedian hyödyntäminen, laitteiden liikkuvuuden mahdollistaminen ja virransäästöohjelmien toteuttaminen. [1] [3]

Lähiverkoista tuttua CSMA/CD-kilpavaraustekniikkaa muistuttavaa CSMA/CA-vuoronvaraustekniikkaa käytetään välttämään langattomassa verkossa tapahtuvaa liikenteen törmäystä. Liikenteen törmäykset johtuvat siitä, että kaksi langattomassa verkossa liikennöivää päätelaitetta kuulee tukiaseman, mutta etäisyyden vuoksi signaalin liikaa vaimetessa ne eivät kuule toisiaan. Tällaista tapausta kutsutaan piilevän aseman ongelmaksi (hidden node problem). [1] [3]

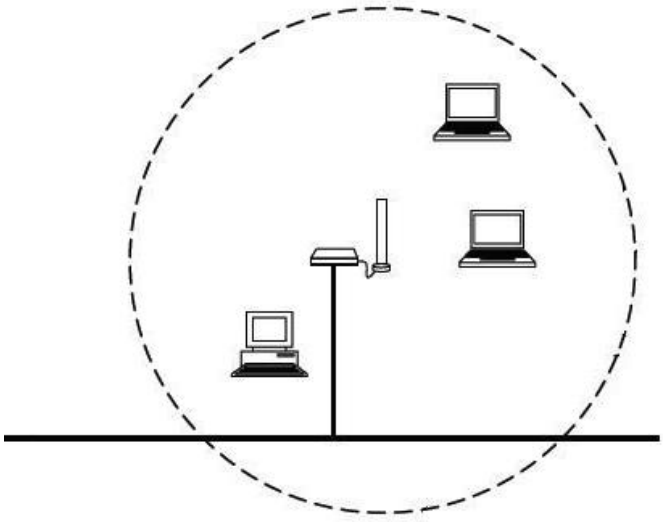
Tukiasema hallitsee siihen liittyneiden päätelaitteiden lähetysvuoroja CSMA/CA-vuoronvaraustekniikan avulla. Päätelaite anoo lähetyslupaa tukiasemalta RTS-sanomalla. Jos langaton verkko on liikenteeltä vapaa, vastaa tukiasema CTS-sanomalla ja antaa luvan lähetykselle sovituksi ajaksi. Langattomassa verkossa jokainen datakehys varmistetaan kuittaamalla ja vain yksi päätelaite voi liikennöidä kerrallaan. [1] [3]

4.2 Topologiat

Erilaiset langattomat topologiat eroavat toisistaan mm. tavassa, jolla langattomat laitteet kommunikoivat keskenään ja myös tukiasemien määrä vaihtelee eri topologioiden välillä. Langattomat verkot toimivat joko Ad Hoc-(IBSS) tai infrastruktuuritilassa (BSS ja ESS). [4]

4.2.1 BSS-verkko

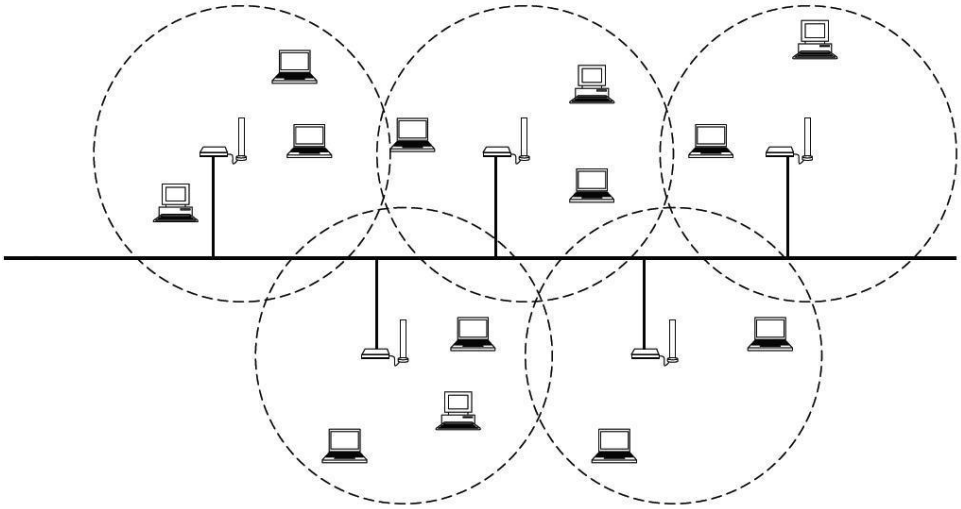
BSS-verkko on langattoman verkon perusarkkitehtuuri, joka koostuu vain yhdestä tukiasemasta ja siihen liitetyistä päätelaitteista. Kaikki tieto verkossa olevien laitteiden välillä liikkuu yhden tukiaseman kautta, joten BSS-topologia ei sovellu suuren käyttäjämäärän tarpeisiin, vaan sitä käytetäänkin kotiverkoissa ja pienissä yrityksissä. [2]



Kuva 5. Basic Service Set -verkko [3]

4.2.2 ESS-verkko

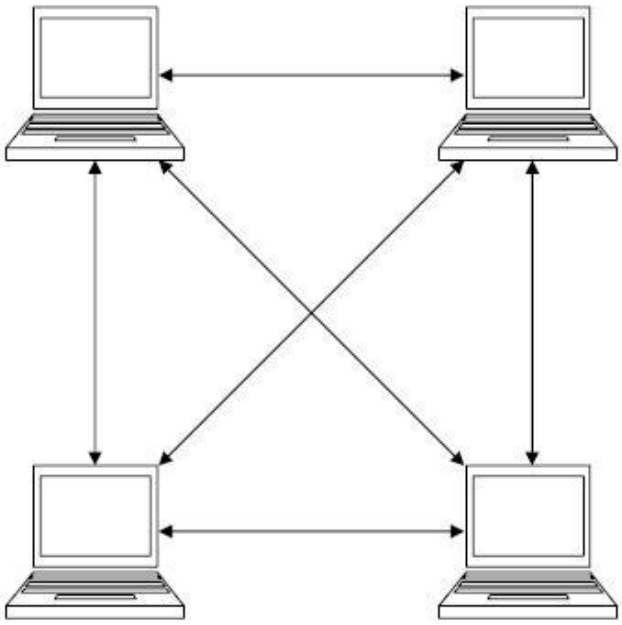
ESS-verkko on BSS-verkkoa laajempi ja koostuu useasta tukiasemasta, jotka kytketään samaan runkoverkkoon. ESS-verkkoja ovat kaikki kaksi tai useamman tukiaseman sisältävät langattomat verkot ja niiden käyttämästä runkoverkosta käytetään lyhennettä DS. ESS-topologiaa käytetään muodostamaan kattava langaton lähiverkko, joka kattaa monia huoneita ja jopa useita kerroksia. [2]



Kuva 6. Extended Service Set -verkko [3]

4.2.3 IBSS-verkko

IBSS-verkot ovat toiselta nimeltään Ad Hoc -verkkoja ja ne tunnetaan myös langattomana vertaisverkkona. IBSS-verkko muodostetaan yleensä johonkin lyhyeeseen tarpeeseen, minkä jälkeen se puretaan. IBSS-verkot eivät sisällä tukiasemaa, vaan data siirtyy suoraan laitteelta toiselle ja verkot ovat täysin langattomia. Jos kaksi asemaa eivät kuule toisiaan, ne eivät myöskään pysty siirtämään tietoa toisilleen. [2] [3]

