LAPIN AMK
Lapland University of Applied Sciences

CISCON WLAN-KONTROLLERIN KÄYTTÖÖNOTTO JA KONFIGUROINTI

Tuukka Hedemäki

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2020

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Tuukka Hedemäki	Vuosi	2020
Ohjaaja	Kenneth Karlsson		
Toimeksiantaja	LapIT Oy		
Työn nimi	Ciscon WLAN-kontrollerin käyttöönotto ja konfigurointi		
Sivumäärä	53		

Opinnäytetyön aiheena oli Cisco-merkkisen WLAN-kontrollerin käyttöönotto sekä sen ominaisuuksien konfigurointi. Käyttöönottovaiheessa esitellään verkon komponentit sekä niiden konfiguraatio, jotta WLAN-kontrollerin käyttö sekä käyttöönotto onnistuu. Tässä työssä WLAN-kontrollerille konfiguroidaan langattomat verkot sekä kontrollerin hallinta. Alustuksena aiheelle esittelen 802.11-standardeja, pääpaino uusimmalla 802.11ax-standardilla. Käyn myös läpi WLAN-kontrollerien sekä tukiasemien käyttötarkoituksen.

Käyttöönotto sekä konfigurointi toteutettiin Cisco Packet Tracer -nimisellä simulaatio-ohjelmalla, jonka tuloksia sekä päätelmiä voidaan hyödyntää operatiivisessa järjestelmässä. Simulaatio-ohjelman ominaisuudet olivat rajalliset, joten osa konfiguraatiosta on tehty Ciscon tuottamien dokumenttien pohjalta. Aineisto standardeihin liittyen on hankittu internetistä löytyvistä materiaaleista. WLAN-kontrollerin sekä tukiaseman materiaali on osaksi kirjoitettu oman harrastuneisuuden ja työelämästä saadun kokemuksen pohjalta sekä internetistä löytyvään aineistoon pohjautuen.

Opinnäytetyön toteutus ei ollut liian vaativa ja itse käyttöönotto ja konfigurointi onnistuivat ilman mitään ongelmia. Opinnäytetyön avulla kuka tahansa tietotekniikan perusteet hallitseva henkilö voi ottaa käyttöön sekä konfiguroida WLAN-kontrollerin.

Avainsanat IEEE 802.11-standardi, konfigurointi, WLAN

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Degree Programme in Information
and Communication Technology
Bachelor of Engineering

Author Tuukka Hedemäki Year 2020
Supervisor Kenneth Karlsson
Commissioned by LapIT Oy
Subject of thesis Deployment and Configuration of Cisco WLAN Controller
Number of pages 53

The aim of this thesis was to find out what kind of a task it is to deploy a Cisco WLAN controller and configure it. The configuration of every network component is shown in order to deploy and configure a WLAN controller. The features that were configured on this bachelor's thesis are wireless networks and WLAN controllers management. In the introduction, the 802.11 standards are explained, mainly focusing on the latest 802.11ax standard to give the reader basic knowledge of the standards used in wireless networking. The reader will also learn basic knowledge of WLAN controllers and access points and what they are used for.

The deployment and configuration of the WLAN controller were done using a simulation program called Cisco Packet Tracer. The simulation program had limited features, so some parts of the configuration were done based on Cisco documentaries. The material used to write of the standards was found on the internet. Part of the material written on WLAN controller and access points section was based on the author's own experience of networking gained in working life, the other part was based on the material found on the Internet.

The overall process to deploy and configure the WLAN controller was not too challenging. Anyone with basic information technology knowledge and skills can deploy and configure a WLAN controller. The results and conclusions of this work can be used in a real-world operative environment.

Key words configuration, IEEE 802.11 standard, WLAN

SISÄLLYS

KÄYTETYT MERKIT JA LYHENTEET

AES	Advanced Encryption Standard
DTIM	Delivery Traffic Indication Message, tukiasema lähettää herätesignaalin, jolloin päätelaitteen verkkokortin täytyy vastaanottaa tietoa (Router Guide 2015)
Gbps	gigabittiä/sekunti
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things, antureita ja sensoreita sisältävä laite, joka on yhdistettynä lähiverkkoon tai internettiin (Itewiki 2020)
KHz	kilohertsiä
Mbps	megabittiä/sekunti
MHz	megahertsiä
GHz	gigahertsiä
MIMO	Multiple Input Multiple Output, usealla radiolähettimellä lähetetään ja vastaanotetaan useaa signaalia (Keith 2018)

MU-MIMO	Multi-User Multiple Input Multiple Output, usealla radiolähettimellä lähetetään ja vastaanotetaan useaa signaalia usean päätelaitteen kanssa samaan aikaan (Keith 2018)
OFDM	Orthogonal Frequency Division Multiplex, signaalin modulointitekniikka, jonka signaali koostuu useasta lähekkäin olevista moduloiduista kantajista (Electronics-notes 2020f)
OFDMA	Orthogonal Frequency Division Multiple Access, signaalin modulointitekniikka, jota käytetään ainoastaan 802.11ax-standardissa (Extreme 2019)
PoE	Power Over Ethernet
PSK	Private Shared Key
QAM	Quadrature Amplitude Modulation, signaalin modulointitekniikka, jossa kaksi kantoaaltoa kulkee 90 asteen kulmassa toisiinsa nähden (Huang 2018)
RU	Resource Unit, tukiaseman lähettämän signaalin tietoa kantavien osien ryhmän nimi (Coleman 2020, 19)
TCP	Transmission Control Protocol
TWT	Target Wake Time, tukiasema lähettää herätesignaalin tietyin väliajoin ja langaton päätelaite lähettää tietoa vain tarvittaessa (Coleman 2020, 43)
TXOP	Transmission Opportunity, tukiasemalla on oma vuoronsa jokaiselle 802.11-standardille lähettää tai vastaanottaa tietoa (Coleman 2020, 20)

UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 JOHDANTO

Nykypäivänä langattoman verkon tarve on suuri. Melkein jokaiselta löytyy tietotekninen laite, joka on koko ajan yhteydessä internettiin. Tulevaisuudessa jokainen kodinkone sekä muut kotona olevat laitteet ovat myös yhteydessä internettiin. Monessa laitteessa voi olla operaattorin tarjoama liittymä, mutta ne voivat olla saldorajoitettuja, joten moni suosii langatonta lähiverkkoa.

Yritysmaailmassa langaton lähiverkko on tärkeä, koska toimistossa voi olla monta ihmistä töissä samaan aikaan. Internet-rasiapaikkoja toimistossa on rajallisesti, eikä ne riitä kaikille sekä laitteita halutaan liikuttaa niin, että ne pysyvät verkossa. Uusissa isoissa rakennuksissa täytyy olla koko rakennuksen kattava langaton internet-yhteys. Tähän on ratkaisuna rakentaa langaton lähiverkko tukiasemista, joita hallitaan keskitetysti WLAN-kontrollerilla.

Opinnäytetyöni tavoitteena on dokumentoida sekä selvittää, kuinka Cisco-merkkinen WLAN-kontrolleri otetaan käyttöön sekä kuinka sen erinäisiä sisäänrakennettuja toimintoja konfiguroidaan. WLAN-kontrollerin käyttöönotto sekä konfigurointi kuvataan vaihe vaiheelta.

Tässä opinnäytetyössä käsitellään nykypäivän sekä vanhempia WLAN-standardeja, standardien tekniikkaa sekä tulevaisuutta. Työssä käsitellään myös yleisesti WLAN-kontrollerien käyttötarkoitusta sekä niiden käyttämistä yritysorganisaatiossa.

Olen aina ollut kiinnostunut tietotekniikasta. Pidemmälle opiskellessani tajusin, että tietoliikennetekniikka on ala, jota haluan opiskella lisää. Hakeuduin töihin tietotekniikan alan yritykseen nimeltä LapIT Oy, jossa työnimikkeeni oli aluksi tietoliikenneharjoittelija myöhemmin tietoliikenneasiantuntija. Sain työtehtävistäni innostusta opiskella tietoliikennettä lisää.

2 IEEE 802.11 -STANDARDIT

IEEE on luonut ensimmäisen WLAN-standardin vuonna 1997. Sen maksimaalinen teoreettinen yhteysnopeus oli vain kaksi megabittiä sekunnissa. Tämä nopeus ei riittänyt useimmille sovelluksille, joten alettiin kehittää nopeampia standardeja. (Mitchell 2020.)

Langattoman verkon kehittämisen alkuvaiheissa langatonta verkkoa kutsuttiin nimellä Wireless Ethernet. Nimitys tulee vastaavasta sanasta Wired Ethernet, joka siis tarkoittaa langallista verkkoyhteyttä. Nykyään langattoman verkon ymmärtää sanalla Wi-Fi, joka on langattoman verkon markkinointinimi. (Bologna 2019.)

WLAN-standardeissa on etuliitteenä nimi 802.11, joka annettiin IEEE:n muodostamille ryhmille, joiden tarkoituksena on kehittää, ylläpitää ja valvoa WLAN-standardeja. Kaikki tähän asti julkaistut WLAN-standardit alkavat 802.11-etuliitteellä. (Mitchell 2020.)

Standardeille on kehitetty uusi nimeämiskäytäntö, joka on käyttäjäystävällisempi kuin nykyinen nimeämiskäytäntö, mutta ei kuitenkaan virallinen. Standardeja on alettu nimeämään Wi-Fi-etuliitteellä vasta 802.11n-standardin julkaisusta lähtien. Numero perustuu standardin julkaisuvuoteen, eli mitä uudempi standardi, sitä isompi numero. (WiFi Adviser 2020.)

Taulukko 1. Standardien uusi nimeämiskäytäntö (WiFi Adviser 2020)

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

Uuden standardin julkaisun myötä on myös teoreettinen maksiminopeus moninkertaistunut. Taulukossa 2 on esitetty standardien taajuusalueet, julkaisuvuosi sekä teoreettinen maksiminopeus.

Taulukko 2. Yhteenveto standardien ominaisuuksista (WiFi Adviser 2020)

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	3.6Gbps	10-12Gbps

2.1 Vanhemmat standardit

Vanhemmat standardit tarkoittavat standardeja, joita enää käytetään hyvin vähän tai ei ollenkaan. Tukiasemat tukevat vielä vanhoja standardeja, mutta ne ovat poistuvia, koska ne ovat paljon hitaampia kuin uudemmat standardit.

2.1.1 802.11b

802.11b-standardi julkaistiin vuonna 1999, eli samaan aikaan kuin 802.11a-standardi. 802.11b-standardi toimii 2,4 GHz:n taajuudella. 802.11b-standardin teoreettinen maksiminopeus on vain 11 Mbps, eli paljon hitaampi kuin samana vuonna julkaistu 802.11a-standardi. Valmistajat käyttivät todennäköisemmin 802.11b-standardia kotireitittimissä, koska se oli halvempi toteuttaa kuin 802.11a-standardi. (Mitchell 2020.)

Lähetettävän signaalin kanavan leveys on 20 MHz sekä tyypillinen kantavuus signaalille on noin 30 metriä sisätiloissa. Vaikka teoreettinen maksiminopeus on 11 Mbps, todellinen tiedonsiirtonopeus on 5,9 Mbps, jos järjestelmä käyttää TCP-protokollaa. UDP-protokollalla todellinen tiedonsiirtonopeus on noin 7,1 Mbps. (Electronics-notes 2020b.)

2.1.2 802.11a

802.11a-standardi oli ensimmäinen IEEE:n julkaisema standardi, joka julkaistiin samaan aikaan kuin 802.11b-standardi. 802.11a-standardi oli vähemmän käytetty kuin 802.11b-standardi, koska sinä aikana teknologia oli kalliimpaa. (Mitchell 2020.)

Signaalin moduloinnissa käytetään OFDM-tekniikkaa ja sitä lähetetään 5 GHz:n taajuudella. Kanavan leveys on 20 MHz sekä kantavuus noin 30 metriä sisätiloissa kuten 802.11b-standardilla. Teoreettinen maksiminopeus on reilusti korkeampi kuin 802.11b-standardin, jopa 54 Mbps. Todellinen tiedonsiirtonopeus oli kuitenkin 25 Mbps. (Electronics-notes 2020c.)

2.2 Nykyaikaiset standardit

Nykyaikaisilla standardeilla tarkoitetaan niitä standardeja, joita nykyajan tukiasemat tukevat tai tulevat tulevaisuudessa tukemaan. Nykyaikaisissa standardeissa ominaisuuksia on parannettu sekä niitä on enemmän verrattuna vanhempiin standardeihin.

2.2.1 802.11g

Vuosina 2002 ja 2003 langattomat laitteet alkoivat tukea uutta standardia nimeltä 802.11g, jonka tarkoituksena oli yhdistää parhaat puolet vanhemmista 802.11a- sekä 802.11b-standardeista. 802.11g-standardissa päästiin samaan nopeuteen kuin 802.11a-standardissa, eli 54 Mbps:n teoreettiseen maksiminopeuteen. 802.11g-standardi käyttää 2,4 GHz:n taajuusaluetta saavuttaakseen paremman kuuluvuuden. (Mitchell 2020.)

Hyvänä puolena 802.11g-standardissa on se, että melkein jokainen laite, joka käyttää langatonta verkkoa, tukee 802.11g-standardia. 802.11g-standardin tukeminen langattomassa laitteessa on kaikista halvin ratkaisu laitevalmistajille muihin standardeihin verrattuna. Tästä syystä 802.11g-standardi oli hallitsevin Wi-Fi-teknologia useiden vuosien ajan. (Electronics-notes 2020a; Mitchell 2020)

802.11g-standardi on taaksepäin yhteensopiva vanhempien standardien kanssa. Tukiasemat, jotka tukevat 802.11g-standardia tukevat myös 802.11b-standardia. (Mitchell 2020.)

2.2.2 802.11n

802.11n-standardi julkaistiin vuonna 2009. 802.11n oli ensimmäinen standardi, joka tuki MIMO-tekniikkaa. Uutta 802.11n-standardissa oli myös sen kanavan leveys, jossa päästiin jo 40 MHz kanavan leveyksiin. Standardin kehittämisen ideana oli paljon parempi suorituskyky sekä nopeasti kehittyvän Ethernet-teknologian nopeuksien mukana pysyminen. (Electronics-notes 2020d.)

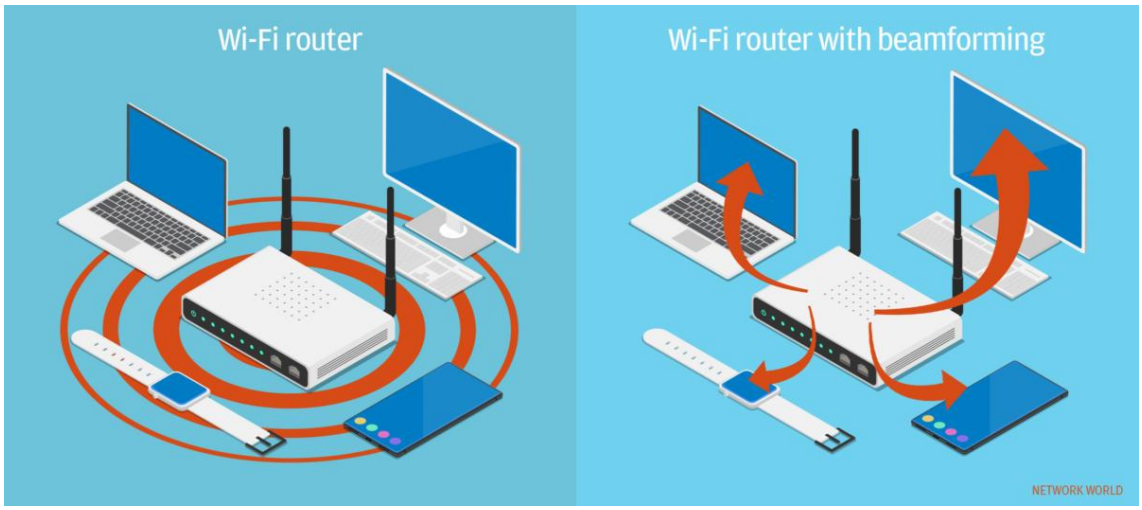
802.11n-standardi toimii 2,4 GHz:n sekä 5 GHz:n taajuusalueilla. Yhteensopivuus aiempien tekniikoiden kanssa oli mahdollistettu standardin kanssa, mutta siinä oli huonojakin puolia suorituskyvyn puolesta. Mikäli langattomassa verkossa oli jokin laite kiinni vanhemmalla tekniikalla, 802.11g-standardin tavoin, langattoman verkon nopeus hidastui muillakin käyttäjillä. Mikäli verkossa oli pelkästään 802.11n-standardia tukevia laitteita, saatiin paras suorituskyky. Uudella MIMO-tekniikalla sekä leveämmällä kanavan leveydellä saavutetaan jopa 600 Mbps:n nopeus. (Electronics-notes 2020d.)

Jotta korkeita nopeuksia pystytään toteuttamaan, standardin mukana julkaistiin uusi tekniikka nimeltään MIMO. Tekniikka mahdollistaa käytettävissä olevan kaistan maksimaalisen hyödyntämisen. Tekniikan toimintaperiaatteena on, että siinä käytetään useaa antennia hyödyksi tiedon kuljettamiseen. (Electronics-notes 2020d.)

802.11n-standardi tukee neljää eri tietovirtaa, eli tämä käytännössä tarkoittaa, että neljä eri tietovirtaa voidaan viedä saman kanavan yli. MIMO-tekniikka mahdollistaa usean antennin käytön tiedon lähettämiseen sekä vastaanottamiseen. Vaikka standardi tukee neljän eri tietovirran sekä neljän antennin käyttämistä lähetykseen sekä vastaanottamiseen, yleisin konfiguraatioratkaisu langattomiin verkkoihin oli kaksi eri tietovirtaa, jota lähetettiin kahdella eri antennilla ja vastaanotettiin kahdella eri antennilla. (Electronics-notes 2020d.)

MIMO-tekniikan toteuttamisessa oli haasteita laitteiden virrankuluttamisen kanssa. Useamman antennin toimiessa, virrankulutus oli myös paljon korkeampi kuin aiempia standardeja tukevissa laitteissa. Tästä päästiin eroon kytkemällä MIMO-tekniikka pois päältä aina kun tiedonsiirtoa ei tarvita. (Electronics-notes 2020d.)

802.11n-standardia julkaistaessa laitevalmistajat esittelivät myös uutta tekniikkaa nimeltä beamforming. Tukiasema muodostaa signaalikeilan laitteeseen mahdollistaen tehokkaan tiedonsiirron verrattuna edelliseen tapaan kaiuttaa signaalia tasapuolisesti joka puolelle. (Fruhlinger 2019.) Kuviossa 1 nähdään vanhan tekniikan sekä beamforming-tekniikan ero.



