TAMPEREEN
AMMATTIKORKEAKOULU

PILVIHALLITTAVAT TIETOVERKOT JA CISCO MERAKI

Eero Mäensivu

Opinnäytetyö
Joulukuu 2017
Tieto- ja viestintätekniikka
Tietoliikennetekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

MÄENSIVU EERO:
Pilvihallittavat tietoverkot ja Cisco Meraki

Opinnäytetyö 62 sivua, joista liitteitä 3 sivua
Joulukuu 2017

Tässä opinnäytetyössä tutkittiin eri tietoteknisten pilvilaskenta- ja pilvipalveluiden markkinatilannetta, saatavilla olevia palvelumalleja sekä ennusteita niiden kehityksestä. Työssä keskityttiin tietoverkkojen palveluihin ja tuotteisiin, joiden tuottamisessa, käytössä sekä hallinnassa on osana hyödynnetty pilvipalveluita. Tavoitteena oli selvittää, millaisia palveluita on saatavilla yrityksille ja miten asiakkaat sekä palveluntarjoajat hyötyvät pilvipalveluiden käytöstä osana tuotteistusta.

Lopuksi työssä suoritettiin eri osa-alueilla pilvipalveluita hyödyntävän langattoman lähiverkkoympäristön käyttöönotto. Käyttöönotossa käytiin läpi eri vaiheet sekä toiminnallisuudet, mitä tulee ottaa huomioon pilvipalvelua hyödyntävän langattoman lähiverkkoympäristön käyttöönotossa. Luottamuksellisista syistä johtuen jotkin käyttöönottoprojektin yksityiskohdat ja yhteystiedot on jätetty pois tästä raportista.

Tutkimuksien tuloksina saatiin kattava näkemys yrityksien vaihtoehdoista hyödyntää pilvilaskentaa sekä pilvipalveluita osana nykyisiä tai täysin uusia järjestelmiä ja ratkaisuja. Näiden seurauksena saatiin myös käsitys siitä, miten ratkaisut mahdollistavat uutta liiketoimintaa, kasvua sekä nykyisten toimintojen tehokkuuden parantamista molemmin puolin palvelumallia. Tutkimustuloksien ja käyttöönottoprojektin tuloksena saatiin tieto ja ymmärrys pilvipalveluiden tuomista hyödyistä osana tietoverkkojen yksittäisien komponenttien sekä ympäristöjen konfigurointia ja hallintaa.

Opinnäytetyön tuloksien pohjalta tehtiin johtopäätöksiä pilvilaskennan ja pilvipalveluiden kasvavasta markkinaosuudesta ja miten niitä hyödyntävät tuotteet sekä palvelut tuottavat etua palveluntarjoajille, yrityksille sekä kuluttajille yli perinteisten ratkaisuiden. Tämän työn pohjalta suositeltuja jatkotutkimusaiheita ovat muun muassa täysin ohjelmistoperustaiset tietoverkkoratkaisut sekä pilvipalveluita hyödyntävät tietoturva- ja analytiikkaratkaisut.

Asiasanat: pilvihallittavat tietoverkot, Cisco Meraki, pilvipalvelut, etähallinta, pilvi

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

MÄENSIVU EERO:
Cloud Managed Networks and Cisco Meraki

Bachelor's thesis 62 pages, appendices 3 pages
December 2017

The purpose of this thesis was to explore the market situation and service models for various cloud computing services available and the predictions of their future development. The thesis focus is on network services and products that utilize cloud services as part of the creation, operation and management processes. The aim was to find out what services are available to companies and how customers and service providers benefit from the use of cloud services as a part of productization.

Later, a wireless local area network that utilizes cloud services in different areas of operation was deployed and configured. The deployment looked at various phases and features that should be considered when using a cloud-managed wireless network. For reasons of confidentiality, some deployment project and customer details have been omitted from this report.

Thesis results provided a comprehensive overview of the possibilities in utilizing cloud services as a part of existing or completely new systems and solutions. As a result, this thesis provides an understanding of how different solutions enable new business, growth and improved efficiency of existing operations on both sides of the service model. The deployment project provided knowledge and understanding of the benefits offered by cloud networking services as part of the configuration and management of individual components and network solutions.

Based on the results of the thesis, conclusions were drawn from the growing market share of cloud computing and cloud services, and how the products and services utilizing them provide benefits to service providers, businesses and consumers over traditional solutions. Further studies in the field of software-defined networking and the utilization of cloud services in information data security and data analytical solutions are highly recommended.

Key words: cloud managed networks, Cisco Meraki, cloud services, remote management, cloud

SISÄLLYS

ERITYISSANASTO

AMP	Advanced Malware Protection Edistynyt haittaohjelmasuojaus
BLE	Bluetooth Low Energy Matalan energiakulutuksen Bluetooth-teknologia
BYOD	Bring Your Own Devices Henkilökohtaisten mobiililaitteiden käyttö
GDPR	General Data Protection Regulation EU:n tietosuoja-asetus
IPS	Intrusion Prevention System Tunkeutumisen estojärjestelmä
SDN	Software Defined Networking Ohjelmistopohjainen tietoverkkojen määritteleminen
XAAS	Anything as a Service Määrittämättömän tietoteknisen toiminnallisuuden tuottaminen tai tarjoaminen pilvipalveluna

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on perehtyä ja tutkia eri tietoteknisten pilvilaskenta- ja pilvipalveluiden nykytilanteeseen, palvelumalleihin sekä tulevaisuuden näkymiin. Opinnäytetyö tarkentuu tietoverkkojen palveluihin, mitkä on tuotettu hyödyntäen pilvipalveluita, kuten verkkolaitevalmistaja Cisco ja heidän tuoteperhe nimeltä Meraki. Lopuksi työssä luodaan ja otetaan käyttöön langattoman lähiverkkoympäristön käyttäen Cisco Meraki -langatonta tukiasemaa ja tuotevalmistajan tarjoamaa pilvipalvelua.

Opinnäytetyön tavoitteena on tuottaa tekijälleen sekä lukijalleen tieto siitä, millaisia pilvilaskenta- ja pilvipalveluita on saatavilla yrityksille ja miten nämä tulevat jatkamaan kehittymistään kuluvan vuosikymmenen aikana. Tavoitteena on myös ymmärtää, miten nykyään saatavilla olevat palvelut ovat kehittyneet ja mitä toiminnollisuuksia ja palvelumalleja ne mahdollistavat sekä asiakkaille, että palveluntarjoajille. Opinnäytetyö antaa selvitystä siitä, miten ratkaisut mahdollistavat molemmille osapuolille uutta liiketoimintaa, kasvua sekä nykyisten toimintojen tehokkuuden lisäämistä.

Tutkimustuloksien saavuttamisessa käytettiin hyödyksi teknisiä artikkeleita, valmistajien dokumentointia, uutisartikkeleita sekä kirjoittajan omaavaa alan ammattiosaamista. Kirjoittaja on opinnäytetyötä kirjoittaessaan ollut alan työtehtävissä lähes viisi vuotta ja tekemisissä eri yrityksien verkko- ja järjestelmäinfrastruktuurien hallinta- ja ylläpitotehtävissä palveluntarjoajan roolissa.

2 TIETOTEKNIIKKA SIIRTYY PILVEEN

Termi pilvilaskenta (*Cloud Computing*) ja varsinkin tietotekniikasta puhuttaessa sana pilvi itsessään koetaan usein liittyvän tiedon säilyttämiseen tai jakamiseen Internetin ylitse. Kyseessä on kuitenkin markkinointinimike, eivätkä ne itsessään tarkoita vain yhtä tiettyä asiaa. Yksi määritelmä pilvilaskennalle on, että se on malli konfiguroitavien resurssien jakamiseen kaikkien saataville verkossa samalla minimoiden tarpeen hallinnalle sekä riippuvuuden kolmannen osapuolen toiminnasta (The NIST Definition of Cloud Computing 2011, 2)[1]

Pelkkää pilveä voidaan kuvailla edellisen perusteella joksikin kaukaiseksi asiaksi, mikä on saatavilla käyttäjilleen lähiverkon tai Internetin ylitse. Pilvilaskenta ja siihen liitännäiset palvelut taas kohdistuvat yksittäisten Internetin kautta saatavilla olevien palveluiden räätälöimiseen, määrittämiseen ja ylläpitoon.

Pilvilaskennan kenties erottavimmat tekijät muusta tietotekniikasta ovat sen skaalautuvuus yksittäisen käyttäjän ja asiakkaan tarpeisiin, saatavuus verkon välityksellä, resurssien jakaminen ja joustavuus tehokkaimmalla mahdollisella tavalla sekä valvonnan ja hallinnan keskittäminen ja yksinkertaistaminen. Nämä mahdollistavat uusia toimintamalleja ja säästöjä niin yksityisille henkilöille, kuin yrityksille ja palveluntarjoajille.

2.1 Pilven historiaa

Pilvilaskennan ja pilvipalveluiden alkuperää on vaikea määritellä, sillä termi itsessään on hyvin laajakäsitteinen. Pilvilaskenta ja pilvipalvelut ovat olleet mahdollisia siitä asti, kun Internetin pohjana toimiva TCP/IP-protokolla alun perin julkaistiin vuonna 1974 osana ARPANET-projektia. Vuotta myöhemmin suoritettiin ensimmäinen TCP/IP-protokollan yli tehty tiedon välitys Stanfordin yliopiston ja Lontoon University Collegen välillä.

[1] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (The NIST Definition of Cloud Computing 2011, 2).

Vuosien varrella TCP/IP-protokolla kehittyi, mutta vasta Internetin saapuessa 1990-luvulla alkoi myös uusien liiketoimintamallien ja mahdollisuuksien aikakausi. Internetin avulla pystyttiin lähettämään tietoa ympäri maapallon ja julkiset palvelut olivat kaikkien saatavilla. Vuosituhannen vaihteessa yritykset ja palveluntarjoajat havahtuivat Internetin tuomaan mahdollisuuksiin markkinoinnissa ja palveluiden tarjonnassa, josta myös lähti käyntiin pilvilaskennan ja pilvipalveluiden tulevaisuus.

Vuonna 2002 Amazon julkaisi Amazon Web Services -palvelunsa, joka tarjosi käyttäjilleen pilvipalveluita tallennustilan, laskentatehon ja jopa tekoälyn muodossa. Amazonin tarjoamassa palveluissa tapahtui suuri harppaus vuonna 2006, kun uuden tuotteen myötä myös pienyrityksillä ja yksityishenkilöillä oli mahdollisuus vuokrata resursseja Amazonin omilta palvelimilta ja palvelinkeskuksista pilvilaskentaan, palveluiden tarjoamiseen tai vain datan säilytystarpeisiin. Pian tämän jälkeen myös muut suuret toimijat kuten Google, IBM ja Microsoft ottivat askeleen kohti sitä, mikä nykyään tunnetaan pilvenä.

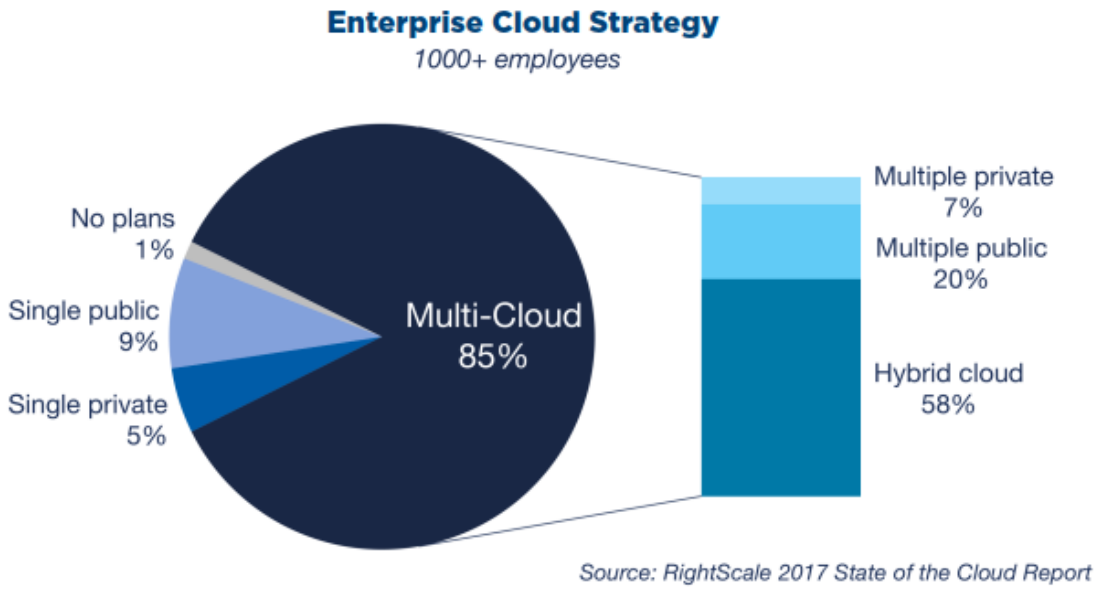
2.2 Pilvi liiketoiminnan apuna

Pilvilaskennan ja pilvipalveluiden kehitys ei näy vain yksityishenkilöille lisääntyneiden palveluiden muodossa, vaan se on myös tärkeä mahdollisuus yrityksille ja palveluntarjoajille kasvaa, parantaa liiketoimintaa ja luoda säästöjä. Vielä vuonna 2010, yrityksien tietotekniikan eli tuttavallisemmin IT:n tehtävänä oli tukea yrityksen toimintoja ja auttaa yksittäisten päätöksien tekemisessä. Nykyään IT nähdään osana yrityksen strategiaa ja yrityksen päätökset ovat riippuvaisia IT:n joustavuudesta tehtyjen päätöksien tukemiseen ja automaatioon (Zhao 2013, 4).

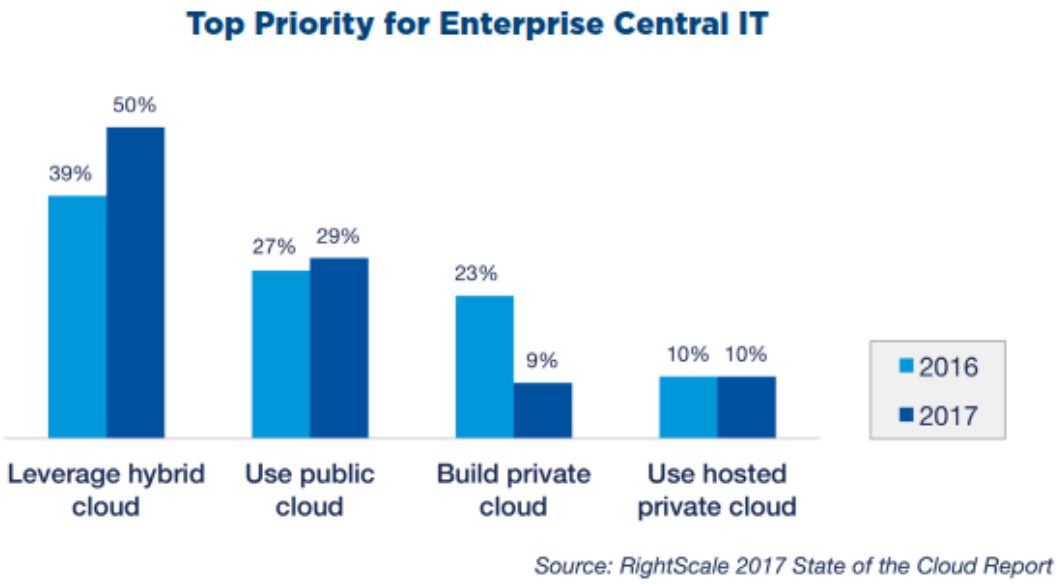
Sama murros on nähtävissä myös yrityksien verkko- ja järjestelmäinfrastruktuureissa. Yritykset siirtyvät omista palvelinkeskuksista kolmannen osapuolen tarjoamiin palveluihin ja laitteistohankinnat vaihtuvat käyttöpohjaiseen sekä jatkuvaan laskutukseen isojen kertamaksujen sijasta. Asiakkaan eli yrityksien ja yksityishenkilöiden etuna ovat käyttöönoton helpottuminen, kertakustannuksien poistuminen sekä palvelun joustavuus ja laajennusmahdollisuudet. Samalla palveluntarjoajat hyötyvät pitkäkestoisista asiakassuhteista, jatkuvasta rahavirrasta sekä palvelinlaitteiston virtualisoinnin tuomista hyödyistä.

Yrityksien siirtyminen pilvipohjaisiin palveluihin ja liiketoiminnan malleihin on ollut käynnissä jo useamman vuoden ajan. Ennusteiden mukaan vuoteen 2018 mennessä 60 prosenttia yrityksien IT-työkuormasta on siirretty pilveen ja 85 prosenttia yrityksistä hyödyntää useampia eri pilvipalveluita (Forbes 2017). Myös yhä useampi yritys siirtyy täysin pilvipohjaisiin ratkaisuihin, oli kyseessä sitten julkinen tai yksityinen pilvipalvelu.

Tätä väitettä tukee myös RightScalen vuosina 2016 sekä 2017 teettämän tutkimus pilvipalveluiden käytöstä yrityksissä, sillä vuonna 2017 58 prosenttia yrityksistä hyödynsi hybridipilviratkaisua ja 85 prosenttia hyödynsi useampaa eri pilvipalvelua (kuvio 1). Kuviosta 2 ja 3 nähdään yrityksien lisäävän sekä hybridi-, että julkisten pilvipalveluiden käyttöä ja keskimääräisesti yritykset hyödyntävät kolmea tai neljää eri pilvipalvelua. (State of the Cloud Report 2017, 10–11).



KUVIO 1: Pilvipalveluita hyödyntävien yrityksen määrä vuonna 2017



KUVIO 2: Yrityksien hyödyntämät pilviratkaisut vuonna 2017

# of Clouds Used	Public Clouds *All respondents*	Private Clouds *All respondents*
Running applications	1.8	2.3
Experimenting	1.8	2.1
Total	**3.6**	**4.4**

Source: RightScale 2017 State of the Cloud Report

KUVIO 3: Yrityksien hyödyntämien pilvipalveluiden lukumäärä

3 PILVIPALVELUT

Pilvipalvelut voidaan jakaa eri kriteerien avuilla luokkiin. Arkkitehtuurisesta näkökulmasta pilvipalvelut voidaan jakaa kolmeen pääryhmään: yksityiseen, julkiseen tai näiden kahden risteymäksi, jota kutsutaan hybridipilveksi. Lisäksi pilvipalvelut voidaan jakaa eri palvelumalleihin riippuen mitä toiminnallisuutta kunkin pilvipalvelun avulla tuotetaan sen käyttäjille.

3.1 Arkkitehtuurit

Yksityiset pilvipalvelut ovat pelkästään yhden tahon, yleensä yrityksen sisäiseen käyttöön tarkoitettuja palveluita. Yksityiset palvelut tarjoavat hyvän tietoturvan ja hallintamahdollisuudet, sillä palvelun saatavuus on rajattu joko yksityisen verkon sisälle eikä ole täten käytettävissä julkisen Internetin ylitse tai sen käyttämät resurssit on rajattu yhdelle ainoalle asiakasyritykselle. Palvelun ei tarvitse toimia yrityksen itse omistamalla palvelimella sen omissa tiloissa, vaan yksityinen pilvipalvelu voidaan tuottaa myös kolmannen osapuolen tarjoamana. Yksityisen pilven vaatimuksena ja haittana on kuitenkin se, että palveluntarjoajan tarjoamat ohjelmistot ja infrastruktuuri eli laitteisto ovat maksullisia ja näistä aiheutuu kustannuksia myös asiakkaalle.

Julkiset pilvipalvelut ovat nimensä mukaisesti julkisia ja ne ovat kaikkien saatavilla Internetin ylitse. Palveluntarjoajan vastuulla on ylläpitää tarvittavaa infrastruktuuria ja ohjelmistoja palvelun tuottamiseksi, jolloin palveluntarjoaja omistaa myös tarvittavan laitteiston, ohjelmistolisenssit ja palvelut omassa palvelinkeskuksessaan. Julkinen palvelu mahdollistaa korkean käyttöasteen laitteistolle, mikä taas itsessään laskee palvelun kustannuksia käyttäjille ja asiakkaille.

Julkiset pilvipalvelut ovat otollisia sellaisiin käyttötarkoituksiin, missä käyttäjiä on paljon eikä tyypillinen työkuorma ole raskas. Sähköpostipalvelut kuten Office 365, Google Mail ja Microsoft Outlook ovat tällaisia palveluita. Julkisen pilven ongelmaksi yrityksissä koostuukin tietoturvan ja hallinnolliset ongelmat, sillä palvelut ovat alttiita hyökkäyksille ja täten vaativat palveluntarjoajalta aktiivista tietoturvan edistämistä.

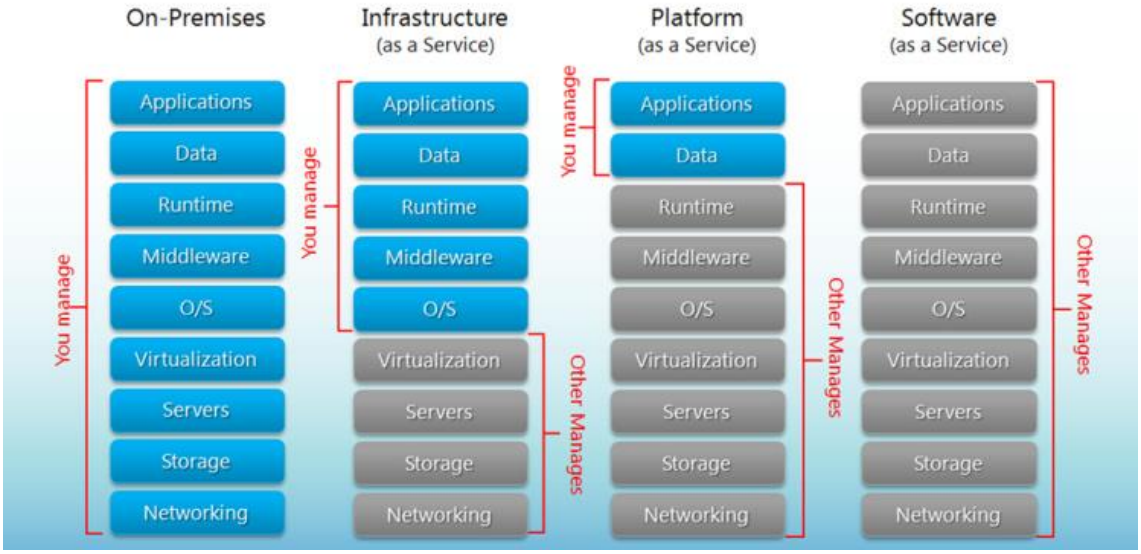
Hybridipilvipalvelut ovat näiden kahden välimaastosta. Yksityisissä ja julkisissa pilvipalveluissa on molemmissa hyötyjä sekä haittoja, mutta nykyään näiden kahden eroavaisuudet ovat sumentumassa kiitos hybridipilven. Käytännössä hybridipilvi on termi sekä yksityisten, että julkisten pilvipalveluiden yhtäaikaiselle käyttämiselle yhdessä ympäristössä. Hybridiratkaisut ovat suosittuja, sillä monen yrityksen siirtyminen pilvipalveluihin tapahtuu hitaasti ja usean vuoden aikajänteellä. Tällöin yrityksellä on käytössään sekä paikallisia resursseja omilla palvelimillaan, että pilvipalveluita eri palveluntarjoajilta.

