Minna Mäkinen

WLAN-VERKON SUUNNITELU JA ASENNUS

Centria-Ammattikorkeakoulu Oy, Kokkolan kampus

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutusohjelma
Tammikuu 2019

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Tammikuu 2019	**Tekijä/tekijät** Minna Mäkinen
Koulutusohjelma Tieto- ja viestintätekniikka		
Työn nimi WLAN-VERKON SUUNNITELU JA ASENNUS		
Työn ohjaaja Sakari Männistö		**Sivumäärä** 38
Työelämäohjaaja Petri Rautiainen		

Opinnäytetyön tavoitteena oli kuvata langattomien internet-verkkojen toteutusta ja tekniikkaa. Lähtökohta työssä oli Centria-ammattikorkeakoulu Oy:n Talonpojankadun kampus Kokkolassa. Käytännön osuudessa käydään läpi verkon päivitys vanhasta verkosta uudempaan. Työn ensisijainen painopiste on kuitenkin teoreettinen, ja työ käy läpi langattomien verkkojen historiaa ja standardeja. Työssä käsitellään myös tietoverkkojen standardeja, joita käytetään tavallisesti langattomien verkkojen yhteydessä.

Langattomien verkkojen historian ja standardien lisäksi arvioidaan Centria-ammattikorkeakoulun Talonpojankadun langatonta verkkoa, ja tutkitaan verkon kehityskohteita. Työn käytännön osuudessa käydään läpi uudistetun langattoman verkon toteutus ja tarkastellaan, toteuttiko uudistus sille asetetut tavoitteet. Opinnäytetyössä arvioidaan, korjasiko uudistettu langaton verkko aiemmassa verkossa tunnistetut heikkoudet.

Asiasanat
langaton, lähiverkko, 802.11, WEP, WPA, PoE, IEEE

ABSTRACT

Centria University of Applied Sciences	**Date** January 2019	**Author** Minna Mäkinen
Degree programme Information and Communication Technology		
Name of thesis DESIGN AND INSTALLATION OF A WLAN NETWORK		
Instructor Sakari Männistö		**Pages** 38
Supervisor Petri Rautiainen		

The goal of this thesis was to describe the implementation and technology of wireless internet networks. The basis for the work was the Talonpojankatu campus of Centria-ammattikorkeakoulu Oy in Kokkola. The practical portion of the thesis examines the upgrade of the old wireless network to a new one. The primary focus of the work was, however, theoretical and the thesis explores the history and standardization of wireless networks. Also explored are the standards commonly used in conjunction with wireless networks.

In addition to the history and standards of wireless networks, the thesis explores the wireless network of Centria-ammattikorkeakoulu at Talonpojankatu and evaluates the areas of development. The practical part of the thesis examines the upgraded network and evaluates if the goals set for the upgraded network were met. The work examines if the new network corrected the issues identified in the old network.

Key words
wireless, local area network, 802.11, WEP, WPA, PoE, IEEE

KÄSITTEIDEN MÄÄRITTELY

WLAN	Wireless Local Area Network
IEEE	Institute of Electrical and Electronics Engineers
PoE	Power over Ethernet
QAM	Quadratic Amplitude Modulation
DSSS	Direct Sequence Spread Spectrum
DBPSK	Differential Binary Phase-Shift Keying
DQPSK	Differentially encoded Quadrature Phase-Shift Keying

1 JOHDANTO

Tämä opinnäytetyö tarkastelee langattomien lähiverkkojen (engl. WLAN, wireless local area network) historiaa, tekniikkaa ja standardeja. Työssä tarkastellaan radioverkkojen kuuluvuuden vaikutusta tiedonsiirtonopeuteen ja rakennusten tyypillisten rakenteiden vaikutusta kuuluvuuteen. Työ käy lyhyesti läpi myös langattomien verkkojen taustalla toimivia tekniikoita, kuten Ethernet ja Power over Ethernet.

Käytännön esimerkkinä työssä käytetään WLAN-verkkoa Centria-ammattikorkeakoulu Oy:n Talonpojankadun kampuksella Kokkolassa. Työn käytännön osuus kostuu vanhan langattoman verkon kuuluvuuden kartoittamisesta ja verkon tarjoaman käyttäjäkokemuksen arvioinnista. Työhön liittyen olisi ollut tarkoituksenmukaista kerätä tilastotietoja verkon käyttäjämäärästä ja tietonsiirtokapasiteetista ennen ja jälkeen päivityksen. Tämä ei kuitenkaan ollut mahdollista Centria-Ammattikorkeakoulun asettaman toimeksiannon yhteydessä, koska langaton verkko on osittain kolmannen osapuolen hallinnoima.

Työssä kuvataan yleisellä tasolla langattoman verkon rakennetta ennen ja jälkeen uudistuksen. Yksityiskohtaisia kuvioita kuuluvuudesta ei ole liitetty työhön kahdesta syystä. Ensiksi, täsmällinen vaimentuma-arvo desibeleinä olisi merkityksetön, ja mahdollisesti harhaanjohtava. Mittaukset suoritettiin kannettavalla tietokoneella, koska varsinaista mittalaitteistoa ei saatu Kokkolan kampukselle työn vaatimien aikarajojen puitteissa.

Merkittävämpi syy tulosten kuvaukseen vain sanallisesti on pohjapiirrosten mahdollinen arkaluontoisuus. Ainoat saatavilla olevat pohjapiirrokset sisältävät yksityiskohtaista tietoa oppilaitoksen rakennuksista ja henkilöstöstä. Piirrosten sisällyttämistä työhön salassa pidettävinä liitteinä ei voida pitää tarkoituksenmukaisena, kun otetaan huomioon niiden vähäinen informaatioarvo.

Työssä kuvataan kuuluvuuden vaikutusta tiedonsiirtonopeuteen. Tässä ei ole menty yksityiskohtiin, koska täsmälliset tulokset eivät ole toistettavissa. Tukiaseman ja päätelaitteen neuvottelema koodaus- ja modulaatiotekniikka, kuuluvuus, ja verkon käyttöaste vaikuttavat kaikki päätelaitteen kokemaan tiedonsiirtonopeuteen.

Tässä työssä käytetystä lähdemateriaalista suurin osa on IEEE:n 802.11-työryhmän julkaisemia dokumentteja, jotka määrittävät langattomien verkkojen standardeja. Muu lähdemateriaali on paljolti verkkoartikkeleita. Suurin osa tietotekniikan alan journalismista julkaistaan verkossa, eikä nopeasti muuttuvista tietoliikenteen tekniikoista ole saatavilla painettua kirjallisuutta.

2 TYÖN MÄÄRITTELY

Työn tavoitteena on käydä läpi langattoman lähiverkon toteutus keskisuuren yrityksen tai organisaation näkökulmasta. Verkkoyhteydet tämän tyyppisessä ympäristössä palvelevat käytännössä julkista tilaa, ja käyttäjien kokemus verkon laadusta saattaa vaikuttaa käyttäjien mielikuvaan koko organisaatiosta, riippumatta siitä, liittyykö langaton internet-yhteys välittömästi organisaation tarjoamiin palveluihin. Tämä työ käy läpi teknisiä ratkaisuja, joilla verkon käyttäjän kokema ’nopeus’ saadaan vähintään tyydyttävälle tasolle riippumatta siitä, missä osassa organisaation tiloja käyttäjä on. Käydään läpi langattomaan tiedonsiirtoon liittyviä rajoituksia ja tekniikoita näiden rajoitusten minimoimiseksi.

Toissijaisesti tämä opinnäytetyö tarkastelee langatonta verkkoa koulutusorganisaation sisäisenä työkaluna. Verkon luotettavuuteen ja tasaiseen tiedonsiirtonopeuteen on kiinnitettävä erityistä huomiota, kun siihen kytkettyjä laitteita käytetään osana organisaation ydintehtävän toteutusta. Verkon on oltava helppokäyttöinen ja samalla tarjottava samat resurssit ja tietoturva kuin organisaation langallinen verkko.

Käytännön esimerkkinä työssä on Centria-Ammattikorkeakoulu Oy:n uudistettu langaton lähiverkko. Tavoitteena oli korvata aiempi verkko, joka ei tukiasemien käyttämän tekniikan ja niiden sijoittelun takia pysty tarjoamaan tyydyttävää käyttäjäkokemusta edes opiskelijoille tarjottuna lisäpalveluna. Verkko oli tarkoitus ottaa käyttöön myös opetustyökaluna, kun tietyissä luokissa siirryttiin pöytätietokoneista kannettaviin tietokoneisiin. Voidaan väittää, että verkon aiemmassa roolissa se palveli lähinnä satunnaisia opiskelijoita, joiden päätelaite ei mahdollistanut mobiiliverkkojen käyttöä. Uuden verkon tiedettiin palvelevan useita 20-30 opiskelijan opetusryhmiä samanaikaisesti eri luokkahuoneissa.

Työ tarkastelee teknisiä ratkaisuja, joita Centria-Ammattikorkeakoulu Oy:n kaltainen organisaatio olisi voinut käyttää edellä esiteltyjen tavoitteiden saavuttamiseen, ja tutkii ratkaisua, jonka oppilaitos valitsi. Tutkitaan, saavuttiko oppilaitos uudelle langattomalle verkolle asetetut tavoitteet, ja tarkastellaan, mitä olisi voitu tehdä toisin.

3 RADIOSIGNAALIT TIEDONVÄLITYKSESSÄ JA LANGATTOMIEN VERKKOJEN KEHITYS

Tietoa on välitetty langattomasti aina Gugliemo Marconin 1894 suorittamasta langattoman lennättimen kokeilusta lähtien. Samaan aikaan, 1893, Atlantin toisella puolella Nikola Tesla esitteli omaa radiotaan. Radioaaltoja on yli sadan vuoden käytetty siirtämään suurempia ja suurempia määriä informaatiota. Radiota on käytetty tiedon levittämiseen 1900-luvun alulta alkaen. Kaksisuuntainen kommunikaatio langattomilla puhelimilla alkoi yhdysvaltalaisen AT&T:n Mobile Telephone Service -verkosta. 60-luvulla, kun AT&T kehitti verkostaan parannetun version, pienemmät toimijat kehittivät kilpailevan Radio Common Carrier -verkon.
(Deffree 2018.)

Radioaaltojen käyttäminen datan välitykseen tietokoneiden välillä alkoi 1970-luvulla, kun Hawaii:n yliopisto tarvitsi nopeamman ja luotettavamman keinon yhdistää tietokoneita eri saarilla. Ylipiston tietokoneet oli yhdistetty Honolulussa sijaitsevaan keskuskoneeseen käyttäen puhelinlinjoja, mikä oli sekä hidasta että epäluotettavaa. Yliopisto kehitti AlohaNET-nimisen radioverkon, jolla tietoa voitiin siirtää Honolulun keskuskoneen ja saarilla olevien koneiden välillä. Toisin kuin esimerkiksi puhelinverkossa, AlohaNET-verkossa koneet pystyivät lähettämään dataa käyttäen verkon koko taajuusspektriä, yksi kone kerrallaan. Ajatus verkosta, jossa päätelaitteet saavat parhaassa tapauksessa käyttöönsä koko verkon kapasiteetin, on WLAN-verkkojen tärkeimpiä elementtejä.
(Bejnum & Barcelo 2011.)

1990-luvun lopulla Internet oli yleistynyt niin paljon, että idea lähiverkon toteuttamisesta langattomasti oli sekä realistinen että tarpeellinen. Useilla yrityksillä oli oma tekniikkansa lyhyen matkan langattomaan datasiirtoon. Kävi kuitenkin selväksi, että langaton verkkotekniikka oli saatava yhtenäistettyä samalla tavalla kuin langallinen tekniikka. Yhdysvaltalainen Institute of Electrical and Electronics Engineers – IEEE – oli määritellyt standardin 802.3, eli Ethernetin. Standardoitua tekniikkaa langattoman lähiverkon toteuttamiseksi kehittivät European Telecommunications Standards Institute – ETSI, ja IEEE. IEEE:n määrittämä standardi 802.11 oli laitevalmistajille helpompi ja edullisempi toteuttaa, joten siitä muodostui alan käyttämä langattomien lähiverkkojen standardi. (Berg.)

