Jouni Nevalainen

YLÄTASON LABORATORIOVERKKO-SUUNNITELMA UUDELLE KAMPUKSELLE

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Tieto- ja viestintätekniikka

2022

Kaakkois-Suomen ammattikorkeakoulu

South-Eastern Finland
University of Applied Sciences

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Jouni Nevalainen
Työn nimi	Ylätason laboratorioverkkosuunnitelma uudelle kampukselle
Toimeksiantaja	Xamk
Vuosi	2022
Sivut	38 sivua, liitteitä 0 sivua
Työn ohjaaja(t)	Jaakko Nurmi

TIIVISTELMÄ

Opinnäytetyön aiheena oli luoda ylätason suunnitelma laboratorioverkosta Kaakkois-Suomen ammattikorkeakoulun (Xamk) valmistuvalle Kotkan kampukselle. Työn tarkoituksena oli vertailla erilaisia datakeskusverkon arkkitehtonisia ratkaisuja, niissä käytettyjä protokollia sekä valita Xamkin käyttötarkoituksiin parhain ratkaisu.

Tutkimusongelmana opinnäytetyössä on selvittää Xamkin nykyisen laboratorioverkon tilalle käytännöllisempi ratkaisu, sillä tämän hetken laboratorioverkko ei vastaa nykypäivän modernin verkon ja lisääntyneen datankäytön vaatimuksia. Tutkimusmenetelmänä on toiminnallinen opinnäytetyö, joka perustuu työelämälähtöiseen toimeksiantoon.

Teoriaosuus käsittelee verkon suunnittelun kannalta oleellisia asioita, kuten tarvittavia alus- ja päällysverkkoprotokollia ja arkkitehtuurillisia vaihtoehtoja, sekä niiden vertailua. Teoriaosuudessa perehdytään myös ohjelmoitavan verkon tuomiin etuihin. Käytännön osuus puolestaan käsittää erään toimivan verkkoratkaisun testauksen sekä jatkokehitysideoita turvallisuuden sekä dataliikenteen rajauksen parantamiseksi.

Lopputuloksena opinnäytetyössä on ylätason suunnitelma laboratorioverkosta Xamkille sekä vankka teoriapohja verkon suunnitteluun, jota voidaan jatkokehittää kampuksen tulevia tarpeita varten.

Asiasanat: päällysverkko, alusverkko, datakeskus, verkkoarkkitehtuuri

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Jouni Nevalainen
Thesis title	Top-level laboratory network plan for a new campus
Commissioned by	Xamk
Time	2022
Pages	38 pages
Supervisor	Jaakko Nurmi

ABSTRACT

The topic of the thesis was to create top-level laboratory network plan to the Kotka's new campus. The purpose of the work was to compare data center architectural solutions, protocols used in them and to choose the best solution for Xamk's intended use.

The research problem in the thesis is to find out a more practical solution to replace Xamk's current laboratory network, as it does not meet the requirements of today's modern network and increased data usage. The research method is a functional thesis, which is based on a work-based assignment.

The theoretical part deals with issues relevant to network design, such as overlay and underlay protocols and architectural options, as well as their comparison. The theoretical part also examines the benefits of a software-defined network. The practical part, in turn, involves testing a working network solution, and ideas for further development to improve security as well as the restriction of data traffic.

The result of the thesis is a solid theoretical basis for network design and a top-level plan for the laboratory network for Xamk, which can be further developed according to campus needs.

Keywords: overlay, underlay, datacenter, network architecture

SISÄLLYSLUETTELO

1 JOHDANTO 6
2 TUTKIMUSASETELMA 7
2.1 Tutkimusongelma 7
2.2 Tutkimusmenetelmä 7
2.3 Tavoitteet ja toimeksiantaja 8
2.4 Aiheen rajaus 8
3 DATAKESKUS 9
3.1 Kolmen tason arkkitehtuuri 10
3.2 Spine-leaf 11
3.3 Fat-Tree 12
3.4 Arkkitehtuurien vertailu 13
3.5 Layer 2 ja layer 3 14
3.6 Control plane ja data plane 15
4 PÄÄLLYSVERKKO 16
4.1 Virtual Extensible Local Area Network eli VXLAN 17
4.2 Network Virtualization Using Generic Routing Encapsulation eli NVGRE 19
5 ALUSVERKKO 21
5.1 Open Shortest Path First eli OSPF 22
5.2 Intermediate System to Intermediate System eli IS-IS 23
5.3 Border Gateway Protocol eli BGP 25
6 OHJELMOITAVA VERKKO 27
7 TYÖN TOTEUTUS JA TOPOLOGIA 28
7.1 Ensimmäinen vaihe 29
7.2 IS-IS-VXLAN-HER 30
7.3 Laitteisto 32
8 TULOKSET 33
9 JOHTOPÄÄTÖS 33

9.1 Pohdinta 34
9.2 Jatkokehitys 34
LÄHTEET 36

1 JOHDANTO

Maailman vuosittain kasvava datankäyttö, lisääntyneet tarpeet palveluille sekä esineiden internetin (eng. Internet of Things, IOT) kasvu ovat tuoneet datakeskusten suunnitteluun uusia haasteita. Datakeskusten tulee kyetä tarjoamaan suoritus- ja laskentatehoa, nopeutta sekä korkeaa saatavuutta (eng. high availability). Lisäksi datakeskusten itsessään tulee olla helposti skaalautuvia ja nykyistä enemmän automatisoituja. (Ganesh 2021, 4.)

Uuden sukupolven datakeskus huomioi nykypäivän vaatimukset ja sen voidaan kuvata koostuvan seuraavista aspekteista (IBM 2016, 2–5.):

1. Ohjelmoitava ympäristö, joka muuttaa ihmisen hallinnoiman verkon automatisoiduksi, viisaasti resursseja käyttäväksi ympäristöksi ilman järjestelmänvalvojan päätöksiä.
2. Jatkuvasti käytettävissä oleva ympäristö, joka kestää komponenttien vioista ja huoltotoimenpiteistä huolimatta.
3. Kognitiivinen laskentaympäristö, jossa järjestelmät voivat oppia ja ratkaista liiketoiminnan ongelmia edistyneen analytiikan avulla.
4. Globaalisti hallittu ekosysteemi, joka tarjoaa yhtenäisen hallinnan yhden pisteen kautta.

On-premise viittaa yrityksen fyysisesti omistamaan ja sen hallinnoimaan datakeskukseen, jonka ylläpidosta yrityksen IT-henkilöstö on vastuussa. Tämän kaltaisessa datakeskuksessa on huomioitava, että kiristyshaittaohjelmien jatkuva kasvu ajaa yrityksen toiminnan kohti *Zero Trust* – luottamattomuuden periaate -mallia. Tärkeä huomio kasvavista trendeistä datakeskuksissa on pilvitekniikan yleistyminen. Monet yritykset haluavat tuoda pilviympäristöjen tarjoamat mahdollisuudet on-premise-datakeskuksiin. (Earls 2022.)

Isoin muutos datakeskuksissa lähivuosina on, että organisaatiot alkavat miettiä infrastruktuurivaatimuksiaan työkuormituksensa suhteen. Koska suuri osa työkuormista muuttuu on-premise-pohjaiseksi lähitulevaisuudessa, organisaatioiden on modernisoitava infrastruktuurinsa, jotta se kykenee käsittelemään nykyaikaisia tieto- ja työkuormitusvaatimuksia kasvaneista toimitusketjun ja sirupulan ongelmista huolimatta. Julkisen pilven käyttöönotto tulee jatkamaan

kasvuaan tulevaisuudessa, joten organisaatioiden tulisi investoida asianmukaiseen verkkoinfrastruktuuriin varautuakseen hybridityökuormiin. (Earls 2022.)

2 TUTKIMUSASETELMA

2.1 Tutkimusongelma

Nykyinen Kotkan kampuksen verkko ei täytä kriteerejä ohjelmoitavuuden tai hallittavuuden osalta uutta kampusta varten. Tutkimusongelmana oli selvittää, miten uudesta verkosta saadaan luotua keskitetysti hallittu sekä ilman sidonnaisuuksia tiettyyn laitevalmistajaan tai lisenssiin, ja kuinka ohjelmoitavuus on implementoitavissa. Lisäksi käytettävien laitteiden kustannuslaskelmat ja niiden vertailu olivat osana tutkimusongelmaa.
Opinnäytetyön tutkimuskysymyksiä ovat

1. Mitä arkkitehtuuria nykypäivän verkkototeutuksille on olemassa?
2. Minkälaisia etuja / haittoja kussakin ratkaisussa on?
3. Mikä verkkoratkaisuista soveltuisi parhaiten kampusverkon toteuttamiseksi?

Opinnäytetyö on jaettu kahteen osaan. Ensimmäinen osa käsittelee työn tutkimusongelmaa ja teoriaosuutta. Teoriaosuudessa pyritään avaamaan lukijalle prosessi, joka vaaditaan onnistuneen laboratorioverkkoympäristön toteuttamiseen. Toinen osa koostuu käytännön osuudesta, jossa teoriapohjaa hyödynnetään virtuaalisessa ympäristössä testaustarkoitukseen. Virtuaalisena testausympäristönä toimii Xamkin VirtualLab, jonka avulla on mahdollista muun muassa emuloida verkkolaitteita.

2.2 Tutkimusmenetelmä

Tutkimusmenetelmänä on toiminnallinen opinnäytetyö. Toiminnallinen opinnäytetyö perustuu työelämälähtöiseen toimeksiantoon. Siinä tuotetaan tuotos tai tuloksia sekä kehittämisehdotuksia toimeksiantajalle. Lisäksi opinnäytetyön tulee täyttää opinnäytetyölle asetetut kriteerit ja se on osoitus opiskelijan asiantuntijuudesta ja korkeakoulutasoisesta osaamisesta. (Jyväskylän Ammattikorkeakoulu 2021.)

Tutkimuskirjallisuutena käytetään internetin tieteellisiä julkaisuja, alan kirjallisuutta sekä artikkeleita. Näiden pohjalta saatua tietoa voidaan hyödyntää käytännön osuudessa testaamisen kautta ja selvittää Xamkin uuden kampuksen tarpeita vastaava verkko. Koska verkon toteuttamiseen on lukematon määrä eri vaihtoehtoja, opinnäytetyössä rajataan käytettyjä tekniikoita yleisesti suosituimpiin ratkaisuihin ja valitaan niistä paras kokonaisuus.

2.3 Tavoitteet ja toimeksiantaja

Opinnäytetyön aiheena on luoda suunnitelma laboratorioverkosta Kaakkois-Suomen ammattikorkeakoulun uudelle, Kotkan kampukselle. Ajatus työhön tuli korkeakoululta. Tavoitteena on suunnitella ylätasolla ohjelmoitava verkko, joka mahdollistaa verkon ohjelmoitavuuden sekä tiettyjen aspektien hallittavuuden keskitetysti, ilman mittavia konfiguraatiomääriä. Tämä poistaa järjestelmänvalvojalta ison määrän työkuormaa tulevaisuudessa, jos verkkoon tehdään muutoksia.

Ohjelmistot valitaan siltä pohjalta, että ne ovat avointa lähdekoodia ja näin ollen muokattavissa ja käytettävissä ilman lisenssimaksuja. Laitevalmistajan valinnan osalta tärkeimpinä näkökulmina on muun muassa hinta sekä sidonnaisuus kyseiseen valmistajaan. Lähtökohtaisesti sidoksisuus yhteen valmistajaan sekä ainoastaan heidän tuotteisiinsa ei ole optimitilanne verkon laajennuksia ajatellen. Opinnäytetyön tilaajalle luodaan ylätason ehdotus uuden kampuksen ICTLAB:n ympäristön verkon arkkitehtuurista ja siihen vaadittavista ratkaisuista.

Työ on toteutettu Kaakkois-Suomen ammattikorkeakoulu Xamkille. Korkeakoulun kampukset sijaitsevat Mikkelissä, Savonlinnassa, Kouvolassa ja Kotkassa. Tarjolla on lähes 50 AMK- tutkintokoulutusta ja yli 30 YAMK-koulutusta. Vuonna 2021 Xamkilla oli 10 872 tutkinto-opiskelijaa. (Kaakkois-Suomen ammattikorkeakoulu 2021.)

2.4 Aiheen rajaus

Laboratorioverkosta tehdään ylätason suunnitelma, jossa käydään läpi sopivin ratkaisu päällys- ja alusverkkoprotokolliksi parhaimpaan arkkitehtoniseen verkkoratkaisuun. Laboratorioverkon suunnitelma on rajattu opinnäytetyössä

sen tietotekniseen osuuteen. Työssä ei oteta kantaa fyysisiin ratkaisuihin, kuten laitteiden sijoitteluun, kaapelointeihin tai sähkötöihin.

