Haaga-Helia
ammattikorkeakoulu Oy

Reititys ja Tietoverkot yrityksissä

Petri Vilhunen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2021

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Petri Vilhunen

Koulutusohjelma
Tietojenkäsittelynkoulutusohjelma

Raportin/Opinnäytetyön nimi
Tietoverkot Yrityksissä

Sivu- ja liitesivumäärä
49

Tässä opinnäytetyössä käsitellään yritysverkkojen topologiaa ja reititysprotokollia yrityksissä. Alussa käsitellään läpi teoriatausta, viitekehykset ja tärkeimmät käsitteet.

Opinnäytetyön alussa käsitellään sisäverkoissa käytettyjä protokollia: EIGRP, IS-IS, OSPF, ja BGB protokollaa, ja käsitellään niiden perustoiminta, niiden erilaisuus, sekä yritetään luoda yleiskuva niiden käytöstä yritysverkoissa. Tarkoituksena on luoda vertaileva yleiskuva reititysprotokollista, joka helpottaisi niistä valitsemista.

Toisessa osiossa pääteemana on yritysverkkojen topologia ja kampusverkot. Aluksi luodaan yleiskuva organisaatioiden verkoista ja hyvän verkon pääpiirteistä. Topologiaa käsitellään pääpiirteissään kampusverkkojen näkökulmasta ja niihin liittyvistä ongelmakohdista kuten redundanttisuuden luomisesta. Taksoituksena on saada selville keskisuurelle organisaatiolle suositeltava verkkotopologia.

Kolmannessa ja viimeisessä osiossa käsitellään uudehkoa SDN verkkoja ja niiden ominaisuuksia ja vaikutuksia tietoverkkoratkaisuihin ja samalla verrata niitä traditionaaliseen kampusverkkoratkaisuun.

Asiasanat
Yritysverkot, Kampusverkot, SDN, Reititys

Sisällys

1 Johdanto

1.1 Työn kuvaus

Tässä työssä on tarkoitus käydä läpi tietoliikenneverkkojen topologiaa ja reititysprotokollia alan kirjallisuuden avulla. Näkökantana työssäni on keskisuuren organisaation näkökulma. Tutkimuskysymys sisältää sen, minkälainen verkkotopologia on sopivanlainen keskisuurelle organisaatiolle, ja miten reititysprotokollat vaikuttavat tietoverkkoon ja siinä käytettävien laitteiden valintaan.
Aluksi tulen tarkastelemaan reitityksessä käytettäviä reititysprotokollia kuten EIGRP IS-IS, OSPF ja BGB, ja toisessa osiossa käsitellään verkon(kampusverkkojen) eri topologioita ja SDN-verkkoja.

Teoriataustana meillä on alan kirjallisuutta, joista tärkeimpinä ovat Deppenkar Mendhin ja Karthikeyan Rammasammyn: Network Routing: Algorithms, Protocols, and Architectures Second edition, Pieter-Jan Nefkenssin Transforming campus networks to intent-based networking, Goranssonin Blackin ja Culverin: Software Defined Networks: A Comprehensive Approach kirjat. Muina lähteinä ovat tietoliikennealan valmistajien kuten Aruban Ciscon omat julkaisut ja muut sekalaiset nettilähteet.

Käytännön tavoitteena työssä on luoda kuva tietoverkkojen topologioista teorioista ja soveltaa niitä keskikokoisen yrityksen tapaukseen. Huomionarvoista on se, että suomalaiset organisaatiot ja yritykset ovat verrattaessa ulkomaalaisiin kollegoihinsa pienempiä, joten näkökulmaa tulee myös verraten pienistä organisaatioista kuten Pk-yrityksissä.

1.2 Tietoliikenneverkot

Tietoliikenneverkot ovat tietokoneista ja muista laitteista, niiden välisistä yhteyksistä koostuvia verkkokokonaisuuksia, joiden tarkoitus on siirtää dataa laitteelta toiselle. Datan ohjaamisesta oikealle päätelaitteelle vastaavat datan siirtoon erikoistuneet laitteet: kytkimet ja reitittimet. Nämä verkkolaitteet yhdessä toimiessaan tietyllä rajatulla alueella muodostavat yhden lähiverkon ns. LAN (Local Area Network) verkon. Näiden rajattujen lähiverkkojen yhtyeenliitettyjä kokonaisuutta kutsutaan Internetiksi (Cisco Inc. Introduction to Networks kappale 1).

1.3 Tietoverkkojen viitemalli/t

Internetin ja verkkojen protokollien viitekehyksenä käytetään TCP/IP-protokolla kokonaisuutta (Stewens, Fall 2011, kappale 1). TCP/IP-protokollamalli on nelitasoinen protokollamalli. Tietoverkkoja tarkastellessa meille mielekkäitä alueita ovat TCP/IP-mallin kaksi alinta tasoa Network acces -taso ja Internet-taso. Näistä Ciscon mukaan Network acces -taso kontrolloi fyysistä mediaa, mistä verkko koostuu, ja Internet-taso hoitaa parhaan reitin fyysisen verkon läpi. Eli käytännössä Network-taso on topologiaa ja fyysisiä laitteita ja Internet-taso reititysprotokollia ja IP-pakettien siirtämistä paikasta A paikkaan B. Tietoliikenteessä on käytössä myös OSI-viitemalli. Verrattaessa viitemalleja OSI-malli on 7-tasoinen ja TCP/IP viisitasoinen malli. TCP/IP-malli on kompaktimpi kuin OSI-malli (Cisco INC, Introduction to networks kappale 1). Opinnäytetyössä pääosin viitataan TCP/IP-viitekehykseen, mutta puhuttaessa tason 2 taikka 3 kytkimistä viittaus on OSI-mallin Datalinkki- ja Network-tasoon, jotka sijoittuvat TCP/IP-mallin Network ja Internet -tasoille.

Taulukko 1 OSI ja TCP/IP mallivertailu.

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application layer</td><td rowspan="3">Application layer</td></tr>
<tr><td>Network layer</td></tr>
<tr><td>Session layer</td></tr>
<tr><td>Transport layer</td><td>Transport layer</td></tr>
<tr><td>Network layer</td><td>Internet layer</td></tr>
<tr><td>Datalink layer</td><td rowspan="2">Network acces layer</td></tr>
<tr><td>Physical layer</td></tr>
</table>

1.4 Käsitteitä

Staattinen reititys	Reityksen muoto missä IP paketin reitti on hallisijan manuaalisesti, määrittelemä. (Cisco Press 2014, kappale 2)
Dynaaminen reititys	Reitityksen muoto mikä on dynamisesti hallittu. (IBM, General Terms)
EIGRP	Enhanced Interior Gateway protokolla Ciscon kehittämä etäisyysvektorityylinen reititysprotokolla (Deepenkar & Karthikeyan 2019, 175)
OSPF	OSPF (open shortest path first) on linkkitilatyylinen reititysprotokolla. (Deepenkar &Karthikeyan 2019, 185)
IS-IS	IS-IS (intermediate system to intermediate system) on linkkitilatyylinen reititysprotokolla. (Deepenkar & Karthikeyan 2019, 185)
Pk-yritys	Yritys, jossa on vähemmän kuin 250 työntekijää ja jonka kokonaisliikevaihto on alle 50 miljoonaa vuodessa. (Tilastokeskus 2021)
BGP	BGP on pääosin suloiseen reitityksen tarkoitettu tietoliikenneprotokolla, joka on käytännössä standardi sisäverkkojen välisen liikenteen välityksessä. (Zhang ym, 2016, kappale 1)
SDN	SDN on verkkoratkaisu, jossa päätös verkkoliikenteen reiteistä tehdään keskeisellä hallintalaitteella. (Goransson, ym, 2016 kappale 3.8)
Kampusverkko	Kampusverkko on klassinen tapa hoitaa organisaation verkkokokonaisuus, jossa verkko usein jaetaan distinktiivisiin kokonaisuuksiin. (Nefkens 2019, kapale 1)
API	Aplication programmable interface eli API on softainstanssi, joka tarjoaa palveluita toiselle sovellutukselle.

2 Reititys ja protokollat

Tässä kappaleessa käydään läpi peruspiirteissään verkoissa käytettäviä reititysprotokollia. Protokollista käydään läpi käyttötarkoitus verkoissa ja niiden perustoiminta. Tarkasteltavana meillä on: staattinen reititys, EIGRP, OSPF, IS-IS ja BGB. Tarkoituksen on luoda näistä reititysprotokollista yleinen käsitys niiden käytöistä tietoverkoista, ja niiden soveltuvuudesta organisaationverkkoratkaisuihin.

Klassisesti jaoteltuina reititysprotokollat jaetaan kahteen eri ryhmään: sisäisiin reititysprotokolliin (IGP), ja ulkoisiin reititysprotokolliin (EGP). Sisäisellä reititysprotokollalla tarkoitetaan IBM:n mukaan protokollia, joita reitittimet käyttävät, kun reititys tapahtuu jonkun tietyn verkon sisällä. Ulkoiset reititysprotokollat taas toimivat näiden verkojen välisen liikenteen välittäjänä. Käytössä olevat protokollat ovat ns. dynaamisia reititysprotokollia, eli ne mukautuvat automaattisesti verkkotopologian muuttuessa. Reitityksessä on myös mahdollista käyttää manuaalisesti määriteltyä reititystä eli staattista reititystä, joka ei mukaudu verkkotopologian muutoksiin. (IBM, General Terms)

2.1 Staattinen reititys

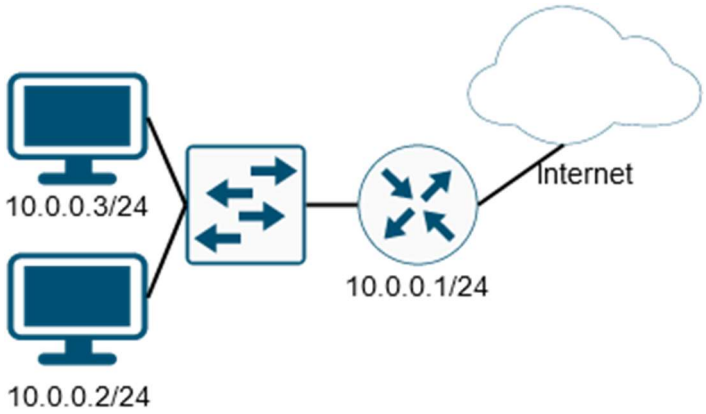
Staattinen reititys on reitityksen muoto, missä reititys on käyttäjän manuaalisesti määrittelemä. Manuaalisella reitityksellä on omat hyvät ja negatiiviset puolensa. Staattista reititystä käytetään tietoverkoissa yleensä vain tietyissä spesifisissä tapauksissa, kuten stubiverkoissa (kuva 1).
Staattisen reitityksen hyviä puolia on se, että se ei oikeastaan käytä verkkolaitteidenverkon resursseja reititysten tekemiseen. Staattisessa reitityksessä reitittimen ei tarvitse laskea parasta reittiä reititettävälle IP-paketille, vaan se tulee suoraan reititystaulusta. Samalla staattista reititystä ei myöskään mainosteta muille, ellei sitä käytetä yhdessä dynaamisten kanssa. Samalla se on Ciscon mukaan tietoturvallisempaa, sillä verkkoa väärinkäyttävän henkilön on vaikeampi saada yleiskuvaa tietoverkosta kuuntelemalla reititysprotokollien reittimainoksia. (Cisco Press 2014, kappale 2)

Tosin staattisessa reitityksessä on myös huonoa. Staattinen reititys ei ole skaalatutuvaa, eikä se myöskään ole vikasietoista ja sen hallinnointi voi tulla raskaaksi. Jos verkossa tapahtuu jotain, joka aiheuttaa vikatilan jollekin reitin osalle ja muuttaa jonkin linkin pois päältä, ei staattisesti määritelty samaista linkkiä käyttävä reitti toimi, jos ei olla määritelty sille redundantteja varayhteyksiä (foating static route) (Cisco Press 2014, kappale 2). Jotta linkki olisi redundantti, verkkoon on määriteltävä varayhteydet. Floating static(varayhteyksien) reititysten määrittäminen lisää verkon kompleksisuutta, ja samalla ver-

kon asetusten määrittämiseen kuluu lisää aikaa ja resursseja, verrattuna dynaamisiin menetelmiin. Tämän takia staattista reititystä käytetään rajatusti tietyissä tilanteissa. Staattista reititystä käytetään Ciscon mukaan yleisesti kun:

- Verkkokokonaisuus on hyvin pieni. Se on joko stubiverkko taikka muutoin pieni verkkokokonaisuus, johon ei odoteta suurta kasvua.
- Gateway of last resort. Viimeisen portti, johon reititin lähettää IP-paketin, jos muuta sopivaa porttia ei ole reititystaulussa.
- Jos verkossa halutaan käyttää jotakin tiettyä spesifistä reittiä, esimerkiksi tietoturvallisuuden kannalta.
- Jos on tarve vähentää verkossa liikkuvien dynaamisten menetelmien reititysmainosten määrää, tai kontrolloida jotakin verkon osaa enemmän. Tosin nykyaikaisissa verkoissa vievät vain pienen määrän verkkokapasiteettia. (Cisco Press 2014, kappale 2)

Organisaation verkon ylläpitäjän näkökulmasta staattinen reititys on hyvä keino pääosin suplementoi verkkokokonaisuuden dynaamisia reitityksiä, ja tynkäverkoissa mahdollisesti hoitaa reititys jopa kokonaan. Suuremmissa verkkokokonaisuuksissa, staattinen reititys on kyllä täydentävä menetelmä dynaamisten protokollien sivussa.



Kuva 1 Stubiverkko. Mukaillen: (Cisco Press 2014, kappale 2)

2.2 EIGRP

EIGRP (Enhanced Interior Gayeway Protocol) on Cisco Systems Inc yrityksen kehittämä reititysprotokolla, joka pohjautuu heidän aikaisemmin kehittämään IGRP-protokollaan. EIGRP Ciscon mukaan on tarkoitettu verkkonimen sisäiseen reititykseen.
EIGRP on etäisyysvektorityylinen reititysprotokolla, jossa suuri painoarvo on reititysten määrällä, eli kuinka monta reititystä kohteen ja kuljetettavan paketin ja sen kohteen välissä on (Cisco Inc, 2005). EIGRP oli Ciscon oma reititysprotokolla, mutta se julkaistiin avoimena standardina vuonna 2013.

EIGRP-protokollan toiminta perustuu IGRP-protokollan rakentamiin perustuksiin. EIGRP käyttää DUAL-algoritmia reitityksen päättelemiseen. Esimerkiksi etäisyysmetriikka, joka IGRP-protokollassa perustuu ”käytettävissä olevaan kaistanleveyteen, sen viiveeseen,

kaistan käyttöprosenttiin ja sen luotettavuuteen” (Cisco 2005), on EIGRP-protokollassa melkein sama. EIGRP-protokollan toiminnassa on neljä tärkeää konseptia:

- Naapurien löytäminen ja niiden takaisinsaaminen: Miten saan tiedot naapureistani ja niiden tilan.
- Reliable transport -protokolla: Tiedon lähettäminen seuraavalle ”hypylle” siten, että se saapuu perille.
- Dual Finite state machine.
- Protokollasta riippuvat moduulit: Vastaavat verkkotason vaatimuksista. kuten IP EIGRP, joka on vastuussa EIGRP-kapseleiden kapseloinnista IP-pakettiin. (Cisco, 2005)

Seuraavaksi käsittelen EIGRP protokollan naapurienlöytämistä ja niiden takaisinsaamista.

2.2.1 EIGRP-paketit

EIGRP käyttää viittä eri pakettityyppiä sen toiminnassa, nämä ovat hello/ack, pyyntö päivitys, kysely ja vastaus paketit. hello/ack-paketteja käytetään naapureiden löytämiseen ja niiden takaisin saamiseen. hello-paketteja lähetetään viiden sekunnin välein verkossa, jolla on suuri kaistaleveys, kuten Ethernet-verkot. 60 sekunnin välein hello-paketteja lähetetään pienen leveyden verkoissa. Kun EIGRP-reititin liitetään verkkoon, se lähettää porteistaan (joihin se on laiteltu toimimaan) hello-viestin multikastina, ilmoittaakseen omasta olemassaolostaan. ack-viestit ovat tyhjiä hello-viestejä, joissa hello-viestin saanut reititin vastaa unikastina hello-viestin lähettäjälle ilmoittaen olemassaolostaan.

Tämän jälkeen reitittimet lähettävät päivityspaketin mainostaen reitityksiään toisillensa, jolloin ne lisäävät paketissa olevat reititykset topologiataulukkoonsa. Topologiataulukko on taulukko, joka sisältää kaikki reitittimen tiedossa olevat reititysmahdollisuudet ja johon Dual vaikuttaa reitittimen mennessä aktiivisen tilaan, jossa reititin laskee reitin kohteeseen Dualin avulla. Aktiivisessa tilassa reititin lähettää kyselyn toiselle reitittimelle, jolloin kyselyn saanut reititin tarkistaa omasta topologiataulusta oman tietonsa ja menee aktiiviseen tilaan. Tällöin kyselyn saanut reititin laskee uuden reitin haluttuun kohteeseen. Kun haluttu reitti on laskettu, vastaa reititin kysyvälle vastauspaketilla. Pyyntö kyselyllä kysytään toiselta reitittimeltä tietoa jostakin spesifisestä reitistä. (Cisco, 2005)

2.2.2 EIGRP protokollan käyttö verkoissa

Käytettävyydessä EIGRP on suuremmalta osalta käytössä lähiverkoissa ja sen soveltuvuus niihin on hyvä. EIGRP pystyy toiminaan myös muden reititysprotokollien kanssa verkoissa ja siinä on IP implementointi sisäisen ja ulkoisen reitityksen käsite, jolloin periaatteessa sitä pystytään käyttämään myös verkkonimen ulkopuolisessa toiminnassa. ”Komentokehotteen tasolla EIGRP-protokollan hallinnointi ja käyttöönotto ovat protokollalla helpohkoa.” (Depenkar, Ramasamy 2018 ,180) EIGRP-protokollan versatiilisuus sopii hyvin erillisiin verkkokokonaisuuksiin. Pienemmissä verkoissa sitä auttaa sen helppo hallinnointi, joka on plussaa, jos yrityksellä ei ole suurta panostusta IT-toimintoihinsa. Huomionarvoista on myös ottaa huomioon, että EIGRP on ollut Ciscon oma yksityinen reititysstandardi, jota ei kaikkien verkkolaitteiden valmistajien reitittimissä tueta natiivisti. Esimerkiksi: ”Huawei-kytkimet eivät pysty toimimaan yhdessä EIGRP laitteiden kanssa suoraan.” (Huawei, 2019). Tämä tarkoittaa sitä, että jos yrityksen verkossa on käytössä Huawein ja Ciscon laitteita, organisaatio ei pysty käyttämään pelkkää EIGRP-protokollaa verkkoratkaisussaan. Jos EIGRP-reititysprotokollaa on pakko käyttää, “lukkiutuu” organisaatio käyttämään vain Ciscon laitteistoja. Tämä on ongelma, joka rajaa organisaatiota yhden laitevalmistajan ”armoille”, sillä jos organisaatio päättäisi ostaa Huawein, Aruban taikka Juniperin valmistamia laitteita, eivät ne natiivisti pystyisi kommunikoimaan EIGRP-protokollalla, vaan niiden on käytettävä OSPF taikka IS-IS protokollaa, missä voi myös sinänsä olla pieniä implementaatioeroja.

