Haaga-Helia
ammattikorkeakoulu Oy

Suljetun lähiverkon uusiminen

Teppo Viljanen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Teppo Viljanen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Suljetun lähiverkon uusiminen

Sivu- ja liitesivumäärä
43 + 1

Tänä päivänä organisaatioiden liiketoiminta on yhä riippuvaisempaa verkkoyhteyksistä. Erilaiset pilvipalvelut näyttelevät kasvavaa roolia organisaatioiden toiminnassa ja organisaatioiden sisäinen ja ulkoinen viestintä vaativat toimiakseen toimivia verkkoyhteyksiä. Nämä kaikki yhdessä aiheuttavat uudistustarpeita verkkoyhteyksille. Verkkoyhteyksien tuleekin tukea organisaatioiden liiketoimintaa turvallisella ja toimintavarmalla tavalla.

Tämän opinnäytetyön tarkoituksena on selvittää mitkä ovat keskeiset huomioitavat seikat lähiverkkoa suunniteltaessa huomioiden mahdolliset verkon laajentamistarpeet tulevaisuudessa sekä tietoturva. Työn tavoitteena on suunnitella ja toteuttaa julkisen sektorin organisaatiolle lähiverkon uudistaminen siten, että verkko vastaa tämän hetken vaatimuksia ja että se on laajennettavissa tulevaisuudessa ilman että sitä pitää suunnitella uudelleen.

Työn tietoperusta on jaettu kahteen osaan. Ensimmäisessä osassa käsitellään lähiverkkoa yleisellä tasolla, sen kuvaamista, siinä toimivia aktiivilaitteita sekä kaapeleita, nopeuksia ja virtuaalisia lähiverkkoja. Toisessa osassa käsitellään lähiverkon suunnittelua ja siinä huomioitavia seikkoja, kuten IP-osoitteita, verkon segmentointia, vikasietoisuutta ja tietoturvaa.

Opinnäytetyön produktiivisessa osassa toteutettiin lähiverkon uusimisen suunnittelu ja lähiverkon uudistaminen suunnittelun pohjalta. Työ piti sisällään palvelimen ja iSCSI-tallennusalustan uusimisen, tietojärjestelmien siirtämisen vanhasta palvelimesta uuteen, uusien kytkinten käyttöönoton, kaapeleiden vaihtamisen ja kytkennät sekä vanhan palvelimen siirtämisen varmistuspalvelimeksi.

Työn lopputuloksena valmistui lähiverkko, johon liitettyjen työasemien määrä kasvoi, tallennustilan määrä lisääntyi ja osa lähiverkosta nostettiin toimimaan suuremmalla nopeudella.

Asiasanat
Tietoverkot, Ethernet, Windows Server

Sisällys

1 Johdanto

Yksityiset sekä julkiset organisaatiot kehittyvät ja muuttuvat kaiken aikaa. Samoin niiden toiminnalle asetettavat vaatimukset. Verkkoyhteyksien tulee tukea organisaatioiden liiketoimintaa ja mahdollistaa organisaatioiden sisäinen ja ulkoinen viestintä turvallisella ja toimintavarmalla tavalla. Tämä aiheuttaa uudistustarpeen niin verkkoyhteyksille kuin tiedon tallennustilalle ja -tavallekin. Esimerkkeinä tästä ovat kaupankäynnin siirtyminen verkkoon kasvavassa määrin, pilvipalveluiden kehittyminen ja yleistyminen sekä viestinnän saamat uudet muodot chat-palveluiden myötä.

Rakennettaessa uusia tai uudistettaessa vanhoja verkkoyhteyksiä tulee nykyhetken lisäksi huomioida tulevaisuuden näkymät. Jo suunnitteluvaiheessa pitäisi pystyä näkemään tulevaan ja suunnitella järjestelmät ja yhteydet siten, että niitä on mahdollista laajentaa toimintatarpeen niin vaatiessa.

Tiedon siirtämiseen ja jakamiseen tarvitaan verkkoyhteyksiä. On tärkeää, että tuotettu tieto saadaan niiden ulottuville, jotka sitä tarvitsevat. Tiedon pitää olla saatavilla silloin kuin sitä tarvitaan, siihen tulee olla pääsy vain niillä, joilla on oikeus käsitellä tietoa ja tiedon tulee olla muuttumatonta eli säilyä juuri siinä muodossa, jossa se on tuotettu. Lisäksi häiriöiden sattuessa verkkoyhteyksien tulee palata toimiviksi mahdollisimman nopeasti.

Tässä opinnäytetyössä on tarkoitus selvittää, mitkä ovat keskeiset huomioitavat seikat lähiverkkoa suunniteltaessa ja uudistettaessa siten, että mahdollinen laajeneminen tulevaisuudessa on huomioitu. Lisäksi työssä on tarkoitus selvittää, miten pieni lähiverkko uudistetaan tietoturva huomioiden.

Opinnäytetyön tavoitteena on suunnitella ja toteuttaa julkisen sektorin organisaation tietyn yksikön käytössä oleva lähiverkko vastaamaan tämän hetken vaatimuksia ja huomioida tulevaisuudessa mahdollisesti tulevat verkon laajentamistarpeet. Tämän työn seurauksena lähiverkko tulee laajenemaan, sen suorituskyky kasvaa ja sitä käyttävien henkilöiden määrä tulee lisääntymään. Lisäksi lähiverkon dokumentaatio saatetaan ajan tasalle.

Ensimmäisessä osassa käydään läpi lähiverkon ominaisuuksia yleisellä tasolla, verkon kuvaamista topologioiden avulla, verkossa toimivia aktiivilaitteita sekä lähiverkon nopeuksia sekä virtuaalisia lähiverkkoja. Toisessa osassa käsitellään lähiverkon suunnittelua, IP-osoitteita, verkon segmentointia ja vikasietoisuutta sekä kaapelointia, tietoturvaa ja mahdollisia ongelmatilanteita. Lopuksi toteutetaan opinnäytetyön toimeksiantajalle pienen lähiverkon uudistaminen suunnittelusta toteutukseen.

2 Keskeiset käsitteet

10 GigabitEthernet	Nimitys 10 Gbit/s tiedonsiirtonopeuteen kykeneville lähiverkkotekniikoille.
ACL	Pääsynhallintalista, jonka perusteella voidaan suodattaa datapaketteja. Pääsynhallintalistan avulla voidaan määrittää käyttäjien oikeuksia kansioille, palomuurin sääntöjä ja verkkolaitteiden reitityskäytäntöjä.
Broadcast	Yleislähetys, nämä viestit lähetetään verkon kaikille laitteille.
Klusteri	Tilanvarausyksikkö, joka on tallennusvälineen esimerkiksi kiintolevyn tai muistitikun pienin osoitettavissa oleva yksikkö.
DHCP	Verkkoprotokolla, joka tulee sanoista Dynamic Host Configuration Protocol. Se jakaa lähiverkkoon kytketyille laitteille IP-osoitteen, mikäli niillä ei ole kiinteää IP-osoitetta.
DNS	Nimipalvelujärjestelmä. joka tulee sanoista Domain Name System. Se muuntaa internetin verkko-osoitteet IP-osoitteiksi.
FastEthernet	Nimitys 100 Mbit/s tiedonsiirtonopeuteen kykeneville lähiverkkotekniikoille.
GigabitEthernet	Nimitys 1 Gbit/s tiedonsiirtonopeuteen kykeneville lähiverkkotekniikoille.
IP-osoite	Verkko-osoite, joka mahdollistaa päätelaitteiden kommunikoinnin toisten päätelaitteiden kanssa internetissä tai eri verkkojen välillä. IP-soitteita on kahta versiota IPv4 ja IPv6.
iSCSI	OSI-mallin kuljetuskerroksen protokolla, joka mahdollistaa tallennusalustojen liittämisen palvelimiin LAN ja WAN -verkoissa. Se tulee sanoista internet Small Computer System Interface.
LAN	Local Area Network eli lähiverkko. Lähiverkko on pienellä rajoitetulla alueella toimiva tietoliikenneverkko.
LEMP	Avoimen lähdekoodin ohjelmistokokonaisuus, joka mahdollistaa selaimella käytettävien sovellusten ja web -sivustojen luomisen ja käyttämisen. Se tulee sanoista Linux (käyttöjärjestelmä), Nginx (web -palvelin), MySQL (relaatiotietokanta) ja PHP (ohjelmointikieli)
MAC-osoite	Media Access Control -osoite, joka on verkkokortin osoite. Se yksilöi päätelaitteen lähiverkossa.
Multicast	Ryhmälähetys. Nämä viestit lähetetään yhdeltä päätelaitteelta usealle päätelaitteelle.

OSI-malli	Open Systems Interconnection Reference Model. Se koostuu seitsemästä kerroksesta ja kuvaa tiedonsiirtoprotokollien toiminnot ja palvelut eri kerroksissa sekä vierekkäisten kerrosten vuorovaikutukset.
Ping	Ohjelma, jolla voidaan testata toisen laitteen saavutettavuutta verkossa. Ping lähettää ICMP echo -pyynnön, johon tavoiteltava laite vastaa, mikäli vastaanottaa pyynnön.
RAID	Tekniikka, jolla useita fyysisiä levyjä yhdistetään yhdeksi loogiseksi kokonaisuudeksi. Tällä tavoitellaan vikasietoisuutta ja nopeutta.
Unicast	Täsmälähetys. Yhden koneen lähettämä viesti yhdelle vastaanottajalle.
UPS	Laite tai järjestelmä, joka huolehtii katkeamattomasta virransyötöstä lyhyiden sähkökatkosten aikana. Se myös tasaa jännitevaihteluja. UPS tulee sanoista Uninterruptible Power Supply.
VirtualBox	Oracle VM VirtualBox on avoimen lähdekoodin hypervisori, jonka avulla voi virtualisoida käyttöjärjestelmiä ja muita ohjelmia toimimaan isäntäkäyttöjärjestelmän päällä.
WAN	Wide Area Network eli laajaverkko. Laajaverkko kattaa laajoja maantieteellisiä alueita yhdistämällä lähiverkot laajemmaksi tietoliikenneverkoksi.
VLAN	Virtual Local Area Network eli virtuaalinen lähiverkko. Sen avulla fyysinen verkko voidaan jakaa useisiin loogisiin verkkoihin, jotka käyttävät yhtä fyysistä verkkoa.
WLAN	Wireless Local Area Network eli langaton lähiverkko, jossa data kulkee sähkömagneettisina radioaaltoina.
Volume	Fyysisen tallennusalustan looginen osa, jolla on oma tiedostojärjestelmä. Yleisesti Volumeksi kutsutaan fyysisen tallennusalustan partitiota eli eriytettyä osaa tai usean levyn muodostamaa loogista kokonaisuutta.

3 Lähiverkko

Lähiverkko on englanninkieliseltä nimeltään Local Area Network (LAN). Englanninkielinen nimi kuvastaa hyvin lähiverkon olemusta, koska se on verkko, joka rajoittuu pienelle, rajatulle alueelle, kuten kotiin, yritykseen tai vaikkapa kouluun. Yleensä lähiverkkoa hallinnoi yksi organisaatio, esimerkkinä yrityksen lähiverkko tai yksi henkilö, esimerkkinä kodin lähiverkko. Yksinkertaisimmillaan lähiverkko on muutaman laitteen muodostama verkko. Vastaavasti taas suurten yritysten lähiverkot voivat olla todella suuria ja monimutkaisia kokonaisuuksia.

Lähiverkkojen kokoa määriteltäessä voidaan käyttää useita eri kriteerejä. Tällaisia kriteerejä ovat muun muassa verkon käyttäjien määrä, verkossa toimivien laitteiden määrä tai verkon tarjoamien palveluiden määrä. Eri tahot luokittelevat verkkojen koon eri kriteerien ja kulloisenkin kuvaustarpeen mukaan. Cisco (Cisco Network Academy 2014) luokittelee verkkojen koon siinä toimivien laitteiden määrän mukaan:

- Pieni verkko: Verkossa toimii enintään 200 laitetta
- Keskikokoinen verkko: Verkossa toimii 200 - 1.000 laitetta
- Suuri verkko: Verkossa toimii yli 1.000 laitetta.

Lähiverkkojen ja yleensäkin verkkojen kehitystä kuvaa hyvin se, että ennen data, puhelinliikenne ja televisioiden kuvaliikenne kulkivat omia verkkojaan pitkin. Jokainen näistä verkoista toimi omalla teknologiallaan, eivätkä verkot pystyneet kommunikoimaan keskenään. Lisäksi jokaista näistä verkoista piti hallinnoida ja huoltaa erikseen. Tänä päivänä samassa lähiverkossa kulkevat niin ääniviestit, IP-puhelut, videokuva kuin dataliikennekin. Tämän etuna vanhaan on se, että ei tarvitse asentaa kuin yksi verkko, jota voidaan hallinnoida ja huoltaa keskitetysti. Tämä tosin lisää verkon monimutkaisuutta ja verkossa toimivien laitteiden määrää. (Cisco Networking Academy 2016a, 1.3.1.1 - 1.3.1.2; Cisco Networking Academy 2016b, 4.1.1.2.)

Lähiverkkoja on kahdenlaisia: langallisia ja langattomia. Langallisessa lähiverkossa data kulkee kaapeleita pitkin eri laitteiden välillä. Langallisessa lähiverkossa käytettävät kaapelit ovat joko kuparikaapeleita, joissa data kulkee sähköisinä sysäyksinä eli impulsseina tai optisia kuitukaapeleita, joissa data kulkee valopulsseina. Langattomassa verkossa data kulkee sähkömagneettisina radioaaltoina. (Cisco Networking Academy 2016a, 1.2.1.4.)

Lähiverkon infrastruktuuri koostuu kolmesta pääkategoriasta: laitteet, siirtomedia ja palvelut. Verkossa toimivat laitteet voidaan jakaa kahteen eri kategoriaan: päätelaitteisiin ja välittäjälaitteisiin. Päätelaitteita ovat muun muassa tietokoneet, tulostimet ja IP-puhelimet. Välittäjälaitteita ovat reititin, langaton reititin, kytkin ja keskitin. Näitä laitteita käsitellään

tarkemmin myöhemmin tässä luvussa. Media käsittää laitteita yhdistävät kaapelit, joita pitkin data kulkee. Sekä laitteet että media ovat fyysisiä verkon osia, jotka on helppo tunnistaa. Palvelut vastaavasti ovat verkon käyttäjien käyttämiä ohjelmistoja tai prosesseja, jotka liikuttavat dataa verkossa ja ovat siten keskeisiä osia verkon toiminnassa, vaikka helposti jäävätkin vähemmälle huomiolle kuin fyysiset laitteet. (Cisco Networking Academy 2016a, 1.2.1.1.)

Lähiverkkotekniikat mahdollistavat suuria nopeuksia siinä olevien laitteiden väleille. Nopeudet ovat vuosien saatossa nousseet huimasti. Lähiverkon yleinen nopeus on joskus ollut 10 Mbit/s. Tämän jälkeen kehitettiin FastEthernet, joka mahdollisti 100 Mbit/s nopeudet. Tätä seurasi GigabitEthernet, joka pystyy tarjoamaan 1.000 Mbit/s (1 Gbit/s) nopeuden. Seuraava vaihe oli 10 GigabitEthernet, joka mahdollistaa 10 Gbit/s nopeuden. Lähiverkon nopeuteen vaikuttavat keskeisesti päätelaitteiden verkkokortit, välittäjälaitteiden portit sekä laitteiden yhdistämisessä käytetyt kaapelit. (Cisco Networking Academy 2016a, 5.1.1.3.) Lähiverkon nopeuksia ja niiden suhdetta käytettäviin kaapeleihin käsitellään tarkemmin myöhemmin tässä luvussa.