Lisäksi työ keskittyy enemmän datakeskusverkon suunnitelmaan ja sen verkkoratkaisuihin niiden ollessa suurempi sekä monimutkaisempi kokonaisuus työstä. Työasemaverkon liittäminen datakeskusverkkoon voidaan toteuttaa sopivimpaan ratkaisuun.

3 DATAKESKUS

Datakeskus on laitos, joka keskittää organisaation yhteiset IT-toiminnot ja -laitteet tietojen ja sovellusten tallentamista, käsittelyä ja levittämistä varten. Koska datakeskukset sisältävät organisaation kriittisimmät ja ominaisimmat omaisuudet, ne ovat elintärkeitä päivittäisen toiminnan jatkuvuuden kannalta. Tästä syystä datakeskusten ja niiden tietojen turvallisuus ja luotettavuus ovat jokaisen organisaation tärkeimpiä prioriteetteja. (Geng 2015, 4–5.)

Virtualisointi on tapa käyttää useita itsenäisiä virtuaalisia käyttöjärjestelmiä yhdessä fyysisessä järjestelmässä. Se on tapa sallia sama määrä prosessointitehoa harvemmilla palvelimilla lisäämällä palvelimen käyttöastetta. Sen sijaan että virtualisointi käyttäisi monia palvelimia alhaisella prosessorin käyttöasteella, se yhdistää prosessointitehon harvemmille palvelimille, jotka toimivat korkeammalla käyttöasteella. (Geng 2015, 5.)

Ohjelmoitava datakeskus (eng. Software Defined Data Center, SDDC) on arkkitehtoninen lähestymistapa, jossa koko ICT-infrastruktuuri (palvelimet, tallennustila, verkot ja turvallisuus) on virtualisoitu laitteistosta riippumattoman hallintajärjestelmän kautta. SDDC kykenee parantamaan ympäristön toimivuutta optimoimalla tallennustilan, laskentatehon sekä tietoverkon hallittavuuden jokaiselle sovellukselle tai työkuormalle ilman fyysisiä muutoksia infrastruktuuriin, samalla vähentäen riskejä sekä kustannuksia. Virtuaalikoneet voidaan ottaa käyttöön muutamassa minuutissa vähäisellä ihmisen osallistumisella. (Geng 2015, 5–6.)

Datakeskusarkkitehtuurilla kuvataan resurssien ja laitteiden fyysistä sekä loogista asettelua datakeskuksessa, joka toimii mallina suunnittelussa ja käyttöönotossa. Se on kerrostettu prosessi, joka tarjoaa arkkitehtonisia ohjeita datakeskusten kehittäjille. (Techopedia s.a.)

3.1 Kolmen tason arkkitehtuuri

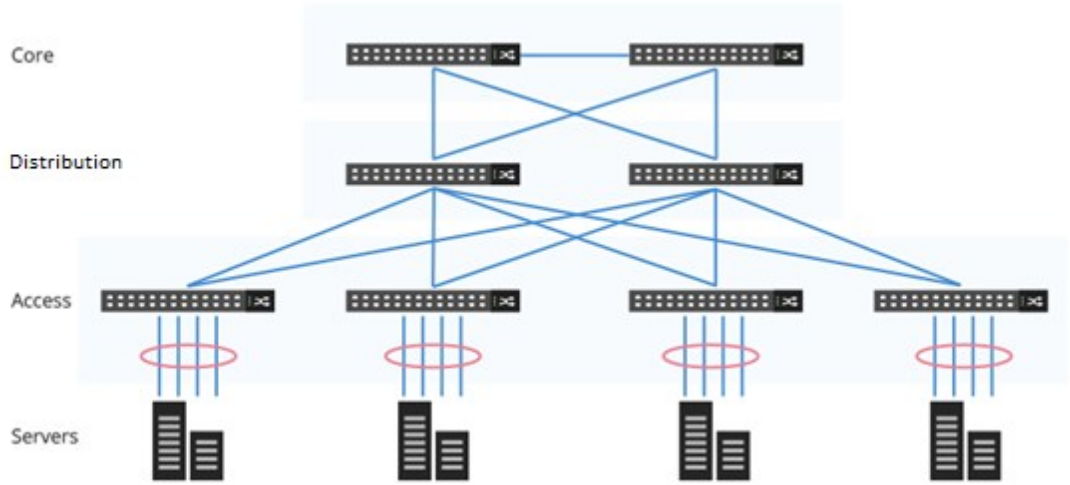
Kuvassa 1 kuvattu perinteinen datakeskusverkko hyödyntää kolmen tason arkkitehtuuria (eng. three-tier architecture), joka koostuu laitteiden muodostamasta runko-, jakelu- sekä pääsykerroksista. Runkokerros on tietoverkon selkäranka, joka siirtää nopeasti suuria määriä paketteja verkon jakelukerrokselle. (Azam s.a.)

Rungon täytyy olla luotettava, redundanttinen, sekä linkkien välillä on oltava kuormantasausta. Sen on siis sovelluttava nopeasti muutoksiin ja säilytettävä toimintakykynsä. On myös huomioitavaa, että runkokerroksen laitteet eivät suorita minkäänlaista paketin tarkastusta, joka hidastaisi sen toimintaa. (Azam s.a.)

Jakelukerros eli hierarkian keskimmäinen kerros erottaa runko- ja pääsykerroksen toisistaan. Sen tehtävänä on ottaa data runkokerrokselta, identifioida se ja siirtää oikealle pääsykerroksen laitteelle. Pääsykerroksen avulla loppukäyttäjät pääsevät verkkoon. Tämä kerros yhdistää verkkoon myös käyttäjälaitteet, kuten tietokoneet, IP-puhelimet, langattomat tukiasemat, tulostimet ja skannerit. (Versitron s.a.)

Kolmen tason datakeskusverkot olivat aiemmin yleisesti suosittuja datakeskusten suunnittelussa. Toimivuus oli hyvä, kun suuri osa tietoliikenteestä oli ns. north-south-suuntaista (datakeskuksen ulkoa sisään tulevaa), tai päinvastoin. Ongelma tämän tyyppisessä mallissa on nykypäivän huomattavasti li-

sääntynyt liikenne datakeskuksen sisällä (east-west / palvelimelta palvelimelle). Ratkaisuna datakeskuksissa on alettu käyttämään muun muassa spine-leaf-arkkitehtuuria. (Sheldon & Younger 2022.)



Kuva 1. Kolmen tason arkkitehtuuri (FS 2021)

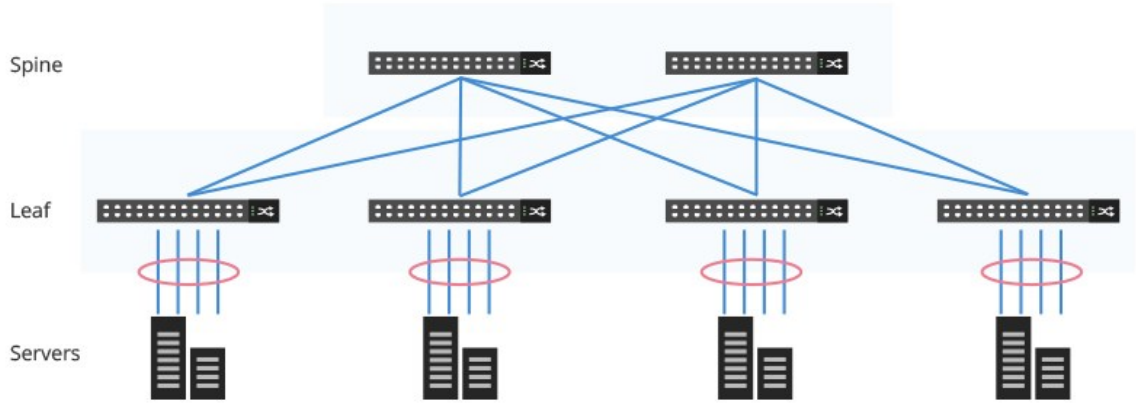
3.2 Spine-leaf

Kuvassa 2 esitellyssä Spine-leaf-arkkitehtuurissa jokainen leaf-kerroksen kytkin on yhdistetty jokaiseen spine-kerroksen. Leaf-kerros koostuu access-kytkimistä, jotka yhdistyvät päätelaitteisiin, kuten palvelimiin. Spine-kerrosta pidetään topologian selkärankana, ja se on vastuussa kaikkien leaf-kerroksen kytkinten yhdistämisestä. Jokainen leaf-kytkin on siis yhteydessä jokaiseen spine-kerroksen kytkimeen. (Silverman & Solberg 2018, 35.)

Kuormantasaus ja vikasietoisuus saavutetaan equal cost multipathing (ECMP) -tekniikalla, jota esimerkiksi OSPF tai IS-IS hyödyntävät. Käytettävä polku on sattumanvaraisesti valittu, jotta liikenteen kuorma on jaettu tasaisesti jokaiselle spine-kytkimelle tarkoittaen, että yhden spine-kytkimen hajotessa verkon kokonaisteho ei heikkenisi huomattavasti. (Hosken 2016, 242.)

Jos verkkoliikenne kasvaa isommaksi, kuin mitä aktiiviset linkit kykenevät käsitellä, on topologiaan helppo lisätä ylimääräinen spine-kytkin. Päinvastoin jos kytkinporttien kapasiteetti alkaa käydä vähiin, voidaan topologiaan lisätä uusia leaf-kytkimiä kapasiteetin kasvattamiseksi. Spine-leaf-arkkitehtuurissa, riippumatta siitä mikä leaf-kytkin on yhteydessä mihinkin palvelimeen, on niiden vä-

linen liikenne aina yhtä monen laitteen päässä toisistaan. Tämä helpottaa latenssin (aikaa, jolla kuvataan paketin matkaa lähettäjältä vastaanottajalle ja takaisin) ennakointia, kun hyppyjä on aina sama määrä. (Hosken 2016, 242.)

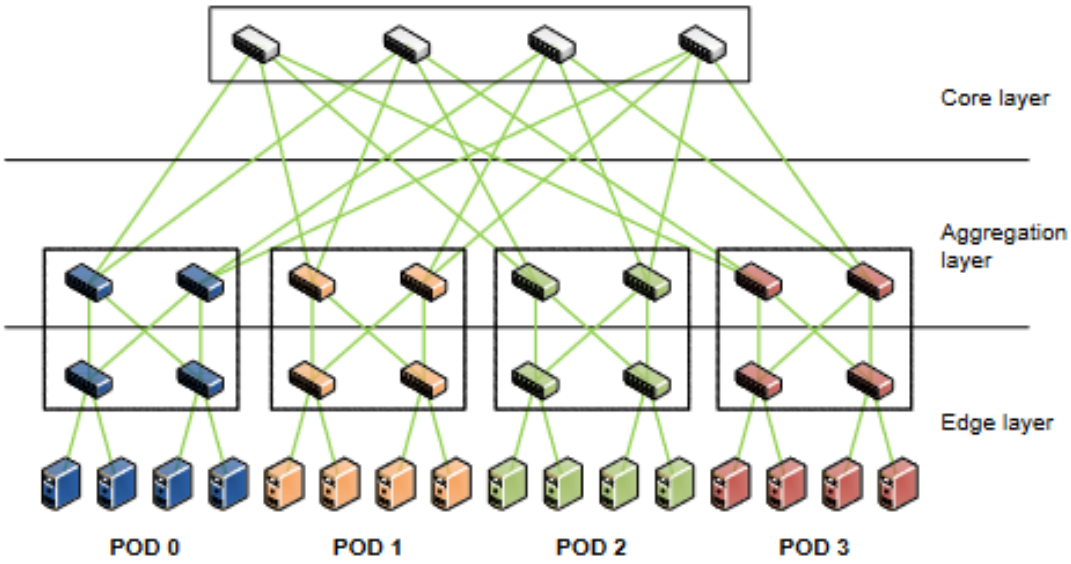


Kuva 2. Spine-leaf-arkkitehtuuri (FS 2021)

3.3 Fat-Tree

Kontrastina kolmen tason arkkitehtuurille, fat-tree kehitettiin ratkaisuksi vähentämään oversubscription-suhdetta verkossa, sekä poistamaan perinteisen arkkitehtuurin ongelmapisteet. Koska topologian kerrokset koostuvat samanlaisista kytkimistä, datakeskusverkon kustannukset voidaan pitää matalina. Fat-tree ei täysin kykene täydelliseen 1:1 oversubscription-suhteesen, mutta tarjoaa silti ”non-blocking”-polut täydellä kaistanleveydellä. (Jarschel ym. 2012, 6.)

Kuten kuvasta 3 nähdään, verkko jaetaan kolmeen eri osaan: runko-, jakelu- sekä reunakerrokseen. Topologiassa on *k*-määrä podeja, ja jokaisella podilla on *k/2* reunakytkimiä sekä *k/2* jakelukytkimiä. Jokainen podi on kytkettynä runkokytkimeen jakelukerroksen kytkimen kautta. Reunakerroksessa kytkimeen kytkeytyy *k/2*-määrä palvelimia. Palvelimien määrä topologiaan saadaan kaavasta $k^3/4$. Spine-leaf-arkkitehtuuri on eräs fat-treehin pohjautuvista verkkoratkaisuista. (Jarschel ym. 2012, 6.)



