Tommi Salmela

Organisaation langattomien lähiverkkojen toteuttaminen pilvihallittavalla verkkoratkaisulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

4.4.2023

Tiivistelmä

Tekijä:	Tommi Salmela
Otsikko:	Organisaation langattomien lähiverkkojen toteuttaminen pilvihallittavalla verkkoratkaisulla
Sivumäärä:	29 sivua
Aika:	4.4.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Tietoverkot ja tietoliikenne
Ohjaajat:	Yliopettaja Janne Salonen ICT-asiantuntija Henri Ohvo

---

Tässä insinöörityössä selvitettiin Cisco Merakin laitteiden ja verkon hallintaa. Työn tavoitteena oli todistaa ammattikorkeakoululle, että uusilla Merakin laitteilla on mahdollista ja kannattavaa toteuttaa käytössä ollut henkilökunta- sekä opiskelijaverkko olemassa olleilla määrityksillä.

Insinöörityössä perehdyttiin Merakin selaimen kautta käytettävään hallintakäyttöliittymään, Windows Server -ympäristöön, sekä pilvihallittavuuden tuomiin hyötyihin organisaatiolle. Insinöörityön teoriaosuudessa perehdytään myös langattomiin verkkoihin yleisesti ja työssä käytettyihin standardeihin. Tietoa hankittiin organisaatiossa myös haastatteluilla ja tiimikokouksissa.

Pilvihallittavat ratkaisut ovat yleistyneet viimeisten vuosikymmenien aikana globaalisti, ja suuri osa yrityksistä on siirtynyt kokonaan pilvipainotteisiin ympäristöihin. Pilvipalvelut ovat usein saatavilla paikasta ja ajasta riippumatta, mikä helpottaa työntekijöiden jokapäiväistä työntekoa.

Työssä rakennettiin yhdellä ammattikorkeakoulun kampuksella opiskelijoiden ja henkilökunnan käytössä oleva verkko Merakin laitteilla. Lisäksi asennettiin uusi RADIUS-palvelin, jotta laitteet voidaan konfiguroida aikaisemmin käytössä olleen verkon mukaisesti toimimaan Windows-sertifikaattien avulla.

Insinöörityön tuloksena saatiin toteutettua toimiva Cisco Meraki -ympäristö Diakonia-ammattikorkeakoululle. Työn tuloksia ja saatuja kokemuksia voitiin ja voidaan hyödyntää organisaatiossa pilvipohjaisen verkkotoimintaympäristön myöhemmässä laajemmassa käyttöönotossa.

Avainsanat: Cisco, Meraki, pilvihallinta, langaton verkko

Abstract

Author:	Tommi Salmela
Title:	Implementation of an Organization's Wireless Local Area Networks Using Cloud-Managed Cisco Meraki
Number of Pages:	29 pages
Date:	4 April 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	Communication Networks and Applications
Instructors:	Janne Salonen, Principal Lecturer Henri Ohvo, ICT-specialist

---

The purpose of this thesis was to investigate the management of Cisco Meraki and networks. The goal was to prove the Diaconia University of Applied Sciences that it is possible and cost-efficient to implement the existing staff and student networks using the existing configurations.

In the thesis we learn about Merakis browser-based management interface, the Windows Server environment and the benefits of cloud-management for the organization. The theory part of the thesis focuses on wireless networks in general and the standards used in the thesis. Information was also acquired through interviews and team meetings while working at Diaconia University of Applied Sciences.

Cloud-managed solutions have become increasingly more popular during the last decades and a large part of companies have completely moved to cloud-focused environments. Cloud services are often available regardless of time and place which makes it easier for employees to complete their daily work.

In the practical section of the work, a network is built using the Meraki devices on one of the campuses. In addition, a RADIUS-server is configured to use Windows certificates in order to configure the network to operate using the same specifications as the old network.

As a result of the thesis, a functioning environment was implemented for the Diaconia University of Applied Sciences using the Cisco Meraki devices and the cloud-managed Meraki Dashboard. The results of the thesis and the experiences gained could and can be utilized in the organizations subsequent wider implementation of cloud-based services.

Keywords: Cisco, Meraki, Wireless networks, Cloud management

Sisällys

Lyhenteet

MU-MIMO Multiple-user, multiple-input and multiple-output. Tekniikka, joka auttaa jakamaan tietoliikenteen usean laitteen ja käyttäjän välillä. Mahdollistaa neljän samanaikaisen yksikön kanssa kommunikoinnin normaalin MIMO-tekniikan yhden yksikön sijaan.

WLAN Wireless local area network eli langaton lähiverkko.

PoE Power-over-Ethernet, tekniikka, jossa ethernet-kaapelin ja parikaapelin välityksellä kulkee virransyöttö.

SDN Software-defined networking, ohjelmallisesti määritetty verkko. Pilvipalveluita hyödyntäen verkon mallin määrittämisen menetelmä.

SSID Service set identifier, langattoman lähiverkon verkkotunnus.

SD-WAN Software-defined Wide Area Network, verkkoarkkitehtuuri, joka mahdollistaa suojatun yhteyden muodostamisen.

OSI-malli Open Systems Interconnection, seitsemän kerroksinen kuvaus tiedonsiirtoprotokollien yhdistelmästä.

NPS Network Policy Server, Windows Serverin komponentti, joka mahdollistaa autentikoinnin verkkoon halutulla tavalla.

RADIUS Remote Authentication Dial In User Service, protokolla, joka mahdollistaa käyttäjien autentikoinnin verkkoon.

AD Active Directory, Windows-toimialueen käyttäjätietokanta ja hallinnointipalvelu. Palvelu sisältää tietoa muun muassa käyttäjistä ja laitteista.

1 Johdanto

1.1 Tausta ja tavoitteet

Pilvipalvelut ovat tulleet jatkuvasti enemmän yleiseen tietoisuuteen, mutta aiheesta on silti vain vähän aineistoa. Aiheen ajankohtaisuus ja yritysten kasvava tarve pilvipalveluratkaisuille oli yksi pääsyistä insinöörityön aiheen valinnalle. Diakonia-ammattikorkeakoulu halusi monien muiden yritysten tavoin siirtyä pilvipalvelupainotteiseksi ja siirtää oman verkkohallinnan pilven kautta hallittavaksi.

Tässä insinöörityössä selvitetään Cisco Merakin laitteiden ja verkon hallintaa. Työn tarkoituksena on todistaa ammattikorkeakoululle, että uusilla Merakin laitteilla on mahdollista ja kannattavaa luoda ammattikorkeakoulussa tällä hetkellä toiminnassa oleva henkilökunta- sekä opiskelijaverkko laitteiden käytössä olevilla määrityksillä.

Työn tavoitteena on tehdä selvitys Cisco Meraki-laitteiston soveltuvuudesta ammattikorkeakoululle sekä sen pohjalta rakentaa kampuksella opiskelijoiden ja henkilökunnan käytössä oleva pilvipohjaisella hallinnalla toteutettava verkko Merakin laitteilla. Selvityksen lisäksi on tarkoituksena asentaa uusi RADIUS-palvelin, jotta laitteet voidaan konfiguroida aikaisemmin käytössä olleen verkon mukaisesti toimimaan Windows-sertifikaattien avulla.

Insinöörityöraportin alussa perehdytään Merakin selaimen kautta käytettävään hallintakäyttöliittymään, Windows Server -ympäristöön, sekä pilvihallittavuuden tuomiin hyötyihin organisaatiolle. Pilvihallittavat ratkaisut ovat yleistyneet viimeisten vuosikymmenien aikana globaalisti, ja suuri osa yrityksistä on siirtynyt kokonaan pilvipainotteisiin ympäristöihin. Pilvipalvelut ovat usein saatavilla paikasta ja ajasta riippumatta, joka helpottaa työntekijöiden työntekoa. Lisäksi insinöörityön teoriaosuudessa perehdytään langattomiin verkkoihin yleisesti ja työssä käytettyihin standardeihin.

1.2 Menetelmät ja rajaus

Laadullisen tutkimuksen keskeisiä tiedonkeruumenetelmiä ovat mm. havainnointi, haastattelut ja erilaiset dokumentit [1]

Avoimessa haastattelussa olennaista on se, ettei keskustelu ole sidottu tiukkaan formaattiin, vaan edetään keskustelunomaisesti. Teemahaastattelu on keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja. Havainnoinnin avulla saadaan välitöntä ja suoraa informaatiota yksilön, ryhmien ja organisaatioiden toiminnasta. Osallistuvassa havainnoinnissa tutkija vaikuttaa aktiivisesti läsnäolollaan tutkittavaan ilmiöön. Hän voi esimerkiksi olla mukana kehittämistyössä, projektissa tai vastaavassa tilanteessa aktiivisena toimijana. [2]

Tässä insinöörityössä havainnoinnilla ja haastatteluilla hankitaan tietoa Diakin verkon toimintaympäristön lähtötilanteesta sekä asetetuista tavoitteista. Aineistoa kerätään myös käyttäjäkokemuksista ennen pilvihallittavan verkon käyttöönottoa ja sen jälkeen. Tietoa kerätään projektin aikana organisaation ja kumppaneiden asiantuntijoilta, loppukäyttäjiltä sekä osallistumalla tiimikokouksiin ja hyödyntäen kokousmateriaaleja.

Tämä insinöörityö on osa Diakin laajempaa verkon kehittämistyötä. Insinöörityö rajataan koskemaan selvitystä Cisco Meraki-laitteiston soveltuvuudesta ja hyödyistä ammattikorkeakoululle. Tähän insinöörityöhön kuuluva käytännön toteutus rajataan selvitystyön pohjalta tehtyyn testiympäristön rakentamiseen ja pilotointiin Helsingin kampuksella.

2 Cisco Meraki

Cisco Meraki on osa Cisco Systems -yritystä, joka tarjoaa pilvihallittavia laitteita ja verkkoratkaisuja. Meraki valmistaa muun muassa tukiasemia, kytkimiä, palomuureja sekä kameroita, jotka ovat kaikki hallittavissa verkon välityksellä. Cisco

Systems työllisti vuonna 2022 noin 83300 työntekijää, joista Merakin puolella työskenteli 2700 työntekijää. Merakilla on maailmanlaajuisesti yli 737000 asiakasta. [3; 4]

2.1 Merakin historia

Kolme Massachusettsin teknillisen korkeakoulun opiskelijaa, Sanjit Biswas, John Bicket ja Hans Robertson perustivat Merakin osana yliopistonsa RoofNet-projektia Kalifornian Mountain Viewssä vuonna 2006. [5]

Yritys siirtyi San Franciscoon vuonna 2007, jossa Meraki tarjosi ilmaista Internet-yhteyttä verkkotoistimien avulla Lower Haightin kaupunginosassa. Saman vuoden lokakuuhun mennessä verkkoa käytti noin 20000 asukasta, ja verkon läpi oli siirretty 5 Teratavua dataa. [6]

Cisco Systems osti Merakin marraskuussa 2012. Kauppasumman on arvioitu olleen 1.2 miljardia dollaria. Kauppa toi Cisco Systemsille jalansijaa keskisuurten asiakkaiden segmentissä, jota Ciscolla ei vielä aikaisemmin ollut. [7]

2.2 Cisco Meraki verkkoratkaisuna

Merakin laitteet ovat suunniteltu pilvipalveluiden kautta tehtävää hallintaa varten. Pilvipalveluhallinta mahdollistaa verkon nopean ja vaivattoman ylläpidon verkossa olevan Dashboardin kautta.

