Timi Jalava

Langaton lähiverkko vanhaan kiinteistöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

5.5.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Timi Jalava Langaton lähiverkko vanhaan kiinteistöön 38 sivua + 4 liitettä 5.5.2017
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ohjaaja	Yliopettaja Matti Puska

Insinöörityössä suunniteltiin ja toteutettiin monikerroksiseen tiili- ja betonirakenteiseen kiinteistöön edullinen, luotettava ja kuormitusta kestävä tietoturvallinen keskitetysti hallittu langaton lähiverkko.

Verkko toteutettiin kattavasti koko kiinteistön alueelle, ja se palvelee testatusti yli 200:aa samanaikaista päätelaitetta. On perustellusti oletettavissa, että verkko kestää myös määrittelyissä esiin tulleen 400 päätelaitteen samanaikaisen käytön. Työssä toteutettiin lisäksi päärakennuksen ja sivurakennuksen välinen siltalinkki, jolla sivurakennus kyettiin liittämään päärakennuksen lähiverkkoon.

Työssä käsiteltiin myös yritystasoisen langattoman verkon pohjakseen vaatimaa verkkoinfrastruktuuria. Työssä suunnitellut ja toteutetut langattomat lähiverkot testattiin tarkoituksenmukaisilla tavoilla, ottaen huomioon organisaation tarpeet.

Työn toteutusvaiheen jälkeen käyttäjiltä pyydetyn palautteen ja suoritettujen testien perusteella uusi langaton verkko täyttää kaikki ennakko-odotukset.

Avainsanat	langattomat lähiverkot, WLAN, kapasiteetti

Author Title Number of Pages Date	Timi Jalava Wireless local area network in an old building 38 pages + 4 appendices 5 May 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Instructor	Matti Puska, Principal Lecturer

The objective of this thesis was to design and implement a wireless local area network in a multi-storey building made of brick and concrete. The network should be affordable, reliable and able to withstand a high load of clients. It should also be centrally managed and secure.

The network was built to cover the whole building, and it has been proven to serve more than 200 simultaneous clients. It is expected to withstand 400 simultaneous clients as demanded in the requirement specifications. Between the main building and a side building there was also built a wireless bridge. The bridge connected the side building to the main building network.

The thesis also covers the fixed network infrastructure, which is demanded by the implemented enterprise scale wireless network. The accomplished network was tested using appropriate methods, considering the needs of the organization.

Finally, the users were asked for feedback relating to the new network. The tests and the feedback show that the network meets user expectations with great satisfaction.

Keywords	Wireless local area networks, WLAN, capacity

Sisällys

Lyhenteet ja käsitteet

MIMO	Multiple-Input Multiple-Output. Nopeutta lisäävä moniantennitekniikka.
SISO	Single-Input Single-Output. Perinteinen yksiantennitekniikka.
Wi-Fi	Wireless Fidelity. Hyväksyntä, jonka saa testatusti 802.11-standardien mukaan toimiva WLAN-laite. Usein Wi-Fillä ja WLANilla tarkoitetaan samaa.
LAN	Local Area Network. Paikallinen fyysiseen kaapelointiin perustuva lähiverkko.
WLAN	Wireless Local Area Network. Langaton paikallinen lähiverkko.
VLAN	Virtual Local Area Network. Virtuaalilähiverkko. LAN-verkon sisällä oleva loogisesti eriytetty vituaalinen LAN-verkko.
WPA	Wi-Fi Protected Access. WLAN-verkoissa käytettävä turvallisuusprotokolla.
AES	Advanced Encryption Standard. Kehittynyt erittäin turvallisena pidetty salausstandardi.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan standardisointijärjestö.
PoE	Power over Ethernet. Sähkönsyöttötekniikka, jolla saadaan cat-verkkokaapelissa kuljetettua datan lisäksi sähkö verkkolaitteelle.
EAP	Extensible Authentication Protocol. Tunnistustoteutuksien kuljetusalusta 802.x-verkoissa.
SSID	Service Set Identifier. Langattoman lähiverkon näkyvä nimi.
LACP	Link Aggregation Control Protocol. Protokolla, joka sitoo yhteen useita fyysisiä Ethernet-portteja tehden niistä yhden nopean virtuaalisen portin.

DHCP	Dynamic Host Configuration Protocol. Palvelu, jolla jaetaan IP-osoitteita verkon laitteille.
SDN	Software-Defined Networking. Keskitetty ohjelmistopohjainen verkon ohjaus, ohjelmisto tekee laitteiden konfiguraatiomuutokset.
Hyper-V	Microsoftin kehittämä hypervisor. Alusta, joka huolehtii virtuaalisen käyttöjärjestelmän ja fyysisen laitteiston välisestä kommunikaatiosta.
DSSS	Direct-Sequence Spread Spectrum. Suorasekvenssihajaspektri.
FHSS	Frequency-Hopping Spread Spectrum. Taajuushyppelyhajaspektri.
Cat 6	Kategorian 6 kuparinen verkkokaapeli, joka käyttää usein RJ-45-liittimiä.
IP	Internet Protocol. Internetissä ja verkoissa liikennöintiin käytettävä protokolla.
ISM	Industry, Scientific, Medical. Lisenssivapaa maailmanlaajuinen taajuusalue. Suomessa 2,4 ja 5,7 GHz:n alueet WLAN-käytössä.
PoE	Power over Ethernet. Standardoitu menetelmä pienien verkkolaitteiden sähkönsyöttöön dataliikenteen kanssa jaetulla Cat-kaapelilla.
CIA	Confidentiality, Integrity, and Availability. Luottamuksellisuus, eheys ja saatavuus. Malli tietoturvallisuuden perusteista.
AD	Microsoft Active Directory. Aktiivihakemisto, jolla toteutetaan muun muassa käyttäjähallinta.
SMB	Server Message Block. Yleinen hajautetun levyjärjestelmän yhteyksiin käytetty protokolla, esimerkiksi Windowsin tiedostojako.

1 Johdanto

Insinöörityön tarkoituksena on keskisuuren eli yli 20 tukiasemaa sisältävän langattoman lähiverkon suunnitteleminen, toteuttaminen ja testaaminen erään pääkaupunkiseudulla sijaitsevan kirkon tiloihin. Hallitulla verkolla tarkoitetaan sitä, että jokaista verkkoelementtiä ei tarvitse konfiguroida ja ylläpitää erikseen, vaan kaikki ylläpitotoimet voidaan suorittaa yhdestä pisteestä.

Työn kohteena on viisikerroksinen vanha kiinteistö, joka on rakennettu betonista ja tiilestä, mikä tuo suunnitteluun ja toteutukseen omat haasteensa. Kapasiteetti- ja suorituskykyvaatimuksien toteuttamiseksi tukiasemia pitää olla paljon. Rakennuksen kivirakenteet tuottavat hankaluuksia tiloissa, joihin pitää sijoittaa useampia tukiasemia. Työmäärää lisäävät myös osittain väärissä paikoissa olevat yleiskaapeloinnin rasiat.

Työn tavoite on suunnitella ja toteuttaa uusi verkko hyvin kattavasti niin, että suorituskyky on erinomainen oleellisissa tiloissa kuormituksen allakin ja että kaikissa tiloissa on pääsy verkkoon. Lisäksi huomattavasti pienempi yksitasoinen sivurakennus aiotaan liittää samaan verkkoon käyttäen langatonta siltaa, koska myös sivurakennukseen halutaan toteuttaa langaton lähiverkko. Ennen työn aloittamista pitää purkaa vanha hidas ja kattamaton yksittäisistä langattomista reitittimistä rakennettu verkko.

Työn etenemisen aikana selvitetään paljon suunnittelun pohjana käytettävää teoriatietoa ja tehdään erilaisia kartoituksia. Organisaation verkkoihin ja palvelimiin tehdään työn ohessa muitakin muutoksia, kuin työssä käsitellään, mutta niiden käsittely on rajattu pois, sillä ne eivät liity insinöörityön aiheeseen. Pois rajataan syvällisempi langattomien verkkojen taustalla olevan teorian käsittely, koska se ei toisi merkittävää lisähyötyä työn suorittamiseen. Myöskään vanhan langattoman verkon käytöstä poistamista ei käsitellä, koska sillä ei nähdä olevan merkitystä insinöörityön kannalta.

2 Langattomien lähiverkkojen kehitys

2.1 802.11-standardi ja langattomuuden historiaa

Langattomat lähiverkot ovat tietotekniikan historiassa vanha keksintö. Motorola esitteli ensimmäisen WLAN (Wireless Local Area Network) -tuotteen, Altairin, jo 1980-luvun puolivälissä. Altair oli, samoin kuin muut aikansa ratkaisut, sidottu saman valmistajan tuotteisiin, eikä mainittavaa yhteensopivuutta muiden valmistajien laitteisiin ollut. Myös suorituskyky oli heikkoa: aluksi saavutettiin vain 3 Mbit/s teoreettinen nopeus. Heikkoutena oli myös 18 gigahertsin taajuuden huono esteidenläpäisykyky. Lisäksi yksi Altair-tukiasema maksoi yli 5 000 dollaria ja vastaanotin 1 000 dollaria. [1; 2.]

IEEE (Institute of Electrical and Electronics Engineers) alkoi kehittää langattoman verkon standardeja vuonna 1990 ja sai valmiiksi ensimmäisen 802.11-standardin vuonna 1997. Vuonna 1999 julkaistiin aluksi huomattavasti nopeampi 802.11b-standardi, joka kykeni 11 Mbit/s teoreettiseen nopeuteen 2,4 GHz:n taajuudella, ja myöhemmin samana vuonna 802.11a, joka kykeni 54 Mbit/s teoreettiseen nopeuteen 5 GHz:n taajuudella. Vuonna 2003 otettiin käyttöön laajasti tunnettu 802.11g, jonka nopeus on sama kuin a-standardilla mutta taajuus on 2,4 GHz. Yhtenäiset standardit ovat mahdollistaneet laitevalmistajista riippumattoman yleisen yhteensopivuuden eri laitteiden välillä. [1.]

2.2 Nykypäivän standardit 802.11n ja 802.11ac

Nykypäivän yleisimmin käytössä oleva standardi 802.11n on julkaistu vuonna 2009, joskin jo ennen varsinaista julkaisua markkinoilla oli usealta valmistajalta standardin luonnoksiin perustuvia laitteita. Standardi mahdollistaa 600 Mbit/s -siirtonopeuden. [3; 4.]

Käytännössä n-standardin verkoissa päästään yli 100 Mbit/s todellisiin siirtonopeuksiin. Jopa yli 300 Mbit/s voidaan päästä, mikäli olosuhteet ovat optimaaliset ja käytössä on suurimman nopeuden mahdollistavat laitteet. Kuormitetulta n-verkolta voi useimmiten odottaa muutaman kymmenen megabitin tiedonsiirtonopeuksia, koska laitteissa ei ole montaa antennia ja kaista jakautuu kaikkien käyttäjien kesken. [5.]

802.11ac-standardi on julkaistu vuonna 2013. Standardin mukaisia laitteita ei ole markkinoilla vielä paljoa, mutta yleensä uusissa kannettavissa tietokoneissa on AC-standardiin yhteensopiva WLAN-radio, kuten myös paremmissa matkapuhelimissa ja tablettitietokoneissa. Standardin mukaiset ensimmäiset Wave 1 -laitteet ovat kyenneet enimmillään 1,3 Gbit/s -tiedonsiirtonopeuteen, mutta uudemmat 802.11ac Wave 2 -mukaiset laitteet kykenevät jopa 2,34 Gbit/s -nopeuteen. [5; 6.]

Wave 2 -sarjan radiot tuovat saavutettaviin nopeuksiin selvän parannuksen, sillä monesti optimiolosuhteiden käytännön maksiminopeuden suuruus on puolet teoreettisesta maksiminopeudesta. Näin ollen uusilla laitteilla voidaan päästä jo yli 1 Gbit/s toteutuvaan nopeuteen. [5.]

Kuvassa 1 on luetteloitu 802.11n- ja 802.11ac-tekniikoiden ominaisuuksia ja eroavaisuuksia. Huomionarvoista on muun muassa AC-standardin mukana kasvanut hyötysuhde (bps/Hz) ja suurten nopeuslisäysten seurauksena heikentynyt kantama. Nopeampi yhteys vaatii monimutkaisemman modulaation takia häiriöttömämpää radiotietä.

Technical Specification	802.11n	802.11ac
Frequency	2.4, 4.9, 5 GHz	5 GHz
Modulation Scheme	OFDM	OFDM
Channel Bandwidth	20, 40 MHz	20, 40, 80 MHz (160 MHz optional)
Nominal Data Rate, Single Stream	Up to 150 Mbps (1x1, 40 MHz)	Up to 433 Mbps (1x1, 80 MHz) Up to 867 Mbps (1x1, 160 MHz)
Aggregate Nominal Data Rate, Multiple Streams	Up to 600 Mbps (4x4, 40 MHz)	Up to 1.73 Gbps (4x4, 80 MHz) Up to 3.47 Gbps (4x4, 160 MHz)
Time to Stream 1.5hr HD	~ 30 min (4x4, 40 MHz)	~ 15 min (4x4, 80 MHz)
Spectral Efficiency	15 bps/Hz (4x4, 40 MHz)	21.665 bps/Hz (4x4, 80 MHz)
EIRP	22-36 dBm	22-29 dBm
Range	12-70 m indoor	12-35 m indoor
Through Walls	Y	Y
Non-Line-of-Sight	Y	Y
World-Wide Availability	Y	Y limited in China

Kuva 1. 802.11n- ja 802.11ac Wave 1 -standardien keskeiset ominaisuudet [6].

Täydelliseen 802.11ac-standardin mukaiseen verkkoon ei päästä vielä vuosiin, sillä hiljattain julkistettu Wave 2 -kehitysversio yltää enimmillään 3,47 Gbit/s teoreettiseen nopeuteen, siinä missä täysi standardi mahdollistaisi 6,9 Gbit/s -nopeuden. [5.]

2.3 Hajaspektritekniikka

Hajaspektritekniikassa radiolle lähetettävä viesti koodataan tietyillä parametreilla, jotka ovat vain tarkoitetun vastaanottajan tiedossa. Alun perin hajaspektritekniikka kehitettiin sotilaskäyttöön parantamaan turvallisuutta, minkä vuoksi laajakaistainen hajaspektrilähetys näyttää ulkopuoliselle pelkältä taustakohinalta. Hajaspektrinen signaali on huomattavasti vähemmän altis häiriöille kuin kapeaspektrinen signaali, koska tietyllä pienellä taajuusalueella oleva häiriö ei vaikuta muihin lähetyksen käyttämiin taajuuksiin. Hajaspektrinen lähetys käyttää hyvin laajaa taajuusaluetta. Tämä mahdollistaa nopean tiedonsiirron, ikään kuin useaa kanavaa pitkin samanaikaisesti. Nykypäivänä kaikki nopeat langattomat teknologiat käyttävät hajaspektritekniikkaa. Hajaspektritekniikka mahdollistaa myös lisenssivapaan käytön pienillä lähetystehoilla, koska interferenssin sieto on hyvä. [17.]

