Pk-yrityksen langattoman verkon kartoitus, dokumentaatio ja jatkokehitys

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäki, syksy 2014

Jani Koski

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikan koulutusohjelma
Tietoliikenneverkot

Tekijä Jani Koski **Vuosi** 2014

Työnnimi Pk-yrityksen langattoman verkon kartoitus, dokumentaatio ja jatkokehitys

TIIVISTELMÄ

Työn toimeksiantajana toimi Isoworks Oy:n asiakas. Opinnäytetyö sai alkunsa asiakkaan tarpeesta saada selville sen kahden toimipisteen langattoman verkon nykytilanne ja niiden jatkokehitysvaihtoehdot.

Työn pääpaino oli asiakkaan langattoman verkon dokumentointi yhteen dokumenttiin, koska aikaisempi dokumentaatio koostui useista eri dokumenteista, eikä kaikkien langattomien verkkojen käyttötarkoitusta tiedetty.

Dokumentoinnin yhteydessä toimipisteissä suoritettiin langattoman verkon peittoalueen mittauksia ja selvitettiin tiedossa olevien ongelmien syitä. Toimipisteisiin tehtiin myös mittausten perusteella parannusehdotuksia muun muassa kanavasuunnitteluun.

Avainsanat 802.11-standardi, Langattomat lähiverkot, Langattoman verkon kuuluvuuden mittaus

Sivut 14 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Riihimäki
in Information Technology

Author Jani Koski **Year** 2014

Subject of Bachelor's thesis Small or medium-sized enterprise's wireless network mapping, documentation and further development

ABSTRACT

The subject of the thesis was commissioned by Isoworks Oy's customer. The thesis began with the customer's need to find out their two office's wireless network status quo and their future development options.

The main focus was getting the customer's wireless network documented into a single document, because previous documentations consisted of a variety of documents. In addition, all of the wireless network's using purposes were unclear.

Documentation includes coverage measurements of the wireless local area network at the customer's offices. These measurements were analyzed and any issues found were written down with their causes. Based on these findings, a set of propositions for improvements were issued to the customer. These improvements included changes to the channel design of the wireless network and other notes regarding the technical implementation of the network.

Keywords 802.11-standard, Wireless networks, Wireless network's coverage measurement

Pages 14 p.

SANASTO

Adapteri	Adapter	Adapterilla tarkoitetaan tekniikassa sovituslaitetta, joka mahdollistaa kahden erityyppisen komponentin yhteisen toimivuuden.
Autentikointi	Authentication	Autentikoinnilla tarkoitetaan tietotekniikassa identiteetin varmentamista.
Firmware	Firmware	Firmwarella tarkoitetaan laitteeseen kiinteästi asennettua ohjelmistoa tai sen osaa, joka kattaa laitteen perustoiminnot.
Krakkeri	Cracker	Krakkerilla tarkoitetaan henkilöä, joka murtautuu tietojärjestelmään ilman haltian lupaa.
Konfigurointi	Configuration	Konfiguroinnilla tarkoitetaan laitteen tai ohjelman asetusten määrittelemistä ja sen käyttöön ottoa.
Kontrolleri	Controller	Tietotekniikassa kontrollerit ohjaavat yhtä tai useamaa erillistä laitetta samanaikaisesti.
OFDM	Orthogonal frequency-division multiplexing (OFDM)	OFDM-modulointi mahdollistaa tiedon siirron usealla toisiaan häiritsemättömällä taajuuskanavalla samanaikaisesti.
Peittoalue	Coverage area	Langattomissa verkoissa peittoalueella tarkoitetaan tukiasemien kattamaa aluetta.
Protokolla	Protocol	Tietoliikenteessä protokollalla määritellään tai mahdollistetaan ohjelmien ja laitteiden väliset yhteydet.
Suorasekventointi	Direct-sequence spread spectrum (DSSS)	Suorasekventointia käytetään toteuttamaan koodijakokanavointia radioteiden kanavanvaraustekniikoissa.
Taajuushyppely	Frequency-hopping spread spectrum (FHSS)	Taajuushyppely on toinen tekniikoista DSSS:n lisäksi, jota käytetään toteuttamaan koodijakokanavointia radioteiden kanavanvaraustekniikoissa.
Tukiasema	Access Point (AP)	Langattoman lähiverkon tukiasema mahdollistaa laitteille langattoman yhteyden lähiverkkoon.

Verkkotunnus	Service Set Identifier (SSID)	Langattoman lähiverkon verkkotunnus, jonka avulla voidaan erottaa samalla alueella olevat WLAN-verkot toisistaan.
VLAN	Virtual LAN (VLAN)	Virtuaalinen lähiverkko, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin.
WLAN	Wireless Local Area Network (WLAN)	Langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

SISÄLLYS

1 JOHDANTO

Toimeksiantajana toimineen Isoworks Oy:n asiakas halusi selkolukuisemman dokumentaation kahden toimipisteen langattomista verkoista. Asiakkaan pyynnöstä työstä on tehty salainen ja julkinen versio, osa tiedoista on muutettu ja osa poistettu kokonaan, kuten liitteet. Tämä versio on julkinen. Tavoitteena oli siis kartoittaa ja dokumentoida asiakkaan toimipisteen 1 ja 2 langattomat verkot, niin että niissä havaitut ongelmat ja puutteet saataisiin korjattua. Lisäksi toivomuksena oli tehdä jatkokehitysehdotuksia kyseisten toimipisteiden langattomiin verkkoihin.

