Lähiverkon vakiointi yrityksen useaan toimipisteeseen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeenlinnan korkeakoulukeskus, Tietojenkäsittelyn koulutusohjelma

syksy, 2019

Jussi Salminen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Hämeenlinnan korkeakoulukeskus

Tekijä Jussi Salminen **Vuosi** 2019

Työn nimi Lähiverkon vakiointi yrityksen useaan toimipisteeseen

Työn ohjaaja Lasse Seppänen

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli luoda ohjeistus opinnäytetyön toimeksiantajayritykselle lähiverkon rakenteesta useammassa toimipisteessä käytettäväksi. Toimeksiantajayrityksellä on kaupan alalla yli 30 toimipaikkaa Suomessa, joiden lähiverkkoa ei ole toteutettu vakioidusti. Yrityksellä oli meneillään samassa yhteydessä verkkolaiteuudistus, jossa lähiverkon aktiivilaitteita päivitettiin nykypäivän vaatimusten mukaisiksi.

Opinnäytetyön käytännön osuudessa uudistettiin yhden myymälän verkkolaitteita ja järjestettiin laitekaappien sisältöä selkeämmäksi. Työn tulosten perusteella laaditaan suunnitelma muidenkin toimipisteiden verkkolaiteuudistuksesta. Laitekaappien ja lähiverkon vakioiminen helpotti verkko-ongelmien selvittämistä ja vähensi ongelmien selvitykseen kuluvaa aikaa. Verkon turvallisuutta lisäsi virtuaalisten lähiverkkojen käyttö ja mahdollisuus poistaa kytkinten kytkemättömät portit käytöstä. Tietohallinon puolelta voidaan tarvittaessa avata portit ja määrittää niille oikea virtuaalinen lähiverkko verkonhallintaan käytetyn ohjelmiston avulla. Lisääntynyt kameravalvonta on luonut haasteita vanhemmissa myymälöissä verkon aktiivilaitteiden iän vuoksi.

Toimiva lähiverkko ja ongelmatilanteiden pikainen ratkaisu vähentää myynnin keskeytyksiä ja lisää tuottavuutta niin tietohallinnon puolella, kuin itse myymälöissä. Paikallinen IT-tuki hoitaa oman työnsä ohella tietotekniikkaan liittyviä asioita. Mikäli verkko-ongelmat voidaan selvittää lyhyemmässä ajassa jää aikaa enemmän asiakaspalveluun, toimistotyöhön ja muihin myymälän toimintoihin.

Avainsanat Lähiverkko, dokumentointi, verkonhallinta

Sivut 37 sivua, joista liitteitä 2 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Hämeenlinna University Centre

Author Jussi Salminen **Year** 2019

Subject Standardization of local area network for multiple branches

Supervisor Lasse Seppänen

ABSTRACT

The purpose of this thesis was to create guidelines for the thesis commissioning company on the structure of the local area network (LAN) for use in multiple branches. The company has over 30 branches in Finland whose local area networks are not standardized. Also, the company had ongoing reform for network devices.

In the practical part of the thesis the network equipment of one store was renewed and the contents of the cabinets were clarified. Based on the results of the work, a plan for upgrading the network equipment of other offices will be prepared.

Standardization of the cabinets and the local area networks reduced used time for solving the network problems and helped finding of the problem faster. Using virtual local area network (VLAN) made network more secure. Information management of the company can administer the ports of the switches via network management software. Increased camera monitoring has put more demands on older switches.

Working LAN and speeded up resolving of the network problems reduces interruptions in sales, makes the company's information management and other functions in branches more effective. Local IT-support acts on the side, so they have more time for normal work if problems are resolved faster than before.

Keywords Local area network, documentation, network management

Pages 37 pages including appendices 2 pages

SISÄLLYS

KÄSITELUETTELO

DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteet lähiverkon laitteille.
GVRP-protokolla	Generic VLAN Registeration Protocol, verkkoprotokolla, jonka avulla lähiverkkoon kytkeytyvät laitteet voivat pyytää kytkimeltä liittymistä oikeaan virtuaaliseen lähiverkkoon.
IETF	Internet Engineering Task Force, organisaatio, joka vastaa internet-protokollien hallinnasta.
Intranet	Tietyn ryhmän, esimerkiksi yrityksen, käyttöön rajattu lähiverkko. Sitä käytetään tavallisesti yrityksen sisäiseen viestintään.
IPX	Internetwork Packet Exchange on TCP/IP-protokollalla korvattu protokolla, joka toimii OSI-viitemallin kuljetuskerroksella.
Jakamo	Kuuluu yleiskaapeloinnin osiin, joista verkko jaetaan eteenpäin. Esimerkiksi talojakamosta jaetaan nousukaapeloinnin avulla verkko kerrosjakamoihin ja siitä eteenpäin kerroskaapeloinnilla kytkentärasioihin.
Komentokehote	Command Promt, Windows-käyttöjärjestelmän tekstipohjainen ohjelma, jolla voidaan antaa käyttöjärjestelmälle käskyjä.
MIB	Management Information Base, SNMP-protokollan käyttämä hallintatietokanta.
Microsoft Visio	Microsoftin kehittämä piirustusohjelma, jolla voidaan piirtää kaavioita, kuvia tai pohjapiirroksia.
NetBIOS	Network Basic Input/Output System, verkkoprotokolla, joka toimii OSI-viitemallin kuljetuskerroksessa laitteiden nimien perusteella. Se ei tue IPv6-standardia ja nimet voivat olla vain 16 merkkiä pitkiä.
Ping	Packet Internet Groper, komentokehotteessa käytetty työkalu, joka lähettää echo request -paketin, johon kohteena oleva laite vastaa omalla echo reply -paketilla.
RFC	Request For Comments, asiakirjajoukko, joka kuvaa internetin erilaisia käytäntöjä ja protokollia. Tätä asiakirjajoukkoa ylläpitää IETF-organisaatio.

Ristikytkentä	Ristikytkennällä tässä opinnäytetyössä tarkoitetaan kytkimien kytkemistä kerroskaapelointiin jakamossa. Ristikytkentäpaneelista voidaan selvittää sähköpiirustusten avulla mihin kytkentärasiaan kytkimen portti kytkeytyy.
SMI	Structure and Indetification of Management, määrittelee MIB:n rakenteen.
SFP+	Small Form-factor Pluggable transceiver, 10Gb liitäntä moduuli, jonka avulla kytkin voidaan liittää esimerkiksi valokaapeliyhteydellä toiseen laitteeseen.
Webropol	Sähköinen kyselyjärjestelmä, jolla voi luoda sähköisiä kyselyitä ja niiden tuottamaa dataa voidaan analysoida tilastollisesti ja laadullisesti.
Yleiskaapelointi	Standardoitu kiinteistön peruskaapelointi tietoliikenteelle ja puhelinjärjestelmille. Se koostuu aluejakamosta, aluekaapelista, talojakamosta, nousukaapeleista, kerrosjakamoista, kerroskaapeloinnista ja kytkentärasioista.

Liitteet

Liite 1 Kysely paikallisesta lähiverkosta

1 JOHDANTO

Tietoverkoissa toimivat palvelut ovat liiketoiminnalle elintärkeitä ja tuovat usein enemmän etuja kuin haittoja. Kehittyvä teknologia ja sen tiedostavat asiakkaat haastavat yritykset vähentämään päällekkäistä työtä, nopeuttamaan toimintoja ja samalla lisäämään myyntiä.

Mikäli verkossa havaitaan ongelma, on vian nopea paikantaminen ja korjaaminen erityisen tärkeää. Pahimmassa tapauksessa verkon ongelmat voivat johtaa myynnin keskeytymiseen tai jopa koko myymälän sulkemiseen, mikäli verkko ei toimi. Vakioitu lähiverkko helpottaa ongelmatilanteiden selvittämistä ja nopeuttaa vikatilanteiden korjaamista, koska myymälän henkilökunta voi helposti IT-tuen avustuksella ilmoittaa vikaan vaikuttavan laitteen tai kytkennän.

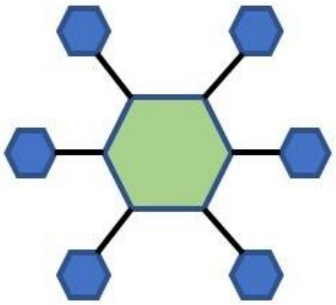
Opinnäytetyön toimeksiantajayrityksellä on Suomessa yli 30 myymälää vähittäiskaupan alalla. Myymälöissä on vaihtelevilla käytännöillä järjestetty lähiverkko. Siihen kuuluvat mm. kassat maksukorttipäätteineen, palvelutiskien työasemat, toimiston työasemat, tallentava valvontakamerajärjestelmä ja internet-yhteys kolmannen osapuolen palveluille. Lähiverkossa on käytössä erilaisia kytkimiä ja reitittimiä eikä täten laitteiston osalta ole yhteneväistä käytäntöä. Yrityksen myymälän paikallisen IT-tuen ja varsinaisen IT-tuen haasteena on IT-ongelman paikallistaminen, koska lähes jokaisella toimipisteellä on oma käytäntönsä ja erilaisten järjestelmien lisääntymisen myötä nämä on asennettu edellisen päälle ja rinnalle. Ongelman selvittelyyn menee tällä hetkellä turhaa aikaa, koska lähiverkot eivät ole vakioituja. Lähiverkon kytkimet uudistamalla ja vakioimalla laitekaappien sisällöt, onnistuu verkon etähallinta sekä paikalliselle IT-tuelle ylemmän tason tuki. Opinnäytetyön tavoitteena on luoda ohjeistus, jota voidaan käyttää muissakin toimipisteissä ja jatkossa uusien toimipisteiden avautuessa.