2.3 OSPF

OSPF on linkkitilatyyppinen reititysprotokolla, jonka versio 3 (IPv 6 integrointi) julkaistiin vuonna 2008. OSPF on käytössä suuremmissa verkkokokonaisuuksissa kuten operaattorien omissa verkoissa. Paras reitti Deepankarin ja Rammasamyn mukaan OSPF protokollassa lasketaan Djikstran algoritmin avulla OSPF-alueiden sisällä, alueiden välinen liikenne vedetään yhteen ilman toisten alueen tarkempia linkkitietoja. (Deepankar & Ramasamy, 2018, 190) Reititys verkosta Internetiin päin hoituu BGP protokollan avulla.

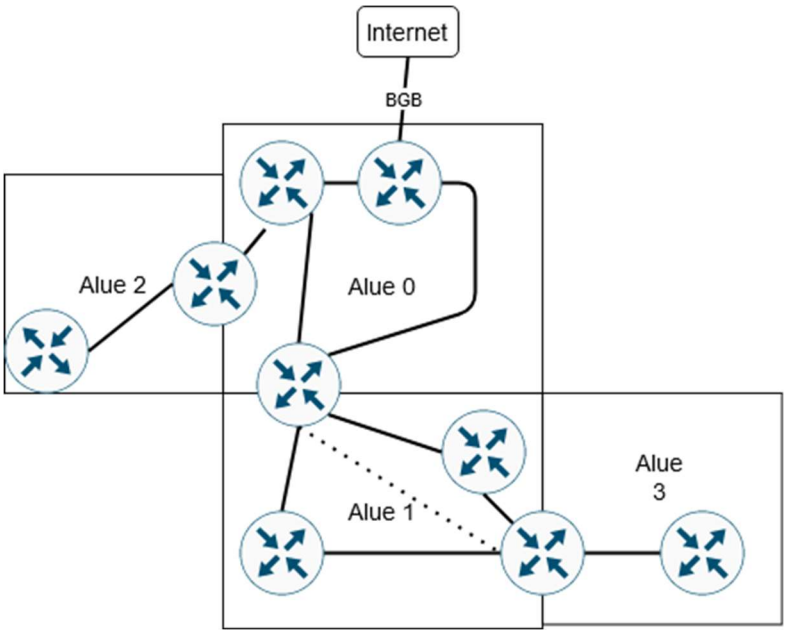
2.3.1 OSPF alueet ja topologia

Toisin kuin EIGRP protokollan, OSPF protokollan funktionaalisuuksiin kuuluu se, että pystytään jakamaan lähiverkkokokokonaisuutta useisiin eri aliverkkoihin, joita kutsutaan alueiksi. Alueita verkossa voi olla useita, mutta niiden looginen topologia pysyy samanlaisena niiden määrästä huolimatta. Verkon alueina on ydinverkko (Alue 0) ja aliverkot (Alueet 1-X). Verkossa Deepankarin ja Ramasamyn mukaan on oltava vähintään yksi ydinalue ja nor-

maalisti myös useita aliverkkoja. Ydinaluealue toimii verkon tukirankana ja yhdistää aliverkot Internetiin/muihin alialueisiin ja hoitaa muiden alueiden verkkojen topologioiden kokoamisen ja niistä infomaisen muille alialueille. Huomionarvoista on myös se, että aliverkko voi olla yhteydessä ydinverkkoon toisen aliverkon kautta toimien normaalin aliverkon tapaan (kuva 2). (Deepankar & Ramasamy, 2018, 185)

Verkon nimeämisessä käytetään 32-bittistä arvoa. Arvo 0.0.0.0, jota sanotaan yleisesti alue nollaksi, on verkon selkärankaverkko ja aliverkot lähtevät arvoista 0.0.0.1 alue yksi eteenpäin. Verkkotyyppejä, joita OSPF ymmärtää, on viisi eri tyyppiä: ponit to point -verkko**,** monilähetysverkot (Ethernet-verkot), NBMA-verkot, Point to multipoint -verkot ja virtuaalilinkit. (Deepankar & Ramasamy, 2018, 187)

Topologiasta johtuen OSPF protokollassa on määritettynä erilaisia reitittimiä. Verkon rajapintareititin, jonka tehtävä on yhdistää ydinverkko (core) ja koko verkkokokonaisuus Internetiin, tämän reitittimen on pystyttävä Deepankarin ja Ramasamyn mukaan käyttämään BGP protokollaa Internetiin suuntautuvassa reitityksessä. Aluerajapintareitittimet, jotka toimivat eri alueiden rajapintoina toisiinsa, jotka yhdistävät verkon aliverkot toisiinsa. Selkärankareitittimet ovat reitittimiä, joilla on yksi verkkoliitäntä selkärankaverkkoon. Sekä sisäiset reitittimet ovat reitittimiä, joilla on yhteyksiä vain aliverkoissa oleviin reitittimiin. (Deepankar & Ramasamy, 2018, 186)



Kuva 2 OSPF verkon topologia. Mukaillen: (Deepankar & Ramasamy, kappale 6.2.1).

2.3.2 Perustoiminta

OSPF protokollan peruskommunikaationa on link state mainostukset (LSA), jotka toimivat sen peruskommunikaationa, eli siirtävät tiedon omista reitityksistä toisille reitittimille. OSPF toimii TCP/IP stäkin päällä tarkoittaen sitä, että sen peruskommunikaatio kulkee IP-protokollaan kapseloituna. Riippuen verkkotyypistä link state mainostusten lähetyksessä on pieniä siihen verkkotyyppiin spesifiä eroa. Point to point -verkoissa LSA-viestit lähetetään käyttäen monilähetys IP-osoitetta 224.0.0.5. Monilähetysverkoissa (LAN verkot) OSPF-paketit lähetetään käyttäen monilähetysosoitetta 224.0.0.6, jos kyseessä ei ole alueen designoitu reititin taikka varadesignoitu reititin, joiden tehtävänä on hoitaa linkkitilamainostusten koordinoidusta lähettämisestä verkossa (jos kaikki lähettäisivät monilähetyksenä oman linkkitilaviestinsä, menisi meiltä verkkokapasiteettia suuresti vain niiden kuljetukseen.). Designoidut reitittimet käyttävät kuitenkin LSA-viestien lähetykseen saama 224.0.0.5 osoitetta kuin point to point ja MBMA verkoissa, jossa linkkitilamainostusviestit lähetetään unikasteina, designoiduilta reitittimiltä designoimattomille ja tosinäpin. (Deepankar & Ramasamy, 2018, 188)

Kuitenkin OSPF IP-protokollan päällä toimivana protokollana ei pysty käyttämään TCP-protokollaa viestien luettavaan lähetykseen vaan se on hoidettu implisiittiä tai selvää vastausta käyttäen. Saadessaan linkkitilamainostusviestin reititin lähettää vastauksena kopion saamastaan LSA-viestistä taikka lähettää linkin tilan tunnistusviestin. (Deepankar & Ramasamy, 2018, 188)

Linkkitilaviestien lisäksi OSPF käyttää kahta aliprotokollaa hello-protokollaa ja tietokannan synkronointiprosessia. hello-protokollalla on osittain sama tehtävä kuin EIGRP protokollassa. hello-protokollaan päätarkoitus on naapurireitittimien löytäminen ja niiden kanssa käytettävän yhteyden parametrien sopiminen. Kaikissa verkoissa hello-protokollalla myös pidetään yllä reitittimien loogisia verekkyyksiä. Monilähetysverkoissa (Ethernet) ja NBMA-verkoissa, toisin kuin muissa verkkotyypeissä, kaikki reitittimet eivät ole loogisesti vierekkäin, vaan verkossa on designoitu reititin, joka hoitaa kontrolloidusti linkkitilaviestien lähettämisestä. Näissä monilähetysverkoissa hello-protokollalla valitaan designoitu reititin vara-reititin sille. (Deepankar & Ramasamy, 2018, 189)

Joissakin tilanteissa kokonaisen linkkitilaviestien lähettäminen on turhaa, joten tietokannan synkronointi voidaan hoitaa tehokkaammin. Tietokannan synkronointiprosessissa reitittimet tarvitsevat vain lähettää linkkitilaviestin headerit, joista reitittimet saavat selville kummalla reitittimellä on uusimmat reititystietokannat ja joita olisi parempi käyttää. Näitä headereita voidaan lähettää tietokannan synkronointiprosessissa useita ja niiden lähetys

ja tarkastelu voidaan jakaa useisiin osiin. Huomionarvoista on myös se, etteivät reitittimet tässä prosessissa toimi tasa-arvoisina, sillä vain toinen reitittimistä toimii maisterina, joka johtaa prosessia ja toinen orjana. (Deepankar & Ramasamy, 2018, 189)

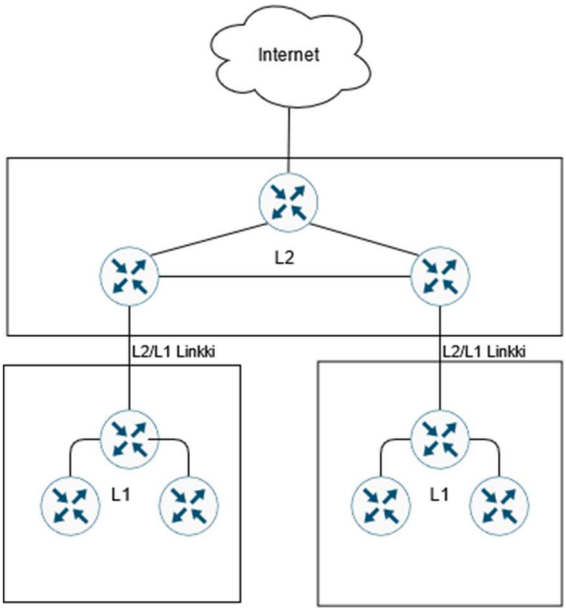
2.3.3 OSPF lähiverkoissa

OSPF on hyvin suosittu reititysprotokolla, ja se sopii hyvin erityyppisiin sisäverkkoihin. Kuitenkin ottaen huomioon pienemmän verkon tarpeet, voi OSPF vaikuttaa ns. raskaammalta protokollalta, kuin EIGRP-protokolla. OSPF-protokollan hallinnointi on Deepankarin ja Ramasamyn mukaan työläämpää, ja sen huomioon ottaminen on tärkeää, sillä OSPFv3-pakettien autentikointi hoidetaan IPsecin avulla, jonka konfiguroiminen on työlästä. (Deepankar & Ramasamy, 2018, 210)

Tilanne Pk-yritykselle voi olla sellainen, että heidän lähiverkkonsa on niin pieni, ettei alialueiden luomiselle ole tarvetta, mikä on yksi OSPF-protokollan hyvistä puolista. Usein tarvetta alueille on vain suurimmissa yritysverkoissa taikka operaattoriverkoissa. Huomionarvoista on se myös, ettei eri alueita ole pakko luoda. OSPF toimii hyvin myös yhden alueen ratkaisuna, jonka hallinnointi on helpompaa verrattuna monialueiseen OSPF-ratkaisuun. Tämän takia monet OSPF-instanssit luodaankin Ramasamyn ja Deepankarin mukaan usein yhden alueen verkoiksi. Tyypillisesti keskisuuret taikka suuret verkko-operaattorit käyttävät joko OSPF-protokollaa taikka IS-IS-protokollaa, kun taas pienet operaattorit ja kampusverkot käyttävät mieluusti EIGRP-protokollaa. OSPF-protokollan taikka muun reititysprotokollan käyttö on myös tarpeellista verkoissa, joissa on usean eri verkkovalmistajan laitteita. Verkko, jossa on Huawein ja Ciscon reitittimiä, ei toimi käyttämällä EIGRP-protokollaa, vaan on käytettävä OSPF-protokollaa taikka jotakin muuta protokollaa kuten IS-IS-protokollaa, mikä olisi tuettu molemmilla laitevalmistajilla. Mitä kuitenkin on aina otettava huomioon, on se, että vaikka OSPF on standardi, voi laitevalmistajien implementoinneissa olla pieniä eroja, jotka voivat sinällään aiheuttaa ongelmia. (Deepankar & Ramasamy, 2018, 211)

2.4 IS-IS

IS-IS (intermediate system to intermediate system) on linkkitilatyylinen sisäverkkoihin tarkoitettu reititysprotokolla. IS-IS kuten OSPF on linkkitilareititysprotokollia ja molemmissa käytetään Djikstran-algoritmia parhaan reitityksen laskemiseen. Vaikka molemmat ovat linkkitilatyylisiä protokollia, jotka käyttävät Djikstran-algoritmia parhaan reitityksen laskemiseen, löytyy niistä myös eroja. Varsinkin terminologia on hyvin eriävää protokollien välillä. Esimerkiksi IS-IS-protokollassa reitittimestä puhutaan välissä olevana systeeminä (intermediate system), alueet ovat L2 (backbone) ja L1 (alialue) ja reitittimet ovat joko L2- tai L1-reitittimiä. Selkeyden vuoksi puhun reitittimestä reitittimenä enkä välissä olevana systeeminä. (Deepankar & Ramasamy, 2018, 203-206)
IS-IS-verkon topologiassa reitittimet eivät seiso alueiden välissä kuten OSPF verkossa, vaan ne ovat jommankumman L2- taikka L1-verkkokokonaisuuden sisällä, joten yhteys alueiden L2- ja L1- reitittimien välillä on niiden välinen linkki (esim kuva 3). Samalla reitittimien designointi on sellainen, että verkossa on vain kahdenlaisia reitittimiä, L2- ja L1-reitittimiä. L2-reitittimet ovat reitittimiä, joilla on vähintään yksi yhteys L2-verkkoon, ja L1-reitittimet ovat reitittimiä, jotka ovat kokonaan verkon sisällä. (Deepankar & Ramasamy, 2018 208)



Kuva 3 IS-IS-verkon topologia. Mukaillen:
(Deepankar & Ramasamy, 2018 kappale 6.6.1)

2.4.1 IS-IS perustoiminta

IS-IS-protokollan reititys perustuu Deepankarin ja Rammasammyn mukaan ISO NSAPille. IS-IS-protokollassa linkkitilaviestit pystytään kapseloimaan OSI-mallin kakkostason protokollan kuten Ethernetin päälle, mutta tarpeen tullessa IS-IS pystytään laittamaan toimimaan IP-protokollan päällä. Linkkitason pakettien käyttö vähentää protokollan haavoittuvaa pinta-alaa OSPF protokollaan verrattuna. Tämä estää erinäisten IP-protokollan haavoittuvuuksien käytön verkkoon kohdistuvissa hyökkäyksissä. Tämä on tietoturvallisempaa kuin IP-protokollan yllä pakettien lähettäminen, joka voi tietyissä tilanteissa tulla ottaa huomioon. (Deepankar & Ramasamy, 2018 208)

Kuten OSPF, IS-IS käyttää Djikstran-algoritmia sen parhaan reitin laskemiseen. IS-IS oli kuitenkin rajoitettuna 6 bitin (short metric) arvoon, joka rajoitti linkin kustannusluvun arvon pienemmäksi tai yhtä suureksi kuin 1023, mutta IS-IS on laajennuksilla saatu käyttämään 24 bittisiä arvoja. (Deepankar & Ramasamy, 2018 206)

IS-IS protokollan käyttämiä paketteja on neljää eri tyyppiä, Hello-paketti, linkin tila -paketti, complete sequence number pdu ja partial sequence number pdu. Hello-paketin tehtävä on samanlainen kuten OSPF-protokollan Hello-pakettien, eli naapurien löytäminen ja yhteyksien ylläpito. Näitä paketteja on kolmea eri tyyliä L1-reitittimille, L2-reitittimille ja point to point interfacelle. (Deepankar & Ramasamy, 2018, 206-207)

Linkkitilaviestit IS-IS-protokollassa sisältävät reitityksen tiedot. Tyyppejä näistä on kaksi L1- ja L2-reitittimille, mutta pääasiassa linkkitilaviesteissä on kuitenkin samat tiedot. Erona OSPF-protokollaan on se, että IS-IS-protokollan linkkitilaviestien aikamääre asetetaan maksimiarvoksi 1200s josta lasketaan alaspäin nollaan, jolloin reitin ei katsota enää olevat kunnollinen, kun taas OSPF-protokollassa lasketaan nollasta ylöspäin. (Deepankar & Ramasamy, 2018, 206)

Complete sequence pdu (kokonainen sekvenssin (järjestyksen) paketti) luodaan reitittimen kaikista linkkitilaviesteistä. Se on OSPF-protokollan tietokannan synkronointiviestien tyylinen paketti, jota käytetään reitittimien reititystietokantojen synkronointiin. Partiaalinen viesti ja paketti tehdään, kun reititin huomaa saaneensa tietokannan synkronointiviestin, mutta siinä ei ole jotakin linkkitilaviestin tietoja, mitä sillä on, jolloin se tekee puuttuvasta osasta kyselyn, ja kysyy uuden version puuttuvasta linkkitilaviestistä. Tämä toimii samantyylisesti kuin OSPF protokollan link state pyyntö. (Deepankar & Ramasamy, 2018, 206-207)

2.4.2 IS-IS lähiverkoissa

IS-IS ja OSPF ovat hyvin läheisiä protokollia, ja samat päätelmät, mitkä voidaan tehdä OSPF-protokollasta, voidaan tehdä IS-IS-protokollaan. IS-IS on hyvä jykevä protokolla, joka luo meille mahdollisuuden luoda monitasoisen alueen alidomaineittain. Tämä kuitenkin on kysymys, onko tarpeellista jakaa verkkoa domainia alidoimaineihin. Pienille yrityksille vastaus on suurella todennäköisyydellä, ei, jolloin voi miettiä olisiko käytännöllisempää käyttää esim EIGRP-protokollaa. Tosin se ei ole vaihtoehto suurelle osalle yrityksistä, jotka eivät käytä Ciscon laitteita, jolloin sitä vaihtoehtoa ei ole. Aliverkotus tulee kuuloon suurimmissa yritysverkoissa ja operaattoriverkoissa, joissa IS-IS-protokollaa on eniten käytössä (Deepankar & Ramasamy, 2018, 210). Kuitenkin IS-IS-protokollaa voi käyttää hyvin lähiverkoissa, ja se soveltuu hyvin keskikokoisiin ja suurempiin operaattoriverkkoihin. Mitä kuitenkin on aina otettava huomioon, on se, että vaikka IS-IS on standardi, voi laitevalmistajien implementoinneissa olla pieniä eroja, jotka voivat sinällään aiheuttaa ongelmia.

