Haaga-Helia
ammattikorkeakoulu Oy

Oivaltava verkko

Stephan Rühlmann

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2020

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

14.1.2020

Tekijä(t)
Stephan Rühlmann

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Oivaltava verkko

Sivu- ja liitesivumäärä
37 + 0

Opinnäytetyön otsikko englanniksi
Intent Based Network

Tämän opinnäytetyön tarkoituksena oli tutkia, mitä oivaltavalla verkolla tarkoitetaan ja mitä ohjelmisto-ohjatut verkot yleisesti ovat. Tutkimus perustui kirjallisiin lähteisiin ja keskittyy lopuksi Ciscon Software Defined Access-palveluun.

Tutkimuskysymyksinä olivat, miksi teknologia on olemassa, mitä ongelmaa se ratkaisee ja mitkä ovat sen toiminnan reunaehdot tai rajoitteet.

Teoria-osuudessa käydään aluksi lyhyesti läpi tietoverkon perusteita ja laitteita yleiskuvan luomiseksi. Seuraavaksi käsitellään ohjelmisto-ohjattua verkkoa yleisesti, jonka jälkeen siirrytään tutkimaan Ciscon ratkaisua.

Yhteenveto-osiossa käsitellään kirjallisten lähteiden perusteella kertaalleen hyötyjä ja pohdintaosiossa pyritään hakemaan käytännön todellisuutta vertailukohteeksi.

Lopuksi todetaan, että teknologia on edelleen uutta ja ohjelmallisena tuotteena kehittyy myös edelleen. Oivaltavan verkon hyödyt ovat ilmeiset ja tavoiteltavat, mutta se ei sovellu kaikille.

Asiasanat
SDN, Software-Defined Networking, IBN, Intent Based Networking, oivaltava verkko, aiepohjainen verkko, Cisco SDA

Sisällys

1 Johdanto

Tietoliikenteessä ja verkkoteknologiassa tapahtuu aika ajoin teknologista edistymistä, joko niin, että parannellaan olemassa olevaa tai tuodaan markkinoille jotain täysin uutta. Digitalisaatio tuo mukanaan uusia haasteita yrityksille, esimerkiksi verkkoteknologia saattaa olla erittäin hajautunutta, laitekanta ei ole ajantasaista tai käytettävät ratkaisut eivät täysin tue toisiaan. Ongelmana ei yleensäkään ole se, ettei teknologiasta tiedettäisi, vaan enemmänkin se, että saatavilla ei ole riittävää tutkimustietoa ja kerääntynyttä kokemustietoa omasta asiantuntijaverkostosta.

Tässä opinnäytetyössä tarkastellaan kohtuullisen uutta teknologiaa, oivaltavaa verkkoa. Taustalla vaikutti ajatus teknologian ja sen tuomien välineiden avulla saatavasta lisähyödystä organisaatiolle. Opinnäytetyö keskittyy teknologian taustaan, sen toimintaan sekä pyrkii analysoimaan siitä saatavat hyödyt, mikäli sellaisia on saatavilla.

Opinnäytetyön alkuvaiheessa asetettiin kysymykset, joita vasten teknologiaa lähdettiin tutkimaan: miksi teknologia on olemassa, mitä ongelmaa se ratkaisee ja mitkä ovat sen toiminnan reunaehdot tai rajoitteet.

Nykyisissä tietoverkoissa saadaan kulumaan kohtuuttoman paljon aikaa laitteiden ja yhteyksien konfiguraatioihin sekä ongelmanselvitykseen vikatilanteissa. Oivaltavan verkon arvolupaus on vähentää aikaa, joka kuluu manuaaliseen työhön sekä helpottaa tietoverkon ylläpitoa ja lyhentää vikojen korjausaikoja.

Teknologian hyödyt ovat nähtävissä, mutta sen käyttöönotto kirjoittamisen hetkellä tulee olemaan haasteellista, vie paljon aikaa ja vaatii paljon resursseja, sekä ihmistyötä että rahaa.

2 Käsitteet

Luetellaan yleisimmät lyhenteet ja niiden merkitys esiintymisjärjestyksessä.

LAN	Local Area Network, lähiverkko
WLAN	Wireless Local Area Network, langaton lähiverkko
WAN	Wide Area Network, laajaverkko
MAC	Media Access Control, laitteen yksilöllinen tunnus
Token Ring	rengasverkko, jossa lähetys perustuu valtuutukseen
Ethernet	yleisesti käytössä oleva pakettipohjainen lähiverkkoratkaisu
SD-WAN	Software Defined networking in Wide Area Network, mahdollistaa ohjelmistopohjaisen WAN-liitynnän, jossa voidaan käyttää operaattoririippumattomia yhteyksiä
MPLS	Multiprotocol Label Switching, reititystekniikka tietoverkoissa
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, tietoliikenteen siirtotien varausmenetelmä
Kytkin	Switch, moniporttinen laite, joka yhdistää paikallisverkon osia toisiinsa
Reititin	Router, laite, joka yhdistää eri tietoverkkoja toisiinsa
Palomuuri	Firewall, laite tai ohjelmisto, joka suojaa tietoverkkoa ulkoa tulevilta uhkilta
Protokolla	määrittää miten laitteet tai järjestelmät välittävät tietoa keskenään
OSI-malli	Open Systems Interconnection Reference Model, kuvaa tiedonsiirtoprotokollat jakamalla ne seitsemään kerrokseen
TCP/IP	Transmission Control Protocol/Internet Protocol, protokollapino, jota tarvitaan Internet-liikennöintiin
ELK	Elasticsearch, Logstash, Kibana, www.elastic.co
DHCP	Dynamic Host Configuration Protocol, protokolla joka jakaa verkon laitteille IP-osoitteita
DNS	Domain Name System, nimipalvelujärjestelmä joka muuttaa verkossa käytettävät nimet IP-osoitteiksi
AD	Active Directory, Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu
SDN	Software Defined Network, ohjelmisto-ohjattu verkko
OpenFlow	ohjelmoitava verkkorajapinta
API	Application Programming Interface, ohjelmointirajapinta
Control Plane	hallintakerros
Data Plane	tiedonvälityskerros
Cisco SDA	Software Defined Access, Ciscon oivaltava verkko-teknologia

Overlay	päällyskerros
Underlay	aluskerros
QoS	Quality of Service, tietoliikenteen priorisointi ja luokittelu
WLC	Wireless LAN Controller, laite, johon langattoman verkon tukiasemat ovat yhteydessä
VXLAN	Virtual Extensible LAN, virtualisointiteknologia, joka pyrkii ratkaisemaan isojen verkkojen ongelmia
GPO	Group Policy Option, SDA-teknologian ryhmäsääntö
SGT	Scalable Group Tag, SDA-teknologiassa käytettävä tunniste
VN	Virtual Network, virtuaalinen lähiverkko, erityisesti SDA-toteutuksissa käytettävä teknologia
VLAN	Virtual LAN, virtuaalinen lähiverkko, perinteisissä verkoissa käytettävä teknologia
ISE	Cisco Identity Services Engine, laite- ja pääsynhallintajärjestelmä
SNMP	Simple Network Management Protocol, verkkojen hallinnassa käytettävä tietoliikenneprotokolla
Netflow	verkkoprotokolla, joka kerää IP-liikenteestä tietoa
Syslog	tapa, jolla verkon laitteet lähettävät lokitietoa keskitetylle palvelimelle

3 Tietoverkot

Tietokoneita käytetään tänä päivänä useisiin eri tarkoituksiin; selataan Internettiä, luetaan ja kirjoitetaan sähköposteja, käytetään sähköisiä kalentereita, jaetaan tiedostoja sekä monia muita vastaavia käyttötapoja. Kaikissa näissä on yhteistä se, että pystyäkseen tähän, on tietokoneen päästävä erilaisiin tietoverkkoihin eri paikoissa, jopa eri maahan tai maanosaan.

Jotta voidaan puhua tietoverkosta, tiettyjen kriteerien täytyy täyttyä. Tietoverkossa täytyy olla vähintään:

- kaksi tietokonetta
- jaettava resurssi, esimerkiksi kansio tai tulostin
- välitysmekanismi, kuten kaapeli tai langaton tukiasema
- sopimus kuinka tietoa välitetään eli millä protokollalla koneet keskustelevat keskenään, esimerkkinä TCP/IP

(McMillan 2012, s. 5)

Tietoverkot saattavat koostua käsitteellisesti esimerkiksi paikallisesta lähiverkosta, langattomasta lähiverkosta tai laajaverkosta.

Seuraavissa kappaleissa kuvataan lyhyesti tietoverkkoon liittyvät tärkeimmät elementit, jotka on hyvä tietää mitä pidemmälle oivaltavan verkon tutkimisessa mennään.

3.1 Lähiverkko

Yleisimmin lähiverkko määritellään nopeaksi dataverkoksi, joka kattaa paikallisesti pienen alueen. Alue voi olla toimisto rakennuksessa, koko toimistorakennus tai useampi rakennus pienellä alueella, hyvänä esimerkkinä voisi käyttää joko yritys- tai koulukampusta.

Tänä päivänä tietoverkoissa käytetään tekniikkaa, jonka yleisimmin tunnemme nimellä Ethernet. Muita teknologioita, kuten Token Ring, on vielä käytössä, mutta ne ovat käytännössä hävinneet kilpailun markkinoilla Ethernetille (McMillan 2012, s. 9).

3.2 Langaton lähiverkko

Langaton lähiverkko laajentaa fyysisiä, kaapeloituja verkkoja käyttämällä radiotietä. Langattomassa yhteydessä kaapeloidaan ainoastaan kytkimen ja langattoman tukiaseman väli. Mikäli kytkin ja tukiasema tukevat PoE-protokollaa, tukiasemaan ei tarvita erillistä

virtalähdettä, sillä PoE-toiminnallisuus kuljettaa tarvittavan sähkön Ethernet-kaapelissa (Beasley & Nilkaew 2016).

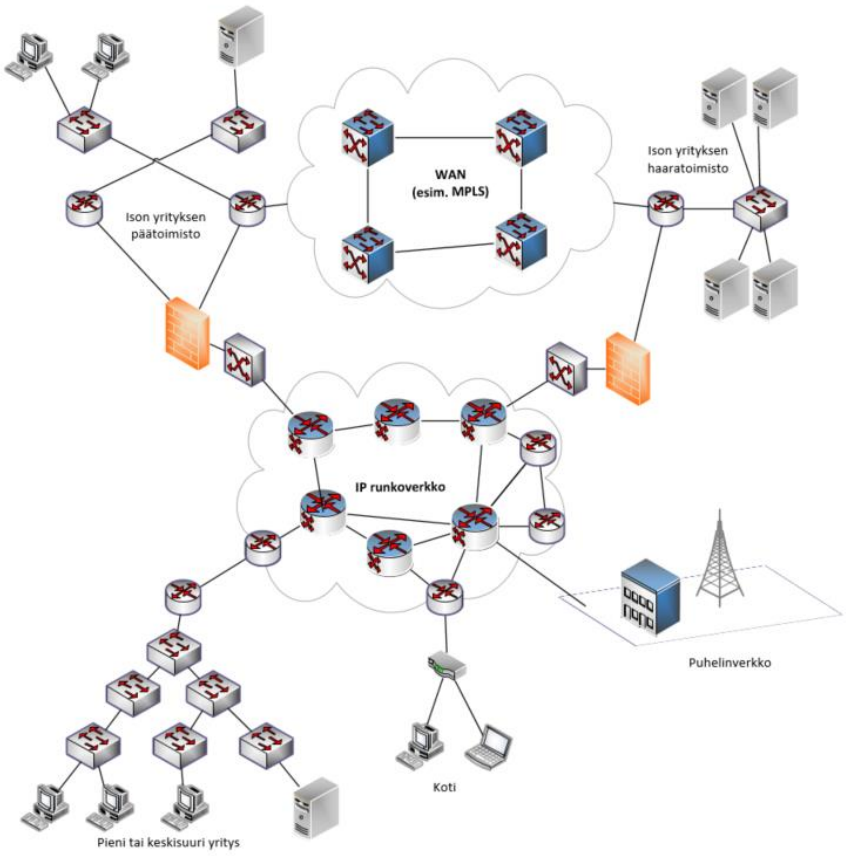
Useimmiten nykyaikaisissa yrityksissä lähiverkko pyritään pääsääntöisesti toteuttamaan langattomasti ja siten vähentämään kaapelointikustannuksia sekä Ethernet- että sähkökaapeloinnin osalta.