3.1 Topologiat

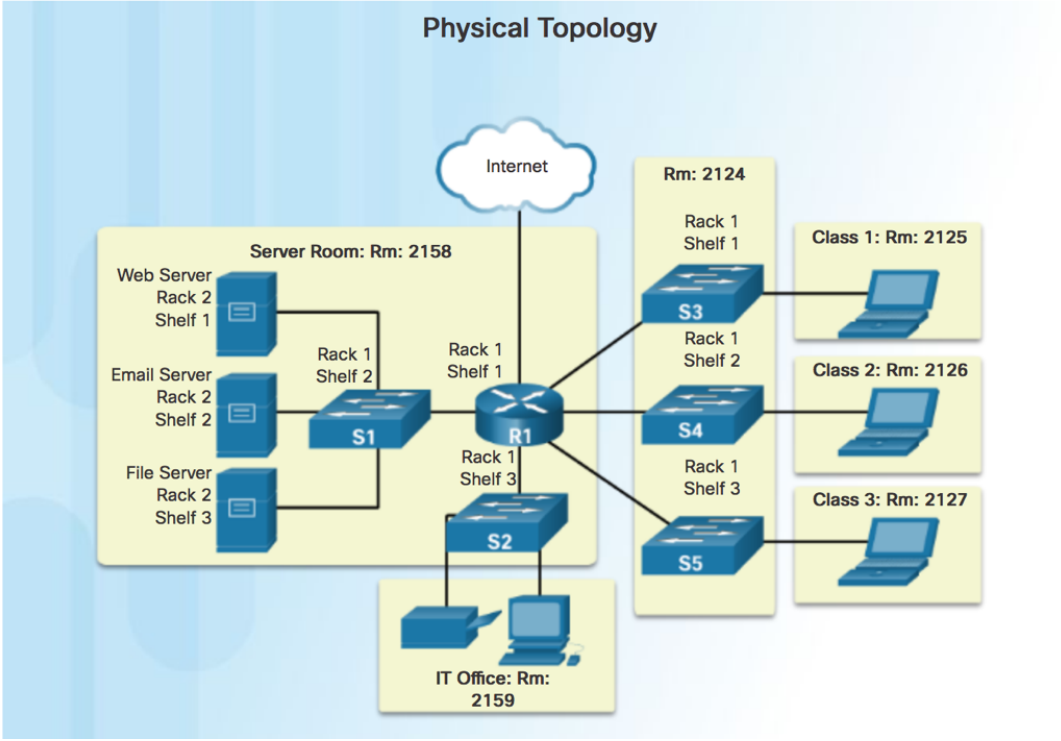
Lähiverkon rakennetta kuvataan topologiadiagrammien avulla. Topologiat visualisoivat verkon rakenteen ja niitä voidaankin kutsua verkkoa kuvastaviksi kartoiksi. Topologiadiagrammit ovat lähes välttämättömiä verkkojen kanssa työskenteleville. Ne auttavat saamaan kokonaiskuvan verkosta ja omalta osaltaan helpottavat vikatilanteiden selvittämisessä. Tästä syystä onkin tärkeää, että verkon laajentuessa tai muuten muuttuessa, topologiadiagrammeja päivitetään vastaamaan kulloistakin verkon rakennetta. (Cisco Networking Academy 2016a, 1.2.1.6.)

Topologiadiagrammit jaetaan kahteen eri kategoriaan: fyysiseen topologiaan ja loogiseen topologiaan.

3.1.1 Fyysinen topologia

Fyysinen topologia yksilöi laitteiden sijainnin ja kuvaa laitteiden välisen kaapeloinnin eli miten laitteet ovat liitetty toisiinsa (Cisco Networking Academy 2016a, 1.2.1.6).

Seuraava kuvio havainnollistaa mistä fyysisessä topologiadiagrammissa on kyse ja millä tarkkuudella se olisi hyvä laatia. Siitä ilmenee laitteiden fyysinen sijainti huoneittain räkki ja hylly kohtaisesti, keskeisten laitteiden nimet sekä niiden yhteydet toisiinsa.



Kuvio 1. Esimerkki fyysisestä topologiadiagrammista (Cisco Networking Academy 2016a, 1.2.1.6)

Fyysisiä topologioita voidaan kuvata myös yleisellä tasolla helpottamaan lähiverkkojen kuvaamista. Yleisimpiä yleisellä tasolla verkkoja ja kaapelointeja kuvaavia fyysisiä topologioita ovat: väylä-, rengas-, tähti-, laajennettu tähti-, hierarkkinen ja mesh-topologia (Philpott 2015).

Väylätopologiassa (Bus) jokainen verkon kone ja oheislaite on liitetty yhteen runkokaapeliin. Väylätopologia sopii hyvin pieniin lähiverkkoihin. Tämän topologian etuna on sen yksinkertainen liitettävyys ja se pystytään toteuttamaan lyhyemmällä kaapeloinnilla kuin esimerkiksi tähtitopologia. Haittapuolia siinä ovat muun muassa se, että vian paikallistaminen on vaikeaa, mikäli koko verkko kaatuu ja laitemäärän lisääntyessä verkon nopeus laskee. (Computer Hope 2018a.)

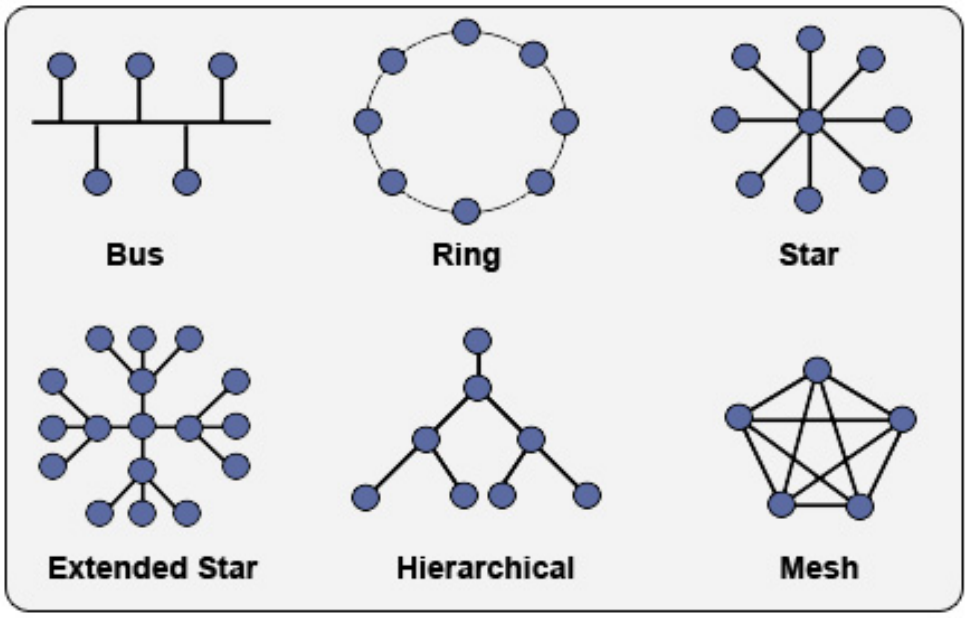
Rengastopologiassa (Ring) jokainen laite on kytketty kahteen muuhun laitteeseen ja laitteet muodostavat keskenään ympyrän. Tässä topologiassa data kulkee laitteelta toiselle, kunnes se saavuttaa määränpäänsä. Useimmat rengastopologiat mahdollistavat datan kulkemisen ainoastaan yhteen suuntaan. Nykyään on myös rengastopologioita, jotka mahdollistavat datan kulkemisen molempiin suuntiin. Yhtenä etuna tässä topologiassa on, että siihen voi lisätä laitteita ilman, että se vaikuttaa verkon suorituskykyyn. Vastaavasti yhtenä haittapuolena on, että yhden päätelaitteen sammuessa se vaikuttaa koko verkon toimintaan. (Computer Hope 2018b.)

Tähtitopologia (Star) on yksi yleisimmistä fyysisistä topologioista. Tähtitopologiassa jokainen päätelaite on yhdistetty keskellä olevaan välittäjälaitteeseen, joka voi olla esimerkiksi kytkin tai keskitin. Sen etuina ovat, että siihen on helppo lisätä päätelaitteita ja mikäli yksi verkon päätelaitteista vikaantuu, niin muu verkko toimii edelleen normaalisti. Tämän topologian haittapuolia ovat muun muassa, että jos keskellä oleva välittäjälaite hajoaa, niin kaikki siinä kiinni olevat laitteet menettävät yhteyden verkkoon sekä se, että keskellä oleva välittäjälaite määrittelee verkossa toimivien laitteiden määrän. (Computer Hope 2018c.)

Laajennettu tähtitopologia (Extended Star) pohjautuu nimensä mukaisesti tähtitopologiaan. Siinä tähden sakaroita on laajennettu välittäjälaitteilla, mikä mahdollistaa sen, että verkkoon on voitu lisätä päätelaitteita enemmän kuin keskellä olevassa välittäjälaitteessa on liitäntäportteja. Tässä topologiassa on käytännössä samat edut ja haittapuolet kuin tähtitopologiassa.

Hierarkkinen topologia (Hierarchical) muistuttaa puuta ja siinä on paljon samaa kuin laajennetussa tähtitopologiassa. Hierarkkinen topologia eroaa laajennetusta tähtitopologiasta siten, että siinä ei ole kaikkia päätelaitteita yhdistävää välittäjälaitetta. Tämän topologian etuna on, että verkon nopeus ja kapasiteetti voidaan suunnitella erikseen jokaiselle hierarkian tasolle ja se on kustannustehokas, koska siinä ei tarvitse hankkia laitteita sellaisilla ominaisuuksilla, joita ei tarvita. Haittapuolena tässä on se, että jos runkokaapeli vaurioituu, niin verkon toiminta lamaantuu. (Arslan 2015; eTutorials 2018.)

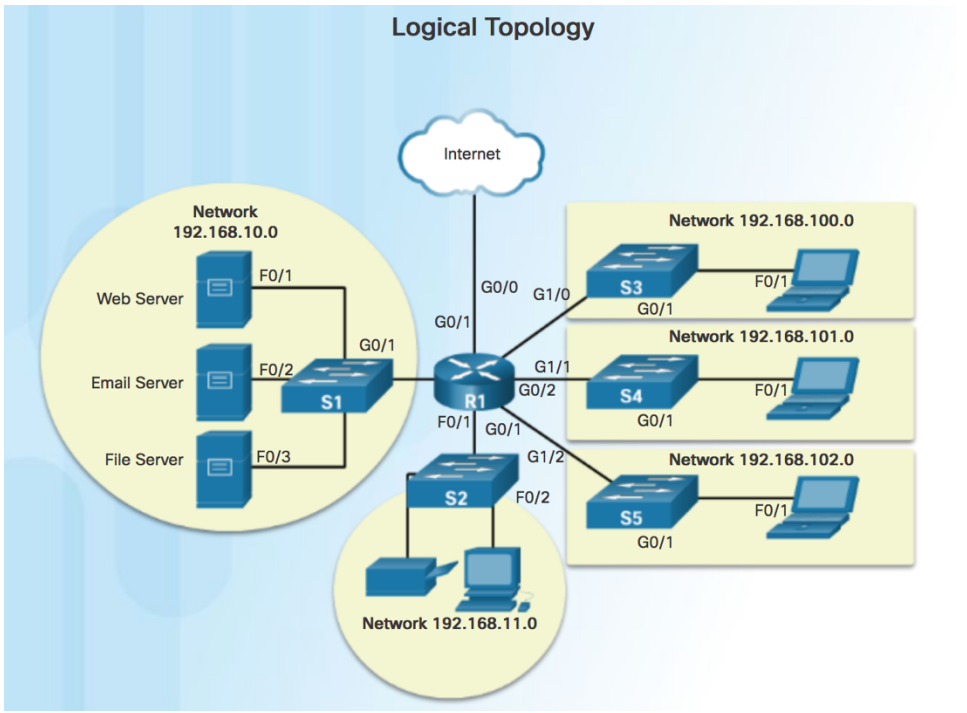
Mesh-topologiassa (Mesh) verkon jokainen päätelaite on yhdistetty kaikkiin toisiin verkossa oleviin laitteisiin. Tätä topologiaa käytetään yleisimmin langattomissa verkoissa. Tämän topologian etuina ovat ne, että usea päätelaite pystyy lähettämään dataa saman aikaisesti, mikä mahdollistaa suuret liikennemäärät sekä se, että yhden päätelaitteen rikkoontuminen ei aiheuta katkoksia datan lähettämiseen. Haittapuolena tässä on se, että sen toteuttaminen on kalliimpaa kuin muiden topologioiden ja tällaisen verkon rakentaminen ja ylläpitäminen on hankalaa. (Computer Hope 2017.)



Kuvio 2. Yleisimmät fyysiset verkkotopologiat (Philpott 2015)

3.1.2 Looginen topologia

Siinä missä fyysinen topologiadiagrammi kuvaa laitteiden fyysisen sijainnin ja miten ne liittyvät toisiinsa, looginen topologiadiagrammi yksilöi laitteet, käytössä olevat portit sekä IP-osoitteiston. Looginen topologiadiagrammi täydentää fyysistä topologiaa ja yhdessä ne antavat kattavan kuvan verkosta (Cisco Networking Academy 2016a, 1.2.1.6).



Kuvio 3. Esimerkki loogisesta topologiadiagrammista (Cisco Networking Academy 2016a, 1.2.1.6)

3.2 Ciscon hierarkkinen verkkomalli

Esimerkkinä paljon käytetystä verkkotopologista on Ciscon hierarkkinen verkkomalli. Sen pääperiaatteita ovat hierarkkisuus (hierarchical), modulaarisuus (modularity), vikasietoisuus (resilency) ja joustavuus (flexibility). Nämä eivät ole toisistaan irrallisia periaatteita vaan ne nivoutuvat saumattomasti yhdeksi kokonaisuudeksi ja tukevat toinen toisiaan. (Al-Shawi & Laurent 2016, luku 1.)

Hierarkkisuus tarkoittaa, että verkko pilkotaan modulaarisiin ryhmiin tai kerroksiin. Kokonaisuuden pilkkominen kerroksiin edesauttaa saamaan selkeän kuvan jokaisen verkossa toimivan laitteet roolista, toimi se missä kerroksessa vain. Lisäksi se yksinkertaistaa verkon käyttöönottoa, toimintaa ja ylläpitoa. (Al-Shawi & Laurent 2016, luku 1.)

Modulaarisuus on sitä, että kokonaisuus koostuu itsenäisistä palasista, moduuleista. Sen suurimpana etuna on, että yhteen moduuliin tuleva vika voidaan havaita helpommin ja vikatilassa oleva moduuli voidaan eristää muusta verkosta, jolloin sen vaikutukset muuhun verkkoon saadaan mahdollisimman pieniksi. Lisäksi moduuleja voidaan helposti päivittää nykyisiä tarpeita vastaavaksi tai niitä voidaan lisätä sekä poistaa ilman, että koko verkkoa tarvitsee suunnitella uudelleen. (Al-Shawi & Laurent 2016, luku 1.)

Vikasietoisuudella tarkoitetaan verkon kykyä olla toiminnassa ilman katkoksia. Tämä on erityisen tärkeää, koska tämän päivän liike-elämän vaatimukset edellyttävät katkeamatonta datavirtaa. Verkon tulee toimia niin normaalioloissa kuin epänormaaleissa oloissa. Epänormaaleiksi oloiksi voidaan laskea laite- tai ohjelmistoviat, epänormaalin suuret datavirrat, kuten palvelunestohyökkäykset tai muut suunnittelemattomat tapahtumat. (Al-Shawi & Laurent 2016, luku 1.)

Joustavuus mahdollistaa verkon kaikkien verkkoresurssien saumattoman käyttämisen. Verkkoon voidaan lisätä laitteita tai sen kapasiteettia voidaan nostaa ilman, että verkkoon tarvitsee tehdä suuria uudistuksia. (Al-Shawi & Laurent 2016, luku 1.)

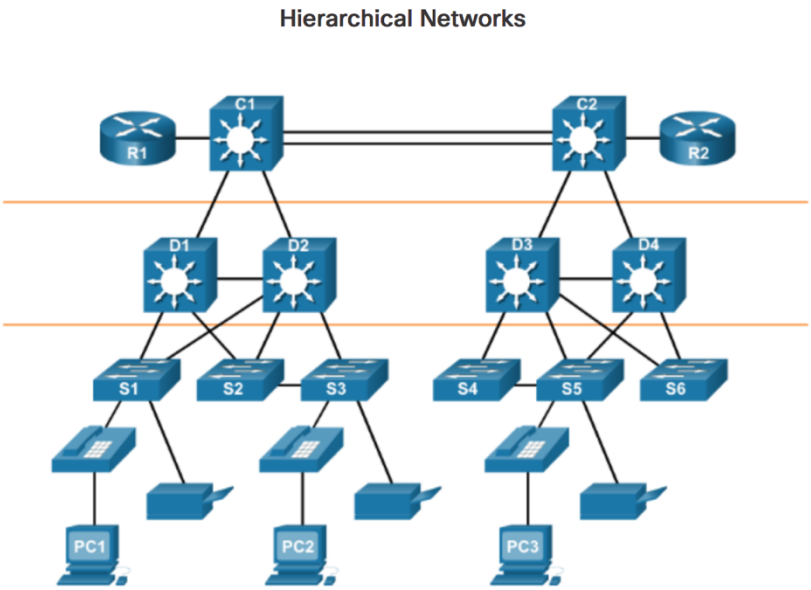
Ciscon hierarkkinen verkkomalli koostuu kolmesta eri kerroksesta: ydinkerros (core), jakelukerros (distribution) ja liityntäkerros (access). Mikäli kolmekerroksiselle mallille ei ole tarvetta, kuten esimerkiksi pienissä ja osassa keskisuuria verkkoja, ydin- ja jakelukerros voidaan yhdistää yhdeksi kerrokseksi, jolloin mallista tulee kaksikerroksinen. Kaksikerroksista mallia kutsutaan ”romahtaneeksi ytimeksi” (collapsed core). Kaksikerroksinen malli alentaa verkon rakentamisen kustannuksia, mutta se säilyttää suurimman osan kolmikerroksisen mallin eduista. (Cisco Networking Academy 2014.)

