Toomas Ristola

PILVIPOHJAINEN LANGATON VERKKO
RUCKUS CLOUD

Opinnäytetyö

Insinööri (AMK)

Tieto- ja viestintätekniikan koulutus

2021

Kaakkois-Suomen
ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Toomas Ristola
Työn nimi	Pilvipohjainen langaton verkko Ruckus Cloud
Toimeksiantaja	Autosalpa Oy
Vuosi	2021
Sivut	41 sivua, liitteitä 0 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on tutustua Ruckus Cloud -pilvialustaan ja suunnitella ja toteuttaa käyttöönotto yrityksen langattomaan verkkoon käyttäen kyseistä pilvialustaa. Langattomasta verkosta on myös tarkoitus tehdä nykyistä verkkoa tietoturvallisempi käyttäen ratkaisuna 802.1X-protokollaa, joka mahdollistaa käyttäjien autentikoinnin.

Ruckus Cloud mahdollistaa keskitetyn hallinnan yrityksen langattomaan verkkoon. Se tuo uusia työkaluja verkon hallintaan sekä analytiikkaan ja helpottaa verkon ylläpitoa ja ongelmatilanteiden selvittämistä.

Työn teoriaosuudessa käytiin läpi langatonta verkkoa ja siihen liittyviä tekniikoita ja standardeja. Työn käytännön osuus aloitettiin tutkimalla, miten Ruckus Cloudin käyttöönotto tapahtuu ja mitä laitteita siihen tarvitaan. Tukiasemien liittäminen pilvihallintaan aloitettiin testausvaiheella ja sen onnistuttua siirryttiin ottamaan Ruckus Cloud käyttöön jokaisessa yrityksen toimipisteessä. Käyttöönoton jälkeen perehdyttiin 802.1X-protokollaan ja sen käyttöönottoon. 802.1X:n käyttöönotossa tarvittavat laitteet saatiin konfiguroitua sekä testausvaihe saatiin onnistuneesti suoritettua. Varsinaista 802.1X käyttöönottoa ei opinnäytetyössä saatu vielä tehtyä, koska se vaatii lisää suunnittelua, jotta mahdollisilta käyttökatkoilta vältyttäisiin.

Työn lopputuloksena oli onnistunut Ruckus Cloud -pilvihallinnan suunnittelu ja käyttöönotto helpottamaan yrityksen langattoman verkon hallintaa sekä parantamaan tietoturvallisuutta.

Asiasanat: langattomat lähiverkot, pilvipalvelut, 802.1X-protokolla

South-Eastern Finland University of Applied Sciences

Degree	Bachelor of Engineering
Author (authors)	Toomas Ristola
Thesis title	Cloud Managed Network Ruckus Cloud
Commissioned by	Autosalpa Oy
Time	May 2021
Pages	41 pages, 0 pages of appendices
Supervisor	Vesa Kankare

ABSTRACT

The purpose of this thesis was to become acquainted with a Ruckus Cloud platform and to design and implement a new wireless network for the company using Ruckus Cloud. The purpose was to make a more data secure WLAN using 802.1X authentication.

Ruckus Cloud enables centralized a network management for the company's wireless network. It brings new tools for network management and analytics and facilitates management and troubleshooting.

The theoretical framework of the thesis introduced the WLAN and its techniques and protocols. The practical part of the work started with examined how a Ruckus Cloud implementation happens and what devices are required for it. Connecting access points to the cloud started with testing and when it succeeded moved on connecting a company office's access points to the cloud. The implementation phase includes also studying and testing of 802.1X. All necessary devices were configured and testing was successfully completed but the actual implementation was left undone because it requires more planning.

The work resulted in a successful cloud management for design and deployment of using Ruckus Cloud solution to make wireless network management easier and more data secure.

Keywords: wireless local area networks, cloud services, 802.1X

SISÄLLYS

1 JOHDANTO

Langaton verkko on nykypäivänä hyvin yleinen niin kuluttajilla kuin yrityksissäkin sen joustavuuden ja helppouden takia. Laitteita pystytään liittämään verkkoon helposti ilman johtoja, jolloin pystytään liikkumaan huoneesta toiseen ilman yhteyden katkeamista. Tarpeeksi kattava langaton verkko koko rakennukseen vaatii myös useampia tukiasemia, jotta yhteys toimii moitteettomasti ilman suurempaa viivettä. Tukiasemien lisääntyessä verkon hallinta käy kuitenkin haastavammaksi ja enemmän aikaa vieväksi.

Pilvipohjaiset ratkaisut langattoman verkon hallintaan ovat oiva ratkaisu erityisesti yrityksille, kun tukiasemia voi olla jopa monia kymmeniä. Pilvipohjaiset alustat mahdollistavat verkon hallinnan yhdestä paikasta, eikä se vaadi lisää ylimääräisiä fyysisiä laitteita. Alustat mahdollistavat myös uusia työkaluja verkon hallintaan, analytiikkaan, turvallisuuteen sekä vikatilanteisiin.

Opinnäytetyön toimeksiantajana toimi Autosalpa Oy, joka on autoliike. Autosalpa Oy perustettiin vuonna 1957 Kouvolassa, ja se toimii seitsemällä eri paikkakunnalla.

Tämän opinnäytetyön tarkoituksena on rakentaa Autosalpa Oy:lle pilvi hallittava langaton verkko. Työssä kartoitetaan yrityksen nykyinen langaton verkko ja suunnitellaan sen pohjalta uusi ja turvallisempi verkko yrityksen tarpeisiin. Työ toteutetaan käyttäen Ruckus Cloud -pilvialustaa ja Ruckuksen tukiasemia.

1.1 Tutkimusongelma

Työn tutkimusongelmana oli selvittää, mitä Ruckus Cloud -pilvihallinnan käyttöönottoon tarvitaan, miten käyttöönotto toteutetaan yrityksen nykyiseen verkkoon ja miten nykyisestä verkosta tehdään turvallisempi. Opinnäytetyön tutkimuskysymyksiä ovat:

1. Mikä on Ruckus Cloud?
2. Mitä Ruckus Cloud pilvihallinnan käyttöönotto vaatii?

3. Mitä hyötyä Ruckus Cloud käyttöönotosta on?
4. Miten langattomasta verkosta saa turvallisemman?

1.2 Tutkimusmenetelmän valinta

Tutkimusmenetelmänä opinnäytetyössä toimii toiminnallinen opinnäytetyö ja tarkemmin projektityö. Projektityö tehdään organisaation sisällä, ja sille on asetettu määräaika sekä tavoitteet. Projektityyppinä toimii kehitysprojekti.

Salosen ja Virtasen (2011) mukaan projektityön tunnusmerkkejä ovat muun muassa, että työn tavoitteet on määritelty, työ on suunnittelu sekä projektin aikana on kehitetty uusi asia. Opinnäytetyössä tunnusmerkit täyttyvät, koska työssä on tavoitteena saada Ruckus Cloud käyttöön onnistuneesti. Käyttöönottoa on suunniteltu ja lopputuloksena saadaan organisaatiolle uusi asia helpottamaan langattoman verkon hallintaa. Onnistunut työ todetaan testaamalla langattoman verkon toimivuus toimipisteittäin.

2 WLAN

WLAN eli wireless local area network tarkoittaa suomeksi langatonta lähiverkkoa. Se tunnettaan myös IEEE 802.11 -standardina, joka kehitettiin 1990 luvun lopulla. Sen avulla pystytään liittämään päätelaitteita verkkoon langattomasti. (Puska 2005, 15.)

Langattoman verkon laitteet toimivat ISM-alueilla, mitkä ovat ITU:n (International Telecommunication Union) määrittelemiä radiotaajuuskaistoja. ISM-alueita on kolme, ja ne ovat 902 - 928 MHz, 2,400 - 2,4835 MHz sekä 5,725 - 5,875. Jokaiselle alueelle on määritelty EIRP (Effective Isotropically Radiated Power) eli maksimi lähetysteho, mikä voidaan lähettää radioantennista. EIRP arvo taajuudelle 2,4 GHz on 20dBm ja alueelle 5 GHz se on 23 - 36 dBm. (Eroglu 1998.)

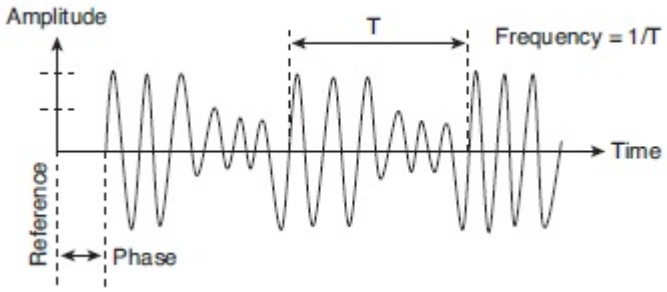
WLAN-tuotteiden yhteydessä tulee usein esille Wi-Fi, mikä on Wi-Fi Alliancen luoma langattoman verkon tekniikka, joka perustuu IEEE 802.11-standardiin. Sen tarkoituksena on luoda nopeampi yhteys ilman viivettä ja tehdä siitä

käyttäjälle helpompaa. Kaikki Wi-Fi-tavaramerkillä olevat laitteet ovat yhteensopivia keskenään. (Wi-Fi Alliance s.a.)

2.1 Radiosignaali

Langattoman verkon tekniikassa käytetään radioaaltoja kuljettamaan data ilmassa pitkin pisteeltä pisteelle. Radioaallot ovat sähkömagneettisia signaaleja, jotka ovat suunniteltu kuljettamaan tietoa ilmassa suhteellisen pitkiäkin matkoja. Radioaallot voivat kohdata matkalla erilaisia rakennuksia ja esteitä mitkä vaikuttavat signaalin nopeuteen sekä kuljettuun matkaan. (Cisco Press 2017.)

Radioaalloista käytetään myös nimitystä radiotaajuus eli RF-signaali (radio-frequency). Tekniikkaa on käytetty jo monien vuosien ajan apuna esimerkiksi FM-radioissa sekä TV-videolähetyksissä. RF-signaali koostuu amplitudi- sekä taajuus elementeistä. (kuva 1; Cisco Press 2017.)



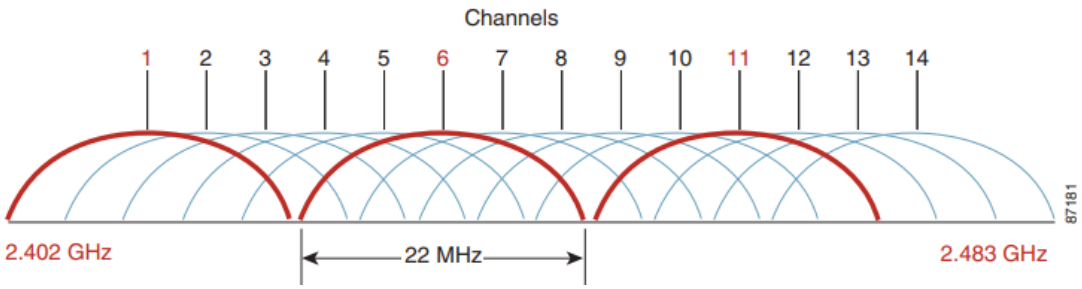
Kuva 1. Radioaalto (Cisco Press 2017)

RF-signaalissa amplitudi ilmaisee sen voimakkuuden. Sähkömagneettinen signaali tarvitsee tietyn määrän tehoa, jotta se pystyy kuljettamaan signaalin halutun matkan. Tehon kasvaessa myös signaalin kuljettu matka kasvaa. Amplitudin yksikkönä käytetään yleensä desibelimilliwattia (dBm). Signaalin taajuus ilmaisee sen, kuinka monta kertaa sekunnissa signaali toistaa itseään. Taajuuden yksikkö on hertsi (Hz). (Cisco Press 2017.)