Työssä haetaan vastauksia seuraaviin kysymyksiin:

- Miten erikokoisiin toimipisteisiin luodaan yhtenäinen ohjeistus lähiverkosta?
- Mikä on järkevin lähiverkon hallintamalli ja mihin ”rajat” vedetään fyysisen tietoturvan kannalta?
- Miten verkon uudistus muuttaa tuottavuutta myymäläympäristössä tai tietohallinnossa?

2 LÄHIVERKKO

Lähiverkko (local area network) on maantieteellisesti rajatun alueen tietoliikenteen toteuttavaa, suuren siirtokapasiteetin omaavaa sisäistä tietoliikennettä. Verkkoa hallinnoi normaalisti yksi organisaatio. Se koostuu kaapeloinneista, kytkimistä, reitittimistä, palvelimista ja työasemista. Verkko voi olla osin tai kokonaan langaton lähiverkko, WLAN (Wireless LAN). Nykyisin lähiverkot ovat rakenteeltaan pari- tai valokaapelilla toteutettuja kuvan 1 tähtiverkkoja, jossa jokaisella laitteella on oma kaapelointinsa. Verkon tärkein aktiivilaite on kytkin. (Hakala & Vainio, 2005, s. 85; Jaakohuhta, 2005, s. 4)



Kuva 1. Tähtiverkko

2.1 Lähiverkon OSI-viitemalli

80-luvun alussa tietoliikenteessä oli tilanne, jossa eri laite- ja ohjelmistovalmistajat rakensivat omia lähiverkkoratkaisujaan, eivätkä ne olleet yhteensopivia toistensa kanssa. Jotteivät markkinat olisi valuneet pois valmistajilta, piti sopia tavoista, joilla pienennettiin vaikutuksia ympäristön muuttuessa ja kehittyessä. Nykyisin noudatetaan pääasiassa kahta eri arkkitehtuuria, OSI-viitemallia sekä TCP/IP-mallia. (Granlund, 2007, s. 6)

OSI-viitemalli on alkuaan tarkoitettu standardiksi, jonka International Standardization Organisation, ISO, hyväksyi vuonna 1983. Tämän standardin avulla valmistajien olisi mahdollista luoda kaikki laitteistot ja ohjelmistot yhteensopiviksi. Alan kilpailu johti tilanteen kuitenkin siihen, ettei sitä otettu laajamittaiseen käyttöön. OSI-viitemallia käytetään kuitenkin kuvaamaan verkon toimintaa, koska se helpottaa järjestelmien välisten toimintojen hahmottamista. Kyseessä on kerrosmalli, jossa seitsemän perustehtävää on kuvattu eri kerroksina ja helpottaa hahmottamaan näiden välisiä toimintoja. Kuvassa 2 esitetään OSI-viitemallin kerrokset. Kerroksista alimmat 1-3, joita yleisesti kutsutaan alakerroksiksi, liittyvät laitteistoon ja näiden välisiin yhteyksiin. Ylemmät kerrokset 4-7 puolestaan ohjelmistoon ja käyttäjään. Näitä kutsutaan yleisesti isäntäkerroksiksi. (Granlund, 2007, s. 7; Hakala & Vainio, 2005, s. 138)

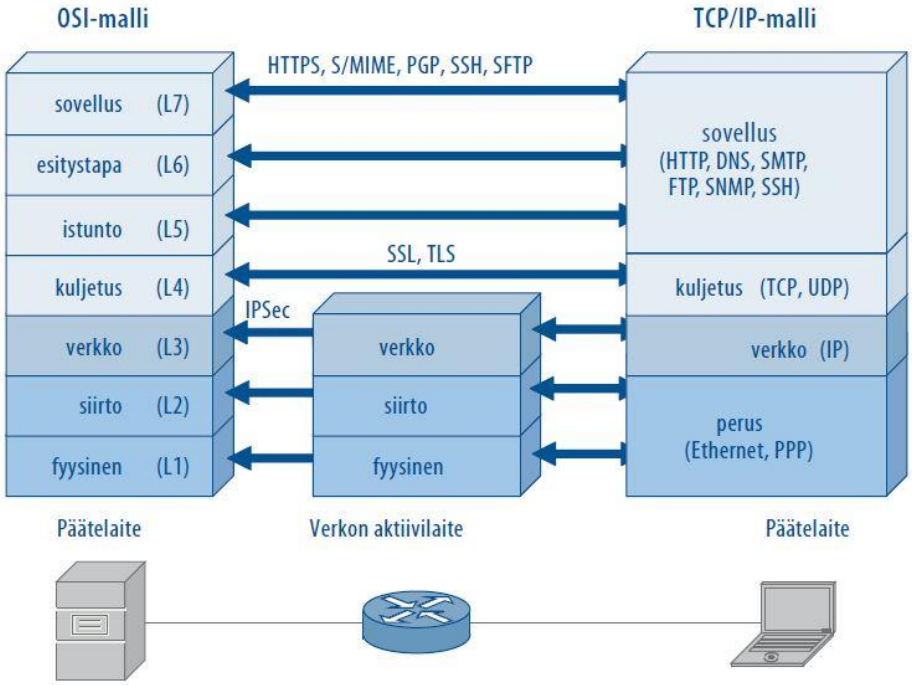
Kuva 2. OSI-viitemallin kerrokset.

Fyysinen kerros on alin alakerroksista. Fyysisessä kerroksessa määritetään siirtoyhteyttä ja sen fyysisiä arvoja. Tavallisia arvoja ovat kaapeli- ja liitintyypit, signaalien tasot, ylikuuluminen ja heijastukset. Tämän kerroksen aktiivisia verkkolaitteita ovat toistimet, keskittimet ja mediamuuntimet. Siirtoyhteyskerroksessa määritetään fyysisessä kerroksessa kulkevan datan yksiköt, kehykset ja solut. Kerroksessa määritetään myös laitteiden fyysiset osoitteet, eli MAC-osoitteet. Aktiivisia verkkolaitteita siirtoyhteyskerroksessa ovat sillat, kytkimet ja verkkokortit. Verkkokerros määrittää verkkojen välisen reitityksen sekä liikennemuotojen priorisoinnin. Lähiverkoissa tähän käytetään pääosin IP-protokollaa. Aktiivilaitteista keskeisin verkkokerroksessa on reititin. (Granlund, 2007, s. 7–11; Hakala & Vainio, 2005, s. 138–141)

Kuljetuskerros on alin isäntäkerroksista. Tässä kerroksessa kuljetuksesta huolehtii lähiverkossa TCP-, UDP-, IPX- ja NetBIOS-protokollat. Näiden protokollien avulla sovellusten lähettämä data pilkotaan pienempiin osiin, segmentteihin ja paketteihin. Kuljetuskerros muodostaa sekä purkaa yhteydet ja huolehtii kuittausmenettelyllä datan perille menosta. Istuntokerros eli yhteysjaksokerros tarkistaa käyttöoikeuksia sekä turvallisuuteen kuuluvia asioita, kuten kirjautumisia, salauksia ja lukituksia tiedostoille, kentille ja tietueille. Nykyisin käyttöjärjestelmä huolehtii istuntokerroksen toimista. Esitystapakerros määrittelee nimensä mukaisesti tietoliikenteen esitystavan laitteiden välille, esim. käyttöjärjestelmä huolehtii käytettävistä tekstikoodauksista. Sovelluskerroksessa määritetään loput toimintatavat, joita ei alemmissa kerroksissa ole määritetty kuten rajapinnan ohjelmistoille. (Granlund, 2007, s. 7–11; Hakala & Vainio, 2005, s. 138–141)

2.2 TCP/IP-malli

Internetin tiedonsiirto perustuu TCP/IP-malliin. Se on kehittynyt hieman erilaiseksi kuin OSI-malli, sisältäen vain neljä kerrosta. Se on kehittynyt markkinoiden vaatimusten mukaisesti avoimeksi, eikä yksitäinen valmistaja päätä protokollista tai standardeista. Näistä päättää IETF, joka hallinnoi TCP/IP-protokollien määrittelyä. Vaikka TCP/IP-malli ei ole perinteinen kerrosmalli, se noudattelee kerrosmallin rakennetta. (Granlund, 2007, s. 6–7; Valtionvarainministeriö, 2010, s. 27; Wendell, 2005, s. 49) Kuvassa 3 esitellään OSI-viitemallin ja TCP/IP-mallin suhteet sekä käytettäviä protokollia.