4 IEEE 802.11

Yhdysvaltalainen Institute of Electrical and Electronics Engineers, IEEE, alkoi kehittää omaa standardiaan internet-liikenteen siirtämiseen langattomasti 90-luvun alussa. IEEE 802 LAN/MAN -standardikomitea aloitti projektin työnimellä IEEE Standard for Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications, vuonna 1991. Työryhmän projektivaltuutuspyyntö (engl. Project Authorization Request, PAR) hyväksyttiin maaliskuun lopulla vuonna 1991. Standardin kehittäminen kesti pidempään kuin sen seuraajien, mikä ei ole yllättävää, kun otetaan huomioon, että myöhemmät versiot ovat lisänneet ominaisuuksia, eikä niitä ole luotu uudelleen tyhjästä. (IEEE.)

4.1 Aiemmat versiot

Standardin ensimmäinen versio tunnetaan nimellä IEEE Std P802.11-1997, julkaisuvuotensa mukaan. Tämä ensimmäinen valmistajariippumaton, yhtenäistetty langaton tiedonsiirtotekniikka toimi 2 megabitin sekuntinopeudella. Nopeus saavutetaan käyttämällä joko DBPSK- tai DQPSK-koodausta. Kumpikin koodaustekniikka välittää dataa vaihesiirron avulla, muokkaamalla kantoaallon vaihetta. Signaalin häiriönsietoisuus varmistetaan käyttämällä verrattain yksinkertaista, Barker-koodiin perustuvaa DSSS-modulaatiota (engl. Direct Sequence Spread Spectrum). DBPSK- tai DQPSK-koodattu signaali kerrotaan pseudosatunnaisella, 11 kertaa korkeampitaajuisella signaalilla. Moduloitu signaali jakautuu laajemmalle taajuusalueelle, eikä häiriö yksittäisellä taajuudella tee datasta lukukelvotonta. (IEEE 1997.)

Standardista kehitettiin rinnakkain kahta uutta versiota. Vuoden 1999 joulukuussa julkaistiin standardi IEEE Std 802.11b-1999, joka määritteli 2,4 GHz:n taajuusalueella toimivan, nopeamman langattoman verkkostandardin. Käytännössä vuoden 1997 standardia seuraavat versiot tunnetaan standardin numeron ja kirjaintunnuksen perusteella, eli Std 802.11b-1999 tunnetaan yleisesti 802.11b:nä. On myös tavallista käyttää pelkkää standardin kirjaintunnusta osoittamaan standardin versiota. Versio b käyttää CCK (engl. Complementary Code Keying)-modulaatiotekniikkaa, ja koodaa signaaliin lisää dataa moduloinnin yhteydessä. Näillä parannuksilla päästään 5,5 tai 11 megabitin nopeuksiin käytetystä tekniikasta riippuen. (IEEE 1999.)

Pian 802.11b:n julkaisun jälkeen julkaistiin 802.11a-1999, joka määritti 5,8 GHz:n taajuusalueella toimivan verkkostandardin. Versio a hyödyntää Orthogonal Frequency Division Multiplexing (OFDM) -modulaatiotekniikkaa, ja toiminta vähemmän käytetyllä taajuusalueella vähentää häiriöitä. OFDM-tekniikalla laite lähettää 48:aa eri kantoaaltoa hiukan eri taajuuksilla, ja lähetykset on ajoitettu niin, etteivät kaiut ja heijastumat häiritse muita kantoaaltoja. lähetysten välissä on myös 800 nanosekunnin odotusaika. Tämä sekä erottaa lähetykset toisistaan, että antaa kaiuille aikaa vaimentua. Versio a pääsee jopa 54 megabittiin sekunnissa. (IEEE 1999.)

Standardin 802.11a määrittämä tekniikka on huomattavasti 802.11b:n tekniikkaa nopeampi, mutta laitevalmistajien huomio kohdistui enemmän b-versioon. Versio a oli huomattavasti vaikeampi, ja näin kalliimpi, toteuttaa. 802.11b:n suosiota saattoi selittää myös se, että lähes kuuden gigahertsin taajuusalueella toimiva 802.11a oli kantamaltaa hiukan lyhyempi. Sekä toimistoissa että kotitalouksissa käytetyt rakennusmateriaalit vaimentavat korkeataajuuksista signaalia jonkin verran. (Berg.)

4.2 802.11g

Heinäkuussa 2000 IEEE muodosti uuden työryhmän, jonka tehtävänä oli luoda standardi OFDM-modulaation käyttämiseen 2.4GHz:n taajuusalueella. Task Force G, kuten työryhmä tunnettiin, loi 802.11b-standardin kanssa yhteensopivan uuden standardin noin kolmessa vuodessa. Langaton lähiverkkostandardi 802.11g ratifioitiin kesäkuussa 2003. Teknisesti 802.11g lähinnä määrittää tekniikan, jolla uuden standardin mukaiset laitteet voivat toimia samalla taajuusalueella vanhemman standardin laitteiden kanssa. Koodaus, ja modulaatiotekniikat ovat lähes täysin samat kuin 802.11a-standardissa, mutta PSK-koodaus voidaan korvata QAM-koodauksella (engl. Quadrature Amplitude Modulation). QAM mahdollistaa huomattavasti suuremman datamäärän siirtämisen samalla taajuusalueella verrattuna DBPSK- tai DQPSK-koodaukseen. Koska kaistanleveydet tiheästi hyödynnetyllä 2.4GHz:n taajuusalueella ovat kapeita, tämä on tärkeää verkon nopeuden kannalta. Kuten samanlaisuudet standardien välillä vihjaavat, g-standardin mahdollistama teoreettinen nopeus on sama kuin a-standardin: noin 54 megabittiä sekunnissa. (IEEE 2003.)

4.3 802.11n

Syyskuussa 2003, vain kuukausia standardin 802.11g ratifioinnin jälkeen, IEEE loi uuden työryhmän, jonka tavoitteena oli kehittää nopeampi verkkostandardi. Virallisesti vuonna 2009 julkaistu 802.11n laskee odotusajan (engl. guard interval) 800 nanosekunnista 400, jos sekä lähettävä että vastaanottava laite tukevat tätä tilaa. Kanavien leveys on kaksinkertaistettu 20 megahertsistä 40 megahertsiin. Modulaatiotekniikat ovat samat kuin 802.11g-standardissa. Lyhyempi odotusaika kasvattaa teoreettista nopeutta vain hiukan, mutta kanavan leveyden kaksinkertaistamine kaksinkertaistaa verkon nopeuden. Käytettäessä vain yhtä 40 MHz leveää kanavaa 64-QAM-modulaatiolla, voidaan saavuttaa teoreettinen 150 megabitin siirtonopeus. (IEEE 2009.)

Merkittävin 802.11n-standardin määrittämä uudistus on usean kanavan yhtäaikainen käyttö, MIMO. (engl. Multiple Input, Multiple Output) Laitteet voivat tukea yhtä, kahta, kolmea tai neljää samanaikaista kanavaa. Jos edellä esitetyn esimerkin laitteet käyttäisivät neljää 40 MHz:n kanavaa samanaikaisesti, teoreettinen tiedonsiirtonopeus olisi 600 megabittiä sekunnissa. Käytännössä laitevalmistajat tuottavat yhtä tai kahta kanavaa samanaikaisesti käyttäviä laitteita. Näitä markkinoidaan usein termeillä WiFi-N 150 Mbps ja WiFi-N 300 Mbps, teoreettisten siirtonopeuksiensa mukaan. (IEEE 2009.)

Standardin 802.11n historiassa on huomattavaa, että laitevalmistajat alkoivat tuottaa laitteita jo standardin vedoksien perusteella, useita vuosia ennen lopullisen standardin julkaisua. Vedos 1.0 vahvistettiin 9. marraskuuta 2006, ja siihen perustuvia laitteita oli markkinoilla jo saman vuoden aikana. Alkuvuonna 2007 vahvistettiin vedos 2.0, ja IEEE ilmoitti, että vedosta 2.0 noudattavat laitteet olisivat täysin yhteensopivia lopullisen standardin kanssa. Jo saman vuoden toukokuussa markkinoilla oli vedoksen 2.0 mukaisia laitteita. Tämä osoittaa, että ajankohta jona IEEE vahvistaa standardin, ei välttämättä osoita laitteiden kaupallista saatavuutta. Verkkosuunnittelun näkökulmasta virallista standardia edeltäneiden laitteiden merkitys on pieni. Jos päätelaitteen verkkokortti perustuu 802.11n vedoksiin, mutta ei ole yhteensopiva lopullista standardia noudattavien verkkolaitteiden kanssa, se muodostaa yhteyden käyttäen vanhempaa 802.11g-standardia.

(Fleishman 2006.)

4.4 802.11ac

Syyskuussa 2008 perustettiin työryhmä tuottamaan vieläkin nopeampaa langatonta verkkostandardia. Vuoden 2013 lopulla ratifioitiin standardi 802.11ac-2013. Siirtonopeutta on kasvatettu hiukan käyttämällä 256-QAM-modulaatiota aiemman 64-QAM modulaation sijasta. Samalla taajuudella, lähetysvirtojen määrällä, ja kaistanleveydellä toimiva 802.11ac-verkko parantaa verkon tiedonsiirtonopeutta hiukan verrattuna 802.11n-verkkoon, jos käytössä on 256-QAM-modulaatio. Jos lähetysvirtojen määrä, taajuus ja modulaatiotekniikka ovat identtiset, 802.11n ja 802.11ac tuottavat saman tiedonsiirtonopeuden. Suurin tiedonsiirtonopeuteen vaikuttava ero standardien välillä on tuettujen yhtäaikaisten lähetysvirtojen määrä.

(IEEE 2013.)

4.5 Langaton tietoturva – WEP ja WPA

Standardi IEEE Std 802.11-1997 määrittää protokollia, joilla verkon käyttäjät voidaan todentaa, ja verkossa liikkuvaa dataa suojata, jos verkon käyttökohde vaatii suojausta. Avoimen järjestelmän tilassa (engl. Open System) päätelaitteet voivat liittyä kaikille avoimeen langattomaan lähiverkkoon. Jokainen verkkoon liittynyt käyttäjä pystyy tarkastelemaan kaikkea verkossa liikkuvaa dataa. Käyttökohteissa, jossa langattomalla verkolla tarjotaan Internet-yhteys erimerkiksi yrityksen tai muun yhteisön asiakkaiden vapaaseen käyttöön, tämä toimintatila saattaa olla tarkoituksenmukainen.

(IEEE 1997.)

Langattomien verkkojen suunnittelussa valmistauduttiin ensimmäisestä standardista alkaen arkaluontoisen tai muuten yksityisen datan siirtoon. Std 802.11-1997 määrittää menetelmän, jolla päätelaitteen ja langattoman tukiaseman välillä liikkuva data voidaan suojata ulkopuolisilta. WEP (engl. Wired Equivalent Privacy) on algoritmi, joka, Std 802.11-1997:n mukaan, suojaa käyttäjiä satunnaiselta salakuuntelulta. Standardin mukaan WEP:n tarkoitus on tarjota langallisten verkkojen tasoinen tietoturvataso langattomien verkkojen käyttäjille.

(IEEE 1997.)

WEP:n kuvaus, sekä nimi, langallisen verkon tietoturvaa vastaavana on langattomien verkkojen yleistyttyä osoittautunut varsin optimistiseksi. Sen tehtäväkuvausta voidaan jopa pitää ironisena, jos sitä tarkastellaan nykyaikaisesta näkökulmasta. Yksi standardissa määritetty WEP:n tavoite on olla suorituskykyinen, mutta toteutettavissa ohjelmistokoodilla, ilman erillistä laitteistoa. Tämä on toteutettu käyttämällä Rivest Cipher 4 -algoritmia 40-bittisellä salausavaimella. Yhdysvaltain silloinen lainsäädäntö esti yli 40-bittisten salausavaimien käytön vientituotteissa, joten Yhdysvalloissa kehitettyä RC4-algoritmia ei voitu maailmanlaajuisessa standardissa käyttää vahvemman avaimen kanssa.