2.2 Taajuudet ja kanavat

802.11 -standardin langattomat lähiverkot käyttävät yleisesti 2,4 GHz sekä 5 GHz -taajuusalueita. Poikkeuksina ovat jotkin standardit kuten 802.11ad, joka käyttää 60 GHz:n aluetta sekä 802.11ah, joka käyttää 900MHz:n aluetta. Taajuusalueet ovat radioaaltojen taajuuksia, joita käytetään datan lähettämiseen langattomassa spektrissä. Taajuusalueissa taajuudet jaetaan vielä eri kanaviin. (Riihikallio 2018.)

2,4GHz taajuusalue on suosituin ja käytetyin alue, koska melkein kaikki laitteet tukevat sitä. Alue toimii 2,400 - 2,483.5 MHz:n ISM-taajuusalueella. Laitteita, jotka käyttävät 2,4 GHz:n aluetta ovat esimerkiksi mikroaaltouuni, bluetooth-laitteet sekä langattomat puhelimet. Se tekee alueesta ruuhkaisen ja häiriöalttiin, mikä näkyy käyttäjillä laitteiden toimimattomuutena sekä hitautena. Taajuusalue on jaettu Euroopassa 13 eri kanavaan (kuva 3), jotka toimivat 2,400 - 2,4835 GHz:n ISM-alueella (Industrial, Scientific Medical). Kanavat on jaoteltu 5 MHz välein ja jokainen kanava on 22 MHz leveä. Näin ollen jotkut kanavat menevät päällekkäin, mikä voi häiritä niiden toimivuutta. Kanavat 1,6 ja 11 ovat toimivuudeltaan varmimpia, koska ne eivät mene toisten kanavien päälle (kuva 2). (Cisco s.a.)



Kuva 2. Kanavien jako (Cisco s.a.)

Taajuusalue (MHz)	Kanava
2401-2423	1
2406-2428	2
2411-2433	3
2416-2438	4
2421-2443	5
2426-2448	6
2431-2453	7
2436-2458	8
2441-2463	9
2446-2468	10
2451-2473	11
2456-2478	12
2461-2483	13

Kuva 3. 2,4 GHz:n taajuusalueen kanavat

Toinen taajuusalue, 5 GHz tuli käyttöön standardin 802.11a:n myötä. Taajuusalue toimii 5,180 - 5,700 GHz U-NII (Unlicensed National Information) alueella. 802.11n-standardin tullessa se tuki 2,4 GHz:n sekä 5 GHz:n taajuusalueita, jolloin myös 5 GHz -taajuudet alkoivat yleistyä käytössä. Taajuusalue on jaoteltu 5 MHz:n kanavoiksi (kuva 4), mutta vain joka neljäs kanava on käytössä eli jako on 20 MHz. Tämä poistaa kanavien päällekkäisyyden ja häiriöitä syntyy vähemmän kuin 2,4 GHz taajuusalueella. Kanavia 36-40 saa käyttää Euroopassa vain sisätiloissa. (Cisco s.a.)

Molempien taajuuksien ollessa saatavilla laite yhdistää ensisijaisesti 2,4 GHz taajuuteen, koska 5 GHz:n signaali ei läpäise seiniä yhtä hyvin kuin 2,4 GHz:n signaali. 5 GHz -taajuusalueella kapasiteetti datan tiedonsiirtoon on suurempi kuin 2,4 GHz:n alueella. (Cisco s.a.)

Taajuusalue (MHz)	Kanava
5180-5200	36
5200-5220	40
5220-5240	44
5240-5260	48
5260-5280	52
5280-5300	56
5300-5320	60
5320-5340	64
5500-5520	100
5520-5540	104
5540-5560	108
5560-5580	112
5580-5600	116
5600-5620	120
5620-5640	124
5640-5660	128
5660-5680	132
5680-5700	136
5700-5720	140

Kuva 4. 5 GHz:n taajuusalueen kanavat

2.3 OFDM

OFDM (Orthogonal Frequency Division Multiplexing) on monikantoaaltomodulointi tekniikka, mitä käytetään menetelmänä monissa tietoliikenneverkoissa. Erityisesti sitä käytetään langattomissa verkoissa sen hyvän häiriösietokyvyn sekä nopeuden vuoksi. Menetelmässä taajuusalueiden kanavat jaetaan vielä pienempiin alikanaviin, joissa data kuljetetaan. Alikanavat eivät häiritse toisiaan. OFDM-tekniikan avulla saadaan kuljetettua samalla taajuusalueella suurempi määrä dataa joka sekunti. (Perez-Neira & Campalans 2009, 151.)

2.4 OFDMA

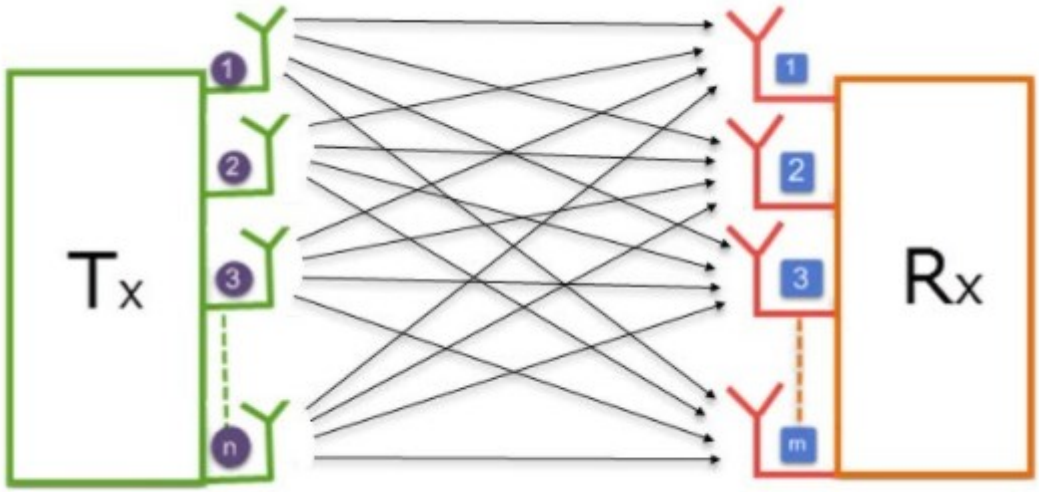
OFDMA (Orthogonal Frequency Division Multiple Access) on paranneltu versio OFDM menetelmästä. OFDMA parantaa langatonta verkkoa muodostamalla itsenäisesti moduloivia alikantoaaltoja taajuuksien sisällä. Tämä menetelmä mahdollistaa taajuuksien tehokkaamman käytön monien

käyttäjien kesken. OFDMA-tekniikkaa käytetään 802.11ax-standardissa (Wi-Fi 6). (Cisco s.a.)

2.5 MIMO

MIMO (multiple-input multiple-output) on radiotekniikassa käytetty menetelmä missä datan lähettämisessä sekä vastaanottamisessa käytetään useampia antenneja. Sitä on käytetty wlan-tekniikassa 802.11n-standardista lähtien luotettavuuden sekä suorituskyvyn parantamiseen. Tekniikassa lähettimessä esimerkiksi tukiasemassa sama data lähetetään käyttäen useita antenneja ja vastaanottimessa antennit vastaanottavat datan eri kulmista ja eri aikoina, mikä vähentää viivettä. (Intel 2021.)

Kuvassa 5 on havainnollistettu MIMO-tekniikkaa, Tx lähettää dataa ja Rx vastaanottaa dataa.



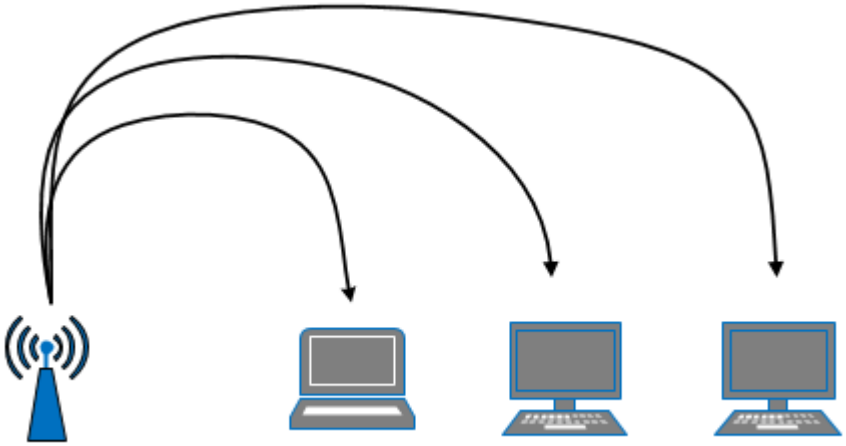
Kuva 5. MIMO-tekniikka (everythingRF 2019)

2.6 MU-MIMO

MU-MIMO (Multi-user Multiple-Input Multiple-Output) pystyy kommunikoimaan monien laitteiden kanssa samaan aikaan, kun aikaisempi tekniikka, MIMO pystyi kommunikoimaan vain yhden laitteen kanssa. MU-MIMO-tekniikkaa

aloitettiin käyttämään 802.11ac-standardissa, mutta se yleistyi 802.11ax:n tullessa käyttöön. Tekniikka lisää tiedonsiirron nopeutta erityisesti paikoissa, joissa langattoman verkon tarvitsevia ihmisiä on paljon, kuten lentokentillä tai stadioneilla. (Shaw 2018.)

Kuvassa 6 on esitetty MU-MIMO:n toimintaperiaatetta.



Kuva 6. MU-MIMO-toimintaperiaate

2.7 WLAN standardit

Yleisimmät standardit

WLAN-standardit ovat IEEE (Institue of Electrical and Electronics Engineers) kehittämiä tekniikoita, jotka määrittävät langattoman verkon arkkitehtuuria sekä tekniikoita. Langattoman verkon standardit tunnistaa 802.11 -alkuisesta nimeämisestä (kuva 7).

Ensimmäinen standardi 802.11 julkaistiin 1997, ja se käytti 2,4 GHz:n taajuusaluetta. Standardi tarjosi tiedonsiirtonopeudeksi vain 1 Mb/s tai 2 Mb/s. Se käytti FHSS:ää (Frequency Hopping Spread Spectrum) eli taajuushyppelyä kanavien välillä, jotta häiriöitä olisi mahdollisimman vähän. Toisena

menetelmänä oli DSSS (Direct Sequence Spread Spectrum) eli suorasekventointi, jossa datasignaali levitetään koko taajuusalueelle. (Guido ym. 2010.)

Vuonna 1999 julkaistiin 802.11a-standardi mikä käyttää 5 GHz:n taajuusaluetta ja mahdollistaa tiedonsiirron jopa 54 Mb/s:n nopeudella. Standardi käyttää OFDM-menetelmää. Samana vuonna julkaistiin myös 802.11b-standardi, joka käyttää samaa menetelmää kuin 802.11, DSSS. Standardi käyttää 2,4 GHz:n taajuusaluetta, ja sen korkein tiedonsiirtonopeus on 11 Mb/s. (Guido ym. 2010.)

Seuraava standardi 802.11g julkaistiin 2003 ja se mahdollisti saman tiedonsiirtonopeuden kuin 802.11a, mutta se käytti matalampaa taajuusaluetta, 2,4 GHz. (Guido ym. 2010).