Useat nykyiset hajaspektritekniikkaa käyttävän verkot toimivat ISM-taajuuskaistoilla (Industry, Scientific, Medical), jotka on varattu teollisuuden, tieteen ja lääketieteen käyttöön vuonna 1975. Langattomissa verkoissa yleisesti käytettävät kaistat sijaitsevat 902 MHz:n, 2,4 GHz:n ja 5,7 GHz:n taajuusalueilla, ja kahta viimeistä käytetään Suomessa WLAN-verkoille. Kaikkien ISM-kaistalla toimivien radiojärjestelmien on käytettävä hajaspektritekniikkaa ja alle 1 W:n lähetystehoa. Valtiot voivat itse määritellä pienempiä lähetystehorajoja. [17.]

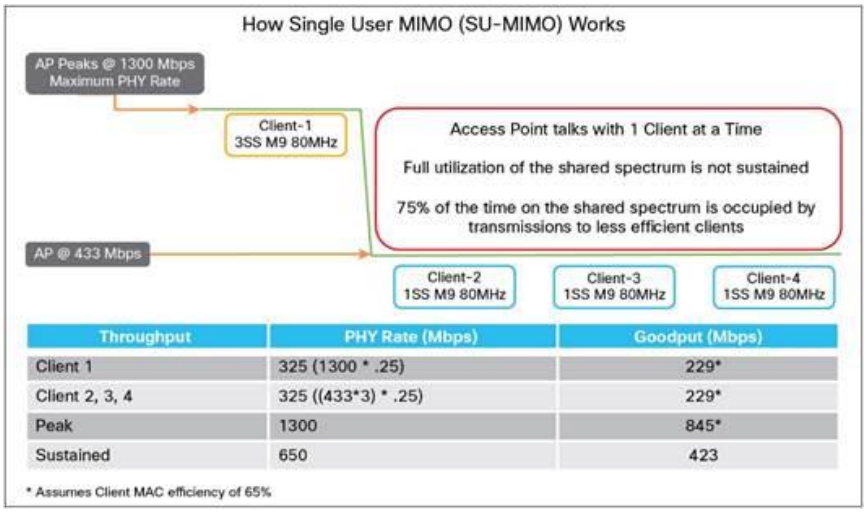
DSSS (Direct-Sequence Spread Spectrum) eli suorasekvenssihajaspektri moduloi signaalia digitaalisella koodilla, jonka bittinopeus on huomattavasti suurempi kuin alkuperäisen informaatiosignaalin. Esimerkiksi, jos informaatiosignaalissa on kolme bittiä, saatetaan radiosta lähettää 36 bittiä. Näin virheitä pystytään korjaamaan paremmin, koska häiriöillekin altistuneesta bittijonosta pystytään paremmin päättelemään, mikä alkuperäinen bitti on ollut. [17.]

2.4 Moniantennitekniikan kehittyminen

MIMO (Multiple-Input Multiple-Output) eli moniantennitekniikka on avain tiedonsiirtonopeuksien kasvattamiseen. Ensimmäisissä 802.11-standardin laitteissa ei ollut kuin yksi lähettävä ja yksi vastaanottava antenni (SISO, Single-Input Single-Output). MIMO on olennainen osa uudempia n- ja ac-standardeja.

MIMO jakaa datavirran useaksi itsenäiseksi virraksi (stream), joista jokainen moduloidaan ja lähetetään eri radioantennien läpi samanaikaisesti samalla taajuuskanavalla. MIMO hyödyntää ympäristön esteiden heijastuksia, ja jokaisen antennin virta kulkee eri reittiä vastaanottavalle antennille. Perinteisesti on totuttu ajattelemaan, että erilaiset esteet ympäristössä heikentävät signaalin kulkua ja että avara tila on paras signaalin välitykseen, mutta MIMO hyötyy heijastuksista ja ympäristössä olevista esteistä. Vastaanottopäässä usean antennin signaali tulee radiolle samaan aikaan, ja eri reittejä tulleet virrat erotellaan vastaanottimessa erityisillä algoritmeilla. Jokaista etenemisreittiä ja antennia voi näin ajatella omana johtimenaan, jota pitkin tieto siirtyy riippumatta toisista virroista. [7.]

Perinteinen MIMO on nykyään nimetty SU-MIMOksi (Single-User MIMO), mikä kuvastaa hyvin sen toimintaa. Se on tehokkaimmillaan, kun yksi tukiasemaradio keskustelee yhden päätelaitteen kanssa. Jos samaan tukiasemaan kuitenkin liittyy kolme uutta laitetta, saa yksi laite vain 25 % tukiaseman lähetysajasta käyttöönsä. Jos yksi laite, esimerkiksi kannettava tietokone, tukee 3 x 3 MIMOa ja kolme muuta laitetta käyttää vain yhtä antennia, saa tietokone käyttöönsä 25 % maksimikapasiteetista. Tällöin toinen 25 % jaetaan kolmen heikomman laitteen kesken. Jos tilannetta tarkastellaan tukiasemasta käsin, hukataan sekunnin sisällä 50 % käytettävissä olevasta kapasiteetista. Jos kaikki neljä päätelaitetta tukisivat 3 x 3 MIMOa, ei kapasiteettia hukattaisi ollenkaan. Tämä on kuitenkin harvinaista; yleisempää on eri tasoisten laitteiden verkossa olo samaan aikaan. [5.] Kuvassa 2 on havainnollistettu SU-MIMOn toimintaa ja saavutettavia nopeuksia. Siitä voi lisäksi nähdä, miten tukiaseman kapasiteettia menee hukkaan.

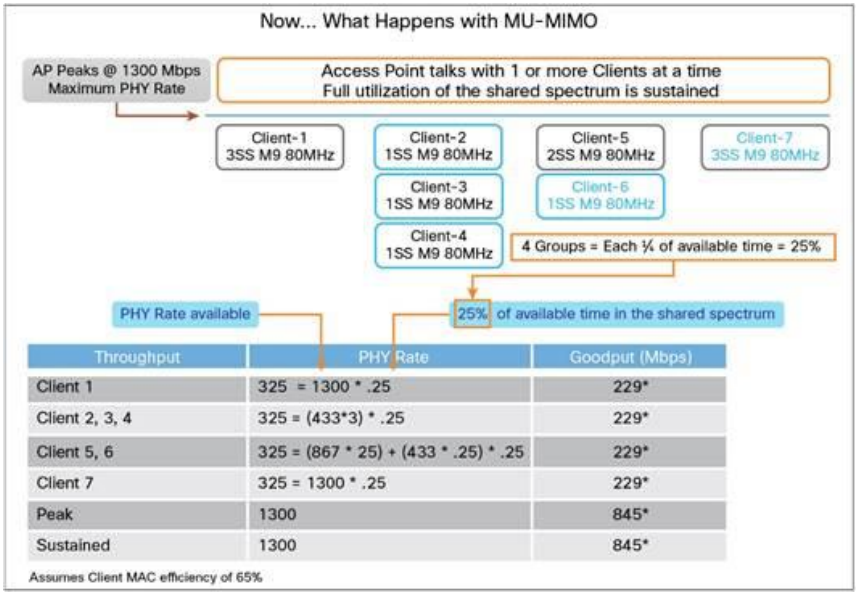


Kuva 2. Kuvassa on havainnollistettu, miksi suorituskykyä menee hukkaan. 1SS tarkoittaa yhden streamin eli antennin lähetystä, 3SS tarkoittaa 3 x 3 MIMOa. [5.]

MU-MIMO (Multi-User MIMO) hyödyntää lähetysajan huomattavasti tehokkaammin kuin SU-MIMO, koska se voi lähettää samaan aikaan monelle yhden antennin vastaanottimelle. Esimerkiksi ajan hetkellä 1 lähetetään kolmen antennin laitteelle. Ajan hetkellä 2 lähetetään kolmelle yhden antennin laitteelle samanaikaisesti. Ajan hetkellä 3 lähetetään kahdelle laitteelle, joista toisella on yksi ja toisella kaksi antennia. On selvää, että MU-MIMOn suorituskyky on oleellisesti parempi kuin SU-MIMOn, mikäli samaan tukiasemaradioon on yhteydessä samanaikaisesti monta eritasoista laitetta. [5.]

MU-MIMO on tullut käyttöön vasta 802.11ac Wave 2 -laitteissa, eikä se ole taaksepäin yhteensopiva. Toisin sanoen menee vielä paljon aikaa, ennen kuin WLAN-verkoissa aletaan saada oikeaa hyötyä tästä tekniikasta. Kun kaikki käytössä olevat laitteet tukevat sitä, saadaan ruuhkaisten sijaintien verkkoon runsaasti lisää kapasiteettia. Siinä missä nykyiset SU-MIMOa tukevat radiot voivat palvella yhtä laitetta kerrallaan, pystyy MU-MIMOa tukeva radio palvelemaan enintään neljää radiota samaan aikaan. [5.]

Oletetaan tukiasemassa olevan kahdeksan antennia. Tällöin MU-MIMO kykenee palvelemaan neljää 2 x 2 -antennista päätelaitetta samaan aikaan. Kuvassa 3 on tarkasteltu kuvan 2 tilannetta, mutta käytössä on MU-MIMO. Kuvia vertailemalla voi havaita seuraavan: koska MU-MIMO tehostaa ajankäyttöä, sitä käyttävä tukiasema kykenee palvelemaan suurempia käyttäjämääriä kuin SU-MIMO. [5.]



Kuva 3. MU-MIMOn toiminta käytännössä. Lähetyskapasiteettia ei mene hukkaan ideaalitilanteessa ollenkaan. [5.]

2.5 Tukiasemien suorituskyvyn kehittyminen

WLAN-tukiasemat ovat kehittyneet muutenkin kuin yksittäisen radion nopeuksien osalta. Tällä on suuri vaikutus, mutta vähintään yhtä paljon vaikuttavat tukiaseman sisällä olevien radioiden määrä ja taajuudet. Suurin osa nykyisistä tukiasemista on niin sanottuja dual-band-laitteita, eli niissä on kahden eri taajuuden radiot. Radioiden määrä on lähes suoraan verrannollinen siihen käyttäjämäärään, jota tukiasema pystyy laadukkaasti palvelemaan. [8; 9.]

Esimerkkinä voidaan käyttää neljän radion tukiasemaa. Yksi radioista toimii 2,4 GHz:n taajuudella, kolme muuta toimivat 5 GHz:n taajuudella. Näin tukiasema kykenee palvelemaan vanhempia laitteita matalammalla taajuudella, mutta uudemmat korkeampaa taajuutta tukevat laitteet saavat runsaasti kapasiteettia. Kun oletetaan, että tukiasema käyttää 802.11n-standardia, voidaan laskea tukiaseman syöttökaapelin riittävyys. Jos 2 x 2 -antenninen MIMO-radio pystyy siirtämään 300 Mbit/s teoreettisella nopeudella 195 Mbit/s, neljä radiota generoi liikennettä verkkoon enimmillään 780 Mbit/s (oletetaan toteutuvan nopeuden olevan 65 % teoreettisesta). Tästä huomataan, että yksi tukiasema voi suurelta osin hyödyntää kytkimeltä tulevan 1 Gbit/s -yhteyden. Tällöin tulee palvelluksi paljon suurempi joukko käyttäjiä kuin vain yhdellä radiolla. [5; 8; 9.]

Edullisempienkin tukiasemien ominaisuuslistoihin on viime vuosina tullut paljon suorituskykyä parantavia lisäyksiä. Yhtenä esimerkkinä on band steering, jolla kyetään ohjaamaan päätelaitteita halutulle radiotaajuudelle. Tästä on hyötyä sellaisissa tilanteissa, joissa molempia taajuuksia tukeva laite haluaisi kytkeytyä 2,4 GHz:n taajuudella. Tukiasema voi kieltäytyä keskustelemasta 2,4 GHz:n taajuudella ja tällöin päätelaite yhdistää 5 GHz:n taajuudella. Hyötyjä ovat muun muassa korkeamman taajuuden pienempi häiriöisyys, suurempi suorituskyky sekä kuormantasaus eri radioiden välillä. [9.]

Uusi suorituskykyyn vaikuttava merkittävä tekniikka on beamforming. Se tarkoittaa signaaliprosessointia, jossa muutetaan antennille vahvistimelta kulkevan signaalin vaihekulmaa. Tällöin antenni muodostaa erilaisen kuvion kuin ilman vaiheen muutosta. Tämä auttaa suuntaamaan signaalia paremmin päätelaitteen suuntaan. [9.]

2.6 Tukiasemien sähkönsyötön kehittyminen

Perinteisesti yksittäisen tai muutaman tukiaseman sähköistämiseen ei ole käytetty erikoisia panoksia, vaan niiden läheisyyteen on viety tavallinen laitteeseen sopiva virtalähde. Tämä on edelleen järkevä tapa syöttää sähköä yhdelle tai kahdelle tukiasemalle, mutta suurempiin verkkoihin on syytä ottaa käyttöön Power over Ethernet (PoE).

PoE kykenee siirtämään sähköä samassa verkkokaapelissa datan kanssa. Se toimii ratkaisusta riippuen joko 100 Mbit/s -yhteyksissä käyttämättä jäävillä kahdella johdinparilla tai 1 Gbit/s -yhteyksillä offset-jännitteenä dataliikenteen alla. PoE tuottaa nimellisesti 48 voltin tasajännitettä, joskin jännite on usein lähtöpäässä suunnilleen 55 volttia. Myös passiivisia PoE-ratkaisuja on paljon, ja niissä erotetaan virransyötön käyttöön kaksi paria cat-kaapelin neljästä parista. Jännite riippuu täysin käytettävistä laitteista, ja tyypillisimmin se on 12, 24 tai 48 volttia. Passiivinen ratkaisu pystyy välittämään yleensä vain 100 Mbit/s -yhteyden, koska nopeampiin vaaditaan kaikki kaapelin neljä paria. [10.]

Yritysympäristöissä on vielä tällä hetkellä laajimmin käytössä vanha PoE-standardi 802.3af. Vuoden 2003 standardi määrittelee laitteen käytettävissä olevaksi tehoksi 13 wattia (W). Tämä teho riittää hyvin kaikille aikaisemmille laitteille, kuten 802.11n-tukiasemille ja valvontakameroille. Uusille 802.11ac-tukiasemille 13 W ei riitä kuormituksessa, etenkään jos tukiasemassa on useampia radioita. [9; 10.]