Kuvio 1. Beamforming tekniikka (Fruhlinger 2019)

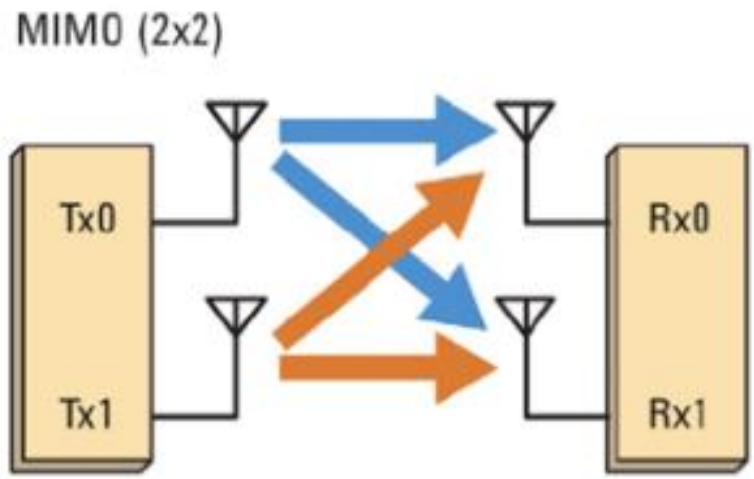
802.11n-standardi oli ensimmäinen Wi-Fi-versio, joka tuki MIMO-tekniikkaa, jota beamforming-tekniikka tarvitsee, jotta se voi lähettää usean toistensa päälle menevän signaalin. Silloiset reitittimet, jotka julkaistiin tukemaan 802.11n-standardia sekä beamforming-tekniikkaa, eivät koskaan tulleet kovin suosituiksi, koska laitevalmistajat vaativat, että käyttäjä ostaa samalta laitevalmistajalta reitittimen sekä langattoman verkkokortin. Esimerkiksi yhden laitevalmistajan langaton verkkokortti ei käynyt toisen laitevalmistajan reitittimen kanssa. (Fruhlinger 2019.)

2.2.3 802.11ac

Ensimmäinen versio 802.11ac-standardista oli nimeltään 802.11ac wave1. Se julkaistiin vuonna 2013, jonka jälkeen julkaistiin uudempi versio 802.11 wave2 vuonna 2016, joka on viimeisin versio standardista. (Electronics-notes 2020e.)

802.11ac-standardi toimii 5 GHz:n taajuusalueella. Uusimmassa versiossa tuli uusia ominaisuuksia, kuten MU-MIMO-tekniikka, 80 MHz:n ja 160 MHz:n kanavan leveydet sekä neljän spatiaalisen tietovirran tukeminen neljällä antennilla, kun wave 1 -versiossa tuettiin vain kolmea antennia. Näiden ominaisuuksien ansiosta teoreettinen maksiminopeus on 6,93 Gbps, mutta laitteet eivät tukeneet näin korkeita nopeuksia, koska sen tukeminen oli kallista valmistajille. Varsinainen nopeus, jota langattomilla laitteilla mainostetaan 802.11ac-standardin nopeudeksi on 1300 Mbps. 1300 Mbps:n nopeus vaatii 3x3-MIMO-tekniikan. (Angell 2013, 8, 10; Electronics-notes 2020e)

802.11-standardin normaalina toimintatapana on, että ensimmäinen käyttäjä, joka kommunikoi tukiaseman kanssa, saa ensimmäisenä palvelua muiden käyttäjien odottaessa vuoroaan. MU-MIMO-tekniikalla on päästy eroon muiden käyttäjien odotuttamisesta, eli tekniikan ansiosta useat käyttäjät pääsevät käyttämään langatonta verkkoa ilman viivettä. (Hintersteiner 2016; Keith 2018)



Kuvio 2. 2x2-MIMO-tekniikka (Hintersteiner 2016)

802.11ac-standardin julkaisun myötä myös beamforming-teknologiasta tuli yleisempi. Teknologian toteuttaminen järjestelmissä ei vaatinut enää saman laitevalmistajan laitteita, vaan laitteet pystyivät olemaan eri laitevalmistajilta. (Fruhlinger 2019.)

2.2.4 802.11ax

802.11ax-standardi on viimeisin IEEE:n julkaisu. Se julkaistiin 2019 sekä sen julkaisun myötä on monia asioita parannettu. 802.11ac-standardia kutsutiin korkean suoritustehon standardiksi. 802.11ax-standardia voidaan kutsua korkean hyötykäytön standardiksi. (Coleman 2020, 8.)

Wi-Fi-teknologia on joustava teknologia, mutta sitä ei ole aiemmin osattu hyödyntää niin hyvin kuin 802.11ax-standardin julkaisun myötä. Aiemmissa standardeissa on julkaistu tekniikoita, jotka toivat muun muassa suurempia tietonopeuksia sekä leveämpiä kanavan leveyksiä, mutta niissä ei otettu huomioon niiden parasta hyödyntämistä. Tätä voidaan verrata käytännössä esimerkiksi ajoneuvoliikenteeseen. Nopeampia autoja sekä isompia sekä leveämpiä moottoriteitä on rakennettu, mutta silti syntyy liikenneruuhkia. Näin käy myös Wi-Fi-liikenteelle, johon vaikuttavat useat tekijät, joka johtaa vähäiseen Wi-Fi-tekniikoiden hyödyntämiseen. (Coleman 2020, 9.)

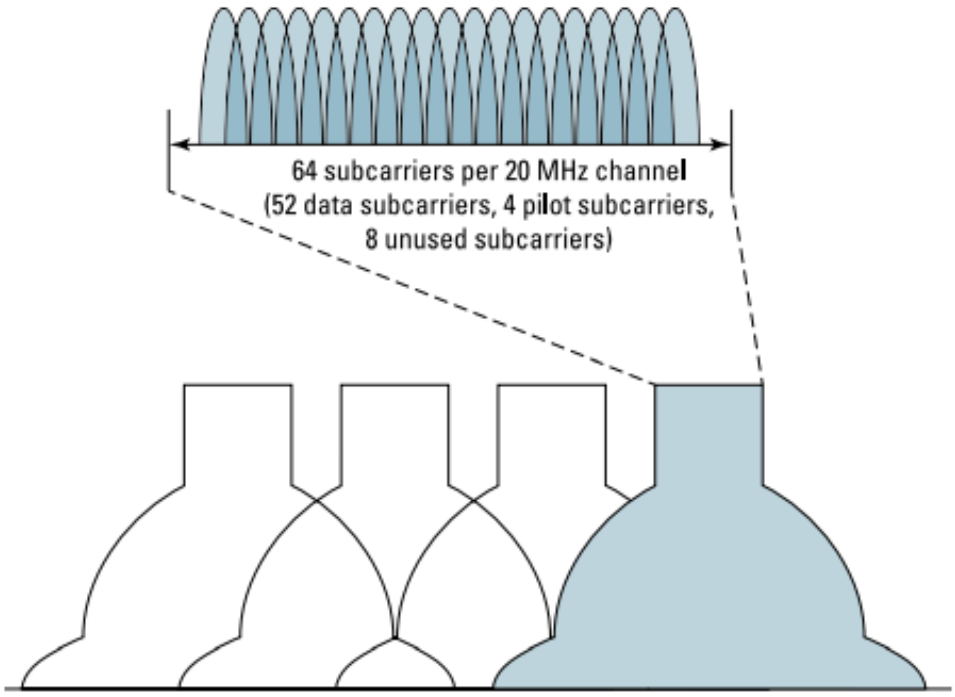
802.11ax-standardi toimii 5 GHz:n sekä 2,4 GHz:n taajuusalueilla. Mahdollisimman suuret tiedonsiirtonopeudet sekä leveämmät kanavat eivät ole olleet standardin kehittämisen tavoitteina, vaan 802.11-standardin liikenteen hallinta. (Coleman 2020, 11.)

802.11ax-standardin parannukset keskittyvät eniten langattoman verkon fyysiselle tasolle sekä uuden monta käyttäjää tukevan version OFDM-teknologiaan. Aiemmat standardit käyttivät OFDM-teknologiaa, kun uudessa standardissa sitä kutsutaan nimellä OFDMA. (Coleman 2020, 15.)

OFDMA-teknologia on 802.11ax-standardin kehityksen kannalta päätekijä. Tekniikka perustuu siihen, että esimerkiksi 20 MHz:n kanava jaetaan osiin kuten

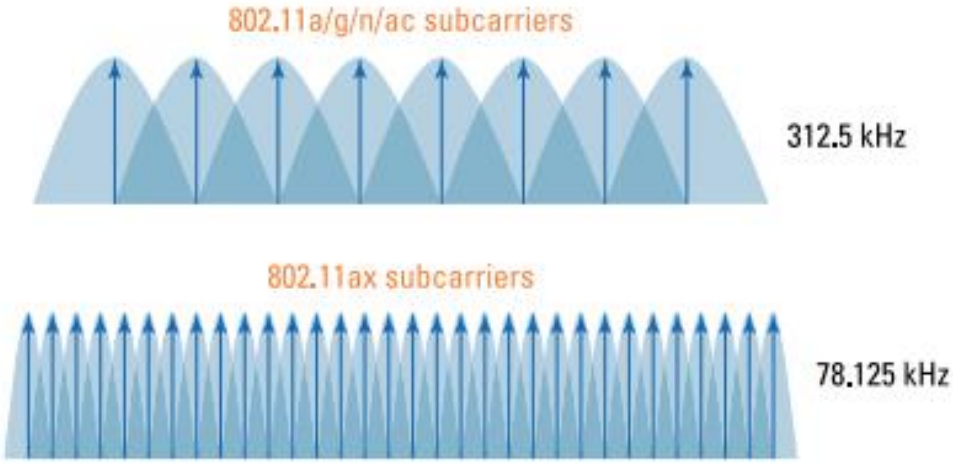
OFDM-tekniikassakin, mutta pienempiin. Mikäli tukiasema sekä käyttäjän laite tukevat 802.11ax-standardia, voi OFDMA-tekniikan ansiosta tukiasema viestiä useamman käyttäjän kanssa samaan aikaan. (Coleman 2020, 15.)

OFDM-tekniikassa 20 MHz:n kanava jaetaan 64:ään eri osaan, joista 52 on varattu moduloidulle datalle, neljä lähettimen ja vastaanottimen synkronisointia varten sekä loppua kahdeksaa ei käytetä muuhun kuin häiriön poistamiseen viereisten kanavien välillä. (Coleman 2020, 16.) Kuviossa 3 nähdään 20 MHz:n kanavan jako.



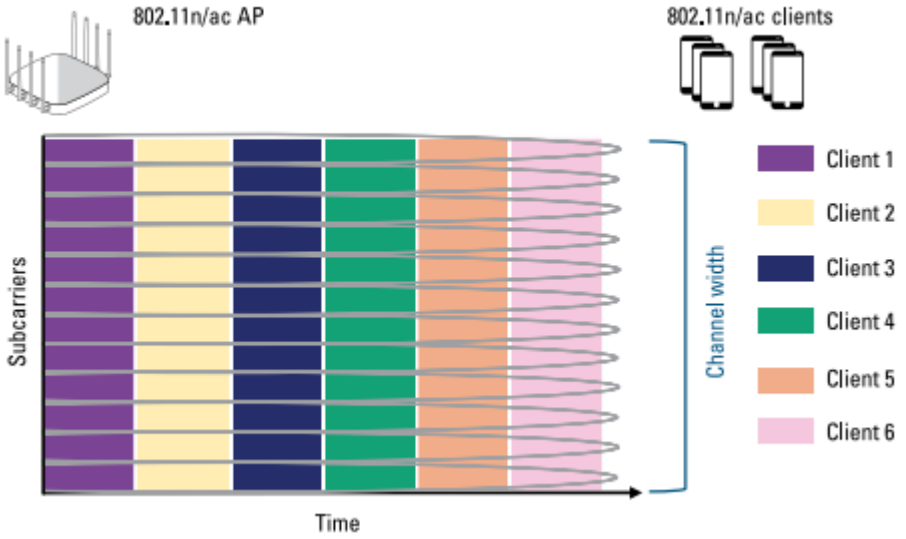
Kuvio 3. OFDM-tekniikan kanavan jako (Coleman 2020, 17)

OFDM-tekniikassa kanava on jaettu 312,5 KHz:n kokoisiin osiin. Numero saadaan, kun jaetaan 20 MHz luvulla 64, eli luvulla, johon aiemmissa standardeissa kanava on jaettu. OFDMA-tekniikassa 20 MHz:n kanava on jaettu 256:een osaan, eli kanavan osan kooksi saadaan 78,125 KHz. (Coleman 2020, 16–17.) Kuviossa 4 nähdään OFDMA-tekniikan kanavan jako.



Kuvio 4. OFDMA-tekniikan kanavan jako. (Coleman 2020, 17)

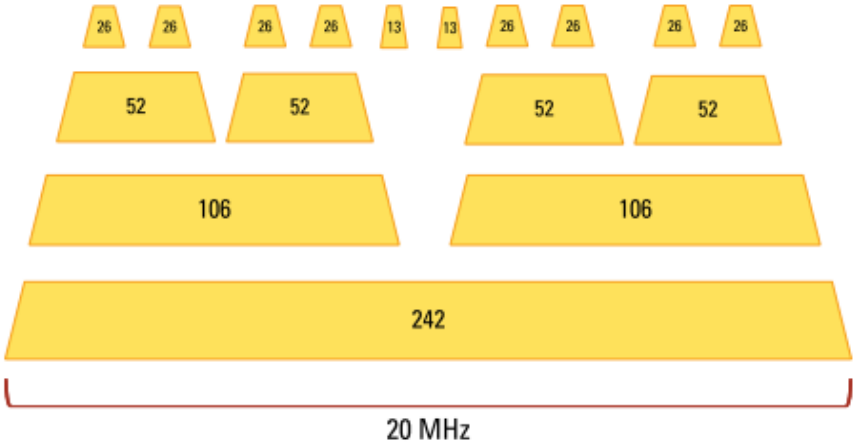
Esimerkiksi tukiasema, joka tukee 802.11n- tai 802.11ac-standardia ja keskustelee käyttäjän laitteen kanssa kummalla protokollalla tahansa, tarvitaan koko kanavan leveys eli kaikki 64 tietoa kantavaa osaa käyttäjän ja tukiaseman väliseen kommunikointiin (Kuvio 5). Laitteiden välinen liikenne on joko datan lähettämistä tai vastaanottamista. Jokainen tukiasemaan yhdistynyt käyttäjä joutuu odottamaan vuoroaan kommunikoida tukiaseman kanssa. (Coleman 2020, 18–19.)



Kuvio 5. OFDM-tekniikan toimintaperiaate (Coleman 2020, 19)

Kun tukiasema sekä käyttäjän laite tukevat 802.11ax-standardia, tukiasema käyttää OFDMA-tekniikkaa laitteiden väliseen liikennöintiin. Niin kuin aiemmin mainit-

tua, 20 MHz:n levyinen kanava on jaettu 256:een osaan. Nämä jaetut osat voidaan koota erikokoisiksi ryhmiksi, joita kutsutaan nimellä RU. Ryhmät voivat olla kanavan leveydeltään kaksi, neljä, tai kahdeksan megahertsiä ja jokaisessa ryhmässä on tietty määrä liikennöintiä varten tietoa kantavia osia (Kuvio 6). Ryhmien määrä riippuu siitä, kuinka monta käyttäjää kommunikoi tukiaseman kanssa samaan aikaan. (Coleman 2020, 19–20.)



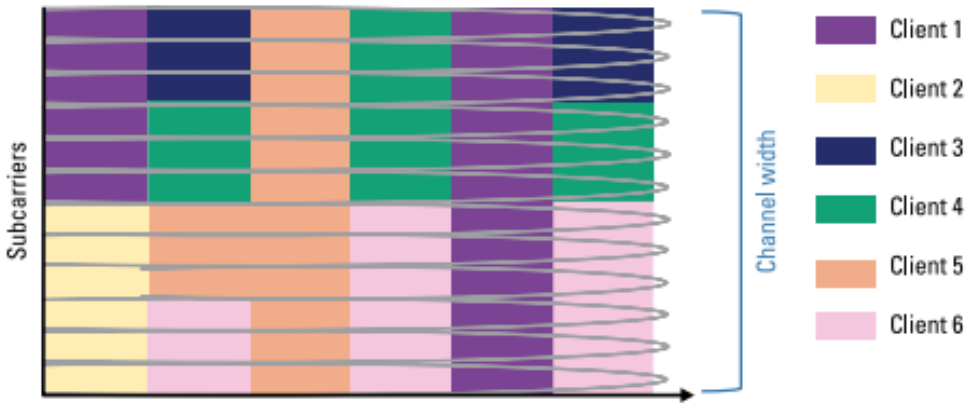
Kuvio 6. OFDMA-tekniikan 20 MHz:n kanavan ryhmäjako. (Coleman 2020, 20)

Käytännön esimerkkinä otetaan tilanne, jossa käyttäjän laite ja tukiasema kommunikoivat keskenään ja käyttäjiä on kaksi kerrallaan, ryhmiä on silloin kaksi eli kummallakin käyttäjällä on 106 tietoa kantavaa osaa käytössään. Ryhmien määrä määräytyy käyttäjien mukaan, eli ryhmiä on sama määrä kuin käyttäjiä. Mikäli palveltavia käyttäjiä on pariton luku, esimerkiksi kolme, yhdellä käyttäjistä on silloin 106 tietoa kantavaa osaa käytettävissään, kun kahdella muulla on käytössään 52 osaa. Maksimimäärä käyttäjiä on kuitenkin 20 MHz:n kanavan leveydellä yhdeksän, koska tietoa kantavia osia ei ole tarpeeksi. (Coleman 2020, 20–21.) Taulukossa 3 on esitelty samaan aikaan palveltavien käyttäjien enimmäismäärä eri kanavan leveyksillä.

