Opinnäytetyö (AMK)

Tietojenkäsittely

NLIIBK14

2017

Aleksi Hakanen

LÄHIVERKON UUDISTUKSEN SUUNNITTELU

– Tapaus Liedon kunta

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2017 | 28

Aleksi Hakanen

LÄHIVERKON UUDISTUKSEN SUUNNITTELU

- Tapaus Liedon kunta

Työn tarkoituksena oli kehittää suunnitelma lähiverkon uudistuksesta Liedon kunnalle. Lähiverkkoja ei oltu toimeksiantajalla kokonaisvaltaisesti suunniteltu, koska verkkolaitteita on hankittu sitä mukaan, kun niitä on tarvittu. Tämä on johtanut kokonaiskuvan hämärtymiseen sekä tulevaisuuden suunnitelmien puuttumiseen. Näistä syistä Liedon kunnalla oli tarve selvittää nykyiset laitteet sekä tehdä selkeä suunnitelma, miten lähiverkkoja toteutetaan vastedes. Suunnittelussa selvitettiin, mitä tekniikoita ja topologioita nykypäiväiset lähiverkot käyttävät ja miten lähiverkkoja voitaisiin hallita.

Työ tehtiin konstruktiivisella otteella tapaustutkimuksena. Ensin tutkittiin lähiverkkojen teoriaa, ja sen jälkeen katsottiin kappalekohtaisesti, miten lähiverkkojen uudistus voitaisiin toteuttaa toimeksiantajalla.

Työn tuloksena syntyi ohjeistus ja suositukset lähiverkkojen toteuttamisesta. Tähän sisältyi käytettävät tekniikat ja nopeudet. Myös lähiverkon hallinta käytiin läpi. Tässä työssä ei otettu suuremmin kantaa langattomiin verkkoihin. Työssä ajateltiin, että langattomat verkot toteutetaan olemassa olevalla ratkaisulla riippumatta muusta lähiverkosta.

Työn aikana esille nousi, miten nykyaikainen ja skaalautuva lähiverkko rakennetaan ja miten sitä hallitaan. Tulevaisuudessa tämän suunnitelman pohjalta voidaan tehdä lähiverkon uudistus. Tapausta käsittelevä kappale on kirjoitettu siten, että sitä voidaan hyödyntää yleisemmin myös muiden organisaatioiden toimesta.

ASIASANAT:

Lähiverkko, laajaverkko, verkkoinfrastruktuuri

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2017 | 28

Aleksi Hakanen

PLANNING OF LOCAL AREA NETWORK RENEWAL

- Case: municipality of Lieto

The purpose of this thesis was to develop a plan for a local area network renewal for the municipality of Lieto. The local area networks of the client had not been planned or designed comprehensively prior to this research. The networking equipment had been acquired as needed without much regard for network design or planning. This has lead to a lack of overall information about the networks and the lack of future plans for the networks. For these reasons the municipality of Lieto had the need to audit the current equipment and make a clear plan how local area networks would be implemented henceforth. Research delved into what technologies and topologies local area networks use and how local area networks are managed today.

The work was done as a constructive case study. First the thesis goes into the theory of local area networks and then addresses how local area networks could be implemented for the client.

The result was guidance and preferences for implementing new local area networks for the client. This included the technologies, speeds and how local area networks could be managed cost-effectively. The work does not take wireless networks into account. The clients existing wireless network solution was implemented regardless of the rest of the local area network.

It was brought up how modern and scalable networks are built and how they are managed. In the future the client can use this document as a reference when implementing the new local area network. The chapter that discusses the client has been written so that it can be used by parties other than the client. It is meant to be widely useful and implementable.

KEYWORDS:

Local area network, wide area network, network infrastructure

SISÄLTÖ

KUVAT

LYHENTEET

BPDU	Virityspuualgoritmin viesti, jossa kerrotaan kytkimen tietoja, kuten MAC-osoite ja STP-prioriteetti (McMillan 2011).
MAC-osoite	2. kerroksen osoite, jonka verkkolaitteen valmistaja määrittää laitteeseen (McMillan 2011).
Mbps	Nopeus jolla dataa siirretään, megabittiä per sekunti (Ciccarelli & Faulkner 2006).
PoC	Projektin vaihe, jossa testataan käytännön toimivuutta pienessä mittakaavassa ennen kokonaista toteutusta (Omni Partners 2017).
STP	Protokolla joka tarkistaa, ettei lähiverkossa ole silmukoita (Dooley 2002).
VLAN	Laitteiden looginen ryhmä, joka mahdollistaa fyysisen verkon jakamisen loogisiin osiin (Dooley 2002).

1 JOHDANTO

Opinnäytetyön tarkoituksena oli tehdä katsaus lähiverkkojen suunnitteluun ja teknologioihin sekä esittää toimeksiantajalle nykyaikainen ratkaisu lähiverkkojen toteuttamiseen. Tämän suunnitelman pohjalta toimeksiantaja voi tehdä ratkaisuja lähiverkkojensa toteutuksesta tulevaisuudessa. Työ on ajankohtainen, koska toimeksiantajan nykyinen verkkototeutus on melko kallis, verkkolaitteet ikääntyvät jatkuvasti sekä uusia ominaisuuksia ja laitteita tulee markkinoille tasaiseen tahtiin.

Työssä käydään ensin läpi lähiverkkojen teoriaa, suunnittelua ja nykypäivänä saatavilla olevia teknologioita. Lähiverkkojen tekniikka on pysynyt suhteellisen samana monia vuosia, mutta kaikkia ominaisuuksia ei ole haluttu tai tiedetty ottaa käyttöön. Tämän suunnitelman pohjalta toimeksiantaja voi parantaa lähiverkkojensa suorituskykyä, luotettavuutta ja hallittavuutta, jotta pystytään vastaamaan verkon tarpeisiin nyt ja tulevaisuudessa. Lopuksi käydään läpi toimeksiantajalle toteutettavat ratkaisut suunnittelun pohjalta.

Verkoista ja etenkin lähiverkoista on kirjoitettu jo vuosikymmeniä. Lähiverkkoja on tarvittu siitä lähtien, kun tietokoneita on alettu käyttämään yliopistoissa. Lähiverkoilla yhdistettiin aluksi vain muutamia tietokoneita saman rakennuksen sisällä, mutta myöhemmin lähiverkot laajenivat niin laitemääriltään kuin fyysiseltä ulottuvuudeltaankin. Tästä syystä lähiverkkojen suunnittelu on erittäin pitkälle edennyt aihe ja luotettavaa kirjallisuutta on saatavilla merkittävästi. (Hakala & Vainio, 4-5.) Teoriaosuuden onkin tästä syystä tarkoitus tuoda esille niitä asioita, joita toimeksiantajan verkoissa pitää pohtia ja mihin kysymyksiin pitää saada vastaus. Tarkoituksena ei ole käydä tyhjentävästi läpi kaikkia verkkosuunnittelun ja verkkolaitteiden ominaisuuksia.

