Opinnäytetyö (AMK)

Elektroniikka

Tietoliikennejärjestelmät

2015

Miikka Arola

LANGATTOMIEN LÄHIVERKKOJEN HALLITTU TUOTANTOONSIIRTO

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Elektroniikka | Tietoliikennejärjestelmät

Toukokuu 2015 | 35

Juha Nikkanen

MIIKKA AROLA

LANGATTOMIEN LÄHIVERKKOJEN HALLITTU TUOTANTOONSIIRTO

Tässä opinnäytetyössä käsiteltiin Turun kaupungin IT-palvelun käynnistämää projektia, jossa tuotannollisia ja hallinnollisia tietoverkkoja levitettiin keskitetysti hallittavalla, ohjausjärjestelmäpohjaisella WLAN-arkkitehtuurilla. Opinnäytetyön tarkoituksena oli selvittää WLAN-verkon suunnitteluun liittyviä seikkoja, esittää ohjausjärjestelmäpohjaisen lähiverkkoratkaisun toimintaa ja kuvailla projektin eri vaiheita. Toteutettu verkkoratkaisu mahdollistaa WLAN-verkkojen levittämisen tietoturvallisesti Turun kaupungin eri toimipisteisiin.

Aikaisemmin käytössä olleessa, ei-keskitetyssä verkkoratkaisussa esiintyi luotettavuuteen, kapasiteettiin, peittoalueeseen ja käytettävyyteen liittyviä ongelmia. Verkon tekninen hallinnointi ja tietoturvaratkaisut olivat vanhentuneita. Uusi langaton lähiverkkoratkaisu oli tarve toteuttaa, jotta pystyttäisiin vastaamaan jatkuvasti kehittyvän WLAN-teknologian asettamiin vaatimuksiin palveluiden ja suorituskyvyn osalta.

WLAN-verkkoratkaisun eduksi osoittautui kustannustehokas ja keskitetty hallinta, joka tapahtuu yhdestä pisteestä, sen sijaan että useita tukiasemia tarvitsisi hallita erikseen. Järjestelmä osoittautui käyttäjäystävällisemmäksi aiempaan verrattuna ja sillä pystytään tarjoamaan monipuolisia palveluita sekä kapasiteettia suurellekin käyttäjämäärälle.

Työn tulokset osoittivat että ohjausjärjestelmäpohjainen verkkoratkaisu soveltuu hyvin laajamittaisiin langattomiin lähiverkkoihin, jossa verkolta vaaditaan monipuolisuutta ja hallinnan helppokäyttöisyyttä.

ASIASANAT:

BYOD, WLAN, CUWN

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Electronics | Telecommunication Systems

May 2015 | 35

Juha Nikkanen

Miikka Arola

DEPLOYMENT OF WIRELESS LOCAL AREA NETWORKS

This thesis is part of a project initiated by the city of Turku IT-services, in which wireless local area networks were distributed with centralized and controller-based WLAN architecture. The thesis introduces the network deployment process, theory of WLANs and the functions of controller-based WLAN architecture. The purpose of this thesis was to investigate WLAN design issues and to present the benefits of a controller-based WLAN solution.

The previously used, non-centralized network solution suffered from reliability, capacity, coverage and usability problems. The old network's technical management and security solutions were out of date. These problems created the need for the new wireless local area network implementation. The controller-based WLAN solution was selected in the project because it is suitable with current and upcoming ICT-technologies.

The advantages of the controller-based network solution turned out to be cost effectiveness and centralized management. Instead of manually managing a large number of access points, the controller-based architecture automates the distribution of configurations to each access point.

The results demonstrated that the controller-based architecture is well suited for large-scale wireless local area network implementations, where demand for bandwidth is high and management is required for ease of use.

KEYWORDS:

BYOD, WLAN, CUWN

SISÄLTÖ

KUVAT JA KAAVIOT

KÄYTETYT LYHENTEET

BYOD	Päätelaiteriippumattomuus (Bring Your Own Device)
CLI	Komentorivipohjainen ympäristö (Command Line Interface)
dBi	Antennin vahvistus verrattuna isotrooppiseen antenniin (The forward gain of an antenna compared with the isotropic antenna)
https	Suojattu tiedonsiirto (Hypertext Transfer Protocol Secure)
Hz	Taajuus (frequency)
IEEE 802.11	IEEE:n standardi langattomille WLAN-lähiverkoille (the Institute of Electrical and Electronics Engineers Specification for wireless local area networks)
ISM	Maailmanlaajuinen radiotaajuuskaista, joka on tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön (Industrial, Scientific and Medical)
IT	Informaatioteknologia (Information Technology)
LAN	Lähiverkko (Local Area Network)
MAC	IEEE 802-verkkojen verkon varaamiseen ja liikennöinnin hoitava osajärjestelmä (Medium Access Control)
Mb/s	Megabittiä sekunnissa
MIMO	Lähetykseen ja vastaanottoon käytetään samanaikaisesti useampaa kuin yhtä antennia (Multiple-Input and Multiple-Output)
OFDM	Useiden kantoaaltojen yhtäaikainen modulaatio (Orthogonal Fre quency-Division Multiplexing)
OSI	Tiedonsiirtoprotokollien yhdistelmien kerros (Open Systems Interconnection Reference Model)
PoE	Käyttöjännitten syöttö datakaapelissa (Power Over Ethernet)
PSK	Esijaettu todennusavain (Pre-Shared key)
QoS	Tietoliikenteen luokittelu ja priorisointi (Quality of Service)
RADIUS	Protokolla laitteiden todentamiseen (Remote Authentication Dial In User Service)
SNR	Signaalin ja kohinan välinen suhde (Signal to Noise Ratio)
SSID	Langattoman lähiverkon tunnus (Service Set Identifier)

VLAN	Dataliikenne kulkee samassa fyysisessä lähiverkossa, mutta eri loogisessa lähiverkossa (Virtual Local Area Network)
W	Tehon yksikkö (Unit of power)
WAN	Laajaverko (Wide Area Network)
WLAN	Langaton lähiverkko (Wireless Local Area Network)

1 JOHDANTO

Langattomien lähiverkkojen tiedonsiirtonopeudet ja kapasiteetin käyttö ovat jatkuvassa kasvussa. Uusien WLAN-standardien ja niiden tuomien tekniikoiden myötä langattomat lähiverkot ovat toiminnaltaan luotettavia, mikä mahdollistaa WLAN-verkkoratkaisun toteuttamisen erilaisiin käyttöympäristöihin. Laajan mittakaavan toteutuksissa keskitetty hallinta tekee WLAN-verkon ylläpidosta helppokäyttöistä ja kustannustehokasta.

Opinnäytetyössä tarkasteltiin Turun kaupungin IT-palveluiden käynnistämää projektia, jossa toteutukseltaan vanhentunut ja ei-keskitetty lähiverkkoratkaisu korvataan Cisco Systemsin kehittämällä, keskitetysti hallittavalla ohjausjärjestelmäpohjaisella WLAN-arkkitehtuurilla. Keskitetyssä lähiverkkoratkaisussa WLAN-tukiasemia hallinnoidaan keskitetysti yhdestä pisteestä, sen sijaan että jokaista tukiasemaa tarvitsisi hallita erikseen.

Työn tavoitteena on selvittää keskitetysti hallittavan lähiverkkoratkaisun toteutusta ja suunnittelua. Työssä tarkastellaan ohjausjärjestelmäpohjaisen lähiverkkoratkaisun tekniikkaa ja sen tarjoamia palveluita. Tämän lisäksi työssä käsitellään yleisluontoisesti langattomien lähiverkkojen teoriaa, järjestelmiä ja tietoturvaa.

Kaupungin verkkoa palveleva opinnäytetyö keskitetystä hallinnasta on tehty Lahden ammattikorkeakoulussa (Sipilä 2009). Projektiluontoista opinnäytetyötä, jossa tukiasemia asennetaan laajamittaisesti kaupungin eri toimipisteisiin ei ole aikaisemmin tehty.

2 LANGATTOMIEN LÄHIVERKKOJEN TEORIAA

Langattomalla lähiverkolla tarkoitetaan WLAN-tekniikkaa, jolla päätelaitteilla voidaan muodostaa langattomasti yhteys reitittimeen ja sen kautta laajempaan verkkoon. WLAN-tekniikan avulla langalliset yhteydet korvataan radioaalloilla toimiviin yhteyksiin, mahdollistaen liikkuvuuden langattoman lähiverkon kantaman sisällä ja vähentäen näin työpistesidonnaisuutta. Langaton lähiverkko mahdollistaa verkon luomisen mm. kaupunkiympäristöön, tehdashalleihin ja paikkoihin, jonne langallisen yhteyden luominen olisi vaikeaa tai mahdotonta.

Sovellukset ja teknologiat, jotka käyttävät tiedonsiirrossa langallista yhteyttä ovat siirtymässä yhä useammin WLAN-tekniikkaan. Tämä edellyttää langattomien lähiverkkojen standardeilta parannuksia tiedonsiirtonopeuksiin ja tekniikoihin, jotta suorituskyky olisi yhdenvertaista langallisen verkon kanssa.

2.1 IEEE 802.11

IEEE on kansainvälinen elektroniikka ja sähkötekniikka alan järjestö, jonka alaisuudessa toimiva IEEEn 802.11-työryhmä määrittelee standardeja langattomalle lähiverkolle. Langattomille lähiverkoille määritellyt standardit kuvaavat OSI-mallin kahta alinta siirtokerroksen osaa, johon kuuluvat fyysinen kerros ja siirtokerroksen MAC-alikerros. Fyysinen kerros vastaa tiedonsiirrosta lähettimestä vastaanottimeen, käyttäen eri modulaatiomenetelmiä ja taajuusalueita. Siirtokerroksen MAC-alikerros vastaa tiedonsiirron kulusta kehystämällä tiedonsiirrossa käytetyn paketin fyysistä kerrosta varten. [1]

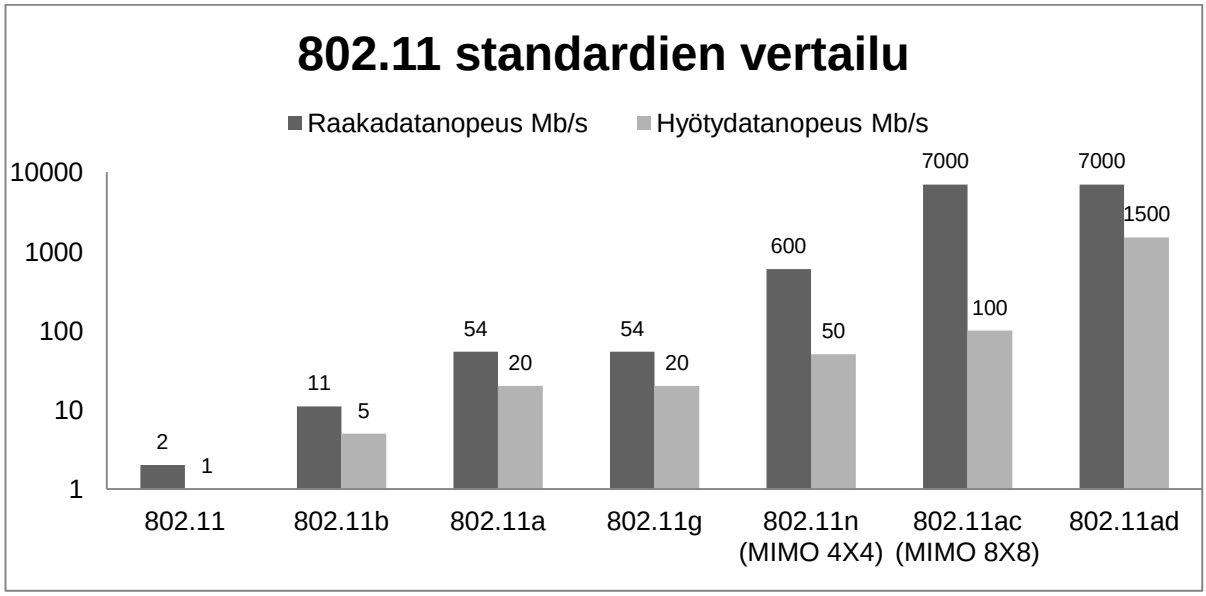
IEEEn julkaisema alkuperäinen versio 802.11-standardeille kuvaa langattoman lähiverkon MAC-kerrosta ja kolmea fyysisen kerroksen tiedonsiirron toteutustapaa. Fyysisiin kerroksiin sisältyvät infrapunataajuus ja kaksi modulaatiotekniikkaa 2,4 GHz:n ISM-taajuusalueella, jotka ovat suorasekvensointi DSSS (Direct Sequence Spread Spectrum) ja taajuushyppely FHSS (Frequence Hopping Spread Spectrum), standardin teoreettinen datanopeus on 1 Mb/s ja 2 Mb/s. [2]