Hyvän verkon toteuttaminen vaatii tarkan suunnitelman, radiomittaukset sekä riittävän tukiasemakattavuuden päätelaitteille, olivat ne sitten tietokoneita tai mobiililaitteita.

3.3 Laajaverkko

Laaja tietoverkko käsittää alueellisesti isoja maatieteellisiä alueita, pääsääntöisesti paikkakuntien välillä, maiden välillä tai jopa maaosien välillä. Laajaverkot yhdistävät lähiverkkoja toisiinsa ja niitä yhdistävän tekniikan toteuttaa pääsääntöisesti tietoliikenne- tai teleoperaattori (Jaakohuhta 2005, s. 5).

Laajaverkosta on myös nykyisin saatavilla ratkaisu, josta käytetään nimitystä SD-WAN, jolla yritykset voivat kytkeä esimerkiksi toimistoja toisiinsa käyttämällä operaattoririippumattomia Internet-liittymiä. Sillä voidaan korvata useimmiten käytössä olevat kalliit yksityiset, operaattoririippuvaiset teknologiat kuten MPLS. Haittapuolena on, että ongelmatapauksissa ei saada samanlaisia korjausvasteaikoja kuin operaattorin suoraan tarjoamassa verkossa.



Kuva 1. Globaali verkko-arkkitehtuuriesimerkki

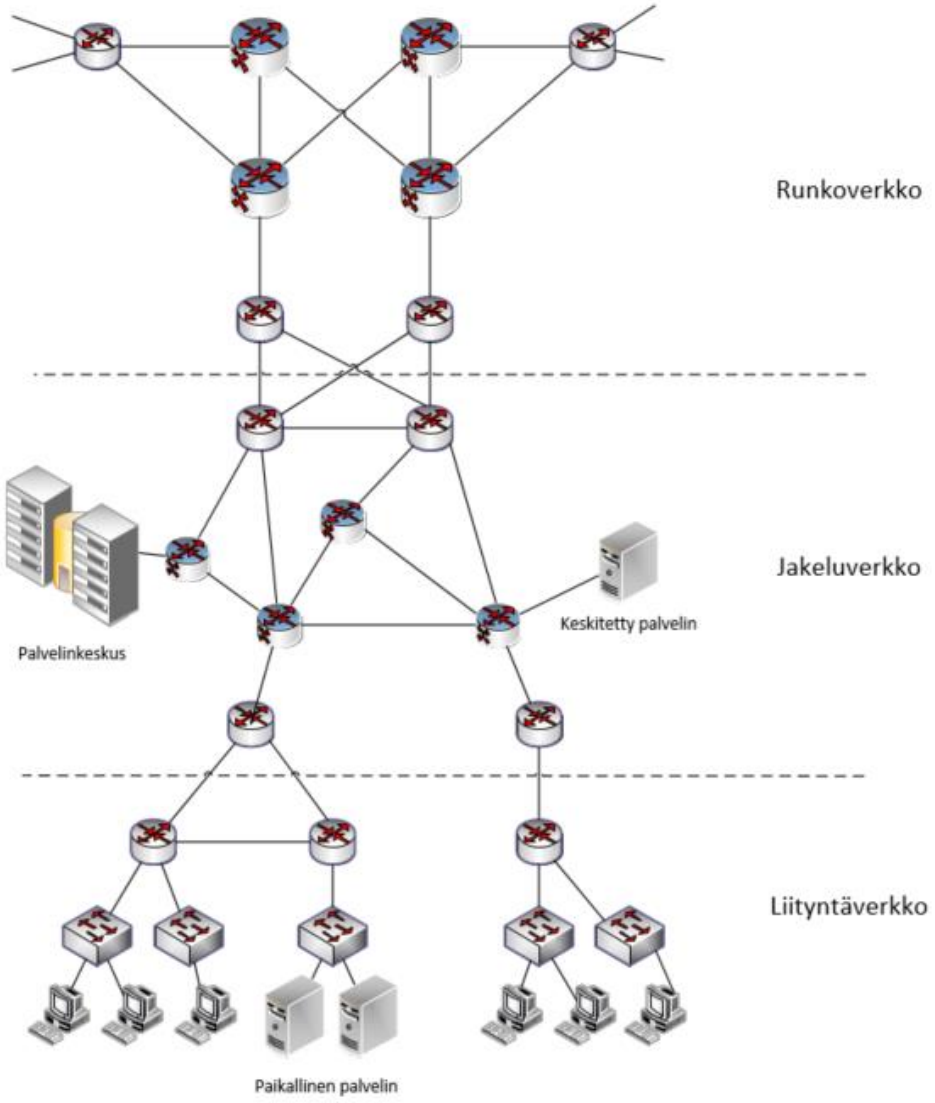
Kuvan 1. keskellä mainittu IP-runkoverkko voi kuvata osaltaan vaikka Internettiä tai yrityksen suljettua IP-verkkoa. Ydinverkossa on suorituskykyisiä reitittimiä, jotka ovat yleensä kiinni toisissaan valokuitukaapeleilla suurten liikennöintivaatimusten takia (Stallings 2016).

Ydinverkon reunalla on ns. reunakytkimet, joiden tehtävänä on kytkeä ulkoiset verkot ja käyttäjän käyttämä verkko toisiinsa. Reitittimestä voidaan käyttää myös nimeä Provider Edge, PE-reititin, jolloin vastaavasti käyttäjän pään verkossa on Customer Edge eli CE-reititin (Stallings 2016).

Kuvan 1. yläosa kuvaa esimerkinomaisesti isompaa yritysverkkoa, joissa toimistot on kytketty suljetun laajaverkon avulla toisiinsa. Toimistoilla on myös yhteys runkoverkkoon keskellä, josta ne voivat myös kommunikoida takaisin toiseen verkkoon, mikäli näin halutaisiin. Ydinverkon ja yritysverkon välissä on yleensä lisäksi palomuurilaite, jolla rajoitetaan ei-toivottua liikennettä sisäverkkoon.

Kuvan 1. alaosassa kuvataan tavallista pienen tai keskisuuren yrityksen Ethernet-verkkoa. Tyypillisesti näillä yhteys Internettiin rakennettaisiin joko kuitu- tai kupariliittymällä tai jopa langattomalla 4G-ratkaisulla.

Hyvän tavan mukainen tietoverkkojen suunnittelu perustuu kuvan 2. tyyppiseen kolmitasoiseen hierarkkiseen malliin (Cisco 2016).



Kuva 2. Hierarkkinen verkkomalli

Lähinnä käyttäjää on liityntäverkko, joka yhdistää käyttäjän paikalliseen lähiverkkoon, jossa sijaitsevat myös käyttäjän käyttämät jaetut verkkolaitteet kuten tulostimet tai monitoimikoneet ja joissain tapauksissa paikalliset palvelimet, kuten tulostuspalvelimet. Liityntäverkko kattaa sekä langallisen että langattoman verkon (Cisco 2016).

Keskimmäisenä on jakeluverkko, joka yhdistää liityntäverkon ja runkoverkon toisiinsa. Isossa, ja miksei pienimmässäkin organisaatiossa, jakeluverkko sisältää organisaation yhteiset palvelut, jotka pääsääntöisesti ovat sovellus-, tietokanta- tai tiedostopalvelimia.

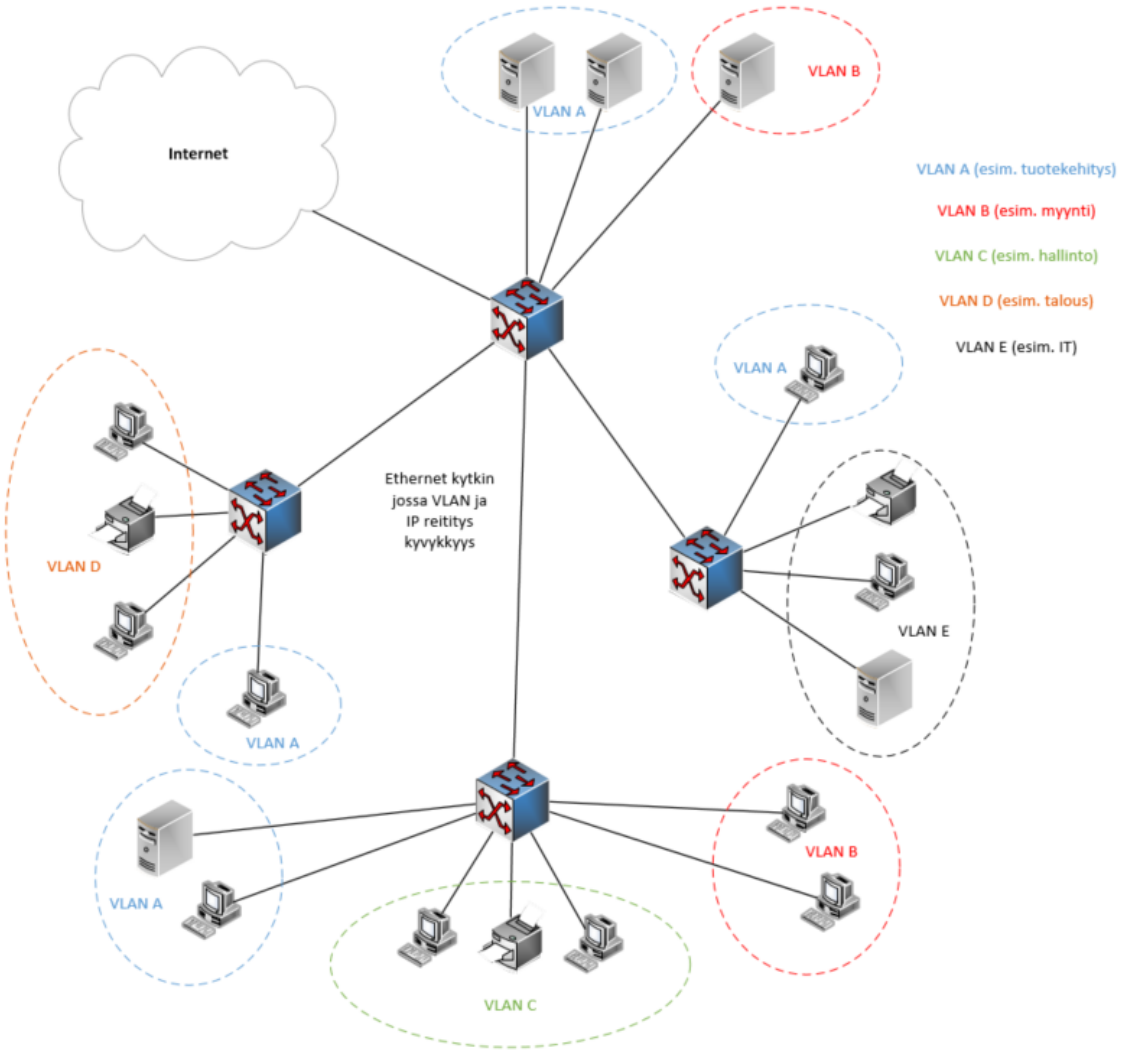
Loppukäyttäjän todennuksen kannalta oleelliset palvelut sijaitsevat myös tässä verkossa (Cisco 2016).