Kuva 3. OSI-viitemallin ja TCP/IP-mallin suhde toisiinsa. (Valtionvarainministeriö, 2010, s. 28)

2.3 TCP/IP-protokolla

Protokolla eli yhteyskäytäntö on kuvaus tavasta, jolla verkkojen laitteet keskustelevat toistensa kanssa. Protokollalla voidaan määrittää, kuinka yhteys luodaan, tietoa siirretään ja kuinka yhteys katkaistaan. Edellä mainittujen lisäksi protokolla sisältää menettelytavat virhetilanteisiin, kuten yhteyden katkeamiseen, vääristymiseen tai puuttuneeseen viestiin. (Granlund, 2007, s. 188)

TCP/IP-protokollan nimi tulee sen pääprotokollista TCP ja IP. Se sisältää useita protokollia. Käytännössä kaikki nykyiset tietokoneet käyttävät tätä protokollaa tai -mallia, joten ne voivat helposti olla yhteydessä toisiinsa. (Wendell, 2005, s. 49–52)

2.4 **TCP-protokolla**

TCP-protokolla liittyy datan kuljettamiseen ja täten TCP/IP-mallin kuljetuskerrokseen. TCP-protokolla on yhteydellinen eli jokaisessa TCP-yhteydessä luodaan kahdenvälinen yhteys laitteiden välille. Protokollalla on kolme päätehtävää: sopiminen yhteyden muodostamisesta, vuonohjaus (flow control) ja TCP-segmenttien (lähetettyjen pakettien) kuittaaminen. Vuonohjaus on mekanismi, jonka avulla laitteet ilmoittavat toisilleen vastaanotettavan datan määrän. (Hakala & Vainio, 2005, s. 302; Wendell, 2005, s. 49–52, 200)

2.5 **UPD-protokolla**

UDP-protokolla eroaa TCP-protokollasta siten, että se on ns. yhteydetön protokolla. Sovellukset, jotka käyttävät UDP:tä datan vastaanottamiseen vain kuultelevat tiettyä UDP-porttia. Mikäli dataa lähetetään, eikä se mene perille, data häviää. Perustellusti UDP:tä voidaan käyttää sovelluksissa, joissa yhden sanoman katoaminen ei häiritse sovelluksen toimintaa. Se säästää myös verkon kapasiteettia, koska lähetystä ei uusita. (Kaario, 2002, s. 23–24)

2.6 **IP-osoite**

IP-protokolla määrittelee mallin loogisen osoitteiston ja reitityksen. Näin ollen IP-kuuluu verkkokerrokseen. Jokaisella verkon aktiivisella laitteella on oltava IP-osoite. Esimerkiksi reitittimissä ja palvelimissa voi olla useampia verkkoliitäntöjä, joten niillä on useampia IP-osoitteita. IP-osoite on 32-bittinen binääriluku, joka voidaan ilmoittaa helpommin desimaalimuodossa. (Wendell, 2005, s. 52, 211–212) Taulukossa 1 on esitetty esimerkkejä IPv4-osoitteesta.

Taulukko 1. Esimerkkejä IPv4-osoitteesta.

Binäärimuoto	Desimaalimuoto
11000000 10101000 00000001 00000001	192.168.1.1
01010000 11011111 00001010 00100001	80.223.10.33

IP-osoite voidaan määritellä laitteelle kiinteästi TCP/IP-protokollaa asennettaessa tai se annetaan verkossa olevalta palvelimelta laitteelle organisaation käytössä olevasta osoiteavaruudesta tarvittaessa. Kun osoitetta ei enää tarvita, se vapautuu käyttöön toiselle laitteelle. IP-osoitteiden jakamisesta huolehtii DHCP-palvelu. IPv4-osoitteet ovat loppuneet ja uusi standardi IPv6 mahdollistaa kertakäyttöiset osoitteet, jotka voidaan asettaa jo tehtaalla laitteisiin, jolloin ne palvelevat koko laitteen käyttöiän. IPv6-osoitteen pituus on 128 bittiä. Tämä lisää käytettävissä olevien osoitteiden määrää huomattavasti. IPv6-osoitetta ei esitetä desimaalilukuna, kuten IPv4-osoitetta, vaan 16-bittisenä heksadesimaalina erotinmerkkinä

kaksoispiste. IPv6-osoitteesta voidaan helposti päätellä mille operaattorille verkko kuuluu tai missä se maantieteellisesti sijaitsee. Standardi vahvistettiin jo vuonna 1995, mutta ei ole vielä otettu laajamittaiseen käyttöön. IPv4-osoitteiden rajallista määrää on ollut mahdollista kiertää rajaamalla osa osoitteista ns. intranet-käyttöön, jolloin samoja osoitteita voidaan käyttää useissa lähiverkossa. Toinen käytössä oleva keino on osoitteenkääntöpalvelu NAT, jossa sisäverkossa olevat laitteet saavat rekisteröimättömän intranet-osoitteen. Kun kone liikennöi internetiin, osoite käännetään julkiseksi IP-osoitteeksi organisaation julkisten osoitteiden mukaan. (Hakala & Vainio, 2005, s. 191, 216–217; Vänskä, 2012)

2.7 **IEEE 802.3 -standardit**

Markkinoiden yleisin lähiverkko on Ethernet. Sen standardit määrittelevät IEEE. 1970-luvulla Xerox-yhtiö kehitti Ethernetin, jota alettiin kehittämään eteenpäin Xeroxin, Intelin ja Digitalin yhteistyönä. Näiden yhteistyön pohjalta IEEE julkaisi vuonna 1983 suosituksensa 802.3. Tämän jälkeen kehitys on ollut nopeaa. Tiedonsiirtonopeus on kehittynyt koaksiaalikaapelilla toteutetusta lähiverkosta suosituksella 802.3a, jonka teoreettinen tiedonsiirtonopeus on 10Mb/s, nykyisin käytössä oleviin valokuidulla toteutettuihin verkkoihin 802.3ae, joiden teoreettinen nopeus yltää 10Gb/s. (Granlund, 2007, s. 262–263)

2.8 **MAC-osoite**

Verkoissa laitteen tunnistaminen tapahtuu OSI-mallin alimmalla tasolla fyysisen, eli MAC-osoitteen, avulla. Sitä voidaan kutsua myös Ethernet-osoitteeksi. Ne esitetään heksadesimaaleina ja tavallisesti tämä osoite annetaan laitteille jo tehtaalla. Osoite muodostuu 48 bitistä, josta 24 bittiä on varattu valmistajan tunnistamiseksi. Näiden määrittelystä ja jakamisesta valmistajille vastaa IEEE. (Granlund, 2007, s. 264; Kaario, 2002, s. 36–37) Kuvassa 4. on esitetty tietokoneen verkkokortin MAC-osoite 00-1F-C6-86-9B-04 komentokehotteessa.

```
C:\WINDOWS\system32>getmac /v /fo list

Connection Name:  Ethernet 2
Network Adapter:  TAP-Windows Adapter V9
Physical Address: 00-FF-A1-19-6C-C1
Transport Name:   Media disconnected

Connection Name:  Citrix Virtual Adapter
Network Adapter:  Citrix Virtual Adapter
Physical Address: Disabled
Transport Name:   Disconnected

Connection Name:  Ethernet
Network Adapter:  Marvell Yukon 88E8056 PCI-E Gigabit Ethernet Controller
Physical Address: 00-1F-C6-86-9B-04
Transport Name:   \Device\Tcpip_{819C556C-89A4-4B3D-825E-298D09EF47B4}
```

Kuva 4. Verkkokortin MAC-osoite komentokehotteessa.