802.11b-standardi on laajennus alkuperäiseen 802.11-standardiin ja on sen kanssa yhteensopiva tukien samoja datanopeuksia. Standardiin lisätyllä CCK (Complementary code keying) modulointitekniikan avulla saavutetaan teoreettiseksi datanopeudeksi 11 Mb/s. [1]

802.11a-standardi lisää alkuperäiseen standardiin OFDM-modulointitekniikan uutena fyysisenä kerroksena ja 5 GHz:n taajuusalueen käytön, standardin teoreettinen datanopeus on 54 Mb/s. [1]

802.11g-standardilaajenuus käyttää 2,4 GHz:n taajuusaluetta ja on yhteensopiva aiempien standardien kanssa, tukien eri datanopeuksia riippuen käytettävästä modulointitekniikasta. Standardin teoreettinen datanopeus käyttäen OFDM-modulaatiotekniikkaa on 54 Mb/s. [1]

IEEEn 802.11-standardit ovat kehittyneet tiedonsiirtonopeuksissa ja modulaatiomenetelmissä. Standardien todellinen tiedonsiirtonopeus eli hyötydatanopeus riippuu käytettävästä virheenkorjausmenetelmistä, modulaatiomenetelmästä sekä signaalireitistä (Kuvio 1.).



Kuvio 1. IEEEn 802.11-standardien raakadatanopeus ja arvioitu hyötydatanopeus. [1, 3, 4]

2.1.1 802.11n-standardi

IEEEn 802.11n-standardin päätavoitteena on kasvattaa datanopeutta ja kehittää luotettavampaa tiedonsiirron onnistunutta perillemenoa (engl. throughput), lisäksi saavutetaan laajempi verkon kantama ja pienempi virrankulutus edeltäviin standardeihin verrattuna. Standardi eroaa edeltäjistään tarjoamalla erilaisia parannuksia, kuten MIMO-tekniikan (Multiple Input Multiple Output), joka tarkoittaa useamman kuin yhden antennin käyttöä lähetyksessä sekä vastaanotossa. Spesifikaatio kehitettiin ottaen huomioon aikaisemmat standardit ja varmistaen yhteensopivuus tällä hetkellä yleisimmin käytössä olevien laitteiden kanssa. [2]

Standardiin lisättiin 20 MHz:n lisäksi vaihtoehto myös 40 MHz:n kaistanleveydelle, jossa kaksi 20 MHz:n rinnakkain olevaa kanavaa yhdistetään 40 MHz:n kanavaksi ja näin datanopeus voidaan kaksinkertaistaa. Haittapuolena tässä on pieni kanavien määrä. 2,4 GHz:n toimintataajuudella on tilaa kolmelle ei-päällekkäiselle 20 MHz:n kanavalle, 40 MHz:n kanava ei jätä riittävästi tilaa muille rinnakkaisille kanaville, joten sitä ei ole hyödyllistä käyttää 2,4 GHz:n toimintataajuudella. Tämän vuoksi älykäs ja dynaaminen hallinta on tärkeää. 5 GHz:n taajuusalueen vaatimukseen kuuluu, että tukiasema siirtyy toiselle kanavalle havaitessaan häiriön. [2]

802.11n–standardissa on mahdollista käyttää kaksi tai neljä antennia signaalin lähetyksessä ja vastaanotossa. 802.11n-spesifikaatiossa on MIMO virransäästötila, joka vähentää virrankulutusta käyttämällä useita antenneja vain silloin kun radioyhteys hyötyy siitä. [2]

Virheenkorjauksessa käytetty FEC (Forward Error Coding) lisää redudanssia signaaliin ja havaitsee tiedonsiirrossa tapahtuneen virheen, jolloin se voidaan korjata ilman signaalin uudelleenlähetystä. FEC-koodaustason nostaminen 802.11a/g-standardeissa käytetystä 3/4:stä 5/6:een tarkoittaa 5 databittiä 1:tä korjausbittiä kohden. Parannetulla koodaustasolla saadaan lähetetyn OFDM-paketin hyötydataosuutta kasvatettua 75 %:sta 83 %:iin. [2]

802.11n-standardissa on lyhennetty OFDM-modulointimenetelmässä käytettävää suojavälin kestoa. Suojaväli liitetään OFDM-symbolin eteen ja se antaa vastaanottimelle aikaa vastaanottaa useita kantoaaltoja sekoittamatta sen toimintaa, sekä vähentämällä edellisen lähetetyn symbolinheijastuksesta aiheutuvaa monitie-etenemisen häiriötä. 802.11n-standardissa suojavälin kestoksi voi valita lyhyemmän 400 nanosekuntia kestävän suojavälin, jolla saavutetaan 10%:n parannus suorituskykyyn tai vaihtoehtoisesti pitää suojaväli 800 ns:ssa, jota aiemmat 802.11a/g-standardin versiot käyttävät. [2]

2.1.2 802.11ac-standardi

IEEEn 802.11ac-standardi on julkaistu jatkokehityksenä 802.11n-standardille, ottaen huomioon 802.11a/n–standardien mukaisten päätelaitteiden yhteensopivuuden 5 GHz:n taajuusalueella. Standardi toimii ainoastaan 5 GHz:n taajuusalueella, joten kahden radion 802.11n–standardin mukaiset päätelaitteet ja tukiasemat käyttävät 2,4 GHz:n taajuusaluetta. Standardin teoreettinen nopeus on 7 Gb/s. Aikaisempia standardeja nopeammat datanopeudet saavutetaan käyttämällä 80 MHz:n ja 160 MHz:n kaistanleveyksiä, suorituskykyisempää modulointitekniikkaa ja MIMO 8x8, joka mahdollistaa kahdeksan lähetys- ja vastaanottoantennia, kahdeksalla rinnakkaisella datavirralla. [3]

Uutena ominaisuutena 802.11ac-standardissa on multi-user MIMO (MU-MIMO) -tekniikka, joka mahdollistaa tukiasemaa lähettämään useita kehyksiä rinnakkaisilla datavirroilla samanaikaisesti useille päätelaitteille. MU-MIMO-tekniikka soveltuu päätelaiteriippumattoman palveluympäristön mallille, jossa kommunikoidaan samanaikaisesti usean eri käyttäjän ja päätelaitteiden kesken mm. älypuhelimien ja tablettien välityksellä. [3]

2.1.3 802.11ad-standardi

IEEEn 802.11ad-standardin teoreettinen datanopeus on 6,75 Gb/s, jolloin se pystyy vastaamaan yhä nopeamman ja enemmän kaistaa vaativan tiedonsiirron tarpeisiin, kuten pakkaamattoman teräväpiirtovideon suoratoistolle. Uutena ominaisuutena standardissa on 60 GHz:n taajusalueen käyttö, jolloin antenneista saadaan pienikokoisia ja näin laitteista kompakteja. Standardissa käytettävä taajuus on vähäisessä käytössä eikä samalla kanavalla toimi muita laitteita kuten esimerkiksi mikroaaltouuni tai bluetooth laitteet, jolloin viereiset kanavat eivät haittaa radiosignaalia. [4]

Standardi on suunniteltu käytettäväksi 1 - 10 m säteellä, sillä 60 GHz:n toimintataajuudella aallonpituus on vain 5 mm. Tämän vuoksi radiosignaali on herkempi häiriöille ja siinä esiintyy enemmän häviöitä 2,4 GHz:n ja 5 GHz:n standardien käyttämiin toimintataajuuksiin verrattuna. Standardissa käytetään onnistuneen perillemenon saavuttamiseksi ryhmäantenneja ja beamforming-teknologiaa, jolla radiosignaali saadaan tehokkaammin suunnattua lähettimeltä vastaanottimelle amplitudia ja vaihetta muuttamalla. [4]

2.2 MIMO-tekniikka

MIMO-tekniikka on ollut käytössä jo 802.11g–standardissa, mutta nämä ovat olleet laitevalmistajien omia ratkaisuja eivätkä ne ole keskenään yhteensopivia. 802.11n–standardi tukee MIMO-tekniikkaa mahdollistaen enintään neljä vastaanotto- ja lähetysantennia.

Monitie-etenemisessä signaalireitti kulkee eri kohdista, jolloin osa lähetetystä signaalista saapuu vastaanottimeen kuten pitääkin ja osa saavuttaa vastaanottimen kulkien pidemmän reitin, jolloin signaaliin on muodostunut vaihe-eroa ja muita häviöitä. Vastaanottimeen saapunut signaali on tällöin alkuperäisen ja heijastumien yhdistelmä, jonka seurauksena signaalin laatu on heikentynyt tai kokonaan vaimentunut. [5]

MIMO-tekniikka hyödyntää radiosignaalin diversiteettiä vastaanotossa. Antenneihin saapuvat signaalit ovat hieman erilaatuisia monitie-etenemisen ja muiden häviöiden vuoksi ja todennäköisesti toiseen antenniin saapuva signaali ei ole heikentynyt haittaavasti. Vastaanotin yhdistää siihen saapuneet signaalit ja prosessoi niistä parempilaatuisen. Diversiteettiä hyödyntämällä on mahdollista kompensoida monitie-etenemisestä aiheutuneet häviöt ja parantaa radiosignaalin onnistunutta perillemenoa. [5]

Useat antennit ja rinnakkaiset datavirrat (engl. Spatial Stream) ilmoitetaan yleensä muodossa A x B:C, jossa A on lähetysantennien lukumäärä, B on vastaanottoantennien lukumäärä ja C on rinnakkaisten datavirtojen lukumäärä. Rinnakkaisilla datavirroilla on suora vaikutus datanopeuteen. Sama informaatio lähetetään useina sen kopioina, jolloin monitie-etenemisestä aiheutuneiden häviöiden haitat vähenevät ja vastaanotetun signaalin SNR-arvo kasvaa. [5]

2.3 WLAN-tietoturva

WLAN-tekniikalla toimiviin tietoverkkoihin on mahdollista murtautua, sillä tiedonsiirto tapahtuu radioaaltojen välityksellä ja käytettävät taajuudet ovat löydettävissä siihen tarkoitetulla laitteistolla. IEEEn 802.11–standardin WLAN-verkkoihin on määritelty erilaisia yhteyden salaus- ja todentamismenetelmiä, joiden tarkoitus on estää verkon luvaton käyttö. Käytössä olevat salausalgoritmit ovat vahvoja ja niiden salausavainten murtaminen on käytännössä työlästä.