Runkoverkko yhdistää ison yrityksen toimipaikat toisiinsa ja tarjoaa siitä eteenpäin yhteyden esimerkiksi Internettiin. Runkoverkkoon saatetaan sijoittaa myös organisaation ulospäin tarjoamat palvelut, kuten www-palvelut, VPN-palvelut loppukäyttäjille tai kolmansien osapuolien käyttöön rakennetut VPN-tunnelit (Cisco 2016).

3.4 Virtuaaliverkoista

Virtuaalilähiverkko eli VLAN on tekniikka, jota tänä päivänä käytetään fyysisen tietoliikenneverkon jakamiseen loogisiin osiin sen sijaan että verkkoa tarvitsisi jakaa osiin fyysisillä laitteilla kuten kytkimillä tai reitittimillä. Näin voidaan esimerkiksi yhdistää yrityksen tietyt toiminnot yhdeksi loogiseksi kokonaisuudeksi useiden eri toimistojen välillä riippumatta niiden maantieteellisestä sijainnista. VLAN löytyy IEEE:n 802.1Q-standardista, jossa määritellään tunnisteet eli VLAN-tagit, joilla verkot voidaan laitteissa tunnistaa (Stallings 2016).

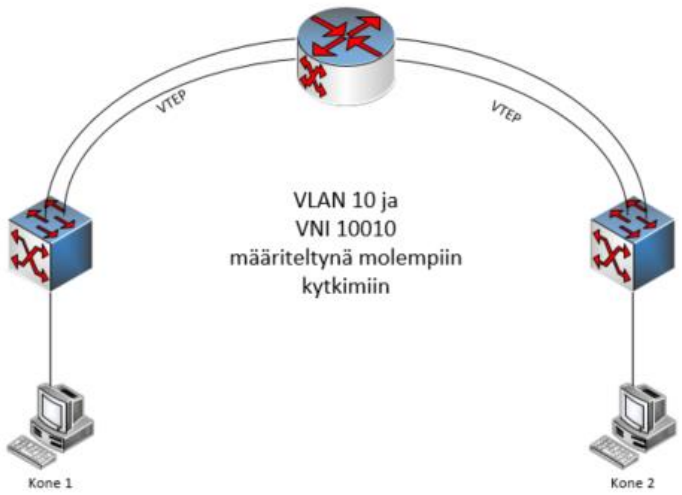
Lähtökohtaisesti kaikki kytkimet eivät tue VLAN mahdollisuutta, mutta jo hiukan kalleimmissa malleissa tuki jo löytyy. Kytkimen hankinnassa on myös hyvä kiinnittää huomiota siihen, että se tukisi edellä mainittua IEEE 802.1Q-standardia, jolloin voidaan välttää tilanne, jossa laitteen valmistajalla on oma standardinsa käytössä ja se ei ole yhteensopiva muiden verkkolaitteiden kanssa tai että ajaudutaan toimittajariippuvaiseen tilaan.



Kuva 3. Esimerkki VLAN-verkosta

Kuvassa 3 on esimerkkinä yrityksen VLAN-verkko, jossa verkon segmentointia on kuvattu eri värein ja käyttämällä yksiköiden nimiä havainnollistamaan miten VLAN käytännössä toimii.

VXLAN on verkon virtualisointiteknologia, jonka tarkoituksena on ratkaista isojen, laajojen tai määrällisesti suurien verkkojen ongelmia. Parhaiten se vastaa verkkojen määrälliseen ongelmaan, mikä taas vastaavasti rajoittaa VLAN-teknologian käyttöä. VXLAN on tyypillisesti käytössä pilviratkaisuissa. Kuvassa 4 VXLAN tunneloi Layer-2 liikenteen käyttäen UDP-protokollaa. Määritetyt kytkinten portit toimivat terminointipisteitä, joissa tunneli puretaan ja niitä kutsutaan nimellä VTEP (Goralski 2017).



Kuva 4. VXLAN esimerkki

Oivaltavan verkon ratkaisussa VXLANia käytetään virtuaalisen päällyskerroksen tekemiseen ja koska se tukee sekä Layer-2 että Layer-3:sta, se mahdollistaa operoinnin minkä tahansa IP-verkon päällä (Cisco 2018).

3.5 Ethernet

Ethernet on tällä hetkellä yleisin käytössä oleva pakettipohjainen lähiverkkotekniikka. Ethernet perustuu CSMA/CD-tekniikkaan (Carrier Sense Multiple Access with Collision Detection), jossa päätelaite kuuntelee ensin verkkoa (CS) ja jos verkossa ei havaita liikennettä voidaan sanoma lähettää (MA). Tämä tarkoittaa käytännössä sitä, että vain yksi päätelaite voi lähettää sanomaa kerrallaan. Mikäli käy niin, että kaksi päätelaitetta lähettäisi samaan aikaan sanoman, tapahtuu törmäys. Törmäyksen havainnut (CD) päätelaite vahvistaa törmäyksen ja seuraavaksi nämä kaksi päätelaitetta arpovat keskenään uudet lähetysajat (Jaakohuhta 2005, s. 90).

Lähetystarpeet kasvavat jatkuvasti ja verkoissa syntyy näin ruuhkaa. Yksi tapa välttää ruuhkia, on nostaa nopeutta. Ethernet tukee tällä hetkellä 10M, 100M, 1G ja 10G nopeuksia. 10M nopeuden kohdalla siirryttiin käyttämään keskittimien sijaan kytkimiä. Lisäksi kehitys 100M nopeuden kohdalla on tuonut mukanaan kaksisuuntaisen tiedonsiirtomahdollisuuden, vaikka kaapelointivaatimuksen siitä eteenpäin ovatkin muuttuneet siten, että 100M verkon minimivaatimus on kategorian 5 parikaapeli.

3.6 TCP/IP ja OSI

Jotta tietoverkossa voitaisiin liikennöidä, tarvitaan jokin standardoitu tapa välittää tietoa laitteelta toiselle. OSI:a suunniteltiin alan standardiksi koska siihen aikaan 1980-luvulla oli käytössä useita ei-yhteensopivia ja osin valmistajakohtaisia ratkaisuja.

Historiasyistä TCP/IP oli jo vakiinnuttanut asemansa ja OSI-mallin kehitys oli liian myöhässä ja OSI-malli on käytännössä tänä päivänä enemmän referenssimalli kuin varsinainen käytännön sovellus. Huomioitavaa kuitenkin on, että verkkoteknologiasta puhuttaessa, viitataan nimenomaan OSI-mallin kerroksiin, esimerkiksi kun viitataan vaikka kytkimiin, jolloin puhutaan Layer-2 tai Layer-3 yhteensopivuudesta tai tuesta.

TCP/IP on usean Internet-liikennöinnissä käytettävän tietoliikenneprotokollan yhdistelmä eli pino. Nimi tulee kahdesta pääprotokollasta TCP ja IP.

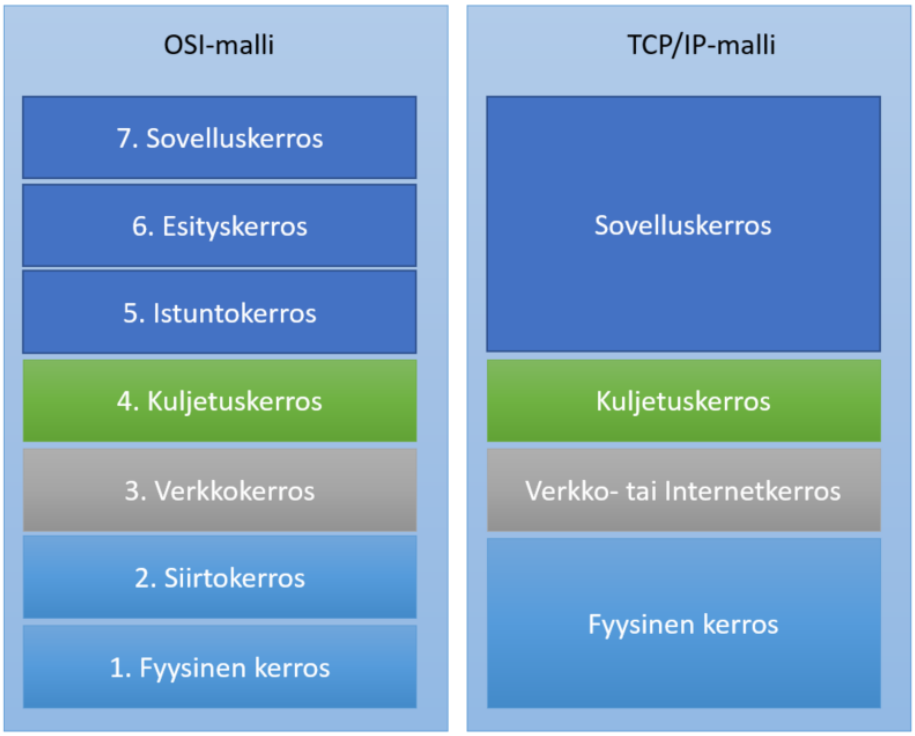
IP-protokolla antaa päätelaitteille tunnistettavan osoitteen ja vastaa pakettien reitittämisestä verkossa. Sen päällä voidaan ajaa monia muita protokollia mutta yleisin näistä on TCP. TCP vastaa kahden päätelaitteen välisestä tiedonsiirrosta, pakettien järjestämisestä sekä mikäli paketteja hukkuu matkalla, niiden uudelleenlähetyksestä (Rintala 2001).

OSI-mallin kehittämisestä on seurannut kuitenkin se, että kerrosajattelua on alettu soveltamaan myös muualla. Kuten aikaisemmin mainittiin, OSI-malliin viitataan alan keskusteluissa edelleen, vaikka varsinaista käytännön toteutusta ei olisikaan tehty mallin mukaan. Näin ollen voidaan ajatella, että tietoliikenteestä puhuttaessa on hyvä ymmärtää OSI-malli, koska sen kautta voidaan ymmärtää muita pinomalleja.

Pinomallin idea on se, että jokainen kerros on yhteydessä seuraavaan kerrokseen ja tietoverkon laitteen käyttävät alemman kerroksen palveluja hyväkseen siirtäessään tietoa. Kuvassa 5 on hahmoteltu OSI-mallin kerrokset sekä mitä varten ne yleisesti ovat käytössä, avaamatta tässä kohden kerroksia kuitenkaan tarkemmin.

Kuva 5. OSI-malli

Myös TCP/IP pino voidaan jakaa kerroksiin ja samalla verrata sitä OSI-malliin (kuva 6).



Kuva 6. OSI-malli vs. TCP/IP-malli

3.7 Reititin

Reititin toimii OSI-mallin kolmannessa kerroksessa eli se toimii verkkokerroksessa ja välittää vastaanottajan IP-osoitteen perusteella paketteja. Reitittimen tehtävänä on yhdistää tietoverkkoja toisiinsa. Reitittimen yhtenä tehtävänä on myös rajata ryhmälähetyksiä.

3.8 Kytkin

Kytkin puolestaan toimii OSI-mallin toisessa kerroksessa, ammattikielessä viitataankin usein Layer-2-kytkimiin. Kytkin välittää tietoa MAC-tasolla. Verkossa jokaisella laitteella, jolla on verkkokortti, on myös MAC-osoite. Kytkimen toimintamallin voisi lyhyesti kuvata siten, että se tallentaa saamansa kehyksen, jota myös siirtokehykseksi kutsutaan, purkaa sen, tarkistaa vastaanottajan osoitteen ja välittää sen eteenpäin.