2.5 BGP

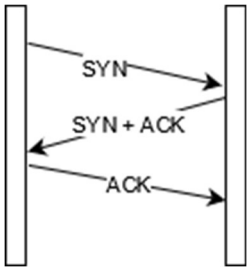
BGP on ulkoisessa reitityksessä käytetty protokolla. Verrattuna protokolliin kuten EIGRP, IS-IS, OSPF, jotka toimivat tietyn organisaation kampusverkossa, joiden tehtävä on välittää organisaation verkon sisäistä reititystä, on BGP-protokollan tehtävänä yhdistää näiden itsenäisten alueiden verkot toisiinsa ja vaihtaa niiden välillä verkkojen saatavuustietoja. ”Nykyisellään Internetissä BGP-version neljä on de facto standardi”. (Zhang ym, 2016 kappale 1)

2.5.1 BGP ja sen toiminta

BGP on ”reittivektori” protokolla, joka lähentelee tyyliltään reittivektoriprotokollia. BGP protokollalle ulkoiseen reititykseen luotuna protokollana on Zhangin mukaan tärkeä skaalautuvuus, luotettavuus, stabiilius ja joustavuus. (Zhang ym 2016, kappale 1) Seuraavaksi käsitellään näitä BGP protokollan osa-alueita.

Luotettavuus tulee BGP-protokollaan käyttäen TCP-protokollan ja BGP-protokollan paketeista. Pakettien lähetys ja yhteyden muodostus tapahtuu TCP-protokollan avulla. Aluksi reitittimet ottavat muodostavan yhteyden komisuuntaisen kädenpuristuksen avulla (kuva 4). Jompikumpi reititin lähettää ensiksi synkronointipyynnön toiselle reitittimelle. Pyynnön vastaanottanut reititin vastaa synkronointipyyntöön kuittaamalla sen ja lähettämällä oman synkronointipyynnön reitittimelle, mistä se on saanut sen. Tämän jälkeen yhteyden aloit-

tanut reititin kuittaa synkronointipyynnön, jonka jälkeen yhteydenmuodostus on valmis. TCP ei kuitenkaan pysty itsessään estämään verkon silmukkatutumista, ja tämä estetään BGB-protokollassa lisäämällä verkossa liikkuviin reititysinformaatiopäivityksiin lista verkoista, minkä läpi se paketti on mennyt, jolloin uudelleen verkon läpi menevät paketit voidaan blokata (Zhang ym 2016, kappale 1).

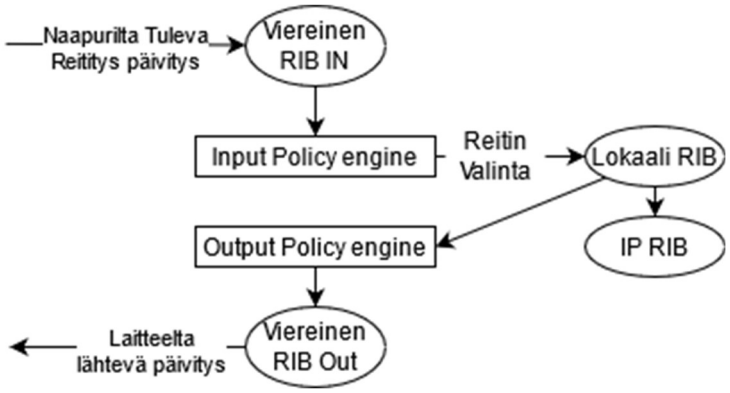


Kuva 4 TCP kolmisuuntainen kädenpuristus.
Mukaillen : (CCNA 2021)

Suurissa verkoissa (mikä Internet on) Zhangin mukaan tärkeää on verkon stabiilius. Suurissa verkoissa reititysten nopea muuttuminen ei ole mielekästä, mikä aiheuttaisi suuria ongelmia sen toimivuudelle. Sanotaan, että reititin mainostaa reittiä kohteeseen ensin reittiä yksi ja heti sen jälkeen reittiä kaksi, jonka jälkeen reitti mainostetaan olevan kiinni. Tämänlaista reititysten nopeahkoa vaihtumista kutsutaan verkon räpyttelyksi, ja se voi aiheuttaa verkossa yhteysongelmia, kun paketit liikkuisivat kohteisiinsa eri reittejä. Stabiiliusongelmia BGP-protokollassa hillitään usealla keinolla, epäluotettavien reittien supressiolla ja reitityspäivitysten lähettämisen vähentämisellä. Verkon supressiossa BGP vieroksuu mahdollisesti epäluotettavien reittien käyttöä reitityksessä, ja BGB on tehty sellaiseksi, että se lähettää reititysinformaatiopäivityksiä vähemmän kuin sisäverkkoon tarkoitetut protokollat. Esimerkiksi ulkoisessa BGP-protokollassa päivitysten lähetysaikaväli on päälle 30 sekuntia. (Zhangym, 2016, kappale 1)

Skaalatutuvuus on otettu huomioon yrittämällä vähentää mainostettavia reittejä. BGP-verkot täten mainostavat vain parhaimpia yhteyksiään. Tämä siitä syystä, että BGP-verkot ovat hyvin suuria ja niissä on paljon yhteyksiä, jolloin kaikkien reittien mainostus ei ole mielekästä. Kun vähennetään mainostettujen reittien määrää, verkossa yhdentymiseen käyttämäaika pienenee, ja käytetään vähemmän laitteiden ja verkon resursseja (Zhang ym 2016, kappale 1). Tämä parantaa verkon toimivuutta ja on hyvin tärkeä ominaisuus operaattorien verkoissa, joissa on satoja reitittimiä ja useita reittejä samaan verkkoon.

BGP protokollan joustavuus pohjautuu attribuutteihin, joilla voidaan määritellä, mitä reittejä BGP ottaa vastaan/mainostaa ja mitkä ovat parhaita reittejä. Reitittimen reittienmäärittely on kolmivaiheinen prosessi. Saadessaan naapurilta tulevan päivityksen se varastoidaan naapureilta tulevia päivitysten taulukkoon, ja Input Policy Engine käsittelee sen ja suodattaa kielletyt reitit. Tämän jälleen BGP protokollan algoritmi ratkaisee parhaan reitin ja tallentaa sen lokaaliin reitti-informaatiotaulukkoon (RIB). Tästä taulukosta Output Policy Engine käy läpi ja suodattaa siitä halutut reitit pois ja tallentaa sen ulosmeneväksi viereisen reitittimen taulukoksi. Illustraatio prosessista kuvassa 5. Zhang ym 2016, kappale 1)



Kuva 5 BGP reitityksen mainostaminen ja vastaanottaminen.
Mukaillen: (Zhang ym 2016, kappale 1)

2.5.2 BGB protokollan käyttö

BGB ei sovellu hyvin verkkojen sisäiseen reititykseen, ja sitä käytetään vain rajatusti sisäverkoissa tuottamaan esimerkiksi MLSP VPN-yhteyksiä (Zhang ym 2016, kappale 1). Mutta ei sen tarvitsekaan toimia, sillä se on luotu organisaatioiden hallitsemien sisäverkkojen väliseen toimintaan, ja siinä se toimii hyvin ja sen versio neljä on Zhangin mukaan ”defakto standardi”. Eli käytännössä BGP on melkein jokaisessa verkossa käytössä ”Internetiin” päin olevalla rajapinnalla. (Zhang ym 2016, kappale 1)

2.6 Konkluusio

Sisäverkkojen reitityksessä meillä on käytössä useita eri protokollia, joissa on erinäisiä eroja. Protokollan/protokollien käytön valinnassa on otettava huomioon: laitteisto, verkon kokonaisuus ja mitä verkolta halutaan tulevaisuudessa. Onko laitevalmistajienvälinen yhteensopivuus tärkeää, voiko verkossa käyttää vain yhden valmistajan laitteita, minkä kokoinen verkko kokonaisuutena on, onko verkon jakaminen alueisiin mielekästä. Jos verkko on todella pieni verkkokokonaisuus (esimerkiksi tynkäverkko), voi staattinen reititys olla sopiva, mutta yleensä sen käyttö on yhdessä dynaamisiin reititysprotokolliin niitä suplementoivana reitityskeinona. Tynkäverkkoja suuremmissa verkkokokonaisuuksissa, joissa

on useita reitittimiä, on käytettävä dynaamisia protokollia. Näissä useiden reititinten kokonaisuuksissa, jos kyseessä on ns. pienempiverkkokokonaisuus ja ei välitetä laitteiden yhtyeentoimivuudesta muiden kanssa, voidaan hyvin käyttää EIGRP-protokollaa ja Ciscon-laitteita, mutta jos on tärkeää olla sitoutumatta käyttämään yhden laitevalmistajan laitteita, niin käytössä on joko OSPF- tai IS-IS-protokolla. Samoin suuremmissa verkoissa OSPF-taikka IS-IS-protokollan käyttö on suositeltavaa, sillä näissä verkoissa, aliverkotus on mielekkäänpää. Ja se että EIGRP protokollassa ei pystytä luomaan samantyylisiä alueita on sen heikko kohta.

Eri organisaation verkkojenyhdistäminen yleensä tapahtuu BGB-protokollalla, sillä se on eri organisaatioiden verkkojen välisen liikenteen välittäjänä ”de facto standardi”. Organisaation näkökulmasta BGP on käytössä vain organisaation Internetiin kytketyllä laitteella nettiin suunnatussa portissa. Zhang ym 2016, kappale 1)

Taulukko 2 Reititysprotokollien vertailu

	ISIS/OSPF	Staattinen	EIGRP	BGP
Tynkäverkko		X		
Keskisuuret verkot	X		X	
Suurempi verkko	X			
Verkot, joissa on useiden valmistajien laitteita	X			
Tarvitaan alidomaineja	X			
Hallinnan helppous on tärkeää.			X	
Ulkoinen reititys				X

3 Tietoverkkojen rakenteesta

3.1 Organisaatiot ja verkot

Organisaatiossa on useita eri koko kokonaisuuksia, meillä on suuria, pieniä ja keskisuuria organisaatioita, joilla jokaisella ovat erilaiset resurssit ja tarpeet. Yritysrintamalla pienet ja keskisuuret yritykset ovat Tilastokeskuksen mukaan yrityksiä, jotka työllistävät vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa, tai taseen loppusumma on enintään 43 miljoonaa euroa. Verkkopuolen kannalta tämä merkitsee tällaiselle organisaatiolle verkon suuruuden rajaamista, sillä pienemmällä yrityksellä ei ole resursseja hallinnoida suurempia verkkokokonaisuuksia, eikä hellä edes ole yleensä tarvetta suurelle kokonaisuudelle. Joillekin pienimille yrityksille yhden reitittimen tynkäverkkokin voi olla sopiva ratkaisu.

Suuria yrityksiä ovat täten yritykset, joilla on yli 250 työntekijää: Näillä organisaatioilla on yleisesti enemmän resursseja hallinnoida, taikka pitää yllä tietoverkkoja niiden kokonsa ja resurssimääränsä takia. Esimerkiksi Aruba suosittelee vähintään kaksitasoista verkkotopologiaa yrityksille, joilla on noin 500 työntekijää heidän ”Aruba campus for midsize networks ” ohjeissaan.

Yrityksen tietoverkko on nykypäivänä yksi yrityksen tärkeimpiä osia, jonka toiminta on hyvin kriittistä yrityksen toiminnan kannalta. Tämä korostuu vielä enemmän käynnissä olevan globaalin pandemian takia, jolloin etätöitä tehdään enemmän. Yrityksen toimintaa ylläpitävänä voimana tietoverkon on tuettava yrityksen toimintoja kokonaisvaltaisesti, eikä pelkän kaistan riittävyyden vahtiminen ole mielekästä. Kaistan riittävyys on toki hyvin tärkeää verkolle, mutta verkossa on otettava huomioon muitakin asioita kuin pelkkää kaistakapasiteettia. Miten erotetaan luotettavan verkon ja epäluotettavan verkon verkkokokonaisuuden (confindentiality), miten huomioidaan verkkokapasiteetin saatavuuden korkean käyttöasteen kohtina(availability), miten hoidetaan verkon toimivuuden vikatiloissa ja miten yritetään estää väärinkäytöksiä (integrity).

4 Kampusverkot

4.1 Kampusverkot ja niiden mallit

Kampusverkot ovat klassinen tapa hoitaa organisaation verkkokokonaisuus. Kampusverkot ovat monitasoisia verkkoja, joissa verkon eri tasoille on määritelty eri funktiot. Kampusverkon koon vaihtelemisen mukaan verkko on joko: kolme, kaksi taikka yksi verkkotasoa. ”Kampusverkko/topologia on yleisesti rakennettu käyttäen kolmea erillistä tasoa.” Tasoina kampustopologiassa verkko on selkäranka (core), jakelu (aggregation) ja pääsytaso (acces layer), joista jokainen taso hoitaa eri tehtäviä. (Nefkens 2019, kappale 1)

4.1.1 Kampusverkon mallit

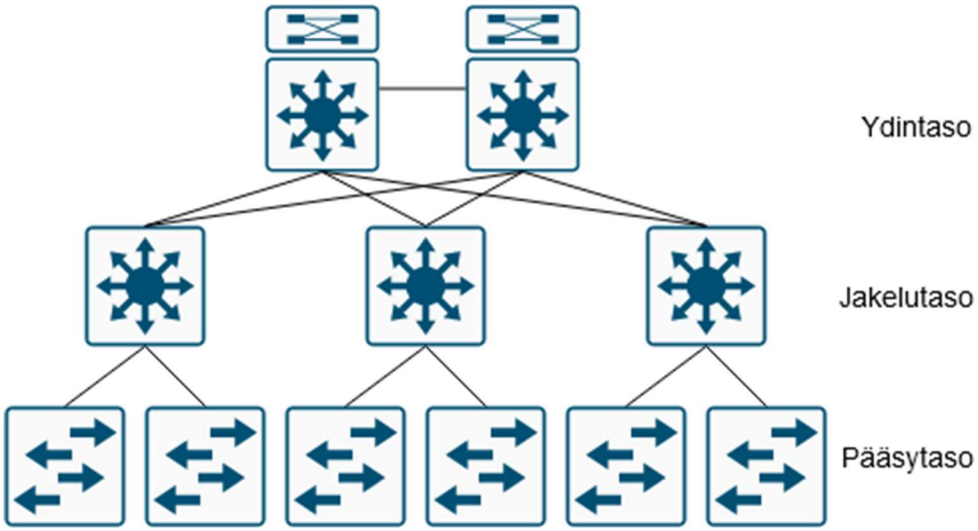
Yleisin kampusverkossa käytetty topologia Nefekenssin mukaan on kolmikerroksinen topologia (kuva 6), jossa verkossa on kaikki kolme kampusverkon tasoa: selkäranka, jakelutaso ja pääsytaso, jotka hoitavat eri tehtäviä. Illustraation kolmekerroksisesta kampuverkosta on kuvassa kuusi.