Ohjausjärjestelmäpohjaisessa CUWN (Cisco Unified Wireless Network) verkkoarkittehtuurissa, jossa tukiasemia on tuhansia kappaleita, tulee myös erilaiset tietoturvauhat ottaa huomioon. Organisaatioiden tietoverkoissa on usein aineistoa, jotka vääriin käsiin joutuessa saattavat aiheuttaa merkittävää taloudellista ja toiminnallista haittaa. Tietoturvaan liittyviä uhkakuvia on monenlaisia ja niihin varautuminen vaatii ennakoivia toimenpiteitä.

Ohjausjärjestelmässä on seuraavia menetelmiä tietomurtojen havaitsemiseksi ja niiden estämiseksi:

- wIPS (wireless Intrusion Prevention System) havaitsee Man in the Middle hyökkäykset, MAC-osoitteen väärentämisen, rogue-tukiasemat, palvelunestohyökkäykset ja verkkohyökkäysohjelmistojen käytön.
- IDS (Intrusion Detection System) havaitsee virus- ja haittaohjelmat sekä hyökkäykset palveluja, käyttäjäoikeuksia ja ohjelmiston haavoittuvuuksia vastaan.
- Cisco CleanAir-teknologia tarkkailee signaalin laatua ja optimoi sen toimimaan oikeilla taajuusalueilla häiriöiden välttämiseksi analysoimalla tietoa WLAN-verkon signaalin laadusta ja verkon tietoturvauhista. [6]

2.3.1 Valetukiasemat

Valetukiasemalla (rogue-tukiasema) tarkoitetaan tukiasemaa, joka on luvattomasti kytketty WLAN-verkkoon ilman että verkon ylläpitäjä olisi tietoinen siitä. Nämä tukiasemat voidaan sijoittaa piilotettuina samalle alueelle, jossa varsinainen infrastruktuuriverkko sijaitsee. Valetukiasema on asetettu toimimaan eri kanavalle kuin oikea tukiasema ja sen käyttämä SSID-tunnus on sama kuin oikeaan WLAN-verkkoon kuuluvan tukiaseman tunnus. Ruuhkauttamalla oikean tukiaseman käytössä olevan kanavan alkavat päätelaitteet verkkovierailla valetukiaseman SSID:n kautta oikean tukiaseman sijaan, jonka kautta on mahdollista päästä sisäverkkoon.

Ohjausjärjestelmäpohjaisessa WLAN-verkossa tukiasemat tarkkailevat kanavia siirtymällä hetkellisesti pois omalta kanavaltaan muille kanaville ja samalla keräten paketteja, joista se havaitsee toimiiko muilla kanavilla valetukiasemia. Havaitessaan tukiaseman joka ei toimi yhdessä ohjausjärjestelmän kanssa se luokitellaan rogue-tukiasemaksi. Prime–hallintakäyttöliittymä havaitsee nämä tukiasemat ja estää päätelaitteita ottamasta siihen yhteyttä. [6]

2.3.2 Ad hoc–verkot

Ad hoc -verkoissa yhteys luodaan suoraan laitteiden välille ilman tarvetta tukiasemalle, jolloin kyseiset verkot ovat organisaation tietoturvan ulottumissa. Verkkoa luodessa päätelaitteet saattavat ottaa samanaikaisesti yhteyden organisaation lähiverkkoon WAN-yhteyden kautta. Hyökkääjä voi näin sillata yhteyden ja päästä käsiksi sisäverkkoon.

CUWN havaitsee luvattomat ad hoc -verkot niiden lähettämien kehysten perusteella, jotka poikkeavat infrastruktuuriverkon kehyksistä. Havaitessaan nämä kehykset CUWN pystyy ehkäisemään niistä aiheutuvat tietoturvariskit lähettämällä todennuksen purku kehyksen, jolloin laitteet eivät liikennöi ad hocin kautta. [6]

2.3.3 Palvelunestohyökkäys

Palvelunestohyökkäyksellä pyritään ruuhkauttamaan verkkoa ja lamaannuttamaan sen toimintaa. Palvelunestohyökkäys voidaan toteuttaa lähettämällä tukiasemalle suuri määrä kyselypyyntöjä tai todennuskehyksiä, jolloin palvelin ylikuormittuu. Tämän kaltaiset hallinta kehykset lähetetään ilman todennusta ja salaamattomina. Todennuksen ja assosioinnin purkuun liittyvät kehykset luokitellaan hallinta kehyksiksi, jotka havaitaan MFP-mekanismilla (Management Frame Protection), jonka tarkoituksena on torjua palvelunestohyökkäys. [6]

Ohjausjärjestelmä luo yksilöllisen tunnuksen, joka lisätään jokaiseen lähetettävään hallinta kehykseen. Kehykseen tehdyt muutokset havaitaan MIC-toiminnolla (Message Integrity Check), jolloin tuntemattomalta SSID-tunnukselta tukiasemalle saapuva hallinta kehys havaitaan ja ilmoitetaan ohjausjärjestelmälle. Tukiaseman saadessa MFP-suojatun kehyksen tuntemattomalta SSID-tunnukselta se pyytää ohjausjärjestelmältä siihen liittyvää tunnistetta. Jos ohjausjärjestelmä ei tunnista tukiaseman kattaman solun

tunnistetta BSSID (Basic Service Set ID), se palauttaa unknown BSSID -viestin ja tukiasema pudottaa kehyksen ja katkaisee näin yhteyden. [6]

2.3.4 BYOD tietoturva

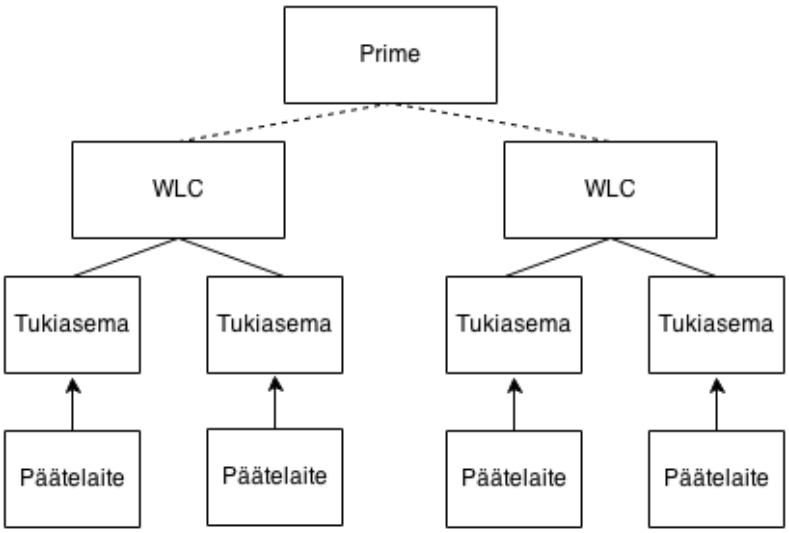
Päätelaiteriippumattomassa BYOD (Bring Your Own Device) ympäristössä, jossa työntekijät käyttävät omia laitteitaan työntekoon, tulee myös sen tuomat tietoturvauhat ottaa huomioon. Yrityksen sisäverkkoon kytketyissä päätelaitteissa saattaa olla haittaohjelmia tai verkkovakoiluun tarkoitettuja ohjelmistoja. Tämän vuoksi on tärkeää turvata organisaation tietoturva esimerkiksi rajaamalla laitteiden käyttöoikeuksia tai ohjaamalla ne niille tarkoitettuihin kohderyhmiin.

ISE (Identity Services Engine) on turvallisuuskäytäntöjen hallintaan tarkoitettu rajapinta, joka yhdistää ja automatisoi pääsynvalvontaa, yksilöiden erilaisten laitteiden yhteyden muodostamista lähiverkkoon ja sen tarjoamiin resursseihin. WLAN-verkkoon liittyviltä Laitteilta vaaditaan todennus RADIUS-palvelimen kautta, joka ohjaa laitteet eri virtuaalilähiverkoihin. Laitteilta voidaan ryhmäkohtaisesti rajata tietyt palvelut osittain tai kokonaan pois, sekä palvelunlaadun avulla jakaa valikoivasti kaistanleveyttä. ISE:n avulla on mahdollista profiloida eri päätelaitteet niiden käyttämän MAC-osoitteen perusteella. Päätelaitteiden profiili tallennetaan ja siitä pystytään keräämään erilaisia tietoja, kuten kaistanleveyden käyttö ja eri palveluiden tarve, jonka avulla päätelaitteelle pystytään jatkossa antamaan käyttöön samat resurssit ja palvelut. [7]

3 KESKITETYSTI HALLITTAVA WLAN-JÄRJESTELMÄ

Laajamittainen langattoman lähiverkon levitys Turun kaupungin eri toimipisteisiin asettaa verkolle erilaisia haasteita liittyen sen suorituskykyyn ja ylläpitoon. WLAN-verkon tulee olla toiminnallisesti luotettava, sillä työpisteiden päätelaitteet käyttävät lisääntyvissä määrin langatonta verkkoa langallisen sijasta. Toimipisteisiin tulee yhteensä noin 3 000 tukiasemaa ja kohteet sijaitsevat maantieteellisesti toisistaan kaukana. Laajamittaiselta verkolta vaaditaan skaalatutuvuutta sekä dynaamista toimintaa.

CUWN on keskitetysti hallittava, ohjausjärjestelmäpohjainen verkkoarkkitehtuuri (Kuva 1.). Järjestelmä koostuu WLC (Wireless LAN Controller) ohjausjärjestelmistä ja niihin kytkeytyneistä LAP (Lightweight Access Point) tukiasemista. Järjestelmää hallinnoidaan Prime (Cisco Prime Infrastructure) hallintakäyttöliittymällä, jonka kautta konfiguroidaan ohjausjärjestelmiä ja niihin kytkeytyneitä tukiasemia. Konfiguraatiot ja tukiasemien päivitykset levitetään keskitetysti Primen kautta kaikille tukiasemille. Tukiasemat eivät toimi itsenäisesti ilman ohjausjärjestelmää, niiden täytyy ensiksi löytää ohjausjärjestelmä ja rekisteröityä siihen. [2]



Kuva 1. Keskitetysti hallittava WLAN.

3.1 Keskitetyn hallinnan hyödyt ja haitat

Aiemmin käytössä olleet, itsenäisesti toimivat ei-keskitetyt (engl. standalone) tukiasemat vaativat jokaisen tukiaseman yksittäistä konfiguroimista. Tämä vaatii paljon työmäärää verkon ylläpidolle lisäten kustannuksia. Tukiaseman vikaantuessa ylläpitohenkilökunnan täytyy mennä kohteeseen selvittämään vika ja WLAN-verkko voi olla kauankin pois käytöstä. Ei-keskitetyt tukiasemat puolestaan soveltuvat pienimittaisiin lähiverkkoratkaisuihin, jossa tukiasemia hallinnoidaan paikallisesti.