Tämänhetkinen standardi 802.3at tuottaa laitteelle jopa 25,5 W:n tehon, joten se pystyy syöttämään kaikki uusimmatkin tukiasemat. Tämä vuoden 2009 standardi tunnetaan myös nimellä PoE Plus. IEEE suunnittelee parhaillaan uutta standardia 802.3bt, joka käyttäisi kaikkia neljää johdinparia ja mahdollistaisi jopa 100 W:n tehonsiirron datan ohella. [10.]

2.7 Tietoturvallisuuden kehittyminen

Tietoturvallisuus on kriittinen osa langattomuutta. Nykyisillä tekniikoilla toteutetun WLAN-verkon perusominaisuuksiin kuuluu ehdottomasti yhteyden salaus. Kotikäyttäjäkään ei saa enää kaupasta tukiasemaa tai reititintä, jossa ei olisi esimääriteltyä salausta käytössä. Täysin avoimia verkkoja näkee enää lähinnä yritysten vierailijaverkkoina ja julkisten tilojen, kuten lentokenttien, kävijöilleen tarjoamina verkkoina.

WLAN-verkkojen tiedonsiirron tietoturva koostuu kahdesta osatekijästä: käyttäjän tunnistamisesta (autentikointi) ja salauksesta. Tunnistamisen tehtävä on varmistaa, että verkkoon yrittävä päätelaite on auktorisoitu yhdistämään. Esimerkkeinä käyvät tunnistamiseen käytettävä yleinen esijaettu avain (salasana) tai henkilökohtainen käyttäjätunnus ja salasana, joilla kirjaudutaan verkkoon tunnistuspalvelinta käyttäen. Tunnistuspalvelin toteutetaan usein käyttämällä RADIUSta (Remote Authentication Dial-In User Service). Vanhentuneita ja turvattomaksi käyneitäkin protokollia on mahdollista käyttää, mutta se ei ole suositeltavaa eikä turvallista. Huomioon tulee ottaa myös tukiasemien fyysinen turvallisuus, turvalliset hallintasalasanat ja laitteiden ohjelmiston pitäminen ajan tasalla. [1.]

Evil twin (paha kaksonen) -tukiasemalla tarkoitetaan vihamielisen tahon asentamaa WLAN-tukiasemaa, joka käyttää täsmälleen samoja asetuksia kuin auktorisoitu WLAN-verkko. Jos alkuperäinen verkko on suojaamaton tai se on vaarantunut, voi käyttäjän päätelaite yhdistää vihamieliseen tukiasemaan, ja hyökkääjä pystyy kaappaamaan kaiken suojaamattoman liikenteen. Usein vihamielisen tukiaseman lähetysteho on suurempi kuin hyökkäyksen kohteena olevan verkon. Tällöin moni käyttäjä yhdistyy parhaan signaalin tukiasemaan, joka on hyökkääjän hallinnassa. [1;12.]

Salauksen lisäksi samat tietoturvastandardit määrittelevät muun muassa lähetettävien ja vastaanotettavien sanomien eheyden tarkistuksen. Sanoman eheys varmistetaan, jotta huomataan, onko kuljetettava tieto muuttunut lähettämisen ja vastaanottamisen välillä. Muutos tarkistussummassa saattaa johtua esimerkiksi radiohäiriöistä tai välissä olevan tunkeutujan häirinnästä. Uudemmissa standardeissa käytetään kehittyneempää datan todennusta. Yhtäältä varmistetaan viestin lähettäjän oikeellisuus, toisaalta tarkistetaan eheys. [1; 9.]

WEP (Wired Equivalent Privacy) on 802.11-standardin ensimmäinen määritelty salausmenetelmä, joka perustuu esijaettuun avaimeen. WEP-salausta pidettiin heikkona jo standardointiaikanaan, ja se onnistuttiinkin murtamaan jo vuonna 2001. Nykyisin WEP-salauksen pystyy murtamaan matkapuhelimella muutamassa minuutissa. WEP-salausta ei suositella käytettäväksi enää missään olosuhteissa, eikä osa uusista WLAN-tukiasemista anna edes käyttää sitä. [1.]

802.1X

802.1X tarjoaa salasanaa laajemman konseptin käyttäjän tunnistukseen. Se perustuu EAP:hen (Extensible Authentication Protocol), joka ei ole tunnistusmenetelmä vaan optimoitu kuljetusalusta tunnistamiselle. EAP:tä käyttävä järjestelmä muodostuu päätelaitteen Supplicant-ohjelmasta, verkon reunalla olevasta tunnistajasta (Authenticator) ja tunnistuspalvelimesta, joka sisältää salasanat ja käyttäjätiedot. Useimmiten tunnistajan ja tunnistuspalvelimen välillä käytettävä protokolla on RADIUS. Esimerkiksi Microsoft Windows -palvelinympäristön Active Directoryn (AD) tunnistuspalvelinta voi käyttää tunnistamaan kirjautumisia WLAN-verkkoon ja muihin verkkolaitteisiin. Näin käyttäjä pystyy tunnistautumaan yrityksen langattomaan verkkoon omilla AD-käyttäjätunnuksillaan. [1.]

802.11i

802.11i on tuorein standardi, jolla pyritään parantamaan langattomien lähiverkkojen tietoturvallisuutta. Siinä on määritelty muun muassa 802.1X-menetelmän käyttäjätunnistus ja esitelty kehittyneempi salausmekanismi AES (Advanced Encryption Standard). Standardin tuorein ilmentymä on WPA2 (Wi-Fi Protected Access 2), jota pidetään oikein käytettynä murtamattomana. AES:ää pidetään erittäin tehokkaana salausmenetelmänä ja sen suurin mahdollinen avainpituus on 256 bittiä. AES on NISTin (US National Institute

of Standards and Technology) vuonna 2001 määrittelemä standardi, joka valittiin avoimen kilpailun perusteella. [1; 13.]

Standardia kehitettiin vuosia, ja se ratifioitiin vuonna 2004. Vuodesta 2006 laitteiden on pitänyt tukea standardin uusimpia ominaisuuksia saadakseen Wi-Fi Certified -hyväksynnän. Pakolliseksi on määritelty muun muassa WPA2-tuki. [1; 13.]

Standardi sisältää paljon muutakin kuin WPA2:n ja 802.1x:n käytön. Esimerkiksi esijaetun avaimen käyttö on perusteltua pienissä toimisto- ja kotiympäristöissä. Tällöin voidaan määritellä salasana, jolla verkkoon pystyy tunnistautumaan. Salasanan käyttöä voidaan pitää perusteltuna myös sellaisissa yritysverkoissa, jotka on suunnattu tulostinten ja muiden kiinteiden laitteiden käyttöön. Esijaetun avaimen turvallisin toteutustapa on tällä hetkellä WPA2/AES, ja turvallisuutta voi parantaa valitsemalla pitkän ja monimutkaisen salasanan. Nykyään ei pitäisi enää käyttää selvästi vanhempaa, jo murrettua TKIP:tä (Temporal Key Integrity Protocol), joka suunniteltiin alun perin paikkamaan WEPin vakavia puutteita. [1;13.]

2.8 Käyttäjämäärien ja vaatimusten lisääntyminen

Internetin käyttäjämäärät kasvavat jatkuvasti, samoin internetiin liitettyjen laitteiden lukumäärä. Statista.com-statistiikkasivuston mukaan maailmassa on tällä hetkellä 23 miljardia internetiin kytkettyä laitetta. Ennusteiden mukaan luku olisi vuoden 2020 loppuun mennessä yli 50 miljardia. Vuonna 2016 puolestaan oli keskimäärin 3,64 internetiin yhdistettyä laitetta henkilöä kohden. Määrä kasvaa jatkuvasti, ja vuonna 2020 odotetaan 4,3 käyttäjäkohtaisen laitteen rajan ylittyvän. [11.]

Käyttäjä- ja laitemäärien kasvu näkyy langattomissa verkoissa. Jos yrityksellä on esimerkiksi 50 työntekijää samassa tilassa, heillä on oletettavasti vähintään kannettava tietokone ja työpuhelin, mahdollisesti omakin puhelin, jotka kytkeytyvät langattomasti verkkoon. Usealla käyttäjällä on lisäksi tablettitietokone. Verkkoon kytkeytyy myös tulostimia, IP-valvontakameroita, kiinteistötekniikkaa, televisioita ja muita laitteita.

Jos käyttäjäkohtaisia laitteita on esimerkiksi kolme ja muita laitteita 20, yhteensä verkkoon liittyy 170 laitetta. Suurin osa tuottaa hyvin vähän tietoliikennettä ja vaatii tukiaseman lähetysaikaa vain vähän, joten yhdelle radiolle voidaan laskea suurempi määrä laitteita kuin käytettäessä esimerkiksi videosuoratoistoa. Internetin ja sähköpostin käytölle mitoitettuna yhteen WLAN-radioon voidaan järkevästi yhdistää noin 50 laitetta, teräväpiirtovideon suoratoistolle optimoidussa verkossa taas enintään 30 (käytettäessä 802.11ac-tekniikkaa). Toimistokäytössä 170 laitteelle riittäisi 3,4 laadukasta tukiasemaradiota. Nämä voitaisiin toteuttaa vaikkapa kahdella kahden radion tukiasemalla. Edellä lasketussa on oletettu, että palvelutason ei tarvitse olla poikkeuksellisen hyvä eikä verkossa tehdä mitään erityisen raskasta. [14.]

2.9 Kontrollerin rooli

Nykyään on kaikissa muutamaa tukiasemaa suuremmissa (3–4+) WLAN-verkoissa syytä käyttää keskitettyä ohjauskonetta eli kontrolleria. Kontrollerin tehtävä on yksinkertaistettuna toimia ainoana konfiguraatiopisteenä langattomaan verkkoon. Kontrollerin asetuksista määritetään kaikki langattomien verkkojen asetukset, kuten verkkojen nimet ja tietoturva-asetukset. Verkon asetukset määritellään kontrollerille, joka huolehtii automaattisesti tukiasemien konfiguroinnista. [19.]

Kontrollerin tärkein yksittäinen tehtävä on konfiguraation hallinta. Se valvoo muun muassa langattomaan verkkoon tehtäviä muutoksia. Yhden tukiaseman rikkoutumista ei välttämättä huomaa, jos alueella on paljon päällekkäisiä tukiasemia. Kontrollerin hallintanäkymästä havaitsee heti, jos jokin on vialla. Kontrollerilta näkee helposti esimerkiksi tukiasemien sijainnit, mikäli tukiasemat on nimetty loogisesti. Kontrolleri myös päivittää tukiasemien ohjelmistot keskitetysti helpoimmillaan yhdellä napin painalluksella. Esimerkiksi satojen tukiasemien ohjelmiston päivittäminen käsin on mahdotonta, koska se veisi kohtuuttomasti aikaa eikä tieto ohjelmistoversioista pysy ajan tasalla. [19.]

Verkkoa voidaan valvoa kontrollerin tilastoja havainnoimalla. Verkon ja yksittäisten tukiasemien kuormitusta on mahdollista seurata. Tästä on apua selvitettäessä verkon ongelmia. Käyttäjämäärien pistemäinen kasvu pystytään pitämään hallinnassa radioiden kuormitusta seuraamalla. Jos yksi tukiasema kuormittuu jatkuvasti liikaa, sen alueelle

voidaan asentaa lisää radiokapasiteettia joko lisäämällä tukiasemia tai kasvattamalla tukiaseman sisäisten radioiden määrää. [19.]

Suorituskyvyn hallinnassa kontrollerilla on suuri merkitys. Se voi esimerkiksi päättää, mihin tukiasemaan uusi laite liittyy. Tämä vaikuttaa etenkin ruuhkaisilla alueilla, joilla on paljon käyttäjiä. Jos esimerkiksi yksi tukiasema on vähemmän kuormitettu kuin muut samalla alueella, kontrolleri voi siirtää käyttäjiä kuormitetuilta asemilta vähemmän kuormitetuille. Kontrolleri osallistuu myös vaeltamisen ohjaamiseen. Tämä on tärkeää silloin, kun päätelaite liikkuu eri tukiasemien alueilla tietoa siirtäen. Vaeltamisen sujuvuuteen vaikuttavat usein käytettyjen laitteiden laatu ja kontrollerille ostetun lisenssin taso. [19.]

2.10 Langattomien siltojen kehitys

WLAN-silta on siirtokerroksen laitepari, joka toimii kuten tavallinen kaapeli. Sillä voidaan yhdistää langattomasti esimerkiksi rakennusten lähiverkkoja toisiinsa. Etäisyys voi olla monia kilometrejä, ja optimaalisissa olosuhteissa voidaan oikealla laitteistolla päästä jopa satojen kilometrien siltoihin. WLAN-sillan toteutukseen vaikuttaa suurimmalta osin vaadittu näköyhteys rakennusten välillä. Erittäin edullisesti voidaan rakentaa esimerkiksi esteetön 1 000 metriä pitkä linkki, jonka pitää läpäistä 100 Mbit/s. [1; 15.]

WLAN-sillan suorituskykyyn vaikuttavia seikkoja ovat signaalin vaimeneminen ja kohinan määrä. Vastaanottoherkkyyttä ja vastaanottimeen poimittavan kohinan määrää voi vähentää tehokkaasti hyvin kapeakeilaisella suuntaavalla antennilla. Suurin osa siltalinkin maksimipituuteen vaikuttavasta vaimennuksesta on vapaan tilan vaimennusta. Tämä johtuu siitä, että lähetysantennin signaali hajaantuu useisiin eri suuntiin, niinpä vain murto-osa signaalista etenee suoraan vastaanottoantenniin. Maksimietäisyyttä pienentää myös mahdollinen estevaimennus, joka voidaan minimoida esteettömällä näköyhteydellä. Vapaan tilan vaimennuksen laskemiseen tarvitaan tiedot käytettävästä taajuudesta ja linkin pituudesta. Internetissä on vapaasti käytettäviä laskureita, joilla pystyy helposti toteamaan käytössä olevan linkkikaluston suurimman mahdollisen jännevälin. Vaimennuksen määrä ei vaikuta suoraan esimerkiksi linkin luotettavuuteen. Sen sijaan se vaikuttaa käytettävään modulaatioon ja virheiden määrään sekä sitä kautta maksiminopeuteen, kunhan pysytään tarvittavien marginaalien sisällä. [1; 16.]

Langattoman sillan asentaminen on aikaisemmin ollut työlästä, sillä tukiasemaradio on pitänyt sijoittaa sisätiloihin. Sisältä on rakennettu koaksiaalikaapelilla yhteys suunta-antennille, joka on ollut perinteisesti rakennuksen katolla. Kaapelien läpiviennit on pitänyt usein tehdä suoraan katon läpi, jotta koaksiaalikaapelin pituus saataisiin minimoitua. Koaksiaalikaapelin vaimennus on suoraan verrannollinen pituuteen, ja kaikki siinä syntyvä vaimennus on pois antennin lähetystehosta eli linkin suorituskyvystä. [1; 15.]