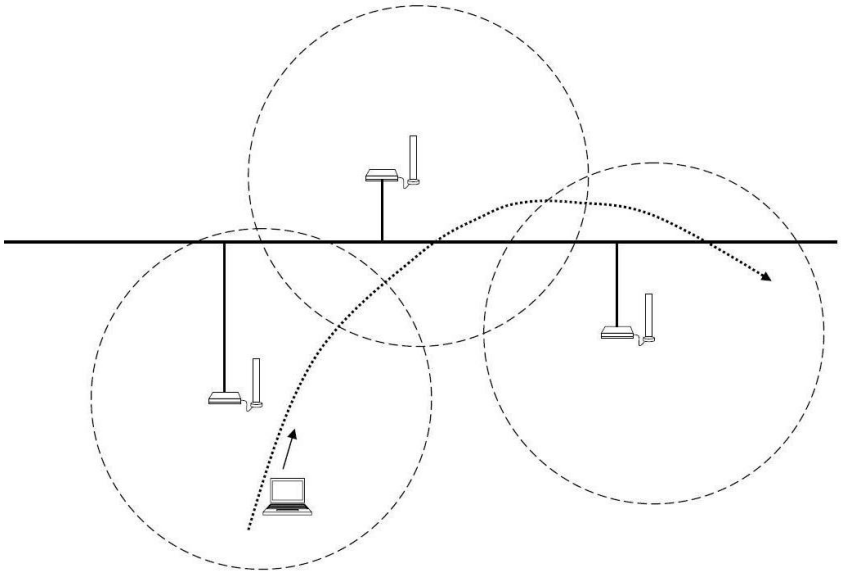


Kuva 7. Independent Basic Service Set -verkko [3]

4.3 Roaming-tekniikka

Roaming-tekniikalla tarkoitetaan langattoman verkon kykyä mahdollistaa pääteaseman siirtyminen yhden tukiaseman hallinnasta toiselle. ESS-verkko sallii tukiaseman saumattoman vaihtamisen langattoman verkon alueella liikuttaessa, kun tukiasemien peittoalueet on rakennettu osittain päällekkäisiksi ja ne on kytketty samaan runkoverkkoon. Tukiaseman vaihtamispäätös on täysin verkkokorttien tehtävä. Verkkokortti viivyttää monesti vaihtamista, koska vaihtaminen vaatii toisille kanaville virittäytymistä ja tämä saattaa samalla keskeyttää verkon liikenteen. [3] [9]

Langattomat verkkokortit tarkkailevat vastaanotettujen kehysten SNR-tasoa sekä käytettävää nopeusluokkaa. Kun nopeusluokka ja SNR-taso ovat alhaiset, alkaa langaton verkkokortti etsiä toista tukiasemaa. Jos uusi tukiasema löytyy, langaton verkkokortti lähettää yhteydenmuodostuspyynnön ja hyväksytyn yhteydenmuodostuspyynnön jälkeen liikenne siirtyy uudelle tukiasemalle. Tämän lisäksi uusi tukiasema ilmoittaa tapahtumasta vanhalle tukiasemalle runkoverkon välityksellä, jolloin vanhan tukiaseman ja päätelaitteen välinen yhteys katkeaa. Tukiasemien välistä protokollaa kutsutaan IAPP-protokollaksi. [9]



Kuva 8. Roaming-malli [3]

5 CISCO WLC -KONTROLLERI

WLC-kontrollerit yksinkertaistavat laajojen langattomien verkkojen käyttöönottoa ja ylläpitoa keskittämällä niiden hallintaa. Lisäksi WLC-kontrollerit auttavat varmistamaan langattoman verkon tasaisen suorituskyvyn ja maksimoimaan käytettävyyttä. Parempi turvallisuus varmistetaan langattomien verkkojen toiminnan seuraamisella ja tunkeutumisten havaitsemisella. [11]

Perinteisissä langattomissa verkoissa tukiasemien rooleihin kuuluvat päätelaitteiden liittäminen langattomaan verkkoon ja asiakaslaitteiden tunnistaminen, mutta kontrolleripohjaisissa toteutuksissa nämä tehtävät ovat kontrollerin vastuulla. Kontrolleripohjaisissa toteutuksissa LAP-tukiasemat rekisteröivät itsensä kontrollerin kanssa ja tunneloivat kaiken hallinnointi- ja tietoliikenteen kontrollerille, joka siirtää paketit langattomien laitteiden ja langallisen verkon välillä. Kaikki konfiguraatiot tehdään kontrollerilla ja LAP-tukiasemat lataavat asetukset kokonaisuudessaan kontrollerilta. [12]

Kommunikointi kontrollereiden ja LAP-tukiasemien välillä tapahtuu OSI-mallin kerroksella 2 tai 3. Kontrolleri hallinnoi LAP-tukiaseman asetuksia ja tukiaseman omaa ohjelmistoa (firmware). Kontrolleripohjaiset järjestelmät tukevat QoS-tekniikkaa, mikä mahdollistaa tietoliikenteen luokittelun ja priorisoinnin. WLC-kontrollerit tukevat useita kerroksen 2 ja 3 tunnistusmenetelmiä, joista WEP, WPA, WPA2 ja 802.1x ovat

kerroksen 2 tunnistusmenetelmiä ja kerroksen 3 menetelmät liittyvät yleisesti verkon liikenteen tunnistukseen ja läpikulkuun. [12] [13]

WLC-kontrolleria voidaan hallita graafisesti internet selaimella tai komentoriviliittymällä. Internet selaimella otetaan yhteys kontrollerin management -liitäntään HTTP tai HTTPS-protokollan välityksellä, minkä jälkeen kontrollerin graafinen liittymä aukeaa selaimen ikkunaan. Komentoriviliittymään voi ottaa yhteyden Telnet- ja SSH-protokollia tukevan ohjelman avulla tai konsoliyhteydellä. Kontrolleria voidaan hallita myös langattoman verkon kautta, mutta tämä vaihtoehto täytyy hyväksyä erikseen kontrollerin asetuksista. [12]

Roaming-tekniikka on tuettuna, kunhan LAP-tukiasemat ja WLC-kontrollerit kuuluvat samaan mobility-ryhmään. Kun langattoman verkon asiakas asioi kontrollerin kanssa ja tunnistautuu kontrolleriin, tämä kirjaa asiakkaan asiakastietokantaan. Merkintä sisältää asiakkaan MAC- ja IP-osoitteet, turvauksen ja QoS-tekniikan määritykset, langattoman verkon sekä yhteenkuuluvan LAP-tukiaseman. Kun verkon asiakas liikkuu samaan kontrolleriin liittyneen toisen tukiaseman alueelle, kontrolleri päivittää asiakastietokannan uuden tukiaseman tiedoilla, jolloin tiedot voidaan siirtää asianmukaisesti eteenpäin asiakkaalle. Kun verkon asiakas liikkuu samassa tai eri aliverkossa sijaitsevan, eri kontrolleriin liittyneen tukiaseman alueelle, kontrolleri lähettää tietokannassa olevat asiakkaan tiedot uudelle kontrollerille. Tämä auttaa asiakasta säilyttämään IP-osoitteen liikkumisen yhteydessä ja ylläpitämään keskeytyksettömiä TCP-istuntoja. [12]

Kontrollereissa on sisäänrakennettuna RRM-ominaisuus, jossa suoritetaan kontrollerin sisäisesti algoritmi, jonka perusteella kontrolleri säätää tukiasemien kanavia ja virta-asetuksia. RRM-ominaisuus on käytössä oletuksena, eikä LAP-tukiasemille tarvitse erikseen asettaa kanavia ja virta-asetuksia. Ominaisuus on kuitenkin ohitettavissa, jolloin tukiasemien kanavat ja virta-asetukset ovat erikseen säädettävissä. Toimiakseen RRM-ominaisuus vaatii, että tukiasema kuulee radiotaajuuksia vähintään kolmelta lähellä sijaitsevalta tukiasemalta, joista yhden tukiaseman signaalinvahvuuden tulee olla suurempi kuin -65 dBm. RRM-ominaisuus sisältää kanavien ja virta-asetuksien säätämisen sekä reiän havaitsemisen langattoman verkon kattavuudessa. Kun tukiasema käynnistyy, se pitää virta-asetukset korkeimmalla asetuksella, ja kun se havaitsee vähintään kolme tukiasemaa, joiden signaalinvahvuus on suurempi kuin -65 dBm, se

yrittää ensiksi vaihtaa käytössä olevaa kanavaa. Tämän jälkeen tukiasema pudottaa virtatasoa, jos kanavat on säädetty käsin tai tukiasemia on enemmän kuin kanavia. [12]

Hyvin suunnitellussa kontrolleripohjaisessa toteutuksessa yhden tukiaseman rikkoutuessa kontrolleri nostaa sen vieressä sijaitsevien tukiasemien lähetystehoja kattaakseen rikkoutuneen tukiaseman alueen. Tälläisessä kontrolleripohjaisessa toteutuksessa yhden tukiaseman tiedonsiirtokapasiteetti jakautuu, tiuhasti sijoitettujen tukiasemien ansiosta, pienemmälle alueelle kuin perinteisessä langattoman verkon toteutuksessa ja se nostaa näin langattoman verkon suorituskykyä. [11] [12] [13]

