jamk.fi

Cloud Managed Network

Cisco Merakin tuotteistus

Tomi Hasanen

Opinnäytetyö
Toukokuu 2019
Tekniikan ja liikenteen ala
Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoverkkotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Hasanen, Tomi	Opinnäytetyö, AMK	Toukokuu 2019
	Sivumäärä 63	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Cloud Managed Network
Cisco Merakin tuotteistus

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Rantonen Mika, Saharinen Karo

Toimeksiantaja(t)
Telia Cygate Oy

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Telia Cygate Oy, joka tuottaa asiakkaille erilaisia tietoturvallisia ICT-palveluja ja ratkaisuja. Työn tavoitteena oli tutkia pilvipohjaisesti hallittavaa verkkoa Cisco Merakin pilvipohjaisesti hallittavan ympäristön avulla. Tavoitteena oli toteuttaa ja vertailla pilvipohjaisesti hallittavan verkon tuomia etuja perinteisempään verkkototeutukseen.

Opinnäytetyön toteutusosaa varten käytössä oli fyysisiä laitteita ja ne konfiguroitiin hallintapaneelista käyttövalmiiksi. Verkon fyysisiä laitteita olivat Cisco Merakin Security Appliance ja WLAN-tukiasema. Konfigurointi tapahtui Template-ominaisuutta käyttäen, jolla laitteiden etukäteen konfigurointi onnistui ennen laitteiden liittämistä verkkoon. Lisäksi konfiguroitiin erikseen kytkin, joka lisättiin verkkoon myöhemmin. Hallintapaneelin ominaisuuksia sekä sen tarjoamia valvonnan ja vianselvityksen työkaluja tutkittiin. Lisäksi kokeiltiin sen reagointia itse aiheutettuihin vikatilanteisiin.

Opinnäytetyön tuloksena saatiin todisteita pilvipohjaisesti hallittavan verkon tuomasta tehokkuudesta tuotettavana palveluna perinteiseen valvonta- ja hallintapalveluun verrattuna. Laitteiden konfigurointi voitiin toteuttaa etukäteen templatella. Template-ominaisuus toi mahdollisuuden siihen, että erilaisiin ympäristöihin voidaan suunnitella ja toteuttaa vakioitu kokonaisarkkitehtuuri. Ympäristössä pystytään toteuttamaan monimutkaisempia standardimuutoksia ilman, että riskit kasvavat. Massamuutoksien toteuttaminen olisi template-ominaisuuden avulla tehokkaampaa. Monipuolisilla valvontatyökaluilla voitiin laitteiden tiloja seurata reaaliaikaisesti ja tarvittaessa reagoida vikatilanteisiin. Häiriötilanteiden elinkaarta pystyttiin lyhentämään automatisoidun viantunnistuksen ja vianselvitykseen suunniteltujen työkalujen ansiosta.

Avainsanat (asiasanat)
Cisco Meraki, Cloud-Based Networking, Cloud Management, SD-WAN, WLAN

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Hasanen, Tomi	Bachelor's thesis	May 2019
		Language of publication: Finnish
	Number of pages: 63	Permission for web publication: x

Title of publication
Cloud Managed Network productization of Cisco Meraki

Degree programme
Information and Communications Technology, Data Network Technology

Supervisor(s)
Rantonen Mika, Saharinen Karo

Assigned by
Telia Cygate Oy

Abstract

The bachelor's thesis was assigned by Telia Cygate Oy, which provides secure ICT-services and solutions for customers. Purpose of the thesis was to explore and implement a cloud-managed network with Cisco Meraki's cloud-managed networking product. The main goal was to compare the benefits of a cloud managed network to more traditional network implementation.

The thesis was implemented with physical equipment. Devices were configured from the dashboard to be ready to use. Physical devices of the network were Cisco Meraki's Security Appliance and WLAN access point. Configuration was done using the Template feature, which made pre-configuration of the devices possible, before devices were even connected to the network. In addition, one switch was individually configured, even though the switch was added later to the network. Features, monitoring and troubleshooting tools of the dashboard were studied and tested. Automatic fault detection was also tested by self-triggering fault situations.

As a result of the thesis, evidence from the efficiency of the cloud managed network as a produced service was obtained, while comparing it to traditional monitoring and management service. Configurations of devices could be implemented in advance. This feature brought an opportunity to design and implement a standardized architecture for environments. More complex standard changes can be implemented without increasing risks. Mass changes were more efficient because of centralized management. The life cycle of incidents was shortened due to automated fault detection and tools designed for troubleshooting.

Keywords/tags (subjects)
Cisco Meraki, Cloud-Based Networking, Cloud Management, SD-WAN, WLAN

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

AF	Assured Forwarding
ARP	Address Resolution Protocol
CLI	Command Line Interface
CS	Class Selector
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DNS	Domain Name System
DSCP	Differentiated Service Code Point
EF	Expedited Forwarding
FIFO	First In First Out
GHz	Gigahertz
ICMP	Internet Control Message Protocol
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITOC	Information Technology Operation Center
LAN	Local Area Network
LLC	Logical Link Control
L2	Layer 2
L3	Layer 3
MAC	Media Access Control
MIMO	Multiple-Input and Multiple-Output
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NIC	Network Interface Controller
OFDMA	Orthogonal Frequency-Division Multiple Access
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PaaS	Platform as a Service
PoE	Power over Ethernet
PSK	Pre-shared Key
QoS	Quality of Service
QSFP	Quad Small Form-Factor Pluggable Transceiver
RF	Radio Frequency
RMA	Return Merchandise Authorization
SaaS	Software as a Service
SFP	Small Form-Factor Pluggable Transceiver
SIP	Session Initiation Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SDN	Software Defined Network

SD-WAN	Software Defined Wide Area Network
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLAAC	Stateless Address Autoconfiguration
SSL	Secure Sockets Layer
TAC	Technical Assistance Center
TCP/IP	Transmission Control Protocol / Internet Protocol
ToS	Type of Service
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMM	Wireless Multimedia Extension
WPA	Wi-Fi Protected Access

1 Johdanto

1.1 Toimeksiantaja ja tavoitteet

Opinnäytetyön toimeksiantajana oli Telia Cygate Oy. Telia Cygate Oy on laajasti IT-alalla toimiva yritys, joka tarjoaa asiakkaille erilaisia ICT-ratkaisuja ja palveluita esimerkiksi verkkojärjestelmien, konesalien ja pilviteknologioiden osa-alueilta. Yritys perustettiin vuonna 1990, ja se toimii osana Telia Company -konsernia. Toimipisteitä Telia Cygate Oy:lla on Suomessa seitsemän, joista pääkonttori sijaitsee Helsingissä. Yrityksellä on 24/7 palvelukeskus ITOC (IT Operations Center), joka valvoo asiakkaiden IT-infrastruktuurin toimintaa jatkuvasti ja pyrkii takaamaan ympäristöjen toimivuuden vuoden jokaisena päivänä. (Telia Cygate Oy n.d.)

Opinnäytetyön toimeksiantona oli tutkia ja tutustua Cisco Merakin pilvipohjaisesti hallittavaan ympäristöön ja vertailla sen ominaisuuksia perinteiseen, monen laitevalmistajan laitteilla toteutettuun verkkoon. Opinnäytetyössä käydään läpi teoriaa pilvipohjaisesti hallittavan verkon arkkitehtuurista, Cisco Merakista ja ITIL-käytänteistä lyhyesti. Käyttöönotto suunniteltiin ja toteutettiin laboratorioympäristössä Cisco Merakin laitteilla. Laitteiden konfigurointi tehtiin Cisco Merakin hallintapaneelista ja samalla tutkittiin sen työkaluja sekä ominaisuuksia. Lopuksi analysoitiin tuloksien osalta pilvipohjaisesti hallittavan verkon etuja perinteiseen verkonvalvontaan sekä hallintaan verraten.

1.2 Tutkimusmenetelmät

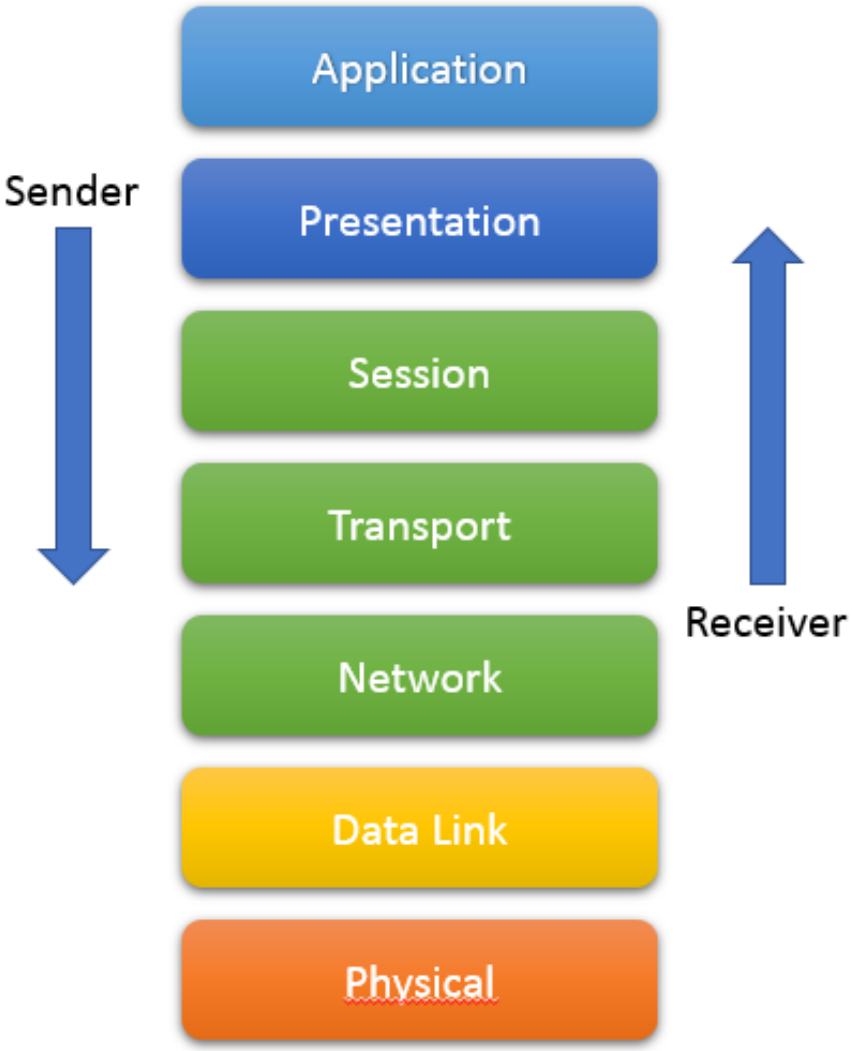
Opinnäytetyön tutkimusmenetelmä oli kvalitatiivinen, koska tavoitteena oli tutkia pilvipohjaisesti hallittavan verkon ominaisuuksia ja laatua. Laadulliseen tutkimukseen mahtuu useita muitakin tutkimusmenetelmiä samaan aikaan (Laadullinen analyysi 2015). Siksi yhtenä tutkimusmenetelmänä opinnäytetyössä toimi vertaileva tutkimus. Vertailun kohteena toimivat pilvipohjaisesti hallittavan verkon sekä perinteisen verkon erot niiden ominaisuuksien ja hallittavuuden näkökulmasta. Pilvipohjaisesti hallittavasta verkkoympäristöstä kerättiin tietoa myös havainnoimalla sen

ominaisuuksia sekä testaamalla sen reaktioita vikatilanteisiin. Keskeisenä kysymyksenä käsiteltiin, mitä etuja pilvipohjaisesti hallittavalla verkolla on perinteiseen verkkoon verrattuna?

2 Tekniikat ja käytänteet

2.1 OSI-malli

OSI (Open Systems Interconnection) on seitsemän kerroksen arkkitehtuuri, jossa jokaisella kerroksella on oma tehtävänsä. Nämä kaikki seitsemän kerrosta työskentelevät yhdessä datan kuljetuksessa kahden päätelaitteen välillä (ks. kuvio 1). Jokaisella kerroksella on oma tärkeä tehtävänsä verkkokommunikoinnissa. Sekä lähettäessä että vastaanottaessa mennään jokaisen kerroksen läpi. Vaikka TCP/IP (Transmission Control Protocol / Internet Protocol) on virallinen käytössä oleva standardi, on OSI-malli joka tapauksessa erittäin hyvä esimerkki kokonaisarkkitehtuurin ymmärtämistä varten. (Raza 2018.)



Kuvio 1. OSI-mallin seitsemän kerrosta (Raza 2018)

Physical Layer

Fyysinen kerros sijaitsee OSI-mallissa ensimmäisenä kerroksena ja se kuvaa kahden fyysisen laitteen välistä yhteyttä. Informaatio on tällä välillä bittimuodossa. Esimerkiksi laitteiden välissä olevaa kaapelia pitkin tai radiolla langattomasti signaloimalla bitit kulkevat, kunnes ne pääsevät laitteelle tiedonsiirtokerrokseen, jolloin bitit kerätään yhteen kehykseksi. (Raza 2018.)

Data Link Layer

Tiedonsiirtokerros huolehtii siitä, että laitteiden välillä oleva tiedonsiirto on virheetöntä fyysisen kerroksen läpi mennessä. Tiedonsiirtokerros on vastuussa paketin lähettämisestä eteenpäin verkossa. Apuna käytetään kahta alikerrosta, jotka ovat MAC (Media Access Control) ja LCC (Logical Link Control). Vastaanottajan MAC osoite saadaan selville vastaanottajan IP-osoitetta käyttäen ARP-kyselyssä, jota lähetetään kaikille verkon laitteille. Mikäli verkosta löytyy laite, jolla on käytössä vastaanottajan IP-osoite, vastaa laite ARP-kyselyyn MAC-osoitteensa kanssa. Tiedonsiirtokerroksesta huolehtii NIC (Network Interface Card) eli verkkokortti. (Raza 2018.)

Network Layer

Verkkokerroksessa huolehditaan datan lähetyksestä toisiin verkkoihin. Tämä vaatii pakettien reititystä joko dynaamisella reititysprotokollalla tai staattisilla reiteillä. Lähettäjän ja vastaanottajan IP-osoitteet lisätään verkkokerroksen toimesta paketin ylätunnisteeseen. (Raza 2018.)

Transport Layer

Kuljetuskerros varmistaa, että data kuljetetaan lähettäjältä vastaanottajalle kokonaisena ja virheettömänä. Se vastaanottaa dataa ylemmiltä kerroksilta ja segmentoi sen pienempiin osiin. Vastaanottopäässä data kootaan jälleen yhteen segmenteistä. TCP:n tapauksessa kuljetuskerros muodostaa yhteyden lähettäjän ja vastaanottajan välille kättelemällä, lähettää dataa ja lopuksi sulkee yhteyden kättelemällä, kun lähetys on ohi. Se myös lähettää virheen sattuessa datan uudelleen ja ilmoittaa onnistuneesta tiedonsiirrosta lähettäjälle. Kuljetuskerroksen ylätunnisteeseen lisätään palvelun käyttämä porttinumero, jotta se löytää oikeaan prosessiin vastaanottopäässä. UDP (User Datagram Protocol) ei muodosta ollenkaan yhteyttä lähettäjän ja vastaanottajan välille, vaan se yksinkertaisesti lähettää dataa eteenpäin. Pakettien kulkua ja vastaanottamista ei varmisteta ollenkaan, jolloin data ei välttämättä saavu vastaanottajalle kokonaisena ja virheettömänä. UDP mahdollistaa tiedonsiirron ja sitä käytetään muunmuassa videokuvan reaaliaikaisessa lähetyksessä, missä pienestä pakettihävikistä ei ole niin suurta haittaa. (Raza 2018.)

Session Layer

Istuntokerros huolehtii yhteyden muodostamisesta, session ylläpitämisestä, autentikoinnista ja turvallisuudesta. Hyvänä esimerkkinä toimivat verkkosivut, missä sessio loppuu, kun ei tee mitään hetkeen sivustolla. Käyttäjä joutuu kirjautumaan uudelleen sivustolle, ennen kuin sivuston käyttämistä tai siellä työskentelyä voidaan jatkaa. Istuntokerroksella varmistetaan myös, että dataa ei katoa välistä ja se tulee perille virheettömänä. (Raza 2018.)

Presentation Layer

Esittelykerroksessa vastaanotetaan data ylemmästä kerroksesta ja muutetaan se tarvittavaan muotoon, jolloin se voidaan kuljettaa verkon yli. Tässä kerroksessa hoidetaan esimerkiksi datan salaus ja salauksen poisto sekä datan pakkaus. (Raza 2018.)

Application Layer

Sovelluskerros on OSI-mallin ylin kerros. Siellä toimivat erilaiset verkkosovellukset, kuten esimerkiksi selaimet, sähköpostipalvelut ja erilaiset viestintäsovellukset. Nämä sovellukset luovat dataa, joka pitää kuljettaa verkon yli vastaanottajalle. (Raza 2018.)

2.2 Pilvipalvelut

Pilvipalvelut ovat verkon yli saatavia resursseja eri käyttötarkoituksia varten. Tarjolla on esimerkiksi tallennustilaa tiedostoille ja hosting-palveluita sovelluksille sekä palvelimille. Pilvipalveluilla pyritään tarjoamaan IT-resursseja alhaisilla hinnoilla. Palvelut ovat saatavilla ympäri maailmaa internetyhteyden välityksellä. Yksittäisten käyttäjien ja yritysten ei tarvitse erikseen hankkia laitteistoa palvelinten tai sovelluksien ylläpitämiseen. Pilvipalvelut toimivat usein isoissa konesaleissa, joista asiakkaat voivat ostaa itselleen käyttöön resursseja tarvitsemansa määrän. (What is cloud computing n.d.)

Julkinen pilvi on kolmannen osapuolen tarjoama pilvipalvelualusta, joka tarjoaa yrityksille ja yksittäisille käyttäjille resursseja internetin välityksellä. Yksityinen pilvi

on taas organisaation sisäinen pilvipalvelu, jota pyöritetään yrityksen omassa konesalissa. Yksityistä pilveä voidaan käyttää vain yrityksen omaan verkkoon yhdistyneenä. Lisäksi on hybridimuodossa olevia pilviä, joissa on sekä yksityisiä että julkisia pilvipalveluja tarjolla. Hybridimuotoisessa pilvessä on mahdollisuus jakaa sovelluksia ja dataa yksityisen ja julkisen pilven välillä. (What is cloud computing n.d.) Pilvipalvelut voidaan jakaa kolmeen pääkategoriaan:

IaaS (Infrastructure as a Service) tarjoaa IT-infrastruktuurin yrityksille pilven kautta. Ympäristö sisältää usein virtuaalisia palvelimia ja tallennustilaa yrityksen tarpeiden mukaisesti. Asiakkaat voivat valita resurssien määrän palvelulle ja tarvittaessa kasvattaa niiden kapasiteetteja. (What is IaaS n.d.)

PaaS (Platform as a Service) tarjoaa kaiken mitä IaaS, mutta lisäksi palveluun sisältyy käyttöjärjestelmät, hallinnointijärjestelmät esimerkiksi tietokannoille ja kehitystyökalut sovelluksille. PaaS tarjoaa ympäristölle ohjelmistolisenssit ilman että niitä joudutaan hankkimaan ulkopuolisesta lähteestä ympäristölle. (What is PaaS n.d.)