Vuonna 2009 hyväksyttiin 802.11n, se oli ensimmäinen standardi mikä mahdollisti käyttämään sekä 2,4 GHz sekä 5 GHz taajuusalueita. Se käytti myös uutta MIMO (Multiple Input, Multiple Output) menetelmää tiedonsiirrossa ja nopeudet ylsivät jopa 600 Mb/s. (Guido ym. 2010.)

802.11ac standardi julkaistiin vuonna 2013 ja se on paranneltu versio standardista 802.11n. Tiedonsiirtonopeudet nousevat teoreettisesti jopa yli 3Gb/s, joten se on huomattavasti nopeampi kuin aikaisemmat standardit. Se käyttää MIMO-tekniikkaa sekä se toimii vain 5 GHz taajuusalueella. (Shaw 2020.)

Vuonna 2019 lanseerattiin seuraavan sukupolven WLAN-standardi 802.11ax. Se toimii 2,4 GHz- ja 5 GHz- taajuusalueilla ja mahdollistaa erittäin nopean tiedonsiirron jopa 10 Gb/s asti. Se käyttää mimo- ja ofdma tekniikoita. Standardi on luotettavampi häiriöitä vastaan. (Shaw 2020.)

Langattomien tietoverkkojen standardit

Standardi	Valmistumisvuosi	Taajuusalueet	Modulaatio	Kanavien kaistanleveys	Teoreettinen maksiminopeus	Tyypillinen kantama sisällä / ulkona
802.11	1997	2,4 GHz	dsss / fhss	22 MHz	2 Mb/s	20 / 100 m
802.11a	1999	5 GHz	ofdm	5 / 10 / 20 MHz	54 Mb/s	35 / 120 m
802.11b	1999	2,4 GHz	dsss	22 MHz	11 Mb/s	35 / 140 m
802.11g	2003	2,4 GHz	ofdm	5 / 10 / 20 MHz	54 Mb/s	38 / 140 m
802.11n	2009	2,4 / 5 GHz	mimo-ofdm	20 / 40 Mhz	600 Mb/s	70 / 250 m
802.11ac	2013	5 GHz	mimo-ofdm	20 / 40 / 80 / 160 MHz	3466 Mb/s	35 m / ei ilmoitettu
802.11ax	2019	2,4 / 5 / 6 GHz	mimo-ofdm	20 / 40 / 80 / 160 MHz	10,5 Gb/s	30 / 120 m

Kuva 7. Langattoman verkon standardit (Mikrobitti 2020)

Wi-Fi Alliance halusi selkeyttää 802.11 standardien nimeämistä ja kehitteli uuden nimeämistavan eri verkkotekniikoille. Esimerkiksi 802.11ac-standardista käytetään myös nimeä Wi-Fi 5 ja 802.11ax-standardista nimeä Wi-Fi 6 (kuva 8). Näin ollen käyttäjät ymmärtäisivät paremmin ja selkeämmin, mistä on kyse puhuttaessa langattoman verkon standardeista. Yhteensopivuusongelmien helpottamiseksi laitteissa ilmoitetaan, mitä standardia se tukee, joten käyttäjät voivat helpommin valita tarvitsemansa tuotteet. (Ostergaard 2019.)

802.11a	Wi-Fi 1	
802.11b	Wi-Fi 2	
802.11g	Wi-Fi 3	
802.11n	Wi-Fi 4	
802.11ac	Wi-Fi 5	
802.11ax	Wi-Fi 6	

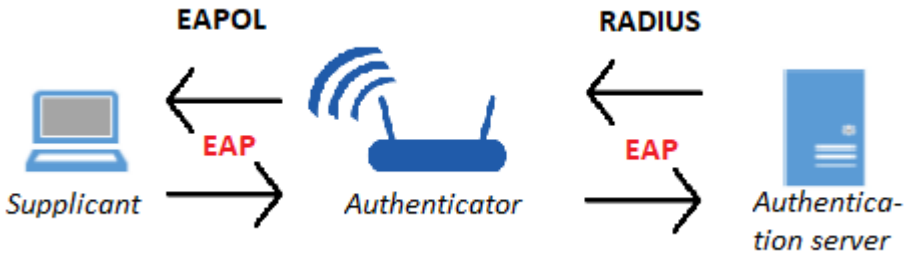
Kuva 8. Langattoman verkon standardit (Wi-Fi Alliance s.a.)

2.7.1 IEEE 802.1X-standardi

IEEE 802.1X-standardi on lähiverkoissa toimiva suojaustapa, mikä käyttää porttikohtaista todentamista asiakkaan sekä palvelimen välillä. Standardin tarkoituksena on estää luvattomien käyttäjien ja laitteiden pääsy verkkoon. 802.1X toimii sekä langattomissa (WLAN) että langallisissa (LAN) verkoissa. (Cisco 2016.)

802.1X tarvitsee toimiakseen kolme komponenttia, jotka ovat: asiakas (supplicant), todentaja (authenticator) sekä autentikointipalvelin (authentication server). Asiakkaana toimii käyttäjä, joka haluaa päästä verkkoon omalla laitteellaan. Todentajana toimii langattomissa verkoissa tukiasema ja langallisissa verkoissa kytkin. Autentikointipalvelimena voidaan käyttää Windowsin RADIUS-palvelinta tai jotain muuta palvelinta, joka kykenee käyttäjätodennukseen. (Cisco 2016.)

Käyttäjän todennus tapahtuu siten, että asiakas haluaa liittää laitteensa verkkoon, jolloin laitteen ja todentajan välillä käynnistyy EAPOL ja todentaja lähettää EAP-pyynnön asiakkaalle. Asiakas vastaa tähän kirjautumalla käyttäjätunnuksillaan, jolloin todentaja kommunikoi autentikointipalvelimen kanssa (kuva 9). Jos käyttäjä löytyy autentikointipalvelimen sallittujen listalta, käyttäjä pääsee verkkoon, muussa tapauksessa verkkoon pääsy evätään. (Cisco 2016.)



Kuva 9. 802.1X-autentikoinnin toiminta

2.8 EAP

Extensible Authentication Protocol(EAP) on viitekehys varsinaisiin todennusmenetelmiin. EAP-protokollaa käytetään todennukseen langattomissa verkoissa, missä käytetään 802.1X autentikointia. EAP-protokollaa käytetään myös langallisissa ja PPP (Point to Point Protocol) yhteyksissä. EAP kuljettaa varsinaisen todennusmenetelmän, joita ovat mm. EAP-TLS, PEAP sekä EAP-TTLS. (Microsoft 2020.)

2.9 EAPOL

Extensible Authentication Protocol Over LAN (EAPOL) on paketointitekniikka 802.1X-standardissa, jotta EAP-viestit pystytään kuljettamaan turvallisesti. EAPOL tukee langattomia- ja Ethernet-verkkoja, ja se toimii pääsääntöisesti asiakaslaitteen ja todentajan välillä. (Vocal Technologies s.a.)

2.10 RADIUS

Remote Authentication Dial-In User Service (RADIUS) on protokolla, joka esiteltiin vuonna 1991. Sitä käytetään todentamaan ja valtuuttamaan käyttäjien ja laitteiden pääsy verkkoon. Protokollaa voidaan käyttää AAA-menetelmän (Authentication, Authorization, Accounting) toteutukseen eli käyttäjän autentikointi, valtuutus ja tilastointi. Protokollassa NAS (Network Access Service), WLAN-tukiasema tai kytkin, toimii RADIUS-asiakkaana, jonka kanssa RADIUS-palvelin kommunikoi autentikoidessaan käyttäjää. RADIUS-protokolla toimii vain RADIUS-asiakkaan ja palvelimen välillä, eikä ylety käyttäjän laitteisiin asti. (Cisco 2006.)

2.11 WLAN-tietoturva

Langattoman verkon yleistyessä myös sen tietoturvan pitää kehittyä, jotta vältyttäisiin tietomurroilta. Langattoman verkon uhat ovat pääosin samoja kuin langallisessa verkossa, mutta uusia uhkia luo juuri langattomuus, sillä data liikkuu ilmassa. Verkon uhat voidaan jakaa passiivisiin sekä aktiivisiin menetelmiin. (Puska 2005, 69.)

Passiivisia uhkia ovat muun muassa liikenteen salakuuntelu sekä analysointi. Salakuuntelu onnistuu rakennuksen ulkopuoleltakin, joten sitä on vaikea havaita. Salakuunneltua dataa voidaan jälkeenpäin analysoida valmiilla ohjelmilla ja sieltä voidaan löytää verkon käytössä olevia suojausmenetelmiä sekä pahimmassa tapauksissa suojausavaimia. (Puska 2005, 69.)

Aktiivisiin uhkiin lukeutuvat signaalien häirintä erilaisilla radiolähettimillä, palvelunestohyökkäykset WLAN-tukiasemiin sekä datan muokkaaminen man-in-the-middle menetelmän avulla. Verkkoon pääsemiseksi voidaan myös langattoman verkon kautta hyökätä hyödyntäen heikommin suojattuja työasemia. (Puska 2005, 69.)

Langattoman verkon suojaukseen hyökkäyksiltä ja muilta uhilta käytetään erilaisia suojaus- ja autentikointimenetelmiä. Seuraavaksi käyn näitä menetelmiä läpi.

2.11.1 WEP

Wired Equivalent Privacy (WEP) on ensimmäinen standardi langattoman verkon suojaukseen. Se tarjoaa kaksi suojausmenetelmää autentikointiin: kaikille avoin (Open system authentication), jolloin kaikki pystyvät liittymään verkkoon sekä yhteinen salausavain (Shared key authentication), jolloin käyttäjät tarvitsevat salausavaimen päästäkseen verkkoon. WEP käyttää salaukseen RC4 menetelmää, mikä on nykypäivänä helppo murtaa. WEP-suojausta pidetään vanhentuneena ja vaarallisena eikä se ole enää käytössä. (Ionos 2019.)

2.11.2 WPA

Wi-Fi Protected Access (WPA) kehitettiin parantamaan aikaisemman WEP-menetelmän heikkoudet, mutta yhteensopivuusongelmien takia siinä on samaa kuin WEP -standardissa, mikä tekee siitä myös helpon murrettavan. WPA käyttää suojauksessa menetelmää Temporal Key Integrity Protocol (TKIP). (Ionos 2019).

2.11.3 WPA2

Vuonna 2004 julkaistiin Wi-Fi Protected Access 2 (WPA2) -standardi, joka on turvallisempi kuin edeltäjänsä ja sen vuoksi se on yleisesti käytössä vielä nykypäivänäkin. WPA2 käyttää Advanced Encryption Standard (AES) autentikointimenetelmää. WPA2 -standardista on julkaistu personal ja enterprise vaihtoehdot. WPA2 personal on suunniteltu kotikäyttöön ja enterprise on tarkoitettu isompien yritysverkkojen suojaukseen. (Panda 2020.)

2.11.4 WPA3

Wi-Fi Protected Access 3 (WPA3) on seuraavan sukupolven Wi-Fi -standardi langattoman verkon suojaukseen. Se julkaistiin vuonna 2018 ja myös siitä tuli kaksi versiota: WPA3-personal ja WPA3-enterprise. WPA3 -standardin uusia ominaisuuksia ovat muun muassa vankempi todennus sekä vahvempi suojaus arkaluontoiselle datalle. WPA3 käyttää salauksessa 256-bittistä Galois/Counter Mode Protocol (GCMP-256), joka käyttää pidempää salausavainta parantamaan tietoturvaa. WPA3 tarvitsee toimiakseen WPA3-sertifioituja laitteita, joten se ei ole vielä yhtä yleisesti käytössä kuin WPA2. (Wi-Fi Alliance s.a.)