5.1 LAP-tukiasema

LAP-tukiasemat on suunniteltu liitettäväksi WLC-kontrolleriin, eivätkä ne kykene toimimaan itsenäisesti. Tällaiset tukiasemat on tehty niin, etteivät ne vaadi yksittäistä konfigurointia. LAP-tukiasemat tarjoavat tuen IEEE 802.11 -standardien kaksitaajuustoiminnolle ja lähetyksien yhtäaikaiselle valvonnalle, mikä mahdollistaa reaaliaikaisen radiotaajuuden hallinnan. LAP-tukiasemat käsittelevät aikaherkkiä toimintoja kuten OSI-mallin toisen kerroksen salauksen, mikä mahdollistaa tuen ääni-, video- ja tietosovelluksille. Kaikki ei-reaaliaikaiset MAC-toiminnot suoritetaan kontrollerissa. [11]

5.2 LWAPP-protokolla

LWAPP-protokolla on IETF-työryhmän protokolla, joka määrittelee valvontaviestit käyttöönottoa, polkujen tunnistusta ja toiminta-ajan toimenpiteitä varten. LWAPP-protokolla määrittelee myös tunnelointimekanismin tietoliikennettä varten. [11]

LAP-tukiasema käyttää LWAPP-protokollan mekanismejä löytääkseen kontrollerin. Ensimmäiset liittymiskeinot käyttävät OSI-mallin kerrosta 2 ja sen jälkeen liittymiseen käytetään kerrosta 3. Tukiaseman liittyessä kontrolleriin se lataa kontrollerilta firmware-ohjelmiston, jos tarkastus tukiaseman ja kontrollerin välillä ei täsmää. Kontrolleriin liittymisestä eteenpäin tukiasema on täysin kontrollerin hallinnassa. LWAPP-protokolla varmistaa tukiaseman ja kontrollerin välisen hallintaliikenteen secure key distribution -menetelmällä. [11] [14]

Kontrollerin ohjelmiston versiosta 5.2 lähtien LAP-tukiasemat kommunikoivat kontrollerin ja muiden LAP-tukiasemien kanssa CAPWAP-protokollan avulla. CAPWAP-protokolla on IETF-työryhmän standardi ja se pohjautuu LWAPP-protokollaan. CAPWAP-protokolla mahdollistaa tulevaisuudessa kolmannen osapuolen tukiasemien toiminnan kontrollerien kanssa. Kontrollerin löytämiseen ja firmware-ohjelmiston lataukseen käytetyt mekanismit ovat CAPWAP- ja LWAPP-protokollissa samat, joten LWAPP-protokollaa käyttävien tukiasemien on mahdollista liittyä CAPWAP-protokollaa käyttävään kontrolleriin. CAPWAP-protokolla ei tue OSI-mallin kerroksen 2 toimintoja. [12]

5.3 DHCP Option 43- ja 60 -vaihtoehdot

RFC 2132 määrittelee kaksi DHCP Option -vaihtoehtoa, jotka liittyvät tietyn valmistajan tai toimittajan valintaan. Nämä ovat Option 43 ja Option 60. Option 60 on VCI-tunniste, tekstijono, joka tarkoittaa toimittajan luokan tunnistinta. Option 60 sisältyy alkuperäiseen DHCP Discover -viestiin, jonka asiakaslaite lähettää broadcast-lähetyksenä hakiessaan IP-osoitetta. RFC 2132 määrittelee myös, että DHCP-palvelimien tulee palauttaa valmistajaan liittyvät tiedot Option 43 -vaihtoehdon muodossa. [15]

LAP-tukiasemat voivat käyttää DHCP Option 43 -vaihtoehtoa liittyäkseen kontrolleriin, joka on eri aliverkossa kuin tukiasema. DHCP Option 43 -vaihtoehdon käyttämien kontrollerien tukiasemien selville saamisen helpottamiseksi DHCP-palvelin tulee konfiguroida palauttamaan yksi tai useampi WLAN controller management -liitännän IP-osoite tukiaseman VCI-tunnisteen avulla. DHCP-palvelin voidaan konfiguroida jakamaan nämä tiedot IP-osoitteita jakaessaan, kun option 43- ja option 60 -vaihtoehdot määritetään DHCP-palvelimen jokaiseen DHCP pool -alueeseen (scope), joka tarjoaa IP-osoitteita LAP-tukiasemille. DCHP-palvelimien konfiguraatioiden käsitteet voivat poiketa DHCP-ohjelman tekijän mukaan. [15]

Valmistajaan liittyvät tiedot yhdistetään DHCP-palvelimella VCI-tekstijonoiksi. Kun DHCP-palvelin näkee tunnistettavissa olevan VCI-tekstijonon DHCP discover -viestissä, se vastaa tähän DHCP offer -viestillä, johon sisältyy valmistajaan liittyvät tiedot Option 43 -vaihtoehdon muodossa. IP-osoitteen DHCP-palvelimelta saadessaan LAP-tukiasema etsii DHCP offer -viestin Option 43 -kentästä WLC-kontrollerien IP-osoitteet. Tämän jälkeen tukiasema lähettää Layer 3 LWAPP discovery request -viestin jo-

kaiselle Option 43 -kentässä listatulle kontrollerille. LWAPP discovery request -viestin vastaanottavat kontrollerit vastaavat viestiin unicast LWAPP discovery response -viestillä, mikä käynnistää tukiaseman rekisteröintiprosessin kontrolleriin. [14] [15]

6 DHCP-PALVELIN

Verkon laitteiden konfiguroinnin helpottamiseksi monissa toteutuksissa DHCP-palvelin jakaa IP-osoitteet kaikille verkkoon liittyville laitteille, myös tukiasemille ja langattoman verkon asiakkaille. Tarkkaan ottaen palvelimen tehtävänä on suorittaa monien muidenkin DHCP-protokollan vastuulla olevien tietojen jakelu verkossa sijaitseville laitteille. Yleisimpiä jaettavia tietoja ovat IP-osoite maskeineen, gateway-laitteen IP-osoite ja tiedot DNS-palvelimesta. Tiedot vastaanotettuaan laite on osa tätä verkkoa. [16]

DHCP-palvelin vastaanottaa DHCP request -viestejä ja vastaa niihin DHCP offer -viestillä. DHCP-asiakasohjelmisto, joka sisältyy käyttöjärjestelmään, lähettää DHCP request -viestejä DHCP-palvelimelle. DHCP relay agent, välittäjäagentti, välittää DHCP request -viestit lähiverkosta toiseen, jolloin jokaisessa lähiverkossa ei tarvitse olla omaa DHCP-palvelinta. [17]

6.1 VMware-virtualisointiohjelmisto

VMware-virtualisointiohjelmisto lisää pöytäkoneiden tai kannettavien tietokoneiden joustavuutta ja vähentää laitteistokustannuksia mahdollistamalla usean käyttöjärjestelmän ajamisen samanaikaisesti yhdellä fyysisellä tietokoneella. Tämä mahdollistaa vähemmällä laitteistolla toimimisen, mikä vähentää myös tarvittavan tilan määrää. Lisäksi VMware-virtualisointiohjelmisto tukee yli 200:aa eri käyttöjärjestelmää. [18]

Snapshot-toiminnolla voi tallentaa virtuaalitietokoneen tilan, johon voi palata milloin tahansa myöhemmin. Snapshot-ominaisuus on hyödyllinen, kun on tarpeen palauttaa virtuaalikoneen aikaisempi vakaa tila. Virtuaalikoneista voi tehdä asennusta nopeuttavia kopioita, jotka sisältävät asennustiedot ja konfiguroinnit. Virtuaalikoneelle jaettavia fyysisen tietokoneen resursseja ja muita asetuksia voidaan hallita virtuaalikoneen asetuksista valitsemalla ohjelmistosta VM → Settings. [18]