Pääsytaso on verkkolaitteita lähinnä oleva verkon taso, jonka tehtävä on yhdistää verkon verkkolaitteet lähiverkkoon. Tämä taso koostuu täysin kytkimistä ja langattoman verkon pääsypisteistä. Tieto liikkuu TCP/IP-mallin Linkki layer-tasolla. Jos verkolle on tärkeä arvottaa liikennettä, eli määrittää jonkin tyyppiselle liikenteelle ”etuajo-oikeus”, tapahtuu se yleisesti tällä tasolla. (Nefkens 2019, kappale 1)

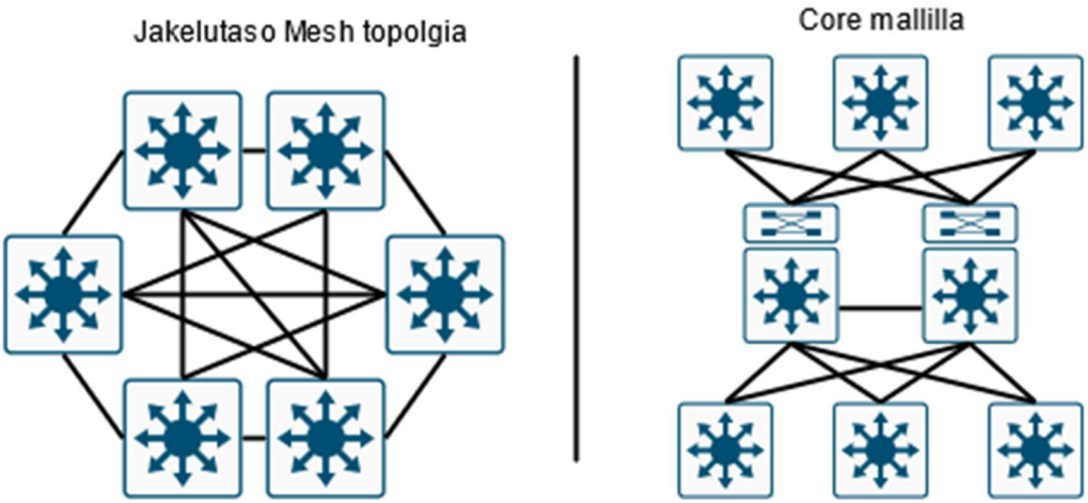
Jakelutaso on pääsytason yläpuolella oleva taso, jonka päätehtävä on luoda verkosta skaalautuvuus ja resilienssi. Tämä taso kokoaa yhteen pääsytasolta saamansa liikenteen ja lähettää sen verkon selkärangalle. Jakelutaso luo yhden kohdan, jossa pääsytason kytkinten liikenne yhdistyy. ”Jakelutaso on myös ideaalinen sijainti yhdistämiseen muihin palveluihin, kuten WAN verkkoon, Internet DMZ ja palvelimiin keskisuurilla organisaatioilla.” (Aruba 2019, 24). Laitteisto jakelutasossa toimii Internet-tasolla (TCP/IP), ja ne jakavat täten pääsytason monilähetysalueet pienempiin osiin. (Nefkens 2019, kappale 1)

Kolmas ja ylin taso verkossa on ydintaso. Tämä tason tehtävä kolmikerroksisessa kampusverkossa on yhdistää kampusverkko muihin kampusverkkoihin, Internetiin ja muihin palveluihin kuten yrityksen omaan palvelintilaan taikka pilvipalveluihin. Ydintasoa käytetään myös simppelöittämään ja luomaan skaalatutuvuutta sen topologiaan (Cisco Inc. 2020,15–16). Suuremmissa verkoissa, joissa on paljon jakelutason jakelukytkimiä (L3-

kytkin), on niiden yhdistäminen täydellisellä mesh-topologialla (kuva 7) epätehokasta, sillä se söisi pois kytkinten porttikapasiteettia ja lisäisi verkon asetusten monimutkaistusta. Core-tason käyttö on skaalatutuvampaa ja helpommin konfiguroitavaa kuin pelkän mesh-topologian käyttö jakelutasolla. (Nefkens 2019, kappale 1)



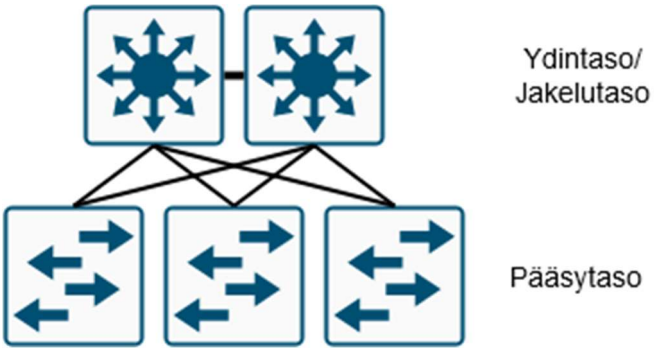
Kuva 6 Kolmitasoinen kampusverkko. Mukaillen: (Nefkens 2019, kappale 1)



Kuva 7 Jakelutaso mesh vs selkärankamalli. Mukaillen: (Nefkens 2019, kappale 1)

4.1.2 Kaksitasoinen malli

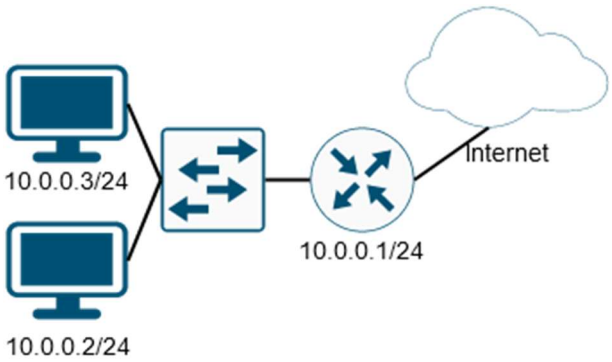
Kolmitasoisen topologian lisäksi verkko on mahdollista rakentaa kaksitasoinen romahdutetun ytimen (kuva 8) mallilla tai joissain tilanteissa tynkäverkkotopologialla. Romahdutetun selkärangan topologiassa verkkotopologia on kaksitasoinen, jossa verkossa kolmitasoiseen verkkotopologiaan verrattuna verkossa on ns. romahdutettu selkäranka ja jakelutaso yhdeksi alueeksi, joka hoitaa verkon yhteydet Internetiin ja muihin palveluihin sekä yhdistyy suoraan pääsytason kytkimiin. Verrattuna komitasoiseen malliin kaksitasoinen topologia on simppelimpi ja käyttää vähemmän verkkolaitteita ja sopii paremmin verkkoihin, jotka ovat pienempiä. (Nefkens 2019, kappale 1)



Kuva 8 Romahdutetun ytimen malli. Mukaillen: (Nefkens 2019, kappale 1)

4.1.3 Yksitasoinen malli

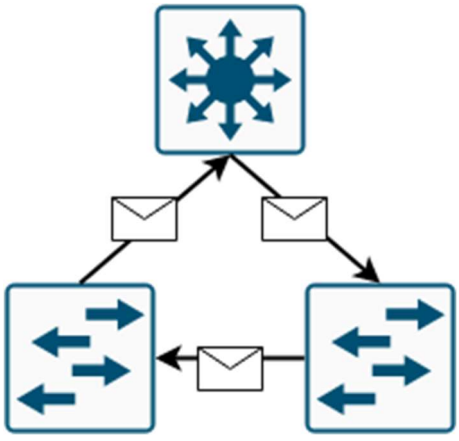
Stubiverkko topologia on pienin malli, jossa verkossa on ns litistetty ytimen jakelutason ja pääsytason yhdeksi kokonaisuudeksi, jossa yksi laite hoitaa kaikkien kolmen eri tason tehtävät (kuva 9). Tämä ei ole käytössä kuin pienimisissä verkoissa Nefkenssin mukaan. Suuri saatavuus/vikasietoisuus tässä verkkotyypissä luodaan (jos on tarpeen) stäkkäämällä useita kytkimiä, jolloin yhden mennessä rikki käyttäjä pystyy siirtymään käyttämään toista. (Nefkens 2019, kappale 1)



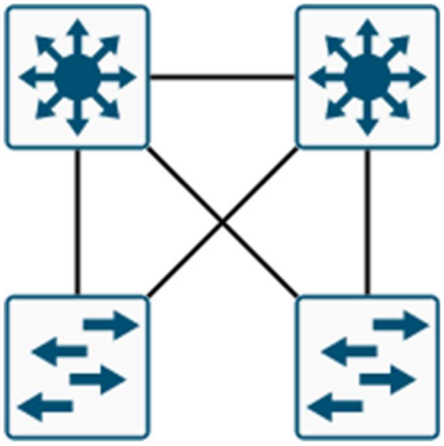
Kuva 9 Tynkäverkko. Mukaillen: (Cisco Press 2014, kappale 2)

4.2 Redundanssisuus kampusverkoissa

Yritysverkoissa ja verkkoratkaisuissa yleisesti tärkeää on verkon redundanssisuus. Redundanttisuudella yleisesti tarkoitetaan sitä, ettei verkossa ole yhtä pistettä, jonka hajoaminen tekisi verkosta toimimattoman. Redundanssisuus verkoissa on yleisesti hoidettu yhteen liittämällä verkkolaitteet usealla eri reitillä kohteeseen. Tämä luo verkolle ongelman, sillä useat reitit kohteeseen voivat aiheuttaa silmukan (kuva 11), jossa data kulkee ympäri verkkoa ympyrässä pääsemättä perille kuluttaen verkon resursseja. Näitä silmukoita voi tapahtua OSI-mallin 2- ja 3-tasoilla eli Ethernet-verkoissa ja IP-verkoissa. IP-verkoissa silmukattomuus on hoidettu reititysprotokollissa olevilla määritellyillä; mutta Ethernet-verkossa on silmukkatutumattomuus luotava topologialla, tai jollain muulla keinolla. Eli pienennettävä Ethernet-verkon kokoa: (käyttää Internet-tason redundanssista), stäkkäämällä useampia kytkimiä yhdeksi loogiseksi kokonaisuudeksi, taikka ottaa käyttöön STP (spanning tree protokolla) ja yhdistää kytkimet yhteen useilla eri reiteillä (kuva 10). (Nefkens 2019, kappale 1)



Kuva 10 Silmukka verkossa. Mukaillen: (Nefkens 2019, kappale 1)



Kuva 11 Yhdistetyt verkkolaitteet. Mukaillen: (Nefkens 2019, kappale 1)

4.2.1 Ethernet-verkkojen jakaminen

Jokaisesta redundanttisuuden luomisen keinosta on hyötyjä ja haittoja. Jos Ethernet-verkosta tehdään pieni, vähenee verkossa silmukkatutumisen mahdollisuus. Käytännössä reititysprotokolla hoitaa tällöin verkon silmukoitumattomuuden. Tällöin Ethernet-verkon on oltava pieni, ja samalla menetetään kytkimissä olevien VLAN verkkojen yhdessä toimivuuden. Samalla verkon hallintamäärä lisääntyy, sillä pääkäyttäjän on määriteltävä eri Ethernet-verkoille eri IP-osoitteet. (Nefkens 2019, kappale 1)

4.2.2 Kytkinten stäkkäys

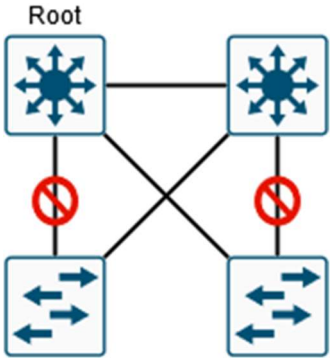
Kytkinten stäkkäyksellä Andrea Mauron mukaan tarkoitetaan useiden kytkintenyhtyeenliittämistä toisiinsa, jolloin ne toimisivat yhtenä loogisena kokonaisuutena. Tällöin kytkin, joka on yhdistettynä kytkinstäkin kahteen kytkimeen, olettaa että se on yhteydessä vain yhteen kytkimeen, jolloin silmukkautuminen ei ole mahdollista. Kun verkossa ei ole silmukoihin johtavia reittejä, ei ole tarpeellista käyttää spanning tree protokollaa silmukoiden ehkäisyyn. Huomionarvoista on kuitenkin ottaa huomioon, että kytkinryhmän (stäkin) suorituskyky voi raskaassa työtaakassa kärsiä riippuen siitä, miten kytkimet ovat liitetty yhteen, ja suuremmissa huoltotoimenpiteissä voi nämä toimenpiteet olla raskaita, sekä tarvita uudelleenkäynnistystä, jokaiselle kytkinryhmän kytkimelle. Huomionarvoista on myös se, että kytkinryhmän yhden kytkimen vääränlainen toiminta voi aiheuttaa ongelmia koko ryhmälle (Andrea Mauro 2019). Samalla kahden linkin käyttäminen, joissakin tilanteissa ei ole aina mahdollistakaan Nefkenssin mukaan. Näistä mahdollisista haitoista huolimatta kytkinten ryhmittäminen(stäkkäys) on hyvin käytössä kampusverkoissa (Nefkens 2019, kappale 1).

4.2.3 Spanning Tree Protokolla (STP)

Kolmas keino estää silmukoita verkoissa on spanning tree -protokolla, joka on silmukkatutumista hallitsevista keinoista ”yleisin” Nefkenssin mukaan. Spanning tree protokollassa (STP) käytetään Moore-Djikstran-algoritmia reitin laskemiseen Ethernet-verkon läpi. Spanning tree protokollassa kytkimet taikka hallinnoija itse valitsee reitittimistä root/pääkytkimen, josta paras reitti lasketaan muihin kytkimiin. Vaihtoehtoiset reitit pääkytkimeltä kohteeseen kytketään pois päältä silmukoiden ehkäisemiseksi, kuten kuvassa 12. (Nefkens 2019, kappale 1)

STP-protokollalla pystytään estämään silmukoita hyvin, mutta siinä on myös useita ongelmia. Kun kytkin saa BPDU (Brige Protocol Data Unit) -paketin, jota käytetään reitin laskuun, ei kytkin pysty välittämään muuta liikennettä (Nefkens 2019, kappale 1).
Tämä voi olla suurinkin ongelma, sillä reitin laskeminen voi kestää kokonaisuudessaan yli 30 sekuntia, mikä ei Goranssonin ym mukaan ole hyväksyttävää esimerkiksi datakeskusten verkoissa, joissa tapahtuu paljon muutoksia ja verkon konvergoitumisaika on tärkeää. Samalla huomionarvoista on, että STP-protokolla laskee kytkimen porttikapasiteettia. Jos verkossa on jokaiselle yhteydelle varareitit, sulkee STP reiteistä huonommat, jolloin reitittimen porttikapasiteetista menee 50 prosenttia hukkaan. STP-protokollan käyttäminen ja hallinnointi myös luonnollisesti lisää Ethernet-verkon kompleksisuutta ja lisää verkon hallinnointitaakkaa. Kuitenkin silmukat verkossa ovat suurempi ongelma, ja STP-protokollan ja sen käyttö on suositeltavaa suuremmissa Ethernet-verkoissa. STP-protokollan käyttö

on kuitenkin tietynlainen vaihtokauppa kompleksisuuden ja kustannusten välillä. (Goransson, ym, 2016 kappale 2.1.2)



Kuva 12 STP ja yhteyksien blokkaus. Mukaillen: (Nefkens 2019, kappale 1)

4.2.4 Redundanttisuus konkluusio

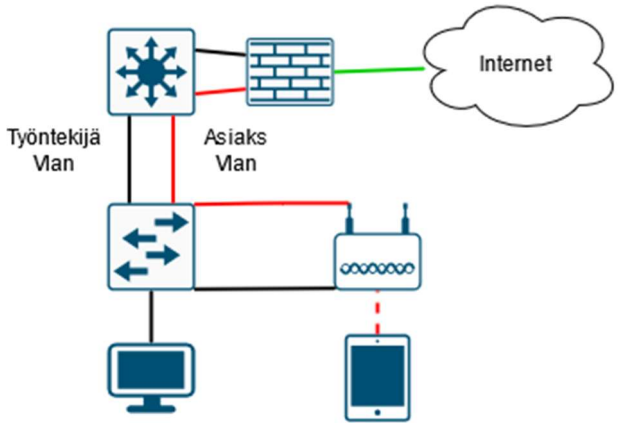
Loppujen lopuksi jokainen keino redundanttisuuden aikaansaamiseksi pyrkii samaan lopputulokseen silmukoiden ja välitysmyrskyjen poistamiseen verkosta. Mikään keino ei tietenkään sovi jokaiseen tilanteeseen, ja verkon ylläpitäjän tehtävänä on tunnistaa omat verkon tarpeensa ja käyttää keinoja silmukkautumisen estämiseen. Yleisesti sanottuna itse suosittelisin pienemmissä verkoissa jakamaan verkon pariin pienempään osaan ja käyttäisin kahden kytkimen stäkkiä yhtenä loogisena kytkimenä.

Suuremmissa ja keskikokoisissa verkoissa en näe hyväksi tavaksi jakaa verkkoja pieniin osiin, sillä se lisää hallinnan kompleksisuutta paljon. Suuremmissa ja keskikokoisissa verkoissa olisi mielestäni parempi käyttää STP-protokollaa ja reitittimien stäkkäystä silmukoiden estämiseksi. Mutta suurissakin verkoissa jotkut erityistä huomiota tarvitsevat voidaan hyvin laittaa omaan pieneen verkkoon, eikä tällaisessa menettelytavassa ole ongelmia.