Työn pääpaino oli toimipisteiden langattomien verkkojen nykytilanteen kartoituksessa. Lisäksi työssä käydään läpi toimipisteiden mahdollisia kehitysvaihtoehtoja, perustuen kartoitukseen ja dokumentointiin.

Opinnäytetyön ensimmäisessä luvussa käydään läpi, minkälaisessa ympäristössä toimipisteiden verkot sijaitsevat, minkä jälkeen tutustutaan verkon kuuluvuuden mittaamiseen käytettyyn ohjelmaan ja sen ominaisuuksiin. Luvun lopussa tutustutaan molempien toimipisteiden mittausprosessiin.

Tekniikkaa käsittelevässä luvussa tutustutaan yleisimpiin langattomien verkkojen IEEE 802.11-standardeihin, joihin kuuluu myös uusin 802.11ac-standardi. Luvussa käydään läpi myös langattoman verkon tietoturvariskejä ja verkkojen salausmenetelmiä.

Opinnäytetyön kartoitus- ja dokumentointiosiossa tutkitaan toimipisteissä havaittuja ongelmia ja niiden syitä. Luvussa tutustutaan myös langattoman verkon käytössä oleviin verkkotunnuksiin (SSID) ja niiden käyttötarkoituksiin.

Viidennessä luvussa käsitellään mahdollisia kehitysvaihtoehtoja ja aiemmin havaittujen ongelmien korjausvaihtoehtoja. Lisäksi luvussa tutustutaan tukiasemien kanavasuunnitteluun, jolla pystyttäisiin minimoimaan vierekkäisten tukiasemien aiheuttamat häiriöt.

Opinnäytetyön lopuksi on vielä tarkasteltu opinnäytetyötä kokonaisuutena ja pohdittu tavoitteiden täyttymistä.

2 SUUNNITTELU

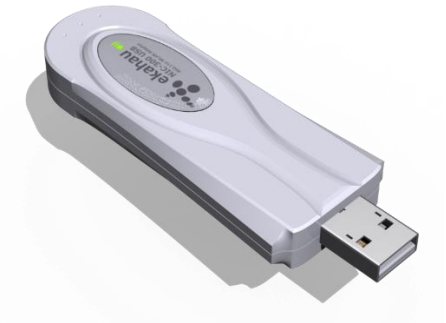
Suunnittelussa tutustutaan toimipisteiden ympäristöön, minkä jälkeen tutustutaan verkkojen mittauksessa käytettyyn ohjelmaan ja sen käyttöön kuuluvuuden mittaamisessa.

2.1 Ympäristö

Langattomien verkkojen mittaukset tehdään asiakkaan kahdessa toimipisteessä. Toimipisteen 1 ympäristö on pääosin varastotyyppinen, mutta toimipisteestä löytyy myös toimistotilaa. Haasteena toimipisteessä 1 on se, että varasto on jaettu kolmeen kerrokseen ja jokaisessa kerroksessa on tiheät hyllykkövälit ja hyllyköiden tavaran määrä vaihtelee kausittain. Tavaran määrä ja materiaali hyllyköissä taas vaikuttaa signaalin heikkenemiseen. Toimipisteessä 2 löytyy erilaisia ympäristöjä kuten toimisto, varasto ja tehdas. Näistä haastavin on todennäköisesti tehdastyyppinen ympäristö suurien laitteiden takia. Ongelmaa voivat aiheuttaa myös vanhan rakennuksen jykevät rakenteet. Laitteista saattaa tulla häiriötä signaaliin ja vanhat jykevät rakenteet voivat taas vaimentaa tukiasemien signaalia.

2.2 Ekahau Site Survey

Site Survey on Ekahau:n tarjoama ohjelma ja se on maksullinen. Ohjelman mukana tulee Ekahaun oma (kuva 1) NIC-300 USB-verkkoadapteri, joka tukee ohjelman tavoin myös uusimpia 802.11ac- ja n-standardeja. Ekahau suosittelee käyttämään mukana tulevaa adapteria ohjelman parhaimman mittaustuloksen saamiseksi. Ohjelmalla pystytään muun muassa suunnittelemaan uusia verkkoja, mittaamaan verkon kuuluvuutta ja ratkomaan verkkoon liittyviä ongelmia. (Site Survey, Ekahau 2014.)



Kuva 1. NIC-300 USB verkkoadapteri

Ohjelma pystyy hetkessä suunnittelemaan langattoman verkon annettujen suoritus- ja kapasiteettivaatimusten perusteella. Suunnittelun jälkeen ohjelma suosittelee, kuinka monta tukiasemaa verkon peittoalue tarvitsee ja ehdottaa parhaimmat paikat ja kanavat tukiasemille.

