Pienyrityksen lähiverkon suunnittelu Cisco Merakin laitteilla

Tanreco Oy

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Riihimäen kampus, Tieto- ja viestintätekniikka

Syksy 2020

Jaakko Kangas

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Riihimäki

Tekijä Jaakko Kangas **Vuosi** 2020

Työn nimi Pienyrityksen lähiverkon suunnittelu Cisco Merakin laitteilla

Työn ohjaajat Marko Grönfors, Mika Toivakka

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli suunnitella uusi langaton lähiverkko pilvihallittavilla Cisco Merakin verkkolaitteilla. Työn toimeksiantajana toimi riihimäkeläinen konepajateollisuuden kone- ja laitetoimittaja Tanreco Oy, joka haluaa tulevaisuudessa uudistaa lähiverkkonsa. Opinnäytetyössä painottui lähiverkkoa suunnitellessa käytetyn palvelun hyötyihin kuuluvat tietoturvallisuus, verkon hallittavuus, vikasietoisuus ja kustannustehokkuus.

Opinnäytetyön teoriaosuudessa käytiin läpi langattomien verkkojen toimintamallia, perehdyttiin pilvipalveluihin ja nykyään myös pilvipalveluina tuotettuihin tietoverkkoratkaisuihin. Lisäksi perehdyttiin Cisco Merakin verkkolaitteiden tarjoamiin palveluihin ja hyötyihin.

Käytännön osuudessa suoritettiin palveluntarjoajan käyttöliittymän demoversiossa virtuaalinen toteutus, josta laaditaan käyttöönottosuunnitelma tulevaisuudessa fyysisillä laitteilla toteutettavasta lähiverkosta.

Työn lopputuloksena saatiin suunniteltua uusi tietoturvallisempi, kustannustehokkaampi ja eheämpi langaton lähiverkko, joka vastaa yrityksen nykyisiä vaatimuksia ja tarpeita.

Avainsanat Cisco, Meraki, Tietoliikenne, WLAN

Sivut 46 sivua, joista liitteitä 3 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology
Riihimäki

Author Jaakko Kangas **Year** 2020

Subject Designing a small business Local Area Network with Cisco Meraki devices

Supervisors Marko Grönfors, Mika Toivakka

ABSTRACT

The purpose of this project was to design a new wireless LAN by using cloud-managed Cisco Meraki network devices. The work was commissioned by Tanreco Oy, a machinery and equipment supplier too the engineering industry in Riihimäki, that wanted to redesign its local area network to the future. In the thesis, the benefits of the service used in the design of the local area network included information security, network manageability, fault tolerance and cost-effectiveness.

In the theoretical part of the thesis, the operating model of wireless networks is reviewed, and cloud services and computer network solutions produced today also as cloud services are introduced. In addition, the services and benefits provided by Cisco Meraki network devices are examined.

In the empirical part, a virtual implementation was performed in the demo version of the service provider's user interface, from which a deployment plan was prepared for the local area network to be implemented with physical devices in the future.

As a result, a new, more secure, cost-effective, and integrated wireless LAN was created that met the company's current requirements and needs.

Keywords Cisco, Meraki, Telecommunication, WLAN

Pages 46 pages including appendices 3 pages

SISÄLLYS

1 JOHDANTO 1

2 LANGATTOMAT LÄHIVERKOT 2

2.1 Historia 2
2.2 WLAN-Tekniikan hyöty 2
2.3 Topologiat 2
2.4 IEEE 802.11 4
2.4.1 Fyysinen kerros 4
2.4.2 Siirtokerros 4
2.4.3 IEEE 802.11 Standardit 5
2.4.4 802.11ac ja ax 6
2.4.5. MIMO ja MU-MIMO 6
2.5 Tietoturvallisuus 8
2.5.1 Palomuurit 8
2.5.2 Langattomien verkkojen salausmenetelmiä 9
2.5.3 VPN 11

3 PILVIPALVELUT 12

3.1 Historia 13
3.2 Haasteet 13
3.3 Arkkitehtuuri 14
3.3.1 Julkinen pilvipalvelu 14
3.3.2 Yksityinen pilvipalvelu 14
3.3.3 Hybridipilvi 15
3.3.4 Multicloud 15
3.4 Pilvipalvelumallit 15
3.4.1 IaaS 16
3.4.2 PaaS 16
3.4.4 SaaS 16
3.5 Tietoverkot pilvessä 17

4 CISCO MERAKI 18

4.1 Historia 19
4.2 Arkkitehtuuri 19
4.3 Pilvihallinta 20
4.4 Tuoteperhe 20
4.5 Tulevaisuus ja haasteet 21

5 LANGATTOMAN LÄHIVERKON SUUNNITTELU JA TOTEUTUS 21

5.1 Nykytilanne 21
5.2 Uuden verkon toteutus 23
5.3 Verkossa käytettävät laitteet 23
5.3.1 MX67W-palomuuri 23
5.3.2 MS125-24-porttinen kytkin 24
5.3.3 MR33-sisäkäyttöinen langaton tukiasema 24

5.3.4 MR74-ulkokäyttöinen langaton tukiasema 25
5.3.5 MV72- ja MV12W-valvontakamerat 25

6 CISCO MERAKIN KÄYTTÖÖNOTTO 25

6.1 Käyttöliittymä 26
6.1.1 Uuden asiakkuuden luominen 26
6.1.2 Langattoman lähiverkon konfigurointi 29
6.2 Lähiverkon dokumentointi ja analysointi 41

7 YHTEENVETO 43

LÄHTEET 45

1 JOHDANTO

Nykyaikaiselta tietoliikenneverkolta vaaditaan paljon enemmän, kun Internet-yhteyttä vaativien palveluiden määrä on kasvanut ja niin suuret kuin pienet yritykset tarvitsevat enemmän verkonhallintaa kuin aikaisemmin. Yrityksien lähiverkkojen on tarkoitus toimia tiedonvälityksen nopeuttajana, jotta työt voitaisiin tehdä kustannustehokkaasti, sekä lähiverkolle on tärkeää olla suunniteltu ja toteutettu niin, että yrityksen sisäinen tiedonkulku olisi esteetön.

Tässä opinnäytetyössä käytäntönä on suunnitella pienyritykselle lähiverkko, jota hallinnoidaan pilvipalvelun tarjoamaa käyttöliittymää hyödyntäen. Työssä tutkitaan pilvipalveluiden toimivuutta, langattomia lähiverkkoja yleisesti, sekä teoriatasolla että teoriapohjaisen käytännönosuuden kautta. Tavoitteena on laatia laajamittainen dokumentaatio teoriaosuuteen pohjautuen, jonka avulla yritys voi arvioida tulevia laitehankintojaan ja näin ollen rakennuttaa lähiverkkonsa uusiksi.

Työn tilaaja on Tanreco Oy, jonka toimipiste löytyy Riihimäeltä. Tanreco Oy on jo pidemmän aikaa halunnut uudistaa lähiverkkonsa. Heillä on yksi iso hallirakennus, johon kuuluu toimisto- sekä varastotilat. Rakennuksen pohjapiirustukset ovat vuodelta 1981, jonka jälkeen tilat ovat muuttuneet paljon eikä tämänhetkinen lähiverkon laitteisto vastaa nykypäiväistä mallia. Yritykselle ei kulje valokuituyhteyttä, vaan yrityksessä on vielä puhelinkaapelointi käytössä. Tanreco Oy:n vaatimuksena lähiverkolle on, että laitteistoa ei tarvitsisi siinä vaiheessa enää uusia, kun valokuitukaapelointi rakennutetaan heidän kiinteistöönsä, vaan laitteisto olisi valokuituvalmis.

Työn aloittamiseen tarvitaan kattava kuvaus siitä, millainen nykyinen verkkotopologia on, ennen kuin aletaan suunnittelemaan muutoksia. Nykyinen lähiverkko on suhteellisen pieni, sillä yrityksellä ei ole tarvetta isommalle verkolle. Kuitenkin huomioitavaa työssä on, että lähiverkon tulee kattaa langattoman verkon kuuluvuus koko kiinteistölle. Tähän tullaan hyödyntämään pohjapiirustuksia, joita käytetään kuuluvuusmittauksissa. Mitatessa langattomien tukiasemien sijaintia on tiedettävä yrityksen tilojen pinta-alat, jotta asennettavat tukiasemat voidaan konfiguroida oikeanlaisiksi, jotta tiloihin ei jäisi katvealueita.

Työtä tehdessä on tärkeää huomioida myös tietoturvallisuus, lähiverkon redundanttisuus ja kustannustehokkuus. Toisin sanoen yrityksen lähiverkon on kyettävä täyttämään vaadittavat kriteerit ja lisäksi myös toimimaan teknillisellä tasolla niin, että yrityksen muu infrastruktuuri hyötyisi siitä.

2 LANGATTOMAT LÄHIVERKOT

WLAN-lähiverkko (Wireless Local Area Network), joka virallisemmin nykyään tunnetaan Wi-Fi:nä (Wireless Fidelity), on langallisen lähiverkon rinnalle kehitetty menetelmä rakennuttaa lähiverkkoja. WLAN-yhteys perustuu lähiverkkoon kytketyn tukiasemana toimivan reitittimen muodostamaan kenttään, jonka kuuluvuusalueella sijaitsevat päätelaitteet, jotka tukevat langatonta yhteyttä voivat yhdistää itsensä verkkoon. (Schwartz. M, 2020)

2.1 Historia

Ensimmäisen langattoman lähiverkon, jonka nimi oli ALOHAnet kehitti Hawajin yliopiston professori Norman Abramson. Vuonna 1971 valmistui kokeellinen neljällä eri saarella sijaitsevan seitsemän tietokoneen välinen verkko, jotka keskustelivat Oahu:n saarella sijaitsevan keskustietokoneen kanssa. Järjestelmä käytti kahta 100 KHz kanavaa UHF-taajuudella, toinen vastaanottavaa yhteyttä tietokoneilta varten ja toinen keskustietokoneen lähetyksiä varten. Lähiverkko oli rakennutettu tähtitopologiaksi, jolloin vain keskustietokone pystyi vastaanottamaan lähetyksiä toisella kanavalla. (Schwartz. M, 2020)

2.2 WLAN-Tekniikan hyöty

WLAN-verkkojen käyttö on yleistynyt sekä kuluttajilla, että yrityksen aloilla, joissa lähiverkon kaapelointi on ollut vaikeampaa käyttäen langallista lähiverkkoa. Nykyään saatavilla on päätelaitteistoa, jotka tukevat sekä langallista että langatonta lähiverkkoa tarjoten mahdollisuuden hyödyntää molempia menetelmiä. Langattoman verkon hyötyihin kuuluu mm., että nykyään päätelaitteet kuten matkapuhelimet, tabletit jne., jotka eivät voi olla lähiverkossa kiinni langallisesti voivat muodostaa yhteyden lähiverkkoon niihin sisään rakennutettujen langattoman verkon vastaanottimien avulla. Lisäksi WLAN-verkko vähentää lähiverkkoon tarvittavaa kaapelointia ja on näin ollen yksinkertaisempi rakennuttaa kuin langallinen lähiverkko. Lisäksi langattoman lähiverkon laajentaminen on kustannustehokasta ja helpompaa kuin kiinteän lähiverkon. (STUK, 2020).

2.3 Topologiat

Langattomien lähiverkkojen rakennusmenetelmiä on kolme päämallia, joista löytyy sovellutuksia: BSS (Basic Service Set), IBSS (Independent Basic Service Set) ESS (Extended Service Set). Kuvassa 1 nähdään näiden rakenne visualisoituina.

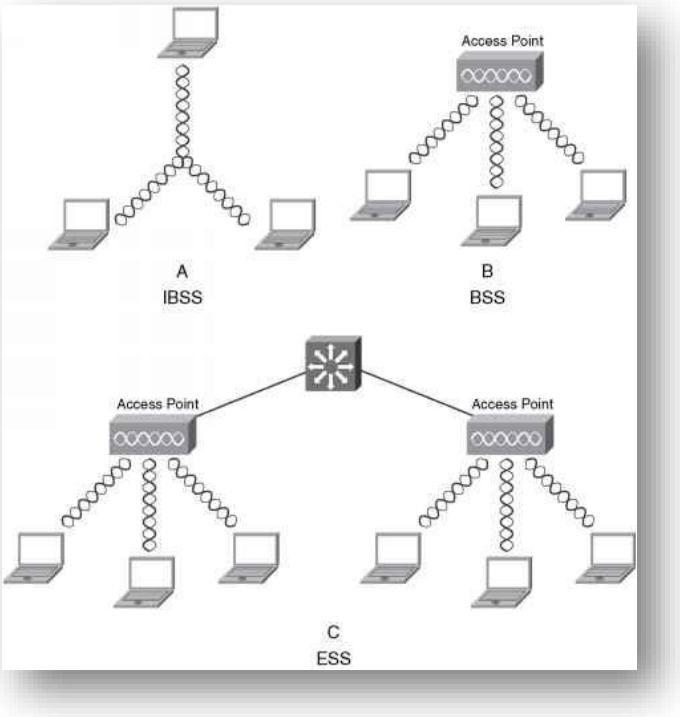
IBSS on ns. ad hoc-verkko eli siltä puuttuu infrastruktuuri, tässä tapauksessa kommunikoiva langaton reititin. Kaikki samaan verkkoon

yhdistetyt laitteet keskustelevat suoraan keskenään, näin ollen kaikkien laitteiden tulee olla toistensa kantaman sisällä pystyäkseen kommunikoimaan.

BSS-mallisella verkolla tarkoitetaan, että verkkoon on liitetty tukiasema (Access Point), joka keskustelee siinä olevien käyttäjien kanssa. Tukiasema yhdistää käyttäjän verkkoon sen mainostaman verkkotunnuksen avulla. Tukiasema vastaanottaa käyttäjien lähettämät tiedonsiirtopyynnöt, ja siirtää ne toiselle käyttäjälle. Jokaista tukiasemaa hallinnoidaan joko suoraan tukiaseman omasta hallinnointiohjelmasta, tai tukiasemalle on määritelty oma tukiasemaohjain (Wireless Lan Controller), johon se on kytkettynä.

ESS-verkko kattaa useamman siihen sisälletyn BSS-mallilla rakennetun verkon. Tukiasemat voivat jakaa samaa tai useampaa verkkotunnusta useamman tukiaseman välityksellä kaikille käyttäjille.

Langaton Mesh-verkko on kehittyneempi tukiasemapohjainen verkko. Usean samassa verkossa olevan langattoman tukiaseman muodostama verkko, jotka keskustelevat keskenään, luoden koko halutun alueen kattavan langattoman verkon. Mesh-tekniikalla toteutettu lähiverkko on myös nopeampi kuin esimerkiksi wlan-toistimien avulla toteutettu, sillä siinä missä Mesh-tukiasemat osaavat siirtää ja ohjata käyttäjän verkkoliikenteen nopeimmalle taajuusalueelle sekä vähäruuhkaisimmalle kanavalle, wlan-toistimet puolittavat niiden kautta kulkevan kaistanleveyden. Mitä enemmän toistimia, sitä pienempi kaistanleveys on saatavilla viimeisillä toistimilla.



Kuva 1. Langattomien lähiverkkojen topologiat (Ccexpert, n.d)

2.4 **IEEE 802.11**

IEEE 802.11 on IEEE: n (Institute of Electrical and Electronic Engineers) kehittämä standardi langattomille lähiverkoille. Nämä standardit koskevat ainoastaan OSI-mallin (Open Systems Interconnection Reference Model) fyysistä- sekä siirtokerrosta. 802.11 standardit pyrkivät toimimaan siirtokerroksella niin, että vaikka kyseessä olisi eri standardi, ne eroaisivat vain fyysisellä kerroksella toisistaan, ja olisivat myös taaksepäin sopivia siirtokerroksella. (Microsoft, n.d.)

2.4.1 Fyysinen kerros

Fyysisellä kerroksella 802.11 standardin OSI-malli kuvaa, miten tieto liikkuu verkkoon liitettyjen tietokoneilla toimivien sovelluksien välityksellä. OSI-malli tarkastelee yksinkertaisimmillaan vain kahden verkkolaitteen tiedon välityksen tapahtumia sen siirtyessä laitteesta toiseen.

OSI-mallin fyysinen kerros kuvastaa laitteiden fyysisiä sekä elektronisia ominaisuuksia. Etenkin verkkolaitteiden ja siirtomedian välistä suhdetta. Fyysiselle kerrokselle päätoimintoja ovat:

- Signaalien oikeaan muotoon muuntaminen, median sekä käytettävien laitteiden mukaisesti.
- Resurssien jakaminen useamman käyttäjän kesken
- Yhteyksien luominen ja sulkeminen siirtomediaan

Fyysinen kerros jaotellaan vielä kolmeen alikerrokseen. PLCP (Physical Layer Convergence Procedure), joka toimii MAC-alikerroksen ja PMD:n välillä sovituskerroksena. PLCP valmistaa paketit erilaisille fyysisen kerroksen toiminnoille. PLCP myös kasaa MAC-alikerrokselta saapuvat paketit muotoon, jotta PMD pystyy lähettämään ne siirtomediaa pitkin. (Studytonight, 2020) PMD (Physical Medium Dependent) huolehtii datan vastaanottamisesta, lähettämisestä sekä vastaa tarvittavasta kanavoinnista moduloinnista. (media.techtarget, n.d.)

2.4.2 Siirtokerros

Siirtokerroksen tehtävä on kehystää kaikki paketit, jotka saapuvat ylemmiltä kerroksilta ja lähettää ne eteenpäin fyysisen kerroksen mediaa pitkin. 802.11-standardissa tämä kerros on jaoteltu kolmeen alikerrokseen. (Liveaction, 2020)

LLC (Logical Link Control) hallitsee toimenpiteitä, joilla luodaan loogisia linkkejä verkossa olevien laitteiden välille. LLC kehystää ylemmältä verkkoprotokollalta saapuvat paketit. IEEE 802.2 LLC tarjoaa myös sekä

langalliselle että langattomalle lähiverkkoteknologialle yhteisen rajapinnan. (Liveaction, 2020)

Siirtokerroksen alaosaan jäävä MAC-alikerros sisältää toiminnot ja menettelytavat, joilla dataa ohjataan verkon ollessa kokonaisuuksien välillä. Tämä alikerros havaitsee ja korjaa myös mahdollisia fyysisellä kerroksella tapahtuvia ongelmia. MAC-alikerrokseen sisältyy vastuualueet, jotka on eritelty MAC-hallinta-alikerrokselle. Hallinta-alikerros hallinnoi virrankulutusta, turvallisuuteen liittyviä toimintoja sekä verkkovierailuita. MAC-alikerros määrittelee pääsytoiminnot sekä pakettiformaatit. (Liveaction, 2020)

2.4.3 IEEE 802.11 Standardit

Alkuperäinen 802.11-standardi kehiteltiin vuonna 1997. Tästä lähtien 802.11-standardien kehitys on jatkunut yli 20 vuotta. Ensimmäisen version päästessä tiedonsiirron nopeuksissa 2 Mbit/s lukemiin, nykyiseltään 802.11ax (Wi-Fi 6) standardin avulla päästään teoreettisesti 11 Gbit/s siirtonopeuksiin. Kuvassa 2 nähdään kaikki 802.11-standardit ja niiden ominaisuudet.