2 VERKKOSUUNNITTELU JA INFRASTRUKTUURI

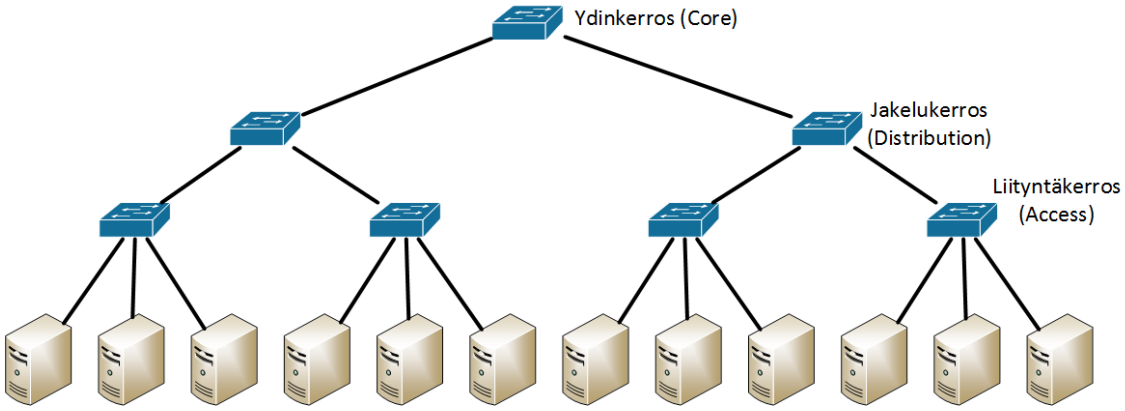
Verkkosuunnittelun yhtenä pääperiaatteena voidaan pitää yksinkertaisuutta. Yksinkertaisuus johtaa vian selvittämisen helppouteen sekä hallinnan helpottumiseen. Jos verkko suunnitellaan mahdollisimman yksinkertaiseksi, myös verkon tehokkuus kasvaa, kun verkkolaitteiden määrä pyritään minimoimaan. Samalla mahdollisten ongelmakohtien määrä pienenee. Myös käytettävien ominaisuuksien tarpeellisuus on oltava perusteltavissa. Laitteissa on nykyään niin paljon ominaisuuksia, että pienelläkin laitemäärällä voidaan saada erittäin monimutkainen toteutus aikaiseksi. Sopivan yksinkertaisuuden mittakeppinä voidaan pitää sitä, että verkkosuunnittelija, jolle verkko on tuttu, voi ratkaista verkon vikoja ilman dokumentaatiota. (Dooley 2002, 125.)

Lähiverkon liikennemääriä voidaan ajatella 80/20-säännön avulla. Sääntö tarkoittaa, että 80 prosenttia verkon liikenteestä pysyy saman lähiverkon sisällä ja 20 prosenttia menee laajaverkkoon. Ajatus perustuu siihen, että aikoinaan työasemat siirsivät dataa keskenään paljon ja tarvittavat palvelimet ja palvelut olivat fyysisesti samassa rakennuksessa tai lähirakennuksissa kuin työntekijätkin.

Nykyisin palvelimet on keskitetty ja ulkoistettu palvelinratkaisujen tarjoajille. Tämä tarkoittaa sitä, että palvelimet eivät ole enää fyysisesti työntekijöiden lähellä, vaan ne saattavat olla jopa toisella mantereella. Esimerkiksi tietokannat, internet, intranet ja sähköposti ovat saatavilla keskitetyiltä palvelimilta (Boyles & Hucaby 2001, 29). Tämä puolestaan tarkoittaa sitä, että 80/20-sääntö on kääntynyt päälaelleen ja nykyisin voidaan ajatella, että 80 prosenttia liikenteestä menee laajaverkkoon ja 20 prosenttia pysyy lähiverkon sisällä. Tämä tarkoittaa merkittävää muutosta, kun suunnitellaan lähi- ja laajaverkkojen kapasiteettia.

2.1 Hierarkkinen verkkosuunnittelu ja topologiat

Hierarkkinen verkkosuunnittelu tarkoittaa verkon jakamista kolmeen eri kerrokseen. Ensimmäisenä tai alimmaisena kerroksena on liityntäkerros (Access). Tämä on kerros, johon päätelaitteet yhdistetään. Liityntäkerros yhdistetään jakelukerrokseen (Distribution), joka yhdistää liityntäkerroksen laitteet. Jakelukerroksen laitteet liitetään ydinkerrokseen (Core), joka yhdistää jakelukerroksen laitteet (Kuva 1). (McCabe 2007, 233-234.)

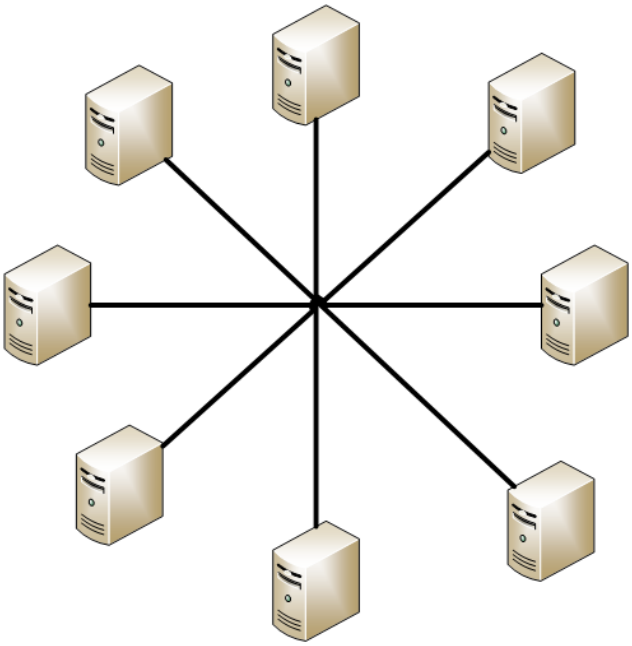


Kuva 1. Verkon hierarkia.

Mallin ideana on se, että eri tehtävää suorittavat laitteet varataan vain tietylle tehtävälle. Liityntäkerroksen tehtävä on yhdistää verkkolaite päätelaitteeseen kuten tietokoneeseen. Jakelukerroksen tehtävänä on yhdistää liityntäkerroksen laitteet ja ohjata liikennettä eteenpäin. Ydinkerroksen tehtävänä on olla viimeisenä yhdistävänä laitteena koko lähiverkon osalta. Mallilla voidaan suunnitella verkkoja ottamatta kantaa siihen, minkälainen laite on verkon eri kohdissa. Tätä mallia käyttämällä saadaan rakennettua luotettava, helposti skaalattavissa sekä ymmärrettävissä oleva verkko.