3 PILVIPOHJAINEN WLAN

Pilvipohjaiset hallintaratkaisut langattomille verkoille yleistyvät koko ajan erityisesti organisaatioiden keskuudessa. Se helpottaa verkkojen käyttöönottoa ja uusien tukiasemien lisäämistä, koska ei tarvita erillisiä fyysisiä ohjaimia ja niiden asetusten määrittelyä. Sillä helpotetaan verkon ylläpitäjien työtä. Samalla saadaan uusia työkaluja käyttöön, kuten tarkempaa tietoa verkon analytiikasta ja virhetilanteista. (Giordano, 2019.)

Pilvipohjaisia ratkaisuja langattomaan verkkoon tarjoavat muun muassa Cisco Meraki, Aruba, Ruckus Cloud sekä Aerohive. Näillä on varmasti erilaisia ratkaisuja käyttöönotossa sekä hallinnassa, mutta kaikkia ratkaisuja en käy työssäni tarkemmin läpi.

Seuraavassa luvussa käyn tarkemmin läpi opinnäytetyöni toteutuksessa käytettävää Ruckus Cloud pilvialustaa.

3.1 Ruckus Cloud

Yksi pilvipohjaisista WLAN hallintaratkaisuista on Ruckus Cloud, mitä tulen käyttämään työssäni. Se on selainpohjainen hallintajärjestelmä langattomalle verkolle. Sen avulla pystytään yhdestä paikasta hallinnoimaan montaa eri langatonta verkkoa ja näkemään verkkojen tila, joten se sopii hyvin myös yrityksille, joilla on useita toimipisteitä. Tukiasemien liittäminen pilveen tapahtuu selaimen tai mobiilisovelluksen kautta, ja niitä voidaan lisätä käytännössä niin monta, kuin on tarpeen. Ruckuc Cloud tukee yleisimpiä Ruckuksen tukiasemia. (Daimler s.a.)

Ruckus Cloudissa on kattava analytiikka, mistä saadaan tietoja muun muassa verkon käytöstä, kuormituksesta, sovelluksista sekä vikatilanteista. Siinä on selkeät raportointinäkymät, ja niihin voidaan valita tietty ajanjakso sekä tietyt verkot, jota halutaan tarkastella. Tämän avulla verkon ylläpitäjät saavat tärkeää tietoa siitä, miten verkkoa käytetään ja pystyvät tekemään muutoksia tarvittaessa. (Daimler s.a.)

Ruckus Cloudin avulla pystytään tekemään verkot turvallisiksi yrityksen tarpeisiin. Cloudin tukemia suojaustapoja käyttäjien autentikointiin ovat: WPA2-PSK, DPSK, 802.1X ja captive portal, jossa autentikointiin käytetään kirjautumista nettisivun kautta käyttäen esimerkiksi kolmannen osapuolen kuten Facebook- tai Google-tunnuksia. Vierailijoille voidaan tehdä omat verkkoprofiilit, jolloin ne eivät pääse yrityksen verkkoon. (Commscope s.a.)

4 KÄYTÄNNÖN TOTEUTUS

4.1 Suunnittelu ja laitteet

Käytännön toteutuksen suunnittelu aloitettiin kartoittamalla toimipisteiden nykyisten langattomien verkkojen tilanne. Seuraavaksi kartoitettiin tukiasemien määrä ja tarkistettiin, onko se riittävä kattamaan verkon kuuluvuus tarpeiden mukaisesti. Tarkistettiin nykyisten tukiasemien malli, ja katsottiin, tukeeko se liittämistä Ruckus Cloudiin. Tarvittaessa tehtiin laitehankintoja.

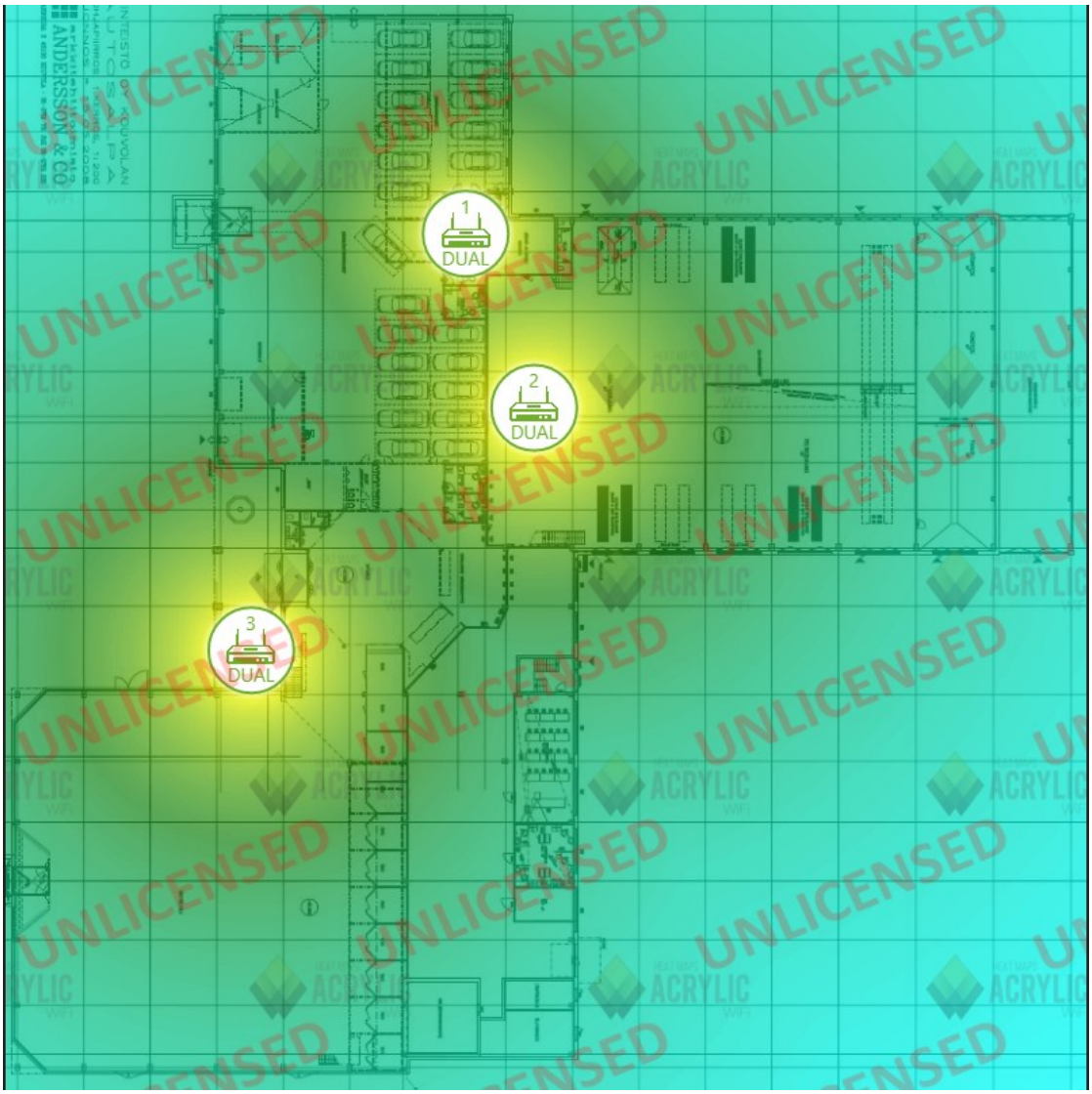
Laitteina käytettiin yrityksen verkon nykyisiä kytkimiä, joissa konfiguraatiot ovat valmiina sekä Ruckuksen tukiasemia. Tukiasemien laite malleissa päädyttiin käyttämään 802.11ac standardoituja laitteita: R510, H320, R320 ja H510, jotka tukevat liittämisen Ruckus Cloud alustaan. Tukiasemat toimivat 2,4GHz sekä 5GHz lähetystaajuuksilla. Tukiasemat tukevat myös Power over Ethernet (PoE) -tekniikkaa, jotta erillisiä virtalähteitä ei tarvita.

4.2 Tukiasemien sijoittelu

Tukiasemien sijoittelussa oleellista oli, että verkko kuuluisi mahdollisimman isolla alueella jokaisessa toimipisteessä. Tärkein alue langattoman verkon kuuluvuuden kannalta olivat toimipisteiden korjaamon puoli. Korjaamolla langattomasti toimivia laitteita on eniten ja niiden sujuva toimivuus on välttämätöntä työskentelyn kannalta.

Vanhat tukiasemat pysyivät vanhoilla paikoillaan ja tarvittavien uusien tukiasemien paikka katsottiin sillä tavalla, että se parantaisi kuuluvuutta tarvittavilla paikoilla sekä olisi olemassa olevan kaapeloinnin lähellä. Kuuluvuuden suunnittelussa käytin apuna Acrylic Wi-Fi Heatmaps kokeiluversiota. Siinä pystyy sijoittamaan tukiasemat oikeille paikoilleen sekä määrittelemään tukiasemille oikeat asetukset, jonka perusteella se näyttää oletetun kuuluvuuden.

Kuvassa nähdään tukiasemien kuuluvuus (kuva 10). Keltaisella värillä kuuluvuus on erinomainen, ja mitä sinisemmäksi väri muuttuu, kuuluvuus heikkenee.



Kuva 10. Tukiasemien kuuluvuus

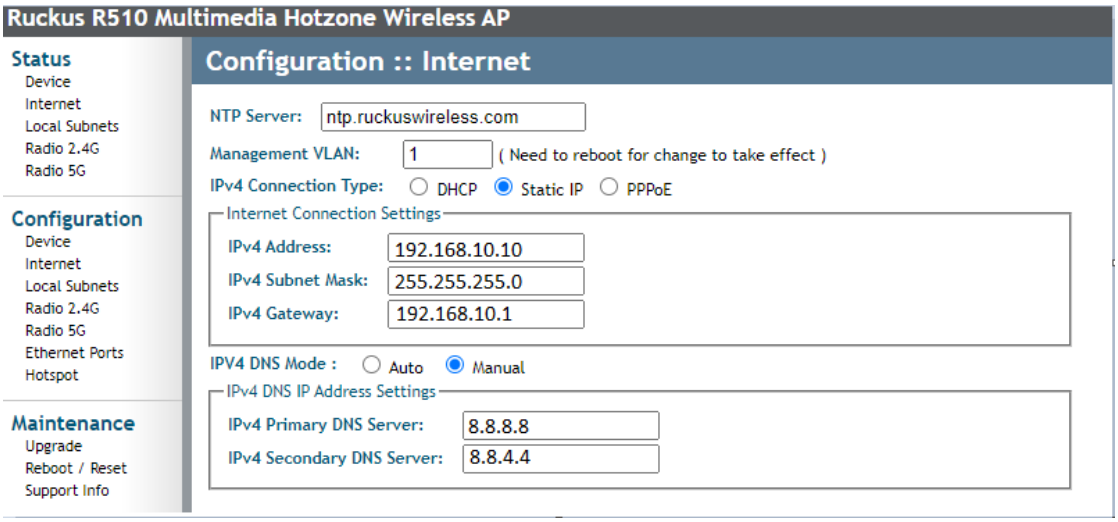
4.3 Käyttöönotto

Käyttöönotossa oli otettava huomioon se, että yrityksen toimipisteiden langattomaan verkkoon ei tule pitkiä käyttökatkoja. Tämä toi pieniä hidasteita ja ongelmia osassa toimipisteissä. Sen vuoksi käyttöönotto aloitettiin testaamalla uuden erillisen tukiaseman liittämistä Ruckus Cloudiin.