Cisco Meraki on pilvihallittava verkkoratkaisu, joka mahdollistaa keskisuurien ja suurien verkkojen laitteiden keskitetyn hallinnan verkossa. Selaimen kautta hallittava Dashboard mahdollistaa johdonmukaisen ja yksinkertaisen alustan pienemmistä ympäristöistä jopa erittäin suuriinkin ympäristöihin. Meraki on käytettävissä myös kotiympäristössä, mutta kotikäytössä osa Merakin ominaisuuksista menee hukkaan ja laitteet vaativat lisenssin toimiakseen, jonka vuoksi Merakia ei pidetä kaikista kustannustehokkaimpana ratkaisuna kotikäytössä.

Dashboardille voi rekisteröidä tilin ennen laitteiden saapumista Dashboardin kotisivulla. Laitteiden tilausnumerolla tai laitteen sarjanumerolla voidaan lisätä uudet laitteet Dashboardille tilin luomisen jälkeen, jonka myötä laitteet ovat välittömästi näkyvissä. Jos laitteilla on yhteys ulkoverkkoon, laitteet alkavat välittömästi päivittää itseään. Dashboardille on mahdollista lisätä useampi ylläpitäjä, joilla on täydet oikeudet hallinnoida verkon ja laitteiden asetuksia.

Pilvipohjainen hallinta mahdollistaa kaikkien Merakin laitteiden hallinnan selaimen kautta, eikä laitteita tarvitse konfiguroida yksitellen erikseen.

2.3 Merakin laitteet

Merakin tarjonnasta löytyy kattava määrä erilaisia Dashboardin kautta hallittavia laitteita, jotka voivat olla yrityksille hyödyllisiä yrityksen koosta riippumatta. Katalogista löytyy Merakin MR-sarjaan kuuluvia tukiasemia, MS-sarjaan kuuluvia kytkimiä, MX-sarjaan kuuluvia palomuureja, MV-sarjaan kameroita, MT-sarjaan kuuluvia sensoreita sekä MG-sarjaan kuuluvia pilvihallittavia matkapuhelinmodeemeita. [8]

Merakin MR-sarjan tukiasemat ovat tarkoitettu yrityksille, jotka haluavat keskitetyn pilvihallinnan kautta toimivia tukiasemia verkon langattomaan jakamiseen. Uusimmat MR-sarjan laitteet tukevat MU-MIMO teknologiaa 802.11ax-standardin mukaisesti, tarjoten entistä enemmän tiedonsiirtokapasiteettia. Meraki markkinoi tukiasemiaan zero touch provisioningia (ZTP) käyttävinä laitteita. ZTP tarkoittaa sitä, että tukiasemat ovat tarkoitettu itsestään toimiviksi. Käyttäjän tarvitsee vain yhdistää tukiasema kytkimeen, ja tukiasema lähtee itsekseen toimimaan verkon ylläpitäjän etukäteen määrittelemillä asetuksilla. Verkon ylläpitäjä voi säätää halutut asetukset Dashboardin kautta joko laitekohtaisesti tai tekemällä Dashboardiin mallipohjan (template), jota on mahdollista käyttää laitetta käyttöönottaessa.

Dashboardin kautta on mahdollista saada analytiikkadataa laitteiden toiminnasta esimerkiksi signaalinvahvuuden, käyttäjämäärän, latenssin ja datan käytön muodossa. Analytiikkaa on mahdollista saada sekä käyttäjäkohtaisesti että tukiasemakohtaisesti. [9]

MS-sarjan kytkimet hyödyntävät ZTP:tä ja ovat täysin konfiguroitavissa verkon välityksellä. Dashboardin avulla on mahdollista konfiguroida jopa tuhansia portteja samanaikaisesti. Kytkimiä käyttöönottaessa on mahdollista hyödyntää aikaisemmin määritettyjä mallipohjia. [10]

MV-sarjaan kuuluvat kamerat ovat tarkoitettu niin sisä- kuin ulkokäyttöön. Kamerat käyttävät koneoppimiseen pohjautuvaa analytiikkaa, joka helpottaa tallenneteiden läpikäymistä. Jokaiseen MV-sarjan malliin kuuluu integroitu tallennustila, joka mahdollistaa kameran taustajärjestelmän skaalautumisen jopa kymmenien tuhansien kameroiden samanaikaiseen käyttöön. Kamerat tallentavat jatkuvasti myös lokaalisti, joka mahdollistaa nauhoitetun videon säilymisen mahdollisten yhteysongelmien tapahtuessa.

Kameroiden verkkoyhteydet toimivat täysin langattomasti ja käyttävät hyvin vähän kaistaa, joten vaikutus verkkoon on minimoitu valtaosan ajasta. Ainoastaan kamerasyötettä tarkastellessa reaaliaikaisesti kamerat vaativat enemmän kaistaa. Kameroiden sisäiseen tallennustilaan tallennettu materiaali on oletuksena salattu, eikä kameran salauksia saa otettua pois päältä asetuksista.

Kamerat tallentavat aina viimeisimmät 72 tuntia, ja tästä ylittyvä materiaali tallentuu perustuen kamerakuvassa tapahtuvaan liikehdintään ylläpitäjien määrittelemien asetusten mukaan. Täysin liikkumaton kamerakuva trimmataan materiaalista pois, ja jäljelle jätetään ainoastaan ne osat videosta, johon sisältyy liikehdintää. Kameran livekuva sekä kaikki tallennetut videot ovat katsottavissa Dashboardista mobiililaitteilla ja tietokoneella. Tallenteiden tai livekuvan katsominen ei vaadi ylimääräisten sovellusten asentamista, vaan toimii selaimen kautta. Käyttäjä voi halutessaan asentaa tietokoneelleen PWA:n (Progressive

Web App), jonka kautta kameroiden hallintasivulle pääseminen helpottuu. [10; 11]

MT-sarjan sensorit ovat tarkoitettu käytettäväksi muiden Merakin laitteiden kanssa havaitsemaan esimerkiksi kosteutta tai lämpötilan muutoksia. Pilvihallittavat sensorit ovat yhteydessä Dashboardiin käyttäen BLE:tä (Bluetooth Low Energy) jo olemassa oleviin Merakin tukiasemiin tai kameroihin, jotka ovat verkon kautta yhteydessä Dashboardiin. Sensorit on mahdollista konfiguroida ilmoittamaan hälytyksistä tekstiviestitse, sähköpostitse, push-ilmoituksilla tai webhookeilla. [12]

Kaikki Merakin laitteet ovat hallittavissa pilven kautta. Tässä insinöörityössä organisaation tarpeisiin riittivät tukiasemien ja kytkinten tutkiminen keskikokoisessa ympäristössä. Diakonia-ammattikorkeakoulun Kalasataman kampuksella on normaaliolosuhteissa satoja kävijöitä päivittäin, ja tukiasemien tulee tukea tarvittaessa kymmeniä ihmisiä kerrallaan.

3 Pilvipalvelut

Pilvipalveluilla tarkoitetaan verkon yli saatavia resursseja, joista laskutetaan usein käytön perusteella. Tarjottu palvelu voi olla esimerkiksi tallennustilaa tai tietokoneohjelmisto. Palvelut ja resurssit ovat täten saatavilla mistä tahansa verkon välityksellä, eikä ohjelmiston tai palvelimen tarvitse täten sijaita fyysisesti lähettyvillä tai sisäverkossa.

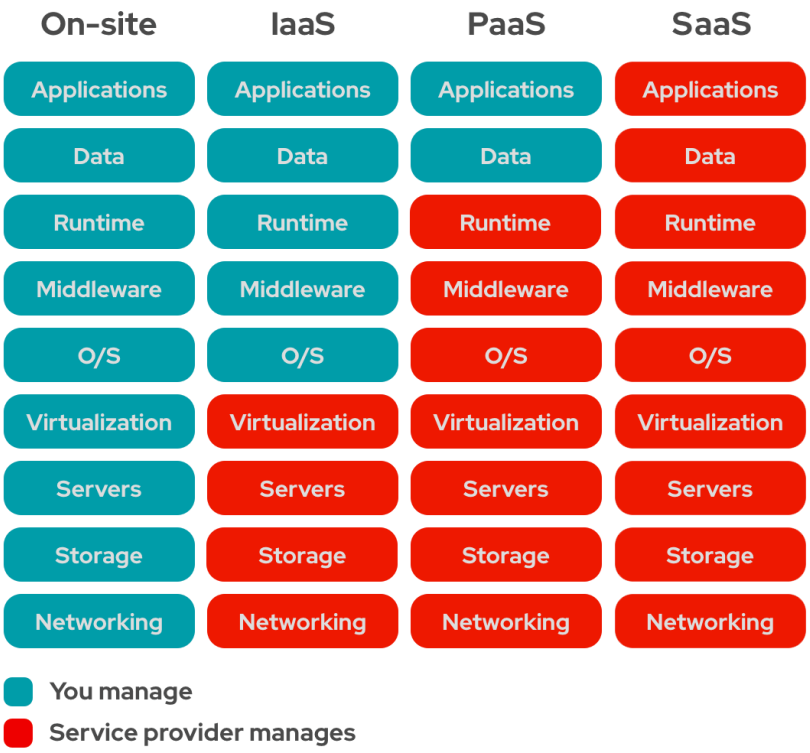
Pilvipalveluiden käyttö eliminoi yrityksiltä hankintakustannuksia, jotka aiheutuvat ohjelmistojen ja fyysisten laitteiden ostokustannuksista sekä paikan päällä olevien palvelinsalien perustamisesta, käyttämisestä ja käyttökustannuksista, kuten sähköstä. Pilvipalveluiden avulla datan varmuuskopiointi helpottuu ja on täysin palveluntarjoajan vastuulla, joka varmuuskopioi datan useammalle palvelimelle sen sijaan, että data olisi tallennettuna vain yhteen sijaintiin. [13]

Pilvipalveluiden skaalautuvuus ja joustavuus mahdollistaa sen, että hallinnoijan ei tarvitse tehdä uusia hankintoja tarpeiden muuttuessa. Nopeat muutokset datamäärissä tai prosessointitehossa saattaisivat vaatia perinteisin menetelmin nopeita laitehankintoja ja asennuksia, jotka eivät aina ole nopealla aikataululla mahdollisia. Tietojen tallennuskapasiteettia, prosessointitehoa ja verkkoa voidaan skaalata asiakkaan tarpeiden mukaan olemassa olevan pilvi-infrastruktuurin avulla. Skaalaus voidaan tehdä nopeasti ja helposti ilman, että käyttäjät huomaavat häiriöitä palvelussa. Tämä mahdollistaa uusien toimintamallien toteuttamisen niin yksityiselle henkilölle kuin yrityksille.