4.3 Asiakasverkot

Liikennettä organisaation kampusverkossa tulee olemaan organisaation työntekijöiden lisäksi myös asiakkailta ja vierailijoilta. Tämä liikenne ei ole yhtä luotettavaa, ja Aruban mukaan on tärkeää, ettei se uhkaa verkon taikka organisaation tietoturvaa. Jo valmiina olevan infrastruktuurin käyttö on kustannustehokasta vierailija Vlanin käytössä (Aruba 2019, 16–17), ja tietoliikenne yleensä kulkee samassa fyysisessä raudassa. Tietoturva vierasverkoissa luodaan eristämällä vierailijoiden liikenne eri virtuaalisiin lähiverkkoihin virtuaalisiin laneihin ja vaatimalla kirjautumista verkkoon taikka fyysisesti käyttämällä eri laitteita (kuva 13). Virtuaalinen lähiverkko vieraille voidaan konfiguroida saamaan vain yhteyden Internetiin ja organisaation sisäisen DHCP- ja DNS-palvelimeen (Cisco Inc 2020,

51), joka estää vieraiden käyttävän organisaation sisäisiä resursseja. Tosin huomionarvoista on, miten erottelu määritellään, ja se riippuu laitevalmistajasta ja heidän omista ohjeistaan. Esimerkiksi Ciscon 2020 campus LAN -ohjeessa puhutaan keskeisestä virtuaalisen lan-hallitsijan käytöstä, kun taas Aruba vastaavanlaisessa ohjeessa puhutaan jokaisen langattoman pisteen itse konfiguroitavuudesta hallitsijaksi. Mutta tärkeää on kuitenkin laitevalmistajasta huolimatta erottaa asialiikenne omista tietoturvallisesti. (Aruba 2019, 16-17)



Kuva 13 Vierasverkon esimerkki Mukaillen: (Aruba 2019, 16-17)

4.4 Pilven vaikutus

Aluksi mitä pilvi on? Käytännössä pilvi on palvelinten päälle rakennettu ekosysteemi, jonka tarkoitus on tarjota muistitilaa, ajaa sovellutuksia ja tarjota palveluita. Eli käytännössä tarjota samoja palveluita kuin organisaation omat fyysiset konesalit, mutta pilvessä se tapahtuu verkon kautta kolmannen osapuolen palvelimilla, joita ostaja provisioi käyttöönsä. (Microsoft Azure)

Organisaation IT-infrastruktuuri on traditionaalisesti ollut Nefekenssin mukaan itse organisaation omassa keskeisessä datasentterissä, ja yhteys organisaation verkon ulkopuolelle on mennyt yhdestä keskeisestä paikasta. Nykypäivänä kuitenkin pilvipalveluiden kehittymisestä johtuen organisaatiot ovat ottaneet pilvi-infrastruktuurin käyttöönsä. Tämä lisää liikennettä organisaation verkosta ulospäin ja organisaation verkkoon, jolloin organisaation keskeisen Internet-yhteyden mahdollistavan verkon taakka kasvaa. Tästä syystä organisaatioilla trendinä on ollut muuttaa keskeisen Internet-yhteyden mahdollistavan verkon SDN-verkkoratkaisuiksi ja mahdollistaa toimipaikkojen ottaa suora yhteys Internetiin. Jos toimipaikoilta on mahdollisuus ottaa yhteys nettiin suoraan, tulee organisaation vahvistaa toimipaikan verkon tietoturvallisuutta ja sen valvontaa. (Nefkens 2019, kappale 2)

Se, minkälaisena liikenne kulkee organisaatiosta pilveen ja sieltä takaisin, riippuu paljolti siitä, mitä pilvessä on pystyssä. Käytännössä meillä on monia tapoja päästä käsiksi pilvi-infrastruktuuriin. Käytännössä tarkasteltaessa esimerkkinä Amazonin virtuaaliverkkoa voi sitä hallita verkkokäyttöliittymän, AWS CLI:n, sovelluskehityspakkauksien (SDK) ja APIen kautta. Loppukäyttäjälle liikenne kulkee organisaatiosta organisaation pilviverkkoon VPN-tunnelin kautta. Tämä VPN voi Amazonin tapauksessa VPN. VPN Amazonin verkkopalveluiden tapauksessa voi olla joko Amazonin palveluna tuottama verkosta verkkoon VPN (eli verkot ovat liitettynä toisiinsa), päätelaitteelta verkkoon menevä VPN taikka organisaatio voi itse luoda kolmannen osapuolen ohjelmistolla (kuten SoftEther, jne.) virtuaalikoneen päälle tarvitsemansa tunnelin. VPN voi olla IPSec- taikka TLS-pohjainen VPN. Idea VPN:llä on salata verkkojen välinen liikenne, kun se kulkee Internetin läpi. (AWS)

4.5 Tietoturvasta yleisesti

Hyvään verkkoon liittyy kapasiteetin resilienssin lisäksi myös tietoturvalliset näkökulmat. Uhkia tietoverkoille on useita, ja niiden vakavuus vaihtelee verkon ja organisaation mukaan. Uhkia tietoverkoille on esimerkiksi: kiellettyjen verkkolaitteiden lisäys verkkoon, DHCP-spoofaus, ARP-myrkytys, väliintulo -hyökkäykset (Cisco Systems Inc, 2020) yms. Uhkia on paljon enemmän, mutta niiden jokaisen listaus ei tässä ole mielekästä.

Uhkien estämisessä ei ole yksittäistä keinoa estää kaikkia uhkia, vaan pääpointteja, joita noudattamalla uhkia pystyy pienentämään. Amerikkalaisen CISAn (Cybersecurity, Infrastructure Security Agency) verkkolaitteisiin keskittyvän turvallisuusohjeistuksen mukaan tärkeitä asioita verkon turvallisuudessa tärkeää on: verkon segmentointi, sensitiivisen informaation erottelu, ”sivuttaisen viestinnän vähentäminen”, verkkolaitteiden turvallisten asetusten käyttöönottaminen/turvalliset yhteydet niihin ja verkkolaitteiden aitouden varmistus. (CISA 2018)

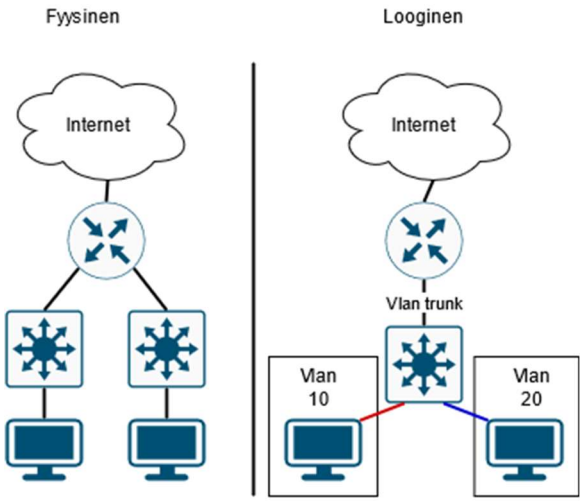
4.5.1 Verkon segmentointi ja kommunikaatio sen sisällä

Verkon segmentoinnin ja sensitiivisen informaation erottelun ideana on vähentää verkon hyökkäyspinta-alaa vähentämällä koneita ja datan määrää, mitä tietystä verkon pisteestä päästään näkemään (kuva 14). Sanotaan verkossa olevan laite, joka propagoi haitallista ohjelmaa eteenpäin. Jos verkossa on yksi laaja verkkosegmentti, pystyy tämä laite propagoimaan haitallista ohjelmaa kaikille laitteille, mikä laittaa suuren määrän organisaation laitteita vaaraan. Verkon segmentoinnilla eri alueisiin pystytään estämään haitallisten ohjelmien hyökkäyspinta-alaa ja turvaamaan sensitiivistä informaatiota. Segmentointi voi tapahtua CiSAn mukaan joko fyysisesti eli käyttämällä fyysisiä laitteita jakamaan verkkoa pienempiin osiin, taikka virtuaalisesti softan tasolla osiin. Fyysisillä menetelmillä verkko

jaetaan eri segmentteihin verkkolaitteilla, jolloin eriarvoinen liikenne kulkee eri verkkosegmenttien kautta kohteeseensa. Virtuaalisissa menetelmissä verkot jaetaan softan tasolla eri segmenteiksi (vlaneiksi), jotka jakavat eriarvoiset liikenteet eri verkoiksi. Nämä verkkosegmentit suunnitellaan sellaisiksi, että vain tietyt ihmiset pääsevät niihin käsiksi ja että niissä käytetään tietoturvallisia asetuksia. Virtuaalisella puolella CISA suosittelee käyttämään Virtuaalisia LAN-verkkoja, Virtuaalista reititystä sekä VPN-yhteyksiä tarvittaessa (CISA 2018). Huomionarvoista on se, että keinot ovat osittain limittäisiä, jotka hoitavat saman asian eri keinoilla.

Kuten jo sanottu, mitä enemmän laitteita laite pystyy tavoittamaan, sen suurempi mahdollisuus haitallisen ohjelman propagoimiseen on. Pelkkä verkon segmentointi alueisiin ei joko riitä taikka se ei ole vaihtoehtona mielekäs. Muuna keinona, jossa hyökkäyspinta-alaa voidaan vähentää, on päätelaitteiden kommunikaation vähentäminen verkossa ja itse verkossa olevien laitteiden tietoturvallisuuteen liittyvien asetuksien käytötönottoa ja yleisesti niihin liittyvien tietoturvallisuusriskien huminoimista. Päätelaitteiden kommunikaation vähennyksellä tarkoitetaan vähentää liikennettä itse päätelaitteilta toisille. (CISA 2018)

Päätelaitteelta päätelaitteelle menevää liikennettä voidaan vähentää asettamalla kytkimiin ja reitittimiin palomuureja ja pääsylistoja, jotka rajoittavat liikennettä päätelaitteelta toiselle taikka liikennetyyppejä sellaisiksi, että haittaohjelmien käytättämät protokollat blokataan. Suositeltavaa on myös jakaa verkkoja segmentteihin ja käyttää virtuaalisissa lähiverkoissa pääsylistaa. Suositeltavaa laitteiden tietoturvaan liittyvien asetusten tarkastelussa on ottaa huomioon tietoturva laaja-alaisesti. Tärkeää turvata laitteiden fyysinen turvallisuus/disabloida käytättämättömät ja epäturvalliset protokollat, pitää huolta salasana/pääsykontrollista, muistaa laitteiden päivitykset sekä niiden auditointi, sekä tietenkin varmuuskopiot, jotta pahimmassa tapauksessa tärkeää dataa ei menetetä kokonaan (CISA 2018).



Kuva 14 Verkon segmentointi Mukaillen: (CISA 2018)

4.5.2 Laitteiden hallinnasta

Verkkolaitteiden hallinnasta organisaation CISAn mukaan on otettava huomioon kolme asiaa: laitteiden validiteetti, hallinnan yhteyden turvallisuus päätelaitteelta hallittavalle laitteelle sekä hallitsijan autentikointi. Hallinnoijan validoiminen on tärkeää, jottei verkkolaitteisiin taikka muihin laitteisiin päästäisi käsiksi ilman lupia. Sanotaan pahantahtoisen toimijanpäässeen käsiksi organisaation verkkolaitteisiin, jos hän saa niissä pääkäyttäjän oikeudet, pystyy hän käytännössä estämään koko organisaation toiminnan. Tästä johtuen laitteiden hallinnassa on pidettävä erityistä huolta varsinkin, kun kyseessä on palvelimet taikka verkkolaitteet. Laitteiden hallinnan yhteydessä CISA suosittelee kyttäämään, monitasoista tunnustautumista, AAA (Authentication Authorization ja Accounting) palvelinta pääsynhallintaan. Jos kuitenkaan ei ole mahdollista käyttää AAA-palvelua taikka monitasoista tunnistautumista, on käytettävä turvallisia salasanoja yli 8 merkkiä (numeroita, merkkejä ja kirjaimia), joita voidaan säilyttää turvallisessa paikassa, kuten kassakaapissa, unohtumisen varalle (CISA 2018).

Kuitenkaan pelkkä hallinnoijan tunnistautuminen ei riitä turvaamaan laitteiden/verkkolaitteiden hallintaa. Jos pahantahtoinen henkilö on päässyt johonkin verkon osaan kiinni, pystyy hän tarkastelemaan siinä verkon osassa liikkuvaa liikennettä. Tästä syystä CISA suosittelee hallintayhteyksien pitämistä erillään tavallisesta liikenteestä ja salaamaan sen, jolloin vaikka jokin verkon osio olisi vaarantunut, ei pahantahtoinen toimija näkisi kaikkea verkon hallintaliikennettä. Myös hallintayhteyksissä on huomionarvoista ottaa huomioon, että hallinnoitavat laitteet ovat päivitettyjä, hallinnointiverkossa sekä se, että hallinnoiva laite on päivitettynä. (CISA 2018)

4.5.3 Sovellutukset ja laitteistot

Olen kuullut tarinoita siitä, kun tietokoneiden yleistymisen alkuaikoina ihmiset suhtautuivat tietoturvaan rennommin ja kun tietokoneet olivat uusinta uutta, niin useat ihmiset keräytyivät katsomaan, kun yksi henkilö laskeutui lentokoneella lentotukialukselle tietokonepelissä työajalla. Nykyään jos missään työpaikalla tapahtuisi näin, tulisi IT puolelta hyvin kovaa sanomista ja syystä. Ongelmana organisaatiolle on laitteiden ja softan turvallisuus ja niiden muuttamattomuuden validointi. Miksi se on tärkeää? Koska laitteet taikka sovellutukset, jotka eivät ole siinä kunnossa kuin valmistaja on sen määritellyt, ovat vaarallisia. Malliesimerkkinä tästä on Partnairin 394 onnettomuus, jonka aiheutti väärennetty osa (AAIB 1989). Vaarallisuudella tarkoitetaan fyysistä turvallisuutta (tulipalo ym.) ja itse tietoturvallisuutta (onko haavoittuva viruksille ym.). Vääränlainen softa voi avata takaportteja verkkoon ja tietokoneiden viallinen toiminta riippuen sen käyttötarkoituksesta voi aiheuttaa suurta tuhoa. Näiden ongelmien ehkäisemiseksi CISA vuoden 2018 ohjeissaan suosittelee pitämään eritystä huolta siitä, mistä laitteet hankitaan, verifioida laitteiden autenttisuus ja niiden muuntelemattomuus pitää huolta logistiikkaketjun turvallisuudesta. Softapuolella tärkeää on pitää huolta siitä, että päivitykset tulevat oikeasta lähteestä ilman muuntelua, monitoroida softaa ja laitteistoa yleisesti muuntelun ehkäisemiseksi. Tärkein asia on kuitenkin se, että IT-puolen työntekijät ovat tietoisia väärennetystä laitteista tuntemattomien/muokattujen sovellutusten käyttämisestä ja muista ongelmista, jotta he osaavat ja pystyvät tunnistamaan nämä ongelmat ja reagoimaan niihin parhaalla mahdollisella tavalla. (CISA 2018)

4.6 Yrityksen näkökulma.

Miten nämä topologiat näkyvät yritykselle? Verkolle ja sen topologialle yleisesti on tärkeää saada määritellyksi, kuinka paljon käyttäjiä, kuinka paljon liikennettä ja millaisia laitteita siellä on. Samalla meitä rajoittaa yrityksen liiketoiminta ja sen vaatimukset. Yritysverkot voidaan käytännössä kampusverkkomallissa rakentaa kaksi-, kolme- taikka yksitasoiseksi. Pääsääntöisesti ajateltaessa mitä enemmän työntekijöitä organisaatiolla on, sen enemmän verkkoon kytkettyjä laitteita heillä on, jolloin heidän verkkonsa on oltava kompleksisempi. (Nefkens 2019, kappale 1)

Kaavio 3 Keskimääräinen laitteiden ja yhteyksien määrä.
Mukaillen: (Cisco 2018-2023)

Alue	2018	2023
Globaali	2.4	3.6
Aasia/Tyynimeri	2.1	3.1
Itä ja Keski-Eurooppa	2.5	4
Latinalainen Amerikka	2.2	3.1
Afrikka/Lähi-itä	1.1	1.5
Pohjois- Amerikka	8.2	13.4
Länsi Eurooppa	5.6	9.4

Katsotaan vaikka keskisuurta yritystä, jossa on tilastokeskuksen määritelmän mukaan maksimissaan 250 työntekijää. Tämä ei kuitenkaan tarkoita sitä, että yrityksellä olisi verkkoon yhdistettäviä laitteita vain 250. Kukaan tuskin käyttää vain pelkkää kannettavaa tietokonetta töissään, vaikka se voi olla pääasiallinen työväline, ja tässä ei ole otettu huomioon itse verkkoinfrastruktuuria ja muuta bisneskriittistä IT infrastruktuuria. Jotta laitelukumäärä olisi paremmin suuntaa antava, olisi siihen lukuun lisättävä itse tarvittava IT infrastruktuurin laitelukumäärä ja ihmisten käyttämien laitteiden määrä, joka lisää verkon kapasiteettitarvetta. Katsottaessa Ciscon vuotuista Internet-raporttia vuosimallia 2018–2023, Länsi-Euroopassa ihmisten keskimääräinen verkkoyhteyksien ja laitteiden määrä ylittää viiden laitteen ja verkkoyhteyden määrän. Hyvin tyypillistä on se, että henkilöllä voi olla työkone ja oma läppäri ja puhelin, laajakaista ja mobiili laajakaista. Tämä tarkoittaa, että organisaatiolle bisneskriittisen infrastruktuurin per henkilö liikkuu 5,6 ja yhden tietokoneen/älylaitteen/verkkoyhteyden välillä.5,6 laitteen logiikalla 250 henkilön organisaatiolla voi olla jopa 1400 verkkoyhteyttä ja laitetta, joista olisi pidettävä huolta. Tietenkin 5,6 laitteen keskiarvossa on ihmisten henkilökohtaiset laitteet mukana, joita ei käytetä töissä. Tästä syystä konservatiivisemmalla arvolla laskeminen voi olla mielekkäämpää. Lasketta-

essa 3 yhteyden ja laitteen keskiarvolla on organisaatiolla silti 750 laitetta ja yhteyttä, joista olisi pidettävä huolta. Ja jos Nefkenssin antama arvio 200 laitteen keskiarvo per hallinnoija pitää paikkansa, olisi organisaatiolla oltava vähintään 4 henkilöä hallinnoimassa näitä laitteita). Ja huomionarvoista on se, että nämä luvut sisältävät vain henkilöiden suoraan käyttämät laitteet, jolloin organisaation tärkeän bisneskriittinen verkkoinfrastruktuuri (reitittimet ja kytkimet) ja palvelimet eivät ole mainittuna, jotka lisäisivät verkon kapasiteetin tarvetta ja kompleksisuutta. Pointtina tässä on se, että verkon suuruus ja sen kompleksisuuden tarve voi vaikuttaa pienemmältä, jos ottaa vain huomioon organisaation ihmisten määrän eikä sitä, kuinka monta laitetta he mahdollisesti käyttävät. (Nefkens 2019, kappale 1)