Ydinkerros toimii koko verkon runkona ja sitä kutsutaan osuvasti verkon selkärangaksi. Se on yksinkertaisin, mutta samalla kriittisin osa verkkoa. Sen tulee olla hyvin vikasietoinen ja pysyä aina toiminnassa. Sen tehtävänä on välittää nopeasti suuria määriä dataa jakelukerroksen laitteille. Ydinkerros on toteutettu L3-tason kytkimillä. Ydinkerrokseen ei liitetä päätelaitteita eikä se sisällä liikennettä hidastavia monimutkaisia palveluja, kuten pakettien suodatusta. (Cisco Networking Academy 2014.)

Jakelukerros toimii ydinkerroksen ja liityntäkerroksen välillä. Sen tehtävänä on yhdistää jakelukerroksen eri osat (LAN-segmentit) ja mahdollistaa jakelukerroksen päätelaitteiden väliset yhteydet. Lisäksi se mahdollistaa jakelukerroksen päätelaitteiden yhteydet ydinkerrokseen, jota kautta päätelaitteet voivat olla yhteydessä kaikkiin verkon osiin tai toisiin verkkoihin. Tässä kerroksessa käytetään L3-tason kytkimiä. Jakelukerroksessa suoritetaan muun muassa datapakettien suodatusta pääsynhallintalistojen (ACL) avulla sekä VLAN-verkkojen välistä reititystä. (Cisco Networking Academy 2014.)

Verkossa olevat päätelaitteet liittyvät verkkoon liityntäkerroksen välityksellä eli toisin sanoen liityntäkerros tarjoaa verkon palvelut käyttäjille. Verkon käyttäjät voivat liittyä liityntäkerrokseen joka langallisesti tai langattomasti. Tämä kerros on yleensä toteutettu L2-tason kytkimillä. (Cisco Networking Academy 2014.)

Seuraava kuvio kuvaa Ciscon hierarkkista verkkomallia. Ylimpänä on ydinkerros. Sen alapuolella on jakelukerros ja alimpana on liityntäkerros. Kerrokset on eroteltu toisistaan oranssilla viivalla.



Kuvio 4. Ciscon hierarkkinen verkkomalli (Cisco Networking Academy 2016b, 4.1.2.1)

3.3 Verkkolaitteet

Päätelaitteet liittyvät verkkoihin välittäjälaitteiden avulla. Tämän lisäksi välittäjälaitteet huolehtivat verkkoliikenteen, datapakettien, välittämisestä verkon sisällä tai eri verkkojen välillä. Näitä välittäjälaitteita ovat reititin, kytkin ja keskitin. Ne jokainen toimivat eri tavalla ja niillä jokaisella on erilainen käyttötarkoitus. (Cisco Networking Academy 2016a, 1.2.1.3.)

3.3.1 Reititin

Reititin huolehtii datapakettien välittämisestä eri verkkojen välillä. Tästä syystä siinä on eri liitännät lähiverkkoja (LAN) ja laajaverkkoja (WAN) varten. Reititin toimii OSI-mallin kolmannessa kerroksessa (verkkokerros) ja se reitittää datapaketit oikeaan määränpäähän vastaanottajan IP-osoitteen perusteella. (Cisco Networking Academy 2016b, 1.1.1.4.)

Reitittimellä on kaksi päätehtävää. Se selvittää parhaan reitin ja välittää datapaketit määritettyyn määränpäähän. Näiden kahden tehtävän suorittamiseen se käyttää reititystaulua. Reititystaulu pitää sisällään tiedot suoraan yhdistetyistä reiteistä, jotka ovat kytkettyinä reitittimen aktiivisiin portteihin ja etäreiteistä, jotka ovat reittejä verkkoihin toisten reitittimien kautta. (Cisco Networking Academy 2016b, 1.1.1.5.)

Reititin oppii reitit etäverkkoihin joko manuaalisesti staattisten reittien avulla tai dynaamisesti dynaamisen reititysprotokollan kautta. Dynaamiset reititysprotokollat käyttävät eri tyyppisiä viestejä oppiakseen ja ylläpitääkseen tietoja muista verkoista. Lisäksi dynaamiset reititysprotokollat pitävät sisällään erilaisia algoritmeja, joiden avulla ne selvittävät parhaan reitin määränpäähän. (Cisco Networking Academy 2016b, 3.1.1.2.)

Dynaamisia reititysprotokollia ovat muun muassa: Routing Information Protocol (RIP). Se valitsee parhaan reitin määränpäähän sen perusteella, kuinka monen reitittimen kautta datapaketti kulkee määränpäähänsä. Open Shortest Path First (OSPF). Se valitsee parhaan reitin lähtöpisteestä määränpäähän kumulatiivisen kaistaleveyden perusteella. Enhanced Interior Gateway Routing Protocol (EIGRP). Se käyttää reitin valitsemiseen yhdistelmää, jossa se huomioi kaistaleveyden, viiveen, kuorman ja luotettavuuden. (Cisco Networking Academy 2016b, 1.2.2.2.)

3.3.2 Kytkin

Kytkin huolehtii datapakettien välittämisestä lähiverkossa. Päätelaitteet voivat liittyä lähiverkkoon kytkinten kautta. Kytkimiä on kahdenlaisia. Tason 2 kytkimet (L2) toimivat OSI-

mallin toisessa kerroksessa (siirtokerros) ja Tason 3 kytkimet (L3) toimivat reitittimien tapaan OSI-mallin kolmannessa kerroksessa (verkkokerros).

Kytkin välittää datapaketit eteenpäin lähiverkossa MAC-osoitteiden avulla. Datapaketit kulkevat siirtokehyksen (ethernet frame) sisällä. Tämä kehys pitää sisällään tiedot muun muassa paketin lähettäjän ja vastaanottajan MAC-osoitteista. Pakettien eteenpäin välittämisessä kytkin käyttää hyväkseen MAC-osoitetaulua. (Cisco Networking Academy 2016a, 5.1.1.4.)

Kytkin toimii siten, että kun sen porttiin saapuu datapaketin siirtokehys se vertaa siirtokehyksen lähettäjän MAC-osoitetta MAC-osoitetaulun tietoihin. Mikäli taulu sisältää jo ennestään tiedot lähettäjän MAC-osoitteesta se nollaa ajastimen, joka laskee aikaa kunkin MAC-osoitteen tietojen iästä. Useimpien kytkimien ajastin on oletuksena asetettu siten, että se poistaa kytkimen MAC-osoitetaulusta yli viisi minuuttia vanhat tiedot. Jos MAC-osoite löytyy MAC-osoitetaulusta, mutta taulun porttinumero on väärä, kytkin päivittää osoitetauluun uuden porttinumeron ja nollaa ajastimen. Mikäli MAC-osoitetta ei löydy MAC-osoitetaulusta, kytkin lisää MAC-osoitteen ja porttinumeron osoitetauluun. Kytkin pystyy lisäämään MAC-osoitetauluunsa ainoastaan lähettäjän MAC-osoitteet. (Cisco Networking Academy 2016a, 5.2.1.2)

Jos vastaanottajan MAC-osoite on unicast-osoite, kytkin vertaa kehyksen vastaanottajan MAC-osoitetietoja MAC-osoitetauluunsa. Mikäli MAC-osoitteen tiedot löytyvät osoitetaulusta, kytkin välittää kehyksen osoitetaulusta löytyvään porttiin. Jos taas MAC-osoitetta ei löydy taulusta kytkin välittää kehyksen kaikkiin muihin portteihin paitsi siihen, josta kehys saapui. Jos vastaanottajan MAC-osoite on multicast- tai broadcast -osoite, kytkin välittää kehyksen kaikkiin muihin portteihin paitsi siihen, josta kehys saapui. (Cisco Networking Academy 2016a, 5.2.1.2.)

Kytkimet voivat lähettää siirtokehyksiä eteenpäin kahdella tavalla. Store-and-Forward -tapa suorittaa saapuneelle kehykselle virheiden tarkistuksen. Kytkin laskee saapuneen kehyksen FSC-arvon (frame-check-sequense) ja vertaa laskemaansa arvoa siirtokehyksen sisältämään FSC-arvoon. Mikäli arvot täsmäävät kytkin välittää kehyksen eteenpäin, mutta mikäli arvot eivät ole yhtenevät, kytkin pudottaa kehyksen pois, eikä välitä sitä eteenpäin. Store and forward -tapa mahdollistaa myös automaattisen puskuroinnin. Tämä tarkoittaa sitä, että kytkin tukee kaikkia ethernet-nopeuksia. Tämä mahdollistaa sen, että kytkin pystyy lähettämään 100 Mbit/s nopeudella saapuneen kehyksen 1 Gbit/s nopeudella eteenpäin. (Cisco Networking Academy 2016b, 4.2.1.4.)

Cut-Through -tapa välittää kehyksiä Store-and-Forward - tapaa nopeammin. Cat-Through -tavassa kytkin välittää kehyksen eteenpäin heti, kun se on saanut verrattua vastaanottajan MAC-osoitetta omaan MAC-osoitetaulunsa tietoihin. Kytkimen ei tarvitse odottaa koko kehyksen saapumista, vaan eteenpäin välitys voi alkaa jo ennen koko kehyksen saapumista. Tässä tavassa ei suoriteta virheiden tarkistusta, vaan kytkin välittää myös virheitä sisältävät kehykset eteenpäin. Tästä johtuen virheelliset kehykset voivat pienentää kaistaleveyttä tukkimalla liikennettä. (Cisco Networking Academy 2016b, 4.2.1.5.)

Tason 2 ja tason 3 kytkimet eroavat siinä, että tason 3 kytkimet pystyvät reitittämään liikennettä lähiverkossa IP-osoitteen perusteella. Ne eivät kuitenkaan pysty reitittämään liikennettä etäverkkoihin, kuten reititin, koska niistä puuttuvat WAN-portit. Tason 3 kytkimien IP-osoitteen perusteella tekemä reititys mahdollistaa VLAN-verkkojen välisen liikenteen ilman reititintä ja siten vähentää reitittimen aiheuttamia pullonkauloja VLAN-verkkojen väliseen liikenteeseen. (Froehlich 2006.)

3.3.3 Keskitin

Keskitin (hub) on verkkolaite, jonka avulla useita päätelaitteita voidaan kytkeä lähiverkkoon. Se tukee lähtökohtaisesti ainoastaan 10 Mbit/s ja 100 Mbit/s nopeuksia. Keskitin eroaa kytkimestä siinä, että se välittää saapuneen datapaketin kehyksen aina kaikkiin portteihin huolimatta siitä, vaikka kehys olisi tarkoitettu ainoastaan yhdelle vastaanottajalle (unicast-osoite). Keskittimet ovat laitteina vanhentuneita ja nykyaikaisissa verkoissa ne on korvattu kytkimillä. Tänä päivänä keskittimiä käytetään lähinnä hetkellisesti korvaamaan vikaantunut lähiverkon kytkin. (Mitchell 2017.)

3.4 Kaapelit ja nopeudet

Verkkojen toteutuksissa käytetään kuparikaapeleita, kuitukaapeleita ja langatonta teknologiaa. Verkkoja toteutettaessa kaapeleiden valintaan vaikuttavat muun muassa kaapeloitavat etäisyydet, verkon nopeus ja hinta. (Cisco Networking Academy 2016a, 4.2.1.1.)

Lähiverkoissa käytetään yleisimmin kuparikaapeleita. Data kulkee kuparikaapelia pitkin sähköisinä impulsseina. Kuparikaapeleilla on rajoitettu matka, jonka ne pystyvät kuljettamaan dataa. Kuparikaapelit voidaan jakaa kolmeen pääryhmään: suojatut parikaapelit (Shielded Twisted-Pair, STP), suojaamattomat parikaapelit (Unshielded Twisted-Pair, UTP) ja koaksiaalikaapelit, joita käytetään lähinnä langattomien laitteiden liittämiseen antenniin tai kaapeliyhtiön tarjoamaan internetverkkoon. (Cisco Networking Academy 2016a, 4.2.1.1, 4.2.1.2.)

Suojattu parikaapeli (STP) muodostuu neljästä johtoparista, jossa johtoparin johdot on kierretty toistensa ympäri. Jokainen johtopari on päällystetty foliosuojalla ja kaikki johtoparit on suojattu joko punotulla metallisella suojakerroksella tai foliosuojakerroksella. Lopuksi koko kaapeli on päällystetty joustavalla muovisella kuorella. STP-kaapelit yhdistetään laitteisiin RJ-45 -liittimillä. STP-kaapelit ovat vähemmän herkkiä häiriöille kuin suojaamattomat parikaapelit, mutta ne ovat kalliimpia ja monimutkaisempia asentaa. Tästä syystä niitä käytetään lähiverkoissa vähemmän kuin suojaamattomia parikaapeleita. (Cisco Networking Academy 2016a, 4.2.1.4.)

Suojaamaton parikaapeli (UTP) on yleisimmin käytetty verkkokaapeli. Lähiverkkojen UTP-kaapelit muodostuvat neljästä johtoparista. Johtoparin johdot on kierretty toistensa ympäri ja siten on saatu vähennettyä johtojen aiheuttamaa signaalien häirintää. Johtoparit kulkevat joustavan muovisen kuoren sisällä. UTP-kaapelit liitetään laitteisiin RJ-45 -liittimillä. (Cisco Networking Academy 2016a, 4.2.1.3.)

UTP-kaapelit jaetaan eri kategorioihin sen mukaan millaisia nopeuksia ne pystyvät toteuttamaan. FastEthernet (100 Mbit/s) nopeudet voidaan toteuttaa kategorian 5 (Cat 5) kaapeleilla. GigabitEthernet (1000 Mbit/s tai 1Gbit/s) toteutus vaatii vähintään kategorian Cat 5e kaapelin, mutta on suositeltavaa käyttää kategorian 6 (Cat 6 tai Cat 6a) kaapeleita. 10 GigabitEthernet (10 Gbit/s) voidaan toteuttaa ainoastaan kategorian 7 (Cat 7) kaapeleilla. (Cisco Networking Academy 2016a, 4.2.2.2.)

UTP kaapeleita on kahta päätyyppiä luokiteltuna käyttötarkoituksen mukaan. Ethernet Straight-through kaapeleita käytetään yhdistämään päätelaitteet kytkimiin ja reitittimiin. Ethernet Crossover kaapeleita käytetään yhdistämään suoraan samanlaiset laitteet keskenään ilman, että niiden välissä on välittäjälaitetta. Esimerkiksi tietokone toiseen tietokoneeseen. (Cisco Networking Academy 2016a, 4.2.2.4.)

Kuitukaapelit pystyvät kuljettamaan dataa pidempiä matkoja ja suuremmilla nopeuksilla kuin kuparikaapelit. Kuitukaapelit ovat joustavia ja erittäin ohuita kaapeleita. Data kulkee niissä valopulsseina. Kuitukaapelit muodostuvat kahden tyylisestä lasista, ytimestä ja verhoilusta. Ydintä ja verhoilua peittää suojaava ulkokuori. (Cisco Networking Academy 2016a, 4.2.3.1.)

Valopulssit muodostetaan joko laserin tai LEDien avulla. Single-mode kuidut (yksimuotokuidut, SMF) modustuvat hyvin ohuesta ytimestä. Ydintä pitkin kulkee laser -tekniikalla muodostettu valonsäde. Näitä kaapeleita käytetään pitkien etäisyyksien kaapeloinnissa. Etäisyydet voivat olla jopa satoja kilometrejä. Multimode kuiduissa (monimuotokuidut,

MMF) on laajempi ydin ja valopulssit on muodostettu LED-tekniikalla. Nämä kaapelit ovat halvempia kuin SMF-kaapelit. Siksi niitä käytetään lähiverkkoja toteutettaessa. MMF-kaapelit tukevat 10 Gbit/s nopeuksia ja niillä voidaan toteuttaa enintään 550 metrin kaapelointeja. (Cisco Networking Academy 2016a, 4.2.3.3.)