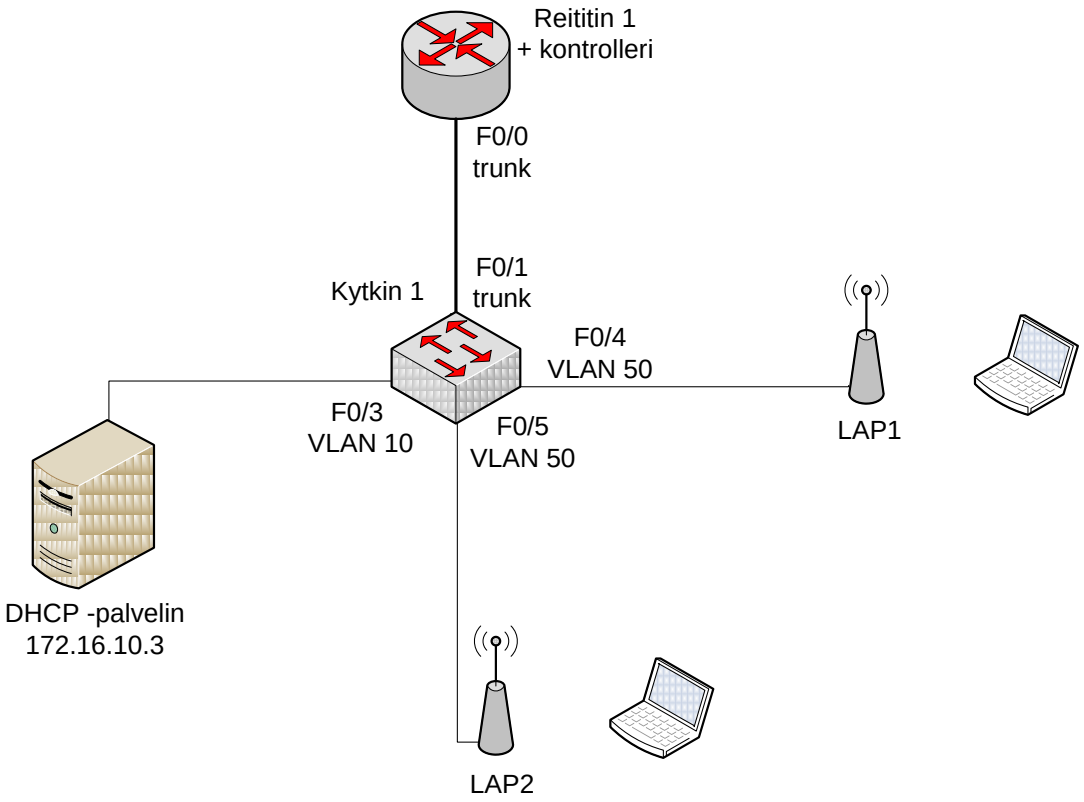
6.2 LABESX-palvelin

LABESX-palvelin ajaa useaa virtuaalikonetta samanaikaisesti useaa eri tarvetta varten VMware ESX -ohjelmiston avulla. VMware ESX -ohjelmisto ei vaadi erillistä käyttöjärjestelmää niin kuin muut VMware-ohjelmistot, vaan se asennetaan suoraan tietokoneelle. Ohjelmisto on varta vasten suunniteltu ajamaan useaa virtuaalikonetta samanaikaisesti ja sillä voidaan määritellä yksilökohtaisesti jokaiselle virtuaalikoneelle jaettavat resurssit ja muut laitteistoon liittyvät asetukset. [19]

Palvelimeen muodostetaan yhteys VMware Infrastructrure Client -ohjelmistolla, jolla voi hallita palvelimella olevia virtuaalikoneita. Kun palvelimella oleva virtuaalikone on käynnissä, ohjelmistolla avataan virtuaalikoneen hallintakonsoli, jonka avulla palvelimella olevaa virtuaalikonetta voi käyttää kuin mitä tahansa muuta virtuaalikonetta. [19]

6.3 Kytkentä

Opinnäytetyön testikytkentään kuului Cisco 2811 -reititin, Cisco 3560 Catalyst multilayer -kytkin ja kaksi kappaletta Cisco 1200 LAP -tukiasemia. Cisco 2811 -reitittimessä on NME-AIR-WLC8-K9-kontrollerimoduuli asennettuna. Cisco 3560 Catalyst -kytkin tukee PoE-tekniikkaa, jonka avulla tarvittava käyttöjännite voidaan jakaa LAP-tukiasemille myös tiedonsiirtoon käytettävän Ethernet-kaapelin avulla. Tämä järjestely helpottaa tukiasemien asentamista testikytkentää varten, mutta siirtää tukiasemien käyttöjännitteen jakamisen täysin Cisco 3560 Catalyst -kytkimen varaan.



Kuva 9. Testikytkentä

6.4 Linuxin asennus

Aluksi asennettiin Fedora 11 Linux -jakelu virtuaalitietokoneeksi VMware Workstation -virtualisointiohjelmistoon tietoliikennelaboratorion työasemalle. Tämän jälkeen VMware-ohjelmiston asetuksia vaihdettiin niin, että virtuaalikoneelta on pääsy internetiin. VMware-ohjelmiston valikoista valitaan VM → Settings → Network Adapter 2 → VMnet 8 (NAT). Fedorasta valitaan System → Preferences → System Proxy, johon kirjoitetaan jokaiseen kohtaan cache.tlt.kyamk.fi ja portiksi 800. Sitten Fedorasta valittiin System → Administration → Software Update, jolloin päivitysohjelma etsii internetin kautta uudempia ja asentamattomia versioita ohjelmista. Listasta etsittiin ISC DHCP Server -ohjelmisto ja asennettiin se, ei siis DHCP client -ohjelmistoa. Haku-kohtaan laitetaan hakusanaksi DHCP, niin asennettava ohjelma on helpointa löytää. Jos lista ei näytä päivittyvän tai ohjelma ei lataudu, kannattaa Linux käynnistää uudelleen. Kun kaikki päivitykset oli tehty, VMware Workstation -ohjelmistossa oleva virtuaalitietokone kopioitiin LABESX-palvelimeen virtuaalikoneeksi VMware-ohjelmiston muunnostyökalun avulla.

6.5 DHCP-palvelimen konfiguraatio

Konfiguraatiota tehtäessä käytettiin vim-tekstieditoria. Koska nano-tekstieditori on aloittelijalle parempi vaihtoehto, alla olevan vim-komennon tilalle kannattaa vaihtaa nano-komento. Nano-tekstieditorissa komennot näkyvät koko ajan tekstieditorin ala-laidassa.

ISC DHCP Server -ohjelmiston konfiguraatiota pääsee muokkaamaan valitsemalla Fedoran vasemmasta yläreunasta Applications → System Tools → Terminal. Root-käyttäjäksi pääsee kirjoittamalla komentoriville su ja salasana. Tämä on tehtävä aina tiedostoja muokattaessa ja DHCP-palvelua käynnistettäessä. Sen jälkeen kirjoitetaan **vim /etc/dhcp/dhcpd.conf** -käsky, joka avaa tiedoston tekstieditoriin. Konfiguraation sijainti voi vaihdella DHCP-ohjelman version tai Linuxin mukaan. Jotta tiedostoa voi muokata, täytyy vim-tekstieditorin käynnissä ollessa painaa näppäimistön insert-näppäintä, jolloin editorin vasempaan alareunaan tulee teksti ”**- - INSERT - -**”. Tilasta pääsee pois painamalla escape-näppäintä. Konfiguraatioon tehdyt muutokset tallennetaan **:w**-komennolla (write) ja tekstieditorista poistutaan **:q**-komennolla (quit), molemmat voi tehdä samanaikaisesti komennolla **:wq**. [20]