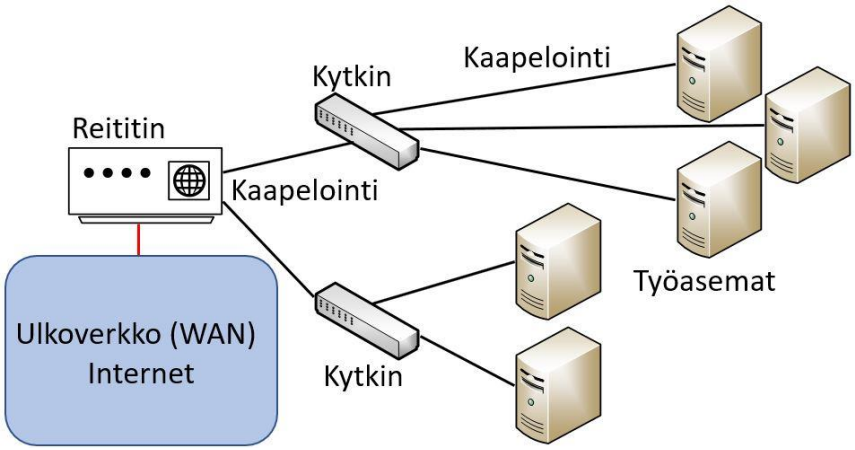
2.9 Lähiverkon kaapelointi ja laitteet

Verkon osaa, jolla verkkolaitteet kytketään toisiinsa, kutsutaan kaapeloinniksi. Se on verkon tiedonsiirtotie verkkolaitteiden, palvelimien ja verkon palveluiden välillä. Kaapelointi toteutetaan nykyisin joko kierretyllä parikaapelilla tai valokaapelilla. Parikaapeli on alun perin lähtöisin puhelin- ja rakennusten sisäisistä kaapeloinneista. Kaapelin sisällä olevat johtimet on kierretty pareittain, joka vähentää elektromagneettisia häiriöitä. Valokaapelissa tiedon välittää valopulssit, eikä siinä ole sähköiseen tiedonsiirtoon liittyviä sähkömagneettisia ongelmia. (Granlund, 2007, s. 42, 48; Jaakohuhta, 2005, s. 35)

Reititin (router) ei varsinaisesti ole lähiverkon laite, mutta on yhteydessä lähiverkkoon. Se yhdistää sisäverkon ulkoverkkoon (WAN) ja internetiin. Reititin voi yhdistää ulkoverkon kautta lähiverkon toiseen lähiverkkoon. Reitittimessä on yleensä Ethernet-liitäntä, jolla se liitetään lähiverkkoon. (Jaakohuhta, 2005, s. 108)

Verkkokortti (NIC) löytyy jokaisesta lähiverkon laitteesta. Tällä tietokone tai muu laite saadaan yhdistettyä verkkoon. Jokaisella verkkokortilla on yksilöllinen MAC-osoite, jolla laite voidaan tunnistaa. MAC-osoitteen voi joissain verkkokorteissa muuttaa. (Jaakohuhta, 2005, s. 115–116)

Kytkin (switch) on aktiivinen verkkolaite. Yksinkertaistetusti se on tietokone, joka välittää tiedon mahdollisimman nopeasti lähdeportista kohdeporttiin. Kytkin mahdollistaa verkon nopean reitityksen porttien välillä ja ohjaa liikenteen oikeaan porttiin. Nykyisten lähiverkkojen komponenteista keskeisin on kytkin. (Jaakohuhta, 2005, s. 135–137) Kuvassa 5 on esitetty yksinkertainen esimerkki lähiverkosta, joka on reitittimen välityksellä yhteydessä ulkoverkkoon ja internetiin.



Kuva 5. Yksinkertainen esimerkki lähiverkosta.

3 KYTKIMET JA NIIDEN ETÄHALLINTA

Kytkimellä verkko voidaan segmentoida osiin ohjelmallisesti, ettei segmentin sisällä oleva liikenne näy muihin segmentteihin. Se mahdollistaa laajat ja monitasoiset lähiverkot, jolloin suorituskyvyn kannalta hidasteeksi jäävät verkossa olevat palvelimet ja niiden väliset reitit. (Granlund, 2007, s. 274)

Kytkimen ero keskittimeen (HUB) on sen kyky välittää liikenne eri lähtevistä porteista eri saapuviin portteihin ilman törmäyksiä. Keskitin ainoastaan välittää liikenteen kohdeporttiinsa. Kytkentää voidaan suorittaa myös OSI-mallin kolmannen tai neljännen kerroksen informaation avulla, esimerkiksi priorisoimalla liikennettä. Kytkimen suodatus perustuu kytkimen informaatioon porteista, joihin laitteet on kytketty. (Kaario, 2002, s. 29–30)

3.1 Kytkimen etähallinta

Verkonhallinnan päätehtävä on taata verkossa olevien palveluiden saatavuus. Tähän kuuluu laitteiden välisten yhteyksien ylläpitäminen, riittävän kaistanleveyden turvaaminen verkossa ja tietoturvan takaaminen. Tärkeänä osana verkonhallintaa on vikatilanteiden havaitseminen fyysisessä kaapeliverkossa, kytkimissä ja reitittimissä sekä työasemien ja palvelimien verkkokorteissa. Verkon etähallinta mahdollistuu kytkimien hallinnalla. Ylläpitäjän ei tarvitse olla fyysisesti verkon luona, vaan tarvitsee turvallisen yhteyden verkkoon. Yhteys voi olla toteutettu nopealla mobiiliyhteydellä tai suojatulla internetyhteydellä. Ylläpitäjä voi selvittää mm. verkon häiriötilanteita, käyttöoikeuksia, tietoturvaan liittyviä loukkauksia. Edellä mainittujen ongelmien havaitsemisen mahdollistaminen johtaa siirtymisen keskitettyyn hallintaan. Verkonhallinnan edellytys on dokumentointi. Verkkoja, joista ei ole dokumentointia, on lähes mahdoton hallita ilman verkon rakenteen tuntemista. (Hakala & Vainio, 2005, s. 322–323; Jaakohuhta, 2005, s. 311, 323)

3.2 Verkonhallinnan osa-alueet

Verkonhallinta jakautuu useampaan eri osa-alueeseen. Vikojenhallinnassa keskitytään verkon vikojen havaitsemiseen, eristämiseen ja korjaamiseen esimerkiksi virhelokien, ohjelmistollisen diagnostiikan ja toimenpiteiden suorittamisen avulla. Laskutuksen hallinnalla seurataan verkossa olevien palvelujen käyttöä, esimerkiksi osastojen välillä. Vaikka tällainen laskutus on usein yrityksen sisäistä laskutusta, saadaan tärkeää tietoa resurssien käytöstä eri toimijoiden välillä. Tulevaisuudessa tämän merkitys kasvaa verkkojen välisten palvelujen myymisellä asiakkaille. (Jaakohuhta, 2005, s. 309–310)

Kokoonpanon hallinnassa paneudutaan verkon fyysisien, esim. verkkokorttien hallintaan ja yksilöimiseen. Myös loogisten verkon osien, esim. VLAN-määrittely, kuuluu kokoonpanon hallintaan. Suorituskykyä mitataan ja analysoidaan suorituskyvyn hallinnassa tarkkailemalla jaettuja resursseja. Suorituskyvyn hallinta jakautuu kahteen toimintoon: valvontaan ja monitorointiin. Turvallisuuden hallinta koostuu käyttöoikeuksien ja niiden rikkomusten valvonnasta. Tätä varten kerätään lokeja, joita analysoimalla voidaan saada selville turvallisuusuhkia. (Jaakohuhta, 2005, s. 310–311)

Raportointi kertoo verkon tapahtumat, vikatilanteet sekä kapasiteetin ja laitteiston käytön. Tietyille palveluille tai sovelluksille voidaan antaa korkeampi prioriteetti, josta huolehditaan politiikan hallinnalla. Tarvittavat proaktiiviset ja reaktiiviset toimenpiteet, joilla vikoja tai kokoonpanoa on hallittu, ovat huoltoa. Ylläpidon hallinta koostuu erilaisten ylläpitosopimusten, palvelusopimusten sekä varaosien ja -laitteiden hallinnasta. Palvelujen hallinnalla varmistetaan ympäristön luetettavuutta, palveluiden saatavuutta oikeille käyttäjille myös mahdollisten vikatilanteiden aikana. Hallintatarkasteluun voidaan myös lukea teknologisen kehityksen hallinta, jossa ennakoidaan tulevaisuuden järjestelmien ja tarpeiden kehitys. (Jaakohuhta, 2005, s. 311)

ISO määrittelee puolestaan OSI-standardin mukaan verkonhallinnan vain viiteen kategoriaan. Vikojen hallintaan, käytön hallintaan, kokoonpanon hallintaan, suorituskyvyn hallintaan ja turvallisuuden hallintaan. Edellä mainittuja kategorioita voidaan vielä jakaa verkonvalvontaan ja verkonhallintaan. (Kaario, 2002, s. 270)

3.3 **SNMP-protokolla**

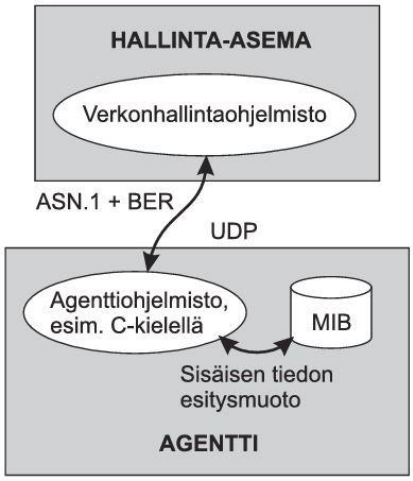
Verkonhallinnan tekninen toteutus järjestetään yleisimmin ohjelmallisesti SNMP-protokollan avulla internetyhteyden yli. TCP/IP-protokollaan pohjautuvissa verkoissa on usein monia palvelimia ja verkon aktiivilaitteita, jotka voivat vikaantua. Muutokset organisaatiossa tai laitteistossa voivat aiheuttaa sen, ettei arkkitehtuuri enää vastaa voimassaolevia prosesseja. Ulkoisina uhkina verkolle ovat krakkerit ja hakkerit, jotka pyrkivät murtautumaan verkkoon internetin kautta. Verkkoa voi uhata myös vihamieliset käyttäjät sisältäpäin. (Hakala & Vainio, 2005, s. 323)