Kytkin muodostaa oman segmenttinsä kaikkien laitteiden kanssa, joita siihen on liitetty. Kytkin muodostaa myös isommassa verkossa yhteyden toisiin kytkimiin ja tarjoaa yhteyden reitittimeen ja muihin laitteisiin WAN-yhteyttä varten (Beasley & Nilkaew 2016).

3.9 Palomuuri

Palomuuri on laite tai järjestelmä, jonka tehtävänä on estää asiaton pääsy verkosta toiseen, varsinkin Internetistä lähiverkkoon.

Reitittimissäkin voi olla sisäänrakennettu palomuurio minaisuus, mutta yleisesti ne eivät ole toiminnallisesti hyvällä tai riittävällä tasolla suojaamaan yritysverkkoja, kotioloissa ne toki toimivat ja niissä niitä yleisesti käytetään.

Palomuuri toimii siten, että se suodattaa liikennettä siihen syötettyjen sääntöjen avulla. Säännöt määräävät sallitaanko liikenne vai ei. Palomuurin tyypistä tai mallista riippuen voidaan määritellä lisäsääntöjä esimerkiksi hälytysten suhteen, kun havaitaan epäilyttävää liikennettä (Beasley & Nilkaew 2016).

3.10 Muut palvelut tietoverkoissa (DHCP, DNS, AD)

DHCP:n tehtävä on jakaa IP-osoitteita verkkoon liittyville laitteille. Erilliselle DHCP-palvelimelle määritellään IP-osoiteavaruus ja liittyessään verkkoon, uusi laite pyytää palvelimelta IP-osoitteen. Yleensä DHCP-palvelin jakaa laitteelle myös oletusyhdyskäytävän, nimipalvelimen tai nimipalvelimien ja aikapalvelimen IP-osoitteen (Beasley & Nilkaew 2016).

DNS on palvelu, joka muuntaa verkkotunnuksia IP-osoitteiksi. Tietoverkon laitteet tarvitsevat IP-osoitetta, mutta meille ihmisille on helpompaa puhua palvelusta ns.google.com, kuin yrittää muistaa sen IP-osoite 216.239.32.10 (Beasley & Nilkaew 2016).

Active Directory eli AD on Windows-toimialueen tietokanta, joka sisältää erilaisia objekteja. Objektit voivat olla käyttäjiä, tietokoneita, ryhmiä, organisaatioita ja toimialueita (domain). Se mahdollistaa näin keskitetyn resurssien jakamisen, kun ne voidaan kuvata ja nimetä järkevällä tavalla. AD:ta tuotteena on helppo ylläpitää ja se skaalautuu hyvin ylöspäin (Hudson & Fullerton 2001).

3.11 Tietoverkon monitoroinnista

Verkon monitorointi kuuluu tärkeänä osana verkon hallintaan. Monitoroinnin tarkoitus on valvoa verkon laitteita, havaita automaattisesti virheitä tai virhetilanteita ja lähettää niistä tietoa verkon valvojalle. Valvottavat asiat ovat yleisesti: vastaako laite ja missä ajassa, laitteen käytettävyys sekä kauanko laite on ollut päällä. Lisäksi valvotaan usein verkon liikennettä liittymäkohtaisesti. Verkon monitorointiin käytetään ohjelmallisia apuvälineitä tai komentokehotetta, josta ajetaan suoraan komentoja verkkolaitteelle. Seuraavaksi käydään lyhyesti läpi mitä yleisesti käytetään verkon tai laitteiden monitoroinnissa.

Simple Network Management Protocol eli SNMP lienee yleisin tapa monitoroida verkkolaitteita, koska pääsääntöisesti jokainen markkinoilla oleva verkkolaite sisältää ns. SNMP-agentin, joka osaa välittää tietoa verkkoon. Agentit voivat perustua joko johonkin standardiin tai ne voivat olla valmistajan omia.

SNMP-agentti tallentaa sekä laitteesta että sen tapahtumista tietoa paikalliseen tietokantaan ja osaa tarvittaessa välittää hälytyksiä eteenpäin verkon monitorointijärjestelmälle. SNMP on kuitenkin melko yksinkertainen, se osaa välittää tietoa onko esimerkiksi reititin tai kytkin toiminnassa, kauanko se on toiminut yhtäjaksoisesti, mikä sen IP-osoite ja nimi on sekä paikkatiedon tai yhteyshenkilön tiedon, mikäli se on laitteeseen syötetty. Lisäksi se kertoo mikä on laitteen liittymien (eng. interface) tila (Beasley & Nilkaew, 2016).

Netflow on puolestaan alun perin Ciscon kehittämä verkkoprotokolla, jonka tarkoitus on kerätä IP-liikenteestä tietoa ja monitoroida tietoverkon liikennettä. Netflow’n tuottamasta tiedosta saadaan selville mitä käyttäjiä verkossa on, mitä sovelluksia he käyttävät sekä sovellusten lataus-ja vasteaikoja. Netflow’lla saadaan myös hyvä käsitys kaistan käytöstä ja WAN-liittymän liikenteestä. Osin samantyyppistä tietoa saadaan myös palomuureista, mutta Netflow tarjoaa enemmän reaaliaikaista tietoa, kun palomuurit yleensä tarjoavat pääsääntöisesti vain esimerkiksi 5 minuutin keskiarvolla tietoa ja ainoastaan vain siitä liikenteestä mikä menee sen lävitse (Collins 2014).

Netflow’n käyttöönotto vaatii käyttöön jonkin tietoverkonhallintaohjelmiston, joka kerää ja analysoi laitteilta saamansa tiedon. Tällaisia ohjelmistoja markkinoilla tarjoavat esimerkiksi Solarwinds, PRTG, Nagios ja Zabbix.

Syslog on tapa, jolla verkon laitteet lähettävät lokitietoa keskitetylle palvelimelle. Syslogissa ei voida suorittaa kyselyä laitteelle kuten SNMP:ssä, vaan laite lähettää tietoa palvelimelle, kun jokin tapahtuma sattuu. Useimmat tietoverkonhallintasovellukset osaavat toimia tiedon jäsentelijöinä, mutta ongelmana on usein se, että syslogissa ei ole määrättyä tapaa kuinka tietoa lähetetään, joten se voi olla äärimmäisen sekavassa muodossa ja vaikea visualisoida järkevästi. Edellisessä kappaleessa mainitut sovellukset osaavat lukea syslog-tietoa ja näille kilpailijaksi on lisäksi markkinoille tullut hyvänä open source-yhteisön tuotteena ELK.

4 Software Defined Network (SDN)

Tässä opinnäytetyössä käytetään otsikkona termiä oivaltava verkko. Yhtä hyvin voitaisiin käyttää nimitystä aiepohjainen verkko tai ohjelmisto-ohjattu verkko. Oivaltava verkko ei ole kuitenkaan vain pelkkä SDN, vaan se on enemmän. SDN vastaa enemmän kysymykseen miten tehdään, tuoden teknologialla ratkaisun verkkojen hallintaan ja operointiin. Oivaltava verkko puolestaan vastaa kysymykseen mitä tehdään, ottamatta niin paljon kantaa teknologiaan. Oivaltavan verkon konseptiin on pakattu kokonaisia tuoteperheitä tuottamaan asiakkaan tarvitsemaa palvelua. Opinnäytetyön nimi sopii siten nykytilanteeseen paremmin sekä siihen mihin uusi teknologia tuo vastauksia tai ratkaisuja.

4.1 SDN – mitä se on?

Konseptina ja ajatuksena SDN ei ole uusi asia, sillä siitä on ollut puhetta jo 90-luvulla. SDN kehitys lähti varsinaisesti liikkeelle suuremmalla voimalla vuonna 2011 kun usean globaalin toimijan yhteenliittymä ja voittoa tavoittelematon Open Networking Foundation aloitti toimintansa verkkoinfrastruktuurin muutoksen edistämiseksi ja liiketoimintamallien kehittämiseksi.

Heidän ansiokseen voidaan myös laskea OpenFlow-verkkoprotokolla, joka toimii ohjelmointirajapintana kontrollerin ja verkkolaitteiden välillä ja jota tukee suurimmat verkkolaitevalmistajat kuten HP, Cisco, Juniper ja Google. Ohjelmoitavana verkkoprotokollana OpenFlow auttaa hallitsemaan ja ohjaamaan verkkoliikennettä reitittimissä ja kytkimissä riippumatta siitä kuka laitteen on valmistanut (Coker & Azodolmolky 2017).

SDN on yksinkertaisimmillaan lähestymistapa siihen, kuinka suunnitellaan, rakennetaan ja ylläpidetään suuria ja usein monimutkaisia verkkoja. Sen toiminta perustuu ohjelmoituun päätöksentekoon reitittimissä ja kytkimissä. Toimiakseen se vaatii taustalle keskitetyn palvelimen, kontrollerin. Erona perinteiseen verkon ylläpitoon on se, että yksittäisiä laitteita ei enää tarvitse konfiguroida käsin, vaan muutokset voidaan välittää tarvittaessa kaikille verkon laitteille yhdellä kertaa (Stallings 2016, s. 67).

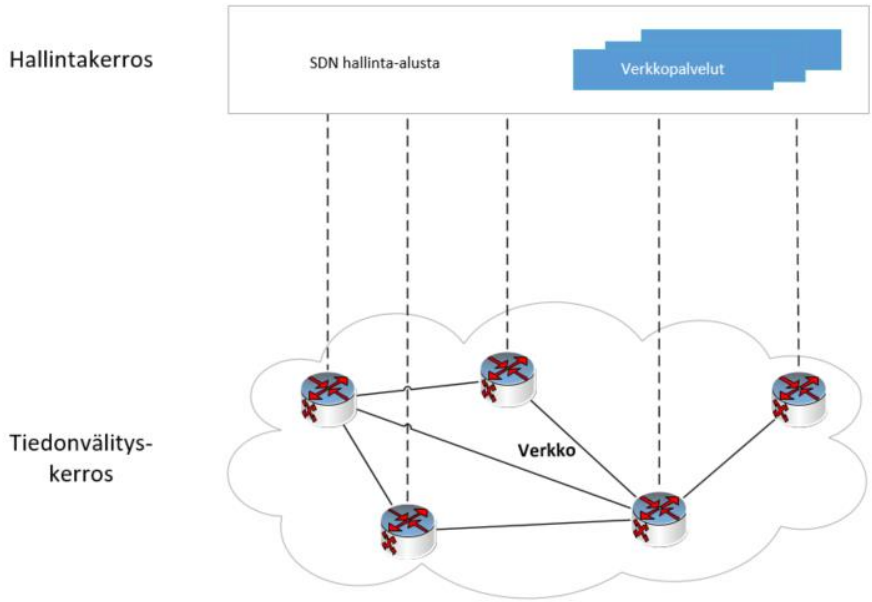
Modernin verkon rakentaminen vaatii ohjelmisto-ohjattua verkkoa. Syyt löytyvät yksinkertaisesti muista ympärillä kehittyvistä tekniikoista tai trendeistä.
Big Data, pilvipalvelut ja langaton verkkoliikenne vaativat yhä enemmän kapasiteettia ja saavat aikaan enemmän verkkoliikennettä kuin perinteiset palvelut. Verkkojen tulee olla sekä helpommin muuttuvia, muutettavia, käyttöönotettavia että skaalautuvia.