Maailmanlaajuisesti pilvipalveluiden markkina-arvo saavutti 312 miljardia dollaria vuonna 2020, ja nousun uskotaan jatkuvan entistä nopeampaan tahtiin. Vuoden 2021 ensimmäisessä puoliskossa nousu oli entistäkin suurempaa, ja markkinajohtajat Amazon Web Services (AWS) ja Microsoft Azure hallitsivat yli puolta markkinaosuudesta. Vuonna 2022 pilvipalveluiden markkina-arvo oli yltänyt jo yli 480 miljardiin dollariin. [14; 15]

3.1 Palvelumallit

NIST (National Institute of Standards and Technology) kategorisoi pilvipalvelumallit kolmeen eri osa-alueeseen: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service).



Kuva 1. NISTin määritelmän mukaiset pilvipalvelumallit [15]

Infrastructure as a Service -palvelussa asiakkaalle tarjotaan infrastruktuuria palveluna. Infrastruktuuripalvelut voivat pitää sisällään esimerkiksi palvelimia ja tietokoneita. Kokonaisuuteen sisältyvät kuitenkin myös tallennustila, verkkoyhteys, sekä fyysisen laitteiston ylläpito. Palvelussa tarjotaan asiakkaalle perusta, jonka päälle asiakas pystyy rakentamaan halutessaan mitä tahansa. Pilvipalvelutarjoajat kuten Amazon Web Services ja Microsoft Azure ovat esimerkkejä IaaS-palvelusta.

Platform as a Service -mallissa asiakkaalle tarjotaan infrastruktuurin lisäksi myös työskentelyalusta käyttöjärjestelmän sekä työkalujen ja viitekehysten (framework) muodossa palveluiden kehittämistä varten. PaaS tarjoaa organisaatioille esimerkiksi työkaluja organisaatioiden datan analysointiin sekä liiketoiminnalle oleellisia työkaluja ja palveluita BI:lle (Business Intelligence).

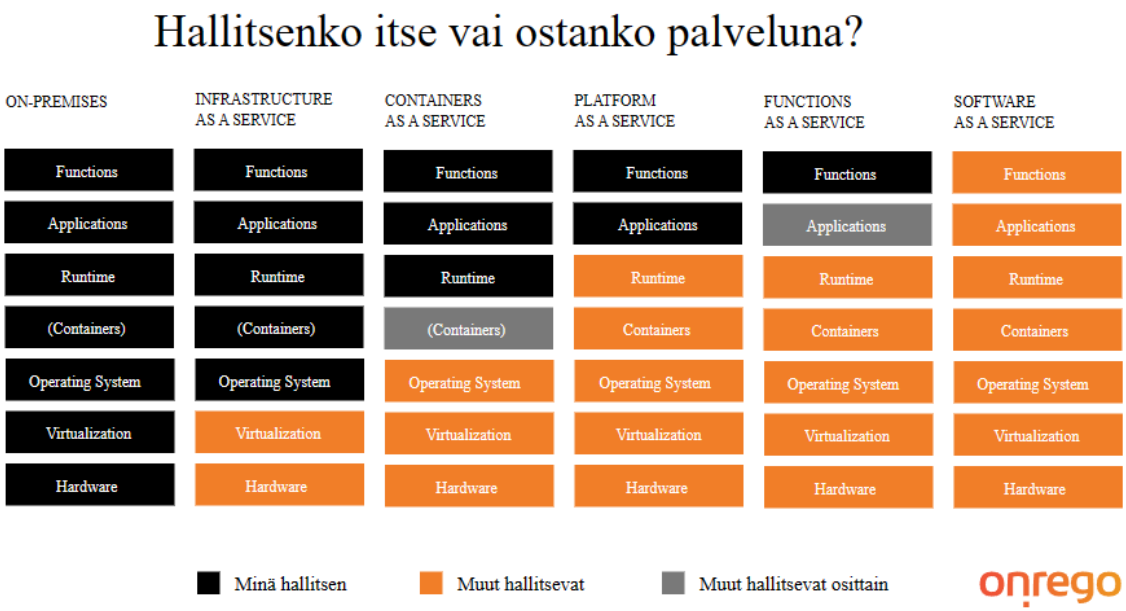
Software as a Service -palvelumallissa asiakkaille tarjotaan infrastruktuurin ja alustan lisäksi myös sovellus. Sovellus tarjotaan usein kuukausittaisella hinnoit-

telulla, josta maksetaan joko käytön mukaan tai kiinteän kuukausihinnan mukaan. Software as a Service -mallia hyödyntävät sovellukset ovat useilla ihmisillä päivittäisessä käytössä, sillä esimerkiksi Dropbox, Office365-sovellukset ja sähköpostisovellukset ovat nimenomaan SaaS-palveluita. [16; 17]

Arkikielessä käytetään kuitenkin muitakin ”aaS”-päätteisiä lyhennelmiä eri pilvipalveluiden tarjoamista ratkaisuista. FaaS (Functions-as-a-Service) ja CaaS (Containers-as-a-Service) ovat esimerkkejä, joita ei voi luokitella täysin IaaS, SaaS tai PaaS-palvelumalleihin sopiviksi, jonka vuoksi kyseisille palveluille on laadittu uusi sopivampi nimi.

CaaS-palvelumallissa asiakkaalle tarjotaan kontteja (container). Kontit mahdollistavat asiakkaalle ohjelmiston pakkaamisen siten, ettei ohjelmistoa tarvitse muokata sen siirtyessä alustalta toiselle. Virtuaalipalvelimien avulla ohjelmistoille on mahdollista tarjota tarvitsemansa ympäristö samalla tavalla kuin konteillakin, mutta virtuaalipalvelimet sisältävät myös kaiken mitä tarvitaan palvelimen ajamiseksi. Konttitiedostot ovat huomattavasti pienempiä kuin virtuaalipalvelintiedostot, ja ovat parhaimmissa tapauksissa vain sadasosan virtuaalipalvelintiedostojen koosta. [18]

FaaS-mallissa käyttäjille tarjotaan alusta, jonka päällä voi ajaa funktioita. FaaS on synonyymi serverless-arkkitehtuurille, joka tarkoittaa, että pilvipalveluntarjoaja vastaa ainoastaan resurssien allokoinnista. Vaikka serverless-ratkaisut olisi mahdollista toteuttaa kaikilla NIST-instituutin määritelmän PaaS-, IaaS- tai SaaS-palvelumalleilla, on tämä palvelumalli optimaalinen kustannusmalli, jos koodia ei tarvitse jatkuvasti ajaa. Useat pilvipalvelutarjoajat veloittavat ainoastaan koodin ajamisajasta.



Kuva 2 Erilaisia pilvipalvelumalleja.

Kaikille pilvipalveluiden palvelumalleille yhteistä on se, että käyttäjät eivät joudu itse huolehtimaan laitteiston, verkon tai tallennustilan hallinnasta. Kaikki nämä palvelut ovat ulkoistettu pilvipalvelun tarjoajalle. Suurimpia pilvipalveluiden tarjoajia ovat esimerkiksi Amazon (Amazon Web Services), Microsoft (Azure), IBM Cloud, Google Cloud ja Alibaba Cloud. [19]

3.2 Pilvityypit

Pilvipalveluiden käyttämä verkko voi olla julkinen, yksityinen tai hybridiverkko. Pilven tyyppi määräytyy sen mukaan, kuinka ja kuka pilvipalvelua pääsee käyttämään.

Julkisella pilvellä (Public Cloud) tarkoitetaan virtuaalisesti toteutettua palvelinympäristöä, jonka palveluntarjoaja on tuottanut tavoitettavaksi julkisen Internet-yhteyden kautta. Julkiset pilvet ovat aina jaettu alusta, joka tarkoittaa, että useat yritykset käyttävät samoja laitteita yhtäaikaisesti. Palvelinkapasiteetti on jaettu pieniin osiin virtuaalipalvelimiksi.

Yksityinen pilvi (Private Cloud) on yrityskohtainen pilvipalveluratkaisu, johon ei tyypillisesti ole pääsyä julkisesta verkosta. Pilven hallinnointi tapahtuu joko suoraan yrityksen sisäverkosta tai suojatun etäyhteyden avulla. Yksityisen pilven voi rakentaa joko yrityksen omilla palvelimilla omia konesaleja hyödyntäen tai ulkoistettuna ulkoisen palveluntarjoajan palvelinsaleja ja laitteita käyttäen. Yksityisen pilven etuna on turvallisuus hallinnan tapahtuessa sisäverkon tai suojattujen yhteyksien kautta.

Hybridipilvi (Hybrid Cloud) käyttää sekä julkista pilveä että yksityistä pilveä. Hybridipilvessä voidaan yhdistää yksityisen ja julkisen pilven parhaat puolet, ja pilvi on käytettävissä maailmanlaajuisesti julkista pilveä hyödyntäen. Tietoturvallisuuden kannalta olennaiset korkean tietoturvatason yksityiset tiedot, kuten henkilötiedot, voidaan säilyttää yksityisessä pilvessä, vaikka julkiseen osaan hybridipilveä pääsy on samanaikaisesti mahdollista mistä puolelta maapalloa tahansa. [20; 21]

4 Langattomat lähiverkot

Langaton lähiverkko on paikallinen tietoliikenneverkko, jossa kaksi tai useampi laite keskustelevat keskenään langattomasti esimerkiksi kampuksella, kotona tai ravintolassa. Tämä antaa käyttäjille mahdollisuuden liikkua langattoman verkon alueella vapaasti, ilman että yhteys verkkoon katkeaa. Yhdyskäytävää (engl. gateway) hyödyntämällä langaton lähiverkko on mahdollista yhdistää myös Internetiin tai toiseen verkkoon.