Taulukko 3. Käyttäjien enimmäismäärä eri kanavan leveyksillä (Coleman 2020, 21)

Resource Units (RUs)	20 MHz channel	40 MHz channel	80 MHz channel	160 MHz channel	80 + 80 MHz channel
996 (2x) subcarriers	n/a	n/a	n/a	1 client	1 client
996 subcarriers	n/a	n/a	1 client	2 clients	2 clients
484 subcarriers	n/a	1 client	2 clients	4 clients	4 clients
242 subcarriers	1 client	2 clients	4 clients	8 clients	8 clients
106 subcarriers	2 clients	4 clients	8 clients	16 clients	16 clients
52 subcarriers	4 clients	8 clients	16 clients	32 clients	32 clients
26 subcarriers	9 clients	18 clients	37 clients	74 clients	74 clients

Tukiaseman mahdollisuutta kommunikoida käyttäjän laitteiden kanssa kutsutaan nimellä TXOP. Jotta 802.11ax-standardi on yhteensopiva vanhempien standardien kanssa, tukiasemalta tulee oma liikennöintivuoronsa jokaiselle standardille. Kun 802.11ax-standardi saa vuoronsa, tukiasema joko lähettää tietoa käyttäjille tai vastaanottaa tietoa käyttäjiltä (Kuvio 7). OFDMA-tekniikan ryhmäjaon ansiosta useat käyttäjät pystyvät liikennöimään samaan aikaan. (Coleman 2020, 20.)

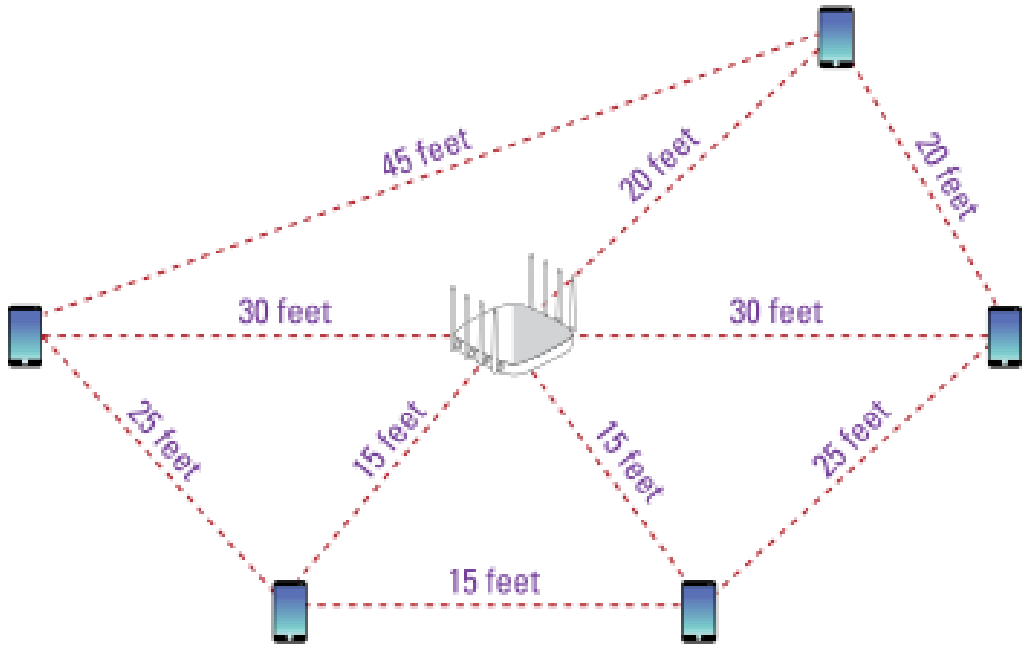


Kuvio 7. OFDMA-tekniikan toimintaperiaate (Coleman 2020, 21)

Wi-Fi-liitto (engl. Wi-Fi Alliance) on sertifioimassa 802.11ax-standardia ja sertifiointi tukee vain neljää eri ryhmää, eli tukiasema liikennöisi maksimissaan neljän eri käyttäjän kanssa samaan aikaan jokaisella TXOP:lla. Tämä johtuu siitä, että

todellisuudessa neljä laitetta maksimissaan kerrallaan liikennöi tukiaseman kanssa. (Coleman 2020, 22.)

802.11ax-standardi tukee myös MU-MIMO-tekniikkaa 802.11ac-standardin tavoin. 802.11ax-standardissa voi jopa kahdeksan laitetta kerrallaan liikennöidä kerrallaan, verrattuna aiempaan standardiin, jossa maksimilaitemäärä oli neljä. Standardi on suunniteltu tukemaan jopa 8x8-MU-MIMO-tekniikkaa, mutta sen hyödyntämisessä on haasteita ympäristöissä, joissa on paljon laitteita, koska laitteiden täytyy olla tarpeeksi kaukana toisistaan, jotta MU-MIMO-tekniikkaa voidaan hyödyntää. Matkaa laitteiden välille vaaditaan, koska spatiaaliset tietovirrat muuten häiriköivät toinen toistaan ja datapaketit eivät saavuta laitetta eheinä. Tästä syystä MU-MIMO-tekniikkaa on hankala toteuttaa ympäristöissä, joissa on paljon laitteita, koska laitteiden välimatkat ovat lyhyitä. (Coleman 2020, 33–34.) Kuviossa 8 on esitetty ihanteellinen laitteiden välimatka MU-MIMO-tekniikkaa varten.



Kuvio 8. Ideaalinen välimatka laitteille MU-MIMO-tekniikkaa varten (Coleman 2020, 34)

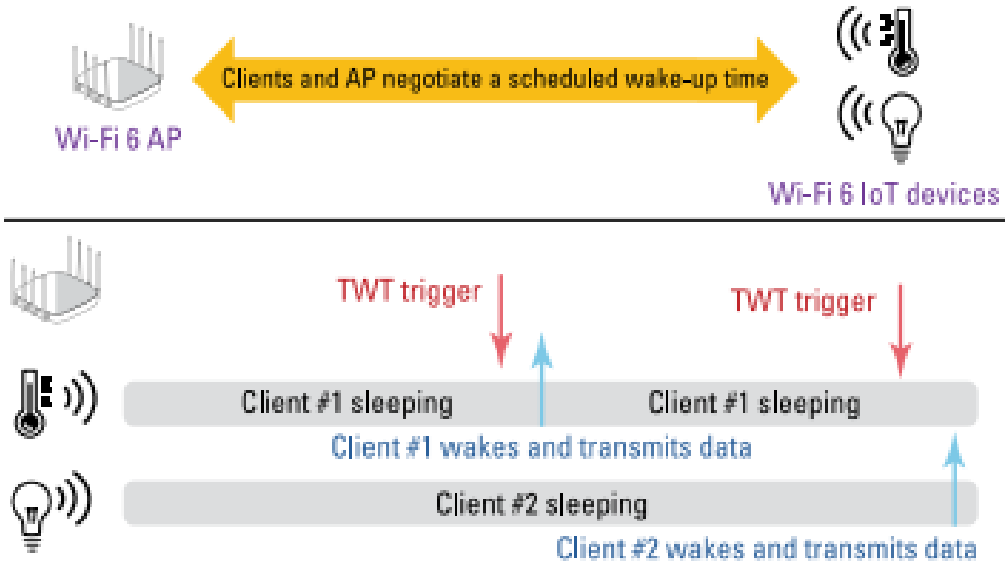
MU-MIMO-tekniikkaa sekä OFDMA-tekniikkaa on mahdollista käyttää kumpaakin samaan aikaan, mutta oletuksena on, että kumpaakin tekniikkaa ei käytetä kommunikoitaessa saman laitteen kanssa. MU-MIMO-tekniikka lähettää usean eri

spatiaalisen tietovirran saman kanavan yli, kun taas OFDMA-tekniikassa kanava jaetaan useaan osaan, joten kumpaakin tekniikkaa ei ole hyödyllistä käyttää yhtä aikaa. (Coleman 2020, 36.) Taulukossa 4 on esitelty MU-OFDMA sekä MU-MIMO-tekniikan pääasialliset erot.

Taulukko 4. Pääasialliset erot OFDMA-tekniikan sekä MU-MIMO-tekniikan välillä (Coleman 2020, 35)

MU-OFDMA	MU-MIMO
Parempi hyötysuhde	Isompi kapasiteetti
Lyhyemmät viiveajat laitteille	Korkeammat nopeudet per laite
Paras sovelluksille, jotka vaativat vähän kaistaa	Paras sovelluksille, jotka vaativat paljon kaistaa

802.11ax-standardin julkaisun myötä julkaistiin myös uusi tekniikka nimeltään TWT. TWT-tekniikka on kehitetty säästämään laitteiden virtaa. TWT-tekniikka perustuu siihen, että tukiasema sekä laite neuvottelevat aikataulut laitteen langattoman verkkokortin liikennöinnille. Kun tukiasemalla on laitteiden ajat tiedossa, tukiasema voi vähentää turhat langattoman verkkokortin herättämiset, kun laitteella ei ole tarvetta liikennöidä ja näin vähentää laitteiden virrankulutusta. (Coleman 2020, 43–44.) Kuviossa 9 on esitetty TWT-tekniikan käytännön toimintatapa laitteiden kanssa.



Kuvio 9. TWT-tekniikan toimintatapa IoT-laitteiden kanssa (Coleman 2020, 44)

Kun verrataan aiempiin standardeihin, laitteiden virrankulutus oli paljon suurempaa, koska langattoman verkkokortin herättämiseen käytettiin tekniikkaa nimeltä DTIM. DTIM-tekniikan arvo määrittää, kuinka usein laitteen langaton verkkokortti herätetään, vaikka liikennöintiä ei olisikaan. Uudella TWT-tekniikalla laitteen langaton verkkokortti voi olla lepotilassa jopa useita tunteja ilman virrankulutusta. (Coleman 2020, 44.)

Vaikka 802.11ax-standardin julkaisun ideana olikin olemassa olevien tekniikoiden mahdollisimman hyvä hyödyntäminen, korkeampia nopeuksia ei siltikään ole jätetty huomioimatta. 802.11ax-standardin edeltäjä 802.11ac-standardi tuki 256-QAM signaalin modulointia, kun taas uusi standardi tukee 1024-QAM modulointia. Uuden modulointitekniikan myötä on päästy jopa 10 Gbps nopeuksiin. (Coleman 2020, 44.)

3 WLAN-KONTROLLERI

Nykyään jokaisessa kahvilassa, hotellissa, yrityksen tiloissa sekä julkisista tiloista löytyy langaton verkko, joka on toteutettu tukiasemilla, joita hallitaan joko WLAN-kontrollerilla tai se on toteutettu mesh-verkkona. WLAN-kontrolleria käytetään siis tukiasemien keskitettyyn hallitsemiseen sekä konfigurointiin. WLAN-kontrollerin kautta voi hallita jokaista tukiasemaa erikseen sekä säätää asetuksia tukiasemakohtaisesti. WLAN-kontrolleri mahdollistaa helpot verkon laajentamismahdollisuudet. (excITingIP 2010.)

3.1 Käyttötarkoitus

Ilman WLAN-kontrolleria jokaisella tukiasemalla joutuisi käydä erikseen säätämässä halutut asetukset. Kun tukiasemia on useita, se veisi todella paljon aikaa tietoliikenne/verkkoasiantuntijalta käydä kirjautumassa jokaisella tukiasemalla erikseen sekä konfiguroida halutut asetukset. Tukiasemat eivät myöskään keskustele keskenään ilman kontrolleria, joten tukiasemat eivät tiedä millä kanavalla toinen tukiasema on ja näin ne voivat häiritä toinen toistaan. (excITingIP 2010.)

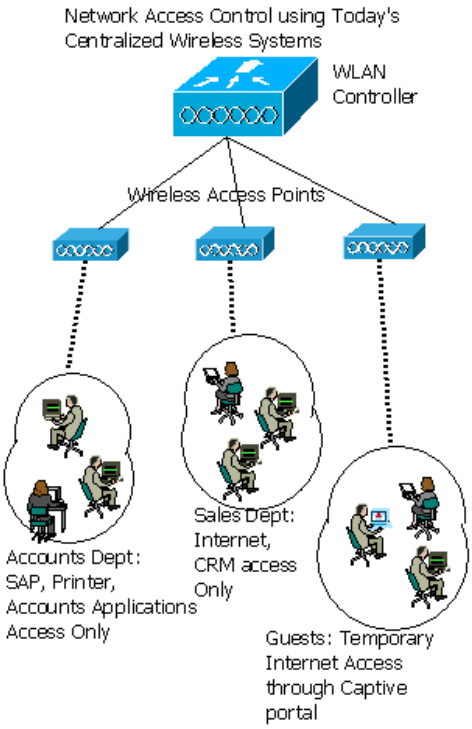
WLAN-kontrollerilla voidaan myös monitoroida langattomien verkkojen statistiikkaa, esimerkiksi tietyn langattoman verkon tiedonsiirtomäärän. WLAN-kontrolleri mahdollistaa tiedonsiirron rajoittamisen joko verkko- tai käyttäjäkohtaisesti. (excITingIP 2010.)

WLAN-kontrollereita on olemassa joko virtuaalisena versiona tai fyysisenä laitteena. Virtuaalisen version voi asentaa omalle virtuaaliselle palvelimelle ja tämä on yleensä halvempi vaihtoehto kuin fyysisen laitteen osto. Etuna virtuaaliseen palvelimeen on se, että palvelimen suoritustehon voi määrittää itse, kun taas fyysisessä laitteessa tulee valmistajan ennalta-asennetut osat.

3.2 Ominaisuudet

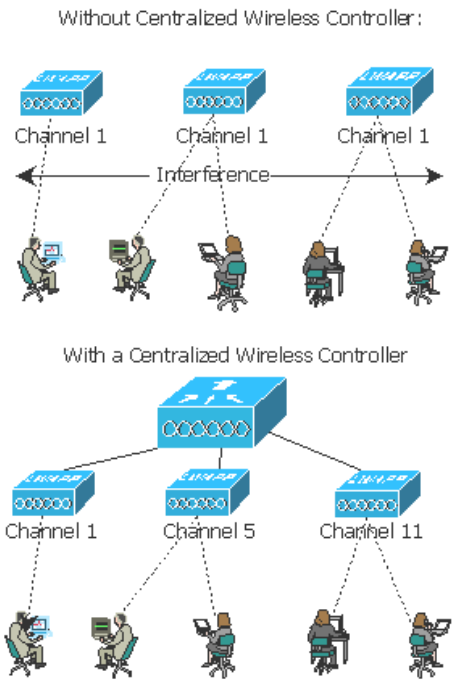
WLAN-kontrolleri tuo paljon hyödyllisiä ominaisuuksia langattoman verkon toteuttamiseen. Yksi paljon käytetty ominaisuus yritysverkoissa on langattomaan verkkoon autentikointi omalla käyttäjätunnuksella, jonka perusteella käyttäjä ohjataan

haluttuun verkkoon. Käyttäjä voidaan ohjata esimerkiksi vain vieraille tarkoitettuun verkkoon tai asiantuntijoille tarkoitettuun verkkoon. WLAN-kontrollerille voidaan määrittää autentikointipalvelin, jonne se ohjaa autentikointipyynnön ja palvelin vastaa pyyntöön sekä ohjaa käyttäjätunnukselle tarkoitetun verkon. (excITingIP 2010.) Kuviossa 10 on esitetty esimerkiksi hallinnon ja myynnin pääsyoikeudet erilaisiin resursseihin kuten tulostimeen ja internettiin.



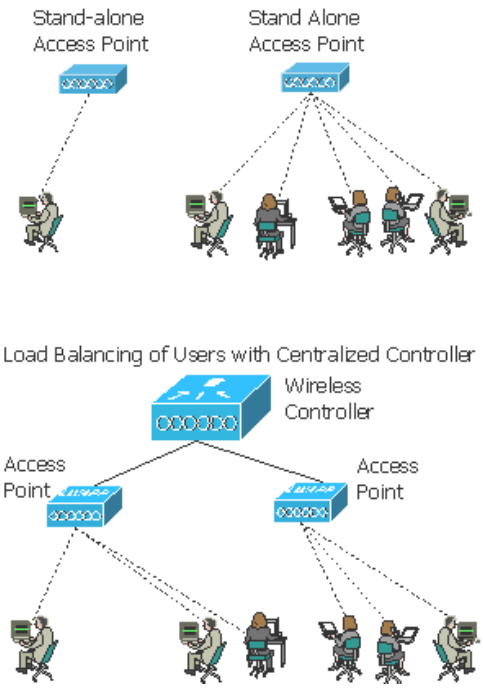
Kuvio 10. Yrityksen henkilöstön pääsyt eri resursseihin (excITingIP 2010)

Yhtenä hyvänä ominaisuutena on muun muassa kanavien automaattinen säätö, jotta tukiasemat eivät lähetä signaaliaan samalla taajuudella häiriten toinen toistaan. Näin kaistaa jää enemmän käyttöön ja kanava ei ruuhkaudu, joten tiedonsiirtonopeudet ovat korkeammat. (excITingIP 2010.) Kuviossa 11 on esitetty tukiasemien kanavat ilman WLAN-kontrolleria sekä WLAN-kontrollerin kanssa.



Kuvio 11. WLAN-kontrollerin hyödyt kanavansäädössä (excITingIP 2010)

Mikäli käyttäjiä on yhdistänyt yhteen tukiasemaan enemmän kuin toiseen lähellä sijaitsevaan tukiasemaan, käyttäjiä jaetaan tukiasemien kesken, jotta tukiasema ei olisi niin ruuhkautunut ja tiedonsiirto ei hidastuisi (excITingIP 2010). Kuviossa 12 on esitetty automaattinen kuormantasaaminen tukiasemien välillä.



Kuvio 12. Automaattinen kuormantasaaminen tukiasemien välillä (excITingIP 2010)

4 TUKIASEMA

Tukiasemalla tarkoitetaan laitetta, jolla kaiutetaan langattomia verkkoja, joista käyttäjä pääsee kiinni internettiin sekä erinäisiin resursseihin, esimerkiksi yrityksen omaan intraan. Tukiasemat lähettävät signaalia 2,4 GHz:n sekä 5 GHz:n taajuudella. Niitä löytyy nykypäivänä jokaisesta esimerkiksi jokaisen hotellin tiloista sekä lentokentiltä (Kuvio 13).