Verkkoa analysoidessa ohjelma mittaa monia eri asioita, muun muassa tukiasemien kanavien päällekkäisyyttä, signaalin voimakkuutta ja kohinaa. Ohjelma käyttää signaalin voimakkuutta sijoittamaan verkossa olevat tukiasemat kartalle. Tämä toiminto on kuitenkin vain suuntaa antava, mikäli pohjapiirustuksen seinien vaimennustehoa ei ole määritelty. Jos seinien ja muiden esteiden aiheuttamat vaimennustehot on määritelty ohjelmaan, ohjelma pystyy sijoittamaan tukiasemat ja kanavien päällekkäisyydet paremmin. Verkon suunnittelu toimii myös useamman kerroksen kanssa, eli ohjelma huomioi muidenkin kerroksien tukiasemien aiheuttamat signaalit ja luo tulokset näiden perusteella

Verkon vianmäärityksessä ohjelmalla voidaan paikantaa sekä luvattomia että rikkinäisiä tukiasemia, väärin konfiguroituja verkkoja ja mahdollisia tietoturvariskejä. Lisäksi ohjelmalla voidaan simuloida eri tilanteita, kuten tukiaseman siirtoa tai korvaamista, verkon kuorman lisäämistä tai tukiasemien kanavien vaihtoa.

2.3 Mittaaminen

Langattoman verkon mittaaminen tapahtui aiemmin esitellyllä Site Survey -sovelluksella. Sovellus asennettiin kannettavaan tietokoneeseen ja siihen liitettiin Ekahau:n oma USB-verkkosovitin. Kun mittaaminen aloitettiin, ohjelmaan liitettiin toimipisteen pohjapiirustus, jossa verkon mittaukset haluttiin tehdä. Tämän jälkeen kierrettiin toimipiste kannettavan tietokoneen kanssa läpi, liikuttaen samalla hiirtä siellä missä liikkui. Mittaamisvaiheessa voidaan kulkea vain suoria reittejä. Käännöksiä tehdessä, täytyi ohjelmasta painaa hiiren vasemmalla painikkeella pysähtymisen ja kääntymisen merkiksi ja tämän jälkeen jatkaa matkaa normaalisti.

Mittaamisvaiheen jälkeen ohjelma sijoittaa tulosten perusteella toimipisteestä löytyneiden tukiasemien (Access Point) sijainnit kartalle ja luo näiden tietojen perusteella kartalle erilaisia mittaustuloksia, kuten signaalin voimakkuuden ja kanavien päällekkäisyyden. Tässä tapauksessa tuloksia analysoidessa pitää muistaa, että ne ovat suuntaa-antavia, koska rakenteiden vaimennustehoa ei ole ollut tiedossa. Suurin epätarkkuus mittauksen tuloksissa syntyy tukiasemien sijainneissa ja näin ollen myös kanavien päällekkäisyydessä. Tämä johtuu siitä että ohjelma on olettanut tukiasemille esteettömän yhteyden.

Toimipisteessä 1 mitattiin myös lastauslaiturin aluetta ilmaisella Wifi Analyzer -kännykkäsovelluksella. Sovelluksella pystyi valitsemaan tukiaseman MAC-osoitteen perusteella ja mittaamaan kuuluvuutta kyseiseen tukiasemaan reaaliaikaisesti. Näin pystyttiin katsomaan kuinka paljon paksu betonikerros vaimentaa tukiaseman signaalia.

3 LANGATTOMAT LÄHIVERKOT

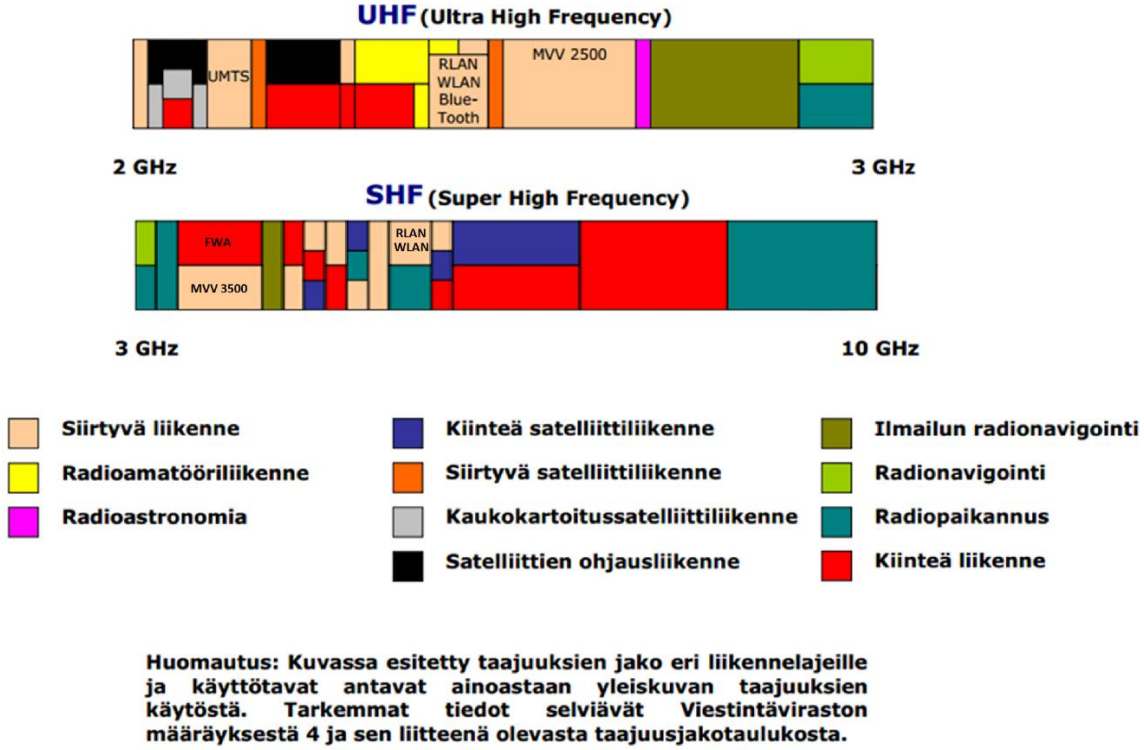
Seuraavissa luvuissa tutustutaan muun muassa langattomien verkkojen standardeihin ja niissä käytettyihin salausprotokolliin.