Hawaijin yliopiston professori Norman Abramson aloitti yhdessä työryhmänsä kanssa maailman ensimmäisen langattoman lähiverkon kehittämisen Hawaijin yliopistolla vuonna 1968. ALOHAnet-projektin tarkoituksena oli yhdistää muilla Hawaijin saarilla olevia tietokoneita Oahun kampuksen keskustietokoneeseen ilman puhelinverkkoja. Verkkoon kuului seitsemän tietokonetta, jotka sijaitsivat neljällä eri saarella Hawaijin lähistöllä. Tietokoneet ottivat yhteyden Oahun pää-

kampuksella sijaitsevaan keskustietokoneeseen ensimmäisen kerran kesäkuussa 1971. [22]

Langattomia lähiverkkoja käyttävien laitteiden kustannukset olivat aluksi todella suuret, joten langatonta teknologiaa käytettiin ainoastaan silloin, jos johtojen käyttäminen oli erittäin vaikeaa tai mahdotonta. Vuonna 1999 802.11b standardin myötä langattomat verkot yleistyivät uusien, halvempien laitemallien ja korkeampien verkkonopeuksien myötä. [23]

4.1 IEEE 802.11ax

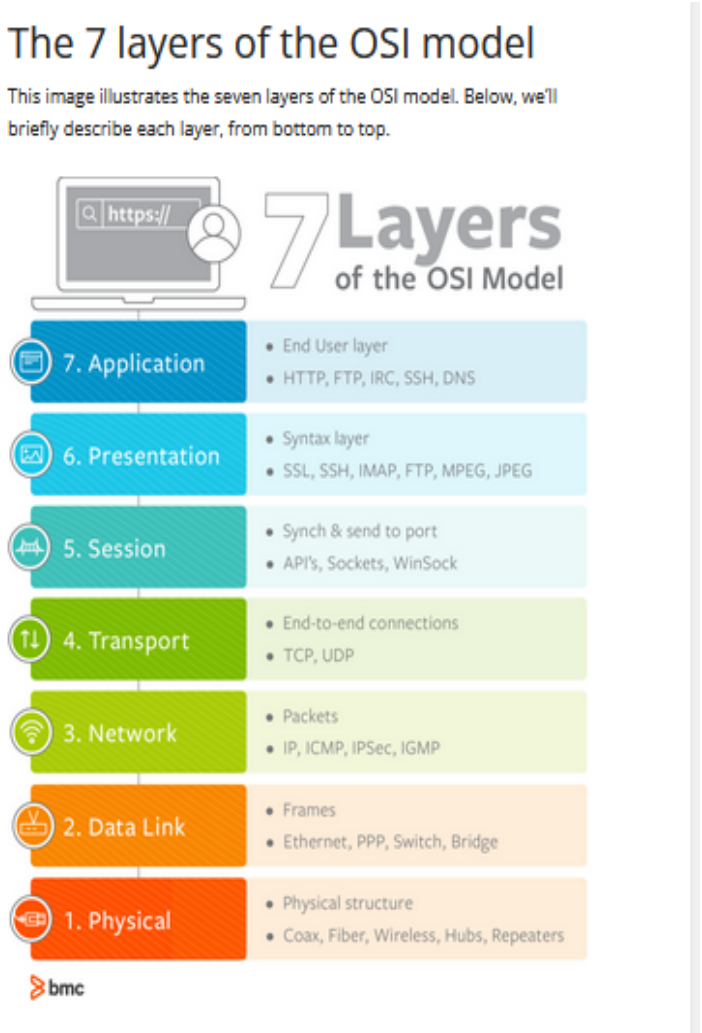
802.11ax -standardi on langattomien verkkojen kuudennen sukupolven standardi, joka tuo parannuksia ja lisäyksiä aikaisempaan Wi-Fi 5 -tekniikkaan. Standardin kehitys aloitettiin vuonna 2014. Vuonna 2018 Wi-Fi allianssi ilmoitti standardista käytettävän myös nimitystä Wi-Fi 6. 802.11ax pohjautuu 802.11ac (tunnetaan myös nimellä Wi-Fi 5) -tekniikan vahvuuksiin lisäten skaalautuvuutta, tehokkuutta ja joustavuutta, joka mahdollistaa nykyisten ja tulossa olevien verkkojen nopeuksien kasvun. 802.11ax -standardi pyrkii ratkaisemaan muun muassa julkisilla paikoilla kohdatun ongelman, jossa aikaisemman standardin 802.11ac tarjoama tiedonsiirtokapasiteetti ruuhkautuu johtaen loppukäyttäjille tarjottuun verkon laskeneeseen suorituskykyyn.

OFDMA-tekniikan (Orthogonal Frequency-Division Multiple Access) ja 1024-QAM-modulaation (Quadrature Amplitude Modulation) johdosta standardi tarjoaa lähes 25 prosenttia nopeamman suorituskyvyn verrattuna aikaisempaan 802.11ac-tekniikkaan. Uuden standardin myötä laitteet voivat lähettää enemmän tietoja yhdessä lähetystiedossa, johtaen jopa 20 % parempaan nopeuteen. Yhdessä nämä kaksi uutta ominaisuutta voivat parantaa lähetysnopeutta jopa 40 %. 802.11ax standardin myötä jokaiseen lähetettävään pakettiin voidaan sisällyttää aiempaa suurempi määrä dataa. Uusi standardi tukee edeltäjänsä tavoin 5 GHz taajuusaluetta, mutta parantaa samalla matalamman 2,4 GHz:n taajuusaluetta. 802.11ax tukee 8x8 MU-MIMO:a aiemman 802.11ac:n mahdol-

listaman 4x4 MU-MIMO:n sijaan, eli kahdeksaa samanaikaista lähetystä aikaisemman neljän lähetyksen sijaan. [24]

4.2 OSI-malli

OSI-malli on seitsemän kerroksinen (Kuva2) datansiirtoarkkitehtuuri, jonka jokaisella kerroksella on oma tehtävänsä. Dataa siirrettäessä jokainen kerros osallistuu datansiirrossa päätelaitteiden välillä niin lähettäessä kuin vastaanottaessa.



Kuva 2. OSI-malli [25]

Sovelluskerros (Application layer) on OSI-mallin ylin kerros. Sovelluskerros vastaanottaa dataa käyttäjältä ja esittää datan käyttäjälle. Selaimet, TelNet-yhteysprotokolla, SMTP (Simple Mail Transfer Protocol) ja FTP (File Transfer Protocol) käyttävät OSI-mallin seitsemättä kerrosta. [26]

Esitystapakerroksessa (Presentation Layer) sovelluskerrokselta saatu data pakataan ja salataan lähetystä varten. Datan pakkaus ja osa salausmetodeista kuten SSL-salaus sekä kyseisten salausten poisto tapahtuvat tässä kerroksessa. [27]

Istuntokerroksessa (Session Layer) varmistetaan kahden laitteen välisen yhteyden muodostaminen, autentikointi ja session ylläpito. Esimerkki istuntokerroksen toiminnasta on OSI-protokollapaketin istuntokerroksen protokolla, joka tunnetaan myös nimeltä X.225. Yhteyden katketessa tai jos yhteys on pitkään käyttämättä, protokolla voi yrittää katkaista tai palauttaa yhteyden. [28]

Kuljetuskerros (Transport Layer) varmistaa, että data siirtyy lähettäjältä vastaanottajalle virheettömänä. Paketit segmentoidaan pienempiin osiin ennen kuljetusta, ja vastaanoton yhteydessä paketit kootaan takaisin kokoon. Kerroksen tehtäviin kuuluu myös tietovirran ruuhkautumisen hallinta. [29]

Verkkokerros (Network Layer) on vastuussa datan reitittämisestä muihin verkkoihin parasta reittiä käyttäen. Lähettäjän ja vastaanottajan välillä ei aina ole suoraa yhteyttä, jolloin paketit on välitettävä eteenpäin matkalla olevien verkkosolmujen kautta. Kerroksen toteuttamiseen käytetään verkkolaitteita, kuten reitittimiä. Verkkokerroksen protokollia ovat esimerkiksi IPv4 (Internet Protocol version 4) ja IPv6 (Internet Protocol version 6). [30]

Siirtoyhteyskerros tai siirtokerros (Data Link Layer) on vastuussa paketin eteenpäin lähettämisessä verkossa. Verkkokortti on toisella kerroksella eli siirtokerroksella toimiva laite. Siirtokerros on jaettu kahteen alikerrokseen, LLC (Logical Link Control) ja MAC (Media Access Control). LLC-alikerros vastaa pakettien eheydestä ja siirrosta verkkolaitteiden välillä. MAC-alikerros on vastuussa pa-

kettien kehysten tarkastamisesta. Alikerros lähettää verkossa olevien laitteiden IP-osoitteisiin ARP-kyselyn saadakseen selville laitteen MAC-osoitteen, johon laite vastaa kertoen MAC-osoitteensa. [31]

Fyysinen kerros (Physical Layer) on OSI-mallin ensimmäinen ja alin kerros, joka kuvaa aina kahden laitteen välistä yhteyttä. Data siirtyy tällä välillä bittimuodossa, kunnes ne pääsevät laitteilla siirtokerrokseen, jossa data kootaan yhteen kehykseksi. Ensimmäisen kerroksen laitteita ovat esimerkiksi toistimet, modeemit ja kaapelit. [31]

4.3 MIMO

MIMO-tekniikalla (multiple input, multiple output) tarkoitetaan tietoliikennetekniikkaa, jossa sekä datan lähettämiseen että datan vastaanottamiseen käytetään useampaa antennia. Useampaa antennia hyödyntämällä lähettäessä ja vastaanottaessa on mahdollista saavuttaa huomattavasti suurempi tiedonsiirtokapasiteetti. MIMO-tekniikkaa hyödyntämällä voidaan kasvattaa datan tiedonsiirtonopeutta ja parantaa tiedonsiirron luotettavuutta.