Keskitetty hallinta luo älykkään tukiasemaverkoston, jossa tukiasemat havaitsevat verkkoympäristössä ilmenevät häiriöt ja pystyvät sopeutumaan niihin. Yhden tukiaseman vikaantuessa sen vieressä olevat tukiasemat nostavat lähetystehoa, paikaten muodostuneen katvekohdan. Virhetilanteiden selvitys ja konfiguraatiomuutosten tekeminen onnistuu keskitetysti hallintakäyttöliittymän kautta. Uusien tukiasemien lisääminen verkkoon ei vaadi asetusten tekemistä jokaiselle yksittäiselle tukiasemalle, vaan asetukset, määritykset ja tukiasemien päivitykset levitetään keskitetysti yhdestä pisteestä. Tämä helpottaa huomattavasti useiden tukiasemien asennustöihin liittyviä toimenpiteitä, vähentäen tukiasemien ylläpitoon vaadittavaa työmäärää ja säästäen näin kustannuksista. Liikuttaessa tukiasemalta toiselle (engl. roaming) päätelaitteen asetukset ovat jaettu tukiasemien kesken, jolloin käyttäjä ei havaitse peittoalueen vaihtumista. Useat päätelaitteet muodostavat automaattisesti yhteyden langattomaan lähiverkkoon niiden WLAN-radion ollessa päällä, jolloin siirtyminen toimipisteen peittoalueen ulottumista toisen toimipisteen peittoalueelle mahdollistaa verkon nopean käyttöönoton. [2]

Haittapuolina keskitetty verkkoratkaisu vaatii kustannuksia ohjausjärjestelmien, lisenssien ja tukiasemien hankintaan sekä niiden ylläpitoon liittyen. Myös toimipisteiden verkkoinfrastruktuuria täytyy paikoitellen uusia, jotta se toimisi tehokkaasti keskitetysti hallitussa ratkaisussa. Tämä lisää kustannuksia mm. kytkimien ja kaapeloinnin osalta. Tukiasemien ollessa riippuvaisia ohjausjärjestelmästä, ensisijaisen ohjausjärjestelmän vikaantuessa verkko

toimii kuten pitääkin, mutta molempien vikaantuessa koko verkosta tulee toimintakyvytön. Molempien ohjausjärjestelmien samanaikainen vikaantuminen on kuitenkin hyvin epätodennäköistä, sillä ne sijaitsevat turvallisissa kohteissa ja ovat maantieteellisesti toisistaan etäällä. Ohjausjärjestelmä edellyttää huolellista konfigurointia, jossa tulee ottaa huomioon palveluiden ja kapasiteetin tarve. Väärin konfiguroitu ohjausjärjestelmä saattaa muodostua pullonkaulaksi ja hidastaa näin verkon toimintaa. Hallintakäyttöliittymässä on paljon parametreja verkon eri toiminnoille, jolloin on mahdollista tehdä verkon asetuksista tarpeettoman monimutkainen. Tämä saattaa osaltaan johtaa tilanteeseen, jossa käytön kannalta tarpeettomia ominaisuuksia on kytketty päälle ja verkon toiminta hidastuu. [2]

3.2 Ohjausjärjestelmä

Cisco 8500 -sarjan ohjausjärjestelmä valittiin mm. koulujen ja kirjastojen tukiasemien hallinnointiin. Näissä verkoissa kapasiteetin tarve on suurempi kuin virastojen verkoissa laajemman käyttäjämäärän vuoksi ja ohjausjärjestelmään on myös liitetty enemmän tukiasemia. Cisco 5500 -sarjan ohjausjärjestelmä valittiin virastojen tukiasemien hallinnointiin, sillä näissä verkoissa edellytetään kapasiteettia ja käytettävyyden luotettavuutta.

Taulukossa 1 on nähtävissä molempien ohjausjärjestelmien tekniset ominaisuudet.

Taulukko 1. Ohjausjärjestelmien tekniset ominaisuudet. [8, 9]

Ominaisuudet	**Cisco 5500**	**Cisco 8500**
Ethernet I/O	8 x 1G	2 x 10G
Tukiasemat	500	6000
Päätelaitteet	7000	64000
VLAN	512	4092
Standardit	802.11a/b/g/n/ac	802.11a/b/g/n/ac

Ohjausjärjestelmät (Kuva 2.) huolehtivat tukiasemien määrityksistä sekä ohjelmiston ajantasaisuudesta. WLAN-verkon toiminnan kannalta kriittisenä komponenttina ohjausjärjestelmä on kahdennettu laitepariksi eli klusteroitu, järjestelmä kopioi asetukset sekä tiedot rekisteröityneistä tukiasemista klusterin jäsenien kesken.

Kuva 2. Ciscon ohjausjärjestelmiä. [8]

Ohjausjärjestelmässä on portteja, rajapintoja ja loogisia WLANeja, joiden ympärille langaton lähiverkkoyhteys kokonaisuudessaan rakentuu (Kuva 3.). Portit ovat ohjausjärjestelmän fyysisiä liitäntöjä, jotka jakavat yhteyden kytkimille ja sitä kautta edelleen tukiasemille. Rajapinnat ovat loogisia yhteyksiä, jotka määrittelevät IP-osoitteen, oletusyhdyskäytävän, VLAN-merkkauksen, ensi- ja toissijaisen fyysisen portin sekä DHCP-palvelimen. WLANit ovat loogisia kokonaisuuksia, mitkä yhdistävät niiden jakamat SSID:t tiettyyn rajapintaan. WLANille konfiguroidaan langattoman lähiverkon tietoturva, palvelunlaatu ja muut vastaavanlaiset määritykset. [9]

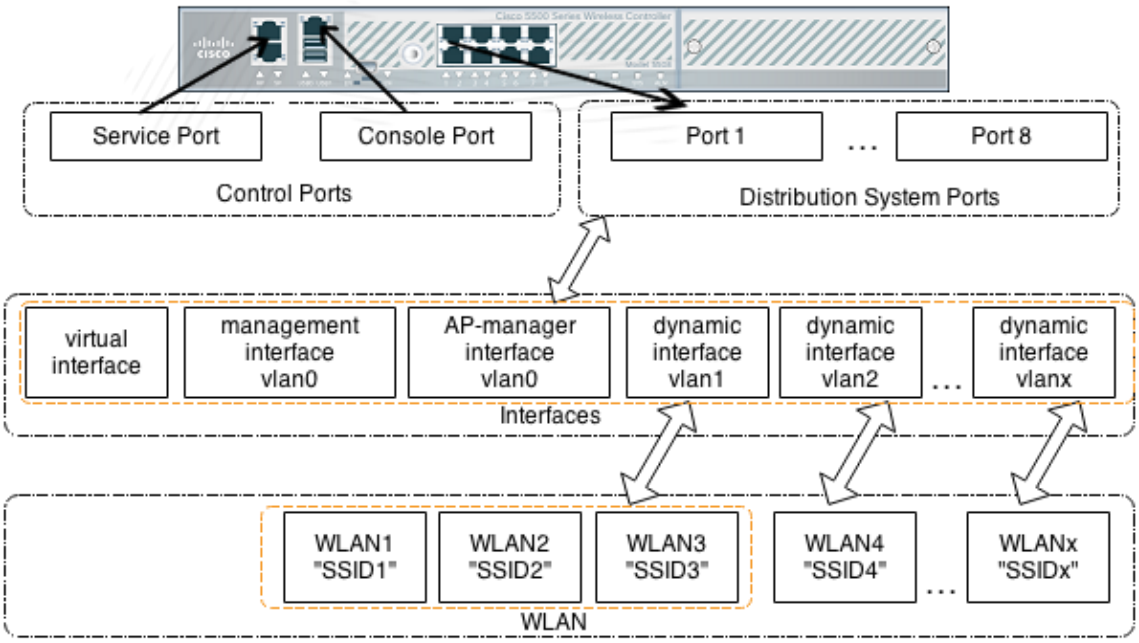
Fyysisiin dataportteihin (Distribution System Ports) liitetään kytkin ja ne ovat määritelty toimimaan 802.1Q-standardin mukaisesti trunk-portteina, jolloin siinä kulkee useamman VLANin dataliikenne samanaikaisesti. Fyysiset kontrolliportit (Control Ports) ovat tarkoitettu vianselvitykseen ja järjestelmän palauttamiseen tilanteissa, jossa sen käyttäminen ei onnistuisi normaalin hallintakäyttöliittymän kautta. [9]

Hallintarajapinnan (Management interface) kautta hallitaan ohjausjärjestelmää ja sen yhteyksiä Radius-todennuspalvelimiin, sekä käsitellään tason kaksi yhteyksiä ohjausjärjestelmän ja tukiasemien välillä. [9]

Tukiasemien hallintarajapinnan (AP-manager interface) kautta määritellään asetukset, joilla tukiasemat toimivat eri aliverkossa kuin ohjausjärjestelmä. Rajapinta käsittelee tason kolme yhteyksiä ohjausjärjestelmän ja tukiasemien välillä. [9]

Virtuaaliset rajapinnat (Virtual interface) hallitsevat ohjausjärjestelmän mobility group -asetuksia, mikä mahdollistaa verkkovierailun ohjausjärjestelmien välisten tukiasemien kesken. Rajapinta hallitsee myös VPN-yhteyksiä, web-todentamista ja DHCP:n välittämistä. [9]

Dynaamisia rajapintoja (Dynamic interface) luodaan tarpeellinen määrä ja niiden välittämä liikenne päätetään SSID kohtaisesti paikalliseen VLANiin tai tunneloidaan ohjausjärjestelmälle. Rajapinnoista jokainen määritellään yhdeksi VLANiksi, joiden kautta jaetaan WLAN-yhteydet. [9]



Kuva 3. Ohjausjärjestelmän portit ja rajapinnat. [6, kuvaa muokattu]

3.3 Tukiasema

Cisco 1600 –sarjan tukiasemat (Taulukko 2.) ovat sisäkäyttöön tarkoitettuja ja niitä toimitetaan sekä ulkoisilla että integroiduilla antenniratkaisuilla. Toteutuksessa valittiin pääosin käytettäväksi kuvassa 4. näkyvä oikeanpuolinen tukiasema, jossa ei ole ulkoisia antenneja. Valintaan päädyttiin esteettisyyden vuoksi, sillä integroitu malli sulautuu asennettavaan ympäristöön.

Tukiasemissa on kolme antenniliitäntää, joihin on mahdollista liittää ympärisäteilevä dipoliantenni, jolla saavutetaan laajempi peittoalue. Ulkoisia tukiasemamalleja käytetään tiloissa, jossa tukiasema asennetaan korkealle ja siltä vaaditaan laajempaa kattavuutta. Tällaisia tiloja ovat esimerkiksi liikuntasalit, luentosalit ja näyttämöt.

Tukiasemien teknisiin vaatimuksiin kuuluu tuki 802.3af-standardin mukaiselle PoE-tekniikalla (Power Over Ethernet) toteutettavaan sähkönsyöttöön, missä käyttöjännite ja dataliikenne kulkee samassa parikaapelissa. Toimiakseen sekä tukiasemien että kytkimien täytyy tukea kyseistä tekniikkaa. Käytössä on myös PoE-injektoreita, jossa kytkimestä tukiasemalle lähtevän parikaapelin välille asetetaan verkkovirtaan kytkettävä adapteri, millä sähkö- ja dataliikenne toteutetaan. PoE-injektoreita käytetään kohteissa, joissa kytkin ei tue kyseistä tekniikkaa tai kohteeseen asennetaan ainoastaan yksi tukiasema.

Taulukko 2. Tukiasemien tekniset ominaisuudet. [10]

Ominaisuudet	**Cisco 1600**
Taajuusalue	2,4-2,5 GHz & 5,15-5,85 GHz
Antennivahvistus	2,4 GHz: 4 dBi & 5 GHz: 4 dBi
Standardit	802.11a/b/g/n
MIMO	3 x 3:2

Tukiasemissa käytetään MIMO 2x2 ratkaisua, jotta se toimisi 802.3af-standardin mukaisella PoE-ratkaisulla, jota suurin osa toimipisteiden käytössä

olevista kytkimistä tukee. Asennuksessa täytyy myös huomioida pitkän kaapeloinnin aiheuttamat jännitehäviöt.