TABLE 1: IEEE 802.11 COMMON WIFI STANDARDS BREAKDOWN

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80= 160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

Kuva 2. 802.11-standardeja (DeLisle. J-J, 2015)

2.4.4 802.11ac ja ax

2013 kesäkuussa ilmestynyt 802.11ac (kuluttajaystävällisemmin Wi-Fi 5) oli edeltäjänsä 802.11n:n jatkajaksi suunniteltu standardi. Uusimpina ominaisuuksina olivat leveämmät 80 MHz ja 160 MHz kanavat 5 GHz:n taajuusalueelle, tehokkaampi 256 QAM-modulointi (Quadrature Amplituide Modulation) sekä parannellut moniantennitekniikat. (Weinberg. N, 2018)

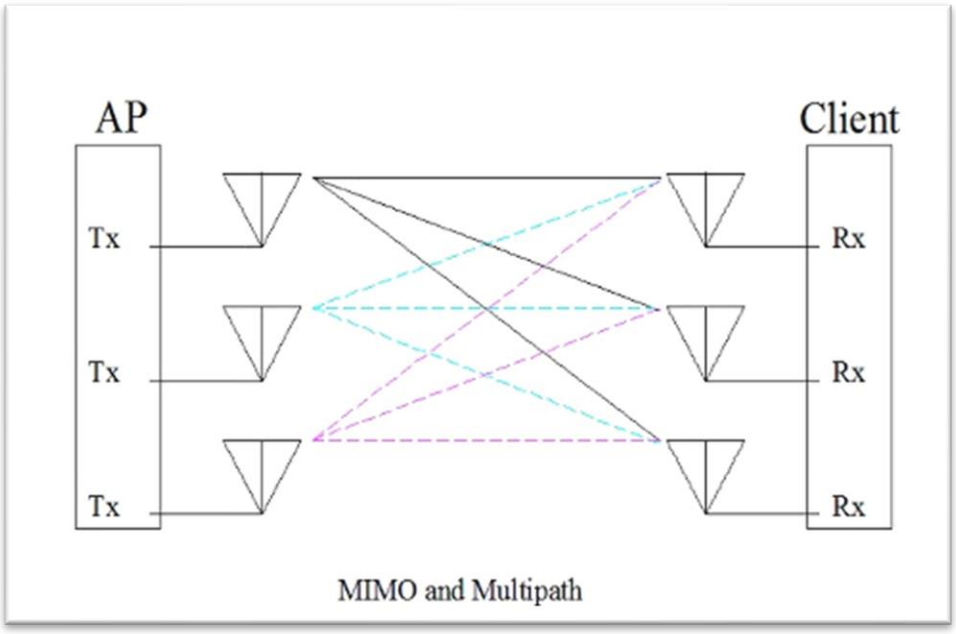
802.11ac:ssä käytetään sekä 5 GHz:n taajuutta että 2,4 GHz:n yhdessä. Kaistanleveys on ollut tärkeä tekijä standardien kehitykselle, jotta tiedonsiirtonopeuksia on edes pystytty nostamaan. Nopeuksien kasvaessa kuitenkin uusia ongelmia kuten 5 GHz:n taajuuden radion kuuluvuuden heikentyminen on noussut esille. Suurempien kaistanleveyksien käyttö johtaa päällekkäisyyksiin, ja 160 MHz:n kanava onkin vain kuluttajalle mahdollista, jos läheisyydessä ei ole paljoa liikennettä samalla taajuusalueella. Myöhemmin on myös huomattu, että reitittimien kyky kommunikoida useamman samaan verkkoon kytketyn laitteen kanssa samanaikaisesti ei ole ollut tehokasta, vaikka verkkoon liitetyt laitteet lähettäisivät ja vastaanottaisivat saman määrän dataa. Tähän on vuosien saatossa kehitelty ratkaisuja, sillä langattomille verkoille on tärkeää pystyä käsitellä montaa laitetta samanaikaisesti. (Weinberg. N, 2018)

802.11ax, joka kuluttajaystävällisemmin tunnetaan Wi-Fi 6:na on vuonna 2019 julkaistu uusin 802.11-standardi. Kuten aiempiin standardien kehitykseen verraten, 802.11ax on tuonut myös parempaa datansiirtonopeutta eri taajuusalueilla. Kuitenkin 802.11ax tarjoaa paljon muutakin. Parempi suorituskyky etenkin, kun laitteita on useita samassa verkossa, parempi verkon tehokkuus sekä liitettyjen laitteiden virran kulutus pienentyy tämän standardin myötä. Kun puhutaan verkon suorituskyvystä, 802.11ax hyödyntää standarditoimintona 10-bittinen 1024-QAM-modulointia, joka on ollut aiemmissa standardeissa vain kokeellisena toimintona. Tämä tarkoittaa noin 25 %:n tiedon siirron nopeuden kasvua aiempaan 8-bittisen 256-QAM-modulointiin verrattuna. (Weinberg. N, 2018)

2.4.5. MIMO ja MU-MIMO

MIMO (Multiple-Input and Multiple-Output) on tietoliikennetekniikka, jossa tiedon lähetykseen ja vastaanottoon käytetään useaa antennia samanaikaisesti. Nykyään MIMO:a käytetään datan siirtoa samalta radiokanavalta välittyen. Radiotekniikassa on otettava huomioon radiosignaalien vaimentuminen sekä kohina-signaalisuhde, joka aiheuttaa paljon virheitä signaalissa. MIMO-tekniikalla voidaan luoda vaihtelevuutta signaalin sijaintiin. Vaikka kommunikoivat laitteet sijaitsevat samassa fyysisessä tilassa, signaalit kulkevat eri reittejä pitkin, näin ollen vähentäen todennäköisyyttä sille, että kaikki signaalit häiriintyisivät, taaten luotettavamman tiedonsiirron. (Stobing. C, 2017)

Luotettavuus ei ole kuitenkaan ainoa hyöty MIMO-tekniikasta, vaan sitä hyödynnetään myös parannettaessa tiedonsiirtojen nopeuksia. Lähettäjän ja vastaanottajan antennit erotellaan yksilöllisiksi pareiksi ja lähetettävä signaali jaotellaan jokaiselle antennille sellaisenaan. Antennit havaitsevat saapuvan signaalin olevan sama kaikille vastaanottaville antenneille. Näin ollen tiedonsiirron nopeus kasvaa, kun saman signaalin käsitteleviä antenneja on useampi. Edellytyksenä tälle menetelmälle on, että lähettäviä sekä vastaanottavia antenneja on sama määrä. Kuvassa 3 esitetään tukiaseman ja käyttäjän tiedonvälitystä MIMO:n avulla. (Stobing. C, 2017)



Kuva 3. MIMO-tekniikka. (Capano. D, 2014)

MIMO-tekniikassa ongelmaksi ilmenee yleisimmin monen käyttäjän samanaikainen yhdistäminen. Jos monta käyttäjää yrittää samanaikaisesti yhdistää itsensä verkkoon, ensimmäiseksi yhdistyspyynnön saanut käsitellään ensin ja muut joutuvat odottamaan ennen kuin saavat itse muodostettua yhteyden. MU-MIMO (Multi-user Multiple-Input and Multiple-Output) on jatkumo MIMO-edeltäjälleen, jossa useampi laitteeseen yhdistyspyyntöä muodostava laite voidaan käsitellä samanaikaisesti perustuen yhden antennin kykyyn käsitellä sekä vastaanottava että lähettävä signaali. Verkkolaitteeseen samanaikaisesti yhdistettävien laitteiden määrä määräytyy verkkolaitteeseen asennettujen antennien määrästä. MU-MIMO-tekniikka tuo myös kaistanleveyttä jokaista käyttäjää kohti ja samalla jakaa sen tasaisemmin jokaiselle samassa verkkolaitteessa yhdistyneenä olevien päätelaitteiden kanssa. (Stobing. C, 2017)

2.5 **Tietoturvallisuus**

Tietoturvalla tarkoitetaan tiedon saatavuuden, luottamuksellisuuden sekä eheyden ylläpitämistä. Myös pääsynvalvonta, saatavuus sekä tarkastettavuus nousevat esille tietoturvasta puhuttaessa. Turvattava tieto voi olla eri muodoissa kuten internetissä olevat tiedostot, fyysiset laitteet tai ihan pelkästään ihmisten tietämys. Tietoturvalla pyritään suojaamaan esimerkiksi yritykselle tai yksityiselle henkilölle tärkeät tiedostot. Luottamuksellisuus on iso osa tietoturvallisuutta, sillä esimerkiksi yrityksien tulee oikeuttaa pääsy tiedostoihinsa vain niille henkilöille, jotka voivat niitä käyttää. Etenkin tietoverkoista puhuttaessa tietoturvallisuus nousee jatkuvasti esille sillä useimmat tietoturvallisuusriskit liittyvät verkkoyhteyden turvattomaan käyttöön tai huonosti toteutettuun tietoturvaan. Näille altistuneimpia voivat olla esimerkiksi luottokorttien tiedot, käyttäjätunnukset ja salasanat tai luottamukselliset tiedostot. Näihin on kuitenkin kehitelty pysyviä teknisiä, hallinnollisia sekä fyysisiä ratkaisuja, jotka kehittyvät jatkuvasti, jotta tietotekniikan käyttäminen olisi turvallista ja huoletonta.

2.5.1 Palomuurit

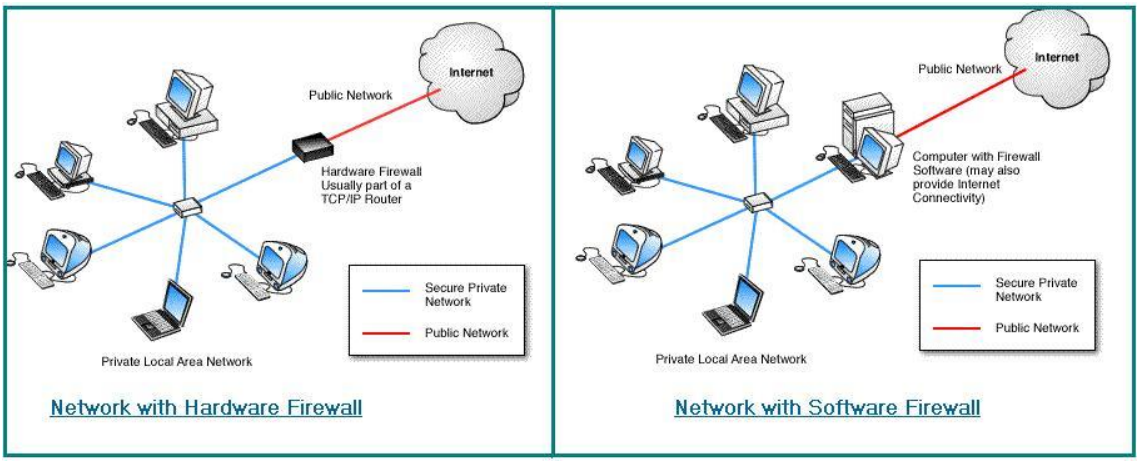
Palomuuri (Firewall) on teknillinen tietoturvaratkaisu, jolla voidaan valvoa saapuvaa ja lähtevää liikennettä. Kuluttajille ja yrityksille on saatavilla ohjelmapohjaisia sekä laitepohjaisia ratkaisuja. Palomuurit sisältävät tavallisesti reitittimen ja Proxy-palvelimen. Proxy palvelin huolehtii käyttäjän tunnistautumisesta, kirjaa tapahtuvan liikenteen ja toimii sovelluskerroksen protokollien yhteyksien monitoroijana. Reititin kanavoi saapuvia IP (Internet Protocol) -paketteja ja analysoi niiden lähtöpaikkaa sekä määränpäätä. Kuva 4 selittää, kuinka ohjelmapohjainen ja laitepohjainen palomuuri toimii verkossa. (Internetopas, n.d)

Laitepohjaiset palomuurit ovat yrityskäyttöön suositeltuja, sillä ne kattavat kaikille samassa verkossa oleville laitteille tietoturvan. Ne toimivat itsenäisinä laitteina sillä ne eivät ole sijoitettuja itsessään päätelaitteisiin. Näin ollen myös ne ovat vähemmän alttiita hyökkäyksille ja niissä on parempi turvallisuushallinnointi kuin ohjelmapohjaisessa palomuurissa. (Internetopas, n.d)

Ohjelmapohjaiset palomuurit ovat kuluttajien keskuudessa yleisin ratkaisu. Nämä suojaavat kodin päätelaitetta, johon palomuuriohjelma on asennettu. Käyttäjä saa itse määritellä haluamansa asetukset ohjelmalle näin ollen vastuun ollessa enemmän kuluttajan käsissä. Palomuuriohjelma suojaa käyttäjän päätelaitteita mm. viruksilta, madoilta sekä keyloggereilta. Ohjelmapohjaiset palomuurit voidaan jaotella vielä kahteen aliryhmään: Sääntöpohjaisiin sekä käytäntöpohjaisiin. Sääntöpohjaiset palomuurit ovat koodattuja tekstipätkiä, joilla asetetaan palomuurille säännöt, millaisista kohteista saapuva ja lähtevä yhteys sallitaan. Nämä säännöt toimivat ilman poikkeuksia tarkoittaen, että palomuuri toimii juuri niin kuin säännöt ovat kirjoitettu sille. Käytäntöpohjaisen palomuurin erona

sääntöpohjaiseen on, että käyttäjä voi luoda palomuurille ehtoja, joiden mukaan palomuuri toimii. Esimerkiksi palomuuri voidaan laittaa tarkastelemaan tietystä IP-osoitteesta saapuvaa yhteyttä. (Internetopas, n.d)

Palomuurien heikkoutena on, että ne pystyvät suodattamaan vain niiden lävitse kulkevaa yhteyttä. Esimerkiksi langattoman lähiverkon tukiaseman kautta voitaisiin ottaa yhteys verkkoon, ellei tukiasemaan itsessään ole konfiguroitu tarvittavia asetuksia. Kehittyneemmillä palomuureilla on ominaisuus pystyä rajaamaan spesifioituja yhteyksiä sekä myöntämään tai eväämään pääsy haluttuihin palveluihin. Esimerkiksi samasta IP-osoitteesta saapuvat hyökkäysyritykset voidaan estää laatimalla palomuurille sääntö, joka estää kaiken liikenteen kyseisestä IP-osoitteesta. (Internetopas, n.d)



Kuva 4. Laitepohjainen sekä ohjelmapohjainen palomuuri. (Hardware Texpert, 2011)

2.5.2 Langattomien verkkojen salausmenetelmiä

Langattomien lähiverkkojen tietoturvallisuuden suurin vastuu on pystyä eväämään luvaton pääsy verkkoon. Tähän hyödynnetään nykyään langatonta yhteyttä hyödyntävien reitittimien sisäänrakennettuja salausmenetelmiä. Ensimmäisenä tukiaseman ja käyttäjän välistä liikennettä suojaavana ratkaisuna on kehitelty WEP (Wired Equivalent Privacy), joka on alun perin hyödyntänyt 40-bittistä salausavainta, josta on tehty myöhemmin 64- ja 128-bittiset versiot 802.11 standardien kehityttyä. WEP hyödyntää RC4- (Ron's Code 4)algoritmilla luotua salausavainta (Shared key), jota käytetään verkkoon yhdistämiseksi. Päätelaite lähettää tunnistautumispyynnön reitittävälle laitteelle, joka on yleisimmin tukiasema. Tukiasema vastaa tähän pyyntöön, jonka jälkeen päätelaite lähettää algoritmilla suojatun viestin. Tämän jälkeen tukiasema vertaa lähettämäänsä pyyntöä käyttäjän lähettämään suojattuun viestiin. Jos viestit vastaavat toisiaan, muodostaa tukiasema käyttäjälle yhteyden verkkoon. WEP:n RC4-algoritmissa on kuitenkin havaittu puutteita, jotka

ovat riskialttiita jos tietoliikennettä kuunneltaisiin. Tämän vuoksi WEP:n rinnalle on kehitelty vuosien saatossa parempia salausmenetelmiä. (Johnson. A, 2020)

WPA (Wi-Fi Protected Access) on salausmenetelmä, joka luotiin lisäämään tietoturvallisuutta langattomille yhteyksille. WPA hyödyntää samaa RC4-algoritmia kuin edeltäjänsä WEP, parannelluin muutoksin. Käyttäjät voidaan esimerkiksi tunnistamaan yksilöllisesti, sekä jokaiselle käyttäjälle voidaan luoda eri avaimet jotta tunnistautumisprosessi olisi turvallisempaa. WPA:sta on yksityiskäyttöön olevat WPA-Personal sekä yrityskäyttöön enemmän painottuva vaihtoehto WPA-Enterprise. WPA-Personal toimii manuaalisesti luoden salausavain jokaiselle käyttäjälle. WPA-Enterprise luo jokaiselle käyttäjälle oman PMK-avaimen (Pair-wice Master Key) erikseen. Kun käyttäjä yrittää yhdistää itseään verkkoon tukiasema kysyy palvelimelta, onko käyttäjä indentifioitu käyttäjä. Riippuen onko käyttäjän avain palvelimen tietokannoissa, tukiasema joko estää tai hyväksyy käyttäjän kirjautumisen. (Johnson. A, 2020)

WPA-salaukselle on myös kehitetty paranneltu WPA2-versio (W-Fi Protected Access 2). WPA2:n suurin ero WPA:han verrattuna on CCMP:n (Counter Mode with Cipher-Block Chaining Message Authentication Protocol) hyödyntäminen käyttäjän yhdistämisessä verkkoon. CCMP on turvallisempi ratkaisu RC4:n sijasta. WPA2:lla on myös WPA2-Personal sekä WPA2-Enterprise versiot. WPA2-Personal luo PMK:n sille asetetun verkkotunnuksen (Service Set Identifier) sekä PSK:n (Pre-Shared Key) avulla. Kaikille käyttäjille PMK on sama, jolloin kaikki avaimen tietävät voivat yhdistyä verkkoon. Yhdistyessä verkkoon järjestelmä luo käyttäjän ja tukiaseman välille PTK:n (Pairwise Transien Key), joka auttaa tiedon salaamisessa. WPA2-Enterprise ottaa edeltäjänsä tavoin kirjautumispyynnön käyttäjältä, tarkistaa palvelimelta löytyykö käyttäjän PMK:n tiedot kannasta ja yhdistää tai evää käyttäjän pääsyn verkkoon. Tämän jälkeen käyttäjä ja tukiasema luovat PTK:n välillensä tiedon salaamista varten. (Johnson. A, 2020)

WPA2 on ollut jo 16 vuotta tietoturvaratkaisumallina langattomille lähiverkoille, mikä on pitkä ikä mille tahansa tietotekniikan maailmassa, jossa laitteiden suorituskyky kasvaa kokoajan eksponentiaalisesti. Vuonna 2018 alettiin nostamaan esille WPA2:n heikkouksia ja tapoja murtaa se. WPA2:n heikkoudet liittyvät siirrettävään salasanaan yhteyttä muodostaessa, jonka kryptauksen tarkistussumma voidaan laskea etukäteen. Tämä mahdollistaa, että asettamasi selväkielisen salasanan tarkistussumma saattaa löytyä jo kirjastoista, joita hakkerit hyödyntävät murtautuakseen verkkoihin. WPA3 on vuonna 2018 Wi-Fi Alliancen julkaisema uusin salausmalli. WPA3 eroaa edeltäjästään siinä, että salasanan tarkistussummaa ei siirretä vaan WPA3 käyttää SAE (Simultaneous Authentication of Equals) -menetelmää, joka perustuu Diffie-Hellman-salausprotokollan avulla vaihdettuihin avaimiin kahden käyttäjän väliseen viestin salaamiseksi. Tämän avulla kolmas osapuoli ei voi

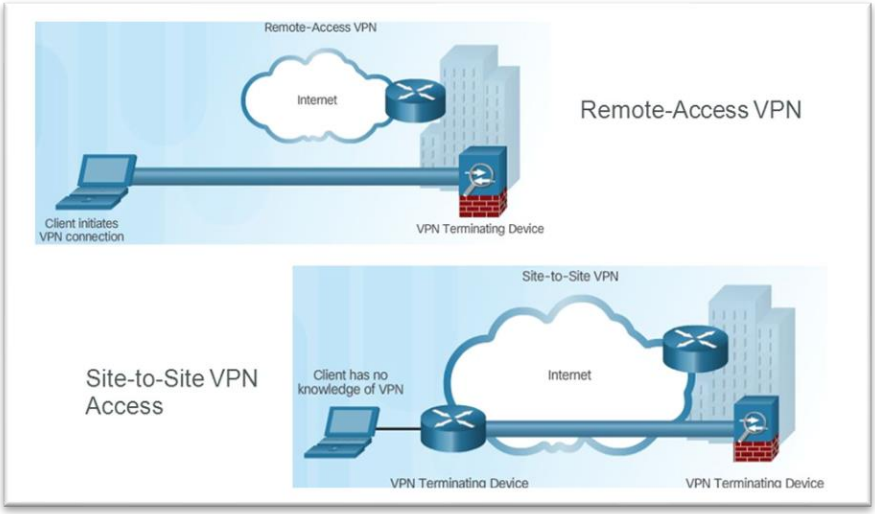
saada selville salattuja viestejä. WPA3 omaa myös Forward Secrecy-toiminnon, jonka avulla vanhat tallenteet ovat turvassa vaikka salausavain paljastuisi. Monet julkiset verkot ovat salaamattomia, vaan vaativat käyttäjältä Splash-sivustokirjautumisen verkkoon yhdistettäessä. Tämä mahdollistaa verkon helpon salakuuntelun. WPA3:n Enhanced Open tarjoaa ratkaisuna julkisille verkoille automaattisen salauksen, jolloin kaikki laitteet yhdistyvät verkkoon suojatulla yhteydellä. (Metis, 2018)

2.5.3 VPN

VPN (Virtual Private Network) on tiedonsiirrossa käytetty turvallisempi menetelmä. Tiedonsiirtoa varten rakennutetaan niin sanottu VPN-tunnelointi, jossa tieto kapseloidaan, minkä jälkeen se voidaan reitittää eteenpäin. Tämän jälkeen lähetetty tieto kryptataan käyttäen yhdessä tunnelointiprotokollia ja salausprotokollia. Esimeriksi L2TP (Layer 2 Tunnel Protocol) tarjoaa verkon tunneloinnin ja etäyhteyden muodostamisen, ja IPsec (IP Security Architechture) tarjoaa tälle yhteydelle suojauksen, joka hyödyntää AES (Advanced Encryption Standard**)** -256-bittistä enkryptausta. Lisäksi VPN-tunnelointi maskeeraa lähettäjän sekä vastaanottajan IP-osoitteet, näin ollen antaa käyttäjälle vielä enemmän tietosuojaa menetelmää käytettäessä. VPN mahdollistaa käyttäjän etäyhteyden erilliseen verkkoon tarkoittaen, että vaikka käyttäjä ei itse fyysisesti olisi lähiverkon alueella, voi hän silti päästä etäyhteyden avulla käsiksi verkkoon, sekä mahdollisiin erillisillä palvelimilla sijaitseviin tiedostoihin. (E-tutes, 2019)

Etäyhteys (Remote Access VPN) on VPN-verkko, joka voidaan implementoida yritys- tai kotiverkkoon. Yrityksen lähiverkkoon on rakennutettu VPN-palvelin, jossa sijaitsevat tunnukset käyttäjille. Etäyhteyden ottaminen kodista tai esimerkiksi työmatkalla ollessa on mahdollista. (E-tutes, 2019)

Site-to-Site VPN on kaikkein suosituin yrityskäytössä oleva VPN-ratkaisu. Etenkin isojen yritysten, joilla on monia toimipisteitä ympäri maailmaa, on helpompi rakennuttaa Site-to-Site VPN, jolla he mahdollistavat toimipisteiden välisen VPN-yhteyden, jolloin toimipisteet voivat salata kaiken yhteyden keskenään. Tästä käytetään yleisesti nimitystä Intranet VPN. Tämä VPN-menetelmä on hyvä myös sekä verkon skaalautuvuuden että laajaverkon (WAN) kaistanleveyden kuormituksen puolesta. Kuvassa 5 on hahmoteltuina yleisimmät VPN-ratkaisut. (Cisco, n.d.)