SaaS (Software as a Service) tarjoaa sovelluspalveluita, joista tunnetuimpiin lukeutuu Microsoft Office 365. Työntekijät pääsevät käyttämään internetin yli sovelluspalveluja, jossa pyörivät toimistolle tärkeät työkalut ja sähköpostilaatikot. Muita tunnettuja sovelluspalveluita ovat esimerkiksi Dropbox, joka tarjoaa käyttäjille tallennustilaa ja Slack, joka mahdollistaa reaaliaikaisen kommunikoinnin yrityksen tai muun organisaation sisällä. (What is SaaS n.d.)

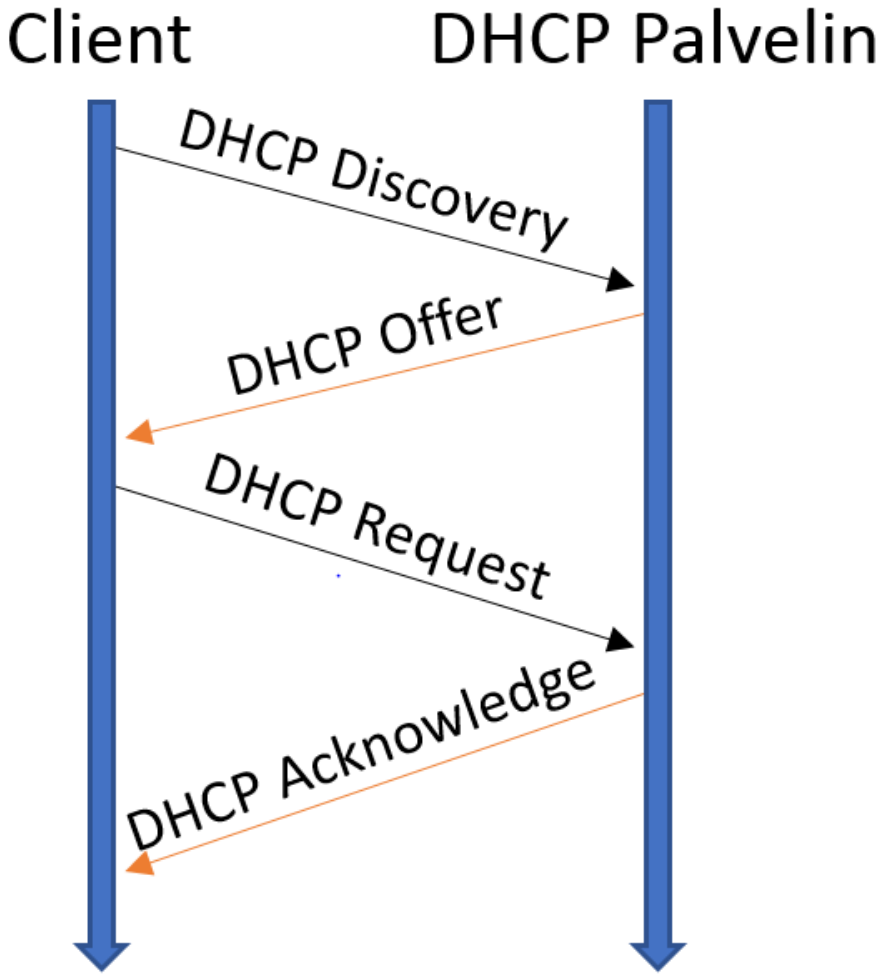
2.3 DHCP

DHCP (Dynamic Host Configuration protocol) tuo mahdollisuuden viedä TCP/IP-konfiguraatiot loppukäyttäjien laitteille verkon kautta. DHCP:n avulla voidaan verkon laitteille allokoida IPv4- tai IPv6-osoite käyttöön automaattisesti riippuen verkon toteutuksesta. Tosin vaikka IPv6:n ominaisuuksiin kuuluu jo ennestään SLAAC

(Stateless Address Autoconfiguration), ei siinä ole kaikkia ominaisuuksia, joita DHCP tuo mukanaan. (Droms 1997.)

DHCP-palvelimelle voidaan eri verkon osille luoda omia IP-pooleja, joista jaetaan päätelaitteille osoitteet määriteltyjen VLAN:ien (Virtual Local Area Network) mukaisesti. Sillä voidaan päätelaitteille viedä myös tieto oletusyhdyskäytävän ja nimipalvelimien osoitteista. DHCP-liikenne ei ole reitittyvää ja sen toiminta perustuu broadcastin tehokkaaseen käyttöön lähiverkossa. Mikäli DHCP-palvelin sijaitsee eri verkossa, DHCP-pyynnöt voidaan lähettää reitittimen, L3-kytkimen tai palomuurin DHCP Relay -ominaisuuden tai toiselta nimeltään IP-helperin avulla. IP-helper määritellään laitteen konfiguraatioon, jonka avulla DHCP-pyynnöt lähetetään eteenpäin määriteltyä osoitetta kohti DHCP-palvelimelle. DHCP on erittäin kätevä isoissa verkoissa, koska erilaisia verkon päätelaitteita voi olla runsaasti ja jokainen niistä tarvitsee konfiguraation. DHCP:n avulla säästetään aikaa, koska verkon jokaista laitetta ei tarvitse konfiguroida erikseen. (Droms 1997.)

Kun uusi laite liittyy verkkoon, se yrittää usein laitteen asetuksista johtuen etsiä DHCP-palvelinta konfiguraation vastaanottoa varten lähettämällä ”Discovery” paketin koko verkkoon. Mikäli verkosta löytyy DHCP-palvelin, se vastaa takaisin lähettämällä Offer-paketissa vapaan IP-osoitteen ja muita määriteltyjä asetuksia verkon käyttöä varten. Päätelaite pyytää lupaa käyttää osoitetta ja asetuksia Request-paketilla ja lopuksi palvelin ilmoittaa Acknowledge-paketilla saaneensa tiedon tästä. Keskustelua DHCP-palvelimen ja laitteen välillä kutsutaan DHCP-prosessiksi (ks. kuvio 2). DHCP-palvelimen päätelaitteelle jakamalla IP-osoitteella on usein määritelty tietty käyttöaika, joka pitää uusia päätelaitteen ja palvelimen välisellä kommunikaatiolla. Mikäli kyseinen IP-osoitteen käyttöaika loppuu, se lisätään takaisin vapaiden IP-osoitteiden joukkoon odottamaan uutta käyttäjää. (Droms 1997.)



Kuvio 2. DHCP-prosessin aikajana laitteen ja palvelimen välillä (Droms 1997.)

2.4 802.11ax ja 802.11ac

IEEE (Institute of Electrical and Electronics Engineers) 802.11ax ja IEEE 802.11ac ovat langattomien lähiverkkojen standardeja. 802.11ac käyttää 5 GHz:n taajuutta hyväkseen. Tukiasemat tukevat usein sekä 2.4 GHz:n että 5 GHz:n tuella, joten laitteet 2.4 GHz:n taajuuksilla käyttävät 802.11n tekniikkaa. 2.4 GHz taajuusalueella on käytössä vain kolme kanavaa, jotka eivät kuulumisellaan häiritse toisiaan. Mikäli lähialueella tukiasemia on enemmän, voi samalla kuuluvuusalueella olevat kanavat häiritä toisiaan. 5 GHz taajuusalueella kanavia voi olla enemmän, joka mahdollistaa useamman radion sijoittamisen samalle alueelle ilman, että ne häiritsevät toisiaan.

802.11ac käyttää useampia lähettäviä ja vastaanottavia antenneja hyväkseen MIMO-teknologian (Multi-Input and Multi-Output) avulla. (Rochim & Sari 2018, 3.)

802.11ax on suunniteltu ympäristöihin, joissa langattoman verkon käyttäjiä on tiheästi pienillä alueilla. Tällaisia alueita voisi esimerkiksi olla toimistot, pikaruokaravintolat ja yleisötapahtumat. Langatonta verkkoa käyttäviä laitteita voi olla pienellä alueella satoja. Tukiasemia ei kannata sijoittaa liian lähelle toisiaan, koska niiden päällekkäiset kanavat häiritsemään toisiaan. 802.11ax luotiin ratkaisemaan nämä ongelmat. 802.11ax käyttää vanhasta tekniikasta kehitettyä OFDMA:ta (Orthogonal Frequency-Division Multiple Access) hyväksi. Se mahdollistaa sen, että tukiasema pystyy samanaikaisesti palvelemaan useampaa laitetta kerralla. Taajuuksia käytetään tämän ansiosta paljon tehokkaammin eikä varata niin leveitä kanavia, toisin kuin 802.11ac tekee. (Rochim & Sari 2018, 2.)

2.5 MIMO

MIMO on 802.11n standardissa saataville tullut langattomien verkkojen teknologia, joka käyttää useita lähettimiä ja vastaanottimia liikuttaakseen dataa enemmän yhdellä kerralla. Tämä onnistuu silloin, kun käytetään useampaa antennia kerralla. Singleuser ja Multiuser MIMO-teknologiat tulivat 802.11ac standardien päivityksissä. SU-MIMO:n tapauksessa laite pystyy sekä lähettää että vastaanottaa dataa samanaikaisesti. MU-MIMO:a käytetään silloin, kun useammalle laitteelle lähetetään dataa samalla taajuusspektrin sisällä. Lähetin lähettää usealle käyttäjälle dataa ilman, että ne häiritsevät toisiaan. Etuna on myös se, että yhdelle käyttäjälle lähetetään dataa useampaa reittiä pitkin. Tämä lisää datan lähetysnopeutta ja langattoman verkon kantamaa. (Rochim & Sari 2018, 3.)

2.6 QoS

Palvelunlaadun eli QoS:n (Quality of Service) avulla voidaan priorisoida liikennettä liikenneluokkien mukaisesti. Sillä pystytään suojelemaan reaaliaikaista liikennettä häiriöiltä, kuten esimerkiksi vikaherkkää ääniliikennettä. Palvelunlaadun

varmistamiseen on työkaluja liikenteen priorisointia varten ja erilaiset jonotustekniikat edelleen lähetyksen kontrollointia varten. Yleisiä priorisointia varten luotuja työkaluja ovat esimerkiksi 802.1p, WMM (Wireless Multimedia Extension) langattomien verkkojen priorisointiin ja DSCP (Differentiated Service Code Point). DSCP on liikenteen priorisointitekniikka, joka käyttää kuusibittistä kenttää IP-paketin headerissa. DSCP:n arvo löytyy IP-paketin ToS- (Type of Service) kentästä. Oletuksena liikenne kulkee verkossa ”Best Efforttina”. DSCP tarjoaa viisi erilaista liikenneluokkaa, joista korkein on EF (Expedited Forwarding). Lisäksi se tuo neljä erilaista AF- (Assured Forwarding) luokkaa, joista jokaiselle on myös erikseen 3 eritasoista pakettien pudotusluokkaa. Mitä korkeampi ensimmäinen numero ja mitä pienempi toinen numero, sitä parempi kohtelu paketille on (ks. taulukko 1). CS (Class Selector) on IP precedencen kolmebittistä lukua vastaava. Se tuo yhteensopivuutta laitteisiin ja protokolliin, jotka eivät pysty käsittelemään koko DSCP-kenttää. Jonotustekniikoita on useanlaisia, joista yleisin on FIFO (First In First Out). Verkkolaitteen jonoissa olevat paketit odottavat vuoroaan seuraavalle laitteelle lähetystä varten. Pakettien headerissa sijaitseva merkintä määrittää niiden järjestyksen jonossa. Järjestys riippuu käytetystä jonotusalgoritmista laitteessa. (Blake, Black, Carlson, Davies, Wang & Weiss 1998.)

Taulukko 1. DSCP-arvot ja koodit (DSCP and Precedence Values 2016.)

DSCP binääriarvo	Desimaaliarvo	Koodi
101 110	46	EF
100 011	38	AF43
100 010	36	AF42
100 001	34	AF41
011 011	30	AF33
011 010	28	AF32
011 001	26	AF31
010 011	22	AF23
010 010	20	AF22
010 001	18	AF21
001 011	14	AF13
001 010	12	AF12
001 001	10	AF11
000 000	0	BE
111 000	56	CS7
110 000	48	CS6
101 000	40	CS5
100 000	32	CS4
011 000	24	CS3
010 000	16	CS2
001 000	8	CS1

2.7 SD-WAN

SD-WAN (Software Defined Wide Area Network) on tekniikka, jossa hyödynnetään SDN-tekniikkaa (Software Defined Network) WAN-yhteyksissä. Sillä pyritään lisäämään kriittisten palveluiden luotettavuutta WAN-yhteyksiä käytettäessä. SD-WAN virtualisoi WAN-palvelut resursseiksi, joita käytetään sulavan yhteyden varmistamiseksi. SD-WAN pystyy käsittelemään liikenteen prioriteetin ja QoS asetusten mukaisesti. Arkkitehtuurissa irrotetaan verkon data- ja hallintatasot toisistaan. Hallinta ja valvonta voi tapahtua ympäristöön asennettavan tuotteen avulla tai fyysisen laitteen ulkopuolella pilvipohjaisessa hallintaympäristössä. (Burke 2017, 7-9.)

Liikenne kulkee VPN-tunneleita (Virtual Private Network) pitkin turvallisesti erikokoisten toimipisteiden välillä. SD-WAN pystyy tunnistamaan sovelluskohtaisesti liikennettä ja sillä varmistetaan laadukkaampi käyttökokemus pilvipalveluja

käytettäessä. Liikennettä voidaan optimoida useammalla eri tavalla. Toimipisteellä käytettäville sovelluksille voidaan päättää reitit linkin suorituskyvyn mukaisesti ja latenssin kasvaessa liikenne voidaan sovelluskohtaisesti siirtää automaattisesti käyttämään toista palveluntarjoajan yhteyttä tai esimerkiksi MPLS-verkkoa (Multiprotocol Label Switching). (Burke 2017, 7-9.)

SD-WAN voi toimia esimerkiksi julkisen verkon tai MPLS-verkon päällä virtualisoituna ja sillä voidaan varmistaa määriteltyjen palveluiden toimintavarmuus loppukäyttäjille. Käytännössä siis SD-WAN alapuolella olevalla verkolla tai sitä tarjoavalla operaattorilla ei ole väliä. Alapuolella olevan verkon tyyppikään ei vaikuta SD-WAN:in toimintaan, joten voidaan langattomia verkkoyhteyksiä tai xDSL-tekniikoita (Digital Subscriber Line) käyttää hyväksi. Lisäksi toimivan verkon saaminen on nopeaa eikä tarvitse odottaa pitkiä aikoja MPLS-verkon toimitusta, kun voidaan käyttää internet tai mobiiliverkkoa. (Burke 2017, 7-9.)

2.8 ITIL

ITIL (Information Technology Infrastructure Library) on kokoelma, mihin on kerätty tietoteknisen ympäristön hallinnan parhaita käytänteitä. Alkujaan ITIL julkaistiin Britanniassa valtion tietoteknisiä osastoja varten vuonna 1980. Myöhemmin on julkaistu ITIL v2, joka luotiin oppaaksi tietotekniikan perusoperaatioita varten, sekä ITIL v3 tukemaan puolestaan liiketoiminnan tavoitteita tietoteknisessä ympäristössä. ITIL on muuttunut vuosien varrella vastaamaan nykyisempiä tietoteknisiä ympäristöjä. Tietoteknisten ympäristöjen kehittyessä niiden tarpeet ylläpitämiseen ovat muuttuneet radikaalisti. (History of ITIL 2018.)

Vuoden 2019 alkuneljänneksellä julkaistiin ITIL v4. Sillä pyritään kehittämään ja laajentamaan ITIL v3 prosesseja ja parhaita käytäntöjä uusilla materiaaleilla. ITIL v3 ydinrakenne säilyy ITIL v4 siirryttäessä. ITIL v3 palvelunhallinnan rakenne voidaan jakaa karkeasti viiteen osaan. (Watts 2018.)

ITIL Service Strategy auttaa organisaatiota tuomaan asiakkaille tarpeellisia palveluita ja tuotteita seuraten tietoteknisen ympäristön palvelunhallinnan käytänteitä. Jokaisessa palvelun elinkaaren vaiheessa keskitytään liiketoiminnallisiin tavoitteisiin, vaatimuksiin ja palvelun ylläpitämiseen. (ITIL Service Strategy 2016.)

ITIL Service Design auttaa organisaatiota tarjoamaan parempia palveluja asiakkaille sen kokonaisvaltaisilla suunnittelumalleilla. Palvelut ja prosessit voidaan suunnitella tarkasti asiakkaita varten. Palvelukeskeisestä näkökulmasta suunnitellaan IT-ympäristön palveluratkaisut, hallinnan tietojärjestelmät ja työkalut, käytetyt tekniikat, prosessit ja mittarit. (ITIL Service Design 2016.)

ITIL Service Transition auttaa suunnittelemaan sekä hallitsemaan palvelun tilanvaihtoa sen elinkaaren aikana. Siinä tarkastellaan uusien ja muuttuvien palveluiden riskejä ja pyritään suojaamaan tuoteympäristöä. Se auttaa tekemään tietoon perustuvia sekä luotettavia päätöksiä, kun palvelua siirretään. Palveluita siirrettäessä riskien hallitseminen sekä palveluntarjonnan tunteminen ovat olennaisia osia siirtymisprosessissa. (ITIL Service Transition 2016.)

ITIL Service Operation sisältää oppaita infrastruktuurin päivittäisten toimintojen ja prosessien ylläpitoon. Sillä pyritään varmistamaan liiketoiminnan jatkuvuus. Prosesseja on muun muassa häiriönhallinta, palvelupyyntöjen toteutus, käyttöoikeuksienhallinta, tapahtumienhallinta ja ongelmienhallinta. Näillä prosesseilla pyritään varmistamaan tarjottujen palvelujen luotettavuus. Vianhallinnalla pyritään reagoimaan vikatilanteisiin ja takaamaan ympäristön toimivuus. Palvelupyyntöjen toteutuksella tehdään pieniä ja matalan riskin muutoksia. Esimerkiksi kytkinportin asetuksien muuttaminen on pienen riskin muutos. Muutoksenhallinnan prosessissa tehdään monimutkaisempia ja korkeamman riskin muutoksia, jotka voivat vaatia aikaikkunan tai suunnitelman. (ITIL Service Operation 2016.)

ITIL Continual Service Improvement perustuu palvelun parannustoimien mittaukseen. Palvelua sekä palvelunhallintaa pyritään siis jatkuvasti kehittämään paremmaksi kaikissa edellä mainituissa osissa. Parannusten tunnistus sekä

käyttöönottaminen palvelunhallinnassa voi esimerkiksi tulla esille työntekijöiden parannusehdotuksina. (Continual Service Improvement 2016.)

3 Cisco Meraki

3.1 Yleistä

Alkujaan Meraki perustettiin vuonna 2006 Sanjit Biswasin, John Bicketin ja Hans Robertsonin toimesta samaan aikaan, kun he opiskelivat Massachusetts Institute of Technologyn teknisessä yliopistossa. Meraki oli alkujaan pieni startup-yritys, joka tarjosi pilvipohjaisesti hallittavia langattomien lähiverkkojen ratkaisuja yritysverkkoympäristöille. Lopulta Meraki kasvoi pilvipohjaisesti hallittavien verkkojen edelläkävijäksi ja tarjosi tämän avulla sujuvaa hallittavuutta langattomiin verkkoihin. Cisco ilmoitti ostavansa Merakin 18 maaliskuuta 2012 noin 1,2 miljardilla dollarilla. Kaupan ansiosta Cisco Merakin tuotteet ovat tulleet paremmin tietoisuuteen globaaleilla markkinoilla ja se on edelleen jatkanut kasvuaan. Ciscon tavoitteena oli saada lisää asiakkaita, joilla verkkoympäristöt ovat pieniä ja keskisuuria. Cisco Meraki tarjoaa nykyään ympäristöön kaikki tarvittavat verkkolaitteet yhdeltä valmistajalta ja niitä kaikkia hallinnoidaan yhdeltä hallintapaneelilta. (Constine 2012.)