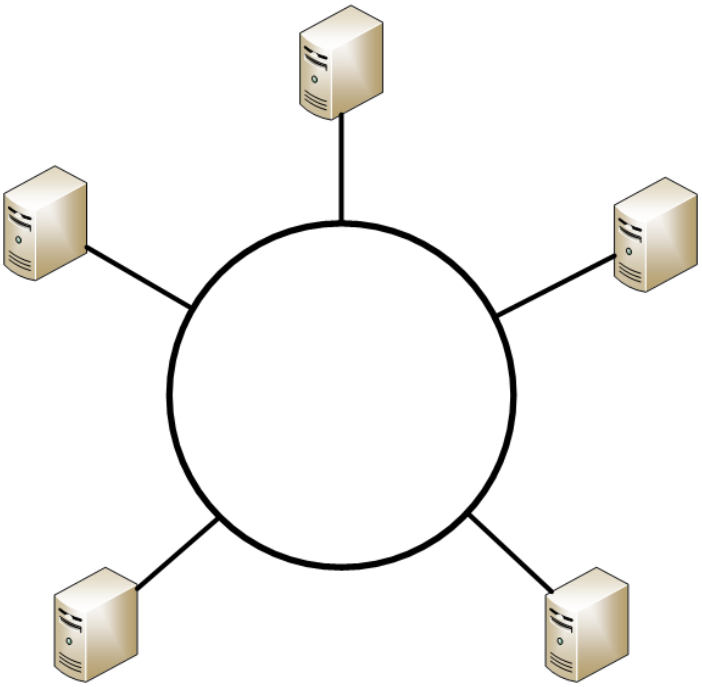
Verkon topologioita on hyvin paljon erilaisia ja käytettävä topologia riippuu paljon fyysisestä kaapeloinnista. Topologialla tarkoitetaan sitä, miten verkon laitteet ja eri osat ovat yhdistetty toisiinsa.

Tähtitopologiassa verkon päätelaitteet liitetään tähden keskipisteessä olevaan verkkolaitteeseen (Kuva 2). Tämä on yleisin fyysinen topologia lähiverkoissa. (Hakala, Vainio 2005, 69.)



Kuva 2. Tähti.

Rengastopologiassa laitteet on liitetty toisiinsa ja tieto kulkee vuoron perään jokaisen laitteen läpi, kunnes se saavuttaa määränpäänsä (Kuva 3) (Hakala, Vainio 2005, 69). Tämä on vanhentunut tapa tehdä verkkoja tehottomuutensa ansiosta. Kaikkien laitteiden, jotka ovat lähettäjän ja vastaanottajan välissä, pitää tehdä kolme asiaa: Katsoa kuuluuko viesti juuri tälle laitteelle ja jos ei kuulu, paketoida data uudelleen ja lähettää viesti edelleen seuraavalle laitteelle. Ylimääräinen viestin käsittely johtaa viiveeseen ja koko verkon kapasiteetti riippuu yksittäisen laitteen suorituskyvystä.



Kuva 3. Rengas.

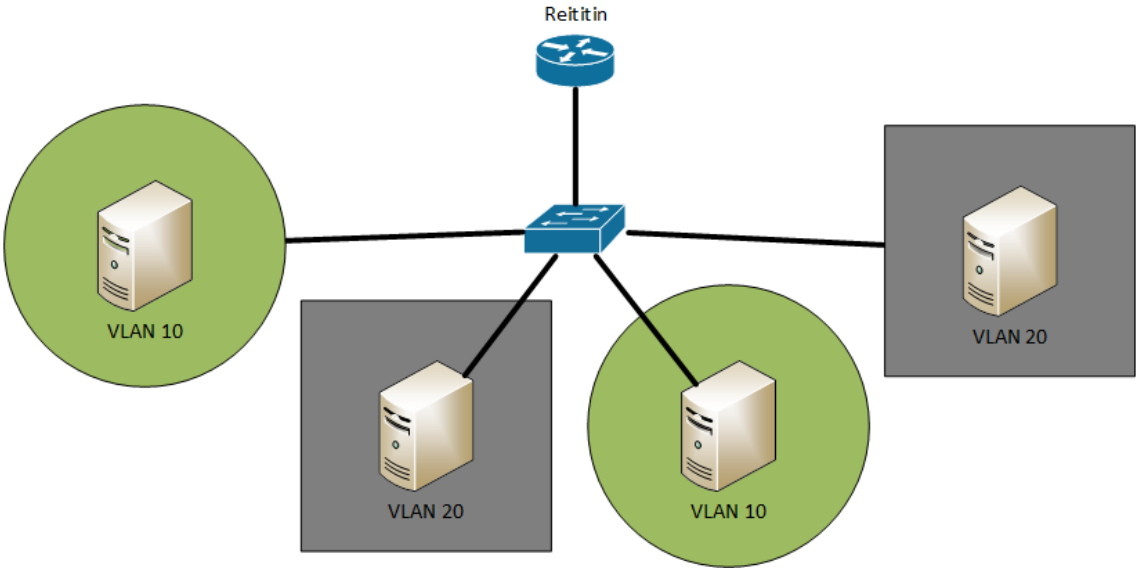
3 LAITTEIDEN OMINAISUUDET

Nykyisin verkon aktiivilaitteissa on paljon ominaisuuksia, joilla voidaan parantaa verkon suorituskykyä ja turvallisuutta. Näissä kappaleissa käydään läpi tekniikoita, jotka varmasti tulevat toimeksiantajan käyttöön. Kyseessä ei ole lopullinen lista kaikista laitteiden ominaisuuksista.

3.1 Virtuaaliset lähiverkot

VLAN (Virtual Local Area Network) tarkoittaa virtuaalista lähiverkkoa. Yksi fyysinen lähiverkko voidaan jakaa moneen virtuaaliseen lähiverkkoon. Päätelaitteet voidaan siis kytkeä samaan fyysiseen verkkoon, mutta erottaa toisistaan VLAN-verkkojen avulla. Eri VLAN-verkoille voidaan määrittää, mitä liikennettä tietyssä VLAN-verkossa sallitaan ja mitä kielletään. (IEEE 802.1Q-2005, 2.) Tällä voidaan parantaa tietoturvaa merkittävästi, jos esimerkiksi koulussa oppilaat ja opettajat halutaan eri verkkoihin. Tällöin oppilaiden liikennettä voidaan tarkastella omana kategorianaan ja opettajien liikennettä omanaan. Päätelaitteet sijaitsevat kuitenkin fyysisesti samassa verkossa. Samalla mahdollistetaan palomuuraus verkkojen välille. Palomuuriin voidaan siis määrittää erikseen, mitä resursseja opettajat saavat käyttää ja mitä resursseja oppilaat saavat käyttää.

Kuvan 4 tilanteessa siis kaikki neljä laitetta ovat yhdistetty samaan fyysiseen verkkoon, mutta laitteet on eroteltu kahteen eri VLAN-verkkoon. Laitteet, jotka ovat VLAN 20:ssä, eivät pysty keskustelemaan laitteiden kanssa, jotka ovat VLAN 10:ssä, ellei sitä erikseen määritetä kuvassa olevalle reitittimelle. Samassa VLAN-verkossa olevat laitteet pystyvät viestimään keskenään.