Nykyisissä WLAN-silloissa on yhdistetty säänkestävä radio ja suunta-antenni yhteen koteloon, johon tulee yksi PoElla sähköistetty cat-parikaapeli. Tällöin matkaa syöttöpisteeltä sillan linkkilaitteelle voi olla jopa 100 metriä, ilman että etäisyys vaikuttaa lähetystehoon tai vastaanottoherkkyyteen. Suurin etu saavutetaankin juuri vastaanottoherkkyyden parantuessa. Tällöin voidaan käyttää joko pidempiä yhteysvälejä tai pienempiä lähetystehoja. Lisäksi nykyiset linkkilaitteet ovat nopeita ja edullisia ottaa käyttöön yksinkertaisuutensa vuoksi. Uusien siltojen rakentamisessa voidaan hyödyntää rakennuksessa mahdollisesti olevaa yleiskaapelointia. [1;15.]

WLAN-silta voi olla myös PtMP-sillta (Point to Multi-Point) eli monipistesilta. Tällöin esimerkiksi kampuksen päärakennuksessa on ympärisäteilevä juuritukiasema ja sivurakennusten linkkilaitteet yhdistävät juureen suunta-antenneilla. PtMP:n huono puoli on, että juuritukiaseman lähetysaika jakautuu kaikkien vastaanottavien linkkilaitteiden kesken, joten suurten nopeuksien saavuttaminen on vaikeaa. [1;15.]

Langattomien siltojen tietoturvallisuus on oikein konfiguroituna hyvä, koska silloissa voidaan käyttää samaa WPA2-AES-tasoista salausta kuin WLAN-verkoissakin. Joissain tapauksissa organisaation tietoturvapolitiikka on niin tiukka, että runkoyhteyttä ei voida toteuttaa langattomalla sillalla. Tällöin ainoaksi suurikapasiteettiseksi vaihtoehdoksi jää käyttää valokuitua. Kun vertaillaan kustannuksia, siltalinkki on valokuituun verrattuna ylivoimainen. [17; 19.]

3 Langattoman lähiverkon toteuttaminen

3.1 Vaatimusmäärittely

Vaatimusmäärittely on välttämätön osa mitä tahansa tietoteknistä projektia. Tämä pätee myös langattoman lähiverkon toteuttamiseen. Vaatimukset tulevat suoraan organisaation toiminnasta, jota kaikkien järjestelmien on tuettava parhaalla mahdollisella tavalla. Teknisiin vaatimuksiin vaikuttavat muun muassa päätelaitteet, käyttäjät, käyttötavat, sovellukset ja palvelut. Vaatimuksia sanelevat myös joustavuuden, muunneltavuuden ja laajennusmahdollisuuksien tarve. [1.]

WLAN-verkkoa suunnitellessa teknisiin vaatimuksiin kuuluvat erottamattomasti peittoalueen, käyttäjämäärien, päätelaitteiden, verkon suorituskyvyn, sovelluksien, tietoliikenteen kohteiden, tietoturvapolitiikan ja palvelutason määrittelyt. Aikataulu ja kustannusarvio ovat oleellinen osa hankkeen valmistelua. [1.]

Vaatimusmäärittelyn tekoon voidaan käyttää organisaation omaa henkilöstöä, mutta mittavissa hankinnoissa voi olla perusteltua käyttää apuna konsultteja, etenkin, jos hankkijan on sovellettava lakia julkisista hankinnoista [19].

3.2 Katselmus

Katselmuksessa on tarkoitus selvittää projektia edeltävä tilanne, jotta tiedetään, mihin kaikkeen projektin aikana pitää varautua. Katselmuksessa otetaan selvää esimerkiksi jo olemassa olevasta WLAN-verkosta ja arvioidaan, riittääkö langallisen lähiverkon kapasiteetti langattomalle verkolle. Sen aikana määritellään tarkat tiedot laitteiden asennukselle. Asennuksessa tarvittavia tietoja ovat tukiasemien sijainnit ja asennot, yleiskaapeloinnin rasiamerkinnät ja lähiverkon kytkinten portit. Lisäksi on kartoitettava mahdolliset erikoistarpeet. [1.]

Mikäli vaatimuksena on aukottoman peittoalueen lisäksi suuret yhteysnopeudet koko alueella ja suuren käyttäjämäärän kestäminen, voidaan tukiasemien sijainteja miettiä vähemmän kuin pienemmän suorituskyvyn ympäristössä. Tukiasemat voidaan asentaa

suurelta osin päällekkäin, jotta tarvittava radiomäärä saadaan käyttöön. Kuvatussa tilanteessa on järkevämpää sijoittaa tukiasemia tavallista lähemmäksi toisiaan ja pienentää radioiden lähetystehoa kuin hakea yhden tukiaseman maksimaalista peittoaluetta. Näin esimerkiksi laiterikon sattuessa voidaan muiden asemien lähetystehoa kasvattaa eikä katvealuetta synny. [9.]

Mikäli ainoastaan peittoalueella on merkitystä eikä nopeuksia ja kuormituksen kestoa pidetä tärkeinä, on kartoituksessa käytettävä testilaitteistoa, jolla todetaan tietyllä alueella toteutuva peitto. Mikäli tukiasemien määrä halutaan minimoida, on tarpeellista mitata kuuluvuus ja määrittää tukiasemien paikat siten, että maksimoidaan yksittäisen tukiaseman kuuluvuusalue. Jos tukiaseman radion vastaanottoherkkyys tai päätelaitteen lähetysteho on huono, tehokkaiden lisäantennien käytöllä ei välttämättä saada verkkoon lisää käytännön peittoaluetta. [1; 9.]

3.3 Suunnittelu

Suunnittelussa pitää huomioida vaatimusmäärittelyssä esille tulleet asiat. Langattoman lähiverkon suunnitelmassa kuvataan määritykset täyttävän WLAN-verkon tekniset ratkaisut. Suunnitelma toimii pohjana tarjouspyynnölle, ja usein toimittajaehdokas haluaa katselmoida organisaation tilat tehdäkseen tarjouksen. Katselmuksen jälkeen suunnitelmaa voidaan joutua muokkaamaan. Yleisimmin muokataan tukiasemien määrää ja sijoitusta. [19.]

Suunnitelmien sisältö, muoto ja tarkkuus riippuvat kohderyhmästä ja käyttötarkoituksesta. Suunnitteludokumentaatio sisältää vaatimusmäärittelyn, WLAN-verkon loogisen ja fyysisen kuvauksen, tukiasemien määrät ja sijoitukset, olemassa olevan verkon tiedot, kustannusarvion, aikataulun, toteutussuunnitelman ja onnistumisen mittarit. [1.]

Oleellinen osa suunnitelmaa on kanavasuunnitelma, jossa määritellään ennalta oma kanavansa kunkin solun (tukiaseman) alueelle. Huolellisesti tehty kanavasuunnitelma ehkäisee ennalta ongelmia, sillä kontrollerien automaattinen kanavanmääritys toimii usein puutteellisesti. Käytettävissä oleva taajuuskaista tulisi käyttää mahdollisimman laajasti. Esimerkiksi Euroopan alueella on 5 GHz:n taajuudella käytettävissä yhdeksän 40 MHz:n levyistä kanavaa, 20 MHz:n levyisiä on 19. Vaikka käytettäisiin 80 MHz:n kaistanleveyttä,

kanavia on neljä. Kaikilla kaistanleveyksillä pystyy helposti rakentamaan verkon, jossa samalla kanavalla olevat tukiasemat eivät häiritse toisiaan, vaikka kaikkia kanavia käytettäisiin. [1; 9.]

Suunnittelussa tulee päättää teknologia, jolla verkkoa ryhdytään rakentamaan. Hyviä suuntaviivoja antaa vaatimusmäärittely. Nykytekniikalla on perusteltavissa kolme mahdollisuutta: 802.11n, 802.11ac Wave 1 tai Wave 2. Kaikilla näillä teknologioilla päästään hyviin tuloksiin, kunhan tarpeet huomioidaan oikein. [9.]

Suunnitelman teossa on pidettävä mielessä suunnitelman kohderyhmä. Ulkoa tilatun toteutuksen urakoijalle on tärkeää, että suunnitelma sisältää kaiken mahdollisen tiedon. Jos organisaatio asentaa laitteiston itse, voi suunnitelma olla hyvinkin yksinkertainen, koska oma henkilöstö tuntee ympäristön. Hyvästä suunnitelmasta pystytään helposti tekemään osa loppudokumentaatiota. [1.]

3.4 Toteutus

Langaton lähiverkko voidaan toteuttaa monella eri tavalla. Se voidaan ostaa avaimet käteen -palveluna tai osaprojekteina eri toimittajilta tai tehdä jopa kokonaan itse. Vastuunjako on helpoin avaimet käteen -toimituksessa, jossa kokonaisvastuu projektin onnistumisesta voidaan ulkoistaa toimittajalle. Vastuunjako on yhtä selkeä käytettäessä omaa henkilöstöä, mutta yrityksissä on harvoin langattomien verkkojen asiantuntijoita. Tällöin voidaan joutua turvautumaan konsultin käyttöön ongelmatilanteissa. Sekavinta vastuunjako on, jos toimittajia on useita. [1; 9.]

Laitteiden asennukset tehdään katselmusdokumenttien ja suunnitelmien mukaisesti. Määriteltyjä asennusohjeita tulee noudattaa tarkasti. Laitteiden ja kaapelien kiinnitysten tulee olla luotettavat ja siistit. [1.]

Toteutusvaiheessa saatetaan joutua lisäämään tai uusimaan yleiskaapelointia, sillä tukiasemat kiinnitetään monesti kattorakenteisiin tai seinän yläosiin. Vanhaa yleiskaapelointia rakennettaessa on mietitty vain tietokoneiden liityntätarpeita, joten kaapelointi on päätetty rasioihin monesti lattian tai vyötärön tasolle. Tästä voi olla hankalaa viedä kaa-

pelia katossa olevalle tukiasemalle. Kaapelointiprojekti voidaan sisällyttää laiteasennusprojektiin, mutta usein ne toteutetaan erikseen. Mikäli projektit eriytetään, pitää kaapeloinnin olla valmis ennen laitteiden asennuksia. [1.]

Asennuksen yhteydessä on lähes aina tarve muuttaa lähiverkon aktiivilaitteiden asetuksia. Tukiasemien hallintaan käytetyt IP-osoitteet (Internet Protocol) ja VLAN (Virtual Local Area Network) eli virtuaaliverkko saattavat erota organisaatiossa yleisesti käytetyistä verkoista. Jos on suunniteltu käytettävän useampaa SSID:tä (Service Set Identifier) eli langattoman verkon nimeä, SSID:t halutaan usein siirtää tukiasemalta kytkinverkkoon käyttäen omaa virtuaaliverkkoaan jokaiselle SSID:lle. [1; 9.]

3.5 Testaus

Langattoman verkon testaamisen tarkoitus on todeta, kykeneekö verkko täyttämään vaatimusmäärittelyissä ja suunnitelmissa kirjatut vaatimukset. Monesti testaaminen tehdään vain laiteasennusten vastaanottotarkastuksen yhteydessä, mutta on myös tärkeää testata jatkuvasti verkkoa, kun se on tuotantokäytössä. Näin havaitaan mahdolliset häiriöt ja vikaantuneet laitteet sekä merkittävät poikkeamat suorituskyvyssä. Esimerkiksi yrityksen avokonttoriin voidaan rakentaa uusi neuvotteluhuone, eikä WLAN-signaali enää tulekaan uuteen huoneeseen riittävän voimakkaasti. Tällöin pitää reagoida muuttuneeseen tilanteeseen lisäämällä neuvotteluhuoneeseen uusi tukiasema. [19.]

Vastaanottotarkastuksessa tarkastetaan, että verkko on suunnitteludokumenttien mukainen. Lisäksi tarkastetaan verkon toiminta ja kaikkien sovittujen laitteiden ja asennusdokumenttien toimitus. Verkon toimintaa voi testata monilla testausohjelmistoilla ja -laitteilla. Ilman niitäkin pystytään toteamaan verkon nopeudet ja viiveet, viiveiden vaihtelu kuormituksen myötä, yhteysnopeudet ja vaeltamisen (roaming) toimiminen. Dokumentaation oikeellisuuden voi todeta vertaamalla toteutusta suunnitelmiin ja asennusdokumentteihin. Langattoman verkon kontrollerilta näkee helposti verkossa olevien tukiasemien mallit ja määrät. [1; 9]

Jatkuva testaaminen on helppoa: aktiiviset käyttäjät ilmoittavat heti, jos verkko ei toimi odotetusti. Edistynyt käyttäjä pystyy omasta päätelaitteestaan etsimään tietoja, jotka auttavat ongelmien rajaamisessa. Verkonhallintatyökalut ovat olennaisia käytönaikaisen

testaamisen osia. Päätelaitteen tietojakin tärkeämpiä tilastoja ja lokitietoja saadaan WLAN-kontrollerilta. Kontrollerin näkymästä pystytään esimerkiksi havaitsemaan ylikuormittuneet ja rikkinäiset tukiasemat, verkkoa runsaasti kuormittavat päätelaitteet, laitteiden jakautuminen eri taajuuksille ja muuta verkkoon liittyvää. Siksi kannattaa katsoa ajoittain, mitä kontrollerilla tapahtuu, vaikka näkyviä ongelmia ei olisikaan. [9.]

3.6 Dokumentointi

Langattoman lähiverkon dokumentaatiolle luodaan pohja hyvin tehdyillä vaatimusmäärittelyillä ja suunnitelmilla, jotka liitetään osaksi lopullista dokumentaatiota. Myös katselmuksessa tuotetut dokumentit on liitettävä lopulliseen dokumentaatioon. Loppudokumentaatiota täydennetään asennusdokumenteissa mainituilla laitteiston yksityiskohdilla ja yleiskaapeloinnin kytkennöillä. [1; 17.]

Tukiasemien tarkat tiedot ja esimerkiksi laitteiden sijainti voidaan dokumentoida myös kontrollerilta tulostamalla. Kontrollerin tiedot ja konfiguraatiot muuttuvat usein, joten on suositeltavaa pitää kaikki yksityiskohtaiset laitetiedot ainoastaan kontrollerilla. [9.]

Tukiasemaradioiden kanavasuunnitelmasta on syytä tehdä erillinen dokumentti, mikäli kanavat suunnitellaan ja asetetaan käsin. Käytettäessä kontrollerin automaattista kanavanmääritystä ei kanavasuunnitelmaa tarvita eikä sitä näin ollen tarvitse dokumentoida, mutta asia on hyvä mainita muun dokumentaation yhteydessä. [19.]