Kuva 3. Fat-tree-arkkitehtuuri (Jarschel ym. 2012)

3.4 Arkkitehtuurien vertailu

Kun otetaan huomioon pilvi- ja kontti-infrastruktuurin yleisyys nykyaikaisissa datakeskuksissa, palvelimelta palvelimelle -liikenne on kasvanut ja kasvaa jatkuvasti. Tämä muutos selittyy ensisijaisesti nykyaikaisilla sovelluksilla, joissa on komponentteja, jotka on jaettu useille palvelimille tai virtuaalikoneille. Sisäisen liikenteen kasvamisen myötä, perinteinen datakeskusverkko laajeni kompleksiseksi ja kalliiksi ympäristöksi ylläpitää. Matala latenssi sekä optimoitu datavirta on suorituskyvyn kannalta välttämätöntä, eritoten kriittisissä applikaatioissa. (Network Centre 2018.)

Kolmen tason arkkitehtuurissa isoimpana ongelmakohtana on sen muodostamat silmukat, joiden takia verkkoon on konfiguroitava STP-protokolla (Spanning Tree Protocol) silmukoiden estämiseksi. Vaikka STP tarjoaa redundanttisen polun kytkinten välillä, vain yksi voi olla aktiivisena kerrallaan, jonka takia linkkiväleistä tulee usein ylikuormitettuja. STP:n estäessä toimivien linkkien käytön ja koska protokolla voi olla arvaamaton, saattaa seurauksena olla koko verkon kaatuminen. (Sheldon & Younger 2022.)

Koska kolmen tason arkkitehtuuria ei ole suunniteltu nykyaikaisten datakeskusstandardien mukaan, se ei ole kykenevä suoriutumaan lisääntyneestä east-west-liikenteestä, joka korottaisi latenssia, muodostaisi pullonkauloja

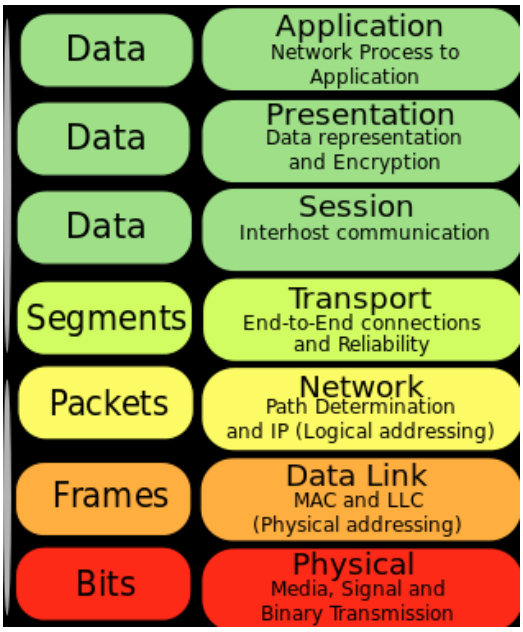
sekä tiputtaisi paketteja tämän kaltaisessa arkkitehtuurissa. (Sheldon & Younger 2022.)

Spine-leafin layer 3-reitityksen ansiosta STP:n käyttö voidaan jättää pois ja implementoida ECMP-protokolla kuormantasaukseen ja jokaisen linkin hyödyntämiseen, joka estää silmukoiden syntymisen. Tietoliikenne kulkee aina vähiten ruuhkautuneen linkin kautta ja latenssi verkossa on erityisen matala sekä ennakoitavissa, sillä topologiassa liikenne on aina kahden hypyn päässä toisistaan. (Network Centre 2018.)

Verkon skaalautuvuus voidaan hoitaa hallitusti ja ilman sen alasajoa kytkinten lisäämisen ajaksi. Ongelmakohdat spine-leaf -arkkitehtuurissa liittyvät pääosin sen suuriin kaapelointimääriin sekä spine-kytkimen kytkeytyessä jokaiseen leaf-kytkimeen, voivat kytkinportit täyttyä nopeasti. (Network Centre 2018.)

3.5 Layer 2 ja layer 3

Siirtoyhteyskerros (eng. Data Link Layer) on toinen taso verkkoprotokollasuunnittelun seitsenkerroksisessa OSI-mallissa (kuva 4). Siirtoyhteyskerros on verkkokerros, jota käytetään siirtämään tietoa vierekkäisten verkkosolmujen (eng. node) välillä WAN-verkossa tai solmujen välillä samassa lähiverkossa. (Juniper 2021.)



Kuva 4. Seitsenkerroksinen OSI-malli (Wikimedia 2015)

Kehys (eng. frame) on protokollatietoyksikkö, joka lähetetään samassa lähiverkossa oleville laitteille ja vastaanotetaan niistä. Toisin kuin biteillä, kehyksillä on määritelty rakenne ja niitä voidaan käyttää muun muassa virheiden havaitsemiseen ja ohjaustason (eng. control plane) toimintoihin. Verkko käyttää joitain kehyksiä itse datalinkin ohjaamiseen. (Juniper 2021.)

Siirtoyhteyskerroksella *unicast* tarkoittaa kehysten lähettämistä yhdestä solmusta toiseen solmuun, kun taas *multicast* tarkoittaa liikenteen lähettämistä yhdestä solmusta useisiin solmuihin ja *broadcast* tarkoittaa kehysten lähettämistä kaikille verkon solmuille. *Broadcast domain* on verkon looginen jako, jossa kaikki kyseisen verkon solmut voidaan tavoittaa Layer 2 -broadcastilla. (Juniper 2021.)

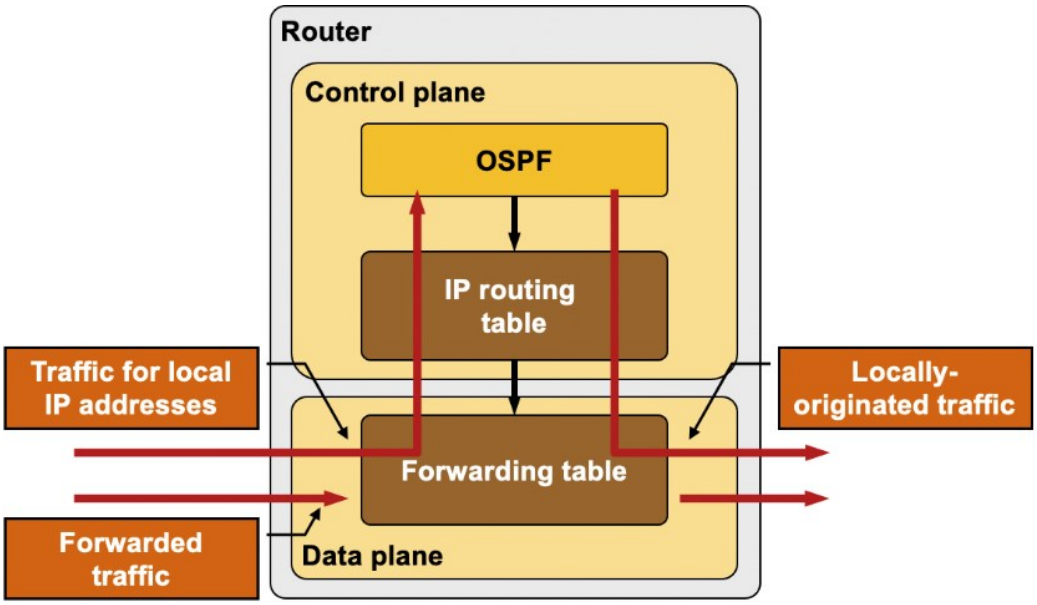
Lähiverkon segmentit voidaan linkittää kehystasolla siltojen (eng. bridge) avulla. Siltaus luo LAN-verkkoon erilliset lähetysalueet luoden VLAN-verkkoja, jotka ovat itsenäisiä loogisia verkkoja. VLAN liittää yhteen saman tarkoitusperän fyysiset laitteet omiin verkkosegmentteihinsä. Laitteiden ryhmittely VLAN-verkossa on riippumaton siitä, mikä laitteiden fyysinen sijoittelu on. Ilman siltausta ja VLAN-verkkoja kaikki lähiverkon laitteet ovat yhdessä broadcast domainissa havaiten kaikki lähiverkon paketit. (Juniper 2021.)

OSI-mallin kolmas kerros, verkkokerros (eng. Network Layer), vastaa kehysten vastaanottamisesta siirtoyhteyskerrokselta ja niiden toimittamisesta niille tarkoitettuihin kohteisiin kehyksen sisällä olevien osoitteiden perusteella. Verkkokerros löytää kohteen käyttämällä loogisia osoitteita, kuten IP-osoitetta. (Forcepoint s.a.)

3.6 Control plane ja data plane

Control plane eli ohjaustaso on verkon osa, joka ohjaa datapakettien välittämistä, eli kuinka dataa lähetetään paikasta toiseen. Esimerkiksi reititystaulun luontiprosessia pidetään osana ohjaustasoa. Reitittimet käyttävät erilaisia protokollia verkkopolkujen tunnistamiseen, ja ne tallentavat nämä reitit reititystauluihin. (Cloudfare s.a.)

Edelleenlähetystoiminnot sijaitsevat, mukaan lukien logiikka ja taulukot saapuvien pakettien käsittelyyn MAC-osoitteen, IP-osoitteen ja VLAN-tunnuksen perusteella datatasolla (eng. data plane). Datatason suorittamat perustoiminnot (kuva 5) voidaan kuvata tavalla, joka havainnollistaa miten datataso luopuu saapuvista paketeista. Se voi välittää, pudottaa, tai replikoida saapuvan paketin. Paketin edelleen ohjausta varten tietoliikennelaite tarkastaa oikean lähtöportin omasta taulukostaan (eng. forwarding table). Datataso tunnetaan myös nimellä forwarding plane. (Black & Goransson 2014, 59.)



Kuva 5. Ohjaus- ja datatason suorittama prosessi saapuvalle paketille (IPspace 2020)

4 PÄÄLLYSVERKKO

Päällysverkko on tietoverkko, joka on rakennettu jo olemassa olevan verkon päälle. Tämä tarkoittaa, että päällysverkon toiminnan riippuvuus on yhteydessä suoraan sen alla toimivaan alusverkkoon. Nykyään useimmat päällysverkot rakennetaan TCP/IP-pinon päällimmäiseen tasoon, sovellustasoon (eng. application layer).

Päällysverkkotekniikoita hyödynnetään paikkaamaan alusverkon rajoituksia, samalla tarjoten uusia reititys- ja edelleenlähetystoimintoja ilman reitittimien muuttamista. Noodit päällysverkossa yhdistyvät toisiinsa loogisten linkkien avulla, jotka ulottuvat moniin fyysisiin linkkeihin. Kahden päällysverkko-noodin välinen linkki voi kulkea usean alusverkkohypyn kautta. päällysverkossa yleisesti käytettyjä tekniikoita ovat muun muassa NVGRE (Network Virtualization

Using Generic Routing Encapsulation) ja VXLAN (Virtual Extensible Local Area Network). (Tarkoma 2010, 3.)

4.1 Virtual Extensible Local Area Network eli VXLAN

Palvelinten virtualisoinnin myötä myös fyysisen verkon vaatimukset ovat lisääntyneet. Fyysisellä palvelimella voi olla useita virtuaalikoneita, joista jokaisella on oma MAC-osoitteensa. Tämän myötä datakeskusympäristön Ethernet-verkon MAC-osoitetaulut ovat kasvaneet todella valtaviksi satojen tuhansien virtuaalikoneiden liikennöidessä keskenään. Tilanteessa, jossa virtuaalikoneet segmentoidaan käyttötarkoituksen mukaan, voi yksi asiakas tarvita tuhansia VLAN:ja tietoliikenteen rajaamiseen. Nykyinen 4094:n VLAN:n maksimimäärä on yksinkertaisesti liian vähäinen. (Mahalingam ym. 2014.)

Tärkeä vaatimus virtualisoidulle ympäristölle, joka käyttää fyysistä L2-infrastruktuuria, on L2-verkon skaalautuvuus koko datakeskukseen. Näin voidaan varmistaa tehokas laskentatehon, verkon sekä palvelinten käyttö. Tämän kaltaisissa verkoissa perinteisten keinojen, kuten STP:n käyttö silmukoiden poistamiseksi ei ole enää kannattavaa, sen sulkiessa useita käyttökelpoisia, liikennöiviä linkkejä. (Mahalingam ym. 2014.)