(Stubblefield, Ioannidis & Rubin 2001.)

Vuonna 2001 julkaistu tutkimusraportti *Weakness in the Key Scheduling Algorithm of RC4* kuvaa menetelmää, jolla Rivest Cipher 4 -algoritmin salausavain voidaan päätellä salatusta datavirrasta. Hyökkäys perustuu haavoittuvuuksiin RC4:n lyhyissä, vain, 24-bittisissä alustusvektoreissa. Koska hyökkäys ei kohdistu avaimeen itseensä, on kyseenalaista, olisiko pidempi salausavain auttanut WEP-protokollaa. Sittemmin myös 128-bittistä avainta käyttävä RC4 on murrettu, joten voidaan spekuloida, että pidempi salausavain olisi parhaassakin tapauksessa vain antanut lisäaikaa uuden suojausstandardin kehittämiseen.

(Fluhrer, Mantin & Shamir.)

IEEE perusti työryhmän luomaan uutta salausstandardia jo vuoden 2001 toukokuussa. On selvää, että IEEE otti RC4-algoritmin matemaattiset haavoittuvuudet vakavasti, ja reagoi kun kävi selväksi, että WEP-suojausstandardi oli riittämätön. Jos oletetaan, että elokuussa 2001 julkaistu *AT&T Technical Report TD-4ZCPZZ Using the Fluhrer, Mantin, and Shamir Attack to Break WEP* kuvaa ensimmäistä käytännön hyökkäystä WPA-suojausta vastaan, käy selväksi, että IEEE reagoi WEP:n potentiaaliseen heikkouteen ennen kuin hyökkäyksen oli todistettu toimivan käytännössä.

(IEEE.)

Kesäkuussa 2004 julkaistiin IEEE Std 802.11i-2004. Standardi kuvaa huomattavasti parannettua suojausstandardia, joka tunnetaan kaupallisissa yhteyksissä nimellä WPA2 (engl. Wireless Protected Access 2). Ensimmäinen versio WPA-suojausprotokollasta ei tosiasiassa ole erillinen protokolla, vaan WiFi Alliancen nimi tuotteille, jotka seurasivat vedosta 802.11i-standardista jo ennen standardin virallista ratifiointia. Uutta suojausprotokollaa hyödyntäviä tuotteita tuli saataville vuoden 2003 aikana,

mutta löyhemmin säädelty WPA-protokolla ei, toteutuksesta riippuen, välttämättä ole yhteensopiva lopullista 802.11i-standardia noudattavien laitteiden kanssa. Nykyaikaisessa verkkosuunnittelussa tätä ei tarvitse erikseen huomioida, koska lähes kaikki WPA2-standardia tukevat laitteet tukevat myös WPA-standardin vähimmäisvaatimuksia.

(IEEE.)

Teknisesti 802.11i määrittää kaksi protokollaa liikenteen suojaamiseen. Näistä ensimmäinen, Temporal Key Intergrity Protocol, käyttää RC4-algoritmia, mutta muuttaa alustusvektorin käsittelyä turvallisemmaksi. WiFi Alliance julkaisi TKIP-protokollan vuonna 2002, se suunniteltiin yhteensopivaksi olemassaolevien WEP-suojausta käyttävien laitteiden kanssa. Tavoitteena oli parantaa olemassaolevien laitteiden tietoturvaa ohjelmistopäivityksillä, ja korjata WEP-protokollan heikkouksien aiheuttama tieturva-aukko nopeasti. Oli tiedossa, että IEEE valmisteli täysin uudistettua suojausprotokollaa, mutta voidaan spekuloida, että WiFi Alliancen jäsenet tiesivät tämän kestävän vuosia. Voidaan edelleen spekuloida, että laitevalmistajat tarvitsivat keinon palauttaa asiakkaidensa luottamus langattomiin verkkoratkaisuihin nopeasti, joten WiFi Alliance ohitti IEEE:n verrattain hitaan suunnittelu- ja ratifiointiprosessin. IEEE olisi tuskin sisällyttänyt TKIP-protokollaa uuteen standardiin, jos ei olisi jo ollut laajasti käytössä. Tätä olettamusta tukee IEEE:n päätös julistaa TKIP vanhentuneeksi vuonna 2009.

(IEEE 2004.)

Standardin 802.11i todellinen vastaus WEP:n heikkouksiin on CCMP-protokolla. CCMP on valinnainen ominaisuus WPA-standardin mukaisissa laitteissa, mutta 802.11i listaa tämän protokollan pakollisena ominaisuutena. CCMP suojaa liikenteen käyttäen AES-standardia. Yhdysvalloissa marraskuussa 2001 julkaistu AES pohjautuu Rijndael-salausalgoritmiin. RC4-algoritmiin verrattuna Rijndael on huomattavasti turvallisempi, eikä AES-standardia noudattavaa salausta ole tämän työn kirjoitushetkellä murrettu matemaattisella hyökkäyksellä. Hyökkäystekniikoista näennäisesti lupaavin, Bicliquehyökkäys ei ole merkittävästi raa'an voiman (engl. brute force attack) käyttöä nopeampaa. Raa'an voiman käyttö, eli jokaisen mahdollisen salausavaimen kokeileminen, kunnes oikea avain löytyy, ei ole edes teoreettisesti käytännöllistä. Ryhmä kryptografian harrastajia voitti vuonna 1997 RSA Laboratories:n haasteen, ja mursi huomattavasti heikomman RC5-algoritmin. Tässä tapauksessa salausavain oli vain 56-bittiä pitkä, ja avaimen murtaminen kesti hajautettua laskentaa käyttäen 250 päivää. Sama ryhmä mursi 64 bittiä pitkän salausavaimen vuonna 2002, ja voitti toisen RSA Laboratories:n haasteen. Avain oli vain 8 bittiä pidempi, mutta sen murtaminen vei 1757 päivää. Ryhmä on yrittänyt mur-

taa 72 bittiä pitkää salausavainta yhtäjaksoisesti joulukuusta 2002 lähtien, eikä ole tämän työn kirjoitushetkellä onnistunut. Kun otetaan huomioon, että CCMP-protokollaa käyttävät laitteet neuvottelevat uuden avaimen säännöllisesti, voidaan todeta, että 256 bittiä pitkää avainta käyttävän AES-salauksen murtaminen ei tällä hetkellä ole mahdollista. Nykyaikaisen langattoman verkon tietoturvaa voidaan siis pitää langallisten verkkojen tasoisena.

(Project RC5 2013.)

Verkkosuunnittelun näkökulmasta on syytä huomioida, että moni vanhempi tukiasema on taaksepäin yhteensopiva WPA-standardin kanssa. On siis mahdollista, että vanhempi päätelaite kytkeytyy näennäisesti suojattuun verkkoon käyttäen TKIP-suojausprotokollaa. Toistaiseksi heikkoudet TKIP-protokollassa ovat olleet teoreettisia, mutta uusia yritysverkkoja ei ole järkevää rakentaa ilman mahdollisuutta poistaa TKIP-protokolla käytöstä. Tällä hetkellä tuki TKIP-protokollalle on kuitenkin syytä pitää käytössä, koska erityisesti yritysten ja yhteisöjen tiloissa käyttäjillä saattaa olla hyvinkin vanhoja päätelaitteita.

Wi-Fi Alliance on laajentanut IEEE:n standardia luomalla uusia todennusmenetelmiä perinteisen käyttäjän syöttämän alfanumeerisen salasanan rinnalle. Wi-Fi Protected Setup, WPS, on protokolla, jolla tukiasema pystyy jakamaan langattoman verkon salasanan hyväksytyille päätelaitteille helpommin. Yhdessä käyttötilassa käyttäjä voi syöttää 8-numeroisen PIN-koodin, ja tukiasema lähettää salasanan päätelaitteelle salattuna. Toinen tekniikka on fyysinen painike tukiasemassa. Tätä painettaessa tukiasema lähettää salasanan mille tahansa päätelaitteelle, joka pyytää sitä. Kumpikin tekniikka käytännössä ohittaa WPA-salauksen. WPS luotiin helpottamaan suojattujen verkkojen käyttöä, erityisesti kokemattomien kotikäyttäjien tapauksessa, mutta tekniikka on monella tapaa puutteellinen. Algoritmi, jolla salasana salataan, on heikko, lähetettäessä salasana painikkeella ei nähdä, mitkä päätelaitteet vastaanottavat salasanan, ja PIN-koodiin perustuvassa suojauksessa on useita puutteita.

(Ducklin 2015.)

On selvää, että 8-numeroinen koodi vaatii vähemmän murtoyrityksiä kuin WPA-salausavain, jonka ominaisuudet käytiin läpi edellä. Koodin viimeinen numero on tarkistusmerkki, joka lasketaan seitsemän aiemman numeron perusteella. Seitsemän merkitsevää numeroa lähetetään lisäksi kahdessa erillisessä osassa, joten murrettavana on yksi 4-numeroinen ja yksi 3-numeroinen koodi. Todellisen 8-

numeroisen koodin murtaminen voi enimmillään vaatia 10^8, eli 100 000 000 yritystä. Nykyaikaiselle tietotekniikalle jo tämä määrä permutaatioita olisi pieni, mutta kun murrettavana on ensin 10^4=10 000, ja sitten 10^3=1000 mahdollista yhdistelmää, vaihtoehtoja on enimmillään 11 000. Tätä voitaisiin verrata kahdella yhdistelmälukolla varustettuun salkkuun tai matkalaukkuun, mutta lukon mekaaninen manipulointi on itse asiassa verrattain hidasta. WPS taas ei aseta rajaa yhdistämisyritysten tiheydelle, joten hyökkääjä voi automatisoidulla komentosarjalla käydä läpi kymmeniä, ellei satoja mahdollisia yhdistelmiä sekunnissa. Jos salkkuanalogiaa viedään pidemmälle, todennäköisten yhdistelmien määrää voidaan vähentää entisestään, jos salkun omistaja tunnetaan. Yhdistelmä on todennäköisesti jokin omistajalle merkityksellinen numerosarja, huolimatta yleisestä suosituksesta olla käyttämättä merkityksellisiä numeroita, kuten päiväyksiä. WPS kärsiin saman tyyppisestä ongelmasta. Ainakin kahden laitevalmistajan, D-Link:n ja Belkin:n, tukiasemien PIN-koodi luodaan laitteen MAC-numerosta tai sarjanumerosta. Koska MAC-numero on osa verkkolaitteiden normaalia kommunikaatiota, ja sarjanumero on mahdollista saada huolto- ja diagnostiikkakomentoja käyttäen, mahdollisten PIN-koodien määrä jää entistäkin pienemmäksi.

(Ducklin 2015.)

WPS ei ole IEEE:n standardi, ja Wi-Fi Alliance itse suosittelee turvattomaksi osoittautuneen PIN-kooditekniikan poistamista käytöstä, jos tukiaseman asetukset mahdollistavat sen. Useimmat alan lähteet suosittelevat WPS:n poistamista käytöstä kokonaan, eikä sitä tule missään tapauksessa käyttää yritysverkossa.