Kuva 4. Cisco 1600-sarjan tukiasemat. [10]

3.4 CAPWAP-protokolla

Tukiaseman ja ohjausjärjestelmän välisessä tiedonsiirrossa käytetään CAPWAP-protokollaa (Control and Provisioning of Wireless Access Points), jolla liikenne tunneloidaan. CAPWAP tunneloidussa liikenteessä tukiasema etsii ohjausjärjestelmän verkosta ja sen kautta välitetään tukiasemien keräämiä tietoja ohjausjärjestelmälle mm. käyttäjistä ja verkkoympäristöstä. [6]

Tukiasemille on esiasennuksena määritelty ohjausjärjestelmän IP-osoite, jonka avulla se löytää ohjausjärjestelmän ja lataa CAPWAP-tunneloidun liikenteen kautta määritykset sekä päivitykset. Mikäli tukiasemalle ei ole esiasennuksena määritelty ohjausjärjestelmän IP-osoitetta, on tukiasemalla mahdollisuus löytää ohjausjärjestelmä, vaikka se olisi eri aliverkossa. Ohjausjärjestelmän IP-osoite voidaan vaihtoehtoisesti myös vastaanottaa DHCP-palvelimelta tai etsiä DNS-kyselyllä. [6]

CAPWAP-protokollan aloittaessa tukiaseman etsintä- ja liittymisvaiheen, tukiasema lähettää etsintäpyyntöjä ohjausjärjestelmän hallintarajapinnoille, jotka vastaavat lähetettyihin etsintäpyyntöihin. Seuraavaksi ohjausjärjestelmä vastaanottaa tukiaseman lähettämän liittymispyynnön, jonka jälkeen tukiasema jää odottamaan liittymisvastausta. Ohjausjärjestelmä todentaa tukiaseman ja

lähettää sille liittymiskutsun. Myös tukiasema todentaa ohjausjärjestelmän ja lopuksi kuittaa CAPWAP -protokollan etsintä- ja liittymisvaiheet valmiiksi. [6]

Tukiaseman liityttyä ohjausjärjestelmään se lähettää CAPWAP heartbeat -viestin ohjausjärjestelmälle tietyin väliajoin, johon ohjausjärjestelmä vastaa CAPWAP acknowledgment -viestillä. Mikäli tukiasema ei saa yhteyttä ohjausjärjestelmään, se käynnistää itsensä uudelleen ja toistaa edellä mainittua etsintä- ja liittymisprosessia, kunnes ohjausjärjestelmä löytyy. [6]

3.5 Vikasietoisuus

Langattomalle lähiverkolle voidaan määritellä ensisijainen, toissijainen ja tertiäärinen ohjausjärjestelmä kuormantasauksen ja redusoinnin vuoksi. CUWN-arkkitehtuuri tarjoaa kolme vaihtoehtoa ohjausjärjestelmän redusoinnille.

Ensisijainen ja redudanttinen ohjausjärjestelmä ilmoitetaan yleensä muodossa N:1, N:N ja N:N:1, jossa N on lähiverkkoa palveleva ensisijainen ohjausjärjestelmä ja numero 1 viittaa runkoverkossa olevaan redudanttiseen ohjausjärjestelmään. [2]

Ohjausjärjestelmän vikasietoisuusvaihtoehdot:

- N:1 on tarkoitettu pääosin verkkoratkaisuihin, jossa on useampi ohjausjärjestelmä ja investointikustannukset ovat korkeat. Redudanttinen ohjausjärjestelmä sijaitsee runkoverkossa tai datakeskuksessa ja se toimii varmuuskopiona useille ohjausjärjestelmille
- N:N ratkaisussa on kaksi ohjausjärjestelmää, joihin tukiasemat ovat asetettu liittymään. Toisen ohjausjärjestelmän hajotessa tukiasemat siirtyvät toissijaiselle ohjausjärjestelmälle.
- N:N:1 ratkaisussa osa tukiasemista on määritelty toimimaan ensisijaisella ohjausjärjestelmällä ja osa toissijaisella. Kaikki tukiasemat ovat määritelty käyttämään tertiääristä varmuuskopioitua ohjausjärjestelmää, joka on sijoitettu runkoverkon tai datakeskuksen yhteyteen.

Toteutettavassa WLAN-arkkitehtuurissa käytetään N:N redudanttista ratkaisua, jossa yhden ohjausjärjestelmän hajoaminen ei estä normaalin verkon toimintaa. Ensisijaisen vikaantuessa toinen ohjausjärjestelmä ottaa sen aseman, samoin tukiasemat jotka ovat rekisteröityneet ensisijaiselle ohjausjärjestelmälle, siirtyvät toissijaisen ohjausjärjestelmän hallintaan.

3.6 Päätelaiteriippumattomuus

Päätelaiteriippumaton BYOD-malli (bring your own device) on nostettu ohjaavaksi kehityskohteeksi langattoman lähiverkon suunnittelussa. Tämän kaltaiset laitteet ovat pääosin GSM- tai WLAN-verkoissa liikennöiviä älylaitteita. Kannettavat älylaitteet ovat helppokäyttöisiä ja suorituskykyisiä, mikä mahdollistaa työntekijöitä käyttämään omia tai yrityksen tarjoamia laitteita henkilökohtaisen käytön lisäksi myös työkäyttöön. Työpistesidonnaisuuden vähentyessä työntekijät voivat käyttää päätelaitteitaan työntekoon työpaikan ulkopuolella. Päätelaitteen ollessa yhteydessä työpaikan sisäverkkoon saadaan käyttöön samat resurssit ja palvelut, jotka ovat saatavilla työpisteessäkin. Tämä mahdollistaa enemmän liikkuvuutta työntekoon, jolloin työntekijälle jää enemmän aikaa hoitaa muita työasioita. [7]

Päätelaitteeseen asennetut sovellukset ovat yleensä työntekijän itsensä valitsemia ja niitä käytetään arkisten asioiden hoitamiseen. Sovellusten käytön ollessa tuttua niitä voidaan tehokkaasti hyödyntää työntekoon, eikä niiden käyttö vaadi erillistä koulutusta. Työntekijän käyttäessä omaa laitetta työntekoon, työpaikan ei tarvitse hoitaa laitetukeen liittyviä asioita, vaan se jää työntekijän vastuulle. Näin voidaan tehokkaasti säästää kustannuksista, kun päätelaitteen laitetuki on työntekijän vastuulla ja sovellusten käyttöön liittyvää koulutusta ei tarvitse järjestää. [7]

BYOD-mallia on sovellettu pääosin Turun kaupungin lukioissa. Oppilaille on jaettu opetuskäyttöön tarkoitettuja iPad tablet-tietokoneita, jonka avulla oppilas voi esimerkiksi jakaa reaaliaikaisesti omalta laitteeltaan näkyvää tietoa luokassa olevan Apple älytelevision kautta.

4 PROJEKTIN TAVOITTEIDEN JA TOTEUTUKSEN KUVAUS

Projektin tavoitteena on Turun kaupungin IT–ympäristöjen toteutuksen, ylläpidon ja hallinnan yhtenäistäminen, jolla saadaan koko kaupungin kattava langattomien lähiverkkojen toteutusmalli. WLAN-teknologialla kaupungin palveluita hyödynnetään hallittujen sekä hallitsemattomien päätelaitteiden kautta.

Projektin siirto tuotantoon viivästyi alkuperäisen suunnitelman mukaisesta aikataulusta, jonka mukaan asennustöiden arvioitiin valmistuvan vuosien 2013-2014 aikana. Viivästymisen syinä olivat pääosin tukiasemien asennustöiden lisääntyminen alkuperäiseen suunnitelmaan verrattuna, eikä alussa osattu ottaa huomioon yhden kohteen asennustöihin kuluvaa aikaa. Toteutuksen alkuvaiheessa ei tiedostettu pienien toimipisteiden verkkoinfrastruktuurin puutteellisuutta, minkä vuoksi niihin täytyi rakentaa verkon valmius tukiasemia varten. Sen sijaan isoissa kohteissa asennustyöt sujuivat helposti, sillä niissä on käytetty tietotekniikkaa pitkään ja kohteiden valmis verkkoinfrastruktuuri helpotti asennustöitä.

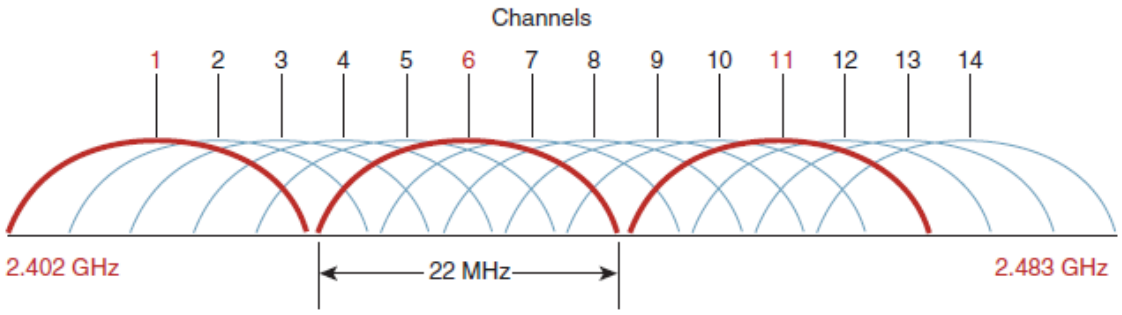
4.1 Lähtötilanteen kuvaus

Turun kaupungilla ei ole hyvinvointitoimialaa lukuun ottamatta käytössään ratkaisua hallinnollisten palveluiden tietoturvalliseen ja WLAN-tekniikalla toteutettuun langattomaan levitykseen. Käytössä on ollut ainoastaan Masterplanin tuottama Sparknet-palvelu, joka on ensisijaisesti tarkoitettu satunnaiseen asiakaskäyttöön. Sparknet on pistemäinen ja yksittäisistä ei-keskitetyistä, standalone-tukiasemista koostuva langaton lähiverkko, eikä se mahdollista tukiasemien keskitettyä hallintaa. Sparknetin tukiasemiin tehtävät muutokset suoritetaan paikallisesti ja yksitellen jokaiseen tukiasemaan. Turun kaupungin noin 550:n tukiaseman laajamittainen ja kaikkia tukiasemia koskeva muutos muodostuisi haasteelliseksi eikä se olisi kannattavaa.

4.2 Nykytilanteen ongelmia

Sparknetin käytettävyysongelma liittyy pääosin sen avoimeen kirjautumiseen, jolloin suuresta käyttäjämäärästä aiheutuu kapasiteettiongelmia. Häiriöt lisääntyvät alueilla, joissa tukiasemien peittoalueella käytetään samalla taajuusalueella toimivia langattomia laitteita. Häiriönlähteinä toimivat laitteet ovat esimerkiksi mikroaaltouunit ja Bluetooth-laitteet, jotka toimivat samalla ja vapaasti käytössä olevalla 2,4 GHz:n ISM-taajuusalueella kuin tukiasemat. Lisäksi 802.11g-standardin mukaiset tukiasemat ovat vanhenevaa tekniikkaa, jolloin toiminnan luotettavuus on heikkoa, eikä standardi pysty tarjoamaan nykyisin käytössä olevien laitteiden vaatimia palveluita ja suorituskykyä.