VXLAN huomioi virtualisoinnin tuomat layer 2- sekä layer 3 -vaatimukset moniasiakas datakeskusinfrastruktuurissa. VXLAN luo loogisen tunnelin lähettävän sekä vastaanottavan laitteen välille, kapseloi L2 Ethernet -kehyksen UDP (User Datagram Protocol) -paketiksi ja siirtää sen L3-verkon yli. Verkkojen segmentointiin sekä niiden tunnistamiseen VXLAN käyttää 24-bittistä VNI:tä (VXLAN Network Indentifier), joka mahdollistaa jopa 16 miljoonan VXLAN-segmentin rinnakkaisuuden samalla hallinta-alueella. (Mahalingam ym. 2014.)

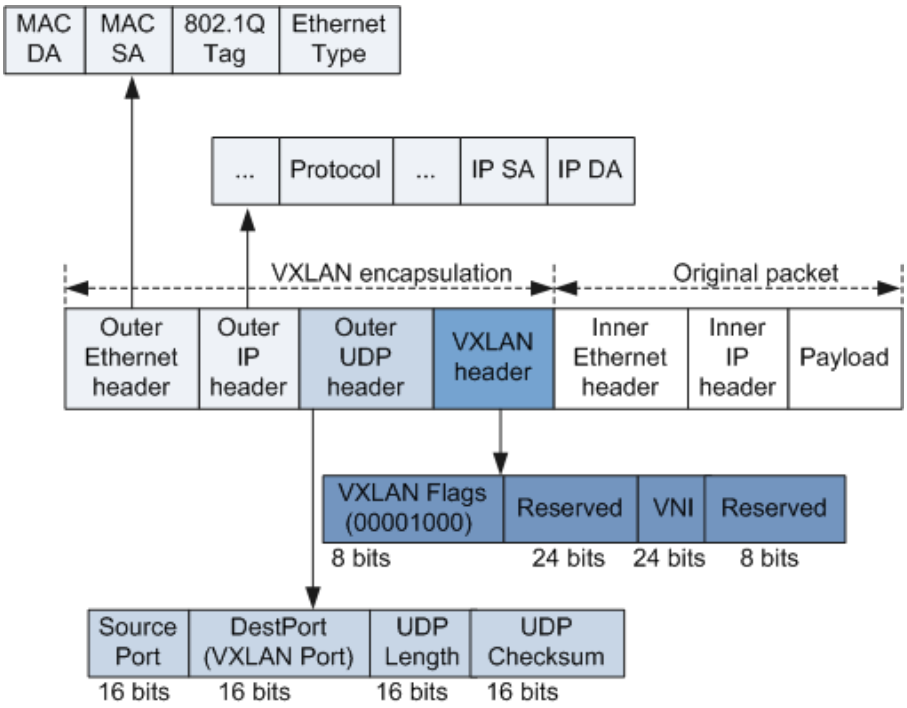
Kuvassa 6 näkyvän VXLAN-paketin kuvataan koostuvan seuraavista osista (Mahalingam ym. 2014.):

1. Ulompi ethernet-otsake koostuu lähettäjän ja vastaanottajan MAC-osoitteesta. Kohde-MAC voi olla joko VTEP, tai L3-reititin. VLAN ID Tag on valinnainen; jos se on asetettu, on mahdollista rajata VXLAN-liikennettä lähiverkossa.

2. Ulompi IP-otsake sisältää lähettäjän VTEP IP -osoitteen, sekä vastaanottajan VTEP IP:n. Protocol kertoo käytettävän tietoliikenneprotokollan. VXLAN käyttää UDP-protokollaa paketin lähetykseen.

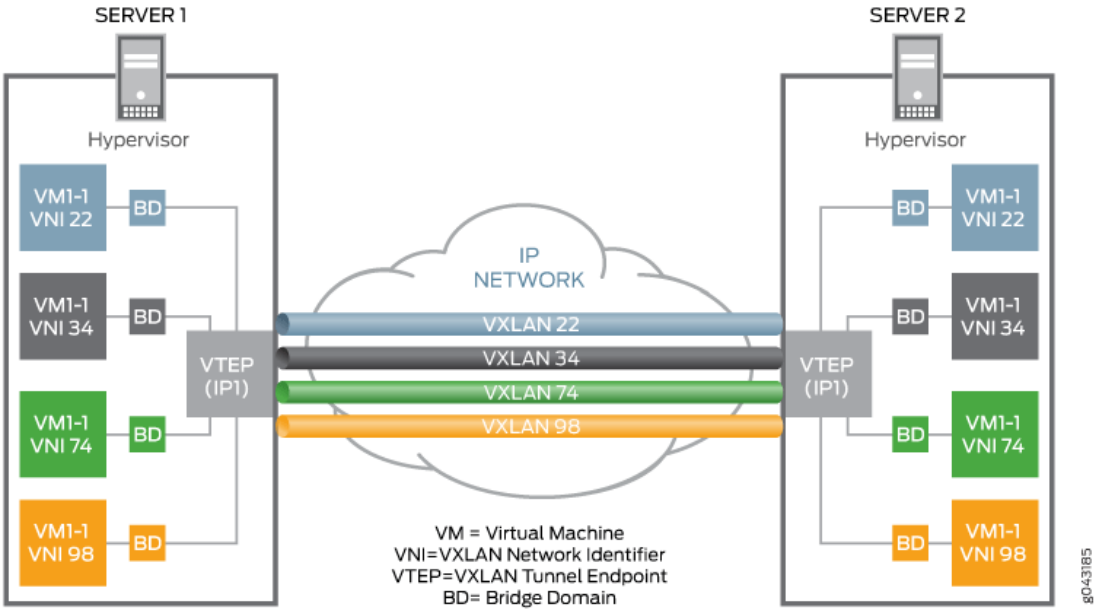
3. Ulompi UDP-otsake, joka kertoo UDP-kohdeportin sekä vastaanottavan UDP-portin. Kohdeportti on IANA:n (Internet Assigned Numbers Authority) määrittämä portti 4789. Lähtöportti saadaan suorittamalla hajautusoperaatio (eng. hash operation) alkuperäiseen L2-kehykseen kuuluvalle sisäiselle ethernet-otsakkeelle.

4. VXLAN-otsake, joka identifioi oikean VXLAN-segmentin sekä käyttää tarkistusbittiä (eng. flag) validille VNI:lle. Muut, varatut kentät asetetaan arvoon nolla siirtoa varten sekä jätetään huomiotta vastaanotettaessa.



Kuva 6. VXLAN-paketin formaatti (Huawei 2020)

VTEP (VXLAN Tunnel Endpoint) viittaa yleensä mihin tahansa laitteeseen, joka luo tai terminoi VXLAN-liikenteen (kuva 7). On olemassa kaksi päätyyppiä sen mukaan, miten VXLAN-pakettien kapselointi tai kapseloinnin purkaminen käsitellään: laitteistopohjainen VTEP, joka käsittelee VXLAN-paketit tietoliikennelaitteiston (kytkin, reititin) avulla, sekä ohjelmistopohjainen VTEP, joka käyttää esimerkiksi palvelimella toimivaa ohjelmistoa pakettien käsittelyyn. (Mahalingam ym. 2014.)



Kuva 7. VXLAN:in toimintaperiaate. VTEP:in luomat loogiset tunnelit kuljettavat liikenteen IP-verkon yli (Fiberopticom 2020)

VXLAN-GBP (VXLAN Group Based Policy) on tapa, jolla saavutetaan mikro- ja makrotason segmentointi esimerkiksi datan tai omaisuuden suojaksi. VXLAN-GBP toimii käyttämällä VXLAN-otsakkeen varattuja kenttiä skaalautuvina ryhmätunnisteina (eng. scalable group tag), joiden pohjalta voidaan tehdä palomuurisääntöjä verkon rajaukseen. Skaalautuva ryhmätunniste voidaan konfiguroida suoraan kytkimeen portti- tai MAC-kohtaisesti, tai RADIUS-palvelimelle hyödyntämällä 802.1X-protokollaa käyttäjän tunnistautuessa. (Kreeger & Smith 2018.)

4.2 Network Virtualization Using Generic Routing Encapsulation eli NVGRE

RFC 7637:n mukaan NVGRE on kehitetty ratkaisuksi uuden sukupolven datakeskuksen tuomiin haasteisiin. Näitä haasteita ovat (Garg & Wang 2015):

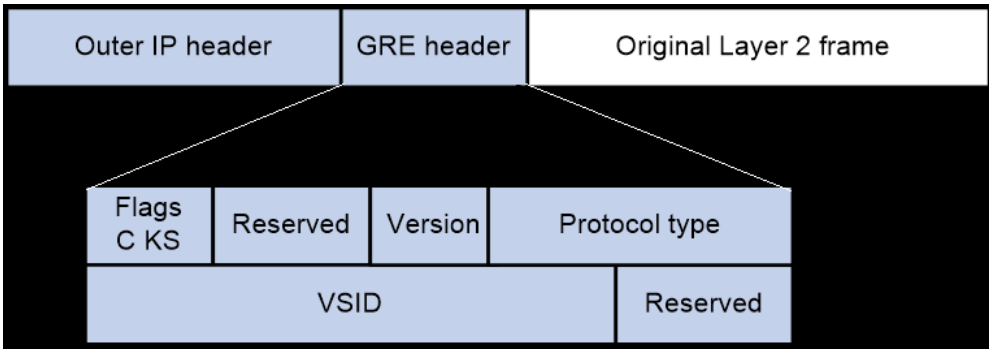
1. Sijainnista riippumaton IP-osoitteistaminen.
2. Mahdollisuus skaalata L2/L3-verkkojen määrää riippumatta taustalla toimivasta alusverkosta tai VLAN:ien määrästä.
3. L2-semantiikan säilyttäminen palveluilla sekä mahdollisuus IP-osoitteen muuttumattomuuteen liikkuessa datakeskuksen sisällä tai datakeskuksesta toiseen.
4. Välttää ohjaustason kuormittamista verkossa.

Tietoverkon virtualisointi vaatii virtuaalisten Layer 2 -verkkojen luomista fyysisen Layer 3 -verkon päälle. Yhteys NVGRE-topologiassa luodaan tunneloimalla Ethernet-kehykset GRE-tunnelia pitkin fyysisen IP-verkon yli. NVGRE:ssä jokainen virtuaalinen L2-verkko identifioidaan 24-bittisellä tunnisteella, VSID:llä (Virtual Subnet Identifier). VXLAN:in tavoin NVGRE tukee jopa 16 miljoonaa virtuaalista aliverkkoa samalla hallinta-alueella. (Garg & Wang 2015.)

GRE on IETF:n (The Internet Engineering Task Force) standardoima IP-tunnelointiprotokolla, joka mahdollistaa halutun protokollan kapseloinnin IP-verkon yli. NVGRE hyödyntää GRE-otsaketta VSID-tietojen siirtämiseen jokaisessa paketissa. Jokaisen paketin sisältämä VSID-tieto voidaan hyödyntää muun muassa luomalla verkon monitorointiin tai verkkoliikenteen analysointiin liittyviä työkaluja. (Garg & Wang 2015.)

NVGRE-päätepisteet (eng. NVGRE endpoint) ovat sisään-/ulospääsypisteet virtuaalisen ja fyysisen verkon välillä. Mikä tahansa fyysinen palvelin tai verkkolaite voidaan konfiguroida NVGRE-päätepisteeksi. Tavallisesti päätepisteen olisi hyvä olla osana virtuaalikoneen suorittamiseen käytettävää hypervisor-ohjelmistokerrosta. Päätepisteen tyypillinen tehtävä on kapseloida GRE-tunneliin siirtyvä Ethernet-kehys, purkaa tunnelista saapuva Ethernet-kehys, ylläpitää L2-semantiikkaa sekä soveltaa VSID:n mukaista eristyspolitiikkaa. (Garg & Wang 2015.)

Verrattuna VXLAN:n kapseloimaan pakettiin kuvassa 8 nähtävä NVGRE-paketin formaatti on protokollan asettamia omia otsakkeita (VXLAN:issa UDP-otsake ja VXLAN-otsake) lukuun ottamatta identtinen. Alkuperäinen L2-kehys kapseloidaan ja siihen lisätään GRE-otsake. Otsake sisältää VSID:n, jolla identifioidaan oikea NVGRE L2 -verkko. Tarkastusbitit C (Checksum Present) ja S (Sequence Number Present) asetetaan arvoon nolla, joista voidaan todeta, ettei GRE-otsake sisällä GRE-tarkastusnumeroa tai sekvenssinumeroa. K-bitti (Key Present) asetetaan arvoon yksi, joka indikoi GRE-otsakkeen pitävän sisällään validin VSID:n. (Garg & Wang 2015.)