Hybridipilven tavoitteena onkin yhdistää palveluita eri arkkitehtuurimalleista ja luoda yhtenäinen, automatisoitu ja hallittava ympäristö (Huwitz, Kaufman, Halper & Kirsch n.d.). Pelkkä julkisten ja yksityisten pilvipalveluiden olemassaolo ei kuitenkaan vielä luo järjestelmästä hybridipilveä. Hybridiratkaisulla tarkoitetaan myös näiden molempien palvelutyyppien hyödyntämistä yrityksen prosesseissa siten, että yrityksen resurssit ja data ovat käytettävissä sulavasti läpi palveluiden ja täten lisäten yrityksen toiminnallisuutta.

3.2 Palvelumallit

Pilvipalveluiden palvelumallit koostuvat kolmesta pääryhmästä: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) sekä SaaS (Software as a Service). Näiden kolmen kategorian lisäksi on yleistymässä eri palvelumalleille oleva yleisnimitys XaaS (Anything as a Service), joka viittaa melkein minkä vain verkko- ja järjestelmäinfrastruktuurin osa-alueen tuottamiseen palveluna. Kuviossa 4 on kuvattu eri palvelumallien eroavaisuudet

ja miten ne vertautuvat perinteisen IT:n eli yrityksen itse ylläpitämään palvelinympäristöön ja sen päälle rakennettuihin palveluihin (Stamey 2017).



KUVIO 4: Palvelumallit pilvipalveluissa

IaaS eli infrastruktuuri palveluna, viittaa tilanteeseen missä yritys vuokraa palveluntarjoajalta palvelinresursseja kuten laskentakapasiteettia tai tallennustilaa. Tällöin yrityksen, eli asiakkaan vastuulle jää käyttöjärjestelmän, mahdollisten ohjelmistojen sekä itse datan luonti palvelun tuottamiseksi. IaaS valitaan yleensä silloin, kun yrityksen oma infrastruktuuri ei riitä ja yritys tarvitsee lyhytaikaista lisäkapasiteettia palveluidensa tuottamiseen. Esimerkki IaaS-palvelun käytöstä on esimerkiksi varmistuskapasiteetin kasvattaminen tai yrityksen varmuuskopioiden säilyttäminen pilvipalveluntarjoajien konesaleissa.

Verrattuna IaaS-palvelumalliin, PaaS tarjoaa hieman enemmän, vaikka se onkin käyttötarkoitukseltaan hyvin erilainen. PaaS on suunnattu varsinkin ohjelmistokehittäjille, jotka tarvitsevat resursseja uusien ohjelmistojen kehittämiseen ja testaukseen. Tällöin asiakkaan ei tarvitse huolehtia fyysisen laitteiston konfiguroinnista, vaan voi keskittyä käytettäviin ohjelmistoihin ja niiden kehitykseen. Webhotellit ovat hyvä esimerkki IaaS-palvelusta, missä palveluntarjoaja toimittaa tarvittavan infrastruktuurin sekä verkkoyhteydet ja asiakkaat voivat asentaa haluamansa toiminnallisuuden palveluntarjoajan ohjelmistokirjastosta.

SaaS on näistä kolmesta suosituin ja laajimmin käytössä oleva malli. Tässä mallissa asiakkaan vastuulle ei jää mikään hallinnollinen osa-alue, vaan asiakas voi keskittyä käyttämään palvelua kuten suunniteltu julkisen Internetin välityksellä. Useimmat julkiset verkkopalvelut kuten sähköposti- ja sosiaalisen median palvelut käyttävät tätä mallia. SaaS on yleinen myös yritysmaailmassa, sillä monet työajanseuranta, finanssi ja sopimuksienhallintajärjestelmät halutaan ostaa ulkopuoliselta palveluntarjoajalta. Hyvänä esimerkkinä SaaS-palveluista ovat Microsoftin tarjoamat julkiset sekä yksityiset pilvipalvelut, kuten julkisen Internetin ylitse käytettävä sähköposti- ja toimisto-ohjelmisto Microsoft Office 365.

Azure on Microsoftin tarjoama IaaS-malliin perustuva palvelu, joka tarjoaa asiakkailleen mahdollisuutta kasata, luoda ja hallita virtuaalikoneita ja eri toiminnollisuuksia Microsoftin palvelinkeskuksissa. Helpottaakseen käyttöönottoa, Microsoft tarjoaa myös esivalmiita malleja virtuaalikoneille, jolloin samainen IaaS palvelu toimii myös PaaS-mallin mukaisesti.

XaaS on uusin pilvipalveluiden palvelumalleissa ja nimensä mukaisesti sillä ei rajata palvelua vain tietyn osa-alueen konseptiksi, vaan enemmänkin kokonaisuuden hahmottamiseksi. XaaS tarjoaa lukemattomia mahdollisuuksia, minkä ansiosta yrityksien ja asiakkaiden on mahdollista räätälöidä palvelu juuri heidän tarpeitaan varten. Ja kun yritykselle sopivan ratkaisun toteutus voidaan toteuttaa hybridipilvenä käyttäen kaikkia eri palvelumalleja, XaaS tuo mukanaan mittavan mahdollisuuden kustannuksien pienentämiseen. (Hegde 2017).

3.3 Kaupallinen tarjonta

Pilvipalveluiden kaupallisia tarjoajia on lukuisia ja palveluita on saatavilla kaikkiin mahdollisiin tarpeisiin. Kaksi esimerkkiä tällaisista ovat Microsoftin Azure sekä Amazonin Web Services. Molemmat tarjoavat sekä valmiita pilvipalveluita, että asiakkaiden räätälöitävissä olevia resursseja eri palvelumallein. Sekä Microsoftin, että Amazonin palvelu on suunnattu enimmäkseen yritysasiakkaille, mutta myös kuluttajilla on mahdollisuus hyödyntää samoja palveluja.

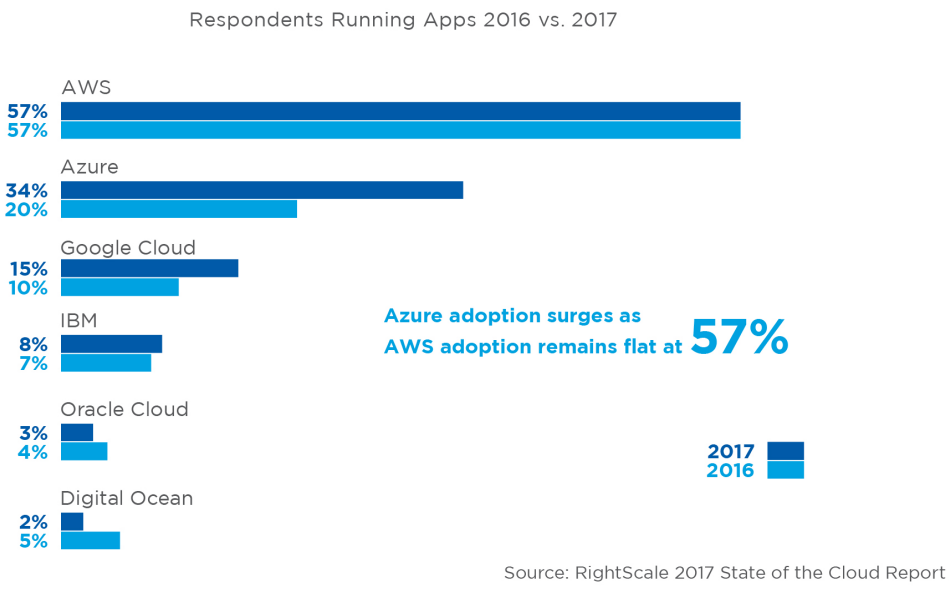
Azure on Microsoftin vuonna 2010 lanseeraama pilvipalveluiden ekosysteemi, joka on tähän mennessä kasvattanut tarjontaansa ja suosiotaan ympäri maailmaa. Azuren tuotekanta kattaa niin yksittäiset resurssit kuten levytilaa ja prosessointitehoa aina kokonaisvaltaisiin infrastruktuuriratkaisuihin. Azure tarjoaa myös mahdollisuuden yrityksille yhdistää Azuren pilvipalvelut osaksi paikallisia resursseja ja palvelinympäristönsä infrastruktuuria.

Azuren käyttöönotto on tehty myös helpoksi nykyisille sekä uusille asiakkaille valmiiden tuotteiden ja arkkitehtuurien muodossa, mistä käyttäjät voivat valita haluamansa. Azuren tuotteita voi kustomoida vapaasti ja lopullisen tuotteen hinnoittelu riippuu käytettävistä resursseista. Azure-tilauksestaan on mahdollista myös sammuttaa esimerkiksi yksittäinen virtuaalipalvelin ja täten vapauttaa resursseja, jolloin myös niihin pohjautuneet kustannukset laskevat.

Microsoft Azure tarjoaa tällä hetkellä palveluita yhteensä 36 eri maantieteellisessä sijainnissa, joka laajenee jatkuvasti (Microsoft n.d.). Tämän ansiosta asiakkaat ja yritykset voivat hyödyntää paikallisia resursseja eri toimipisteiden palveluiden tuottamiseen. Azuren ja Microsoftin datakeskuksien saatavuus Kiinassa on myös suuri markkinahyöty, sillä tähän mennessä yrityksien toiminta ja Kiinan ulkopuolella olevien palveluiden käyttö on ollut ongelmallista Kiinan valtion ylläpitämien palomuurien ja Internet-liikenteen sensuroinnin johdosta.

Azure ja muiden samanlaisten pilvipalveluiden käyttö on ollut kasvussa jo useamman vuoden ajan. Kuviosta 5 nähdään, että vuoden 2016 alusta esimerkiksi Azuren käyttäjämäärä on kasvanut 14 prosenttia samalla, kun Azuren suurin kilpailija AWS (Amazon

Web Services) säilytti käyttäjämääränsä ennallaan (State of the Cloud Report 2017, 25–26).



KUVIO 5: Pilvipalveluiden markkinaosuus vuosina 2016 ja 2017

AWS on samankaltainen Microsoft Azuren kanssa, mutta siinä missä Azure julkaistiin vuonna 2010, AWS ehtinyt toimimaan markkinoilla jo neljän vuoden ajan. Amazonin datakeskuksia on tällä hetkellä saatavilla 16 eri maantieteellisessä sijainnissa (Amazon n.d.). Tämän ansiosta AWS on suositumpi yrityksien keskuudessa, kuin Microsoftin Azure.

4 TIETOVERKOT PILVESSÄ

Viimeisen vuosikymmenen aikana, pilvipalveluiden tulo ja yleistyminen on luonut uusia mahdollisuuksia ja konsepteja. Pilvi on muuttanut tapaa, miten toimimme verkossa ja mitä palveluita Internetin kautta on saatavilla niin yrityksille, kuin myös yksittäisille kuluttajille. Pilvipalveluiden taustalla ovat kuitenkin silti samat infrastruktuuriset komponentit kuin muissa palvelinympäristöissä.

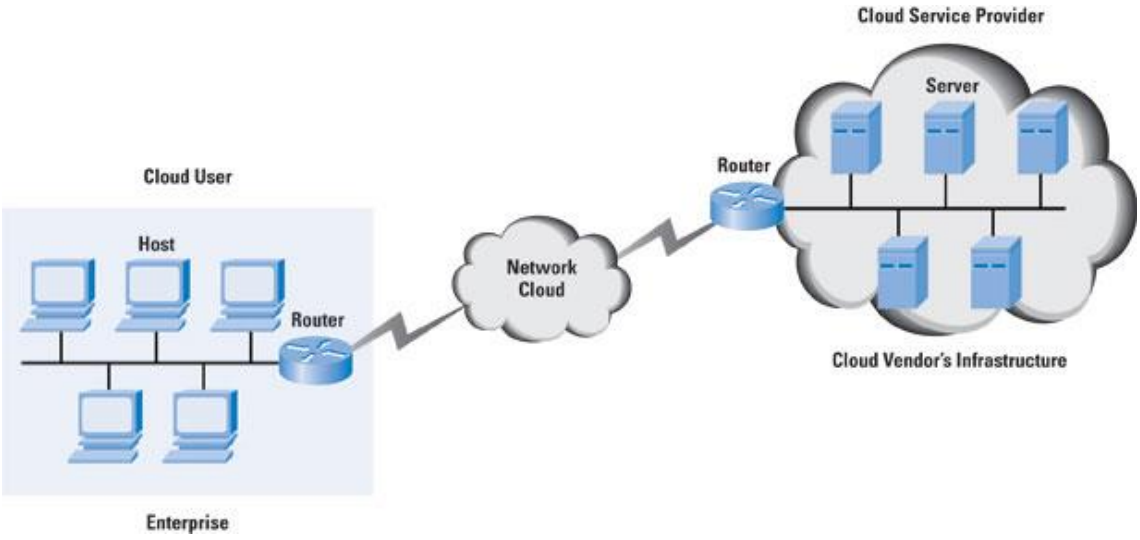
Pilvipalveluiden suosio ei johdu infrastruktuurin muutoksista, vaan palvelukonseptien parantamisesta ja uusien liiketoimintamallien kehityksestä. Näiden ansiosta pilvipalveluiden saatavuus, skaalautuvuus ja hallinta on parantunut samalla vähentäen kustannuksia. Tämä sama muutos on hiljalleen yleistymässä myös tietoverkoissa. Kyse ei ole suoraan Internetistä, vaan fyysisten tietoverkkojen ja -infrastruktuurien muuntamisessa kohti pilvipalveluiden ottamaa muotoa.

Tietoverkkojen siirtäminen pilveen (*Cloud Networking* tai *Cloud Based Networking*) pohjautuu samaan konseptiin, kuin pilvipalvelut. Käytettävissä olevat resurssit jaetaan asiakkaille ja yksittäisille käyttäjille, samalla parantaen resurssien käyttöastetta ja alentaen molempien osapuolien kustannuksia. Pilvipalveluina tuotetut tietoverkot tai pikemminkin pilviverkot, lainaavat tätä samaa periaatetta. Pilviverkoissa tätä noudattaen on nykyään mahdollista siirtää enemmän verkon hallinnollisia komponentteja pilveen, joka taas tarkoittaa pienempää määrää fyysisiä verkon laitteita tai asiakaspäätelaitteita.

Pilvipalveluiden hyödyntäminen tietoverkoissa yleistyi, kun yritykset kuten Aerohive Networks, Meraki ja Pareto Networks mahdollistivat suurien langattomien sisäverkkojen luomisen ja hallinnan keskitetysti käyttäen pilvipalveluita (Sdxcentral n.d.). Sittemmin, Aerohive Networks osti Pareto Networksin vuonna 2011 tuntemattomalla summalla (Wexler 2011) ja verkkolaitevalmistaja Cisco osti Merakin vuonna 2012 1,2 miljardilla dollarilla (Constine 2012).

4.1 Verkon hallinta

Tietoverkkojen hallinta pilvipalveluiden välityksellä on mahdollista myös parantuneen verkkoinfrastruktuurin ja verkkoyhteyksien ansiosta. Verkkoyhteyksien toimiessa luotettavammin sekä nopeammin kuin vuosikymmenen alussa, eri infrastruktuurin osa-alueiden siirtäminen verkkoon helpottui. Pilvipalveluiden yleistyessä ja yrityksien ohjelmistojen siirtyessä pilveen kysyntä pilviverkoille on lisääntynyt asiakkaiden ja yrityksien keskuudessa. Molemmat osapuolet kaipaavat helppoa ja tehokasta tapaa ylläpitää, luoda uusia sekä laajentaa nykyisiä verkkoympäristöjä. Kuvassa 1 on Ciscon hahmotelma pilviverkosta, jossa asiakkaan sisäverkon hallinta on toteutettu pilvipalveluna. Yksittäisiä asiakkaita voisi olla lähes rajaton määrä, joiden hallinta tapahtuu yhden pilvipalvelun kautta.



KUVA 1: Ciscon hahmotelma pilviverkosta

Pilviverkot tarjoavat keskitettyä hallintaa ja näkyvyyttä tietoverkkoihin, oli kyseessä sitten yksittäisen yritysasiakkaan sisäverkko tai maailmanlaajuisen yrityksen koko verkkoinfrastruktuuri ympäri maailman. Keskitetyn hallinnan kautta on mahdollista hallinnoida lähes kaikkia verkon osa-alueita mukaan lukien muttei rajoittuen palomuureihin, kytkimiin sekä langattoman verkon tukiasemiin.

Pilviverkkojen suurin hyöty tulee kuitenkin, kun siirrytään kohti suurempia ja monimutkaisempia verkkoympäristöjä. Usean toimipisteen ympäristön hallinta ja palveluiden toiminnan varmistaminen toimipisteiden välillä on haaste, jossa eri infrastruktuurin komponenttien ja laitteiden hallinta pilvipalveluna helpottaa ja vähentää järjestelmän ylläpitäjän

työkuormaa huomattavasti. Cisco illustroi tätä mahdollisuutta Meraki-tuotesivullaan kuvan 2 avulla, jossa on hahmoteltu usean toimipisteen hallinta yhden käyttöliittymän ja pilvipalvelun taakse.

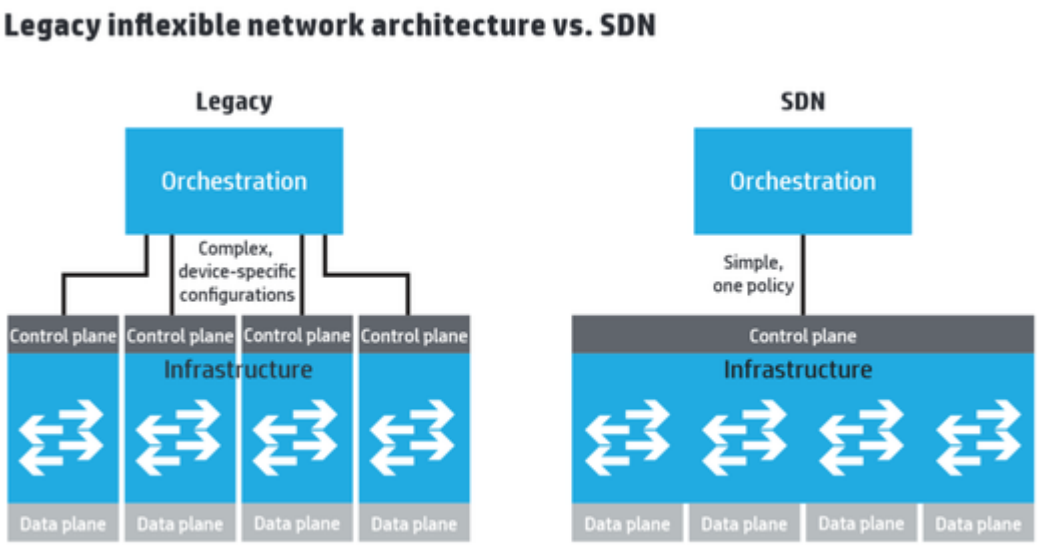
KUVA 2: Ciscon hahmotelma moniosaisen verkkoympäristön hallinnasta

Yksi suurimmista haasteista nykyajan tietoverkoissa löytyy usean toimipisteen yrityksissä. Haasteena on luoda ympäristö, missä käyttäjät ja infrastruktuurin eri osa-alueet voivat työskennellä ja kommunikoida saumattomasta toistensa kanssa. Perinteisen tietotekniikan järjestelmät palvelimien ja verkkolaitteiden osalta vaativat resursseja niiden suunnittelemiseen, käyttöönottoon, ylläpitoon sekä valvontaan.

Useat suuret yritykset omaavat nykyään toimipisteitä ja etätyöntekijöitä eri kaupungeissa sekä maissa, jotka kaikki tarvitsevat riittävät yhteydet yrityksen ohjelmistoihin ja tietoon. Yrityksien ulkoistaessa sisäisiä palveluita palveluntarjoajille ja siirtyessä pilvipalveluiden käyttäjiksi, täytyy verkko-operaattoreiden pystyä toimittamaan luotettavat ja kaistanleveydeltään riittävät verkkoyhteydet. Tämä vaatii verkko-operaattoreilta myös infrastruktuurien uusintaa ja tehostamista kustannuksien minimoiseksi. Tähän yhtenä vaihtoehtona on SDN (Software Defined Networking).

4.2 Software Defined Networking

SDN-teknologia on arkkitehtuuri, jonka keskeinen idea on verkon komponenttien määritys, hallinta ja resurssien jakaminen ohjelmallisesti. Se ottaa osan toiminnallisuudesta mikä on normaalisti toteutettu fyysisillä laitteilla kuten reitittimillä ja kytkimillä, ja sallii niiden hallinnan sekä konfiguroinnin dynaamisesti. Tuloksena on parempi ja tehokkaampi laajennettavuus verkolle, mikä taas heijastuu kustannussäästöinä ja joustavuutena yrityksen verkossa. (Nohling 2016). Kuvassa 3 on kuvattu ylläpitäjän hallinnollisesta näkökulmasta, miten SDN-arkkitehtuuriin pohjautuva verkkoympäristö vähentää ylläpitäjän vaatimaa työkuormaa eri komponenttien hallinnoimiseksi.



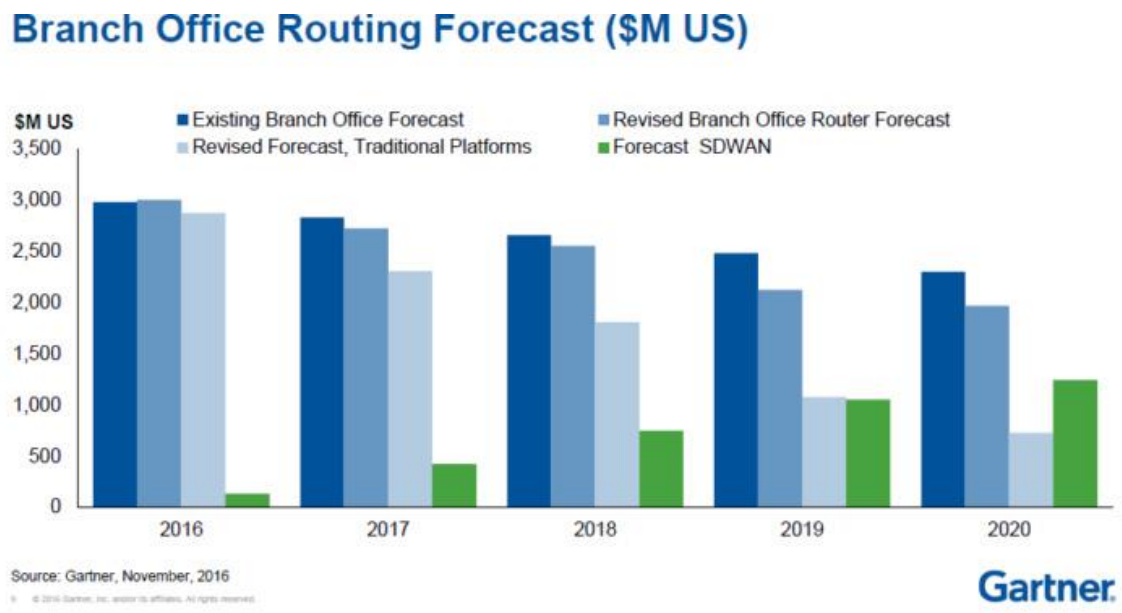
KUVA 3: Ero perinteisen verkkoarkkitehtuurin ja SDN-arkkitehtuurin hallinnassa

SDN tuo mahdollisuuksia verkon hallintaan, mutta tuo ensimmäisten joukossa myös koko verkkoympäristön ja arkkitehtuurin hallintaan sekä käyttöön joustavuutta. Jousto syntyy siitä, että verkon toiminnollisuuksia voidaan ottaa käyttöön tai poistaa verkon ohjelmistokerroksessa. Uusia toimintoja voidaan luoda ilman laitehankintoja, kun toiminnallisuus ei ole enää sidottu yksittäiseen laitteeseen tai komponenttiin. (Saarelainen 2016). Mikäli yrityksen verkkoinfrastruktuuri koostuu moderneista laitteistoista, ei yrityksen tarvitse edes tehdä uusia laiteinvestointeja hyödyntääkseen SDN-arkkitehtuurin tuomaa toiminnallisuutta ja mahdollisuuksia.