Alla on viimeisin versio ISC dhcpd -ohjelman konfiguraatiosta, johon jokaiselle erilaiselle tukiasemalle voi lisätä oman aliluokan (subclass). Erilaisia tukiasemia varten muutetaan vain tukiaseman oma VCI-tunniste, joka on alla **Cisco AP c1200**, tämä vastaa Option 60 -vaihtoehtoa. Jos kontrollereita on useampia, ne voidaan listata konfiguraatioon pilkulla eroteltuna ”**option LWAPP.controller**” -kohtaan, tämä kohta vastaa Option 43 -vaihtoehtoa. Koko konfiguraatio kirjoitetaan samaan tekstitiedostoon. [15] [21]

```
 # Globaalit asetukset
ddns-update-style interim;
allow bootp;
option space LWAPP;
option LWAPP.controller code 241 = array of ip-address;

# VLAN 1
subnet 172.16.1.0 netmask 255.255.255.0 {
  range dynamic-bootp 172.16.1.150 172.16.1.250;
```

```
  option routers 172.16.1.1;
  option broadcast-address 172.16.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}

# VLAN 2
…
#VLAN 3
…

# VLAN 50
subnet 172.16.50.0 netmask 255.255.255.0 {
  authoritative;
  range dynamic-bootp 172.16.50.150 172.16.50.250;
  option routers 172.16.50.1;
  option broadcast-address 172.16.50.255;
  default-lease-time 600;
  max-lease-time 7200;

class "LWAPP" {
  match option vendor-class-identifier;
}
subclass "LWAPP" "Cisco AP c1200" {
  vendor-option-space LWAPP;
  option LWAPP.controller  172.16.100.100;}
}

# MANAGEMENT VLAN
subnet 172.16.100.0 netmask 255.255.255.0 {
  range 172.16.100.150 172.16.100.250;
  option routers 172.16.100.1;
  option broadcast-address 172.16.100.255;
  default-lease-time 600;
  max-lease-time 7200;
```

}
[15] [25]

Täytyy muistaa, että DCHP-palvelimien konfiguraatioiden käsitteet voivat poiketa DHCP-ohjelman tekijän mukaan. Tästä syystä jotain muuta kuin ISC DHCP server -ohjelmaa käytettäessä on option **LWAPP.controller code 241 = array of ip-address;** -kohdan numeron 241 tilalla usein Option 43 -vaihtoehdosta tuleva numero 43. [15]

6.6 Muita huomioitavia asioita

DHCP-palvelin tarvitsee staattisen IP-osoitteen, jotta sen voi määritellä kontrollerin konfiguraatioon. Reitittimeen on myös määriteltävä **ip helper-address** -komento. Lisäksi tiedostoon **etc/sysconfig/dhcpd** on laitettava määritys **DHCPDARGS=eth0**, jolloin DHCP-palvelin tietää jakaa osoitteita eth0-liityntäporttiin. Tiedosto avataan tekstieditorilla komennolla **vim etc/sysconfig/dhcpd**. [22]

6.6.1 Staattinen IP-osoite DHCP-palvelimen Ethernet-porttiin

Staattinen IP-osoite määritetään **/etc/sysconfig/network-scripts/ifcfg-eth0** -tiedostoon. Jotta tiedostoa pääsee muokkaamaan, täytyy root-käyttäjänä kirjoittaa komentoriville **vim /etc/sysconfig/network-scripts/ifcfg-eth0**. Tämä komento avaa tiedoston vim-tekstieditorilla, ja siihen kirjoitetaan alla oleva konfiguraatio. [22]

DEVICE=eth0
BOOTPROTO=static
IPADDR=172.16.10.3
NETMASK=255.255.255.0
GATEWAY=172.16.10.1
BROADCAST=172.16.10.255
ONBOOT=yes

Tämän jälkeen komentoriville kirjoitetaan **ifdown eth0** -käsky, joka sulkee eth0-liityntäportin, ja sen jälkeen liityntäportti käynnistetään uusiksi **ifup eth0** -käskyllä, jolloin liityntäportti käynnistyy uusilla määrityksillä. [22]

6.6.2 IP-helper-osoite reitittimen Ethernet-porttiin

Jotta lähiverkkoon kytketyt laitteet saisivat osoitteet, on reitittimen liityntäportin konfiguraatioon lisättävä **ip helper-address** -komento ja sen perään DCHP-palvelimen osoite. Osoitteiden on siirryttävä VLAN-verkosta toiseen, ja tämän vuoksi myös reitityksprotokollan täytyy olla käynnistetty.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.10.3
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.50.1 255.255.255.0
 ip helper-address 172.16.10.3
```

Ciscon kurssimateriaalin mukaan on reitittimeen määritettävä lisäksi **ip forward-protocol** -käskyt. Reititin päättää näiden määrittelyiden mukaan, mitä protokollia lähetetään eteenpäin ja mitä ei lähetetä.