Kuva 4. VLAN-havainnekuva

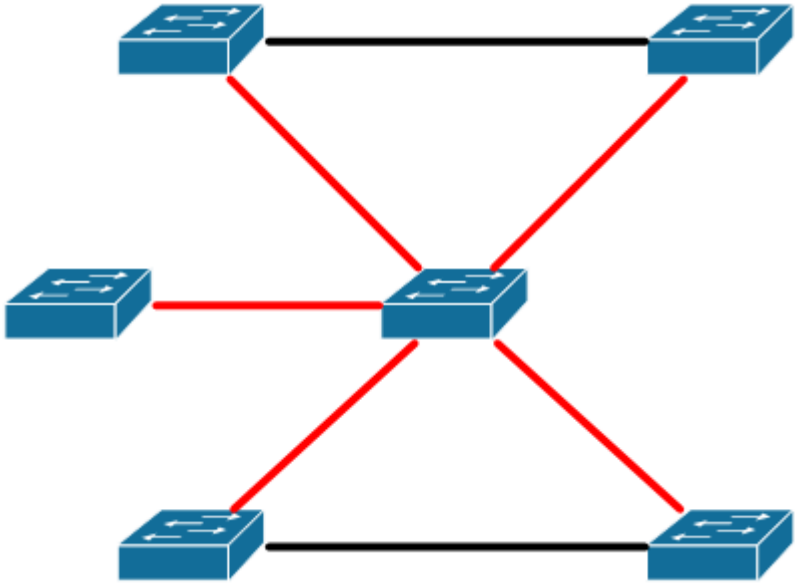
VLAN-verkot voidaan määrittää kytkimeen monella eri tavalla. Yleisin tapa on käyttää porttiperusteista VLAN-jakoa, jolloin esimerkiksi kytkimen portti numero yksi liitetään tiettyyn VLAN-verkkoon. Tällöin työasema, joka on kytketty porttiin numero yksi, kuuluu tiettyyn VLAN-verkkoon. Jos joku muu työasema tai päätelaite kytketään samaan porttiin, portin VLAN määritys pysyy samana.

VLAN voidaan määrittää myös MAC-osoitteeseen perustuen tai Policy-perusteisesti. MAC-osoitteeseen perustuvassa VLAN-määrityksessä VLAN-verkko määräytyy työaseman MAC-osoitteen eli laitteen verkkokorttiin asetetun osoitteen mukaan. Tämä mahdollistaa työasemien linkittämisen tiettyyn VLAN-verkkoon riippumatta siitä, mihin kytkimen porttiin työasema on kytketty. Kytkin siis tunnistaa työaseman MAC-osoitteen ja vaihtaa kytkimen portin automaattisesti MAC-osoitteelle asetettuun VLAN-verkkoon.

Policy-perusteisessa VLAN määrityksessä voidaan käyttää esimerkiksi laitteen loogista tai fyysistä osoitetta tai laitteen käyttämiä protokollatyyppejä . (Hakala, Vainio 2005, 99).

3.2 Virityspuualgoritmi

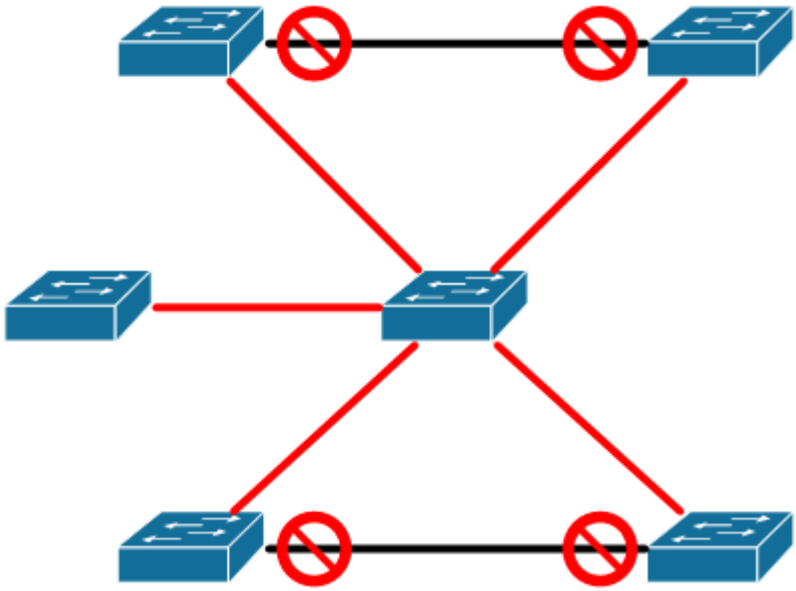
Spanning Tree Protocol (STP) eli virityspuualgoritmi on 2. kerroksen varayhteysmenetelmä. Se mahdollistaa varayhteyksien luomisen kytkinten välille ilman, että syntyy verkon silmukoita. Ilman STP:tä tai manuaalista porttien sulkemista kytkimiä ei ole mahdollista kytkeä toisiinsa niin, että kytkinten välillä on varayhteys (Kuva 5).



Kuva 5. Spanning Tree on pois päältä joten silmukat ovat mahdollisia.

Kuvassa 5 ylemmät ja alemmat kytkimet ovat kiinni toisissaan sekä tähden keskellä olevassa kytkimessä. Jos verkkoon lähetetään broadcast-viesti se jää verkkoon kiertämään loputtomasti kasvaen, jolloin broadcast-viestit vievät kaiken kapasiteetin verkolta estäen normaalin liikenteen. Broadcast-viestit ovat viestejä, jotka tavoittavat koko verkon. Kun kytkin saa tällaisen viestin, kytkin lähettää viestin edelleen ulos jokaisesta portista, paitsi siitä portista, josta viesti tuli.

STP rakentaa kytkimiin puumaisen hierarkian, jolla kuvataan verkon topologiaa. Tämä tehdään mainosviesteillä, joita lähetetään kytkimeltä toiselle. Tällöin kytkimet tietävät, mikä linkki johtaa mihinkin kytkimeen. Kun hierarkia on rakennettu, voivat kytkimet päättää mikä linkki suljetaan, jotta silmukoita ei pääse syntymään. STP pystyy myös dynaamisesti muuttamaan viestien lähetysreittiä, jos verkon topologia muuttuu. Tämä mahdollistaa sen, että verkko voi korjaantua itsestään, jos jokin aktiivisista linkeistä poistuu, joko kytkimen tai linkin hajoamisen takia.



Kuva 6. Spanning Tree on päällä, joten silmukoiden syntyminen on estetty.

Kuvassa 6 tilanne on kuvattuna kun STP on rakentanut hierarkian ja sulkenut tarpeettomat linkit. Tässä tilanteessa voidaan esimerkiksi menettää jompikumpi ylemmistä punaisista linkeistä ja verkko korjaantuu itsestään 30–90 sekunnin kuluttua. Kytkimet lähettävät toisilleen mainosviestejä, joilla varmistetaan, että viereinen kytkin ja sen portti on päällä. Jos kytkin ei vastaa oletetaan, että topologia on muuttunut ja varayhteys otetaan käyttöön.

STP:n normaalia toimintaa ja nopeutta voidaan säätää virityspuuhallinta-alueella. STP:hen liittyy muutama parametri, jotka kuvaan seuraavaksi.