3.1 WLAN-Standardit

Kun laitteiden standardit yleistyivät, oli standardit kehitettävä myös protokollille. IEEE (The Institute of Electrical and Electronics Engineers) on maailman suurin ammatillinen yhdistys, joka on omistautunut omien sanojen mukaan edistämään teknologista innovaatiota ja huippuosaamista ihmiskunnan hyväksi. Yhdistys on kehittänyt maailmalla tunnetun ja käytettävän WLAN-standardin 802.11. (About, IEEE 2014.)

Ensimmäinen standardi valmistui vuonna 1997, joka oli tämän päivän versioihin verrattuna paljon hitaampi (1-2 Mbit/s). Vuosien varrella standardista on julkaistu useita versioita, joista merkittävimmät ovat 802.11a, 802.11b, 802.11g, 802.11n ja 802.11ac. Standardeissa käytetyt taajuusalueet vaihtelevat 2,4 GHz:n alueesta 5 GHz:n alueeseen, joista osa käyttää vain toista ja osa molempia.

Suomessa radiotaajuuksien käytöstä vastaa viestintävirasto. Radiotaajuusmääräys 4 koskee radiotaajuuksien käyttöä ja sillä on tarkoitus muun muassa turvata radiotaajuuksien tehokas, tarkoituksenmukainen ja riittävän häiriötön käyttö. Kuvassa 2 on kuvattu 2 – 10 GHz välillä olevien taajuuksien käyttötarkoituksia. (Radiotaajuusmääräys 4, Viestintävirasto 2014.)



Kuva 2. Radiotaajuuksien käyttö Suomessa (Viestintävirasto)

3.1.1 IEEE 802.11

IEEE 802.11 on IEEE:n laatima standardi langattomille WLAN-lähiverkoille. Koska tekniikka on läheistä sukua Ethernetille (802.3), varsinkin alkuaikoina, käytettiin usein nimitystä langaton Ethernet. Nykyään käytetään nimitystä WiFi. Taulukossa 1 on listattu 802.11-standardin eri versioita.

Taulukko 1. IEEE-standardeja

Standardi	Ratifioitu	Hajaspektri-tekniikka	Teoreettinen bittinopeus	Taajuus-alue	Kanavia yht.	Ei-päällekk. kanavia
802.11	1997	FHSS, DSSS	1 ja 2 Mbit/s	RF: 2,4 GHz	DS: 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	2009	OFDM	1 – 54 ja 150 + Mbit/s	2,4 ja 5 GHz	12/12	3/12
802.11ac	2014	OFDM	500 + Mbit/s	5 GHz	12	*

802.11ac-standardilla ei-päällekkäisten kanavien määrä vaihtelee maakohtaisesti. Suomessa viestintäviraston mukaan ei-päällekkäisiä kanavia on mahdollista saada 12 kappaletta, mutta mikäli halutaan nopeampia tiedonsiirtonopeuksia, voidaan kanavienleveyttä muuttaa. Tällöin ei-päällekkäisten kanavien määrä vaihtelee kanavanleveydestä riippuen. Valittavia kanavanleveyksiä on neljä, 20 MHz, 40 MHz, 80 MHz ja 160 MHz. Viestintävirasto ei ilmoita tarkkoja käytössä olevia 5 GHz 802.11ac-standardin taajuuksia, joten ei-päällekkäisten kanavien määrän laskeminen Suomessa suuremmilla kanavanleveyksillä ei ole mahdollista.

3.2 Tietoturva

Tietoturva on yksi tärkeimmistä asioista, kun kyse on langattoman verkon suunnittelusta, toteutuksesta ja hallinnoinnista. Suojaamaton verkko altistaa yrityksen tietoliikenteen ja resurssit luvattomalle käytölle yrityksen ulkopuolella. Yksittäinen henkilö voi halutessaan kaapata dataa ja käyttää hyväkseen verkkopohjaisia resursseja. Pahimmassa tapauksessa yrityksen verkon pystyisi kaatamaan, aiheuttamaan jonkin yrityksen palvelun kaatumisen tai mahdollisesti käyttämään yrityksen verkkoa laittomuuksiin. (Wireless LAN Security, Symantec 2014.)

Tietoturvalla pyritään myös säilyttämään liikkuvan datan eheys, jolloin tieto ei saa muuttua tai muutokset pitää vähintäänkin havaita.