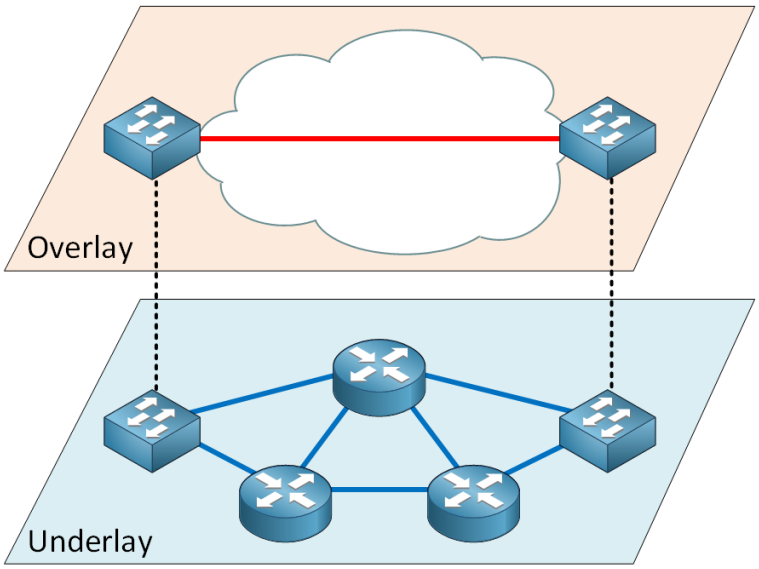


Kuva 8. NVGRE-kapseloidun paketin formaatti (H3C s.a.)

5 ALUSVERKKO

Alusverkko (kuva 9) tarkoittaa verkon fyysistä infrastruktuuria, jonka päälle päällysverkko rakennetaan. Alusverkko on taustalla oleva verkko, joka vastaa pakettien siirtämisestä ja toimittamisesta tietoverkkojen välillä. Kaikkien alusverkko-laitteiden on määritettävä IP-yhteys toistensa välillä. Yleensä yhteys luodaan IGP (Interior Gateway Protocol) -reititysprotokollan avulla.

IGP:llä kuvataan protokollaa, joka jakaa reititystiedot yhden autonomisen järjestelmän (eng. Autonomous System, AS) kesken. Näihin kuuluvat muun muassa IS-IS (Intermediate System to Intermediate System) sekä OSPF (Open Shortest Path First). Datakeskusympäristöissä fyysisen alusverkon tehtävänä on tarjota unicast IP-yhteys mistä tahansa fyysisestä laitteesta (palvelin, tallennuslaite, reititin tai kytkin) mihin tahansa muuhun fyysiseen laitteeseen. (Route-XP s.a.)



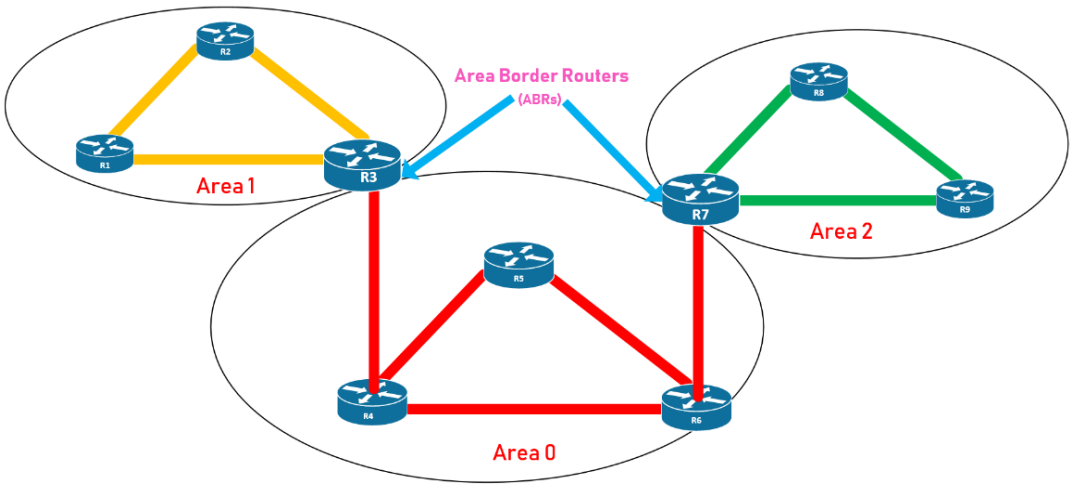
Kuva 9. Yksinkertaistettu kuva päällysverkon ja alusverkon toimintaperiaatteesta (Cisco 2013)

5.1 Open Shortest Path First eli OSPF

OSPF (Open Shortest Path First) on IETF:n kehittämä linkkitilaprotokolla (link-state routing protocol), jonka toimintatapa perustuu Djikstran shortest path first (SPF) -algoritmiin naapurilaitteiden sekä lyhimpien reittien määritykseen. Kuvasta 10 nähdään, että reitityksen turvana OSPF käyttää aluereititystekniikkaa, jossa reititettävä verkko voidaan segmentoida alueisiin ja rajata näin liikennettä verkon sisällä. (Moy 1998.)

Kaikki OSPF-reitittimet jakavat keskenään tietoa paikallisesta tilastaan (käytettävissä olevat portit, tavoitettavat naapurilaitteet sekä kunkin reitin etäisyys (eng. cost) Link State Advertisement (LSA) -viestein. Viestin vastaanottavat reitittimet muodostavat oman alueensa sisällä identtisen tietokannan (eng. link-state database), josta käy ilmi autonomisen järjestelmän topologia. Jos alueita on useampi kuin yksi, ne voidaan yhdistää toisiinsa reunareitittimien avulla (eng. area border router). (Moy 1998.)

Reunareitin ylläpitää jokaiseen yhdistettyyn alueeseen liittyen erillistä tietokantaa. OSPF-alue 0, eli OSPF:n selkäranka sisältää aina kaikki alueen reunareitittimet. Alue 0 on vastuussa reititystietojen jakamisesta muille alueille. Jos topologiassa tapahtuu muutoksia, OSPF kykenee laskemaan uuden reitin nopeasti hyödyntämällä minimimäärän verkon reititysprotokolla-liikenteestä. (Moy 1998.)



Kuva 10. OSPF-verkon toimintaperiaate (Expert Network Consultant 2019)

5.2 Intermediate System to Intermediate System eli IS-IS

IS-IS (Intermediate System to Intermediate System) on vuonna 1992 ISO:n (International Organization for Standardization) standarisoima linkkitilaprotokolla. IS-IS:n reittienmääritys pohjautuu SPF-algoritmiin. Verrattuna OSPF:n LSA-viesteihin, IS-IS-reititin lähettää vastaavaa informaatiota omasta tilastaan (portit, naapurilaitteet, etäisyys) LSP (Link State PDU) -viestein. (ISO/IEC 10589 2002, 27 ja 153.)

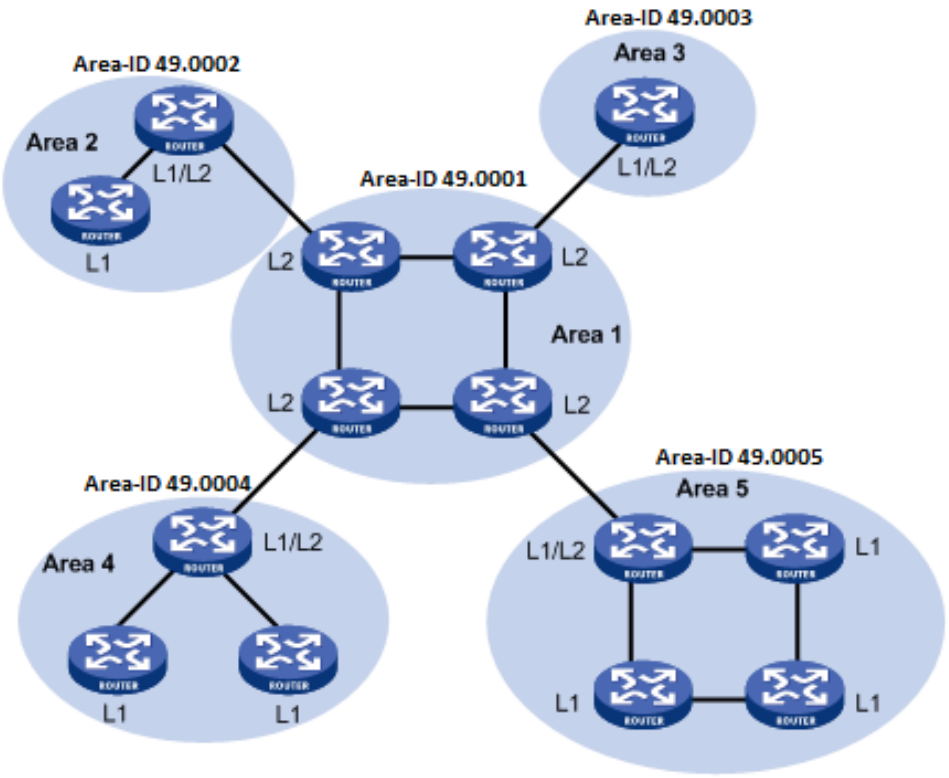
IS-IS:ssä autonominen järjestelmä jaetaan alueisiin (kuva 11), jonka avulla saadaan minimoitua reititystaulun koko, sekä vähennetään LSP-viestien määrää. Jokainen saman alueen IS-IS-reititin ylläpitää OSPF:n tavoin identtistä link-state-tietokantaa järjestelmän topologiasta. Topologia on aluekohtainen, eivätkä muiden alueiden IS-IS-laitteet näe toistensa tietokantoja. (Callon 1990.)

IS-IS käyttää aluejaossa kahden tason hierarkiaa (eng. two-level hierarchy). Tason yksi (level 1, L1) reitittimet tunnistavat oman alueensa topologian, sisältäen reitittimet sekä päätelaitteet (esimerkiksi palvelin), mutta eivät osaa tunnistaa alueensa ulkopuolisia reittejä tai laitteita. L1-reitittimet ohjaavat alueensa ulkopuolelle menevän liikenteen tason 1/2 (level 1 / level 2, L1/L2) reitittimelle. (Callon 1990.)

L1/L2-reitittimien toiminta pohjautuu karkeasti OSPF:n ABR-reitittimen toimintaan. L1/L2-reitittimet vaihtavat topologiatietoja ja reitittivät liikennettä alueensa sisällä, sekä alueiden kesken. Ne ylläpitävät kahta link-state-tietokantaa, joista toinen pitää sisällään oman alueensa L1-tietokannan ja toinen kattaa koko järjestelmän L2- sekä L1/L2 -reitittimien tietokannan. (Alcatel-Lucent 2015.)

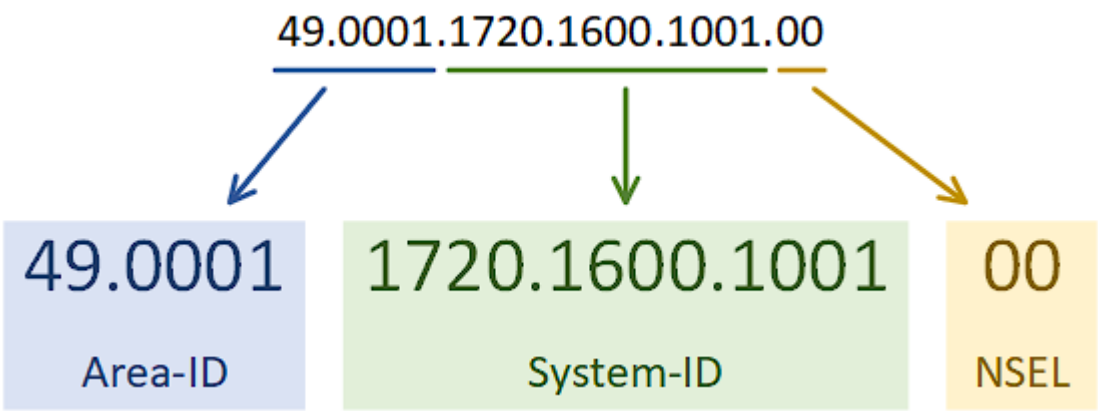
L2-reitittimet reitittävät liikennettä ainoastaan muiden L2-reitittimien välillä sekä muita autonomisia järjestelmiä kohden. IS-IS-topologiassa ei ole selvää OSPF:n alue 0:aan verrattavissa olevaa, niin sanottua selkäranka-aluetta. L2-

reitittimet muodostavat alueesta riippumatta IS-IS:n selkärangan. (Callon 1990.)



Kuva 11. IS-IS topologia. Alueet erotetaan toisistaan NET-osoitteeseen sisältyvän Area-ID:n avulla (Techhub s.a.)

Kuvan 12 Network Entity Title (NET) on osoite, joka identifioi reitittimen. Se on jaettu neljään osioon. Ensimmäinen on yhden tavun kokoinen AFI (Authority and Format Indicator), joka useimmiten saa arvon 49, sillä se kuvaa yksityistä osoitealuetta. Seuraavat 1–13 tavua kertovat, mihin alueeseen reititin kuuluu. System ID (SID), eli järjestelmän tunnus on kuusitavuinen numerosarja, joka erottaa alueella reitittimet toisistaan. Viimeinen yhden tavun kokoinen NSEL (Network Service Access Point Selector), joka IS-IS-protokollassa asetetaan aina arvoon 0. (ISO/IEC 10589 2002, 15–18.)