Valo voi kulkea kuitukaapelissa ainoastaan yhteen suuntaan. Tästä syystä tarvitaan kaksi kuitukaapelia, jotta laitteet voivat vastaanottaa ja lähettää dataa saman aikaisesti. Tätä kutsutaan full duplex -toiminnoksi. Toimintoa, jossa laitteet voivat lähettää ja vastaanottaa dataa vuorotellen, kutsutaan half duplex toiminnoksi. (Cisco Networking Academy 2016a, 4.2.3.4.)

Kuitukaapeleille on useita erilaisia liittimiä. Yleisimmät liittimet ovat ST, SC, ja LC sekä multimode LC -mallisia. ST-malliset (Straight-Tip) liittimet ovat kiinni/auki -käännettäviä tappi -tyylisiä liittimiä. SC-liittimet (Subscriber Connector) ovat neliön mallisia liittimiä, jossa kuitukaapelit ovat erillään. Tämä on hyvin yleinen liitin lähi- ja kaukoverkoissa. Tämä liitin sopii sekä MMF että SMF kuitukaapeleille. LC-liittimet (Lucent Connector) ovat pienennetty versio SC-liittimistä. Nämä liittimet ovat nopeaan tahtiin yleistymässä pienen kokonsa ansiosta. Duplex Multimode LC-liittimet ovat LC-liittimiä, joihin kiinnittyy kaksi kuitukaapelia. (Cisco Networking Academy 2016a, 4.2.3.4.)

Seuraavassa taulukossa on vertailtu UTP- ja kuitukaapeleiden eroja.

Taulukko 1. UTP-kaapelien ja kuitukaapelien vertailua (Cisco Networking Academy 2016a, 4.2.3.6)

Toteutus	UTP-kaapeli	Kuitukaapeli
Tuettu nopeus	10 Mbit/s - 10 Gbit/s	10 Mbit/s - 100 Gbit/s
Etäisyys	1 - 100 metriä	1 - 100000 metriä
Immuniteetti häiriöille	Matala	Korkea
Immuniteetti sähköiskuille	Matala	Korkea
Kustannukset	Matalin	Korkein
Asennuksen vaativuus	Matalin	Korkein
Turvallisuus tekijät	Matalin	Korkein

3.5 VLAN

VLAN tulee sanoista Virtual LAN eli virtuaalinen lähiverkko. Se perustuu loogisiin yhteyksiin fyysisten yhteyksien sijaan. VLANit mahdollistavat fyysisen verkon pilkkomisen itsenäisiin loogisiin verkkoihin, jotka jakavat yhteisen fyysisen verkon. VLAN-verkkoja voidaan luoda esimerkiksi siten, että organisaation eri ryhmille tai projekteille luodaan omat VLAN-

verkot, jotta ne voivat toimia itsenäisinä kokonaisuuksina organisaation fyysisen verkon sisällä. (Cisco Networking Academy 2016b, 6.1.1.1.)

Kytkimet voivat välittää unicast-, multicast- ja broadcast -lähetysten datapakettien kehyksiä ainoastaan samassa VLAN-verkossa oleville päätelaitteille. Mikäli datapakettien kehyksiä pitää välittää VLAN-verkosta toisessa VLAN-verkossa olevalle päätelaitteelle tai päätelaitteelle, joka ei kuulu mihinkään VLAN-verkkoon, kehykset tulee reitittää joko reitittimen tai tason 3 kytkimen avulla. Kytkimen porttiin voi olla määriteltynä ainoastaan yksi VLAN. Poikkeuksena tästä ovat IP-puhelimet ja portin määrittämien trunk-portiksi. (Cisco Networking Academy 2016b, 6.1.1.1.)

VLAN trunk-portit eivät ole sidoksissa yhteen tiettyyn VLANiin, vaan ne voivat välittää enemmän kuin yhden VLANin liikennettä. Kytkinten portit, jotka ovat liitettyinä toisiin kytkimiin tai reitittimiin tulee olla määritettynä trunk-porteiksi. Tällä mahdollistetaan se, että samassa VLAN-verkossa olevat päätelaitteet voivat olla yhteydessä toisiinsa, vaikka ne ovat fyysisesti kytkettyinä eri kytkimiin. (Cisco Networking Academy 2016b, 6.1.2.1.)

VLAN-verkkojen käyttö tarjoaa ainakin seuraavat hyödyt (Cisco Networking Academy 2016b, 6.1.1.2):

- Turvallisuus lisääntyy. VLAN-verkko on erotettu muusta fyysisestä verkosta ja siten mahdollisuus VLAN-verkon sisällä lähetettyjen tai jaettujen tietojen päätymisestä VLAN-verkon ulkopuolisille päätelaitteille pienenee.
- Kustannukset pienevät. VLAN-verkkojen käyttö vähentää fyysiseen verkkoon tehtävien kalliiden muutosten tarvetta ja verkon kaistaleveyttä voidaan käyttää tehokkaammin.
- Verkon parempi suorituskyky. VLAN-verkot vähentävät fyysisen verkon tarpeetonta liikennettä.
- Broadcast -toimialueet pienevät. Fyysisen verkon jakaminen VLAN-verkkoihin vähentää broadcast -toimialueella olevien koneiden määrää, koska broadcast -lähetykset kulkevat ainoastaan VLAN-verkon sisällä.
- IT -henkilöstön tehokkuus kasvaa. Fyysisen verkon ylläpito on helpompaa VLAN-verkkojen avulla, koska oikein ryhmitellyissä VLAN-verkoissa käyttäjillä on yhtenevät tarpeet verkon vaatimuksille.
- Yksinkertaisempi projektien ja sovellusten hallinta. Esimerkiksi tiettyjen erityisohjelmien tai tiettyyn projektiin liittyvien toimintojen jakaminen ainoastaan tietyn VLAN-verkon sisällä.

4 Lähiverkon suunnittelu

Lähiverkon suunnittelu voi olla kokonaan uuden verkon suunnittelua tai vanhan jo olemassa olevan verkon uudistamista. Suunniteltavan verkon käyttötarkoitus, vaatimukset ja budjetti asettavat reunaehdot verkon suunnittelulle. Nykyaikaisen verkon keskeisiä ominaisuuksia ovat: luotettavuus, skaalautuvuus, vikasietoisuus, turvallisuus ja kustannustehokkuus (Cisco Networking Academy 2014).

4.1 Suunnittelun keskeiset vaiheet

Lähiverkon suunnittelun lähtökohtana tulee olla kohdeorganisaation toiminnan tarpeet tällä hetkellä ja tulevaisuudessa. Tämä vaatii tutustumista organisaation toimintaan ja tulevaisuuden näkymiin niin teknisten kuin hallinnollisten vaatimusten kautta. Uudistettavasta verkosta eli verkosta, joka on tällä hetkellä toiminnassa, tulisi kerätä mahdollisimman paljon tietoa. Tekninen tieto pitää sisällään esimerkiksi sovellukset, protokollat ja suorituskyvyn. Hallinnollinen tieto pitää sisällään esimerkiksi organisaation rakenteen, henkilöstöhallinnan, käytänteet ja tulevaisuuden tavoitteet. Tässä ensimmäisessä vaiheessa kerätään mahdollisimman paljon tietoa, jonka perusteella pystytään muodostamaan kuva tämän hetkisen verkon nykytilasta ja siitä mihin vaatimuksiin uuden verkon tulisi vastata tulevaisuudessa. (Pasricha & Jagu 2004, 58 - 60.)

Toisessa vaiheessa kerätty tieto pitää dokumentoida ja analysoida. Dokumentoinnin olisi hyvä pitää sisällään muun muassa nykyiset verkossa toimivat sovellukset, verkkoprotokollat, verkon topologia, IP-osoiteavaruus ja sen rakenne, verkon tietoturva sekä verkossa olevat potentiaaliset pullonkaulat. Kerätyn ja dokumentoidun tiedon pohjalta voidaan tehdä analyysi, jonka perusteella saadaan selkeä kuva uuden verkon vaatimuksista sekä siitä mihin tarpeisiin sen tulee vastata tulevaisuudessa. (Pasricha & Jagu 2004, 65 - 77.)

Kolmas vaihe pitää sisällään uuden verkon rakenteen suunnittelun. Tässä vaiheessa rakenteen suunnittelu pohjautuu edellisessä vaiheessa tehtyyn analyysiin. Tänä päivänä hyvin yleisesti käytetty verkkomalli on Ciscon kolmekerroksinen hierarkkinen verkkomalli. Tässä vaiheessa kuvataan verkon fyysinen ja looginen topologia. Topologioiden valmistuttua saadaan selville vaadittavat verkkoresurssit eli välittäjälaitteiden määrät ja vaatimukset sekä käytettävien kaapeleiden vaatimukset. (Pasricha & Jagu 2004, 107 - 115.)

Viimeinen vaihe ennen asennusta on prototyypin tai pilotin rakentaminen. Ne eroavat toisistaan siinä, että pilotissa esitellään ainoastaan osa verkon keskeisimmistä toiminnalli-

suuksista, kun taas prototyypissä esitellään koko verkon toiminnallisuudet. Pilotti on tarkoitettu käytettäväksi pienissä verkoissa, kun taas prototyyppiä käytetään suuremmissa verkoissa. (Pasricha & Jagu 2004, 293.)

4.2 IP-osoitteet

IP-osoitteet mahdollistavat päätelaitteiden välisen yhteydenpidon riippumatta siitä, missä verkossa ne ovat. IPv4-osoitteet ovat 32 bittisiä ja IPv6-osoitteet ovat 128 bittisiä. IPv6-osoitteille tuli tarve, koska IPv4-osoitteiden määrä on rajallinen ja käytännössä ne loppuivat kesken. Tässä työssä käsitellään ainoastaan IPv4-osoitteita.

IP-osoite koostuu verkko-osasta ja laiteosasta. Verkko-osa määritellään aliverkon peitteellä (subnet mask). Verkko-osa kertoo mihin verkkoon laite kuuluu. Lähiverkon laitteiden tulee olla samassa verkossa. Laiteosa yksilöi verkossa olevan laitteen. IP-osoitteet jakaantuvat yksityisiin osoitteisiin ja julkisiin osoitteisiin. Julkiset osoitteet voidaan reitittää internetiin. Niitä hallinnoi Internet Assigned Numbers Authority (IANA). Yksityisiä osoitteita ei voi reitittää internetiin. Lähiverkon yksityisiä IP-osoitteita voidaan hallinnoida paikallisesti oman organisaation toimesta. (Pasricha & Jagu 2004, 219.)

Seuraavasta taulukosta ilmenee yksityisten IP-osoitteiden osoiteavaruus. Nämä osoitteet ovat käytännöllisiä organisaation omassa lähiverkossa, koska niitä voidaan hallinnoida paikallisesti. Lisäksi ne lisäävät turvallisuutta, koska niitä ei voi suoraan reitittää internetiin.

Taulukko 2. Yksityiset IP-osoitteet (Pasricha & Jagu 2004, 225)

Alku	Loppu
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Verkon IP-osoitteiden tulee olla hyvin suunniteltuja, ylläpidettyjä ja dokumentoituja. IP-osoitteiden suunnittelu on tärkeää, että verkossa riittää IP-osoitteita kaikille laitteille ja että IP-osoitteet eivät muodosta estettä verkon laajentumiselle. Lisäksi IP-osoitteiden suunnittelussa tulee huomioida mahdolliset aliverkot, joiden avulla laajempia lähiverkkoja voidaan segmentoida. IP-osoitteiden ylläpito voi olla hankalaa varsinkin laajemmissa lähiverkoissa. Palvelimille, välittäjälaitteille ja verkkotulostimille tulee antaa staattiset eli kiinteät IP-osoitteet. Pienessä lähiverkossa kaikille päätelaitteille voi antaa staattisen IP-osoitteen, mutta verkon laajentuessa staattisten IP-osoitteiden käyttö päätelaitteissa on hyvin työlästä, miltei jopa mahdotonta. Laajoissa verkoissa IP-osoitteiden ylläpitoa helpottaa dynaamisesti

muodostettavat IP-osoitteet. Tästä huolehtii DHCP-protokolla (Dynamic Host Configuration Protocol). Se jakaa verkkoon liittyville laitteille, joilla ei ole staattista IP-osoitetta IP-osoitteen. IP-osoitteiden dokumentointi on tärkeää, koska kahdella laitteella ei voi olla samaa IP-osoitetta. Mikäli näin on, se aiheuttaa ongelmia verkon toiminnassa. Ajantasainen dokumentointi vähentää mahdollisuutta saman IP-osoitteen antamiseen kahdelle eri laitteelle. (Pasricha & Jagu 2004, 219, 242.)

4.3 Segmentointi

Lähiverkon segmentointi tapahtuu jakamalla IP-osoitteen laiteosa kahteen osaan. Tällöin IP-osoitteen rakenne on muotoa verkko ID, aliverkko ID, laite ID. Suuremmalla aliverkon peitteellä alkuperäisestä osoitteesta muodostetaan pienempiä aliverkkoja. Aliverkkoja voidaan muodostaa esimerkiksi toimintojen tai rakennuksen kerrosten mukaisesti. Aliverkkojen välinen liikenne vaatii reititystä ja tähän tarvitaan joko reititin tai tason 3 kytkin. Nykyaikainen tapa hoitaa segmentointi on tehdä se VLAN-verkkojen avulla. (Pasricha & Jagu 2004, 229 - 230.) VLAN-verkkoja ja niiden etuja on käsitelty aiemmin kohdassa 3.5.

4.4 Vikasietoisuus

Organisaatioiden toiminta on hyvin paljon riippuvaista lähiverkkojen ja internetyhteyksien toiminnasta. Verkkoyhteyksien tulisikin olla jatkuvasti toiminnassa. Tämä on mahdollista ainoastaan teoriatasolla ja käytännössä verkkoliikenteeseen muodostuu aina katkoksia. Tästä syystä lähiverkot ja verkkoyhteydet tulee suunnitella mahdollisimman vikasietoisiksi.

Vikasietoisuutta parannetaan suunnittelemalla ja rakentamalla datalle vaihtoehtoisia reittejä lähtöpisteestä määränpäähän. Mikäli yksi reitti pettää esimerkiksi laite- tai kaapelivian vuoksi, data pystyy käyttämään toista, vaihtoehtoista reittiä määränpäähän. Vaihtoehtoisia reittejä saadaan muodostettua lisäämällä verkkoon välittäjälaitteita ja näiden välisiä yhteyksiä. Mikäli organisaatiolla on ainoastaan yksi yhteys internetiin, niin vikasietoisuuden parantamiseksi investointi toiseen, varalla olevaan, internetyhteyteen olisi harkinnan arvoista. (Cisco Networking Academy 2016a, 11.1.1.4.)

Välittäjälaitteiden lisääminen verkkoon nostaa myös verkon rakentamisen kustannuksia. Suunnitteluvaiheessa tulee harkittavaksi missä kulkee rakennuskustannusten suhde siihen, kuinka kauan verkko voi olla pois toiminnasta. Hyvä esimerkki vikasietoisesta verkosta on Ciscon kolmitasoinen hierarkkinen verkkomalli kuviossa 4.

4.5 Kaapelointi

Tietoliikennekaapelointi on huomioitava lähiverkkoja suunniteltaessa. Rakennusten kiinteät rakenteet saattavat aiheuttaa vaikeuksia jälkikäteen rakennettavalle kaapeloinnille. Uusissa kiinteistöissä tietoliikennekaapelointi on osa rakennukseen kuuluvaa perusjärjestelmää ja sitä on helppo hyödyntää lähiverkkoja suunniteltaessa. (Sesko 2016, 3.)

Talojakamo on tila, jossa rakennukseen saapuvat yhteydet yhdistyvät nousukaapelointiin. Nousukaapeloinnilla tarkoitetaan kaapelointia talojakamosta kerrosjakamoihin. Nämä yhteydet toteutetaan yleisimmin MMF-kuitukaapeleilla, mutta ne voidaan toteuttaa myös UTP-kuparikaapeleilla. Kerrosjakamo on tila, jossa nousukaapelointi yhdistyy kerroskaapelointiin. Kerroskaapeloinnilla tarkoitetaan kaapelointia kerrosjakamoista huoneiden tietoliikennerasioihin. Nämä yhteydet toteutetaan UTP-kuparikaapeleilla, joiden luokka on Cat 6a tai Cat 7. Kerroskaapeloinnissa voidaan käyttää erillisiä keskityskohtia, esimerkiksi kattorasioita, mahdollistamaan avokonttoreissa tietoliikennerasioiden sijoittelu tai siirtäminen. Päätelaitteet yhdistetään tietoliikennerasioihin työpistekaapeloinnilla. Nämä yhteydet toteutetaan joko Cat 6a tai Cat 7 -luokan kaapeleilla. (Sesko 2016, 13.)