4.2.1 SD-WAN

SD-WAN (Software Defined Wide Area Network) osa SDN-arkkitehtuuria ja sen tavoitteena on optimoida verkon kytkeneisyyttä ja tehokkuutta. SD-WAN on optimoitu varsinkin yritysverkkojen yhdistämiseen, kuten etäisten toimipisteiden ja pääkonttorin verkkojen toiminnollisuuksien yhteen sulauttamiseen. Verkkoyhteyksien nopeutuessa SD-WAN tarjoaa myös palveluntarjoajille mahdollisuuden laajentaa tarjontaansa asiakkailleen erilaisten hallinnallisten tuotteiden muodossa.

SD-WAN on noussut verkko-operaattoreiden suosioon vuosien 2016 ja 2017 aikana ja Gartnerin vuonna 2016 julkaistujen arvioiden mukaan (kuvio 6) SD-WAN-teknologian markkinaosuus tulisi nousemaan 60 prosenttiin vuoteen 2020 mennessä, kun vuonna 2016 sen markkinaosuus oli vain 5 prosenttia (Garson & Greenfield 2016). Tämä kertoo siitä, että SD-WAN on teknologiana hyvin tuore ja samalla sen odotetaan syrjäyttävän perinteiset verkkoratkaisut hyvinkin nopeasti.

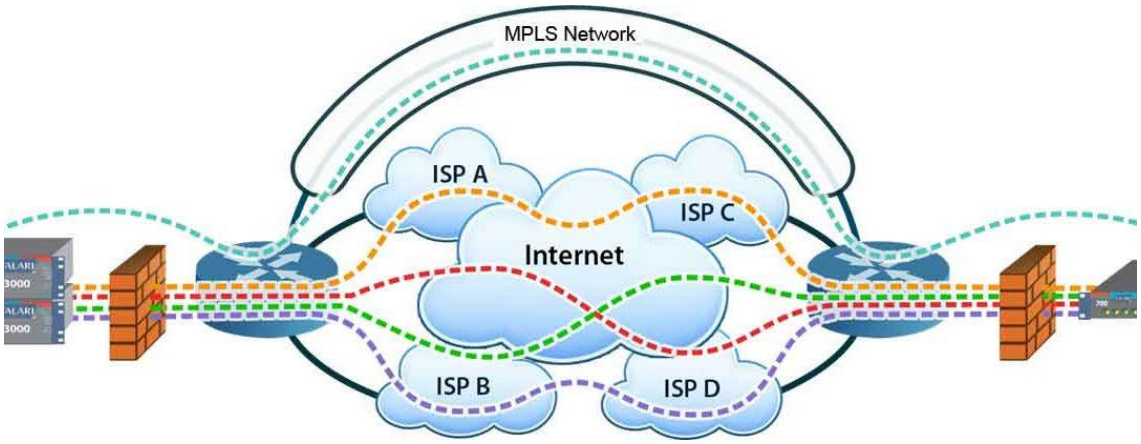


KUVIO 6: Tilastotietoa verkkoteknologioiden markkinaosuuksista ja niiden ennusteesta

Poiketen perinteisistä laajaverkkoyhteyksistä, missä tietoturva ja hallinta on toteutettu toimipistekohtaisesti, SD-WAN tarjoaa keskitetyn hallinnan ja loogiset yhteydet kaikille toimipisteiden reunalaitteille. Kyse ei ole kuitenkaan perinteisestä toimipisteiden välille luotavasta VPN-putkesta (Virtual Private Network), jossa putki luodaan olemassa olevan

verkkoyhteyden päälle. Sen sijaan, SD-WAN mahdollistaa VPN-putken luonnin useiden eri verkkoyhteyksien yli, jossa perinteinen ratkaisu vaatisi rinnakkaisten putkien konfiguroinnin.

SD-WAN osaa reitittää liikenteen eri yhteyksien ylitse ilman erillistä konfigurointia ja valitsee käytettävät yhteydet niiden nopeuden sekä luotettavuuden perusteella. Kuvassa 4 on kuvattu, miten SD-WAN voi hyödyntää neljää eri verkko-operaattorin yhteyttä yrityksen toimipisteiden välillä. Tämä tuo yrityksellä mahdollisuuden hyödyntää eri liittymiä, toimittajia ja teknologioita verkon toiminnallisuuden ja luotettavuuden varmistamiseksi. (Garson 2016).



KUVA 4: Hahmotelma, miten SD-WAN voi käyttää useita eri verkkoyhteyksiä

5 CISCO MERAKI

Meraki on Massachusettsin teknillisen korkeakoulun (MIT) opiskelijoiden Sanjit Biswasin, Josh Bicketin sekä Hans Robertsonin vuonna 2006 perustama yritys (Sequoia n.d.). Vuonna 2012 tämä 330 työntekijän yritys myytiin verkkolaitevalmistaja Ciscolle 1,2 miljardin dollarin hintaan. Vuonna 2012 Meraki tarjosi keskisuurille yritysasiakkailleen enimmäkseen langattomien lähiverkkojen ratkaisuja, joiden hallinta oli mahdollista käyttäen pilvipalveluna tuotettua keskitettyä hallintaa.

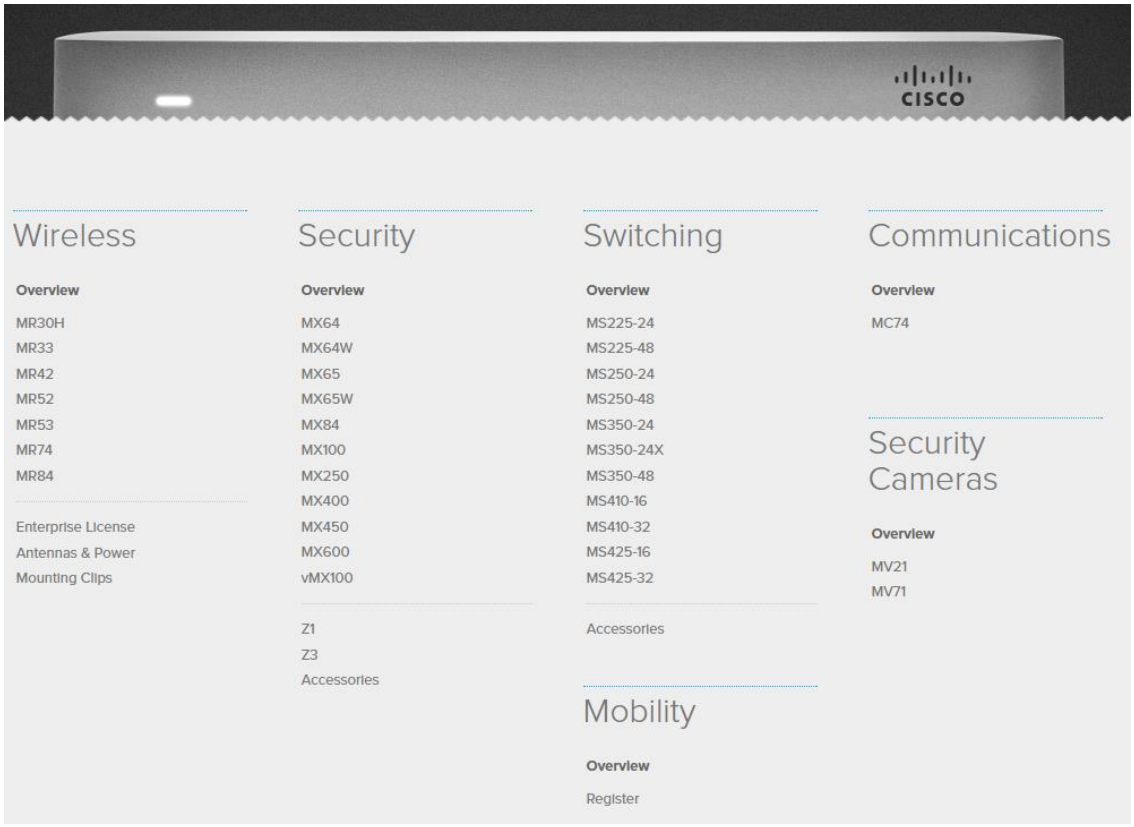
Nykyinen Cisco Meraki on yksi alan johtajista, mitä tulee pilvipalveluina hallittavien verkkotuotteiden tarjontaan. Cisco Merakilla on tällä hetkellä yli 230 000 asiakasta ja toimitettuja laitteita noin 3 miljoonaa kappaletta. (About Meraki n.d.). Cisco Merakin tuoteperhe on kasvanut vuosien varrella, sillä kun aikaisemmin yritys keskittyi vain langattomien lähiverkkojen toteutukseen, tarjoavat he nykyään myös kytkimiä, palomuureja, valvontakameroita sekä konferenssipuhelimia. Kaikkien näiden tuotteiden hallinta ja käyttöönotto ovat mahdollista käyttäen heidän webpohjaista pilvipalvelua.

Pilvipalveluiden etuja sekä mahdollisuuksia käsiteltiin aikaisemmissa kappaleissa, joten tässä osiossa perehdyn tarkemmin Cisco Merakin verkkoinfrastruktuurin tuotteisiin kuten langattomiin tukiasemiin, palomuureihin ja kytkimiin ja näiden eritysominaisuuksiin. Lisäksi tutkin, miten Cisco Merakin palvelun käyttöönotto onnistuu langattoman lähiverkon toteutuksessa.

5.1 Tuoteperhe ja pilvihallinta

Merakin ydinosaaminen on yrityksen perustamisesta lähtien ollut langattoman lähiverkon toteutuksessa ja tukiasemissa. Cisco Meraki tarjoaa kuitenkin kattavan valikoiman tuotteita yrityksien eri tarpeisiin. Kuvassa 5 on kuvakaappaus Cisco Merakin tuoterepertuaarista, jossa on listattuna Cisco Merakin tarjoamat langattoman lähiverkon MR-tukiasemat, MX-sarjan palomuurit sekä MS-sarjan kytkimet. Eri tuotteiden erot koostuvat lähinnä tarjottavasta kapasiteetista ja yrityksen tarpeellisiksi kokemista ominaisuuksista, joita käyn läpi myöhäisemmässä vaiheessa. Tässä opinnäytetyössä tutustun tarkemmin

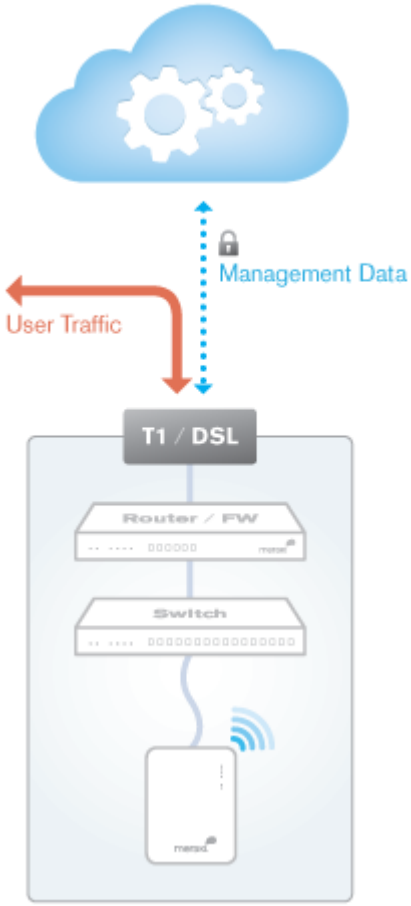
Cisco Meraki MR33 -tukiasemaan, mikä on Ciscon langattomien lähiverkkojen tukiasemista peruskäyttöön suunnattu malli.



KUVA 5: Kuvakaappaus Cisco Meraki tuoteperheestä kokonaisuudessaan

Kuten aikaisemmin mainittu, kaikki Cisco Merakin tuotteet ovat hallittavissa käyttäen samaa pilvipalveluna tarjottavaa webpohjaista hallintaa. Tämän kaltainen ratkaisu vaatii mittavan panostamisen palvelun tietoturvaan, sillä pahimmillaan palveluun tavalla tai toisella tunkeutunut henkilö voisi aiheuttaa mittavaa vahinkoa yritysasiakkaan verkolle tai yksityisen henkilön tietosuojalle. Tämän johdosta Cisco Merakin pilvihallinta on täysin eriytetty muusta yrityksen verkosta (kuvio 7).

Cisco Meraki kutsuu tätä hallinnan eriyttämistä nimellä OOB (Out-of-Band) eli muun liikenteen tavoittamattomissa olemiseksi. Tämän ansiosta Cisco Merakin palvelinkeskuksiin ohjautuu vain laitteiden hallinnointiin tarkoitettu liikenne, eikä esimerkiksi käyttäjien verkkoliikennedataa. Samaa reittiä käyttäen toteutetaan myös verkkolaitteiden automaattiset ohjelmistopäivitykset, jolloin laitteet ovat aina ajan tasalla ja tietoturvallisia. Mikäli laitteiden hallintaan tai Cisco Merakin pilvipalveluun tulisi vika, tämä ei aiheuttaisi käyttäjilleen ja asiakkailleen verkon käyttökatkoa, vaan yrityksen verkko toimisi edelleen normaalisti.



KUVIO 7: Cisco Merakin tuotteiden hallinnan ja käyttäjäliikenteen erotus

Cisco Meraki lupaa pilvipalvelulleen vähintään 99,99 prosentin palvelutason eli SLA-tason (Service Level Agreement), joka tarkoittaa palvelun saatavilla oloa kunakin ajankohtana (Cisco Meraki Service Level Agreement n.d.). Mikäli palveluntarjoaja ei kykenisi tarjoamaan palveluaan tason vaatimaa määrää, olisi asiakasyritys oikeutettu joko hyvitykseen palvelun hinnassa tai muuhun ennalta sovittuun korvaukseen. Palvelutasosopimukset ovat yksi pilvipalveluiden kriittinen sopimusasia, kun yritysasiakas on sellaista ottamassa käyttöön.

Cisco Meraki on valmistautunut myös tulevaan Euroopan unionin tietosuojalakiuudistukseen eli GDPR:ään (General Data Protection Regulation), jonka myötä kaikki Euroopan alueella olevien asiakkaiden pilvipalvelutoiminnot täytyy tuottaa, varmistaa ja säilyttää saman maanosan sisällä (EU Privacy and Data Protection Compliance n.d.). Cisco Merakin palvelinkeskukset ovat myös SAS70 type II ja SSAE16 sertifioitu, eli ne täyttävät viranomaisvaatimukset tietoturvallisuuden ja järjestelmien vähimmäisvaatimuksien suhteen (Cisco Meraki Datacenter Design n.d.).

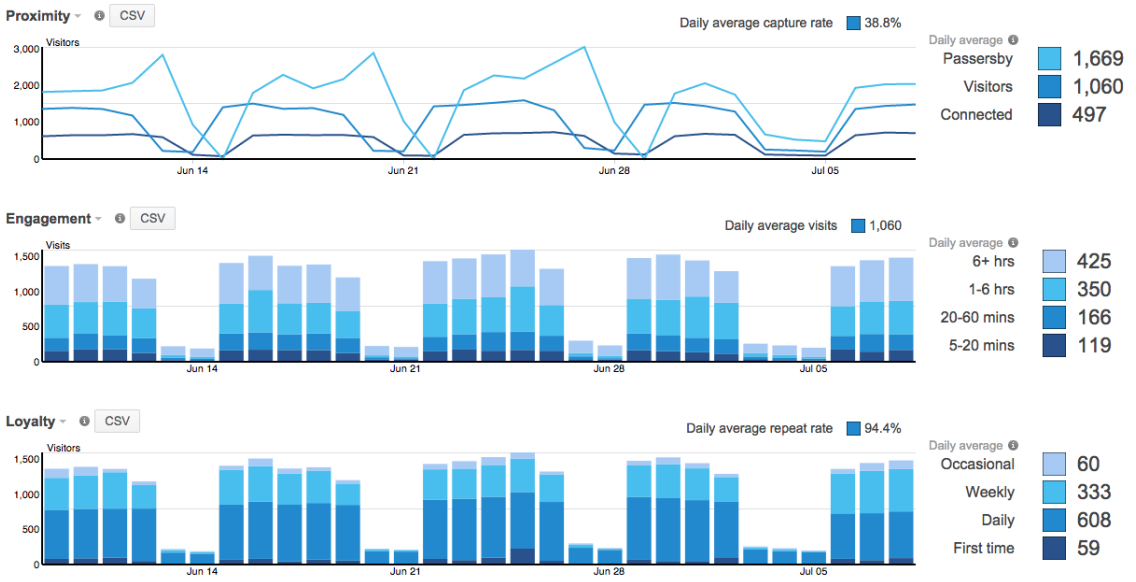
5.2 Langattomat lähiverkot

Cisco Merakin langattomien lähiverkkojen tukiasemat tarjoavat ominaisuuksia, joista osa on yleisiä langattomien verkkojen tukiasemissa ja osa yleistymässä nopeasti kiitos pilvipalveluiden. Itse tukiasemat ovat teknisiltä ominaisuuksiltaan normaaleja langattoman verkon tukiasemia. Ne tukevat IEEE 802.11ac -verkkostandardia (Institute of Electrical and Electronics Engineers) ja toimivat sekä 2,4 GHz, että 5 GHz taajuusalueilla. Cisco Merakin tukiasemien ominaisuudet ja hyödyt astuvat esiin vasta, kun siirrytään pilvihallinnan puolelle ja verkon liikennettä analysoidaan hyödyntäen Cisco Merakin palvelinkeskuksien resursseja ja tekoälyä.

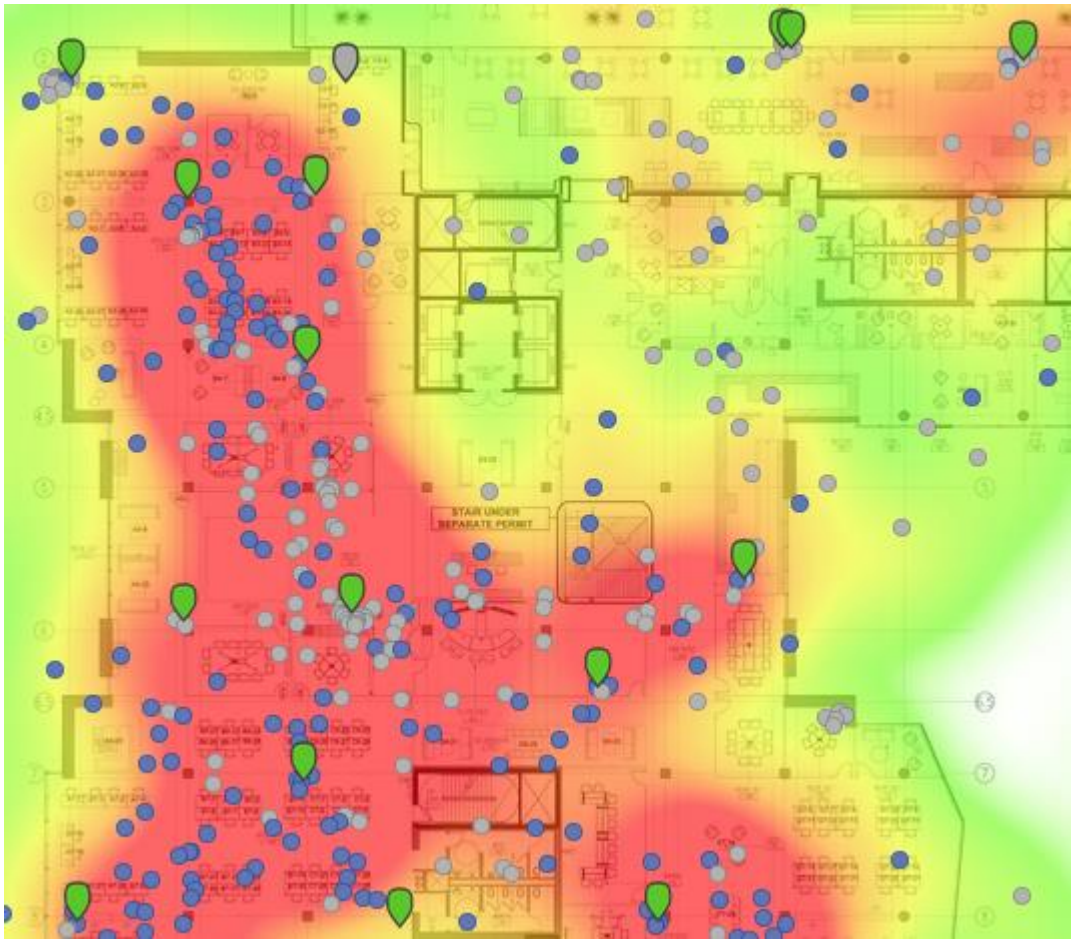
Ciscon tuotteita käyttäneille ei tule yllätyksenä, että kaikki Cisco Meraki -laitteet vaativat voimassaolevan ohjelmistolisenssin. Cisco Merakin tapauksessa jokainen tukiasema vaatii lisenssin, mutta hankitut lisenssit eivät ole sidottu yksittäiseen tukiasemaan tai tuotemalliin. Jos yrityksen ympäristössä on esimerkiksi käytössä viisi Meraki-tukiasemaa, tarvitaan näitä varten myös saman verran lisenssejä. Cisco Merakin lisenssihinnoitteluita ei ole saatavilla kuluttajille suoraan.

5.2.1 Paikka-analytiikka

Yksi tukiasemien isoista ominaisuuksista on Cisco Merakin kutsuma paikka-analytiikka (*Location Analytics*), jonka avulla verkon ylläpitäjä voi seurata verkon käyttöä ja käyttäjien käyttäytymistä verkossa. Muun muassa miten kauan käyttäjä viihtyy verkon käyttäjänä (kuva 5) ja missä verkon kuormitus on suurimmillaan (kuva 6). Kaikki Cisco Merakin tuotteilla mitattu analytiikka käsitellään ja analysoidaan yrityksen määrittämällä tavalla hyödyntäen Cisco Merakin palvelinkeskuksen resursseja ja tekoälyä.