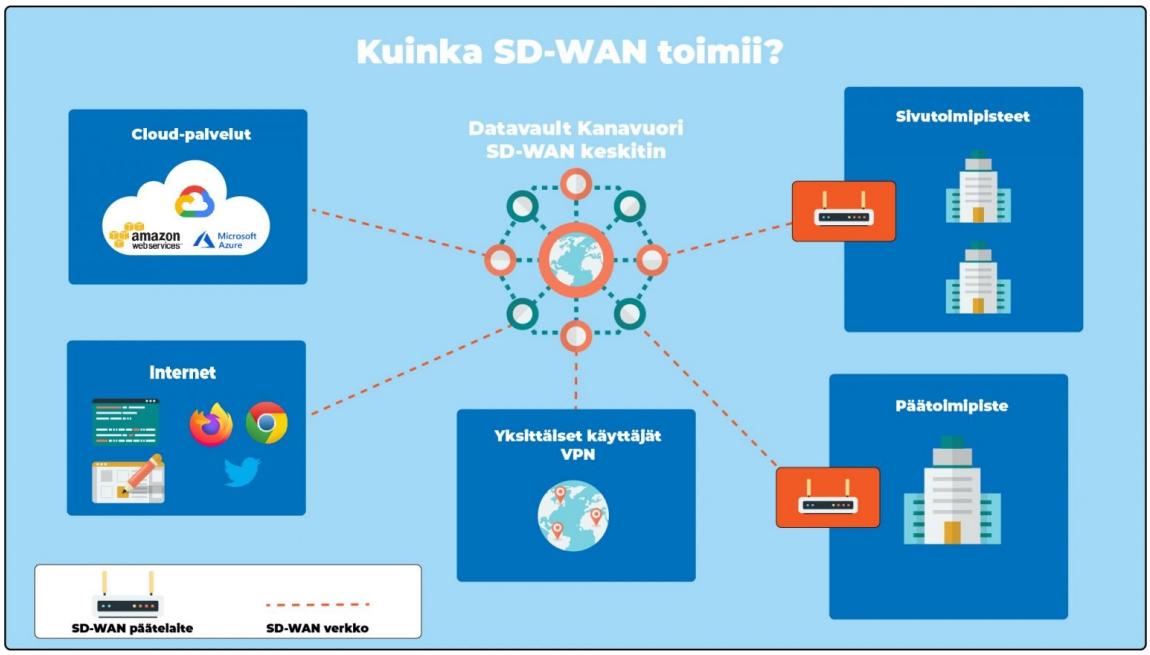
MU-MIMO (multiple user, multiple input, multiple output) on tekniikka, joka mahdollistaa reitittimen kommunikoinnin useamman laitteen kanssa samanaikaisesti. SU-MIMO:a (single user, multiple input, multiple output, joka tunnetaan myös pelkkänä MIMO:na) käyttävät reitittimet, jotka ovat vielä tällä hetkellä yleisempiä markkinoilla, pystyvät keskustelemaan vain yhden laitteen kanssa kerrallaan ja reititin katkaisee yhteyden laitteeseen (tosin vain hyvin lyhyeksi aikaa). MU-MIMO mahdollistaa jopa kahdeksan laitteen samanaikaisen yhdistämisen reitittimeen ilman katkoja. [32]

4.4 SD-WAN

Pilvipalveluiden yleistyessä käyttäjien on päästävä pilvipalveluihin käsiksi sijainnista ja kellonajasta riippumatta. Ohjelmistopohjaisessa suuralueverkkopalve-

lussa (SD-WAN-palvelu) yritysverkot eivät ole sidottu mihinkään tiettyyn verkkoyhteyteen, palveluntarjoajaan tai fyysiseen sijaintiin. Yritysverkkoon on mahdollista päästä minkä tahansa verkkoyhteyden avulla sijainnista riippumatta. [33]

SD-WAN on verkkoratkaisu, jolla voidaan yhdistää työntekijöiden toimipisteitä ja hallita niitä keskitetysti (Kuva 3). Julkisen verkon päälle rakennettu virtuaalinen ja ohjelmoitava verkkoratkaisu mahdollistaa entistä paremman näkyvyyden verkon toimintaan. [34]



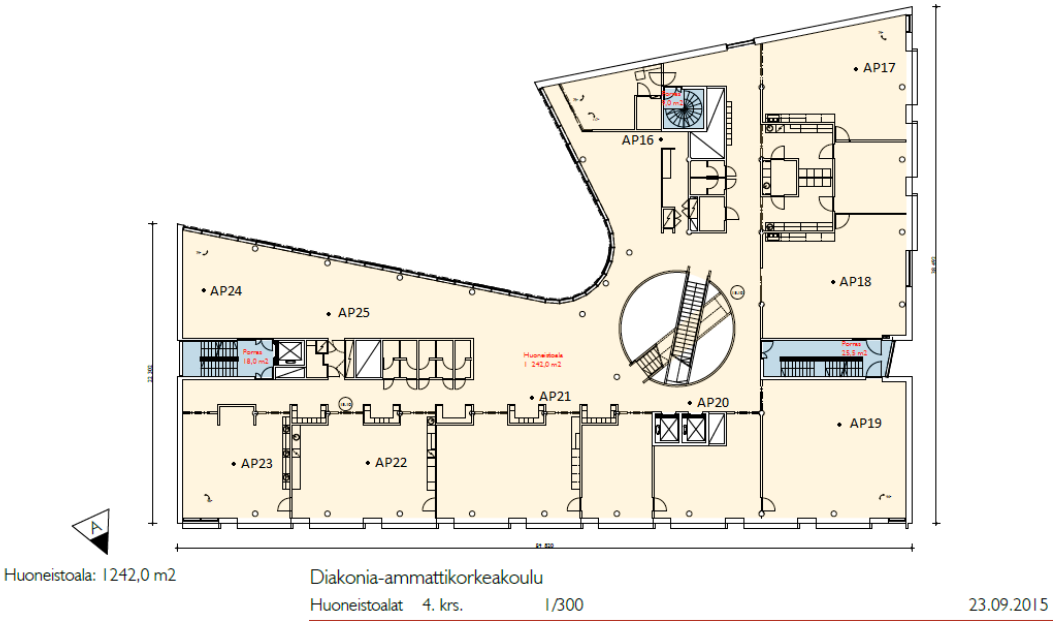
Kuva 3. Kuinka SD-WAN toimii? [35]

5 Käyttöönotto

5.1 Lähtötilanne

Diakonia-ammattikorkeakoulun Kalasataman kampuksella on 56 kappaletta Extremum WS-AP3825i laitteita sijoitettuna ympäri kampusta. Keskitetyn hallinnan puutteen vuoksi laitteiden hallinta on ollut hankalaa, ja ammattikorkeakoulu harkitsi tästä syystä Merakin laitteistoon siirtymistä.

Insinöörityöprosessiin kuului tukiasemien sijainnin kartoitus, jossa paikallistettiin kaikki käytössä olevat tukiasemat. Sijainnit merkittiin kerrosten pohjapiirroksiin ja kampuksella tehtiin testejä verkon kuuluvuuden varmistamiseksi jokaisessa kerroksessa.



Kuva 4. Diakonia-ammattikorkeakoulun neljännen kerroksen tukiasemien sijainnit.

Tukiasemat on sijoiteltu kampuksella kuuteen eri kerrokseen kattolevyjen päälle. Tukiasemien kartoituksen yhteydessä huomattiin, että yhdessä neljännen kerroksen (Kuva4) luokkahuoneessa langattoman verkon heikko kuuluvuus on johtunut tukiaseman puuttumisesta luokkatilassa. Sen sijaan, että tukiasema

olisi luokkahuoneen rakenteissa, tukiasema AP20 on sijainnut luokan edustalla olevien hissien takana, eikä kuuluvuus riittänyt luokkatilaan.

Ammattikorkeakoulun ensimmäisen kerroksen tukiasemien paikantaminen tuotti ongelmia suuren huonekorkeuden vuoksi. Alimman kerroksen kattolaattoihin kiipeäminen oli mahdotonta ilman nosturia, jota ei kustannus- ja logistisista syistä voitu kampukselle tilata. Ulkoiselta toimijalta pyydettiin pääsykokeiden verkkojen varmistamisen yhteydessä verkkojen mittaus, jonka avulla saatiin suurpiirteinen kuva tukiasemien tarkasta sijainnista.

Diakonia-ammattikorkeakoulun kaikilla kampuksilla on käytössä diak_private-henkilökuntaverkko, eduroam-verkko opiskelijoita varten sekä diak_guest-verkko vierailijoita varten. Insinöörityön päätavoitteena oli saada uudet Merakin päälle rakennetut verkot toimimaan samalla tavalla, kuten verkot olivat aikaisemmin vanhoilla laitteilla toimineet.

Eduroam-verkko oli rakennettu käyttämällä Windows Network Policy Serveriä (NPS) RADIUS-palvelimena, joka lähetti autentikointipyynnöt eteenpäin Diakin ise-palvelimelle, joka lähetti pyynnöt eteenpäin eduroamin omille RADIUS-palvelimille. Verkon toiminnan dokumentaatio oli puutteellista ja ylimääräinen kierto ise-palvelimen tarpeellisuus herätti kysymyksiä verkon ylläpitäjissä, joten Diakonia-ammattikorkeakoulun tietohallinto halusi, että eduroam-verkko rakennetaan kokonaisuudessaan uudelleen.

Insinöörityöprosessin aikana tarve eduroam-verkolle muuttui ja DIAK päätti osallistua geteduroam-pilottiin, joka yksinkertaisti verkkostruktuuria. Tekemällä yhteistyötä CSC:n kanssa, tukiasemat konfiguroitiin lähettämään autentikointipyynnöt eduroam-SSID:stä suoraan eduroamin RADIUS-palvelimille, eikä autentikointipyyntöjä tarvitsisi enää jatkossa lähettää oman RADIUS-palvelimen kautta eduroamin omille RADIUS-palvelimille. Tätä varten ammattikorkeakoulun palomuurista jouduttiin avaamaan reitti WLAN-kontrollerin ja eduroamin RADIUS-palvelimen välille molempiin suuntiin käyttäen UDP-portteja 1812 ja 1813.

Ulkopuolisille käyttäjille diak_guest SSID:llä pyörivää verkkoa päätettiin myös muuttaa. Aikaisemmin diak_guest-verkkoon kirjauduttiin guest-tunnuksilla, jotka saatiin tarvittaessa ammattikorkeakoulun aulapalveluista heti kampukselle saavuttaessa. Guest-tunnuksia oli yhteensä 10 kappaletta, ja käyttäjätunnusten salasana vaihdettiin aina kolmen kuukauden välein. Yhdistäessään guest-verkkoon selain uudelleenohjasi käyttäjän kirjautumissivulle, johon käyttäjän täytyi syöttää aulapalveluista saadut tunnukset, jotta käyttäjä pääsi kirjautumaan verkkoon.

Merakia käyttöönotettaessa guest-verkon toimintaa päätettiin muuttaa siten, että jatkossa guest-verkko konfiguroitaisiin toimimaan samalla tavalla, kuin miten tässä insinöörityössä DiakMeraki-verkko rakennettiin.
DiakMeraki-verkkoon kirjautuminen onnistui käyttämällä esimääritettyä salasanaa (Pre-shared Key), eli toisin sanoen samalla tavalla, kuin valtaosaan verkoista kirjaudutaan. Guest-tunnusten tavoin verkon salasanaa vaihdetaan tietyn aikavälin välein, mutta verkkoon kirjautuessa käyttäjän ei tarvitse enää syöttää aulapalveluista saatuja erillisiä guest-tunnuksia selaimen kirjautumisruutuun.