Wi-Fi Alliancen standardit WPA-Enterprise ja WPA2-Enterprise hyödyntävät IEEE:n 802.1X-standardia käyttäjän todennukseen ja RADIUS-protokollaa todennusdatan välittämiseen. Enterprise-todennus perustuu käyttäjien käyttäjätunnuksiin ja salasanoihin yhden jaetun avaimen sijaan. RADIUS on laajasti käytössä yrityksissä ja yhteisöissä, kun käyttäjät kirjautuvat yhteisön tietokoneille. Käyttäjän henkilöllisyys ja salasana vahvistetaan keskitettyä tietokantaa vasten, joten jokainen käyttäjä voi potentiaalisesti käyttää omia tunnuksiaan jokaisella yhteisön verkkoon kytketyllä tietokoneella. Esimerkiksi oppilaitoksissa on tavallista, että opiskelijat kirjautuvat tietokoneille luokkahuoneissa ennen oppitunnin alkua. Opiskelijat voivat käyttää mitä tahansa luokassa olevaa tietokonetta, ja käyttöjärjestelmä varmistaa kirjautumistiedot RADIUS-palvelimelta. WPA2-Enterprise mahdollistaa samojen kirjautumistietojen käyttämisen liityttäessä suojattuun langattomaan verkkoon.

(IEEE 2001.)

WPA2-Enterprise hyötyy 802.1X-todennuksen kaikista ominaisuuksista. 802.1X hyödyntää Extensible Authentication Protocol -todennusprotokollaa. EAP todentaa käyttäjän, ja tallentaa sertifikaattitiedoston käyttäjän laitteelle. Käyttäjän ei siis tarvitse syöttää tunnuksiaan uudelleen joka kerta liittyessään samaan verkkoon, mutta koko suojaus ei myöskään perustu yhteen muuttumattomaan salasanaan. EAP mahdollistaa myös niin sanotun luottosuhteen eri verkkojen välillä. Jos käyttöpaikkojen välillä on luottosuhde, käyttäjä sijainnista A voi kirjautua tietokoneelle, langattomaan verkkoon, tai vastaavaan suojattuun resurssiin sijainnissa B. Kun käyttäjä kirjautuu verkkoon, todennuspalvelin sijainnissa B välittää todennuspyynnön todennuspalvelimelle A. Maantieteellinen etäisyys käyttöpaikkojen välillä on merkityksetön, koska todennuspyyntö välitetään TCP/IP-verkossa. Kansainvälinen oppilaitosverkkojen yhteenliittymä Eduroam hyödyntää luottosuhteita, ja on luonut kansainvälisen todennuspalvelinten verkoston. Oppilaitos voi tarjota opiskelijoille suojatun Wi-Fi verkon käyttäen opiskelijoiden olemassa olevia käyttäjätunnuksia. Koska Eduroam-verkkojen välillä on luottosuhde, esimerkiksi Vaasan ammattikorkeakoulun opiskelija pystyy kirjautumaan Vaasan yliopiston tai vaasalaisen Yrkeshögskolan Novian langattomaan verkkoon, mutta oppilaitokset voivat ylläpitää ja kehittää langattomia verkkojaan toisistaan riippumatta. Jos sama opiskelija vierailisi vapaa-ajallaan Harvardin yliopiston kampuksella, hän voisi edelleen käyttää Vaasan ammattikorkeakoulun käyttäjätunnuksia ja kirjautua Eduroam-verkkoon.

(GÉANT 2018.)

5 WLAN-verkot yrityskäytössä

Tilastoja langattomien lähiverkkojen käyttöönotosta yrityksissä ei käytännössä ole saatavilla. Käytännössä voidaan olettaa, että yrityskäyttöön markkinoitujen päätelaitteiden kehitys heijastaa verkkoteknologioden yleistymistä. BlackBerry Ltd:n BlackBerry 7270 julkaistiin vuoden 2004 lopulla, ja tuki 802.11b-standardia. (Slavin 2004.) Nokia 9300i, Nokia Oyj:n yrityskäyttäjille suunnattu matkapuhelin vuodelta 2005, tuki standardia 802.11g. (Nokia 2005.) Intel Corporation alkoi markkinoida Centrino-tuotemerkkiään vuonna 2003. Intel Centrino oli laitealusta kannettaviin tietokoneisiin, ja sen ensimmäinen versio koostui 855-piirisarjasta, Pentium M-suorittimesta ja PRO/Wireless 2100B -verkkokortista. (Coelho 2009.) Tästä voidaan päätellä, että langattomat verkot alkoivat todella yleistyä yrityskäytössä noin vuodesta 2004 alkaen, samaan aikaan kun 802.11g-standardia noudattavia päätelaitteita alkoi saapua markkinoille. Tämä on tuskin satumaa, kun otetaan huomioon g-standardin mahdollistama tiedonsiirtonopeus verrattuna b-standardiin ja kiinteisiin Ethernet-verkkoihin.

5.1 Usean tukiaseman muodostama yhtenäinen verkko

Kotikäytössä yksi langaton tukiasema riittää usein kattamaan käyttävien tarvitseman alueen. Yrityskäytössä tilat ovat suurempia, ja verkon katteen on oltava yhtenäinen. Usean tukiaseman on tarjottava verkko, joka on käyttäjän näkökulmasta saumaton. Käyttäjän liikkuessa esimerkiksi rakennuksen päästä toiseen tai kerroksesta kerrokseen, päätelaitteen verkkoyhteyden on oltava katkeamaton, ja siirtymän uuteen tukiasemaan looginen. IEEE:n standardi 802.11k-2008 määrittää tekniikan, jolla verkon hallintapalvelin ja päätelaite seuraavat päätelaitetta ympäröivien signaalien voimakkuutta. Tämän tiedon perusteella päätelaite voi siirtyä käyttämään tukiasemaa, jonka signaali on vahvin, kun edeltävän tukiaseman signaalin voimakkuus on riittämätön. Standardi 802.11r-2008 määrittää tekniikan, jolla päätelaite voi tunnistautua uudelle langattomalle tukiasemalle verkossa, johon se on yhdistetty. Käyttäen niin sanottua BSS-siirtymää (engl. BSS transition), päätelaite ottaa olemassa olevat turva- ja nopeusasetukset käyttöön uuden tukiaseman kanssa. Standardi pyrkii lähes saumattomaan siirtymään, jossa päätelaitteen verkkoyhteys ei häiriinny merkittävästi, ja käyttäjän tarvitsee yhdistää päätelaitteensa verkkoon vain kerran. Käytännössä mitattu 40 millisekunnin siirtymäaika saattaa marginaalisesti

häiritä reaaliaikaiseen tiedonsiirtoon perustuvia palveluja kuten video- tai äänipuheluita. (Huotari 2015.)

5.2 Tukiasemien päällekkäisyys ja kapasiteetti

Usean tukiaseman verkossa signaalin voimakkuus ei ole ainoa valintaperuste päätelaitteen käyttämälle tukiasemalle. Standardi 802.11v määrittää tekniikan, jolla langattoman verkon laitteet tarkkailevat palvelun laatua kokonaisuudessaan. 802.11v mahdollistaa kuormantasauksen tukiasemien kesken tilanteessa, jossa useamman tukiaseman singaalivoimakkuus riittää päätelaitteiden palvelemiseen. (Cisco Systems.)

5.3 Ethernet-taustaverkko

Ethernet-verkkoyhteyksien kaapelointiin lyhyillä matkoilla käytetään useimmiten kahdeksanjohtimista, neljästä kierretystä johdinparista koostuvaa kategorian 5, 5e, tai 6 -kaapelia. Nämä kaapelityypit tunnetaan tavallisesti englanninkielisen lyhenteen Cat mukaan. (engl. Category) Kategoria 4 oli ensimmäinen neljästä kierretystä johdinparista koostuva kaapelityyppi. Kategoria 4 mahdollistaa 20 megahertsin taajuuden ja 16 megabitin tiedonsiirtonopeuden sekunnissa. Sitä voitaisiin siis käyttää 803.1-standardin mukaiseen Ethernet-liikenteeseen nopeudella 10 megabittiä sekunnissa. Käytännössä tähän kuitenkin käytettiin jo laajasti kategorian 5 kaapelia. (ANSI, TIA & EIA 2001.)

Kategorian 5 kaapeli on määritetty standardissa TIA/EIA-568 vuonna 1991, ja parannettu versio Cat 5e saman standardin revisiossa vuonna 2001. Standardi ISO/IEC 11801 määrittää tälle kaapelille ja sen seuraajille vähimmäistiedonsiirtonopeuden. Kategorioiden 5 ja 5e kaapeleiden on standardien mukaan tuettava 100 megabitin IEEE 802.3u-standardia sadan metrin mittaisilla kaapeleilla. 802.11u, joka tunnetaan myös nimellä 100BASE-TX, käyttää vain kahta kaapelien neljästä johdinparista. Nopeampi 1000BASE-T, IEEE 802.11ab, käyttää kaikkia neljää johdinparia, mutta toimii edelleen Cat 5-kaapeleilla 100 metriin asti. Kuten nimestä käy selville, tämän standardin määrittämä tiedonsiirtonopeus on 1000 megabittiä, eli yksi gigabitti sekunnissa. (ANSI, TIA & EIA 2001.)

Standardi 802.3an määrittää standardin kymmenen gigabitin tiedonsiirtonopeuteen. Tämä myös nimellä 10GBASE-T tunnettu standardi vaatii kategorian 6a kaapelien käyttöä, jos kaapelin pituus on standardin suurin sallima 100 metriä. Kymmenen gigabitin Ethernet-verkot eivät kuitenkaan ole laajasti käytössä. Suurin osa päätelaitteista, tai esimerkiksi langattomista tukiasemista, ei toistaiseksi tue 10GBASE-T-standardia. Voidaan kuitenkin todeta, että oikein toteutettu Ethernet-verkko langattoman verkon taustalla tukee aina korkeampaa tiedonsiirtonopeutta kuin langaton verkko itse. (IEEE 2006.)

IEEE:n standardit 802.3af-2003 ja 802.3at-2009 määrittävät tekniikoita, joilla päätelaitteille voidaan syöttää virtaa kategorian 5 tai 6 Ethernet-kaapeleita käyttäen. Vanhempi standardi mahdollistaa noin 15 watin tehon syöttämisen. Päätelaitteen vastaanottama jännite on välillä 37 ja 57 volttia. Uudempi standardi määrittää päätelaitteen jännitteen välille 42.5 ja 57 volttia, ja suurin syötetty teho on 30 wattia. Virta Ethernetin yli (engl. PoE, power over Ethernet) on käytännöllinen tekniikka, jos päätelaite sijoitetaan epätavalliseen paikkaan, kauas virtapistokkeista. Valvontakamerat, liiketunnistimet ja muut kiinteistöjen turvalaitteet käyttävät tätä tekniikkaa. Kun erillistä virtajohtoa tai virtapistoketta ei tarvita, laite voidaan sijoittaa mihin tahansa, kunhan kohteeseen on mahdollista johtaa Ethernet-kaapeli. Sijoittelun vapaus on myös hyödyllistä langattomien tukiasemien tapauksessa. (IEEE 2003.)

PoE-standardi mahdollistaa virran syöttämisen kaapelin käyttämättömissä pareissa, jos tiedonsiirtoon käytetään standardia 100BASE-T. Tämä tunnetaan toimintatilana B. Virtaa voidaan myös syöttää aktiivisia datajohtimia pitkin, joten tekniikkaa voidaan käyttää 1000BASE-T-standardia noudattavissa verkoissa. Koska Ethernet-tiedonsiirto perustuu eroihin jännitetasoissa, datajohtimiin syötetty jännite ei vaikuta tiedonsiirtoon, kunhan päätelaite tukee PoE-standardia. Standardi vaatii, että virtaa syöttävä laite ja päätelaite neuvottelevat käytetyn tekniikan, joten jos päätelaite ei tue PoE-standardia, virtaa syöttävä laite, joko Ethernet-kytkin tai erillinen virransyöttölaite, ei syötä kaapeliin virtaa. Virransyöttö Ethernet-kaapelia käyttäen mahdollistaa langattomien tukiasemien sijoittelun joustavasti, koska niiden ei tarvitse olla tietyllä etäisyydellä virtapistokkeesta. (IEEE 2009.)