Kaapeleita ja niiden mahdollistamia nopeuksia on käsitelty kohdassa 3.4. Kaapeloinnin suorituskyky riippuu käytetyistä kaapeleista, kaapeloinnin pituudesta, kaapeloinnissa käytettyjen liitoksien lukumäärästä sekä asennustyön laadusta (Sesko 2016, 18, 26).

4.6 Tietoturva

Tietoturva on oleellinen osa nykyaikaisia tietoverkkoja ja -järjestelmiä. Tietoturvaa kuvattaessa käytetään usein niin sanottua CIA-kolmiota. Se kuvaa kolme keskeistä tietoturvan tekijää. CIA tulee sanoista Confidentiality (luottamuksellisuus), Integrity (eheys) ja Availability (käytettävyys). (Stewart, Chapple & Gibson 2012, 3.)

Luottamuksellisuudella tarkoitetaan sitä, että ainoastaan henkilöillä, joilla on luvallinen pääsy järjestelmiin tai tietoihin pääsevät käsiksi niihin. Pääsynhallinnalla ja salausmenetelmillä pyritään estämään luvattomien tahojen pääsy järjestelmiin tai tietoihin. On ensiarvoisen tärkeää, että organisaation salassa pidettävät tiedot esimerkiksi liikesalaisuudet eivät päädy ulkopuolisten haltuun. (Stewart ym. 2012, 4.)

Eheys turvaa järjestelmien konfiguraatioita ja tietoa luvattomilta muutoksilta sekä vahingossa tapahtuvilta virheiltä. Pääsynhallinnalla ja esimerkiksi hash-funktioilla voidaan turvata tiedon eheyttä. On tärkeää, että tieto on muuttumatonta, jolloin siihen voidaan luottaa ja sen perusteella tehtävät päätökset perustuvat oikeaan tietoon. (Stewart ym. 2012, 4.)

Käytettävyys tarkoittaa sitä, että järjestelmät ja tieto on saatavissa niihin oikeutetuilla tahoilla silloin kun he sitä tarvitsevat. Pääsynhallinnalla ja esimerkiksi verkon vikasietoisuutta kasvattamalla ja varmuuskopioinnilla pyritään turvaamaan tiedon ja järjestelmien saatavuus. Tieto ja järjestelmät pitää olla käytössä silloin, kun niitä tarvitaan. (Stewart ym. 2012, 4.)

Pääsynhallinnan osa-alueita kuvataan AAA-prosessilla. Se sisältää neljä osatekijää: Identification (tunnistaminen), Authentication (todentaminen), Authorization (valtuuttaminen) ja Accountability (vastuullisuus). Tunnistamisessa pääsynhallintaprosessille ilmoitetaan kenestä on kysymys (oma identiteetti), esimerkiksi käyttäjätunnuksella. Tämän jälkeen todentaminen tapahtuu esimerkiksi antamalla käyttäjätunnukseen liittyvä salasana. Valtuutuksessa käyttäjälle myönnetään pääsy siihen sisältöön, johon hänellä on ennalta määrätty oikeus. Vastuullisuus tarkoittaa sitä, että käyttäjä on vastuullinen toimistaan. Käyttäjän suorittamat toimet voidaan tarkastaa esimerkiksi lokitiedoista. (Stewart ym. 2012, 9.)

Turvallisiin IT-ympäristöihin liittyy keskeisesti kaksi vakioperiaatetta, jotka ovat Need to Know ja Least Privilege. Need to Know -periaate tarkoittaa sitä, että käyttäjälle myönnetään pääsy ainoastaan niihin tietoihin, järjestelmiin ja muihin resursseihin, mitä hän tarvitsee työtehtäviensä hoitamiseksi. Tällä periaatteella on tarkoitus turvata tiedon luottamuksellisuutta, esimerkiksi ettei salassa pidettävistä tiedoista tiedä muut kuin ainoastaan ne, jotka tietoa tarvitsevat. Least Privilege -periaatteen mukaan henkilölle myönnetään ainoastaan työtehtäviensä kannalta välttämättömät käyttöoikeudet. Tällä periaatteella turvataan tiedon eheyttä. Esimerkkeinä tästä ovat, että käyttäjällä on oikeus muuttaa vain niitä tietoja tai tiedostoja, joita hän työtehtävissään tarvitsee tai että tavalliselle käyttäjälle ei myönnetä pääkäyttäjäoikeuksia. (Stewart ym. 2012, 533.)

Edellisten periaatteiden tarkoitus on turvata luottamuksellisuutta ja eheyttä. Keskeinen saatavuutta uhkaava tekijä on fyysinen uhka. Saatavuuden lisäksi fyysiset uhat uhkaavat myös tiedon eheyttä. Tällaisia uhkia ovat laiteviat, sähkön jakeluhäiriöt, jakamoiden lämpötila ja ilmankosteus, tulipalot sekä vesivahingot. (Stewart ym. 2012, 764 - 772.)

Laitevikoja voi esiintyä kaikissa verkon laitteissa. Toisten laitteiden laiteviat ovat kriittisempiä kuin toisten. Esimerkiksi kytkinten tai reitittimien porttivika tai koko laitteen vaurioituminen vaikuttaa keskeisesti verkon toimintaan, mutta hyvin suunnitellussa verkossa, jossa vaihtoehtoisia reittejä on toteutettu, verkko toipuu nopeasti tällaisesta viasta ja vioittunut

laite voidaan korvata myöhemmin. Palvelimen tai tallennusalustan vikaantumista sen sijaan ei pystytä hetkessä korvaamaan. Varalaitteet ja ajantasaiset varmuuskopiot nopeuttavat toimintojen palauttamista ennalleen. (Stewart ym. 2012, 772.)

Verkon välittäjälaitteet, palvelimet, tallennusalustat ja päätelaitteet toimivat sähköllä. Verkon toimivuuden turvaaminen sähkökatkojen aikana tulee huomioida suunnittelussa. Verkon toiminnan kannalta keskeiset laitteet tulee kytkeä siten, että ne saavat varavirrasta sähköä sähkökatkojen aikana. Hetkellisenä varavirtana voidaan käyttää muun muassa UPS -laitteita turvaamaan sähkönsaanti ja tarvittaessa mahdollistaman laitteiden hallittu sammuttaminen. (Stewart ym. 2012, 764.)

Jakamoiden lämpötila ja ilmankosteus voivat aiheuttaa sähköllä toimivissa laitteissa toimintahäiriöitä tai jopa niiden vahingoittumisen. Jakamoiden lämpötilan tulee olla 15 - 23 asteen välillä (Celsiusta). Ilmankosteuden tulee olla 40 ja 60 prosentin välillä. Liika kosteus aiheuttaa korroosiota ja liian kuiva ilma puolestaan aiheuttaa staattista sähköä. (Stewart ym. 2012, 766.)

Laitesaliin tai jakamoon valuva vesi voi aiheuttaa valtavia vahinkoja sähkölaitteille. Lisäksi sähkö ja vesi yhdessä muodostavat vaaran kaikille lähellä oleville henkilöille. Tästä syystä laitesalit ja jakamot tulee sijoittaa mahdollisimman kauaksi vesipisteistä ja -putkista. Edellä mainitut tilat tulisi myös varustaa veden tunnistus ja hälytyslaitteistolla sekä lattiakaivoilla, että tiloihin mahdollisesti päässyt vesi voidaan johtaa sieltä pois. (Stewart ym. 2012, 766.)

Toinen erittäin suurta vahinkoa aiheuttava ulkoinen uhkatekijä on tulipalo. Tulipalojen aiheuttamia vahinkoja voidaan ehkäistä poistamalla laitetiloista palavat materiaalit sekä varustamalla tilat palohälyttimillä sekä sammutusjärjestelmillä. (Stewart ym. 2012, 767 - 771.)

Verkon tietoturvaa, joka turvaa kaikkia kolmea tietoturvan osatekijää (CIA), voidaan lisätä palomuurien avulla, tunkeutumisen havaitsemisjärjestelmillä (IDS) ja tunkeutumisen estämisjärjestelmillä (IPS). Palomuuri suodattaa sääntöihin perustuen IP-paketteja ja siten pystyy estämään haitallista liikennettä internetistä lähiverkkoon tai estämään koko verkkoliikenteen. IDS tarkkailee verkkoliikennettä monelta eri kantilta pyrkien havaitsemaan mahdolliset tunkeutumiset verkkoon. IPS vastaavasti taas pyrkii sääntöihin perustuen estämään tunnettuja turvallisuusuhkia. (Stewart ym. 2012, 115 - 119; Snyder 2009.)

4.7 Mahdollisesti kohdattavia ongelmia

Hyvästä suunnittelusta huolimatta on riski, että käytännön toteutusvaiheessa kohdataan erilaisia ongelmia, jotka vaikuttavat verkon toimintaan hidastavasti tai jopa estävät verkon toiminnan. Osa ongelmista saattaa johtua suunnittelussa tapahtuneista virheistä tai huolimattomuudesta asennustöissä.

Lähiverkoissa, joissa on useita kytkimiä ja joissa on tavoiteltu vikasietoisuutta, on mahdollista, että kytkinten välillä on useampia käytössä olevia reittejä. Tämä aiheuttaa sen, että määränpäähän on useampi kuin yksi reitti ja datapaketti saattaa jäädä ikuiseen silmukkaan kiertäen verkkoa saavuttamatta koskaan määränpäätä. Tämä hidastaa verkon toimintaa. Tämä ongelma voidaan korjata käyttämällä Spanning Tree Protocollaa (STP). Tämä protokolla sulkee väliaikaisesti vaihtoehtoiset reitit ja käyttää pääreitiksi määriteltyä reittiä datapakettien välittämiseen. Pääreitin katketessa protokolla ottaa käyttöön vaihtoehtoisen reitin ja käyttää sitä datapakettien välittämiseen. (Harrington 2007, 74; Wilkins 2011.)

Yksi erittäin yleinen ongelma on kaapeloinnista johtuvat ongelmat. Näitä ongelmia ovat muun muassa, että käytetyt kaapelit eivät pysty välittämään datapaketteja laitteiden lähettämällä nopeudella tai että kaapelointietäisyydet ovat pidempiä kuin mitä käytetyt kaapelit tukevat. Esimerkiksi UTP Cat 6 kaapeli ei pysty välittämään datapaketteja 10 Gbit/s -nopeudella tai UTP-kaapelia käytetään yli sadan metrin kaapelivetoihin. Nämä ongelmat saattavat estää koko verkon tai sen osan toiminnan. (Cisco Networking Academy 2016a, 4.2.2.2, 4.2.3.6.)

Mikäli verkkokortit tai kytkinten portit toimivat half dublexina, laitteet pystyvät lähettämään ja vastaanottamaan dataa vuorotellen. Tämä altistaa tällaisen verkkosegmentin datapakettien törmäyksille. Se taas johtaa verkon nopeuden laskuun. Tämä ongelma poistuu, mikäli portit voivat kommunikoida full dublexina, jolloin törmäyksiä ei tule. (Cisco Networking Academy 2016b, 4.2.2.1.)

Laajemmissa verkoissa, joissa on paljon laitteita suuret broadcast -alueet hidastavat verkon toimintaa. Tämä johtuu siitä, että broadcast -sanomat kuormittavat verkkoa. Ratkaisuna tähän on verkon segmentointi pienempiin broadcast -alueisiin esimerkiksi VLAN-verkkojen avulla. Yleinen VLAN-verkkoihin liittyvä ongelma on, että trunk-portit on määritelty väärin, jolloin eri VLAN-verkkojen liikenne ei välity kytkinten porteista eteenpäin. (Cisco Networking Academy 2016b, 6.2.3.3.)

5 Lähiverkon uusiminen

Tämä opinnäytetyö tehdään toimeksiannosta julkisen sektorin organisaatiolle. Kyseessä on suljettu pieni lähiverkko, joka on toteutettu kytkimillä, eikä verkossa ole reititintä eikä yhteyksiä muihin verkkoihin tai internetiin. Verkon pääasiallinen tehtävä on huolehtia tuotetun datan siirtämisestä verkkotallennusalustalle ja vastaavasti mahdollistaa datan hakeminen sieltä sekä huolehtia tiedonsiirrosta varmistuspalvelimelle.

5.1 Lähtötilanne

Lähtötilanne verkon uusimiselle oli se, että tarve sen uudistamiselle oli ollut jo jonkin aikaa olemassa. Verkkotallennustila oli käytännössä täynnä ja sitä oli paikattu paikallisten, konekohtaisten tallennustilojen lisäämisellä. Verkossa liikkuva datamäärä oli kasvanut vuosi vuodelta ja nopeammat yhteydet olivat lähes välttämättömyys palveluiden tuottamiselle. Verkon kautta tallennetun datan loppukäyttäjille ei ollut omia päätelaitteita, vaan he joutuivat tutustumaan tuotettuun dataan jo ennestään ahtaissa tuotantotiloissa, mikä omalta osaltaan häiritsi tuotantotyötä.

Verkkoon oli ajan myötä liitetty paljon uusia koneita ja osa verkon laitteista kuten kytkimet olivat vanhentuneita ja niissä ilmeni aika ajoin porttivikoja, mikä vaikeutti datan saatavuutta. Tämän johdosta liitäntöjä oli jouduttu vaihtamaan kytkinten porteista toisiin. Uusien koneiden lisääminen ja kytkentöjen muuttelu oli aiheuttanut sen, että verkon kuvaukset olivat vanhentuneet ja nykytilanteen kuva oli ainoastaan yhden henkilön mielessä. Verkkoon liitetyistä koneista, kytkimistä, liitännöistä tai IP-osoitteista ei ollut ajan tasaista dokumentaatiota. Varmuuskopiopalvelin oli myös vanhentunut ja kaipasi uudistamista.

Oikeastaan oli ajauduttu tilanteeseen, johon ei missään tilanteessa pitäisi joutua. Osa verkon laitteista oli tullut elinkaarensa päähän ja samaan aikaan palveluiden tuottaminen ja loppukäyttäjien tarve tuotetulle datalle oli kasvanut verkon enimmäiskapasiteetin ylärajoille. Verkon käyttäjiltä saadun palautteen perusteella verkon laajentamiselle olisi myös tarvetta kokonaisprosessin tehostamiseksi.

5.2 Tavoiteltu lopputulos

Uusimisen jälkeen verkon on tarkoitus palvella sekä datan tuottajia että sen loppukäyttäjiä mahdollisimman tehokkaalla ja tarkoituksenmukaisella tavalla, mikä tukee yksiköiden toimintaa. Lopputuloksena on kytkinten avulla muodostettu verkko, jossa toimii päätelaitteiden lisäksi palvelin ja tallennusalusta. Tallennusalustan data varmuuskopioituu automaattisesti toisessa rakennuksessa sijaitsevalle varmistuspalvelimelle.

Verkon uusimisen jälkeen datan tuottajilla on 10 Gbit/s nopeuksiset yhteydet palvelimeen ja tallennusalustaan. Datan loppukäyttäjien yhteydet ovat nopeudeltaan 1 Gbit/s palvelimeen ja tallennusalustaan. Suurempien datan loppukäyttäjien osastoille asennetaan päätelaitteet, jotta he pystyvät käyttämään tuotettua dataa silloin kuin heillä on sille tarve ilman ylimääräisiä viiveitä. Tämä mahdollistaa sen, että datan käsitteleminen ei ole ajankohdasta kiinni.

Verkossa olevien päätelaitteiden sijoittaminen muualle kuin tuotantotiloihin aiheuttaa haasteita tietoturvalle. Verkkoon ja verkossa sijaitsevalle palvelimelle pääsevät sisään ainoastaan ne, joilla on oikeus tarkastella verkkoon tallennettuja tietoja ja vielä siten, että jokainen pääsee käsiksi ainoastaan niihin tietoihin, joihin hänellä on oikeus.

Verkon tallennuskapasiteetin tulee olla riittävä ja sitä tulee pystyä tarpeen tullen laajentamaan yksinkertaisesti ja nopeasti. Samoin verkkoon liitettävien koneiden määrän kasvu tulevaisuudessa otetaan huomioon.