3.2 Cloud Management

Cisco Meraki tarjoaa reaaliaikaisen Web-pohjaisen hallintapaneelin, millä voidaan valvoa ja hallita Cisco Merakin laitteilla luotuja verkkoja. Cisco Merakin pilvipohjaisesti hallittavalla ympäristöllä voidaan luoda erikokoisia verkkoja ja skaalata niitä tarpeiden mukaisesti. Hallinnointiin ei tarvita erillisiä graafisia käyttöliittymiä tai komentorivipohjaista käyttöliittymää. Cisco Merakin laitteiden ja hallintapaneelin kommunikointiin yksittäinen laite käyttää noin yhden kilobitin kaistaa per sekunti. Liikennemäärä on minimaalista, eikä se vaikuta muuhun verkossa tapahtuvaan liikenteeseen merkittävästi. Liikennemäärät kasvavat väliaikaisesti, kun

laitteita päivitetään tai tehdään konfiguraatiomuutoksia hallintapaneelin kautta. Verkossa olevien käyttäjien liikenne ei kuitenkaan mene pilven kautta hallintaliikenteen tavoin. Hallintaliikenne on eristettynä omaan VLAN:in (Virtual Local Area Network), joten se ei sekoitu käyttäjien liikenteen kanssa. LAN-verkko on suunniteltu toimimaan myös silloin, kun yhteys laitteilta Merakin pilveen katkeaa. Hallintapaneelin palvelut ovat tosin väliaikaisesti poissa käytöstä, kunnes yhteys pilveen palautuu. Hallinnan data käsittää valvonnan, konfiguroinnin, päivitykset ja statistiikan. Kaikki verkon käyttäjien data kulkee suoraan kohteeseen ja takaisin laitteelle. Hallintaliikenteen avulla pystytään valvomaan verkon laitteita hallintapaneelissa reaaliaikaisesti. Graafisen käyttöliittymällä pätkivä ja ajoittaisesti korkean latenssin seuraaminen on visualisoitu. (Cloud Management 2013, 1-2,4.)

Kaikki Cisco Merakin laitteet ottavat yhteyttä internetin kautta Cisco Merakin konesaleihin turvallisesti SSL-yhteyttä (Secure Sockets Layer) käyttäen. Cisco Merakin ympäri maailmaa sijaitsevissa konesaleissa toimii Cisco Merakin Pilvipohjaisen hallinnan alusta, jonka avulla voidaan reaaliaikainen hallintapaneeli tarjota käyttäjille. Yhdellä hallintapaneelilla voidaan keskitetysti täten hallita eri toimipisteiden laitteita ympäri maailmaa. Sillä on mahdollista myös päivittää kaikki verkon laitteet kerralla automatisoituna, tai tarvittaessa päivitykset voidaan tehdä porrastettuna laite kerrallaan. Päivitys voidaan ajoittaa esimerkiksi hiljaisempaan hetkeen verkkokohtaisesti. (Cloud Management 2013, 1-2.)

3.3 Cisco Merakin konesalit

Cisco Merakilla on viisi konesalia ympäri maailmaa, jotka ylläpitävät pilvipohjaista hallintapalvelua jatkuvasti. Konesalit on suunniteltu turvallisiksi, vikasietoisiksi ja luotettaviksi. Jokaisen yksittäisen asiakkaan tallennetut konfiguraatiot ja valvottava käyttödata replikoidaan vähintään kolmen konesalin välillä. Konesaleja valvotaan 24/7 ja sinne pääsee vain kulkuoikeutetut henkilöt. Pilvipohjaisten hallintapalveluiden saatavuutta ja turvallisuutta seurataan automatisoituna 24/7. Arkkitehtuuri mahdollistaa verkon toiminnan, vaikka hallintapaneeli ei olisikaan käytössä. Konesaleissa on katastrofeja varten varauduttu konesaleille tyypillisillä

ominaisuuksilla, kuten UPS (Uninterruptible Power Supply), varavirtageneraattorilla, kahdennetuilla yhteyksillä ja vikasietoisuudella. Muualla päin maailmaa olevilla konesaleilla ehkäistään vikatilanteita ja varmistetaan pilvipohjaisen hallintapalvelun saatavuus, mikäli jonkun konesalin toiminta lakkaa katastrofin takia. Cisco Meraki on luvannut pilvipohjaisen hallinnan saatavuudelle 99.99 % SLA:n (Service Level Agreement). (Cloud Management 2013, 5.)

3.4 Valvonnan ja vianselvityksen työkalut

Cisco Merakin hallintapaneelissa pystytään valvomaan liikennettä ja verkon suorituskykyä reaaliaikaisesti. Hallintapaneelissa on näkyvyys verkon laitteisiin, käyttäjiin ja käytettäviin sovelluksiin. Näiden avulla voidaan nopeasti reagoida vikatilanteisiin ja tunnistaa haitallinen liikenne. Tarvittaessa luomalla turvallisuuspolitiikkaa haitallisen sovelluksen tai liikenteen estämiseksi voidaan välttyä suuremmilta vahingoilta. (Cloud Management 2013, 3.)

Vianselvitystä varten hallintapaneelissa voidaan laitekohtaisesti tehdä ICMP/ping (Internet Control Message Protocol) valittua laitetta, IP-osoitetta tai verkkosivua kohti. Traceroutella voidaan tarkistaa reitin hypyt määriteltyyn kohteeseen. Lisäksi liikenteestä voidaan tehdä pakettikaappaus, jonka avulla verkon vikatilanteita pystytään analysoida tarkemmin. Laitteet voidaan myös tarvittaessa uudelleenkäynnistää etänä, tehdä kaapelitesti valituille porteille ja käyttää valittu kytkinportti alhaalla. Tukiasemissa voidaan asettaa sen ledit vilkkumaan paikantamista varten, listata ARP-taulun (Address Resolution Protocol) sisältö ja katsoa sen yhteyden nopeus. (Cloud Management 2013, 3.)

Verkon laitteille ei tarvitse mennä yksi kerrallaan selvittämään vikatilannetta, vaan toimenpiteet pystytään tekemään keskitetyn hallintapaneelin avulla. Rutiininomaiset vianselvityksen askeleet hoituvat vianselvitykseen tarkoitettujen työkalujen avulla nopeammin kuin perinteisessä verkossa. Meraki pystyy myös havaitsemaan erilaisia vikatilanteita, ja ilmoittaa niistä hallintapaneelissa käyttäjälle. (Cloud Management 2013, 3.) Esimerkiksi kun kytkinportit eivät ole samassa VLAN:ssa tai nimipalvelin ei

vastaa DNS (Domain Name System) kyselyihin, niin hallintapaneeliin tulee laitekohtaisesti ilmoitus näistä ongelmista. Aikaa ei täten mene niin suurta määrää vianetsintään, vaan voidaan suoraan lähteä ratkaisemaan vikatilannetta.

Hallintapaneelista löytyy myös muita hyödyllisiä valvontatyökaluja, kuten ”RF (Radio Frequency) spectrum, jolla voidaan seurata tukiasemien langattoman verkon käyttömääriä, signaalin kuuluvuutta ja toisten tukiasemien kanavien vaikutusta toimintaan. Location heatmap -työkalulla voidaan seurata, minkä tukiaseman piirissä on eniten laitteita yhdistettynä langattomaan verkkoon. Tämän avulla voidaan arvioida tukiasemille parempia sijainteja kuuluvuuden näkökulmasta. (Cloud Management 2013, 3.) Valvontatyökaluista on hyötyä esimerkiksi vianselvityksessä kapasiteetin ja verkon kuuluvuuden kannalta sekä sitä voidaan käyttää apuna uusien tukiasemien sijoittelun suunnittelussa.

3.5 Turvallisuutta lisäävät työkalut

Cisco Merakin hallintapaneelissa on erilaisia työkaluja turvallisuuden parantamiseksi. Kaksi-vaiheisella tunnistautumisella luodaan lisäsuojaa ympäristöön. Vaikka kyberrikollinen onnistuisi saamaan haltuunsa käyttäjätunnuksen ja salasanan, hän ei silti pääsisi kiinni hallintapaneeliin. Käyttäjille voidaan asettaa salasanapolitiikkaa, esimerkiksi salasanan maksimi-ikä, monimutkaisuusvaatimus, salasanahistoria ja pystytään estämään kirjautumiset valituista IP-osoitteista. Cisco Meraki auditoi konfiguraatiomuutokset ja kirjautumisyritykset. Auditoinnin etuna on se, että konfiguraatiovirheen tehneen käyttäjän muutos voidaan korjata ja informoida käyttäjää virheellisestä konfiguraatiosta. Hallintakäyttäjille voidaan luoda organisaatiokohtaisia rooleja ja esimerkiksi käyttäjiä lukuoikeuksilla, jotka pystyvät esikatselemaan valvontanäkymiä ja osallistua vianselvitykseen työkalujen avulla. Näillä ja useilla muilla ominaisuuksilla saadaan parannettua ympäristön turvallisuutta muun arkkitehtuurin lisäksi. (Cloud Management 2013, 6.)

3.6 Laitteet

3.6.1 Meraki-kytkimet

Cisco Merakilla on tarjolla useita kytkinmalleja eri käyttötarkoituksia varten. Useissa reunakytkimissä on ominaisuutena PoE (Power-over-Ethernet) tuella varustetut portit, joista tukiasemat ja kamerat saavat virtansa. Kytkimissä on myös uplinkkejä varten SFP-moduulit (small form-factor pluggable), jotka mahdollistavat valokuitujen ja parikaapeleiden käytön verkkolaitteiden välillä. Kytkimillä voidaan erotella verkkoja toisistaan Virtuaalisiksi verkoiksi. VLAN:it tuovat turvallisuutta ja voidaan varmistaa, ettei vierailijoiden tai työntekijöiden omat laitteet ole samassa verkossa yrityksen laitteiden kanssa. (Cloud Managed Switches n.d.)

Reunakytkimet

MS120-8 Series on pienin tarjolla oleva L2-kytkin. Siinä on kahdeksan gigabittistä Ethernet porttia ja kaksi SFP-moduulia. Se on pienikokoinen, joten se voidaan sijoittaa myös ahtaisiin paikkoihin. MS120 Series laitteet ovat hieman isompia L2-kytkimiä, jotka ovat saatavilla 24x1Gb ja 48x1Gb portilla varustettuna ja niissä on neljä SFP-moduulia. Pinottavilla reunakytkinmalleilla voidaan rakentaa vikasietoinen verkkoarkkitehtuuri, joka ei tarvitse spanning-tree protokollaa linkkiaggregoitujen kytkinpinojen välille. Kapasiteettia saadaan enemmän käyttöön eikä spanning-tree tuki vikasietoisia linkkejä kytkinpinojen välillä. Kytkimiä voidaan pinota yhteen pinoamiseen tarkoitettujen porttien avulla, normaalien kytkinporttien avulla tai jopa virtuaalisesti ilman että kytkimet ovat toisissaan kiinni. MS210 ja MS225 mallin kytkimet ovat L2-kytkimiä, jotka pystyvät staattiseen reititykseen ja kummatkin kytkinmallit tukevat toisiinsa pinoamista. (Cloud Managed Switches n.d.)

L3-kytkin

MS250, MS350 ja MS355 ovat tehokkaampia L3-kytkimiä, jotka pystyvät reitittämään dynaamisen OSPF (Open Shortest Path First) reititysprotokollan avulla. Kytkimille voidaan konfiguroida DHCP (Dynamic Host Control Protocol) jakamaan IP-osoitteita verkon päätelaitteille. Kytkimillä voidaan myös toteuttaa vikasietoisuutta VRRP (Virtual Router Redundancy Protocol) avulla. VRRP käyttäessä, mikäli L3-kytkinparista

master-kytkin menee rikki tai muuhun vikatilaan, varakytkin vaihtuu automaattisesti masteriksi ja se hoitaa reitityksen sekä muut kytkimelle määritetyt tehtävät, kunnes alkuperäinen L3-kytkin on taas toimintakunnossa. VRRP on vaihtoehtoinen tekniikka pinoamiselle. (Cloud Managed Switches n.d.)

Aggregoivat kytkimet

Aggregoivia kytkimiä on saatavilla MS410 ja MS425 mallit 16 ja 32 SFP-moduulipaikoilla varustettuina sekä MS450, jonka kaikki 12 porttia ovat 40 gigabittisiä QSFP+-moduulilla (Quad SFP) varustettuja. Moduulipaikoissa voidaan käyttää sekä kuitu että RJ-45 liitännällä olevia SFP-moduuleita. Aggregoivat kytkimet tarjoavat paljon SFP-moduulipaikkoja yhdessä kytkimessä ja niitä Cisco Meraki suosittelee yrityksille, joiden ympäristöt tarvitsevat runsaasti tehoa toimiakseen sulavasti. Normaalisti kytkimet jouduttaisiin kytkemään peräkkäin toisiinsa ja linkkien kuorma lisääntyisi tämän johdosta, koska kaikki liikenne menee vain yhtä linkkiä pitkin. Aggregoivilla kytkimillä voidaan kytkennät tehdä jokaiselta kytkimeltä toisiinsa, jolloin kytkintenvälisiä hyppyjä tapahtuu vähemmän kuin jonoon kytketyssä topologiassa. Aggregoiviin kytkimiin voidaan liittää normaaleja reunakytkimiä topologian lehtikytkimiksi, joiden taakse loppukäyttäjien laitteet ja tukiasemat sijoittuvat. Topologiassa voisi esimerkiksi olla kaksi aggregaattikytkintä ja kumpaankin liitetty lehtikytkimiä vikasietoisesti. (Cloud Managed Switches n.d.)

3.6.2 Tukiasemat

Cisco Merakin yritystason tukiasemien ominaisuuksina ovat niiden radioiden tehokkuus ja vastaanottimien herkkyys. Ne tukevat 2.4 GHz:n sekä 5 GHz:n käyttötaajuuksia. Tukiasemat on suunniteltu ympäristöihin, joissa on korkea käyttäjätiheys. Pienellä alueella voi olla runsaasti langatonta verkkoa käyttäviä laitteita. Alueelle tarvitaan ratkaisu, joka mahdollistaa langattoman verkon häiriöttömän käytön. Kaikki tukiasemat käyttävät hyväksi MIMO-tekniikkaa, joka mahdollistaa useamman antenninkäytön kumpaakin suuntaan kulkevassa liikenteessä. Tukiasemamalleja on useita ja ominaisuuksien perusteella niille on omat suositukset toimipisteelle sijoittamisen kannalta. (Cloud Managed Wireless n.d.)

MR55 ja MR45 ovat ainoat 802.11ax -tekniikkaa käyttävät tukiasemat Cisco Merakilta. Ne ovat tehokkaita ja suunniteltu sijoitettavaksi paikkoihin, missä käyttäjämäärät ovat suuria. Muut tukiasemamallit esimerkiksi MR42, MR52 ja muut MR-sarjan mallit käyttävät 802.11ac -tekniikkaa ja suurin osa niistä ovat ympäröivän alueen kattavia tukiasemia. Niiden teoreettinen käyttäjien maksimimäärä on 128 per radio (Approximating Maximum-- n.d). Erikseen ovat vielä tukiasemamallit, joihin voidaan liittää ulkoisia antenneja kohdistamaan signaalit valittuihin suuntiin loppukäyttäjiä kohti. Kohdistamalla voidaan varmistaa signaalin vahvuus käyttäjille. Mikäli käyttäjät ovat levittäytyneinä esimerkiksi toimistotiloihin, on silloin ympärisäteilevä tukiasema parempi vaihtoehto. (Cloud Managed Wireless n.d.)

3.6.3 Kamerat

Kameroilla voidaan lisätä työympäristön turvallisuutta ja valvoa, ettei tiloihin pääse ulkopuolisia henkilöitä. Kameroita voidaan seurata Cisco Merakin hallintapaneelista ja ominaisuuksina on liikkeentunnistus sekä kuvassa tapahtuvien liikkeiden analysointi tekoälyä hyväksikäyttäen. Yleisimmin käytettävät reitit saadaan analysoinnin avulla esille liikkeistä. MV22, MV21 ja MV12 ovat sisätiloihin tarkoitettuja kameroita, joista MV12 series -mallit voivat tarvittaessa toimia langattomasti. Ulkotiloihin on suunniteltu erikseen sään ja iskunkestävät kameramallit MV71 ja MV72. Videokuva salataan ja tallennetaan kameran omaan muistiin, etteivät ulkopuoliset henkilöt pääse katsomaan sitä. Vaihtoehtoisesti varkaiden varalta kameraan on saatavilla Cloud Archive lisenssi, jolla videokuva tallennetaan myös pilveen. (Cloud Managed Smart Cameras n.d.)

3.6.4 Security Appliance & SD-WAN

Cisco Meraki tarjoaa palomuureina MX-sarjan laitteita, jotka toimivat myös SD-WAN-laitteina. Laitemalleja löytyy kapasiteettitarpeiden mukaisesti. Niillä suojataan ympäristöä hyökkäyksiltä ja viruksilta. Laitteet pystyvät käyttämään hyväksi SD-WAN-ominaisuuksia. Sovelluskohtaisia SD-WAN-sääntöjä voidaan luoda hetkessä varmistamaan niiden jatkuva toimivuus. SD-WAN sovelluskohtaisilla säännöillä voidaan siirtää liikenne automaattisesti toiseen linkkiin, mikäli ensisijaisessa linkissä

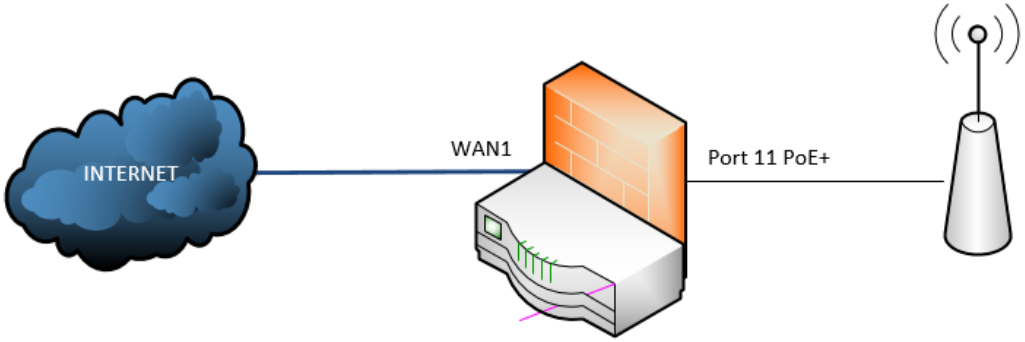
yhteys ei ole tarpeeksi hyvä. Kriittisien ja vikaherkkien sovelluksien, kuten äänipuheluiden ja erilaisten pilvipalvelujen toimintaa pystytään varmistamaan sovelluskohtaisilla suorituskykyluokilla.