5.4 Tietoturvanäkokohtia

Useimmiten yrityksen tai julkisyhteisön tiloihin sijoitettu langaton verkko on eriytetty yhteisön mahdollisesta sisäisestä verkosta. Pienissä tiloissa on periaatteessa mahdollista käyttää erillistä laajakaistaliittymää, johon on liitetty erillinen DLS- tai kaapelimodeemi. Tänä päivänä jopa kuluttajille markkinoitavissa langattomissa tukiasemissa on kuitenkin saatavilla käytännöllisempi vaihtoehto. Tukiasema voi luoda niin kutsutun vierailijaverkon ensisijaisen langattoman verkon rinnalle. Vierailijaverkossa ei useimmiten ole käytössä edellä kuvattuja suojausominasuuksia. Verkkoon kytketyt päätelaitteet eivät voi kommunikoida ensisijaisen verkon kanssa, eivätkä yleensä myöskään keskenään. (Dondurmacioglu 2012.)

Laajemmissa yritysverkoissa verkkoliikenteen eristäminen toteutetaan ohjelmallisesti. Kaikki verkkoliikenne käyttää samoja verkkokytkimiä, mutta on eristetty erillisiin virtuaalilähiverkkoihin. (VLAN, engl. Virtual local area network) Tämän teknologian toteutuksen määrittää IEEE:n standardi 802.1Q. Standardin ensimmäinen versio julkaistiin vuonna 1998, ja viimeisin vuonna 2018. VLAN-järjestelmässä kytkimet merkitsevät eri lähteistä peräisin olevat Ethernet-paketit eri tunnisteella, ja paketti välitetään vain sen VLAN-tunnisteella varustettuja reittejä pitkin. Näin voidaan esimerkiksi varmistaa, että vierailijaverkosta lähtenyt paketti ei voi liikkua muualle kuin julkiseen Internet-verkkoon liitetylle reitittimelle. Verkko käyttäytyy kuin se olisi fyysisesti kytketty erillisillä kaapeleilla omiin kytkimiinsä ja reitittimiinsä.

(IEEE 1998.)

VLAN-tekniikalla voidaan myös eristää yrityksen sisäisiä verkkoja toisistaan. Näin esimerkiksi oppilaitoksen luokkahuoneissa olevilta pöytäkoneilta ei ole mahdollista olla suoraan yhteydessä henkilökunnan käyttämiin tietokoneisiin. Mahdollinen liikenne kulkee oppilaitoksen palomuurin kautta, ja haitallinen liikenne voidaan estää samoin kuin se olisi tullut oppilaitoksen ulkopuolelta. Yrityskäyttöön suunnitellut langattomat tukiasemat pystyvät myös luomaan useamman langattoman verkon samanaikaisesti, ja ohjaamaan eri verkkojen liikenteen eri virtuaalilähiverkkoihin. Esimerkiksi yrityksen eri osastot voidaan eristää toisistaan käyttämällä eri verkkoja, joiden liikenne ohjataan eri virtuaalilähiverkkoihin. Tavallisesti käyttäjä tunnistautuu yrityksen sisäiseen langattomaan verkkoon käyttäen aiemmin kuvattua 802.1X-todennusprotokollaa. (Cisco Systems.)

6 KORKEATAAJUUKSISTEN RADIOSIGNAALIEN KYKY LÄPÄISTÄ RAKENTEITA

Tavalliset rakennusmateriaalit vaimentavat radioaaltoja 2.2 ja 2.4 gigahertsin välisellä taajuusalueella jonkin verran. Rakennusmateriaalien aiheuttama vaimentuma 5,15 ja 5,35 gigahertsin välisellä taajuusalueella on huomattava. Etelä-Kalifornian yliopiston opiskelija Robert Wilson on aihetta käsittelevässä lopputyössään mitannut eri materiaalien tuottamaa vaimentumaa taajuuksilla 2,3 gigahertsiä ja 5.25 gigahertsiä. Mittaustulokset osoittavat, että 5 gigahertsin taajuusalueella vaimentuma voi olla useita kertoja suurempi verrattuna 2.4 gigahertsin taajuusalueeseen. (Wilson 2002.)

6.1 Seinien ja rakenteiden aiheuttama vaimennus

Eniten vaimentumaa langattomille Internet-verkoille olennaisilla taajuusalueilla tuottavat tiili, betoni ja metallirakenteet. Kipsilevy ja puu vaimentavat signaalia suhteellisen vähän, mutta näitä materiaaleja ei juurikaan käytetä muualla kuin asuinrakennuksissa. Vaikka tämän opinnäytetyön puitteissa suoritetut mittaukset eivät ole yhtä täsmällisiä, Centria-Ammattikorkeakoulun tiloissa tehdyt mittaukset vastaavat Wilsonin suorittamia mittauksia. Toisaalta karkaistusta lasista ja teräksestä valmistetut ovet vaimentavat signaalia huomattavasti, vaikka Wilsonin tulosten mukaan lasi vaimentaa 2,3 gigahertsin taajuisia radioaaltoja vain noin puoli desibeliä. Ovissa käytetyn lasin koostumusta ei ole tarkoituksenmukaista analysoida tämän työn yhteydessä, mutta on mahdollista, että karkaistu turvalasi heijastaa radioaaltoja perinteistä ikkunalasia voimakkaammin. Lisäksi turvalasi on perinteistä ikkunalasia paksumpaa. Tämä selittäisi havaitun vaimentuman. (NIST 1997.)

6.2 Eri 802.11-sukupolvien rakenteista kokema vaimennus

Yhdysvaltain standardi- ja teknologiainstituutin (engl. National Institute of Standards and Technology) mittaukset vahvistavat, että tiili ja sementti vaimentavat radioaaltoja merkittävästi, kun taas lasi ei aiheuta juurikaan vaimentumaa. NIST:n raportti myös osittaa, että nopeampi 5 gigahertsin taajuusalue kokee useimmiten enemmän vaimentumaa kuin 2,4 gigahertsin taajuusalue. Kumpikin edellä viitattu

tutkimus paljastaa epätavallisen poikkeaman. Vanerilevy vaimentaa korkeampaa taajuusaluetta vähemmän. NIST:n raportti näyttää, että vanerilevyn läpäisykyky on suurimmillaan neljän ja viiden gigahertsin välillä, ja laskee voimakkaasti tämän taajuusalueen kummallakin puolella. (NIST 1997.)

Kun otetaan huomioon, että langaton lähiverkkoteknologia on alusta alkaen käyttänyt sekä 2.4 että 5 gigahertsin taajuusalueita samoilla kanavilla, voitaisiin sanoa, että standardin 802.11 eri versiot eivät koe vaimentumaa eri tavalla. 802.11a-standardin mukainen 5 gigahertsin kantoaalto reagoi esteeseen samoin kuin 802.11n-standardin mukainen kantoaalto samalla taajuusalueella. Sama pätee 2,4 gigahertsin taajuusalueeseen.

Keskusteltaessa eri standardin eri versioiden kokemasta vaimennuksesta, on tärkeää huomata, että edellä mainittu johtopäätös pätee vain verrattaessa verkkoja samalla taajuusalueella. Kuten edellä on todettu, 5 gigahertsin taajuusalueella este vaimentaa signaalia moninkertaisesti 2,4 gigahertsin taajuusalueeseen verrattuna.

6.3 Vaimennuksen vaikutus verkon tiedonsiirtonopeuteen

Edellä todetusta huolimatta, datan koodaus kantoaaltoon useimmiten vaikuttaa siihen, paljonko esteen läpäisseestä signaalista on käyttökelpoista. Tällainen analyysi on kuitenkin niin monimutkaista, että se ei kuulu tämän työn piiriin. On myös perusteltua olettaa, että mahdollisen virheenkorjauksen vaikutus on marginaalinen verrattuna eroihin eri 802.11-versioiden tiedonsiirtonopeudessa. Aiemmin kuvattu MIMO-teknologia ei myöskään vaikuta esteisiin. MIMO-lähetyksen jokainen datavirta kokee saman vaimentuman. Lopullinen vaikutus tiedonsiirtonopeuteen on vaimentumien summa.

7 AIEMMAN WLAN-VERKON KARTOITTAMINEN

Centria-Ammattikorkeakoulun Talonpojankadun kampus Kokkolassa koostuu vain yhdestä kolmikerroksisesta rakennuksesta. Aiempi langaton verkko on saatavilla olevien tietojen perusteella rakennettu palvelemaan opiskelijoita ja henkilökuntaa opetuksen ulkopuolella. Verkko kattaa ensisijaisesti käytäviä ja yleisiä tiloja. Kuuluvuus luokkahuoneissa on sattumanvaraista.

7.1 Mittalaitteisto, ohjelmisto ja mittausmenetelmä

Verkon kuuluvuus mitattiin käyttäen Xirrus WiFi Inspector -ohjelmistoa Microsoft Windows 10 -käyttöjärjestelmässä. Mittausten suorittamiseen ei ollut käytettävissä varsinaista mittalaitteistoa, vaan kaikki mittaukset suoritettiin Dell Latitude 7350 -tietokoneella. Tietokoneen langaton verkkokortti on Intel 7265 WiFi- ja Bluetooth-moduuli. Epävirallisesti mittaustuloksia vahvistettiin Android-sovelluksilla puhelimissa ja tablet-tietokoneissa. Varsinaisten mittausten tulokset vastaavat epävirallisia mittauksia puhelimilla ja tablet-tietokoneilla. Voidaan siis todeta, että tulokset vastaavat luotettavasti käyttäjien kokemaa verkon tilaa.

Koska mittauksiin käytetty tietokone on kuluttajalaite, sen langaton verkkokortti käyttää virransäästöominaisuuksia, ja muuten optimoi toimintaansa. On siis pidettävä todennäköisenä, että WiFi Inspector -ohjelmiston ilmoittama kuuluvuus ei kaikissa olosuhteissa vastaa verkon kokemaa todellista vaimentumaa. Työn puitteissa tätä ei pidetä merkittävänä. Kuten jäljempänä käydään läpi, kuuluvuuden vaikutus tiedonsiirtonopeuteen ei ole merkittävä ennen tiettyä raja-arvoa. Jos vaimentuma on vähemmän kuin noin 60 desibeliä, verkon käyttöaste, taustaverkko ja vastaavat tekijät vaikuttavat käyttäjäkokemukseen enemmän.

Käytetyssä verkkokortissa on myös Bluetooth-lähetin, joten työn kuluessa tehtiin epävirallinen kokeilu, jossa tarkasteltiin Bluetooth-lähettimen mahdollista vaikutusta mittaustuloksiin. Ensimmäisessä mittauksessa tietokoneen Bluetooth-lähetin käytössä, ja yhdistetty langattomiin kuulokkeisiin. Toisessa

mittauksessa Bluetooth oli poissa käytöstä. Verkon nopeus testattiin kaupallisen palveluntarjoajan nopeustestisivustoa käyttäen kolme kertaa kummassakin testiasetelmassa. On selvää, että julkisen, kaupallisen nopeustestin käyttäminen on epätarkkaa, mutta tarkempaa mittausmenetelmää ei ollut käytettävissä. Vaihteluväli testistä toiseen oli suurempi kuin Bluetooth-lähettimen mahdollinen vaikutus. Lähettimen tilalla ei myöskään ollut vaikutusta havaittuun signaalivoimakkuuteen. Tästä huolimatta tietokoneen Bluetooth-lähetin oli kytketty pois käytöstä kaikkien tässä työssä kuvattujen mittausten aikana.

Luokkahuoneissa ja vastaavissa tiloissa mittaukset suoritettiin ulkoseinän vieressä, päätelaitteen takaosa, ja näin antenni, suunnattuna ulkoseinää kohti. Kun otetaan huomioon aiemman verkon tukiasemien sijoittelu, tämä vastaa heikointa mahdollista signaalivahvuutta, jonka käyttäjä kokisi tilassa. Käytävillä mittaukset suoritettiin useassa kohdassa, ja tulokset kirjattiin erikseen käytävien eri osille.