Kuva 5. VPN-ratkaisuja. (Cisco, n.d.)

Hallittaessa VPN-verkkoa on tärkeää huomioida sen turvallisuus sekä eheys. Kenellä on pääsy verkkoon, kuka sitä ylläpitää eli kuka hallinnoi ja valvoo. Pääsynvalvonnalla tarkoitetaan IP-osoitteiden valvontaa, jossa tarkastellaan mistä lähteestä yhteys tulee. Tällä myös saadaan tarkasteltua tiedonsiirron aikana lähetettyjen pakettien sisältöä. Salauksien lisäksi tulee määritellä, mihin kaikkeen käyttäjillä on pääsy VPN-yhteyden yli ja mitä resursseja voidaan käyttää. VPN-yhteyden ei ole pelkästään tarkoitus lisätä turvallisuutta verkkoyhteyksille, vaan myös lisätä niiden kustannustehokkuutta. (Cisco, n.d.)

3 PILVIPALVELUT

Pilvipalvelulla tarkoitetaan esimerkiksi sovelluksia, tietokantoja sekä kapasiteettipalveluja, jotka eivät sijaitse omalla päätelaitteella tai yrityksen palvelimilla. Nämä palvelut ovat palveluntarjoajan omissa konesaleissa sijaitsevia palvelimia, joista tiedot kulkeutuvat asiakkaiden käytettäviksi. Näistä palveluista hyvänä esimerkkinä on julkinen sähköposti. Kaikki pilvessä olevat palvelut ovat saatavilla riippumatta käyttäjän sijainnista ja päätelaitteesta. Yritysten näkökulmasta, jotka hyödyntävät pilvipalveluita eivät säästä vain pelkkää kapasiteettia ulkoistamalla tiedostonsa vaan lisäävät kustannustehokkuutta, näin ollen yrityksen ei tarvitse esimerkiksi itse rakennuttaa konesalia tiedostopalvelimille eikä hankkia työntekijöitä vastaamaan konesalin ylläpidosta. Myöskään käyttäjien ei tarvitsisi lähteä itse asentelemaan omille työasemillensa ohjelmistoja ja sovelluksia, kun kaikki löytyisi pilvipalvelimilta. Yrityksen sisäiset konesalit ovat muutenkin herkempiä tietoturvahyökkäysten kohteita. Konesaleissa sijaitsevat pilvipalvelimet ovat salattuja ja niiden sisältämiin tiedostoihin pääsee käsiksi vain salausavaimella, jotka ovat palveluntarjoajan hallinnassa.

Palveluntarjoajilla on suuri vastuu yritysten tietoturvasta ja ylläpidosta. Esimerkiksi jos konesalien palvelimille tulee ongelmia, voi palveluntarjoaja esimerkiksi siirtää palvelimilla olevat palvelut tilapäisesti toiselle palvelimelle, taaten asiakkaille esteettömän pääsyn pilvipalveluihin. (Lavanko, 2018)

3.1 Historia

Pilvilaskenta eli Cloud Computing on käsitteenä vakiintunut vuosien saatossa, mutta pilvipalveluita on ollut saatavilla jo huomattavasti pidempään. Ensimmäiset testailut tehtiin osituskäytöllä (time-sharing), jonka avulla useat käyttäjät pystyivät olemaan yhteydessä yhteen tietokoneeseen. Tämä mahdollisti sen, että siinä missä yksittäinen henkilö työskentelee tietokoneella tehottomasti, ryhmä saman tietokoneen käyttäjiä tekisi saman työn moninkertaisesti tehokkaammin. Palvelua alettiin myymään yrityksille sen suosion kasvaessa räjähdysmäisesti. Myöhemmin, kun paikallisoperaattorit alkoivat myymään yrityksille VPN-palveluita, vakiintui tämän ohella pilvisymboli määrittelemään rajapinnan, mistä palveluntarjoaja ja asiakas olivat vastuussa. Pilvilaskenta tulisi pian kattaa ulkoistettuja palvelimia sekä tietoverkkojen infrastruktuurin. (Wikipedia, 2020)

Vuonna 2006 Amazon kehitti AWS:n (Amazon Web Service), joka tarjosi yrityksille ja kuluttajille virtuaalikoneita, jotka pyörittäisivät heidän sovelluksiaan, näin ollen vähentäen yrityksen omaa kapasiteettia. Palvelusta kasvoi suurin pilvipalveluiden tarjoaja yrityksille sekä kuluttajille. Nopeasti muut seurasivat Amazonia ja julkaisivat omia pilvilaskentojaan. Näistä tunnetuimmat tähän päivään asti ovat Google App Engine, sekä Microsoft Azure. (Wikipedia, 2020)

3.2 Haasteet

Pilvipalveluiden skaalautuvuus ja saatavat resurssit ovat nykyiseltään jo niin konkreettisia piirteitä, että pilvipalveluntarjoajan datan sijoittuvuus on noussut suuremmaksi kysymykseksi. Monet suomalaiset palveluntarjoajat eivät omista konesaleja Suomessa, ja vaikka omistaisivat, datan sijoittuvuus on rajoitetumpaa kuin ennen. GDPR (General Data Protection Regulation) on Euroopan Unionin keväällä 2018 asettama yleinen tietosuoja-asetus, jonka tarkoituksena on säädellä henkilötietojen käsittelyä EU-maissa. Tämä asetus vaikuttaa myös datan suojaamiseen, sekä hallittavuuteen. Esimerkiksi kaikkien Euroopan alueella tuotettujen pilvipalveluiden tulee sijaita samassa maanosassa kuin missä heidän asiakkaansa ovat. Tietosuojan perustuessa lakiin tarkoittaa tämä pilvilaskennoille ja heiltä palveluita ostaville yrityksille sitä, että määritellyn datan ulkoistaminen palveluksi sekä sen sijoittaminen palvelimille tulee olla täysin luottamuksellista. Aina kun jaetaan tai siirretään haluttua dataa pilvessä, on tietovuodon riski mahdollinen. Koska palveluntarjoajat voivat halutessaan siirtää yrityksen datan toiselle palvelimelle, voi datan saatavuudelle tulla ongelmia, kun

palvelimet sijaitsevatkin alueella, jossa on tietoliikennehäiriöitä. (Kauppi. J, 2019)

Pilvipalvelut ovat tietoturvan kannalta nostattaneet keskusteluja palveluntarjoajan ja asiakkaan vastuualueista. Kuitenkin palveluntarjoajillakin on toisiinsa nähden vaihtelevia määritelmiä tietoturvavastuulle ja yritys ei ole aina tietoinen, kuinka paljon heidän itse tulisi kiinnittää huomiota tietoturvaan. Yrityksien tulisi aina pilvipalveluita harkitessa huomioida tietoturvaan liittyvät haavoittuvuudet ja uhat. Se, että vastuu yrityksen datan saatavuudesta ulkoistetaan tuo mukanaan saatavuus- sekä luotettavuusongelmat, joiden vuoksi yrityksen liiketoiminta saattaa kärsiä. (Lundberg. J, 2018)

3.3 Arkkitehtuuri

Pilvipalvelut ovat lisääntyneet kovaa vauhtia yrityksissä ja kuluttajien keskuudessa. Pilvipalvelut on jaoteltu neljään eri kategoriaan lisäämään käyttäjille käsitystä siitä, minkälainen pilvitekniikka tukee heidän tarpeitaan parhaiten. Kuvassa 6 on esiteltyinä kolme käytetyintä pilvipalvelua.

3.3.1 Julkinen pilvipalvelu

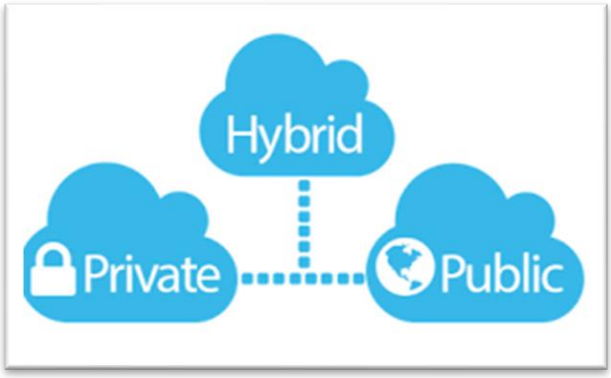
Nimensä mukaisesti julkisen pilvipalvelun tarjoamat palvelut ja resurssit myydään julkiseen verkkoon. Tämä on valintana käyttäjille, kun he haluavat testata ja kehittää esimerkiksi ohjelmistokoodia tai omia sovelluksia. Lisäksi prosessoitavien sovelluksien suorituskyvyn lisääminen sekä kustannustehokkuus on julkista pilvipalvelua käyttävälle usein tarpeena. Tämä onnistuu julkisen pilvipalvelun avulla koska käyttäjä maksaa vain käytetyistä resursseista. Julkisen pilvipalvelun etuihin kuuluu myös mahdollisuus maailmanlaajuiseen toimivuuteen tarkoittaen, että palvelut toimivat maailmanlaajuisesti, vaikka palveluntarjoaja toimisi itsessään eri mantereella. Julkisten pilvipalveluiden tarjoajista tunnetuimpia ovat Amazon, Google sekä Microsoft. (Netapp, 2020)

3.3.2 Yksityinen pilvipalvelu

Yksityisellä pilvipalvelulla taataan käyttäjälle turvallisuutta sekä hallittavuutta. Palvelu edellyttää käyttäjältä, että tämä ylläpitää itse omaa datakeskusta, josta se jakaa palvelua yritykselleen, sekä ostaa palveluntarjoajalta ohjelmistoja oman infrastruktuurin tueksi. Yksityisiä pilvipalveluita suositaan yleisimmin isojen yritysten keskuudessa, joissa sekä tietoturva että tietosuoja ovat tärkeitä arvoja yritykselle. Lisäksi yrityksen tulee pystyä hyödyntämään tehokkaasti omaa datakeskustansa. Tämän pilvipalvelumallin hyötyihin kuuluu myös eheä kokonaisuus, joka tarjoaa nopean pääsyn dataan sen sijaitessa yrityksen omissa tiloissa. Lisäksi yritykselle kustannustehokkuus nousee jalustalle siinä vaiheessa, kun puhutaan suurista, staattisista työkuormista. (Netapp, 2020)

3.3.3 Hybridipilvi

Vaikka yksityistä pilvipalvelua käytettäisiin kontrolloidusti, se ei takaa, etteivät yhteydet ruuhkaantuisi. Tähän ratkaisumallina on mahdollistettu, että yritys voi siirtää pilvitoimintojaan julkiseen pilveen tarvittaessa. Tämän ansiosta yritys hyötyy sekä yksityisen pilvipalvelun että julkisen pilvipalvelun tuomista eduista. Hybridipilvi on joustava ratkaisu yrityksille, jotka hakevat nopeita muutoksia yrityksessään. (Netapp, 2020)



Kuva 6. Yleisimmät pilvipalveluarkkitehtuurit. (MiCore solutions, 2016)

3.3.4 Multicloud

Multicloud on sekoitus yksityistä ja julkista pilvipalvelua. Multicloudin sijoittuminen julkiseen sekä yksityiseen verkkoon takaa monipuolisen saatavuuden palveluille mutta samanaikaisesti monimutkaistaen koko infrastruktuuria. Lisäksi on huomioitavaa palveluiden ollessa eri palvelimilla, nousee kustannukset tietoliikenteen sekä palvelinkäyttömaksujen myötä. Pilvipalvelun hajaannuttaminen kuitenkin pienentää riskiä tilanteissa, joissa pilvipalveluun liittyvät ongelmat eivät vaikuta koko yrityksen mittakaavassa. Suurimmat haasteet multicloud tuo, kun kysytään asiantuntevuutta pilviympäristön hallinnassa. Lisäksi yrityksen halu käyttää resursseja pysyäkseen pilvipalveluiden kehityksessä mukana. (Lavanko. H, 2018)

3.4 Pilvipalvelumallit

Pilvipalvelumalleista käytetään usein nimitystä XaaS (Anything as a Service), joka viittaa kaikkiin palveluihin, joita käyttäjä voi ostaa pilvipalveluiden tarjoajilta. XaaS koostuu kolmesta pääsääntöisestä palvelumallista, joiden tarjoamat palvelut on esiteltyinä kuvassa 7:

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

3.4.1 IaaS

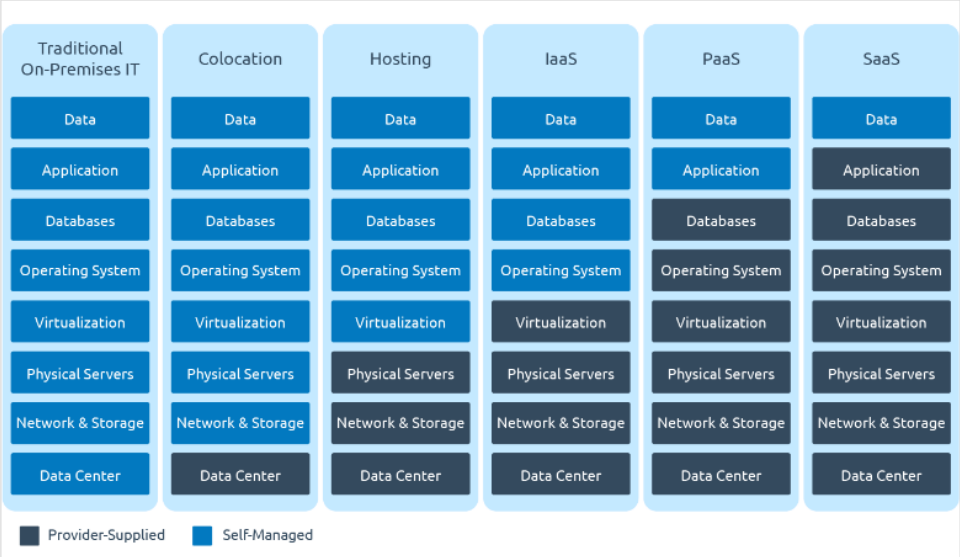
Nimi itsessään jo viittaa palvelimien ja konesalien ulkoistamiseen palveluna. Asiakas ostaa palveluntarjoajalta infrastruktuurin, kattaen serverit, reitittimet, tallennustilaa sekä laskentakapasiteettia. Yrityksen omalla vastuulla ovat palomuurit, tietoturva, sekä itse käyttöjärjestelmän, sovelluksien että ohjelmistojen luonti ja näiden säilyttäminen tietokannoissa. IaaS sopii parhaiten yritykselle, joka ei halua investoida omiin laitteisiin mutta haluavat omat ohjelmistot. Suurimpiin palveluntarjoajiin kuuluu mm. Amazon Web Services, Google Compute Engine ja IBM SmartCloud Enterprise. (Uusitalo. T, 2018)

3.4.2 PaaS

PaaS on enimmäkseen suunnattu käyttäjille, joilla on ohjelmistokehityksestä kokemusta. IaaS-palvelumallin tarjontaan käyttäjä saa lisäksi myös käyttöjärjestelmän. Käyttäjän ei tarvitse huolehtia itse ohjelmistojen skaalautuvuudesta tai näiden tehontarpeesta käyttäjämäärien kasvaessa, koska itse alusta on laajennettavissa käyttötarpeen mukaan. Palveluntarjoaja yleisimmin tarjoaa Web-käyttöliittymän sovellusalustoja ohjelmistokehityksen tarpeisiin. PaaS-palvelumallissa käyttäjän vastuulle jää omien sovelluksien lisäksi näiden tietoturva sekä julkaisujärjestelmän päivittäminen. (Uusitalo. T, 2018)

3.4.4 SaaS

Yleisin palvelumalli, jossa asiakkaan vastuulle ei jää mitään vaan koko ohjelmisto tulee omana palvelunaan. Yrityksille tämä on helpoin valinta, sillä näitä ohjelmistoja käytetään yleisimmin Internet-selaimen avulla ja ovatkin siksi helppokäyttöisiä. Palveluntuottaja vastaa kaikesta hallinnollisuudesta, jättäen käyttäjälle vain maksun ylläpidosta. Tehden SaaS-mallista kustannustehokkaimman palvelumallin. Esimerkkinä SaaS-palvelumallista voidaan nostaa esille yritysten asiakkuudenhallinta- sekä toiminnanohjausjärjestelmät. (Uusitalo. T, 2018)



Kuva 7. Pilvipalvelumallien tarjonnan visualisointi. (Varshney . V, 2020)

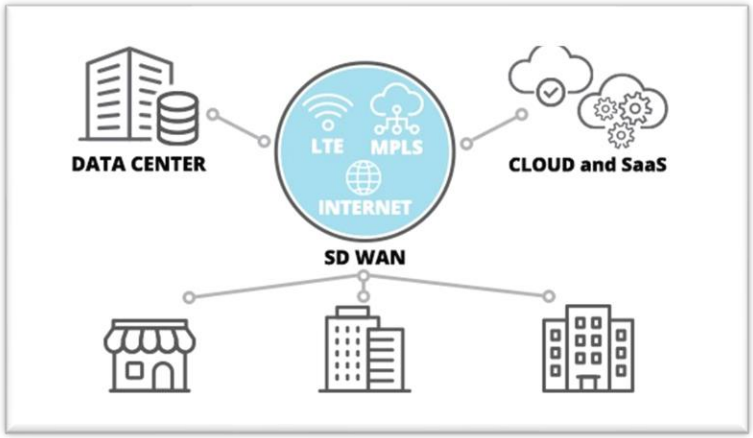
3.5 Tietoverkot pilvessä

Digitaalisen murroksen, globaalien trendien- mm. etätyö, tekoäly, kaupungistuminen ja kuluttajistuminen asettavat tietoverkkojen infrastruktuurille uusia haasteita. Päivittäin siirrettävä datan määrä on kasvanut räjähdysmäisesti ja siksi tietoverkkojen tulee pystyä palvelemaan käyttäjiään yhä nopeammin, joustavammin, skaalautuvammin, turvallisemmin sekä kustannustehokkaammin. Tämän päivän yritykset ovat niin riippuvaisia tietotekniikasta, että niiden yritystoiminta salpaantuu, jos niiden perustana oleva tietoliikenne lakkaisi. Nykyään palveluita voidaan ulkoistaa omien konesalien lisäksi myös julkisissa pilvipalveluissa niiden tarjoamien pilvipalvelumallien kautta. Tietoturvan merkitys korostuu osana älykkäämpiä tietoverkkoja, jotka hyödyntävät analytiikkaa ja automaatiota. Pilvipalveluiden yleistyminen tietoverkoissa ei ole suoraan linkitettynä internettiin vaan pikemminkin pohjautuu fyysisen laitteiston ja infrastruktuurin siirtämisestä pilveen. (Elisa Oyj, n.d.)