SNMP (Simple Network Management Protocol) koostuu standardeista rakentuen SNMP-protokollaksi, josta on olemassa kolme versiota: SNMPv1, SNMPv2 ja SNMPv3. Verkonhallinta perustuu hallittaviin laitteisiin ns. SNMP-agentteihin, näiden tilan seurantaan ja konfigurointiin. SNMP-liikenne hoidetaan UDP-protokollan avulla, jolla ylimääräistä rasitusta verkolle pyritään minimoimaan. Verkonhallinnassa tarvitaan pelkän protokollan lisäksi hallintatietokantaa, MIB ja rakenteen määrittelyä tietokantaolioille, SMI. (Kaario, 2002, s. 270–271) Taulukossa 2 esitetään SNMP-verkonhallintaan liittyviä RFC-dokumentteja.

Taulukko 2. SNMP-verkonhallinnan RFC-dokumentteja. (Kaario, 2002, s. 271)

Joitain SNMP-verkonhallintaan liittyviä RFC-dokumentteja	
RFC	**Nimi**
1155	Structure and Identification of Management Information for TCP/IP-based Internets
1156	Management Information Base for Network Management of TCP/IP-based internets
1157	A Simple Network Management Protocol (SNMP)
1212	Concise MIB Definitions
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
1215	A Convention for Defining Traps for use with the SNMP
1757	Remote Network Monitoring Management Information Base
1901	Introduction to Community-based SNMPv2
1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
1909	An Administrative Infrastructure for SNMPv2
1910	User-based Security Model for SNMPv2
2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2
2271	An Architecture for Describing SNMP Management Frameworks
2272	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
2275	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

Verkonhallinta-asemalla hoidetaan SNMP-verkon hallinta. SNMP-agenteilta kysellään tietoja käyttäen ISOn OSI-malliin kehittämää kieltä ASN.1 (Abstract Syntax Notation One), jota kaikki agentit ja hallinta-asema ymmärtävät. Koodauksena käytetään BER-koodausta (Basic Encoding Rules). (Kaario, 2002, s. 273,279) Kuvassa 6 on esitetty SNMP hallinta-aseman ja agenttien välinen toiminta.



Kuva 6. SNMP-verkon kokoonpanoon kuuluu agentit, eli hallittavat laitteet, sekä hallinta-asema. (Kaario, 2002, s. 273)

Hallintaan SNMPv1 käyttää kolmenlaisia operaatioita. GET-operaatiolla pyydetään agentilta arvoa oliolle. Näitä pyyntöjä tehdään tavallisesti ajastettuna ja huolellisesti suunnitellusti. Toinen operaatio on SET, jolla olion arvo muutetaan hallinta-aseman toimesta. TRAP-operaation puolestaan lähettää agentti hallinta-asemalle määriteltyjen hälytysrajojen ylittyessä. Tällainen ilmoitus voisi olla tavallisuudesta poikkeava määrä virheitä sanomien vastaanotossa. SNMPv2 laajentaa näitä operaatioita ja SNMPv3 lisää mahdollisuuden sanomien salaukseen. (Kaario, 2002, s. 277–279)

3.4 **RMON-protokolla**

RMON (Remote Network Monitoring) on luotu SNMP:n puutteiden korvaajaksi ja sitä voidaan käyttää yhdessä SNMP:n kanssa. Se mahdollistaa laajemman tiedon keräyksen ja raportoinnin, kuin pelkkä SNMP. Se kerää historiatietoa omaan MIB-tietokantaansa ja näin vähentää verkossa tapahtuvaa liikennettä, johon se käyttää SNMP-protokollaa. RMON voi kerätä tietoa tietystä lähiverkon osasta kaikilta seitsemältä OSI-mallin kerrokselta, jota voidaan tutkia etäyhteyden kautta. Yleensä RMON on toteutettu valmistajan toimesta verkon aktiivilaitteisiin. (Jaakohuhta, 2005, s. 316–318)

4 TIETOTURVA

Nykypäivän organisaatioissa arvokkainta omaisuutta on tieto. Tietoturvan ylläpidossa varaudutaan usein ulkoapäin tuleviin uhkiin ja hyökkäyksiin, vaikka suurimmat riskit tietoturvalle tulevat sisältäpäin. Täysin varmoja järjestelmiä ei pystytä luomaan, koska aina jos on yhdelläkin ihmisellä mahdollisuus päästä kiinni johonkin aineistoon, se on tietomurron mahdollisuus. Kaikissa järjestelmissä heikoin lenkki on ihminen. (Hakala & Vainio, 2005, s. 341; Kaario, 2002, s. 292)

Joka päivä raportoidaan uusia mahdollisuuksia murtaa järjestelmiä. Tietoturva on aina jäljessä murtautujia ja hakkereita vastaan. Murtamattomia järjestelmiä ei saada aikaiseksi ja samalla täytyy ottaa huomioon tietoturvan kustannukset, sekä tiedon saatavuus ja käytettävyys. Tietoturva voidaan jakaa kuuteen eri tehtäväkenttään. (Kaario, 2002, s. 292)

4.1 Luottamuksellisuus ja eheys

Luottamuksellisuudella tarkoitetaan tiedon säilymistä niillä, joilla on siihen oikeus. Se suojaa sekä omistusoikeutta että yksityisyyttä. Tietoverkoissa tätä hoidetaan salaamalla tiedostoja ja käyttäjän tunnistuksella, jotta vain oikeutetuilla henkilöillä on päästy tietoon. (Hakala & Vainio, 2005, s. 342; Kaario, 2002, s. 293)

Mikäli tieto, joka on siirretty tai säilytetty, ei ole muuttunut, se on eheää. Tieto voi muuttua tahattomasti esimerkiksi ohjelmiston virheen vuoksi tai tahallisesti esimerkiksi krakkerin toimesta. Yhteydellisellä TCP-protokollalla voidaan pyrkiä estämään tiedon tahaton muuttuminen. Eheyteen liittyy aina tiedon tuottajan tai toimittajan oikeellisuuden vahvistaminen. (Hakala & Vainio, 2005, s. 342; Kaario, 2002, s. 293)

4.2 Todennus ja kiistämättömyys

Todennuksella varmistetaan, että osapuolet ovat niitä, keitä heidän tulisikin olla. Salasana on yksi menetelmä tähän. Se ei kuitenkaan yksinään ole hyvä varmistus, koska salasana helposti murrettavissa. Salasanan tulee olla riittävän vahva. (Kaario, 2002, s. 293)

Kiistämättömyys on vahva muoto todennuksesta. Siinä osapuoli, joka on tapahtumassa mukana, ei voi kiistää sitä. Virallisemmissa verkoissa edellytetään kiistämättömyyttä esimerkiksi digitaalisen allekirjoituksen avulla. (Kaario, 2002, s. 293)

4.3 **Pääsynvalvonta ja käytettävyys**

Pääsynvalvonta liittyy luottamuksellisuuteen ja eheyteen. Sillä tarkoitetaan mekanismeja, joilla käyttäjät todennetaan ja rajoitetaan verkkoihin pääsyä. Etenkin ulkoisten uhkien estämiseen nähden pääsynvalvonta on tärkeässä osassa. (Hakala & Vainio, 2005, s. 342; Kaario, 2002, s. 293)

Käytettävyys on tiedon saatavilla olemista heille, kenellä siihen on tarve ja oikeus, kohtuullisessa ajassa. Yleensä käytettävyys laskee, kun tietoturvan taso nousee. Tästä aiheutuu eniten ristiriitaa aiemmin mainittujen periaatteiden kesken. Käytettävyyttä voidaan ylläpitää takaamalla esimerkiksi riittävä kaistanleveys ja käyttämällä varayhteyksiä. (Hakala & Vainio, 2005, s. 342; Kaario, 2002, s. 294)

4.4 **Suojautuminen**

Suojautumisen pääperiaate on käyttäjän oikeudet käyttämiinsä laitteisiin ja näiden sisältämään tietoon. Tähän päästään käyttäjän vahvalla tunnistamisella. Myös tietoliikenteen salauksella vahvistetaan tietoturvaa. Ulkoisten yhteyksien suojauksesta huolehtii yleensä palomuuri, joka valvoo ja hallitsee näitä. Palomuurin tulee suodattaa liikennettä, mutta myös varmistaa riittävä suorituskyky ulkoisiin yhteyksiin. Yksistään palomuuri ei riitä takaamaan riittävää tietoturvaa, vaan tarvitaan myös muita keinoja. Mekaaninen suojautuminen on tehokas tapa parantaa tietoturvaa. Esimerkiksi palvelintilojen lukitus ja kulunvalvonta sekä asiattomilta henkilöiltä pääsyn estäminen kuuluu mekaaniseen suojautumiseen. (Hakala & Vainio, 2005, s. 343; Kaario, 2002, s. 304–305)