5.3 Toteutussuunnitelma

Lähdin suunnittelemaan verkon uudistamista tuotantopuolella havaittujen ja toisaalta taas loppukäyttäjiltä saadun palautteen perusteella. Sekä havainnot että saatu palaute olivat hyvin pitkälle yhteneväisiä, mikä helpotti uuden verkkokokonaisuuden suunnittelua. Suunnittelun pohjana oli vanha, edelleen käytössä oleva verkko sekä rakennuksessa valmiina olevat nousu ja kerroskaapeloinnit, jotka ovat toteutettu kuitu- ja kuparikaapelointeina. Uudistettu verkko toteutetaan Ciscon hierarkkista verkkomallia mukaillen.

Talojakamosta oli valmiina kaikkiin kerrosjakamoihin sekä kuitu- että kuparikaapeloinnit. Lisäksi kerrosjakamoista oli kytkentätaulun kautta yhteydet kaikkiin työhuoneisiin. Tuotantokoneiden tarvitsema verkkokapasiteetti on siinä määrin suuri, että niiden ja palvelimen sekä tallennusalusta väliset yhteydet nostetaan 10 Gbit/s -nopeuteen. Datan loppukäyttäjille riittää tässä vaiheessa 1 Gbit/s -nopeudet. Tämä on myös kustannuskysymys, koska useissa vakiokoneissa on valmiina 1 Gbit/s -nopeuksia tukevat verkkokortit. Näin olleen ainoastaan tuotantokoneisiin pitää uusia verkkokortit, jotka tukevat 10 Gbit/s -nopeutta. Suuremmat 10 Gbit/s -nopeudet toteutetaan MMF-kuitukaapeleita ja cat7 kuparikaapeleita pitkin. Pienemmät 1 Gbit/s -nopeudet toteutetaan cat6 kuparikaapeleiden avulla.

Verkko toteutetaan niin sanottuna kytkinverkkona, jolloin siinä ei ole reititintä. Reititintä ei tarvita, koska toteutettavasta verkosta ei ole yhteyksiä toisiin verkkoihin. Yhteyksiä toisiin

verkkoihin tai internetiin ei toteuteta, koska se heikentäisi verkon tietoturvaa ja altistaisi verkon helpommin ulkopuolisen hyökkäyksen kohteeksi. Verkkoon sijoitetaan kahden eri tason kytkimiä. Tason 3 kytkimet mahdollistavat 10 Gbit/s -nopeudet ja muodostavat yhdistetyn runko ja jakelukerroksen sekä liityntäkerroksen datan tuottajille. Tason 2 kytkimet mahdollistavat 1 Gbit/s -nopeudet ja niitä käytetään liityntäkerroksen muodostamiseen datan loppukäyttäjille. Kytkimille mahdollistetaan etäyhteys, jotta niitä voidaan hallinnoida etänä verkon toisilta koneilta.

Käytännön kautta havaittu ja sisäisestä kirjausjärjestelmästä saadut tiedot auttavat suunnittelussa ja luovat tietopohjan siitä, mihin yksiköihin ja kuinka monta verkkoon liitettävää päätelaitetta kuhunkin yksikköön tulee sijoittaa. Näin osataan hankkia oikea määrä päätelaitteita ja osataan sijoittaa ne oikeisiin yksiköihin. Faktatietoihin perustuva suunnittelu on kustannustehokasta, koska turhia päätelaitteita ei tule hankittua, mutta päätelaitteita tulee hankittua riittävä määrä, jotta verkon ja yksiköiden toiminta on tehokasta.

Verkossa toimiva palvelin uusitaan. Uusi palvelin toimii ohjauspalvelimena ja tiedostopalvelimena, johon on liitetty verkkotallennusalusta. Lisäksi palvelimelle asennetaan DHCP helpottamaan IP-osoitteiden ylläpitoa verkon laajentuessa sekä DNS-nimipalvelin. Palvelimelle määritellään verkon käyttäjät ja heidän käyttöoikeutensa. Palvelimelle mahdollistetaan etäyhteys, jotta sitä voidaan hallinnoida etänä verkon toisilta koneilta. Lisäksi palvelimelle siirretään vanhassa palvelimessa toimineita tietojärjestelmiä.

Palvelimeen liitettävä verkkotallennusalusta toteutetaan siten, että siihen voidaan tarvittaessa lisätä yksinkertaisesti levyjä ja lisämoduuleja tallennuskapasiteetin nostamiseksi. Tallennusalustan levyt yhdistetään RAID 5 -pakaksi vikasietoisuuden sekä tallennus- ja lukunopeuden nostamiseksi. Tallennusalustalle mahdollistetaan etäyhteys, jotta sitä voidaan hallinnoida etänä verkon toisilta koneilta.

Verkon vanhasta palvelimesta tulee varmistuspalvelin, jonne automaattisesti varmuuskopioituu data, joka on tallennettu. Samalla vanha varmistuspalvelin jää ainoastaan vanhojen varmuuskopioiden tietovarastoksi.

5.4 Haasteet

Tämän työn toteuttamisessa oli muutamia haasteita, jotka tuli ratkaista ja joihin tuli varautua jo suunnitteluvaiheessa. Kaikkiin haasteisiin ei kuitenkaan voinut ennalta varautua ja niihin törmäsi vasta käytännön asennustöitä tehdessä. Pyrin minimoimaan näitä asennus-

töissä kohdattavia haasteita hyvällä ennakkosuunnittelulla. Kokonaisuuden kannalta suurimpana haasteena oli se, että verkkoa uudistettaessa verkon tuli olla toiminnassa ja sen toiminnassa sai olla vain lyhyitä katkoksia. Näin ollen toimenpiteiden aikataulutus oli tärkeä suunnitella huolella ja ajoittaa asennustyöt niihin aikoihin, kun verkon käyttö oli vähäistä tai sitä ei käytetty lainkaan, kuten iltaisin ja viikonloppuisin. Lisäksi asennustöiden ajan datalle oli rakennettava korvaavia reittejä pääreittien ollessa pois käytöstä.

Fyysiset laitteet, kuten kytkimet, palvelin ja tallennusalusta piti konfiguroida valmiiksi mahdollisimman pitkälle ja saada ne etähallinnan piiriin ennen paikalleen asentamista. Fyysisten laitteiden osalta pyrin tekemään varasuunnitelmat, mikäli asennuksen jälkeen ilmenisi, että ne eivät toimi vaaditulla tavalla.

Tietoturva tuli huomioida koko asennustöiden ajan. Tiedon luottamuksellisuudesta huolehtiminen ei ollut haasteellista, mutta tiedon eheys ja käytettävyys olivat haasteita, jotka tuli huomioida mahdollisimman hyvin suunnitteluvaiheessa. Tiedon eheys oli haasteena dataa siirrettäessä tallennusalustalta toiselle. Pyrin suunnittelussa huomioimaan sen, että datan eheys on varmistettu varmuuskopioilla jokaisessa tilanteessa ja mikäli jostain syystä data olisi vaurioitunut tai muuttunut toimenpiteiden aikana, niin se olisi nopeasti palautettavissa oikeaan muotoon varmuuskopiosta. Tiedon käytettävyyden varmistin rakentamalla korvaavia reittejä siksi aikaa, kun niin sanotut pääreitit eivät olleet toiminnassa ja pyrin pitämään verkon toiminnassa olevat katkokset mahdollisimman lyhyinä.

6 Käytännön asennustyöt

Kun suunnitelma lähiverkon toteuttamiseksi oli valmis, se piti hyväksyttää toimeksiantajan edustajalla. Hänen kanssaan käytyjen keskustelujen perusteella tein alkuperäiseen suunnitelmaani jotain pieniä muutoksia ja tarkennuksia. Nämä muutokset koskivat lähinnä IP-osoitteita, laitteiden nimeämiskäytäntöä sekä verkkoon sijoitettavien päätelaitteiden määriä ja niiden ominaisuuksia. Omassa alkuperäisessä suunnitelmassani oli määritelty laitteille tiettyjä ominaisuuksia, jotka lähtökohtaisestikin olivat vain ehdotuksia.

Lopullisen hyväksynnän jälkeen tehtiin toimeksiantajan toimesta tarvittavien laitteiden ja tarvikkeiden tilaus. Uusina laitteina tilattiin palvelin ja siihen Windows Server 2016 käyttöjärjestelmä; modulaarisia kytkimiä, joihin voidaan jatkossa liittää lisää porttimoduuleja tarpeen mukaan; skaalautuva tiedontallennusalusta, jotta tallennustilaa on mahdollisuus tulevaisuudessa kasvattaa nopeasti ja suhteellisen pienillä kustannuksilla. Lisäksi piti tilata oikeita nopeuksia tukevia kaapeleita sekä verkkokortteja.

Minä en osallistunut laitteiden tai järjestelmien hankintamenettelyyn millään tavoin. Toimeksiantaja suoritti laitteiden hankinnan täysin itsenäisesti omien käytäntöjensä ja hankintaohjesääntöjen mukaan. Näin ollen en ole voinut vaikuttaa hankittujen laitteiden merkkeihin tai malleihin enkä siihen mistä laitteet on hankittu. Laitteiden ominaisuuksista olen käynyt keskusteluja toimeksiantajan kanssa.

Tuotteet saapuivat eri aikaan ja niiden saapumisjärjestys saneli pitkälle sen, missä järjestyksessä mitäkin asennustöitä pystyi tekemään. Osa laitteista oli itselleni uusia, joita en ollut itse aikaisemmin käsitellyt, saati asentanut. Laitteiden käyttöjärjestelmiin ja asennusohjeisiin tutustuminen vaati aikaa. Tämän lisäksi selvittelin parhaita käytäntöjä laitteiden asennuksiin ja konfigurointiin liittyen. Pyrin mahdollisimman huolellisesti tutustumaan kuhunkin laitteeseen ja sen toimintaperiaatteisiin ennen niiden asentamista. Tällä pyrin välttämään sen, että joutuisin tekemään samoja asioita moneen kertaan ainoastaan siksi, että luulin jonkin asian toimivan tietyllä tavalla ilman, että olin ottanut siitä etukäteen selvää.

Yleisellä tasolla kuvattaessa käytännön asennustyöt etenivät siten, että ensin kokosin modulaariset kytkimet ja konfiguroin ne. Tämän jälkeen asensin uuteen palvelimeen käyttöjärjestelmän ja liitin sen verkkoon sekä asensin tarvittavat roolit ja palvelut. Seuraavana vuorossa oli tallennusalustan kokoaminen, konfigurointi ja liittäminen verkkoon sekä yhdistäminen palvelimeen. Kun tämä vaihe oli suoritettu, kopioin vanhasta palvelimesta tarvittavat järjestelmät uuteen palvelimeen. Lisäksi kopioin vanhasta tallennusalustasta hakemistorakenteen ja datan uuteen tallennusalustaan. Tätä seurasi vanhan palvelimen ja

vanhan tallennusalustan siirtäminen varmistuspalvelimeksi. Seuraavaksi määritin varmuuskopioinnin asetukset. Tämän jälkeen vuorossa oli verkkokorttien vaihtaminen käytössä oleviin päätelaitteisiin ja uusien päätelaitteiden asentaminen sekä kaikkien päätelaitteiden nimeäminen ja liittäminen verkon toimialueeseen. Lopuksi tein viimeiset puuttuvat liitokset uuden verkon kaapelointiin ja purin vielä jäljellä olleet, asennustöiden aikaiset reitit, joilla oli turvattu datan saatavuus. Tässä vaiheessa verkossa olevien päätelaitteiden määrä on siinä määrin vähäinen, etten segmentoinut verkkoa VLAN-alueisiin.

Koska verkon piti olla pieniä katkoksia lukuun ottamatta koko ajan käytössä, rakensin kytkinten avulla datalle reittejä siten, että katkoksilta vältyttiin muutamaa lyhyttä katkosta lukuun ottamatta. Pisimmät katkokset aiheutuivat palvelimen ja tallennusalustan vaihtamisesta. Lisäksi järjestelmän varmuuskopioinnissa oli katkos, kun vaihdoin vanhan palvelimen ja vanhan tallennusalustan varmistuspalvelimeksi.

Lopuksi dokumentoin kaikkien laitteiden sijainnit, nimet, IP-osoitteet ja liitännät. Keskeisimpien laitteiden ja järjestelmien asennusta sekä konfigurointia käsitellään tarkemmin omissa alakohdissaan.

6.1 Kytkimet

Uuteen lähiverkkoon liitin kaksi uutta modulaarista L3-tason kytkintä. Niiden kokoamisen jälkeen tein asetusten määrittämisen konsoliyhteydellä käyttäen Hyper Terminalia. Yhteyden muodostamissa piti antaa yhteysasetukset, jotka sain käyttöjärjestelmäohjeesta. Konsoliyhteyden auettua ensimmäistä kertaa näytölle aukesi kytkimen perusasetusnäyttö, jossa määrittelin kytkimen nimen, pääkäyttäjän salasanan, aikavyöhykkeen, IP-osoitteen ja aliverkon peitteen. Tallennuksen jälkeen suljin perusasetusnäytön. IP-osoitteen määrittäminen kytkimelle mahdollistaa sen hallinnoimisen etänä, esimerkiksi SSH-yhteydellä.

Perusasetusnäytön sulkemisen jälkeen yhteys kytkimen merkkipohjaiseen käyttöliittymään (CLI) oli auki pääkäyttäjäoikeuksilla. Annoin käyttöliittymässä komennon ’configure terminal’, minkä jälkeen pystyin antamaan asetusten määrityskomentoja. Asetin kytkimen kellon oikeaan aikaan komennolla ’clock set’. Komennon parametrit piti antaa järjestyksessä vuosi, kuukausi, päivä, tunnit, minuutit ja sekunnit. Tämän jälkeen tallensin tekemäni muutokset antamalla komennon ’write memory’. Lopuksi kirjauduin ulos ja suljin konsoliyhteyden. Tämän jälkeen asensin kytkimet niiden oikeille paikoille.

L3-tason kytkinten porttien nopeudet olivat oletuksena määritelty asetukselle auto. Tämä mahdollistaa sen, että kytkin pystyy automaattisesti muuttamaan porttien välistä liikennöintinopeutta 1Gbit/s ja 10Gbit/s välillä, jolloin eri nopeutta käyttävien laitteiden välille ei synny nopeuseron johdosta yhteysongelmia.

L3-tason kytkinten lisäksi käytin verkon toteutuksessa neljää aiemmin käytössä ollutta L2-tason kytkintä, jotka olivat toimivia. Näille kytkimille oli aikaisemmin määritelty IP-osoitteet, jolloin niitä pystyi konfiguroimaan etänä SSH-yhteydellä käyttämällä PuTTY:a Kirjauduin kytkimen CLI-käyttöliittymään pääkäyttäjänä. Nimesin kunkin kytkimen sen sijainnin mukaan ja asetin kellonajan oikeaksi. Käytetyt komennot olivat ’configure terminal’, ’clock set’, ’hostname’ ja ’write memory’. Lopuksi asensin kytkimet niiden omille paikoilleen.

Kytkinten asetusten määrittämiseen käytin apuna HP Enterprise Companyn Reference Guide Aruba 8.0.0.0 Command-Line Interface -nimistä ohjetta.

6.2 Palvelin

Lähiverkkoon tuli uusi palvelin. Ennen sen sijoittamista omalle paikalleen asensin siihen Windows Server 2016 -käyttöjärjestelmän USB-tikulta käyttäen palvelimelle esiasennettua käyttöjärjestelmän asennustoimintoa. Aktivoin Windowsin ja asensin siihen internetin välityksellä viimeisimmät päivitykset, joita oli neljä kappaletta. Tämän jälkeen nimesin palvelimen ja määrittelin sen 10 Gbit/s nopeutta tukevaan porttiin IP-osoitteen. Seuraavaksi otin etähallinnan käyttöön sallimalla Remote Desktopin ja Remote Managementin. Lopuksi asensin palvelimen sen omalle paikalleen ja liitin L3-tason kytkimeen.

Etähallinnan välityksellä asensin palvelimelle rooleja yksi kerrallaan. Roolien asennus tapahtui Server Managerissa valitsemalla Add roles and features. Sen kautta aukesi Wizard, joka ohjasi asennusta eteenpäin. Valitsin aina rooliin perustuvan asennuksen (Role-based or feature-based installation). Tämän jälkeen valittavaksi tuli palvelin, jolle rooli asennettiin. Seuravaksi valittavaksi tuli asennettava rooli. Käsittelen asentamani roolit yksi kerrallaan.