Tietoverkkojen pilveen siirtäminen toimii samoin tavoin kuin pilvipalvelut. Resurssit tarjotaan käyttäjille erilaisina palveluina tarkoituksen mukaisesti parantaa kustannustehokkuutta, skaalautuvuutta sekä käyttöastetta niin palveluntarjoajan kuin käyttäjän osalta. Nämä ns. pilviverkot voivat nykyiseltään sisällyttää verkon hallinnollisia osia, tarkoittaen että fyysisen laitteiston määrä niin palveluntarjoajalla kuin käyttäjällä vähenee. Palveluntarjoajan näkökulmasta kustannustehokkuus pilviverkoissa painottuu siinä vaiheessa, kun aletaan vertailemaan esimerkiksi massatapahtumiin rakennettavia langattomia verkkoja, joissa saattaa vierailla jopa kymmeniä tuhansia ihmisiä. Langattomien verkkojen skaalautuvuus ei ole koskaan kehittynyt tasolle, jossa verkon taajuudet eivät menisi tukkoon liian monen käyttäjän ollessa samassa verkossa yhdenaikaisesti. Näihin

massatapahtumiin rakennutettavat verkot tulee suunnitella tarkasti, jotta langattomat yhteydet toimisivat kaikilla vierailijoilla. (Elisa Oyj, n.d.)

SD-WAN on laajaverkolle kehitelty pilvipalvelumallia hyödyntävä verkkoteknologia, jolla yksinkertaistetaan laajaverkon hallinnointia ja kuluja. SD-WAN hyödyntää linkkiaggregaatiota, jolla laajaverkon toiminta tiivistetään yhden käyttöliittymän taakse. Näin ollen kaikki laajaverkossa olevat laitteet ovat keskitettyinä ja helpommin hallinnoitavissa (Kuva 8). SD-WAN tuo ominaisuutenaan markkinoille myös kuormituksen tasapainotuksen, jolla voidaan tasapainottaa laitteen linjojen välityksellä tapahtuvaa liikennöintiä yksittäisen linjan tukkiutumisen ehkäisemiseksi. SD-WAN omaa helpon käyttöönottotoiminnon ZTP:n (Zero Touch Provisioning), jolla tarkoitetaan laitteen automaattista konfigurointia, kun se liitetään verkkoon. Lisäksi SD-WAN-laitteisiin on integroituina palomuurit, VPN-hallinnointi sekä mobiiliyhteysmahdollisuudet vikasietoisuuden ja tietoturvan lisäämiseksi.



Kuva 8. SD-WAN havainnollistettuna. (Aruba, 2020)

4 CISCO MERAKI

Cisco Meraki on Cisco Systemsin yritykseen kuuluva osasto, joka tuottaa SaaS-pilvipalvelumallin tason ratkaisuja yrityksille. Yrityksen tarjontaan kuuluvat verkossa hallinnoitavat laitteet kuten langattomat tukiasemat, kytkimet ja tietoturvaratkaisut, jotka sisältävät reaaliaikaiset raportointi- ja seurantatyökalut hallinnoinnin helpottamista varten.

Cisco Merakin ja Cisco Systemsin tarjoamien ratkaisujen päällimmäisimpinä eroina ovat, että Meraki tarjoaa käyttölisenssiä omille laitteilleen, mutta pienentää käyttäjältä vaadittavaa osaamista sekä käyttöönotosta koituvia kustannuksia. Cisco Systemsin tarjontaan kuuluvat Cisco-on-premise-ratkaisumallit vaativat käyttäjän ostamaan itse laitteiston verkkonsa

tueksi. Näin säästytään käyttölisensseistä aiheutuvilta maksuilta mutta samanaikaisesti käyttäjä joutuu itse ylläpitämään verkkoaan, näin ollen työkustannukset kasvavat korkeammiksi kuin Merakin tarjoaman pilven kautta tapahtuvan hallinnoinnin myötä. Merakin tarjoama palvelumalli on hyvä ratkaisu käyttäjälle, joka ei halua investoida oman verkon hallinnoimiseen, ja maksaa ainoastaan lisenssin käytetyille laitteille, kun taas Cisco Systems on joustavampi ratkaisu käyttäjän halutessa itse olla vastuussa omasta lähiverkostaan ja maksaa sekä laitteistosta että asiantuntijuudesta. (Constine. J, 2020)

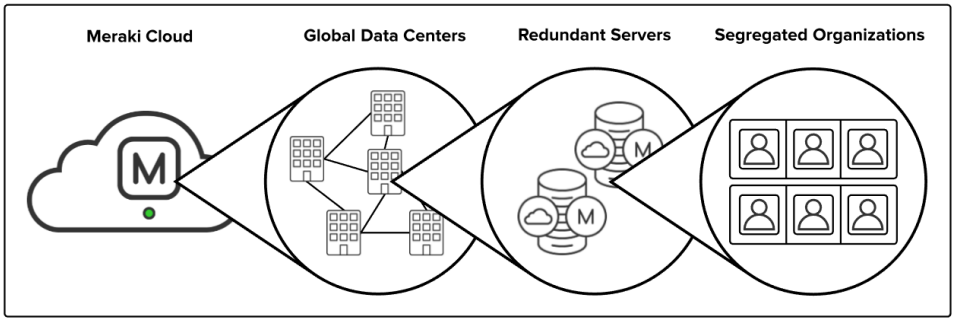
4.1 **Historia**

Meraki aloitti startup-yrityksenä, joka perustettiin vuonna 2006 Yhdysvaltain Kalifornian osavaltiossa Mountain Viewissä kolmen MIT:n opiskelijan toimesta. Yritys toimi MIT:n langattomia verkkoja kehittäneen kokeellisen mesh-verkkoprojektin parissa, jolla oli tarkoitus saada kytkettyä useampi kaupunki samaan verkkoon, jota voitaisiin tarkastella reaaliaikaisesti. Vuonna 2007 yritys muutti San Franciscoon ja aloittivat jakamaan yhdelle kaupunginosalle ”ilmaista internetyhteyttä”. He asensivat alueelle laajamittaisen verkon ja jakoivat alueen asukkaille toistimia. Puoli vuotta myöhemmin Merakin rakennuttamassa verkossa oli lähes 20000 käyttäjää ja tämän verkon läpi kulki lähes 5 terabittiä dataa. Vuotta myöhemmin käyttäjämäärä oli kasvanut jo sataantuhanteen ja Meraki päätti lakkauttaa kampanjansa. Cisco Systems osti Merakin vuonna 2012 tarkoituksen mukaisesti alkaa kehittämään pilvialustaa, jonka Meraki heille tarjosi. Tuohon aikaan Cisco kävi kamppailua langattomien verkkojen johtoasemasta Hewlett Packardin tytäryhtiötä Aruba Networkia vastaan. Merakin ostaminen varmisti Cisco Systemsille johtavan aseman langattomien verkkojen markkinoilla. (Constine. J, 2020)

4.2 **Arkkitehtuuri**

Cisco Merakin pilvipalvelimet sijaitsevat konesaleissa, joihin kaikki laitteet ovat suoraan yhteyksissä. Käyttäjien oma dataliikenne ei kuitenkaan kulje pilven kautta vaan suoraan vastaanottajalle. Pilvipalvelimien konesalit ovat kahdennettuja joka mantereella vikasietoisuuden takia, joihin kaikki muut konesalit ovat yhdistyneinä. Jos toiseen konesaliin tulee esimerkiksi ongelmia, voidaan yhteydet ohjata toisen konesalin palvelimien kautta. Kuvassa 9 on eriteltyinä kaikki Meraki-pilven arkkitehtuurin sisällyttämät tahot. Merakin laitteet käyttävät tapahtumapohjaista RPC (Remote Procedure Call) -järjestelmää, jonka avulla laitteet kommunikoivat käyttöliittymän kanssa. Merakin pilvipohjainen hallinta pyrkii korvaamaan langattoman verkon hallintalaitteet vaikkakin Merakin hallintajärjestelmän kautta langattomien tukiasemien konfigurointi on paljon rajoitetumpaa kuin perinteisemmän WLC:n kautta. Käyttöliittymä takaa korkean saatavuuden (High Availability) arkkitehtuurin, jonka ansiosta esimerkiksi vikatiloissa

palvelimet käyttävät varmuuskopiointia, jotta asiakkailla olisi esteetön pääsy palveluihin.



Kuva 9. Meraki-pilven arkkitehtuuri. (Meraki, 2020)

4.3 **Pilvihallinta**

Tietoverkkojen rakennutuksessa tärkeimpänä huomiona heti toimivuuden jälkeen voidaan nostaa esille verkon dokumentointi. Cisco Merakin laitteet ovat suunniteltuja pilvihallinnointia varten, ja sisältävät reaaliajassa toimivia ominaisuuksia kuten tapahtumaloki- ja seurantapalvelut, joiden avulla nähdään verkossa tapahtuva liikennöinti selkeämmin. Koska verkot toteutetaan pilvipohjaisina, on uuden verkon rakennuttaminen tai vanhan verkon päivittäminen nopeaa ja helppoa. Lisäksi nykyiset verkot ovat helposti laajennettavissa ja voivat kattaa tuhansiin osiin jaoteltuja verkkoja. Merakin hallintaliittymän avulla käyttäjä pystyy näkemään ja hallinnoimaan kaikkia langattomia sekä langallisia yhteyksiä hyödyntäviä laitteita. Käyttöliittymältä pilven välityksellä lähettäessä kyselyä laitteille datan keruuseen ja konfigurointiin liittyvissä tilanteissa toimii pilvipalvelin kyselyiden aloittajana tarkoittaen, että laitteiden ei tarvitse olla kytkettyinä vaan käsittelevät pyynnöt yhdistyttyään pilveen. Kaikki käsitellyt konfiguroinnit, jotka laitteisiin tehdään, varastoidaan ja varmuuskopioidaan Merakin omaan tietokantaan, joka päivittää itseään aina kun laitteisiin ajetaan konfigurointeja tai päivityksiä.

4.4 **Tuoteperhe**

Merakin tuotevalikoimista löytyy niin pienistä yrityksistä aina julkisen sektorin koko maan kattavien yritysten verkkojen rakennutukseen toteutettavia kustannustehokkaita sekä tietoturvallisia ratkaisuja, jotka huolehtivat myös käyttäjän yksityisyydestä ja turvallisuudesta. Tuotteita ovat mm. Langattomat MR-sarjan tukiasemat, MS-sarjan kytkimet, MX-palomuurit, WWAN-yhdyskäytäviä (Wireless Wide Area Network), sekä esineiden internetin (Internet of Things) tason ratkaisuja kuten langattomia, tallentavia videokameroita. Kaikissa tuotekategorioissa on huomioitu yrityksien eri tarpeet ominaisuuksille, joita Merakin tuotteet tarjoavat. Merakin

tuotteita päivitellään jatkuvasti lisäten laitteiden datan näkymistä ja parantaen myös vikatilanteissa toimimista. Lisäksi ne ovat hälytyssuojattuja eli jos esimerkiksi laite viedään sille määritellyn alueen ulkopuolelle, tekee se järjestelmälle hälytyksen. (Dustin Finland, n.d.)

4.5 **Tulevaisuus ja haasteet**

Vaikka Cisco Meraki tarjoaa laajan valikoiman myötä asiakkailleen verkkoratkaisumalleja, on huomioitavaa, että Cisco Meraki ei ole ainoa näitä palveluja tarjoava taho alalla. Kilpailu pilvipalveluiden tarjonnasta on lisääntynyt niiden tuomien etujen myötä ja monet suuret tietotekniikan alan yritykset ovat alkaneet valmistamaan omia pilvihallittavien verkkolaitteiden palveluita. Esimerkiksi Extreme Networks tarjoaa samanlaisia palveluja asiakkailleen.

Vaikka Merakin tuotteissa on panostettu vikasietoisuuteen sekä tietoturvaan, eivät ne ole täysin näiltä suojattuja kuten ei mikään julkista verkkoa käyttävä palvelu tai laite. Verkkoympäristöissä tapahtuvat haavoittuvuudet vaikuttavat myös Cisco Merakin laitteisiin. Kuitenkin pilvihallittavuudesta voidaan todeta olevan hyötynä myös nopea vianetsintä sekä haavoittuvuuksien nopea ehkäiseminen.

5 **LANGATTOMAN LÄHIVERKON SUUNNITTELU JA TOTEUTUS**

Yritysverkon suunnittelussa huomioitavina tekijöinä on nykytilanne eli millainen tämänhetkinen lähiverkko yrityksellä on, miten nykyinen lähiverkko on dokumentoitu ja millaista dataa verkossa kulkee. Kartoituksen jälkeen voidaan lähteä toteuttamaan uutta verkkoa ja millaisia muutoksia siihen halutaan tehdä. Yrityksen kannalta on myös tärkeää, että tietoturvallisuudesta, vikasietoisuudesta sekä palvelun esteettömyydestä huolehditaan verkkoa toteutettaessa. Palveluntarjoajan näkökulmaa ajatellen tulee huomioida, että uuden verkon dokumentointi on toteutettu niin, että sen hallinnointi ja ylläpito olisi kustannustehokasta. Verkon suunnittelun yhteydessä huomioidaan myös verkon skaalautuvuus yrityksen mukana eli jos yritys esimerkiksi tekee hankintoja, jotka lisäävät lähiverkon käyttöä, tulee nykyisen verkon olla joustava, jotta yrityksen ei tarvitse tehdä lisäinvestointeja lähiverkkonsa suhteen.

5.1 **Nykytilanne**

Tanreco Oy:n nykyinen sisäverkko on rakennutettu VDSL (Very high-speed Digital Subsciber Line) -tekniikalla, sillä yrityksen kiinteistöön tulee puhelinkaapelointi. Yrityksen verkkoa on muutaman kerran päivitetty kaistanleveyden vuoksi, mutta nyt yritykseen halutaan pidempiaikaisempi ratkaisu, joka skaalautuisi yrityksen tarpeiden mukaan tulevaisuudessakin.

Yrityksellä on teletila, jonne yritykseen aluejakamolta johdettu verkko tulee. Teletilasta löytyy myös ristikytkentäpaneeli, joita pitkin verkko johdetaan työpisteille (Kuva 10). Yleiskaapelointina yrityksessä on käytetty EN 50173-standardiperhettä, joka on vakio kaapelointimenetelmä yritysten sekä yksityisasuntojen yleiskaapelointeja suunniteltaessa. Yleiskaapelimallina on käytetty Kategoria-5e-kaapelia, jota voidaan käyttää aina 1gbit/s kaistanleveyttä omaaviin lähiverkkoihin asti. Kiinteistössä on laitteina nykyisen palveluntarjoajan tarjoama Cisco 860 sarjan reitin, sekä paikallisen Hämeen Konttoritekniikka Oy:n toimittamat Zyxelin USG20-VPN-palomuuri, Digitus Networkin 12-porttinen kytkin, yksi Telewellin tukiasema, Alcatelin puhepalvelin, Lenovon tiedostopalvelin sekä UPS (Uninterruptible Power Supply). Kiinteistössä on useampi työpiste, jotka kaikki tarvitsevat verkkoyhteyden. Yrityksellä on kaksi tulostinta, jotka ovat langallisesti yhdistettyinä verkkoon. Yrityksen tämänhetkinen kaistanleveys on 100Mbit/s, koska puhelinkaapelointi rajoittaa saatavilla olevia nopeampia yhteyksiä. Valokuitukaapelointia ei ole vielä harkittu vedettäväksi yrityksen tiloihin.

Yrityksen nykytilanne huomioidaan erityisesti verkkoa suunnitellessa, sillä nykyiset laitteet kuten tulostimet, UPS sekä puhe- että tiedostopalvelimet tullaan liittämään osaksi uutta verkkoa. Yrityksen lähiverkon kaapelointia tarvitsee muuttaa uusien tukiasemien sijaintien määrittelyn vuoksi.

Kuva 10. Yrityksen teletilan topologiaa.

5.2 **Uuden verkon toteutus**

Uusi verkko toteutetaan teoriapohjaisena työnä Cisco Merakin laitteilla, koska he ovat kasvattaneet itse markkina-arvonsa tietoteknilliseen osaamiseen ja luotettavuuteen pohjautuen ja ovat näin ollen myös markkinoiden suurin tietoverkkopalvelujen tuottaja. Laitteiksi on valittu yrityksen kokoon ja tarpeisiin perustuen MX67W-palomuuri, yksi MS125-24-porttinen kytkin, kaksi kappaletta MR33-tukiasemia sekä yksi ulkokäyttöön sertifioitu MR74-tukiasema, 2 ulkokäyttöistä MV72-valvontakameraa, ja 2 sisäkäyttöön tarkoitettua MV12W-valvontakameraa. Kaikki Merakin laitteet tulevat tehdasasetuksilla varusteltuina, eli laitteiden fyysinen asennus on paljon nopeampaa, eivätkä vaadi asiantuntevuutta. Kuitenkin sisäverkon kaapelointia joudutaan tulevaisuudessa muokkaamaan hieman, jotta tukiasemat saadaan asennettua niille suunnitelluille paikoille. Verkko tullaan kahdentamaan eli jos langaton verkkoyhteys katkeaa, toimispisteille saadaan parikaapelia pitkin verkkoyhteys lisäten näin ollen vikasietoisuutta. Lisäksi yritys- sekä tiedostopalvelimet voidaan helposti liittää osaksi uutta verkkoa, jotta yritys saa pääsyn tiedostoihinsa ilman että heidän infrastruktuurinsa muuttuu siltä osin. Langattoman verkon tukiasemien kuuluvuutta ei voida mitata sillä fyysisiä laitteita ei ole saatavilla.

5.3 **Verkossa käytettävät laitteet**

Käytettyjen laitteiden osalta halutaan huomioida niiden tarjoamat ominaisuudet sekä miksi kyseisiä laitteita käytetään suunnitellussa verkossa. Kaikki käytetyt laitteet ovat pilvihallittavia, eli niihin päästään käsiksi mistä vaan. Verkko tarjoaa korkeaa suorituskykyä ja laitteiden myötä verkko on skaalautuva ja tietoturvan avulla yrityksen oma infrastruktuuri ei kärsi. Kaikkiin laitteisiin tulee hankkia lisensointi erikseen, joka vaihtelee 1–10 vuoden välillä yrityksen tarpeiden mukaan. Yritys voi halutessaan hallinnoida omaa verkkoaan helposti ja vaivattomasti. Yrityksen verkon rakennutukselle lasketaan kulut kattaen laitteet ja niiden lisenssit, sisäverkon kaapeloinnin ja laitteiden asennukset. Kuluissa huomioidaan myös tulevaisuuden kannalta yritykseen kuituliittymän kytkeminen.