SDN on kehityskaaressaan jo siinä vaiheessa, että sitä otetaan yhä enemmän käyttöön palvelinkeskuksissa ja pilvipalveluissa. Verkkoteknologia perinteisesti kehittyy ensin alustapalveluiden osalta ja seuraavaksi sitä otetaan käyttöön yritysverkkopuolella.

SDN pähkinänkuoressa sisältää kerrosten erottamisen laitteista, keskitetyn hallinnan, avoimuuden, verkon automatisoinnin ja virtualisoinnin sekä yksinkertaisemmat verkkolaitteet.

4.2 SDN toiminnallisuus

SDN:n kaksi olennaista elementtiä ovat hallintakerros ja tiedonvälityskerros (kuva 7). Hallintakerros huolehtii liikenteen reitityksestä, seurannasta ja priorisoinnista ja tiedonvälityskerros vastaa pakettien välittämisestä sen perusteella mitä hallintakerros ohjeistaa.



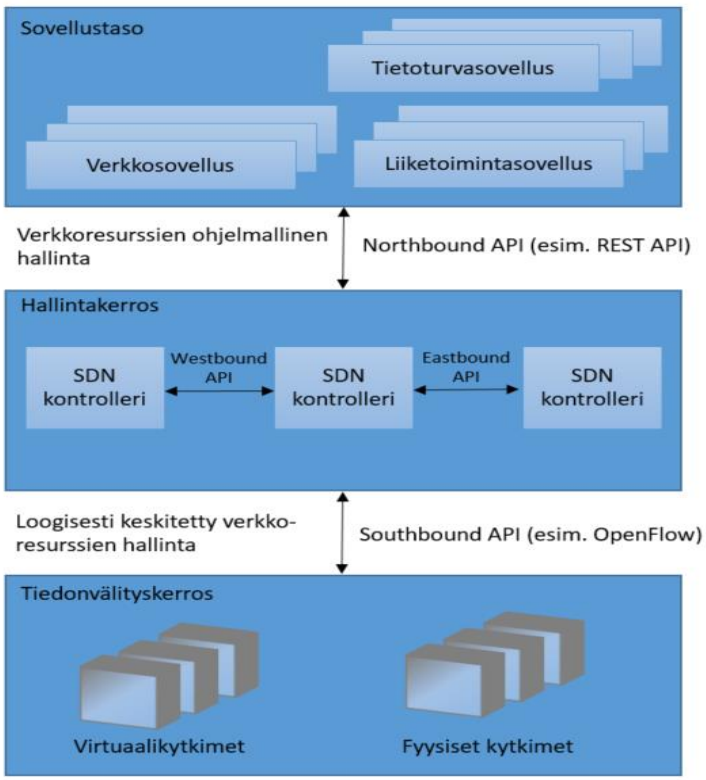
Kuva 7. Software-Defined Networking – ohjelmisto-ohjattu verkko

Tämän päivän verkkolaitteet hoitavat integroidusti molempia edellä mainittuja tehtäviä, mikä tekee verkonhallinnasta haasteellista, varsinkin jos laitteita on useita. Käytännössä se tarkoittaa sitä, että jos halutaan tehdä organisaation tietoverkossa laajoja muutoksia, vaikka reititykseen, niin muutokset on täytynyt tehdä manuaalisesti jokaiseen laitteeseen erikseen. Perinteisesti on pitänyt huolehtia siitä, että kaikki tietoverkon laitteet ovat, jos eivät samalta valmistajalta, niin ainakin tukevat samoja verkkoprotokollia, jotta niiden käyttö on ollut yksinkertaisempaa. Pääsääntöisesti tämä on ohjannut organisaatioita ostamaan yhden ja saman valmistajan laitteita, koska silloin verkkoa hallitsevien ihmisten on tarvinnut osata konfiguroida vain näiden verkkolaitteita.

SDN:n etu perinteiseen teknologiaan ja tapaan toteuttaa tietoverkkoja on siinä, että hallintakerros on erotettu omalle hallinta-alustalleen. Hallinta-alustasta käytetään nimeä kontrolleri. Kontrolleri on usein virtuaalipalvelimella pyörivä ohjelmisto ja on useimmiten myös kahdennettu tai niitä voi olla useampiakin, riippuen organisaation ja tietoverkon arkkitehtuurista sekä rakenteesta. SDN siirtää siis hallinnan pois verkkolaitteilta keskitettyyn palveluun, jolla on näkymä tietoverkkoon tai tietoverkkoihin ja joka pystyy tekemään koko tietoverkon kannalta parhaita ratkaisuja reaaliaikaisesti ja automaattisesti (Cisco 2018).

Verkkolaitteilta pitää löytyä ohjelmallinen tuki, jotta SDN vaatimat ominaisuudet voidaan ottaa käyttöön. Tämä toivottavasti tulevaisuudessa johtaa verkkolaitteiden yksinkertaistumiseen sekä hintojen laskuun.

Jotta tietoverkon hallinta onnistuisi tällä tavalla, täytyy olla tapa, jolla laitteistolle voidaan viestiä. Yksi tapa on käyttää aikaisemmin mainittua avointa OpenFlow-viestintäprotokollaa. Perustasolla vaatimuksena on, että tietoverkon laitteiden pitää tukea yhteisiä ja avoimia rajapintoja.
Kuvassa alla avataan hiukan sitä, miten SDN:ssä erilaiset rajapinnat keskustelevat keskenään.



Kuva 8. Software-Defined Networking arkkitehtuuri

Huomioitavaa on, että kun uusia tapoja tehdä asioita otetaan käyttöön, ne vaativat tuekseen muitakin ratkaisuja ja SDN mukana siirrytään hyvin vahvasti rajapintojen käyttöön. Silloin riittää, että laitteiden ohjelmistoissa on sen verran älykkyyttä, että niitä voidaan ohjata ohjelmallisesti rajapintojen avulla eikä olla enää sidottu yhden valmistajan suljettuihin ohjelmistoihin.

SDN hyötyjä ovat siis keskitetty hallinta, joka esimerkiksi suurissa organisaatioissa vähentää sivutoimistojen paikallisen IT henkilöstön tarvetta. Kontrollerin älykkyys puolestaan osaa ratkaista ongelmatilanteita ilman manuaalista työtä tai ilman että käyttäjän pitää puuttua tilanteeseen. Avoimet rajapinnat tulevat lisäämään ohjelmallisia mahdollisuuksia tehdä asioita eri tavalla tai uudella tavalla. Verkkolaitteisto voi jatkossa olla yksinkertaisempaa, kun niiden ei tarvitse tehdä itse kaikkea päättelytyötä vaan sitä ohjataan muualta käsin.

5 Oivaltava verkko

Digitalisaatio vaatii investointia verkkoteknologiaan, koska sillä on suuri vaikutus tuottavuuteen ja käyttäjäkokemukseen. Huonosti suunniteltu tai toimiva tietoverkko voi kaataa hienotkin hankkeet. Tänä päivänä useimmat sovellukset ovat myös palvelinsaleissa tai pilvessä ja tietoverkkojen toiminta sekä tietoturva ovat ensisijaisen tärkeitä (Cisco 2019).

Siinä missä SDN vastaa enemmän verkon arkkitehtuuriin ja tapaan rakentaa tietoverkkoja, oivaltava verkko tuo ohjelmallisesti lisämahdollisuuksia tietoverkon suunnitteluun ja ylläpitoon SDN-kyvykkään infrastruktuurin päälle.

Oivaltava verkko on olemassa ja tehty nimenomaan tarpeeseen, jossa tietoverkon monimutkaisuus ja laajuus alkavat tuottaa ylläpidollisia ongelmia. On monia erilaisia verkkoja, joita pitää kytkeä toisiinsa erilaisilla teknologioilla, on useita virtuaalilähiverkkoja, erilaisia sääntöjä eri laitteissa jne.

Laitteiden ja verkkojen määrästä huolimatta verkon ylläpitäjiä on silti usein vain tietty määrä ja varsinkin isoissa hankkeissa tämä osoittautuu usein organisaation pullonkaulaksi. Verkkojen laajentamiseen ja toiminnan kehittämiseen ei tunnu löytyvän resursseja eikä aikaa. Mikäli tietoverkoissa on ongelmia, niiden ratkaisemiseen menee paljon aikaa ja usein lisäksi puuttuu vielä näkyvyys verkon tarkalle tasolle, jolloin ongelman rajaus on hidasta ja vaikeaa. Varsinainen tekeminen on hyvin laitekeskeistä ja kaikki tehdään useimmiten vielä käsin.

Ciscon tekemän tutkimuksen mukaan verkkojen operointiin käytetään kolme kertaa enemmän rahaa kuin varsinaiseen fyysiseen verkkoon ja laitteisiin (Cisco 2016).

Oivaltavaa verkkoa markkinoidaan keskitetyn tietoverkonhallinnan tuotteena, joka tuo ratkaisun mm. edellä mainittuihin ongelmiin.

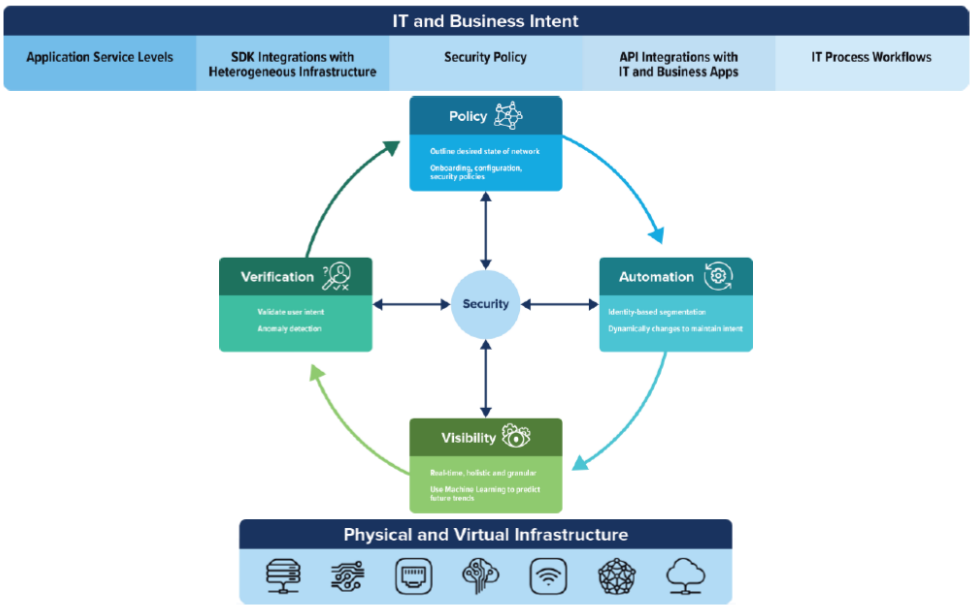
Oivaltava verkko on ratkaisu, jossa joko liiketoiminnan tai IT-osaston aikomukset käännetään verkkoautomaatioksi. Verkoksi joka itse osaa annettujen reunaehtojen perusteella tehdä päätöksiä verkon tilasta tai konfiguraatiosta ja toimia automaattisesti niiden perusteella ilman ihmisen käsityön tarvetta (Cisco 2019).

Oivaltavan verkon periaatteena on nähdä koko tietoverkko yhtenä kokonaisuutena ja antaa verkon ylläpitäjille kyky määritellä mitä he haluavat tietoverkon tekevän. Onnistuak-

seen tässä, oivaltava verkko tarjoaa automatisoidun hallinta-alustan, joka luo tietoverkkoon halutun tilan ja huolehtii erilaisilla säännöillä, että tila säilyy.