5.2 Käytettävät laitteet

Insinöörityön selvitystyötä varten tilattiin Diakonia-ammattikorkeakoulun Kalasataman kampukselle kolme eri laitetta. Yksi laitteista oli 24-porttinen MS120-kytkin (Kuva 5), johon liitettiin työn aikana kaksi kappaletta MR44-tukiasemia (Kuva 6). MR44-tukiasemat konfiguroitiin Meraki Dashboardin kautta jakamaan langatonta verkkoa kampuksen IT-tiloissa kokeilumielessä.

MS120-24P-malli sisältää 24 kappaletta 10/100/1000BASE-T Ethernet (RJ45) porttia ja neljä SFP-porttia (small form-factor pluggable) uplinkiä varten. Kytkimen älykäs virranjako mahdollistaa virranjaon jokaisen portin päätelaitteille samanaikaisesti. PoE:n kokonaisulosanti maksimissaan 370W tai 30W porttia kohden. [36; 37]

Kuva 5. MS120-24P-kytkin, joka otettiin käyttöön kampuksella. [36]

MS120-kytkimen lisäksi kampukselle tilattiin kaksi kappaletta MR44-tukiasemia. Tukiasemat ovat IEEE 802.11ax standardin mukaisia, joten ne tukevat sekä 2.4 GHz että 5 GHz taajuuksia. Laitteet saavat virran kytkimeltä hyödyntäen PoE-tekniikkaa. ja laitteet hyödyntävät MU-MIMO-verkkotekniikkaa, joka mahdollistaa huomattavasti suuremman tiedonsiirtokapasiteetin laitteilla. Laitteen MU-MIMO-tekniikka hyödyntää 5 GHz:n taajuusalueella 4x4:4 MU-MIMO:a ja 2.4 GHz:n taajuusalueella 2x2:2 MU-MIMO:a. [37]

Kuva 6. MR44-kytkin, joita tilattiin kaksi kappaletta kampukselle. [37]

Kytkin ja tukiasemat ovat täysin hallittavissa ja konfiguroitavissa Meraki Dashboardin kautta mistä päin maailmaa tahansa, kunhan verkkoyhteys on saatavilla.

5.3 Laitteiden käyttöönotto

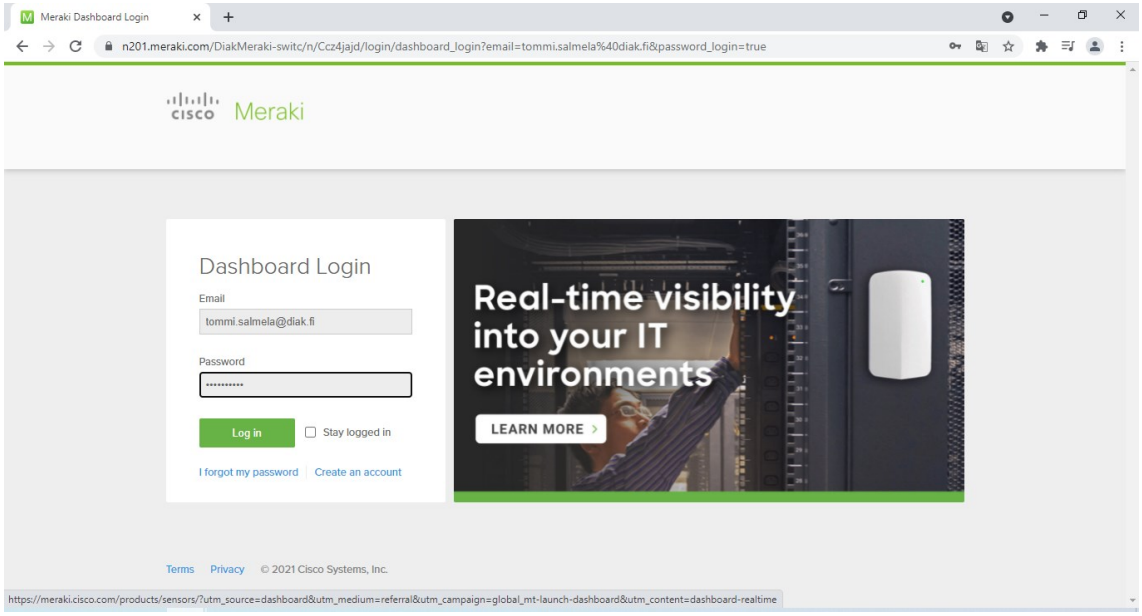
Cisco lähetti kampukselle testilaitteina yhden MS120-kytkimen ja kaksi kappaletta MR44-tukiasemia. Laitteet tulivat erillisinä pakkauksina, ja mukana tuli tilausvahvistus, jonka yhteydessä oli myös tilausnumero, jota voi hyödyntää laitteita lisätessä hallintapaneeliin. Laitteet otettiin ulos pakkauksista, ja kytkin asennettiin kampuksen toisessa kerroksessa sijaitsevaan IT-tukeen. Kytkimen käyttöönotto tapahtui rekisteröimällä kytkimen sarjanumero Dashboardille, jolloin laite ilmestyi välittömästi näkyviin Dashboardin laitteisiin. Kytkin latasi omatoimisesti laitteiston päivitykset, ja noin 15 minuutin jälkeen laite oli toiminnassa.

Kytkimestä varattiin neljä porttia Merakia varten (portit 1.10–1.13), ja tukiasemat liitettiin portteihin 1.10 ja 1.11. Merakin tukiasemat päivittävät itsensä automaattisesti, jos niillä on pääsy ulkoverkkoon, joka kesti noin 20 minuuttia. Päivitysten jälkeen tukiasemat ilmestyivät hallintapaneeliin (Dashboard).

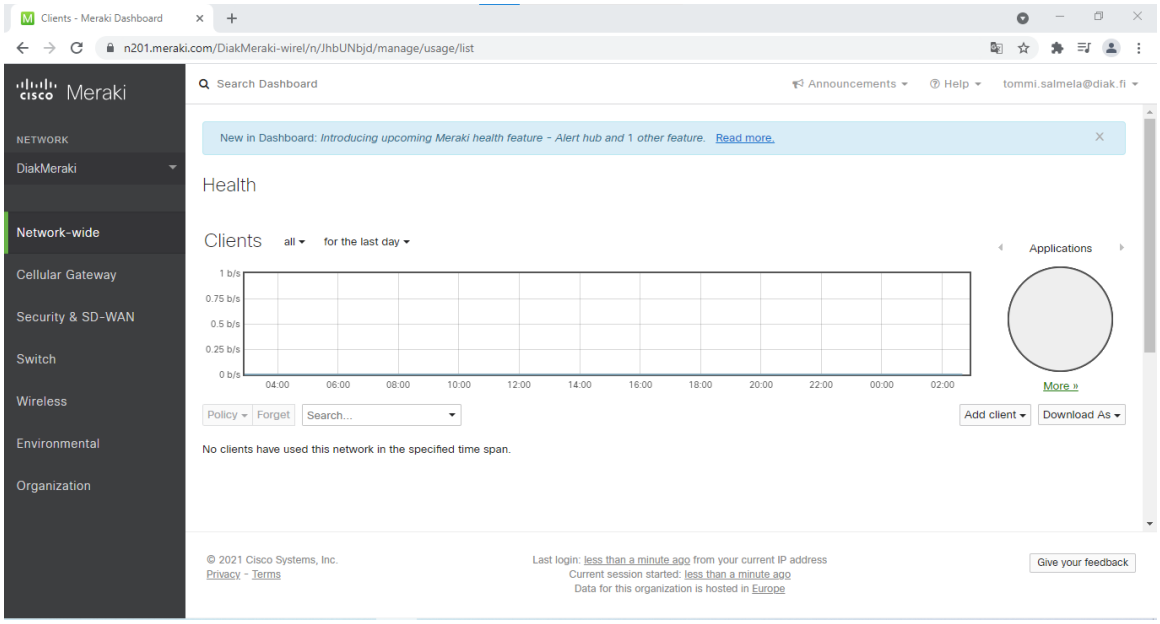
5.4 Meraki Dashboard

Dashboard on Merakin laitteiden ja verkon hallinnointiin käytettävä verkkoliittymä, jota hallitaan selaimen kautta. Dashboard on käytettävissä mistä päin maailmaa tahansa, kunhan verkkoyhteys on käytettävissä.

Verkkosivustolle (Kuva 7) pääsee kirjautumaan rekisteröimällään sähköpostiosoitteella, ja itse valitulla salasanalla. Dashboardiin kirjauduttua sisään, käyttäjä pääsee välittömästi hallinnoimaan verkkoa, laitteita tai halutessaan lisäämään muita ylläpitäjiä Dashboardille.



Kuva 7. Dashboardin kirjautumissivu.



Kuva 8. Dashboardin aloitussivu Dashboard Networkin luomisen jälkeen.

Ensimmäistä kertaa kirjautuessa (Kuva 8) Dashboardille, käyttäjää pyydetään antamaan tilausnumero tai laitteiden sarjanumerot, jotta laitteet voidaan rekisteröidä hallintapaneeliin. Tilausnumeron syöttämällä Dashboard tunnistaa välittö-

mästi kaikki tilausnumeroon liitetyt laitteet ja lisää kaikki laitteet suoraan hallittavaksi Dashboardin kautta.

Diakonia-ammattikorkeakoulun Merakin hallintaverkoksi luotiin tässä insinöörityössä DiakMeraki -niminen Dashboard Network. Hallintaverkon luomisen jälkeen luotiin kaksi eri SSID:llä toimivaa verkkoa. MerakiTest3-verkkotunnuksella toimiva verkko, joka konfiguroitiin toimimaan diak_private-verkon tavoin Windowsin sertifikaateilla, sekä DiakMeraki SSID:llä toimiva testiverkko, johon pääsi yhdistämään käyttämällä verkolle määritettyä salasanaa.

6 RADIUS-palvelimen konfigurointi

RADIUS (Remote Authentication Dial-In User Service) on vuonna 1991 kehitetty verkkoprotokolla, joka mahdollistaa keskitetyn hallinnan AAA-protokollalle. AAA-protokollalla (Authentication, authorization and accounting eli todentaminen, valtuutus ja tilastointi) tarkoitetaan menetelmää, jolla on mahdollista tunnistaa toinen osapuoli tietoverkossa.