5.3.1 MX67W-palomuuri

Cisco Merakilla on tuotevalikoimassa useaan käyttötarkoitukseen olevia palomuureja. Tässä työssä käytettiin MX67W-mallia, koska se vastasi yrityksen tarvetta saada tietoturvallinen valinta, jolla on kuitenkin tulevaisuusvalmius, esimerkiksi yrityksen laajentuessa nykyistä palomuuria ei tarvitse päivittää uudempaan. Palomuuri itsessään tarjoaa 450Mbit/s suodatuksen sen läpikulkevalle verkolle. Langallisen yhteyden rinnalla palomuuri tarjoaa myös langattoman 2.4GHz ja 5GHz taajuuksia hyödyntävää yhteyttä, joiden avulla voidaan saada enimmillään 1.3Gbit/s nopeuksia. Laitteessa on staattinen reititys käytössä, jonka avulla palomuurin perään liitettävät laitteet on helppo yhdistää samaan verkkoon. Laite tukee

tietoturvaratkaisuina automaattista VPN-systeemiä, jonka avulla voidaan luoda VPN-yhteyksiä nopeasti verkkoon. Lisäksi Palomuurin läpi voidaan filtteröidä Layer 7:n applikaatioita, mikä tarkoittaa, että laitteelle voidaan määritellä sovelluspohjaisia käytäntöjä, jotka joko sallitaan tai evätään palomuurin läpi kulkevalta yhteydeltä.

5.3.2 MS125-24-porttinen kytkin

Suunnittelutyössä käytettävä kytkin tarjoaa 24 käyttöporttia verkolle sekä 4x 10gbit/s SFP+ (Small form-factor Pluggable) -porttia siirtoyhteyksille. Vaikka yrityksellä ei ole kuin kolmasosalle porteista tarve, on kuitenkin hyvä, että portteja jää vapaaksi tulevaisuuden kannalta. Kytkimeen liitetään kaikki päätelaitteet, joita verkkoon halutaan liittää esimerkiksi langattomat tukiasemat. Lisäksi kytkimeen kytketään fyysisesti kaikki toimipisteet, jotta verkkoon saadaan lisää vikasietoisuutta tarkoittaen, että jos tukiasemien yhteys katkeaisi, käyttäjien toimipisteisiin kulkeutuisi kuitenkin verkkoyhteys parikaapelia pitkin. Kytkimen ominaisuuksiin kuuluu dynaaminen ja interaktiivinen verkon löytäminen, eli jos kytkin liitetään toiseen verkkoon, se osaa automaattisesti havainnoida verkossa sijaitsevat laitteet sekä topologian. Kytkimen läpikulkevan kaistanleveyden maksimikapasiteetti on 128Gbit/s sekä tarjoaa porttispesifioitua hallintaa läpikulkevan yhteyden tasapainottamiseksi sekä tietoturvan vuoksi. Kytkin tarjoaa Layer 3 reititysmahdollisuudet, joihin kuuluvat Staattiset reitit ja DHCP-palvelin.

5.3.3 MR33-sisäkäyttöinen langaton tukiasema

Käytetyt sisäkäyttöön tarkoitetut tukiasemat ovat0 hyvä valinta tämän kokoiselle yritykselle. Tukiasemat tarjoavat yhteensä 3 radiota, joista 2.4GHz ja 5GHz toimivat aina 1,3Gbit/s nopeuksiseen datan siirtoon asti verkkotaajuuksina. Kolmantena radiona toimii tietoturvallisuutta lisäävä WIPS (Wireless Intrusion Prevention System), joka monitoroi radiotaajuuksia sen varalta, ettei verkossa ole valetukiasemia, jotka saattaisivat vaurioittaa verkkoa. Laitteissa on 2x2 MU-MIMO-signaalireittiä pitkin kulkeva 802.11ac-standardia tukeva yhteys. Laitteet ovat myös mahdollisia kytkeä IEEE 802.3af-standardisoidulla PoE (Power over Ethernet) -tekniikalla, jolla tukiasemien virtaliitäntänä toimii RJ-45 (Registered Jack-45) -parikaapeli, joka syötetään joko PoE-tekniikkaa tukevalta kytkimeltä tai hyödyntäen injektoria, jonka avulla erilliseen parikaapeliin syötetään virtajännite, jonka laite vastaanottaa. Laitteessa on hyvät tietoturvaa lisäävät toiminnot kuten WPA2-Enterprise, IP-turvattu VPN, AES, sekä sisäänrakennettu tason 7 palomuuri, jolla voidaan esimerkiksi suodattaa sallittuja sivustoja tai palveluita, joihin verkkoa käytetään. Laitteita halutaan kaksi täydellisen langattoman verkon kuuluvuuden kattamiseksi. Tämä saavutetaan laitteiden integroiduilla mesh-topologiaa hyödyntävällä protokollalla, jolla laitteet voivat optimoida itsensä jakamaan verkkoa muille tukiasemille sekä vikatilanteiden sattuessa uudelleen ohjata verkon parikaapelia pitkin käyttäjien toimipisteille.

5.3.4 MR74-ulkokäyttöinen langaton tukiasema

Yrityksen verkolle on tärkeää langaton verkon kuuluvuus. Tämän vuoksi ulkoista käyttöä varten suunnitellaan yksi IP67-luokiteltu tukiasema, joka kestää esimerkiksi vesisadetta. Ulkoasema asennetaan täysin kattamaan verkkoa ulos asennettaville turvakameroille mutta samanaikaisesti yrityksen lähiverkon kuuluvuus on myös saatavilla sisäpihalla, eli käyttäjän ei tarvitse missään vaiheessa lähteä verkon alueelta ollessaan työympäristössä. Ulkotukiasemassa on 3 aiemmin mainitun radion lisäksi myös 4. radio, joka tarjoaa mahdollisuuden Bluetooth-yhteyden muodostamiseksi laitteeseen.

5.3.5 MV72- ja MV12W-valvontakamerat

Koska yritys haluaa lisätä omaa turvallisuuttaan, asennetaan heille 2 kappaletta ulkokäyttöisiä MV72-valvontakameroita ja 2 kappaletta sisäkäyttöön tarkoitettuja Merakin MV12W-valvontakameroita, jotka saavat yhteyden verkkoon langattomasti. Ulkokäyttöisten valvontakameroiden sisään on rakennettu 256GB nopeasti luettavaa tallennustilaa, tarkka 1080 p-HD-videotallennus, sekä äänen tallentamista varten mikrofoni. Valvontakamerat ovat IP67, ja IK10 sertifioituja, eli sateen kestävyyden lisäksi myös iskunkestäviä. Valvontakameroiden lähettämää videomateriaalia voidaan tarkastella livenä, kunhan palomuurista avataan pilvestä reititettävää yhteyttä varten portit. MV12W-valvontakamerat toimivat isolla näkökentällä, jotta niiden kuvaama materiaali näkyisi paremmin. Lisäksi yhdenkään valvontakameran ei tarvitse olla liitettynä käyttöliittymään sillä ne ovat itsehallinnollisia.

6 CISCO MERAKIN KÄYTTÖÖNOTTO

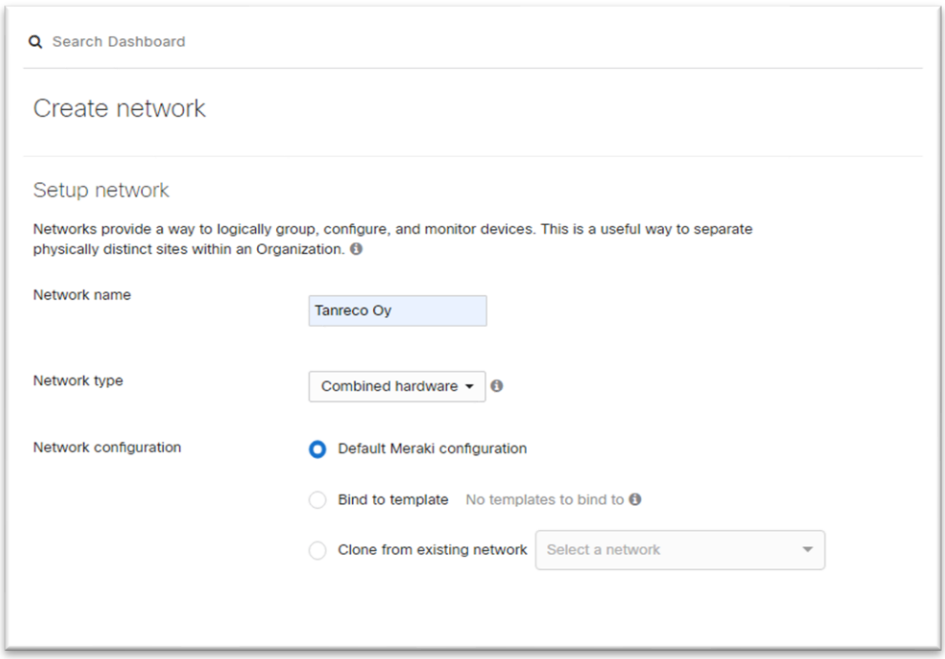
Opinnäytetyön käytännönosuus suoritettiin täysin teoreettisena pohjautuen opinnäytetyössä käytyihin asioihin, koska fyysisiä laitteita ei ollut saatavilla. Työn tilaajana toimi Tanreco Oy. Työssä hyödynnettiin Cisco Merakin tarjoamaa Demo-ympäristöä oikealle käyttöliittymälle, jonka avulla saatiin verkko suunniteltua kuitenkin ilman, että laitteet olisivat fyysisesti kytkettyinä. Kuitenkaan demon rajoitettujen toimintojen takia virtuaalisen verkon laitteisiin ei saatu muodostettua yhteyttä, joten työ jouduttiin rajaamaan pelkästään suunnittelutyöksi. Verkkoon liitettiin pohjapiirros yrityksen tiloista, joka helpotti verkon dokumentointia sekä käyttöönottoa. Tässä osuudessa käydään myös läpi työn eri vaiheet, jotka käytäisiin läpi lähiverkon luomisessa oikeilla laitteilla.

6.1 Käyttöliittymä

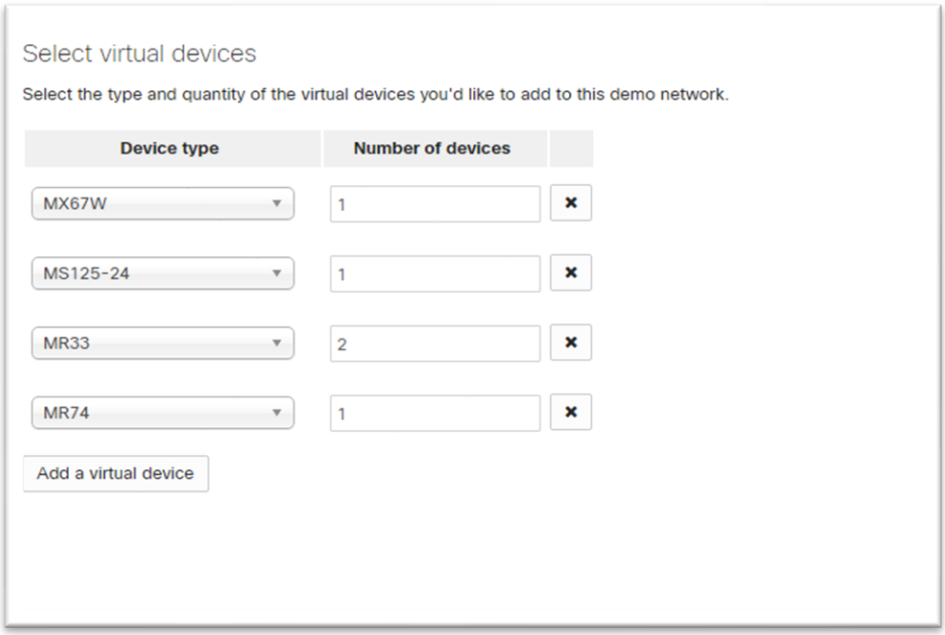
Cisco Merakin käyttöliittymä on selainpohjainen Meraki Dashboard, johon pääset kirjautumalla sisään millä tahansa internetyhteyttä tukevalla päätelaitteella. Ensimmäisenä kirjautumisen jälkeen avautuu käyttäjälle hallintaportaali, joka kattaa kaikki organisaatiot joihin käyttäjätunnus on liitetty. Hallintaportaalista voidaan valita haluttu organisaatio, jota tarkastellaan. Itse käyttöliittymässä on paljon ominaisuuksia, joilla voidaan hallinnoida sekä konfiguroida organisaatioiden verkkoja halutunlaisiksi. Järjestelmä lähettää lokitietoja käyttäjälle joko sähköpostitse tai suoraan puhelimeen aina, kun verkossa oleviin laitteisiin tehdään muutoksia tai itse käyttöliittymää päivitetään. Tämä parantaa hallinnoijan tietoisuutta verkon tapahtumista.

6.1.1 Uuden asiakkuuden luominen

Kun halutaan liittää uusi verkko Merakin käyttöliittymään, tulee ensiksi luoda verkolle tunnus. Tämän jälkeen valitaan, halutaanko luoda kaikille Merakin laitteille yhtenäinen verkko vai erillinen hallintaverkko jokaiselle laitteelle. Tämän jälkeen verkolle määritellään geolokaatio dokumentointia varten (Kuva 11). Tämän jälkeen valitut laitteet liitetään virtuaalisesti järjestelmään käyttäen tuotteiden mallinumeroa (Kuva 12). Oikeiden laitteiden lisäyksessä käytettäisiin tässä vaiheessa laitteissa olevia rekisterikoodeja, joilla ne saadaan liitettyä verkkoon. Käyttöliittymän demoympäristössä ei voida lisätä käytettäviä valvontakameroita verkkoon. Kuitenkin niiden yhdistäminen verkkoon on helppoa, sillä valvontakamerat noudattavat samaa Zero touch provisioning -menetelmää kuin kaikki muut Merakin laitteet, eli laitteet saavat ensimmäisen verkkoon liittämisen aikana suoraan kaikki verkon tiedot, joiden avulla saavat verkkoyhteyden muodostettua.



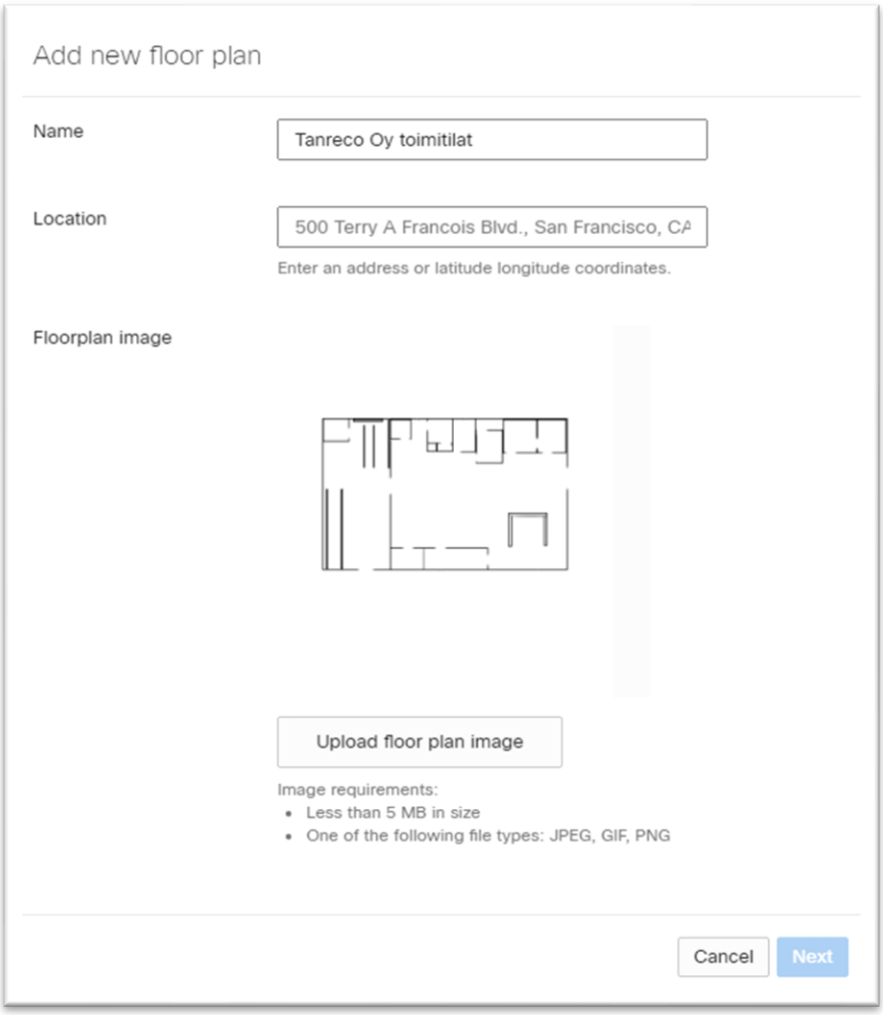
Kuva 11. Uuden asiakkaan luominen käyttöliittymälle.



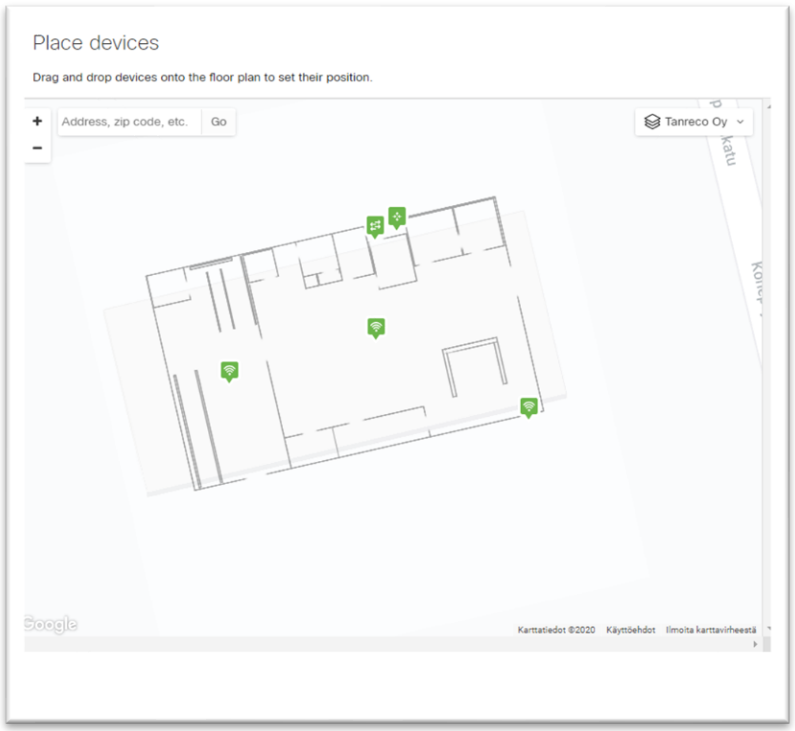
Kuva 12. Uusien laitteiden valitseminen juuri luodulle verkolle.

Laitteiden lisäämisen sekä organisaation nimeämisen jälkeen järjestelmä generoi käyttäjälle organisaatiosivun, joka avautuu ensimmäiseksi aina kun käyttöliittymälle kirjaudutaan. Tältä sivustolta voidaan tarkastella verkon yleisnäkymää, joka kertoo verkossa liikkuvan datan määrän, siinä kiinni olevat laitteet ja lisäksi jos jokin laite on katkaissut yhteyden verkkoon. Kuvassa 13 käydään läpi, kuinka voidaan liittää haluttu

pohjapiirustus ja kuvassa 14 liitetään aiemmin listatut laitteet dokumentoinnin helpottamiseksi pohjapiirustuksen päälle. Pohjapiirustukset helpottavat myös langattoman verkon kuuluvuuden mittauksia tehtäessä. Tässä työssä ei kuitenkaan pystytä kuuluvuusmittauksia tekemään.