Kytkimen prioriteetti on parametri, jolla määrätään juurisillan prioriteetti. Jos tätä ei aseteta käsin, käytetään kytkimen MAC-osoitetta. Laitteesta, jolla on pienin MAC-osoitteen arvo, tulee juurisilta. Juurisillan tarkoitus on olla virityspuun ydin, johon kaikki muut verkkolaitteet yrittävät yhdistää mahdollisimman edullista reittiä pisin. Kytkimen prioriteetti kannattaa ainakin halutussa juurisillassa määrittää käsin, koska muuten juurisilta määräytyy MAC-osoitteen mukaan ja se voi aiheuttaa epäedullisen tai epäloogisen STP-topologian.

Edullisin reitti on parametri, joka määrittää kuinka edullisesti kytkin pääsee juurisillalle. Esimerkiksi kuvassa 6 voidaan ajatella tähden keskimmäisen kytkimen olevan juurisilta. Ylimmät kytkimet ovat suoraan kiinni tässä kytkimessä, jolloin edullisin reitti on suoraan punaista linkkiä pisin. Linkin edullisuus lasketaan kollektiivisesti kaikista linkeistä, jotka

ovat matkan varrella. Tähän vaikuttaa etäisyys sekä nopeus. Esimerkiksi voidaan ajatella, että vasen ylempi punainen linkki olisi vain 10 megabittiä per sekunti (Mbps) nopeudeltaan. Oikea punainen linkki on 1000 Mbps ja ylemmät kytkimet yhdistävä musta linkki on myös 1000 Mbps. Tällaisessa tilanteessa edullisin reitti vasemmalta ylemmältä kytkimeltä tähden keskelle olisi oikean ylemmän kytkimen kautta, koska vaikka kytkimellä on suora yhteys juurisiltaan (yksi linkki), se on niin hidas, että on edullisempaa kiertää kahden linkin kautta koska ne ovat niin paljon nopeampia. Eli edullisimman reitin valintaan vaikuttaa sekä hyppyjen määrä että linkkien nopeus.

Välitysviive on aika, jonka kytkin käyttää STP-viestien kuunteluun. Tässä tilassa kytkin kuuntelee juurisillalta tulevia Bridge Protocol Data Unit (BPDU) -viestejä. Kaikki muut viestit hylätään. Välitysviive otetaan käyttöön kun verkon topologia muuttuu, jotta kytkimet voivat oppia uuden topologian ja reitit ilman, että oppimisen aikana aiheutuu broadcast-viesteistä johtuvaa verkon tukkeutumista.

Mainosviestien lähetysväli on aika, jonka välein kytkimet lähettävät toisilleen hello-viestejä. Näillä viesteillä päätetään onko linkki aktiivinen vai ei. Niin kauan kuin linkki pysyy aktiivisena, hierarkiaan ei tule muutoksia ja STP pysyy muuttumattomana. Jos viereinen kytkin ei vastaa, aloitetaan hierarkian muutos. Viestejä lähetetään yleensä 1–3 sekunnin välein. Aika voi olla suurempi, mutta se suurentaa vikatilanteesta palautumiseen kuluvaa aikaa. (Jaakohuhta 2002, 183-186.)

4 KYTKINTEN HALLINTA

Verkon hallinta voidaan jakaa viiteen painopisteeseen. Painopisteet ovat vikojenhallinta, kokoonpanon hallinta, tilastoinnin hallinta, suorituskyvyn hallinta ja tietoturvan hallinta (Jaakohuhta 2002, 309-311). Hallinnan jakaminen eri painopisteisiin mahdollistaa priorisoinnin ja helpottaa kokonaisuuden hallintaa.

4.1 Vikojenhallinta

Vikojenhallinta sisältää vikojen havaitsemisen, eristämisen ja korjaamisen. Havaitseminen voidaan toteuttaa laitteelle lähetettävillä kyselyillä (polling) ja laitteen lähettämillä viesteillä (trapping). Laitteelle lähetettävä kysely voi olla esimerkiksi ping, joka mittaa vasteaikaa lähettävältä laitteelta vastaanottavalle laitteelle tai jokin tarkempi kysely esimerkiksi laitteen päälläoloajasta. Jos laite vastaa kyselyyn sen voidaan olettaa olevan päällä ja toiminnassa. (Jaakohuhta 2002, 309; Dooley 2002, 281). Kyselyitä käytetään yleensä vain laitteen päälläolon todentamiseen.

Trap-viesteillä voidaan toteuttaa tarkempaa vikojen havainnointia. Verkon laitteelle voidaan määrittää minkälaisista muutoksista lähetetään trap-viesti. Viesti voidaan lähettää esimerkiksi, jos kytkimen linkki menee pois päältä, kun se on aikaisemmin ollut päällä. Trap-viesti lähetetään, kun muutos tapahtuu. Jos verkko on toimiva ja muuttumaton, trap-viestejä ei lähetetä. Tästä syystä havainnointia täytyy tehdä molempiin suuntiin, jotta voidaan varmistua verkon toimivuudesta. Jos verkkolaitteilta ei tule ollenkaan trap-viestejä ei silti voida olettaa, että verkkolaitteet ovat toiminnassa. Trap-viestit käyttävät normaaleja verkon siirtoteitä, joten jos siirtotiet häiriöityvät eivät myöskään trap-viestit pääse perille. Laitteita pitää siis myös kysellä, jotta tiedetään varmasti, että verkko on toiminnassa.

Kun vika havaitaan voidaan siirtyä vian eristämiseen ja korjaamiseen. Eristäminen tarkoittaa vian etsimistä poissulkemalla mahdollisia vian aiheuttajia. Mahdollisimman tarkalla havainnoinnilla voidaan vian etsintää helpottaa ja nopeuttaa, mikä edelleen nopeuttaa vian korjaamista. Näin viat saadaan selvitettyä nopeasti ja tehokkaasti ja verkko voidaan palauttaa normaalille toiminnan tasolle.

4.2 Kokoonpanon hallinta

Kokoonpanon hallinta voidaan jakaa fyysiseen ja loogiseen osaan. Fyysinen osa sisältää laitteiden tyypit, sarjanumerot, sijainnin ja muut laitteeseen liittyvät tiedot. Näillä tiedoilla voidaan selvittää esimerkiksi laitteen elinikä ja takuun tilanne. Loogisilla tiedoilla tarkoitetaan laitteeseen asetettua konfiguraatiota. Kokoonpanon hallinnan loogiseen osaan kuuluu myös konfiguraatioiden muutokset, varmuuskopiointi ja palautus. (Dooley 2002, 273.)

Fyysiset tiedot voidaan ottaa kerralla talteen ja säilyttää esimerkiksi taulukossa, joka on helposti saatavilla verkkoa hallinnoivalle henkilöstölle. Näitä tietoja täytyy pitää yllä, jotta verkon laitteista on ajantasaista tietoa ja voidaan suunnitella esimerkiksi laitteiden uusiminen, kun laitteet väistämättä ikääntyvät.