```
no ip forward-protocol udp time
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
ip forward-protocol udp bootpc
ip forward-protocol udp 8000
```

7 VALMISTAUTUMINEN LANGATTOMAN VERKON TOTEUTTAMISEEN

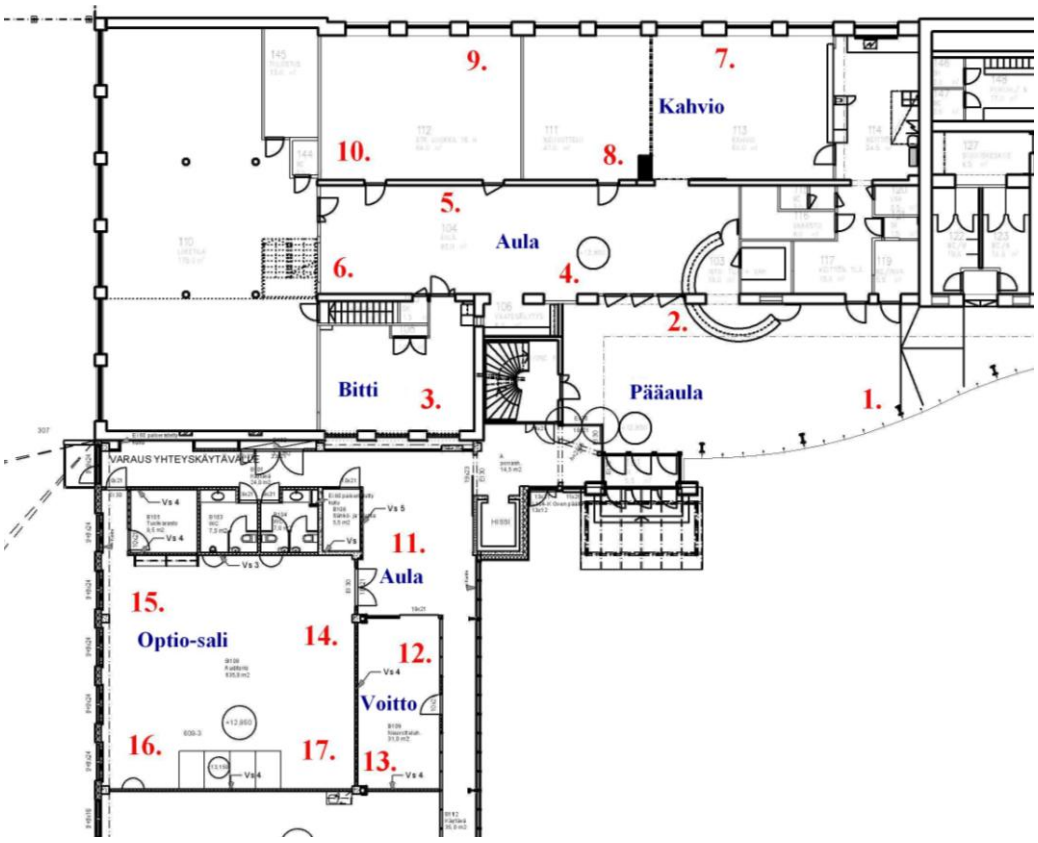
Ennen kuin langaton verkko voidaan toteuttaa, tulee verkon kattavat alueet kartoittaa mahdollisten toisten langattomien verkkojen varalta, jotta langattoman verkon kanavat

voidaan valita ilman häiriöitä aiheuttavia ja verkon suorituskykyä alentavia päällekkäisyyksiä. [3]

7.1 Langattomien verkkojen kartoittaminen

Datariinan langattomat verkot kartoitettiin minikannettavalla, johon oli asennettu NetStumbler versio 0.4.0. NetStumbler-ohjelmaa käytetään selvittämään alueella sijaitsevien tukiasemien SSID-tunnukset, signaalinvoimakkuudet ja tukiasemien käyttämät kanavat. Tämä järjestely löytää vain 802.11-standardin mukaiset langattomat verkot, joten muut samaa taajuutta käyttävät häiriölähteet, esimerkiksi mikroaaltouunien ja langattomien hälytysjärjestelmien tuottamat taajuudet, jäävät havaitsematta. [4]

Datariinan langattomien verkkojen kartoitus sujui lähes ongelmitta, sillä mikään kartoitettavista tiloista ei ollut käytössä. Tulokset kirjattiin Datariinan ensimmäisen kerroksen ja kellarikerroksen pohjakuviin.



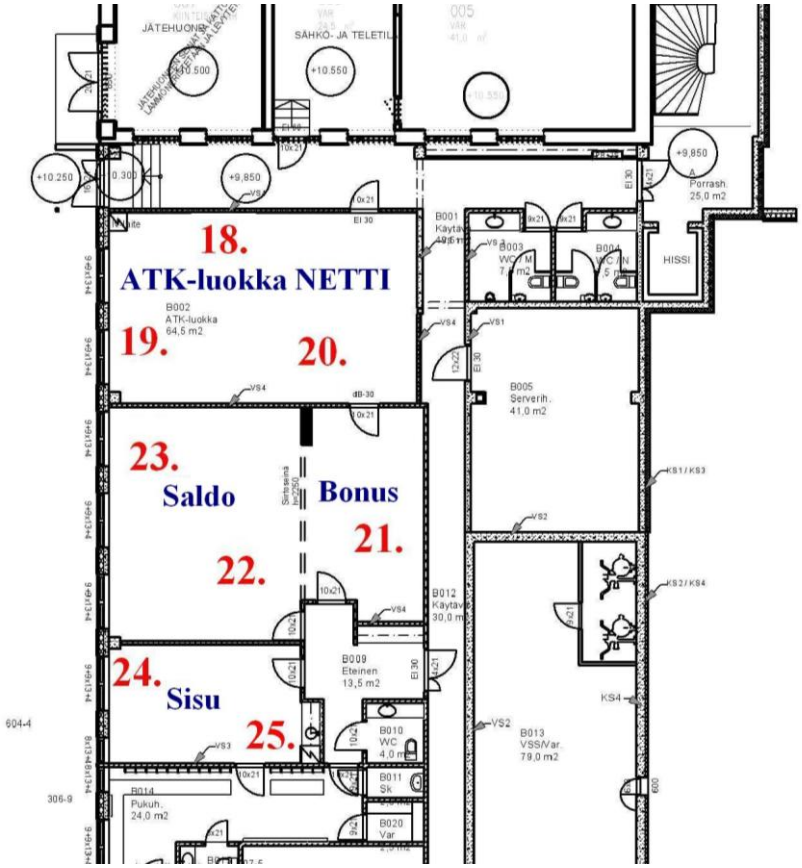
Kuva 10. Datariinan ensimmäisen kerroksen mittauspisteet [23] [24]

Ensimmäisen kerroksen kartoituksessa löytyi useita käytössä olevia kanavia, jotka on otettava huomioon tukiasemien kanavia valittaessa. Erityisesti kanavat 1 ja 6 olivat jo valmiiksi käytössä olevia kanavia. [24]

Taulukko 2. Datariinan ensimmäisen kerroksen mittauksen tulokset. [24]

Mittauspiste	Löydetyt kanavat	Mittauspiste	Löydetyt kanavat
1.	1, 6, 8 (3)	2.	1, 6, 8 (3, 13)
3.	1 (3,8)	4.	1, 6 (3, 8)
5.	1 (3)	6.	1, 11 (3, 6, 8, 13)
7.	1, 6 (3, 8)	8.	1, 6 (3, 8)
9.	1, 6 (3, 8)	10.	1, 6 (3, 8)
11.	1 (6, 11, 13)	12.	1 (6)
13.	1 (6)	14.	1
15.	1	16.	1
17.	1		

Tulosten suluissa olevat kanavat tarkoittavat kanavia, joiden signaalinvoimakkuus on heikko, ja niitä ei ole otettu huomioon kanavia valittaessa.



Kuva 11. Datariinan kellarikerroksen mittauspisteet [23] [24]

Kellarikerroksen langattomien verkkojen kartoituksessa löytyi vain etäisiä langattomia verkkoja, joten kanavia valittaessa on otettava huomioon ensimmäisessä kerroksessa sijaitsevaan Optio-saliin ja kellarikerrokseen sijoitettavien tukiasemien kanavat. [24]

Taulukko 3. Datariinan kellarikerroksen mittauksen tulokset. [24]

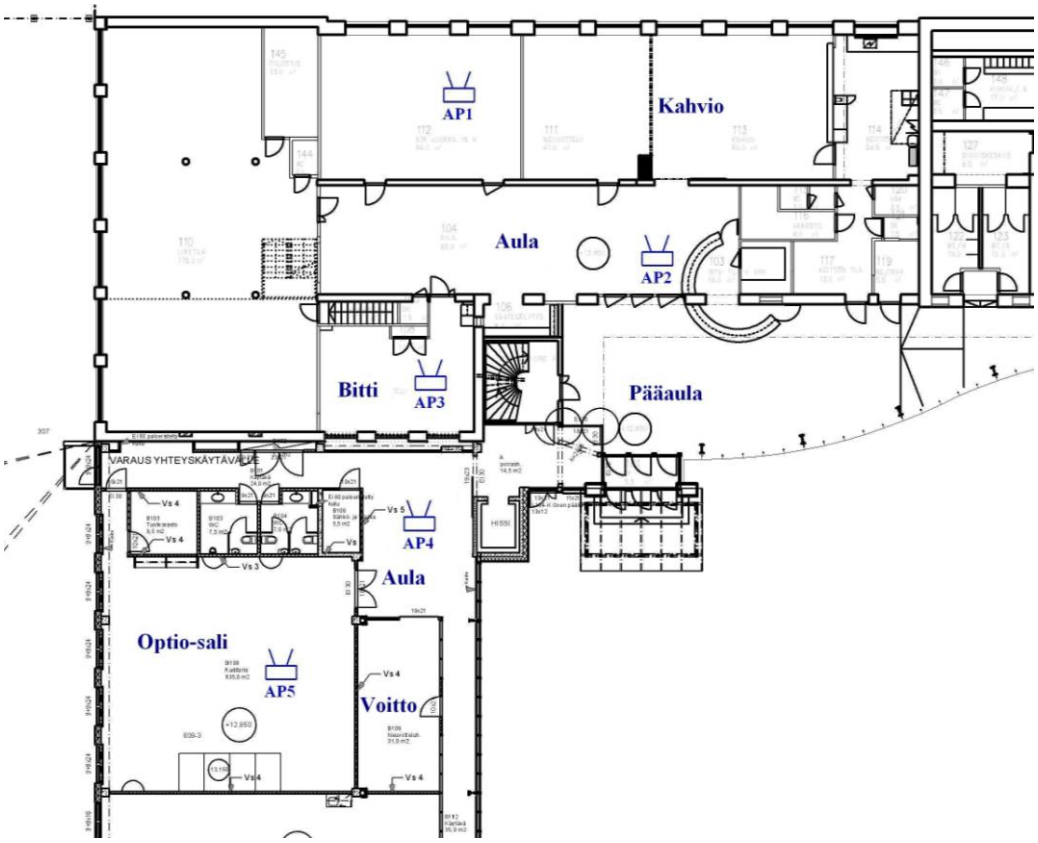
Mittauspiste	Löydetyt kanavat	Mittauspiste	Löydetyt kanavat
18.	(1,6)	19.	(1,6)
20.	(1)	21.	(1)
22.	(1,6)	23.	(1,6)
24.	(1,6)	25.	(1)

Tulosten suluissa olevat kanavat tarkoittavat kanavia, joiden signaalinvoimakkuus on heikko, ja niitä ei ole otettu huomioon kanavia valittaessa.

7.2 Tukiasemien sijoittaminen

Tukiasemien sijoittamisessa on huomioitu vierekkäiset tukiasemat, kartoituksessa löytyneet mahdollista häiriötä aiheuttavat kanavat, eri alueiden langattoman verkon tarpeen määrä sekä rakennuksen sisätiloissa sijaitsevat mahdolliset tukiasemien asennuspaikat. Tukiasemien sijainnit ja kanavat on valittu siten, että vältytään päällekkäisyyksiltä. Suunnittelu on tehty 802.11g-standardiin pohjautuen ja käytettävänä antennityyppinä on ympärisäteilevä antenni. Tukiasemat on sijoitettu kontrolleripohjaista järjestelmää ajatellen, mistä johtuu tukiasemien runsas määrä. [3] [13]

Ensimmäisen kerroksen langattomien verkkojen kartoituksessa löytyi useita langattomia verkkoja, ja jo käytössä olevien kanavien takia tukiasemien kanavien valintaa joutui miettimään tovin. Tukiasema AP1 kattaa kahvilan tilat ja osan aulasta. Tukiasema AP2 kattaa loppuosan aulasta ja pääaulan. Koulutusluokka Bitissä on paksuista seinistä johtuen varmuuden vuoksi oma tukiasemansa, tukiasema AP3. Tukiasema AP4 kattaa aulan ja kokoustila Voiton. Tukiasema AP5 kattaa Optio-salin. [24] [25]

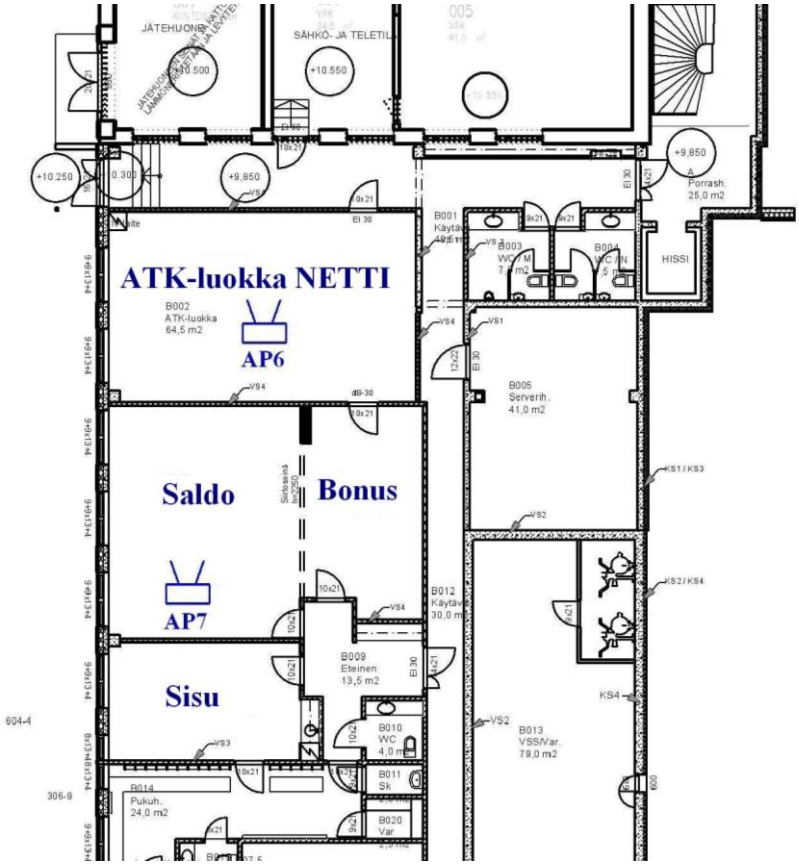


Kuva 12. Datariinan ensimmäisen kerroksen tukiasemien sijoittelu [23] [24]

Taulukko 4. Datariinan ensimmäisen kerroksen tukiasemien kanavat. [24]

Tukiasema	Kanava	Tukiasema	Kanava
AP1	13	AP2	1
AP3	5	AP4	9
AP5	13		

Kellarikerroksen langattomien verkkojen kartoituksessa ei löytynyt häiritseviä langattomia verkkoja, mutta yläkerrassa on langaton äänijärjestelmä ja suunnitteluasteella oleva AP5-tukiasema, jotka toimivat kanavilla 1 ja 13. Tukiasemien AP6 ja AP7 kanavien valintaan vaikutti ensimmäisessä kerroksessa sijaitsevan Optio-salin sijainti kellarikerroksessa olevien neuvottelutilojen yläpuolella, koska tukiasemien kuuluvuusalueissa on päällekkäisyysriski. Tukiasema AP6 kattaa ATK-luokka Netin. Tukiasema AP7 kattaa neuvottelutilat Bonuksen ja Saldon sekä Sisu-saunatuvan. [24] [25]



Kuva 13. Datariinan kellarikerroksen tukiasemien sijoittelu [23] [24]

Taulukko 5. Datariinan kellarikerroksen tukiasemien kanavat [24]

Tukiasema	Kanava	Tukiasema	Kanava
AP6	5	AP7	9

7.3 Laitteisto