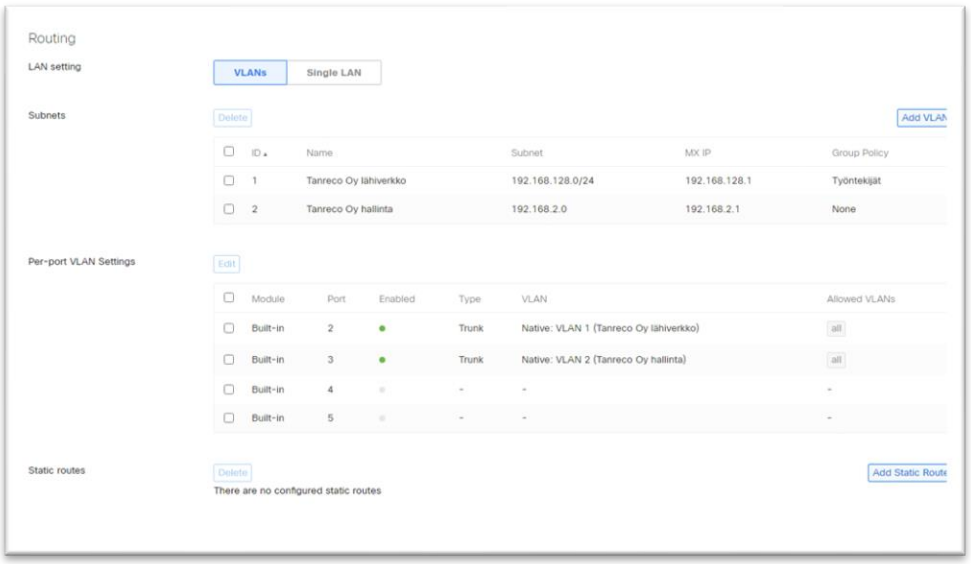
Kuva 13. Pohjapiirustuksen lisääminen aiemmin luotuun verkkoon.



Kuva 14. Laitteiden lisääminen pohjapiirustukseen.

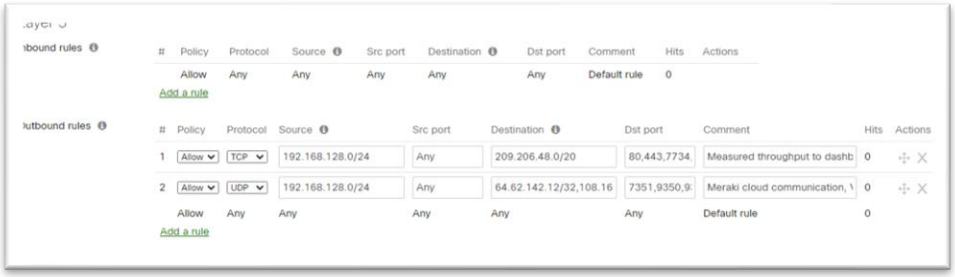
6.1.2 Langattoman lähiverkon konfigurointi

Lähiverkon konfigurointi aloitetaan topologian mukaisesti, eli ensimmäiseksi konfiguroidaan palomuurille fyysiset aliverkotukset ja virtuaalisen lähiverkon (Virtual Local Access Network), joita palomuuri jakaa verkon muille laitteille. Verkolle liitetään erillinen hallintaosoite, jotta laitteeseen voidaan tarvittaessa päästä käsiksi sen omasta hallintaosoitteesta. (Kuva 15.) Tämän jälkeen palomuurille asetetaan langattoman verkon asetukset, eli avataan radiokanavat, jotta verkko voidaan kahdentaa sekä langattomasti että langallisesti. Tämän jälkeen palomuurilta avataan portit, jotta esimerkiksi kytkin sekä itse palomuuri voivat ottaa yhteyden pilveen.



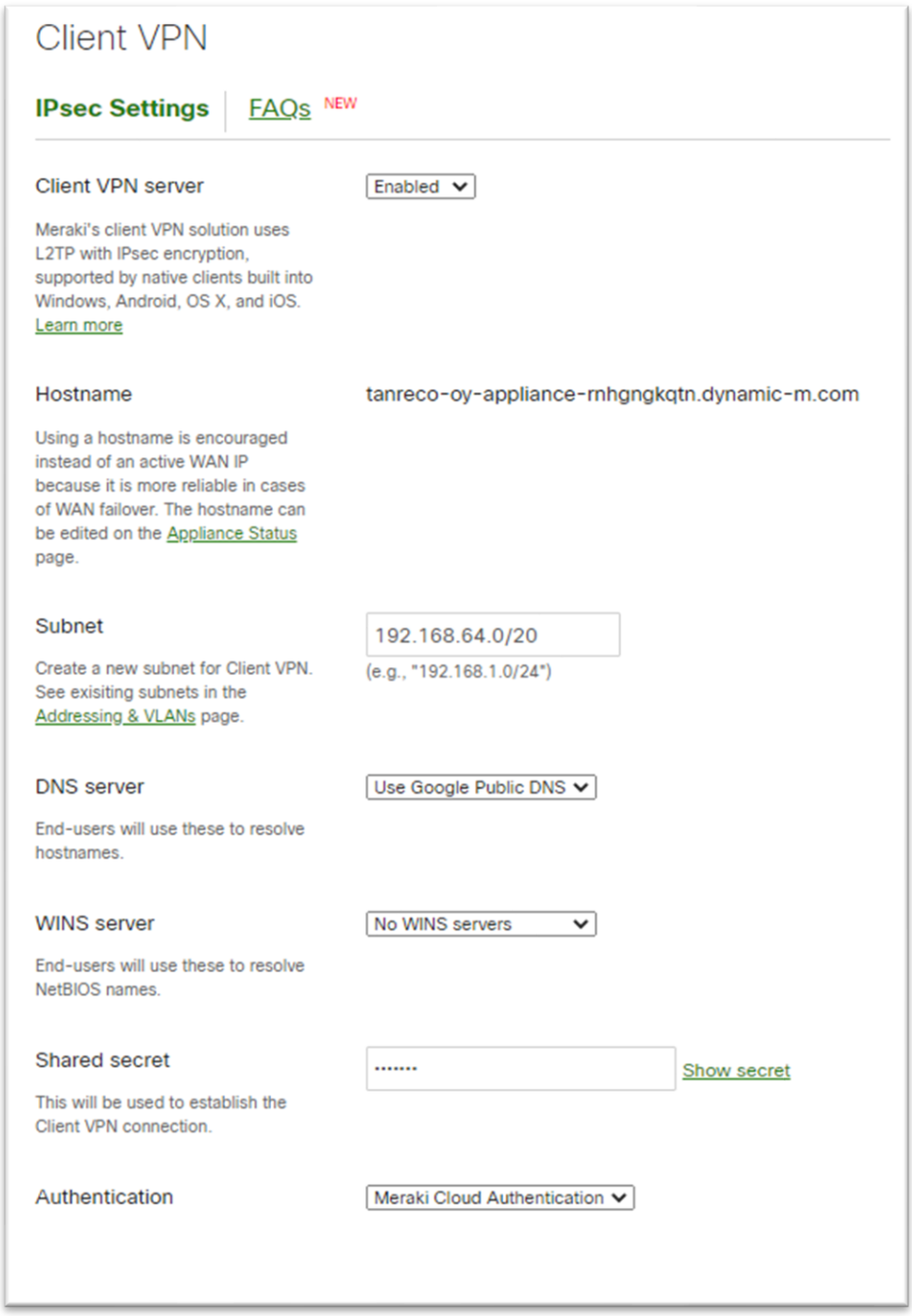
Kuva 15. Palomuurin reitityksien määrittely.

Jaettavaksi VLAN-tunnisteiksi on määritelty yleiseen datan siirtoon VLAN 1, ja hallintaan varten VLAN 2. Näin ollen hallinnointipalveluihin ja datan siirtoon käytettävä yhteys eivät sekoitu keskenään. (Kuva 16.)



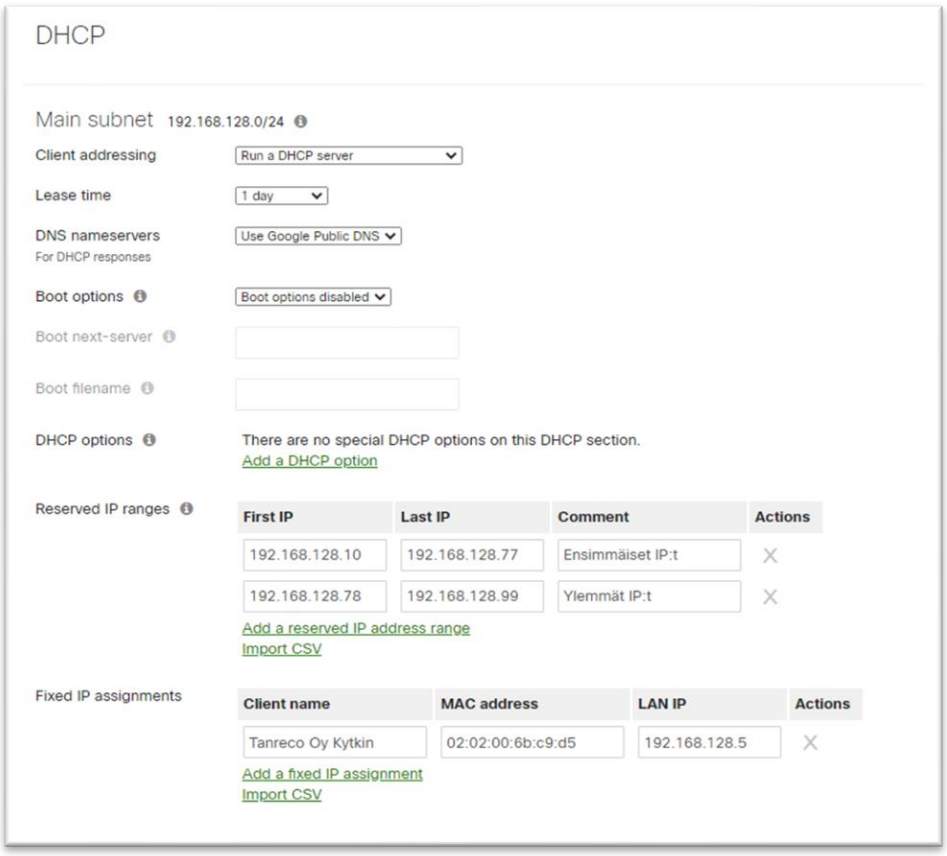
Kuva 16. Palomuurin porttien avaus pilviyhteyden muodostamiseksi.

Palomuuriin lisätään Client VPN, jonka avulla yritys voi naamioida käyttäjien IP-osoitteet verkossa. VPN-yhteydelle luodaan oma aliverkko sekä salausprotokolla, jolla, verifioidut käyttäjät voidaan yhdistää verkkoon. (Kuva 17.)



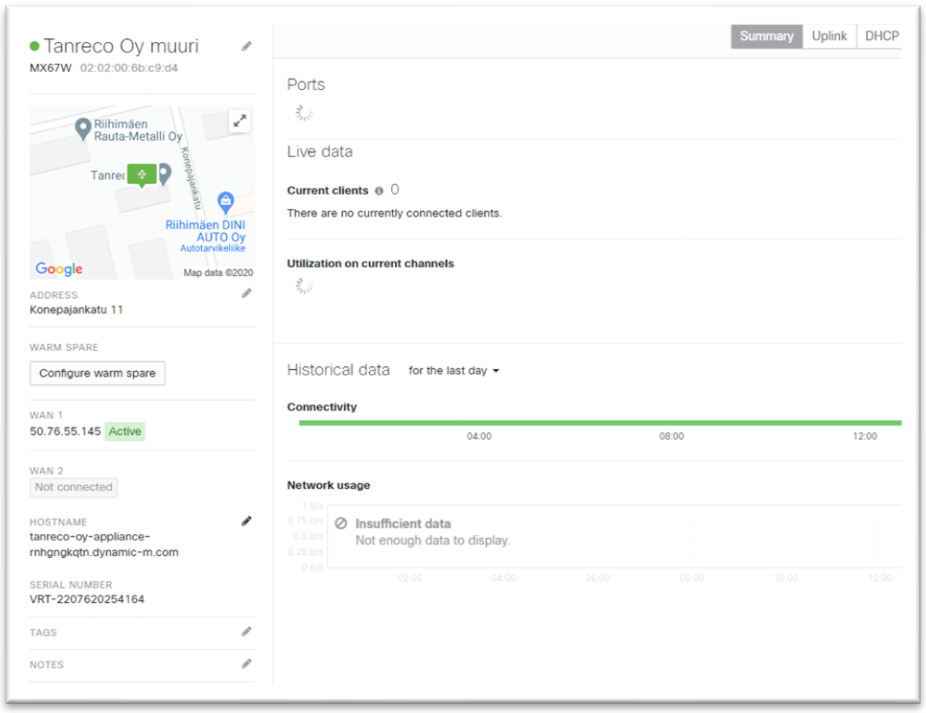
Kuva 17. Client VPN-yhteyden luominen verkolle.

Palomuurille voidaan myös määritellä DHCP-palvelin, jonka avulla verkon muut laitteet voivat ottaa ennalta määritettyjä osoitteita käyttöön näin ollen verkon konfigurointi on helpompaa, kun päätelaitteille ei tarvitse määritellä omia staattisia IP-osoitteita. Alla olevassa kuvassa määritellään DHCP-palvelulle varatut IP-osoitteet sekä varataan kytkimen IP-osoite staattiseksi (Kuva 18).



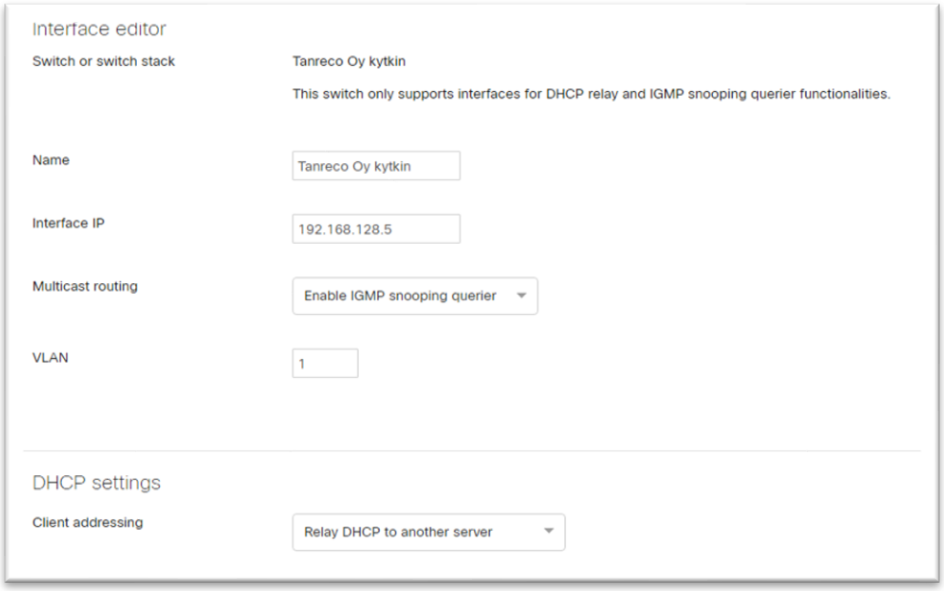
Kuva 18. DHCP-palvelun määrittely

Palomuurin yleisnäkymästä voidaan tarkastella siihen liitettyjen laitteiden läpikulkevaa dataa ja laitteen omia tietoja kuten tämän MAC-osoite ja annetut konfiguroinnit (Kuva 19). Laiteelta voidaan myös pingaamalla, eli lähettämällä testipaketteja toiselle laitteelle havaita, onko muut verkossa olevat laitteet konfiguroitu oikein keskustelemaan keskenään. Yleisnäkymä kattaa myös tiedot laiteohjelman päivityksistä, ja onko laitepäivitykset ajan tasalla. Laitteiden yleisnäkymässä Power-valikosta voidaan nähdä laitteiston virranhallintaan liittyviä asioita kuten kuinka paljon PoE jakaa porteille käytettävissä olevaa virtaa. Tämän lisäksi laite voidaan paikantaa Location-valikon alta löytyvästä sille aiemmin määritellystä paikasta. Event Log-valikosta löydetään kaikki kyseisen laitteen tapahtumatiedot sisältäen kaikki laitteelle tehdyt konfiguroinnit ilmoituksina.

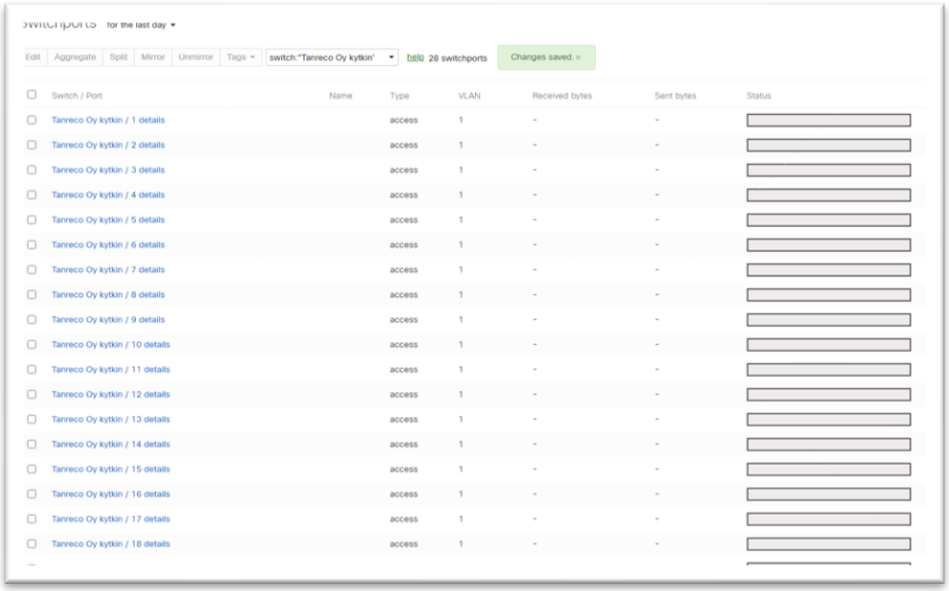


Kuva 19. Palomuurin yleisnäkymä.

Palomuurin konfiguroinnin jälkeen siirrytään kytkimen konfigurointiin. Kytkimelle pitää määritellä oma laite IP-osoite samasta avaruudesta kuin palomuurille (Kuva 20), jotta ne olisivat samassa verkossa dokumentoinnin helpottamiseksi. Lisäksi kytkimelle määritellään hallinta IP-osoite ja kytkimen portit yhdistetään jakamaan samaa virtuaalista lähiverkkoa kuin mitä palomuuri tarjoaa. Näin ollen kytkimen portit voivat jakaa yhteyttä sekä päätelaitteille ja asennettaville tukiasemille (Kuva 21). Kytkimelle asetetaan vielä lupa vastaanottaa palomuurille määriteltyä DHCP-palvelun IP-avaruutta automaattisesti.

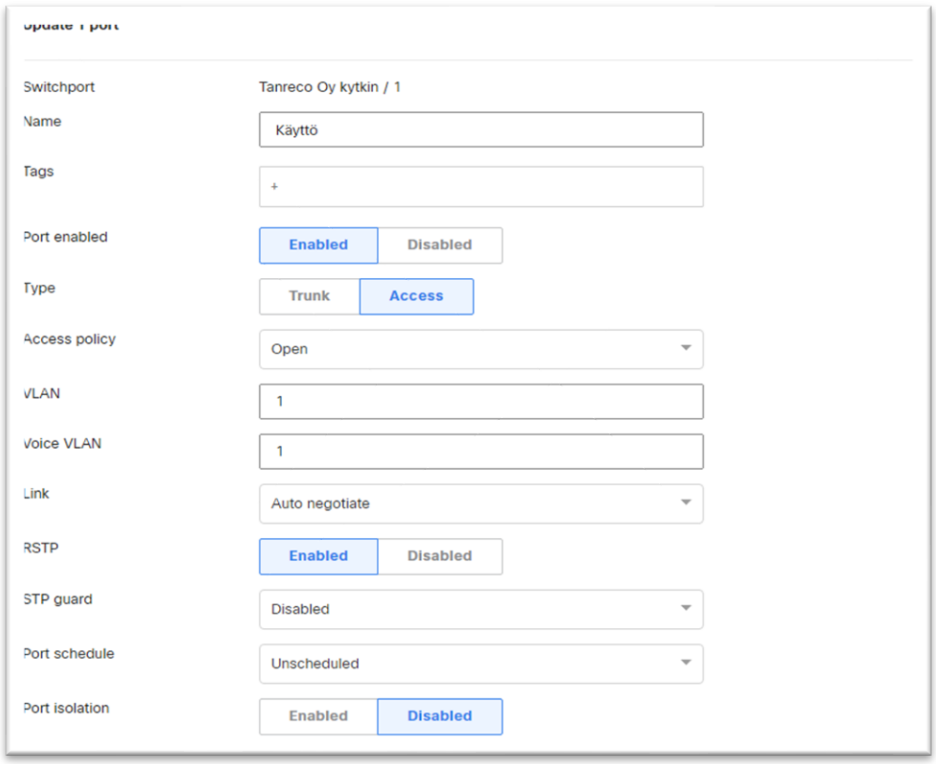


Kuva 20. Kytkimen osoitteen määrittely.