Verkon tai palvelun kaataminen voisi tapahtua palvelunesto- eli Denial of service (DoS)-hyökkäyksenä. Yksi tapa palvelunestoon on niin sanottu väsytyshyökkäys, jossa verkkoa tulvitetaan suurella määrällä paketteja. Suuri määrä paketteja pystyy kuluttamaan verkon kaikki resurssit ja tästä voi seurata verkon kaatuminen. Hyökkääjien hajautettuun palvelunestoon (Distributed Denial of Service, DDoS), tiedettävästi käytettyjä ohjelmia ovat muun muassa Stacheldraht, Trinoo, TFN, ja TFN2K, nämä ohjelmat

toimivat niin että tartunnan saaneet koneet lähettävät hajautetusti paketteja samaan kohteeseen ja näin ollen saavat palvelun tai peräti koko verkon kaatumaan. (Palvelunestohyökkäys, Web-opas 2014.)

Toinen tapa on käyttää voimakasta radiosignaalia, joka käytännössä tukkii ilmatiet omalla signaalillaan ja näin ollen tekee tukiasemista käyttökelvottomia. Tämä johtuu siitä että 802.11:n kaltaiset protokollat päästävät palvelunestohyökkäyssignaalin häiritsemään ilmateitä niin kauan kuin hyökkääjä haluaa. Tämä on kuitenkin hyökkääjän kannalta huonompi hyökkäystapa, koska hyökkäykseen tarvittavan laitteen täytyy sijaita lähellä verkkoa ja näin ollen hyökkääjä voi jäädä helpommin kiinni, koska niin suuren signaalin paikantaminen nykylaitteilla on helppoa. (Geier 177.)

3.2.1 WEP

Wireless Equivalent Privacy (WEP) on symmetrinen salausmenetelmä, jossa salaukseen ja sen purkuun käytetään samaa avainta. Tästä syystä krakkeri pystyy riittävästi liikennettä seuraamalla selvittämään salaisen avaimen. Vähentääkseen tätä riskiä, tulisi salainen avain vaihtaa riittävän usein, mutta todellisuudessa samoja avaimia saatetaan käyttää viikkoja tai jopa vuosia. (Geier 181.)

3.2.2 TKIP & AES

Temporal Key Integrity Protocol (TKIP) ja Advanced Encryption Standard (AES)-protokollat on suunniteltu parantamaan 802.11-standardin tietoturvaa.

TKIP on niin sanottu välivaiheen ratkaisu, koska se korjaa WEP:n sisältämiä avaimen uudelleenkäyttöongelmia. TKIP-prosessi perustuu siihen, että tukiasemien ja asiakkaiden kesken jaetaan väliaikainen 128-bittinen avain ja TKIP yhdistää tämän avaimen asiakkaan MAC-osoitteen kanssa ja lisää tähän melko suuren 16 oktetin alustusvektorin tuottaakseen avaimen, jolla data salataan. Tällä tavalla jokainen asema salaa datan eri avainmerkkijonolla. (Geier 183.)

Vuoden 2012 jälkeen TKIP-salaus todettiin vanhaksi eikä sen käyttö ole enää suositeltu.

AES taas tarjoaa hieman vahvemman salauksen. AES:n ongelmana oli aikaisemmin se, että se vaati enemmän tehoa prosessorilta verrattuna aikaisempiin salauksiin, nykyään lähes kaikki laitteet tukevat protokollaa. AES-protokollaa on lisäksi pidetty lähes murtamattomana. (Geier 184.)

3.2.3 CCMP

CCM mode Protocol (CCMP) on normaali salausprotokolla WPA2-salauksen käyttöön ja on paljon turvallisempi verrattuna vanhaan WEP ja WPA:n TKIP-protokolliin. CCMP:ssä on paranneltu salauksen kapselointimekanismia ja näin ollen tietojen luottamuksellisuutta. Protokolla perustuu Counter Mode CBC-MAC (CCM) AES-standardiin. (Geier 186.)

3.2.4 WPA & WPA2

Wi-Fi Protected Access (WPA) ja siitä uudempi WPA2. WPA tuli käyttöön 2003 ja sitä käytettiin välivaiheena ennen vahvemman WPA2-protokollan saapumista. WPA2 ratifioitiin vuonna 2004, minkä pohjana toimi vanhempi WPA. WPA2 tunnetaan myös nimellä IEEE 802.11i-standardi. (WPA ja WPA2 Salausprotokollien Ominaispiir-teitä, TWiki 2014.)

Molemmissa tekniikoissa autentikointi aloitetaan, kun käyttäjä pyrkii yhdistymään langattomaan verkkoon. Tällöin asiakas toimittaa tukiasemalle tunnistetiedot, jotka tukiasema toimittaa eteenpäin autentikointipalvelimelle. Käyttäjä ja autentikointipalvelin tunnistautuvat toisilleen tukiaseman kautta. Molemminpuoleisessa tunnistautumisessa on myös se, että asiakas tietää olevansa tekemisissä oikean autentikointipalvelimen kanssa. (WPA ja WPA2 Salausprotokollien Ominaispiirteitä, TWiki 2014.)

Salausta käytetään pienemmissä yrityksissä ja kodeissa, jolloin asiakas kirjaa salasanan tukiasemaan, jota käytetään autentikoinnissa. Pre-Shared Key (PSK) on käyttäjän todentamisen metodi, jossa käyttäjä syöttää ennalta määritellyn avaimen yhdistääkseen langattomaan verkkoon.