Varsinaiseen toteutukseen suunniteltiin käytettäväksi HP ProCurve MultiService Controller -sarjasta MSM710 Mobility Controller -kontrolleria. Tukiasemiksi valittiin HP ProCurve MSM310 -tukiasemat. Hintaluokaltaan valittu kontrolleri on HP:n toiseksi edullisin malli, noin 900 euroa, ja yksi MSM310-tukiasema maksaa noin 400 euroa. Jos langaton verkko toteutettaisiin tässä suunnitelmassa olevalla tukiasemien määrällä (7 kpl), tulisi laitteiston hinnaksi noin 3700 euroa. [26] [27]

Langattoman verkon tiedonsiirtokapasiteetin suurentamiseksi voi tukiasemiksi valita HP ProCurve MSM410 -tukiasemat, jotka tukevat uutta 802.11n-standardia. 802.11n-

standardia käyttävien tukiasemien kuuluvuus on vanhoja standardeja suurempi, joten laitteiston kustannukset saattavat pudota tukiasemien määrän vähentyessä. Standardien erojen vuoksi 802.11n-standardia varten langattoman verkon suunnittelu täytyy kuitenkin uusia. MSM410-tukiasemat ovat hintaluokaltaan noin 500 euroa, mikä nostaa koko laitteiston hinnan 4400 euroon, jos tukiasemien määrä pidetään samana. [28]

MSM710-kontrollerissa on kaksi gigabitin Ethernet-porttia ja yksi konsoliportti. Kontrolleri tukee maksimissaan kymmentä IEEE 802.11n/a/b/g -tukiasemaa, mikä riittää helposti pienen langattoman verkon toteuttamiseen. Lisäksi MSM710-kontrolleri sisältää mm. langattoman verkon hallintaominaisuudet, mahdollisuuden sadalle samanaikaiselle vierasverkon käyttäjälle, reaaliaikaiset paikannuspalvelut sekä kehittyneen roaming-tekniikan. MSM710-kontrolleri vaatii pienikokoisuutensa vuoksi sovitussarjan normaalin kokoiseen laitekaappiin asennettaessa. [26]

Kuva 14. HP MSM710 Mobility Controller -kontrolleri [27]

MSM310-tukiasemat tukevat IEEE 802.11a/b/g -standardeja ja PoE-tekniikkaa. Tukiasemat voivat toimia kontrollerin ohjaamana ja myös itsenäisesti. Tukiasemat sisältävät kaksi 10/100 megabitin Ethernet-porttia, jotka tunnistavat verkon nopeuden auto-sensing-ominaisuuden avulla. [27]

Kuva 15. HP ProCurve MSM310 -tukiasema [27]

MSM410-tukiasemat tukevat samoja IEEE 802.11 -standardeja kuin MSM310-tukiasemat ja näiden lisäksi myös uutta IEEE 802.11n -standardia. Tukiasemat voivat toimia itsenäisesti tai kontrollerin hallittavina. 802.11n-standardi on hyvissä olosuhteissa nopeampi kuin perinteinen 100 megabitin verkko, ja tästä syystä MSM410-tukiasemat sisältävät kaksi gigabitin Ethernet-porttia, jotka tukevat PoE-tekniikkaa. [28]

Kuva 16. HP ProCurve MSM410 -tukiasema [28]

7.4 Asennuksessa huomioitavaa

Asennuksen helpottamiseksi tai sähköpistokkeen puuttuessa tukiasemalle voi antaa sen tarvitseman virran PoE-tekniikkaa käyttämällä. Toteuttaminen PoE-tekniikalla vaatii kyseessä olevaa ominaisuutta tukevan kytkimen ja tukiaseman. Maksimitehotasoon vaikuttaa kytkimen virtalähteen tehokkuus sekä kytkimen ja tukiaseman välinen kaapeli. Tukiaseman omaa virtalähdettä kannattaa käyttää aina, kun se on mahdollista; tällöin käyttöjännitteen syöttäminen ei ole vain kytkimen varassa. Jos esimerkiksi puolet langattoman verkon tukiasemista saisi käyttöjännitteen samalta kytkimeltä ja tämän kytkimen virtalähde rikkoutuisi, johtaisi se siihen, että puolet langattomasta verkosta olisi poissa käytöstä. [29]

Suunnitelma tukiasemien sijoituspaikoista on ikään kuin lähtökohta niiden lopullisen tarpeen ja lukumäärän selvittämiseksi. Langattoman verkon toteutusta jatkettaessa pitäisi tarkentaa kuuluvuusalueiden riittävyydet ja sen jälkeen päättää tukiasemien määrä, sijoituspaikat sekä laitteiston määritykset. Esimerkiksi Datariinan ensimmäisessä kerroksessa sijaitseva AP4-tukiasema ja kellarikerroksessa sijaitseva AP6-tukiasema saattavat kuuluvuusalueiden mittauksissa osoittautua tarpeettomiksi, mikä pienentää vastaavasti kustannuksia.

8 JOHTOPÄÄTÖKSET

Opinnäytetyön lähtökohtana oli suunnitella ja rakentaa keskitetysti hallinnoitu langaton lähiverkko digitaalisen liiketoiminnan keskuksen Datariinan kokous- ja koulutustiloihin huomioiden tiloissa jo käytössä olevat lähiverkot.

Opinnäytetyö aloitettiin suorittamalla Datariinan ensimmäisen kerroksen ja kellarikerroksen aiempien langattomien verkkojen kartoitus. Tulosten pohjalta tehtiin suunnitelma uusien tukiasemien sijoittamisesta sekä suunniteltiin varsinaiseen toteutukseen käytettäväksi tulevaa laitteistoa ja selvitettiin laitteiston kustannukset.

Tietoverkkolaboratorioon rakennetussa testiverkossa simuloitiin suunnitelman mukaista toteutusta ja sen tuloksena on dokumentoitu Ciscon WLAN-kontrollerin ja LAP-tukiasemien sekä niiden vaatiman DHCP-palvelimen käyttöönotto ja tarvittavat määrittelyt. DHCP-palvelimen konfiguraatiota tehtäessä suurimmat ongelmat ovat Linuxin käytön hankaluus aloittelijalle sekä option 43- ja 60-vaihtoehtojen konfiguroi-

minen toimivaksi kokonaisuudeksi. Opinnäytetyön aikana tein laboratorion testiverkkoon DCHP-palvelimen, joka on suunniteltu Ciscon LAP-tukiasemia varten. Mikäli langaton verkko toteutetaan dokumentin lopussa esitellyillä HP:n laitteilla, pitää kyseinen palvelin konfiguroida niiden vaatimalla tavalla.