Kuva 12. NET-osoitteen rakenne (Networkdirection s.a.)

5.3 Border Gateway Protocol eli BGP

BGP (kuva 13) on vuonna 1989 Lougheedin ja Rekhterin yhteistyönä alkunsa saanut inter-autonominen reititysprotokolla. Inter-autonomisella tarkoitetaan, että sen primäärifunktio on vaihtaa verkon saavutettavuusinformaatiota muiden BGP-järjestelmien välillä. BGP:n ylläpitämä reititysinformaatiotaulukko (eng. Routing Information Base, RIB) sisältää tiedot tietoliikennelaitteeseen liittyneistä ulkoisista ja sisäisistä jäsenistä sekä mitä reittejä tulisi käyttää. (Hares ym. 2006.)

BGP:n reitityspäätökset pohjautuvat polkuihin, jotka määritellään säännöin tai poliitikoin järjestelmänvalvojan asettamina. BGP tuo verkolle stabiliteettia ja varmistaa, että reitittimet sopeutuvat nopeasti lähettämään paketteja uuden yhteyden kautta, jos jokin poluista menee alas. BGP:tä voidaan hyödyntää myös autonomisen järjestelmän sisäiseen reititykseen. (Hares ym. 2006.)

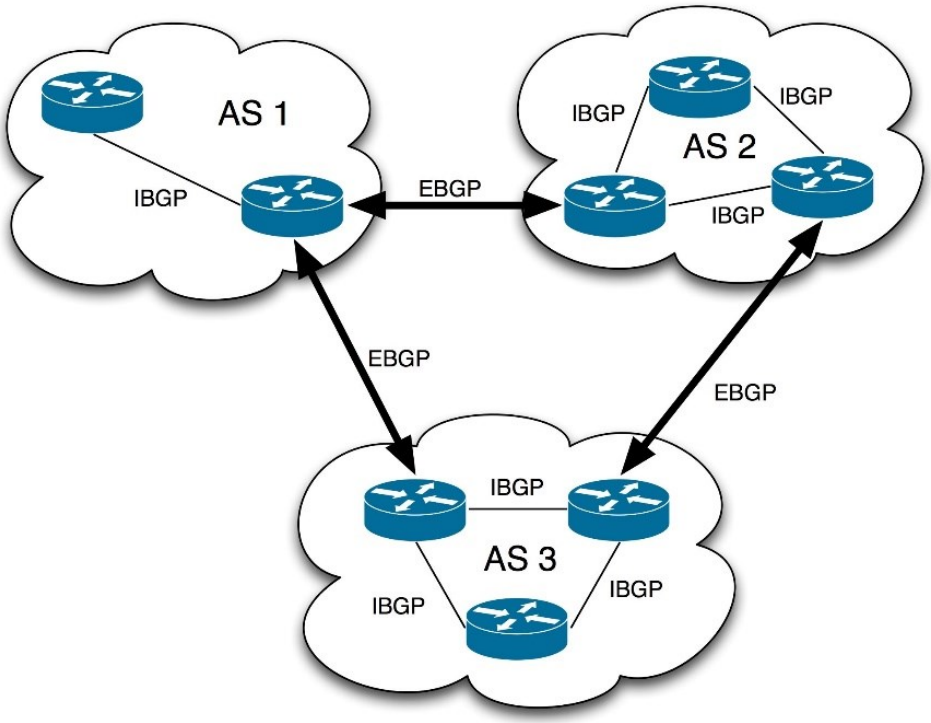
BGP päivittää järjestelmien välistä informaatiota vain muutosten tapahtuessa, ja siinäkin tapauksessa se jakaa ainoastaan muuttuneet tiedot. BGP:llä ei ole automaattista tunnistusmekanismia naapuruuksille (OSPF:n alueet, IS-IS:n tasot), eli yhteydet asiakkaiden välillä on konfiguroitava manuaalisesti. BGP tekee parhaimman reitin määrityksen polkuvektoreita hyödyntämällä. (Hares ym. 2006.)

Polkuvektorin perustana on, että reititin vastaanottaa autonomisen järjestelmän reunareitittimeltä (eng. Autonomous System Border Router, ASBR) pol-

kuvektori-viestin, joka sisältää tiedon kohdeverkon etäisyydestä pohjautuen johonkin metriikkaan, esimerkiksi hyppyjen määrään ja tiedon suunnasta (eng. next-hop), mihin datan on lähdettävä päästäkseen kohdeverkkoon. Tätä ASBR:n lähettämää tietoa kutsutaan etäisyysvektoriksi. Etäisyysvektorin lisäksi BGP vastaanottaa polkuinformaation, joiden pohjalta se kykenee laskemaan reitin kohteena olevaan autonomiseen järjestelmään. (Hares ym. 2006.)

External Border Gateway Protocol -protokollaa (EBGP) käytetään autonomisten järjestelmien välillä. Sitä käytetään ja toteutetaan reunareitittimissä, joka tarjoaa yhteenliitettävyyden kahdelle tai useammalle autonomiselle järjestelmälle. EBGP toimii protokollana, joka vastaa eri organisaatioiden tai Internetin verkkojen yhteenliittymisestä. (Hares ym. 2006.)

IBGP:n (Internal Border Gateway Protocol) tehtävä on vaihtaa tietoja autonomiseen järjestelmään kuuluvien laitteiden välillä. Käyttö edellyttää, että kaikki laitteet järjestelmässä muodostavat full-mesh-topologian tai route reflectorien käytön prefiksien oppimiseksi.



Kuva 13. BGP-verkon toimintaperiaate (Noction 2012)

6 OHJELMOITAVA VERKKO

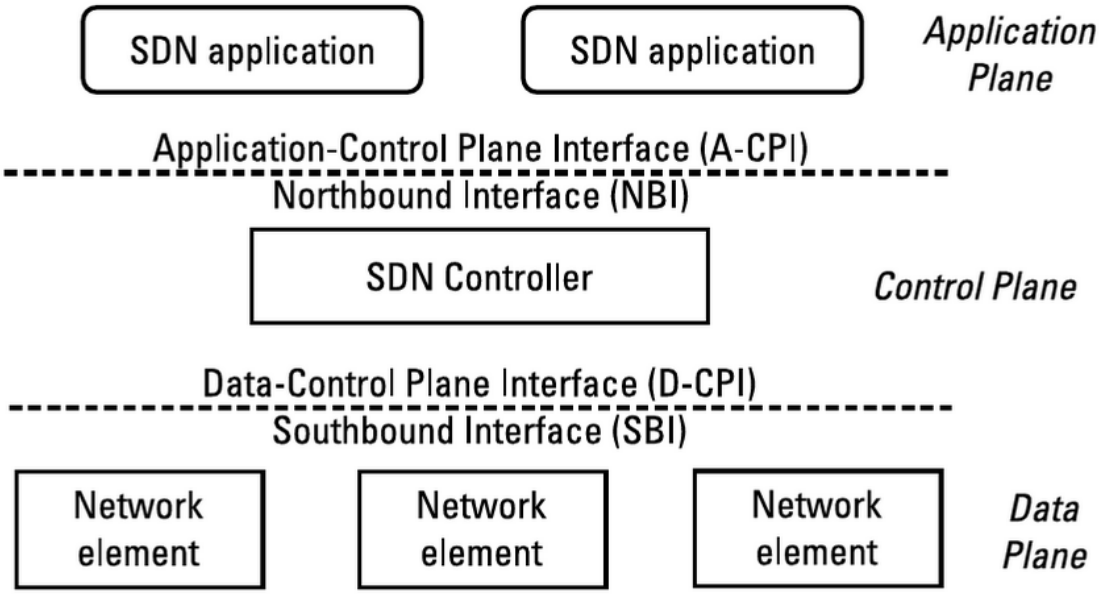
Pilvitekniikan yleistyessä monille uusille tietoverkkoratkaisuille on suunniteltu tapoja yksinkertaistaa verkonhallintaa, sekä tuoda uudenlaisia innovaatioita verkon ohjelmoitavuuden myötä. Ohjelmoitava verkko (eng. Software-Defined network, SDN) on lähestymistapa, joka käyttää ohjelmistopohjaisia ohjaimia tai ohjelmointirajapintoja (eng. Application Programming Interface, API) verkon liikenteen ohjaamiseen tai kommunikointiin verkkolaitteiden kanssa. Tämä malli eroaa perinteisestä tietoverkosta, joka käyttää verkkolaitteita (kytkimet, reitittimet) liikenteen kontrollointiin verkossa. (Duan & Mehmet 2016, 2–4.)

Ohjelmoitavan verkon perusperiaate on, että siinä erotetaan ohjaustason funktiot datatason prosesseista ja keskitetään verkon kontrolli siitä vastaavalle SDN-ohjaimelle. Tämän erotuksen ansiosta verkosta muuttuu yksinkertaisempi, ohjelmoitava ympäristö ja se antaa ohjelmistolle laajemmat valtuudet määritellä verkon toimintaa. Tasojen erotus toisistaan mahdollistaa verkossa datatason laitteiston suorittavan pelkästään pakettien siirtämistä SDN-ohjaimen asettamien sääntöjen mukaan. Monimutkaisten ohjaustoimintojen poistaminen yksittäisistä laitteista ja ohjauslogiikan yhdistäminen yhdelle ohjaimelle yksinkertaistaa huomattavasti verkkolaitteita ja vähentää siten niiden kustannuksia. (Duan & Mehmet 2016, 5–6.)

Kuvassa 14 nähtävä SDN-arkkitehtuuri koostuu sovellus-, ohjaus- ja datatasosta. Datataso sisältää verkon resurssit suorittamaan datan prosessointia sekä sen siirtämistä verkossa. Datatason verkkoelementit ovat yksinkertaisesti pakettien välitys- ja/tai käsittelykoneita ilman monimutkaista ohjauslogiikkaa itsenäisten päätösten tekemiseksi. D-CPI (kutsutaan myös Southbound Interface) mahdollistaa datatason elementtien paljastavan resurssiensa ominaisuudet ja tilan ohjaustasolle. Lisäksi se sallii SDN-ohjaimen säätelyn datatason verkkoelementeille. (Duan & Mehmet 2016, 6–8.)

Ohjaustaso esittää globaalin näkymän datatason infrastruktuurista SDN-sovelluksille ja tarjoaa keskitetyn ohjausalustan, jonka kautta sovellukset voivat määritellä datatason elementtien suorittamat toiminnot. A-CPI (Northbound In-

terface) tarjoaa standardin ohjelmointirajapinnan, jonka avulla sovellukset voivat ohjelmoida taustalla olevan verkkoinfrastruktuurin. (Duan & Mehmet 2016, 6–8.)



Kuva 14. Ohjelmisto-ohjatun verkon arkkitehtoninen kehysmalli (Duan & Mehmet 2016)

7 TYÖN TOTEUTUS JA TOPOLOGIA

Toteutusvaiheeseen valittiin perustellusti verkossa käytetty topologia sekä alusverkko- ja päällysverkkoprotokollat. Valittuun tekniseen ratkaisuun hyödynnettiin Xamkin kurssimateriaalina toiminutta harjoitusta, jonka avulla voitiin varmistaa kyseisen arkkitehtuurin soveltuvuus validiksi verkkoratkaisuksi uutta kampusta varten. Lopulliseen arkkitehtuuriin voidaan kehittää myös verkon toimivuutta ja turvallisuutta parantavia keinoja, kuten käyttäjien autentikointia koskevia asioita.

Topologioista parhaaksi Xamkin käyttötarkoituksia varten valittiin Closin arkkitehtuurin pohjautuva spine-leaf-topologia. Datakeskusten lisääntyneen east-west-liikenteen takia kolmen tason arkkitehtonisia ratkaisuja ei harkittu käytettäväksi työssä. Päätöstä tuki topologian ominaisuudet maksimoida kaistanleveyden hyödyntäminen, latenssin ennakoiminen, helpot laajennusmahdollisuudet sekä silmukoiden syntymisen esto. Verkosta saadaan ”non-blocking” STP-protokollan jäädessä pois kaikkien kytkinporttien välittäessä liikennettä.

7.1 Ensimmäinen vaihe

Ensimmäisessä vaiheessa luotiin datakeskusverkko (kuva 15) IS-IS alusverkkoprotokollana sekä VXLAN päällysverkkona Xamkin VirtualLab-ympäristöön. Tietoliikennelaitteistona toimivat Aristan kytkimet EOS-4.28.0F käyttöjärjestelmällä, avoimen lähdekoodin Proxmox-hypervisor virtualisoinnin hallintaan sekä yksi Linux-palvelin.