Oivaltavalla verkolla on neljä tunnistettavaa ominaisuutta (kuva 9), joista yleisesti ollaan yhtä mieltä:

- Säännöt, jotka määrittelevät verkon halutun tilan ja joiden perusteella laitteita ja käyttäjiä tunnistetaan
- Automaatio, joka mahdollistaa muutokset, joilla haluttu tavoitetila säilytetään
- Näkyvyys, reaaliaikainen näkyvyys verkkoon, laitteisiin ja käyttäjiin
- Varmistaminen, joka huolehtii siitä, että käyttäjä toimii sääntöjen mukaan sekä pyrkii löytämään verkosta poikkeamia ja korjaamaan ne automaattisesti



Kuva 9. Oivaltavan verkon malli (IDC 2018)

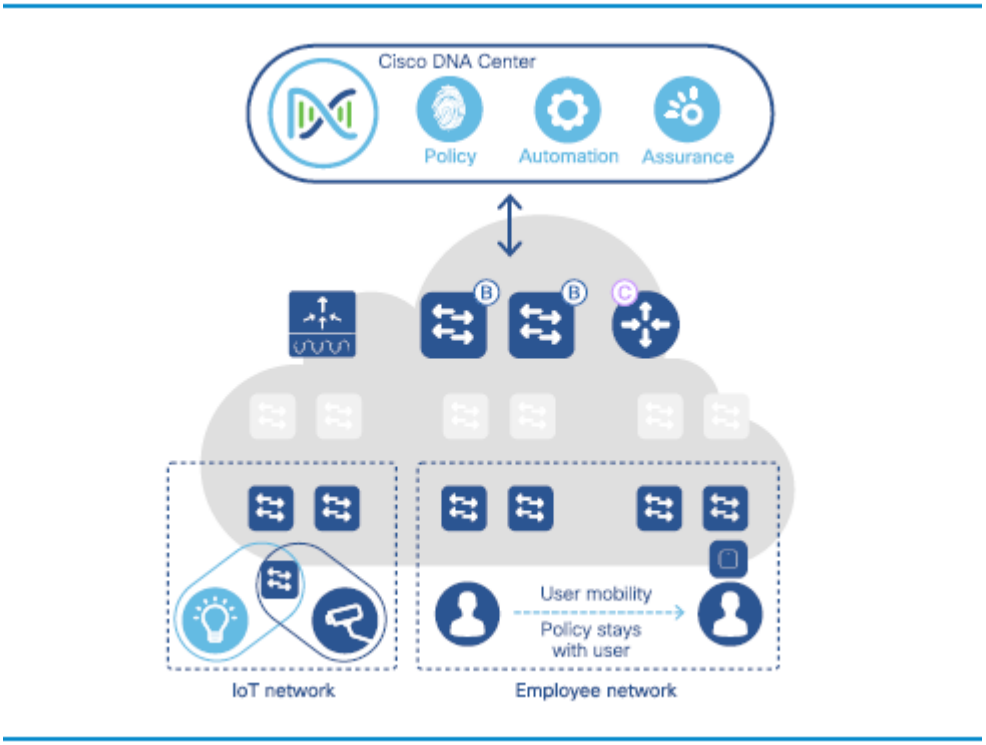
IDC:n mukaan oivaltava verkko on seuraava evoluutio SDN:stä, jolla saavutetaan vielä suuremmat hyödyt yksinkertaistamalla operatiivista toimintaa ja automatisoimalla älykkyyttä hallinta-alustalla. Oivaltava verkko on ensimmäinen etappi matkalla autonomiseen infrastruktuuriin, joka sisältää itseohjaavan tietoverkon, samaan tapaan kuin autoteollisuudessa kehitetään parhaillaan itsestään ajavia autoja (IDC 2018).

Oivaltavan verkon teknologiat ovat vielä kirjoitushetkelläkin uusia, mutta Gartnerin arvion mukaan vuoteen 2020 mennessä yli 1000 isoa yritystä käyttää oivaltavaa verkkoa tuotantojärjestelmissään (Gartner 2017).

5.1 CISCO SDA

Ciscon SDA, Software-Defined Access, oli alan ensimmäinen julkaistu ratkaisu, jolla pyritään vastaamaan oivaltavan verkon vaatimuksiin. SDA tuottaa automatisoituja ratkaisuja käyttäjälle, laitteelle ja sovellusliikenteelle. Näihin kuuluvat esimerkiksi monitorointi, verkon segmentointi, palvelun laatu ja analytiikka. SDA automatisoi myös käyttäjän pääsynhallintaa, jolloin organisaatiot voivat varmistaa, että riittävä pääsynhallinta ja sovelluskäyttäjäkokemus toimivat käyttäjälle tai laitteelle mihin tahansa sovellukseen tietoverkossa (Cisco 2018, s. 14).

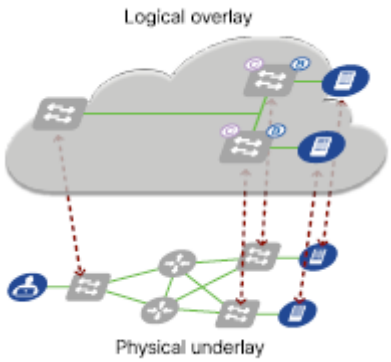
Oheinen kuva selventää Ciscon SDA ratkaisua, jossa hallintakerroksen kontrollerina toimii Ciscon Digital Network Architecture Center, DNA Center tai DNAC. Tiedonvälityskerroksesta käytetään nimeä SDA Fabric.



Kuva 10. Software-Defined Access (Cisco 2018)

5.1.1 SDA Fabric

SDA Fabric (suom. kudos) jakaa tietoverkon kahteen eri kerrokseen samaan tapaan kuin perinteinen SDN ratkaisu. Fyysiset laitteet ja pakettien ohjaaminen kuuluvat aluskerrokseen. Päällyskerros on taas täysin virtuaalinen kerros, jossa langalliset ja langattomat laitteet sekä käyttäjät yhdistetään loogisesti toisiinsa ja missä ennalta määritellyt palvelut ja säännöt otetaan käyttöön.



Kuva 11. Alus- ja päällyskerrokset (Cisco 2018)

Aluskerros sisältää fyysiset verkkolaitteet kuten reitittimet, kytkimet ja langattoman verkon kontrollerit sekä näitä yhdistävän perinteisen Layer 3 reititysprotokollan. Tällä saadaan aikaan yksinkertainen, skaalautuva ja kestävä perusta eri verkkolaitteiden keskinäiseen tiedonvälitykseen. Kaikki verkkolaitteet ovat toisiinsa yhteydessä IP-verkon välityksellä, joten olemassa olevia IP-verkkoja voidaan käyttää aluskerros-verkoissa.
DNAC sisältää palvelun, joka automaattisesti löytää verkkoon liitetyt laitteet ja ennalta määritellyillä säännöillä voi konfiguroida laitteen käyttökuntoon.

Päällyskerros on looginen, virtualisoitu kerros aluskerroksen päällä. Päällyskerros koostuu kolmesta eri teknologiasta, jotka se vaatii toimiakseen:

- Tiedonvälityskerros käyttää VXLAN-teknologiaa, johon on yhdistetty yleiset ryhmäsäännöt, joilla toimintaa hallitaan
- Hallintakerros vastaa loogisesta käyttäjien ja laitteiden kartoituksesta
- Sääntökerros, jossa liiketoiminnan aikeet tai tarpeet on käännetty tietoliikennesäännöiksi käyttämällä ryhmäsääntöjä ja SGT-ryhmätunnisteita

Erottamalla tietoverkko kahteen kerrokseen, saadaan järjestelmään aikaan selkeät vastuurajat ja esimerkiksi päällyskerrokseen voitaisiin tehdä sääntömuutoksia laitteiden tai käyttäjien pääsyjen osalta eikä aluskerrokseen tarvitse koskea ollenkaan.

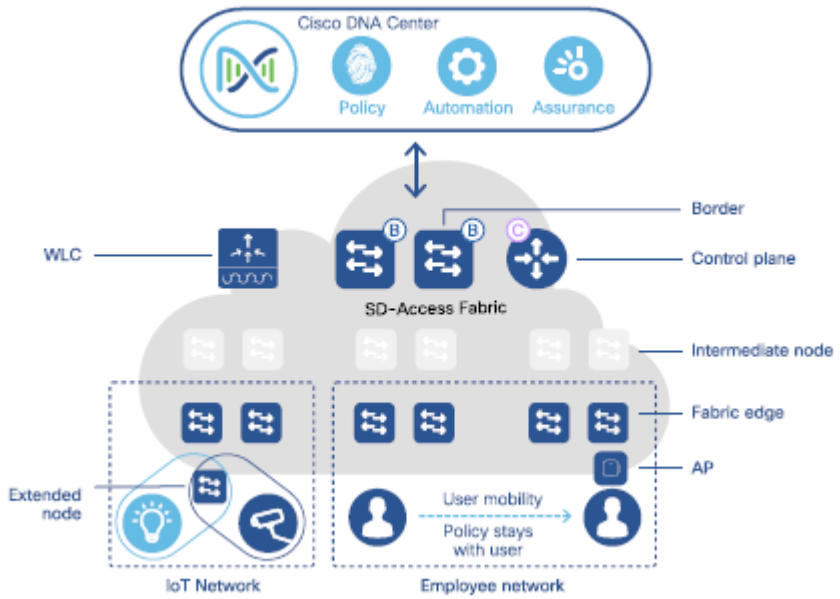
Yhtenä SDA:n hyötynä voidaan siis nähdä sen kyky toteuttaa loogisia verkkosääntöjä riippuen siitä mitä palveluita tietoverkko tarjoaa. SDA pyrkii antamaan kaikille käyttäjille yhteiset säännöt ja samanlaisen käyttökokemuksen riippumatta siitä onko käyttäjä langallisessa tai langattomassa verkossa.

Käyttämällä SGT-ryhmätunnisteita, voidaan eri käyttäjäryhmät tai laitteet erottaa toisistaan esimerkiksi tietoturvan takia. Tätä kutsutaan makrosegmentoinniksi ja siinä hyödynnetään virtuaaliverkkoa.

Käytännössä virtuaaliverkko, VN, on sama asia kuin nykyisissä verkkototeutuksissa VLAN, esimerkkinä organisaatiossa voitaisiin erotella toimistoverkko, vierasverkko, BYOD- ja IoT-laitteet toisistaan määrittelemällä jokaiselle oma VN. VN:n sisällä voidaan vielä erotella laitteet toisistaan SGT:llä, esimerkiksi työasemat ja tulostimet toisistaan.

5.1.2 SDA Fabric komponentit

Tässä kappaleessa kuvataan lyhyesti mistä komponenteista SDA rakentuu.



Kuva 12. SDA Fabric komponentit (Cisco 2018)

Kuvassa 12, hallintakerroksen solmu (C) toimii keskitettynä tietokantana, joka seuraa kaikkia verkon käyttäjiä ja laitteita ja tallentaa tiedon itselleen. Muut verkon laitteet kyselevät siltä tarvitessaan tietoa. SDA:n reunasolmut (B) kytkevät SDA:n perinteiseen Layer-2 tai Layer-3 verkkoon tai toisiin samanlaisiin SDA:hin muualla.

Reunasolmut puolestaan vastaavat päätelaitteiden liittämisestä SDA:han, liikenteen tunneloimisesta sekä välittämisestä.

Välityssolmut, kuten nimi sanoo, vastaavat välittäjän roolissa vain Layer-3 liikenteen välittämisestä eteenpäin reuna-, raja- tai hallintakerroksen solmuille.
WLC kuvassa tarkoittaa langattoman verkon kontrolleria, joihin langattoman verkon tukiasemat ovat rekisteröityneitä.