KUVA 6: Kuvakaappaus paikka-analytiikan statistiikasta



KUVA 7: Kuvakaappaus verkon kuormituksesta kartalle piirrettynä

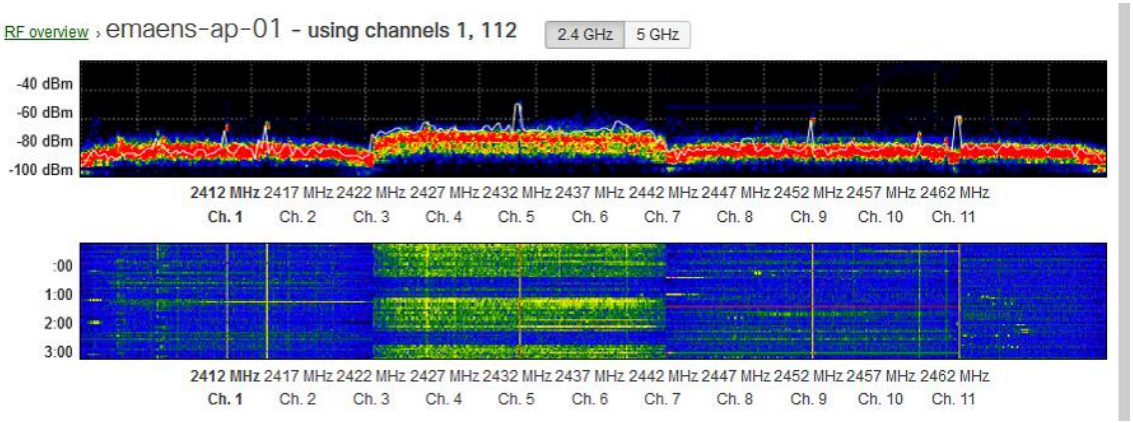
Toinen ominaisuus kaikissa Cisco Meraki -tukiasemissa on Bluetooth-teknologian käyttö. Tukiasemat kykenevät joko lähettämään Bluetooth-teknologian avulla paikkatietoa mobiililaitteille tai vaihtoehtoisesti kuuntelemaan saatavilla olevia Bluetooth-laitteita

ja paikantamaan esimerkiksi vähävirtaisia Bluetooth-majakoita (Bluetooth Low Energy Beacons) ja täten ohjeistamaan niiden käyttäjiä. Tämänkaltaiseen käyttöön toteutettuja projekteja on maailmalla muutamia, missä majakoita käytetään esimerkiksi opastamaan urheilukatsojia oikeille paikoilleen suurilla stadioneilla (Computerworld 2014).

5.2.2 Verkon laatu ja tietoturva

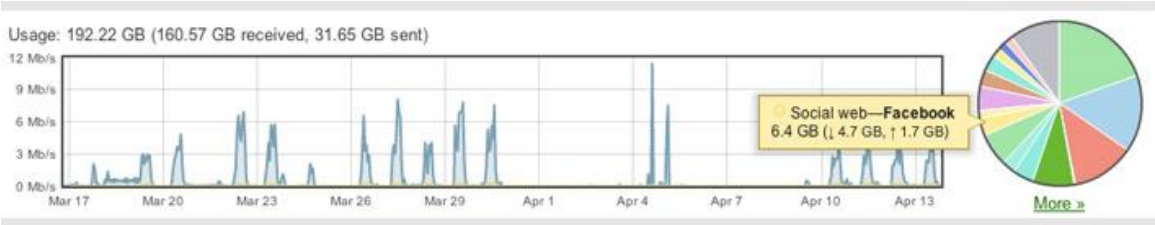
Cisco Merakin tukiasemat tarjoavat verkon laadun seurantaan ja parantamiseen useita uudempia työkaluja. Näitä ovat muun muassa verkkoliikenteen seurantaan omistettu vastaanotin, OSI-mallin (Open Systems Interconnection) tasolla seitsemän toimiva liikenteen analysoija sekä oma vastaanotin ulkopuolisten ja mahdollisesti haitallisten tukiasemien tunnistamiseen. Cisco Merakin hallintapalvelu tarjoaa myös omia ominaisuuksia verkon käytettävyyden parantamiseen, kuten integroidun tuen Bonjour-laitteille.

Verkkoliikenteen seurantaan omistettu vastaanotin mittaa ympäristöään jatkuvasti parantaakseen langattoman verkon tehokkuutta ja luotettavuutta. Spektrianalysaattorin kaltaisesti vastaanotin mittaa tukiaseman toiminta-alueella olevien toisten laitteiden lähettämien signaalien tehotasoja, kaistanleveyttä ja muita häiriölähteitä langattomien tukiasemien lisäksi. Mittaustulosten perusteella tukiaseman omia lähettimiä ohjataan ja säädetään parhaan mahdollisen tehokkuuden saamiseksi. Mittaustuloksista analysoidaan muun muassa niiden spektriä, kaistojen käyttöastetta ja tehoa kuten kuvassa 8. (Technologies: RF Optimization n.d.).



KUVA 8: Kuvakaappaus tukiaseman havainnoista lähiympäristössä

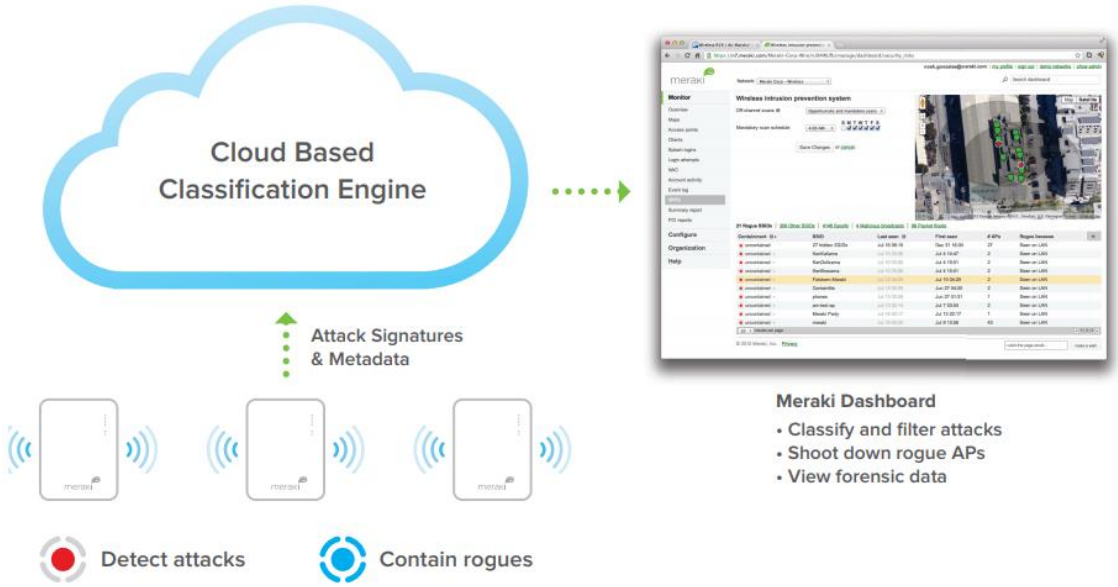
Tukiasemien liikennettä analysoidaan OSI-mallin tasolla seitsemän eli ohjelmistotasolla. Cisco Merakin analysointi ei jää vain IP-osoitteiden ja isäntänimien seurantaan, vaan järjestelmä tutkii ja tunnistaa liikennettä heuristisesti. Kuvassa 9 on kuvakaappaus Cisco Merakin tukiaseman kautta kulkeneesta liikenteestä, josta esimerkkinä on korostettu Facebookiin yhdistetty liikenne viimeisen kuukauden aikana. (Technologies: Application QoS n.d.).



KUVA 9: Kuvakaappaus tukiaseman verkkoliikenteen statistiikasta

Koska liikenteen analysoinnin avulla voidaan saada selville ja yksilöityä yleisiin palveluihin suuntautuva liikenne, on siihen kohdistuvien rajoituksien tai erinäisten sääntöjen määritteleminen mahdollista. Esimerkiksi VoIP-liikenteen (Voice over IP) priorisointi on mahdollista yli normaalin verkko- tai P2P-liikenten (Peer to Peer) allokoimalla sille enemmän käytettävissä olevaa kaistanleveyttä.

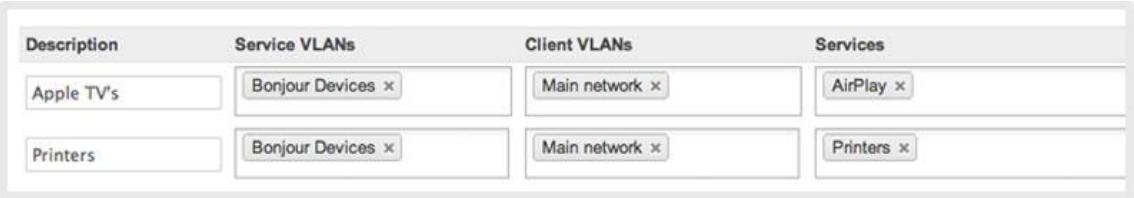
Cisco Merakin tukiasemissa on myös mukana omaisuus nimeltä Air Marshal, joka on heidän oma langattomien verkkojen tunkeutumisenestoratkaisu WIPS (Wireless Intrusion Prevention System). Tätä varten tukiasemissa on oma sille omistettu vastaanotin mikä kuuntelee ympäristöään ja tekee toimenpiteitä, mikäli se tunnistaa aktiivisen hyökkäyksen verkkoa kohtaan. Järjestelmä kykenee tunnistamaan muun muassa haitallisia ja väärennettyjä tukiasemia, lähiverkon tunnuksia eli SSID-tunnisteita (Service Set Identifier) ja datapakettitulvia esimerkiksi tukiasemiin kohdistuvan palvelunestohyökkäyksen eli DoS:n (Denial of Service) aikana. Uhkien tunnistaminen on mahdollista hyödyntäen Cisco Merakin palvelinkeskuksen resursseja ja pilvihallintaa, jonka toiminnallisuutta on kuvattu kuvassa 10. (Air Marshal n.d.).



KUVA 10: Cisco Meraki ja Air Marshalin toiminta uhkien tunnistamisessa

Tukiasemien hallinnassa on myös integroitu toiminnallisuus Bonjour-laitteiden hallintaan. Bonjour on Applen vuonna 2002 alun perin julkaisema protokolla erinäisten verkkolaitteiden kuten tulostimien ja muiden tietokoneiden löytämiseen verkossa ilman erillistä konfigurointia. Tähän mennessä normaalisti yritysverkoissa Bonjour-protokollan salliminen vaatii erillistä konfigurointia kaikille verkon laitteille, minkä kautta Bonjour-liikennettä halutaan siirtää. Bonjour-protokollan käyttöönottaminen langattomassa verkossa vaatisi siten konfigurointia langattoman verkon kontrollerille sekä kaikille tukiasemien ja muiden verkkolaitteiden välisille kytkimille.

Cisco Meraki -tukiasemissa tuki Bonjour-laitteille on suoraan integroituna ja sen käyttöönotto on tehtävissä helposti pilvihallinnan kautta. Olettamus kuitenkin on, ettei tukiaseman ja muiden verkkolaitteiden välissä ole laitteita, jotka vaatisivat tämän tuen käsin konfigurointia. Pilvihallinnan kautta on myös helposti hallittavissa, mitä Bonjour-tuen omistavia laitteita verkossa halutaan sallia. Esimerkiksi Applen AirPlay, AirPrint tai AFP (Apple Filing Protocol) voidaan sallia erikseen halutuille aliverkoille. Kuvassa 11 on kuvakaappaus pilvihallinnan käyttöliittymästä tällaisten määrityksien tekemiseen.



KUVA 11: Kuvakaappaus Bonjour-verkkolaitteiden konfiguroinnista

5.3 Palomuurit

Cisco Meraki tarjoaa asiakkailleen kymmenkunta eri tuotevaihtoehtoa palomuurien tuoteperheestään, joista jokainen on suunnattu eri kokoluokan yrityksille ja eri ominaisuuksin. Mallien suositellut käyttäjämäärät alkavat 50 henkilön yrityksistä aina 10 000 käyttäjän ympäristöihin, joita yksittäinen palomuuri kykenee käsittelemään. Käyttäjämäärien kasvaessa palomuurien täytyy kyetä käsittelemään asiakas- ja liikennemäärä, mikä kulkee laitteen kautta. Esimerkkinä alhaisimman tason palomuuri tarjoaa 250 Mb/s (megabittiä sekunnissa) läpisyötön eli miten paljon dataa se kykenee käsittelemään sekunnissa. Suuriin, 10 000 henkilön ympäristöihin tarkoitetuissa laitteissa suurin tuettu läpisyöttö on jopa 6 Gb/s (gigabittiä sekunnissa).

Cisco Merakin MR-tukiasemien lisensoinnin perustuessa kappalemääriin, vaatii MX-sarjan palomuuri jokainen oman yksilöllisen lisenssinsä. Cisco Meraki tarjoaa palomuureilleen kahta eri lisenssiä: Enterprise sekä Advanced Security. Näiden kahden eri lisenssin eroavaisuudet ominaisuuksissa on listattu taulukossa 1. Merkittävimmät lisenssien väliset erot tulevat kehittyneemmistä ominaisuuksista, millä voidaan tarkastella ja tutkia palomuurin läpi kulkevaa liikennettä.

Palomuurien perusominaisuudet eivät eroa paljoa muista palomuurien kaltaisista laitteista. Virtuaaliverkkojen välinen reititys (*VLAN to VLAN routing*), VPN sekä muut reititys ja palomuurisäännöt ovat varmasti tuttuja palomuurilaitteita käyttäneille. Ominaisuudet kuten ohjelmistoperustaiset tunkeutumisen havainnointi ja esto, sisällön suodattaminen sekä haittaohjelmien estäminen ovat saatavilla vain Advanced Security -lisensoinnissa. (Cisco Meraki Licensing n.d.).

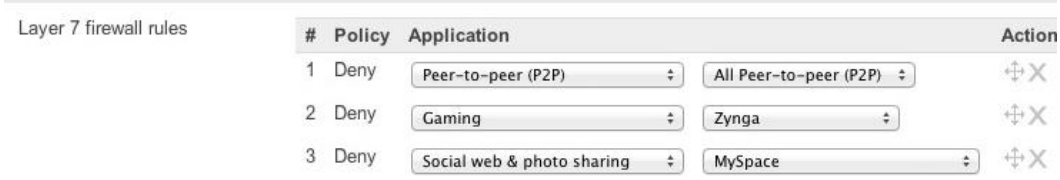
TAULUKKO 1: Palomuurien lisenssien väliset erot

Ominaisuus	**Enterprise**	**Advanced Security**
Stateful firewall	✓	✓
VLAN to VLAN routing	✓	✓
Link bonding / failover	✓	✓
3G / 4G failover	✓	✓
Traffic shaping / prioritization	✓	✓
Site-to-site VPN	✓	✓
Client VPN	✓	✓
MPLS to VPN Failover	✓	✓
Splash pages	✓	✓
Configuration templates	✓	✓
HTTP content caching	✓	✓
Group Policies	✓	✓
Client connectivity alerts	✓	✓
SD-WAN	✓	✓
Geography based firewall rules		✓
Intrusion detection / prevention		✓
Content filtering		✓
Anti-virus and anti-phishing		✓
Youtube for Schools		✓
Web Search Filtering		✓
AMP / Anti-malware		✓

5.3.1 Verkkoliikenteen suodatus ja analysointi

Käyttäen Advanced Security -lisensointia Cisco Merakin palomuureilla, voidaan verkkoliikennettä analysoida entistä syvällisemmin ja täten tunnistaa mahdollisia uhkia tai haittaohjelmia. Pilvihallinnasta on mahdollista määrittää kuvan 12 ja kuvan 13 kaltaisesti, mitä liikennettä verkosta halutaan mahdollisesti estää tai rajoittaa. Samankaltaista sisällön rajoittamista on mahdollista toteuttaa myös eri oikeustasoilla, kunhan järjestelmä on yhdistetty yrityksen omaan AD-ympäristöön (Active Directory). (Technologies: Content Filtering n.d.).

KUVA 12: Kuvakaappaus estetyn verkkosisällön konfiguroinnista



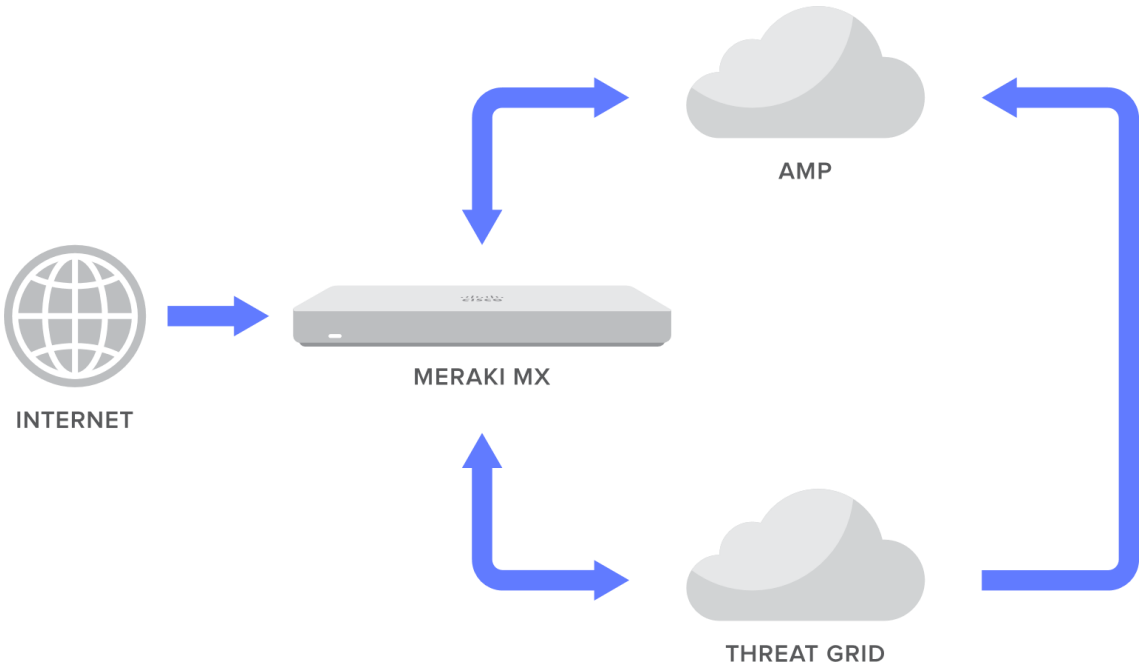
KUVA 13: Kuvakaappaus palomuurisääntöjen konfiguroinnista

Cisco Meraki palomuurien tarjoama tunkeutumisen estojärjestelmä eli IPS (Intrusion Prevention System) käyttää yrityksen nimeltä Sourcefire luomaa ja alalla varsin tunnettua avoimen lähdekoodin ohjelmaa nimeltä Snort. Ohjelma tutkii verkkoliikennettä ja vertaa sitä sääntöjoukkoihin, joita Sourcefire ylläpitää ja lisää päivittäin. Nämä sääntöjoukot perustuvat verkkoliikenteen allekirjoituksien, protokollien sekä tunnettujen poikkeuksien tunnistamiseen liikenteestä, joita on aikaisemmin havaittu eri haittaohjelmien ja tunkeutujien käytössä. Tämän avulla verkkoliikenteestä voidaan tunnistaa jo tunnettuja poikkeuksia ja estää se, mikäli poikkeus muistuttaa tunnettua haittaohjelmaa.

Tunkeutumisen estojärjestelmä on tärkeä osa yrityksien tietoturvaa nykypäivänä, sillä ilman niitä tai kehittyneitä työkaluja haavoittuvuuksien seurantaan yrityksien mahdollisuudet havainnoida näitä omassa ympäristössään tai siellä tapahtuneita tietovuotoja on lähes

mahdotonta. Toinen Cisco Merakin MX-palomuureista löytyvä ja tietoturvaa parantava ominaisuus on kehittynyt haittaohjelmien suojausjärjestelmä AMP (Advanced Malware Protection). AMP on toiminnallisuus, mikä sisältyy Advanced Security -lisenssin piirissä oleviin laitteisiin. Kuviossa 8 on kuvattu, miten MX-sarjan palomuurit hyödyntävät AMP-järjestelmää ja siihen linkattua tietokantaa tunnetuista haittaohjelmista sekä Threat Grid -nimistä järjestelmää.

Threat Grid tarjoaa niin kutsutun hiekkkalaatikkoympäristön (*Sandbox)*, missä voidaan ajaa virtuaalisesti haittaohjelmien koodia ilman, että se saastuttaisi verkkoympäristöä. Yhdessä näiden kanssa, MX-sarjan palomuureilla voidaan suorittaa verkkoliikenteeseen haittaohjelmaskannausta ja estää niitä ennen, kuin ne ovat päätyneet käyttäjien tietokoneille. Sama järjestelmä osaa myös ilmoittaa ympäristön ylläpitäjälle, mikäli aikaisemmin ympäristöön päästetty tiedosto on myöhemmin tunnistettu ja merkattu tunnetuksi haittaohjelmaksi, jolloin he voivat aloittaa tarvittavat toimenpiteet niiden estämiseksi. (Advanded Malware Protection for Meraki MX n.d.).



KUVIO 8: MX-palomuurin toiminta AMP ja Threat Grid -järjestelmien kanssa

Kiitos keskitetyn pilvihallinnan, haavoittuvuuksien paikkaaminen tai vähintäänkin sen hyödyntämisen estäminen verkkoympäristön laitteissa voidaan jakaa nopeasti kaikille laitteille. Vuonna 2014, Heartbleed eli haavoittuvuus OpenSSL-salauskirjastossa jätti aukon tietoturvaan miljoonissa laitteissa. Cisco Merakin MX-sarjan palomuurituotteita käyttävät yritykset saivat kuitenkin haavoittuvuuden paikkaavan päivityksen käyttöön

vielä saman vuorokauden aikana, kun haavoittuvuus tuli julkisuuteen. (How MX Customers Contained Heartbleed In a Day 2014).

5.3.2 VPN-yhteyksien automatisointi

Cisco Meraki MX-sarjan palomuurit tarjoavat myös kattavat ominaisuudet VPN-verkkojen luomiseen ja ylläpitämiseen. Pilvihallittavien laitteiden etu on nähtävissä varsinkin yrityksien verkkoympäristöissä, missä useat eri konttorit täytyy pystyä kytkemään toisiinsa. Normaalisti, tämä vaatisi erillistä konfigurointia jokaiselle rajalaitteelle eli palomuureille ja joskus myös kytkimille, että konttorien välille voidaan muodostaa salatut yhteydet eli VPN-putki.

Cisco Merakin laitteisto kykenee konfiguroimaan VPN-yhteyksien muodostamiseen vaaditut parametrit automaattisesti sekä luomaan yhteydet eri toimipisteverkkojen välillä. Esimerkiksi assosiaatiot, salausavaimet ja pilvihallintaan jo ennalta määritetyt tietoturva-asetukset kopioidaan automaattisesti toisille laitteille, mitkä halutaan yhdistää keskenään. Kuvassa 14 on kuvakaappaus pilvihallinnasta ja toimipisteiden välisen VPN-putken asetuksien valinnasta. (Technologies: Auto VPN n.d.).