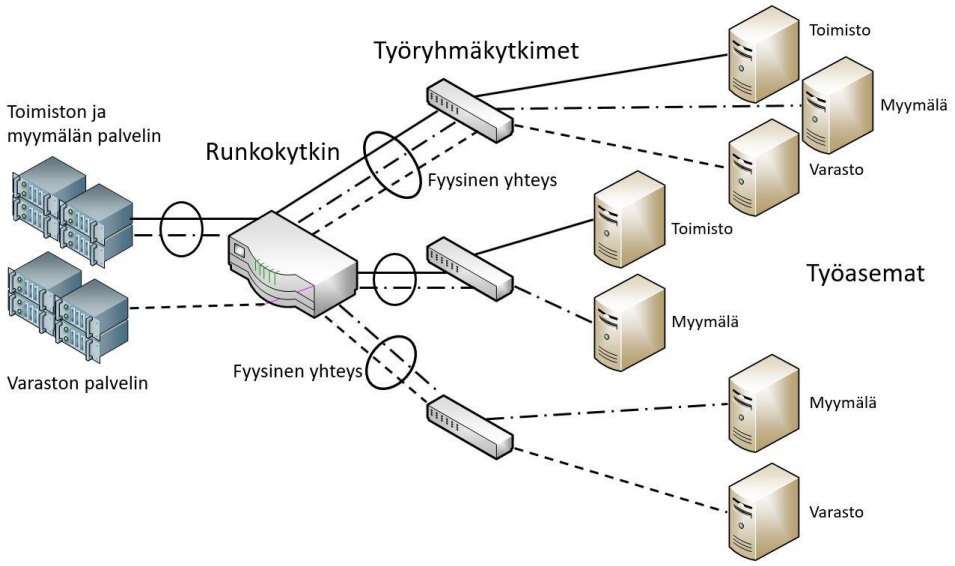
Rakenteellinen tietoturva on osa suojautumista, joka täytyy ottaa huomioon jo verkkoa rakennettaessa. Toiminnan kannalta on tärkeää luoda mahdollisimman vähän liikenteen pullonkauloja ja ettei sisäverkkoon päästä, kuin suojatuilla VPN-yhteyksillä. Liikenteen pullonkauloja voidaan välttää kytkemällä palvelimet ja työasemat suoraan kytkimiin. Kytkimille voidaan asettaa toisistaan riippumattomia ryhmiä, jotka muodostavat virtuaalisia lähiverkkoja (VLAN). (Hakala & Vainio, 2005, s. 344; Jaakohuhta, 2005, s. 157)

5 VIRTUAALINEN LÄHIVERKKO

IEEEn suositus 802.3ac vuodelta 1998 mahdollisti Ethernet-verkoissa käytettävät virtuaaliset lähiverkot (VLAN, virtual LAN). Dataan lisättiin tunnistus, jolla tieto voidaan ohjata oikeaan lähiverkkoon. Tämä helpotti erilaisten ryhmien ja yhteisöjen liikenteen yhdistämistä samalle runkoyhteydelle vaarantamatta yksityisyyttä. (Granlund, 2007, s. 267)

Virtuaalisten lähiverkkojen käytöllä voidaan parantaa lähiverkon tietoturvaa, kasvattaa verkon tiedonsiirtokapasiteettia, rajoittaa lähiverkon liikennettä, hallita levitysviestien käyttämistä ja helpottaa käyttäjien siirtymistä lähiverkon sisällä. VLAN voidaan toteuttaa normaalisti MAC-osoitteiden perusteella, kytkimen porttien määrittelyllä, verkko-osoitteella tai verkkoprotokollien avulla. (Jaakohuhta, 2005, s. 157)

Fyysiseen verkkoon on mahdollista luoda kytkinten avulla virtuaalinen lähiverkko. Tiedon kulku voidaan määritellä vain tiettyihin virtuaalisiin verkkoihin. Tämä tapahtuu OSI-mallin toisessa eli siirtokerroksessa. Nykyisissä kytkimissä on käytössä IEEE 802.1Q/p -standardi, jonka GVRP-protokollan avulla työasemat voivat pyytää liittyä virtuaaliseen lähiverkkoon. Tämä helpottaa VLANien hallintaa verkonhallintaohjelmistoa käyttämällä. (Jaakohuhta, 2005, s. 158–159) Kuvassa 7 on esitetty virtuaalinen verkko, jossa saman fyysisen yhteyden läpi kulkee useampia VLANeja.



Kuva 7. Virtuaalisesti toteutettu verkko.

5.1 MAC-osoitteinen VLAN

MAC-osoitteiden perusteella jaettaviin VLANeihin määritetään kaikki MAC-osoitteet, jotka pääsevät kyseiseen verkkoon. Sama osoite voi kuulua useampaan virtuaaliseen lähiverkkoon. Hankaluutena tässä on, että

jokainen MAC-osoite tulee tuntea ja uudet MAC-osoitteet lisätä määrittelyihin. Käytännössä kytkimet huolehtivat MAC-osoitteisesta VLANista. (Jaakohuhta, 2005, s. 157)

5.2 **Porttipohjainen VLAN**

Toisessa vaihtoehdossa kytkimien porttimäärittelyllä hoidetaan virtuaalisen lähiverkon järjestely. Menetelmän huonona puolena on, että laite voi kuulua vain yhteen VLANiin. Hyvänä puolena on määritettävien porttien vähäinen määrä verrattuna verkossa olevien MAC-osoitteiden määrään. (Jaakohuhta, 2005, s. 157–158)

5.3 **Verkko-osoiteperusteinen VLAN**

Verkko-osoitteiden, eli IP-osoitteiden perusteella järjestetty VLAN on protokollasidonnainen. Kunkin protokollan verkko-osoitteet muodostavat oman verkon. Menetelmän hyvä puoli on hallittavuuden helppous, koska kytkimet huolehtivat dynaamisesti virtuaalisen lähiverkon osoitteet laitteiden vaihtuessa tai siirtyessä. (Jaakohuhta, 2005, s. 158)

5.4 **Protokollapohjainen VLAN**

Verkkoprotokollan avulla järjestetty virtuaalinen lähiverkko toteutetaan protokollien mukaan, esimerkiksi IP, IPX. Jokainen protokolla muodostaa oman VLANinsa. Hallittavuuden kannalta tämä järjestely on helppo, mutta eniten käytetyn protokollan verkosta tulee suurin. (Jaakohuhta, 2005, s. 158)

6 DOKUMENTOINTI

Lähtökohta toimivalle verkolle on ajantasainen ja riittävä dokumentointi. Hyvin suunnitellussa verkossa dokumentointi on kunnossa. Suurin haaste on dokumentaation ylläpito. Verkonhallintaohjelmistolla voidaan helpottaa dokumentaatiota, jos perusdokumentointi on kunnossa. Pelkän verkonhallintaohjelmiston hankkimisella ei voida korjata suunnitelman tai dokumentaation puutteita. (Kaario, 2002, s. 256)

Tietojärjestelmät ovat jatkuvassa muutoksessa. Mikäli muutoksia tapahtuu paljon ja nopeasti, voi ylläpidon olla vaikea pysyä mukana, ellei dokumentaatio ole kunnossa. Tietoverkkoihin tulee vikoja ja häiriöitä, mutta niiden haitat voidaan minimoida. (Jaakohuhta, 2005, s. 324)

Tehokkaasti hoidettu vikojen selvitys vaatii ylläpidolta hyvät tiedot verkon rakenteesta ja toiminnasta. Tietojen määrä riippuu verkon koosta ja oletetun vian haitasta organisaatiolle. Vähimmäisvaatimuksiksi voidaan määritellä asiat, joista tieto tulisi olla, jotta verkon viat ja korjaus olisi mahdollista. Näitä voivat olla esimerkiksi:

- Ajantasainen dokumentaatio järjestelmästä ja sen rakenteesta
- Laitteiden ja ohjelmistojen toimittajat ja valmistajat
- Varaosien saatavuus
- Palveluiden saatavuus
- Välineet vikojen tunnistamiseksi
- Taitoa havaita ja korjata viat (Jaakohuhta, 2005, s. 324–325)

Dokumentaatioon kuuluu sähköiset ja fyysiset asiakirjat, joissa on kuvattu järjestelmän rakenne ja komponenttien toiminta. Hyvällä dokumentoinnilla vikojen selvittämiseen menevä aika lyhenee, palveluiden osto ja suunnittelu helpottuu, henkilöstöstä tulevat riskit pienenevät, turvallisuustaso käytössä paranee ja se helpottaa käyttöönottoa. Yleisesti dokumentointi nähdään vain kuluna, mutta vian ilmetessä dokumentaatiossa säästöt syödään moninkertaisesti. (Jaakohuhta, 2005, s. 325)