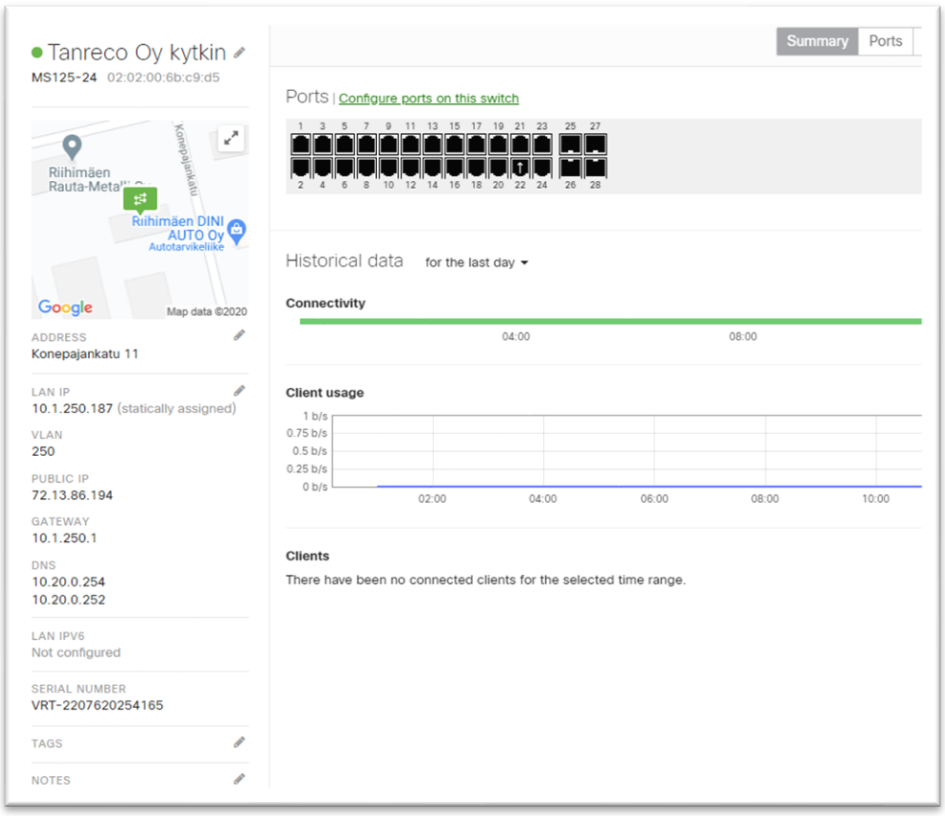
Kuva 21. Kytkimen porttihallinta.

Kytkimen porteille voidaan erikseen määritellä, jakaako portit vain dataa vai toimivatko ne linkin ylläpitäjänä toiselle kytkimellle. Tämän verkon yhteydessä ei kuitenkaan käytetä kuin yhtä kytkintä, mutta yksi kappale kytkimen porteista on määritelty trunk-asentoon, ja loput ovat access-asennossa. Trunk-portti on hallintaverkkoyhteyttä varten mutta kuitenkin sallii datan ensimmäisestä virtuaaliverkosta (Kuva 22). Porteille voidaan myös määritellä erikseen ajankohdat koska portit ovat päällä ja kuinka paljon niistä voi kulkea dataa kerralla. Porteille määritellään natiivi VLAN:ksi 1 tiedonsiirtoa varten.



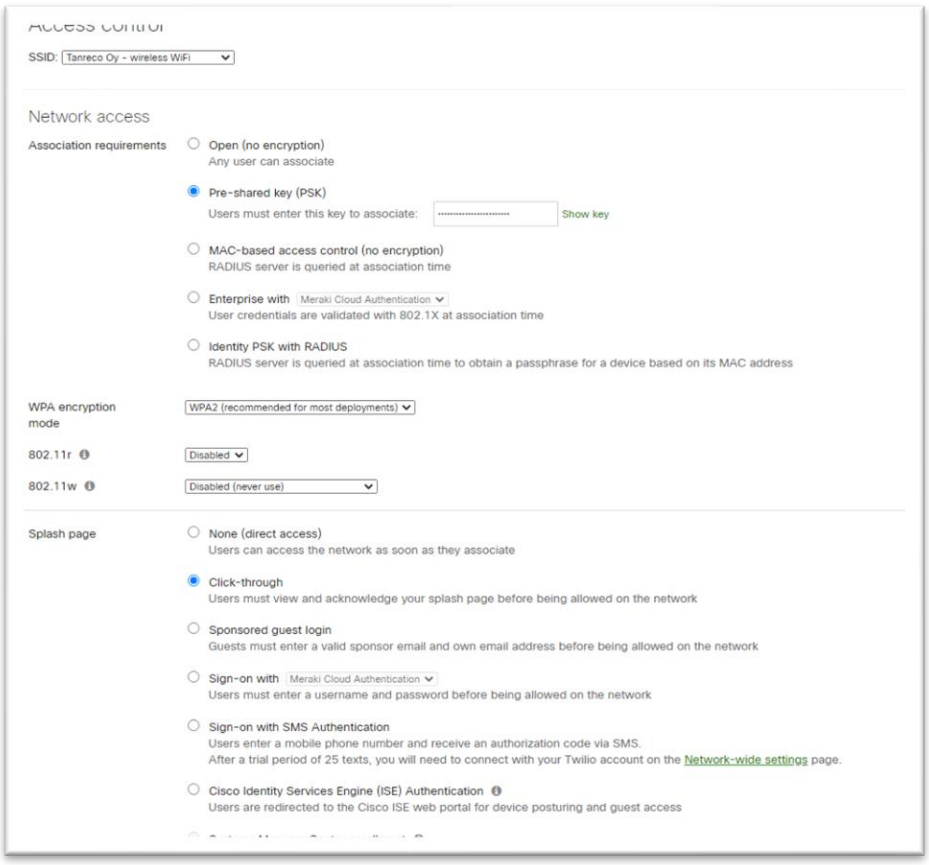
Kuva 22. Kytkimen porttispesifioitu konfigurointinäkymä.

Kytkimen yleisnäkymästä voidaan katsastella sille määriteltyjen porttien kytkeytymistä verkkoon ja kuinka paljon dataa mikäkin portti suodattaa lävitseen (Kuva 23). Tapahtumalokeista voidaan katsastella esimerkiksi ARP (Address Resolution Protocol) -taulua, josta voidaan tunnistaa verkkoon kytketyt laitteet näiden MAC-osoitteiden perustella. Yleisnäkymästä voidaan myös tehdä kaapeloinnintestauksia portteihin kytkettyihin kaapeleihin, jolla voidaan esimerkiksi havaita, jos kaapeleiden sisällä kulkevissa johdinpareissa on vikaa, joka vaikuttaisi esimerkiksi kulkevan yhteyden laatuun. Lisäksi kytkimen yleisnäkymästä voidaan nähdä sille määritelty IP-osoite sekä yhdyskäytävä, jota pitkin yhteys kulkeutuu kytkimelle.



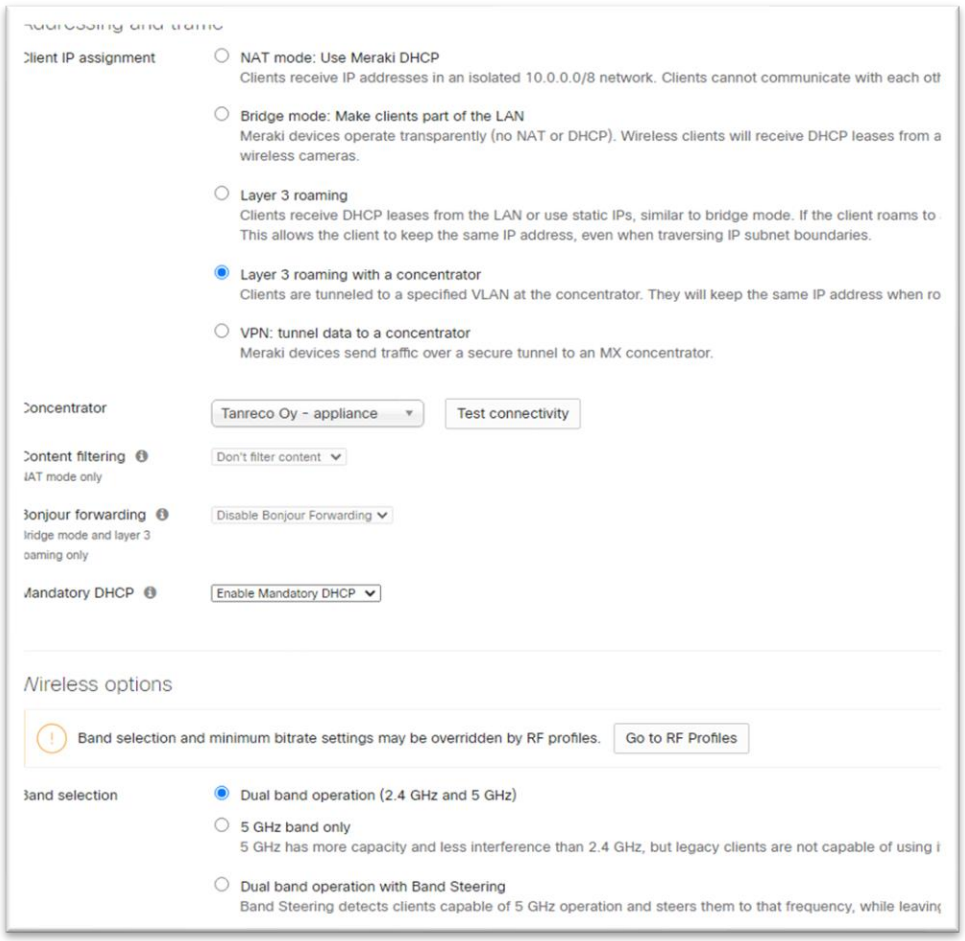
Kuva 23. Kytkimen yleisnäkymä.

Kytkimen jälkeen siirrytään konfiguroimaan tukiasemia. Tämä aloitetaan määrittelemällä tukiasemille verkkotunnukset, joita tukiasemat mainostavat käyttäjille verkossa (Kuva 24). Jokaiselle verkkotunnukselle voidaan antaa oma nimi dokumentoinnin helpottamiseksi sekä määritellä erikseen, kumpaa taajuusaluetta tai mitä radiokanavaa pitkin yhteys kulkee. Yritykselle konfiguroidaan erikseen yrityksessä vieraileville asiakkaille oma verkko, jota asiakkaat voivat halutessaan hyödyntää. Yrityksen omalle verkolle muodostetaan salaus WPA2-salauksella, joka on vain yrityksen työntekijöiden saatavilla. Lisäksi työntekijöiden tulee liittyä verkkoon erillisen Splash-sivuston kautta, joka aukeaa, kun verkkoon yritetään liittyä. Tukiasemat määritellään käyttämään ensisijaisemmin 5GHz-tajuutta, mutta tarvittaessa pystyvät vaihtamaan 2.4GHz taajuudelle. Tämä johtuen siitä, että 5GHz-taajuudella saadaan taattua esteettömämpi verkon kuuluvuus, kun lähialueella ei ole niin paljoa samalla taajuudella olevaa liikennöintiä. Kuitenkin on huomioitavaa, että kaikkien langattomien päätelaitteiden tulee tukea 5GHz-taajuutta tämän toimivuuden kannalta.



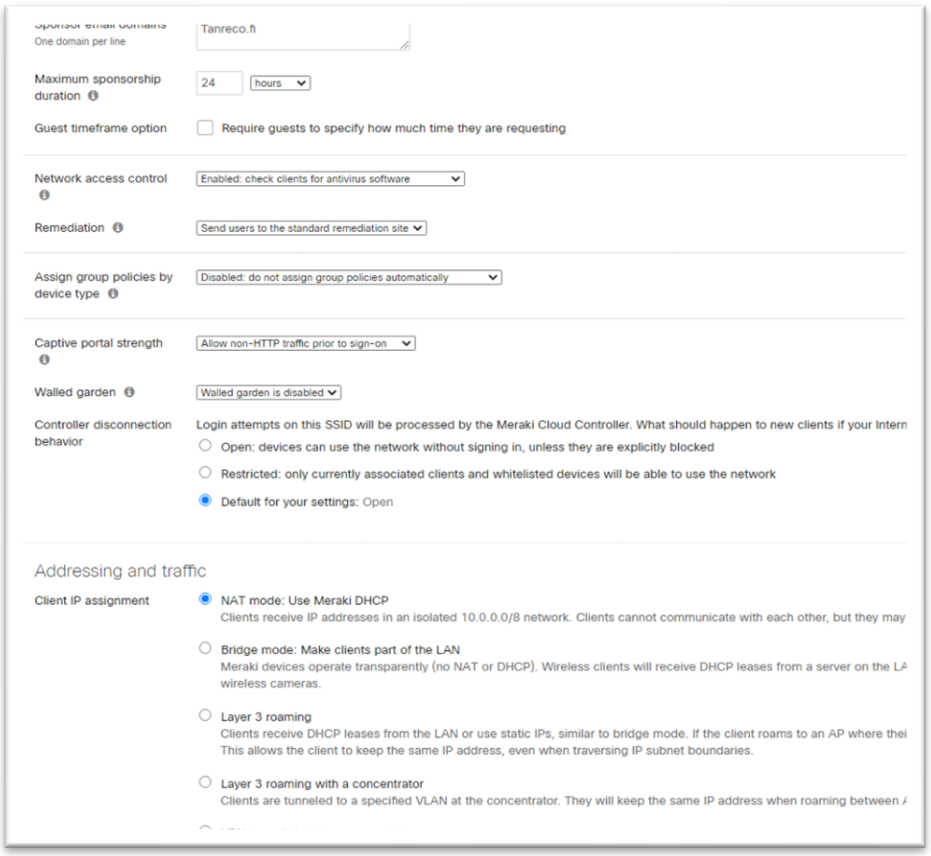
Kuva 24. Yrityksen oman verkkotunnuksen määrittely verkon määrittely.

Yrityksen omalle verkkotunnukselle tehdään vielä konfigurointi, joka määrittelee tukiasemat mesh-verkoksi, jonka avulla käyttäjien verkkoliikenne optimoituu sen mukaan, minkä kanavan ja taajuusalueen tukiasemat näkevät käyttäjän parhaaksi. Yrityksen työntekijät tulevat osaksi verkkoa, näin ollen he saavat suoraan ennalta määritellyn DHCP-palvelimen IP-osoitteen yhdistyessä verkkoon, joka pysyy samana, vaikka käyttäjä menisi eri tukiaseman kuuluvuusalueelle. (Kuva 25.) Konfiguroinneista säädetään vielä, että kaikki käyttäjät pakotetaan käyttämään DHCP-palvelimen IP-osoitetta tähän verkkotunnukseen yhdistyäkseen. Jos staattista osoitetta yritetään käyttää, käyttäjä ei voi yhdistyä. Vierasverkolle määritellään Merakin oma NAT-mode, joka tarjoaa eritellystä aliverkosta osoitteet vieraili-joille. Tukiasemat käyttävät automaattisesti molempia, sekä 2.4GHz että 5GHz taajuuksia.



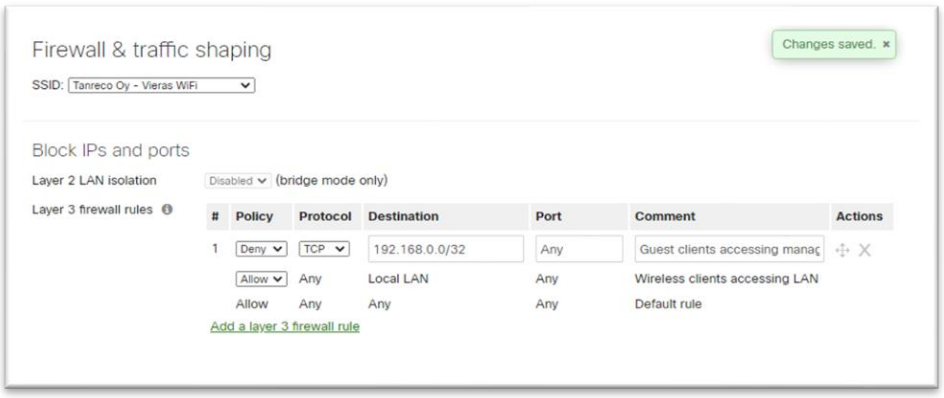
Kuva 25. Tukiaseman liikennöinnin määrittely.

Määritellyille verkkotunnuksille tehdään hieman erilaiset konfiguroinnit sillä vierasverkon ei ole tarkoitus antaa kaikkia samoja ominaisuuksia kuin itse yritysverkko tietoturvallisuuden kannalta. Näin ollen esimerkiksi yritysverkon hallintaan pääsy evätään vierasverkolta. Lisäksi itse yritysverkkoon pääsee vain yrityksen työntekijät heille jaetulla salasanalla. Vierasverkkoon sen sijaan määritellään WPA2-salauksen lisäksi sponsoroitu vieraskirjautuminen, jonka vieraat voivat pyytää yrityksen työntekijältä verkkoon liittyessä. (Kuva 26.) Tätä lisäverifikaatiota voi yrityksen työntekijät halutessaan vaihtaa, jotta tukiasemien tarjoamaan vierasverkkoon ei pääse kuka tahansa milloin tahansa.



Kuva 26. Vierasverkon lisäverifikaation lisäys.

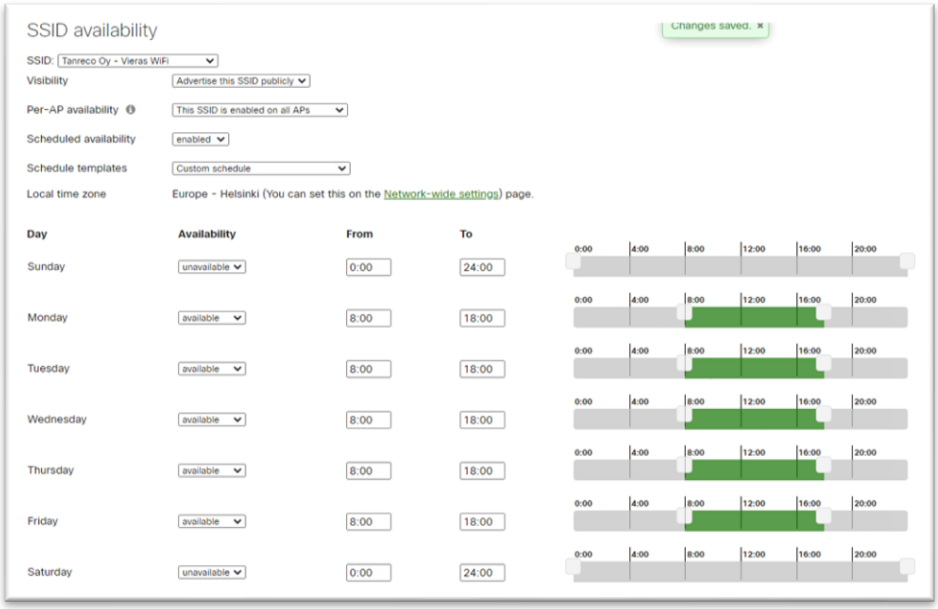
Vierasverkon eristämiseksi yrityksen omasta langattomasta verkosta vierasverkon omista tason 3 palomuurin asetuksista rajataan verkkohallinnan IP-osoitteet, jotta vierasverkosta ei päästä itse laitteiden hallintaan käsiksi. (Kuva 27.)



Kuva 27. Vierasverkon palomuuriasetusten määrittely.