4.3.1 Testaus

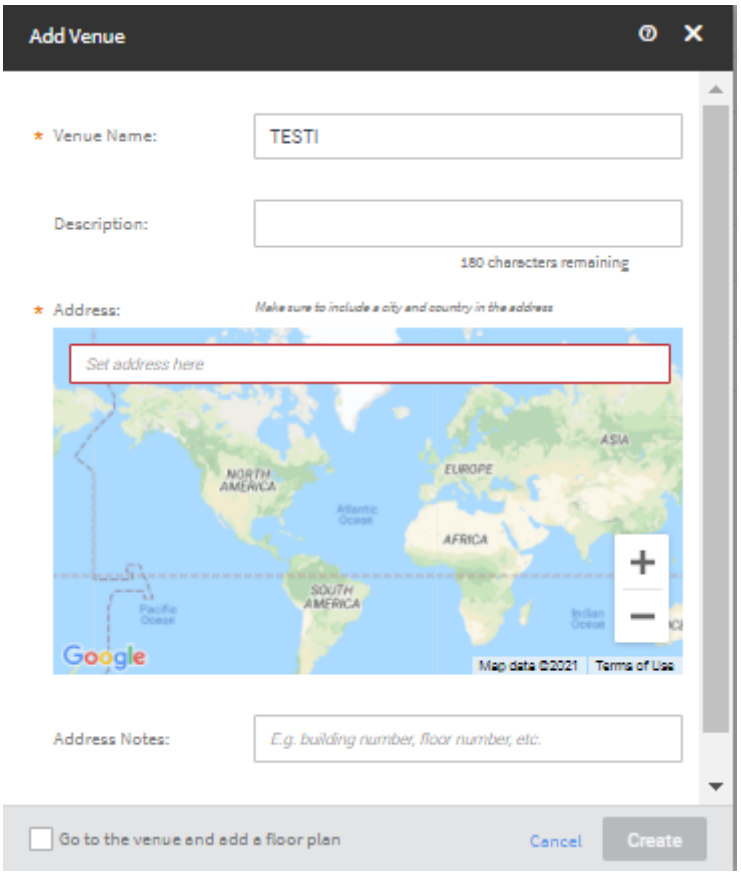
Uuden tukiaseman käyttöönotossa käytettiin PoE-injektoria tukiaseman ja tietokoneen välillä. Tietokoneen IP-osoite vaihdettiin samaan osoitealueeseen kuin tukiasema. Tämän jälkeen avattiin selaimella tukiaseman oletus IP-osoitteella sen hallintasivu.

Tukiasemaan tehtiin tarvittavat konfiguroinnit: IP-osoite, aliverkon peite, oletusyhdyskäytävä sekä DNS-osoitteet. IP-osoitteina käytettiin vapaita kiinteitä osoitteita (kuva 11).



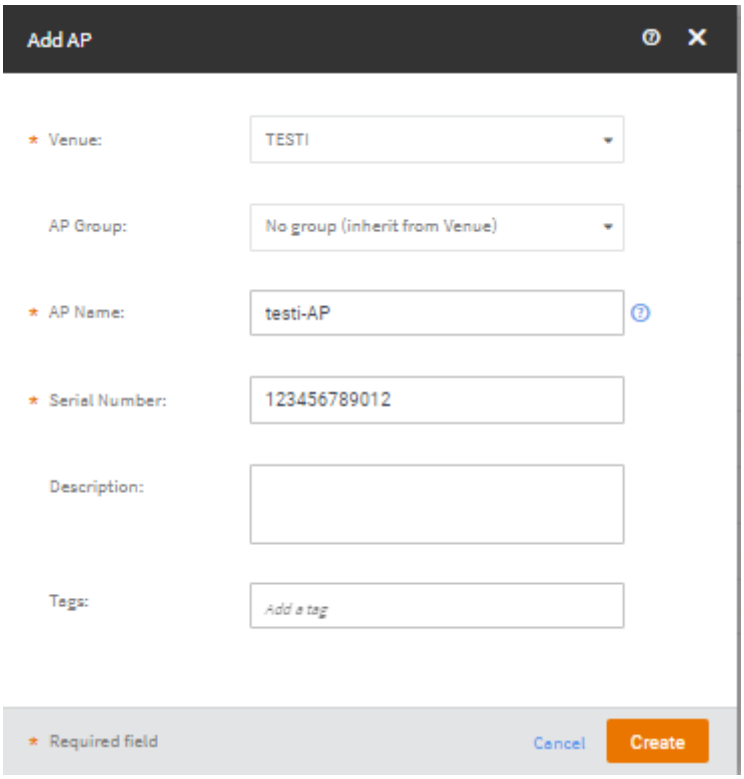
Kuva 11. Tukiaseman konfigurointi

Tukiaseman liittämiseen Ruckus Cloudiin tarvitaan luoda ensin paikka(venue), johon tukiasema halutaan liittää. Tässä tapauksessa luotiin ensin TESTI venue (kuva 12).



Kuva 12. Venuen luominen

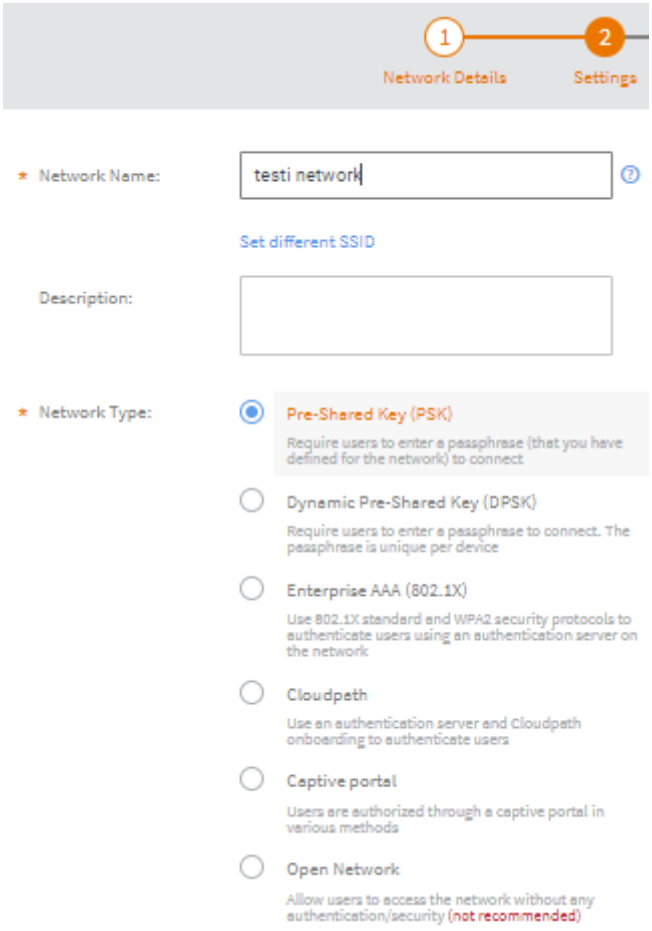
Tukiaseman lisäämiseen päästään siirtymällä *networking devices* välilehdelle ja painamalla *add ap*. Jotta tukiasema voidaan liittää pilveen, tarvitsee valita, mihin paikkaan se halutaan liittää, lisätä tukiasemalle nimi sekä selvittää tukiaseman sarjanumero. Testaus vaiheessa luotiin TESTI-alueeseen *testi-ap* (kuva 13).



Kuva 13. Tukiaseman lisääminen

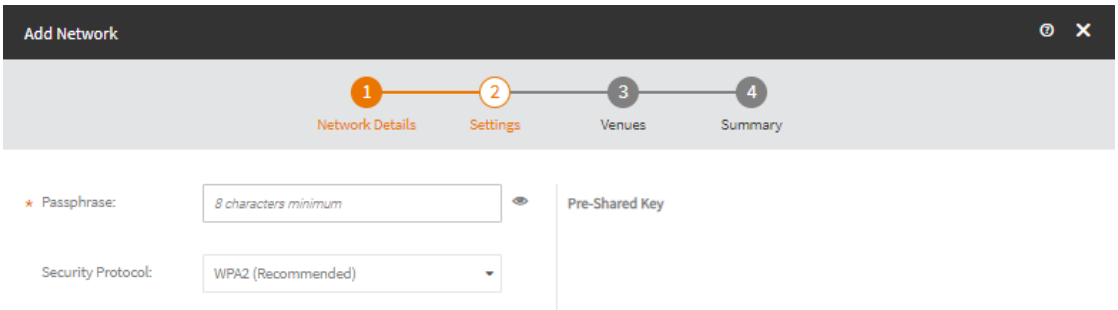
Kun tukiasema saa yhteyden pilveen, se alkaa automaattisesti lataamaan tukiasemalle oikeita asetuksia sekä uusinta firmwarea eli ohjelmistoa. Päivitysten onnistuttua tukiasema näkyy operational tilassa ja tukiasema on liitetty onnistuneesti pilveen.

Langattoman verkon luomiseen päästään wireless networks välilehdeltä painamalla *add network*. Avautuvassa ikkunassa lisätään verkolle nimi, joka toimii myös verkon SSID:nä, sekä valitaan haluttu verkkotyyppi (kuva 14). Valittavissa on 6 eri verkkotyyppiä: PSK, DPSK, 802.1X, cloudpath, captive portal ja open network. Ne käyttävät erilaisia menetelmiä tunnistautumiseen ja suojaukseen. Tässä vaiheessa valittiin PSK-verkkotyyppi.



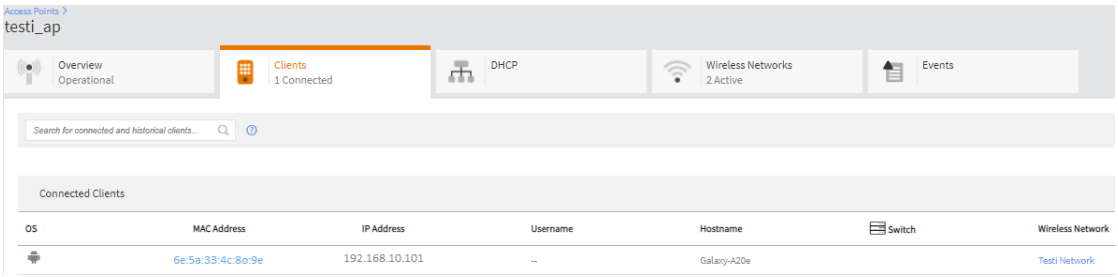
Kuva 14. Uuden verkon luominen

Seuraavassa vaiheessa päästään muokkaamaan verkon asetuksia. Luodaan verkolle salausavain (pre-shared key) ja valitaan suojausprotokolla, jota langaton verkko käyttää (kuva 15). Suojausprotokollina ovat valittavissa WPE, WPA, WPA2 sekä WPA3. Testiverkkoon valittiin yleisesti käytössä oleva WPA2-protokolla. Lopuksi valitaan vielä paikka (venue), johon verkko halutaan ottaa käyttöön.



Kuva 15. Uuden verkon luominen

Kun verkko on luotu onnistuneesti, voidaan testata toimivuutta liittämällä laite siihen. Testausvaiheessa käytettiin mobiililaitetta ja etsittiin sillä käytössä olevia langattomia verkkoja. Luotu testi network löytyi ja yhdistäminen onnistui. Ruckus Cloudista pystyttiin tarkistamaan liitetyt laitteet, ja kyseinen mobiililaite löytyi ja oli saanut IP-osoitteen (kuva 16).