4 Verkon rakennusprojekti

Insinöörityön tarkoituksena oli rakentaa hyvin toimiva ja nykyvaatimusten mukainen langaton lähiverkko. Kohteena ollut vanha kiinteistö vaikeutti optimaalisen kuuluvuuden rakentamista halutuille alueille. Koska kuormituksen alainen suorituskyky on insinöörityöni keskeisin vaatimus, käsittelen sitä työssäni toistuvasti eri tavoin.

Vaatimusmäärittely

Insinöörityön toteutusta aloittaessa totesin vaatimusmäärittelyn olevan tärkeä. Onnistuneella vaatimusmäärittelyllä ja sen mukaisella suunnittelulla varmistin, että lopputulos eli käyttöönotettu WLAN-verkko vastaa kaikin puolin tarvetta.

Käyttötarinat

Käyttötarinoita kerätessäni selvisi, että tulevilla loppukäyttäjillä oli ennen kaikkea pettymykseen johtaneita kokemuksia WLAN-verkoista. Esimerkiksi toiveita roamingin toimimisesta en kuullut, koska päällimmäisenä monilla käyttäjillä oli toive vakaasta yhteydestä paikallaan työskennellessä. Nopeuden merkitystä ei erikseen korostettu, koska nopeuden oletettiin kuuluvan luotettavuuteen.

Onnistuin muodostamaan joitakin hyviä käyttötarinoita. Esimerkkinä erään käyttäjän kuvailema tarina: ”Tulen aamulla töihin ja avaan kannettavan tietokoneen lepotilasta. Pystyn käyttämään internetiä heti, kun saan koneen nettiselaimen auki, riippumatta siitä, missä kohtaa kiinteistöä olen. Illalla pidettävään yleisötilaisuuteen tulee paljon väkeä, ja nettiyhteys toimii edelleen moitteettomasti. Tilaisuuteen osallistuva englantia puhuva kävijä voi ongelmitta liittyä verkkoon, josta saa simultaanitulkkauksen äänipalvelun matkapuhelimeen. Voin keskittyä ohjeistamaan, miten tulkkausäänen vastaanotto-ohjelma ladataan sen sijaan, että tappelen verkon kanssa.”

Tästä tarinasta oli helppo poimia muun muassa kattavuutta, kuorman sietoa, verkkojen määritystä ja käytettäviä sovelluksia koskevia vaatimuksia. Lisäksi selvisi, että organisaatiossa aiottiin käyttää paitsi internetissä olevia palveluita myös sisäverkossa tuotettua reaaliaikaista sisältöä, joten pelkästään ulos lähtevän internetyhteyden kapasiteettia ei voinut pitää kapasiteetin mittarina. [18.]

Toiminnalliset vaatimukset

Toiminnallisia vaatimuksia määrittäessäni nousi suurimmaksi yksittäiseksi asiaksi henkilökunnan laitteiden käyttämän verkon tietoturvallisuus. Turvallisuuden haluttiin olevan mahdollisimman hyvä. Harkitsin RADIUS-palvelimen käyttöönottoa henkilöstön verkkoon, mutta totesin käyttäjämäärän olevan niin pieni, että siitä ei olisi suurta hyötyä. [9.]

Turvallisuuteen liittyvänä vaatimuksena totesin myös, että tavallisille kävijöille suunnatusta verkosta ei saanut päästä mihinkään muuhun lähiverkon palveluun kuin tulkkausääntä jakavalle palvelimelle. Lisäksi jokaisen peruskäyttäjän yhteysnopeuden piti olla rajattu, jotta yksittäinen käyttäjä ei pystyisi aiheuttamaan haittaa tukkimalla tukiaseman tai internetin. Organisaatio halusi myös minimoida ilkivallan ja verkkohyökkäysten mahdollisuudet.

Yhteysnopeuksien tuli olla tavanomaisissa työskentelypaikoissa niin hyvät, että henkilökunnan verkon yksittäinen käyttäjä pystyisi hyödyntämään tarvittaessa kokonaan 100 Mbit/s -internetyhteyden langattomasti. Lisäksi sisäverkon tiedostopalvelimelle tuli saavuttaa vähintään 100 Mbit/s todellinen yhteysnopeus. [9.]

WLAN-järjestelmän haluttiin olevan ”yhdestä portaalista hallittava” eli käytännössä kontrollerin ohjaama. Esimerkkinä mainittiin, että verkon salasanan pitää olla helposti vaihdettavissa. Tämä ei onnistu 20–30 tukiaseman toteutuksessa ilman kontrolleria. [17.]

Laatuvaatimukset

Järjestelmän haluttiin olevan luotettava ja tarvittaessa helposti korjattavissa. Purkaessani vaatimusta toteutukseksi tuli selväksi, että luotettavuus tarkoitti käyttäjille samaa kuin yhteyden nopea muodostuminen, nopeus, pieni viive ja vakaa toiminta yhdessä. Jos jokin mainituista puuttuisi, ei verkkoa pidettäisi luotettavana. Haluttiin, että mahdollinen luotettavuuden puute pystyttäisiin korjaamaan helposti, eli käytännössä koko verkon laitteiston uudelleenkäynnistämisen tuli olla yksinkertaista.

Kapasiteettivaatimuksena määriteltiin, että kun verkkoon on yhdistynyt 200 päätelaitetta, toiminnassa ei huomaisi merkittävää eroa hiljaisempiin hetkiin verrattuna. Tuen maksimi päätettiin asettaa 400 päätelaitteeseen siten, että laitteiden ollessa verkossa sallittaisiin

pieni hidastelu. Verkon tulisi kuitenkin edelleen palvella perusasioissa, joita ovat esimerkiksi kevyt internetsivujen selailu ja tulkkauksen äänivirtaukset. [9; 14.]

Laatuun vaikuttaa oleellisesti myös signaalin voimakkuus. Työn kohteena oleva kiinteistö on betonista valettu viisikerroksinen kirkkorakennus, jonka kerroksista kaksi on maan alla. Erilaisia tiloja on paljon, ja seinät ovat paksua betonia. Vaatimuksia mietittäessä jokainen projektiin osallistunut ymmärsi, että kattavan verkon rakentaminen vaatisi paljon tukiasemia. Tukiasemien suuri määrä parantaisi kapasiteettia, mikä oli myös tavoitteena. Vaatimuksiin päätettiin kirjata, että yhteyden laadun tulisi olla jokaisessa tilassa vähintään niin korkea, että saavutettaisiin todellinen 15 Mbit/s -yhteysnopeus verkon palveluihin (muun muassa internetiin). Päätettiin myös, että jokaisessa tilassa, jossa voi työskennellä, tulisi yhteysnopeuden olla vähintään 30 Mbit/s. Jokaisessa vakituisessa työskentelytilassa tulisi yhteyden mahdollistaa vähintään 100 Mbit/s -tiedonsiirtonopeus. [5; 7; 9.]

Luotettavuuden takaamiseksi haluttiin, että yhden tukiaseman rikkoutuminen ei merkittävästi heikentäisi verkon toimintaa tärkeimmissä tiloissa. Tämä lisäsi vaatimuksia tukiasemien sijoittelulle ja määrille. Pidettiin hyväksyttävänä, että yksittäisen tukiaseman rikkoutuminen poistaisi verkon toiminnan toissijaisilta alueilta, kuten varastoista ja teknisistä tiloista. Haluttiin myös, että talonmies voisi itse tarvittaessa vaihtaa rikkoutuneita tukiasemia. [9; 19.]

Ylläpitosuunnitelma

Ylläpitoon ei ole varattu henkilöstöä. Eräs teknisempi henkilökunnan jäsen kykenee tarvittaessa vaihtamaan verkon salasanan ja käynnistämään laitteet uudelleen, mutta muu työ pitää hankkia tulevaisuudessa ulkopuolisena palveluna. Tästä syystä toivottiin, että järjestelmä vietäisiin kerralla niin pitkälle, kuin olisi mahdollista ja järkevää. Lisäksi dokumentoitaisiin erityisesti kontrollerin käyttö ja piirrettäisiin kunnolliset topologiakuvat ja muut ylläpitoa helpottavat dokumentit. Tämä helpottaisi tulevan ylläpitäjän työtä. [18.]

Organisaatio halusi, että kaksi tukiasemaa jätettäisiin sijoittamatta. Niiden tuli kuitenkin olla valmiiksi synkronoituina kontrollerin kanssa. Näin ne olisi helppo sijoittaa mahdollisesti uusiin lisäkapasiteettia vaativiin tiloihin tai vaihtaa rikkoutuneiden tilalle.

4.1 Suunnittelu ja pohjakartoitus

Kartoitus- ja suunnitteluvaiheissa on tärkeää kerätä riittävästi tietoa toteutusympäristöstä ja pyrkiä huomioimaan ennalta mahdollisia ongelmia sekä löytämään ratkaisuja ilmenneisiin haasteisiin. Näin voidaan helpottaa ja nopeuttaa asennustyötä ja urakoitsijalla teetettäessä pienentää asennuksesta syntyvää laskua tuntuvasti. [1; 19.]

Kiinteän lähiverkon riittävyyden ja sähkönsyötön arviointi

Aloitin kiinteän verkon kartoituksen selvityksellä kytkinverkon laitteista ja lähiverkon valmiista kaapeloinnista. Havaitsin kaapeloinnin olevan enimmäkseen riittävää laadultaan ja määrältään. Yleiskaapelointi oli tehty suurelta osin 2010-luvulla, joten käytetty kaapeli täytti kategorian 6 (Cat 6) kaapelointistandardin, jota pidetään hyvätasoisena. Kaapelointi kattoi lähes kaikki tarvittavat tilat, ja uusien kaapelien rakentaminen olisi helppoa kunnollisten kaapelireittien ansiosta. [19.]

Kytkinverkossa oli usean eri valmistajan laitteita, ja kaikissa laitteissa oli vähintään 1 Gbit/s -kytkinportit. Gigabit-luokan nopeudet riittävät erinomaisesti, kun huomioidaan, että kiinteistön internetyhteyden nopeus on 100 Mbit/s eikä lähiverkon sisäistä liikennettä ole kovin paljoa. Tulkkausäänen bittinopeus on niin pieni, että sitä ei juuri huomaa verkon kuormitusta tarkkaillessa. Osa kytkimistä tukee PoE-virransyöttöä, joten ne olivat tukiasemaverkon rakentamista ajatellen juuri oikeanlaisia. Yksi PoE-kytkin täytyi vaihtaa toiseen jakamoon, koska näin sain suuremman osa tukiasemista suoraan kytkimiin kiinni ilman PoE-injektoreita. Pääjakamon kytkimen ja tärkeimpien jakelukytkinten välillä oli käytetty kahden portin LACP:tä (Link Aggregation Control Protocol), joten kytkinten väliset yhteydet kykenevät 2 Gbit/s -nopeuteen. Ne ovat siis erittäin nopeita käytön määrään nähden. Kytkinverkkoa voidaan pitää hyvin riittävänä, eikä siitä tule tiedonsiirron pullonkaulaa lähitulevaisuudessa. [17; 19.]

Kytkinverkossa oli otettu käyttöön VLANit. Virtuaaliverkkoja oli tehty eri tarkoituksiin ja muun muassa laitteiden hallintaverkko oli jo olemassa. Tukiasemien hallintaan käytetty IP-osoite sijoitetaan yleensä hallintaverkkoon, joten olemassa oleva verkko nopeutti toteutusvaihetta. Tukiasemat saavat osoitteensa DHCP-palvelimelta (Dynamic Host Configuration Protocol). Hallintaverkossa ei ollut vielä DHCP-palvelinta, joten asensin sellaisen kontrollerin virtuaalikoneelle. [19.]

Rakennusmateriaalien ja tilojen vaikutus

Opinnäytetyön kohteena olleen kiinteistön pääasiallinen rakennusmateriaali on paikalleen valettu betoni. Ovien materiaali on kokopuuta, metallia ja lasia. Ulkoverhoilu ja jotkin väliseinät on tehty tiilestä. Tilojen koko vaihtelee erittäin suuresta salista lukuisiin pieniin huoneisiin.

Tilojen kartoituksen yhteydessä totesin, että rakennusmateriaalit vaikuttaisivat yksittäisen WLAN-tukiaseman peittoalueeseen erittäin rajoittavasti. En pitänyt tätä ongelmana, sillä solukoko haluttiin muutenkin pitää pienenä suorituskyvyn takia. Raskaista rakenteista aiheutuva radioaaltojen kimpoilu eli monitie-eteneminen usein jopa parantaa MIMOa tukevien yhteyksien toimintaa. Siksi en ajatellut materiaalien aiheuttavan suurta ongelmaa. Tärkeää oli vain pitää solukoko eli tukiaseman vaikutusalue pienenä. [1; 7; 9; 19.]

Paksut betonirakenteet tuovat erään hyvänkin ominaisuuden, toisin sanoen interferenssin pienenemisen. Tällöin WLAN-verkon tukiasemien toiminta häiriintyy vähemmän kuin avoimemmassa tilassa. Näin voitaisiin käyttää myös suurempaa kaistanleveyttä, mikäli se olisi tarpeen. [17; 19.]

Radioiden määrä: suuret peittoalueet vai suuri suorituskyky

Tyypillinen kuluttaja miettii WLAN-tukiasemaa hankkiessaan kahta asiaa: nopeutta ja peittoaluetta. Samat asiat kiinnostavat organisaatioitakin, mutta huomioon otettavia asioita on enemmän. Tukiasemien ja radioiden määrä kannattaa pitää suurena, jos ajatus on palvella montaa käyttäjää monessa paikassa. Rajoittavia tekijöitä voivat olla esimerkiksi liian vähäinen yleiskaapelointi tai erittäin suuri interferenssi. Tämä on yleistä toimittaessa liikerakennuksessa, jossa on pienellä alueella monta yritystä. [19.]

Kaapelointi oli työni käsittelemässä kiinteistössä riittävä, eikä häiriön lähteitä juuri ollut. Jo vaatimusmäärittelyjä tehdessäni oli selvää, että toteutuksessa haluttaisiin tukiasemiin osittain päällekkäiset peittoalueet. Lisäksi haluttiin panostaa aiempaa paljon suurempaan suorituskykyyn. Suuremmissa tiloissa piti jopa laskea muutaman tukiaseman lähetystehoa ja sijoittaa ne hieman lähemmäksi toisiaan. Näin saavutettiin tarpeeksi hyvä suorituskyky ruuhkaisimmille alueille. [19.]