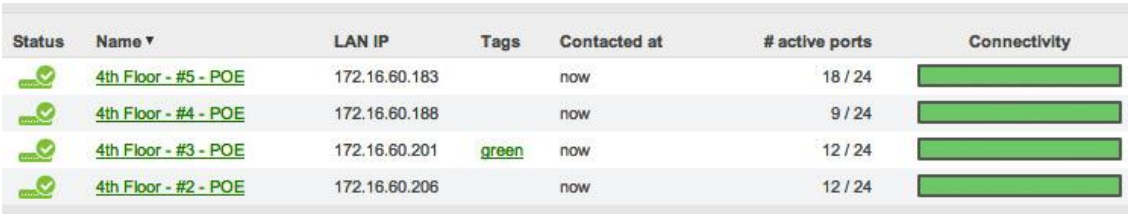
KUVA 14: Kuvakaappaus MX-palomuurien VPN-asetuksista

5.4 Kytkimet

Kuten palomuureja ja langattomia tukiasemia, tarjoaa Cisco Meraki myös kytkinlaitteita eri kokoluokissa ja eri tarpeisiin. Kytkimien lisensointi poikkeaa sekä palomuurien, että tukiasemien lisensoinnista. Kukin kytkinlaite ei vaadi omaa yksilöllistä lisenssiä ja vain siihen yksilöön sidottua lisenssiä, mutta lisenssi pitää olla juuri kyseiselle tuoteperheen mallille hankittu. Lisenssejä voi siis käytännössä siirtää laitteesta toiseen, kunhan ne ovat

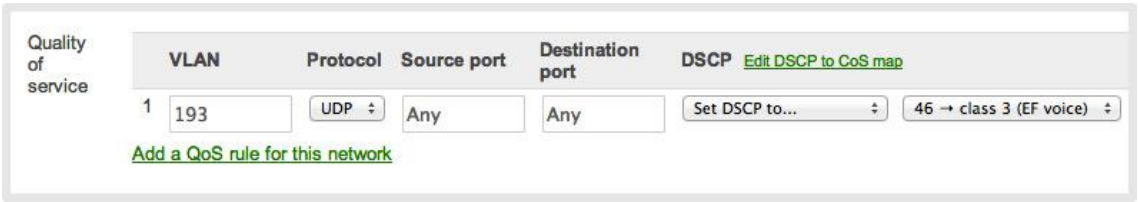
samaa tuotemallia. Cisco Merakin pilvihallittavissa kytkimistä löytyvät kaikki ominaisuudet, mitä normaalilta kytkimeltä voisi odottaa kuten virtuaaliverkkojen porttikohtainen hallinta, porttikohtaiset tietosuoja-asetukset sekä haitallisten DHCP-palvelimien (Dynamic Host Configuration Protocol) tunnistaminen.

Cisco Merakin pilvihallinnan toiminallisuudet tuovat myös kytkimien hallintaan uusia ja helpottavia ominaisuuksia ja toiminnollisuuksia. Esimerkiksi verkon topologian rakentaminen ja havainnollistaminen pilvihallinnan kautta, eikä se tai laitteiden havainnointi verkosta vaadi kaikkien verkkolaitteiden olevan edes samalta valmistajalta. Topologian hallinnan lisäksi pilvihallinta mahdollistaa kuvan 15 mukaisesti kytkimien pinoamisen tai ryhmittämisen esimerkiksi sijainnin tai toimipisteen perusteella, mikä helpottaa ympäristön hallintaa (Technologies: Stacking n.d.).



KUVA 15: Kuvakaappaus MS-sarjan kytkimien hallinnasta

Pilvihallinnan kautta voidaan kytkimille määrittää myös erilaisia sääntöjä liikenteen reititykseen tai priorisoimiseen liittyen. Kuvassa 16 on kuvattu, miten esimerkiksi yrityksissä nousevissa määrin olevat verkon ylitse tapahtuvat puhelut eli VoIP-liikennettä voidaan priorisoida ja säädellä jo ympäristön kytkinlaitteilla. Täten ympäristössä voidaan varmentua siitä, että verkkoa kriittisesti tarvitsevat palvelut saavat niiden tarvitseman kaistan ja prioriteetin yli muun liikenteen. (Technologies: Voice Optimization n.d.).

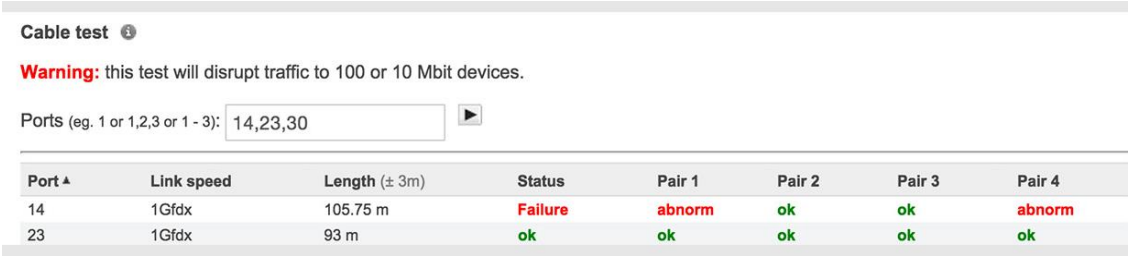


KUVA 16: Kuvakaappaus pilvihallinnan reitityssäännöistä

Pilvihallinnan avulla verkon ylläpitäjällä on myös entistä parempi näkyvyys koko ympäristöön sekä mahdollisiin vikatilanteisiin. MS-sarjan kytkimien hallinnasta löytyy joukko

eri diagnostiikkatyökaluja ja näistä osa on hyvinkin yleisiä ja löytyvät lähes kaikista hallittavista verkkolaitteista kuten toisen verkkolaitteen ping-testi eli testaaminen, vastaavatko ne kyselyyn laitteen saatavuudesta verkossa. Cisco Merakin kytkimien hallinnasta löytyy myös mahdollisuus ajaa yksinkertaisia testejä fyysisten kaapelivikojen löytämiseksi, jollaisia ei ole mahdollista toteuttaa useimmissa yritysverkkojen kytkimissä.

Kuvassa 17 on kuvakaappaus pilvihallinnan kaapelitestistä, millä voidaan tarvittaessa testata kyseisen kytkimen portin ja toisessa päässä kytketyn laitteen kykyä kommunikoida keskenään ja tunnistaa, mikäli näiden välissä käytetty kaapeli on fyysisesti viallinen. Tämän esimerkin tapauksessa on huomattavissa, että porttiin 14 kytketty kaapeli sisältää väärin kytketyt parit kaapelin sisällä. Tämän testin avulla voitaisiin siis välttää ainakin osa asentajan tai huoltomiehen käynneistä toimipisteille, jotka tutkisivat mahdollista vian aiheuttajaa ja erillisellä käynnillä kävisivät korjaamassa ne.



KUVA 17: Kuvakaappaus kytkimen pilvihallinnan kaapelitestistä

5.5 Haasteet ja tulevaisuus

Cisco Meraki tuoteperhe on laaja ja tarjoaa asiakkailleen etuja monilla eri tavoin verkkoympäristöään uusiessa tai uutta rakennettaessa. Cisco Meraki ei kuitenkaan ole ainoa toimija alalla, joka tarjoaa pilvihallittavia tuotteita asiakkailleen. Esimerkiksi Aerohive Networks ja Hewlett-Packard Enterprisen omistama Aruba Networks tarjoavat samankaltaisia palveluita asiakkailleen. Opinnäytetyön kirjoittajana päädyin kuitenkin Cisco Merakin tuoteperheeseen, koska he ovat kyseisen tuotesektorin kokeneimpia ja tarjoavat mahdollisesti kypsimmän kokonaisuuden verkon hallintaan pilvipalveluita hyödyntäen.

Cisco Merakin tuotteet eivät kuitenkaan ole aukottomia, kuten ei mikään julkisen verkon ylitse toimiva laite tai palvelu. Vaikka järjestelmät olisivat mahdollisimman hyvin suojattuja ja hyödyntävät uusimpia tietoturvakehotuksia, ilmenee maailmalla kymmenittäin

uusia haavoittuvuuksia joka päivä, joista osa voi vaikuttaa myös Cisco Merakin tuotteisiin. Tästä huolimatta on huomattu, että pilvihallittavalla verkkoympäristöllä on etunsa korjauksien jakamisen nopeudessa sekä tunnettujen haavoittuvuuksien ja haittaohjelmien lieventämisessä tai kokonaan estämisessä.

Elokuussa 2017, Cisco Merakin työntekijän tekemä asetusmuutos aiheutti virhetilanteen Pohjois-Amerikan palvelimille. Tämän virhetilanteen johdosta 3.8.2017 aamuyön ja aamupäivän aikana Cisco Merakin palvelimille ladatut tiedostot ja asetukset hävisivät. Vahinko ei vaikuttanut asiakkaiden verkkojen toimintaan, mutta hävinnyt data sisälsi esimerkiksi kirjautumissivujen ulkoasutiedostoja, yrityksien pohjapiirustuksia sekä logoja hallintapaneelista.

Cisco Merakin hävinnyt data ei onneksi sisältänyt kriittistä dataa verkkotoimintojen edellyttämiseksi, mutta tilanne olisi voinut olla vakavampikin. Cisco Meraki julkaisi asiasta tiedotteen samana päivänä ja 12 päivää myöhemmin suurin osa datasta oltiin pystytty palauttamaan ja lopuille Cisco Meraki tarjosi erikoistyökalut, millä asiakkaat pystyivät lisäämään puuttuvat tiedot uudelleen omaan pilvihallintaansa ilman tarvetta muuttaa tai poistaa olemassa olevia asetuksia. (North American Object Storage Service 2017).

Tapaus herätti keskustelua pilvipalveluiden luotettavuudesta ja asiakasdatan redundanssista, sillä usein pilvipalveluiden tarjoajilla ei ole itsellään pääsyä asiakkaiden dataan erinäisten tietoturvamääräysten noudattamiseksi. Kyseisen tapauksen kaltaisia vahinkoja voidaan kuitenkin välttää datan redundanssin lisäämisellä, tarkoittaen datan varmuuskopiointia ja kahdentamista esimerkiksi toisista loogisesti erillään oleviin järjestelmiin tai fyysisesti kokonaan eri palvelinkeskuksiin.

Palveluntarjoajien, yrityksien ja asiakkaiden täytyy kuitenkin tiedostaa mahdolliset riskit ja valita käytettävä pilvipalvelu siten, että saatavilla oleva palvelutasosopimus, redundanssi sekä toiminnallisuus tuottavat käyttäjilleen parhaan mahdollisen kokonaisratkaisun. Tulevaisuudessa pilvipalveluiden hyödyntäminen tulee kasvamaan edelleen ja yleistymään asiakasyrityksissä sekä kuluttajamarkkinoilla, kun palveluiden kustannukset laskevat ja palveluilla voidaan tuottaa hyötyä kaikille asiakasryhmille.

6 LANGATTOMAN LÄHIVERKON KÄYTTÖÖNOTTO

Opinnäytetyön aikana suoritettiin käyttöönotto langattomalle lähiverkolle käyttäen Cisco Merakin tuotetta ja pilvipalveluna tuotettua hallintaa. Käyttöönoton tavoitteena oli tutustua Cisco Merakin ratkaisuihin sekä tukiasematuotteeseen ja selvittää, mitä toiminnollisuuksia tuote mahdollistaa ja vaatimuksia täytyy ottaa huomioon sen käyttöönotossa. Viimeisen vuoden aikana kirjoittajan työnantajan yritysympäristöön on otettu käyttöön useita Cisco Merakin langaton tukiasema niiden helpon käyttöönoton ja sopivan palvelumallin ansiosta, joten kyseinen tuoteperhe valikoitui myös tähän käyttöönottoon.

6.1 Käytettävä laitteisto

Langattoman lähiverkon pystyttämiseen käytettiin kuvan 18 mukaista Cisco Meraki MR33 -tukiasemaa, joka on Cisco Merakin peruskäyttöön tarjoama malli. Tukiasema on fyysisiltä mitoiltaan 215mm leveä, 110mm syvä ja 32mm korkea, eli laite on ominaisuuksistaan ja lisävastaanottimista huolimattaan säilyttänyt normaalin langattoman tukiaseman koon. Laite tukee langattomaan tiedonsiirtoon 2,4 GHz sekä 5 GHz taajuuksia ja pitää sisällään lisäksi erillisen 2,4 GHz Bluetooth-radion sekä erillisen molempia langattoman tiedonsiirron taajuuksia tukevan radion spektrianalysaattoria ja paikka-analytiikkaa varten. Tukiaseman tarkempi tuote-esittely ja tuotetiedot löytyvät tämän opinnäytetyön liitteenä (liite 1).

KUVA 18: Cisco Meraki MR33 -langaton tukiasema

Tukiasemassa käytettävä antenni on ympärisäteilevä ja tarjoaa vähintään 3,8 dBi:n vahvistuksen molemmilla operointitaajuuksilla. Laitteen RJ45-portti tukee tiedonsiirtonopeuksia 1 Gb/s asti ja laitteen sähkönsyöttöä PoE-standardin (Power over Ethernet) mukaisesti. Cisco toimittaa laitteen mukana erillisen seinäadapterin, mikäli asiakkaalla ei ole mahdollista hyödyntää PoE-standardia. Laitteen mukana tulee myös seinään tai kattoon kiinnitettävä asennusrauta sekä tarvittavat kiinnitystarvikkeet. Cisco myöntää langattomille tukiasemilleen myös elinikäisen takuun elektroniikan osalta. (Indoor Access Points: MR33 n.d.).

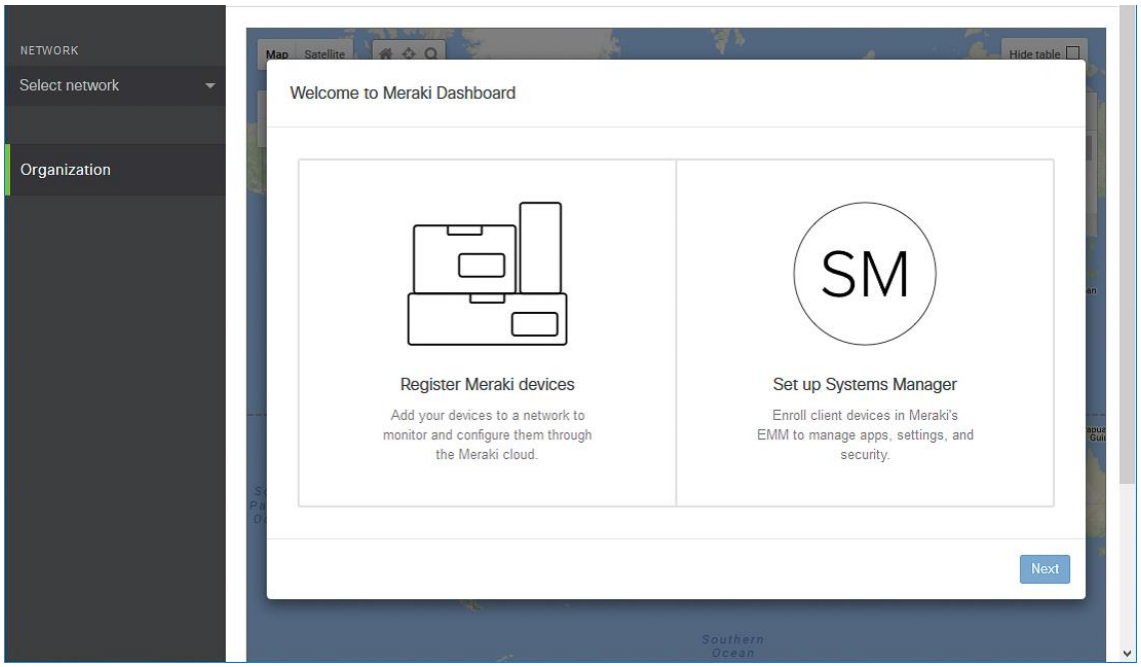
Langaton tukiasema saatiin Cisco Merakin tarjoaman webinaarin myötä, jonka katsojille Cisco Meraki tarjoaa ilmaisen tukiaseman sekä 3 vuoden ohjelmistolisenssin sen käyttöön. Tarjous ei ollut saatavilla kuitenkaan kaikille, vaan ilmaisen tukiaseman ja lisenssin saamiseksi täytyi olla tietotekniikka-alan ammattilainen ja töissä tietotekniikasta päättävässä tai hallinnoivassa asemassa sellaisessa yrityksessä, joka ei ollut Cisco Meraki -tukiasemien jälleenmyyjä. Tämän opinnäytetyön kirjoittajana olin oikeutettu kyseiseen tarjoukseen ja seuraavissa kappaleissa käyn läpi, miten laitteen käyttöönotto ja konfigurointi käyttäjän eri tarpeisiin tehdään.

6.2 Palvelun käyttöönotto ja yleiset asetukset

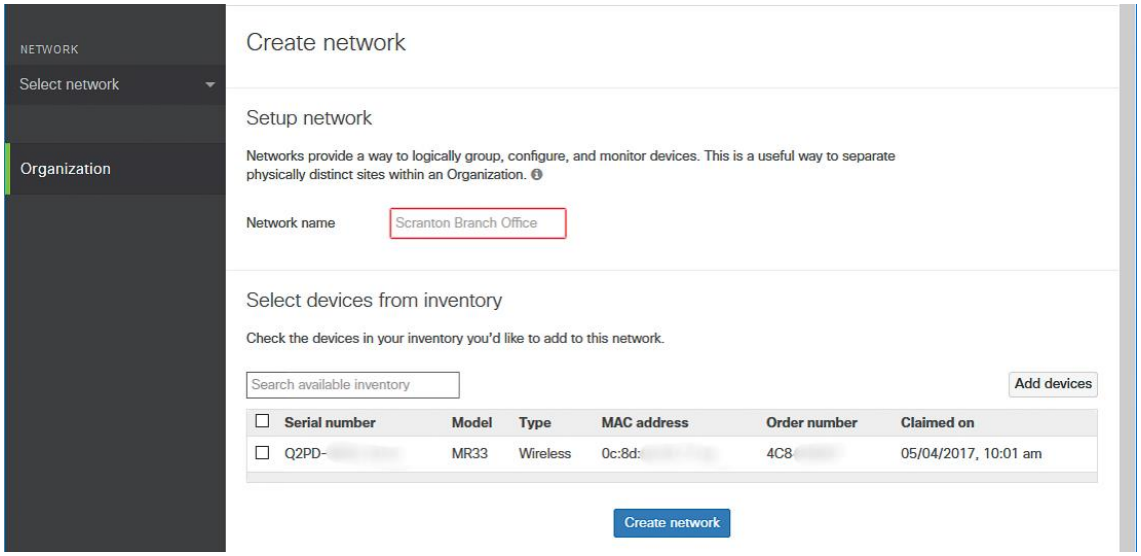
Langattoman tukiaseman käyttöönotto alkaa luonnollisesti asentamalla se haluttuun kohteeseen ja kytkemällä se yrityksen tai asiakkaan verkkoon ja sähköihin käyttäen joko erillistä virta-adapteria tai sähkönsyöttöä verkkoliitännän kautta. Ensimmäisen kerran käynnistyessään laite yhdistää Cisco Merakin pilvipalveluun ja lataa uusimmat saatavilla olevat ohjelmistopäivitykset. Pilvipalveluun kirjautuminen tapahtuu käyttäen tilausvaiheessa annettua ja rekisteröityä sähköpostiosoitetta ja sähköpostiin lähetettyä salasanaa.

Sisäänkirjautumisen ja uuden salasanan syötön jälkeen päästään pilvihallinnan etusivulle (kuva 19), josta voidaan edetä rekisteröimään verkkoon kytkettyjä laitteita. Jos yrityksen tai asiakkaan verkossa olisi käytössä myös yhteensopivia mobiililaitteita, niitä kyettäisiin hallitsemaan käyttäen Cisco Meraki Systems Manager -hallintaa. Laiterekisteröinnin kautta päästään luomaan uutta lähiverkkoa käyttäen inventaariossa olevia laitteita.

Aikaisemmin verkkoon kytketty langaton tukiasema on tähän mennessä ehtinyt lataamaan uusimmat ohjelmistopäivitykset ja on valmis käytettäväksi (kuva 20). Inventaarioon on mahdollista lisätä lisää laitteita joko sarja- tai tilausnumeron perusteella. Tässä tapauksessa ympäristöön tulee vain yksi langaton tukiasema ja valinnan jälkeen lähiverkolle voidaan allokoida nimitunniste. Lähiverkon nimeksi valittiin tätä opinnäytetyötä varten Meraki-ympäristö.

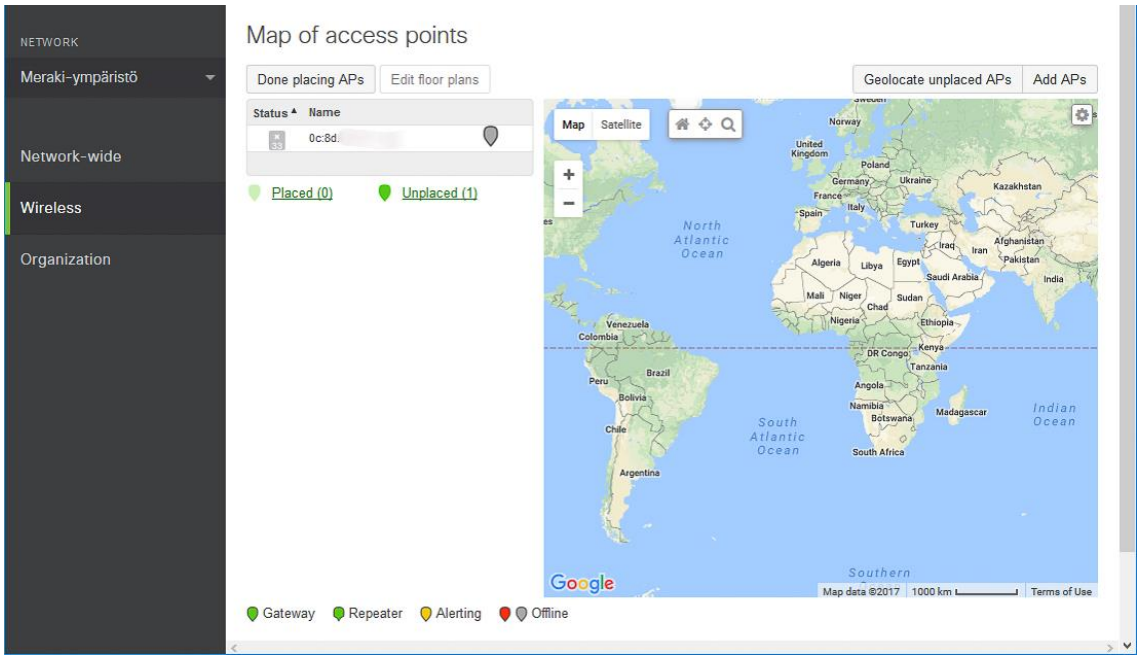


KUVA 19: Cisco Meraki pilvihallinnan etusivu



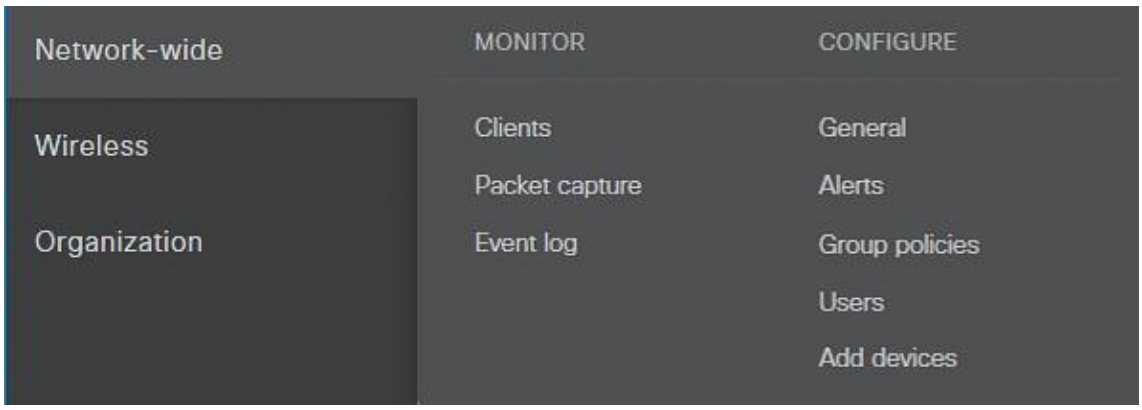
KUVA 20: Uuden lähiverkon luonti pilvihallinnassa

Uuden lähiverkon laitteiden valinnan jälkeen järjestelmä luo verkon automaattisesti käyttäen oletusasetuksia ja ohjaa käyttäjän kuvan 21 mukaiseen näkymään. Tässä näkymässä käyttäjä voi sijoittaa verkon eri toimipisteiden laitteet kartalle käyttäen pohjana Google Maps -karttapalvelua tai suorittaa paikannuksen automaattisesti sitä tukeville laitteille. Tämä auttaa verkkoympäristön sekä yrityksen tietotekniikkaa hallinnoivien osapuolien näkyvyyttä verkkoon, varsinkin suurissa ja monimutkaisissa ympäristöissä.