4 NYKYTILA

Tässä luvussa tutustumme asiakkaan toimipisteiden nykyiseen langattoman verkon tilaan ja toimipisteissä havaittujen ongelmien mahdollisiin syihin.

4.1 Havaitut ongelmat

Ennen kartoituksen ja dokumentoinnin aloittamista, tiedettiin molemmissa toimipisteissä olevan puutteita, joten jo mittausvaiheessa ne pyrittiin ottamaan huomioon ja keräämään niistä mahdollisimman paljon tietoa.

4.1.1 Toimipiste 1

Toimipisteessä 1 oli entuudestaan tiedossa, että trukkipäätteet eivät toimi halutulla tavalla. Mittausten aikana kerätyn palautteen mukaan verkon toimivuudessa havaittiin ongelmia trukkipäätteiden käyttäjillä, mutta vastaavasti käsipäätteiden käyttäjillä ongelmia ei ilmennyt. Trukkipäätteiden käyttäjien mukaan ongelmaa esiintyi pääasiassa hallin lattiatasolla.

Punaisella merkatun lastauslaiturialueen katonrajassa olevaa tukiasemaa ja sen tuottaman signaalin voimakkuutta tutkittiin puhelimeen ladattavalla ”Wifi Analyzer”-sovelluksella. Mittauksissa huomattiin, että lastauslaiturin ja tukiaseman välissä oleva betonikerros vaimentaa tukiaseman signaalia huomattavasti. Signaalin voimistui siirryttäessä betonikerroksen alapuolelta yläpuolelle.

4.1.2 Toimipiste 2

Toimipisteen 2 hallissa 3 sijaitsee kaksi pöytäkonetta, jotka eivät saa langatonta yhteyttä WLAN3-verkkoon tuntemattomasta syystä. Ongelman on arveltu johtuvan valmistajan tukiasemien omasta salauksesta. Salausta ei ole kuitenkaan pystytty tarkistamaan verkon asetuksista, koska verkkoon ei ole saatu kannettavalla tietokoneella toimivaa yhteyttä. Verkon muiden tukiasemien signaali ei myöskään kanna hallin 3 kahdelle pöytäkoneelle.

4.2 Käytössä olevat WLAN-verkot

Seuraavissa luvuissa on käyty läpi toimipisteiden 1 ja 2 tukiasemien jakamia langattomia verkkoja.

4.2.1 WLAN1

WLAN1-verkko on tarkoitettu toimistokäyttöön ja sitä käytetään sekä toimipisteessä 1 että 2.

4.2.2 WLAN2

WLAN2-verkkoa käytetään trukkipäätteiden ja käsipäätteiden uutena verkkona. Verkko ei kuitenkaan ole käytössä trukeissa, koska päätteet toimivat tuntemattomasta syystä hitaasti. Vaikeutta tuo myös se, että trukeissa on tietoteknisesti eri kokoonpanot.

4.2.3 WLAN3

WLAN3-verkkoa käytetään toimipisteessä 2 tuotantoverkkona käsipäätteille. Verkko on toteutettu kokonaan erillisillä tukiasemilla. Tukiasemista osa on paikannettu fyysisesti.

Tukiasemista oli valmiit listat. Laitteiden fyysisestä sijainnista johtuen, ei laitteiden kyljessä olevia tarroja tai MAC-osoitteita ole päästy tarkistamaan, joten listojen mukaan muutama tukiasema oli kateissa. Mittauksen perusteella voisi olettaa yhden kadoksissa olevista tukiasemista sijaitsevan hallin 1 ja 2 välissä, mutta mittausta tehdessä tukiasemaa ei löytynyt.

IT-vastaavan tietojen mukaan tukiasemilla on käytössä valmistajan kehittämä salaus ja tästä syystä tavallisella koneella, oikeista tunnuksista huolimatta, yhteyttä verkkoon ei ole saatu. Käsipäätteillä verkkoon yhdistäminen onnistuu, mutta varmuutta niiden käytöstä verkon konfigurointiin ei saatu testilaitteiden puuttumisen vuoksi.

4.2.4 WLAN4

Verkko on tarkoitettu vierailijoille ja se on näkyvissä sekä toimipisteessä 1 että 2, mutta verkko on käytössä vain toimipisteessä 2. Tämä johtuu siitä, että vain toimipisteen 2 vastaanottotiski on jakanut tunnuksia verkkoon. Toimipisteen 1 vastaanottotiskille ei ole opastettu tunnuksien jakoa vierailijoita varten, joten tästä syystä verkko ei ole ollut käytössä toimipisteessä 1.

4.2.5 Muut verkot

Molemmissa toimipisteissä on käytössä myös muita verkkoja. Toimipisteeseen 1 on, vierailija verkon käyttämättömyydestä johtuen, asennettu erillinen tukiasema, jolla on jaettu vieraille tarkoitettu WLAN 5-verkko. Tämä verkko on kuitenkin ollut jo pidempään poissa käytöstä, koska henkilökunnalta kysyttäessä ei verkon tunnuksista ollut tietoa. Verkko on poissa yrityksen sisäisestä verkosta, joten pääsy on vain ulospäin. Tukiasemaa käytetään myös muuhun verkon jakamiseen. Aseman porteista neljä on käytössä, joista yksi menee lähellä olevaan neuvotteluhuoneeseen, kaksi porteista on mennyt lähituen entiselle paikalle ja yksi on irrallaan ristikytkentäkaapissa.