Miettiessäni suorituskyvyn ja solukoon välistä rajanvetoa halusin huomioida, että mobiililaitteiden määrä on jatkuvasti kasvussa. Mobiililaitteiden WLAN-radioiden lähetystehot ja vastaanottoherkkyydet ovat oleellisesti heikompia kuin kannettavissa tietokoneissa. Nykypäivän langatonta verkkoa suunnitellessa on otettava huomioon, että mobiililaitteidenkin pitäisi toimia hyvin verkon aiotun peittoalueen ulkoreunalla. Tämä vaatii totuttua tiheämpää tukiasemien sijoittelua. Osa käyttöönottotesteistä on syytä tehdä myös mobiililaitteilla, jotta varmistutaan riittävän hyvästä signaalitasosta. [11; 19.]

Laitetoimittajan ja -mallin valinta

Tukiasemien laitevalmistajan ja -mallin valintaan vaikutti muutama rajaava tekijä. Eniten perusteissa painoivat hankinta-, asennus- ja ylläpitokustannukset. Pelkät WLAN-kontrollerin lisenssien ylläpitomaksut sulkivat pois muutamia moderneja pilvipalveluun perustuvia toimijoita. Myös tukiasemien korkeat hankintahinnat sulkivat pois useita tunnettuja laitevalmistajia. Useimmiten erillinen kontrollerilaite oli myös niin kallis, että kontrollerin hinta yksinään rajasi tiettyjä valmistajia ja mallisarjoja pois. Laitteiden elinkaarikustannusten lisäksi valinnassa painoivat laitteiden suorituskyky, luotettavuus ja helppo asennus. [15; 19.]

Muuttaessani vaatimusmäärittelyjä suunnitelmiksi totesin, että ainoa tapa päästä vaadittuihin yhteysnopeuksiin kuormittuneessa verkossa on valita tukiasemien standardiksi 802.11ac. AC-standardin tuore Wave 2 -versio olisi ollut suotava MU-MIMOn ja kasvaneiden nopeuksien tuomien etujen takia. Tuoreen version laitteet ovat hankintahinnoiltaan 2–3 kertaa kalliimpia kuin vastaavat Wave 1 -laitteet, joten tiukan budjetin takia oli tyydyttävä vanhemman version laitteisiin. Lisäksi tukkurilla olisi voinut olla pahoja uudempien laitteiden toimitusvaikeuksia. [19.]

Laitetoimittajaksi valikoitui Ubiquiti Networks, joka on melko uusi amerikkalainen laitevalmistaja (perustettu 2005). Se valmistaa korkean suorituskyvyn verkkoteknologiaa internetpalveluntarjoajille ja yrityksille. Ubiquitin teknologiakehityksen päätavoite on toimittaa edistyneitä ja helposti käyttöönotettavia järjestelmiä. Ubiquitin yrityskäyttöön suunnatun WLAN-tukiasemien malliston nimi on UniFi. Mallistosta valittiin asennettavat tukiasemat. Ubiquiti valmistaa myös pitkän kantaman radiolinkkikalustoa. Pisimpien saavu-

tettujen linkkien pituudet ovat yrityksen tietojen mukaan 100–300 km, ja parhaan suorituskyvyn laitteistolla päästään lyhyillä matkoilla jopa 2 Gbit/s -nopeuteen. Rakennusten väliseen siltalinkkiin käytettävä radiopari valikoitui hieman kevyemmästä mallista. [15.]

Valittu WLAN-tukiasemamalli on nimeltään UAP-AC-PRO. Se on 3 x 3 -antenninen 802.11ac-standardia tukeva kahden radion tukiasema. Toinen radio toimii 2,4 GHz:n ja toinen 5 GHz:n taajuudella. Tukiasema on kosteussuojattu, joten sen voi tarvittaessa asentaa ulkotiloihin, kunhan suoraa kosketusta veteen ei synny. Laite tukee 802.3af-standardin PoE-sähkönsyöttöä ja suurta määrää eri verkkostandardeja. Laitteessa on kaksi 1 Gbit/s -Ethernet-liitintä, joista toinen vastaanottaa sähköä. Nä in tukiasemia pystyy ketjuttamaan, kunhan lisää PoE-injektorin aina ennen seuraavaa tukiasemaa. [15.]

Valitun tukiaseman ominaisuudet täyttivät asetetut vaatimukset. Toiveet hyvästä suorituskyvystä ja asennuksen helppoudesta toteutuivat. Laite on lisäksi silmää miellyttävä ja ulkokäyttöönkin soveltuva. Hinta on erittäin kilpailukykyinen: yksi tukiasema maksaa 150 euroa ja viiden kappaleen paketin hinta on 700 €. Lisäksi avoimen lähdekoodin kontrolleriohjelmisto on ilmainen. Esimerkiksi Cisco Systemsin yksi vastaavan luokan ac-tukiasema (Aironet 1830) maksaa yli puolet (399 €) Ubiquitin viiden tukiaseman pakkauksesta, joten kyseessä on todella edullinen tuote. [15; 19; 21.]

Siltalinkin laitteistoksi valikoitui saman valmistajan NanoStation Loco M5. Pienessä 5 GHz:n alueella toimivassa laitteessa on kaikki tarpeellinen: suunta-antenni, radio, seinä- tai pylväskiinnitys ja tuki PoE-sähkölle. Kantomatka on tietojen mukaan optimiolosuhteissa jopa 15 kilometriä, ja linkin maksiminopeudeksi ilmoitettu 150 Mbit/s osoittautui testeissä oikean suuntaiseksi. Yhden laitteen hinta on 50 euroa. Näin 100 eurolla pystyy rakentamaan todella nopean linkin, kun rakennusten etäisyys on enintään 500 metriä. [15; 16; 17.]

Tietoturvallisuuden suunnittelu

Tietoturva on erittäin kriittinen osa kaikkea nykypäivän toimintaa. Mitään tietoliikennettä ei tulisi kuljettaa salaamattomana, etenkään langattomasti. Organisaatioita langaton tietoturva kiinnostaa vähintään kahdesta eri näkökulmasta. [19.] Käsittelen näkökulmia tässä luvussa.

Turvallisuuden kulmakivenä käytetty niin sanottu CIA-malli (Confidentiality, Integrity and Availability) kuvaa hyvin langattoman verkonkin turvallisuussuunnittelussa tarvittavia asioita. Sitä soveltamalla varmistetaan tietoliikenteen luottamuksellisuus, eheys ja saatavuus. Halutaan varmistaa, että luottamuksellisia tietoja voi käsitellä turvallisesti langattoman verkon kautta ilman, että tiedot päätyvät vääriin käsiin – tai jos päätyvät, ne eivät salattuna hyödytä hyökkääjää mitenkään. Lisäksi halutaan, että langaton käyttäjä saa esimerkiksi internetselaimeensa oikean palvelun eikä hyökkääjän tuottamaa palvelua. Palvelun laadun pitää myös olla niin korkea, että tarvittavat verkkoresurssit ovat saatavilla aina tarvittaessa. CIA-mallin onnistumiseen voi osaltaan vaikuttaa tietoturvan oikeanlaisella suunnittelulla ja toteutuksella. [19; 20.]

On tärkeää suojata organisaation sisäiset verkkoresurssit, kuten palvelimet ja verkossa olevat laitteet sekä verkkoidentiteetti. Monilla organisaatioilla on sisäverkossa palveluita, joita ei pysty turvallisuussyistä käyttämään muualta kuin sisäverkosta. On ikävää, jos tunkeutuja löytää verkosta tulostimen, tulostaa yö toisensa jälkeen musteet ja paperin loppuun tai pääsee käsiksi yrityksen tiedostopalvelimeen. Ei ole vaikeaa miettiä seurauksia, jos vaikkapa sähköyhtiön operatiivisiin hallintajärjestelmiin pääsee tunkeutumaan huonosti suunnitellun langattoman tietoturvallisuuden takia. [19, 20.]

Tietoturvallisuuden suunnittelussa otin tässä työssä huomioon eri SSID:iden käyttäjäryhmät ja näiden tarvitsemat palvelut. Jokainen SSID on omassa VLANissaan, joiden välillä on sallittu palomuurin pääsylistoissa ainoastaan tarpeellinen liikenne. Esimerkiksi verkossa olevan valvontakameran tarvitsee päästä verkossa ainoastaan siihen kameratallentimen IP-osoitteen porttiin, jolla kamera ja tallennin keskustelevat. Kaikki muut pääsymahdollisuudet estetään. Insinöörityön kohteessa virtuaaliverkkojen välinen liikenne oli valmiiksi palomuurilla rajoitettua. Langaton verkko siis piti toteuttaa olemassa olevien tietoturvaa parantavien ratkaisujen päälle. [19; 20.]

Turvallisin tapa suojata yrityksen langaton lähiverkko on tunnistuspalvelimen käyttäjätunnukseen ja salasanaan pohjautuva todentaminen. Tämä menetelmä saattaa olla liian raskas, mikäli yrityksen verkossa ei ole valmista tapaa hallita käyttäjätunnuksia ja salasanoja, esimerkiksi Microsoftin AD-ympäristöä. Työn kohdeorganisaatiossa oli valmiiksi AD ja verkkolaitteiden todennus oli toteutettu RADIUS-palvelimella. Verkkoon liitettäville kiinteille laitteille kannattaa luoda oma esijaetulla avaimella todennettava verkko, jossa on erittäin vahva salasana. Tällaisia omaan verkkoonsa liitettäviä kiinteitä laitteita ovat

vaikkapa valvontakamerat tai tulostimet. Vahvan salasanan kirjoittaminen on vaikeaa ja hidasta, mutta tämä ei haittaa, koska salasanan syöttö on kertaluontoinen. [19.]

Vierasverkon liikenteen olisi hyvä olla salattua, mutta tämä ei aina ole mahdollista. Avointa vierasverkkoa suunnitellessa on syytä varmistaa, että verkon käyttäjät eivät pysty liikennöimään keskenään. Myös kaikki liikenne organisaation sisäverkkoon tulee estää. Tukiasemaverkossa kannattaa käyttää toimintoa, joka tunnistaa luvattomat tukiasemat ja ilmoittaa niistä. Näin voidaan välttyä pitkäkestoisilta evil tvin -hyökkäyksiltä. [17; 19.]

Tein insinöörityön kohdeorganisaatioon avoimen vierasverkon, jossa otin huomioon edellä esittämäni asiat. Lisäksi rakensin erillisen reitityksen niin, että vierasverkko ja sisäverkko käyttävät eri julkista IP-osoitetta internetiin liikennöitäessä. Näin vierasverkko on loogisesti täysin eristetty organisaation sisäverkosta ja sieltä internetiin liikkuvan datan voi erottaa organisaation omasta. Lisäksi otin vierasverkossa käyttöön käyttäjäkohtaisen 5/5 Mbit/s -nopeusrajoittimen, joten muutama vihamielinen käyttäjä ei pysty tukkimaan internetyhteyttä. [17; 19.]

4.2 Käytännön toteutusvaihe

Laitehankinnat

Aloitin laitehankinnat pikapuolisella kilpailutuksella. Vertailin kotimaisten ja eurooppalaisten internetkauppojen ja -tukkujen hintoja ja tein muutaman tarjouspyynnön. Valitsemallani laitevalmistajalla ei ollut montaa kotimaista toimittajaa, eivätkä suomalaisten toimittajien hinnat olleet kilpailukykyisiä. EU-alueen ulkopuolelta laitteita ei kannata ostaa, koska maahantuontikulut kasvavat suuriksi.

Toimittajaksi valitsin puolalaisen verkkotukun Inter Projekt S.A:n, jonka tarjous oli ylivoimainen sekä kustannusten että toimitusajan perusteella. Tilasin 25 tukiasemaa ja kaksi linkkiradiota tavallisella yritysluottokortilla, jonka käyttöraja riitti hyvin alle 3 600 euron tilauksen tekemiseen.

Laitteet toimitettiin ilmoitetussa aikataulussa, noin kymmenen päivän päästä tilauksesta.

Kontrollerin asennus virtuaalikoneelle

Ubiquiti Networksin SDN-kontrolleri (Software-Defined Networking) on Java-ohjelmointikielellä rakennettu ohjelmisto, jossa on myös WLAN-verkon kontrolleriominaisuus. Ohjelmisto vaatii toimiakseen käyttöjärjestelmän. Käyttöjärjestelmäksi käy moni Windows-, Linux- tai Mac OS -versio. [15.]

Organisaatiossa oli työtä aloittaessani Windows Server 2008 R2 -tasoinen palvelin, jossa oli käytössä Hyper-V ja muutamia virtuaalikoneita. Loin palvelimelle kontrolleria varten virtuaalikoneen, jonka käyttöjärjestelmäksi valitsin Linux Debian 8:n. Debian oli luonnollinen valinta, koska se on palvelinkäytössä erittäin luotettava ja monille Linux-käyttäjille tuttu. Kontrollerin asennus onnistui Linuxin päälle odotusten mukaan, kun noudatin Ubiquitin internetsivuilla olevia ohjeita. Kun kontrollerin asennus ja määrittelyt olivat valmiina, otin virtuaalikiintolevystä varmuuskopion organisaation verkkolevylle. Näin virtuaalikoneen saa tarvittaessa käynnistettyä toisella Hyper-V-palvelimella vikatilanteessa.

Kontrollerin määrittelyt

Vaatimusmäärittelyistä esiin nousseet tarpeet antoivat WLAN-verkon SSID:iden suunnitteluun hyvin suuntaviivoja. Tarvittiin kolme verkkoa: yksi täysin avoin ja erittäin rajoitettu vieraskäyttöön, toinen salasanalla suojattu (WPA2) yleiseen käyttöön ja kolmas henkilökunnan käyttöön. Suunnittelin henkilökunnan verkkoa alun perin 802.1X-todennusta käyttäväksi, mutta palomuurisääntöjen takia tähän verkkoon sijoitettiin myös muun muassa tulostimia ja langattomia kameroita. Kameroiden 802.1X-todennus olisi aiheuttanut hankaluuksia puutteellisten WLAN-ohjaimen ominaisuuksien vuoksi. Toteutin myös henkilökunnan verkon WPA2:lla. Tämän verkon esijaettu salasana oli erittäin vahva. [19.]

Avoimesta vierasverkosta sallin liikennöinnin ainoastaan internetiin rajoitetulla nopeudella. Myöhemmin haluttiin sallia liikenne myös tulkkausäänen palvelimelle. Määritin rajoitukset sekä kontrollerin asetuksissa että palomuurin pääsylistoissa. Estin päätelaitteiden välisen liikennöinnin ja rajoitin nopeudet kontrollerin asetuksissa. Näin nopeusrajoitukset purisivat jo päätelaitteen ja tukiasemaradion välillä.

Suojatusta yleisverkosta sallin vierasverkkoa suuremman nopeuden verkkoon. Määrittelin yleisverkosta pääsyn useaan lähiverkon palveluun; sallin muun muassa kopiokoneen käytön. Valitsin käyttöön WPA2-salauksen ja asetin muistettavissa olevan salasanan.