Palomuureilla voidaan toteuttaa korkeaa verkon saatavuutta. Toimipisteelle voidaan konfiguroida master- ja warm spare palomuurit. Tämä toimii samalla tavalla kuin VRRP. Mikäli toimipisteelle on tarjolla kahdennettu WAN-yhteys (Wide Area Network), on suositeltavaa varata palomuureilta portti kumpaakin kohti. Jos master palomuuri hajoaa, niin warm spare ei tällöin menetä yhteyttä ensi- tai toissijaiseen internetyhteyteen. Palomuuri seuraa sen läpi menevää liikennettä ja tarvittaessa sillä voidaan suodattaa kategoriakohtaisesti pois sivustoja ja sovelluksia. Palomuuri voidaan konfiguroida toimimaan DHCP-serverinä tai lähettämään DHCP-pyynnöt määriteltyä osoitetta kohti. Cisco Merakin palomuureissa on myös ”Auto VPN”-ominaisuus, jolla voidaan automaattisesti konfiguroida VPN-tunneleita toimipisteiden välille. Tämän ominaisuuden avulla pystytään kätevästi luomaan myös HUB- ja Spoke topologioita. (Cloud Managed Security & SD-WAN n.d.)

4 Käyttöönotto

4.1 Topologia ja osoitteistus

Cisco Merakin laitteiden ja hallintapaneelin testaamiseen käytettiin kahta laitetta, jotka voisivat toimia pienen toimipisteen laitteina. Topologiaan (ks. kuvio 3) sisältyy yksi Security Appliance MX68CW-WW, johon on mahdollista liittää SIM-kortti (Subscriber Identity Module) langatonta varayhteyttä varten. Lisäksi palomuurissa on mahdollisuus luoda langattomia verkkoja ilman erillistä tukiasemaa. Toisena laitteena toimii MR33 mallin tukiasema, jossa toteutettiin langattomat verkot. Myöhemmin verkkoon oli tarkoitus lisätä kytkin, joka toisi ympäristöön käyttöön enemmän PoE-ominaisuudella varustettuja portteja.



Kuvio 3. Verkon topologia

Laitteiden konfigurointi tapahtui Cisco Merakin selainpohjaisesta hallintapaneelista. Kun Cisco Merakin laitteet yhdistetään internetiin, ne ottavat suoraan yhteyttä pilveen, jolloin ne voidaan hallintapaneelissa ottaa konfiguroitavaksi. Ensin kuitenkin laitteet täytyy hakea käyttöön hallintapaneelissa laitteiden sarjanumeroiden avulla. Laitteet ilmestyvät luetteloon, josta ne voidaan lisätä haluttuun verkkoon. Verkkoja voidaan luoda, yhdistää ja tarvittaessa poistaakin. Laitteita voidaan myös hallintapaneelissa siirtää verkosta toiseen. Hallintapaneelista luotiin verkko ja laitteet liitettiin sinne. Laitteet olisivat tulleet tässä vaiheessa Online-tilaan konfiguroitavaksi, mikäli ne olisivat olleet verkkoon liitettynä ja käynnissä. Konfigurointi voidaan hallintapaneelin kautta tehdä suoraan Cisco Merakin laitteille, mutta laboratoriossa käytettiin Template-toiminnallisuutta. Templateilla voidaan konfiguroida valmiiksi laitteita, ennen kuin ne ovat koko hallintapaneeliin edes haettu ja kytketty toimipisteellä verkkoon. Verkko liitetään templateen, jolloin siihen verkkoon asennettavat laitteet hakevat valmiit konfiguraatiot pilvestä ja ovat siten toimintavalmiina kytkentöjen jälkeen.

Verkkoon suunniteltiin muutama VLAN omilla DHCP-pooleilla varustettuina (ks. taulukko 2). Oletuksena kaikilla laitteilla on management VLAN konfiguroituna valmiiksi natiivina portteihin, jolloin laitteet pystyvät ottamaan suoraan yhteyttä hallintapaneeliin ilman ylimääräisiä konfiguraatioita kytkennän yhteydessä. Portit

ovat myös ”trunk”-toimintatilassa, jolloin oletuksena kaikki VLAN:it voivat mennä portista läpi seuraavalle laitteelle. Verkkoon kytkettäville työasemille ja tulostimille tarkoitetut portit konfiguroidaan access -tilaan ja niille jokin VLAN käyttöön.

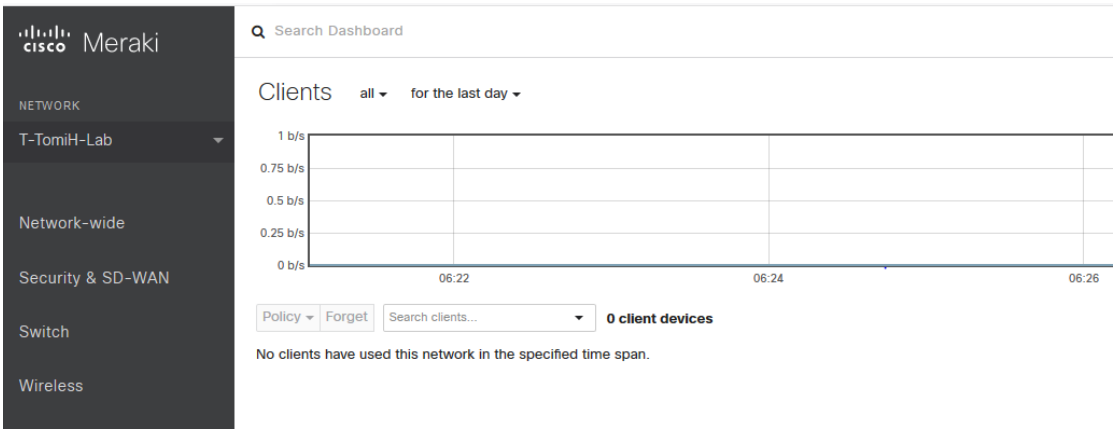
Taulukko 2. VLAN aliverkkojen osoitteistus

VLAN ID	Name	Network	Default gateway
1	Management	192.168.0.0/24	192.168.0.1
10	Office	192.168.124.0/24	192.168.124.1
20	WLAN	192.168.130.0/24	192.168.130.1
30	Quest	10.1.1.0/24	10.1.1.1

4.2 Templaten konfigurointi

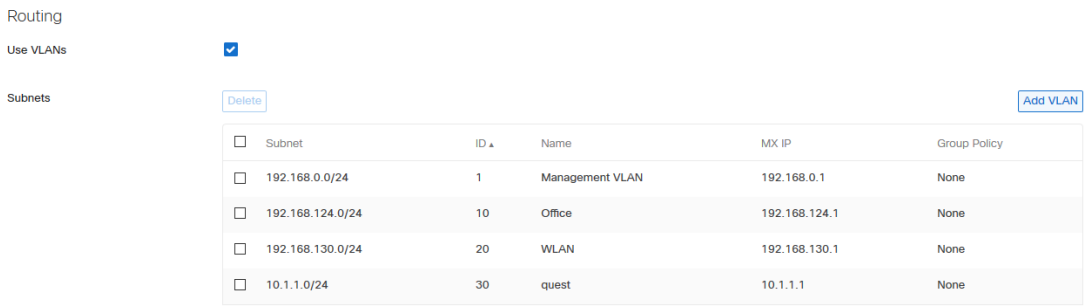
4.2.1 Security Appliance

Verkon konfigurointia varten luotiin oma template (ks. kuvio 4), jossa kaikki verkon laitteiden konfiguraatio tapahtui. Templateen voidaan liittää useampi eri verkko, jotka käyttävät samaa konfiguraatiota alustana ympäristölle. Vasemmasta sivupaneelista voidaan valita laitekategorioiden mukaisesti kohde konfiguraatiota varten.



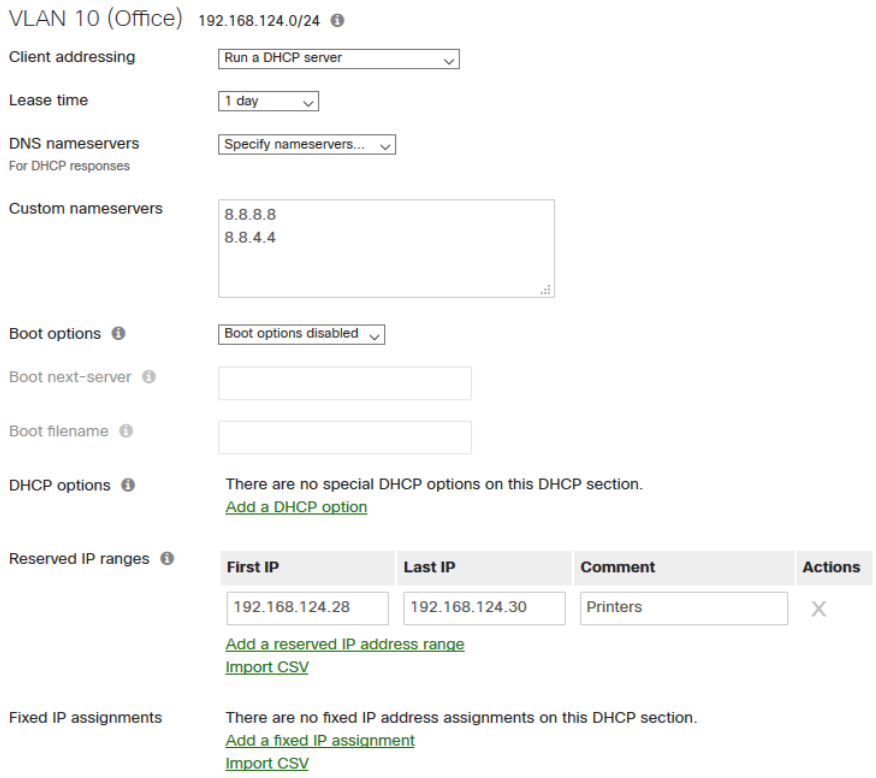
Kuvio 4. Template-sivun näkymä

Cisco Merakin laitteiden konfigurointi on suoraviivaista ja sujuvaksi tehty hallintapaneelin avulla. Oletuksena MX-laite käyttää vain yhtä management VLAN, mutta sille voidaan konfiguroida useampi VLAN eri käyttötarkoituksia varten ja asettaa laite toimimaan DHCP-palvelimena. (ks. kuvio 5).



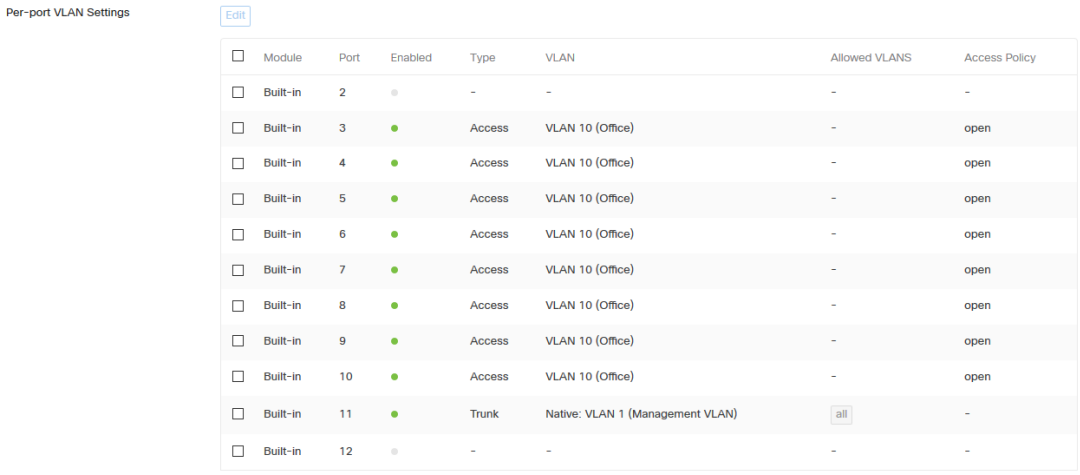
Kuvio 5. MX-laitteelle konfiguroidut VLAN:it

Koska VLAN:lle konfiguroitiin omat aliverkot, niin MX-laite loi valmiiksi DHCP-konfiguraatiot jokaista VLAN:ia varten (ks. kuvio 6). MX-laite voidaan konfiguroida hakemaan osoitteet jostakin toisesta verkosta DHCP relay -ominaisuuden avulla tai yksinkertaisesti asettaa laite olemaan vastaamatta DHCP-pyyntöihin. Sisäverkossa voisi jo erikseen olla valmiiksi DHCP-palvelin tai L3-kytkin hoitamassa verkon osoitteistuksen. Osoitteita voidaan varata aliverkosta ja asettaa halutut DNS-nimipalvelimet, kuten perinteisessäkin verkossa. VLAN 10 aliverkosta varattiin kaksi osoitetta tulostimia varten ja asetettiin halutut DNS-nimipalvelimet käyttöön.



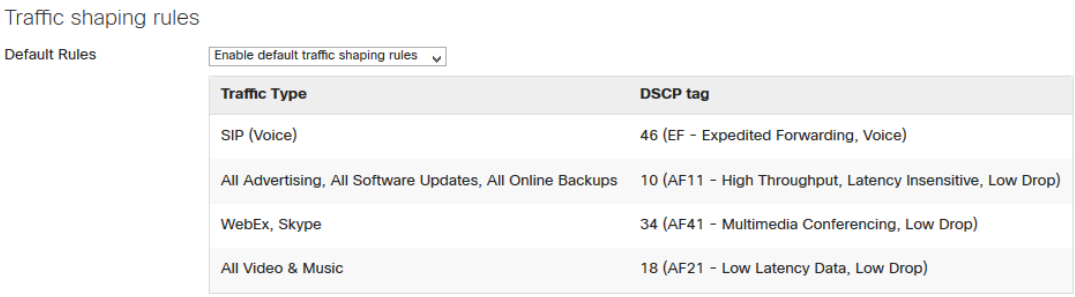
Kuvio 6. DHCP-asetukset Office VLAN:ssa

MX-laitteelle tehtiin kokeiluksi kaksi Layer 7 eli applikaatiotason sääntöä. Niissä estettiin vertaisverkkoyhteydet ja kaikenlainen sisältö peleihin liittyen. Lisäksi MX-laitteelle voidaan erikseen konfiguroida sisällönsuodatusta. Sisältöä pystyisi suodattamaan kategoriakohtaisesti tai estää sivustoja domain nimen mukaan. MX-laitteen porttikohtaisia konfiguraatioita muutettiin turvallisemmaksi. Käyttämättömät portit 3-10 siirrettiin käyttämään Office VLAN:ia ja portti 12 disabloitiin, koska se ei ollut sillä hetkellä käytössä (ks. kuvio 7). Porttien pääsynhallintaa voidaan kontrolloida ja ohjata myös RADIUS-palvelimien avulla.



Kuvio 7. MX-laitteen porttikonfiguraatiot

Kahden WAN-linkin kanssa voidaan tasata kuormaa kummallekin linkille. MX-laitteelta löytyy SD-WAN:in ja liikenteen muokkaamiseen toimintoja. Liikenteen muokkauksessa käytetään palvelunlaadusta tuttuja DSCP-arvoja, joilla läpimenevät paketit merkitään niille määritetyn tärkeyden mukaisesti ToS-kenttään. Oletuksena MX-laitteella on käytössä neljä sääntöä liikennetyyppien mukaisesti (ks. kuvio 8). Nämä voidaan tarvittaessa poistaa tai muokata ympäristölle sopivammaksi.

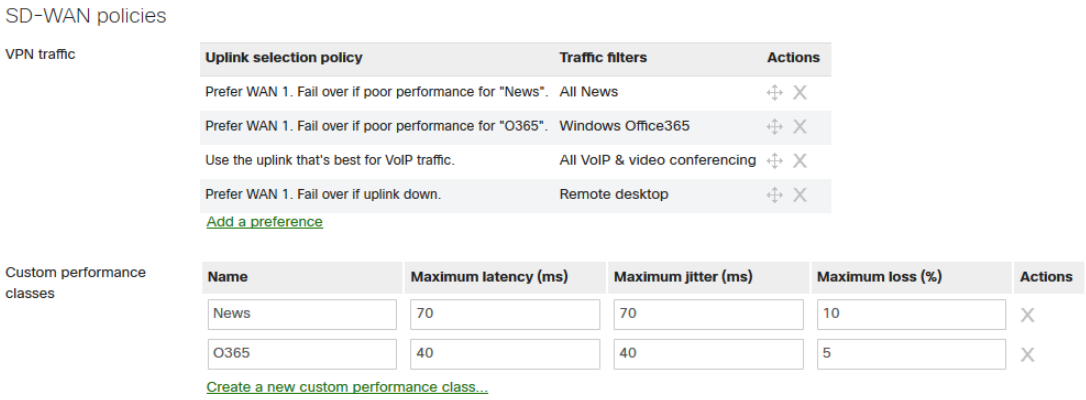


Kuvio 8. Liikenteen muokkaamisen säännöt liikenteen tärkeyden mukaisesti

Oletuksena SIP-äänipuheluiden (Session Initiation Protocol) liikenne menee korkeimmalla prioriteetilla muiden jonojen ohi, koska äänipuheluissa pakettien

pudotuksesta äänenlaatu kärsii huomattavan paljon. Kaikissa muissa liikennekohtaisissa jonoissa on pakettien pudotustodennäköisyydet määritelty pienemmiksi normaaliin liikenteeseen verrattuna. Liikenne, mitä ei ole näissä jonoissa määritelty, menee läpi ”Best Efforttina”. Paketteja pudotetaan välistä korkeamman prioriteetin liikenteen toiminnan varmistamiseksi.

MX-laitteelle voidaan luoda SD-WAN sääntöjä sovellus- ja kategoriakohtaisesti. Sääntöjä varten voidaan konfiguroida luokkia vaadituille suorituskyvyn tasoille. Kun suorituskyky on latenssin tai pakettihävikin takia liian huono, liikenne siirretään menemään muun kuin mieluisimman linkin kautta. Toisena vaihtoehtona olisi vaihtaa linkkiä silloin, kun se menee alas kokonaan. Sääntöjä voidaan myös luoda itse lähde- ja kohdeosoitteista sekä verkoista määriteltyihin portteihin. Pystytään käytännössä lisäämään omien organisaationsisäisten palveluiden toimintavarmuutta. Lisäksi saman hallintapaneelin muiden verkkojen välillä voidaan VLAN:in mukaan toteuttaa näitä sääntöjä. MX-laitteelle tehtiin neljä SD-WAN -sääntöä ja kaksi suorituskykyluokkaa (ks. kuvio 9).