Jos tarkastelee suurempia yrityksiä ja keskisuuria organisaatioita, on näissä tarve melkein aina käyttää kaksitasoista taikka kolmitasoista mallia verkoissa, sillä niissä liikkuvan datan ja laitteiden määrä on niin suurta, ettei yksitasoinen topologia olisi mielekäs. Jos tarkastelee topologiaa Aruban Campus for midsize networks manuaalin kautta, olisi keskisuurelle organisaatiolle kaksitasoinen malli sopiva, sillä heidän mukaansa alle viidensadan käyttäjän verkoissa on normaalia käyttää verkon kaksitasoista mallia (Aruba 2019, 22), eli romahdutetun selkärankaverkon mallia. Nämä mallit ovat myös tyypillisiä yhden rakennuksen verkkotopologiaksi. Milloin siten kolmitasoista topologiaa käytetään? Kolmitasoinen topologia tulee Nefkenssin mukaan kyseeseen, kun organisaatiolla on useampi toimipaikka kytkettävänä toisiinsa, jolloin jakelutason kytkinten yhdistäminen mesh tai puolittaisella mesh-topologialla, ei ole järkevää. Sanotaan vaikka toimipaikan verkossa olevan kuusi jakelutason reititintä yhdistettynä mesh-topologialla (mikä on suositeltavaa jakelutasossa). Jos tähän verkkoon olisi yhdisteltävä toinen toimipaikka, jossa on myös kuusi jakelutason reititintä, olisi kaikkien reitittimien yhdistäminen mesh-topologialla tai osittaisella mesh-topologialla työläämpää kuin käyttää kolmitasoista ydinmallia. (Nefkens 2019, kappale 1)

4.7 Minkälaisen mallin laittaisin minkälaiselle ylitykselle.

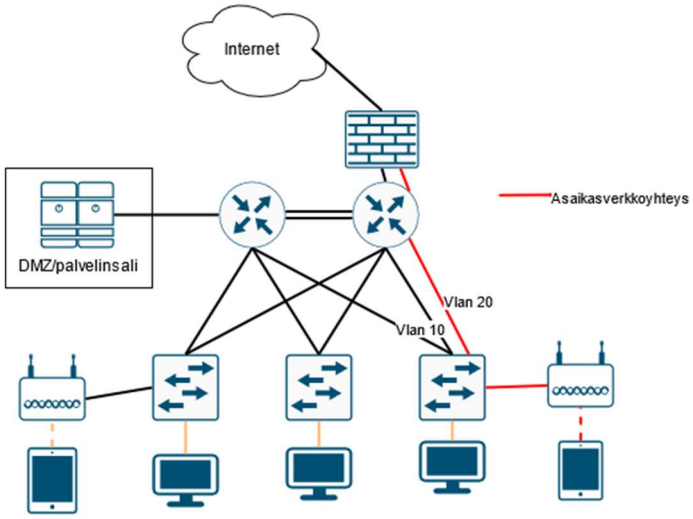
Eritasoisten valinnassa on aina otettava huomioon organisaation tarpeet ja mukaistettava sille sopivaksi. Minun mielestäni kaikissa paitsi tynkäverkoissa olisi parasta käyttää kaksi- tai kolmitasoista topologiaa. Kolmitasoisen topologian käytön raja on mielestäni osittain häilyvä. Nefkessin mukaan kolmitasoinen malli sopii tapauksiin, joissa organisaatiolla on useita toimipaikkoja yhdistettävänä, kun taas Aruban mukaan kaksitasoisen mallin raja liikkuu noin viidensadan henkilön käyttäjän rajamaissa. Näiden pohjalta suosittelisin käyttämään kolmitasoista mallia aina kun organisaation on kytkettävä useampi eri toimipaikka toisiinsa ja suurimmissa yhden toimipaikan verkoissa, joissa jakelutaso tason kytkinten yhdistäminen toisiinsa ei ole mielekästä. Käytännössä suurin osa suomalaisista yrityksistä on pieniä taikka keskisuuria yrityksiä, jolloin kaksitasoinen topologia ja yksitasoinen topologia ovat mielekkäimpiä.

4.7.1 Keskisuurelle organisaatiolle.

Riippuen organisaation tarpeista verkon topologiat ovat erilaisia ja vaihtelevat. Se sanottu, keskisuuren organisaatiolle minun mielestäni hyvä verkkotopologia näyttäytyy pääpiirteittäin seuraavanlaiselta:

- Kaksitasoinen topologia, jossa reitit on tuplattu Internetin ja lähiverkon välisistä reitittimeltä päätelaitteelle.
- Eritasoinen liikenne on eroteltu toisistaan fyysisesti taikka virtuaalisesti softan kautta, tietoturvallisuuden takia. Vierailijaliikenne on eroteltu myös muusta liikenteestä.
- Ethernet-tason silmukkakutuminen estetään joko STP-protokollan taikka kytkinten stäkkäyksen avulla.
- Tietoturvallisuus on otettu huomioon yleisesti ja eri osastot ovat segrekoitu omiin verkkoihinsa ja verkossa on myös hyvä olla DMZ-verkko hyökkäysten varalle.

Kuvaksi laitettuna se näyttää noin kuvan 15 laiselta verkolta.



Kuva 15 Esimerkkiverkko keskisuurelle yritykselle.

5 Software Defined Network (SDN)

5.1 SDN ja sen päämäärä

Software defined network (ohjelmistolla määritelty verkko) on uudehko verkon rakentamisen idea, jonka pääideana on keskittää verkon topologiatiedot ja reitin määrityksen verkossa yhdelle keskeiselle laitteelle(kontrollerille), joka tekee yksittäisten verkkopuolten laitteiden puolesta määritykset, mitä tietylle paketille on tehtävä. Tämä ajattelutapa on tullut esiin traditionaalisten verkkojen laajentuessa. Näissä verkoissa silmukoita estäviä protokollia kuten STP-protokollaa (Spanning tree protokolla) on käytetty verkon silmukkatutumisen estämiseen. SPT-protokollan konvergenssi eli tila, jossa kytkimen portit ovat lähetystilassa eikä kytkin laske parhaita reittejä, on ongelmallista. Tai no ei itse verkon konvergenssi ole ongelmallista vaan laitteen aktiivinen tila, jossa se laskee parhaita reittejä, voi olla ongelmallista, sillä tämä tila voi kestää noin 30–50 sekuntia, joka Goranssonin ym mukaan on liian suuri aika konvergenssin saamiseen, varsinkin suuren skaalan verkoissa. Esimerkiksi suurissa palvelinverkoissa, joissa tärkeää on saada data nopeasti vietyä palvelimelta toiselle, ei ole mielekästä odottaa verkon konvergoitumista. Näissä verkoissa, joissa tapahtuu paljon muutoksia verkon topologiassa, 50 sekunnin konvergoitumisaika toimisi yhtenä verkon pullonkaulana. Mutta jos yksi laite hoitaisi verkon topologian laskemisen, niin se olisi vähentämässä tuota ongelmaa. Tarkoituksena Goranssonin ja muiden mukaan SDN-verkossa on simppelöittää verkkoa (Goransson, ym, 2016 kappale 2.1.5), tuoda niiden hintaa ja kompleksisuutta alas ja mahdollistaa enemmän innovaatiota mikä SND-verkon puolestapuhujien mukaan ei ole nykytilassa ollut hyvällä tasolla. (Goransson, ym, 2016 kappale 2.3, 2.1.2, 2.1.5)

5.2 SDN-verkon pääpiirteet

Huomionarvoista on se, ettei SDN-verkko ole mikään yksi tietty verkkotopologia, vaan verkon rakennuksen idea. Tämän idean pohjalta on tehty useita SDN-ratkaisuja, jotka eroavat toisistaan. Ratkaisuja meillä on: täysin uuteen softaan perustuvia ratkaisuja (OpelFlow ym), API-pohjasia ratkaisuja ja hyperviisoripohjaisia ratkaisuja. Jotta verkkoa pystyttäisiin kutsumaan SDN-verkoksi, on sen kuitenkin seurattava viittä eri piirrettä, jotka ovat:

I. Plane seperation (tasojen separaatio).
II. Laitteiden simppelöittäminen.
III. Keskitetty kontrolli/hallinta.
IV. Verkon automatisointi/virtuaalisointi.
V. Avoimuus

Seuraavaksi käydään läpi mitä nämä piirteet tarkoittavat. (Goransson, ym, 2016 kappale 3.8)

Tasojenseparaatiolla tarkoitetaan verkkolaitteiden datan lähetysosion ja hallintaosion erittelyä eri osatoimijoille. Datanlähetysosiolla tarkoitetaan verkkolaitteille saapuvien pakettien siirtoa portista toiseen ja hallintaosiolla sitä, miten datan siirto lasketaan. Traditionaalisesti verkkolaite on hoitanut datan siirron ja itse datan laskutoimituksen, mihin data on siirrettävä, vaikkakin ne ovat loogisesti olleet erillään. SDN-verkon ideana on kuitenkin siirtää hallintataso pois kytkimeltä erilliselle hallitsijalle. (Goransson, ym, 2016 kappale 4.1.1)

Keskitetty hallinta on SDN-verkon yksi pääidea. Ideana on siirtää verkon topologiatieto, joka traditionaalisesti on ollut hajautettuina eri verkkolaitteilla, yhdelle hallittavalle keskuslaitteelle. Tämä laite hoitaa hallintatason laskelman verkon verkkolaitteiden puolesta, joka simppelöittää käytössä olevia verkkolaitteita, sillä niihin ei tarvitse lisätä hallintatason ohjelmistoa. Käytännössä tämä keskeinen hallintalaite toimii koko verkon keskeisenä päätösten tekijänä. (Goransson, ym, 2016 kappale 4.1.2)

Avoimuudella tarkoitetaan sitä, että verkon käyttöliittymien olisi oltava vapaata softaa. Tällä on haluttu ihmisten ja organisaation interaktioita SDN-käyttöliittymien kanssa, jonka tarkoituksena olisi lisätä innovointia. Mikä parantaisi verkkolaitevalmistajien laitteiden yhdessä toimimista, mikä on voinut traditionaalisesti olla ongelmana, sillä laitevalmistajien verkkostandardien implementoinnissa on voinut olla eroja. Huomionarvoista on myös se, ettei SDN ole minkään yhden laitevalmistajan taikka yrityksen luoma konsepti, vaikkakin

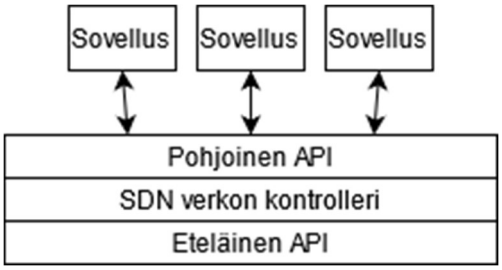
laitevalmistajilla on siihen perustuvia omilla käyttöliittymillä luotuja ratkaisuja. Ja jos katsotaan OpenFlowta, joka on ensimmäinen protokolla, joka aloitti SDN buumin, niin hallitsee sitä ONF (Open Networking Foundation) säätiö. Tämä säätiö koostuu OpenFlowsta kiinnostuneista yrityksistä kuten Google, Yahoo, Deutsche Telekom. Facebook, Microsoft ja Verizon. (Goransson, ym, 2016 kappale 3.4.2, 4.1.4)

Verkon automaatiolla ja virtualisaatiolla yleisesti tarkoitetaan verkon laitteiden ja niissä käytettävien protokollien abrstraktiointia. Abstraktioinnissa verkkoa hallitseva henkilö ei suoraan hallitse veikkolaitteistoa vaan hän hoitaa sen ohjelmiston kautta, joka piilottaa fyysisen verkkomedian ja laitteiden oman hallintaliittymän itsensä alle itse, ja hallitsijan ei tarvitse olla tietoinen niistä. SDN-verkossa kolme asiaa on haluttu abstraktioida: hajautetun tilan abastraktointi, sekä datan lähetyksen ja asetusten hallinta. Hajautetun tilan abstraktioinnilla tarkoittaa verkon näkymistä yhtenä kokonaisuutena eikä useiden latteiden kokonaisuutena, datan lähetys sitä, ettei ylläpitäjän tarvitse tietää vendiori spesifisenä CLI-komentoja halutun tilan luomiseksi, ja asetuksilla sitä, että verkon haluttu tila olisi saatava informoitua ilman spesifistä tietoa, miten verkko fyysisesti hoitaa halutun tilan luomisen (ei jargonia). (Goransson, ym, 2016 kappale 4.1.3).

Sanotaan, että verkkoa hallitaan ja verkossa halutaan estää tiettyyn IP-osoitteeseen liittyvä liikenne sen sijaan, verkossa määritellään jokaiselle laitteille komentorivissä pääsynvalvontaluettelon komennoilla:

access-list 1 deny esimerkki_IP
Interface serial0/0/0
IP access-group 1 out
IP access-group 1 in
(Ciscon IOS laitteiden syntaksi)

Verkossa määriteltäisiin verkolle halutun ”virtausmallin” ohjelmistolla keskitetysti ilman tietyn laitevalmistajan komentoja. Jolloin verkossa on abstraktoituna hajautetun tilan, laitevalmistajien komennot sekä sen, miten fyysisesti verkon muutokset toteutuvat.



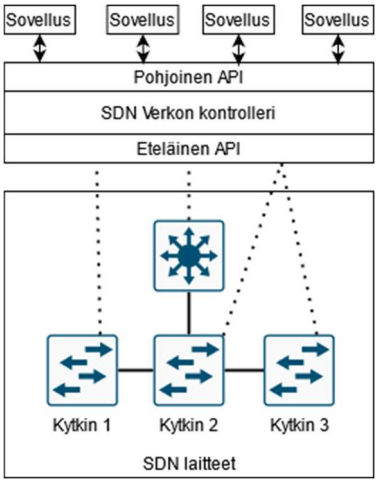
Kuva 16 verkon kontrollerin API. Mukaillen: (Goransson, ym, 2016 kappale 4.2)

Verkon automatisoinnilla tarkoitetaan verkon asetusten hallinnan automatisoinnista. Verkon asetusten automatisoinnin mahdollistaa verkon keskitetty kontrolli ja SDN-kontrollerin APIt. SDN-kontrollerin pohjoinen API on yhteydessä loppukäyttäjään toimien abstraktointiokerroksena, joka mahdollistaa eri sovellusten käytön SDN-verkon hallinnassa ja verkon hallinnan automatisaation erinäisillä skripteillä ja sovellutuksilla (kuva 16). (Goransson, ym, 2016 kappale 4.1.3)

5.3 Miten SDN verkko toimii?

Kuten jo sanottu, SDN-verkon ideana on jakaa pakettien lähetys ja niiden reittienhallinta useisiin osiin. SDN-verkossa on fyysiset verkkolaitteet(kytkimet) ja SDN-verkon hallintalaite (kontrolleri). SDN-verkossa SDN-laitteet (kytkimet), sisältävät vain (jos ei ole vanha laite) pakettien lähetystä koskevan logiikan, eli mitä paketille tehdään, ja dataa, minne paketti on lähetettävä, mitä kutsutaan flow entryksi, joista koostuu flow-taulukot. Eli SDN-laite sisältää käytännössä vain lähetystason logiikan, mutta ei hallintatason logiikkaa. Tämä hallintatason logiikka on siirretty yhdelle hallintalaitteelle, joka kontrolloi verkossa olevia laitteita ja laskee datan siirtoreitit keskitetysti. Tämä tarkoittaa sitä, että L2- ja L3-tason kytkimet ja muut SDN laiteet on oltava yhteydessä kontrolleriin, jotta ne saavat tiedon, mihin paketti on lähetettävä. (Goransson, ym, 2016 kappale 4.2)

Sanotaan verkon olevan kuvan 17 tyylinen SDN-verkko ja verkkoon kytketään kytkemässä uuden entuudestaan tuntemattoman laitteen kiinni kytkin ykköseen. Kun kytkin 1 saa tiedon uudesta paketista, katsoo se itsellään tiedossa olevat flow-taulukon. Jos kytkimellä on ohjeistus, mitä paketille on tehtävä (lähettää eteenpäin, pudottaa sen jne.), toimii se sen tavalla, mutta jos se ei löydä tiedoistaan pakettia, lähettää se sen verkon kontrollerille. Kontrolleri, jonka tehtävä on hallita verkkoa, hoitaa sen päällä toimivilla sovelluksilla/sovelluksella paketin toiminnan määrittelyn, kun se on määrittänyt, mitä paketille on tehtävä, päivittää se kytkinten flow-taulukot, jolloin kytkimet tietävät miten reagoida sentyyppisiin paketteihin tulevaisuudessa.



Kuva 17 SDN esimerkkiverkko (Goransson, ym, 2016 kappale 4.

5.4 SDN-verkon tyypit

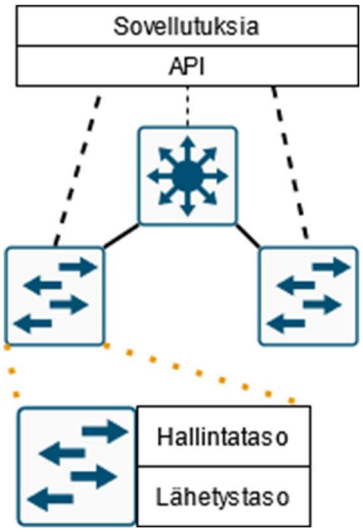
SDN kuten jo olen sanonut, SDN ei ole mikään yksi verkon topologia, vaan ennemminkin viitekehys verkon hallinnalle. Tästä syystä ei ole ihme, että SDN-tyylisen verkkoratkaisuun on myös eri keinoja, kuin Open SDN ja OpenFlow. Näitä tyyppejä on kaksi: SDN APIen kautta ja Hyperviisorin päällä olevia verkoilla (Hypervisor-Based Overlay Networks).