Henkilökunnan käytössä olevaan verkkoon en tehnyt nopeusrajoituksia. Palomuurin pääsylistoihin ei tarvinnut koskea, sillä ne olivat jo valmiiksi halutulla tavalla. Salaukseksi valitsin WPA2:n, johon asetin pitkän ja vaikean salasanan. Salasanan ei tarvitse olla muistettava, sillä sitä tarvitaan ainoastaan harvoin, kun otetaan käyttöön uusia laitteita.

Tukiasemien asentaminen ja kevyt testaus

Tukiasemien fyysinen asentaminen vei paljon aikaa. Aloitin asentamisen kontrollerin määrittelyn jälkeen. Olin suunnitellut asennuksen pääosin valmiiksi esikartoitusten pohjalta, eikä yllätyksiä tullut. Joissakin tiloissa valittiin tietoisesti tavallista huonompi paikka tukiasemalle, jotta sain asennuksesta huomaamattoman. Joissakin tiloissa pystyin asentamaan tukiasemat suoraan alas lasketun katon villalevyihin. Tällöin on helpompaa selvittää vikatilanteita. Myös signaalin turha vaimeneminen asennuspaikan takia on pienempi, kun tukiasema on näkyvissä ja se ikään kuin kelluu vapaasti ilmassa. [19.]

Joissakin tiloissa olisi ollut tarpeen rakentaa uutta yleiskaapelointia, mutta vähäisten resurssien takia en voinut lisätä kaapelointia. Ratkaisuna kokeilin ketjuttaa viereiseen tilaan asennetun tukiaseman yhteyden tavallisella pitkällä cat-kaapelilla. Ennen ketjutettua tukiasemaa piti kaapelin väliin lisätä PoE-injektori. Kun tukiasemia ketjutetaan kaapelilla, PoE-sähkö ei kulje laitteen läpi. Siksi linjaan on aina lisättävä PoE-injektori ennen seuraavaa laitetta. [15.]

Kun kaikki päärakennuksen tukiasemat olivat paikallaan, testasin ne kevyesti. Testaukseen en käyttänyt erityisiä testauslaitteita enkä käyttänyt standardoituja menetelmiä osin laitteistojen, osin ajan puutteen vuoksi. Testasin jokaisen tukiaseman aluksi erikseen siten, että ainoastaan yksi tukiasema kerrallaan oli kytketty käyttöön. Jokaisen tukiaseman kohdalla testasin liittymisen kaikkiin verkkoihin ja IP-osoitteen saamisen oikealta alueelta. Tein nopeustestin lataamalla suurikokoisen tiedoston paikalliselta tiedostopalvelimelta. Varmistin, että salaukset toimivat asianmukaisesti. Päätelaitteiden välisen liikennöinnin estoa koestin vain vierasverkossa. Kaikki tukiasemat toimivat oikein yhtä lukuun ottamatta. Viaksi paljastui väärin konfiguroitu kytkinportti. [19.]

Yksittäistestauksen jälkeen kytkin kaikki tukiasemat verkkoon ja testasin vaelluksen (roaming) toimivuutta. Testaukseen käytin tablettitietokoneen videopuhelua matkapuhelimeen, jonka yhteys oli muodostettu mobiilidataverkon kautta. Tukiaseman vaihtuessa esiintyi pieniä ylimääräisiä viiveitä, mutta videopuhelu ei katkennut käydessäni eri tiloissa. Myös peittoalueessa olevat ongelmat olisivat tulleet esille kattavassa vaellustestissä. [19.]

Langattoman sillan asennus rakennusten väliin

Päärakennuksesta ei ollut muuta yhteyttä sivurakennukseen kuin teleoperaattorin vanha puhelinverkko. Uusi yhteys päätettiin toteuttaa langattomalla sillalla. Suunnitellessani sillan toteutustapaa ja laitteistoa totesin, että olisi järkevintä käyttää Ubiquiti Networksin edullisia laitteita, koska niistä minulla oli hyviä kokemuksia. Ne toimivat täysin läpinäkyvinä verkolle, joten muutama käytössä oleva VLAN ei tuottaisi vaikeuksia eikä sivurakennukseen tarvittaisi omaa reititintä. [15; 19.]

Sillan linkkilaitteet toimivat PoE-sähköllä. Suurin työ asennusvaiheessa oli rakentaa cat6-kaapeli päärakennuksen laitetilasta ulkoseinälle ja sivurakennuksessa ulkoseinältä ensimmäisen tukiaseman luokse. Kaapelien rakentamisen jälkeen asensin siltalinkin laitteet rakennusten ulkoseiniin, noin neljän metrin korkeudelle. Valitsin seinäasennuksen muun muassa siksi, että katolla työskentely olisi vaatinut henkilönostimen käyttöä, eikä valmista mastoa ollut. Seinäasennusta pidettiin esteettisesti ainoana mahdollisuutena. Rakennusten välissä on suora näköyhteys ja etäisyyttä noin 100 metriä, joten muutama puu ei heikentänyt yhteyden laatua. Lähetystehoa piti jopa laskea reilusti oletusarvoista, jotta signaali ei olisi liian voimakas. [15; 19.]

Päärakennuksessa syötin linkin PoE-sähkön laitetilasta erillisellä PoE-injektorilla, sillä linkkiradio käyttää 24 V:n jännitettä. Sivurakennuksessa cat-kaapeli tulee suoraan linkkiradiolta tukiasemalle, joka on sijoitettu kaapelihyllylle pistorasian viereen. Samasta pisteestä syötetään sähkö passiivisilla PoE-injektoreilla linkkiradiolle ja kahdelle tukiasemalle. Ketjutin tukiasemat toisiinsa samalla tavoin kuin päärakennuksessa aiemmin. [15; 19.]

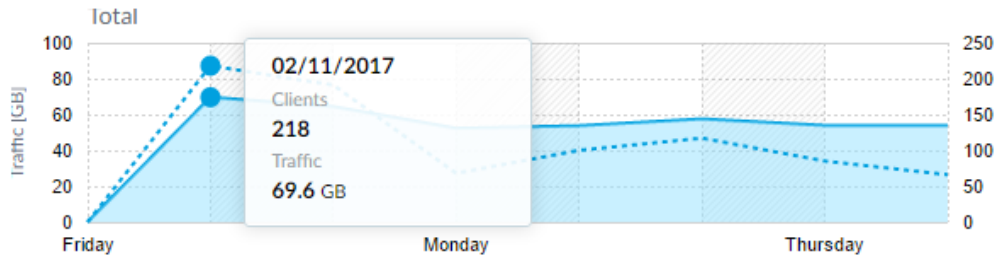
4.3 Testausvaihe

Suorituskyvyn mittaukset

Ensimmäinen kiinnostava testauksen kohde oli uuden, juuri toteutetun WLAN-verkon suorituskyky rasitustilanteessa. Osaako verkko jakaa käyttäjät tasaisesti tukiasemien kesken? Riittääkö kapasiteetti, vai muuttuuko verkko kuormituksessa käyttökelvottomaksi? [19.]

WLAN-verkon rasitusta on vaikeaa testata keinotekoisesti ilman kalliita testauslaitteita tai suurta päätelaitemäärää. Suuren päätelaitemäärän sain verkkoon järjestämällä tiedotuksen käytössä olevasta vierasverkosta suuren yleisötilaisuuden yhteydessä. [19.]

Kuvasta 4 voidaan havaita, että verkossa oli yli 200 samanaikaista käyttäjää kuormituksen varsinaisena testauspäivänä. Myös liikennettä oli paljon. Kun pyysin palautetta käyttäjiltä, kävi ilmi, että verkko oli toiminut hyvin eikä erityistä hidastelua ollut havaittu. Tarkastelin myös kontrollerin tilastoja tukiasemien käytöstä. Mikään tukiasema ei ollut kerännyt merkittävästi enempää käyttäjiä kuin muut alueen tukiasemat. Myös 15 minuutin keskiarvolle pyöristetyt tukiasemaradioiden käyttöasteet olivat kohtuulliset, reilusti alle 50 prosenttia. Kuvasta voi havaita myös valvontakameroiden aiheuttaman liikennemäärän.



Kuva 4. WLAN-kontrollerin tilastosivu. Yhtenäinen viiva kuvaa tietoliikenteen ja katkoviiva päätelaitteiden määrää. Pystysarake kuvaa yhtä viikonpäivää.

Edellä esitetyistä havainnoista päättelimme yhdessä organisaation edustajan kanssa, että kuormituksen jakaminen toimi ja että suorituskyky oli testausmahdollisuuksien rajoissa riittävä.

Testasin kuormitettuina olleiden tukiasemien suorituskykyä pistemäisillä mittauksilla. Testit toteutin speedtest.net-internetpalvelulla ja lataamalla suurikokoista testitiedostoa tiedostopalvelimelta SMB-yhteydellä (Server Message Block). Tiedostopalvelimelta hakemani testipaketin latausnopeus vaihteli välillä 60–450 Mbit/s. Tätä voidaan pitää erinomaisena suorituksena, kun verkossa oli paljon muitakin käyttäjiä. Kuormittamatonta tukiasemaa testatessani vaihteli latausnopeus tiedostopalvelimelta välillä 300–600 Mbit/s. Tätäkin voidaan pitää erittäin hyvänä saavutuksena langattomalle verkolle. [19.]

Radioiden ja kiinteän verkon riittävyyden arviointi

Kiinteän verkon riittävyyttä arvioidessani otin huomioon, että lähiverkko kykeni kauttaaltaan vähintään 1 Gbit/s -siirtonopeuksiin. Verkossa ei ollut tiedostopalvelimen lisäksi muita palveluita, jotka olisivat vaatineet suurta kapasiteettia. En löytänyt tarvetta päätelaitteiden välisille yhteyksille, joten niiden vaikutusta ei tarvinnut huomioida. WLAN-verkon aiheuttamiin liikennemääriin nähden totesin kiinteän verkon kapasiteetin riittävän erittäin hyvin. [19.]

Radioverkon riittävyyden analysoinnin perusteita olen luetellut jo aiemmin tässä luvussa. Voidaan todeta, että 200 päätelaitetta liittyi ongelmattomasti verkkoon, kuten vaatimuksissa oli määritelty. Oletettavasti verkko kestäisi hyvin myös 400 päätelaitetta. [19.]

Kevyt turvallisuustestaus

Liityttyäni eri WLAN-verkkoihin varmistin palomuurin pääsylistojen toimivuuden. Tarkistin, että jokaisesta verkosta pystyy muodostamaan yhteyden tarkoituksenmukaisiin sallittuihin laitteisiin ja palveluihin. [19.]

Varmistin WLAN-verkon radiorajapinnan määrittelyjen ja konfiguraation yhdenmukaisuuden. Koin fyysisen tason WPA2-salauksen turvallisuustestauksen merkityksettömäksi, koska siinä käytettävä AES on vielä murtamaton. [19.]

Vaeltamisen testaus

Testasin vaeltamisen (roaming) kahteen kertaan, kahdella eri tavalla. Avasin ensimmäistä testiä luvussa 4.3. Loin testissä videopuheluyhteyden WLAN-verkossa vaeltavan ja 4G-verkossa pysyvän laitteen välille. Toisessa testissä loin videopuheluyhteyden tablettitietokoneen ja kannettavan tietokoneen välille. Vaelsin ympäri kiinteistöä, päätelaitteet olivat fyysisesti eri tukiasemien peittoalueilla. Kannettavalla tietokoneella oli käynnissä myös jatkuva ping-pyyntö tiedostopalvelimelle, jotta pystyin arvioimaan vaeltaessa syntyviä verkon sisäisiä viiveitä. [19.]

Päärakennuksen sisällä vaeltaessani videopuhelu ei katkennut, mutta välillä siihen tuli pitkiä viiveitä tukiaseman vaihtuessa. Muutamia poikkeuksia lukuun ottamatta paketteja ei hävinnyt, mutta ping-vastauksen viive kasvoi hetkellisesti, kun tukiasema vaihtui. Tyypillinen hetkellinen ping-pyynnön viive muuttui 1–2 millisekunnista 100–2000 millisekuntiin. [19.]

Loppupäätelmänä vaeltamisen testauksesta voin todeta, että ominaisuus ei valitulla laitteistolla toiminut vielä aivan niin hyvin, kuin voisi toivoa. Vaeltaminen onnistuu ja konsepti toimii, mutta viivekriittiset palvelut eivät toimi kunnolla. Kohdeorganisaatiolle vaeltamisesta ei ole muuta hyötyä kuin aina parhaan mahdollisen signaalin löytyminen, joten tukiaseman vaihdosta johtuvan viiveen hetkellisestä kasvamisesta ei ole haittaa. [19.]

Olen havainnollistanut tietokoneen vaeltaessa tekemääni ping-testiä liitteessä 1. Ping-vastauksista näkee selvästi kohdat, joissa tukiasema vaihtui. Tein testin alueella, jolla on paljon tukiasemia. Vastausten viive on tukiasemaa vaihtaessa huomattavasti suurempi kantoalueen äärilaidoilla ja alueilla, joilla tukiasemia on vähän.

Langattoman sillan suorituskyky ja luotettavuus

Testatessani langattoman sillan suorituskykyä käytin pitkälti samoja menetelmiä kuin päärakennuksen sisäisen verkon kohdalla. Ladatessani tiedostoa tiedostopalvelimelta nopeus vaihteli välillä 80–130 Mbit/s. Sillan takana olevassa verkossa oli testausajankohtana kiinni kolme laitetta, joten en pystynyt suorittamaan suuren kuormituksen testausta.

Sillan luotettavuutta testasin jättämällä tietokoneen viikonlopuksi sivurakennukseen suorittamaan jatkuvaa ping-pyyntöä. Kahden testauspäivän jälkeen vain yksi paketti oli hävinnyt, joten totesin sivurakennuksen verkon luotettavuuden vastaavan täysin toivottua tasoa.

Kuvakaappaus sillan luotettavuustestin ping-statistiikan lopputiedoista on esitetty liitteessä 2.

4.4 Dokumentointi ja kustannusten arviointi

Ylläpitoon tarvittava dokumentaatio

Dokumentoinnin tasoa määritettäessä päätettiin, että dokumentoisin kaiken oleellisen fyysisten vikojen korjausta helpottavan tiedon ja kontrollerilla tapahtuvaa satunnaista ylläpitoa tukevan tiedon. Tämä opinnäytetyö toimii kattavana osana dokumentaatiota, joten tuotettavat lisädokumentit olivat opinnäytetyötä tukevia yksittäisiä dokumentteja. Nämä lisädokumentit sisältävät yleiskaapeloinnin kytkennät, laitteiden sijainnit ja konfiguraatiot, tarvittavat salasanat ja keskeiset asetukset, laitetilauksen lähetyslistan, hieman testauspöytäkirjoja sekä yksittäisten laitteiden konfiguraatiodokumentteja (esimerkiksi siltalinkin laitteet).