Loogiset tiedot on hyvä pitää ajan tasalla ottamalla niistä varmuuskopio esimerkiksi joka yö tai viikon välein. Tällä mahdollistetaan se, että jos laite vikaantuu, voidaan se vaihtaa helposti uuteen samanlaiseen laitteeseen ajamalla vain edellinen konfiguraatio sisään uuteen laitteeseen. Tällöin vaihtoprosessi on helppo ja sen voi tehdä ilman syvempää tietoa verkon toiminnasta. Vikaantuneen laitteen vaihdosta tulee merkittävästi hankalampaa jos se pitää konfiguroida alusta asti samanlaiseksi kuin aikaisempi laite oli. (Dooley 2002, 273–274.)

4.3 Tilastoinnin hallinta

Tilastoinnin hallinnalla tarkastellaan, kuka käyttää verkon resursseja ja kuinka paljon. Tämä mahdollistaa laskutuksen ja tietoturvan hallinnan. Tilastoinnin hallintaan liittyy myös verkon käytön tarkastelu jokaisen käyttäjän tai käyttäjäryhmän perusteella.

4.4 Suorituskyvyn hallinta

Suorituskyvyn hallinnalla etsitään mahdollisia verkon pullonkauloja. Voidaan siis löytää verkon pullonkauloja, joihin liikenne hidastuu. Pullonkauloja etsimällä ja korjaamalla koko verkon suorituskykyä voidaan parantaa.

Verkkoa voisi ajatella suorituskyvyn kannalta monena pienenä jokena, jotka johtavat yhteen suurempaan jokeen. Joet ovat tässä tapauksessa yksittäisiä siirtoteitä. Jos yksittäiset joet virtaavat liian kovaa, eikä suurempi joki pysty virtaamaan riittävän nopeasti, aiheutuu siitä tulva ensin alajuoksulle ja myöhemmin yläjuoksulle, kun vedellä ei ole enää riittävän nopeaa reittiä mereen. Suorituskyvyn hallinta siis johtaa kapasiteettisuunnitteluun (Dooley 2002, 275).

4.5 Tietoturvan hallinta

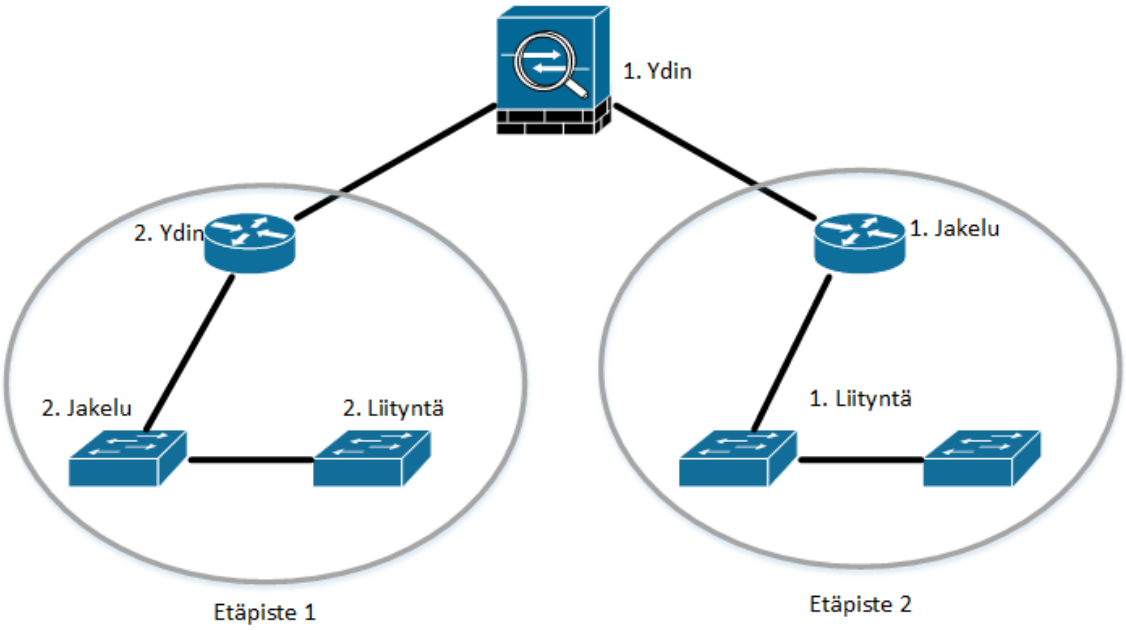
Tietoturvan hallinta tarkoittaa verkon tietoturvakeinojen tarkastelua (Dooley 2002, 275). Itse säännöt kuuluvat joko yrityksen tietoturvapolitiikkaan tai kokoonpanon hallintaan. Tietoturvan hallinnalla siis varmistetaan, että määrättyjä sääntöjä noudatetaan ja rikkomukset kirjataan ylös (Jaakohuhta 2002, 310). Kun esimerkiksi palomuurin säännöstöä parannetaan rikkomuksen johdosta, se kuuluu kokoonpanon hallintaan.

5 TAPAUS LIEDON KUNTA

5.1 Verkkosuunnittelu ja hierarkia

Verkkosuunnittelun kannalta täytyy ottaa huomioon, että kunnan toimipisteillä on aina reititin, jonka kautta toimipiste saa yhteyden tarvittaviin palvelimiin ja internetiin. Lähiverkon suunnittelussa tämä tarkoittaa sitä, että kunnalla ei ole suuria lähiverkkoja, vaan sarja kohtalaisen pieniä lähiverkkoja. Tällöin ei tarvitse käyttää merkittävästi aikaa esimerkiksi Spanning Tree-suunnittelussa, kun ydinkytkin on aina vain muutaman hypyn päässä ja verkon silmukat on helppo havaita.

Kun ajatellaan kunnan verkkoa hierarkkisen verkkosuunnittelun näkökulmasta, huomataan pian, että topologiat riippuvat paljon siitä, miten verkkoa kuvataan. Verkon hierarkia muuttuu merkittävästi, jos kuvataan vain toisen tason (Layer 2) kytkimiä tai jos mukaan otetaan kolmannen tason (Layer 3) reitittimet ja palomuurit.



Kuva 7. Kaksi tapaa kuvata hierarkiaa.

Kuvassa 7 voitaisiin ajatella palomuurin olevan ydinreititin, etäpisteiden reitittimien olevan jakelukerrosta ja kytkimet liityntäkerrosta. Toisaalta asia voidaan kuvata niin, että etäpisteen reititin on ydin, johon tulee kiinni jakelukerroksen kytkin ja siinä kiinni olevat kytkimet ovat liityntäkerroksen kytkimiä.

5.2 Laitteiden ominaisuudet

Liedon kunnan koko verkko on järjestetty nyt niin, että suurta osaa kytkimillä olevista ominaisuuksista ei tarvitse hyödyntää. Tämä yksinkertaistaa konfiguraatiota merkittävästi ja helpottaa hallintaan. Samalla verkossa on vähemmän muuttujia, jotka voivat aiheuttaa vikoja.