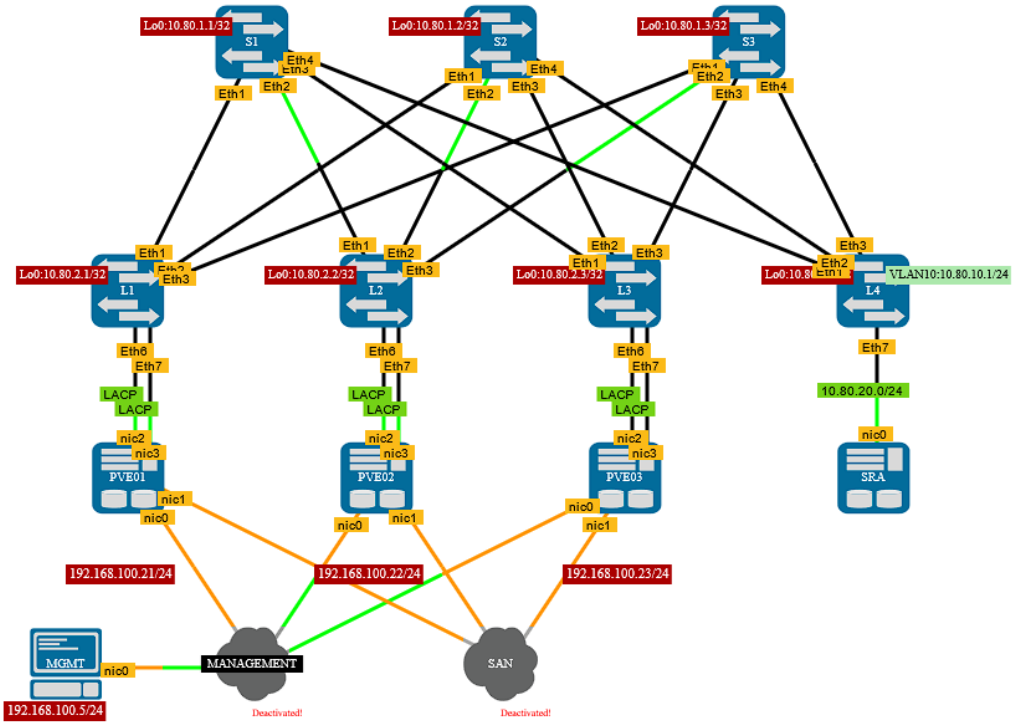
Alusverkkoprotokollan valintaan VXLAN:n toimivuuden kannalta ei ole selvää vastausta. Jotkin IS-IS:n ominaisuudet, kuten säädettävä LSP-elinaika tai vähäisempi määrä attribuutteja, joiden tarvitsee olla yhteneviä muodostaakseen ja ylläpitääkseen IS-IS-naapuruuden ovat hieman OSPF:ää parempia, mutta eivät relevantteja verkon toimivuuden kannalta. BGP on usein ison skaalan datakeskuksissa käytetty protokolla, ja vaikka se toimisi hyvin myös Xamkin ympäristössä, ei sille koeta tarvetta IS-IS:n ja OSPF:n ajaessa saman asian vähemmällä työmäärällä.

IS-IS:n valintaa tuki lopulta parhain tietämys protokollasta ja sen ominaisuuksista. Xamkin kannalta IS-IS on sopiva protokolla pieneen/keskikokoiseen datakeskusverkkoon. VXLAN taas on yleisesti käytetyin ja tuetuin päällysverkkoprotokolla datakeskusverkoissa (Bhattacharya 2021), joka oli myös peruste valita se käytettäväksi protokollaksi.

Kytkimiin konfiguroitiin porttien IP:t, loopback 0-osoite sekä VxLan-liikennettä varten MTU (Maximum Transmission Unit) nostettiin 1500:sta 1600:n. IP-osoitteistamiseen verkossa käytettiin 10.80.0.0/18-verkkoaluetta. Proxmoxien sekä leaf-kytkinten väliset linkit konfiguroitiin LACP-linkeiksi (Link Aggregation Control Protocol), mikä parantaa redundanttisuutta, kuormantasausta ja performanssia. Toinen vaihtoehto redundanttiselle konnektiviteetille on yhdistää hypervisorit kahteen erilliseen leaf-kytkimeen. Erillisenä verkkona topologiassa on management-verkko, jonka kautta proxmox-hypervisoreita hallitaan keskitetysti yhden koneen kautta.

Proxmox-klusteriin luotiin kaksi konttia (eng. container) sekä yksi virtuaalikone. Neljänteen leaf-kytkimeen konfiguroitiin VLAN 10 päällysverkon toimivuuden testausta varten. Palvelinta päin osoittava portti muutettiin reitittäväksi

portiksi, sekä asetettiin palvelimelle IP-osoite ja verifioitiin palvelimen sekä leaf-kytkimen välinen toimivuus pingaamalla VLAN 10 osoitetta.



Kuva 15. VirtualLab:iin luotu datakeskusympäristö

7.2 IS-IS-VXLAN-HER

Toisessa vaiheessa konfiguroitiin IS-IS-alusverkkoreititys sekä VXLAN hyödyntämällä Head-End Replicationia (HER), joka on tekniikka, jossa kaikki BUM-liikenne (Broadcast, Unknown-unicast and Multicast) replikoidaan jokaisen leaf-kytkimen välillä. Replikoinnin sekä manuaalisen konfiguroinnin takia, HER ei ole parhain ratkaisu isoihin datakeskuksiin skaalautuvuusrajoituksien vuoksi. Päällysverkon kannalta perinteistä kytkinverkkoa tärkeämpää on hyödyntää jokaista spine-leaf topologian käytettävissä olevaa linkkiväliä IS-IS:n utilisoimalla ECMP-tekniikalla.

Topologiassa ainoastaan leaf-kytkimet luovat sekä terminoivat VXLAN-tunneleita, joten spine-kytkimiin konfiguroitiin ainoastaan IS-IS-reititys. Leaf-kytkimiin konfiguroitiin toinen loopback-osoite, loopback 5, jota käytetään tunnelien pääte- sekä lähtöpisteinä. IS-IS:n luonti tapahtui konfiguroimalla jokaiselle kyt-

kimelle oma NET-osoite, sallimalla IS-IS jokaisessa kytkinportissa sekä mainostamalla molempia loopback-osoitteita verkkoon. Toimivuus tarkastettiin pingaamalla kytkinten loopback-osoitteita. Kuvasta 16 voidaan nähdä ECMP:n toimivuus, joka todettiin reititystaulusta, jossa reitti leaf-kytkimeltä toiselle kulki jokaisen kolmen spine-kytkimen kautta.

```
I L2     10.80.2.2/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
I L2     10.80.2.3/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
I L2     10.80.2.4/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
C        10.80.5.1/32 is directly connected, Loopback5
I L2     10.80.5.2/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
I L2     10.80.5.3/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
I L2     10.80.5.4/32 [115/30] via 10.80.11.1, Ethernet1
                               via 10.80.21.1, Ethernet2
                               via 10.80.31.1, Ethernet3
```

Kuva 16. ECMP:n toiminta LEAF1-kytkimen reititystaulusta

VXLAN:n konfiguraatiossa tarkoituksena oli luoda tunnelointi VLAN 10:lle käyttäen VNI:nä 1000:ta. VXLAN:lle luotiin oma interface (vxlan1), johon konfiguroitiin tunnelin lähdeosoite (loopback 5), BUM-liikenteen vuoto, eli tässä tapauksessa muiden topologian leaf-kytkinten loopback 5-osoitteet, sekä VLAN 10 määriteltiin käyttämään VNI 1000:ta. VXLAN:n toimivuus todettiin pingaamalla palvelimelta kontteja tai virtuaalikonetta ja varmistettiin VXLAN:n luomasta osoitetaulusta (kuva 17), että se oppi MAC-osoitteita.

```
LEAF4#show vxlan address-table
          Vxlan Mac Address Table
----------------------------------------------------------------------

VLAN  Mac Address     Type      Prt  VTEP             Moves   Last Move
----  -----------     ----      ---  ----             -----   ---------
  10  4e55.4c6d.3c44  DYNAMIC   Vx1  10.80.5.2        1       0:00:53 ago
  10  52c4.8b7a.cff3  DYNAMIC   Vx1  10.80.5.3        1       0:00:24 ago
  10  da5a.6c14.9a75  DYNAMIC   Vx1  10.80.5.1        1       0:02:02 ago
Total Remote Mac Addresses for this criterion: 3
```

Kuva 17. VXLAN:n oppimat MAC-osoitteet

7.3 Laitteisto

Spine-leaf-arkkitehtuuria suunnitellessa laitevalinnassa tulee ottaa huomioon seuraavia asioita (FS-Community 2022a.):

1. Verkon oversubscription-suhde, joka on tilanne, jossa jokainen verkon laite lähettää liikennettä samanaikaisesti. Sitä voidaan mitata north-south-suuntaisesti tai east-west-suuntaisesti. Modernin datakeskusverkon oversubscription-suhde tulisi olla 3:1 tai vähemmän, mikä mitataan suhteena alkupään (eng. upstream) kaistanleveytenä (spine-kytkimiä kohti) ja loppupään (eng. downstream) kapasiteettina (palvelimille/tallennustilaa kohti).

2. Skaalautuvuus: leaf-kytkinten määrä verkossa määräytyy porttimäärän perusteella, joka tarvitaan kytkemään päätelaitteet verkkoon. Koska jokainen leaf-kytkin yhdistyy kaikkiin spine-kytkimiin, määrää spinen porttitiheys leaf-kytkinten maksimimäärän. Spine-kytkinten tarve saadaan yhdistämällä tarvittu datan läpisyöttö (eng. throughput) leaf-kytkimelle sekä redundanttisten polkujen määrä leaf-kytkinten välillä.

3. Tarpeeksi tehokkaat uplinkit leaf- ja spine-kytkinten välillä. Tyypillisesti linkkiväli on 40 G tai 100 G. Ideaalitilanteessa uplinkit toimivat aina suuremmalla nopeudella, kuin downlinkit, ettei verkkoon synny ruuhkaa.

Laitevalmistaja FS:n tarjoamat leaf- ja spine-kytkimet sopivat hyvin Xamkin tarpeisiin. Ne tukevat suurinta osaa protokollista, eivät ole lisensoituja ja tukevat ohjelmoitavan datakeskusverkon mahdollistavia protokollia (muun muassa OpenFlow). Toisena yhtä hyvänä vaihtoehtona on laitevalmistaja Arista, joka tarjoaa samoilla kriteereillä vastaavia laitteita. Kuvasta 18 nähdään, että hintaerot Aristan sekä FS:n välillä ovat melko suuret ja FS tarjoaa paremman suoritustehon kytkimiä halvempaan hintaan.

Laite	Valmistaja	Hinta (kpl.)	Tyyppi	Muuta
N8560-32C	FS	11093€	Spine	32x100Gb QSFP28
N5860-48SC	FS	4456€	Leaf	48x10Gb SFP+, 8x100Gb
N8560-64C	FS	13466€	Spine	64x100Gb QSFP28
N8560-48BC	FS	6542€	Leaf	48x25Gb SFP28, 8x100Gb
DCS-7060CX-32S	Arista	17850€	Spine	32x100Gb QSFP
DCS-7050SX-64-F	Arista	7735€	Leaf	48x10G SFP+, 4xQFSP+

Kuva 18. Laitevalmistajien osoittamia hintoja kytkimille

8 TULOKSET

Tutkimusongelmasta johdettuihin kysymyksiin saatiin työn teoriaosuudessa vastaukset. Arkkitehtuurillisia ratkaisuja miettiessä nykypäivän datakeskusverkkosuunnitelmaan tulee ottaa huomioon ympäristön modernisoituminen sekä on-premise-datankäytön lisääntyminen. Arkkitehtonisia vaihtoehtoja toimivan datakeskusverkon suunnittelemiseksi olisi lukematon määrä, mutta niiden eroavaisuudet ovat käyttötarkoituksesta riippumatta todella pienet. Karkeasti jaettuna arkkitehtuurit pystytään lokeroimaan perinteisiin (kolmen tason malli) ja ”puumallista” johdettuihin vaihtoehtoihin (spine-leaf).

Arkkitehtuureja verrattaessa edut ovat selkeästi spine-leaf-arkkitehtuuriin päin, sillä sen utilisoima ECMP-protokolla ja sen myötä STP:n poisjäänti tekee verkon käyttäytymisestä ennakoitavaa ja tehokasta. Skaalautuvuutta ajatellen spine-leafiin voidaan tulevaisuudessa laajennusten takia vaivattomasti lisätä laitteita tarpeiden mukaan. Yhtenä tärkeimpänä etuna perinteiseen malliin verrattuna ja Xamkin tarpeita ajatellen on alus- ja päällysverkon tuomat hyödyt VXLAN:n ja ohjelmoitavan verkon myötä.