Todentamispalvelun tarkoituksena on varmistaa, että verkkoon haluava käyttäjä on yksi verkon käyttöoikeuden omaavista käyttäjistä. Varmistus voi tapahtua esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmällä, kertakäyttöavaimella tai digitaalisella sertifikaatilla. Diakonia-ammattikorkeakoulun henkilökunnan työntekijöiden autentikointi tapahtuu Windows-sertifikaateilla, jotka RADIUS-palvelimella sijaitseva CA (Certificate Authority) todentaa sertifikaatin olevan aito ja hyväksyy yhteyden muodostamisen. [38]

Valtuutuspalvelulla käyttäjiä on mahdollista profiloida käyttäjille tarjottuja palveluita. Käyttäjälle voidaan myöntää tai evätä käyttöoikeuksia verkossa sijaitseviin palveluihin.

Tilastointipalvelulla kerätään tilastotietoja käyttäjien toiminnasta. Sen avulla on mahdollista tilastoida esimerkiksi yhteydenmuodostus- ja päättymisaikoja, IP-osoitteita, datan käyttöä ja käytettyjä palveluita.

6.1 Windows NPS

Langattomien verkkojen autentikointia varten otettiin käyttöön Windows Serverin päällä toimiva RADIUS-palvelin, johon lisättiin Windows Serverin ominaisuuksista Network Policy Server (NPS). NPS mahdollistaa autentikoinnin verkkoon käyttäen tietokoneille Active Directoryn kautta luotuja sertifikaatteja, jolloin verkkoon liityttäessä ei tarvitse käyttää salasanaa.

RADIUS-palvelimelle lisätyn NPS-komponentin ja ryhmäkäytäntöjen (Group Policy) avulla oli mahdollista luoda verkko, jonka SSID (Service Set Identifier) ei ollut julkisesti jaettu. Ryhmäkäytäntöihin lisätyllä verkkokäytännöllä (Network Policy) työntekijöiden tietokoneet yhdistettiin automaattisesti henkilökunnalle tarkoitettuun diak_private-verkkoon, ja NPS:n päälle rakennetun sertifikaatti-autentikoinnin myötä kone yhdisti automaattisesti verkkoon ilman salasanaa.

6.2 Windows Active Directory Domain Services

Windows Active Directory Domain Services (AD DS) on Microsoftin Windows-toimialueen työkalu, joka pitää sisällään käyttäjä- ja hakemistotoimintoja. Active Directory pitää sisällään tietoa käyttäjistä, ryhmistä, tietokoneista ja verkossa olevista resursseista, joita kutsutaan objekteiksi. Objekteille voi lisätä myös muita tietoja, kuten nimiä tai puhelinnumeroita, jotka ovat muille ylläpitäjille näkyvissä.

Diakonia-ammattikorkeakoulun AD:sta löytyy käyttäjät, käyttäjien ryhmät, tietokoneet ja muita laitteita. Ammattikorkeakoulun verkkoon kirjautuminen edellyttää, että käyttäjän tietokone on rekisteröity ammattikorkeakoulun Windows Active Directoryyn, jotta laite saa tarvitsemansa laitesertifikaatin. [39]

6.3 Henkilökunnan verkko

Ammattikorkeakoulun henkilökunnalle on rakennettu diak_private -verkko, johon yhdistäminen on mahdollista ainoastaan työpaikan työkoneilla. Jos tietokone ei ole rekisteröity AD:hen, käyttäjä ei pääse kirjautumaan ammattikorkeakoulun diak_private-sisäverkkoon.

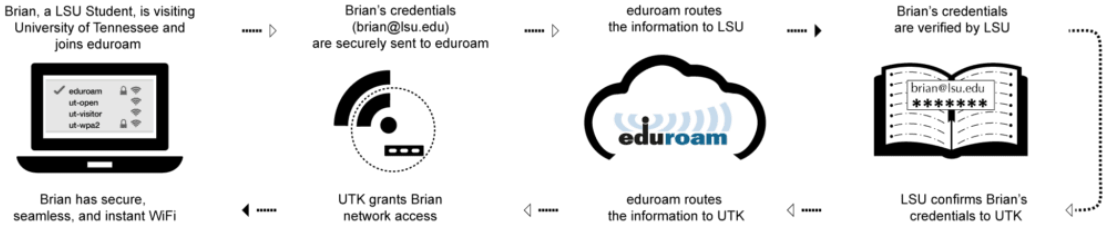
Verkko on piilotettuna Dashboardin asetusten kautta, eli verkko on näkyvissä ainoastaan työtietokoneilla, joille verkkoon kirjautuminen on määritetty ryhmäkäytännön kautta, mutta verkko ei ole näkyvissä muilla laitteilla. Verkkoon voi yrittää kirjautua, jos tietää verkon SSID:n, mutta verkkoon yhdistäminen ei onnistu, ellei laite ole rekisteröity Diakonia-ammattikorkeakoulun Windows Active Directoryyn. Henkilökunnan työtietokoneille on ryhmäkäytäntöjen kautta määritettynä diak_private-verkko automaattisesti haettavaksi, ja tietokoneet yhdistävät automaattisesti kyseiseen verkkoon.

Insinöörityössä rakennettu MerakiTest3-verkko konfiguroitiin toimimaan samoilla Windows-sertifikaateilla, kuin diak_private-verkko. Verkko ei ollut näkyvissä automaattisesti millään laitteilla, mutta työtietokoneilla verkkoon pääsi yhdistämään manuaalisesti Windowsista SSID:tä käyttämällä. Muilla laitteilla, kuten puhelimilla, ei verkkoon yhdistäminen ole mahdollista Windows-sertifikaatin puuttumisen vuoksi.

6.4 Eduroam-verkko

Eduroam on kansainvälinen langaton verkkovierailupalvelu, joka mahdollistaa pääsyn verkkoon esimerkiksi opiskelijoille tai opettajille, jotka ovat käymässä muussa kuin omassa oppilaitoksessa. Käyttäjät käyttävät verkkoon kirjautuessaan oman kotiorganisaationsa käyttäjätunnusta ja salasanaa sijainnista riippumatta. Vieraillun organisaation verkko lähettää autentikointipyynnön (Kuva 9) käyttäjän kotiorganisaatiolle RADIUS-palvelinjärjestelmän kautta, joka tarkistaa käyttäjän tunnistetiedot ja lähettää vieraillulle laitokselle tarkastuksen tuloksen

RADIUS-palvelimien kautta, jonka perusteella kirjautumisyritys hyväksytään tai evätään.



Kuva 9. Eduroamin autentikointipyyntö. [40]

Eduroam on maksuton palvelu, joka on mahdollista ottaa käyttöön kaikissa oppi- ja tutkimuslaitoksissa tai koulutukseen liittyvissä organisaatioissa. Palvelua tarjotaan kuitenkin vierailijoille myös esimerkiksi lentoasemilla, kahviloissa ja jopa opiskelija-asunnoissa. Eduroam on käytössä kaikissa yliopistoissa sekä ammattikorkeakouluissa Suomessa. [40; 41; 42]

Alun perin eduroam SSID:tä varten oli tarkoitus konfiguroida RADIUS-palvelimelle autentikointi eduroamin RADIUS-palvelimia käyttäen, mutta geteduroam-applikaation myötä tarve tälle poistui. Geteduroam on applikaatio, joka on tehty eduroam-verkkoon kirjautumisen helpottamiseen käyttäjämäärien lisäämiseksi. [43]

Eduroam-verkkoon yhdistäminen oli ajoittain koulun opiskelijoille haastavaa johtuen laitemalleista olevista eroista verkkoasetusten suhteen sekä eduroam-verkon verkkomäärityksistä. Geteduroamiin siirtymisen myötä opiskelijoiden oli helpompi päästä verkkoon, sillä verkkoon yhdistäminen vaatii mobiililaitteille ja tietokoneille ohjelmiston lataamisen, jonka myötä laitemallien verkkoasetusten eroista johtuvat ongelmat poistuivat.

7 Työn tulokset

Puolitoista vuotta Merakin käyttöönoton jälkeen haastattelin ammattikorkeakoulun IT-tuessa toimivia henkilöitä eduroam-verkon muutoksista ja Merakin käyttöönoton hyödyistä ja kokemuksista. Eduroam-verkon muutosten myötä Diakonia-ammattikorkeakoulun IT-tuki on saanut vähemmän yhteydenottoja opiskelijoilta eduroam-verkkoon yhdistämiseen liittyvistä ongelmista. Aikaisemmin eduroam-verkkoon kirjautumiset aiheuttivat ongelmia opiskelijoille johtuen laitemallien ja laitteiden verkkoasetusten eroista sekä käyttäjätunnusten salasanamuutoksista. Opiskelijoiden täytyy vaihtaa salasanaansa muutamaan kertaan opintojen aikana, ja salasanan muuttamisen jälkeen verkkoon kirjautuminen oli aiheuttanut ongelmia, kun laitteet olivat edelleen yrittäneet kirjautua eduroam-verkkoon käyttäen käyttäjän vanhaa salasanaa. Verkko oli näissä tapauksissa täytynyt unohtaa tietokoneen verkkoasetuksista, jotta eduroam-verkkoon pääsee kirjautumaan.

Muutosten myötä opiskelijoille ei välittömästi välittynyt viesti muutoksista ja tästä johtuen lähitukihenkilöt olivat saaneet muutamia kyselyitä eduroam-verkon toimimattomuudesta. Siirtyminen geteduroam-sovelluksen kautta tapahtuvan kirjautumiseen normaalin verkkokirjautumisen sijaan oli ollut opiskelijoille haastavaa. Ilmenneiden haasteiden takia opiskelijoille tiedotettiin uudelleen ammattikorkeakoulun geteduroam-applikaatiosta, jonka jälkeen opiskelijat ovat omatoimisesti päässeet kirjautumaan verkkoon ilman suurempia ongelmia.

Insinöörityön tarkoituksena oli todistaa Diakonia-ammattikorkeakoulun pilvihallittavuuden tuomat hyödyt. Insinöörityössä testattu Meraki ja sen selaimen kautta tapahtuva hallinta on vähentänyt verkon hallinnoimiseen käytettyjä henkilötyötunteja huomattavasti. Erityisesti valvontaan käytetty aika on vähentynyt huomattavasti, sillä valvonnan hälytyksistä tulee sekä verkkoasiantuntijoille että IT-tukihenkilöille sähköpostia, mikäli ongelmia ilmenee.