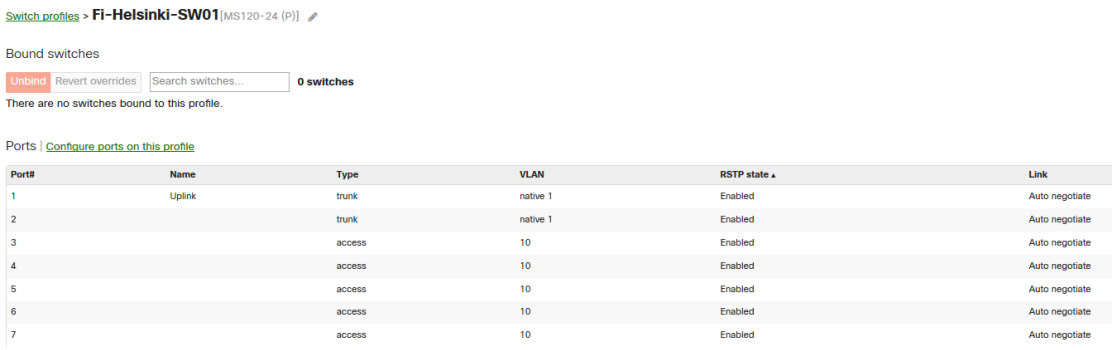
Kuvio 9. SD-WAN -säännöt ja suorituskykyluokitukset

Auto VPN -teknologialla pystytään nopeasti luomaan toimipisteiden välille tunneleita. Tunnelit luodaan automaattisesti ja tämä mahdollistaa Hub- ja Spoke-topologioiden nopean luonnin. Toimipisteiltä valitut aliverkot mainostetaan VPN:ään. Konfiguraatioissa valitaan toimipisteen tyyppi ja siihen osallistuvat aliverkot. Tämän

jälkeen Cisco Merakin pilvi muodostaa tunnelit ja reitit ilmestyvät reititystauluun. VLAN:ien aliverkkojen täytyy olla uniikkeja templatessa, jotta Auto VPN voidaan sallia verkkoon. Näin pystytään estämään päällekkäisyyksiä.

4.2.2 Kytkin

Kytkimen konfigurointi templateista tapahtuu kytkinmallikohtaisesti. Kytkinmallin mukaan tehdään profiileja ja konfiguroidaan ne verkon tarpeiden mukaisesti. Portit ovat oletuksena konfiguroitu käyttämään management VLAN:ia. Lisäksi porteissa on sallittuna valmiiksi PoE. Virtaa tarvitsevat laitteet, kuten tukiasemat, käynnistyvät ja liittyvät verkkoon ilman erillistä virtalähdettä. Konfiguraatiomahdollisuudet vaihtelevat kytkinmallien ominaisuuksien ja tehtävän mukaisesti. Kytkin konfiguroitiin etukäteen template-toiminnallisuuden avulla valmiiksi odottamaan verkkoon liittämistä. MS120-24 mallin kytkimelle luotiin oma profiili ja konfiguroitiin portit valmiiksi. Kytkimelle konfiguroitiin yksi linkki MX-laitetta kohti, yksi linkki tukiasemaa kohti PoE-toiminnallisuuden kanssa ja loput Access-porteiksi Office VLAN:iin (ks. kuvio 10). Tulevaisuudessa voitaisiin siis verkkoon lisätä MS-120-24 -kytkin, jonka konfiguraatiot ovat jo valmiiksi tehtynä.

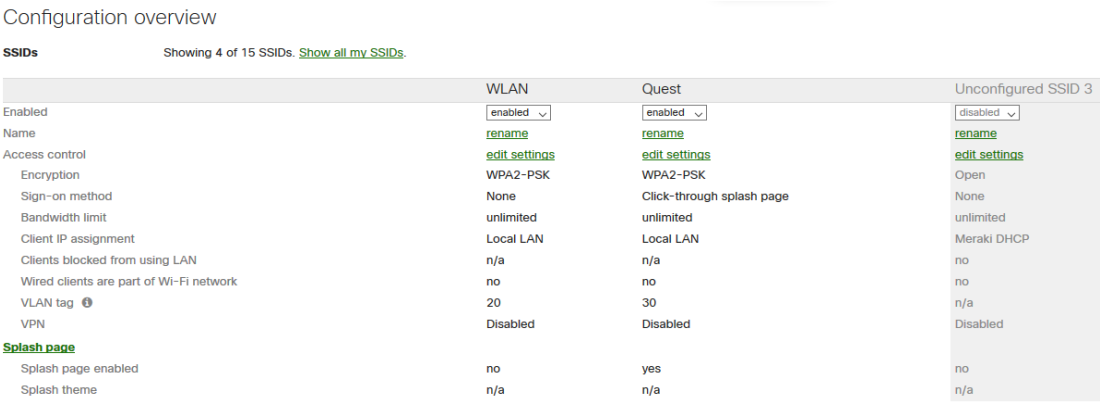


Kuvio 10. Kytkinporttien konfiguraatiota

4.2.3 Tukiasema

Tukiasemalle konfiguroitiin kaksi SSID:tä (Service Set Identifier) (ks. kuvio 11). Kummatkin liitettiin omaan VLAN:iin, jonka kautta päätelaitteet saivat osoitteensa.

Vierasverkkoon liittyessä langattomasti täytyi ensiksi hyväksyä käyttöehdot, jonka jälkeen voitiin internet-yhteyttä käyttää. Salauksena kummassakin käytettiin WPA2 (Wi-Fi Protected Access) ja kirjautuessa PSK (Pre-shared Key) eli salasanaa. Koska vierasverkon käyttäjille ei haluttu antaa oikeutta käyttää lähiverkon laitteita, niin estettiin vielä erikseen kaikki LAN:ia kohti oleva liikenne vierasverkosta.



Configuration overview

SSIDs Showing 4 of 15 SSIDs. Show all my SSIDs.

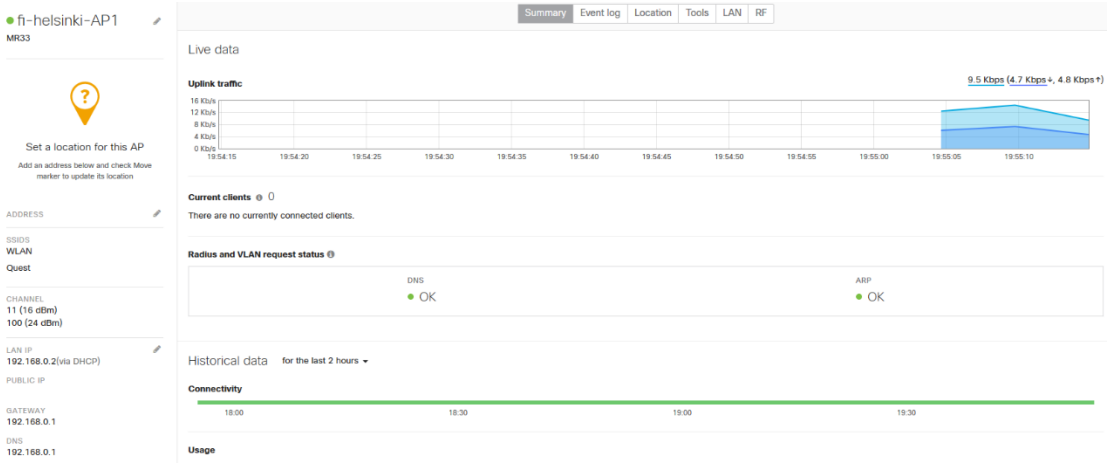
	WLAN	Quest	Unconfigured SSID 3
Enabled	enabled	enabled	disabled
Name	rename	rename	rename
Access control	edit settings	edit settings	edit settings
Encryption	WPA2-PSK	WPA2-PSK	Open
Sign-on method	None	Click-through splash page	None
Bandwidth limit	unlimited	unlimited	unlimited
Client IP assignment	Local LAN	Local LAN	Meraki DHCP
Clients blocked from using LAN	n/a	n/a	no
Wired clients are part of Wi-Fi network	no	no	no
VLAN tag	20	30	n/a
VPN	Disabled	Disabled	Disabled
Splash page			
Splash page enabled	no	yes	no
Splash theme	n/a	n/a	n/a

Kuvio 11. Konfiguraatiot SSID:n mukaisesti

Laitteet liitettiin verkkoon yksi kerrallaan konfiguraatioiden valmistuttua templatessa. Ensin liitettiin MX-laite (ks. kuvio 12), joka Cisco Merakin hallintapaneelissa tuli Online-tilaan automaattisesti. MX-laitteen etusivulla näkyi reaaliaikaista kuvaa porttien tiloista, yhteyden tilasta ja verkon käytöstä. Sivuilta pystyttiin katsomaan laitteen perustietoja ja asetuksia. Laitteille voidaan erikseen vielä asettaa sijainnit Googlen karttapalvelun tuoman ominaisuuden avulla esimerkiksi analytiikkaa varten.

Kuvio 12. Palomuurin valvonnan etusivu

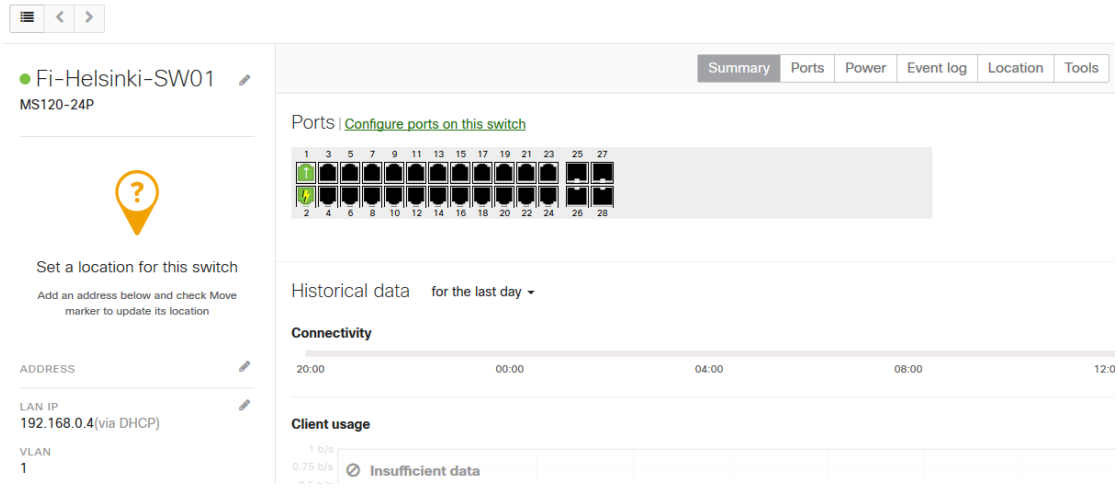
Tukiasema kytkettiin kiinni porttiin 11, koska portin on PoE+ -ominaisuus mahdollisti tukiaseman virransaannin. Tukiasema tuli Online-tilaan (ks. kuvio 13) ja vierasverkon SSID:n lähetys ympäristöön alkoi. WLAN SSID:tä ei ollut näkyvissä, koska se oli asetettu piilotetuksi.



Kuvio 13. Tukiaseman valvonnan etusivu

Verkkoon tuli ympäristön testauksien jälkeen mahdollisuus lisätä jo aikaisemmin konfiguroitu kytkin, joka oli malliltaan MS120-24p. Laite rekisteröitiin ja liitettiin verkkoon. Template-ominaisuudella oltiin luotu kytkinprofiili ja konfiguraatiot valmiiksi. Tukiasema kytkettiin irti MX-laitteesta ja tilalle liitettiin kytkin portista yksi.

Tukiasema liitettiin kytkinporttiin kaksi. Hetken päästä laitteet olivat keskitetyllä hallintapaneelilla Online-tilassa ja laitteita oli mahdollista operoida muutoksen jälkeen (ks. kuvio 14). Aikaisemmin luodut konfiguraatiot toimivat, niin kuin ne oli suunniteltukin.



Kuvio 14. Kytkimen valvonnan etusivu

4.3 Ympäristön tarkastelu

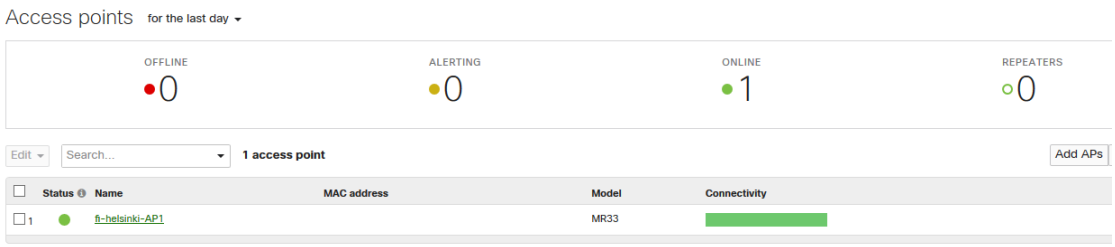
Luvussa tarkastellaan Cisco Merakin hallintapaneelin ominaisuuksia, valvonnan- ja vianselvityksen työkaluja. Lisäksi luvussa käydään läpi analytiikan työkalua ja lyhyesti ympäristön dokumentaatiota. Hallintapaneelin työkaluja kokeiltiin ja pohdittiin niiden tuomia hyötyjä.

4.3.1 Hallintapaneelin ominaisuudet

Hallintapaneelissa laitteilla on neljä eri tilaa, jotka ovat Online, Offline, Alerting ja Dormant. Tukiasemat voivat myös olla Repeater -tilassa (ks. kuvio 15), jolloin ne toimivat verkossa ”toistimena”. Kun tukiasemalla ei ole suoraa kaapelilla menevää yhteyttä LAN-verkkoon, tukiasema menee Repeater -tilaan ja luo mesh-linkin toiseen samassa tilassa tai LAN-verkossa kiinni olevaan tukiasemaan. Käyttäjiä ei missään vaiheessa pudoteta pois langattomasta verkosta, mikä tuo verkkoon lisää

luotettavuutta. Jos yksi kytkin välistä menee vikatilaan, usein kuitenkin PoE-toiminnallisuus säilyy ja tukiasemat jatkavat toimintaansa Repeater -tilassa.

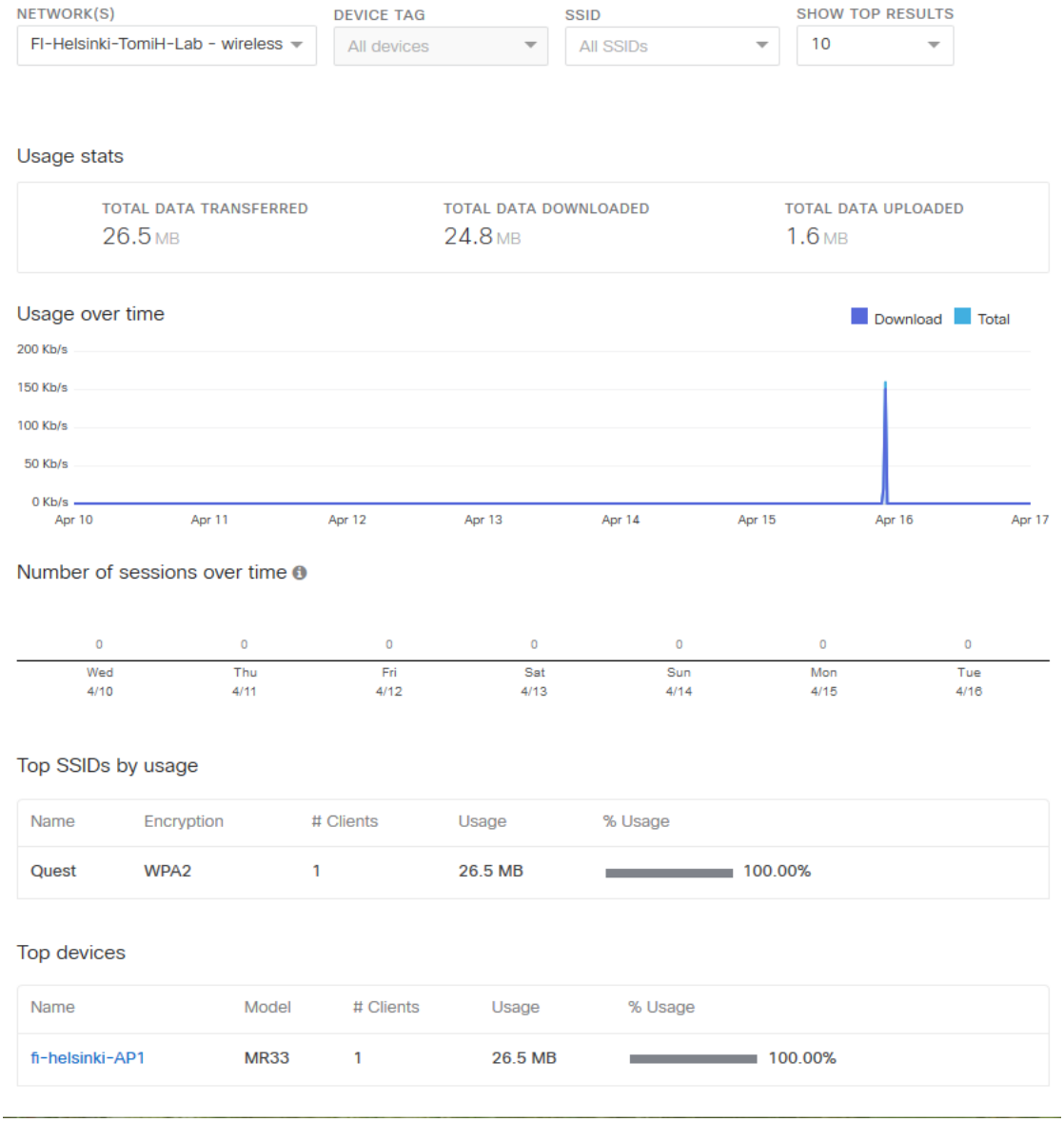
Kahdennetuilla MX-laitteilla varustetuissa ympäristöissä voidaan toteuttaa korkeaa saatavuutta, jolloin toinen laitteista toimii Warm Spare -periaatteella odottaen, että aktiivinen muuri menee alas. Kahdennetuilla yhteyksillä ja SD-WAN-toiminnallisuudella voidaan nostaa verkon vikasietoisuutta vielä pykälän korkeammaksi.



Kuvio 15. Tukiasemien tilat

4.3.2 Valvonta

Valvontaa varten jokaiselle laitetyypille on omat sivunsa. Laitteiden yhteyksiä, läpikulkevaa liikennettä, porttien tiloja ja laitteen tapahtumia voidaan valvoa reaaliaikaisesti. Vikatilanteissa, kuten ensisijaisen WAN-yhteyden katkeamisesta, voidaan hallintapaneeli konfiguroida lähettämään hälytys haluttuun kohteeseen. Hälytyksiä voidaan asettaa useita erilaisia, joten hallintapaneelin ei tarvitse olla jatkuvasti auki verkkoa valvottaessa. Verkosta pystytään keräämään yhteenvetoraportti (ks. kuvio 16) viimeiseltä kuukaudelta ja viedä se hallintapaneelista Exceliin. Yhteenvetoraportti sisältää tietoa liikenteestä, liikennetyypeistä ja käyttäjien laitteista. MX-laitteille, kytkimille ja tukiasemille on jokaiselle omat yhteenvetoraporttinsa. Ominaisuuden avulla verkon käyttömäärien ja statistiikan raportointi voidaan hoitaa sujuvammin. Verkolle ei erikseen tarvitse suorittaa mittaustoimenpiteitä. Kytkimien yhteenvetoraportissa käyttöasteet on kuvattu porttikohtaisesti.