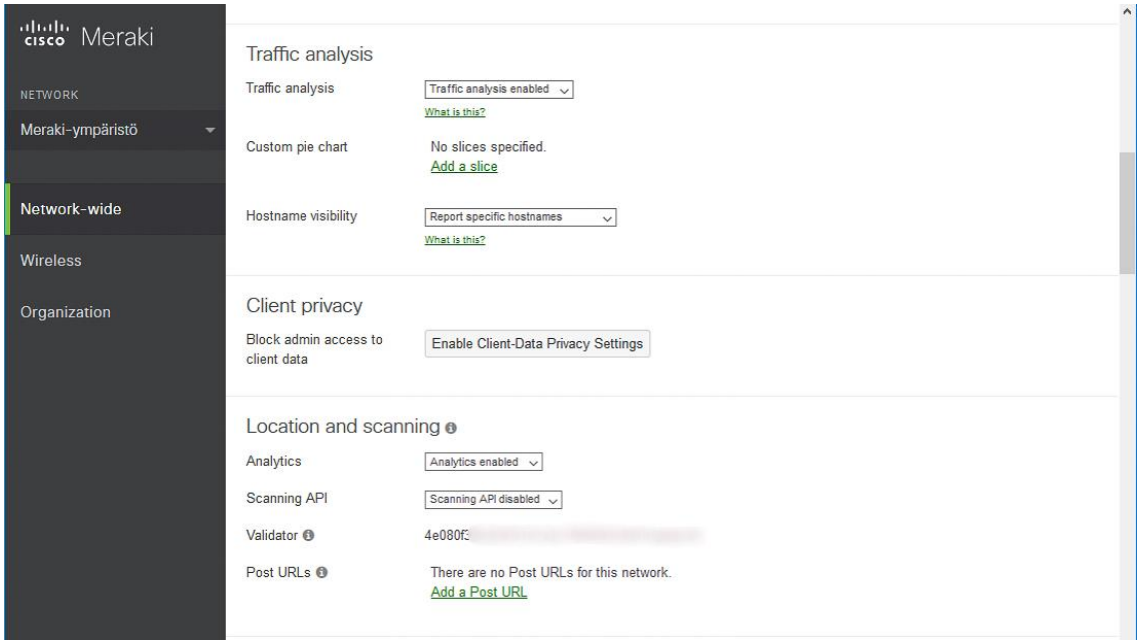
KUVA 21: Listaus langattomista tukiasemista ja niiden sijainneista

Kun halutut laitteet on lisätty lähiverkkoon, voidaan aloittaa niiden konfigurointi. Ennen yksittäisten laitteiden ja langattoman lähiverkon luontia kuitenkin konfiguroidaan muut lähiverkon asetukset (kuva 22). General- eli yleisasetuksien alta voidaan muuttaa muun muassa lähiverkon nimeä ja kuvausta, muuttaa laitteiden paikallisia tunnuksia ja automaattisten ohjelmistopäivityksien asennusajankohtaa häiriöiden tai käyttökatkoksien minimoiseksi.

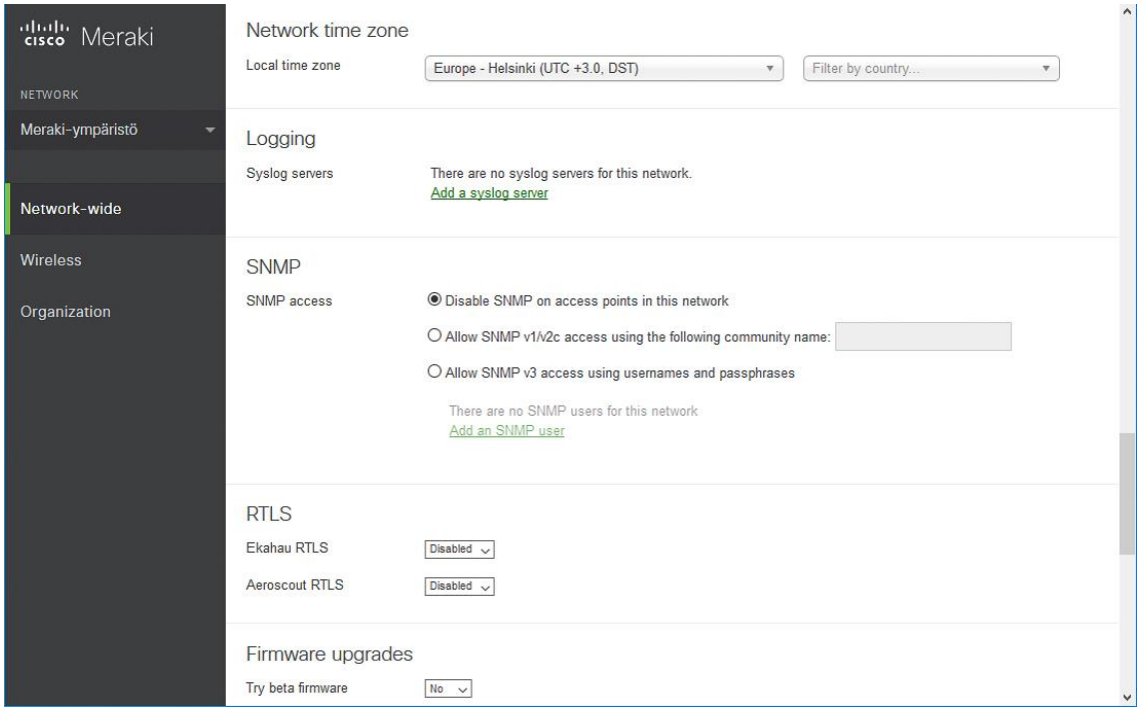


KUVA 22: Lähiverkon asetukset pilvihallinnassa

Yleisasetukset-sivulla on myös useita eri verkon analysointiin ja valvontaan liittyviä asetuksia, kuten liikenteen analysointi yleisimpien sovelluksien tai verkkosivujen tunnistamiseksi, käyttäjätietojen ja -datan pseudonymisointi käyttäjien yksityiseen suojaamiseksi sekä tukiaseman käyttäjien paikannuspalvelut ruuhkaisten sijaintien tunnistamiseksi (kuva 23). Käyttäjätietojen pseudonymisointi varsinkin on tärkeä, ottaen huomioon Euroopan Unionin toukokuussa 2018 voimaan astuvan tietosuojalakiuudistuksen. Samalta sivulta löytyvät asetukset myös erillisen lokipalvelimen hyödyntämiseen virhetietojen tallentamiseksi, SNMP-hallintaprotokollan (Simple Network Management Protocol) käyttöönottoon tai kolmannen osapuolen paikannuspalveluiden hyödyntämiseen lähiverkossa (kuva 24).

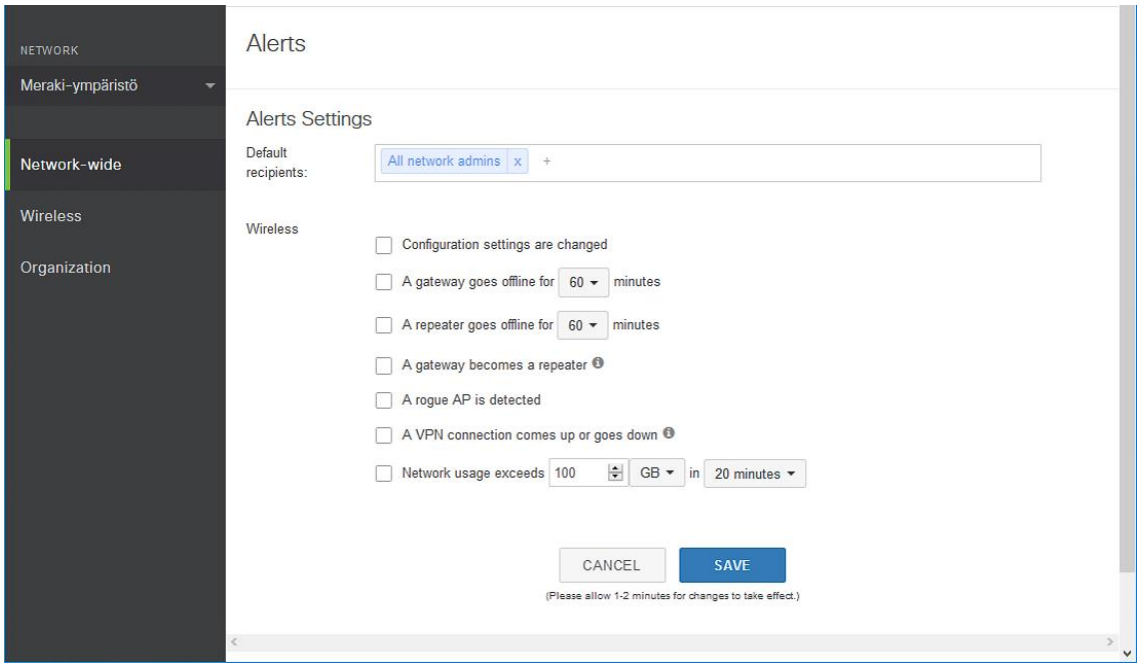


KUVA 23: Liikenteen analysointi- ja paikannuspalveluasetukset



KUVA 24: Järjestelmälokien ja ulkoisten paikannuspalveluiden käyttö

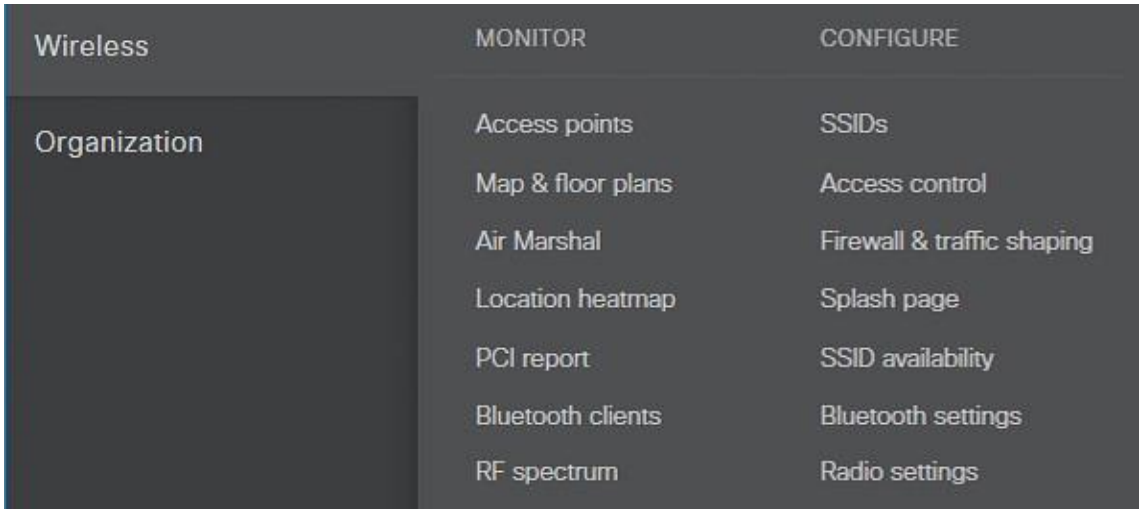
Yleisasetuksien ohella lähiverkon kattavasta valikosta on mahdollista määrittää myös automaattisia hälytyksiä, mikäli jokin verkon laite häviää tai sen saatavuus heikkenee. Hälytyksiä voidaan myös generoida, mikäli verkossa havaitaan haitallinen tukiasema, mitä mahdollinen hyökkääjä saattaisi käyttää yrittääkseen päästä verkon laitteiden väliin tai mikäli verkossa havaitaan muuta poikkeuksellista toimintaa (kuva 25).



KUVA 25: Automaattisten hälytyksien konfigurointi

6.3 Langattoman lähiverkon konfigurointi

Langattoman lähiverkon luonti onnistuu Wireless-valikon alta, josta löytyvät asetukset langattoman verkon tunnisteiden eli SSID-tunnisteiden asettamiseen, langattoman verkon pääsyn konfiguroimiseen sekä verkon toiminnallisuuteen (kuva 26). Samasta valikosta löytyvät myös Bluetooth-radion asetukset, mikäli yrityksen tai asiakkaan käytössä on Bluetooth-laitteita ja näitä halutaan ohjata tai käyttää Bluetooth-majakoita käyttäjien opastamiseen.

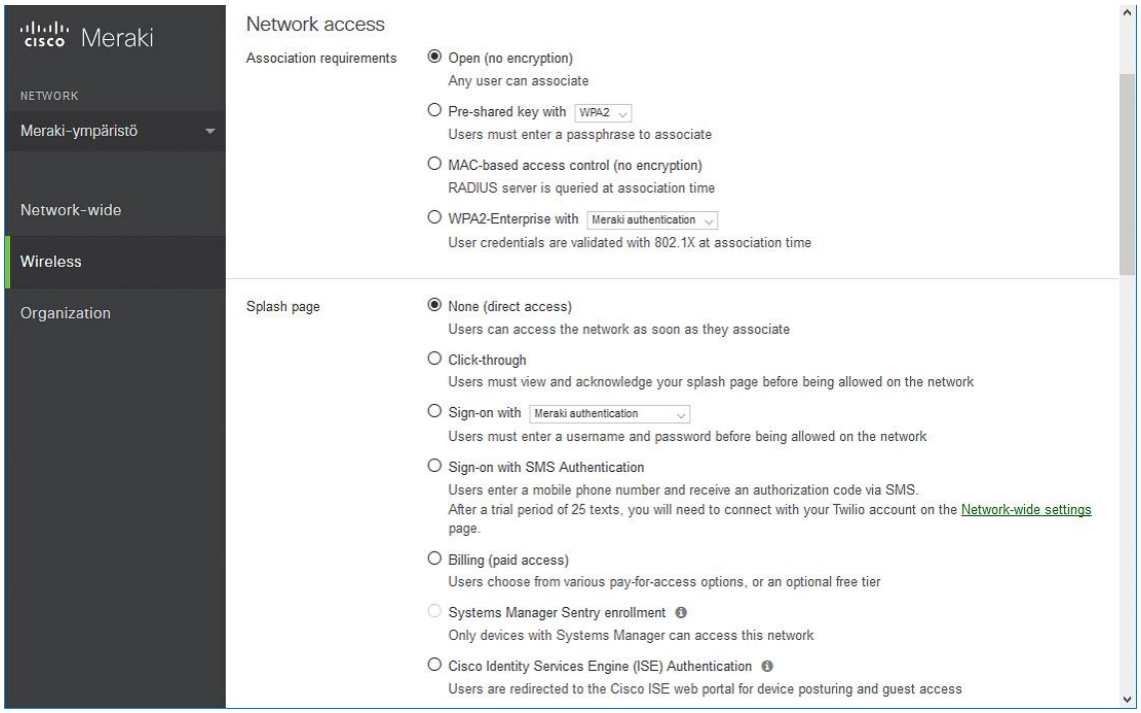


KUVA 26: Langattoman lähiverkon asetukset

Cisco Meraki -tukiasemat mahdollistavat maksimissaan 15 eri SSID-tunnisteen käyttämistä, eli yhdelläkin tukiasemalla voidaan mainostaa 15 eri langatonta verkkoa eri asetuksin ja rajoituksin. Yksittäiselle verkolle voidaan määrittää muun muassa oma tunnistautumistapa laitteille ja miten niille myönnetään pääsy verkkoon (kuva 27). Langaton lähiverkko voidaan pitää avoimena, suojata kiinteällä salasanalla tai käyttäjien tunnistaminen voidaan todentaa käyttäen RADIUS-palvelinta (Remote Authentication Dial In User Service). RADIUS-palvelimen käyttö on yleistä varsinkin isoissa yritysympäristöissä, missä käyttäjiä on runsaasti ja liittyminen verkkoon halutaan suorittaa käyttäen jo käytössä olevia käyttäjätunnuksia.

Verkkoon liittyville käyttäjille voidaan myös pakottaa verkkosivulla asiointi, ennen kuin heille myönnetään pääsy verkkoon. Cisco Merakin pilvihallinnasta voidaan määritellä

suoraan pääsy ilman verkkosivulla vierailua tai esimerkiksi pakottaa erillisten käyttäjäehtojen hyväksyminen. Käyttäjä voidaan myös todentamaan henkilöllisyytensä pyytäen tätä kirjautumaan RADIUS- tai muilla yritystunnuksilla, tekstiviestivahvistuksella tai Ciscon ISE-palvelua (Identity Services Engine) hyödyntäen. Mahdollisuutena on myös periä käyttäjiltään erillinen maksu verkkoon pääsystä, mikä on käytössä esimerkiksi monilla lentokentillä ja lentoyhtiöillä.



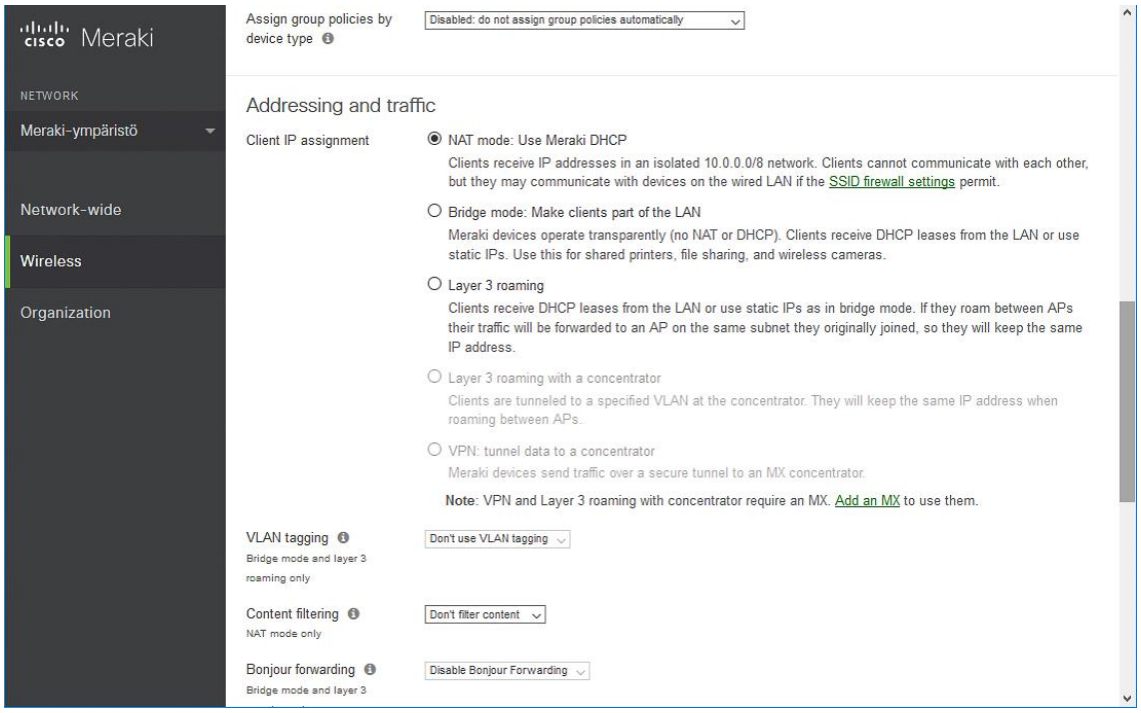
KUVA 27: Langattoman lähiverkon pääsynhallinta

Oletuksena Cisco Merakin tukiasemat toimivat NAT-tilassa (Network Address Translation), eli ne luovat oman aliverkkonsa langattomille laitteille (kuva 28). Tämä on tietoturvallinen vaihtoehto, mikäli langattomaan verkkoon yhdistettyjen laitteiden ei tarvitse saada oletuksena yhteyttä muihin lähiverkon laitteisiin, mitä ympäristössä saattaisi olla kytkettynä. Vaihtoehtoisesti tila voidaan muuttaa siltaavaksi, jolloin langattomaan verkkoon yhdistetyt laitteet saavat verkko-osoitteensa muualla verkossa toimivalta DHCP-palvelimelta. Tällöin laitteet näkevät koko lähiverkon sellaisenaan ja langaton tukiasema toimii vain verkon toistimena.

Cisco Merakin langattomat tukiasemat voidaan konfiguroida myös OSI-mallissa tason 3 verkkovierailuja varten, jolloin yhdistetyt laitteet saavat verkko-osoitteensa edelleen lähiverkon omalta DHCP-palvelimelta, mutta säilyttävät sen siirtyessään langattomasta tukiasemasta toiseen. Tämä ominaisuus on hyödyllinen varsinkin yritysverkoissa, missä on

käytössä BYOD-politiikka (Bring Your Own Devices) tarkoittaen sitä, että työntekijät käyttävät omia mobiililaitteitaan ja saavat kytkeä näitä yrityksen langattomaan lähiverkkoon. Tätä toiminnallisuutta varten on kuitenkin verkkoon suositeltavaa luoda oma langaton lähiverkko ja virtuaaliverkko mobiililaitteita varten, jolloin mahdolliset haittaohjelmat eivät pääse leviämään niistä muuhun yritysverkkoon.