Uusien laitteiden käyttöönotto on helpompaa ja tästä syystä myös Diakonia-ammattikorkeakoulun kaikille muille kampuksille on jo pääosin otettu Merakin laitteet käyttöön. Aikaisemmin käytössä olleet laitteet alkoivat olla elinkaarensa päässä ja laitehankintoja oli harkittu jo aikaisemmin. IT-osasto koki, että Merakin käyttöönotto on vähentänyt heidän kustannuksiaan ja työtaakkaa. Käyttöön liittyvien ongelmatilanteiden selvittelyyn käytetty aika on vähentynyt huomattavasti.

Ammattikorkeakoulu on myös osittain insinöörityössä saavutettujen tavoitteiden täyttymisen myötä päättänyt siirtää muitakin palveluitaan pilvihallittaviksi tulevina vuosina. [44]

8 Yhteenveto

Insinöörityön tarkoituksena oli perehtyä pilvihallittavien ratkaisuiden tuomiin etuihin organisaatiolle. Työssä perehdyttiin erityisesti Cisco Merakin tuoteperheen ratkaisuihin keskisuuressa ympäristössä. Työtä tehdessä pohdittiin ja vertailtiin pilvihallittavan ympäristön ja on-premise-ympäristön eroavaisuuksia ja pilvipalveluiden tuomia mahdollisuuksia.

Organisaation tarpeet muuttuivat työn aikana, eikä alun perin suunniteltua opiskelijaverkkoa tarvinnut rakentaa alkuperäisen suunnitelman mukaisesti. Teknologian ja uusien ratkaisuiden kehittyessä tämä on nykypäivän IT-standardien mukaista ja organisaatio halusi luonnollisesti siirtyä helpommin saavutettavaan ja toimivampaan geteduroam-ratkaisuun, jonka käyttöönotto oli huomattavasti helpompaa organisaatiolle kuin alun perin kuviteltiin.

Loppukäyttäjien näkökulmasta uusi ratkaisu oli myös hyödyllinen, sillä aikaisemmassa opiskelijaverkkoratkaisussa oli ollut ongelmia erityisesti verkkoon kirjautumisessa.

Pilvihallittavat verkkoratkaisut olivat sekä organisaatiolle että minulle uusi konsepti ennen insinöörityön aloittamista. Käyttöönoton alusta lähtien organisaation tietoliikenteen asiantuntijat olivat vakuuttuneita järjestelmän tuomista hyödyistä.

Uusien laitteiden käyttöönotto oli alusta lähtien helpompaa kuin normaaleissa on-premise-ratkaisuissa. Laitteiden konfigurointi ja asennus oli suoraviivaista ja käyttöönoton dokumentaatio oli laadukasta mahdollistaen nopean siirtymisen pilvihallittaviin laitteisiin.

Pilvipalveluiden yleistyessä on luonnollista, että yritykset haluavat siirtyä helpommin konfiguroitaviin ja ylläpidettäviin pilvipohjaisiin ratkaisuihin. Hallittavuuden sijaitessa pilvessä ongelmat ovat usein helpompi korjata yksinkertaistetun käyttöliittymän avulla jopa etänä.

Ennen Merakin käyttöönottoa laitteisiin täytyi ottaa SSH-yhteys laitteen konfiguroimiseksi ja verkkolaitteiden IP-osoitteet oli listattu Excel-tiedostoihin tehden laitehallinnasta työlästä. Skaalautuvuuden myötä uusiin tarpeisiin on helpompi reagoida ja tarvittaessa lisätä tai poistaa laitteita käytöstä.

Keskitetyn selaimen kautta tapahtuvan hallinnoinnin myötä vianhallinta ja valvonta on tehty helpommaksi kuin perinteisissä verkkoratkaisuissa ja vikatilanteissa hälytykset tulevat automatisoidusti sähköpostiin. Näin myös vikatilanteiden hallinta nopeutuu ja tehostuu.

Lähteet

1 Kananen, Jorma. 2010. Opinnäytetyön kirjoittamisen käytännön opas. Jyväskylän ammattikorkeakoulu.

2 Kvalimotv. Menetelmäopetuksen tietovaranto. Laadullisen tutkimuksen Verkkoaineisto. https://www.fsd.tuni.fi/fi/tietoarkisto/julkaisut/kvalimotv.pdf

3 About Meraki. Cisco. Verkkoaineisto. https://meraki.cisco.com/about/

4 Annual report. Cisco. Verkkoaineisto. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf

5 Meeson, Will. 2019. A Must Read About Cisco Meraki. Verkkoaineisto. https://medium.com/@WillMeeson/a-must-read-about-cisco-meraki-cca188977371

6 Sawers, Paul. 2023. Meraki vs. Ubiquiti: Full Networking Comparison. Verkkoaineisto. https://history-computer.com/meraki-vs-ubiquiti-full-networking-comparison/

7 Dignan, Larry. 2012. Cisco buys Meraki for $1.2 billion: 5 reasons the deal makes sense. Verkkoaineisto. https://www.zdnet.com/article/cisco-buys-meraki-for-1-2-billion-5-reasons-the-deal-makes-sense/

8 Experience the Meraki IT product portfolio. Cisco. Verkkoaineisto. https://meraki.cisco.com/products/

9 Meraki Wireless Cloud-Managed Wireless Access Points. Cisco. Verkkoaineisto. https://meraki.cisco.com/product-collateral/meraki-wireless-cloud-family-datasheet-managed-wireless-access-points/?file

10 Cisco. Switches. Verkkoaineisto. https://meraki.cisco.com/products/switches/

11 Cisco. Smart Cameras. Verkkoaineisto. https://meraki.cisco.com/products/smart-cameras/

12 Cisco. MT Cloud-Managed Sensors. Verkkoaineisto. https://meraki.cisco.com/product-collateral/mt-family-datasheet-20220308-english/?file

13 Microsoft. What is cloud computing? Verkkoaineisto. https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits

14 Cloud Computing Market. Verkkoaineisto. https://www.fortunebusinessinsights.com/cloud-computing-market-102697

15 Hiter, Shelby. 2021. Cloud Computing Market. Verkkoaineisto. https://www.datamation.com/cloud/cloud-computing-market/

16 Red Hat. 2022. IaaS vs. PaaS vs. SaaS. Verkkoaineisto. https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas

17 Eronen, Heidi. 2016. IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Verkkoaineisto. https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/

18 Wallenius, Niklas. 2022. Konttiteknologia – mitä kontit ovat ja mitä hyötyä niistä on? Verkkoaineisto. https://niklaswallenius.fi/konttiteknologia-mita-hyotya/

19 Gray, Jasmine. 2022. The 10 Largest Cloud Computing Companies In The World, And What They Do. Verkkoaineisto. https://history-computer.com/largest-cloud-computing-companies-in-the-world/

20 Raza, Muhammad. 2020. Public vs Private vs Hybrid: Cloud Differences Explained. Verkkoaineisto. https://www.bmc.com/blogs/public-private-hybrid-cloud/

21 Microsoft. What are public, private, and hybrid clouds? Verkkoaineisto. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#overview

22 Abramson, Norman. 1970. THE ALOHA SYSTEM—Another alternative for computer communications*. Verkkoaineisto. https://www.clear.rice.edu/comp551/papers/Abramson-Aloha.pdf

23 History of Wireless LANs. Verkkoaineisto. https://jfearn.fedorapeople.org/fdocs/en-US/Fedora/17/html/Wireless_Guide/sect-Wireless_Guide-Introduction-History_Of_Wireless_LANs.html

24 Netgear Support. 2021. Miten Wi-Fi 6 eroaa Wi-Fi 5:stä? Verkkoaineisto. https://kb.netgear.com/fi/000059637/Miten-Wi-Fi-6-eroaa-Wi-Fi-5-st%C3%A4?language=fi

25 Raza, Muhammad. 2018. OSI Model: The 7 layers of Network Architecture. Verkkoaineisto. https://www.bmc.com/blogs/osi-model-7-layers/

26 What is layer 7? | How layer 7 of the Internet works. Verkkoaineisto. https://www.cloudflare.com/learning/ddos/what-is-layer-7/

27 Presentation Layer (Layer 6). Verkkoaineisto. http://www.tcpipguide.com/free/t_PresentationLayerLayer6.htm

28 Session Layer. Verkkoaineisto. https://osi-model.com/session-layer/

29 What is Layer 4 of the OSI Model? Verkkoaineisto. https://www.a10networks.com/glossary/what-is-layer-4-of-the-osi-model/

30 Network Fundamentals – Layer 3 Technologies. Verkkoaineisto. https://www.howtonetwork.org/design/ccda/chapter-1-network-fundamentals/network-fundamentals-layer-3-technologies/

31 Layers of OSI Model. Verkkoaineisto. https://www.geeksforgeeks.org/layers-of-osi-model/

32 Shaw, Keith. 2022. What is MU-MIMO, and why is it essential for Wi-Fi 6 and 6E? Verkkoaineisto. https://www.networkworld.com/article/3250268/what-is-mu-mimo-and-why-is-it-essential-for-wi-fi-6-and-6e.html

33 Mikola, Janne. Blogi: Mikä on SD-WAN? Verkkoaineisto. https://www.telia.fi/yrityksille/artikkelit/artikkeli/mika-on-sd-wan

34 Elisa. SD-WAN siirtää yritysverkkosi pilveen. Verkkoaineisto. https://yrityksille.elisa.fi/sdwan

35 Niinijärvi, Niko. 2020. Mikä on SD-WAN? Verkkoaineisto. https://www.tnnet.fi/blogi/mika-on-sd-wan/

36 Cisco. 2022. MS120 Overview and Specifications. Verkkoaineisto. https://documentation.meraki.com/MS/MS_Overview_and_Specifications/MS120_Overview_and_Specifications

37 Cisco Meraki MS120-24 Managed L2 Gigabit Ethernet [10/100/1000] 1U Grey. Verkkoaineisto. https://www.lambda-tek.com/Cisco-MS120-24-HW~sh/B25396093

38 Metzler, Sam. How to Create and Enroll a RADIUS Server Certificate. Verkkoaineisto. https://www.cloudradius.com/how-to-create-and-enroll-a-radius-server-certificate/

39 Microsoft. Active Directory Domain Services Overview. Verkkoaineisto. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

40 What is eduroam and how does it work? Verkkoaineisto. https://incommon.org/eduroam/what-is-eduroam/

41 Introduction to geteduroam. Verkkoaineisto. https://www.geteduroam.app/about/

42 Frequently Asked Questions. Verkkoaineisto. https://eduroam.org/faqs/

43 Oma organisaatio mukaan eduroamiin. Verkkoaineisto. https://www.eduroam.fi/liity-eduroamiin

44 Ohvo, Henri. 2023. ICT-Asiantuntija, Diakonia-ammattikorkeakoulu, Helsinki. Haastattelu 8.3.2023.