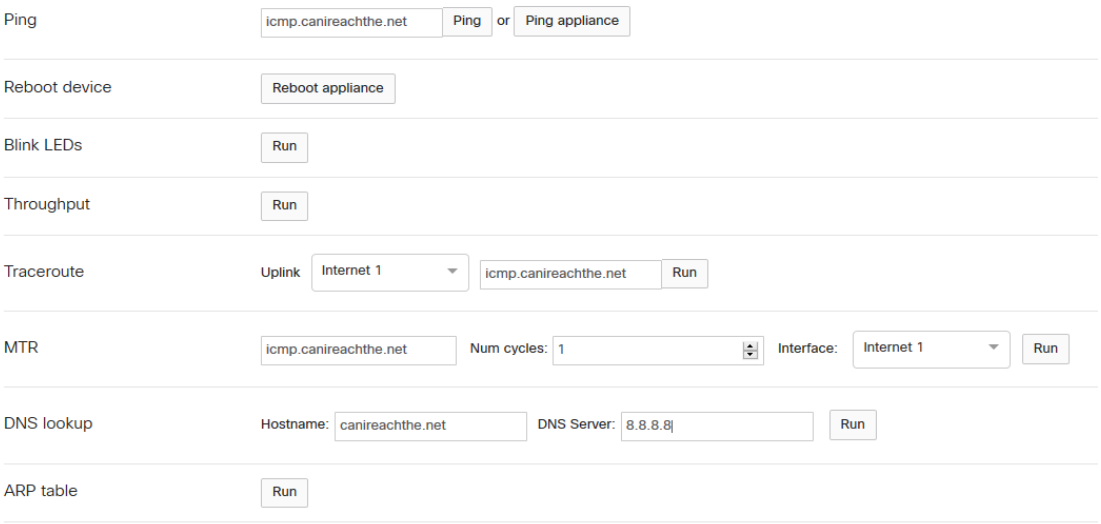


Kuvio 16. Osa tukiasemien yhteenvetoraportista

4.3.3 Vianselvitys

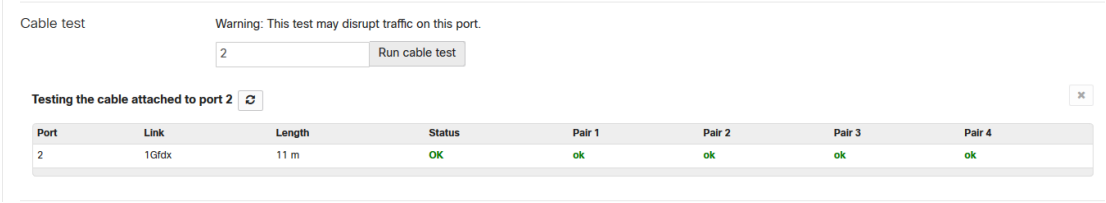
Hallintapaneelissa on laitekohtaisesti työkaluja vianselvitystä varten (ks. kuvio 17). Moni näistä työkaluista osoittautuivat testeissä todella hyödyllisiksi. Hallintapaneelista pystyttiin testaamaan yhteyksiä haluttuihin kohteisiin, tarvittaessa käynnistämään laitteita uudelleen ja seuraamaan laitekohtaisesti, kuinka paljon liikennettä menee sen läpi. Tukiasemien vikatilanteisiin toimiva työkalu kytkimissä on porttien disablointi ja enablointi, jolloin PoE:n varassa olevat laitteet voidaan

pakottaa käynnistymään uudelleen. Porttitesti työkalulla pystytään myös tutkimaan mahdollista viallista kaapelia ilman paikan päällä suoritettavia testauksia.



Kuvio 17. MX-laitteen vianselvityksen työkalut

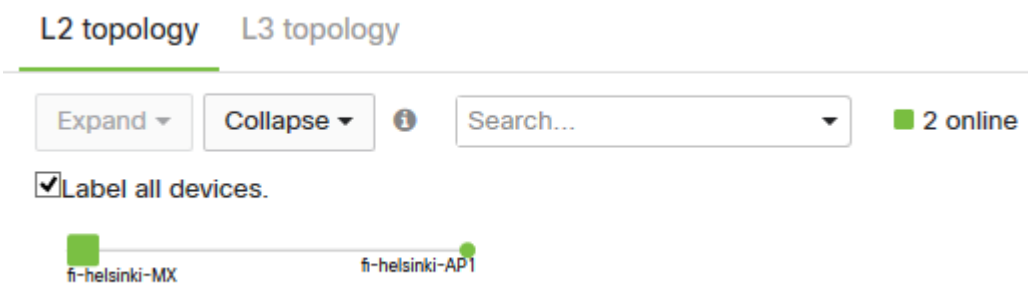
Kytkimessä on vianselvitystä varten useita samoja työkaluja, kuten MX-laitteissakin. Kytkimessä testattiin kaapelitesti -työkalua (ks. kuvio 18). Porttiin kaksi oli kytketty tukiasema. Kaapelin tila on hyvä, eikä siitä löytynyt kaapelitestissä ongelmia. Lisäksi kytkimen vianselvitystä varten löytyy työkalut MAC-taulun katselemista varten ja portit voidaan estää ja sallia yhdellä painalluksella.



Kuvio 18. Kytkinporttiin 2 tehty porttitesti.

Hallintapaneeli luo verkosta Layer 2- ja Layer 3 -topologiat. Tämä tuo sen edun, ettei erikseen ole tarvetta dokumentoida ja piirtää topologiakuvia. Hallintapaneelin

topologiakuva muuttuu myös verkon muutosten ja vikatilanteiden mukana. Layer 2 kuvassa näkyy laitteiden väliset liitännät (ks. kuvio 19).



Kuvio 19. Hallintapaneelin luoma L2-topologiakuva

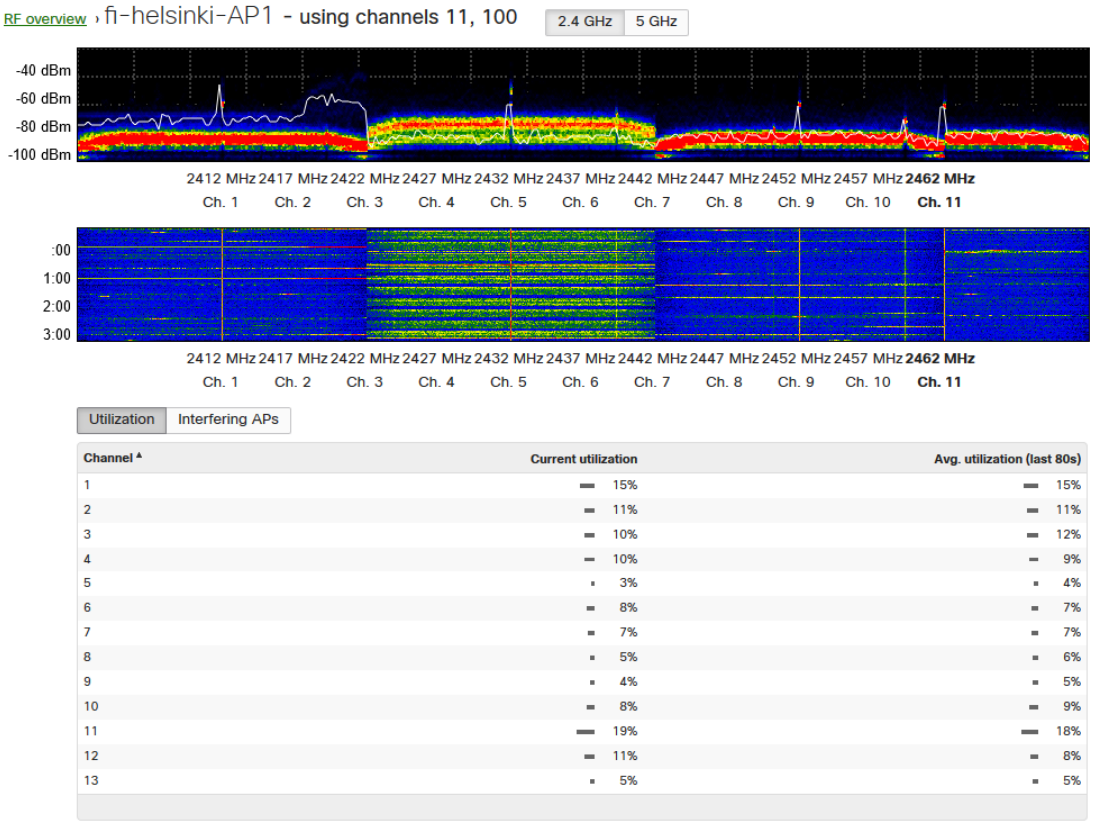
Layer 3 kuvassa näkyy L3-tason laitteet ja verkot (ks. kuvio 20). VLAN nimien alta pystyttiin katselemaan niihin konfiguroituja aliverkkoja.

Kuvio 20. Hallintapaneelin luoma L3-topologiakuva

Tukiasemien hallintaa ja valvontaa varten on erikseen omia työkaluja niiden toimintavarmuuden ja turvallisuuden varmistamiseksi. Air Marshal -työkalu on Cisco Merakin oma WIPS (Wireless Intrusion Prevention System) -ratkaisu, joka on integroitu jokaiseen tukiasemaan. Air Marshal skannaa ympäristöä reaaliaikaisesti ja estää uhkia automaattisesti tunnistamalla ”rogue” -tukiasemia. Ympäristöstä kerätään tietoa ja ”rogue”-tukiasemat neutralisoidaan pois verkosta, kuten myös muutkin langattomaan verkkoon kohdistuvat uhat.

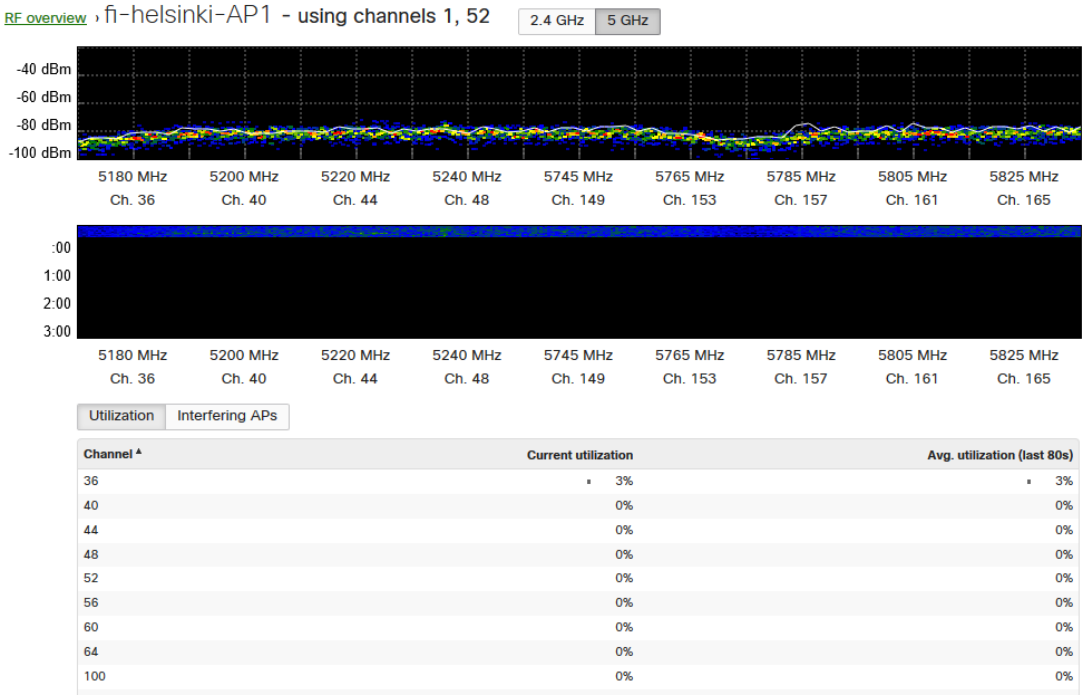
RF Spectrum -työkalulla (ks. kuvio 21) voidaan seurata kanavien käyttömääriä ja tutkia, häiritsevätkö lähistöllä olevat tukiasemat toisiaan. Työkalua käytetään sekä vianselvityksessä että tukiasemien sijaintien suunnittelussa, kun niitä lisätään verkkoon. Kuvio 21 esiintyvässä kuvaajassa näkyy kuinka tukiaseman käyttämä

kanava 5 häiritsee hieman lähellä olevien tukiasemien kanavia 1 ja 9. Cisco Merakin tukiasema toimi kuvanottohetkellä kanavalla 11.



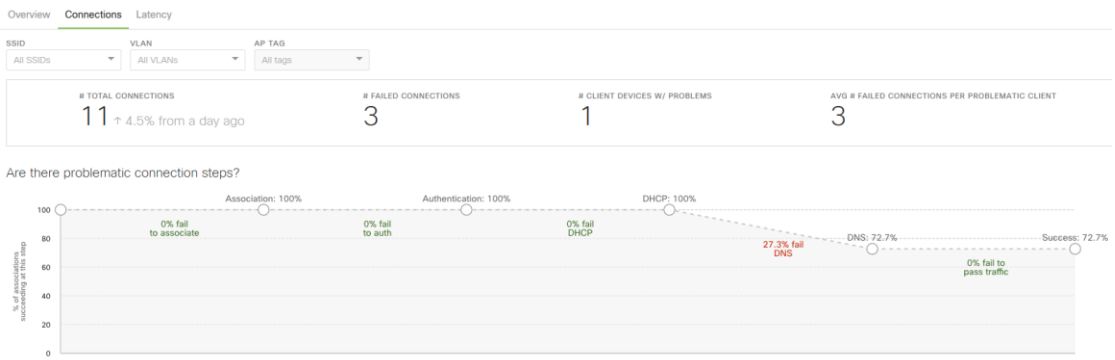
Kuvio 21. RF Spectrum työkalun 2.4 GHz:n kanavien yleiskatsaus

Taajuuksien eroja tarkasteltiin ja samalla huomattiin, kuinka suuri ero toisten kanavien häirinnässä oli 2.4 GHz:n ja 5 GHz:n välillä (Ks. Kuvio 22). 5 GHz:n taajuudella on enemmän kanavia, joka vähentää kanavien välisiä häiriöitä.



Kuvio 22. RF Spectrum työkalun 5 GHz:n kanavien yleiskatsaus

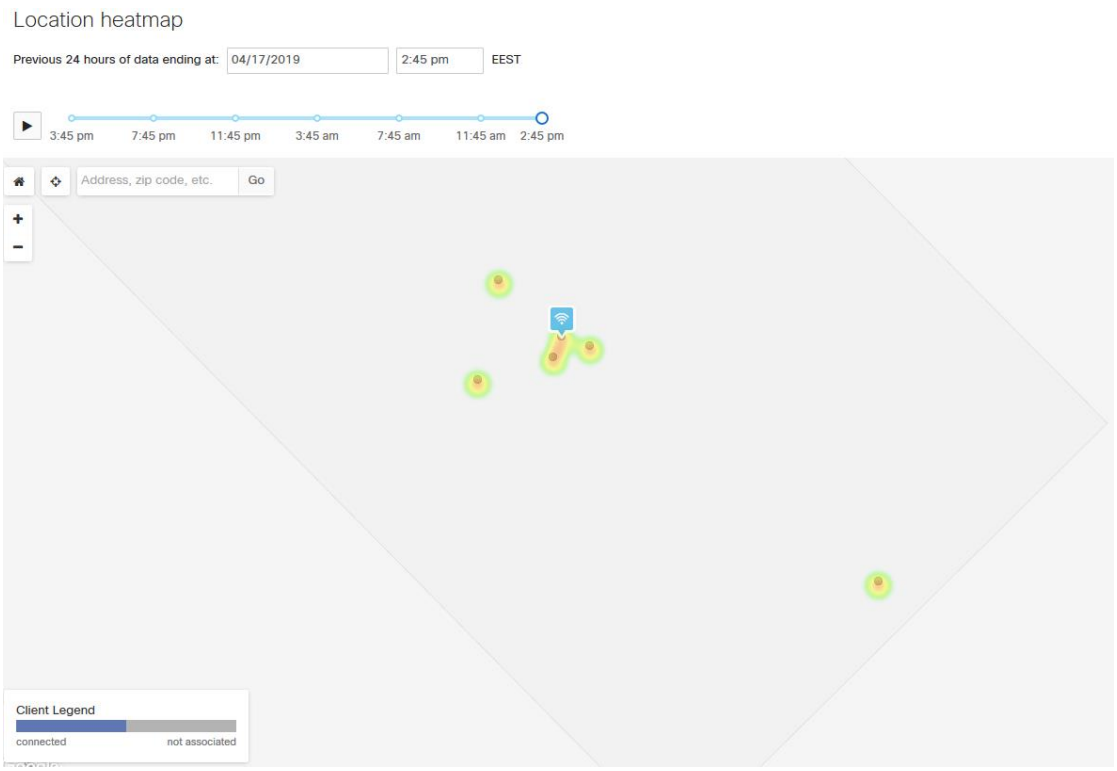
Wireless Health -työkalulla (ks. kuvio 23) voidaan katsella menneitä ongelmia langattoman verkon käyttäjien osalta. Työkalulla yhteyksien hetkelliset häiriöt, jotka eivät välttämättä luo pitkäaikaisempaa hälytystä jäävät häiriöhistoriaan. Sivuilta pystytään lisäksi seuraamaan eri liikennetyyppejä ja niiden latensseja.



Kuvio 23. Wireless Health -työkalu ja DNS-kokeilun aiheuttamat ongelmat

4.3.4 Analytiikka

Laitteiden sijainti voitiin merkitä karttaan ja hallintapaneeliin voidaan myös lisätä kuvia tilojen pohjapiirroksista. Näiden avulla voidaan sijoitella laitteita ja analysoida ympäristöä kartoitustyötä varten. Sijainti ja skannaus -analytiikka täytyy sallia, jotta saadaan käyttöön enemmän analytiikkatyökaluja. Location Heatmap -työkalun (ks. kuvio 24) avulla voidaan tutkia, minkä tukiaseman piirissä laitteet ovat olleet langattomassa verkossa. Tämä kuitenkin vaatii sen, että tukiasemat on sijoiteltu tarkasti karttaan eikä tukiasemat ole samassa linjassa toistensa kanssa. Tukiasemat on myös sijoitettava eri suuntiin toisistaan katsottuna esimerkiksi rakennuksen tai tilan reunoille. Päätelaitteen on kuultava kolme tukiasemaa eri suunnista, jolloin signaaleilla mitatut etäisyydet ovat tällöin tarkempia, vaikkakin suuntaa antavia.



Kuvio 24. Location Heatmap ja päätelaitteiden sijainteja

4.3.5 Dokumentaatio

Cisco Merakin dokumentaatiosta löytyy ohjeita niin vianselvitykseen, konfigurointiin, kuin yleiseen ympäristönhallintaakin. Hallintapaneelin yläosassa on ”Search Dashboard” -lomakepalkki, josta pystytään hakemaan Cisco Merakin tuen luomia oppaita esimerkiksi konfigurointiin ja vianselvitykseen liittyen. Se on käytännössä Cisco Merakin oma ”Knowledge Base”, joka on täynnä Cisco Merakin tuen luomaa dokumentaatiota ympäristöstä yhdessä paikassa. Cisco Merakin hallintapaneelissa on myös erikseen omat dokumentaatiot tuotteelle.