5.1.3 SDA hallinta

Cisco DNA Center tarjoaa keskitetyn hallintakerroksen SDA Fabricin rakentamiseen ja ylläpitoon. Hallintakerros vastaa siitä millä säännöillä tietoverkon paketit välitetään, mutta samalla myös laitehallinnasta ja analytiikasta.

Laitehallinnassa DNAC voidaan integroida suoraan Ciscon Identity Service Engineen, jotta laitteita voidaan automaattisesti tunnistaa verkossa ja jolla voidaan toteuttaa näille laitteille etukäteen määriteltyjä sääntöjä.

Kun säännöt on määritelty etukäteen, DNACin automaatio toimii ilman ihmisen apua ja toteuttaa useita eri toiminteita saadakseen aikaan halutun lopputuloksen. DNAC kykenee myös orkestrointiin, jossa se automaattisesti suorittaa määriteltyjä prosessin osia tai jopa kokonaisia työnkulkuja, jotka voivat vaatia monimutkaisiakin toimintoja ja käsittää useita eri järjestelmiä (Cisco 2018).

Tämä on ehkä käytännössä se näkyvin osa ohjelmisto-ohjatun järjestelmän hyödyistä. Riittävällä etukäteistyöllä ja määrityksillä voidaan haluttu aie kääntää automaattiseksi toiminnoksi. Lisähyötynä on se, että verkon ylläpitäjät voivat jatkossa keskittyä ylläpitämään aiepohjaista järjestelmää sen sijaan, että heidän aikansa menisi laitteistojen manuaaliseen konfigurointiin. Odotettavissa on myös laadun parantuminen, koska automaatio tekee asiat aina samalla tavalla eli standardisoi tekemisen ja ihmisen vahingossa tekemät virheet jäävät pois.

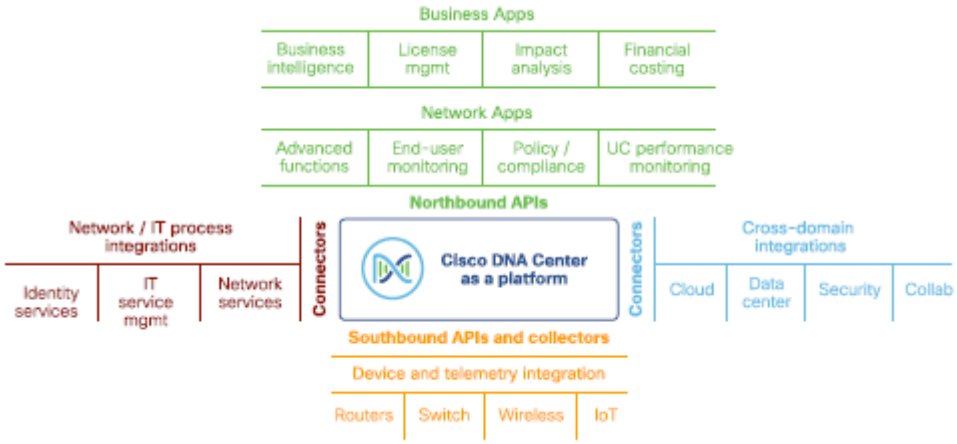
Laitehallinnan lisäksi DNAC huolehtii varmistamisesta. Varmistamisen tehtävänä on huolehtia, että laitteet ovat saatavilla ja seurata tietoverkon yleistä riskitasoa. Toiminnallisuus perustuu tietoverkon reaaliaikaiseen laajaan analytiikkaan käyttämällä perinteisiä verkonhallinnan tiedonkeräystapoja, kuten aikaisemmin mainitut SNMP, Netflow ja syslog. Lisäksi tietoa kerätään langattoman verkon kontrollereilta. Tietoa ei kerätä vain laitteista, vaan myös käyttäjistä ja sovelluksista (Cisco 2018).

Keräämällään tiedolla varmistamispalvelu pyrkii myös proaktiivisesti etsimään ja ennustamaan tapahtumia, kuten laiterikkoja. DNACin käyttöliittymässä tämä näkyy käyttäjälle terveysarvona eli Health-lukuna.

Terveys-näkymiä DNACissa on useita erilaisia. Niillä voidaan seurata yleistasoa kuten edellä olevassa kuvassa tai sitten seurata langattomien tai langallisten laitteiden, verkon tai sovellusten terveystilaa.

5.1.4 Integraatiot

SDA:n käytön merkitys laajentuu entisestään silloin kun siihen voidaan liittää muita sovelluksia tai muut sovellukset saadaan integroitua siihen saumattomasti. Rajapintojen avulla voidaan auttaa hallitsemaan yrityksen koko ympäristöä mukaan lukien tietoverkko. Mahdolliset integraatiot voidaan hoitaa käyttämällä ns. Northbound API:a (kuva 13). Rajapinnan avulla voidaan mm. tuottaa tietoa palvelunhallinnan ITSM-työkaluille, IP-hallintajärjestelmälle, reaaliaikaiseen monitorointiin ja analytiikkaan sekä elinkaarenhallintaan (Cisco 2018, s. 154).



Kuva 13. DNAC integraatiot (Cisco 2018)

Rajapintojen avulla voidaan esimerkiksi kysellä laitteiden asetustietoa tai tilaa. DNACilla on oma rajapintansa, joka mahdollistaa tietoverkon laajuisen automaation. Cisco ISEn rajapintaa käyttämällä saadaan tietoa käyttäjästä, laitteista tai pääsynhallinnasta.

5.2 Yhteenveto

Kirjallisten lähteiden perusteella SDA:n käytölle on useita hyötyjä organisaatiossa. Sillä saadaan enemmän nopeutta ja joustavuutta toimintaan, kun manuaalista käsityötä tarvitaan vähemmän. Myös tehokkuus paranee, kun tietoverkosta saadaan keskitetysti enemmän tietoa ja ongelmiin reagoiminen on nopeampaa, samoin kuin vian paikallistaminen. SDA:n käyttö vähentää myös riskejä, kun tietoverkon toimintaa voidaan säädellä käyttäjä-, laite- tai sovellustasolla. Mikäli on tarvetta tehdä nopeita korjausliikkeitä esimerkiksi tietomurtojen tapahtuessa, on verkkoa ja sinne pääsyä helpompi ohjelmallisesti rajoittaa.
SDA mahdollistaa tehokkaan ja joustavan tavan hallita yritysverkkoja, tehden sen suunnittelusta, laajentamisesta ja ylläpidosta paljon yksinkertaisempaa ja helpompaa.
SDA myös säästää organisaation resursseja ja aikaa ylläpidosta ja verkon toiminnan turvaamisesta ja vapauttaa niitä muuhun tekemiseen (Cisco 2018, s. 164).

6 Pohdinta

Opinnäytetyön alkuvaiheessa asetettiin kysymykset, joita vasten teknologiaa lähdettiin tutkimaan: miksi teknologia on olemassa, mitä ongelmaa se ratkaisee ja mitkä ovat sen toiminnan reunaehdot tai rajoitteet.

Opinnäytetyön tarkoituksena oli näihin kysymyksiin perustuen tarkoitus arvioida kirjallisiin lähteisiin pohjaten varsin uutta teknologiaa. Oivaltava verkko tuotannollisessa käytössä ei ollut kirjoitushetkellä vielä erityisen laajaa, joten varsinainen tutkimus siitä mitä voitaisiin oppia käytännön ratkaisuista, parhaista toteutusmalleista tai kuinka välttää mahdolliset toteutuksiin liittyvät ongelmat tai haasteet, ei ollut saatavilla.
Paljon materiaalia, pohdintaa ja kirjallisuutta on kuitenkin saatavilla ohjelmisto-ohjatuista tietoverkoista, mutta ne ovat usein hyvin yksipuolia ja keskittyvät yhden tietyn osa-alueen tai haasteen ratkaisemiseksi, kuten esimerkiksi monimutkaisen tai laajan pilviympäristön verkonhallintaan.

Mikä sitten tietoverkon hallinnan kannalta on tärkeää ja mihin organisaatiot kiinnittäisivät huomiota valitessaan uutta teknologiaa? Pääsääntöisesti halutaan tietää mitä laitteita on verkossa ja miten ne toimivat. Jos ne eivät toimi, niin halutaan paikallistaa vika mahdollisimman nopeasti. Halutaan yksinkertaista ylläpitoa, jotta työntekijöitä voidaan käyttää tuottavampaan työhön, kuten kehitystyöhön. Pyritään siihen, että verkossa ei ole katkoksia, jolloin liiketoiminta voi tehdä työtänsä. Useimmissa organisaatioissa on yhä tärkeämpää pitää kustannukset hallinnassa sekä ennustettavissa.

Mitä organisaatiolta tai tietoverkkojen kanssa työskenteleviltä tarvitaan, jotta uusi teknologia voitaisiin ottaa käyttöön? Riittääkö perinteinen verkko-osaaminen vai pitääkö osata jotain muuta sen lisäksi? Lyhyt vastaus voisi olla, että riittävä osaaminen tietoverkkojen toiminnasta riittää, mikäli ei aio itse rakentaa uutta teknologiaa, vaan rakentaminen toteutettaisiin yhdessä jonkin alan toimijan kanssa. Uuden teknologian haasteeksi muodostuu loppujen lopuksi kuitenkin se, että varsinainen rakentaminen tehdään käsityönä ja se vaatii syvällistä teknistä osaamista ja ymmärrystä. Mikäli omassa organisaatiossa on riittävästi asiantuntijoita, niin kaikki on periaatteessa mahdollista. Silloin voisi riittää vain avainhenkilöiden kouluttaminen uuteen teknologiaan. Suomessa tällä hetkellä haasteena on se, että toimittajapuolella kenelläkään ei ole vastaavia toteutuksia, joista voitaisiin oppeja ammentaa sekä myös se, että teknologia on uutta. Kun on kyse ohjelmistoon pohjautuvasta ratkaisusta, niin se on aina yhtä hyvä kuin sillä hetkellä vallitseva koodi ja ohjelmis-

ton kyvykkyys suorittaa tiettyjä toiminteita, mutta myös se, kuinka käytössä olevat verkkolaitteet tukevat kaikkia tarjottuja ominaisuuksia.

Muualla tutkimuksissa ja kirjallisuudessa oivaltavan verkon käyttöönotto perustuu yleisesti siihen, että koko verkko tehdään kerralla tällä täysin uudella tavalla. Käytössä ei ole juurikaan kirjallisuutta tai tutkimusta kuinka vanhan ja uuden teknologian yhteensovittaminen onnistuisi. On oletettava, että mahdolliset toteutukset tehtäisiin siten, että jokin tietty osa-alue rakennetaan kokonaan oivaltavan verkon päälle ja muu vanha tietoverkkoinfrastruktuuri jää ennalleen. Miten se käytännössä toteutettaisiin, vaatinee pitkällistä suunnittelua, pitkää kallista projektia ja katkoksia liiketoimintaan siirtymien aikana. On myös oletettava, että ensisijaisesti rakennettaisiin testiverkko, jossa teknologiaa ja käytössä olevia ratkaisuja testattaisiin yhteensopivuusongelmien selvittämiseksi.

Nykyisten nähtävissä olevien ratkaisujen ja mahdollisuuksien valossa, on oletettava, että mikäli oivaltavaa verkkoa haluttaisiin ottaa käyttöön, siihen olisi parhaat mahdollisuudet isoilla yrityksillä, joilla on riittävästi aikaa, rahaa ja resursseja onnistuneeseen käyttöönottoon. Tutkimuksen perusteella on melko selvää, että ratkaisu tarvitsee myös sillä hetkellä hyvin dokumentoidun ja vakioidun tuotantoympäristön, jotta uutta voidaan edes harkita tilalle. Käyttöönoton aikana organisaatiolla ei ole varaa alkaa selvittämään ongelmia ja mikäli ratkaisu ei toimisi vaikkapa tiettyjen päätelaitteiden kanssa, jouduttaisiin välittömästi ratkaisemaan ongelmaa kiertämällä se, mikä johtaisi taas mitä erilaisimpiin virityksiin varsinaisessa tuotantoympäristössä. Hyvin yleisesti on tiedossa, että jälkeenpäin jonkin viritelmän korjaaminen on aina aikaa vievää, kallista ja aiheuttaa lisää katkoksia liiketoimintaan.