Ensimmäisenä asensin ohjauspalvelin -roolin valitsemalla Active Directory Domain Services (AD DS). Lisäsin Wizardin automaattisesti ehdottamat ominaisuudet. En tehnyt mitään muutoksia Wizardin oletusvalintoihin. Vahvistusvaiheessa valitsin kohdan automaattinen uudelleen käynnistys ja käynnistin asennuksen. Asennus kesti muutaman minuutin, jonka jälkeen suljin Wizardin.

Asennuksen oltua valmis vuorossa oli aktiivihakemiston määritykset (Active Directory Domain Service). Server Managerissa valitsin eniten vasemmalla olevasta sarakkeesta ”AD DS” -kohdan. Servers -kohtaan tuli keltaisella pohjalla ilmoitus, että aktiivihakemistoon pitää tehdä lisämäärityksiä. Niihin pääsi valitsemalla ilmoituksesta ”More”. Tästä aukesi Wizard, jossa lisämääritykset tehtiin. Lisämäärityksissä valitsin lisää uusi metsä, koska aiempaa toimialuetta (domainia) ei ollut ja nimesin toimialueen root domain name -kohtaan. Seuraavassa kohdassa annoin olla Windowsin ehdottamat oletukset toimintatasoiksi, jotka olivat korkeimmat mahdolliset eli ”Windows Server 2016”. Valitsin vielä DNS-Serverin ja sen mukana tuli automaattisesti Global Catalog. Lisäksi annoin Directory Services Restore Moden (DSRM) salasanan. DSRM on toiminto, johon kone voidaan käynnistää, mikäli aktiivihakemisto jostain syystä vikaantuu. Seuraavassa kohdassa tuli ilmoitus, ettei DNS-serverin parent zonea löydy. Ilmoituksesta ei tarvinnut välittää, koska asennus tapahtui suljetussa ympäristössä. Seuraavassa kohdassa määritin palvelimen NetBIOS-nimen. Annoin sen olla oletuksena. Seuraavassa kohdassa määritin tietokannan, lokitiedostojen ja SYSVOL-hakemiston sijainnit. Annoin niiden olla järjestelmän antamina oletusarvoina. Tämän jälkeen aukesi yhteenvetoikkuna, joka jälkeen käynnistin asennuksen. Asennus kesti muutaman minuutin, jonka jälkeen palvelin käynnistyi uudelleen.

Otin uuden etäyhteyden palvelimeen ja asensin Tiedostopalvelin (File Server) -roolin. File and Storage Services -rooli oli jo valmiiksi asennettuna. Valitsin Wizardista kohdan File Server ja lisäsin asennukseen Wizardin automaattisesti ehdottamat ominaisuudet. Asennuksen oltua valmis suljin Wizardin.

Lopuksi asensin DHCP -palvelimen (DHCP Server). Valitsin Wizardista kohdan DHCP Server ja lisäsin asennukseen Wizardin automaattisesti ehdottamat ominaisuudet. Asennuksen oltua valmis suljin Wizardin. DHCP-palvelimen määritykset pääsin asentamaan Server Managerin kautta valitsemalla Tools ja DHCP. Auenneesta ikkunasta valitsin palvelimen ja sen alta IPv4-protokollan. Napsautin tätä hiiren oikealla painikkeella ja valitsin New Scope. Nimesin toimialueen, minkä jälkeen määritin IP-osoiteavaruuden alku- ja loppuarvot. Tämän jälkeen määritin prefixin, joka määrittelee IP-osoitteen verkko-osan. Seuraavana vuorossa oli kohta poikkeukset (Exclusions). Tähän kohtaan pystyi syöttämään IP-osoiteavaruudesta ne osoitteet, joita DHCP ei jaa päätelaitteille. Määritin tähän kohtaan kytkinten, palvelimien ja tallennusalustojen IP-osoitteet. Viimeisenä kohtana ennen hyväksyntää piti määrittää aika, jonka DHCP:n antama IP-osoite on voimassa (Lease Duration). Annoin olla sen oletuksena, joka oli kahdeksan päivää. Lopuksi hyväksyin tekemäni määritykset.

Viimeiseksi loin aktiivihakemistoon kaksi organisaatioyksikköä (OU). Toiseen niistä loin toimialan käyttäjät ja toisen tein toimialueen tietokoneita varten. Nämä pääsin tekemään valitsemalla Server Managerista Tools ja Active Directory Administrative Centre. Käyttäjät loin valitsemalla toimialueen alta käyttäjiä varten luomani organisaatioyksikön ja valitsemalla New ja User. Syötin jokaisesta käyttäjästä etunimen, sukunimen ja kirjautumistunnuksen sekä määritin käyttäjälle salasanana ja salasanan asetukset.

Kun palvelimen asennus oli valmis, asensin siihen ohjelmiston, joka huolehtii tiedostojen automaattisesta varmuuskopioinnista. Ohjelmisto kopioi asetuksiin määritetyn aikavälein yhdistettyyn ohjaus- ja tiedostopalvelimeen yhteydessä olevan tallennusalustan datan varmistuspalvelimeen yhteydessä olevalle tallennusalustalle. Varmuuskopiointi tapahtuu ainoastaan muuttuneiden tiedostojen osalta ja varmuuskopioita ei pakata.

Palvelimen käyttöönotossa ja asetusten määrittämisessä käytin apuna Haaga-Helian Windows palvelimet -kurssilla opetettuja tietoja ja kurssilla käytettyä oppimateriaalia.

6.3 Tallennusalusta

Asensin tallennusalustan omalle paikalleen ja laitoin siihen ensimmäisessä vaiheessa yhdeksän kappaletta SSD-levyjä. Liitin tietokoneen suoraan ethernet-kaapelilla tallennusalustan RMT-porttiin. Käynnistin tietokoneen ja tallennusalustan. Avasin selaimen ja kirjauduin pääkäyttäjänä tallennusalustan graafiseen käyttöliittymään. Määritin tallennusalustalle nimen, vaihdoin pääkäyttäjän salasanan ja määritin MNT-portille IP-osoitteen. Tallennusalustan etähallinta tapahtuu samassa verkossa olevalta koneelta MNT-portin välityksellä.

Etähallinnan välityksellä tein tallennusalustalle tarvittavat määritykset, jotta sain sen toimintakuntoon. Ensimmäiseksi loin tarvittavat RAID-ryhmät valitsemalla RAID-ryhmä välilehden ja napsauttamalla ’Luo’. Nimesin ryhmän ja määritin RAID Leveliksi RAID5:den sekä valitsin RAID -ryhmään kuuluvat levyt. Seuraavaksi määritin Volumen (tallennustilan) valitsemalla Volume -välilehden ja napsauttamalla ’Luo’. Nimesin Volumen, määritin RAID Levelin ja liitin RAID -ryhmät manuaalisesti Volumeen. Lopuksi alustin levyt.

Tämän jälkeen valitsin Connectivity-välilehden alta Porttiryhmän ja iSCSI-portin. Syötin avautuneen ikkunan kenttiin portin IP-osoitteen ja aliverkon peitteen sekä portin nopeuden. Muut arvot annoin olla oletuksina. Saman välilehden alta määrittelin Host-ryhmään iSCSI Hostin syöttämällä siihen palvelimen iSCSI-nimen. Lopuksi määritin LUN-ryhmän,

joka mahdollistaa sen, että palvelin tunnistaa Volumet. Tämän jälkeen liitin tallennusalustan L3-tason kytkimen kautta verkkoon.

Seuraavaksi yritin yhdistää tallennusalustan palvelimeen avaamalla palvelimen Server Managerista Tools ja iSCSI Iniator. Palvelin tunnisti tallennusalustan, mutta ei liittänyt sitä. Löysin ratkaisun internetistä tallennusalustan valmistajan tukisivuilta. Ongelman aiheutti se, että en ollut määritellyt tallennusalustalle Host Affinitya, joka yhdistää Host -ryhmän ja porttiryhmän sekä Host -ryhmän ja LUN -ryhmän. Host Affinityn luomisen jälkeen tallennusalustan liittäminen palvelimeen onnistui ongelmitta.

Tallennusalustan käyttöönotossa käytin lähteenä Fujitsu ETERNUS AF250 All-Flash Arrays Setup Guidea. Lisäksi luin Server Worldin artikkelin Configure iSCSI Iniator ennen tallennusalustan liitämistä palvelimeen.

Myöhemmin lisäsin tallennusalustaan lisää SSD-levyjä. Loin näistä uusista levyistä RAID5 -ryhmiä ja laajensin aiemmin luomaani Volumea näillä uusilla RAID -ryhmillä. Volumen kokonaistallennuskapasiteetin kasvaessa tein huomion, että koska olin ensimmäisessä vaiheessa alustanut yhdeksän levyä, niin tässä alustuksessa valittu klusterikoko määritti Volumen enimmäistallennustilan.

NTFS -tiedostojärjestelmässä klusterikoko määräytyy Volumen koon mukaan. Tässä tapauksessa klusterikoko määräytyi ensivaiheessa tehdyn yhdeksän levyn koon perusteella. Volumen klusterikokoa ei voi levyjä lisättäessä muuttaa ilman, että alustaa Volumen kaikki levyt uudelleen. Mikäli jälkikäteen Volumen kokoa kasvatetaan lisälevyillä, niin alkuperäisen alustuksen klusterikoko määrää kuinka suureksi tai pieneksi Volume voidaan muuttaa. Seuraavassa taulukossa on Volumen raja-arvot, jotka määrittävät klusterikoon.

Taulukko 3. Volumen koon vaikutus klusterikokoon NTFS -tiedostojärjestelmässä (Microsoft 2017)

Volumen koko	Klusterikoko
7 MB - 16 TB	4 KB
16 TB - 32 TB	8 KB
32 TB - 64 TB	16 KB
64 TB - 128 TB	32 KB
128 TB - 256 TB	64 KB
> 256 TB	Ei tuettu

6.4 LEMP ja tietojärjestelmän siirto

Yksi keskeisimmistä tietojärjestelmistä, jonka siirsin vanhalta palvelimelta uudelle palvelimelle, toimii Debian käyttöjärjestelmän päällä ja sitä käytetään selaimen välityksellä. Siirron yhteydessä päivitin järjestelmän. Varmistuakseni, että järjestelmä oli koko ajan käytössä yhtä lyhyttä katkosta lukuun ottamatta, suoritin järjestelmän asennuksen ja toiminnan testauksen ensin testiympäristössä.

Asensin merkkipohjaisen Debian käyttöjärjestelmän toimimaan Windowsin päällä Oracle VM Virtual Boxin avulla. LEMP tulee sanoista Linux, Nginx, MySQL ja PHP. Asensin tarvittavat paketit seuraavilla komennoilla:

- sudo apt-get update
- sudo apt-get upgrade
- sudo apt get install mysql-server php7.0 php7.0-fpm php7.0-mysql nginx

Kun paketit olivat asentuneet, latasin tietojärjestelmän viimeisimmän asennuspaketin. Tein tarvittavat asetusten muutoksen Nginx:ään ja asensin tietojärjestelmän. Lopuksi testasin tietojärjestelmän toiminnan. Saadakseni toimivan kokoonpanon asennettua palvelimelle latasin Debianin virtuaalilevykuvan valitsemalla Export Appliance ja tallensin Appliancen USB-tikulle.

Seuraavaksi asensin USB-tikulta päivitetyn Oracle VM VirtualBoxin ohjauspalvelimelle. Käynnistin VirtualBoxin ja toin siihen USB-tikulta edellisessä kohdassa tekemäni Appliancen valitsemalla import Appliance. Kun virtuaalikone oli valmis, määritin sille kiinteän IP-osoitteen. Se tapahtui menemällä muuttamaan hakemiston /etc/network/ tiedostoa interfaces komennolla sudoedit interfaces. Kommentoin vanhat rivit pois ja lisäsin tiedostoon seuraavat rivit:

- auto enp0s3
- iface enp0s3 inet static
- address 192.xxx.xxx.xxx
- netmask 255.255.255.0

Lopuksi tallensin tiedot ja sammutin virtuaalikoneen. LEMP:n asentamiseen käytin apuna Unixmenin artikkelia How to install LEMP Stack On Debian 8. Staattisen IP-osoitteen määrittämiseen käytin lähteenä Debian Wikin artikkelia Network Configuration.

Saadakseni staattisen IP-osoitteen käyttöön muutin virtuaalikoneen verkkoasetuksiin ethernet adapteriksi Bridged Adapter ja verkkokortiksi palvelimen käytössä olevan verkkokortin. Lopuksi käynnistin virtuaalikoneen.

6.5 Varmistuspalvelin

Verkkoon liitetty uusi palvelin korvasi kokonaan siinä olleen vanhan palvelimen. Vanha palvelin oli kuitenkin toimintakuntoinen ja paljon uudempi kuin varmistuspalvelimena ollut palvelin. Siirsin verkossa olleen vanhan palvelimen ja siihen yhteydessä olevan iSCSI tallennusalustan varmistuspalvelimeksi toiseen rakennukseen.

Ennen palvelimen ja tallennusalustan siirtoa olin kopioinut vanhan tallennusalustan sisältämän datan uudelle tallennusalustalle. Tämä data on varmuuskopioituna vanhalle, aiemmin käytössä olleelle varmistuspalvelimelle.

Palvelimen ja tallennusalustan siirto ei sujunut täysin ongelmitta, vaikka siirsin toimivan kokoonpanon ainoastaan toiseen rakennukseen tekemättä siihen mitään muutoksia. Palvelin toimi moitteetta, mutta iSCSI-tallennusalustasta toimi ainoastaan MNT-portti (ylläpitoportti). Yksikään iSCSI-portti ei toiminut. Tallennusalustan asetuksista en löytänyt mitään vikaa, en myöskään palvelimen iSCSI Iniator kytkennästä. Kokeilin eri vaihtoehtoja tallennusalustan uudelleen käynnistämisestä asetusmuutoksiin, mutta mikään niistä ei auttanut. Sekä palvelin että tallennusalusta olivat kiinni vanhassa kytkimessä. Vaihdoin kytkimen uudempaan, jolloin iSCSI-portit alkoivat toimimaan. Ongelman aiheuttajaksi ilmeni kytkin, jossa palvelin ja tallennusalusta olivat ensin kiinni. Tarkemman tarkastelun jälkeen ilmeni, että kytkin tuki vain 100 Mbit/s nopeuksia. Sen asetuksiin oli porttinopeudeksi määritelty ’auto’ eli portin piti toimia automaattisesti oikealla nopeudella. Koska tallennusalustan iSCSI-portit toimivat 1 Gbit/s nopeudella, niin kytkin ei pystynyt välittämään 1 Gbit/s nopeuksista liikennettä porteistaan, jotka tukivat ainoastaan 100 Mbit/s nopeutta. Tästä opin sen, että porttinopeudet pitää tarkastaa ennen muita toimenpiteitä, mikäli yhteyttä ei saa muodostettua. Lopuksi alustin uuden varmistuspalvelimen ohjaaman tallennusalustan.

6.6 Työasemat

Asensin työasemiin, jotka tulevat käyttämään 10 Gbit/s nopeutta uudet verkkokortit, jotka tukevat tätä nopeutta. Työasemissa, jotka käyttävät 1 Gbit/s nopeutta oli valmiina tätä nopeutta tukevat verkkokortit.

Työaseman liittäminen toimialueelle tapahtui seuraavasti. Ensin määritin työasemalle kiinteän IP-osoitteen, aliverkon peitteen ja gatewayn sekä määritin DNS-palvelimen osoitteeksi ohjauspalvelimen IP-osoitteen. Jos DNS-palvelimen osoite on jokin muu kuin ohjauspalvelimen IP-osoite, työaseman liittäminen toimialueelle ei onnistu. Tämän jälkeen

valitsin Resurssienhallinnasta (File Explorer) - Tämän tietokoneen (This PC) ja sen ominaisuudet (Properties). Valitsin tietokoneen nimen kohdalta 'Muuta' ja nimesin koneen suunnitellun nimeämiskäytännön mukaan ja valitsin jäsenyydeksi (Member Of) Domainin. Tähän kohtaan annoin arvoksi aiemmin ohjauspalvelimelle määritellyn toimialueen nimen. Lopuksi hyväksyin muutokset. Tämän jälkeen piti syöttää toimialueen administrator -tunnus ja sen salasana, että kone hyväksyttiin toimialueelle. Lopuksi kone käynnistyi uudelleen, jonka yhteydessä ohjauspalvelin lisäsi koneen NetBIOS-nimen automaattisesti ohjauspalvelimen aktiivihakemiston toimialueen alla olevaan Computers -säiliöön. Mikäli ohjauspalvelimelta ei löydy kirjautuvan koneen NetBIOS-nimeä, ohjauspalvelin ei anna työasemasta kirjautua toimialueelle.