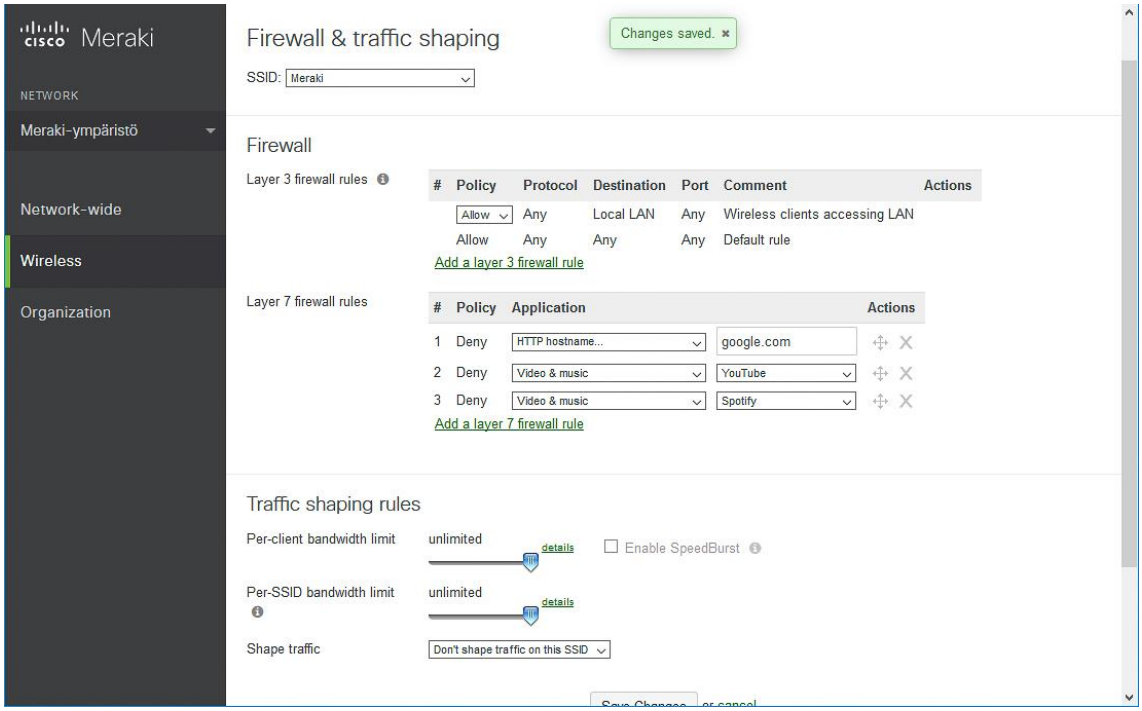
Mikäli verkon toiminta on asetettu NAT-tilaan, Cisco Merakin tukiasemat tarjoavat myös mahdollisuuden estää aikuisviihdesivustoja ja niiden liikennettä yritysverkoissa automaattisesti. Toisena vaihtoehtona tämän saavuttamiseksi on käyttää omaa DNS-palvelinta, jonka avulla on mahdollista tehdä omia rajauksia verkkoliikenteeseen. Siltaavassa tai tason 3 tilassa langattomille tukiasemille voidaan ottaa käyttöön Bonjour-liikenteen edelleen lähetys, mikäli lähiverkossa on käytössä Bonjour-protokollaa hyödyntäviä laitteita kuten Google Chromecast. Tällöin protokollan hyödyntäminen ei vaadi muuta konfigurointia verkon laitteille, mikäli käytössä on vain Cisco Merakin verkkolaitteita.



KUVA 28: Langattoman lähiverkon reititysasetukset

Langattoman lähiverkon asetuksista on mahdollista myös asettaa liikenteelle omia rajoituksia palomuurin kaltaisesti. Oletuksena langaton tukiasema lähettää kaiken liikenteen edelleen, ellei se täsmää ennalta asetettuihin palomuurisääntöihin. Cisco Merakin pilvihallinnasta on mahdollista asettaa eri tason 3 sääntöjä, esimerkiksi TCP-, UDP- tai ICMP-liikenteen estäminen koko verkossa tai vain tietylle laitteelle. Pilvihallinnan kautta on

mahdollista määrittää myös tason 7 sääntöjä, kuten estää pääsy kokonaisuudessaan tiettyyn verkko-osoitteeseen tai rajoittaa esimerkiksi video- tai musiikkipalveluiden saatavilla olevaa kaistanleveyttä kullakin eri SSID-tunnisteella (kuva 29).



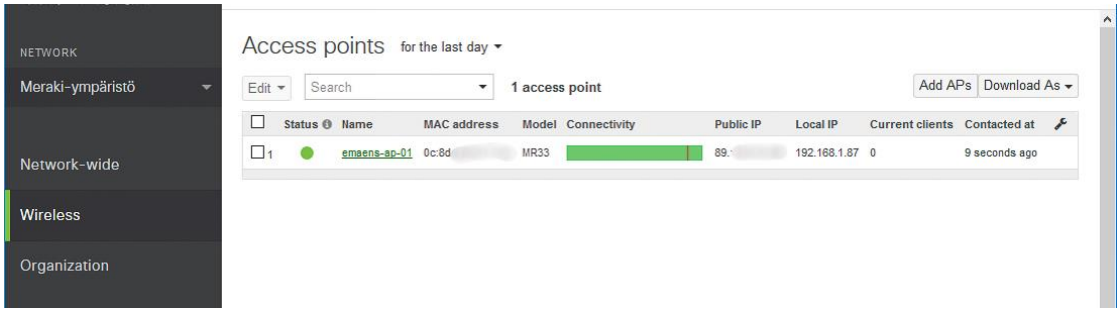
KUVA 29: Verkkoliikenteen sääntöjen luonti

6.4 Valvonta ja analytiikka

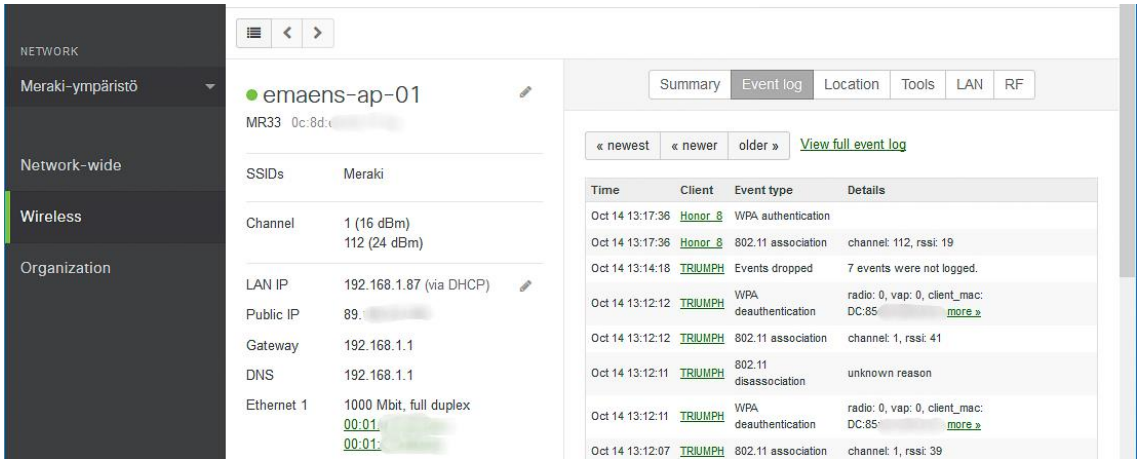
Kuten aikaisemmin mainittu, Cisco Merakin tuotteilla saadaan yrityksen tai asiakkaan verkosta paljon erilaista statistiikkaa ja analytiikkaa, jota voidaan hyödyntää lähiverkon kehittämiseen tai jopa haitallisten laitteiden tunnistamiseen ja mahdollisten verkkohyökkäysten ehkäisemiseen. Seuraavaksi tutustuin, mitä tietoa saadaan käytössä olevasta langattomasta lähiverkosta ja sen käyttäjistä. Palatessa ensin listaukseen verkon laitteista, nähdään asennetun langattoman tukiaseman olevan toimintakuntoinen. Samalle voidaan huomata punaisena viivana aika, jolloin pilvihallinta on havainnut tukiaseman olleen hetkellisesti pois verkosta (kuva 30).

Avatessa yksittäisen langattoman tukiaseman tarkemmat tiedot, saadaan tarkempaa statistiikkaa verkon kuormituksesta, signaalin vahvuudesta, yhdistetyistä langattomista laitteista sekä tämän hetkisistä verkkoasetuksista (kuva 31). Tapahtumahistoriasta nähdään,

miten käytössä olleet testilaitteet eli Windows-kannettava ja älypuhelin ovat kytkeytyneet langattomaan verkkoon ja pois siitä useamman kerran.



KUVA 30: Listaus langattomista tukiasemista ja niiden tämänhetkinen tila

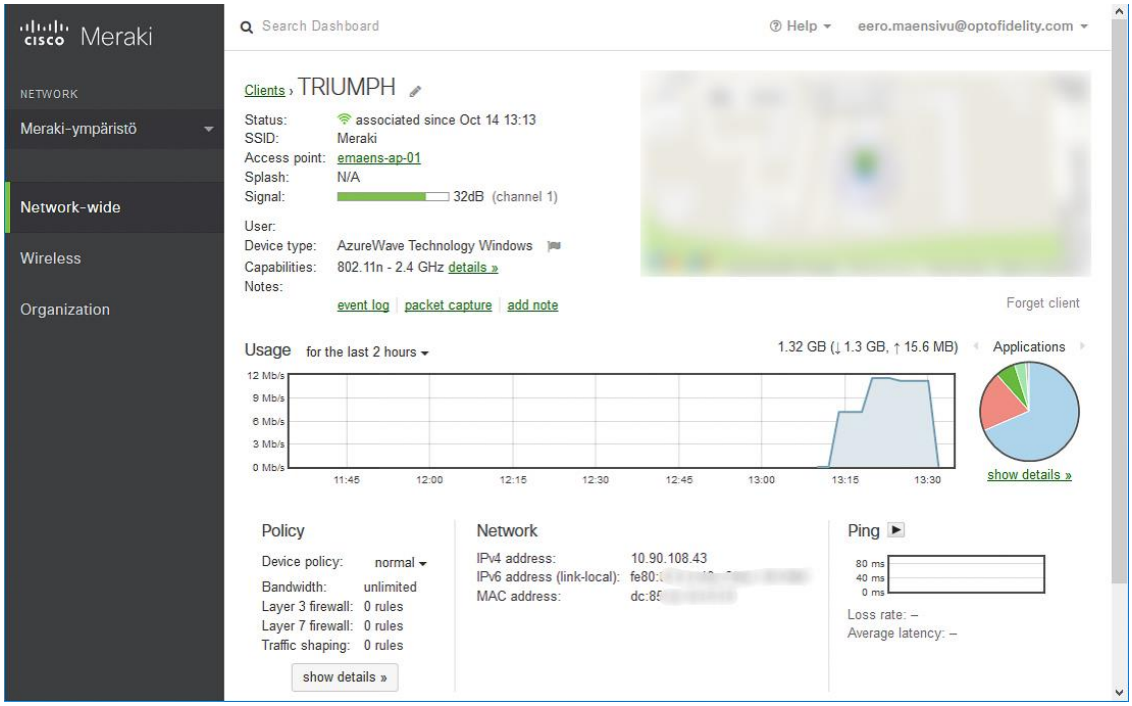


KUVA 31: Langattoman tukiaseman asetukset ja tapahtumahistoriaa

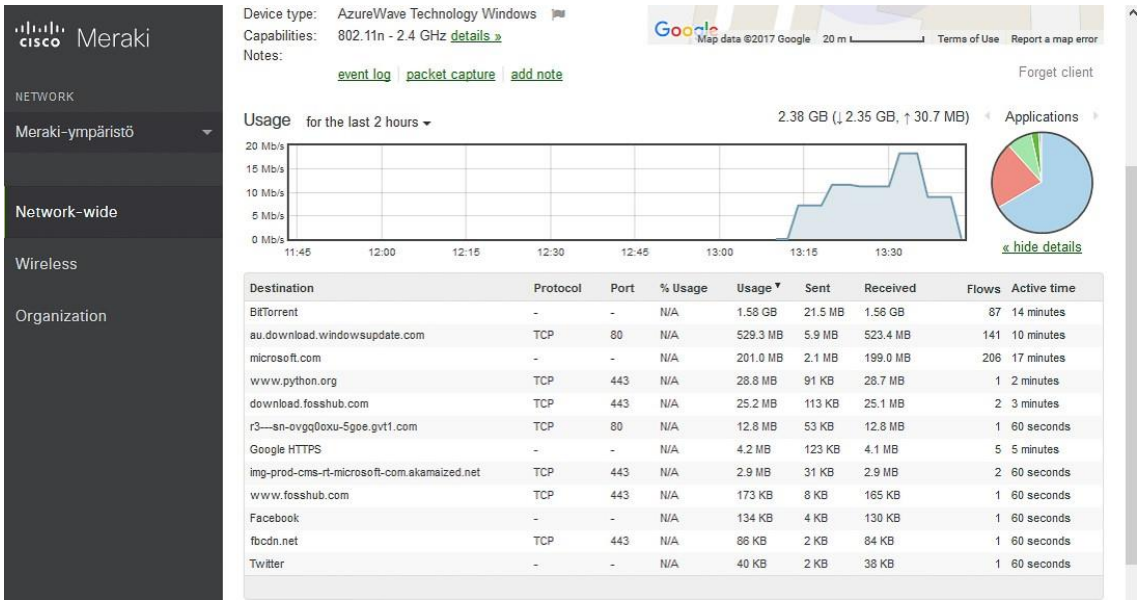
Kun historiatiedon laitteista valitaan yksi, päästään käsiksi sen tarkempiin statistiikka- ja analytiikkatietoihin. Kuvassa 32 nähdään kyseisen verkkolaitteen tämän hetkinen osoitteen, signaalin vahvuus sekä mistä lähtien laite on ollut verkkoon kytkettynä. Näiden lisäksi saadaan tietoja itse laitteesta ja mitä verkkoteknologioita se tukee. Mikäli niin halutaan, voidaan tältä sivulta myös avata kyseisen laitteen tapahtumahistoria verkossa tai suorittaa tarkempaa analysointia tälle ja tältä laitteelta tulevalle liikenteelle.

On mahdollista myös tarkastella tarkempia tietoja yksittäisen verkkolaitteen verkon käytöstä, vaihdellen kahdesta tunnista jopa 30 vuorokauteen (kuva 33). Tässä tapauksessa huomataan, että laitteen verkkoliikenteestä suurin osa kuluneen kahden tunnin ajalta on BitTorrent- eli P2P-liikennettä. Tämän lisäksi laitteelle on ladattu Windows-päivityksiä portin 80 kautta sekä vierailtu erinäisillä verkkosivuilla. Liikenteen seasta havaitaan myös

epäilyttävä osoite r3---sn-ovgq0oxu-5goe.gvt1.com, joka kuitenkin osoittautuu Googlen omistamaksi palvelimeksi.



KUVA 32: Yksittäisen langattoman verkkolaitteen analytiikkaa

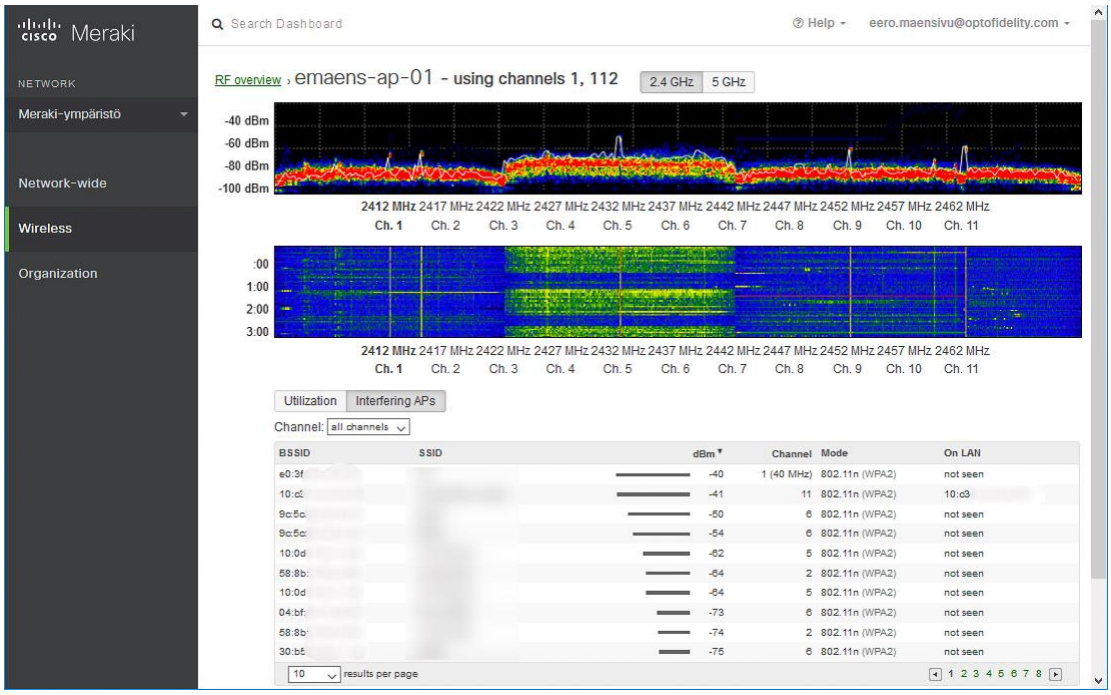


KUVA 33: Analytiikkaa testilaitteen verkkoliikenteestä

Cisco Merakin pilvihallinnan analytiikka ja statistiikka ei kuitenkaan rajoitu vain langattoman lähiverkon laitteiden lähettämän ja vastaanottavan liikenteen seurantaan, vaan myös tukiasemien lähiympäristöjen tutkimiseen. Nykypäivänä monissa yrityksissä langattoman lähiverkon pystyttäminen vaatii myös langattomien tukiasemien mitoittamista

ja konfigurointia siten, että ne häiritsevät tai vastaanottavat häiriötä muista tukiasemista ja laitteista mahdollisimman vähän. Tässä astuu apuun Cisco Merakin tukiasemissa oleva, erillinen radio spektrianalysaattoria ja paikka-analytiikkaa varten.

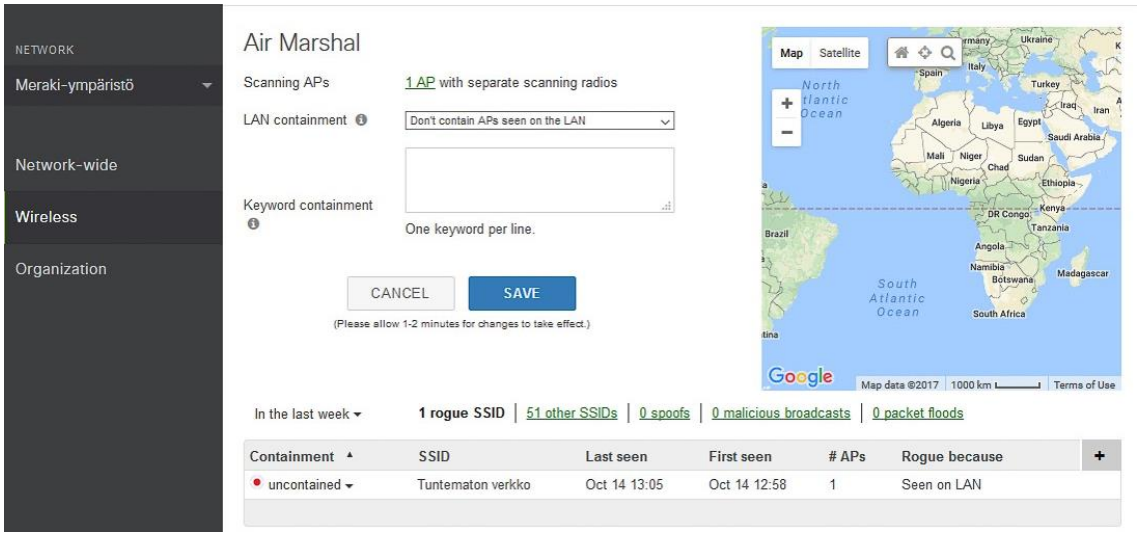
Spektrianalysaattoria hyödynnetään muiden langattomien lähiverkkojen ja häiriölähteiden kartoittamiseen ja täten säätämään Cisco Merakin langattomien tukiasemien omia asetuksia automaattisesti (kuva 34). Järjestelmä listaa muut lähialueen langattomat verkot sekä näiden voimakkuudet sekä sen, mitä kanavaa ne käyttävät. Näitä tietoja hyödyntäen, langattomien tukiasemien asetuksia kuten käytettyä kanavaa ja lähettimien tehoa säädetään automaattisesti. Täten Cisco Meraki -tukiasemien käyttäjille kyetään tarjoamaan paras mahdollinen käytettävyys eri ajan hetkillä.



KUVA 34: Spektrianalysaattori ja historiatietoa lähiympäristöstä

Muita Cisco Merakin pilvipalvelun avulla havaittavia asioita ovat mahdollisesti haitalliset verkkolaitteet yrityksen tai asiakkaan omassa lähiverkossa tai langattomien tukiasemien läheisyydessä. Kuvassa 35 on kuvattu Cisco Merakin Air Marshal -näkymää, joka kuuntelee langattoman verkon laitteita tukiasemien läheisyydessä. Mikäli järjestelmä havaitsee sisäverkossa muita aiheettomia tukiasemia tai laitteita, se ilmoittaa siitä verkkoa hallinnoivalle taholle. Tässä tapauksessa Cisco Merakin langattoman tukiaseman lisäksi samassa lähiverkossa on toinen langaton reititin, joka tarjoaa langatonta verkkoa. Tämän

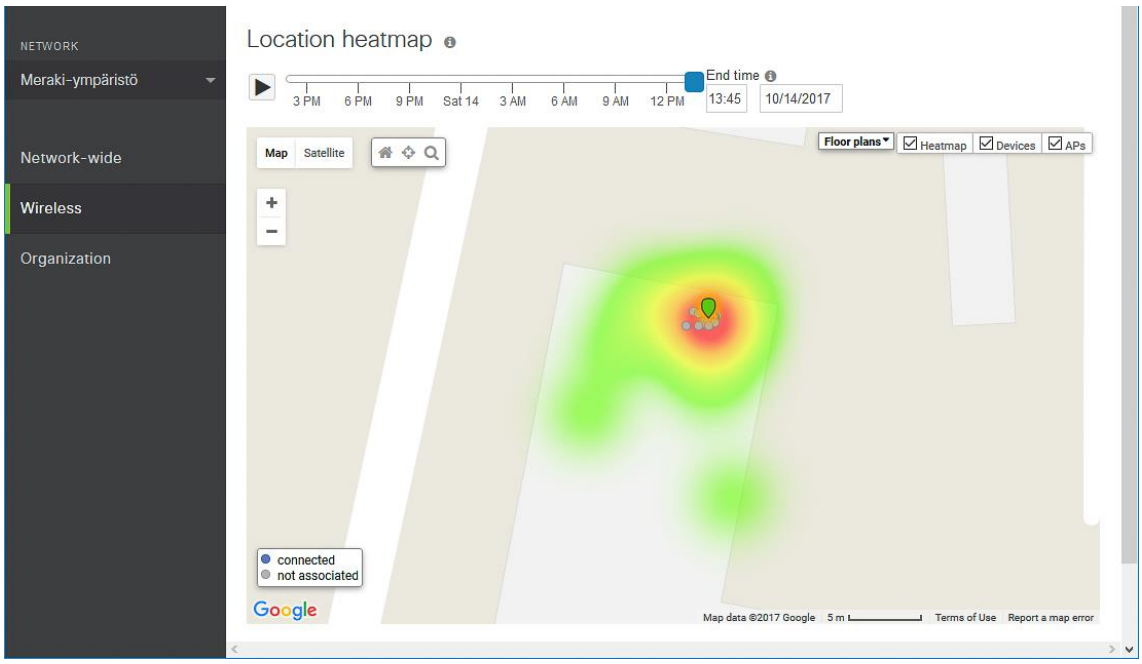
johdosta järjestelmä ilmoittaa laitteesta ja mahdollistaa laitteen valkolistaamisen tai eristämisen.