Suunnittelussa ei ilmennyt langattoman verkon toteuttamiselle mitään esteitä. Tulevaisuuden tarpeita ajatellen keskitetysti hallittava langaton järjestelmä on suositeltava vaihtoehto, koska kontrolleripohjainen toteutus tukee helpommin langattoman verkon laajentamista. Pienempään laajentamiseen riittää uuden tukiaseman hankkiminen ja kytkeminen verkkoon, minkä jälkeen hallinta onnistuu kontrollerin hallintaohjelmistolla. Suurempaan, keskitetysti hallittavan langattoman verkon laajentamiseen tarvitaan joko uusi tehokkaampi kontrolleri tai toinen pieni kontrolleri. Suuremmassa laajennuksessa, tehokasta kontrolleria käytettäessä, sopivat vanhat tukiasemat myös tämän hallittaviksi.

LÄHTEET

1. Puska, Matti. Langattomat lähiverkot. Helsinki: Talentum, 2005.

2. Granlund, Kaj. Langaton tiedonsiirto. Jyväskylä: Docendo Finland Oy, 2001.

3. Siirtyvä tietoliikenne: Langaton lähiverkko [online] Saatavana osoitteesta: http://www.it.lut.fi/kurssit/03-04/010651000/luennot/wlan.pdf [Viitattu 25.8.2009]

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

5. WHITE PAPER IEEE 802.11g [online] Saatavana osoitteesta: http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf [Viitattu 14.2.2010]

6. Cisco Systems. 802.11n: The Standard Revealed [online] Saatavana osoitteesta: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-427843_v1.pdf [Viitattu 11.2.2010]

7. 802.11n MIMO Wi-Fi [online] Saatavana osoitteesta: http://80211n.com/ [Viitattu 15.2.2010]

8. Tuominen Toni. WLAN TIETOTURVA [online] Opinnäytetyö 2005. Tampereen ammattikorkeakoulu. Saatavana osoitteesta: https://oa.doria.fi/bitstream/handle/10024/5143/TMP.objres.226.pdf?sequence=1 [Viitattu 12.8.2009]

9. Gast, Matthew S. 802.11(R) Wireless Networks: The Definitive Guide, Second Edition.

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

11. Cisco Systems. Lightweight Access Point FAQ [online] Saatavana osoitteesta: http://www.cisco.com/application/pdf/paws/70278/lap_faq.pdf [Viitattu 2.3.2010]

12. Cisco Systems. Wireless LAN Controller (WLC) FAQ [online] Saatavana osoitteesta: http://www.cisco.com/application/pdf/paws/69561/wlc_faq.pdf [Viitattu 25.3.2010]

13. Cisco Systems. Wireless LAN Controllers Improve Visibility and Control [online] Saatavana osoitteesta: http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html [Viitattu 2.3.2010]

14. Cisco Systems. Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) [online] Saatavana osoitteesta: http://www.cisco.com/application/pdf/paws/70333/lap_registration.pdf [Viitattu 2.3.2010]

15. Cisco Systems. DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration [online] Saatavana osoitteesta: http://www.cisco.com/application/pdf/paws/97066/dhcp-option-43.pdf [Viitattu 23.6.2009]

16. Understanding the DHCP Protocol (Part1) [online] Saatavana osoitteesta: http://www.windowsnetworking.com/articles_tutorials/Understanding-DHCP-Protocol-Part1.html [Viitattu 15.3.2010]

17. What is ISCDHCP and what does it do? [online] Saatavana osoitteesta: http://www.isc.org/software/dhcp/about [Viitattu 15.3.2010]

18. VMware Workstation – Run Multiple OS Including Linux on Windows on Virtual Machines [online] Saatavana osoitteesta: http://www.vmware.com/products/workstation/ [Viitattu 16.3.2010]

19. VMware ESXi: Bare Metal Hypervisor [online] Saatavana osoitteesta: http://www.vmware.com/products/esxi/ [Viitattu 18.3.2010]

20. The Vim commands cheat sheet [online] Saatavana osoitteesta: http://www.tuxfiles.org/linuxhelp/vimcheat.html [Viitattu 1.2.2010]

21. Cisco Wireless LAN Controllers and DHCP option 43 [online] Saatavana osoitteesta: http://blog.pressure.net.nz/2009/01/cisco-wireless-lan-controllers-and-dhcp-option-43/ [Viitattu 23.6.2009]

22. Staattisen IP-osoitteen määrittäminen [online] Saatavana osoitteesta: http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch03_:_Linux_Networking [Viitattu 24.11.2009]

23. Tietoeväste Oy: Datariina_pohjakuvat_101008_pdf.pdf

24. Datariinan langattomien verkkojen kartoitus, suoritettu 20.1.2009

25. Datariina | Varattavat tilat [online] Saatavana osoitteesta: http://webserver.tietoevaste.fi/datariinantilavaraus/ [Viitattu 13.2.2010]

26. HP ProCurve MultiService Controller Series [online] Saatavana osoitteesta: http://www.procurve.com/products/wireless/HP_ProCurve_MultiService_Controller_Series/overview.htm#J9325A [Viitattu 30.3.2010]

27. HP ProCurve 802.11a/b/g MultiService Access Point Series [online] Saatavana osoitteesta: http://www.procurve.com/products/wireless/HP_ProCurve_802_11a_b_g_MultiService_Access_Point_Series/overview.htm#J9374A [Viitattu 30.3.2010]

28. HP ProCurve 802.11n MultiService Access Point Series [online] Saatavana osoitteesta: http://www.procurve.com/products/wireless/HP_ProCurve_802_11n_MultiService_Access_Point_Series/overview.htm#J9427A [Viitattu 30.3.2010]

29. Power over Ethernet – The Definitive Resource [online] Saatavana osoitteesta: http://www.poweroverethernet.com/ [Viitattu 2.4.2010]