5.4.1 API-pohjaiset verkot

API-pohjaisilla SDN-verkoilla tarkoitetaan Goranssonin ja muiden mukaan yleisesti sitä, että SDN-tyylinen toimivuus hoidetaan verkkolaitteissa jo olevilla apeilla ja toiminnallisuuksilla. Tämäntyyppiset ratkaisut ovat usein yhden verkkolaitevalmistajan luomia ratkaisuja ja voivat sisältää verkkolaitevalmistajan patentoituja sovellutuksia APEja, jolloin ratkaisu ei toimi kuin yhden verkkolaitevalmistajan laitteilla (Goransson, ym, 2016 kappale 4.6.2). API-pohjasia ratkaisuja meillä on kolmea eri tyyppiä:

I. Laitteiden APIen kautta luodut ratkaisut
II. Kontrolleritason APIen kautta luodut ratkaisut
III. Policy tason API luodut ratkaisut

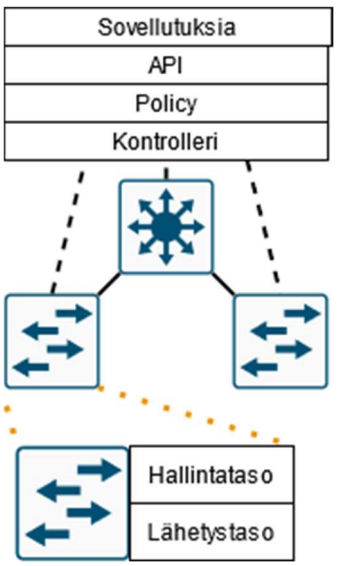
Laitteiden APIen kautta tehdyt ratkaisut perustuvat laitteissa itsessään oleviin apeihin ja toiminnallisuuksiin (kuva 18). Tässä ratkaisussa verkon hallinnoija ja sovellukset, joilla verkkoa hallinnoidaan, hallinnoivat verkkoa suoraan laitteissa olevien traditionaalisten APIen kautta ilman keskeistä kontrolleria, sillä käytettäessä verkkolaitteissa olevia APEja ei ole täysin tarpeellista käyttää kontrolleria (Goransson, ym, 2016 kappale 4.6.2). Samalla pakettien lähetystaso ja hallintatasot ovat jaettuna verkkolaitteisiin.



Kuva 18 API-pohjaiset SDN-ratkaisut. Mukaillen:
(Goransson, ym, 2016 kappale 4.6.1)

Kontrolleritason APIen kautta luodut SDN-verkot eivät eroa suuresti paljoakaan jo puhutusta ns. ”normaalista” SDN-verkon toiminnasta. Tässä mallissa verkossa on keskeinen kontrolleri, jonka kautta verkon hallinnoija ja sovellutukset pystyvät hoitamaan verkon hallinnoinnin keskitetysti. Erona ns. ”normaaliin” open SDN-verkon tyyliseen ratkaisuun on se, että kontrolleritason APIen kautta luotujen verkoissa kontrollerin eteläinen API käyttää jo käytössä olevia ns. ”perinteisiä (legacy) ohjelmia” SDN-tyyppisten toiminnallisuuksien tuottamiseen. Samalla verkkolaitteiden lähetys ja hallintatasojen erottaminen ei ole tapahtunut. Mahdollisuutena kontrolleritason APIen käytöllä on myös hallinnoida hybridiverkkoja. Esimerkiksi OpenDaylight, joka tukee useita eteläisen APIn protokollia (OpenFlow, netconf, jne), jolloin pystytään hallinnoimaan myös legacy-laitteita täysveristen SDN-laitteiden rinnalla. Tosin tämänlainen hybridiratkaisu ei kuitenkaan tarjoa kaikkia OpenFlow-kontrolleja, ja on mietittävä, onko tämänlainen ratkaisu järkevää. Mutta toisaalta se tarjoaa keinon käyttää legacy-laitteita uusien rinnalla, mikä vaikuttaa hyvältä tilapäisratkaisulta, jos organisaation kaikkia verkkolaitteita ei haluta muuttaa kokonaan SDN-laitteistoksi. (Goransson, ym, 2016 kappale 4.6.1 - 4.6.2)

Kolmas keino luoda SDN-verkolle tyypillisiä ominaisuuksia on hoitaa se policy-tasolla (kuva 19). Tässä mallissa pohjoiset APIt luodaan abstraktiokerroksen päälle, niin että ne vuorovaikuttavat policyjen yksittäisiin verkon laitteisiin taikka verkon kokonaisuuksiin (Goransson, ym, 2016 kappale 4.6.1). Policyllä tarkoitetaan deklaratiivisia lauseita, jotka kertovat mitä halutaan tehdä eikä, miten asia loppupeleissä hoidetaan.



Kuva 19 Policy tason API. Mukaillen
(Goransson, ym, 2016 kappale 4.6.1)

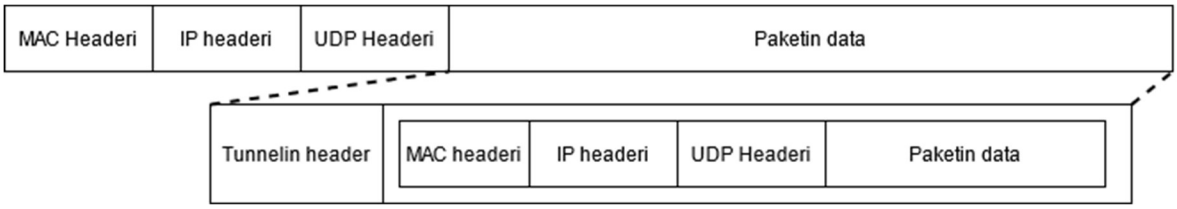
API-pohjaisissa ratkaisuissa on myös ja huonoja puolia. Nämä ratkaisut tarjoavat mahdollisuuden tehdä SND-tyylisiä ratkaisuja vanhemmilla verkkolaitteilla ilman suurta investointia uusiin OpenFlow yhteensopiviin verkkolaitteisiin (Goransson, ym, 2016 kappale 4.6.2). Tämä mahdollistaa suuremman avoimuuden, joustavuuden, automaation ja keskeisemmän verkonhallinnan ilman suuria investointeja.

Tosin on otettava huomioon, että API-pohjaisissa ratkaisuissa on myös rajoituksia. Sanotaan verkossa olevien laitteiden kautta luotu API-ratkaisu, jossa ei ole keskeistä kontrolleria, niin verkko ei saa keskeisestä hallinnasta tuovia etuja ollenkaan. On myös otettava huomioon vanhojen APIen rajallisuus, jotka voivat myös ja usein ovat yhden organisaation omia patentoituja APEja. Joissain tilanteissa vanhojen APIen käyttö ei luokaan meille halutunlaista abstraktiokerrosta, vaan on mietittävä yksittäisiä laitteita, jos halutaan muuttaa verkkon toimintaa taikka tehdä sovellutuksia pohjoisen APIn päälle. Samalla lähetys ja hallintatasot ovat vielä samalla laitteella, jolloin kontrollerin päällä olevan sovellutuksen on koordinoitava verkkolaitteessa toimivan hallinatatason kanssa, mikä ei ole ideaalia. (Goransson, ym, 2016 kappale 4.6.2)

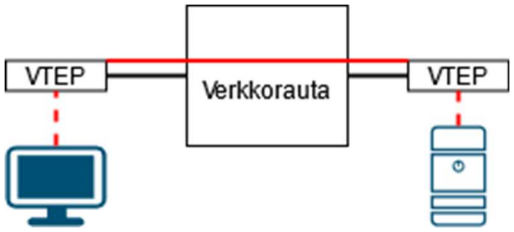
5.4.2 Hyperviisoripohjaiset virtuaaliverkot

Hyperviisoripohjaiset virtuaaliverkot ovat verkkoja, joissa fyysisen verkkomedian päälle on luotu virtuaalisia verkkoja. Näissä fyysisen verkkomedian päälle rakennetuissa verkoissa hyperviisorin tehtävänä on lähettää ja vastaanottaa verkosta liikennettä. Tämä liikenne lähetetään fyysisen verkkomedian päällä toiselle virtuaaliselle verkolle tunneloinnin avulla ilman, että fyysinen verkkokomedia havaitsee virtuaaliverkon topologia, taikka se olisi mielekästä näille laitteille (Goransson, ym, 2016 kappale 4.6.3).

Tunneloinnissa hyperviisori kapseloi virtuaaliverkossa liikkuvan paketin kokonaan toisen tietoliikennekapselin sisään (kuva 21), jolloin kapseloitu paketti pystytään lähettämään fyysisen verkkomedian päällä ilman, että sen tarvitsee ottaa kantaa virtuaaliverkon ominaisuuksiin. Nämä paketit lähetetään virtuaaliverkon päätepisteestä (VTEP) toiselle virtuaaliverkon päätepisteelle, jossa hyperviisori dekapseloi saapuneen paketin ja lähettää se sen virtuaaliverkossa olevalle päätepisteelle (kuva 20).



Kuva 21 Virtuaaliverkon pakettien kapselointi. Mukaillen: (Goransson, ym, 2016 kappale 4.6.3).



Kuva 20 Virtuaaliverkon päätepisteet ja yhteys. Mukaillen: (Goransson, ym, 2016 kappale 4.6.2).

Virtuaaliverkot softapohjaisina ratkaisuina mahdollistavat kesken verkonhallinnan ja ominaisuuksiltaan abrstraktoivat fyysisen verkkoinfrastruktuurin. Tämä mahdollistaa SDN-verkolle tyypillisiä ominaisuuksia, ja virtuaaliverkot ovat hyvin sopivia suurille datasentteriverkoille, joissa liikennettä on paljon ja palveluja on virtualisoitu ennestään (Goransson, ym, 2016 kappale 4.6.3).

Virtuaaliverkoilla ei kuitenkaan pystytä ratkaisemaan kaikkia SDN-verkkojen ratkaisemia ongelmia. Loppupeleissä virtuaaliverkot eivät ota kantaa verkon fyysiseen verkkoinfrastruktuuriin, jolloin kaikki ne ongelmat verkon hallinasta eivät muutu virtuaaliverkkoja käytettäessä. Esimerkiksi fyysinen verkkoinfrastruktuuri on vieläkin manuaalisesti hallinnoitava, ja samalla verkossa käytetään jo käytössä olevia perinteisiä ns. legacy protokollia, jolloin STP ja muiden legacy protokollien ohjelmat säilyvät (Goransson, ym, 2016 kappale 4.6.3). Kun virtuaaliverkot eivät koske fyysisiin verkkolaitteisiin, ei se myöskään insentivoi seppelöittämään verkkolaitteita, mikä on yksi SDN-verkon pääideoista.

5.5 SND-verkon tulevaisuus

SDN ideana on täysin erilainen traditionaaliseen verkkoon verrattuna. Päätavoitteena SDN-verkolla olisi luoda Goranssonin ym mukaan muuttaa verkkomaailmaa simppelimmäksi, progressiivisemmaksi (innovointimielessä), avoimemmaksi sekä tehdä laitteista tehokkaampia ja halvempia. SDN-verkon lupaukset ovat hyviä, ja mieluusti mikä tahansa organisaatio ottaisi verkkoonsa halvempia ja helpommin hallittavia verkkolaitteita, joita hallitsemaan ei tarvittaisi mahdollisesti itse tietoliikennelaitteiden asetusten konfiguroimista. (Goransson, ym, 2016 kappale 2.2.3).

SDN on kuitenkin uudehko kehittyvä idea, jonka perustuvien ratkaisuidenmaturiteetti kasvaa vielä. SDN yrittää ratkaista useita ongelmia, joita tietoverkoissa on noussut esiin kuten VLAN ehtymistä ja verkon hidasta konvergoitumisaikaa. Kuitenkin Goranssonin ym mukaan SDN-verkkoratkaisuja ei ole vielä suuria määriä otettu käyttöön. Syynä tähän on kokemattomuus SDN-ratkaisuista ja se, ettei heterogeenisiä SDN-ratkaisuja ole vielä kunnolla tehty ja luottoa SDN teknologiaan ei vielä täysin ole. Vaikka Sdi-verkko on vielä uudehko ratkaisu, on se viemässä itseään läpi. Esimerkiksi Vodafone Australian tekninen johtaja on sanonut vuonna 2014, että suuri osa heidän verkostaan tullaan virtualisoimaan viiden vuoden sisällä. (Goransson, ym, 2016 kappale 4.4.4)

5.6 SDN Verkon toiminta ja mielekkyys organisaatiolle.

SDN-verkossa, kuten traditionaalisessa verkossa, on hyviä ja huonoja puolia, eikä argumentti, jota yksi henkilö pitää hyvänä, mahdollisesti kuulosta järkevältä toiselle henkilölle. Siellä on useita eri asioita, mitä voi tarkastella arvioitaessa SDN-verkon mielekkyyttä organisaatiolle. Mitä SDN verkossa on hyvää ja mikä ei?

5.6.1 SDN-verkon tehokkuus ja kapasiteetti

SDN-verkon keskeisen kontrollin ideana on saada verkon hallinta keskitetysti yhdelle laitteelle, joka pystyy keskitetysti mukautumaan verkon topologian muutoksiin paremmin kuin nykyisen jalkautetun hallinnan verkkolaitteet pystyvät. Tehokkuus SDN-verkon kontrollerille tulee siitä, että se pystytetään palvelimelle, jolloin sillä on enemmän laskentatehoa laskea verkon reittejä. Tämä sinänsä pitää paikkansa. Nykyisellään peruskytkimet eivät ole tunnettuja niiden laskentatehosta, jos verkkolaitteiden hallintataso on laitettu yhdelle tehokkaalle laitteelle, pystyy se periaatteessa laskemaan parhaimmat reitit nopeammin verkon lävitse. Samalla, jos miettii eri verkkolaitevalmistajien tai eri verkkolaitteiden yhdessä toimimista, pitäisi siitä aiheutua vähemmän ongelmia, sillä eri laitevalmistajien laitteiden ei

tarvitse jakaa tietoa toistensa kanssa vaan yhden keskeisen laitteen kanssa, joka pystytään asettamaan tukemaan eri laitevalmistajien implementointia protokollista, taikka sitten ne voivat olla täysiverisiä avoimia SDN-laitteita, joissa ei ole eri laitevalmistajien omaa koodia pyörimässä.

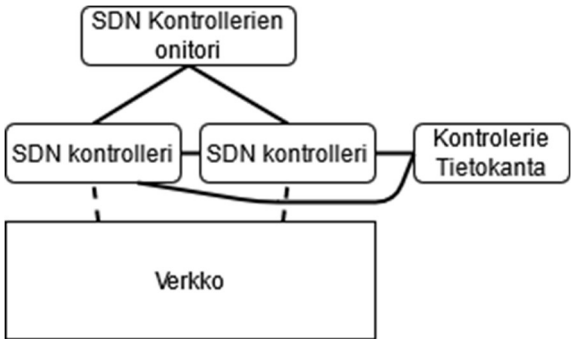
Kuitenkin jokaisella laiteella on omat laskentateholliset rajansa. Verkon kontrolleri voi sinänsä myös koitua pullonkaulaksi. Jotta SDN-tyylisestä verkkoratkaisusta olisi mitään hyötyä, olisi verkon mukautumisaika topologiamuutoksiin oltava nopeampaa kuin traditionaalisissa verkoissa. Goransonin mukaan Open SDN on nopeampi taikka vähintään yhtä nopea verkon topologiamuutoksissa kuin jalkautetut verkkolaitteet. Huolta on kuitenkin pidettävä siitä, että SDN-kontrolleri on riittävä verkon toiminnan ja mahdollisen kasvun kannalta. Kasvun kannalta kontrollerien ryhmittämiseen (usean kontrollerin toimiminen yhdessä) on mielekästä, ja vaikka OpenFlow-spesifikaatiossa ei ole vielä määritelty kontrollerien klustereita, on verkkolaitevalmistajien puolelta tullut ohjeistuksia kontrollerien ryhmittämiseen. (Goransson, ym, 2016 kappale 6.1.3)

5.6.2 Kontrolleri ja sen tietoturva

Samalla kun tarkastelee kontrolleria voi keskitetyn hallintaratkaisun miettiä tietoturvallisuuden näkökulmasta. Käyttäjäkontrolli SDN-tyylisessä kampusverkossa pystytään tekemään hyvin keskitetysti, ja se mahdollistaa ns. ”persoonallisten palomuuriasetusten” käytön verkossa. SDN-kontrollerilla pystytään hyvin määrittämään verkkoon liittyvälle käyttäjälle tietyn tason käyttöoikeudet, eli kuinka paljon hän pystyy näkemään verkossa (Goransson, ym, 2016 kappale 9.3). Kestitetyssä ratkaisussa organisaation haavoittuva hyökkäyspinta-ala vähenee, sillä organisaation verkossa ei ole suuria määriä laitteita, jotka voisivat propagoida väärää taikka muuten haitallista verkkotopologiaa. Ongelmana ei tarvitse olla vääränlaisen verkkotopologian mainostus. Ongelmaksi riittävät erheessä laitetut väärät asetukset taikka pelkkien asetusten poistaminen. Sanotaan vaikka laitteen ACL (pääsylistan) asetusten olevan pielessä, mahdollistaa se pahan toimijan propagoivan haitallista koodia eri laitteille.

Kolikon toisella puolella verkossa on yksi taikka pari loogisesti keskitettyä laitetta, jotka hoitavat verkon asetusten hallinnasta. Vaikka keskitetyssä ratkaisussa verkkotopologian haavoittuva osa pienenee, voi keskitetyt laitteet olla tietoturvariski taikka alttiita ongelmille, mikä voi sinänsä tietyissä tilanteissa koitua ongelmaksi. Jos SDN-verkko halutaan ajaa alas, tarvitsee pahantahtoisen toimijan estää kontrollerin ja verkkolaitteiden kommunikaation, joka voidaan toteuttaa esimerkiksi lähettämällä suuret määrät tietoliikennettä kontrollereille, jolloin verkko ei pystyisi mukautumaan verkossa tapahtuviin muutoksiin, joka käy-

tännössä paralysoi koko verkon toiminnan, jos siihen tapahtuu muutoksia. Myös itse verkon kontrolleri voidaan hakkeroida, jolloin paha toimija periaatteessa pystyy saamaan koko verkon hallintaansa. Samalla jos miettii mitä verkolle tapahtuu, jos verkon kontrolleri menee rikki. Jos verkossa on yksi laite vain yksi laite kontrollerina ja se hajoaa. Mitä sitten? Koko verkko on käytännössä kykenemätön toimimaan. Tästä syystä kontrollerilla ei tarkoiteta aina yhtä laitetta vaan loogisesti keskitettyä laitetta eli kontrollereita voi verkossa olla useita, jotka työskentelevän yhdessä, kuten kuvassa 22. (Goransson, ym, 2016 kappale 6.1.2)



Kuva 22 SDN redundanttisuus. Mukaillen: (Goransson, ym, 2016 kappale 6.1.2).