KUVA 35: Langattoman lähiverkon Air Marshal -näkymä

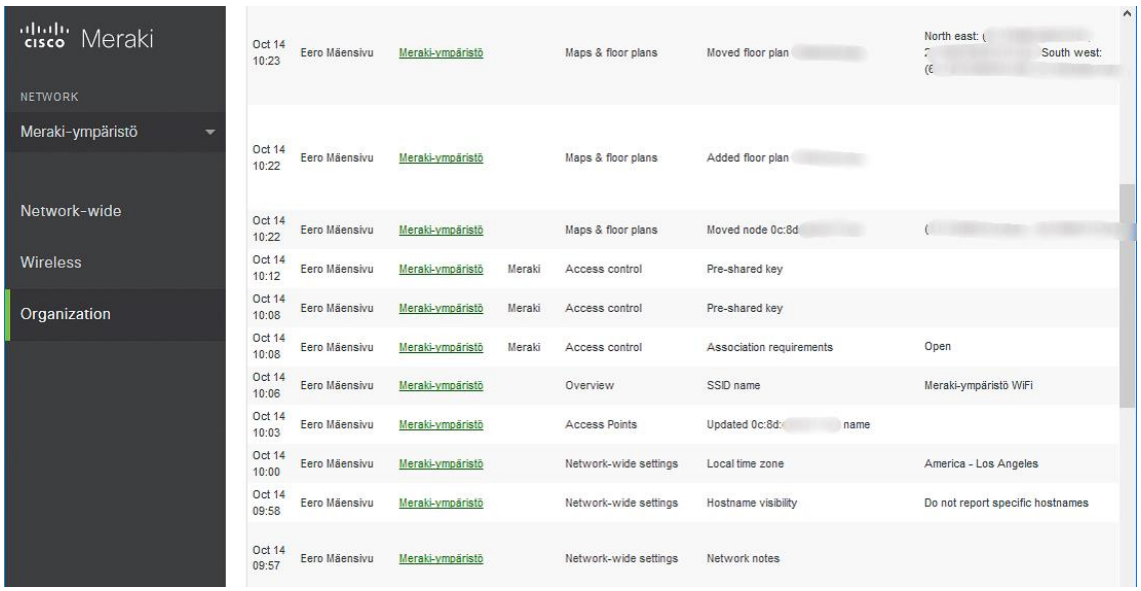
Järjestelmä osaa myös havaita, mikäli johonkin yksittäiseen tukiasemaan tai verkkotunnisteeseen kohdistetaan deauth-hyökkäystä, jossa haitallinen laite tai henkilö yrittää saada mobiililaitteita tai muita langattoman lähiverkon käyttäjien laitteita katkaisemaan yhteys Cisco Merakin langattomista tukiasemista. Tällaisen tukiaseman tai verkkotunnisteen järjestelmä kykenee estämään automaattisesti, tai pilvihallinnasta niin valikoiden. Tällöin järjestelmä kuuntelee langattomien verkkolaitteiden pyyntöjä ja mikäli havaitsee langattoman laitteen yhdistävän haitalliseen tukiasemaan, lähettää se automaattisesti laitteelle pyynnön irtautua kyseisen tukiaseman tarjoamasta verkosta.

Verkon kuormitusta voidaan seurata pilvihallinnassa niin kutsutun lämpökartan avulla. Pilvihallinnan avulla voidaan seurata käyttäjien lukumäärää sekä verkon kuormitusta eri ajan hetkillä, kuten on näytetty kuvassa 36. Kuvasta voidaan päätellä, että suurin osa verkon käytöstä on keskittynyt lähelle yksittäistä langatonta tukiasemaa, mutta jonkin verran kuormitusta tai häiriöitä tulevan myös käytössä olevien tilojen ulkopuolelta. Nämä johtuvat todennäköisimmin muista lähistöllä olevista langattomista tukiasemista, mitkä hyödyntävät tiedonsiirrossa samoja kanavia kuin Cisco Merakin langaton tukiasema kyseisellä hetkellä.



KUVA 36: Langattoman tukiaseman käyttäjien kuormitus

Eri tietoturvasyistä johtuen yrityksen tai asiakkaan verkkoympäristön ja tietotekniikkainfrastruktuurin kannalta on tärkeää säilyttää ja ylläpitää tietoa, mitä muutoksia järjestelmiin on tehty aikojen saatossa. Myös Cisco Merakin pilvihallinnassa pidetään seurantaa siitä, mitä muutoksia laitteille tai verkkokonfiguraatioihin on tehty. Kuvassa 37 on esimerkkilistaus yhden päivän aikana tehdyistä muutoksista, jotka sisältävät esimerkiksi aikavyöhykkeen vaihtamisen ja langattoman tukiaseman uudelleensijoittamista karttanäkymässä.



KUVA 37: Loki järjestelmän asetuksiin tehdyistä muutoksista

6.5 Johtopäätökset käyttöönotosta

Langattoman verkon tukiaseman käyttöönoton myötä sain rakennettua uuden ympäristön, joka sallii ylläpitäjälleen runsaat ominaisuudet ja vaihtoehdot verkon liikenteen valvontaan sekä mahdollisuuteen sen rajoittamisessa. Ympäristön laajentaminen lisätukiasemilla onnistuu nopeasti ja kiitos Cisco Merakin pilvihallinnan, asetuksien määritys verkkoon kytkettyihin tukiasemiin suoritetaan automaattisesti pilvihallinnan kautta niin valikoitaessa.

Langattoman verkon konfigurointi toteutettiin nykyisiin tarpeisiin ja pilvipalvelun mahdollistamien toiminnollisuuksien ja analysoinnin myötä langatonta lähiverkkoa ei tarvittu erikseen mitoittaa, vaan järjestelmä sääti laitteen asetukset automaattisesti parhaiksi mahdollisiksi. Myös verkon tietoturva on huomattavasti parempi, kun verkon laitteiden ohjelmistopäivitykset asennetaan automaattisesti ja verkossa havaitut poikkeukset tai hyökkäykset voidaan havainnoida, analysoida ja toimenpiteet niiden korjaamiseksi aloittaa automaattisesti ja ylläpitäjää tiedottaen.

Langattoman lähiverkon käyttöönotossa ei tullut eteen maininnan arvioisia ongelmia eikä pilvipalveluna toteutetussa hallintapaneelissa tai itse verkon toiminnassa havaittu vikatilanteita. Käyttöönoton helppoudesta huolimatta pilvipalvelun käyttö tai konfigurointi vaatii tekijältään huomattavaa osaamista ja ymmärrystä tietoverkoista sekä näiden termistöstä. Kun tuotteen ja sen mukana tulevan pilvipalvelun tavoitteena on tyydyttää eri käyttökohteiden ja asiakkaiden tarpeet, tuloksena on usein huomattavasti normaalia monipuolisempi ja samalla monimutkaisempi tuote.

7 POHDINTA

Tässä opinnäytetyössä perehdyin pilvilaskennan sekä pilvipalveluiden historiaan lyhyesti ja tutkin sitä, miten pilvipalvelut ovat yleistyneet vuoteen 2017 mennessä ja sen aikana. Lisäksi tutkin, miten pilvipalveluiden hyödyntäminen ja konsepti on tuotu myös tietoverkkojen maailmaan ohjelmistopohjaisten tietoverkkojen muodossa. Tutustuin pilvipalvelupohjaisiin Cisco Meraki -tuoteperheen verkkolaitteisiin ja mitä toiminnallisuutta ja uusia mahdollisuuksia ne tuovat tietoverkkojen käyttöönottoon, ylläpitoon, valvontaan, hallintaan sekä tietoturvaan.

Lopuksi otin käyttöön Cisco Meraki MR33 -langattoman tukiaseman uudessa ympäristössä ja tutkin mitä vaatimuksia, ominaisuuksia ja toiminnollisuuksia langaton tukiasema ja sen pilvipalveluna Internetin ylitse tuotettu hallinta mahdollistavat. Käyttöönoton yhteydessä saatiin tarvittava näkemys ja osaaminen vastaavanlaisen ympäristön suunnittelemiseen sekä toteuttamiseen, mutta myös yleisesti Internetin ylitse toimivan ja pilvipalveluna tuotetun hallinnan ja sen tuomista mahdollisuuksista tietoverkkojen eri komponenttien ja laitteiden konfiguroinnissa ja hallinnassa.

Cisco Meraki ja vastaavanlaiset ratkaisut ovat saapuneet markkinoille ja saavuttaneet palveluntarjoajien sekä yritysasiakkaiden huomion vuodesta 2015 alkaen ja vuodesta 2017 eteenpäin ennusteiden mukaan kasvu tulee olemaan merkittävä ja alati kiihtyvä. Pilvipalvelut ja muut Internetin ylitse saavutettavissa olevat palvelurajapinnat eivät ole aukottomia, eivätkä välttämättä koskaan tule olemaan. Viimeisien vuosien aikana olemme voineet huomata eri uutislähteistä, miten asiakasyrityksien sekä kuluttajien tietoteknisten laitteiden suojaaminen ja päivittäminen ovat entistä tärkeämpää ja osa myös jokaisen kuluttajan ja loppukäyttäjän vastuuta.

Palveluntarjoajat ovat tuoneet kuluvan vuoden aikana runsaasti uusia pilvipalveluita hyödyntäviä tuotteita, jotka osaavat muun muassa asentaa ohjelmistopäivitykset automaattisesti. Tämä on sekä kuluttajien ja yritysasiakkaiden etu, sillä ne vähentävät loppukäyttäjän vaatimaa työtä ja siitä aiheutuvia keskeytyksiä. Käytännössä kuluttajien sekä yritysasiakkaiden täytyy ottaa huomioon erilaiset riskit ja valita käytettävä tuote sekä palvelumalli siten, että palvelutasosopimus, toiminnallisuus sekä luotettavuus tuottavat käyttäjilleen parhaan mahdollisen kokonaisratkaisun.

Tulevaisuudessa pilvipalveluiden hyödyntäminen ja sen markkinaosuus tulee jatkamaan kasvua sekä asiakasyrityksissä, että myös kuluttajamarkkinoilla palveluiden kustannuksien laskiessa ja uusien tuotteiden ja palvelumallien saapuessa kaikkien asiakasryhmien saataville. Pilvipalvelut ja pilvihallittavat tietoverkot ovat laajoja käsitteitä, mitä on mahdollista pilkkoa myös moniin pienempiin osa-alueisiin.

Opinnäytetyön lähtökohtana tekijä ei omannut aikaisempaa kokemusta pilvipalveluna tuotettavista verkkoratkaisuista, mutta oli tietoinen näiden olemassaolosta ja markkinatilanteesta. Työn aikana saadut tulokset ja niistä luodut johtopäätökset perustuvat yleisesti luotettuihin lähteisiin, omaan kokemukseen ja tutkimustuloksiin. Tekijä on alan ammattilainen, joka omaa viiden vuoden kokemuksen yritysasiakkaiden verkko- ja järjestelmäinfrastruktuureista sekä näiden ylläpidosta. Tutkimustulokset ja johtopäätökset ovat tämän ja alan kokemuksen perusteella aiheelleen eettisiä, luotettavia ja onnistuneita.

Tätä opinnäytetyötä tehdessä ilmaantui useita jatkotutkimusaiheita sekä pilvihallittavien tietoverkkojen, että muiden tietoturvaa parantavien tietoverkko- ja pilvipalveluratkaisujen piirissä. Pilvihallittavien tietoverkkojen mahdollisia tutkimusaiheita ovat muun muassa Cisco Merakin kilpailijat kuten Hewlett-Packard Enterprisen ja Aruba Networksin keskenään lanseeraama tuoteperhe. Tietoverkkojen SD-WAN ja muut ohjelmistoperustaiset tietoverkkoratkaisut ovat saapumassa sekä verkko-operaattoreiden, että yritysasiakkaiden hyödynnettäväksi jo vuoden 2017 aikana.

Tietoturva-aspektista palomuurien kehittyneet toiminnallisuudet sekä tietoverkkojen AMP ja IPS -ratkaisut ovat yleistymässä yritysasiakkaiden verkkoympäristöissä nopeasti. Pilvipalveluiden myötä tekoäly ja koneoppiminen tekevät saapumistaan niin yritysasiakkaiden kuin myös kuluttajien tuotteisiin. Näiden toiminnollisuuksia on mahdollista hyödyntää Cisco Merakin palomuurituotteissa, sekä myös kilpailevien toimijoiden tuotteissa kuten F-Securen SENSE, kuluttajille suunnattu ja pilvipalveluita sekä tekoälyä hyödyntävä verkkoreititin. Monet listatuista jatkotutkimusaiheista ovat vielä toistaiseksi alaa opiskeleville tuntemattomia, mutta sellaisia joiden ymmärtäjille ja ammattilaisille on kasvava tarve tieto- ja viestintätekniikan alalla tulevien lähivuosien aikana.

LÄHTEET

Mell & Grance. 2011. The NIST Definition of Cloud Computing. Julkaistu 2011. Tulostettu 9.9.2017. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Zhao. 2013. Cloud Computing Model as Service Oriented Architecture. Julkaistu 3.3.2013. Tulostettu 9.9.2017. https://www.slideshare.net/yan_zhao/cloud-computing-model

Forbes. 2017. Cloud 2.0: Companies Move From Cloud-First To Cloud-Only. Julkaistu 7.4.2017, Tulostettu 10.9.2017. https://www.forbes.com/sites/vmware/2017/04/07/cloud-2-0-companies-move-from-cloud-first-to-cloud-only/#1e8b8dc04d5e

State of the Cloud Report. 2017. RightScale. Julkaistu 2017. Tulostettu 23.9.2017. https://www.rightscale.com/lp/state-of-the-cloud

Huwitz, Kaufman, Halper & Kirsch. N.d. What is Hybrid Cloud Computing? Tulostettu 16.9.2017. http://www.dummies.com/programming/cloud-computing/hybrid-cloud/what-is-hybrid-cloud-computing/

Stamey. 2017. IaaS vs. PaaS vs. SaaS Cloud Models. Julkaistu 30.5.2017. Tulostettu 23.9.2017. http://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/

Hegde. 2017. The Rise of Anything as a Service (XaaS): The New Hulk of Cloud Computing. Julkaistu 13.4.2017. Tulostettu 16.9.2017. https://www.botmetric.com/blog/xaas-new-hulk-cloud-computing/

Microsoft. N.d. Azure regions. Tulostettu 29.10.2017. https://azure.microsoft.com/en-us/regions/

Amazon. N.d. AWS Global Infrastructure. Tulostettu 29.10.2017. https://aws.amazon.com/about-aws/global-infrastructure/

Sdxcentral. N.d. What is Cloud Networking of Cloud Based Networking. Tulostettu 17.9.2017. https://www.sdxcentral.com/cloud/definitions/all-about-cloud-networking/

Wexler. 2011. Aerohive Buys Cloud Startup Pareto Networks. Julkaistu 18.1.2011. Tulostettu 17.9.2016. https://www.networkworld.com/article/2198882/wireless/aerohive-buys-cloud-startup-pareto-networks.html

Constine. 2012. Cisco Acquires Enterprise Wi-Fi Startup Meraki For $1.2 Billion In Cash. Julkaistu 18.11.2012. Tulostettu 17.9.2017. https://techcrunch.com/2012/11/18/cisco-acquires-enterprise-wi-fi-startup-meraki-for-1-2-billion-in-cash/

Nohling. 2016. Multi-Site Network Architecture: Handling Challenges That Lie Ahead. Julkaistu 20.9.2016. Tulostettu 17.9.2016. https://www.edgewaternetworks.com/blog/multi-site-network-architecture-challenges-ahead

Saarelainen. 2016. Sdn-teknologia mullistaa verkot ja tuo kilpailuetua. Julkaistu 13.1.2016. Tulostettu 23.9.2017. http://www.tivi.fi/Kaikki_uutiset/sdn-teknologia-mullistaa-verkot-ja-tuo-kilpailuetua-6244259

Garson & Greenfield. 2016. Gartner predicts SD-WANs to replace routers, but which SD-WAN is the question. Julkaistu 16.11.2016. Tulostettu 23.9.2017. https://www.networkworld.com/article/3142053/lan-wan/gartner-predicts-sd-wans-to-replace-routers-but-which-sd-wan-is-the-question.html

Garson. 2016. How Does SD-WAN Work? Julkaistu 4.1.2016. Tulostettu 2.11.2017. https://www.sd-wan-experts.com/blog/how-does-sd-wan-work/

Sequoia. N.d. Meraki. Tulostettu 1.10.2017. https://www.sequoiacap.com/companies/meraki/

About Meraki. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/company/about

Cisco Meraki Service Level Agreement. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/trust#sla

EU Privacy and Data Protection Compliance. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/trust#privacy

Cisco Meraki Datacenter Design. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/trust#data-centers

Computerworld. 2014. Levi's stadium app makes use of Aruba beacons to help 49ers fans get around. Julkaistu 4.11.2014. Tulostettu 1.10.2017. https://www.computerworld.com/article/2842829/levis-stadium-app-makes-use-of-aruba-beacons-to-help-49ers-fans-get-around.html

Technologies: RF Optimization. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/technologies/rf-optimization

Technologies: Application QoS. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/technologies/application-qos

Air Marshal. N.d. Tulostettu 1.10.2017. https://meraki.cisco.com/lib/pdf/meraki_datasheet_airmarshal.pdf

Cisco Meraki Licensing. N.d. Tulostettu 8.10.2017. https://documentation.meraki.com/zGeneral_Administration/Licensing/Cisco_Meraki_Licensing

Technologies: Content Filtering. N.d. Tulostettu 8.10.2017. https://meraki.cisco.com/technologies/content-filtering

Advanced Malware protection for Meraki MX. N.d. Tulostettu 8.10.2017. https://meraki.cisco.com/amp?utm_source=overview%20features&utm_medium=overview&utm_campaign=AMP%20launch%202016

How MX Customers Contained Heartbleed In a Day. 2014. Julkaistu 17.4.2014. Tulostettu 8.10.2017. https://meraki.cisco.com/blog/2014/04/how-mx-customers-contained-heartbleed-in-a-day/

Technologies: Auto VPN. N.d. Tulostettu 8.10.2017. https://meraki.cisco.com/technologies/auto-vpn

Technologies: Stacking. N.d. Tulostettu 8.10.2017. https://meraki.cisco.com/technologies/stacking

Technologies: Voice Optimization. N.d.. Tulostettu 8.10.2017. https://meraki.cisco.com/technologies/voice-optimization

North American Object Storage Service Impact. 2017. Julkaistu 4.8.2017. Tulostettu 8.10.2017. https://documentation.meraki.com/zGeneral_Administration/Support/North_American_Object_Storage_Service_Impact_(8-4-2017)#Revision_History

Indoor Access Points: MR33. N.d. Tulostettu 15.10.2017. https://meraki.cisco.com/products/wireless/mr33#tech-specs

LIITTEET

Liite 1. Cisco Meraki MR33 -tukiaseman tekniset tuotetiedot

1 (3)

Radios:
2.4 GHz 802.11b/g/n client access radio
5 GHz 802.11a/n/ac client access radio
2.4 GHz & 5 GHz WIDS/WIPS, spectrum analysis, and location analytics radio
2.4 GHz Bluetooth Low Energy (BLE) radio with beacon and BLE scanning support
Concurrent operations of all four radios
Supported frequency bands (country-specific restrictions apply):
2.412-2.484 GHz
5.150-5.250 GHz (UNII-1)
5.250-5.350 GHZ (UNII-2)
5.470-5.600, 5.660-5.725 GHz (UNII-2e)
5.725 -5.825 GHz (UNII-3)

802.11ac and 802.11n Capabilities:
2 x 2 multiple input, multiple output (MIMO) with two spatial streams
SU-MIMO and MU-MIMO support
Maximal ratio combining (MRC) & Beamforming
20 and 40 MHz channels (802.11n), 20, 40, and 80 MHz channels (802.11ac)
Up to 256 QAM on both 2.4 GHz and 5 GHz bands
Packet aggregation

Power:
Power over Ethernet: 37 - 57 V (802.3af compatible)
Alternative 12 V DC input
Power consumption: 11W max (802.3af)
Power over Ethernet injector and DC adapter sold separately

(jatkuu)

Mounting:
All standard mounting hardware included
Desktop, ceiling, and wall mount capable
Ceiling tile rail (9/16, 15/16 or 1 ½" flush or recessed rails), assorted cable junction boxes
Bubble level on mounting cradle for accurate horizontal wall mounting

Physical Security:
Two security screw options (included)
Kensington lock hard point
Concealed mount plate with anti-tamper cable bay

Environment:
Operating temperature: 32 °F to 104 °F (0 °C to 40 °C)
Humidity: 5 to 95% non-condensing

Physical Dimensions:
8.5" x 4.3" x 1.3" (215 mm x 110 mm x 32 mm), not including mount feet or plate
Weight: 13.2 oz (376.5 g)

Antenna:
Integrated omni-directional antennas (3.8 dBi gain at 2.4 GHz, 3.9 dBi gain at 5 GHz)

Interfaces:
1x 10/100/1000 BASE-T Ethernet (RJ45)
1x DC power connector (5.5 mm x 2.5 mm, center positive)

Security:
Integrated layer 7 firewall with mobile device policy management
Real-time WIDS/WIPS with alerting and automatic rogue AP containment with Air Marshal
Flexible guest access with device isolation
VLAN tagging (802.1Q) and tunneling with IPSec VPN
PCI compliance reporting

(jatkuu)

WEP, WPA, WPA2-PSK, WPA2-Enterprise with 802.1X
EAP-TLS, EAP-TTLS, EAP-MSCHAPv2, EAP-SIM
TKIP and AES encryption
Enterprise Mobility Management (EMM) & Mobile Device Management (MDM) integration

Quality of Service:
Advanced Power Save (U-APSD)
WMM Access Categories with DSCP and 802.1p support
Layer 7 application traffic identification and shaping

Mobility:
PMK, OKC, and 802.11r for fast Layer 2 roaming
Distributed or centralized layer 3 roaming

LED Indicators:
2 Ethernet status
1 power/booting/firmware upgrade status

Warranty:
Lifetime hardware warranty with advanced replacement included

Compliance:
RoHS
EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC

Ordering Information:
MR33-HW: Meraki MR33 Cloud Managed 802.11ac AP
MA-PWR-30W-XX: Meraki AC Adapter for MR Series (XX = US, EU, UK or AU)
MA-INJ-4-XX: Cisco Meraki 802.3at Power over Ethernet Injector (XX = US, EU, UK or AU)
Note: Meraki Enterprise license required.