Kävin dokumentaation läpi organisaation edustajan kanssa. Totesimme sen riittäväksi.

Olen dokumentoinut kytkinten tukiasemaporttien konfiguroinnin liitteeseen 3. Käsittelen ohjeessa Ciscon ja HP:n kytkinten konfiguraatiota, sillä valtaosa organisaation kytkimistä oli niiden valmistamia.

Liitteeseen 4 olen tallentanut siltalinkin tärkeimmät parametrit. Luonnollisesti en julkaissut verkon yksilöiviä tai todennukseen liittyviä tietoja tässä työssä.

Toteutuneiden kustannusten arviointi

Toteutuneiden kustannusten arviointi oli oleellinen osa insinöörityöni aiheena ollutta projektia, sillä eräs keskeinen vaatimus oli äärimmäinen kustannustehokkuus. Projektin laitehankintoihin oli budjetoitu 6 000 euroa. Tätä summaa pidettiin pienenä suhteessa tavoitteisiin, mutta onnistumista pidettiin mahdollisena. Budjetin alakohdat olivat laitteiden hankinta, laitteiden asennus, muun verkon valmistelevat toimenpiteet ja varaus uuden PoE-kytkimen hankintaan.

Laitteiden hankintaan kului toimituskuluineen noin 3 600 euroa. Tämä sisälsi 25 tukiasemaa ja siltalinkin molemmat päät. Asennuskulut olivat noin 1 100 euroa. Tähän sisältyi uusia cat6-kytkentäkaapeleita, PoE-injektoreita, kaapelilistoja ja asennusten pientarvikkeita. Kontrollerin kulut olivat 0 euroa, koska pystyin hyödyntämään olemassa olevia palvelimia. En hankkinut uutta 48-porttista PoE-kytkintä, vaan ostin useammalle tukiasemalle PoE-injektorit syöttämään sähköä.

Koko projektin kulut olivat yhteensä 4 700 euroa, mitä voi pitää erinomaisena saavutuksena. Pysyin budjetissa reilulla plussatuloksella, ja sain toteutettua kaikki halutut asiat mallikelpoisesti. Rahankäytössä pitää huomioida työvoimakulujen puuttuminen. Jos vastaavan työn teettää ostopalveluna tai edes osittain ulkoistettuna, nousevat kulut huomattavan paljon.

5 Yhteenveto

Insinöörityön tekeminen oli suurilta osin opitun teoriatiedon soveltamista käytäntöön. Tietoa etsiessä huomasin, että monessa vanhemmassa lähteessä oleva tieto on niin vanhaa, että sillä ei ole enää merkitystä rakennettaessa uusia verkkoja. Historiaan perehtyminen on kiinnostavaa, mutta se ei auta nykyaikaisen verkon rakentamisessa.

Langattomat lähiverkot ovat kehittyneet paljon viimeisen 30 vuoden aikana. Langattomuuden alkuaikoina hinnat olivat kohtuuttomia ja verkkojen suorituskyky oli heikko. Standardeja ei ollut. Vähitellen standardeja on saatu luotua ja laitteistojen suorituskyky on kehittynyt hintojen samalla laskiessa. Nykyään erittäin suorituskykyisten verkkolaitteiden hinnat ovat edullisia ja kaikissa päätelaitteissa on valmiiksi asennettuna laadukas langaton verkkokortti. Epäilemättä nykypäivän standardit ovat riittämättömiä ja vanhentuneita 10–15 vuoden päästä, mutta on hyvä, että kehitys etenee.

Langattomilla verkkolaitteilla voidaan rakentaa nykyään myös edullisia langattomia siltoja. Silloilla voidaan yhdistää esimerkiksi rakennusten tai kampusten verkkoja toisiinsa. Sillan kustannukset ovat pienet verrattuna perinteiseen operaattorilta vuokrattuun valokuitu- tai datayhteyteen. Saatavilla olevat laitteet ovat erittäin suorituskykyisiä, saavutettava nopeus voi olla jopa useita gigabittejä sekunnissa.

Projektin onnistuneeseen toteutukseen on monta avainta, tärkeintä on kuitenkin tehdä vaatimusmäärittelyt ja katselmukset kunnolla heti alussa. Mikäli näin ei tehdä, suunnitelmat ja toteutus epäonnistuvat lähes varmasti. Projektia suunnitellessani oli selvää, että pohjatyöt tehdään hyvin. Päätin myös panostaa laadukkaaseen dokumentaatioon.

Aloittaessani tätä insinöörityötä kohdeorganisaation WLAN-verkon kunto oli huono. Verkossa oli vanhentuneita, tarkoitukseensa sopimattomia laitteita, eikä yksikään käyttäjä ollut tyytyväinen vallitsevaan tilanteeseen. Lisäksi oli suunniteltu toteutettavaksi paljon uusia WLAN-verkossa tarjottavia palveluita, mutta niitä ei olisi pystytty tarjoamaan verkon huonon kunnon takia.

Työ lähti etenemään selkeästi ja projektimaisesti. Aluksi tutustuin laajaan teoriamateriaaliin, joka yhdistyi aikaisempaan tietoon ja osaamiseen. Tältä pohjalta aloitin suunnittelun.

Suunnitteluvaiheen alussa tehtiin vaatimusmäärittelyjä, kartoituksia ja katselmuksia. Vaatimusmäärittelyiden onnistuminen johti siihen, että tekemistäni suunnitelmista tuli realistisia ja riittävän kattavia. Suunnittelussa pyrin mahdollisimman uuden teknologian käyttöönottoon siten, että toteutus olisi joustava ja skaalautuva. Suunnitteluvaiheen jälkeen tilasin ja asensin laitteet. Asennusdokumenteista sain käyttökelpoisen pohjan loppudokumentaatiolle.

Lopputestauksissa sain testattua kaikki oleellisimmat asiat, joita verkossa haluttiin kehittää. Testauksien jälkeen organisaation edustajat olivat vaikuttuneita verkossa tapahtuneista muutoksista. Verkon suorituskyvystä tuli erinomainen kaikissa oleellisissa tiloissa, ja verkko kattaa aukottomasti koko kiinteistön alueen. Myös sivurakennukseen saatiin toimiva langaton lähiverkko. Verkko ei häiriinny suurestakaan kuormituksesta. Kokonaisuudesta tuli joustava ja vikasietoinen.

Toteuttamaani verkkoa on tarvittaessa helppo kehittää, kunhan käytetään saman laitevalmistajan tuotteita. Kapasiteettia pystyy kasvattamaan lisäämällä verkkoon uusia tukiasemia, ja suorituskykyä on mahdollista parantaa uudemmilla tukiasemilla.

Verkon toteutuksessa päästiin haluttuihin tavoitteisiin, ja alun perin erittäin tiukkana pidetty hankintabudjetti jopa alitettiin reilusti.

Lähteet

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

2 Motorola upgrades Altair wireless ethernet speed 70%. 1992. Verkkodokumentti. Computer Business Review. <http://www.cbronline.com/news/motorola_upgrades_altair_wireless_ethernet_speed_70/>. Luotu 9.11.1992. Luettu 12.1.2017.

3 WLAN 802.11n: From SISO to MIMO. 2013. Verkkodokumentti. Rohde & Schwarz. <https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma179/1MA179_10e_WLAN80211n_from_SISO_to_MIMO.pdf>. Luotu 26.4.2013. Luettu 12.1.2017.

4 Arar, Yardena. 2006. PC World Analysis: Deconstructing the Draft 802.11n Wi-Fi Hype. Verkkodokumentti. <http://www.pcworld.com/article/125612/article.html>. Luotu 2.3.2006. Luettu 12.1.2017.

5 Cisco 802.11ac Wave 2 FAQ. 2015. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html>. Päivitetty 23.12.2015. Luettu 12.1.2017.

6 IEEE 802.11ac: What Does it Mean for Test? 2013. Verkkodokumentti. Litepoint. <http://litepoint.com/whitepaper/80211ac_Whitepaper.pdf>. Luotu 1.10.2013. Luettu 12.1.2017.

7 Kassner, Michael. 2007. 802.11n, MIMO, and multipath environments. Verkkodokumentti. <http://www.techrepublic.com/blog/mobile-enterprise/80211n-mimo-and-multipath-environments/>. Luotu 11.11.2007. Luettu 12.1.2017.

8 Ketonen, Veli-Pekka. 2014. Wi-Fi / WLAN Performance Management and Optimization. Verkkodokumentti. <https://www.surf.nl/binaries/content/assets/surf/nl/2014/3-juni-2014_wi-fi-summit_veli-pekka-ketonen_wi-fi-performance-optimization.pdf>. Luotu 3.6.2014. Luettu 13.1.2017.

9 Gast, Matthew S. 2013. 208.11ac: A Survival Guide. Sebastopol, California: O'Reilly Media.

10 PoE Explained. 2008. Verkkodokumentti. Veracity. <http://www.veracityglobal.com/media/27197/vwp-002%20poe%20explained.pdf>. Luotu 11.12.2008. Luettu 13.1.2017.

11 Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020. 2014. Verkkodokumentti. Statista. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>. Luotu 2014. Luettu 13.1.2017.

12 Defeating Evil Twin attacks. 2009. Verkkodokumentti. TechTarget. <http://search-security.techtarget.com/feature/Defeating-Evil-Twin-attacks>. Luotu 1.6.2009. Luettu 18.1.2017.

13 IEEE 802.11i-2004. 2004. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/IEEE_802.11i-2004>. Päivitetty 18.1.2017. Luettu 19.1.2017.

14 Approximating Maximum Clients per Access Point. 2016. Verkkodokumentti. Cisco Meraki. <https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Approximating_Maximum_Clients_per_Access_Point>. Luotu 23.3.2016. Luettu 19.1.2017.

15 UniFi Products. 2017. Verkkodokumentti. Ubiquiti Networks. <https://www.ubnt.com/products/>. Päivitetty 2017. Luettu 19.1.2017.

16 Koivumäki, Antti. 2013. Radioyhteys: Perusteita. Verkkodokumentti. <http://users.metropolia.fi/~koiva/S2013/TT12S1E-TLT/radioyhteys.pdf>. Luotu 2013. Luettu 1.3.2017.

17 Geier, Jim. 2005. Langattomat verkot. Helsinki: Edita.

18 Martti, Tapani. 2015. Tietojärjestelmien suunnittelu ja määrittely sekä tietojärjestelmähanke. Luentomateriaali 23.3.2015. Metropolia Ammattikorkeakoulu.

19 Geier, Jim. 2015. Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications. Indianapolis, Indiana: Cisco Press.

20 Rouse, Margaret. 2014. Confidentiality, integrity, and availability (CIA triad). Verkkodokumentti. <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>. Päivitetty 1.11.2014. Luettu 13.3.2017.

21 WLAN-tukiasemien hintavertailu. 2015. Verkkodokumentti. Hinta.fi. <https://hinta.fi/977540>. Päivitetty 28.2.2017. Luettu 1.3.2017.

Vaeltaessa tehty ping-testi

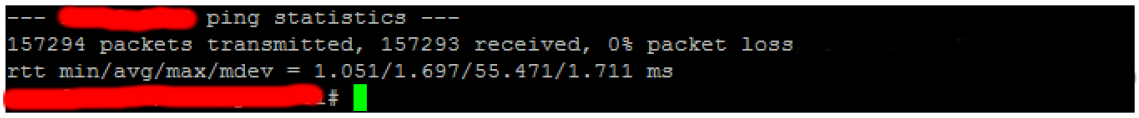
Nopean vaellustestin supistettu tulos. Pitkä tasaisten ping-vastausten sarja on lyhennetty kolmeksi pisteeksi (…).

Pinging 10.10.77.200 with 32 bytes of data:
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=3ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time<1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time<1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
...
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=3ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=131ms TTL=63
Reply from 10.10.77.200: bytes=32 time=97ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
…
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=57ms TTL=63
Reply from 10.10.77.200: bytes=32 time=268ms TTL=63
Reply from 10.10.77.200: bytes=32 time=91ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
…

Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=1ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=45ms TTL=63
Reply from 10.10.77.200: bytes=32 time=258ms TTL=63
Reply from 10.10.77.200: bytes=32 time=154ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63
Reply from 10.10.77.200: bytes=32 time=2ms TTL=63

Sivurakennuksen ping-testi

Ruudunkaappaus viikonlopun yli kestäneen ping-pyyntöjen lähetyksen ja vastaanoton tilastoista osana sivurakennuksen verkon testaamista.



Tukiasemaportin konfigurointi HP:n ja Ciscon laitteisiin

Tukiasemaportin konfiguraatio on oleellinen tieto vaihdettaessa rikkoutunutta kytkintä uuteen. Luonnollisesti on tärkeää sallia kaikki tarpeelliset VLANit trunkin läpi. Lisäksi hallintaverkon VLAN pitää asettaa natiiviksi tai untaggediksi, jotta tukiasemat saavat IP-osoitteen oikeasta aliverkosta.

HP:n laitteessa portit 19–20 on konfiguroitu tukiasemakäyttöön ja portit 21–24 ovat trunk-portteja:

```
vlan 77
   name "hallinta"
   untagged 19-20
   tagged 21-24
   exit
vlan 70
   name "henkilokunta"
   untagged 1-18
   tagged 19-24
   exit
vlan 76
   name "peruswlan"
   tagged 19-24
   exit
vlan 73
   name "vieras"
   tagged 19-24
   exit
```

Ciscon kytkimissä riittää pelkän portin konfiguraatio:

```
interface GigabitEthernet1/0/20
switchport trunk native vlan 77
switchport trunk allowed vlan 70,73,76,77
switchport mode trunk
spanning-tree portfast
```

Siltalinkin parametrit

Päärakennus:
Mode: Station
IP-osoite: xxx
SSID: xxx
SSID broadcast: pois
WLAN-suojausavain: xxx
AirMax: päällä
Tx Power: 13 dBm

Sivurakennus:
Mode: Client
IP-osoite: xxx
SSID: xxx
SSID broadcast: pois
WLAN-suojausavain: xxx
AirMax: päällä
Tx Power: 13 dBm

Lähetystehoa on vielä varaa nostaa tarvittaessa. Sisäänrakennetun antennin vahvistus on 13 dB. Kun 5 GHz alueen sallittu lähetysteho on 30 dBm, voidaan lähetystehoa nostaa vielä 4 dBm, koska 30 dBm–13 dBm–13 dB=4 dBm.
Tällä hetkellä lähetystehoa ei ole syytä nostaa, koska vastaanottotehon voimakkuus on linkin kummassakin päässä –56 dBm, joka mahdollistaa parhaan tuetun nopeuden hyvällä marginaalilla.