Tässä työssä hyvänä kuuluvuutena pidetään vaimentumaa, joka on välillä -30 ja -69 desibeliä. Noin -60 desibeliin saakka päätelaitteen yhteys langattomaan verkkoon on tyypillisesti moitteeton, eikä verkon nopeutta rajoita signaalin vahvuus. Jos vaimentuma on välillä -61 dB ja -69 dB, verkon nopeus ja viive (engl. latency) saattavat heikentyä hiukan, muttei kuitenkaan merkittävästi. On perusteltua huomioida, että jo tukiaseman ja päätelaitteen kotelointi vaimentaa mitattua signaalia jonkin verran. Jos tukiasema ja päätelaite ovat yhden metrin päässä toisistaan, eikä niiden välillä ole esteitä, havaittu vaimennus on noin -40:stä -45 desibeliin. Pienin mahdollinen vaimentuma ja näin korkein mahdollinen signaalivahvuus on -30 desibeliä.

Heikkona kuuluvuutena pidetään signaalivahvuutta välillä -70 ja -89 desibeliä. Tällä alueella singaalivahvuus vaikuttaa verkon nopeuteen enenevässä määrin, ja mikäli verkon nopeutta eivät rajoita muut tekijät, signaalin vahvuus vaikuttaa käyttäjäkokemukseen. Mikäli lähimmän tukiaseman tarjoama signaalivahvuus on heikompi kuin 90 desibeliä, voidaan todeta, ettei mittauspisteessä ole käytettävissä langatonta verkkoa. Mittaukset osoittivat, että jos kannettavalla tietokoneella saatu tulos on -90 dB tai heikompi, matkapuhelimet tai tablet-tietokoneet eivät tavallisesti pysty pitämään yllä vakaata yhteyttä verkkoon. Kannettavien tietokoneiden suuremmat antennit ja verkkokorttien suurempi lähetysteho mahdollistavat vakaan yhteyden verkkoon, mutta tiedonsiirtonopeus on riittämätön nykyaikaisten internet-sivujen lataamiseen. -90 desibelin vaimentumalla verkon viive on myös liian pitkä esimerkiksi videopuheluihin.

7.2 Signaalivoimakkuus rakennuksen eri osissa vanhassa verkossa

Aiempi verkko koostuu kahdestatoista tukiasemasta. Ylimmässä kerroksessa opetustiloihin on sijoitettu kaksi tukiasemaa ja hallinnon tiloihin yhtä lailla kaksi. Ensimmäisessä kerroksessa on viisi tukiasemaa, yksi B-siivessä ja loput vanhemmassa siivessä. Pohjakerroksessa käytössä on kolme tukiasemaa, näistä kaikki vanhemman siiven puolella. Tämä selittyy osittain B-siiven pohjakerroksen vähäisellä käytöllä, kun vanha verkko otettiin käyttöön.

Toisen kerroksen B-siivessä vain aula on katettu riittävästi. Luokkahuoneet siiven perällä kokevat huomattavaa vaimentumaa, alle -70 desibeliä. Tällaisella signaalivahvuudella voidaan odottaa verkon nopeuden olevan huomattavasti nominaalinopeutta alempi. A-siiven opetustiloissa signaali on erittäin vahva käytävällä ja keskimmäisessä viidestä luokkahuoneesta. Hallinnon tiloissa ja muissa luokkahuoneissa signaali on kohtalaisen vahva, eikä vaimentuman pitäisi juurikaan vaikuttaa käyttäjäkokemukseen. Näissä tiloissa singaalivahvuus on heikko vain kolmessa toimistohuoneessa.

Ensimmäisessä kerroksessa signaalin vahvuus on heikko suurimmassa osassa B-siipeä. Vain siiven aulassa on mitattavissa vahva langaton signaali. Liikuttaessa aulasta siiven perälle, luokkahuoneet ovat signaalin näkökulmasta peräkkäin kahdessa jonossa. Tämä selittää heikkoa kuuluvuutta B-siiven perällä sekä toisessa että ensimmäisessä kerroksessa. A-siivessä verkon kantama on suurimmaksi osaksi hyvä tai erinomainen. Rakennuksen pääaulassa ja ensimmäisen kerroksen auditoriossa on mitattavissa vahva signaali kahdesta tukiasemasta. Nämä tilat ovat ainoa osa rakennusta, jossa päätelaitteilla on käytettävissä vahva signaali kahdesta tukiasemasta, ja luvussa neljä keskusteltua kuormantasausta on mahdollista hyödyntää tehokkaasti.

Mittauksia suoritettaessa kävi selväksi, että rakennukset lattiat eivät vaimenna langattoman verkon signaalia enempää kuin seinät. Tukiasemat luovat ympärilleen pallon muotoisen katealueen, ja ensimmäisestä kerrosta kattavat myös toisen kerroksen ja kellarikerroksen tukiasemat. Ainoa alue, jossa signaalivahvuus on heikko, on henkilökunnan toimistoalue. Lähimpien tukiasemien ja näiden toimistojen välillä on useita tiiliseiniä, eikä niiden ylä- tai alapuolella ole tukiasemia. Pääovien eteistila on poikkeama, joka ei selity kappaleessa kuusi läpi käydyillä tiedoilla. Vaikka lähin tukiasema on melkein suoraan ovien edessä, signaalivahvuus eteistilassa on heikko. On mahdollista, että metalliovet heijasta-

vat tai vaimentavat radioaaltoja. Tämä ei kuitenkaan tunnu loogiselta. Ovien pinta-alasta suurin osa on lasia. Sama ilmiö havaittiin toimistotilassa eteisen vieressä. Tässä tilassa on samanlaiset lasitetut metalliovet ja -seinät.

Yhteenvetona voidaan todeta, että vanha verkko saavuttaa alkuperäisen tavoitteensa signaalivahvuuden osalta. Käytävillä ja aulatiloissa päätelaite havaitsee kohtalaisen vahvan signaalin ainakin yhdestä tukiasemasta. Käytännössä missä tahansa osassa rakennusta oli havaittavissa useampia langattomia verkkoja, mutta kaikki paitsi yksi olivat signaalivahvuudeltaan erittäin heikkoja.

7.3 Signaalivoimakkuuden vaikutus verkon nopeuteen nykyisellä tekniikalla

Vanhan verkon tuottama käyttökokemus on epätyydyttävä. Singaalivoimakkuus on heikko suurimassa osassa rakennusta. Kun langattoman verkon kuuluvuus heikkenee, tukiasema ja päätelaite neuvottelevat uuden modulaatio- ja koodaustekniikan. Näitä tekniikoita käytiin läpi luvussa 4. Korkeampi tiedonsiirtonopeus vaatii tavallisesti monimutkaisemman koodaustekniikan, joka on puolestaan alttiimpi häiriöille. Jos heikko kuuluvuus pakottaa laitteet käyttämään yksinkertaisempaa tekniikkaa, päätelaitteen ja tukiaseman välinen tiedonsiirtonopeus laskee.

Jos päätelaite ja tukiasema eivät neuvottele yksikertaisempaa koodaustekniikkaa, radiosignaalin kuljettama data saattaa vääristyä matkalla, tai vastaanottava asema ei kuule sitä ollenkaan. Jos liikenne käyttää tavallisempaa TCP-protokollaa (engl. Transmission control protocol), vastaanottava laite ei kuittaa datapakettia vastaanotetuksi, ja lähettäjä joutuu lähettämään sen uudelleen. Verkon vähäinen tiedonsiirtokapasiteetti vähenee entisestään, kun aiemmin lähetettyjä datapaketteja on lähetettävä uudelleen. Reaaliaikaisia datavirtoja varten suunniteltu UDP-protokolla (engl. User datagram protocol), määritelty standardissa RFC 768, ei vaadi kuittausta saapuvasta paketista, ja tavallisesti vastaanottaja reagoi puuttuvaan tai lukukelvottomaan datapakettiin hyppäämällä sen yli. (Internet Engineering Task Force 1989.)

Video- tai audiovirrassa datapakettien katoaminen saattaa näkyä videon pysähtymisenä sekunnin murto-osaksi, kun päätelaite näyttää edellistä virheetöntä ruutua, kunnes seuraava virheetön ruutu saapuu.

Audiovirta tavallisesti mykistyy, kunnes päätelaite saa toistokelpoista dataa. Esimerkiksi videokonferenssien tapauksessa tällainen pysähtely voi olla erittäin häiritsevää. Centria-Ammattikorkeakoulun nimenomaisessa tapauksessa on kuitenkin huomioitava, että vanhan langattoman verkon tiedonsiirtonopeus ei tavallisesti riitä reaaliaikaisen videokuvan toistoon, vaikka itse langaton signaalivoimakkuus olisikin moitteeton.

7.4 Muita teknisiä huomioita nykyisestä verkosta

Aiemman langattoman verkon analyysin yhteydessä käy selväksi, että langattoman verkon taustalla toimivan Ethernet-verkon tiedonsiirtonopeus on riittämätön. Kuten edellä kuvattu, verkko ei mahdollista tyydyttävää käyttäjäkokemusta edes, kun signaalivoimakkuus on riittävä. Uuden verkon langattomat tukiasemat on fyysisesti liitetty samoihin Ethernet-kytkimiin kuin vanhan verkon tukiasemat. Tästä voidaan päätellä, että tiedonsiirtonopeus ei johdu tästä osasta taustaverkkoa. On perusteltua olettaa, että verkossa on käytetty luvussa 5 kuvattua ratkaisua, jossa langattoman verkon liikenne ohjataan omassa virtuaalilähiverkossaan erilliseen laajakaistaliittymään. Tämä on kuitenkin pelkkää spekulointia. Osa tässä työssä kuvatusta taustaverkosta on kolmannen osapuolen hallinnoimaa, eikä verkon rakenteeseen liittyviä tietoja ole saatavilla. On mahdollista, että aiemman langattoman verkon liikenne ohjattiin samaan verkkoliittymään, mutta eri palomuuriin. On yhtä lailla mahdollista, että verkon sallittiin käyttää vain hyvin pieni määrä taustaverkon tiedonsiirtokapasiteettia, koska se nähtiin toissijaisena.

Aiemmassa verkossa ei ole käytössä minkäänlaista todennusta. Mikä tahansa päätelaite voi liittyä verkkoon eikä liikennettä ole mahdollista jäljittää tiettyyn käyttäjään. Teoriassa tämä tarkoittaa siis sitä, että verkkoon on mahdollista liittyä rakennuksen ulkopuolelta, ja ulkopuolisten henkilöiden on mahdollista käyttää verkon resursseja. Oppilaitos kuitenkin sijaitsee alueella, jossa rakennuksen lähellä ei liiku muita kuin opiskelijoita ja oppilaitoksen henkilöstöä. Ei siis voida pitää todennäköisenä, että todennuksen puuttuminen olisi johtanut tällaisiin väärinkäytöksiin.

Käyttäjäkohtaisen todennuksen käyttöön suuren organisaation langattomassa verkossa on toinenkin syy. 802.11X-standardin mukainen todennus antaa, ainakin teoriassa, mahdollisuuden käyttäjäkohtai-

seen verkon käytön seurantaan. Jos tietty päätelaite käyttää kohtuuttoman määrän verkon resursseja, laitteen käyttäjä on mahdollista tunnistaa, koska käyttäjä on kirjautunut verkkoon omilla käyttäjätunnuksillaan. Lähtökohtaisesti verkkoresurssien kohtuuttoman käytön ei kuitenkaan pitäisi olla mahdollista, koska yksittäisen päätelaitteen käyttämiä resursseja voidaan rajata laadunvalvonta-asetuksilla. (engl. QoS, quality-of-service) Toisaalta voidaan olettaa, että verkon väärinkäyttö on paljon epätodennäköisempää, kun käyttäjä tietää tunnistautuneensa. Jos verkkoa käytettäisiin laittomaan toimintaan tai käyttöehtojen vastaisesti, vanhassa verkossa väärinkäytökseen syyllistynyttä käyttäjää ei olisi mahdollista jäljittää. Verkosta riippumatta liikenne voidaan jäljittää päätelaitteeseen. Päätelaitteen jäljittäminen käyttäjään ei ole edes teoreettisesti mahdollista, jos verkossa ei ole käytössä todennusta.