Lähiverkoissa ei tarvitse suodattaa liikennettä, koska liikenne ohjataan palomuurille. Tämä johtaa siihen, että esimerkiksi tietoturvaominaisuuksia ei tarvitse suuremmin huomioida kytkinten tasolla. Näin annetaan siis laitteiden tehdä sitä, mitä ne tekevät parhaiten eli kytkimet lähettävät viestejä eteenpäin ja palomuurille jätetään liikenteen suodatus.

Kun ominaisuuksia jätetään nyt käyttämättä, voidaan niitä ottaa myöhemmin käyttöön, jos niille tulee tarve. Verkkojen jatkuvasti muuttuvat vaatimukset on siis huomioitava niin, että laitteet eivät tule riittämättömiksi ominaisuuksien tai kapasiteetin puolesta lähitulevaisuudessa. Jatkossa voidaan tutkia, mitä ominaisuuksia voitaisiin ottaa käyttöön ja tehdä ominaisuuksien osalta oma suunnitelma ja käyttöönotto.

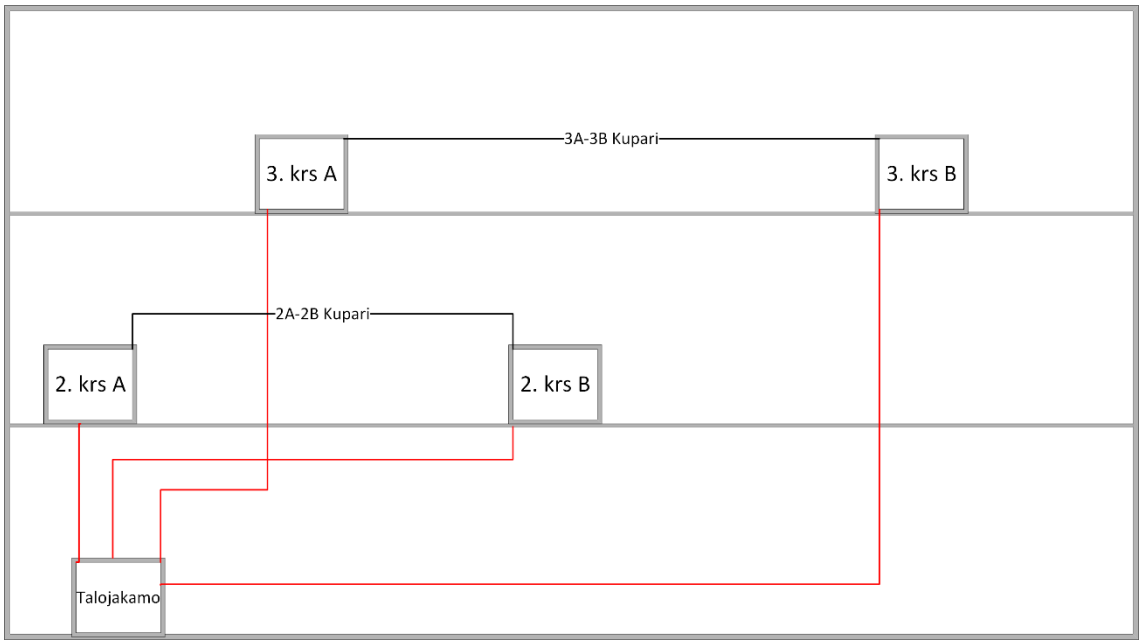
5.2.1 Virtuaalilähiverkot

Liedon kunnalla verkot on jaettu virtuaalilähiverkkoihin. Eri verkoilla luodaan selkeät rajat eri käyttäjätyyppien mukaisesti. Käyttäjät jaetaan pääosin työntekijöihin, oppilaisiin sekä vierailijoihin. Näiden lisäksi uutena verkkona tulee laitteiden hallintaan tarkoitettu verkko. Kaikilla ryhmillä on omat säännöstöt siitä, miten käyttäjän päätelaite päästetään verkkoon ja mihin palveluihin päätelaitteet päästetään. Työntekijöillä on eniten vapauksia koska he tarvitsevat eniten sisäisiä palveluita. Vierailijoilla on vähiten vapauksia koska heidän ei tarvitse päästä kunnan sisäisiin palveluihin.

Laitteiden hallintaan tarkoitettu verkko pitää luoda, koska sellaista ei aikaisemmin ole ollut käytössä. Tämä johtuu siitä, että laitteiden hallinta on tapahtunut palveluntarjoajan toimesta ja kunnan työntekijöillä ei ole ollut käytössä tällaista verkkoa.

5.2.2 Virityspuualgoritmi ja esimerkki topologiasta

Virityspuualgoritmi tulee käyttöön esimerkiksi Liedon kunnantalolla. Kunnantalo on kaapeloitu siten, että fyysiset kaapelit muodostavat tähtitopologian. Tämän lisäksi 2. ja 3. kerroksiin on tehty lisäkaapelointi kerroksen sisällä. Tämä mahdollistaa varalinkin kytkemisen jos jokin punaisista nousukaapeleista katkeaa (Kuva 8).



Kuva 8. Kunnantalon fyysinen kaapelointi.

Kuvan 8 tilanteessa syntyy silmukka jos kaikki kaapelit kytketään ja virityspuualgoritmia ei käytetä. Tästä syystä kunnantalolla otetaan käyttöön virityspuualgoritmi.

5.3 Kytkinten hallinta

Kytkinten hallinta voidaan toteuttaa monella eri tavalla. Tähän voidaan käyttää erilaisia sovelluksia ja protokollia, jotka helpottavat hallintaa ja antavat kokonaiskuvan verkosta sekä yksityiskohtaisen konfiguraatiolistauksen tietystä kytkimestä. Toisaalta kytkinten hallinta voidaan yksinkertaistaa telnet- tai selainpohjaiseen hallintaan. Pelkästään näiden käyttö ei anna hyvää kuvaa verkossa liikkuvasta datasta, vaan mahdollistaa vain yksittäisen kytkimen hallinnan. Verkkohallinnan ohjelmistoja käyttämällä mahdollistetaan kytkinten massahallinta, jolloin samoja konfiguraatioita voidaan ajaa moneen kytkimeen samaan aikaan.

5.3.1 Ei hallintaohjelmaa

Tässä tilanteessa kytkimiä konfiguroidaan yksitellen ja mahdolliset vikatilanteet tulevat asiakkaalta. Asiakas siis soittaa IT-tukeen tai lähettää sähköpostia, jonka jälkeen asiaa voidaan alkaa tutkia. Kyseessä on siis passiivinen menetelmä, jossa kytkimiä ei sinänsä valvota erikseen. Tällä mallilla menetetään paljon muutoksenhallinnan ominaisuuksia, joita verkonhallinnan ohjelmistoissa yleensä on. Malliin voidaan lisätä myös hieman aktiivisuutta siten, että laitetta kysellään esimerkiksi ping-komennolla. Tällöin näkyisi selvästi, jos kytkin ei enää vastaa.