Kun olin liittänyt toimialueelle kaikki verkon työasemat, kävin siirtämässä koneiden tiedot ohjauspalvelimen aktiivihakemistossa toimialueen alla Computers säiliöstä työasemia varten luotuun organisaatioyksikköön.

Työaseman liittämisessä toimialueelle tulee huomioida, että Windows luo toimialueen käyttäjälle uuden työpöydän, kun toimialueen käyttäjä kirjautuu ensimmäisen kerran toimialueelle. Aiemmin käytössä olleen tietokoneen paikallisen profiilin tiedostot eivät siirry uudelle työpöydälle.

6.7 Testaus

Aina, kun liitin uuden laitteen verkkoon, testasin sen saavutettavuuden lähettämällä ping -paketin palvelimelta sekä yhdeltä verkon työasemalta liitettyyn laitteeseen. Kaikki verkkoon liitetyt laitteet vastasivat heti, pois lukien varmistuspalvelimen tallennusalusta. Muita yhteysongelmia ei ilmennyt.

Työaseman verkkoon liittämisen jälkeen tarkastin työasemalta, että kaikki verkossa olevat työasemat ja palvelimet näkyivät työaseman resurssienhallinnassa. Samoin tarkastin, että palvelimen resurssienhallinta löysi verkossa olevat työasemat.

Lopuksi suoritin verkolle vielä nopeuden mittaamisen siihen suunnitellulla ohjelmistolla. Nopeuden mittaamisessa käytin 9 GB -kokoista datapakettia. Ohjelmisto mittasi lähetyksen ja vastaanoton nopeudet. Testin tuloksena oli, että uuden verkon nopeus oli merkittävästi suurempi kuin mitä vanhan verkon nopeus oli.

Lisäksi testasin ohjauspalvelimen aktiivihakemiston toiminnan. Ainoastaan niillä koneilla, jotka olivat aktiivihakemistossa, pääsi käsiksi palvelimella oleviin tietoihin käyttäjän käyttöoikeuksien rajoissa.

6.8 Toteutuksen lopputulos

Asennustöiden lopputuloksena syntyi suljettu kytkinverkko, joka ei sisällä langattomia yhteyksiä eikä siitä ole yhteyksiä muihin verkkoihin. Verkossa on kaksi tason 3 -kytkintä, jotka on yhdistetty toisiinsa kahdella MMF-kuitukaapelilla. Kytkinten välinen tiedonsiirtonopeus on 10 Gbit/s. Nämä kytkimet muodostavat verkon yhdistetyn runko- ja jakelukerroksen.

Verkon liityntäkerros on toteutettu tason 2 -kytkimillä pois lukien ne päätelaitteet, jotka tarvitsevat 10 Gbit/s tiedonsiirtonopeutta sekä ohjauspalvelin ja siihen kytketty tallennusalusta. Nämä laitteet on yhdistetty suoraan Cat7- luokan UTP-kuparikaapeleilla tason 3 kytkimeen. Liityntäkerroksen tason 2 -kytkimet mahdollistavat 1 Gbit /s tiedonsiirtonopeuden ja ne on liitetty tason 3 kytkimiin Cat 6a -luokan UTP-kuparikaapeleilla. Poikkeuksena tästä on tason 2 kytkin, johon varmistuspalvelin on kytketty. Tämän kytkimen ja tason 3 kytkimen välinen yhteys on toteutettu MMF-kuitukaapeleilla. Päätelaitteet, jotka käyttävät 1 Gbit/s tiedonsiirtonopeutta on yhdistetty tason 2 kytkimiin Cat 6a -luokan UTP-kuparikaapeleilla. UTP-kuparikaapeleissa on käytetty RJ-45 -liittimiä ja MMF-kuitukaapeleissa on käytetty Duplex Multimode LC -liittimiä.

Verkossa toimii noin kaksikymmentä työasemaa ja kaksi palvelinta, joista toinen on yhdistetty ohjaus- ja tiedostopalvelin ja toinen on varmistuspalvelin. Ohjauspalvelin huolehtii verkkoon luodun toimialueen käyttäjien ja koneiden hallinnasta. Lisäksi siihen on asennettu DNS- sekä DHCP-palvelin. Kyseinen palvelin toimii myös tiedostopalvelimena ohjaten siihen iSCSI-yhteydellä liitettyä tallennusalustaa. Edellä mainittujen lisäksi palvelimella on toiminnassa järjestelmiä, jotka ovat saatavilla ainoastaan tässä verkossa. Varmistuspalvelin ohjaa toista tallennusalustaa, joka on yhdistetty siihen iSCSI-yhteydellä.

Tietoturvan toteutumisesta uudistetussa verkossa on huolehdittu siten, että tiedon luottamuksellisuus, eheys ja käytettävyys toteutuisivat mahdollisimman hyvin. Luottamuksellisuus toteutuu siten, että verkkoon pääsee kirjautumaan ainoastaan ohjauspalvelimelle syötetyillä käyttäjätunnuksilla ja salasanoilla ja ainoastaan koneista, jotka ovat liitetty verkon toimialueelle. Lisäksi käyttäjä pääsee näkemään ainoastaan ne hakemistot, joihin hänellä on työtehtäviensä puolesta oikeus. Eheys on turvattu siten, että käyttäjillä, jotka tarvitsevat tuotettua tietoa on ainoastaan lukuoikeus tietoihin. Näin ollen he eivät pääse

muuttamaan tietoja. Lisäksi pääkäyttäjäoikeudet on eriytetty kaikista käyttäjätunnuksista. Käytettävyydestä on huolehdittu automatisoidulla varmuuskopioinnilla.

Verkon fyysinen topologia on kuvattu liitteessä 1.

7 Yhteenveto

Toteutettu työ oli kokonaisuutena arvostellen haastava. Se koostui monesta eri osa-alueesta ja piti sisällään useita eri työvaiheita. Haastavinta työssä oli verkon suunnittelu ja kokonaisuuden hahmottaminen siten, että lopputulos on toimiva ja vaatimusten mukainen. Suunnittelutyön haastetta lisäsi se, että verkon tuli olla pieniä katkoksia lukuun ottamatta koko ajan toiminnassa. Pelkän toteutuksen lopputuloksen suunnittelu ei riittänyt, vaan aina ennen uutta asennustyövaihetta piti suunnitella korvaava reitti datalle, jotta pitkiä katkoksia ei muodostunut.

Sen lisäksi, että työ oli haastava, se oli myös erittäin mielenkiintoinen ja opettava. Mielenkiintoiseksi työn teki sen haastavuus ja että pääsin käytännössä fyysisillä laitteilla toteuttamaan verkkoratkaisun. Ennen tätä työtä olin toteuttanut verkkoja ainoastaan virtuaaliympäristössä, lähinnä Ciscon Packet Tracer -ohjelmalla. Opettavaksi työn teki asennustöissä ilmenneiden ongelmien ja haasteiden ratkaiseminen sekä se, että käytännön asennustyöt osoittivat suunnittelussa huomioimatta jääneet asiat.

Mielestäni onnistuin hyvin työn toteutuksessa. Lopputuloksena on toimiva kokonaisuus, joka vastaa hyvin tämän hetken toiminnan vaatimuksiin ja on helposti laajennettavissa, mikäli siihen on tulevaisuudessa tarvetta. Päädyin toteuttamaan verkon toimialueena (domain) enkä yksityisenä verkkona (private network). Syy tähän oli se, että toimialuetoteutuksena palvelimen aktiivihakemisto huolehtii verkon käyttäjien ja siinä olevien työasemien hallinnasta ja näin lisää verkon tietoturvaa. Palvelimelle siirtämäni selaimella toimiva ohjelmisto toimii LEMP-alustalla. Se on aikanaan rakennettu LEMP-alustan päälle, enkä nähnyt tarvetta vaihtaa Nginx:ää Apacheksi tai muuksi web-palvelimeksi. Modulaariset tason 3 kytkimet valikoituivat yhdistetyn runko- ja jakeluverkon kytkimiksi, koska ne mahdollistavat automaattisen nopeuden muuntamisen 1 Gbit/s ja 10 Gbit/s välillä, joten eri nopeudella toimivat laitteiden portit eivät aiheuta ongelmia verkon toiminnalle. Lisäksi niiden avulla pystyy tarvittaessa tulevaisuudessa reitittämään eri VLAN-verkkojen välistä liikennettä, mikäli verkon segmentoinnille tulee tarvetta. Niiden etuna on myös, että verkon laajetessa niihin pystyy liittämään lisää porttimoduuleja, eikä koko kytkintä tarvitse vaihtaa.

Vaikka verkko tällä hetkellä vastaa hyvin toiminnan tarpeisiin, niin jatkossa sitä voi vielä kehittää parantamalla sen vikasietoisuutta ja lisäämällä ylläpitoa helpottavia ominaisuuksia sekä segmentoimalla sitä VLAN-verkkojen avulla. Verkon vikasietoisuutta voidaan tulevaisuudessa parantaa lisäämällä verkkoon kytkimiä, joiden avulla saadaan muodostettua vaihtoehtoisia reittejä alkuperäisen reitin katketessa esimerkiksi laite- tai kaapelivi-

kaan. Tämä kuitenkin nostaa verkon kokonaiskustannuksia, eikä se ole tällä hetkellä ajankohtaista. Ylläpitoa helpottavia ominaisuuksia, kuten automatisoituja hälytyksiä ja verkon monitorointia tulee harkita tulevaisuudessa etenkin, jos verkko laajenee nykyisestään. Toistaiseksi verkon työasemien määrä on siinä määrin vähäinen, ettei verkon segmentoiminen ole ajankohtaista, mutta mahdollisen laajenemisen myötä sekin saattaa tulla ajankohtaiseksi.

Produktiivisen osuuden eli varsinaisten asennustöiden tekeminen ei pelkästään ollut kulkemista onnistumisesta onnistumiseen. Esimerkiksi kummankin tallennusalustan kanssa oli ongelmia. Näiden ongelmien selvittelemiseen meni aika paljon aikaa. Tämä johtui suurelta osin kokemattomuudestani tällaisen toteutuksen tekemiseen. Aikaa kului ongelmatilanteiden paikantamiseen ja mahdollisten ratkaisujen etsimiseen internetistä. Jossain vaiheessa projektia tuntui siltä, että olen haukannut liian suuren palan. Jatkoin kuitenkin sinnikkäästi ja lopulta yritysten ja erehdysten kautta sain projektin vietyä onnistuneesti loppuun. Tämän toteutuksen jälkeen olen paljon valveutuneempi tekemään vastaavia projekteja.

Opinnäytetyöprosessi on kokonaisuutena ollut kaikkien haasteiden myötä palkitseva ja omaa oppimista tukeva. Opinnäytetyön aihe valikoitui helposti, koska opinnäytetyön tullessa ajankohtaiseksi työpaikalla ilmeni tarve suljetun lähiverkon uusimisesta. Koko prosessi alkoi suunnitelmalla ja eteni produktiivisen työn onnistuneeseen toteutukseen. Prosessin aikana alkuperäinen suunnitelma koki pieniä muutoksia käytännön sanelemana. Nämä muutokset olivat lähinnä opinnäytetyössä käsiteltävien asioiden tarkentumista ja rajaamista.

Tämä työ tuki hyvin omaa oppimistani, koska luin omat profiiliopintoni ICT-infrastruktuureista. Käytännön työn tekeminen konkretisoi teoriassa oppimiani asioita ja työn toteuttamiseksi lukemani lähdeaineisto syvensi tietoja tästä aihepiiristä. Työn avulla pääsin käytännössä toteuttamaan oppimiani asioita lähiverkkojen toiminnasta, palvelimista ja tietoturvasta. Tärkein tässä työssä oppimani asia on, että kaikki toimenpiteet tulee dokumentoida, että on selvillä, mitä on tehnyt ja miten. Koska jos jokin asia ei muutoksen tai asentamisen jälkeen toimi, niin vanhaan pystyy palaamaan eikä tee samoja asioita useaan kertaan. Lopuksi uskallan todeta, että tämän opinnäytetyön jälkeen omaan valmiudet suunnitella ja toteuttaa pienen lähiverkon, joka on vikasietoinen, skaalautuva ja tietoturvallinen.

Lähteet

Al-Shawi, M. & Laurent, A. 2016. Designing for Cisco Network Service Architectures (ARCH). Cisco Press.

Arslan, E. 2015. Hierarchical Topology. Luettavissa: https://prezi.com/yjasnbrogosp/hierarchical-topology/. Luettu: 13.2.2018.

Cisco Networking Academy 2014. Connecting Networks Companion Guide: Hierarchical Network Design. Cisco Press. Luettavissa: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. Luettu: 18.2.2018.

Cisco Networking Academy 2016a. Introduction to Networks Companion Guide v5.1. Cisco Press.

Cisco Networking Academy 2016b. Routing and Switching Essentials v6 Companion Guide. Cisco Press.

Computer Hope 2017. Mesh topology. Luettavissa: https://www.computerhope.com/jargon/m/mesh.htm. Luettu: 13.2.2018.

Computer Hope 2018a. Bus Topology. Luettavissa: https://www.computerhope.com/jargon/b/bustopol.htm. Luettu: 13.2.2018.

Computer Hope 2018b. Ring Topology. Luettavissa: https://www.computerhope.com/jargon/r/ringtopo.htm. Luettu: 13.2.2018.

Computer Hope 2018c. Star Topology. Luettavissa: https://www.computerhope.com/jargon/s/startopo.htm. Luettu: 13.2.2018.

Debian Wiki 2017. Network Configuration. Luettavissa: https://wiki.debian.org/NetworkConfiguration. Luettu: 21.2.2018.

eTutorials 2018. Hierarchical Topology. Luettavissa: http://etutorials.org/Networking/Lan+switching+first-step/Chapter+10.+LAN+Switched+Network+Design/Hierarchical+Topology/. Luettu: 13.2.2018.

Froehlich A. 2006. Layer 3 switches explained. Luettavissa: http://searchnetworking.techtarget.com/tip/Layer-3-switches-explained. Luettu: 16.2.2018.

Fujitsu 2017. Fujitsu Storage ETERNUS AF250 All-Flash Arrays Setup Guide. Luettavissa: https://sp.ts.fujitsu.com/dmsp/Publications/public/P3AG-1862-EN.pdf. Luettu: 13.2.2018.

Harrington J. 2007. Ethernet Networking for the Small Office and Professional Home Office. Elsevier Science.

HP Enterprise Company 2016. Reference Guide Aruba 8.0.0.0 Command-Line Interface. Luettavissa: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c05321928-1.pdf. Luettu: 10.1.2018.

Microsoft 2017. Default cluster size for NTFS, FAT and exFAT. Luettavissa: https://support.microsoft.com/en-us/help/140365/default-cluster-size-for-ntfs-fat-and-exfat. Luettu: 25.2.2018.

Mitchell B. 2017. What is a Hub. Luettavissa: https://www.lifewire.com/ethernet-and-network-hubs-816358. Luettu: 16.2.1018.

Pasricha H. & Jagu D. 2004. Designing Networks with Cisco. Charles River Media.

Philpott, L. 2015. Network Topology. Luettavissa: https://www.thinglink.com/scene/649398917267456002. Luettu: 12.2.2018.

Server World 2017. iSCSI: Configure iSCSI Iniator (Server OS). Luettavissa: https://www.server-world.info/en/note?os=Windows_Server_2016&p=iscsi&f=3. Luettu: 16.2.2018.

Sesko 2016. Tietotekniikka yleiskaapelointijärjestelmät. Kaapelointi on tietoliikennepalvelujen kivijalka. Luettavissa: http://www.sesko.fi/files/629/Tietotekniikka_Yleiskaapelointijarjestelmat.pdf. Luettu: 22.2.2018.

Snyder J. 2009. Do you need an IDS or IPS, or both? Luettavissa: http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both. Luettu: 24.2.2018.

Stewart J, Chapple M & Gibson D. 2012. CISSP: Certified Information Systems Security Professional Study Guide. John Wiley & Sons, Incorporated.

Unixmen 2015. How to Install LEMP (nginx, MySQL or MariaDB, PHP) Stack on Debian 8. Luettavissa: https://www.unixmen.com/how-to-install-lemp-stack-on-debian-8/. Luettu: 21.2.2018.

Wilkins S. 2011. Spanning Tree Protocol Concepts and Configuration. Luettavissa: http://www.ciscopress.com/articles/article.asp?p=1728837. Luettu: 24.2.2018.

Liitteet

Liite 1. Valmiin verkon fyysinen topologia