Kuvio 13. Cisco C9115AX Wi-Fi 6-tukiasema (Cisco 2020a)

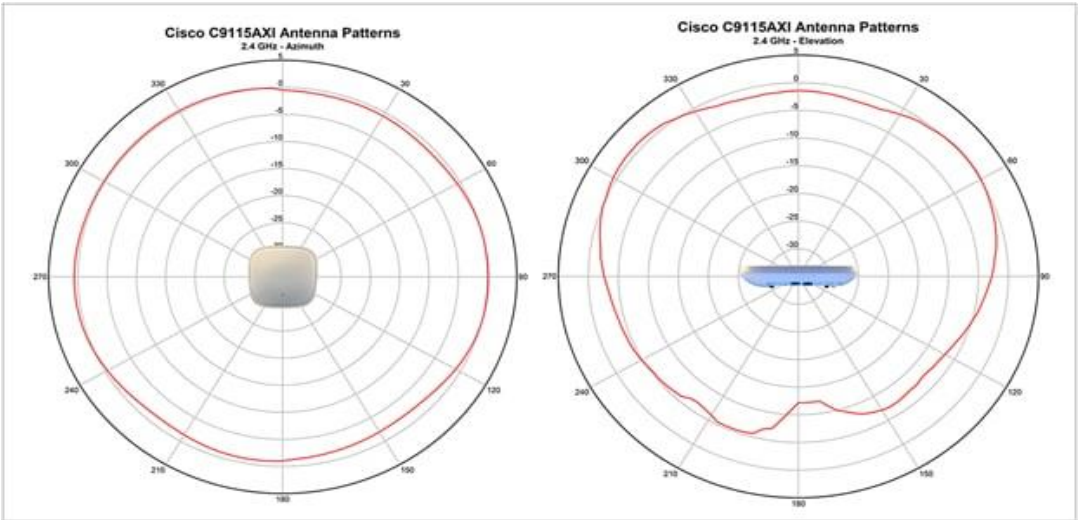
4.1 Käyttötarkoitus

Tukiasemilla voidaan rakentaa halutun rakennuksen tai tilan kokonaan kattava langaton verkko. Tukiasemia käytetään paljon yrityksissä, koska tukiaseman asentamisella ja käyttöönotolla käyttäjät pääsevät internettiin ilman fyysistä yhteyttä verkkolaitteeseen, kuten kytkimeen tai reitittimeen.

Tukiasema vaatii fyysisen yhteyden verkkolaitteeseen, kuten kytkimeen tai reitittimeen. Tukiasemat vaativat myös sähkönsyötön toimiakseen. Sähkönsyöttö on yleensä toteutettu PoE-sähkönsyötöllä, eli virta tukiasemalle tulee verkkokaapelin kautta, mutta on myös olemassa virtalähdettä tukevia versioita.

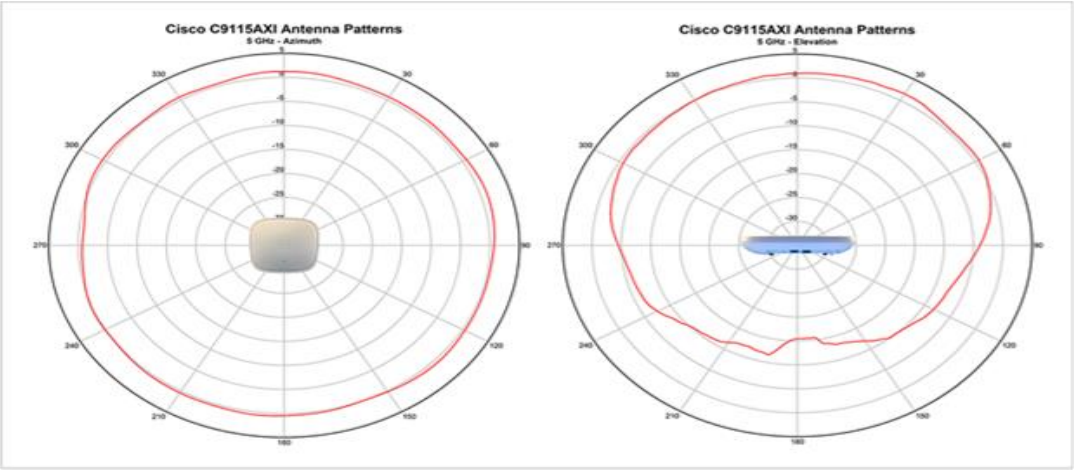
4.2 Ominaisuudet

Cisco C9115AX-tukiasema lähettää signaaliaan ympyränmuotoisessa kuviossa. Tukiaseman takapuolelle signaalin kuuluvuus on heikompi, jolloin tukiaseman takana signaalin kantavuus ei ole niin pitkä (Kuvio 14). (Cisco 2020a)



Kuvio 14. Cisco C9115AX-tukiaseman 2,4 GHz:n signaalin kuuluvuus eri puolille tukiasemaa (Cisco 2020a)

5 GHz signaali ei kuulu materiaalien läpi yhtä hyvin kuin 2,4 GHz, koska signaalin aallon tiheys on korkeampi, joten se ei lävistä materiaaleja niin hyvin. Tukiasema olisi suositeltavaa asentaa siis takapuoli kattoa päin, jolloin saavutetaan paras kuuluvuus (Kuvio 15).



Kuvio 15. Cisco C9115AX-tukiaseman 5 GHz:n signaalin kuuluvuus eri puolille tukiasemaa (Cisco 2020a)

5 KÄYTTÖÖNOTTO

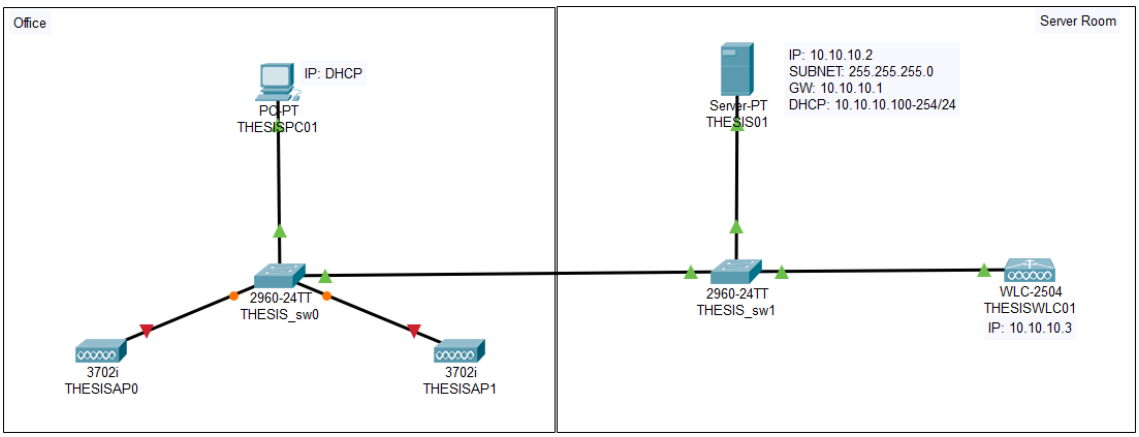
WLAN-kontrollerin käyttöönotto toteutettiin virtuaalisessa ympäristössä, Cisco Packet Tracer -simulaatio-ohjelman avulla. Toteutuksessa on kaksi eri huonetta, joihin on sijoitettu laitteita. Virtuaalinen ympäristö kuvaa normaalin toimiston mahdollista asettelutapaa.

Työ siirrettiin operatiivisesta järjestelmästä virtuaaliselle alustalle tietoturvallisista syistä. Käyttöönoton vaiheet pystyttiin toteuttamaan vapaammin virtuaalisessa ympäristössä. Tässä työssä tehtyjä havaintoja ja tuloksia voidaan hyödyntää operatiivisessa järjestelmässä.

Virtuaalisen ympäristön ominaisuuksien rajallisuuden vuoksi en pystynyt toteuttamaan esimerkiksi RADIUS-autentikoinnin perusteella verkkoon ohjaamista. Tukiasemien ominaisuuksien konfigurointi oli myös rajattu pois.

5.1 Verkon määritykset

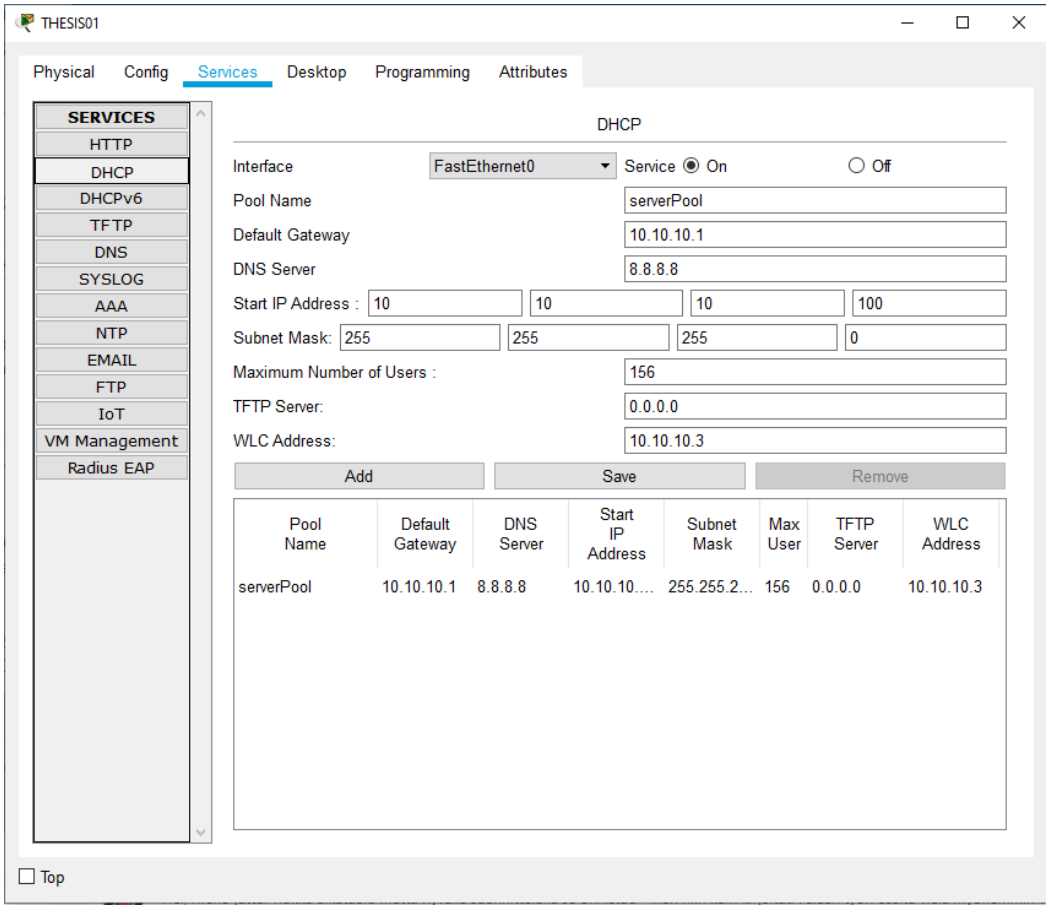
Käyttöönottoa varten rakensin virtuaaliseen ympäristöön kaksi eri tilaa, joissa verkkolaitteet sijaitsevat. Verkkolaitteina kuvassa ovat tietokone THESISPC01, DHCP- sekä RADIUS-palvelin THESIS01, kytkimet THESIS_sw0 ja THESIS_sw1 sekä WLAN-kontrolleri THESISWLC01 (Kuvio 16).



Kuvio 16. Virtuaalisen käyttöönottoympäristön asettelu

Palvelimelle konfiguroin DHCP- sekä RADIUS-palvelut käyttöön. DHCP-palvelu otettiin käyttöön, jotta tukiasemat, työasemat sekä langattomat laitteet saavat IP-osoitteen ilman kiinteän IP-osoitteen määrittämistä. Tällä saavutetaan mahdollisimman nopea ja vaivaton verkkoon pääsy.

Määritin virtuaaliympäristön aliverkoksi 10.10.10.0/24, josta DHCP-alueena toimii 10.10.10.100–254. Oletusyhdyskäytävänä toimii aliverkon ensimmäinen osoite sekä DNS-osoitteena Googlen DNS-palvelin. DHCP-poolille piti myös asettaa WLAN-kontrollerin osoite WLC Address -kenttään, jotta tukiasemat löytävät WLAN-kontrollerille verkkoon kytkeytyessään (Kuvio 17).

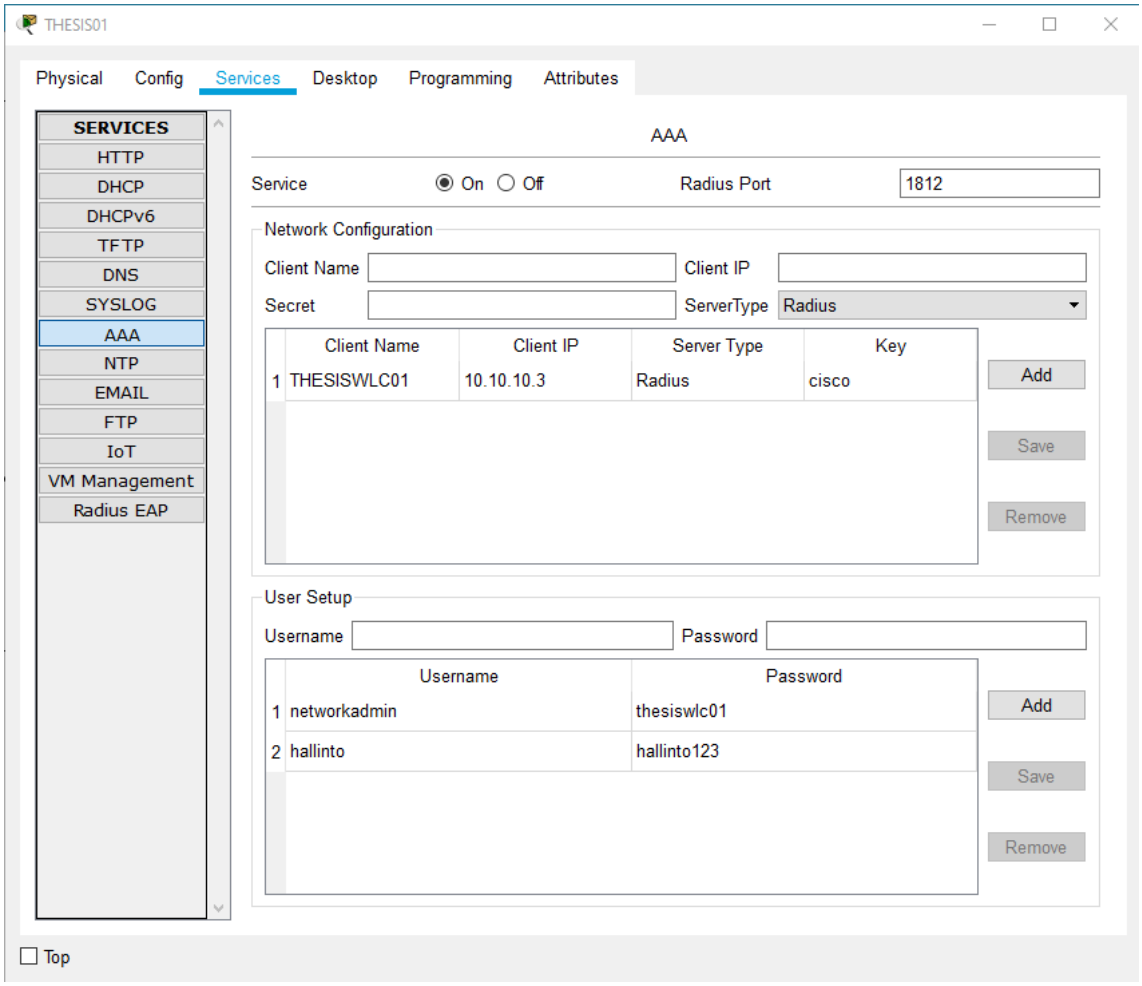


Kuvio 17. DHCP-alueasetukset THESIS01-palvelimella

Määritin myös THESIS01-palvelimelle RADIUS-palvelun käyttöön. Mikäli verkko joskus laajentuu, autentikointi esimerkiksi uudelle WLAN-kontrollerille voidaan hoitaa samalla käyttäjätunnuksella, eikä jokaiselle kontrollerille tarvitse erikseen

määritellä paikallisia tunnuksia. Näin käyttäjätunnuksien muokkaaminen on helppoa ja se vaihtuu kaikkiin laitteisiin samalla kertaa.

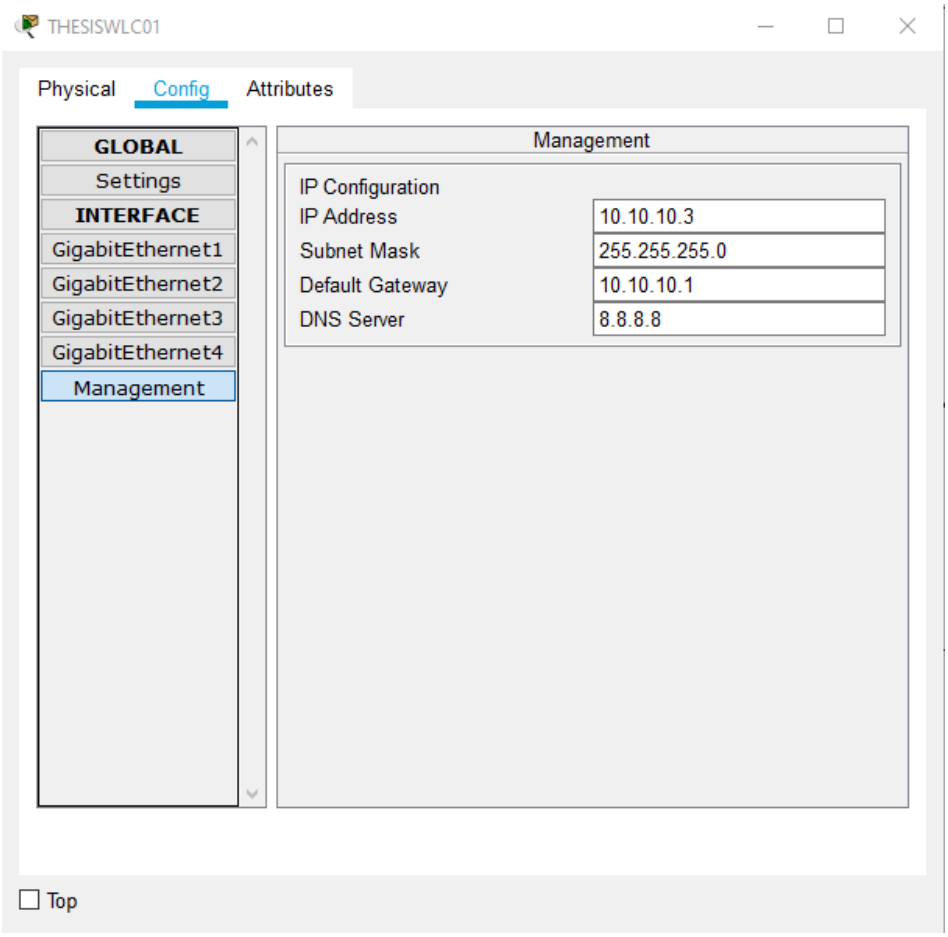
RADIUS-palveluun määritin autentikoinnin portiksi 1812. Lisäsin myös WLAN-kontrollerin RADIUS-palvelun käyttäjäksi. Jokaiselle RADIUS-käyttäjälle määritetään oma salasana. Tässä tapauksessa käytin sanaa cisco, joka täytyy myös määrittää WLAN-kontrollerin päässä samaksi palvelinta konfiguroidessa. Tein myös kaksi käyttäjää, joita käytetään kirjautumiseen. Kuvitteellisen yrityksen hallinnolla sekä tietoliikenteestä vastaavalla tiimillä on erilaiset käyttäjätunnukset (Kuvio 18).