6.1 Dokumentaation sisältö

Organisaatio itse päättää mitä dokumentaatioon sisällytetään. Perussääntönä voisi olla, että liiketoiminnan kannalta tärkeät elementit on dokumentoitu hyvin ja dokumentoinnista voidaan selvittää ongelmatilanteiden tarvittavat jatkotoimenpiteet. Dokumentoinnissa tulisi olla kaapelointi, johtotiet, jakamot, verkon aktiivilaitteet ja niiden konfiguraatiot, langattoman verkon tukiasemat, palvelimet, varusohjelmistot, sovellukset, varavirtajärjestelmä (UPS), käytetyt ohjelmistot, työasemat ja tulostimet sekä liitännät. (Jaakohuhta, 2005, s. 326)

Dokumentointi suoritetaan yleensä loogisena ja fyysisenä kuvauksena. Loogisella kuvauksella verkon rakenne esitetään helposti hahmotettavassa

muodossa laitteiden ja liitäntöjen perusteella. Fyysisestä kuvauksesta selviää verkon fyysinen rakenne ja missä esimerkiksi verkon laitteet, jakamot ja kaapelit sijaitsevat. (Jaakohuhta, 2005, s. 326)

Dokumentaation on hyvä kattaa myös laitelista, johon on määritelty vähintään laitteiden IP- ja MAC-osoitteet, käyttötarkoitus, sijainti ja omistaja sekä verkon suojaukset. Suurissa verkkojen organisaatioissa olisi suositeltavaa nimetä täysipäiväinen henkilö, joka vastaa dokumentoinnista hallinnollisella työllä sekä henkilö verkon ylläpitoon. Pienemmissä organisaatioissa dokumentaation osille tulisi määrittää henkilö, joka vastaa dokumentaatiosta. (Valtionvarainministeriö, 2010, s. 36)

6.2 **Dokumentoinnin järjestelmät**

Dokumentaatio tehdään nykyisin sähköisesti piirrosohjelmilla, normaaleilla toimisto-ohjelmistoilla tai yhä useammin suuremmissa organisaatioissa verkon suunnitteluun ja dokumentointiin kehitetyillä ohjelmistoilla. Myös useissa verkonhallintaohjelmistoissa on dokumentaatiota helpottavia ominaisuuksia. Aiemmin dokumentaatio on ollut paperimuodossa. (Hakala & Vainio, 2005, s. 421; Jaakohuhta, 2005, s. 330)

7 CASE: YRITYS OY

Opinnäytetyön toimeksiantajayritys toimii vähittäiskaupan alalla ja sillä on yli 30 myymälää ympäri Suomea. Yrityksen pitkän historian vuoksi myymälät on rakennettu tai hankittu eri aikoina, eikä lähiverkolle ole muodostettu yhtenäistä käytäntöä. Verkkojen suunnitelmallinen yhtenäistäminen on ollut jo pidempään harkinnassa. Yrityksen tietohallinto on aloittanut myymälöiden lähiverkon vakioimistyön ja pääpiirteet on asetettu. Verkon aktiivilaitteistoa tullaan päivittämään etähallittavaksi, laitekaappien sisältö yhtenäistetään, laitekaappien Ethernet-kaapelit ovat värikoodattuja ja dokumentaatio saatetaan ajan tasalle. Myös paikallisen IT-lähituen koulutuksen tarvetta kartoitetaan ja suunnitellaan. Paikalliset IT-tukihenkilöt hoitavat IT-puolta oman toimensa ohella.

Tulevaisuudessa avattavien myymälöiden lähiverkko on tarkoitus järjestää yhtenäisellä käytännöllä, tämän opinnäytetyön tuloksien perusteella. Myös käytössä olevien myymälöiden lähiverkko tullaan yhtenäistämään toimipaikka kerrallaan.

Lähiverkkojen yhtenäistäminen vähentää verkko-ongelmien selvittämiseen kuluvaa aikaan, jolloin paikallinen ja tietohallinnon IT-tuki voi keskittyä itse ongelman ratkaisuun, eikä aika kulu esimerkiksi vian aiheuttavan laitteen paikallistamiseen. Tämä puolestaan lisää tuottavuutta sekä myyntikatkojen lyhentyessä, että henkilöstö voi toimia oman päätyönsä mukaisesti.

7.1 Kysely paikallisesta lähiverkosta

Osana opinnäytetyötä luotiin Webropol-kysely, jolla kartoitettiin nykyisten lähiverkkojen toimivuutta, ongelmia, mielipidettä verkon yhtenäistämisestä ja vakioimisesta sekä lisäkoulutuksen tarvetta. Kysely löytyy liitteestä 1. Kysely lähetettiin sähköpostilla yksiköiden päälliköille sekä tietohallinnon henkilöstölle ennen lähiverkon vakioinnin aloittamista. Yksiköiden päälliköitä pyydettiin välittämään se paikallisille IT-tukihenkilöille, koska listausta heistä ei tällä hetkellä ole. Yrityksessä on meneillään paikallisten IT-tukihenkilöiden kirjaaminen henkilöstönhallintaohjelmaan.

Kysely toteutettiin skaaloihin perustuvilla kysymyksillä, monivalintakysymyksillä ja avoimilla kysymyksillä. Skaaloihin perustuvissa kysymyksissä skaala oli yhdestä viiteen. Yksi tarkoitti huonoa tai ei toimivaa ja viisi puolestaan hyvää tai toimivaa.

7.2 **Kyselyn tulokset**

Vastauksia määräaikaan mennessä saatiin 28 kpl. Vastaajista 18 kuului paikalliseen IT-tukihenkilöstöön, viisi tietohallintoon ja loput vastaajista muuhun, kuin kahteen edelliseen ryhmään. Kyselyn vastausmäärä jäi odotettua alhaisemmaksi.

Pääosin verkon toimintaan ja käytettävyyteen oltiin tyytyväisiä keskiarvojen ollessa 4,0 ja 4,2. Haasteiksi koettiin verkon ajoittainen hitaus sekä toimimattomuus. Myös verkon dokumentointi on kyselyn mukaan olematonta. Yli puolet (58%) vastaajista ilmaisi lisäkoulutuksen tarpeen suurimmaksi haasteeksi lähiverkossa. Verkon ongelmien selvittämiseen kuluva aika arvioitiin pääosin olevan alle puoli tuntia. Suurin osa vastaajista tuntee oman yksikkönsä lähiverkon rakenteen ja hallitsee sen tietoturvan perusteet.

Avoimissa vastauksissa ilmeni laitekaappien epäjärjestyksestä ja dokumentoinnin puutteesta seuraava ongelmien selvittämisen vaikeus ja siihen kuluva aika. Lisääntynyt kameravalvonta ja sen tuoma liikenne verkkoon on hidastanut muita toimintoja kytkinten ollessa liian hitaita kasvaneelle tietoliikennemäärälle. Verkon aktiivilaitteiden päivitystä samanlaiseksi toivottiin toimipisteisiin.

Lähiverkon yhtenäistämistä pidettiin kyselyn mukaan hyvänä asiana ja parannuksena nykyiseen. Toimipaikkojen erilaisuudesta johtuvaan vakioinnin hankaluuteen kiinnitettiin huomiota.

8 LÄHIVERKON VAKIOINTI

Opinnäytetyön tarkoituksena on kerätä parhaita käytäntöjä yhteen ja luoda perusta vakioinnille, jota voidaan käyttää myös muissa myymälöissä näiden erilaisuus huomioiden. Opinnäytetyön osana suoritetaan Webropol-kysely, jossa selvitetään myymälöiden lähiverkon tilaa ja toimintaa sekä paikallisen IT-tukihenkilöiden tarvetta lisäkoulutukselle. Kyselyyn vastaa myös tietohallinnon henkilöstöä, jotta saadaan lisää näkemystä verkon tilasta ja ajatuksista lähiverkkojen yhtenäistämisestä.

Käytännön asennustyö pyritään suorittamaan minimoimalla katkot lähiverkossa liikkeen aukioloaikana. Tämän vuoksi asennustyö täytyy ajoittaa osin myymälän aukiolon ulkopuolelle, jotta myynnin kannalta tärkeimmät toiminnot, kuten kassat ja asiakaspalveluun liittyvät työasemat toimivat ilman katkoksia.

Verkon uusittavat aktiivilaitteet asennetaan laitekaappeihin ja kytketään verkkoon. Tämän jälkeen vaihdetaan kameraverkon laitekaapin Ethernet-johdot myymälän aukioloaikana, koska ne eivät häiritse myyntiä. Aukiolon ulkopuolella kytketään myynnin kannalta kriittisimmät työasemat.