7.5 Verkon tarjoama käyttäjäkokemus - kehityskohteet

Oppilaitos on siirtymässä käyttämään kannettavia tietokoneita pöytäkoneiden sijaan tietyissä luokkahuoneissa. Uusi verkko on tästä syystä sekä opetustyökalu että palvelu opiskelijoille. Vaatimukset verkon kantamalle ovat myös lähestulkoon päinvastaiset aiempaan verkkoon verrattuna. Aiempi verkko suunniteltiin kattamaan yleiset tilat, kun taas uuden verkon on ensisijaisesti katettava luokkahuoneet.

Aiemman verkon langattomat tukiasemat tukivat 802.11g-standardia. Kuten luvussa 4 kuvattiin, tämän standardin teoreettinen tiedonsiirtonopeus on 54 megabittiä sekunnissa. Tätä uudistustyötä tehtäessä 802.11ac on laajasti käytössä, ja mahdollistaa yli kymmenkertaisen tiedonsiirtonopeuden. Kun otetaan huomioon, kuinka monta käyttäjää yksittäisellä tukiasemalla on, on selvää, miksi 802.11g on vanhentunut standardi tässä käyttökohteessa. Aiemman 80211g-standardin hyödyntämistä opetuskäytössä ei voida edes harkita. Yksittäinen tukiasema kahden opetustilan välissä saattaa palvella jopa 60 opetuskäytössä olevaa päätelaitetta. Lisäksi tukiasema palvelee yleisiä tiloja opetustilojen läheisyydessä.

Koska Centria-Ammattikorkeakoulun verkkoyhteyksistä vastaa kolmas osapuoli, verkon nopeutta tai signaalivoimakkuuden vaikutusta päätelaitteen kokemaan nopeuteen ei ole mahdollista arvioida luotettavasti. Kuten aiemmin todettu, on mahdollista, että langattoman verkon nopeutta oli rajoitettu keinotekoisesti ja taustaverkon resurssit oli kohdennettu toisaalle. Epävirallinen testaus osoittaa, että oppilaitoksen Ethernet-verkot olivat selvästi nopeampia. Internet-yhteyden nopeus luokissa opetuskäytössä

olevilla tietokoneilla oli erittäin hyvä. Tämä vahvistaa, että vanhan langattoman verkon nopeus selittyy ainakin osittain resurssien priorisoinnilla. Kun uusi langaton verkko otetaan käyttöön opetustyökaluna, on selvää, että sille varataan enemmän taustaverkon resursseja.

8 UUDEN VERKON SUUNNITTELU

Uuden verkon on ensisijaisesti katettava luokkahuoneet. Erityisesti toteutuksessa on huomioitava luokkatilat, joissa aiotaan käyttää kannettavia tietokoneita opetustyökaluina. Verkon kuuluvuuden näissä tiloissa on oltava moitteeton. Käytännössä tavoitteena on saada laadukas langaton verkko jokaiseen opetustilaan. Uudessa verkossa on 25 tukiasemaa aiemman kahdentoista sijaan.

Verkon käyttämät tukiasemat tukevat 802.11ac-standardia, sekä 2,4 ja 5 gigahertsin lähetystaajuuksia. Alkuvaiheessa verkko otetaan käyttöön 802.11n-standardin mukaisena, mutta tuki uudemmalle ac-standardille voidaan ottaa käyttöön ohjelmallisesti koska tahansa. Tämän työn tavoitteena oli uusia verkon fyysinen infrastruktuuri, eikä tietoja taustaverkosta tai tukiasemien asetuksiin johtaneista päätöksistä ole tämän työn puitteissa saatavilla.

Tukiasemat tukevat kappaleessa 5 kuvattua Power over Ethernet -tekniikkaa. Tukiasemien sijoittelu ei siis ole riippuvainen virtapistokkeista, ainoastaan Ethernet-liittimistä. Useimpien tukiasemien tapauksessa Ethernet-portteihin syötetään virtaa erillisillä PoE-syöttölaitteilla heti Ethernet-kytkimen jälkeen. Tiloissa, joissa tukiasemia tai muita PoE-laitteita on useita, on käytössä PoE-standardia tukevia Ethernet-kytkimiä.

Työn alkuvaiheessa tavoitteena oli taata verkon kuuluvuus koko rakennuksessa, kaikissa tiloissa. Tähän liittyen luotiin alustava suunnitelma tukiasemin sijoittelusta. Tässä vaiheessa toimeksianto ei kuitenkaan ollut tehnyt selväksi kannettavien tietokoneiden käyttöä opetuksessa. Kun tämä vaatimus tuli esille, verkkosuunnittelun painopiste muuttui. Vanhat tukiasemat korvattiin uusilla muuttamatta niiden paikkaa, ja kaksitoista uutta tukiasemaa asennettiin luokkahuoneisiin. Tukiasemien sijoittelu ei vaatinut varsinaista suunnittelua, vaan ne sijoitettiin luokkahuoneisiin niin tasaisin välimatkoin kuin mahdollista. Yksi uusi tukiasema asennettiin opettajien taukotilaan kattamaan kappaleessa seitsemän kuvattu heikko kuuluvuus opetushenkilökunnan tiloissa ensimmäisessä kerroksessa. Myös aulaan asennettiin toinen tukiasema kuormantasausta varten. Tavoitteena on myös asentaa yksi uusi tukiasema auditorioon, jos kaapelointi saadaan toteutettua järkevästi.

9 UUDEN VERKON TOTEUTUS

Uusi verkko koostuu uudesta virtuaalilähiverkosta WLAN-liikenteen kuljettamiseen Ethernet-taustaverkossa, tukiasemien hallintayksiköstä, sekä uusista 802.11ac-standardia tukevista tukiasemista. Taustaverkon tai hallintayksikön toteutuksesta ei ole saatavilla tietoja tämän työn puitteissa. Voidaan kuitenkin olettaa, että uusi verkko käyttää nopeampaa yhteyttä kampukselta julkiseen Internet-verkkoon. Kappaleessa 7.4. kuvattu verkon resurssien priorisointi QoS-tekniikoilla on lähes varmasti edelleen käytössä, mutta nyt opetuskäytössä olevalle verkolle on varattu enemmän resursseja. Virtuaalilähiverkko on edelleen eristetty oppilaitoksen muista lähiverkoista. Lähiverkkoresursseja, jotka ovat käytettävissä oppilaitoksen pöytäkoneilla, ei voi käyttää langattomassa verkossa.

9.1 Laitteisto

Verkon käyttämät tukiasemat ovat Hewlett-Packard Enterprise 525 -mallia. Malli tukee kaksikanavaista toimintatilaa, eli kappaleessa neljä kuvattu MIMO-toimintatila on käytettävissä. Tukiasemiin on mahdollista liittää kaksi ulkoista antennia sekä 2,4 gigahertsin, että 5 gigahertsin taajuusalueelle. Tämän työn tapauksessa ulkoisia antenneja ei kuitenkaan käytetty. Tukiasemien määrän ansiosta niiden sisäiset antennit riittävät kattamaan rakennuksen. Kuuluvuutta ongelmakohdissa on mahdollista parantaa tulevaisuudessa, jos se osoittautuu tarpeelliseksi.

Tukiasemien virrankulutus on korkeimmillaan alle 13 wattia, mikä tarkoittaa, että 802.3af-standardin mukainen virransyöttö Ethernet-kaapelia käyttäen on mahdollista. Vanhassa verkossa käytettiin yhtä lailla 802.2af-standardin mukaista Power over Ethernet-tekniikka virransyöttöön. Vanhojen tukiasemien korvaaminen uusilla toteutettiin vaihtamalla uusi tukiasema vanhan tilalle, ja ottamalla se käyttöön langattoman verkon hallintayksikössä. HPE™ 525-sarjan kanssa yhteensopivia hallintayksiköitä ovat esimerkiksi 850- ja 870-sarjan tuotteet. Tämän työn puitteissa ei ole tiedossa, mitä hallintayksikköä verkon ylläpitoon käytetään. Ei ole myöskään tiedossa, sijaitseeko hallintayksikkö Talonpojankadun kampuksella vai kolmannen osapuolen tiloissa.

Kuten luvussa 7 tuotiin esille, uudessa verkossa on noin kaksi kertaa enemmän tukiasemia kuin aiemmassa verkossa. Tukiasemien sijoittelu ei vaadi varsinaista suunnittelua, mutta verkkoliitäntöjen sijainti luokissa asettaa rajoituksia sijoittelulle. Tästä huolimatta uusi verkko kattaa onnistuneesti suunnitellut tilat.

9.2 Verkon kattavuus

Uusi langaton verkko kattaa koko rakennuksen siten, että vaimentuma 2,4 gigahertsin taajuusalueella ei käytännössä missään ole heikompi kuin -70 desibeliä. Luokkahuoneista vain yksi, B-siiven ensimmäisessä kerroksessa, saattaa tietyissä käyttötilanteissa kokea yli -70 desibelin vaimentumaa. Opetushenkilökunnan toimistot kyseisen luokkahuoneen läheisyydessä ovat samassa tilanteessa. Tämä voitaisiin tarvittaessa ratkaista asentamalla tukiasema luokkahuoneen etuosaan. Tätä ei työn toteuttamishetkellä kuitenkaan koettu tarpeelliseksi.

Toisessa kerroksessa verkon kattavuus on yllämainittua tavoitetasoa heikompi henkilökunnan toimistotiloissa B-siivessä. Samoin kuin ensimmäisessä kerroksessa, opetushenkilökunnan tilojen kattamista ei pidetä tarpeellisena. On myös huomattava, että edellä kuvattu tukiasema ensimmäisen kerroksen B-siivessä kattaisi oikein sijoitettuna myös tämän toimistotilan toisessa kerroksessa.

Pohjakerroksessa käytävä rakennuksen siipien välillä vaimentaa verkon signaalia huomattavasti, oletettavasti paksujen teräsbetoniseinien vuoksi. Kyseessä on kuitenkin vain käytävä, ei oleskelutila, joten tällä ei ole käytännön merkitystä. Tilassa ei myöskään ole Ethernet-portteja tukiaseman asentamiseen. Pohjakerroksen B-siivessä verkon kattavuutta ei mitattu muualla kuin aulassa, eikä B-siipeen asenneta tukiasemaa. Ensimmäiseen kerrokseen sijoitettu tukiasema kattaa aulatilan tyydyttävästi, mutta tämä on sattumaa, ei osa suunnitelmaa. Pohjakerroksen B-siipeen voitaisiin sijoittaa tukiasema, joka sijainti kattaisi tämän osan rakennusta riittävästi, mutta kampuksella suunnitellun rakennus- ja laajennustyön johdosta tähän tilaan ei ole tarkoituksenmukaista sijoittaa resursseja.

9.3 Tiedonsiirtonopeus uudessa verkossa

Verkon tiedonsiirtonopeus on huomattavasti vanhaa verkkoa korkeampi, mutta kuten edellä on todettu, tämä on yhtä paljon seurausta ohjelmallisista muutoksista taustaverkossa kuin uusista tukiasemista. Täsmällisiä tiedonsiirtonopeuksia vanhassa tai uudessa verkossa ei virallisesti kokeiltu, eikä kirjattu osana tätä työtä. Syynä tähän on epävirallisissa nopeuskokeiluissa havaitut tulokset. Vanhaa langotonta verkkoa käytettäessä tiedonsiirtonopeus oli selvästi 802.11g-standardille tavallisia nopeuksia alempi. Uudessa verkossa tulosten vaihteluväli oli erittäin suuri riippuen kokeilun ajankohdasta. Tulokset oppilaitoksen ollessa suljettuna ja suurimmaksi osaksi tyhjillään eivät vastanneet kaksikanavaisen 802.11n-standardin verkon tyypillistä tiedonsiirtonopeutta. Voidaan olettaa, että yksittäisen päätelaitteen käytettävissä olevaa tiedonsiirtokapasiteettia on rajoitettu palvelunlaatuasetuksilla. Verkossa käytettyjä asetuksia, tai sen teoreettista tiedonsiirtonopeutta ei ole mahdollista vahvistaa. Kuten työssä on jo tuotu esille, tietoja taustaverkosta ei ole tämän työn puitteissa saatavilla.