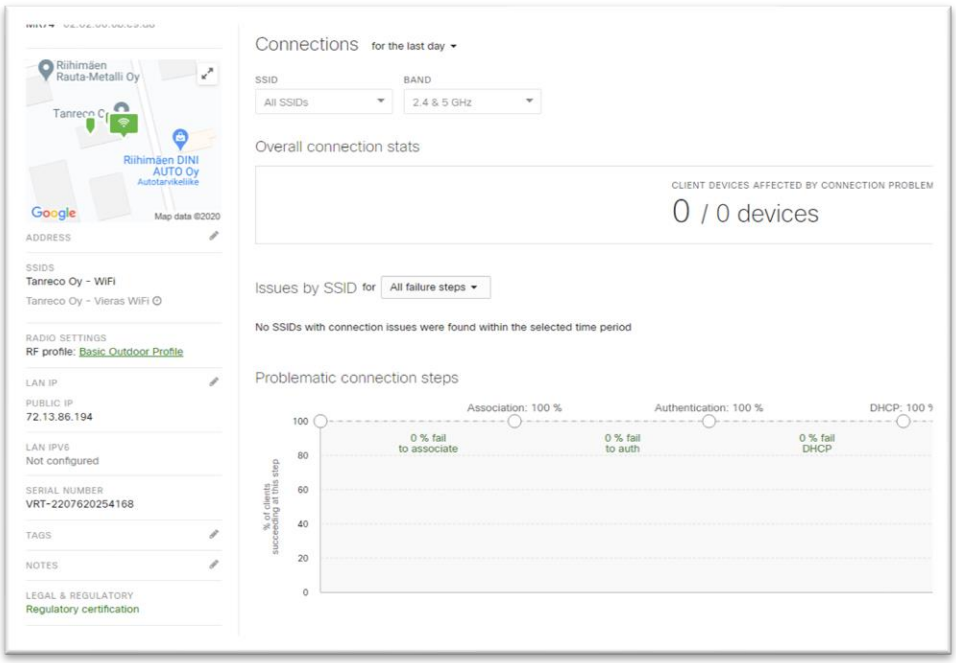
Koska vierasverkkoon olisi mahdollista päästä mihin kellonaikaan tahansa sillä tukiasemien kuuluvuusalue yltää yrityksen omalle piha-alueelle, määritellään vierasverkolle aikaikkuna, jolloin vierasverkkoa mainostetaan.

Tämä määritellään tukiasemien verkkotunnuksien saatavuusvalikosta (Kuva 28.), jossa voidaan valita halutut ajankohdat verkkotunnuksien näkyvyydelle päiväkohtaisesti. Tässä tapauksessa yritykselle ei ole väliä, vaikka verkkotunnus näkyisi viikonloppuisin, joten tietoturvallisuuden lisäämiseksi vierasverkon saatavuus rajoitetaan vain arkipäiviin.



Kuva 28. Vierasverkon tunnuksen rajaus.

Tukiasemien yleisnäkymä tarjoaa tarkkaa liikennöintidataa käyttäjälle. Esimerkiksi tukiasemista voidaan nähdä kuinka kattavat kuuluvuusalueet ovat milläkin taajuudella. Tukiasemista nähdään myös, kuinka kauan esimerkiksi yksittäinen käyttäjä on ollut kiinni missäkin tukiasemassa, kuinka paljon dataa on siirretty päätelaitteen ja verkon välillä ja mitä kanavia tukiasema on käyttänyt (Kuva 29).

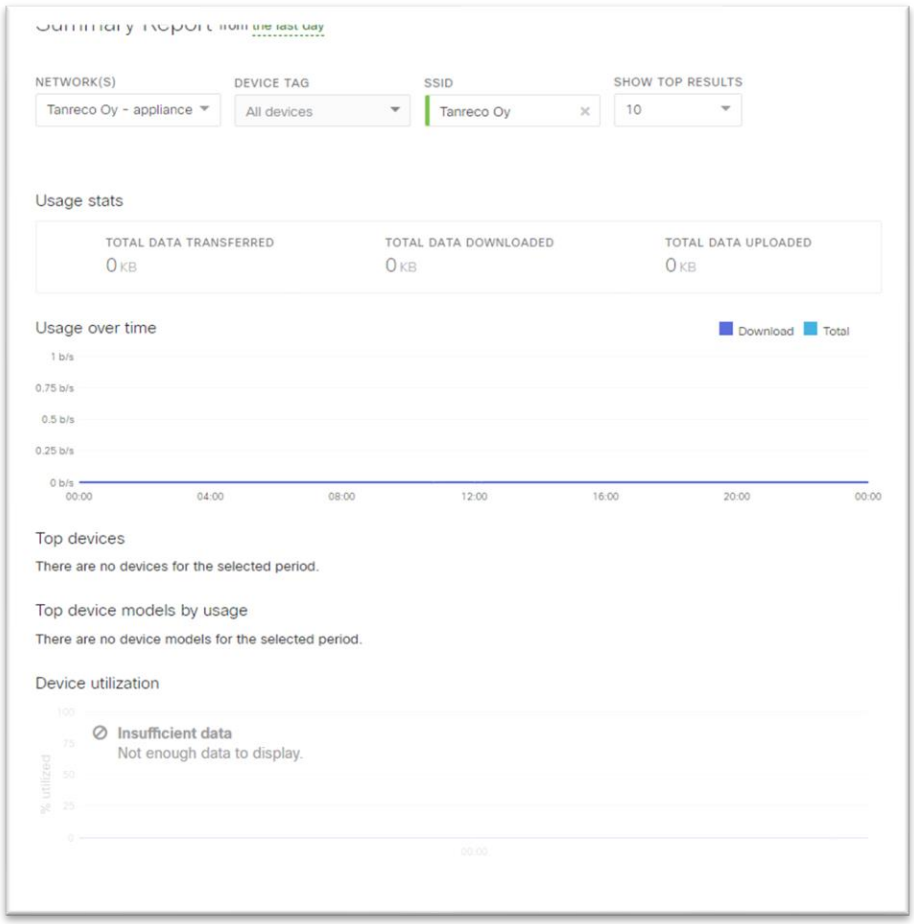


Kuva 29. Tukiaseman yleisnäkymän tarjoamaa statistiikkaa.

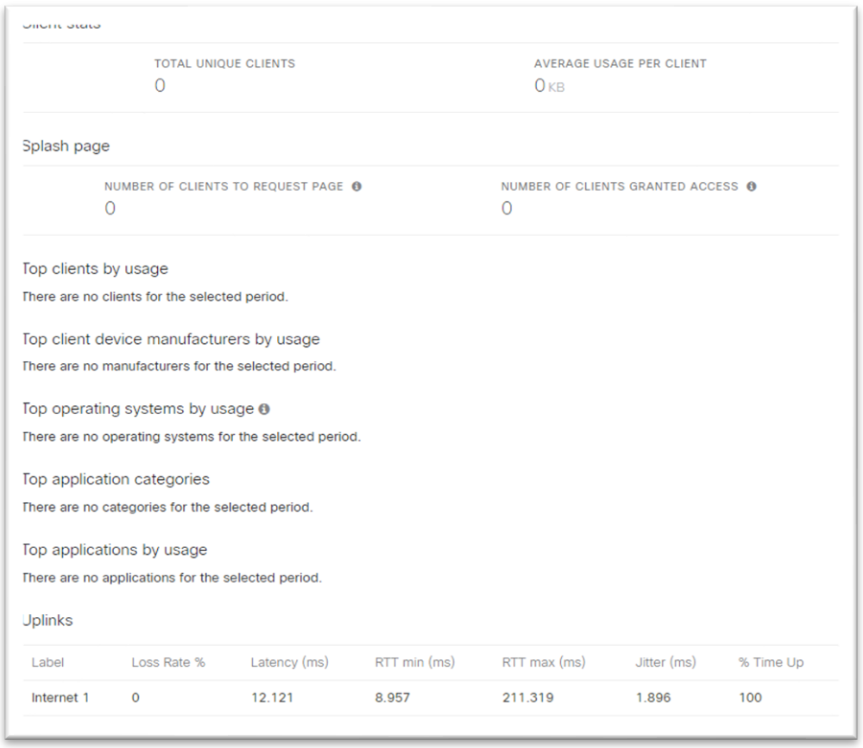
6.2 **Lähiverkon dokumentointi ja analysointi**

Verkon dokumentointi on jo suunnitteluvaiheessa tärkeää tehdä tarkasti, sillä tieto laitteiden sijainneista, niiden fyysisestä kaapeloinnista, konfiguroinneista sekä laitetiedoista on oltava saatavilla helposti ja esteettömästi etenkin niissä tilanteissa, kun verkkoon tarvitsee päästä nopeasti tekemään muutoksia. Huolellinen dokumentointi helpottaa muiden työtä, ja on pidemmällä katseella kustannustehokkuuteen vaikuttava tekijä, kun rakennetun verkon tiedot ovat helposti saatavilla niille, jotka niitä tarvitsevat.

Cisco Merakin laitteille ominaista on tarkka verkon laitteiden ja käyttäjien liikennöinnin seuraaminen. Laitteiden monipuolinen hallittavuus seurantatyökalujen kanssa mahdollistavat käyttäjien päätelaitteilla suoritettavien sovellusten tarkkailun. Laitteiden seurantatyökalut keräävät päätelaitteiden verkon käytön tietoja reaaliajassa ja kerää kaikki tapahtumat lokiin, josta saadaan yleistietoa myös, jos verkossa tapahtuu esimerkiksi katkoksia sinä aikana, kun verkkoa ei käytetä (Kuva 30 ja Kuva 31).



Kuva 30. Koko verkon tapahtumalokin tarjoamaa dataa.



Kuva 31. Verkon käyttäjiin liittyvää statistiikkaa.

Meraki tarjoaa laitehallintaa päätelaitteille Meraki Systems Manager-toiminnon avulla, joka monitoroi laitteiden tiedoista ja sijainnista saatavaa statistiikkaa. Meraki tarjoaa myös spesifioidumpaa mobiililaitteiden, kuten tablettien, kannettavien tietokoneiden sekä matkapuhelinten hallinnointiin tarkoitettua kolmannen osapuolen palvelua. Mobiililaitehallinnassa määritellään laitteille turvallisuuskäytäntöjä, joiden tarkoitus on suojata laitteita ja niiden sisältämää dataa, rajoittaa laitteiden käyttämää sisältöä, esimerkiksi Youtube-sivusto tai päätelaitteen kameran käyttö voidaan estää.

7 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli suunnitella Tanreco Oy:lle uusi langaton lähiverkko hyödyntäen Cisco Merakin laitteita ja näiden tarjoamaa pilvihallinnoitavaa käyttöliittymää, jonka avulla Tanreco Oy voisi tulevaisuudessa oman lähiverkkonsa uudistaa. Työssä hyödynnettiin oikeiden laitteiden sijasta Merakin demoympäristöä, jonka myötä verkkoympäristön toteuttaminen osoittautui haastavaksi, sillä vaikka verkon konfigurointia ei ollut rajoitettu, oli kuitenkin verkossa käytettyjen laitteiden virtuaalinen kytkentä mahdotonta. Tämä rajoitti suunniteltavan verkon dokumentointia sekä analysointia, kun siitä ei pystytty saamaan minkäänlaista dataa nähtäväksi, joita laitteet olisivat prosessoineet, jonka vuoksi työ painottuu käyttöalustan käyttöönoton dokumentointiin. Verkkolaitteiden konfigurointi sekä järjestelmän käyttöönoton dokumentointi onnistuivat kuitenkin hyvin.

Työssä painottavina tekijöinä olivat suunniteltavan verkon kustannustehokkuus ja tietoturvallisuus. Kustannustehokkuus näkyy jo itse langattomassa lähiverkon topologiassa, sekä laitevalinnoissa, jotka ovat tehty perustuen yrityksen omiin tarpeisiin kuitenkin huomioiden myös verkon skaalautuvuuden, jonka vuoksi yrityksen ei tarvitse tehdä lisäinvestointeja heidän laajentuessa yrityksenä. Laitteiden investointikulut ja niistä laskettava hyötysuhde käytiin läpi toimeksiantajan kanssa. Langattoman verkon tietoturvallisuudesta on huolehdittu palomuurin mesh VPN-yhteyksien, verkkojen salauksien, sekä käyttäjien että verkonkäytön hallinnan osalta. Huomioituina on esimerkiksi, ettei yrityksen omaa verkkotunnusta ole saatavilla muille kuin työntekijöille vaan heidän yksityisyytensä säilyy koskemattomana. Langaton lähiverkko kattaa kuitenkin vierasverkon, joka on saatavilla yrityksessä vieraileville. Lisäksi yrityksen tiloihin asennetut valvontakamerat tuovat yritykselle lisää turvallisuutta, kun voidaan nähdä reaaliajassa tapahtuvat liikkeet. Valvontakameroiden live-kuvaa voidaan seurata päätelaitteilla mistä vaan VPN-yhteyden ansiosta.

Yrityksen lähiverkko yksinkertaistuu huomattavasti Merakin laitteiden ja niiden valvonnan myötä, kun tarkka statistiikka verkossa tapahtuvasta

liikennöinnistä on saatavilla. Uudesta lähiverkosta on myös suuri hyöty yrityksen toiminnan kannalta, kun huomioidaan että päätelaitteiden yhteydet verkossa ovat kahdennettuja lisäten vikasietoisuutta. Työpisteiden verkkokorteille asetetun prioriteetin vuoksi langaton yhteys on ensisijaisesti käytössä myös työpisteillä. Langattoman yhteyden estyessä langallinen yhteys on myös saatavilla toimipisteillä.

Työ oli haastavampi suorittaa ilman fyysistä laitteistoa, mutta toimiva lähiverkko saatiin kuitenkin suunniteltua. Suunnittelutyö esiteltiin toimeksiantajalle ja he olivat tyytyväisiä työn vastatessa heidän vaatimuksiansa ja tarpeita. Lopputulos olisi voinut olla mielestäni parempi koska verkon datankeruusta tai toiminnallisuudesta ei ollut mitään muuta näytettävää kuin topologia, jolla verkko oli rakennettu. Opinnäytetyö kuitenkin opetti minua ymmärtämään enemmän lähiverkkojen suunnitteluun liittyvistä asioista sekä käyttäjän että palveluntarjoajan näkökulmasta. Johdonmukaisuus, selkeä visio ja teoriaan pohjautuva lähestymistapa helpottivat verkon toteuttamista.

LÄHTEET

Arubanetworks, (2020) *SD-WAN havainnollistettuna*. Haettu 21.8.2020 osoitteesta https://www.arubanetworks.com/products/networking/sd-wan/

Ccexpert, (n.d.) *Langattomien lähiverkkojen topologiat*. Haettu 3.9.2020 osoitteesta https://www.ccexpert.us/root-bridge/wlan-building-blocks.html

Cisco, (n.d.) *VPN-ratkaisuja*. Haettu 20.8.2020 osoitteesta https://en.ppt-online.org/459547

Cisco Systems, (n.d.) *VPN by Cisco*, Inc. Haettu 20.8.2020 osoitteesta https://www.cisco.com/c/m/en_za/solutions/vpn.html

Constine. J. (2020) *Cisco acquires enterprise Wi-Fi Startup Meraki*. Haettu 24.8.2020 osoitteesta https://techcrunch.com/2012/11/18/cisco-acquires-enterprise-wi-fi-startup-meraki-for-1-2-billion-in-cash/

Capano. D, (2014) *MIMO-tekniikka*. Haettu 11.7.2017 osoitteesta https://www.controleng.com/articles/mimo-and-spatial-multiplexing/

Dustin Finland, (n.d.) *IT-ympäristön tilannekuva helposti Cisco Merakilla*. Haettu 25.8.2020 osoitteesta https://www.itewiki.fi/p/it-ymparistön-tilannekuva-helposti-cisco-merakilla

Elisa Oyj, (n.d.) *Eilisisen teknologialla ei voi ratkaista huomisen haasteita*. Haettu 27.8.2020 osoitteesta https://yrityksille.elisa.fi/tietoverkot

Hardware Texpert, (2011) *Laitepohjainen sekä ohjelmistopohjainen palomuuri*. Haettu 20.8.2020 osoitteesta http://hardwaretexpert.blogspot.com/2011/01/hardware-firewall.html

Internetopas, (n.d.) *Palomuurit*. Haettu 19.8.2020 osoitteesta http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/

DeLisle. J-J, (2015) *802.11-standardeja*. Haettu 2.9.2020 osoitteesta https://www.mwrf.com/technologies/active-components/article/21846205/whats-the-difference-between-ieee-80211af-and-80211ah

Johnson. A. (2020) *Wireless encryption protocols*. Haettu 20.8.2020 osoitteesta https://www.ciscopress.com/articles/article.asp?p=2999384&seqNum=6

Kauppi. J. (2019) *Pilvipalveluiden tietoturva, sekä haitat ja hyödyt*. Verkkoartikkeli. Haettu 20.8.2020 osoitteesta https://www.leijonasecurity.fi/2019/09/18/pilven-tietoturva-hyodyt-ja-haitat/

Lavanko. H. (2018) *Pilvipalvelut*. Verkkoartikkeli. Haettu 20.8.2020. osoitteesta https://blogi.valtti.com/multicloud-hybridipilvi-erot

Liveaction, (2020) *Logical link control*. Haettu 18.8. 2020 osoitteesta https://www.liveaction.com/docs/glossary/llc-ieee-802-2-logical-link-control/

Lundberg. J. (2018) *Vastuu tietoturvasta jakautuu pilvessä useille harteille*. Haettu 26.8.2020 osoitteesta https://www.talouselama.fi/kumppaniblogit/f-secure-oyj/vastuu-tietoturvasta-jakautuu-pilvessa-useille-harteille/bacd8a37-12c2-355b-9411-145894a3a8b9

E-tutes, (2019) *The Intranet VPN*. Haettu 20.8.2020 osoitteesta https://e-tutes.com/lesson12/the-intranet-vpn/

Media.techtarget, (n.d.) *Physical layer sublayers PLCP and PMD overview*. Verkkodokumentti. Haettu 18.8.2020 osoitteesta http://media.techtarget.com/searchMobileComputing/downloads/CWAP_ch8.pdf

Meraki, (n.d.) *Meraki-pilven arkkitehtuuri*. Haettu 20.8.2020 osoitteesta https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Architecture

Metis, (2018) *WPA3 eli uusin Wi-Fi Protected Access*. Haettu 3.9.2020 osoitteesta https://metis.fi/fi/2018/09/wpa3-fi/

MiCore Solutions, (2016). *Yleisimmät pilvipalveluarkkitehtuurit*. Haettu 20.8.2020 osoitteesta https://micoresolutions.com/hybrid-cloud-approach-best-approach-cloud/

Microsoft, (n.d.) *The OSI Model's Seven Layers Defined and functions Explained*. Verkkoartikkeli. Haettu 18.7.2020 https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model

Netapp, (2020) *Hybrid cloud benefits*. Haettu 20.8.2020. osoitteesta https://www.netapp.com/us/info/what-is-hybrid-cloud.aspx

Schwartz. M. (2019) *History of communications. IEEEE communications Magazine*. Haettu 17.6.2020 osoitteesta https://www.eng.hawaii.edu/wp-content/uploads/2020/06/THE-ALOHANET-%E2%80%94-SURFING-FOR-WIRELESS-DATA.pdf

Stobing. C. (2017) *What is MU-MIMO, and Do I need it on my router?* Haettu 18.8.2020 osoitteesta https://www.howtogeek.com/242793/what-is-mu-mimo-and-do-i-need-it-on-my-router/

Studytonight (2020) *ISO/OSI Reference models*. Verkkoartikkeli. Haettu 18.8.2020 https://www.studytonight.com/computer-networks/osi-model-physical-layer

STUK, (2020) *Langaton lähiverkko*. Verkkoartikkeli. Haettu 17.6.2020 osoitteesta https://www.stuk.fi/aiheet/kodin-ja-toimiston-sateilevat-laitteet/langaton-lahiverkko

Uusitalo. T. (2018) *XaaS – Anything as a Service*. Haettu 21.8.2020 osoitteesta https://esseepankki.proakatemia.fi/xaas-anything-as-a-service/

Varshney. V. (2020) *Pilvipalvelumallien tarjonnan visualisointi*. Haettu 20.8.2020 osoitteesta https://medium.com/@vanshvarshney_/what-is-iaas-vs-saas-vs-paas-and-xaas-whats-the-difference-examples-cea-deee146e6

Weinberg. N. (2018.) *What is 802.11ax (Wi-Fi 6), and what will it mean for 802.11ac?* Haettu 18.8.2020 osoitteesta https://www.networkworld.com/article/3258807/what-is-80211ax-wi-fi-6-and-what-will-it-mean-for-80211ac.html

Wikipedia, (2020) *Cloud computing history*. Haettu 20.8.2020 osoitteesta https://en.wikipedia.org/wiki/Cloud_computing