Kuva 16. Tukiaseman tarkastelu

4.3.2 Toteutus

Kun testaus saatiin onnistuneesti suoritettua, siirryttiin liittämään tukiasemia Ruckus Cloudiin toimipiste kerrallaan. Liittämiset aloitettiin Kouvolan toimipisteestä, jossa oli 4 tukiasemaa. Luotiin uusi venue Kouvola, ja luotiin langaton verkko ennen tukiasemien yhdistämistä, jotta vältyttiin käyttökatkolta. Verkon tyypiksi valittiin PSK ja suojausprotokollaksi WPA2, koska melkein kaikki laitteet tukevat WPA2 protokollaa.

Lopuksi yhdistettiin tukiasemat pilveen yksi kerrallaan ja testattiin, että tukiasemiin yhdistetyt laitteet pääsevät yrityksen verkkoon. Kun testaus saatiin onnistuneesti suoritettua, tehtiin samat toimenpiteet muiden toimipisteiden verkkoihin.

Tukiasemia jouduttiin uusimaan joissain toimipisteissä, koska ne eivät tukeneet liittämistä Ruckus Cloudiin. Osassa toimipisteissä lisättiin tukiasemien määrää verkon kantavuuden parantamiseksi. Uusien tukiasemien käyttöönotot tehtiin samalla tavalla kuin testausvaiheessa.

4.4 802.1X-käyttöönotto

Seuraavaksi käydään läpi 802.1X-todennuksen käyttöönottoa yrityksen langattomaan verkkoon. Se luo verkosta turvallisemman ja sen avulla pystytään hallinnoimaan verkon käyttäjiä paremmin.

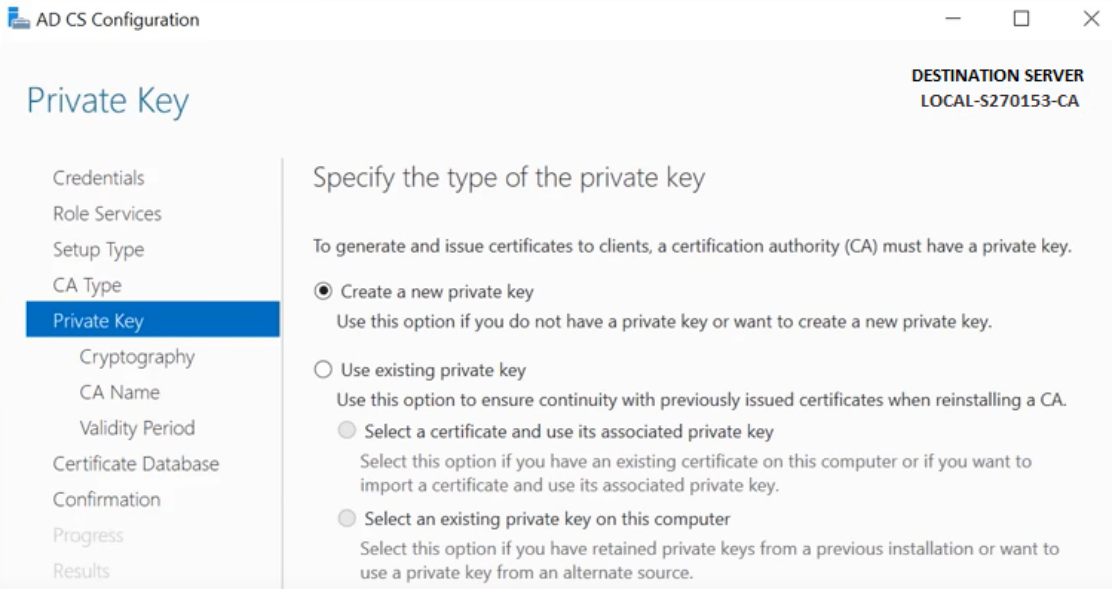
802.1X-käyttöönotossa tarvitaan Windows-palvelin, jossa on Active Directory sekä RADIUS-palvelin käyttäjien autentikointia varten. Active Directory oli valmiiksi asennettuna palvelimella, joten sinne lisättiin vain Testaus-ryhmä testausta varten. 802.1X-todennuksessa tarvitaan myös sertifikaatti, joka luotiin palvelimelle Certificate Servicellä.

Testausvaiheessa käytettiin erillistä tukiasemaa, joka toimi autentikaattorina. Asiakkaina toimivat muutama työasema, jotta toimivuutta pystyttiin testaamaan.

4.4.1 Sertifikaatin luominen

802.1X-todennus käyttää EAP-protokollaa, mikä tarvii toimiakseen sertifikaatin. Sillä varmennetaan, että käyttäjällä tai laitteella on oikeus liittyä verkkoon. Tarvittava sertifikaatti luotiin asentamalla windows-palvelimelle Active Directory Certificate Services (AD CS).

Asennus tapahtui Server managerista avaamalla manage ja sieltä add roles and features. Sen jälkeen valittiin *Server Roles* □ *Active Directory Certificate Services* □ *AD CS* □ *Role Services* □ *Certification Authority* □ *Install*. Asennuksen jälkeen palvelin pyytää vielä määrittämään muutamia lisäasetuksia.



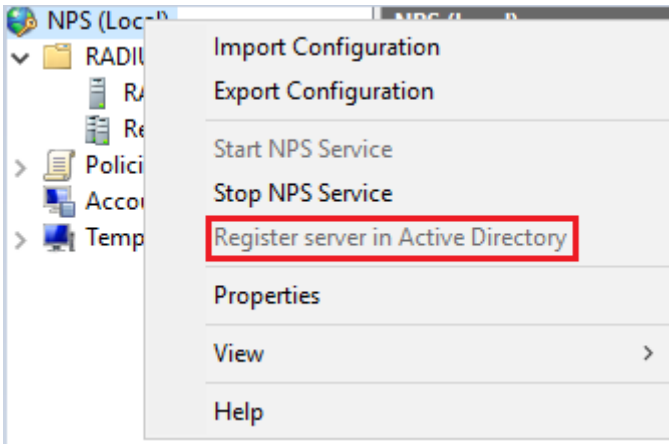
Kuva 17. Sertifikaatin luominen

Lisämäärityksissä *Role Services* -kohdassa valitaan *Certification Authority.* Asennustyypiksi valitaan *Enterprise CA* ja *CA Type → Root CA. Private Key* kohdassa valitaan *Create a new private key* (kuva 17) ja testausvaiheessa *Cryptography* -kohdasta valitaan *SHA1.* Varmenteen voimassaoloajaksi valittiin oletus 5 vuotta. Lopuksi painetaan *Configure* ja asetukset on määritelty.

4.4.2 RADIUS-palvelimen konfigurointi

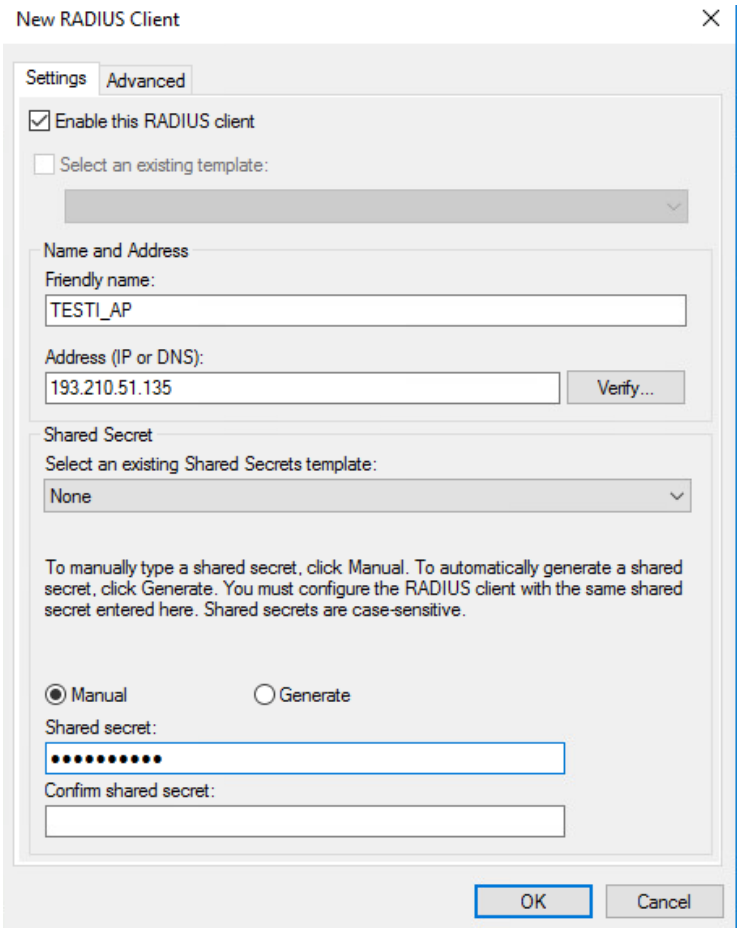
Ensin asennettiin windows-palvelimelle Network Policy and Access Services (NPS). Asennus tapahtuu avaamalla Server manager dashboard ja sen jälkeen: *Manage* □ *Add Roles and Features* □ *Server Roles* □ valitaan *Network Policy and Acces Services* □ *Install*.

Asennuksen jälkeen avataan *Tools* □ *Network Policy Server* ja päästään määrittämään tarvittavat asetukset. Active Directoryä ollut asennettu samalle palvelimelle kuin RADIUS, joten NPS-palvelin rekisteröitiin (kuva 18).



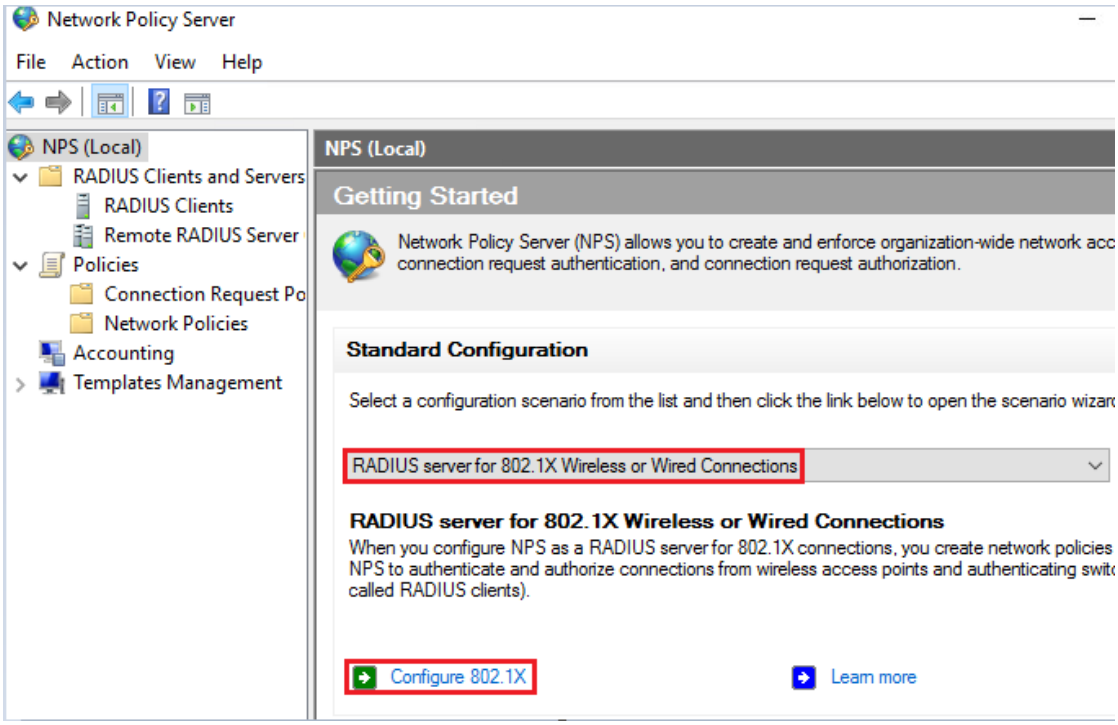
Kuva 18. NPS konfigurointi

Sen jälkeen lisättiin RADIUS-Client, joka on autentikaattorina toimiva tukiasema. Lisäys onnistuu antamalla nimi, tukiaseman IP-osoite sekä salausavain (kuva 19). Salausavaimen tulee olla sama kaikilla RADIUS-asiakkailla.