Toimipisteellä 2 sijaitsevassa koulutustilassa on yksi erillinen tukiasema, joka jakaa WLAN6-verkkoa. Tämä verkko on myös poissa yrityksen sisäisestä verkosta. Käyttötarkoitus verkolle oli vielä epäselvä, koska verkkoa ei ole käytetty vähään aikaan.

4.3 WLAN-kontrollerit

WLAN-kontrollerit ohjaavat verkkoja WLAN1, WLAN2 ja WLAN4. Muut toimipisteessä 1 ja 2 olevat verkot on toteutettu erillisillä laitteilla.

WLAN3-verkko toimii itsenäisesti, mutta on kuitenkin liitettynä sisäverkkoon. Verkon konfigurointi tapahtuu käsipäätteillä. Tämän verkon laitteet kannattaisi korvata uusilla laitteilla, jotta verkkoa voitaisiin hallinnoida WLAN-kontrollereilla

Laitteiden eroavaisuuksien takia olisi hyvä harkita trukkiverkkojen ja toimistoverkkojen erottamista toisistaan, mikäli niiden yhdistämiselle ei ole varsinaista tarkoitusta.

WLAN-kontrollereille on olemassa uudemmat versiot firmwaresta. Yksi ominaisuuksista, mikä tulisi firmware-päivityksen mukana, olisi nopeuden rajoittaminen jokaiselle langattomalle verkolle erikseen. Tätä pystyttäisiin hyödyntämään rajoittamalla pienempää tiedonsiirtonopeutta vaativien verkkojen kaistaa ja vastaavasti tarjoamaan enemmän tiedonsiirtokaistaa sitä tarvitseville verkoille.

5 JATKOKEHITYS

Seuraavissa luvuissa on käyty läpi toimipisteiden jatkokehitysvaihtoehtoja.

5.1 Kehitysvaihtoehdot

Kehitysvaihtoehtoina toimipisteiden verkoille on nykyisten verkkojen laajentaminen, kaiken korvaaminen uudella tai valmiin palvelun hankkiminen esimerkiksi Fujitsulta.

Nykyisen verkon laajentamisvaihtoehdossa tämänhetkinen järjestelmä säilytettäisiin ja sitä laajennettaisiin. Mikäli aiempi sopimus valmistajan kanssa on vielä voimassa, selvitettäisiin voiko sopimusta jatkaa ja kuinka huollot ja takuut toimisivat. Tämän jälkeen tilattaisiin tarvittava määrä valmistajan laitteita korvaamaan yksittäiset WLAN-kontrollereille sopimattomat tukiasemat. WLAN-kontrollereilla on tällä hetkellä tukiasemien lisenssejä sekä aktiivisesti että passiivisesti varattuina. Passiivisten tukiasemien tilanne on selvitettävä, ovatko tukiasemat todella käytössä, mikäli eivät ole, lisenssit vapautettava käyttöön WLAN-kontrollereilta.

Kaiken korvaavassa vaihtoehdossa uusittaisiin kaikki, sekä tukiasemat että WLAN-kontrollerit. Tässä vaihtoehdossa pitää huomioida myös toimipisteiden käsipäätteet. Uusien tukiasemien pitää olla yhteensopivia vanhojen ja mahdollisesti uusien käsipäätteiden kanssa.

Valmiissa palvelussa tulevat sekä tukiasemat että tarvittavat kytkimet ja WLAN-kontrollerit. Myös käsipäätteiden yhteensopivuus on huomioitava.

5.2 Nykytilan jatkokehitys

Tällä hetkellä tukiasemat käyttävät kolmea kanavaa, siten että kanavavalinta tapahtuu automaattisesti. Toimipisteissä 1 ja 2 olisi suositeltavaa siirtyä kolmen tai neljän kanavan manuaaliseen käyttöön. Näin pystyttäisiin hyvin suunnittelemalla varmistamaan mahdollisimman häiriöttömät kanavat tukiasemille.

Mikäli trukkipäätteillä ei tarvitse käsitellä suuria tiedostoja, jotka vaatisivat suurta tiedonsiirtonopeutta, voitaisiin langattomien verkkojen nopeutta laskea vastaamaan laitteiden tarpeita. Tällä hetkellä kaikki verkot tukevat maksimi nopeutta 54 Mb/s, joten verkkojen nopeuden voisi suunnitella rajoitettavan maksimissaan 11 Mb/s:iin riippuen liikkuvan datan suuruudesta, koska vanhimmat laitteet eivät välttämättä toimi moitteettomasti käyttäen suurinta tarjottua nopeutta.

Jotta tulevaisuudessa langattoman verkon hallinta olisi helpompaa ja selkeämpää, olisi verkosta hyvä karsia ylimääräisiä tukiasemia ja niiden tarjoamia verkkoja, esimerkkinä toimipisteen 1 erillinen tukiasema, joka jakaa WLAN5-verkkoa. Mikäli verkkoa päädytään laajentamaan nykyisestä, saattaa lisenssien tarve kasvaa. Tällä hetkellä lisenssejä on vielä vapaana.