Tämä voitaisiin tehdä esimerkiksi niin, että kirjoitetaan jokin komentosarja, joka kyselee kytkimiä jatkuvasti ja ilmoittaa vastuuhenkilölle kun kysely epäonnistuu. Jos tähän voitaisiin liittää sähköposti tai tekstiviesti toiminto, ilmoitus menisi heti perille kun kysely epäonnistuisi. Tällöin vastuuhenkilön ei tarvitse tarkastella komentosarjan suoritusta jatkuvasti, vaan vastuuhenkilö voi tehdä muita töitä ja aktivoitua vasta sitten kun ilmoitus tulee hänelle.

Tämän toteutuksen vahvuutena on se, että hallintaohjelmaan ei tarvitse varata rahaa. Mahdollinen komentosarja voidaan tehdä jollekin olemassa olevalle palvelimelle. Hallintaohjelman opettelemiseen ja konfigurointiin ei myöskään tarvitse käyttää aikaa.

5.3.2 Hallintaohjelma

Hallintaohjelman kanssa saadaan paras näkyvyys verkkoon ja mahdollistetaan kytkinten massahallinta. Massahallinta voi tulla tarpeen, kun kytkimiä vaihdetaan toimipisteillä tai verkkoon täytyy tehdä jokin suuri muutos. Esimerkki tästä voisi olla uuden VLANin tekeminen jokaiseen toimipisteeseen. Jos tällainen tarve tulee, komennot voidaan ajaa kerran hallintaohjelmalla ja ne monistuvat jokaiseen kytkimeen. Jos hallintaohjelmaa ei ole, jokainen kytkin pitää konfiguroida erikseen, jolloin työhön menee aikaa moninkertaisesti verrattuna massahallintaan.

Hallintaohjelmalla saadaan myös hyvä näkyvyys verkkoon. Suurin osa hallintaohjelmistoista tukee karttojen ja rakennusten piirustusten tuontia, jolloin kuvista voidaan nähdä selkeästi missä laite sijaitsee. Tämä helpottaa vianetsintää kun fyysinen topologia on selkeästi esillä.

Ohjelmat tukevat myös sähköpostin tai tekstiviestin lähettämistä suoraan, jolloin vikatilanteista saadaan välitön ilmoitus.

5.4 Käyttöönotto

Ennen suuria muutoksia tehdään suunnittelun jälkeen Proof of Concept (PoC). Suunniteltu toteutus siis testataan tuotannossa pienessä mittakaavassa. Verkkouudistuksen kannalta sen voi toteuttaa esimerkiksi hankkimalla yksi uusi kytkin, johon laitetaan halutut asetukset ja sen jälkeen sitä testataan. Tällä ajanjaksolla laitetta tarkastellaan normaalia useammin, jotta mahdolliset viat löytyisivät jo pienessä mittakaavassa. Kun PoC tehdään ensin, voidaan uusia laitteita testata kunnolla ja jos ne eivät toimi halutulla tavalla, voidaan siirtyä vielä takaisin edelliseen tilanteeseen kohtalaisen helposti.

PoC-vaiheita voi olla myös useampia. Ensin voidaan tehdä yhden laitteen testausta ja sen jälkeen useamman laitteen testausta. Kunnan tapauksessa uusien laitteiden testaaminen toteutetaan siten, että ensin hankitaan yksi kytkin, joka tulee kunnantalolle. Kytkin on siis fyysisesti lähellä, jolloin siihen päästään helposti käsiksi ja se voidaan nopeasti vaihtaa pois, jos se ei toimi halutulla tavalla.

Tässä vaiheessa alkuperäiseen palautuminen on vaikeampaa, mutta vielä melko helppoa. PoC:llä siis minimoidaan riskejä kun päästään testaamaan uudistusta kunnolla ennen lopullista toteutusta.

Kun suurempi PoC-skenaario on käyty huolella läpi, voidaan sen jälkeen alkaa tekemään verkkomuutosta toimipiste kerrallaan.

6 POHDINTA

Lähiverkon uudistaminen on suuri kokonaisuus ja tässä työssä ei käyty läpi kaikkia mahdollisia vaihtoehtoja. Työssä kuitenkin käytiin läpi toimeksiantajan kannalta olennaisimmat asiat ja tavoitteet. Lähiverkon laitteita ei suuremmin vertailtu, koska päätös tiettyjen laitteiden hankinnasta tuli toimeksiantajalta. Ominaisuudet, jotka käytiin läpi tässä työssä, ovat kuitenkin saatavilla suurimmilta laitevalmistajilta kuten Cisco, Hewlett Packard Enterprise ja Juniper.

Tavoitteena oli käydä läpi toimeksiantajan nykyinen verkko ja suunnitella sen uudistaminen ja laitteiden tuominen omaan hallintaan. Toimeksiantajan nykyisistä verkoista on kirjoittajalla nyt erittäin hyvä käsitys, vaikka tarkempia ominaisuuksia ja topologioita ei tässä työssä käytykään läpi. Tämä helpottaa uusien lähiverkkojen toteuttamista, kun nykyinen toteutus on tiedossa. Tulevaisuudessa voidaan myös vertailla nykyistä ja tulevaa toteutusta keskenään, kun uudistus on saatu tehtyä. Uudistuksen onnistuminen selviää käytännössä vasta sen tekemisen jälkeen. Tässä työssä oli tarkoitus suunnitella ja käydä läpi lähiverkkojen teoriaa, jotta käytännön tekeminen olisi mahdollista. Kun alkuperäinen toteutus on hyvin kartoitettu, voidaan sitä helposti verrata uuteen toteutukseen ja arvioida sen onnistumista.

Seuravaksi voidaan aloittaa toteuttaminen tämän opinnäytetyön pohjalta. Tämän opinnäytetyön lisäksi on tehty paljon dokumentaatiota ja suunnitelmia, miten uudistus voidaan toteuttaa käytännössä. Nämä dokumentit on tietoturvasyistä jätetty kuitenkin päättötyön ulkopuolelle, koska ne sisältävät tarkkoja konfiguraatioita uusille laitteille.

LÄHTEET

Boyles, T. & Hucaby, D. 2001. Cisco CCNP switching exam certification guide. Indianapolis (IN): Cisco Press.

Ciccarelli, P. & Faulkner, C. 2006. Networking Foundations. Alameda: John Wiley & Sons, Incorporated

Dooley, K. 2002. Designing large-scale LANs, 1. ed. edn. Beijing ; Cambridge ; Farnham ; Köln ; Paris ; Sebastopol ; Taip: O'Reilly.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyvskylä: Docendo.

IEEE 2006. IEEE Standard for Local and metropolitan area networks. New York: IEEE-SA. http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

Jaakohuhta, H. 2002. Lähiverkot : Ethernet. 3. uud. p. edn. Helsinki: Edita, IT Press.

McCabe, J. 2007. Network Analysis, Architecture, and Design. San Francisco: Elsevier Science.

McMillan, T. 2011. Cisco Networking Essentials. Hoboken: John Wiley & Sons, Incorporated.

Omni Partners 2017. PoC eli Proof of Concept. Viitattu 2.5.2017 https://omnipartners.fi/sanakirja/poc-eli-proof-of-concept/