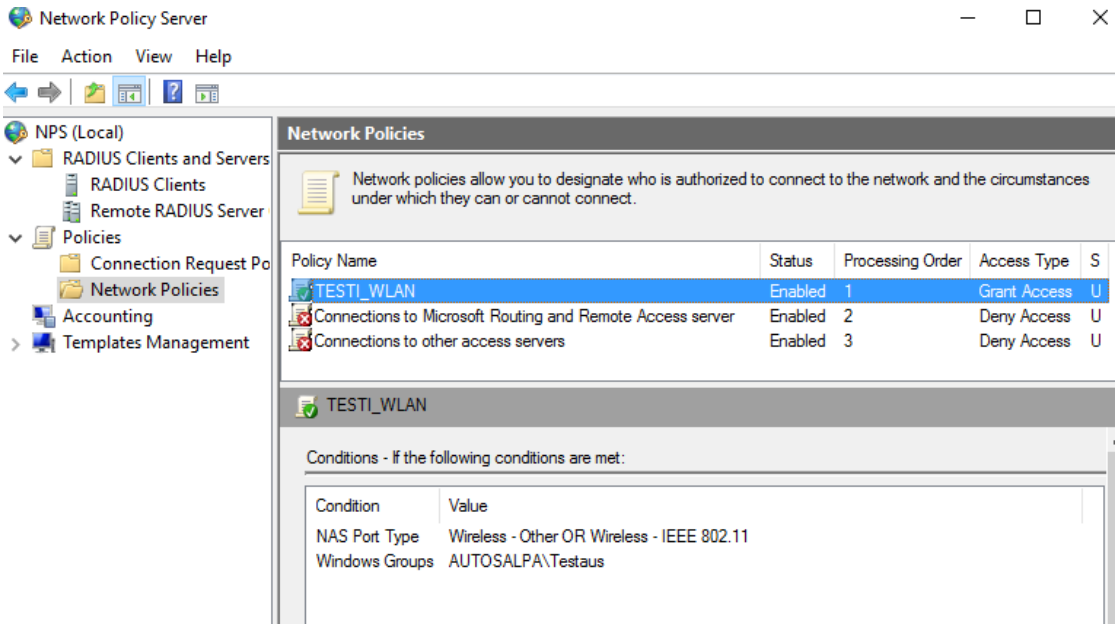
Kuva 19. Radius-asiakkaan konfigurointi

Kun tukiasema oli saatu lisättyä RADIUS-asiakkaaksi, voitiin määrittää 802.1X-verkkoliikenteelle sääntö *Network Policies -kohdasta* (kuva 20).



Kuva 20. NPS konfigurointi

Avautuvasta ikkunasta valitaan *Secure Wireless Connections,* koska sääntö luodaan langattomaan verkkoon. Säännölle annetaan nimi, joka testausvaiheessa on *TESTI_WLAN*. Seuraavassa kohdassa valitaan määritetty RADIUS-asiakas, *TESTI_AP.* Autentikointi menetelmäksi valitaan *Microsoft: Protected EAP (PEAP)* ja painetaan *Configure* josta voidaan tarkistaa, että aiemmin luotu sertifikaatti on käytössä. Painetaan *Next.* Seuraavaksi määritetään käyttäjäryhmäksi aktiivihakemistoon aiemmin luotu *Testaus* ryhmä, johon kuuluvat käyttäjät sallitaan liittymään verkkoon. Säännön määritykset on tehty ja lopuksi painetaan *Finish.* Luotu sääntö löytyy nyt *Policies → Network Policies*-kohdasta (kuva 21).



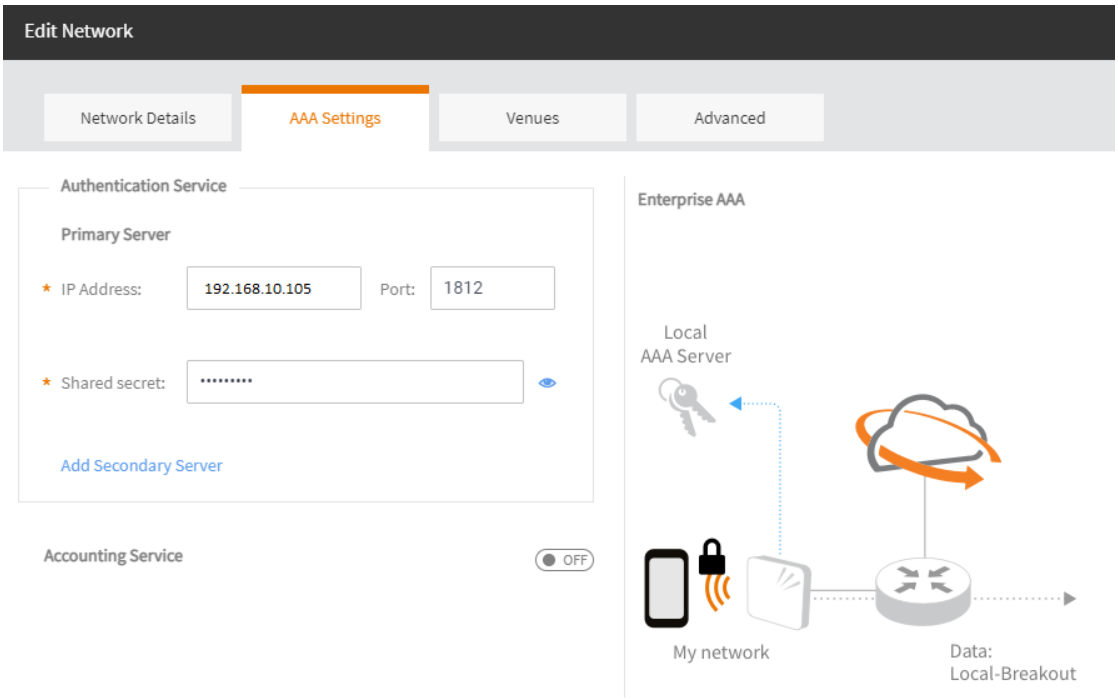
Kuva 21. Luotu sääntö.

4.4.3 Tukiaseman konfigurointi

Kun palvelimien asetusten määritykset oli saatu tehtyä, konfiguroitiin Ruckus Cloud -alustan kautta tukiasemaan tarvittavat asetukset ja lisättiin uusi verkko, mikä käyttää 802.1X-todennusta.

Tukiaseman asetuksien määritysten jälkeen se liitettiin TESTI -*Venueen*. Paikkaan luotiin uusi verkko, mikä nimettiin *TESTI_AAA* ja verkkotyypiksi valittiin *Enterprise AAA (802.1X).* Seuraavaksi määriteltiin *AAA Settings,* johon *Authentication Servicen* IP-osoitteeksi laitettiin RADIUS-palvelimen osoite sekä käytettävä portti, joka on 1812. Suojausavaimeksi tuli sama avain kuin RADIUS-asiakkailla (kuva 22).

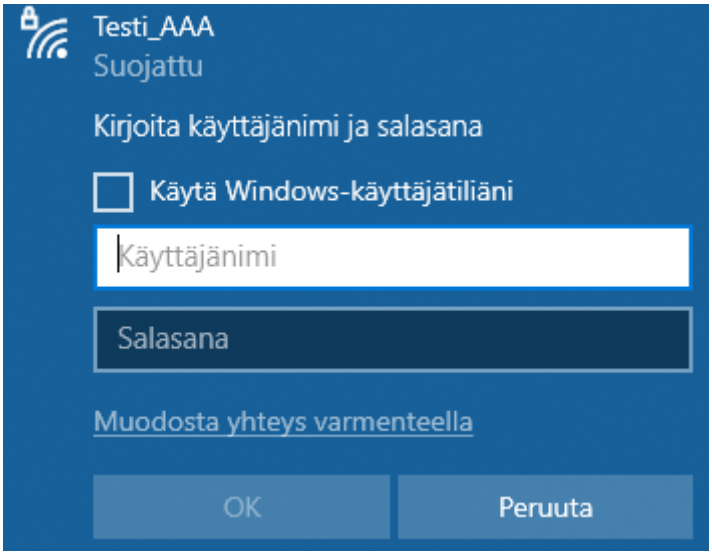
Advanced-asetukset pidettiin oletuksina ja lopuksi painettiin *Greate* ja verkon luominen onnistui.



Kuva 22. Verkon luominen.

4.4.4 Testaus

Verkkoa testattiin työasemalla. Langaton verkko löytyi ja yhdistäessä se kysyi kirjautumistietoja (kuva 23).

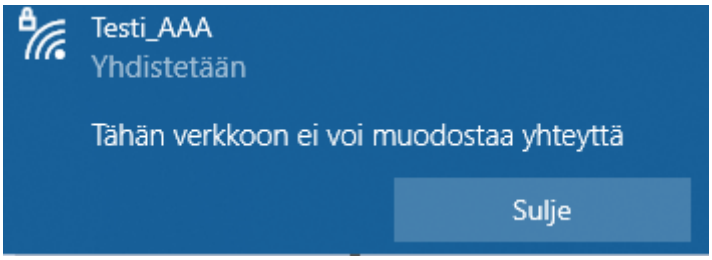


Kuva 23. Verkon testaus.

Kirjautuessa käytettiin käyttäjän tietoja, joka löytyy aktiivihakemiston *Testaus* -ryhmästä. Yhdistäminen verkkoon onnistui (kuva 24).

Kuva 24. Verkon testaus.

Toimivuuden takaamiseksi yritettiin kirjautua verkkoon vielä käyttäjätunnuksella, joka ei ole *Testaus* -ryhmässä.



Kuva 25. Verkon testaus.

Verkkoon yhdistäminen ei onnistunut (kuva 25), joten voidaan päätellä, että luotu verkko toimii halutulla tavalla. Tämä voidaan tarkistaa myös pilvialustasta *Testi_AAA* -verkon tapahtumalokista. Sieltä nähdään, että ensimmäinen kirjautumisyrityksistä onnistui:
User testi@local.autosalpa.fi who connected to the Wi-Fi network Testi_AAA was authorized for access.
Toinen kirjautumisyritys epäonnistui: User testi2@local.autosalpa.fi was unable to connect to the Wi-Fi network Testi_AAA.

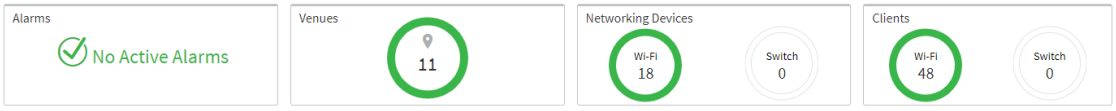
4.4.5 Toteutus

Varsinaista 802.1X-todennuksen käyttöönottoa yrityksen langattomaan verkkoon ei ehditty tekemään tässä opinnäytetyössä, koska se vaatii monien jatkuvasti verkkoa tarvitsevien laitteiden uudelleen konfigurointia. Tämä tullaan kuitenkin toteuttamaan tulevaisuudessa yrityksen verkkoon, joten 802.1X-todennuksen testausvaiheesta on hyötyä sitä ajatellen.