Paras edellytys käyttöönotolle näyttäisi siten olevan mahdollisimman segmentoitu ympäristö tai jopa täysin uusi käyttökohde, esimerkiksi uusi toimistorakennus tai tehdas. Yksi mahdollisuus voisi olla myös se ajankohta, kun verkkolaitteiden uusiminen tulee ajankohtaiseksi, jolloin uudistus voitaisiin tehdä samaan aikaan kun laitteet vaihtuvat.

Tutkimuksen aikana selvisi myös, että ohjelmisto-ohjattua verkkoa tukevat laitteet ovat pääsääntöisesti vähintään noin kaksi kertaa kalliimpia kuin ns. tyhmät laitteet. Tämä tulee vaatimaan organisaatioilta todella tarkkaa suunnittelua ja laskentaa, onko teknologian käyttöönotto halvempaa kuin siitä saatavat hyödyt sen jälkeen.
Mikäli organisaatio edelleen joutuu painimaan samojen ongelmien tai haasteiden kanssa kuin vanhan teknologian kanssa, niin mikä on saavutettu hyöty uudesta teknologiasta? Uusi, parempi näkymä verkon tilaan, mutta samat ongelmat verkon kanssa, ongelmat päätelaitteiden kanssa, yhteensopivuusongelmat tms.

Ilman kunnollista tutkimusta ja julkaistua aineistoa, on tätä erityisen vaikeaa arvioida kirjallisten lähteiden näkökulmasta.

6.1 Johtopäätökset

Oivaltavan verkon lupaus on tarjota yksinkertaisempaa, edistyksellisempää tietoverkkoa, joka on avoin, tehokas ja edullinen. Kirjallisten lähteiden perusteella uusi teknologia ja luvatut hyödyt ovat todellakin vakuuttavat ja alan ammattilainen poimii sekä ymmärtää ne kohtuullisen helposti.

Edellä pohdintaosiossa nousi esiin monta näkökulmaa, joilla voisi olla vaikutusta lopulliseen päätöksentekoon uuden teknologian käyttöönotosta.

Oivaltavan verkon hyödyt ovat sellaisia, että varsinkin isojen organisaatioiden tulisi ehdottomasti käyttää aikaa teknologian tutkimiseen ja arvioimiseen. Pelkästään kustannusvaikutukset laitteiston osalta, puhumattakaan projektista, jolla ratkaisu toteutettaisiin, tulevat olemaan merkittävät, joten huolellista analyysiä tullaan tarvitsemaan.

Teknologia on uutta, toteutuksia on suhteessa vielä vähän, kirjallisuutta tai tutkimusta käyttöönotoista vielä vähemmän, joten tällä hetkellä ei näyttäisi olevan järkevää lähteä etenemään vaan odottaa teknologian kypsymistä sekä valmiita toteutuksia, jossa joku muu on tehnyt alkuvaiheen virheet ja haluaa jakaa opitut asiat muillekin.

6.2 Kehitysideat/jatkotutkimus

Aihetta voisi tutkia vielä lisää jonkin Ciscon SDA-ratkaisun osa-alueen osalta tai jonkun organisaation oikean toteutuksen muodossa tai mahdollisesti suunnitella ja toteuttaa Ciscon tuotteilla laboratorio-oloissa toimiva ratkaisu ja tutkia sitä vielä tarkemmin.

6.3 Kokonaisprosessi ja oma oppiminen

Kokonaisprosessin osalta tutkimuksen tekeminen ei ollut läheskään niin haasteellista kuin sopivan kirjallisuuden löytäminen ja sen lukeminen. Materiaalia oli paljon, mutta varsinaisesti aiheeseen sopivaa tai ajankohtaista vähän. Vaikeuksia tuotti löytää juuri oikeaa materiaalia tutkimuksen pohjaksi. Hieman haasteita aiheutti lisäksi se, että jonkin asian ymmärtämiseksi piti etsiä ja lukea muuta materiaalia tueksi. Ajankäytöllisesti prosessi oli siten haastava ja aikaa meni suunniteltua enemmän kirjallisuuden lukemiseen.
Kirjallisuus on tällä hetkellä pelkästään englanninkielistä ja terminologian tuonti suomenkieliseen opinnäytetyöhön ei ollut aina yksinkertaista.

Itse opin eniten uudesta teknologiasta lukiessani lisää ja ymmärsin myös samalla mitä minun tulisi lukea tai opiskella lisää, jotta ymmärtäisin kokonaisuutta entistä paremmin.

Lähteet

Beasley, J., Nilkaew, P. 2016. Networking Essentials: A CompTIA Network+ N10-006 Textbook. 4. Painos. Pearson. Indianapolis. Luettavissa: https://learning.oreilly.com/library/view/networking-essentials-a/9780134299761/cover.xhtml. Luettu 9.8.2019.

Beasley, J., Nilkaew, P. 2016. Networking Essentials: A CompTIA Network+ N10-007 Textbook. 5. Painos. Pearson. Indianapolis. Luettavissa: https://learning.oreilly.com/library/view/networking-essentials-a/9780134866116/cover.xhtml. Luettu 9.8.2019.

Briscoe, N. 2000. Understanding the OSI 7-Layer Model. ITP 7/2000. Luettavissa: http://memberfiles.freewebs.com/61/55/58745561/documents/OSI.pdf. Luettu 9.8.2019.

Cisco. 2018. Software Defined Access Ebook. Luettavissa: https://www.cisco.com/c/dam/en/us/products/se/2018/1/Collateral/nb-06-software-defined-access-ebook-en.pdf. Luettu 9.8.2019.

Cisco. 2019. Software-Defined Access Solution Design Guide. Luettavissa: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2019SEP.pdf. Luettu 9.8.2019.

Cisco. 2019. Cisco DNA Assurance. Luettavissa: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-cisco-dna-assurance-technical-ebook-cte-en.pdf. Luettu 9.8.2019.

Cisco. 2019. Cisco Assurance Demo page. Luettavissa: https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-analytics-assurance/demos.html. Luettu 9.8.2019.

Cisco. 2016. Access Switching Infographic. Luettavissa: https://www.cisco.com/c/dam/en/us/products/collateral/software/access-switching-infographic.pdf. Luettu 9.8.2019.

Coker, O., Azodolmolky, S. 2017. Software-Defined Networking with OpenFlow. 2. Painos. Packt Publishing. Birmingham. Luettavissa: https://learning.oreilly.com/library/view/software-defined-networking-with/9781783984282/cover.xhtml. Luettu 29.8.2019.

Collins, M. 2017. Network Security Through Data Analysis. 2. painos. O'Reilly Media. Sebastopol. Luettavissa: https://learning.oreilly.com/library/view/network-security-through/9781491962831/titlepage01.html. Luettu: 10.11.2019.

Cooney, M. 2019. What is SDN and where software-defined networking is going. Luettavissa: https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html. Luettu 10.9.2019.

ELK. 2019. Luettavissa: https://www.elastic.co/what-is/elk-stack. Luettu 10.11.2019.

Ethernet. 2019. Luettavissa: https://fi.wikipedia.org/wiki/Ethernet. Luettu 10.9.2019.

Gartner. 2017. Luettavissa: https://blogs.gartner.com/andrew-lerner/2017/02/07/intent-based-networking/. Luettu 10.12.2018.

Goralski, W. 2017. The Illustrated Network, 2. painos. Elsevier. Cambridge. Luettavissa: https://learning.oreilly.com/library/view/the-illustrated-network/9780128110287/xhtml/Cover.xhtml Luettu 29.8.2019.

Goransson P., Black C., Culver T. 2016. Software Defined Networks: A Comprehensive Approach. 2. painos. Elsevier. Cambridge. Luettavissa: https://learning.oreilly.com/library/view/software-defined-networks/9780128045794/Cover.xhtml. Luettu 29.8.2019.

Hakala, M, Vainio, M. 2005. Tietoverkon rakentaminen. WS Bookwell. Jyväskylä.

Hudson, J., Fullerton, S. 2001. Special Edition Using Microsoft Active Directory. Que. Luettavissa: https://learning.oreilly.com/library/view/special-edition-using/0789724340/. Luettu 8.8.2019.

IDC. 2018. https://www.idc.com/. Luettu 4.12.2018.

IDC. 2018. Cisco's Network Assurance Tools Take Intent-Based Networking One Step Further.
Luettavissa: https://www.cisco.com/c/dam/assets/nb-09-idc-cisco-analytics-cte-analyst-rpt-en.pdf?ccid=cc000006&oid=%20anren008646. Luettu 4.12.2018.

ISO. 2019. International Organization for Standardization, ISO/IEC 7498-1:1994. https://www.iso.org/standard/20269.html. Luettu 8.8.2019.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. 4. uudistettu painos. Edita. Helsinki.

Lea, P. 2018. Internet of Things for Architects. Packt Publishing. Birmingham. Luettavissa: https://learning.oreilly.com/library/view/internet-of-things/9781788470599/. Luettu 10.9.2019.

Mahler D. 2014. Introduction to Cloud Overlay Networks – VXLAN. https://www.youtube.com/watch?v=Jqm_4TMmQz8. Katsottu 10.9.2019.

McGillicuddy S. 2018. EMA. Preparing Your Network for the Digital Age.
Luettavissa: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/NB/NB06/nb-06-ema-network-upgrade-wp_cte_en.pdf. Luettu 4.12.2018.

McMillan, T. 2012. Cisco networking essentials. John Wiley & Sons. Indianapolis.

Nikkilä E. 2003. Lähiverkkojen kaapelointi. https://www.tivi.fi/uutiset/lahiverkkojen-kaapelointi/640ef498-2034-38d7-b0ee-d38a5f3b66d6. Luettu 14.8.2019.

Noble, S. 2017. Building Modern Networks. Packt Publishing. Birmingham. Luettavissa: https://learning.oreilly.com/library/view/building-modern-networks/9781786466976/cover.xhtml. Luettu 10.9.2019.

ONF. 2019. Open Networking Foundation. Luettavissa: https://www.opennetworking.org/. Luettu 29.8.2019.

OpenFlow. 2019. Luettavissa: https://en.wikipedia.org/wiki/OpenFlow. Luettu 29.8.2019.

OSI-malli. 2019. Luettavissa: http://fi.wikipedia.org/wiki/OSI-viitemall. Luettu 10.9.2019.

OSI-malli vs. TCP/IP-malli. 2017. https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html. Luettu 10.9.2019.

Pujolle, G. 2015. Software Networks: Virtualization, SDN, 5G and Security. WILEY-ISTE. Hoboken-London. Luettavissa: https://learning.oreilly.com/library/view/software-networks/9781848216945/000_ACover.xhtml. Luettu 10.9.2019.

Rintala M. 2001. TCP/IP-protokollat. Luettavissa: http://mrin.mbnet.fi/paattotyo/. Luettu 10.9.2019.

SNMP-protokolla. 2019. Luettavissa: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol. Luettu 10.9.2019.

Stallings, W. 2015. Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Pearson. Indianapolis.

TCP/IP-malli. 2019. https://fi.wikipedia.org/wiki/TCP/IP. Luettu 10.9.2019.