Sparknetin tukiasemien käyttämä 802.11g-standardi toimii 2,4 GHz:n taajuusalueella, jossa kanavien lukumäärä on 13. Taajuusalueella on mahdollista jakaa kolme ei-päällekkäistä (Kuva 5.) kanavaa samanaikaisesti. Tukiasemien tiheyden kasvaessa päätelaitteet joutuvat usein käyttämään samoja kanavia päällekkäin, tällöin tukiaseman peittoalue pienenee ja häiriöt lisääntyvät. Osa tukiasemista vaihtaa kanavaa automaattisesti häiriöiden lisääntyessä. Tämä kuitenkin saattaa aiheuttaa tilanteen, jossa tukiasema vaihtaa jatkuvasti kanavaa heikentäen siihen kytkeytyneiden päätelaitteiden signaalitasoa ja käytettävyyttä. [6]



Kuva 5. Päällekkäiset kanavat. [6]

4.3 Langattoman lähiverkon suunnittelu

Langattomien lähiverkkojen kantavuuden vaihteluväli on suuri ja signaalin eteneminen tapauskohtaista ympäristöstä riippuen. Lähetetty radiosignaali leviää laajemmalle alueelle sen edetessä pidemmälle, jolloin vastaantulevat esteet aiheuttavat signaalille heijastumia, taipumista ja taittumista. Sisätiloissa signaalireittiä häiritsevät useimmiten mm. seinät, hyllyt, ilmastointiputket ja muut signaalia heijastavat materiaalit.

Käytettävä taajuus vaikuttaa merkittävästi langattoman lähiverkon etenemiseen. Taajuuden kasvaessa radiosignaalin aallonpituus pienenee, jolloin se läpäisee heikommin esteitä kuin pienemmällä taajuusalueella toimiva langaton lähiverkko, jolla on puolestaan suurempi aallonpituus.

Samalla taajuusalueella saattaa toimia laitteita, jotka aiheuttavat häiriöitä ja vierekkäisillä tukiasemilla olevat kanavat voivat häiritä toisiaan. Suunnittelussa otetaan huomioon tarvittavat palvelut ja niiden vaatima kapasiteetti, kuten videopuhelut ja päätelaiteriippumattomuuden palvelut. Näistä saatujen tietojen pohjalta valitaan tukiasemien tarvittava määrä, tyypit ja sijainnit jotta kaikille verkon käyttäjille riittää kapasiteettia samoille palveluille eikä alueelle tulisi katvekohtia.

Ennen asennustöiden aloittamista kohteisiin suoritetaan Site Readiness sekä Site Survey kartoituskäynnit. Kohteen kartoituksen jälkeen seuraa asennusprosessin vaihe, jonka aikana rakennetaan kaapeliverkon valmius langattoman lähiverkon tukiasemia varten.

Toimipisteiden kartoituskäyneillä pohjakuviin merkittävät asiat:

- Ristikytkentäkaapelien paikat, kaapelointi ja asennettavien laitteiden kytkentäkohteet.
- Etäisyys ATK-rasioilta uusien tukiasemien asennuspaikkoihin.
- PoE kohteiden tarkastus vapaiden kytkinporttien riittävyydestä ja sähköpistokkeista.

- Tukiasemien paikat merkitään pohjakuviin nykyisten ATK rasioiden sijainnin perusteella.
- Ohjelmistolla tehtävissä kartoitusmittauksissa asetetaan mittauksissa käytettävät tukiasemat ATK-rasioiden kohdalle tai suoritetaan mittaus optimaalisilta paikoilta.

Site Surveyn aikana mitataan ensin tukiasemien optimaaliset paikat rakennuksessa ja laaditaan sen jälkeen tukiasemien asennussuunnitelma. Site readiness kartoituksessa ei tehdä mittauksia, vaan käydään ainoastaan tarkistamassa rakennuksen kaapeliverkon tilanne ja arvioidaan parhaimmat asennuspaikat tukiasemille. Pääsääntöisesti site survey tehdään isoille ja monimuotoisille kohteille. Pienissä ja arkkitehtuuriltaan selkeissä kohteissa tehdään vain site readiness kartoitus. Site Survey voidaan suorittaa kolmella tapaa: Passive, Active ja Predictive. [5]

Passive Site Survey suoritetaan tukiaseman monitorointitilassa, jolloin päätelaitteet eivät voi olla yhteydessä tukiasemaan. Näillä kartoituksilla pyritään löytämään tietoturvauhkia, kuten tietoja varastavat valetukiasemat tai paikallistamaan häiriöille alttiina olevat kohteet. [5]

Active Site Survey suoritetaan päätelaitteelle, joka on yhteydessä tukiasemaan kartoituksen aikana. Kartoituksen aikana päätelaitteen signaalitasoa tarkkaillaan sen siirtyessä tukiasemalta toiselle. Päätelaitteen liittyessä tukiasemaan sen datanopeus ja signaalitaso vaihtelee. Kartoituksesta saadun tiedon pohjalta, arvioidaan mihin uuden WLAN-verkon kattavuuden suunnittelussa tulisi kiinnittää huomiota ja minkälaisia vaatimuksia sen toiminnalle tulisi asettaa. Kartoitusmenetelmä voidaan toteuttaa kahdella eri tapaa: BSSID (Basic Service Set Identifier) metodilla päätelaite lukitaan tukiaseman radion MAC-osoitteeseen, jolloin päätelaitteelta estetään verkkovierailu. SSID (Service Set Identifier) metodilla tukiasema sallii päätelaitteelta verkkovierailun. [5]

Predictive Site survey suoritetaan ohjelmistolla, joka käyttää peittoalueen tietoja luodakseen simuloidun mallin tukiasemien optimaalisesta sijoittamisesta toimipisteeseen. Tämä kartoitusmenetelmä on tarkoitettu esimerkiksi

suunnitteilla oleviin toimipisteisiin, jotta saataisiin suunnittelutyöt nopeammin aloitettua ja tilattua toimipisteeseen soveltuvat järjestelmät ennen varsinaisten asennustoimenpiteiden aloittamista. [5]

4.4 Toteutus ja käyttöönotto

Turun kaupungin olemassa olevan langattoman lähiverkon (Sparknet) korvaaminen aloitettiin WLAN kehitysprojektina, jossa toteutetaan pilottikohteiden asennus ja käyttöönotto. Pilottikohteiksi valittiin toimipisteet, joissa henkilökunnalla on testaamiseen liittyvää tietoteknistä osaamista. Tällöin henkilökunta pystyy havaitsemaan WLAN-verkossa olevia häiriöitä ja ilmoittamaan niistä.

Ensisijaisiksi asennuskohteiksi kohteiksi koettiin koulut ja lukiot, jonka jälkeen tulivat virastojen neuvotteluhuoneet. Erityisesti lukioiden tarve ottaa verkkoa oppilaskäyttöön korostui tärkeäksi.

4.4.1 Valmistelevat toimenpiteet

Prosessin ensimmäinen vaihe koostuu valmistelevista toimenpiteistä ennen WLAN-tukiasemien kartoitusmittauksia ja niiden asennustöitä. Prosessin aikana suoritetaan PoE-kytkimien asennukset, hankitaan pohja- ja ATK-kuvat toimipisteeseen tehtävän kartoituksen vuoksi. Kohteen yhteyshenkilö kertoo, mitkä alueet tulee kattaa langattomalla verkolla. Tämän jälkeen toimittaja tekee ehdotuksen tukiasemien sijoittelusta ja mallista. Lisäksi määritetään kattavuusvaatimukset niille alueille, joihin halutaan täydellinen langattoman lähiverkon peitto.

Asennuksessa huomioitavaa ovat erityiskohteet, kuten suojeltavat kohteet ja kosteat tilat. Suojeltavissa kohteissa tukiasemaa ei tulisi asentaa näkyvälle paikalle, eikä niihin saa tehdä rakenteellisia muutoksia esimerkiksi kaapelivalmiutta varten, tällöin WLAN-yhteys on mahdollista välittää toimipisteeseen toistimen avulla. Kosteisiin tiloihin, kuten uimahalliin

asennettavat tukiasemat tulee suojata kosteudelta. Tukiasema asennetaan kuivaan tilaan ja WLAN-yhteys jaetaan ulkoisella antennilla allashuoneen puolelle.

4.4.2 Asennus ja määritykset

Tukiasemien asennustyöt aloitetaan kartoitusmittausten ja PoE-kytkinten asennusten valmistuttua. Ennen tukiasemien asennustöitä tulee myös määrittää Prime hallintakäyttöliittymään kohteiden pohjakuvat ja niiden mittasuhteet.

Toimipisteiden vanhat tukiasemat poistetaan ja uudet tukiasemat asennetaan niiden tilalle. Tukiasemien asennusten aikana päätelaitteille asennetaan WLAN-verkon todentamiseen tarvittavat toimipistekohtaiset sertifikaatit. Kytkimen porteille määritetään toimipistekohtaiset VLAN-tunnukset, jotka jakavat toimipisteeseen tulevat SSID:t.

Lähiverkon reitittimessä käytetään CentralSwitched-tunnelointia, jolloin siinä kulkeva dataliikenne tunneloidaan CAPWAP-protokollan kautta ohjausjärjestelmälle. Tukiasemissa käytetään FlexConnect–moodia, jolla dataliikenne päätetään tiettyyn paikalliseen VLANiin. [6]

4.4.3 Eri kohderyhmien palvelut

Uusi langaton lähiverkko tarjoaa useita kirjautumistapoja eri käyttäjä- ja kohderyhmille. IT-palveluiden tukemat päätelaitteet kirjautuvat automaattisesti langattomaan lähiverkkoon ja muiden päätelaitteiden liikenne ohjataan vierailijaverkkoihin, joista ei ole pääsyä tulostimiin tai muihin vastaavanlaisiin sisäverkon tarjoamiin palveluihin.

Käyttäjän kirjautuessa työasemalleen, yhteys muodostetaan oikeaan langattomaan lähiverkkoon riippuen käyttäjän tunnuksesta ja profiilista. Käyttäjän kirjautuessa jatkossa työasemalleen, laite osaa kirjautua oikeaan verkkoon ensimmäisellä kerralla tehtyjen asetusten perusteella.

Turku-A, Turku-O, Turku-P ja Turku-T ovat automaattisesti käyttöönotettavia verkkoja IT-palveluiden tukemille päätelaitteille, joihin IT-palvelut järjestävät tarvittavat laitekohtaiset asetukset. Käytössä ovat Turun kaupungin toimihenkilöille tarkoitetut sisäverkon palvelut.

Hallinto- ja opetusverkkojen verkkotunnukset:

- Turku-A (hallinto): hallintoverkon kannettaville laitteille josta on pääsy kaikkialle.
- Turku-O (oppilas): oppilaskäytössä oleville kannettaville tarkoitettu opetusverkko, joka jakautuu henkilökunnan ja oppilaiden päätelaitteisiin.
- Turku-P (oppilaitosten henkilökunta): opetusverkon henkilökuntaosuus, joka mahdollistaa joihinkin henkilökunnan palveluihin pääsyn.
- Turku-T (terveys): hyvinvoinnin ja terveydenhuollon toimipisteissä käytettävä verkko. Esimerkiksi vuodeosastoilla on tässä verkossa olevia kannettavia, jotka kulkevat mukana lääkärikierroilla.

Vierailijaverkkoja on käytössä kolme ja ne käyttävät eri todennusmenetelmiä. Päätelaitteet käyttävät valmistajakohtaisesti eri todennusmenetelmiä ja yhteensopivuusongelmien välttämiseksi verkkoihin on mahdollisuus kirjautua päätelaitteelle sopivalla todennusmenetelmällä.