Kuvio 18. RADIUS-määritykset THESIS01-palvelimella

Seuraavana vaiheena määritin THESISWLC01-nimiselle WLAN-kontrollerille IP-osoitteen luomastani aliverkosta. Määritin IP-osoitteeksi 10.10.10.3 WLAN-kont-

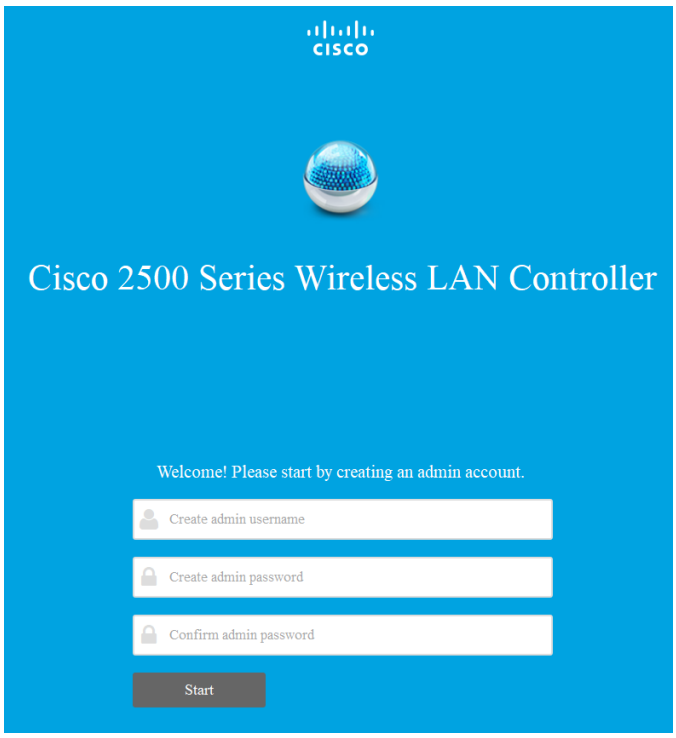
rollerin Management-porttiin sekä oletusyhdyskäytäväksi 10.10.10.1, DNS-osoitteeksi Googlen DNS-palvelimen sekä aliverkon maskiksi 255.255.255.0 (Kuvio 19). IP-osoite määrityksien jälkeen WLCTHESIS01-nimiseen WLAN-kontrolleriin voidaan ottaa etäyhteys.



Kuvio 19. Virtuaalisen THESISWLC01-kontrollerin IP-määritykset

5.2 WLAN-kontrolleri

Tietokone THESISPC01 on saanut DHCP-palvelimelta osoitteen, joka sijaitsee samassa aliverkossa WLAN-kontrollerin kanssa. Tämä mahdollistaa yhteyden ottamisen kontrolleriin, jotta käyttöönotto voidaan aloittaa. WLAN-kontrolleriin otetaan etäyhteys syöttämällä selaimeen WLAN-kontrollerin IP eli 10.10.10.3, minkä jälkeen avautuu ikkuna, jossa käsketään luoda paikallinen hallintatunnus (Kuvio 20).

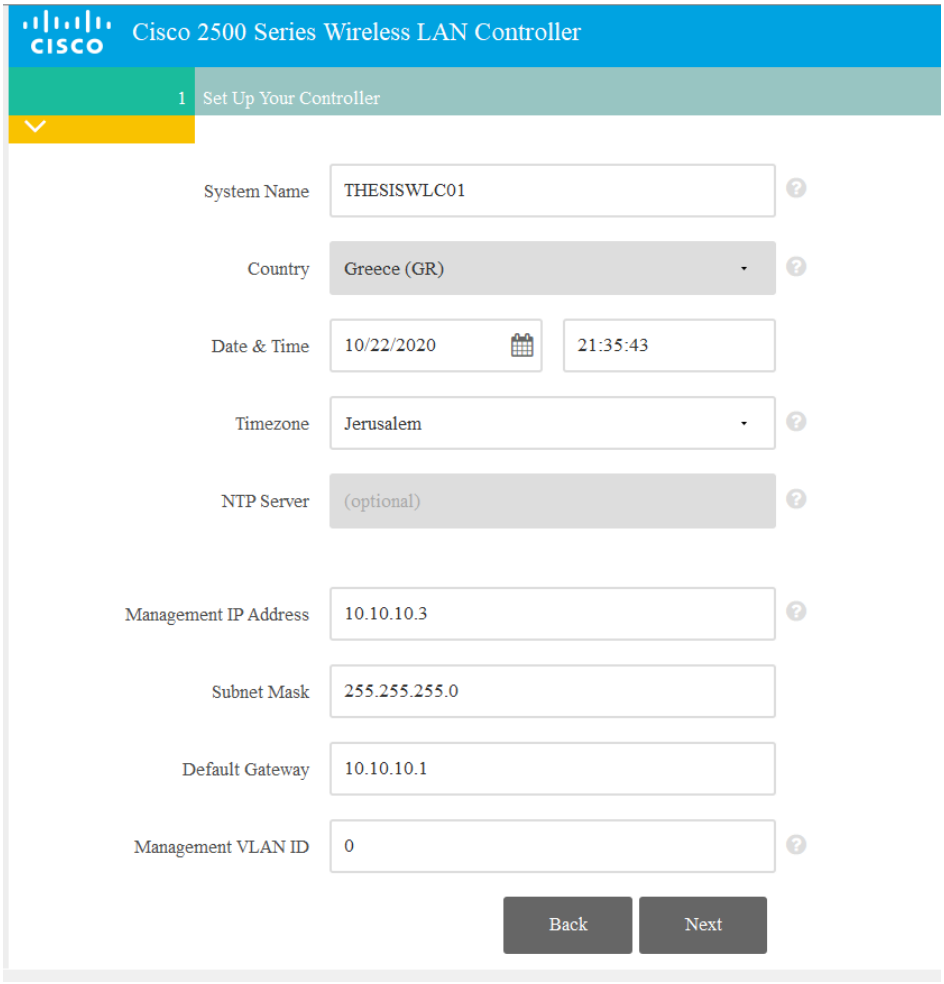


Kuvio 20. Paikallisen käyttäjän määritys käyttöönottovaiheessa

Paikallinen tunnus täytyy luoda käyttöönotettaessa, koska RADIUS-autentikointi konfiguroidaan vasta myöhemmässä vaiheessa. Paikallista käyttäjätunnusta tarvitaan myös, mikäli yhteys RADIUS-palvelimeen katoaa, paikalliset käyttäjätunnukset ovat silloin ainoa tapa kirjautua sisään.

Määritin käyttäjätunnukseksi adminin sekä salasanaksi Opinnaytetyo2020. Iso alkukirjain on vaatimus salasanassa. Ilman isoa alkukirjainta salasanassa WLAN-kontrolleri ei päästä seuraavaan vaiheeseen. Napauttamalla Start-nappia päästään käyttöönoton seuraavaan vaiheeseen.

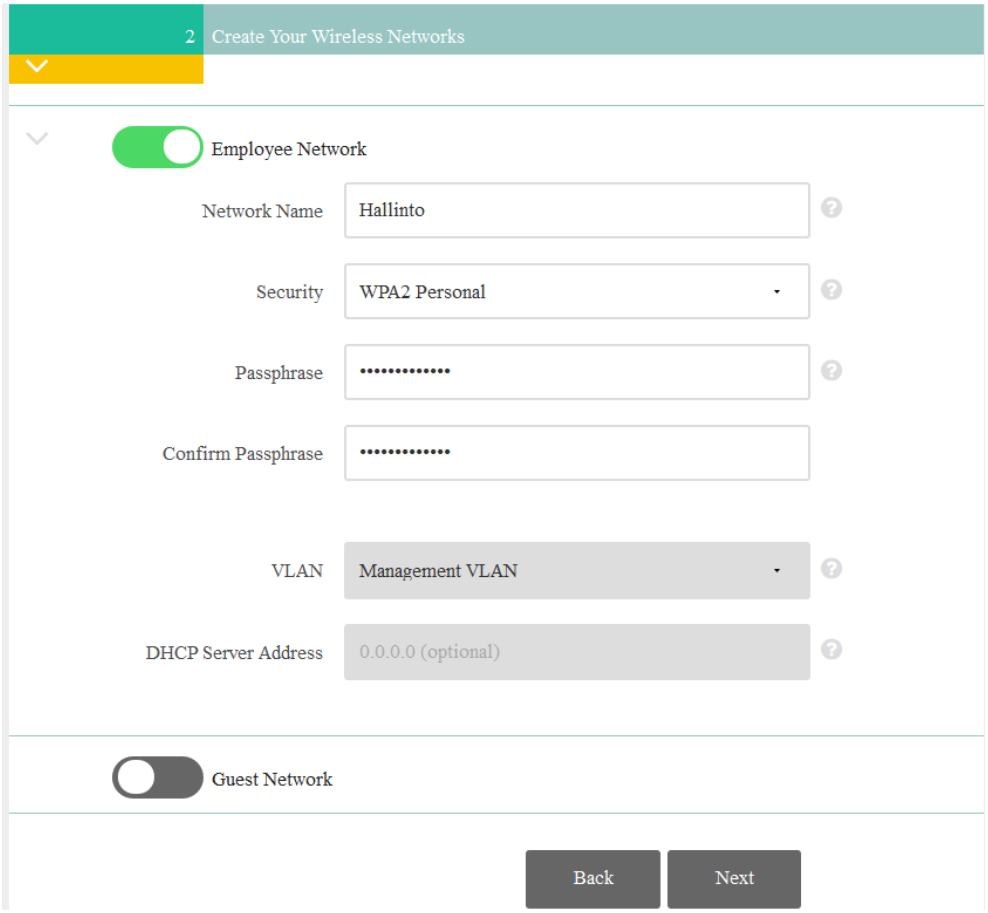
Seuraavassa käyttöönottovaiheessa WLAN-kontrollerille määritellään järjestelmälle nimi, aika-alue, maa, NTP-palvelin (ei pakollinen) sekä IP-määritykset. Määrittelin nimeksi aiemmin mainitsemani nimen THESISWLC01. IP-osoitteeksi määrittelin aiemmin mainitut arvot eli 10.10.10.3, aliverkon maskiksi 255.255.255.0 sekä oletusyhdyskäytäväksi 10.10.10.1 (Kuvio 21).



Kuvio 21. Määritetyt asetukset käyttöönottovaiheessa

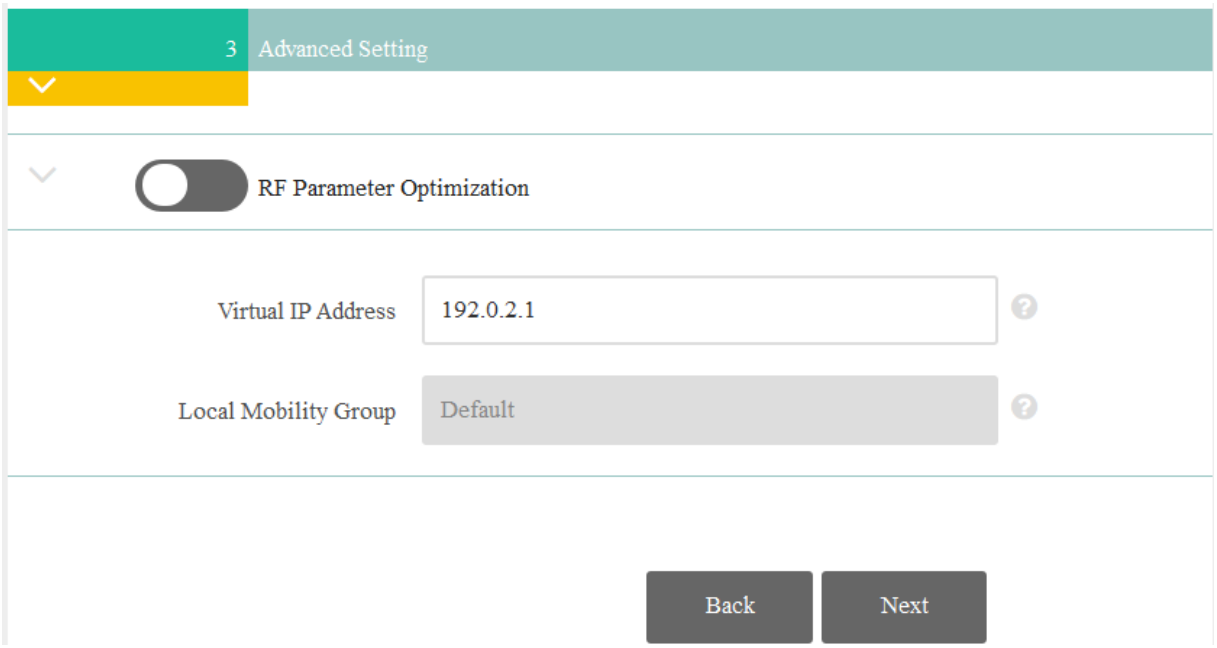
Kuviossa 21 nähdään, että maaksi on määritetty Kreikka sekä aika-alueeksi Jerusalem. Näitä ei virtuaalisessa ympäristössä voinut muuttaa. Tämä johtuu siitä, että Kreikassa on sama aika kuin Suomessa sekä Jerusalemin aika-alue on sama Helsingin kanssa. Asetukset otetaan käyttöön painamalla Next-nappia.

Käyttöönottovaiheessa WLAN-kontrollerille täytyy myös määrittää yksi langaton verkko. Langattomalle luodaan verkon nimi sekä sille määritetään salasana sekä salasanan suojaustyyppi. Langattomalle verkolle voidaan myös määrittää VLAN sekä DHCP-palvelimen osoite, mutta tässä opinnäytetyössä näitä ei tuettu simulaatio-ohjelman rajallisten ominaisuuksien vuoksi (Kuvio 22).



Kuvio 22. Langattoman verkon luonti käyttöönottovaiheessa

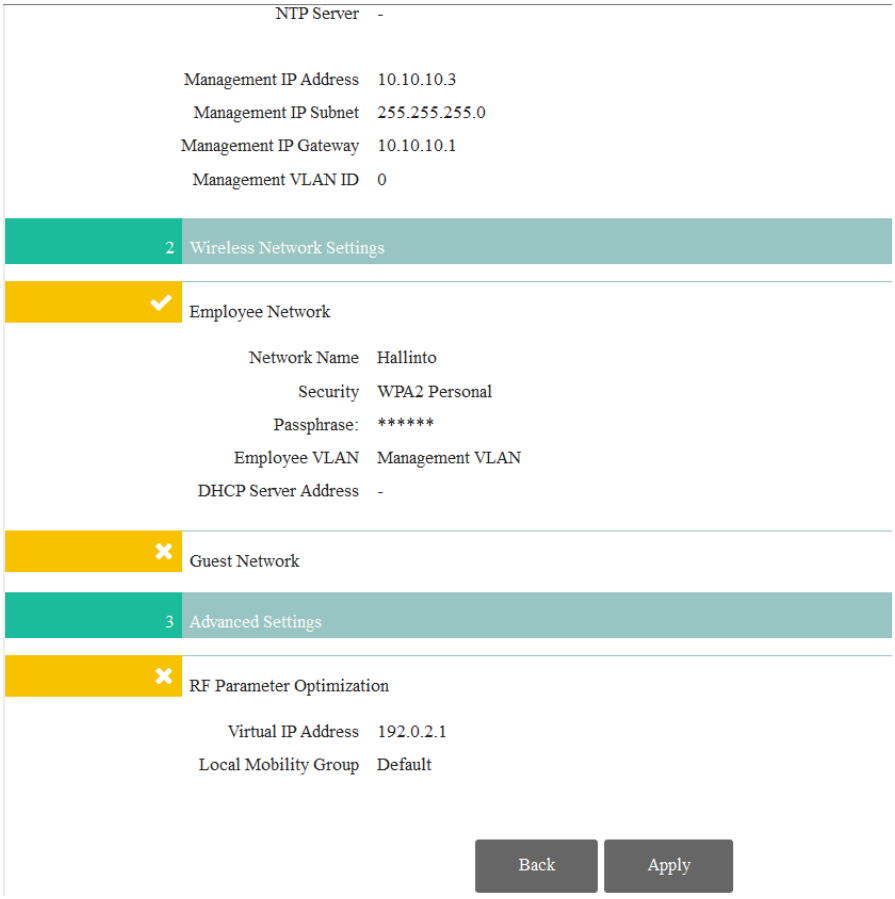
WLAN-kontrollerille asetetaan myös virtuaalinen IP-osoite sekä ryhmä (Kuvio 23). Ryhmän kautta useat WLAN-kontrollerit voivat jakaa tietoa esimerkiksi käyttäjistä, kunhan ne ovat samassa ryhmässä (Antunes 2019).



Kuvio 23. Virtuaalisen IP-osoitteen sekä ryhmän määritys käyttöönottovaiheessa

WLAN-kontrollerille on luotu langaton verkko nimeltään Hallinto, jossa käytetään salauksena WPA2-Personal eli käyttäjän itse määrittämää langattoman verkon salasanaa. Asetin salasanaksi tyontekija123.

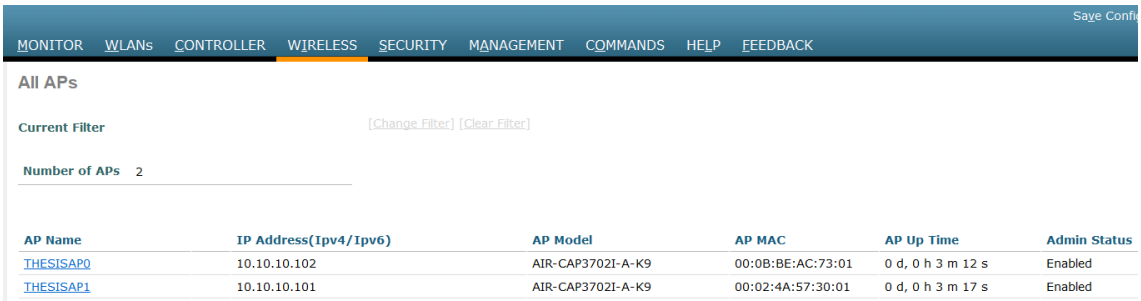
Kun kaikki aiemmat vaiheet on suoritettu, asetukset täytyy vielä vahvistaa, jotta ne otetaan käyttöön. Tässä vaiheessa on hyvä tarkistaa, että kaikki määritellyt asetukset ovat niin kuin niiden pitää. WLAN-kontrolleri tallentaa asetukset sekä käynnistää itsensä uudelleen (Kuvio 24).