Se on selvää, että SDN-verkon kontrollerien ja sen ja SDN-verkkolaitteiden väliseen kommunikaation on laitettava erityistä huomiota. Kommunikaatiossa verkkolaitteiden kanssa olisi käytettävä muusta verkkoliikenteestä erotettuja reittejä. tärkeää on myös pitää kontrolleissa tiukempia tietoturva asetuksia, sekä huolehtia että redundanssisudesta. Redundanssi luodaan helposti käyttämällä useita kontrollereita, joilla on varakontrollereita, sekä pitämällä kontrollerin tietokannat ”tuplattuna”, jolloin yhden tietokannan ongelmat eivät haittaa sekä seuraamalla SDN-kontrollerien toimintaa, jolloin ongelmat saadaan korjattua nopeasti. (Goransson, ym, 2016 kappale 6.1.2)

Tietotuvallisuuden näkökulmasta yksi suurehko ongelma OpenFlow SDN-verkoilla on se, että, jotkut IDS/IPS-applikaatiot ylittävät OpenFlow-kyvykkyydet. OpenFlowlla ei ole kyvykkyyttä nähdä itse verkossa liikkuvan IP-paketin sisältöä. Tämä on ongelmallista palomuureille, joille paketin sisällön tarkasteleminen on päätösten tekemisen kannalta tarpeellista. Tosin ongelmaa voidaan kiertää siten, että SDN-kontrolleri lähettää mahdolliset ongelmalliset paketit erilliselle laitteelle, joka pystyy analysoimaan paketin dataa, ja antamaan SDN kontrollerille tarvittavat ohjeet, miten toimia. (Goransson, ym, 2016 kappale 6.1.4)

5.6.3 SDN-verkon mielekkyys

Onko SDN-verkko sitten mielekäs keskisuuren organisaatiolle? Oma kantani on kyllä, mutta ei vielä. SDN on uudehko ja kehittyvä teknologia, jossa on vielä haasteita sen maturiteetin kanssa. SDN-verkkojen kehittyessä ja kokemusten lisääntyessä SDN-verkon käyttöönottojen lisääntyessä tulevat SDN-verkot paremmaksi vaihtoehdoiksi ”keskikokoiselle” organisaatiolle.

Nykyisellään SDN-verkko on väljä ajattelutapa, miten verkko parannetaan, eikä mikään yksittäinen ratkaisu kuten OpenFlow. SDN-verkon pääideoina kuten sanottu olivat keskeinen kontrolli, avoimuus, verkon virtualisointi/automatisointi, simppelimmät verkkolaitteet ja lähetys ja hallintatason erottaminen. Tämä ajattelutapa näkyy SDN-kentässä sen heterogeenisyytenä, jossa SDN-määrittely ja sen ratkaisut vaihtelevat hyvin paljon ratkaisusta ratkaisuun. Kun SDN-ratkaisuja on monia erilaisia, organisaatiolle, jolla ei ole suurta määrää resursseja eri ratkaisujen tutkailemiseen, voi mielestäni olla haastavaa valita ja rakentaa organisaatiolle suotuisa ratkaisu. Organisaatiolla on valittavana avoimen lähdekoodin OpenFlowta, useita API-pohjaisia ratkaisuja ja virtuaaliverkkoja. Mutta mikä näistä sitten olisi organisaatiolle se paras ratkaisu? Samalla kyseeseen tulee miettiä, miten valittu ratkaisu on tuettu yleisesti ja varsinkin, miten organisaation jo käytössä olevat laitteet tukevat valittua ratkaisua. Esimerkiksi yksi maailman suurin verkkolaitevalmistaja Cisco tukee vapaan lähdekoodin OpenDaylight-projektia, mutta he markkinoivat hyvin paljon omiin patentoituihin protokolliinsa nojaavaa API-pohjaista SDN-ratkaisua. Luontaisesti tässä tulee mieleen kysyä, minkälainen sitoutuminen heillä on vapaan lähdekoodin SDN-ratkaisun kehittämiseen, jos heillä on omaan lähdekoodiin perustuva ratkaisu. Periaatteessa Ciscolle taikka muulle laitevalmistajalle olisi parempi pitää asiakkaat kiinni omassa ekosysteemissään ja maksimoida voitot sen kautta. Minä en kuitenkaan nyt syytä Ciscoa siitä, etteivätkö he vakavissaan tukisi OpenDaylight-projektia, vaan pointtina on se, että verkkolaitevalmistajalla on omia intressejä esimerkiksi pitää asiakkaat kiinni omassa ekosysteemissä (API-pohjainen SDN-ratkaisu), jolloin kaikki SDN-verkon ajattelutavan aksiomit eivät toteudu taikka ne toteutuvat osittain. Tällöin voi miettiä, oliko SDN-verkkoratkaisun rakentamiseen käytetty investointi järkevää, jos ratkaisu ei tuotakaan taikka tuottaa vähemmän haluttuja hyötyjä. Eli käytännössä, ovatko uuden ratkaisun investointikulut suuremmat kuin operaationallisissa kuluissa tulevat säästöt ja siitä saatavat muut hyödyt.

Jos tarkastelee SDN-verkkoa verkkolaitteiden ja verkon yleisen tietoturvan kannalta, traditionaalinen kampusverkko ja SDN-verkko näyttäytyvät minulle tilanteena, jossa organisaatio juo kuvainnollista myrkkyä kumman verkkomallin se valitseekaan. Se ei tietenkään tarkoita, että kuvainnolliset myrkyt olisivat samanarvoisia. Minun mielestäni hyvin suunnitellun SDN-verkon keskitetyllä ratkaisulla on potentiaalia olla parempi ratkaisu kuin traditionaalisella verkkoratkaisulla, jossa hallintataso on jaettu.

SDN-verkossa kuten jo sanottu voi olla ongelmia, mahdollisen kapasiteetin tietoturvan ja redundanssisuuden kanssa, jotka johtavat juurensa yhden loogisen laitteen käytöstä. Kuitenkin minä argumentoisin sitä, että hyvin suunnitellulla SDN-verkkoratkaisulla yhden loogisen (ei yhden fyysisen laitteen) laitteen käyttö ei ole ongelma. Jos verkossa olevilla kontrollereilla on varakontrollerit, niiden tietoturvallisuudesta pidetään huolta sekä kapasiteettiasiat ovat kunnossa, niin mielestäni SDN olisi parempi ratkaisu kuin traditionaalinen verkkoratkaisu. Verrattuna traditionaalisen verkkoratkaisuun SDN verkossa pienennetään haavoittuvaa verkkopinta-alaa ja saadaan helpommin hallinnoitavan ratkaisu. Esimerkiksi verkkolaitteiden hallinnassa ei tarvitse jokaiselle verkkolaitteelle erikseen määrittä ACL-päivitystä, vaan se voidaan hoitaa helposti koko verkolle verkon kontrollerilla, joka säästää verkon hallinnoijan aikaa ja organisaation resursseja.

Kuitenkin SDN-verkkoratkaisu on uudehko ja vielä kehittyvää teknologiaa, jossa on vielä kehitettävää. Vaikka se on mahdollisesti traditionaalista parempi ratkaisu, haluaisin minä pariin tietoturvallisuuteen liittyvän kohdan paremmin määritellyksi. Paremmin määritellyksi minä haluaisin kontrollerien ryhmittämiseen, sekä IP-pakettien sisällön tarkemman tarkastelun. Tämä siitä syystä, että se ei ole mielekästä millekään organisaatiolle laittaa verkkoon pystyyn yhtä kontrolleria, joka rikkoutuessaan aiheuttaa verkon hajoamisen, mikä on ongelma varsinkin OpenFlow-pohjaisille ja muille SDN ratkaisulle, joissa kontrolleri on käytössä SDN-ratkaisuille, jossa kontrollerien ryhmittämistä ei ole vielä naiivisti määritelty (Goransson, ym, 2016 kappale 6.1.3). Sekin myös, ettei esim. OpenFlowssa pystytä kunnolla käyttämään tarkempia IDS IPS-järjestelmiä on ongelmallista tietoturvallisuuden kannalta, varsinkin verkoissa, joissa liikkuu tietoa, joka on erittäin salaista. Kun näihin kohtiin saadaan selvennystä, niin voin sanoa, että SDN-verkko on parempi ratkaisu kuin traditionaalinen kampusverkko, jossa lähetys ja hallintatasot ovat jokaisella verkkolaitteella.

6 Yhteenveto

6.1 Yleisesti

Tarkoituksena minulla oli käsitellä yritysverkoissa käytettyjä reititysprotokollia, verkkotopologioita ja esittää hyvä verkkotopologia/ratkaisu keskisuurelle organisaatiolle. Käsittelyssä minulla oli reititysprotokollista käytetyimmät (EIGRP; IS-IS, OSPF, BGB ja staattinen reititys) sekä verkkoratkaisuista kampusverkot ja SDN. Loppupeleissä hyvä verkkoratakisu/topologia on hyvin tapauskohtainen, ja verkkoratkaisu/topologia joka toimii yhdelle organisaatiolle, ei toimi toiselle. Samalla ilman kohdeyritystä, jonka tarpeiden ja tilanteen pohjalta asiaa tulisi käsitellä, jää hyvän verkkoratkaisun käsittely hyvin yleisluontoiselle pohjalle, mikä sinänsä ei ole kaikkein ideaalein tilanne. Ja samalla kaikki päätelmät/ajatukset eivät saata sopia jokaiselle organisaatiolle.

Prosessina työn tekeminen oli pitkähkö ja ajallisesti pidempi kuin alun perin suunniteltu. Tähän vaikuttavia asioita oli työn laajuus, jota olisi mahdollisesti voinut rajoitta selkeämmin. Yleisesti aikaa meni enemmän pieniin toimenpiteisiin kuten tekstin kieliasun tarkastamiseen jne. Pääasiallisesti suurimman osan fokuksesta itsellä oli aineistojen lukemisessa ja tekstin kirjoittamisessa niiden pohjalta ja aihe fokuksena reititysprotokollat ja verkkotopologia.

Tietyt asiat kuten kampusverkot ja reititysprotokollat olivat itselle, jossakin määrin ennestään tuttuja, SDN ei oikeastaan, mutta loppupeleissä valitsemieni aiheiden tarkempi käsittely ja niistä selvää ottaminen vie/vei hyvin aikaa. Mutta se on tärkeä ymmärtää ja osata käsitellä näitä asioita, jos on kiinnostunut verkkopuolen hommista, niiden merkittävyyden takia. Ja ovathan nämä asiat ihan mielenkiintoisia. varsinkin verkkolaitteiden hallinnassa näkee suoraan oman työnsä jäljen.

6.2 Pohdintaa

Reititysprotokollien vaikutus verkkoratakisuun on sinänsä pienehköä loppupeleissä. Käsiteltyjen sisäisten reititysprotokollien erot ovat sinänsä pienehköjä, ja kaikissa protokollissa tärkeät asiat kuten verkon silmukoiden ehkäisy on määritelty ja toteutettu. Suurin ero sisäisessä reitityksessä on se, että EGRP protokolla käytettäessä organisaatio sitoutuu käyttämään vain Ciscon laitteita, vaikka EIGRP protokolla on heidän tasoltansa julkaistu avoimena standardina. Se mikä tulee ulkoiseen reititykseen, on se, että ulkoisessa reitityksessä BGB on standardi. Eli käytännössä organisaation verkon sisällä käytössä IS-IS,

OSPF taikka EIGRP, jota tukee staattiset määritykset, ja sisäverkon ulkopuolisessa reitityksessä BGP.

Kampusverkoissa verkkorakenne on, joko kolmitasoinen, kaksitasoinen, taikka yksitasoinen. Yleisesti verkojen topologia vaihtelee koon ja kompleksisuuden tarpeen mukaan. Verkoissa, joissa ei ole paljoa käyttäjiä voi madollisesti käyttää yksitasoista topologiaa ja suurimmat verkot, joissa käyttäjiä on paljon käyttävät kolmitaosta taikka kaksitoista topologiaa. Verkon kompleksisuteen ja topologiaan vaikuttavat myös paljon myös muut verkon tarpeet, kun sen koko, tietoturvallisuus (verkkojen erittely) redundanssisuuden luominen, käytetäänkö tuplattuja yhteyksiä, onko jakelutasolla mesh topologiaa, onko pääsytasolla spannig tree protokolla käytössä. Kaikki tämä vaikutta verkon topologiaan ja ratkaisuun, yleisesti keskisuuren organisaation näkökulmasta kaksitasoinen topologia näyttäisi mielleäimältä.

SDN verkko on uusi idea veikkoratkaisun luomiseen minkä ideana on muuttaa verkon rakennetta siirtämällä osa verkkolaitteissa tapahtumista tehtävistä keskeiselle kontrollerille, joka hoitaisi ne tehtävät tehokkaammin parantaen verkon tehokkuutta ja mahdollistaen verkon abstraktivoinnin. SDN ei ole kuitenkaan yksi homogeeninen idea taikka ratkaisu vaan pikemminkin ajattelusuunta, siihen miten verkko tulisi rakentaa. Tästä johtuen SDN verkkotyyppejä on useita ja SDN verkoista varttumattomalle SDN verkon valinta voi ehkä vaikuttaa pikkaisen sekavalta. Samalla SDN on vielä uudehko idea ja kehittyvä idea, joka ei ehkä vielä ole sopiva kaikille organisaatiolle. SDN verkot kehittyvät kuitenkin vielä ja mahdollisesti tulevaisuudessa ohittavat traditionaaliset kampusverkot tietoverkkojen standardina. Tosin nykyään SDN verkkoja ei ole yhtä paljon käytössä, kun traditionaalisia kampusverkkoja, mutta SDN verkkojen kehittyessä niiden prosentti verkoista lisääntyvät. Onko SDN verkko parempi kuin traditionaalinen kampusverkko? Sitä on vaikea sanoa, kummassakin verkossa kuten jo käsitelty on ongelmia, mutta SDN verkko on uudempi idea, jossa mahdollisesti on enemmän potentiaalia.

Lähteet

AAIB 1989: Report on the Convair 340/580 LN-PAA aircraft accident North of Hirtshals, Denmark on September 8 Luettavissa: https://reports.aviation-safety.net/1989/19890908-0_CVLT_LN-PAA.pdf Luettu: 27.8. 2021

Andrea Mauro. 2019. Stacking Network Switches: Why and Why Not. Luettavissa: https://blogs.arubanetworks.com/solutions/stacking-network-switches-why-and-why-not/. Luettu: 27.5.2021

AWS. What is Amazon VPC? Luettavissa: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html Luettu: 5.6.2021

Aruba 2019. Aruba campus for midsize networks Design & Deployment Guide. Saatavissa: https://www.arubanetworks.com/assets/tg/AVD_Midsize-Campus-Design-Deploy.pdf. Luettu: 20.4.2021

CCNA 2021 TCP three-way handshake Luettavissa: https://study-ccna.com/tcp-three-way-handshake/ Luettu: 16.11.2021

CISA. 2018. Security Tip (ST18-001). Luettavissa: https://us-cert.cisa.gov/ncas/tips/ST18-001 Luettu: 6.5.2020

Cisco press 2014. Routing protocols companion guide. Cisco press. Luettavissa: https://learning.oreilly.com/library/view/routing-protocols-companion/9780133476309/?ar= Luettu: 20.3.2021.

Cisco Systems Inc. 2020. Annual Internet Report (2018–2023) White Paper https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Luettu: 30.5.2020

Cisco Systems Inc, 2020. Campus LAN and Wireless LAN Solution Design Guide Luettavissa: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.pdf Luettu: 20.3.2021

Cisco Systems Inc.2005.Introduction to EIGRP. Saatavissa: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html Luettu: 16.3.2021

Cisco Systems Inc. Introduction to Networks. Luettavissa: https://contenthub.netacad.com/legacy/CCNA/ITN/6.0/en/index.html. Luettu: 4.3.2021

Deepankar, M. & Karthikeyan, R. 2018. Network Routing: Algorithms, Protocols, and Architectures Second edition. Morgan Kaufmann. Luettavissa: https://ebookcentral.proquest.com/lib/haaga/detail.action?docID=5042250 Luettu: 27.3.2021

Goransson, P.& Black, C. &Culver, 2017 Software Defined Networks: A Comprehensive Approach. Morgan Kaufmann. Luettavissa: https://learning.oreilly.com/library/view/software-defined-networks/9780128045794/?ar. Luettu: 10.5.2021

Huawei. 2019. S2700, S3700, S5700, S6700, S7700, and S9700 Series Switches Interoperation and Replacement Guide Luettavissa: https://support.huawei.com/enterprise/en/doc/EDOC1000114005/40432f23/ospf-and-eigrp-interoperation-and-replacement-solution Luettu: 24.4.2021

IBM. General Terms. Luettavissa: https://www.ibm.com/docs/en/zos/2.1.0?topic=terminology-general-terms Luettu: 28.5.2021

Microsoft Azure https://azure.microsoft.com/en-us/overview/what-is-the-cloud/ Luettu: 1.6.2021

Nefkens, P. 2019. Transforming campus networks to intent-based networking. Cisco Press. Luettavissa: https://learning.oreilly.com/library/view/transforming-campus-networks/9780135466254/?ar Luettu: 20.4.2021

Richard Stevens. W. & R. Fall, K. 2011 TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley Professional. Luettavissa: https://learning.oreilly.com/library/view/tcpip-illustrated-volume/9780132808200/?ar. Luettu: 20.4.2021

Tilastokeskus käsitteet 2021PK-yritys: Luettavissa: http://www.stat.fi/meta/kas/pk_yritys.html Luettu: 19.4.2021

Zhang, R; Alcaide, J; Bartell, M; Looney, J; Suazo, V. 2016.
BGP Design and Implementation. Cisco press. Luettavissa:
https://learning.oreilly.com/library/view/bgp-design-and/9781587058646/ Luettu:
20.5.2021