5.2.1 Toimipiste 1

Tällä hetkellä tukiasemien verkkojen kanavat hakeutuvat automaattisesti (asetus ACS, Automatic Channel Selection). Tämän voisi muuttaa manuaaliseksi käyttäen neljää kanavaa. Mikäli vaihdon jälkeen vielä ongelmat jatkuvat, voisi alueelle lisätä vielä yhden tukiaseman. Lisäksi lastauslaiturin tukiaseman sijaintia tulisi miettiä uudelleen, koska tällä hetkellä tukiasema sijaitsee katonrajassa ja tukiaseman kohdalta lähtee paksu betonikerros lastauslaiturien suuntaan. Tukiaseman voisi siirtää vastapäätä oleviin hyllykköihin kiinni, tällöin tukiasema kattaisi paremmin sekä betonikerroksen yläpuolen että alapuolen. Toinen vaihtoehto on lisätä tukiasema betonikerroksen alapuolelle. Mikäli päädytään lisäämään tukiasemia, on muistettava katsoa kanavat uusille tukiasemille niin, että häiriö viereisille tukiasemille olisi mahdollisimman pieni.

5.2.2 Toimipiste 2

Toimipisteen 2 tukiasemat on myös asetettu automaattiselle kanavan haulle, jota voisi myös harkita vaihdettavaksi manuaaliseksi käyttäen neljää kanavaa. Nykyiset laitesijainnit tulevat muuttumaan poistuvien alueiden takia, joten kanavat on katsottava uudelleen kun tukiasemien uudet paikat on suunniteltu. Mikäli tukiasemia tulee lisää ja välimatkat lyhenevät, täytyy kanavien tilanne tarkastella uudelleen tarvitseeko kolmesta kanavasta siirtyä neljään kanavaan.

6 LOPPUSANAT

Opinnäytetyössä oli tavoitteena kartoittaa asiakkaan kahden toimipisteen langattomien verkkojen nykytila ja ottaa kantaa mahdollisiin puutteisiin ja aiemmin havaittuihin ongelmiin.

Toimipisteiden langattomien verkkojen peittoalueiden mittaamiset suoritettiin kesällä. Haastetta mittauksiin toivat toimipisteiden aukioloajat, sillä toimipisteiden suurten kokojen takia mittauksien suorittaminen aukioloajan puitteissa tuotti ongelmia. Lisäksi kesälomakauden aikaan tiedossa olevien ongelmien tutkiminen osoittautui hankalaksi, sillä havaituista ongelmista enemmän tietävät henkilöt olivat kesälomilla.

Ennen opinnäytetyötä minulla ei ollut aikaisempaa kokemusta langattomien verkkojen mittaamisesta, joten Ekahaun Site Survey – ohjelman käyttö oli uutta. Rajallisista resursseista johtuen opastus ohjelman käyttöön oli vähäinen, joten jouduin tutustumaan ohjelman käyttöön pääosin itsenäisesti. Opinnäytetyön kannalta olisi ollut parempi, mikäli sovellukseen tutustumiseen olisi annettu enemmän aikaa tai käytön opastukseen olisi panostettu enemmän.

Kokemuksena uskon opinnäytetyön olleen erittäin hyödyllinen. Työn aikana opin paljon langattomien verkkojen kuuluvuuden mittaamisesta ja eri IEEE 802.11-standardeista. Lisäksi opinnäytetyöhön kuulunut verkon kartoitus ja dokumentointi antoivat hyvän käsityksen pk-yritysten langattomien verkkojen rakenteesta.

LÄHTEET

2.4GHz vs 5GHz Deployment Considerations, Wi-Fi Planet. Viitattu 26.11.2014.
http://www.wi-fiplanet.com/tutorials/article.php/1569271/24GHz-vs-5GHz-Deployment-Considerations.htm

About IEEE, IEEE Advancing Technology for Humanity. Viitattu 17.7.14.
http://www.ieee.org/about/index.html

Ekahau Site Survey & Planning, Ekahau. Viitattu 4.12.2014.
http://www.ekahau.com/wifidesign/ekahau-site-survey

Geier, J. 2005. Langattomat verkot – perusteet. Helsinki: Edita, IT Press. ISBN-10: 9518267898

Palvelunestohyökkäys, Web-opas. Viitattu 26.8.2014.
http://www.webopas.net/palvelunestohyokkaus.html

Radiotaajuuksien käyttö suomessa, Viestintävirasto. Viitattu 27.11.2014.
https://www.viestintavirasto.fi/attachments/Radiotaajuuksien_kaytto.pdf

Radiotaajuusmääräys 4, Viestintävirasto. Viitattu 27.11.2014.
https://www.viestintavirasto.fi/ohjausjavalvonta/lainsaadanto/maaraykset/radiotaajuusmaarays4.html

Wireless LAN Security, Symantec. Viitattu 21.8.2014.
http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf

WPA ja WPA2 Salausprotokollien Ominaispiirteet, TWiki. Viitattu 29.8.2014.
https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/Tutkielmat/WPAWPA2SalausprotokollienOminaispiirteet