Kuvio 24. Asetuksien vahvistus käyttöönottovaiheessa

Uudelleenkäynnistyksen jälkeen WLAN-kontrollerille ei enää pääse kiinni käyttäen HTTP-protokollaa. WLAN-kontrolleri ottaa automaattisesti käyttöön HTTPS-protokollan, joten tämä täytyy huomioida, kun etäyhteyttä otetaan uudelleen WLAN-kontrolleriin selaimen kautta.

Käyttöönoton jälkeen tukiasemat voidaan kytkeä verkkoon, jolloin ne hakevat DHCP-palvelimelta osoitteen ja nousevat kontrollerin ”Wireless” välilehdelle konfiguroitaviksi. Kuviossa 25 nähdään WLAN-kontrollerin löytäneet tukiasemat.



Kuvio 25. Tukiasemat WLAN-kontrollerilla

6 KONFIGUROINTI

WLAN-kontrollerin konfigurointi aloitetaan ensin kirjautumalla sisään aiemmin luoduilla käyttäjätunnuksilla, josta päästään WLAN-kontrollerin hallintapaneeliin. Kirjautumisen jälkeen kaikki tarvittavat ominaisuudet voidaan määritellä.

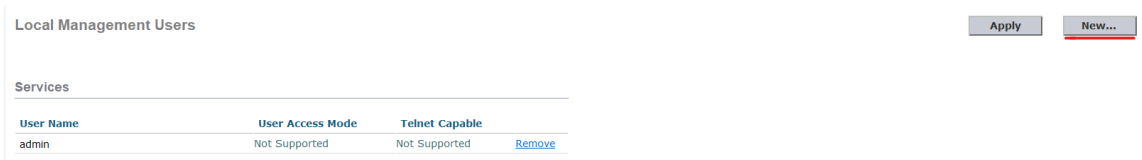
Kun halutut määritykset on asetettu kontrollerille, täytyy muistaa painaa kontrollerin oikeassa yläreunassa sijaitsevaa Save Configuration -nappia. Mikäli virransyöttö katkeaa WLAN-kontrolleriin, kaikki määritetyt asetukset säilyvät. Jos tätä toimenpidettä ei suorita, WLAN-kontrolleri palaa siihen tilaan missä viimeksi tätä nappia on painettu.

6.1 Käyttäjätunnukset

Kirjautuminen WLAN-kontrollerille voidaan hoitaa joko RADIUS-autentikoinnilla, joka tarkoittaa siis, että kirjautuminen hyväksytään erikseen määritellyllä palvelimella. WLAN-kontrollerille voidaan myös määrittää paikallinen käyttäjätunnus, jolla on täydet käyttöoikeudet. Paikallisen käyttäjätunnuksen muokkaaminen sekä lisääminen alkaa Management-välilehdeltä (Kuvio 26).

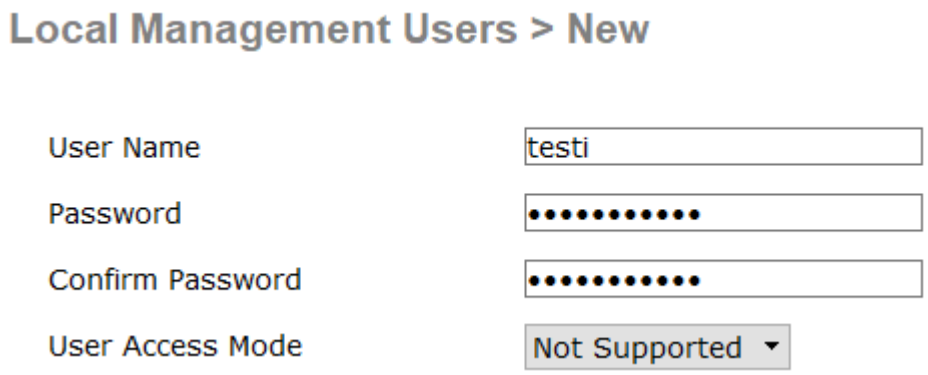
Kuvio 26. Välilehden sijainti navigointipalkissa

Sivupalkista valitaan Local Management Users -välilehti, josta päästään näkemään kaikki WLAN-kontrollerille määritetyt paikalliset käyttäjätilit sekä muokkaamaan niitä. Oletuksena käyttäjätunnus on admin, jolla on oletuksena kaikki oikeudet. Käyttäjätunnukselle voidaan määrittää haluttu salasana. Uuden käyttäjätunnuksen luonti onnistuu oikealta ylhäältä löytyvästä New-napista (Kuvio 27).



Kuvio 27. Kaikki paikalliset käyttäjätunnukset

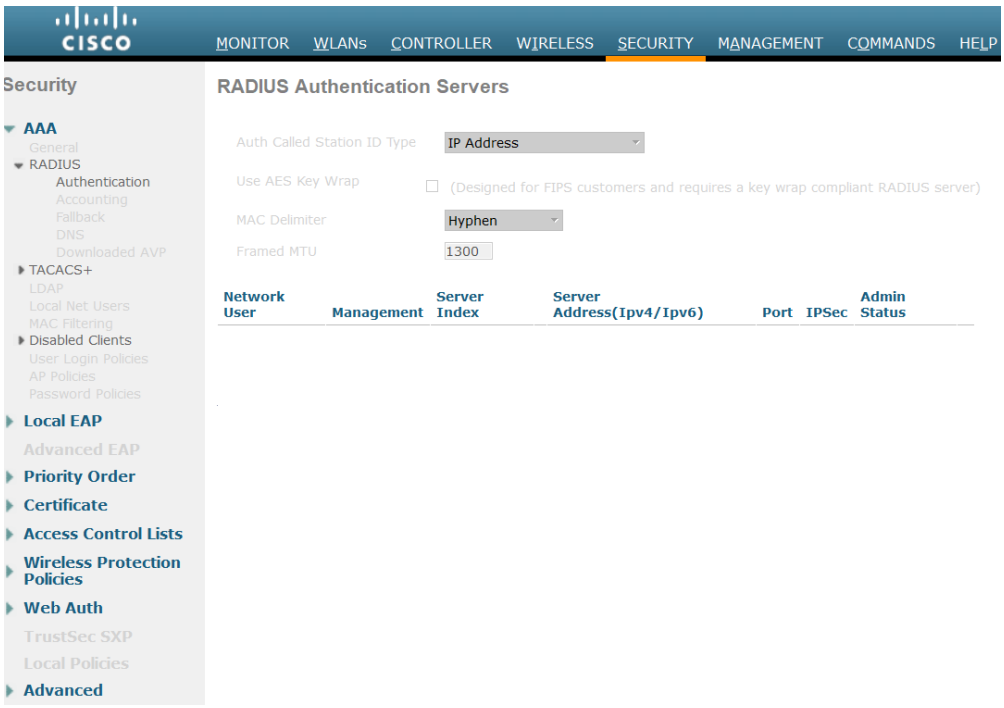
Napin painalluksen jälkeen avautuu ikkuna, josta määritellään käyttäjätunnuksen nimi sekä sille määritellään salasana. Tässä tapauksessa tein käyttäjätunnuksen, jonka nimi on testi ja sille määrittelin salasanaksi testitunnus123 (Kuvio 28). Tunnus vahvistetaan oikealta ylhäältä löytyvällä Apply-napilla, jonka jälkeen se ilmestyy paikallisten hallintakäyttäjien listalle.



Kuvio 28. Uuden käyttäjätunnuksen luonti

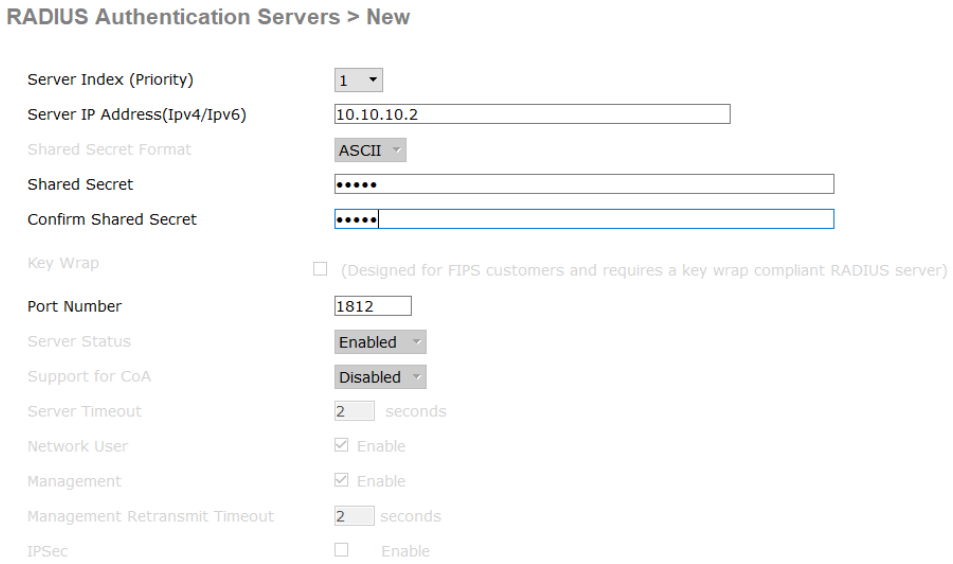
6.2 RADIUS-palvelimen määritys

WLAN-kontrollerille voidaan määrittää RADIUS-palvelin, jonka kautta autentikoidutaan esimerkiksi langattomaan verkkoon. RADIUS-palvelimen määritys aloitetaan kontrollerin Security-välilehdeltä (Kuvio 29). Sivupalkista löytyy välilehti AAA, josta valitaan RADIUS, jonka alta löytyy valinta Authentication, josta palvelin päästään määrittämään. (Cisco 2012.)



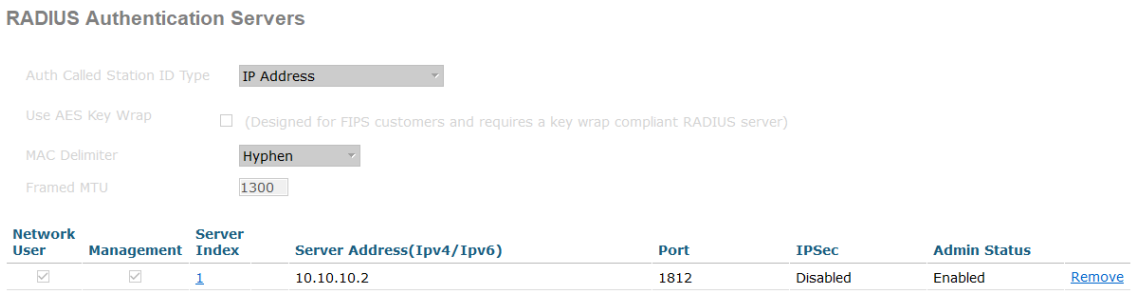
Kuvio 29. RADIUS-palvelimen määritysikkuna

Aloitetaan uuden palvelimen määritys klikkaamalla oikealta yläkulmasta löytyvää New-painiketta, josta päästään RADIUS-palvelimen määritysikkunaan. Palvelimelle määritetään järjestysnumero, palvelimen osoite, salasana sekä portin numero (Kuvio 30).



Kuvio 30. RADIUS-palvelimen määritys

Määritin palvelimeksi aiemmin luomani RADIUS-palvelimen osoitteen sekä palvelimelle määrittämäni salasanan eli cisco. Asetin tämän RADIUS-palvelimen ensimmäiseksi järjestyksessä. Määrittelin RADIUS-palvelimelle autentikoitumisen portiksi 1812, joten sen täytyy olla sama myös WLAN-kontrollerin päässä. Palvelimen määritys hyväksytään Apply-napilla, jolloin se ilmestyy RADIUS-palvelimet listalle. (Kuvio 31).



Kuvio 31. RADIUS-palvelin määritettynä

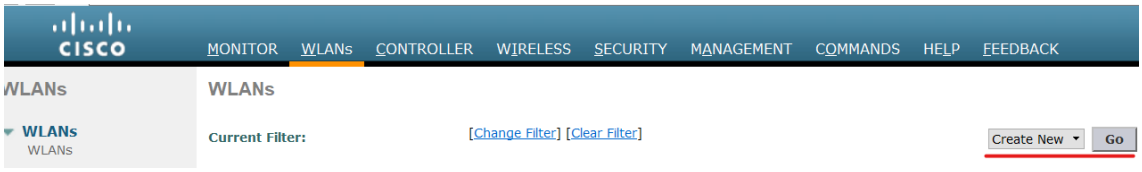
6.3 Tukiasemat

Tukiasema hakee DHCP:llä IP-osoitteen ja alkaa etsiä WLAN-kontrolleria verkosta. Kun tukiasema löytää WLAN-kontrollerin, se lataa uusimman ohjelmistoversion ja päivittää sen tukiasemalle, jolloin tukiasema käynnistää itsensä uudelleen uusimmalla ohjelmistoversiolla. Mikäli tukiasemat ovat eri aliverkossa WLAN-kontrollerin kanssa, täytyy näillä aliverkoilla olla yhteys keskenään, jotta tukiasema löytää WLAN-kontrollerille. (Cisco 2020b.)

Tukiasema täytyy muuttaa FlexConnect-tilaan, jotta se osaa ohjata tietoja tukiasemaan liittyen WLAN-kontrollerille. Mikäli yhteys WLAN-kontrolleriin häviää, on sillä kuitenkin tiedossa WLAN-kontrollerilla määritetyt asetukset muistissaan ja se voi jatkaa normaalia toimintaa. Opinnäytetyössä käytetyssä simulaatio-ohjelmassa tukiasemat menivät automaattisesti FlexConnect-tilaan. (Cisco 2020b.)

6.4 Langattomat verkot

Uusi langaton verkko luodaan WLAN-kontrollerin WLANs-välilehdeltä. Aloitetaan uuden verkon luonti valitsemalla alasvetovalikosta Create New-asetus ja napauttamalla Go-nappia (Kuvio 32).

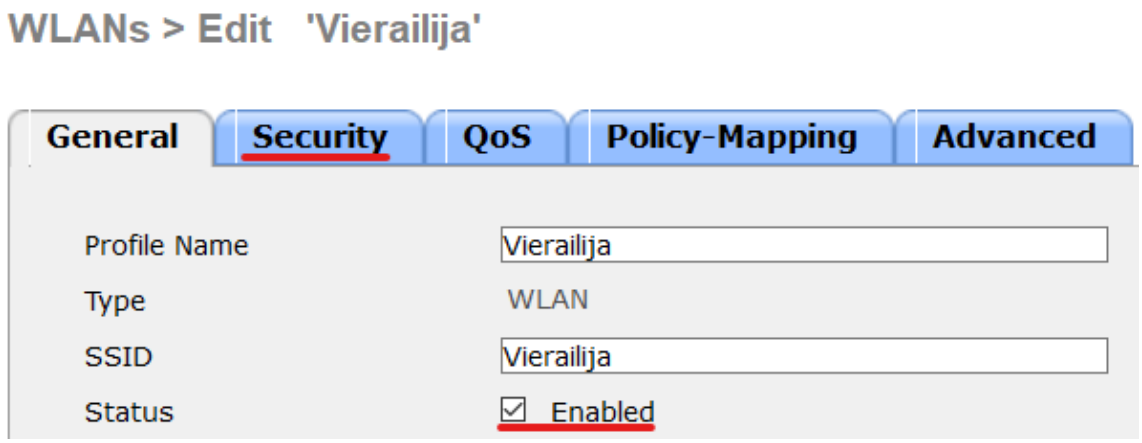


Kuvio 32. Langattoman verkon luonnin aloitus

Loin uuden langattoman verkon vieraita varten. Nimesin verkon profiilin nimeksi Vierailija sekä langattoman verkon nimeksi Vierailija. Langattoman verkon asetuksien määrittelyyn siirrytään alleviivatusta Apply-napista (Kuvio 33).

Kuvio 33. Langattoman verkon profiilin määritys sekä nimeäminen

Uusi langaton verkko on oletuksena pois päältä. Verkko täytyy ottaa käyttöön laittamalla rasti Enabled-laatikkoon, joka on alleviivattuna kuviossa 34. Tämän jälkeen voidaan siirtyä langattoman verkon salauksen määrittelemisen välilehdelle eli Security.

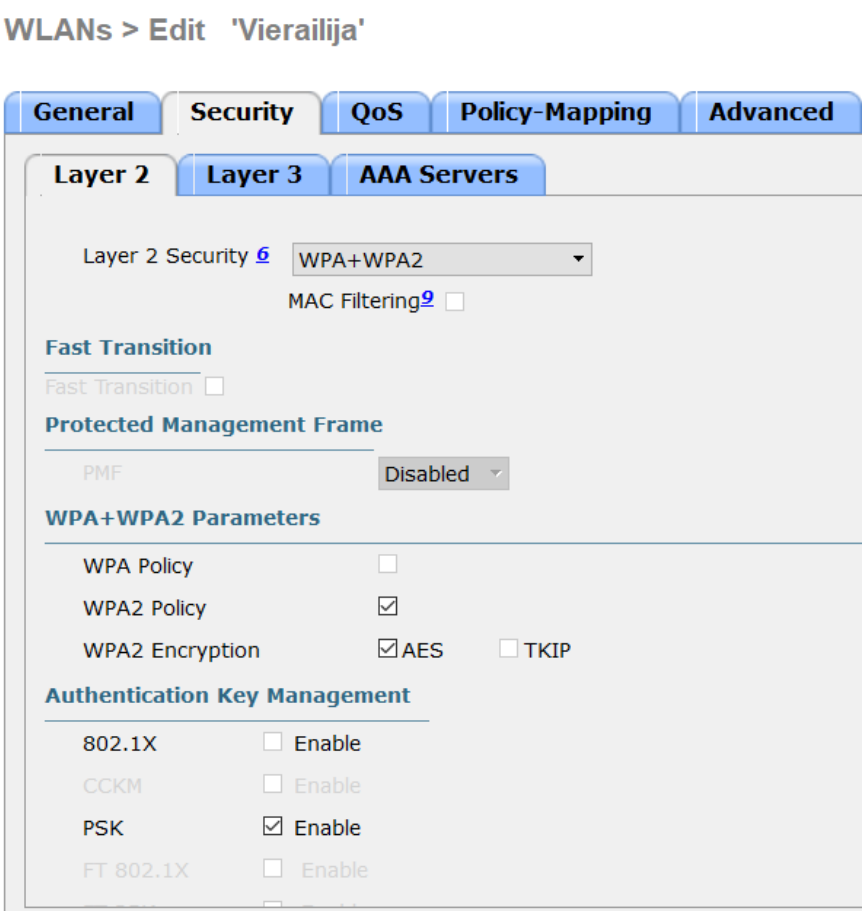


Kuvio 34. Langattoman verkon aktivointi sekä salauksen välilehden sijainti

6.4.1 Autentikointi salasanalla

Oletuksena langattomalla verkolla ei ole mitään salausta. Langattomalle verkolle suositellaan kuitenkin laittamaan salasana, koska jos salasanaa ei ole, kuka tahansa voi käyttää langatonta verkkoa ja esimerkiksi salakuunnella verkossa liikkuvia datapaketteja.