4.4 Ympäristön testaus

4.4.1 Ympäristön reagointi ja hälytykset

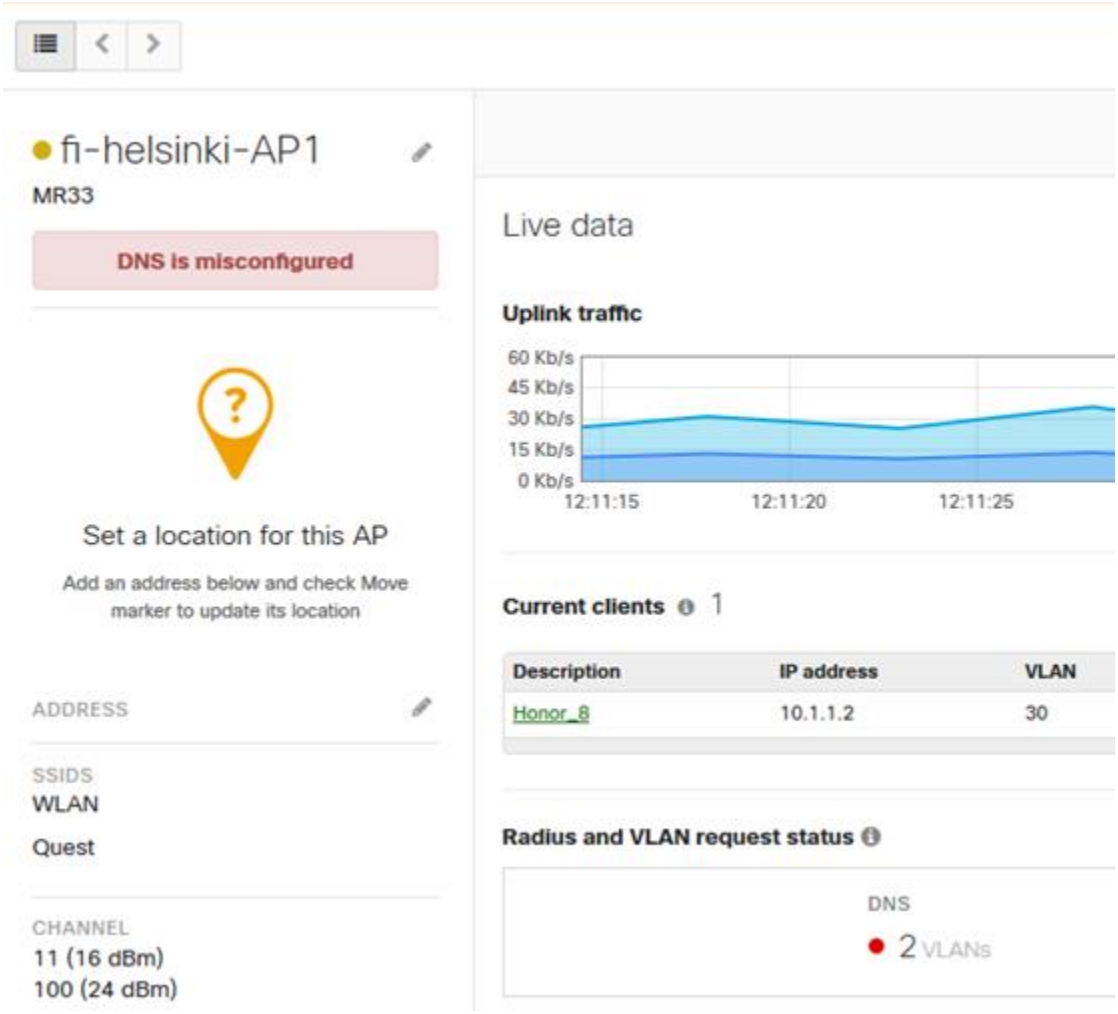
Ympäristön toimintaa ja sen reaktioita testattiin muutamalla kokeilulla. Tiettyjä vikatilanteita, kuten tukiaseman jumitilaan menemistä tai muita laiterikkotapauksia ei voitu testata erikseen. Tukiaseman mennessä jumitilaan ensin on hyvä kokeilla käynnistää tukiasema uudelleen etänä käyttämällä PoE-ominaisuus pois päältä. Mikäli tukiasema tule Online-tilaan, eikä konfiguraatioista tai kaapelista löydy selitystä vikatilanteelle, Cisco Merakin tukeen voidaan hallintapaneelista ottaa suoraan yhteyttä. Tuesta saadaan apua laajempiin vikatilanteisiin ja laitevaihtotapauksissa he lähettävät uuden laitteen vanhan rikkimenneen tilalle. Laitevaihtotapauksissa täytyy ottaa huomioon, että Cisco Merakin laitteet ovat konfiguroitu oletuksena käyttämään VLAN 1. Mikäli koko VLAN on muista laitteista poistettu, ei verkkoon kytkettynä kyseinen laite saa yhteyttä keskitettyyn hallintaan.

MX-laitteella on mahdollisuus tällä hetkellä saada internet-yhteys WAN1-portista tai mobiiliverkkoa hyödyntäen. Kun WAN1-portista yhteys katoaa, niin yhteys vaihtuu hetkessä toimimaan langattomasti. Mikäli internetyhteydessä on jokin ongelma, siitä aiheutuu hälytys ja toissijainen yhteys otetaan käyttöön. Erilaisia hälytyksiä pystytään konfiguroida hallintapaneelista laitteille, kuten esimerkiksi kytkimissä voidaan tärkeisiin portteihin lisätä vikatilanteita varten hälytys. Laitteen yhteyden kadotessa Merakin keskitettyyn hallintaan tulee hälytys ja laitetta ei pilvestä pysty silloin käsin

operoimaan. Laite kuitenkin jatkaa toimintaansa normaaliin tapaan, vaikka hallinta ei väliaikaisesti toimi. Kun tukiasemalta irrotettiin kaapeli, se alkoi hallintapaneelissa hälyttämään, koska tukiasema ei saanut enää virtaa.

4.4.2 Konfiguraatiovirhe

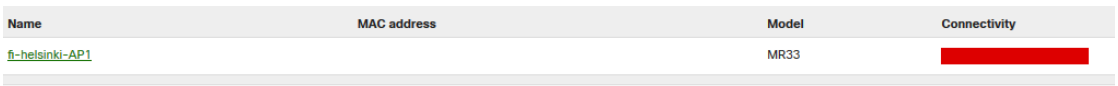
Ympäristössä testattiin, miten se reagoi konfiguraatiovirheeseen. DHCP-palvelimen jakamia DNS-nimipalvelimen tietoja muokattiin ja siitä aiheutui hälytys suoraan tukiasemalle (ks. kuvio 25). Tällä kertaa kuitenkin sivustoille pääsee palomuurin käyttämän nimipalvelimen ansiosta. Muussa tapauksessa tulisi ”DNS Server Unreachable”-hälytys. Tässä tapauksessa konfiguraation korjaus poisti hälytyksen ja samalla sen aiheuttamat ongelmat poistuivat. Samoin esimerkiksi kytkinten välisistä porttikonfiguraatioista aiheutuisi hälytys VLAN-epäsuhtaisuuksista porttien välillä. Aina ei ole erikseen tarvetta etsiä vianselvityksessä vian aiheuttajaa, koska älykäs viantunnistus kertoo jo valmiiksi vian aiheuttajan, kuten testatun DNS-konfiguraatiovirheen tapauksessa. Templaten toiminnallisuuden avulla pystytään konfiguraatiovirheitä osittain ehkäisemään, koska konfiguraatiot eivät sijaitse verkon hallintasivulla missä analytiikka, valvonnan ja vianselvityksen työkalut ovat.



Kuvio 25. Nimipalvelimen saavuttamattomuus aiheutti hälytyksen

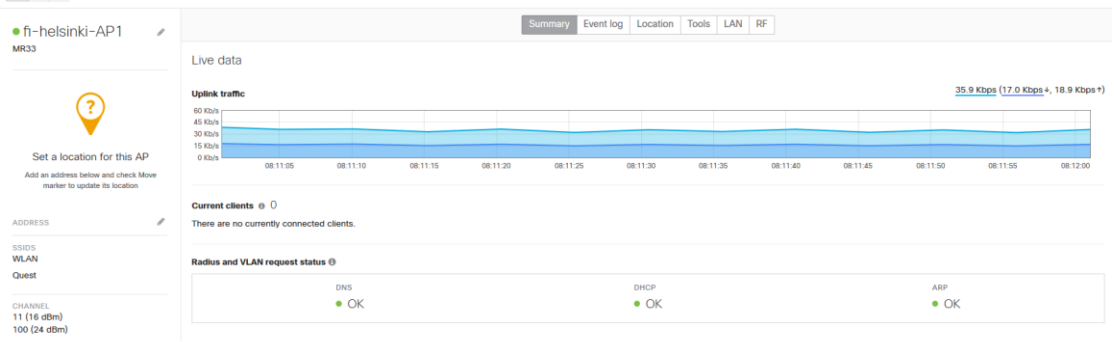
4.4.3 Tukiaseman vikatilanne

Hallintapaneelia kokeiltiin ja sen ominaisuuksia tutkittiin runsaasti. Erilaisia asetuksia kokeiltiin ja annettiin verkon olla pystyssä ilman muutoksia. Tänä aikana tukiasema oli onnistunut menemään vikatilaan joko omista kokeiluista, tai sen yhteys Merakin pilveen oli jostain syystä kadonnut (ks. kuvio 26).



Kuvio 26. Tukiasema ollut alhaalla jonkin aikaa

Tämä toi täydellisen mahdollisuuden testata hallintapaneelin työkaluja. PoE-uudelleenkäynnistys toteutettiin poistamalla portti käytöstä ja hetken päästä ottamalla se takaisin käyttöön. Tukiasemaan saatiin jälleen kontakti, mutta se ei jostain syystä saanut haettua konfiguraatiotaan Merakin pilvestä. Tukiasema oli toiminnassa, mutta siihen jäi vielä aktiivinen hälytys. Kuitenkin hallintapaneelista tukiasemaa pystyttiin kontrolloimaan, joten lopuksi se käskettiin käynnistymään uudelleen työkalun avulla. Tukiasema tuli tämän jälkeen Online-tilaan ja se onnistui hakemaan päivitetyt konfiguraatiot pilvestä (ks. kuvio 27).



Kuvio 27. Tukiaseman tila vikatilanteen jälkeen

5 Tuloksien tarkastelu

Luvussa vertaillaan perinteistä verkkoa ja pilvipohjaisesti hallittavaa verkkoa. Tarkasteltiin etuja Cisco Merakilla luodussa ympäristössä verrattuna perinteiseen verkkoon verrattuna hallinnan, valvonnan, vianhallinnan sekä muutoksien näkökulmasta. Lisäksi erikseen pohdittiin SD-WAN toteutuksen etuja kummassakin tapauksessa.

5.1 Perinteinen verkko

5.1.1 Hallinta

Perinteisessä verkossa laitteita hallitaan ja konfiguroidaan usein laitekohtaisen hallintaliittymän kautta. Verkossa on usein laitteita eri laitevalmistajilta ja ne voivat olla hankittu kaikissa verkon elinkaaren vaiheissa. Usean laitevalmistajan laitteilla luotu verkko on usein myös monimutkaisempi valvottava ja hallittava. Suurimmalla osasta laitteita ei ole minkäänlaista keskitettyä hallintaan, vaan niitä hallitaan sekä valvotaan laitekohtaisesti joko paikallisesti tai etäyhteyden avulla.

Yhden laitevalmistajan laitteilla toteutetussa verkossa ongelmia on vähemmän, koska laitteet on suunniteltu yhteensopiviksi toistensa kanssa. Laitteita valvotaan ja hallitaan usein laitekohtaisen hallintaliittymän kautta. Asennusvaiheessa laitteille tarvitaan usein etäyhteys konfigurointia varten. Hyvänä poikkeusesimerkkinä toimii Palo Alton Panorama, jolla voidaan kontrolloida palomuureja keskitetysti. Panoramasta voidaan tehdä sääntöihin muutoksia useampaan kohteeseen kerralla, mutta se on usein manuaalista ja rajoittuu laiteryhmiin. Panorama ei poista tarvetta etäyhteydelle ja paikalliselle konfiguraatiolle asennusvaiheessa. Keskitetyn hallinnan ulkopuolelle jäävät kaikki muut verkon tarpeelliset laitteet.

5.1.2 Valvonta ja dokumentointi

Valvonnasta jää puuttumaan verkon kokonaiskuva, koska se on komponenttikohtaista. Vuosien varrella muuttunut arkkitehtuuri on voinut jo aiheuttaa ongelmia, joita ei ole aikaisemmin huomattu. Mahdollisesti tällaisissa tapauksissa verkkoa joudutaan korjaamaan jo hallintaan ja valvontaan ottaessa. Yhden laitevalmistajan laitteilla toteutettu verkko toisi hallittavuutta ja vähentäisi vikatilanteita. Liikennemäärien seurantaa varten täytyy usein erikseen verkossa tehdä mittauksia.

Lokitukset lähetetään usein erilliselle palvelimelle säilöön, koska muuten laitteiden muisti voisi loppua kesken ja horjuttaa sen toimintavarmuutta. Lokituksesta erilliselle

palvelimelle on kuitenkin hyötyä, koska laitteen lokeja voidaan seurata senkin jälkeen, kun laite on mennyt rikki ja säästetään laitteen muistia. Layer 2- ja Layer 3-topologiakuvat täytyy luoda manuaalisesti ja muokata niitä aina, kun verkossa tulee jokin suurempi muutos. Koska laitevalmistajia on usein paljon, jokaiselle täytyy olla omat dokumentaatiot niiden operoimista varten. Syventävä dokumentaatio on hajaantunut pitkin laitevalmistajien sivuja. Vianhallinnan näkökulmasta katsottuna jokaisen eri laitevalmistajan laitteella voi esiintyä toisistaan huomattavasti eroavia ongelmia.

5.1.3 Häiriönhallinta

Eri laitevalmistajien laitteet eivät aina ole täysin yhteensopivia toistensa kanssa ja se tuo omat riskinsä erilaisiin ongelmatilanteisiin. Esimerkiksi eri laitevalmistajien spanning-treen käyttäytyminen ja oletusprioriteetit voivat erota huomattavasti, joka tuo ongelmia verkon sulavaan toimintaan. Yhteensopivuusongelmia voi myös tulla esimerkiksi eri laitevalmistajien MTU:n (Maximum Transfer Unit) oletusarvoissa, joka aiheuttaa verkossa hitautta ja pakettien putoamista välistä. Yhden laitevalmistajan laitteilla toteutetussa verkossa ongelmia on vähemmän, koska laitteet on suunniteltu yhteensopiviksi toistensa kanssa. Useita sekaverkon vikatilanteita voidaan välttää, mutta esimerkiksi liikenteen mittaaminen, kaapeleiden testaus ja pakettien sieppaus joudutaan useimmiten tekemään laiteiden luona. Missä tahansa verkossa voi tulla häiriöitä, mutta laitevalinnoilla niitä voidaan ennaltaehkäistä ja lyhentää vikatilanteita.

Eri elinkaaressa olevien laitteiden olemassaolo verkossa voi aiheuttaa sen, että vanhat laitteet eivät välttämättä tue kaikkia tarvittavia toimintoja ja niistä on jo tekninen tuki voinut lakata kokonaan. Laitteen rikkoutuessa samanmallista laitetta ei ole välttämättä tällöin saatavilla RMA-prosessissa (Return Merchandise Authorization). Uuden laitteen konfigurointi toimintavalmiiksi vanhaan ympäristöön syö myös aikaa ja pitkittää vikatilannetta. Koska verkon kaikissa elinkaaren vaiheissa on voitu lisätä erilaisia laitteita ympäristöön, on sen alkuperäinen arkkitehtuuri muuttunut verkkoympäristön evoluution tulokseksi. Alkuperäinen suunniteltu ympäristö on voinut muuttua vuosien varrella radikaalisti.

Dokumentoimaton verkko voi venyttää vianselvitystä huomattavasti. Vaikka vianselvitykseen lähtötiedot olisivat huonot, niin dokumentoidussa verkossa asiat löytyvät nopeammin. Esimerkiksi vikatilassa olevan laitteen löytäminen MAC-osoitteen avulla voi pitkittyä, koska heikoilla lähtötiedoilla ei voida laitteen sijaintia päätellä. MAC-osoitteen avulla täytyy kulkea laitteelta toiselle, kunnes löydetään portti laitetta kohti ja pystytään vianselvitys aloittamaan. Aikaa menee turhaan ympäristön esiselvitykseen. Ilman dokumentointia ympäristöön tutustuminenkin on huomattavasti haastavampaa.

5.2 Pilvipohjaiseen keskitettyyn hallintaan perustuva verkko

5.2.1 Hallinta

Cisco Merakin laitteet kytketään paikallisesti ja internetyhteyden saatuaan laitteet ottavat yhteyttä pilvipohjaiseen hallintaan. Ne voidaan joko konfiguroida tai käyttää valmista konfiguraatiota templatesta jo suunnitellulle topologialle. Käytännössä voidaan etukäteen suunnitella jokin vakioitu kokonaisarkkitehtuuri, joka valitaan käyttöön riippuen asiakkaan verkon tarpeista. Toimipisteiden kaikki laitteet olisivat etukäteen konfiguroituina ennen kuin ne on asennettu tai lisätty hallintapaneeliin. Saman sukupolven ja laitevalmistajan laitteet on suunniteltu yhteensopiviksi toistensa kanssa. Ympäristö tunnistaa päätelaitteita mallien mukaisesti. Koska ympäristö on joustava, sitä voidaan tarvittaessa laajentaa lisäämällä laitteita verkkoon. Aliverkkoja voidaan tarvittaessa lisätä ja laajentaa, kuten perinteisessä verkossakin.

Cisco Merakin laitteissa ei ole ollenkaan CLI:tä (Command Line Interface), vaan sitä hallitaan kokonaan graafisen käyttöliittymän kautta keskitetysti tai harvinaisemmissa vikatilanteissa paikallisesti etäyhteyden välityksellä selainpohjaisella käyttöliittymällä. Hallinta on siis visualisoitu ja yksinkertaistettu moderniksi ja käyttäjäystävälliseksi. Koska useiden toimipisteiden laitteita voidaan hallita template-ominaisuudella, tämä mahdollistaa ja helpottaa huomattavasti massamuutosten toteuttamista ympäristöille. Tämän ansiosta pystytään vaivattomammin tekemään yhdellä kertaa muutoksia useammalle toimipisteelle laajemmalla skaalalla.

Template -toiminnallisuuden ansiosta liikkuvien toimipisteiden asentaminen on vaivattomampaa. Cisco Merakin laitteet ottavat yhteyttä pilveen, kun niillä on yhteys internettiin. Konfiguraatiot odottavat pilvessä laitteiden käyttöönottoa aina uudella toimipisteellä. Logistiikan näkökulmasta katsottuna tämä on myös vaivattomampaa, koska laitteet voidaan lähettää valmistajalta suoraan kohteeseen. Uusi laite rekisteröidään ja liitetään keskitetyssä hallinnassa haluttuun toimipisteen verkkoon. Templatella määritetyt asetukset latautuvat automaattisesti uudelle laitteelle, kun se kytketään kiinni verkossa sijaitsevaan verkkolaitteeseen. Auto VPN -ominaisuus varmistaa väliaikaisen spoke-toimipisteen yhteyden Hub-toimipisteelle.