10 JOHTOPÄÄTÖKSET

Voidaan todeta, että Centria-Ammattikorkeakoulun käyttämä langaton lähiverkko oli riittävä tarkoitukseensa, kun se otettiin käyttöön. Käyttäjien määrä, päätelaitteiden tyyppi sekä odotukset verkon palvelutasosta ovat kuitenkin kasvaneet, ja rakennuksen vain osittain kattava, vanhaan tietonsiirtostandardiin perustuva verkko on nyt riittämätön. Kun otetaan huomioon, että verkon ensisijainen käyttötarkoitus on muuttumassa, on selvää, että päivitys oli tarpeellinen.

On selvää, että verkon suorituskykyyn vaikutti ainakin kaksi merkittävää tekijää. Toisaalta, langattomat tukiasemat tukivat vain standardia 802.11g. Standardin teoreettinen tiedonsiirtonopeus, 54 megabittiä sekunnissa, olisi periaatteessa riittävä lähes mihin tahansa käyttötarkoitukseen kampuksella, mutta käytännössä 802.11g-päätelaite saavuttaa murto-osan tästä tiedonsiirtonopeudesta. Voidaan kuitenkin perustellusti olettaa, että suurempi yksittäisen käyttäjän saavuttamaan tiedonsiirtonopeuteen vaikuttava tekijä on käyttäjien määrä. 54 megabitin tiedonsiirtonopeus jakautuu kaikkien tukiaseman käyttäjien kesken. Jos uusia tukiasemia käytetään yhteensopivuussyistä vain 802.11n-tilassa 20 megahertsin kanavaleveydellä, tiedonsiirtonopeus on teoriassa noin viisinkertainen vanhoihin tukiasemiin verrattuna.

Uuden verkon tukiasemien määrä vaikuttaa merkittävästi käyttäjien kokemaan tiedonsiirtonopeuteen. Kuten aiemmin todettu, suurimmassa osassa rakennusta päätelaite on useamman kuin yhden tukiaseman kuuluvuusalueella. Verkko pystyy hyödyntämään kuormantasausta, eikä yhden tukiaseman kapasiteetin pitäisi jakautua kohtuuttoman suurelle määrälle käyttäjiä. On kuitenkin huomattava, että verkossa toimivien päätelaitteiden määrä on huomattavasti suurempi, kun langatonta verkkoa käyttävät enenevässä määrin opetuskäytössä olevat tietokoneet ja henkilökunta.

Langattoman verkon taustalla toimivan Ethernet-verkon vaikutusta ei ollut mahdollista tutkia tämän työn puitteissa, mutta kuten aiemmin todettiin, vanha langaton verkko ei saavuttanut standardille 802.11g tyypillistä tiedonsiirtonopeutta edes tyhjässä rakennuksessa, jossa verkon testaamiseen käytetty päätelaite oli tukiaseman ainoa käyttäjä. On perusteltua olettaa, että langattoman verkon tiedonsiirtonopeutta rajoitti jokin tekijä taustaverkossa. Ei voida varmuudella sanoa, oliko kyse keinotekoisesta

rajoituksesta vai laitteistorajoituksesta. On kuitenkin selvää, että uuden verkon taustalla toimiva Ethernet-verkko on huomattavasti nopeampi.

Tarkkaa käsitystä uudistuksen vaikutuksesta käyttäjäkokemukseen ei ole mahdollista muodostaa käytettävissä olevien tietojen pohjalta. Tämän työn puitteissa ei ollut mahdollista tarkastella dataa langattoman verkon hallintayksiköltä vanhassa tai uudessa verkossa. Myöskään taustaverkon rakenteesta tai asetuksista ei ollut saatavilla tietoja. Voidaan kuitenkin spekuloida, että tämä tyyppiset tilastot eivät olisi vertailukelpoisia keskenään, vaikka niitä olisi saatavilla molemmista verkoista. Uudessa verkossa on lähes varmasti enemmän käyttäjiä ja päätelaitteita, kun opetuskäyttö ja henkilökunta siirtyvät käyttämään uuden langattoman verkon kapasiteettia.

LÄHTEET

Berg, J. The IEEE 802.11 Standardization It's History, Specifications, Implementations, and Future. Fairfax: George Mason University. Saatavissa: http://telecom.gmu.edu/sites/default/files/publications/Berg_802.11_GMU-TCOM-TR-8.pdf. Viitattu 13.7.2017.

CableFree 2017. The History of WiFi: 1971 to Today. Www-dokumentti. Saatavissa: http://www.cablefree.net/wireless-technology/history-of-wifi-technology. Viitattu 16.7.2018.

Cisco Systems. 2009. FAQ on Cisco Aironet Wireless Security. Www-dokumentti. Saatavissa: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/68583-FAQ-Wireless-Security.html. Viitattu 17.7.2017.

Cisco Systems. Enterprise Mobility Design Guide. Chapter 11. 802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/Chapter-11.pdf. Viitattu 16.7.2018.

Cisco Systems. Multi-SSID Deployment Considerations. Www-dokumentti. Saatavissa: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Multi-SSID_Deployment_Considerations. Viitattu 24.7.2018.

Coelho, R. 2009. Everything You Need to Know About The Centrino Platform. Sivu 3. Www-dokumentti. Saatavissa: https://www.hardwaresecrets.com/everything-you-need-to-know-about-the-centrino-platform-3. Viitattu 20.11.2018.

Deffree, S. 2013. Tesla gives 1st public demonstration of radio, March 1, 1893. Www-dokumentti. Saatavissa: https://www.edn.com/electronics-blogs/edn-moments/4460257/Marconi-sends-transatlantic-wireless-message--January-19--1903. Viitattu 7.11.2018.

Distributed.net. 2013. Project RC5. Www-dokumentti. Saatavissa: https://www.distributed.net/RC5. Viitattu 14.7.2017.

Dondurmacioglu, O. 2012. The Impact of Multiple SSIDs on Wi-Fi Performance. Www-dokumentti. Saatavissa: https://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/The-Impact-of-Multiple-SSIDs-on-Wi-Fi-Performance/ta-p/25374. Viitattu 23.11.2018.

Ducklin, P. 2015. We TOLD you not to use WPS on your Wi-Fi router! We TOLD you not to knit your own crypto! Www-dokumentti. Saatavissa: https://nakedsecurity.sophos.com/2015/04/13/we-told-you-not-to-use-wps-on-your-wi-fi-router-we-told-you-not-to-knit-your-own-crypto. Viitattu 23.7.2017.

Fleishman, G. 2006. Breaking News: 802.11n Draft 1.0 Approved. Www-dokumentti. Saatavissa: http://wifinetnews.com/archives/2006/03/breaking_news_80211n_draft_10_approved.html. Viitattu 10.7.2017.

Fluhrer, S., Mantin, I. & Shamir, A. Weaknesses in the Key Scheduling Algorithm of RC4. PDF-dokumentti. Saatavissa: http://www.mattblaze.org/papers/others/rc4_ksaproc.pdf. Viitattu 12.7.2017.

GÉANT. 2018. What is eduroam? Www-dokumentti. Saatavissa: https://www.eduroam.org/what-is-eduroam. Viitattu 20.11.2018.

Huotari, A. 2015. What is 802.11r? Why is it important? Www-dokumentti. Saatavissa: https://blogs.cisco.com/wireless/what-is-802-11r-why-is-this-important. Viitattu 16.7.2018.

IEEE 802.11-1997. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. 1997. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: https://ieeexplore.ieee.org/servlet/opac?punumber=5258. Viitattu 3.12.2018.

IEEE 802.11Q-1998. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks. 1998. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: https://standards.ieee.org/getieee802/download/802.1Q-1998.pdf. Viitattu 24.7.2018.

IEEE Std 802.1X-2001. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control. 2001. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: https://ieeexplore.ieee.org/servlet/opac?punumber=7449. Viitattu 4.12.2018.

IEEE Std 802.11at-2003. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI). 2003. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: http://standards.ieee.org/getieee802/download/802.11at-2003.pdf. Viitattu 15.8.2018.

IEEE Std 802.11at-2009. Standard for Information Technology - Telecommunications and Information Exchange Between Systems – LAN/MAN - Specific Requirements Part 3: CSMA/CD Access Method and Physical Layer Specifications - Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T. 2006. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: http://standards.ieee.org/getieee802/download/802.11an-2006.pdf. Viitattu 15.8.2018.

IEEE Std 802.3at-2009. IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements. 2009. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: http://standards.ieee.org/getieee802/download/802.11at-2009.pdf. Viitattu 15.8.2018.

IEEE Std 802.11n-2009. IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physi-

cal Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. 2009. New York: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: https://ieeexplore.ieee.org/servlet/opac?punumber=5307291.

IEEE 802.11ac-2013. IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 Ghz. 2013. []: Institute of Electrical and Electronics Engineers IEEE. Saatavissa: https://ieeexplore.ieee.org/servlet/opac?punumber=7797533. Viitattu 10.7.2017.

IEEE. Official IEEE Working Group project timelines. Www-dokumentti. Saatavissa: http://www.ieee802.org/11/Reports/802.11_Timelines.htm. Viitattu 6.7.2017.

ISI/IEC 11801. Information technology – Generic cabling for customer premises. 2002. Geneve: ISO/IEC Copyright Office. Saatavissa: https://webstore.iec.ch/preview/info_isoiec11801%7Bed2.0%7Den.pdf. Viitattu 18.8.2018.

RFC 768. User Datagram Protocol. 1989. Internet Engineering Task Force IETF. Saatavissa: https://www.rfc-editor.org/rfc/rfc768.txt. Viitattu 20.8.2018.

Nokia Oyj. 2005. Nokia 9300i -käyttöohje. Www-dokumentti. Saatavissa: http://nds1.webapps.microsoft.com/phones/files/guides/Nokia_9300i_UG_fi.pdf. Viitattu 20.11.2018.

Slavin, W. 2014. 7270 First BlackBerry To Support Wi-Fi. Www-dokumentti. Saatavissa: http://www.netstumbler.com/2004/10/18/7270-first-blackberry-to-support-wi-fi. Viitattu 20.11.2018.

Stubblefield, A., Ioannidis, J. & Rubin, A. D. 2001. AT&T Labs Technical Report TD-4ZCPZZ: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Florham Park:AT&T Labs. PDF-dokumentti. Saatavissa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.8027&rep=rep1&type=pdf. Viitattu 12.7.2017.

TIA/EIA-568-B.2. Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components. 2001. Arlington: Telecommunications Industrial Association TIA. Saatavissa: https://www.csd.uoc.gr/~hy435/material/TIA-EIA-568-B.2.pdf. Viitattu 18.8.2018.

United States Department of Commerce, Technology Administration, National Institute of Standards and Technology. 1997. NIST Construction Automation Program Report No. 3. Electromagnetic Signal Attenuation in Construction Materials. Saatavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6055.pdf. Viitattu 25.7.2018.

Van Beijnum, I. & Barcelo, J. 2011. Cutting the cord: how the world's engineers built Wi-Fi. Saatavissa: http://arstechnica.com/gadgets/2011/10/cutting-the-cord-how-the-worlds-engineers-built-wi-fi. Viitattu 13.7.2017.

Wilson, R. 2002. Propagation Losses Through Common Building Materials. University of Southern California. Saatavissa: https://www.am1.us/wp-content/uploads/Documents/E10589_Propagation_Losses_2_and_5GHz.pdf. Viitattu 24.7.2018.