Määritin langattoman verkon salaukseksi WPA2-asetuksen valitsemalla Layer 2 Security -valikosta valinnan WPA+WPA2 sekä laittamalla rastit WPA2 Policy- sekä WPA2 Encryption -laatikoihin. Laitoin myös rastin AES-laatikkoon. Tällä määrityksellä sain käyttöön AES-koodauksen, jotta salasanaa ei voi helposti murtaa. Laitoin vielä rastin PSK-laatikkoon, jotta sain määritettyä verkolle salasanan. Salasanaksi määritin Vierailija123, jonka syötin PSK Format -kenttään (Kuvio 35). Kaikki verkkoon tehdyt muutokset otin käyttöön napauttamalla Apply-nappia.

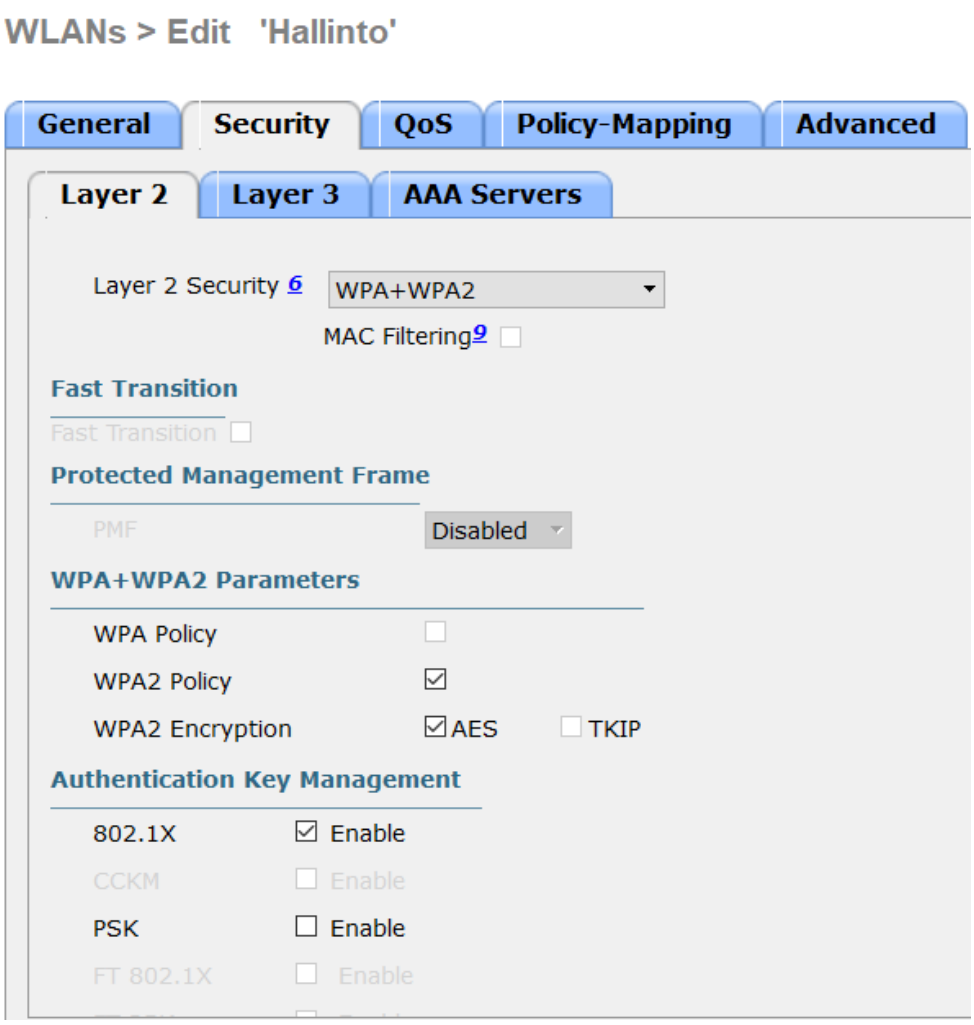


Kuvio 35. Konfiguroitavat kentät salasanalliselle verkolle

6.4.2 RADIUS-palvelimella autentikointi

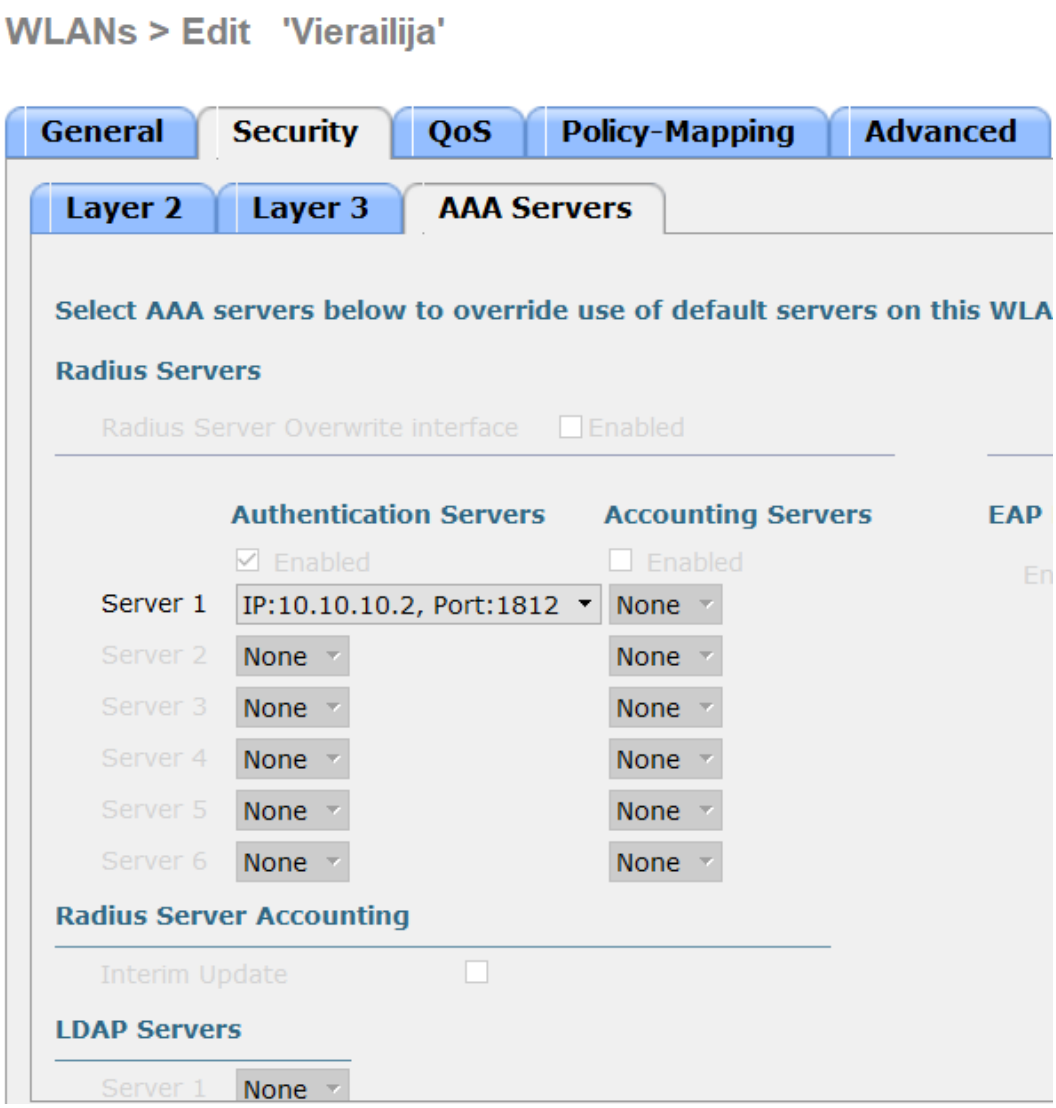
Muutin aiemmin luodun Hallinto-nimisen langattoman verkon RADIUS-palvelimen kautta autentikoitavaksi. RADIUS-palvelimella voidaan ohjata käyttäjä eri verkkoon käyttäjätunnuksen perusteella esimerkiksi myynnin työntekijät omaan verkkoonsa sekä hallinnon työntekijät omaansa. Virtuaaliympäristössä palvelimella verkon ohjaus ei ollut mahdollista virtuaaliympäristön rajoitteiden takia.

Valitsin WLANs-välilehdeltä Hallinto-verkon ja menin Security-välilehdelle aloittaakseni konfiguroinnin. Valitsin Layer 2 Security -valikosta WPA+WPA2 -asetuksen, jotta sain WPA2-salauksen käyttöön. Laitoin myös rastit WPA2 Policy- sekä WPA2 Encryption -laatikoihin. Laitoin myös AES-salauksen päälle laittamalla rastin AES-laatikkoon. Otin myös käyttöön 802.1X-ominaisuuden, jotta autentikointitapa muuttuu RADIUS-palvelimen kautta meneväksi (Kuvio 36).



Kuvio 36. Konfiguroitavat kentät RADIUS-palvelimen kautta autentikoitumiselle

Seuraavaksi siirryin AAA Servers -välilehdelle ja valitsin Radius Servers -otsikon alta Server 1 -kohdalta alasvetovalikosta WLAN-kontrollerille määrittelemäni RADIUS-palvelimen, jonka kautta verkkoon yhdistävä käyttäjä autentikoituu. Kuvissa 37 nähdään RADIUS-palvelin valittuna langattomalle verkolle.

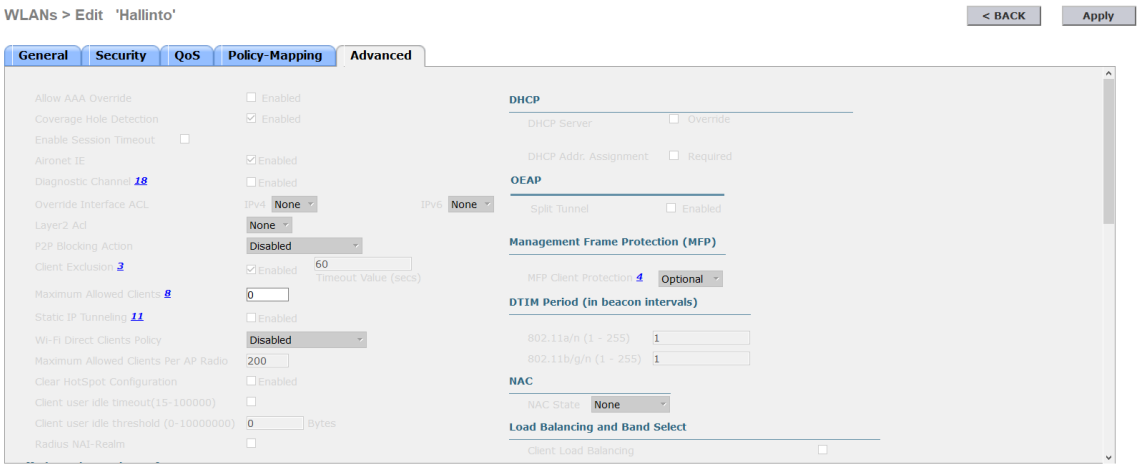


Kuvio 37. RADIUS-palvelimen valinta autentikoinnin palvelimeksi

6.4.3 Lisäasetukset

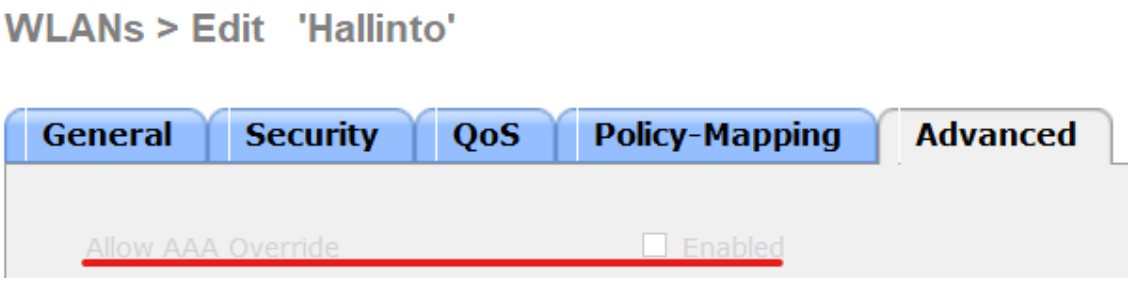
Langattoman verkon lisäasetuksien määrittelyyn pääsee siirtymällä Advanced-välilehdelle (Kuvio 38). Lisäasetuksista voidaan määritellä erikseen verkolle esimerkiksi verkkoon yhdistäneen käyttäjän IP-osoitetiedon saaminen, RADIUS-

palvelimelta saatujen tietojen perusteella verkon ohjaus ja DHCP-palvelin. Simulaatio-ohjelman rajallisten ominaisuuksien vuoksi en voinut toteuttaa kaikkia ominaisuuksia.



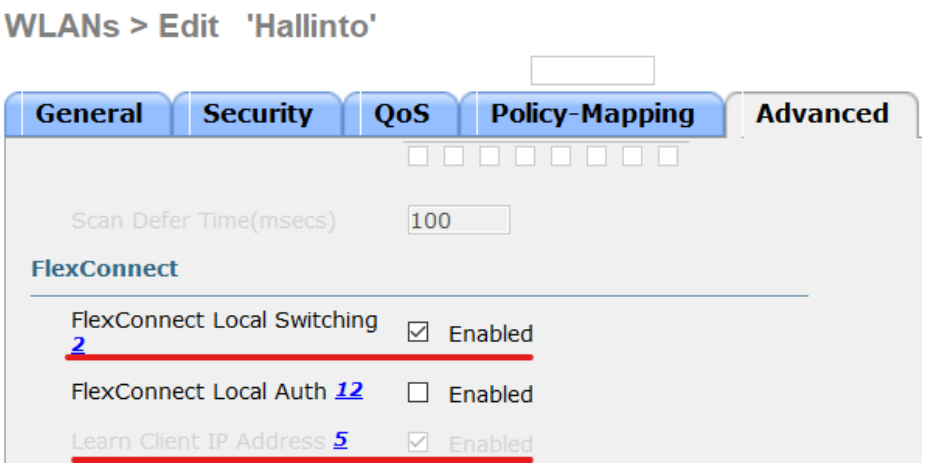
Kuvio 38. Lisäasetuksien määritysikkuna

RADIUS-palvelimelta saatujen tietojen perusteella verkon ohjaus otetaan käyttöön laittamalla rasti Allow AAA Override -laatikkoon (Kuvio 39). Tämä ominaisuus otetaan yleensä käyttöön, mikäli verkkoon kirjaudutaan erillisen RADIUS-palvelimen kautta (Cisco 2020c).



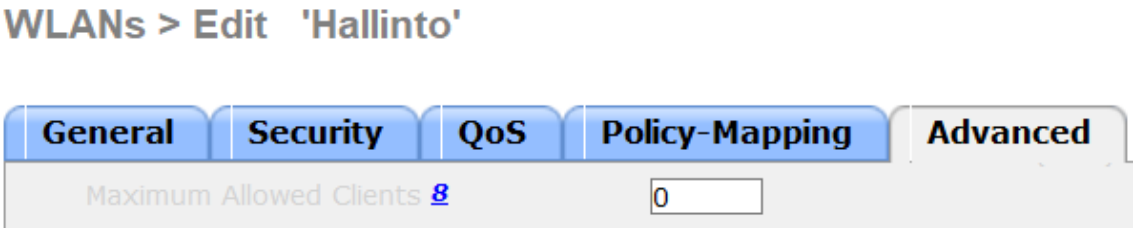
Kuvio 39. Allow AAA Override -asetuksen sijainti

Langattomaan verkkoon yhdistävien laitteiden IP-osoitteet saadaan tietoon laittamalla ensin päälle FlexConnect Local Switching -asetus, jonka jälkeen WLAN-kontrolleri antaa vasta ottaa käyttöön Learn Client IP Address -asetuksen (Kuvio 40).



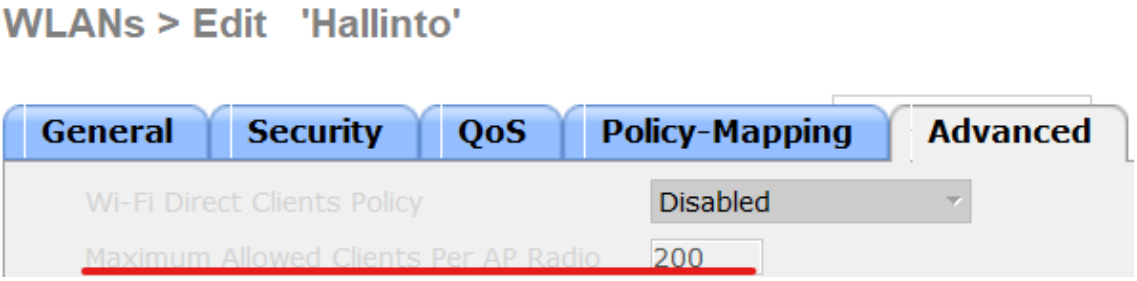
Kuvio 40. Learn Client IP Address- sekä FlexConnect Local Switching -asetukset

Koko langattomalle verkolle voidaan myös määrittää käyttäjien enimmäismäärä, eli kuinka monta käyttäjää verkossa saa olla yhdistyneenä kerrallaan. Oletuksena arvo on 0 eli rajaton määrä (Kuvio 41).