5.2.2 Valvonta ja dokumentointi

Valvonta toteutuu hallintapaneelissa. Liikennemääriä ja statistiikkaa voidaan seurata laitekohtaisesti 30 päivän ajalta. Statistiikkaa voidaan viedä hallintapaneelista Exceliin raportointia varten. Analytiikalla pystytään seuraamaan laitteiden yleisimpiä sijainteja toimipisteellä ja tarvittaessa voidaan ennaltaehkäistä langattoman verkon kuuluvuusongelmia. Tukiasemia voidaan uudelleen sijoittaa tai lisätä toimipisteelle jälkeenpäin. Hallintapaneelista pystytään konfiguroimaan erilaisia hälytyksiä, jotka jo itsessään tekevät vianselvityksestä vaivattomampaa automaattisen viantunnistuksen tuoman ilmoituksen perusteella. Hälytykset lähetetään valittuun kohteeseen halutulla metodilla. Asiantuntija, jolla on jo ennestään kokemusta tietoverkoista, pystytään perehdyttämään vaivattomammin ympäristöön kuin perinteisen verkon osalta. Lisäksi keskitetty hallinta ja templateilla vakioidut toimipisteet helpottavat ympäristöntuntemusta.

Moni asia pilvipohjaisesti hallittavassa verkossa on automatisoitu. Laitteiden ohjelmistopäivitykset voidaan ajoittaa päivän tai viikon hiljaisimpaan hetkeen. Verkkojen dokumentaatio, kuten esimerkiksi topologiakuvat, luodaan automaattisesti ja ne löytyvät silloin, kun niitä eniten tarvitaan. Verkossa tapahtuvat muutokset päivittyvät topologiakuviin automaattisesti. Konfiguroitavat hälytykset perustuvat ympäristön automaattiseen ongelmien havaitsemiseen. Se säästää aikaa häiriönhallinnassa, koska sen avulla saadaan suora vihje siitä, mikä verkossa on vialla ilman ylimääräistä etsimistä.

5.2.3 Häiriönhallinta

Webbipohjainen hallintapaneeli on jo itsessään työkalu vianselvitystä varten. Valvontatyökaluilla ja hälytyksillä pystytään rajaamaan vikatilanteen laajuutta. Työkaluilla ja automaattisella ongelmienhavaitsemisella voidaan nopeuttaa ja jopa ohittaa tyypillisiä vianselvityksen askelia. Esimerkiksi kaapelitestejä voidaan tehdä hallintapaneelista ja liikennemäärät ovat selvitettävissä ilman, että tarvitsee lähteä laitteiden luokse testaamaan erikseen.

Koska laitteita hallitaan keskitetysti yhdestä paikkaa, ei laitteille tarvitse ottaa SSH-yhteyttä (Secure Shell) tai käyttää graafisen käyttöliittymään tarkoitettua erillistä ohjelmaa. Useamman käyttöliittymän välillä vianselvityksen aika venyy. Kaikkien laitetyyppien löytyminen samasta paikasta helpottaa siten, ettei tarvitse eri paikoista lähteä tutkimaan eri verkon osia. Esimerkiksi konfiguraatiovirheet aiheuttavat usein viasta ilmoittavia hälytyksiä ja muutokset nähdään lokituksen avulla. Reaaliaikaisilla ja graafisilla työkaluilla on huomattavasti vaivattomampaa selvittää langattoman verkon kuuluvuus- ja yhteysongelmia kuin manuaalisesti päivitettävällä käskyllä vanhemmissa verkkoympäristöissä. Sieltä pystytään myös selvittämään käyttäjäkohtaisia ongelmia kätevästi.

Laitteet ovat samalta valmistajalta, niillä on keskitetty hallinta ja dokumentaatio löytyy yhdestä paikasta. Hallintapaneelista löytyy toimipisteiden omat Layer 2- ja Layer 3-topologiat. Topologiakuvia ei tarvitse etsiä tai luoda juuri silloin, kun niitä eniten tarvitaan. Dokumentoidussa ympäristössä ei tarvitse tehdä niin suurta esiselvitystä kuin dokumentoimattomassa verkossa, mikä lyhentää häiriön kestoa. Hallintapaneeli oppii käyttämään nopeasti ja arkkitehtuurin vakiointi helpottaa ympäristön vianselvitystä. Vakioidun ympäristön muistaminen on asiantuntijalle huomattavasti vaivattomampaa ja lähtötiedot uutta häiriönselvitystä varten ovat vahvemmat. Häiriönhallinnan kannalta häiriön kestä lyhentyisi näiden ympäristön ominaisuuksien avulla perinteisen verkon häiriönhallintaan verraten.

Hallintapaneelista voidaan keskitetyn hallinnan avulla nopeasti luoda tiketti laitekohtaisesti Cisco Merakin TAC:le (Technical Assistant Centre) ja saada sieltä

tukipyyntöihin apua 24/7. Templaten toiminnallisuuden avulla vianselvityksessä ja valvonnassa konfiguraatiovirheiden mahdollisuus on pienempi, koska verkon valvontasivuilta ei juuri voi muutoksia tehdä, vaan ensin täytyy mennä templaten alle ja konfiguroida sieltä halutut muutokset. Useiden asioiden muuttaminen ja poistaminen kysyy vielä erikseen varmistuksen päätökselle. Esimerkiksi verkon poistaminen vie erillisille varmistussivulle, jossa vielä toisen kerran varmistetaan, että näin halutaan tehdä.

5.3 Standardimuutos

Standardimuutokset, kuten esimerkiksi portti- tai VLAN-muutokset, ovat pienen riskin muutoksia. Pilvipohjaisesti hallittavan ympäristön konfigurointia on tehty yksinkertaisemmaksi ja käyttäjäystävällisemmäksi. Koska laitteet hakevat konfiguraationsa pilvestä, niin konfiguraatiovirheiden korjaaminen on siinä mielessä vaivattomampaa, ettei itse laitteelle ole tarvetta ottaa etäyhteyttä tai konfiguroida sitä paikallisesti. Muutos voidaan toteuttaa kaikille laitteille yhdellä toimenpiteellä. Tämä nopeuttaa suurienkin ympäristöjen muutosprosessia huomattavasti, koska jokaiselle laitteelle ei tarvitse erikseen käydä muutosta tekemässä. Hallintapaneelissa voidaan korjata virheitä tai tehdä rollback, mikäli muutos aiheuttaa ongelmia verkon toimintaan. Keskitetty hallinta mahdollistaa myös samasta hallintapaneelista muutoksien teon useiden toimipisteiden välisiin VPN-yhteyksiin. VPN-tunnelit luodaan Merakin pilven toimesta automaattisesti, mutta tarvittaessa niitä voidaan luoda myös muiden laitevalmistajien laitteita kohti. Ympäristön käyttäjäystävällisen hallintapaneelin ja automatisoinnin avulla monimutkaisempien standardimuutosten riskit pienenevät. Ympäristön vakiointi pienentää myös konfiguraatiovirheiden riskejä.

5.4 SD-WAN

SD-WAN-toiminnallisuutta varten pitää perinteiseen LAN-verkkoon hankkia erillinen SD-WAN-laite muiden laitteiden rinnalle. Ominaisuutta ei löydy vanhemmista palomuureista tai reitittimistä integroituna. Moni sovellus ja työskentelyalusta on

siirtynyt pilveen. SD-WAN tarkoituksena on vähentää häiriöitä ja lisätä luotettavuutta sekä turvallisuutta yhteyksissä. Perinteisellä ratkaisulla rakennettuun LAN-ympäristöön voidaan erikseen SD-WAN toteutus tehdä. Se lisää hallittavuutta ja näkyvyyttä sekä tuo nykyaikaista kyvykkyyttä ympäristöön.

Cisco Merakin MX-laitteissa on yhdistetty palomuurin ja SD-WAN:in toiminnallisuus. Tästä syystä ei ole tarvetta hankkia verkkoon erillisiä laitteita näiden ominaisuuksien käyttöä varten. Cisco Merakin ympäristö sisältää sekä SD-WAN- että SDN-ominaisuudet. Aryakan tuottaman tutkimuksen mukaan SD-WAN:in ansiosta toimipisteiden WAN-yhteyksien häiriöitä pystyttiin vähentämään jopa 90 %. (Burke 2017, 20). Tutkimuksen tulos tukee sitä teoriaa, että SD-WAN:in toiminnallisuus suojaa toimipisteiden kriittisiä palveluja entistä paremmin. Säännöillä pystytään jo latenssiongelmien sattuessa suojelemaan tärkeiden sovelluksien toimintaa ja varmistamaan automaattinen failover kahden WAN-yhteyden välillä.

5.5 Ympäristön edut ja haitat

Perinteisen verkon valvontaan ja hallintaan verrattuna Cisco Merakin pilvellä hallittavassa verkossa on huomattava määrä etuja:

- Laitteet ovat samaa sukupolvea ja samalta valmistajalta
- Keskitetty hallinta
- Useita ominaisuuksia automatisoitu
- Modernit vianselvityksen työkalut ja valvontamahdollisuudet
- Älykäs analytiikka
- Mahdollisuus suunnitella vakioitu arkkitehtuuri moniin tarpeisiin
- Etukäteen määriteltävissä oleva ympäristö
- Sopii muuttaville toimipisteille

Perinteisen verkon arkkitehtuuria ei kuitenkaan tule sivuuttaa, koska sitä tullaan käyttämään vielä vuosia. Keskitetyn hallinnan ominaisuuksien lisääminen verkkoon on tuonut verkkoympäristöön tarvittavaa hallittavuutta ja älykkyyttä.

Pilvipohjaisella hallinnalla toteutetun verkon edut sivuuttavat paljon perinteisen verkon haittoja, mutta jokaisessa ympäristössä on aina omat haittatekijänsä.

Tietynlainen yksinkertaistaminen voi olla harvinaisemmissa tapauksissa haitaksi, koska näkyvyys yksityiskohtaisempiin asetuksiin on vähäisempi. Merakin TAC:lla on näihin tilanteisiin toki apua saatavilla, mutta oletusarvoisesti tällaisia tilanteita ympäristössä ei pitäisi normaalisti tulla vastaan. Hallintapaneelista ei löytynyt työkalua, jolla voisi tarkistaa tarkemmin SFP-moduulien tiloja tai mitata optisten kuitukaapelien suureita. Toki automaattinen ongelmanhavaitseminen ilmoittaa, kun kytkinportissa on ongelmia. Tässä olisi kuitenkin hyvä olla tarkempi työkalu mittauksia varten, jotta ongelmia pystytään paikantamaan vaivattomammin.

6 Pohdinta

Pilvipohjaisella hallinnalla toteutettu verkko oli tutkittavana kohteena mielenkiintoinen. Cisco Merakin ympäristössä oli käytetty pilveä hyväksi useilla eri tavoilla, joiden avulla voidaan muodostaa erinomainen ympäristö keskisuurille toimipisteille. Kaikenkokoisia toimipisteitä pystytään luomaan tuotteen joustavuuden ansiosta. Konfigurointi on varsin suoraviivaista ja dokumentaation avulla niiden kanssa pääsi hyvin alkuun. Yhtenä suurimpina eduista pilvipohjaisesti hallittavassa ympäristössä oli laitteiden etukäteen konfiguroinnin mahdollisuus. Template-toiminnallisuus ohittaa sen, että laite pitäisi konfiguroida paikan päällä tai etäyhteydellä asennusvaiheessa.

Pilvipohjaisella hallinnalla toteutettuun ympäristöön perehdyttiin laboratorion avulla suunnitelmien mukaisesti. Opinnäytetyön ansiosta saatiin valmiudet työskennellä Cisco Merakilla toteutetussa ympäristössä vianselvityksien ja erilaisten muutoksien kanssa. Hallintapaneelin työkaluja ja ominaisuuksia saatiin käytyä läpi ja testattua, miten ympäristö reagoi vikatilanteisiin. Valvonnan ja vianselvityksen työkalut tekivät vikatilanteiden selvityksestä sujuvampaa. Ympäristössä voidaan toteuttaa korkeaa vikasietoisuutta kahdentamalla laitteet ja SD-WAN:in ansiosta voidaan sovelluskohtaisesti turvata tärkeiden sovellusten toimivuutta.

Pilvipohjaisella hallinnalla toteutettua verkkoa tutkimalla pystyttiin tukemaan väitteitä sen tuomista eduista perinteiseen verkkoon verrattuna. Sekä hallinnan että valvonnan näkökulmasta pilven tuoma keskitetty hallinta on huomattava etu, koska kaikkia verkon laitteita hallitaan keskitetystä paikasta. Samoin valvonta ja hälytysten generoituminen pystytään toteuttamaan yhdestä paikasta. Vianhallinnan kannalta ympäristössä voidaan ohittaa vianselvityksessä vaiheita automaattisen viantunnistuksen avulla. Standardimuutoksien ja massamuutoksien toteutus on ympäristössä entistä vaivattomampaa. Johtopäätöksenä pilvipohjaisesti hallittavan verkon edut tekevät Cisco Merakin ympäristöstä erinomaisen tuotettavan kokonaispalvelun.

Mitä jos Cisco Merakin pilvipohjaiseen hallintapaneeliin ei saakkaan yhteyttä? Yhteys laitteisiin katoaa, mutta sen ei pitäisi horjuttaa laitteiden toimintaa toimipisteillä. Merakin laitteet on suunniteltu toimimaan myös ilman hallintayhteyttä. Laitteita pitäisi operoida paikallisesti tässä tilanteessa. Oletettavasti on epätodennäköistä, että 3 konesalia hajoaa yhdellä kerralla, mutta ihmisen tekemän virheen takia voi tällekin skenaariolle olla mahdollisuus.

Cisco Merakin ympäristöön perehdyttiin työtä tehdessä. Ympäristöntuntemuksesta on hyötyä häiriönhallinnassa, standardimuutoksissa ja tarvittaessa muutoksenhallinnassa. Työstä on varmasti hyötyä tulevaisuudessa ja se tulee helpottamaan työskentelyä pilvipohjaisesti hallittavien ympäristöjen parissa. Raporttia tehdessä tutustuttiin ja saatiin syvennettyä tietoja langattomista tekniikoista. Opinnäytetyöllä saavutettiin omia oppimistavoitteita ja saatiin tehtyä johtopäätöksiä pilvipohjaisesti hallittavan verkon eduista.

Lähteet

Approximating Maximum Clients per Access Point. N.d. Cisco Merakin dokumentaatio. Viitattu 6.5.2019. https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Approximating_Maximum_Clients_per_Access_Point

Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. & Weiss, W. 1998. An Architecture for Differentiated Services. IETF. Viitattu 18.4.2019. https://tools.ietf.org/html/rfc2475

Burke, J. 2017. The CIOs Guide to SD-WAN. Viitattu 16.4.2019. https://info.aryaka.com/rs/477-WNL-836/images/The-CIOs-Guide-to-SD-WAN.pdf

Cloud Managed Smart Cameras. N.d. Cisco Merakin verkkojulkaisu pilvipohjaisesti hallittavista turvallisuuskameroista. Viitattu 29.3.2019. https://meraki.cisco.com/products/security-cameras

Cloud Managed Security & SD-WAN. N.d. Cisco Merakin verkkojulkaisu tietoturvalaitteista. Viitattu 29.3.2019. https://meraki.cisco.com/products/appliances

Cloud Managed Switches. N.d. Cisco Merakin verkkojulkaisu pilvipohjaisesti hallittavista kytkimistä. Viitattu 29.3.2019. https://meraki.cisco.com/products/switches

Cloud Managed Wireless. N.d. Cisco Merakin verkkojulkaisu pilvipohjaisesti hallittavista tukiasemista. Viitattu 29.3.2019. https://meraki.cisco.com/products/wireless

Cloud Management. 2013. Cisco Merakin verkkojulkaisu pilvipohjaisesta hallinnasta. Viitattu 23.3.2019. https://meraki.cisco.com/lib/pdf/meraki_datasheet_cloud_management.pdf

Constine. J. 2012. Cisco Aquires Enterprise Wi-Fi Startup Meraki For 1.2 Billion In Cash. Artikkeli Techcrunch verkkosivustolla. Viitattu 23.3.2019. https://techcrunch.com/2012/11/18/cisco-acquires-enterprise-wi-fi-startup-meraki-for-1-2-billion-in-cash/

Continual Service Improvement. 2016. BMC:n artikkeli ITIL-käytänteistä. Viitattu 28.3.2019. https://www.bmc.com/guides/itil-continual-service-improvement.html

Droms, R. 1997. Dynamic Host Configuration Protocol. IETF. Viitattu 7.4.2019. https://tools.ietf.org/html/rfc2131

DSCP and Precedence Values. 2016. Ciscon opas DSCP ja IP Precedence arvoihin. Viitattu 18.4.2019. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/qos/configuration/guide/n1000v_qos/n1000v_qos_6dscpval.html

History of ITIL. 2018. Artikkeli Itiltraining verkkosivustolla. Viitattu 28.3.2019. https://www.itiltraining.com/blog/2018/11/06/itil-history/

ITIL Service Design. 2016. BMC:n artikkeli ITIL-käytänteistä. Viitattu 28.3.2019. https://www.bmc.com/guides/itil-service-design.html

ITIL Service Operation. 2016. BMC:n artikkeli ITIL-käytänteistä. Viitattu 28.3.2019. https://www.bmc.com/guides/itil-service-operation.html

ITIL Service Strategy. 2016. BMC:n artikkeli ITIL-käytänteistä. Viitattu 28.3.2019. https://www.bmc.com/guides/itil-service-strategy.html

ITIL Service Transition. 2016. BMC:n artikkeli ITIL-käytänteistä. Viitattu 28.3.2019. https://www.bmc.com/guides/itil-service-transition.html

Laadullinen analyysi. 2015. Opas aineiston analyysimenetelmiin Jyväskylän yliopiston Koppa -verkkosivustolla. Viitattu 7.4.2019. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/laadullinen-analyysi

Khorov, E., Kiryanov, A., Lyakhov, A. & Bianchi, G. 2018. A Tutorial on IEEE 802.11ax High Efficiency WLANs. IEEE Communications Surveys & Tutorials, 2. doi: 10.1109/COMST.2018.2871099. Viitattu 29.3.2019. https://janet.finna.fi/, IEEE.

Raza, M. 2018. What is the OSI Model? Explore the 7 Layers of the Open Systems Interconnection Model. Viitattu 28.3.2019. https://www.bmc.com/blogs/osi-model-7-layers/

Rochim, A. & Sari, R. 2016. Performance comparison of IEEE 802.11n and IEEE 802.11ac. International Conference on Computer, Control, Informatics and its Applications (IC3INA), 2. doi: 10.1109/IC3INA.2016.7863023. Viitattu 29.3.2019. https://janet.finna.fi/, IEEE.

Telia Cygate Oy. N.d. Yrityksen esittelysivu. Viitattu 23.3.2019. https://www.teliacygate.fi/fi/lyhyesti

Watts, S. 2018. ITIL V4: Intro to the 2019 ITIL Update. Viitattu 28.3.2019. https://www.bmc.com/blogs/itil-v4/

What is cloud computing. N.d. Microsoftin artikkeli pilvilaskennasta. Viitattu 31.3.2019. https://azure.microsoft.com/en-ca/overview/what-is-cloud-computing/

What is IaaS. N.d. Microsoftin artikkeli IaaS:sta. Viitattu 31.3.2019. https://azure.microsoft.com/en-ca/overview/what-is-iaas/

What is PaaS. N.d. Microsoftin artikkeli PaaS:sta. Viitattu 31.3.2019. https://azure.microsoft.com/en-ca/overview/what-is-paas/

What is SaaS. N.d. Microsoftin artikkeli SaaS:sta. Viitattu 31.3.2019. https://azure.microsoft.com/en-ca/overview/what-is-saas/