Vierailijaverkkojen verkkotunnukset:

- Turku-Guest verkkoon kirjaudutaan käyttäjän omalla laitteella web-selaimen kautta ja istunto on voimassa määräaikaisesti. Tunnuksena käytetään sähköpostin käyttäjätunnusta ja vierailijoita varten luodaan määräaikaisia tunnuksia, joita voi tehdä vain Turun kaupungin verkosta. Verkko on tarkoitettu lähinnä satunnaiseen käyttöön.
- Turku-Personal verkkoon kirjaudutaan käyttäjän omalla laitteella. Kirjautuminen perustuu henkilökohtaiseen varmenteeseen ja verkko on tarkoitettu käyttäjien omille laitteille. Verkko on tarkoitettu jatkuvasti toistuvaan käyttöön.

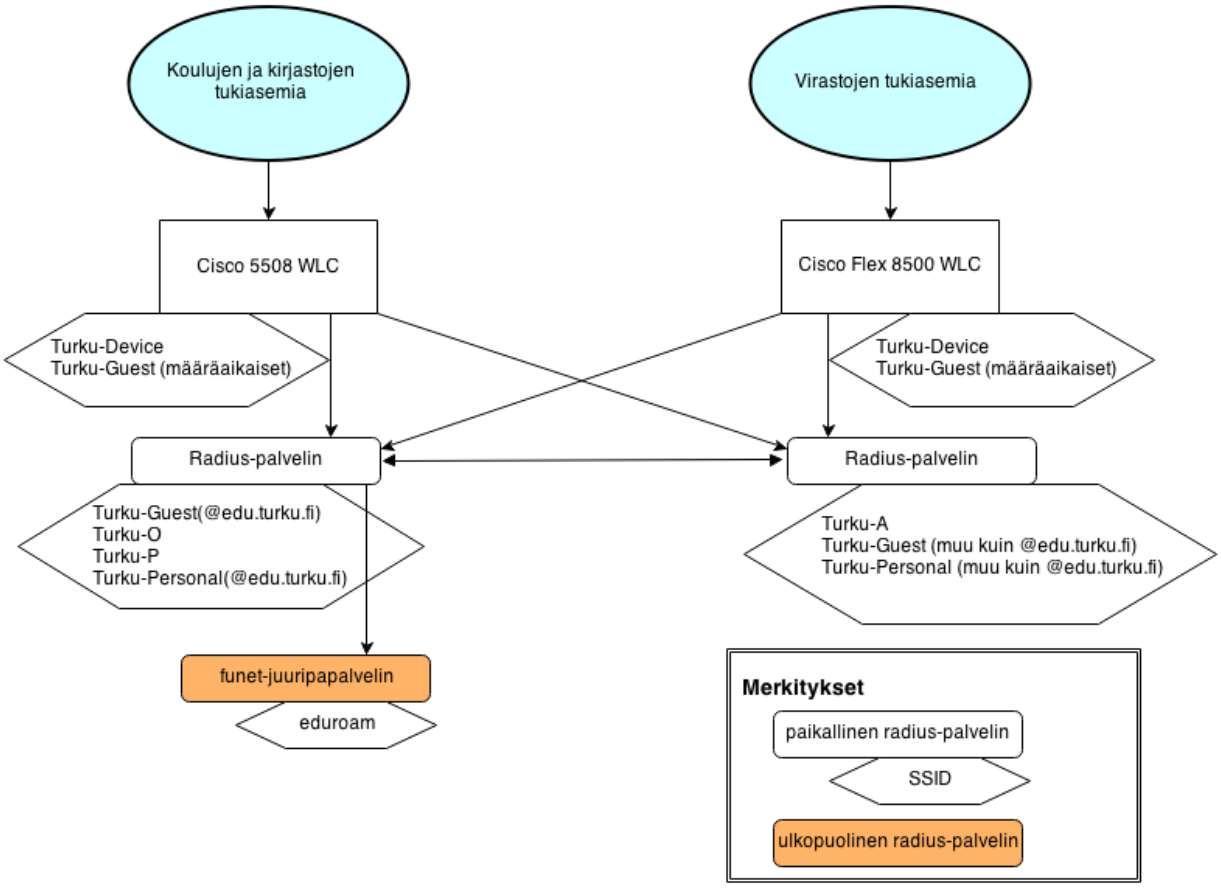
- Turku-Device verkkoon kirjaudutaan kaupungin omistamilla laitteilla. Tällaisia laitteita ovat mm. koulun omistamia iPad, Surface, Apple TV tai muut laitteet.
- Sparknet-verkkoa jaetaan uusien tukiasemien kautta. Verkko on toistaiseksi käytössä, mutta poistuu käytäntöjen yhtenäistyessä.

Kaikissa langattomissa lähiverkoissa vaaditaan kirjautuminen. SCCM (System Center Configuration Manager) ryhmäkäytäntö ohjaa laitteet hakemaan varmenteen RADIUS-palvelimelta, jota myös sparknet verkkoon kirjautuminen vaatii. Varmennetta pidetään voimassa määräaikaisesti ja työaseman Windows käyttöjärjestelmä osaa automaattisesti uusia varmenteen. Käyttäjäkohtaisissa varmenteissa käyttäjän tulee itse hoitaa varmenteen uusiminen, sillä niitä säilytetään käyttäjän ylläpitämissä laitteissa. Turku-Device verkkoon kirjaudutaan jaetulla salausavaimella (PSK), joka vaihdetaan vuosittain. Web-kirjautumisissa käytetään sähköpostiosoitetta ja salasanaa, yhteys on suojattu https-yhteydellä ja salasana vaihdetaan määritetyn vaihtoajan mukaisesti.

4.4.4 Verkkotopologia

Langattomaan lähiverkkoon luodaan tarpeellinen määrä verkkotunnuksia (SSID), joita tukiasemat ja ohjausjärjestelmät hallinnoivat (Kuva 6.), molempiin ohjausjärjestelmään luodaan samannimiset ja -sisältöiset SSID:t. Kaikki langattoman lähiverkon tukiasemat levittävät hallinnon, opetuksen ja vierailijaverkkotunnuksia. Toimipisteen tai ryhmän levittämät SSID:t valitaan toimipistekohtaiseen AP Groupiin.

AP Grouping ominaisuudella ohjausjärjestelmän yksittäinen WLAN-rajapinta tukee useampaa VLANia, jolloin sen kautta voidaan jakaa useampaa toimipistekohtaista SSID:tä. AP Grouping ominaisuutta hyödyntämällä ohjausjärjestelmään on mahdollista liittää useampi päätelaite, mitä ohjausjärjestelmän lisenssi sallii. [6]



Kuva 6. Toteutettava verkkotopologia.

Päätelaite käyttää EAP-protokollaa (Extensible Authentication Protocol) muodostaessaan yhteyden tukiasemaan avoimella todentamisella. Tukiasema lähettää päätelaitteelle EAP Request-paketin, joka sisältää tunnistetietojen pyynnön verkkoon pyrkivältä päätelaitteelta. Päätelaite vastaa tähän lähettämällä tukiasemalle tunnistetiedot EAP Response-paketilla, joka välitetään todennettavaksi RADIUS-palvelimelle. Onnistuneessa todentamisessa RADIUS-palvelin lähettää EAP Success-paketin tukiasemalle ja päätelaitteelle, jonka jälkeen yhteys tukiasemaan sallitaan. [6]

Mikäli RADIUS-palvelimessa ei ole vaadittuja varmennustietoja, yhteys ohjataan funet-juuripalvelimeen, joka koordinoi Suomen osaa eduroamista.

5 JATKUVAT PALVELUT

Langattomaan lähiverkkoon kuuluvia laitemääriä, kapasiteetteja sekä tukipalveluita voidaan jatkossa kehittää, laajentaa tai muuttaa tarpeiden mukaan. WLAN-tekniikka ja siihen liittyvät päätelaitteet kehittyvät jatkuvasti, joten jatkokehityksen kannalta on oleellista huomioida verkon suorituskyky muuttuvassa ympäristössä.

5.1 Langattoman lähiverkon hallinta

Cisco Prime Infrastructure (Prime) on graafinen hallintakäyttöliittymä, jonka kautta hallitaan CUWN (Cisco Unified Wireless Network) arkkitehtuuria, johon kuuluvat ohjausjärjestelmät sekä tukiasemat. Yhteys hallintakäyttöliittymään muodostetaan selain- tai komentorivipohjaisella yhteydellä.

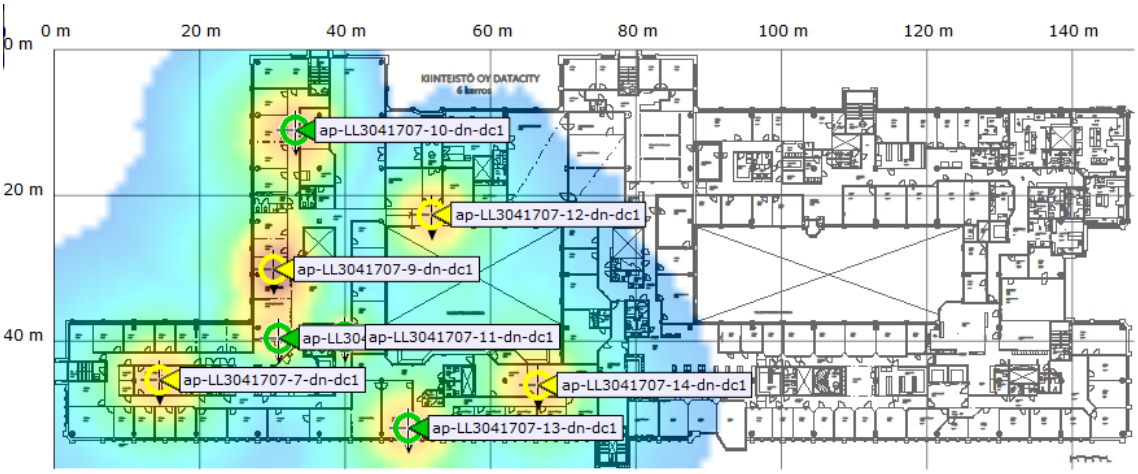
Prime hallintakäyttöliittymän kautta ohjausjärjestelmien asetuksia voidaan vaihtaa, joka puolestaan levittää muutokset tukiasemiin. Prime kerää tukiasemilta tietoa siihen liittyneistä päätelaitteista, peittoalueista ja häiriöistä. Näiden tietojen pohjalta saadaan kokonaiskuva langattoman lähiverkon toiminnasta ja häiriöistä. [2]

Prime ei ole kriittinen osa järjestelmää sillä se vastaa ainoastaan ohjausjärjestelmiin tehdyistä asetuksista. Hallintakäyttöliittymällä voi tarkkailla tukiasemien välittämää tietoa langattomaan lähiverkkoon liittyneiden päätelaitteiden määrästä, tiedoista ja niiden käyttöhistoriasta. Tukiasemien ja niihin liittyvien päätelaitteiden reaaliaikainen analysointi verkon resurssien käytöstä, häiriöistä ja muista kerätyistä tiedoista auttaa ohjausjärjestelmää parantamaan koko verkon toimintaa. [2]

Prime hallintakäyttöliittymä:

- Suunnittelu (design) tarjoaa ominaisuuksia ja malleja, joiden pohjalta toteutetaan verkon määritykset. Suunnittelutyökalujen avulla luodaan muokattavissa olevia mallipohjia verkon määritysten ja asetusten toteuttamiseen.
- Käyttöönotto (deploy) mahdollistaa suunniteltujen mallien, määritysten ja ominaisuuksien käyttöönoton. Käyttöönotossa määritellään millä tavalla ja missä verkon alueella mallit ja niiden määritykset toteutetaan.
- Käyttö (operate) monitoroi verkon käyttöä, tukiasemia ja niihin liittyviä päätelaitteita sekä havaitsee ongelmatilanteita. Tämän kautta voidaan myös tehdä rajatusti määritystietoja.
- Raportointi (report) kerää tietoa järjestelmän tilasta ja verkon häiriöstä. Näistä tiedoista luodaan tilastoja verkkoon liittyneistä laitteista ja kapasiteetin käytöstä.
- Hallinta (administration) hallinta-asetuksien kautta hallitaan Primen ja järjestelmään kuuluvien ohjausjärjestelmien sekä tukiasemien määritystietoja.