4.5 Pilvialustan tarkastelu

4.5.1 Hallintapaneeli

Ruckus Cloudin hallintapaneelissa näkyy hälytykset, luodut paikat (venues), liitetyt verkkolaitteet sekä verkkoon liitetyt asiakaslaitteet (kuva 26).



Kuva 26. Hallintapaneeli

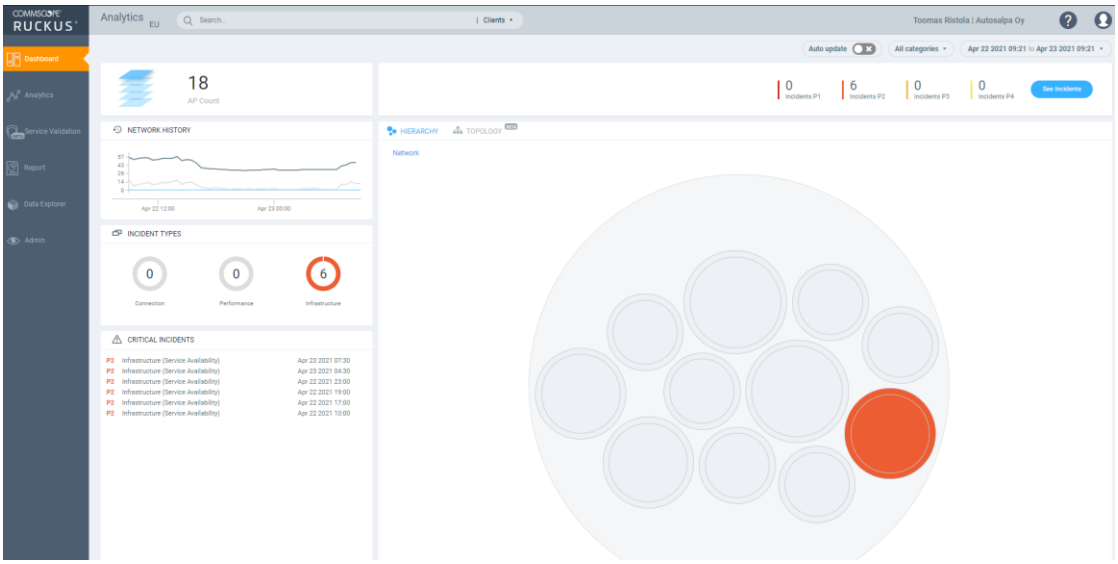
Hälytysilmoituksia tulee esimerkiksi silloin, kun pilvipalvelu ei saa yhteyttä tukiasemaan. Tukiasema voi olla sammunut esim. sähkökatkon takia tai verkossa pilven ja tukiaseman välillä on ongelmia, jolloin yhteyttä ei voi muodostaa.

4.5.2 Vikatilanteet

Vikatilanteissa hallintapaneelissa näkyy hälytys sekä ilmoitus tulee sähköpostiin, jos esim. tukiasema on ollut tietyn ajan tavoittamattomissa, jolloin pystytään reagoimaan mahdollisimman nopeasti. Vikatilanteiden selvittämiseen on käytössä Commscopen dokumenttejä, josta näkee yleisimpiä ongelmia. Jos ongelmaan ei löydy sieltä vastausta pystytään avaamaan uusi “case” eli tapahtuma, johon ongelman selvittämiseen on apuna Commscopen omia asiantuntijoita.

4.5.3 Analytiikka

Pilvipalvelussa on myös erillinen analytiikka-työpöytä (kuva 27). Analytiikkaa kerätään muun muassa datasta, tukiasemista, verkon tapahtumista, sovelluksista, asiakkaista sekä langattomista verkoista. Sen avulla pystytään tarkasti seuraamaan verkon toimintaa ja nähdään myös esimerkiksi tarkalleen, mihin aikaan mahdollisia häiriöitä on ollut. Analytiikka-työpöytää myös kehitetään koko ajan, joten tulevaisuudessa siihen on tulossa uusia ominaisuuksia.



Kuva 27. Analytiikan työpöytänäkymä

5 TULOKSET JA JOHTOPÄÄTÖKSET

Opinnäytetyössä tutustuttiin Ruckus Cloud -pilvialustaan ja sen käyttöönottoon. Teoriaosuudessa käytiin läpi langatonta verkkoa ja siihen liittyviä tekniikoita sekä standardeja.

Ensimmäisessä vaiheessa pilvialustan käyttöönottoa testattiin ensin erillisellä tukiasemalla, joka ei vaikuttanut verkon toimintaan. Testi saatiin suoritettua onnistuneesti, minkä jälkeen käyttöönotto aloitettiin yrityksen varsinaiseen langattomaan verkkoon. Käyttöönotto tehtiin ensin yrityksen Kouvolan toimipisteessä, jotta nähtiin, miten verkko toimii pilvialustan käyttöönoton jälkeen. Suuremmilta ongelmilta vältyttiin, joten sen jälkeen käyttöönotto suoritettiin muissakin yrityksen toimipisteissä. Lopulta käyttöönotto saatiin tehtyä onnistuneesti yrityksen langattomaan verkkoon.

Toisessa vaiheessa etsittiin ratkaisua siihen, miten langattomasta verkosta saadaan tietoturvallisempi. Päädyttiin 802.1X -protokollan käyttöönottoon, mikä mahdollistaa verkon käyttäjien autentikoinnin. 802.1X käyttöönoton testaus saatiin onnistuneesti suoritettua. Varsinaista käyttöönottoa yrityksen langattomaan verkkoon ei vielä saatu tehtyä, koska se vaatii tarkempaa suunnittelua, jotta suuremmilta verkon käyttökatkoilta vältyttäisiin.

Ruckus Cloud -alustan käyttöön ottaminen yrityksen langattomaan verkkoon tuo yritykselle uuden työkalun verkon hallintaan ja analytiikkaan. Se helpottaa myös verkon ylläpitäjien työtä.

Opinnäytetyön tavoitteisiin päästiin suurimmaksi osaksi. 802.1X-protokollan käytännön toteutusta ei saatu vielä suoritettua, mutta muuten tavoitteisiin päästiin. Työn tutkimuskysymyksiin saatiin vastattua onnistuneesti. Yhtenä jatkokehityshankkeena on 802.1X käyttöönotto yrityksen langattomaan verkkoon.

LÄHTEET

Cisco. s.a. WLAN Radio Frequency Design Considerations. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch3_WLAN.pdf [viitattu 6.5.2021].

Cisco. s.a. What is OFDMA? WWW-Dokumentti. Saatavissa: https://www.cisco.com/c/en/us/products/wireless/what-is-ofdma.html [viitattu 25.4.2021].

Cisco. 2006. How Does RADIUS Work? WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html [viitattu 26.2.2021].

Cisco Press. 2017. WiFi Networking: Radio Wave Basics. WWW-dokumentti. Saatavissa: https://www.networkcomputing.com/wireless-infrastructure/wifi-networking-radio-wave-basics [viitattu 20.2.2021].

Cisco. 2016. Catalyst 6500 Release 12.2SX Software Configuration Guide. WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html [viitattu 8.5.2021].

Commscope. s.a. Ruckus Cloud. WWW-dokumentti. Saatavissa: https://support.ruckuswireless.com/product_families/20-commscope-ruckus-cloud [viitattu 20.3.2021].

Daimler. s.a. Ruckus Cloud Wi-Fi. WWW-dokumentti. Saatavissa: https://www.daimler.fi/tuotteet/langattomat-verkot/wlan-verkot/ruckus-networks/tuotteet/ruckus-cloud [viitattu 20.3.2021].

Eroglu, K. 1998. The Worldwide Approval Status for 900 MHz and 2,4 GHz Spread Spectrum Radio Products. IEEE. PDF-dokumentti. Saatavissa: https://www.ipen.br/biblioteca/cd/ieee/1999/Proceed/00640.pdf [viitattu 16.5.2021].

Everything RF. 2019. What is MIMO Technology? WWW-dokumentti. Saatavissa: https://www.everythingrf.com/community/what-is-mimo-technology [viitattu 19.5.2021].

Giordano, B. (2019). The Benefits of Cloud-Managed Wi-Fi. Commscope. WWW-dokumentti. Saatavissa: https://www.commscope.com/blog/2019/the-benefits-of-cloud-managed-wi-fi/ [viitattu 20.3.2021].

Guido, R., Denteneer, T., Stibor, L., Zang, Y., Costa-Perez, X. & Walke, B. 2010. The IEEE 802.11 universe. IEEE. PDF-dokumentti. Saatavissa: https://ieeexplore.ieee.org/document/5394032 [viitattu 8.5.2021].

Ionos. (2019). WLAN security: how to make your wireless network into a fortress. WWW-dokumentti. Saatavissa:

https://www.ionos.com/digitalguide/server/security/wlan-security-the-best-protection-for-your-network/ [viitattu 1.3.2021].

Intel. (2021). Learn about Multiple-Input Multiple-Output. WWW-dokumentti. Saatavissa: https://www.intel.com/content/www/us/en/support/articles/000005714/wireless/legacy-intel-wireless-products.html [viitattu 10.3.2021].

Microsoft. (2016). 802.1X Authenticated Wireless Access Overview. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994700(v=ws.11) [viitattu 25.2.2021].

Microsoft. (2020). Extensible Authentication Protocol (EAP) for network access. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access [viitattu 25.2.2021].

Ostergaard, M. 2019. Langaton verkko saa uuden selkeän nimen. Kotimikro. WWW-dokumentti. Saatavissa: https://kotimikro.fi/internet/verkko/wifi/802-11ac-on-wi-fi-5-langaton-verkko-saa-uuden-selkean-nimen [viitattu 21.2.2021].

Panda. (2020). WPA vs WPA2: Which WiFi Security Should You Use? Artikkeli. Saatavissa: https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/ [viitattu 1.3.2021].

Perez-Neira, A. & Campalans, M. 2009. Cross-Layer Resource Allocation in Wireless Communications. Yhdysvallat: Academic Press.

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Talentum.

Riihikallio, P. (2018). WLAN 2,4 GHz taajuusalueen käyttö. Metis. WWW-dokumentti. Saatavissa: https://metis.fi/fi/2018/01/2dot4-kanavat/ [viitattu 20.2.2021].

Salonen, K. 2013. Näkökulmia tutkimukselliseen ja toiminnalliseen opinnäytetyöhön. Turun Ammattikorkeakoulu. PDF-dokumentti. Saatavissa: http://julkaisut.turkuamk.fi/isbn9789522163738.pdf [6.5.2021].

Shaw, K. 2018. What is MU-MIMO and why you need it in your wireless routers. Network World. WWW-dokumentti. Saatavissa: https://www.networkworld.com/article/3250268/what-is-mu-mimo-and-why-you-need-it-in-your-wireless-routers.html [viitattu 10.3.2021].

Shaw, K. 2020. 802.1X: Wi-Fi standards and speeds explained. Network World. WWW-dokumentti. Saatavissa: https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html [viitattu 21.2.2021].

Vocal Technologies. EAPoL Extensible Authentication Protocol over LAN. WWW-dokumentti. Saatavissa: https://www.vocal.com/secure-

communication/eapol-extensible-authentication-protocol-over-lan/ [viitattu 8.5.2021].

Wi-Fi Alliance. s.a. Security. WWW-dokumentti. Saatavissa: https://www.wi-fi.org/discover-wi-fi/security [viitattu 2.3.2021].

Wi-Fi Alliance. s.a. History. WWW-dokumentti. Saatavissa: https://www.wi-fi.org/who-we-are/history [viitattu 6.5.2021].

KUVALUETTELO