Kuvio 41. Käyttäjien enimmäismäärä langattomalle verkolle

Vaihtoehtoisesti käyttäjien enimmäismäärän voi määrittää myös tukiaseman 2,4 GHz:n sekä 5 GHz:n lähettimille. Oletuksena arvo on 200, eli 200 käyttäjää voi olla yhdistyneenä kerrallaan yhteen lähettimeen (Kuvio 42).

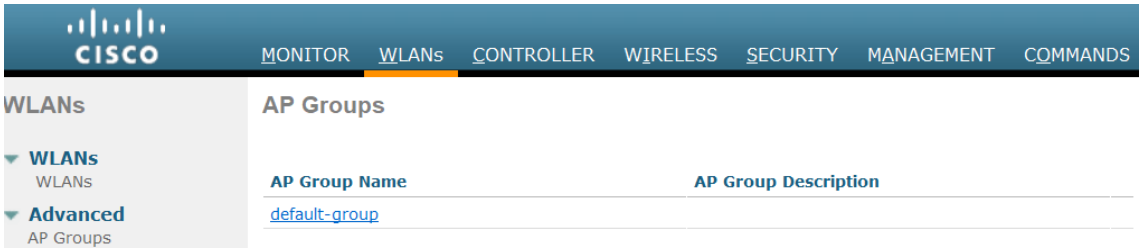


Kuvio 42. Käyttäjien enimmäismäärä/lähetin

6.5 Langattoman verkon ryhmät

Tukiasemat täytyy lisätä langattoman verkon ryhmiin, jotta ne kaiuttavat langattomia verkkoja. Ryhmiä voi luoda useita, mutta yksi tukiasema ei voi kuulua kuin yhteen ryhmään. Langattoman verkon ryhmässä määritetään ryhmään kuuluvat langattomat verkot sekä tukiasemat.

Langattomien verkkojen ryhmiin pääsee kontrollerin WLANs-lehdeltä ja valitsemalla vasemmasta palkista Advanced-otsikon alta AP Groups -valinta. Oletuksena WLAN-kontrollerilla on olemassa ryhmä nimeltään default-group, johon oletuksena kuuluvat kaikki uudet luodut langattomat verkot sekä kaikki WLAN-kontrollerille nousevat tukiasemat (Kuvio 43).



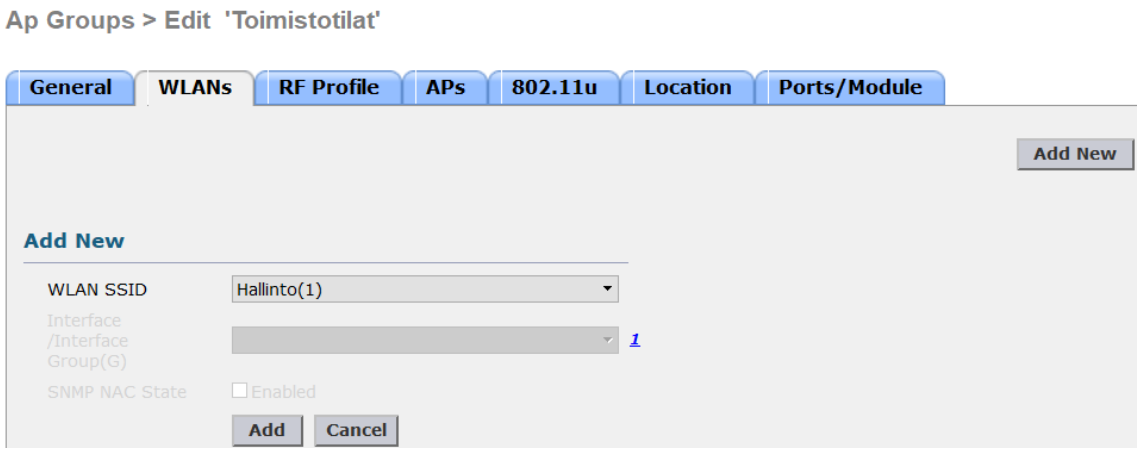
Kuvio 43. Langattomien verkkojen ryhmät

Tässä työssä tein kaksi eri ryhmää nimeltään Julkinen sekä Toimistotilat. Ideana on, että toimistotiloissa ei kuulu vierailijoille tarkoitettua langatonta verkkoa ja julkisissa tiloissa ei kuulu hallinnon langatonta verkkoa.

Ryhmän luonti alkaa oikealta ylhäältä löytyvällä Add Group -napilla. Ryhmän nimi syötetään AP Group Name -kenttään sekä ryhmälle voi antaa kuvauksen Description-kenttään. Ryhmän määrittely aloitetaan Add-napilla. Annoin ryhmälle nimeksi Toimistotilat sekä kuvauksen samalla nimellä (Kuvio 44).

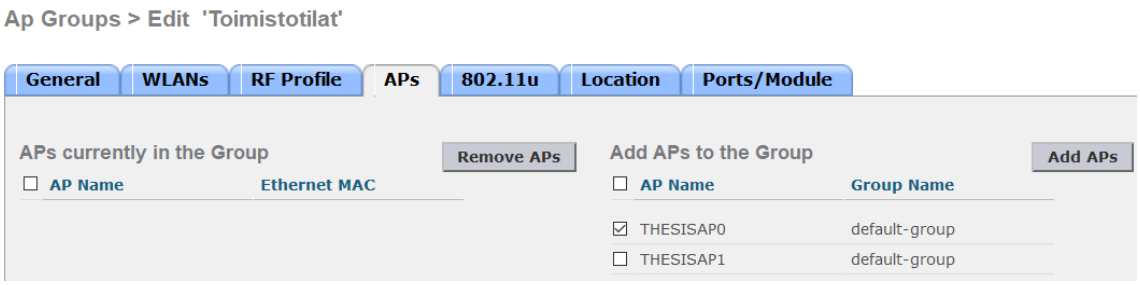
Kuvio 44. Langattoman verkon ryhmän nimeäminen

Siirryin WLANs-välilehdelle, jotta pystyin määrittämään ryhmälle sille kuuluvat langattomat verkot. Lisäsin langattoman verkon Add New -napista, josta pääsin lisäämään Hallinto-nimisen langattoman verkon. Lisäsin verkon painamalla Add-nappia, jonka jälkeen se ilmestyi langattomien verkkojen listalle (Kuvio 45).



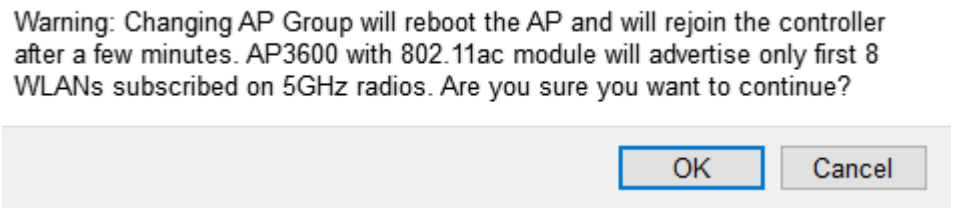
Kuvio 45. Langattoman verkon lisäys ryhmälle

Seuraavaksi määritin ryhmään kuuluvat tukiasemat, eli Toimistotilat-ryhmään lisättävät tukiasemat kaiuttavat vain ryhmälle määritettyä langatonta verkkoa. Ryhmään lisääminen alkaa APs-välilehdeltä. Tukiasema valitaan Add APs to the Group -otsikon alta ja napautetaan Add APs -nappia, jonka jälkeen tukiasema ilmestyy APs currently in the Group -otsikon alle. Jos tukiasema kuului aiemmin toiseen ryhmään, se poistuu muista ryhmistä automaattisesti. Lisäsin THESISAP0-tukiaseman Toimistotilat-nimiseen langattoman verkon ryhmään (Kuvio 46).



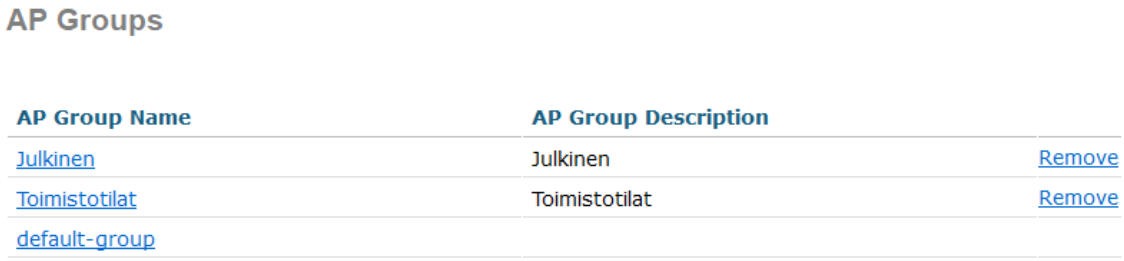
Kuvio 46. Tukiaseman lisäys langattoman verkon ryhmään

WLAN-kontrolleri ilmoittaa, että tukiasema käynnistetään uudelleen ja se yhdistyy uudelleen kontrolleriin muutaman minuutin kuluttua. Tämä voidaan hyväksyä napauttamalla OK-nappia, jolloin tukiasema ottaa määritellyt asetukset käyttöön uudelleenkäynnistyksen jälkeen (Kuvio 47).



Kuvio 47. WLAN-kontrollerin ilmoitus tukiaseman uudelleenkäynnistämisestä

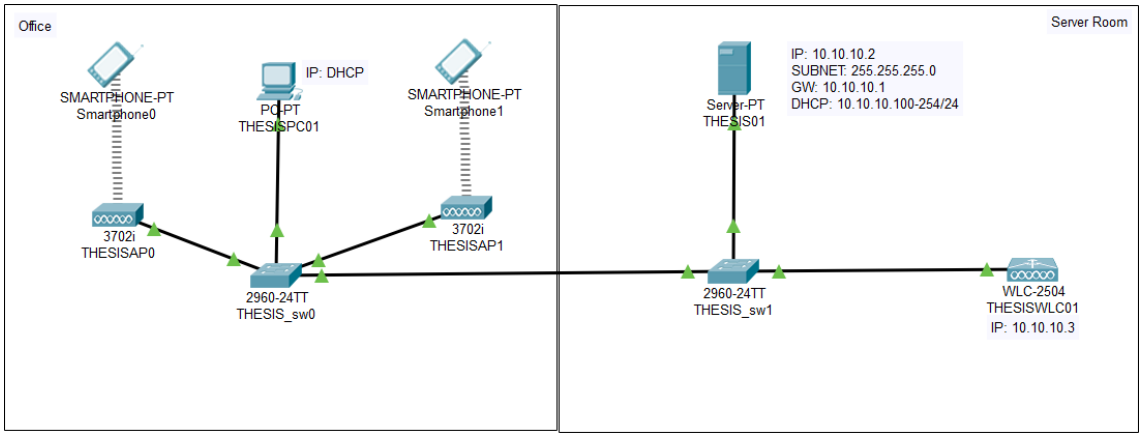
Tein myös ryhmän nimeltään Julkinen, johon lisään THESISAP1-tukiaseman. THESISAP0-tukiasema kaiuttaa vain Hallinto-nimistä langatonta verkkoa sekä THESISAP1-tukiasema kaiuttaa vain Vierailija-nimistä langatonta verkkoa (Kuvio 48).



Kuvio 48. Ryhmät luotuna kontrollerille

Ryhmien luonnin jälkeen tukiasemat kaiuttavat vain niille määriteltyjä verkkoja. Verkkojen toimivuus voidaan testata langattomilla laitteilla, jotka yhdistetään näihin verkkoihin.

Testausta varten sijoitin kaksi puhelinta virtuaaliseen ympäristöön. Smartphone0-niminen puhelin on yhdistetty Hallinto-nimiseen langattomaan verkkoon käyttäjätunnuksilla ja Smartphone 1-niminen puhelin yhdistetty Vierailija-nimiseen verkkoon sille määritellyllä salasanalla (Kuvio 49).



Kuvio 49. Laitteet yhdistettynä langattomiin verkkoihin

7 POHDINTA

Tämän opinnäytetyön tavoitteena oli esitellä IEEE:n julkaisemat 802.11-standardit keskittyen uusimpaan 802.11ax-standardiin eli Wi-Fi 6:een. Opinnäytetyössä käsiteltiin WLAN-kontrollerin ja tukiaseman kuvaus sekä niiden käyttötarkoitus. Näillä aiheilla oli tarkoitus antaa lukijalle peruskäsitys langattomien verkkojen komponenteista sekä standardeista. Pääaiheena oli kuitenkin Cisco-merkkisen WLAN-kontrollerin käytännön käyttöönotto sekä ominaisuuksien konfigurointi.

Standardeista, WLAN-kontrollerin tieto-osuudesta ja tukiasemista kirjoittaessani käytin internetistä löytyviä artikkeleita sekä e-kirjoja. Luin myös Ciscon internet-sivuilta löytyviä dokumentteja käyttöönottoa sekä konfigurointia kirjoittaessani. Cisco Packet Tracer -simulaatio-ohjelman ominaisuuksien rajallisuuden vuoksi en voinut käytännössä toteuttaa kaikkia konfiguroitavia ominaisuuksia. Aiheen rajaamisessa täytyi miettiä kaikki olennaisimmat asiat, sillä WLAN-kontrollerissa on todella paljon ominaisuuksia mitä voi eri tilanteissa konfiguroida käyttöön, mutta tässä työssä keskitytään vain perus ominaisuuksien konfigurointiin.

Käyttöönotto sekä konfigurointi olivat helppo toteuttaa, koska käyttöliittymä on selkeä ja helppo käyttää. Tavoitteenani tällä opinnäytetyöllä oli osoittaa, että kuinka WLAN-kontrolleri otetaan käyttöön sekä konfiguroidaan. Kuka tahansa voi käyttää tätä työtä esimerkiksi operatiivisessa järjestelmässä toimivan WLAN-kontrollerin konfigurointiin.

Opinnäytetyötä kirjoittaessa ja toteuttaessa opin, että minkälainen prosessi sekä kuinka ison työmäärän takana WLAN-kontrollerin saattaminen toimintakuntoon on. Huomasin, että prosessi oli melko helppo ja kivuton suorittaa. En kohdannut ongelmia käyttöönotossa sekä konfiguroinnissa.

WLAN-kontrollerin voi konfiguroida useilla eri tavoilla. Jatkokehitysideana WLAN-kontrollerille voidaan konfiguroida esimerkiksi tukiasemien automaattinen kanavien säätö, muun merkkisten tukiasemien tunnistus sekä tukiasemien lisäasetuksien säätö.

LÄHTEET

Angell, D. 2013. Next-Gen 802.11ac Wi-Fi For Dummies. Viitattu 2.9.2020 https://www.intel.com/content/dam/www/public/us/en/documents/pdf/next-gen-80211ac-wifi-for-dummies.pdf.

Antunes, T. 2019. Wireless LAN Controller Mobility Groups FAQ. Viitattu 15.9.2020 https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.html#anc2.

Bologna, C. 2019 Here's Why It's Called 'Wi-Fi'. Viitattu 22.6.2020 https://www.huffpost.com/entry/why-called-wi-fi_l_5cace3f7e4b01bf960065841.

Cisco 2012. RADIUS Server Authentication of Management Users on Wireless LAN Controller (WLC) Configuration Example. Viitattu 10.9.2020 https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71989-manage-wlc-users-radius.html.

Cisco 2020a. Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet. Viitattu 15.9.2020 https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html?oid=otren016598.

Cisco 2020b. Cisco Wireless LAN Controller Configuration Guide, Release 7.2. Viitattu 15.9.2020 https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html#86268.

Cisco 2020c. Cisco Wireless LAN Controller Configuration Guide, Release 7.4. Viitattu 12.10.2020 https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010110111.html.

Coleman, D. 2020. Wi-Fi 6 For Dummies. Viitattu 21.5.2020 https://www.ait-pg.co.uk/wp-content/uploads/2019/12/Wi-Fi-6-FD_-Extreme-Networks-Special-Edition-_1_.pdf.

Electronics-notes 2020a. IEEE 802.11g Wi-Fi. Viitattu 22.6.2020 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11g.php.

Electronics-notes 2020b. IEEE 802.11b. Viitattu 22.6.2020 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11b.php.

Electronics-notes 2020c. IEEE 802.11a. Viitattu 22.6.2020 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11a.php.

Electronics-notes 2020d. IEEE 802.11n WLAN Standard. Viitattu 24.6.2020 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11n.php.

Electronics-notes 2020e. IEEE 802.11ac Gigabit Wi-Fi. Viitattu 8.7.2020 https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php.

Electronics-notes 2020f. What is OFDM: Orthogonal Frequency Division Multiplexing. Viitattu 10.11.2020 https://www.electronics-notes.com/articles/radio/multicarrier-modulation/ofdm-orthogonal-frequency-division-multiplexing-what-is-tutorial-basics.php.

excITingIP 2010. Why is a Controller required in a wireless network. Viitattu 2.9.2020 http://excitingip.com/673/features-of-todays-centralized-wireless-wi-fi-networks/.

Extreme 2019. Why is OFDMA One of the Most Important Features in 802.11ax? Viitattu 10.11.2020 https://www.extremenetworks.com/extreme-networks-blog/why-is-ofdma-one-of-the-most-important-features-in-802-11ax/.

Fruhlinger, J. 2019. Beamforming explained: How it makes wireless communication faster. Viitattu 8.7.2020 https://www.networkworld.com/article/3445039/beamforming-explained-how-it-makes-wireless-communication-faster.html.

Hintersteiner, J. 2016. How Does MU-MIMO Work? Viitattu 2.9.2020 https://www.networkcomputing.com/wireless-infrastructure/how-does-mu-mimo-work.

Huang, D. 2018. Wi-Fi 6 fundamentals: What is 1024-QAM? Viitattu 10.11.2020 https://www.commscope.com/blog/2018/wi-fi-6-fundamentals-what-is-1024-qam/.

Itewiki 2020. IoT ja Teollinen internet. Viitattu 10.11.2020 https://www.itewiki.fi/opas/iot-ja-teollinen-internet/.

Keith, S. 2018. What is MU-MIMO and why you need it in your wireless routers. Viitattu 2.9.2020 https://www.networkworld.com/article/3250268/what-is-mu-mimo-and-why-you-need-it-in-your-wireless-routers.html.

Mitchell, B. 2020. 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a. Viitattu 16.6.2020 https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

Router Guide 2015. DTIM Interval (Period) Best Setting. Viitattu 4.11.2020 https://routerguide.net/dtim-interval-period-best-setting/.

WiFi Adviser 2020. WiFi Standards Explained. Viitattu 16.6.2020 http://wifiadviser.com/archives/741.