Toimipisteiden heatmap pohjakuvasta (Kuva 7.) näkee kohteessa olevat tukiasemat ja niiden simuloidun peittoalueen.



Kuva 7. Hallintakäyttöliittymän heatmap.

5.2 Ylläpitotasot

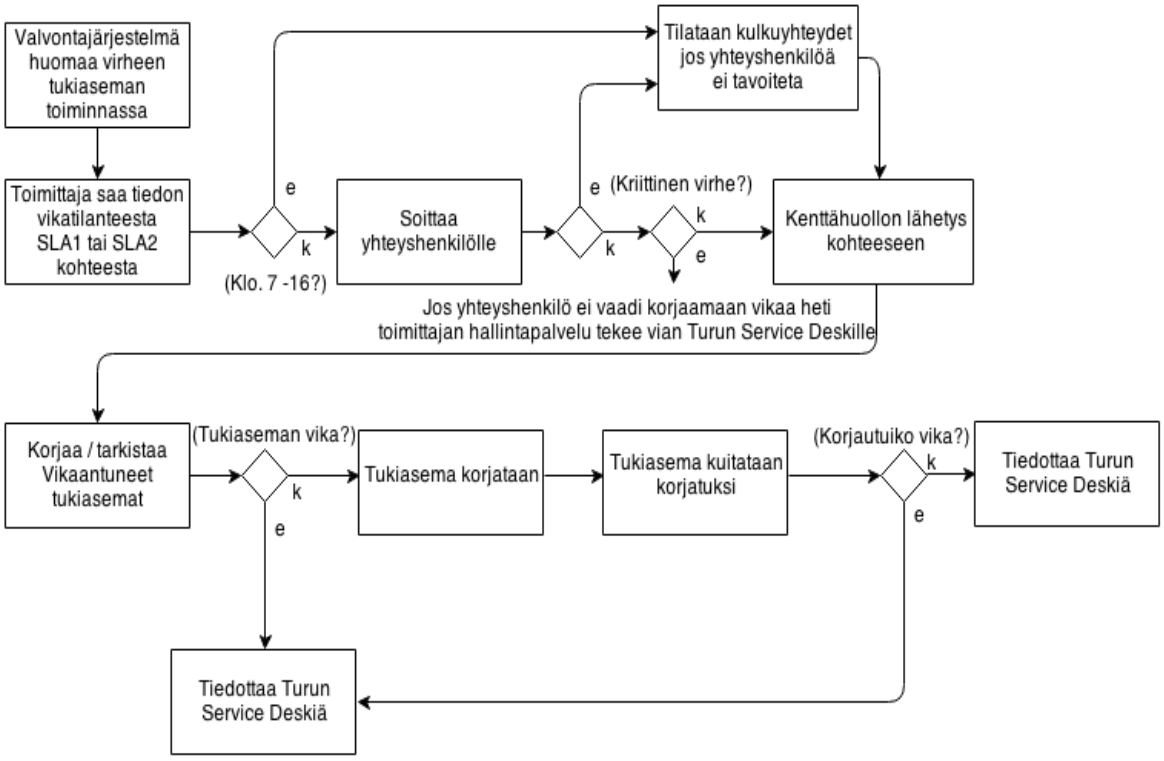
SLA (engl. Service Level Agreement) eli ylläpitotasoissa määritetään Toimittajan ja Asiakkaan välillä sovitut palveluiden laatutasot sekä niiden yksityiskohdat. Kuvatut ylläpitotasot liittyvät tukiasemiin ja ylläpitotasoon häiriön tai vian selvityksessä.

Ylläpitotason 1 osalta vikatilanteen korjausaika-arvio annetaan viimeistään yhden tunnin kuluessa vian rekisteröinnistä. Ylläpitotason 2 osalta arvio on annettava viimeistään kahden tunnin kuluessa ja ylläpitotason 3 osalta viimeistään seuraavan arkipäivän aamuna.

SLA 1-2 -tason kohteita ovat kohteita jotka vaativat laitteiden vikaantuessa välitöntä korjaustoimenpiteiden aloittamista. Kohteisiin kuuluvat ohjausjärjestelmät, terveyskeskukset, sairaalat ja palvelutalot. SLA 3-4 – tason kohteita ovat koulut, päiväkodit, virastot ja vanhainkodit.

- Ylläpitotaso 1: Vika on korjattu kaikkina viikonpäivinä ympärivuorokautisesti alle 2 tunnissa. Korjaavat toimenpiteet on aloitettava 15 minuutin kuluttua vikatilanteen ilmaantuessa.
- Ylläpitotaso 2: Vika on korjattu arkisin klo 7.30–18.00 alle 2 tunnissa. Korjaavat toimenpiteet tulee aloitettava 30 minuutin kuluttua vikatilanteen ilmaantuessa.
- Ylläpitotaso 3: Vika on korjattu arkisin työaikana alle 4 tunnissa. Korjaavat toimenpiteet on aloitettava yhden tunnin kuluttua vikatilanteen ilmaantuessa.
- Ylläpitotaso 4: Vika on korjattu viimeistään seuraavana työpäivänä.

Langattoman lähiverkon hälytys- ja vianselvitysprosesseille on määritelty kuvassa 8. näkyvät erilaiset toimintamenetelmät eri ylläpitotason alaisille kohteille. Vikahälytysprosessi lähtee joko loppukäyttäjän ilmoittamasta verkossa olevasta toimintahäiriöstä tai valvontajärjestelmän havaittua virheen tietyn tukiaseman toiminnassa.



Kuva 8. SLA vikahälytysprosessikaavio.

5.3 RACI

Tuotantoon jäävät tehtävät ja vastuut listataan RACI (Responsible Accountable Consulted Informed) toimenpidelistaan jossa kerrotaan, mitä tehdään, kuka tekee ja mihin mennessä. Ilman toimenpidelistaa voi unohtua mitä kenenkin pitää tehdä, koska työtehtäviä on paljon. [11]

RACI listan käsitteet:

- Responsible (vastuullinen) R-henkilö suorittaa annetun tehtävän tai kuuluu suoritustiimiin. Jokaisella tehtävällä on ainakin yksi R-henkilö.
- Accountable (vastuussa oleva) A-henkilö valvoo että tehtävä tulee tehtyä. Jokaisella tehtävällä on vain yksi A-henkilö.
- Consulted (neuvoja) C-henkilöltä voidaan kysyä ohjeita ja neuvoja. Jokaisella tehtävällä voi olla nollasta rajattomaan määrään C-henkilöitä.
- Informed (tiedotettava) I-henkilöä tiedotetaan tehtävän suorittamisesta. Jokaisella tehtävällä voi olla nollasta rajattomaan määrään I-henkilöitä.

Toimenpidelista WLAN palvelun tehtävistä ja vastuusta:

- WLAN toimitusprosessi: Asennuskohteiden pohjakuvat ja infrastruktuurimuutosten toteuttaminen toimipisteessä.
- Teknisen valmiuden valmistelun ylläpito: Käyttäjä ja työasema sertifikaattien jakelu, asennukset, päivitykset ja määritystietojen sekä kohteiden ylläpito.
- WAN verkon valmius: Lähiverkon suunnittelu, verkkoinfrastruktuuri, tilaukset, palvelinkomponenttien ylläpito ja asennusten koordinointi.

Näiden lisäksi tehtäviin ja vastuihin kuuluvat palvelunhallinta, laskutus ja raportointi, sidosryhmäyhteistyö sekä käyttäjätuki.

6 YHTEENVETO

Opinnäytetyössä suunniteltiin uusi langaton lähiverkko Turun kaupungin toimipisteiden verkkojen tietoturvalliseen levitykseen keskitetysti hallittavalla, ohjausjärjestelmäpohjaisella WLAN-arkkitehtuurilla. Työssä kuvailtiin Turun kaupungin IT-palveluiden käynnistämää projektia, keskitetyn hallinnan ominaisuuksia ja langattoman lähiverkon teoriaa.

Työssä kuvaillun WLAN-toteutuksen tavoitteena oli luoda eri kohderyhmille suunnatut palvelut ja pystyä vastaamaan olemassa olevan langattoman lähiverkkoratkaisun ylläpidon ja hallinnan tuomiin haasteisiin. Lopputuloksena saavutettiin yhtenäinen ja eri käyttötarpeisiin soveltuva langattoman lähiverkon ratkaisu- ja palvelukokonaisuus.

Toteutus mahdollistaa langattoman lähiverkkoyhteyden jakamisen hallinnoille, oppilaille ja vierailijoille. Uusi langaton lähiverkko tarjoaa helppokäyttöisen tavan kirjautua, suuren käyttäjämäärän sekä luotettavan tiedonsiirtoyhteyden. Laaja peittoalue tehostaa ylläpitoa ja käytettävyyttä, edistäen päätelaiteriippumattoman (BYOD) palveluympäristön toteutumista.

Jatkokehittämisen kannalta oleellisia asioita ovat kuntalaisten asiointipalveluiden kehittäminen, mobiililaitteiden ominaisuuksien laajamittaisempi hyödyntäminen päätelaiteriippumattomuuden näkökannalta, sekä puhe- ja tietoverkkojen integraatio.

LÄHTEET

[1] Viljay, K. & Garg. 2007. Wireless Communications and Networking: An Introduction. Burlington, MA, USA: Morgan Kaufmann.

[2] Smith, J.; Woodhams, J.; Marg, R. 2011. Controller-Based Wireless LAN Fundamentals.Indianapolis, IN USA: Cisco Press

[3] 802.11ac - The Fifth Generation of Wi-Fi Technical White Paper. [www-dokumentti]. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.pdf (Luettu: 13.4.2015)

[4] Wells, J. Multigigabit Microwave and Millimeter-Wave Wireless Communications. 2010. Norwood, MA, USA: Artech House

[5] Burton, Marcus; Head, Tom; Shawn, M. 2011. CWDP: Certified Wireless Design Professional Official Study Guide. Hoboken, NJ, USA: Sybex.

[6] Enterprise Mobility 7.3 Design Guide. 2013. [www-dokumentti]. Saatavilla: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73.html (Luettu 27.4.2015)

[7] Cisco Bring Your Own Device. [www-dokumentti]. Saatavilla: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf (Luettu: 17.4.2015)

[8] Cisco Wireless Controllers. [www-dokumentti]. Saatavilla: http://www.cisco.com/c/dam/en/us/products/collateral/interfaces-modules/services-modules/at_a_glance_c45-652653.pdf (Luettu: 20.4.2015)

[9] Cisco Wireless LAN Controller Configuration Guide, Release 8.0. [www-dokumentti]. Saatavilla: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.pdf (Luettu: 27.4.2015)

[10] Cisco Aironet Series 1600/2600/3600 Access Point Deployment Guide, Release 7.5 [www-dokumentti]. Saatavilla: http://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/7-5/Cisco_Aironet75.pdf (Luettu 17.4.2015)

[11] RACI. [www-dokumentti]. Saatavilla: http://fi.wikipedia.org/wiki/RACI (luettu 17.4.2015)