VXLAN on verkon virtualisoitumisen ja sen seurauksena VLAN:ien riittämättömyyden takia erinomainen keino segmentoida verkkoa lukemattomiin käyttötarkoituksiin. Ohjelmoitava verkko puolestaan vähentää järjestelmänvalvojan osallistumista sekä työkuormaa ylläpitoa varten. Se tuo myös uusia mahdollisuuksia verkon monitorointiin ja sen kehittämiseen. Paras verkkoratkaisu Xamkin uudelle kampukselle on spine-leaf-arkkitehtuuri sekä siihen mikä tahansa työssä esitellyistä alusverkko-protokollista VXLAN päällysverkkoa hyödyntäen.

9 JOHTOPÄÄTÖS

Opinnäytetyön vaatimukset ylätason suunnitelmasta laboratorioverkoksi saatiin toteutettua onnistuneesti ja perustellusti. Xamkin oppimateriaalista hyödynnetty ratkaisu on validi ja kevyt vaihtoehto verkon toteutukseen. Lopullinen suunnitelma jätettiin ylätasolle sen takia, että sitä on suhteellisen helppo jatkokehittää, eikä jatkokehityksiä toteutettaessa tule ristiriitoja esimerkiksi väärien protokollavalintojen tai muiden tietoteknisten ratkaisujen osalta.

Datakeskusverkkoon liitettävän työasemaverkon osuuden käsittely jätettiin pois, sillä se ei ollut relevantti lopullisen tuloksen kannalta. Työasemaverkko voidaan liittää, kun lopullinen päätös käytettävästä verkkoratkaisusta on tehty.

Opinnäytetyö antaa mahdollisuuden puntaroida eri valintojen välillä, kun verkkoa aletaan lopulta rakentamaan uuden kampuksen valmistuessa. Alusverkon protokollan valinnan kannalta ei ole suoraa vastausta, sillä jokainen (IS-IS, OSPF, BGP) toimii yhtä hyvin mihin tahansa käyttötarkoitukseen. Topologiassa oleviin Proxmox-hypervisoreihin voidaan konfiguroida verkon ohjelmoitavuutta helpottavia aspekteja, sekä laitevalintaehdotuksilla verkkoa on mahdollista käyttää ilman sitoutumista yhteen tiettyyn valmistajaan.

9.1 Pohdinta

Tärkein asia opinnäytetyön lopputuotoksena oli, että työssä opittiin paljon verkon suunnittelusta lisää ja saatiin vahvat perusteet tulevaisuutta varten vastaavien ratkaisuiden toteuttamiseen. Ylätason suunnitelma ei ollut kaikista haasteellisin vaihtoehto toteuttaa, vaan verkkoa olisi voinut testata useista eri näkökulmista.

Tähän ratkaisuun päädyttiin kuitenkin ajankäytön säästämiseksi, sillä jos verkon olisi rakentanut aivan valmiiksi kaikki sen aspektit huomioiden, olisi mahdollisten, tekijästä riippumattomien muutosten tullessa uudelle kampukselle koko suunnitelma mennyt uusiksi.

Kriittisestä näkökulmasta tarkasteltuna työssä olisi voitu perehtyä enemmän ohjelmoitavan verkon toimintaan ja sen implementointiin, sillä se on ehdottomasti yksi tulevaisuuden datakeskusverkon kulmakivistä. Myös BGP:n syvempi tarkastelu olisi ollut hyvä lisä työhön, sillä sen toiminta on hyvin erilaista verrattuna perinteisiin IGP-protokolliin.

9.2 Jatkokehitys

Verkon kehitystä voidaan jatkaa eteenpäin implementoimalla *Zero Trust* -turvallisuusmallin mukaista politiikkaa. Zero Trust eli ”luottamattomuuden periaate” on kehitetty modernien ja nopeasti kehittyvien ICT-ympäristöjen suunnit-

teluun. Se auttaa rakentamaan tietoturvaa nykypäivän monimutkaisessa maailmassa, jossa eri ICT-järjestelmät integroituvat toisiinsa. Zero Trust -mallin perustana on nimensä mukaisesti, että luottamus on nolla kaikilla ajan hetkillä. Laitteet ja käyttäjät tunnistetaan kaikissa tilanteissa ja päätös pääsyn sallimisesta perustuu riskiarvioon. Vahvan tunnistautumisen käyttö on yksi perusasioita. (Salo 2021.)

Toinen jatkokehitysidea työasemaverkon liittämisen mukaan tullessa datakeskusverkkoon on privaatti VLAN (Private VLAN, PVLAN), toiselta nimeltään portin eristys. Se on verkon eristystekniikka layer 2 -verkoille, joka mahdollistaa liikenteen tai portin eristämisen samassa IP-segmentissä. PVLAN:n käyttöönotto verkossa säästää IP-osoitteita sekä tuo kytkimelle lisää porttiturvallisuutta layer 2 -tasolla. (FS-Community 2022b.)

Kolmantena ajatuksena jatkoa varten on VXLAN-GPB:n käyttöönotto, johon on viitattu luvussa 4.1. Sen tuoma mikro- ja makrotason segmentointi verkossa on hyvä lisä tärkeiden tietojen suojaksi. VXLAN-GBP:n mahdollistama segmentointi on erityisen hyödyllinen kampuksen VXLAN-ympäristöissä, koska se antaa käytännöllisen tavan luoda verkon pääsykäytäntöjä, jotka ovat riippumattomia taustalla olevasta verkkotopologiasta. Se yksinkertaistaa verkkosovellusten ja päätelaitteiden suojauskäytäntöjen kehittämisen. (Kreeger & Smith 2018.)

LÄHTEET

Alcatel-Lucent. 2015. 7705 SAR OS Routing Protocols Guide R6.2.R1. WWW-dokumentti. Saatavissa: https://infocenter.nokia.com/public/770562R1A/index.jsp?topic=%2Fcom.sar.routing_protocols%2Fhtml%2Fisis.html [viitattu 21.03.2022].

Argawal, P., Bursell, M., Duda, K., Dutt, D., Kreeger, L., Mahalingam, M., Sridhar, T. & Wright, C. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/rfc7348 [viitattu 23.03.2022].

Azam, W. s.a. Cisco 3 layer Hierarchial Network Model | Core | Distribution | Access. WWW-dokumentti. Saatavissa: https://w7cloud.com/cisco-3-layer-hierarchical-network-model-core-distribution-access/ [viitattu 15.02.2022].

Battacharya, A. 2021. VXLAN, OVSDB, and BGP EVPN – 3 pillars of data center overlay. WWW-dokumentti. Saatavissa: https://blogs.keysight.com/blogs/tech/trafgen.entry.html/2021/03/25/vxlan_ovsdb_and_bg-5d8X.html [viitattu 05.05.2022].

Black, C. & Goransson, P. 2014. Software Defined Networks: A Comprehensive Approach. Waltham: Elsevier Science & Technology.

Bouguerra, F. 2021. Data centre networking: SDN fundamentals. WWW-dokumentti. Saatavissa: https://ubuntu.com/blog/data-centre-networking-sdn-fundamentals [viitattu 01.03.2022].

Callon, R. 1990. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/rfc1195 [viitattu 21.03.2022].

Cloudfare. s.a. What is the control plane? | Control plane vs. data plane. WWW-dokumentti. Saatavissa: https://www.cloudflare.com/learning/network-layer/what-is-the-control-plane/ [viitattu 28.02.2022].

Duan, Q. & Mehmet, T. 2016. Virtualized Software-Defined Networks and Services. Norwood: Artech House.

Earls, A. 2022. Key data center trends in 2022. WWW-dokumentti. Saatavissa: https://www.techtarget.com/searchdatacenter/tip/Key-data-center-trends [viitattu 13.05.2022].

Forcepoint. s.a. What is the OSI Model? WWW-dokumentti. Saatavissa: https://www.forcepoint.com/cyber-edu/osi-model [viitattu 21.02.2022].

FS-Community. 2022a. What Is Leaf-Spine Architecture and How to Design It. WWW-dokumentti. Saatavissa: https://community.fs.com/blog/leaf-spine-with-fs-com-switches.html [viitattu 17.05.2022].

FS-Community. 2022b. What Is Private VLAN and How It Works? WWW-dokumentti. Saatavissa: https://community.fs.com/blog/what-is-private-vlan-and-how-it-works.html [viitattu 18.05.2022].

Ganesh, S. 2021. The data center of the future. PDF-dokumentti. Saatavissa: https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2021KS_Ganesh-The_Data_center_of_the_Future.pdf [viitattu 11.04.2022].

Garg, P. & Wang, Y. 2015. NVGRE: Network Virtualization Using Generic Routing Encapsulation. WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/rfc7637 [viitattu 26.03.2022].

Geng, H. 2015. Data center handbook. New Jersey: John Wiley & Sons Inc.

Hares, S., Li, T. & Rekhter, Y. 2006. A Border Gateway Protocol 4 (BGP-4). WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/rfc4271 [viitattu 17.05.2022].

Hosken, M. 2016. VMware: Software-Defined Storage: A Design Guide to the Policy-Driven, Software-Defined Storage Era. Indianapolis: John Wiley & Sons Inc.

IBM Global Technology Services. 2016. The next-generation data center: A software defined environment where service optimization provides the path. PDF-dokumentti. Saatavissa: https://www.ibm.com/downloads/cas/MVWBAJE4 [viitattu 12.04.2022].

ISO/IEC 10589:2002. 2002. International standard. PDF-dokumentti. Saatavissa: https://standards.iso.org/ittf/PubliclyAvailableStandards/c030932_ISO_IEC_10589_2002(E).zip [viitattu 16.03.2022].

Jamk. 2021. Opinnäytetyön ohjaajan käsikirja. WWW-dokumentti. Saatavissa: https://oppimateriaalit.jamk.fi/yamk-kasikirja/tyoelaman-tutkiva-kehittamistoiminta/projektityo-vs-ns-toiminnallinen-tutkimuksellinen-kehittamishanke-opinnaytetyo/ [viitattu 11.02.2022].

Jarschel, M., Pries, R., Schlosser, D. & Tran-Gia, P. Power Consumption Analysis of Data Center Architectures. PDF-dokumentti. Saatavissa: https://www.researchgate.net/profile/Rastin-Pries/publication/220018693_Power_Consumption_Analysis_of_Data_Center_Architectures/links/5649f66008ae295f644f9937/Power-Consumption-Analysis-of-Data-Center-Architectures.pdf?origin=publication_detail [viitattu 18.05.2022].

Juniper Networks. 2021. Ethernet Switching User Guide. WWW-dokumentti. Saatavissa: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/layer-2-understanding.html [viitattu 17.02.2022].

Kreeger, L. & Smith, M. 2018. VXLAN Group Policy Option. WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/draft-smith-vxlan-group-policy-05 [viitattu 10.05.2022].

Moy, J. 1998. OSPF Version 2. WWW-dokumentti. Saatavissa: https://datatracker.ietf.org/doc/html/rfc2328 [viitattu 15.03.2022].

Network Centre. 2018. Advantages of spine-and-leaf architecture. WWW-dokumentti. Saatavissa: http://www.networkcentre.net/advantages-of-spine-and-leaf-architecture/ [viitattu 12.05.2022].

Route-XP. s.a. Difference between Underlay and Overlay Networks. WWW-dokumentti. Saatavissa: https://www.routexp.com/2019/09/difference-between-underlay-and-overlay.html [viitattu 24.02.2022].

Salo, A. 2021. Zero Trust – Nollaluottamus modernin turvallisen ICT-ympäristön perustana. WWW-dokumentti. Saatavissa: https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/ [viitattu 09.05.2022]

Sheldon, D. & Younger, R. 2022. Comparing Two-Tier and Three-Tier Data Center Networks. WWW-dokumentti. Saatavissa: https://www.wwt.com/article/comparing-two-tier-three-tier-data-center-networks [viitattu 18.02.2022].

Silverman, B. & Solber, M. 2018. OpenStack for Architects: Design production-ready private cloud infrastructure. Birmingham: Packt Publishing Ltd.

Taylor, J. 2018. VXLAN explained. WWW-dokumentti. Saatavissa: https://medium.com/@NTTICT/vxlan-explained-930cc825a51 [viitattu 24.02.2022].

Tarkoma, S. 2010. Overlay Networks: Toward Information Networking. Boca Raton: CRC Press.

Techopedia. s.a. Data Center Architecture. WWW-dokumentti. Saatavissa: https://www.techopedia.com/definition/29867/data-center-architecture [viitattu 08.04.2022].

Versitron. s.a. Understand the Use of Core Switches, Distribution Switches, and Access Switches in Ethernet Networks. WWW-dokumentti. Saatavissa: https://www.versitron.com/whitepaper/use-of-core-switches-distribution-switches-and-access-switches [viitattu 15.02.2022].

Xamk. 2021. Xamkin avainluvut. WWW-dokumentti. Saatavissa: https://www.xamk.fi/xamk/xamkin-avainluvut/ [viitattu 08.02.2022].