Laitekaapin sisältöä järjestellään uudelleen, dokumentoidaan valokuvin ja Microsoft Visio -ohjelmiston avulla piirretään laitekaappien sisällöt sekä kytkimen portin ristikytkennät listataan taulukkolaskentaohjelmalla. Tarkempaa laitteiden dokumentaatiota ei tehdä, koska yritys on siirtymässä DHCP-palveluun, jolloin laitteiden IP-osoitteet muuttuvat usein. MAC-osoitteet saadaan tarvittaessa kytkimen hallinnan kautta tietoon.

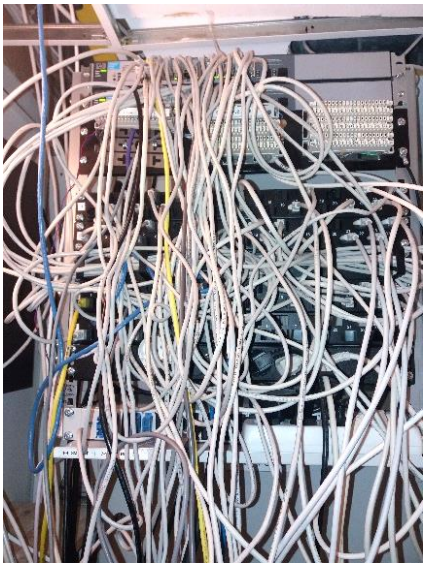
8.1 Lähtötilanne

Osa yrityksen myymälöistä on jo vuosia vanhoja ja lähiverkkojen vaatimukset ovat kasvaneet ajan myötä. Myymälöissä on käytössä työasemia kassoilla, palvelutiskillä, varastossa, yritysmyynnissä, asiakaspäätteinä sekä toimistossa. Palvelimia toimipisteissä on yleensä kolme: toimipistepalvelin, kamerapalvelin ja valaistusohjain.

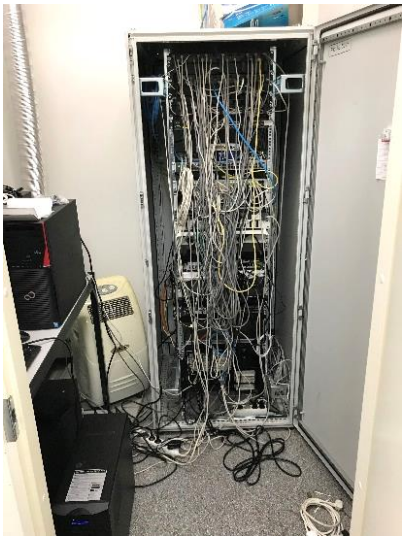
Yrityksessä on panostettu viimevuosina huomattavasti turvallisuuteen ja hävikin torjuntaan lisäämällä kameravalvontaa sekä tuotesuojahälyttimiä. Tämä on johtanut verkossa kulkevan tiedon määrän kasvuun, joka on aiheuttanut ongelmia hitaampien kytkimien vuoksi. Jakamoissa tähän asti on ollut erilliset kytkimet kameraverkolle, jotka tullaan korvaamaan uusilla kytkimillä, joihin kytketään sekä työasemat, että kamerat. Myös muiden toimijoiden laitteita on osana lähiverkkoa. Esimerkiksi Veikkauksen rahapeliautomaatit tarvitsevat internet-yhteyden maksukortilla tapahtuvaa pelaamista varten.

Yrityksellä on muitakin palveluita, jotka tarvitsevat pääsyn internetiin, mutta eivät lähiverkkoon tietoturvasyistä. Erilaiset verkon laitteet, kuten valvontakamerat ja työasemat, jaetaan omiin virtuaalisiin verkkoihinsa (VLAN) porttikohtaisesti. Näin kaikki laitteet voidaan kytkeä samoihin kytkimiin ja esimerkiksi muiden toimijoiden laitteet eivät pääse yrityksen lähiverkkoon.

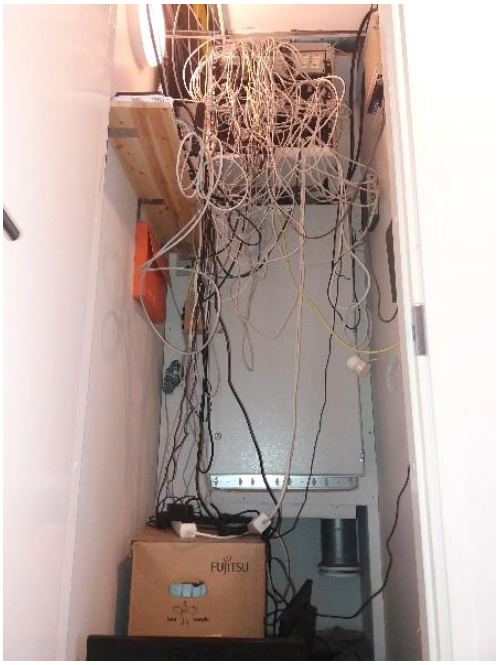
Myymälät eivät ole kaikki samankokoisia, vaan luokitellaan eri kategorioihin myymälän pinta-alan ja tuotevalikoiman avulla. Näin ollen myös verkkoratkaisut ovat hieman erilaisia. Toimipaikoilla on käytössä erilaisia kytkimiä, jotka eivät ole etähallittavia. Myöskään Ethernet-johdotus ei ole värikoodattu, kuin osassa myymälöitä. Kuvissa 8-10 on eri toimipisteiden käytössä olevia ratkaisuja laitekaappien sisällöstä ennen verkkolaiteuudistusta.



Kuva 8. Myymälän A ryhmäkeskuksen laitekaappi. (Yritys Oy, 2018)



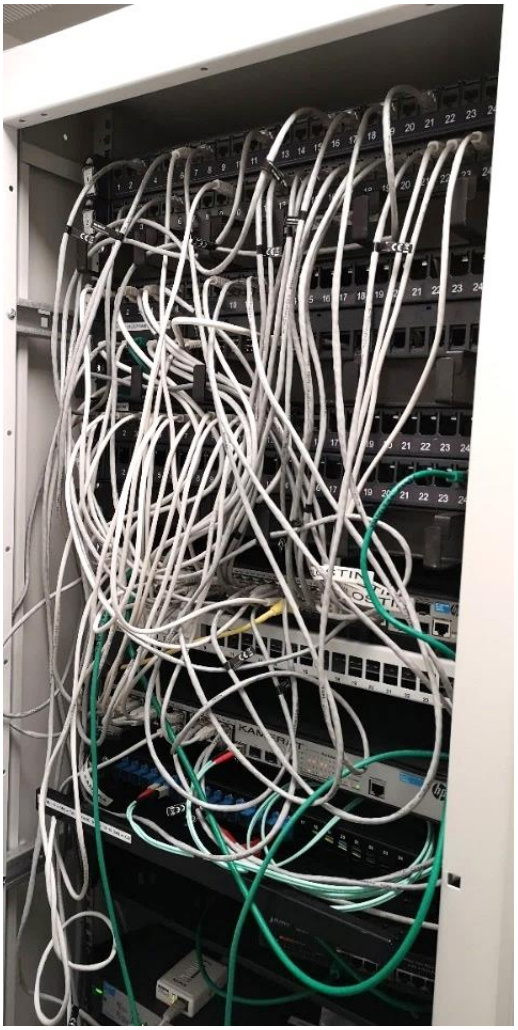
Kuva 9. Myymälän B palvelinhuone. (Yritys Oy, 2018)



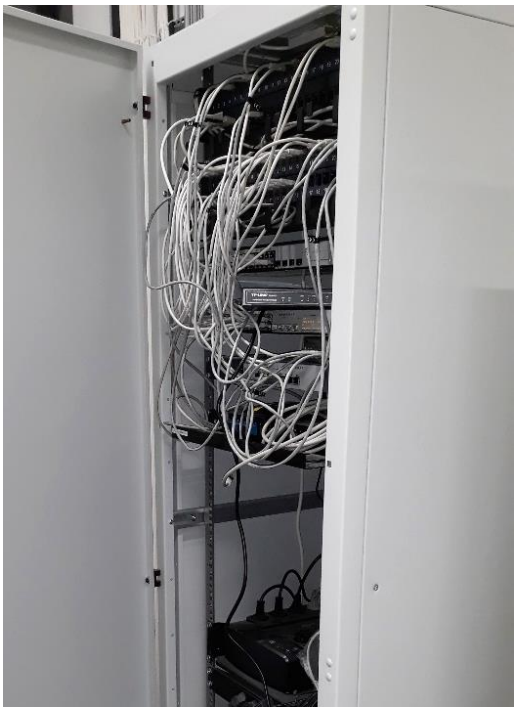
Kuva 10. Myymälän C yläkerran reititintila. (Yritys Oy, 2018)

Kuten kuvista 8-10 voi päätellä, ei yhtenäistä käytäntöä ole ja laitekaapit tarvitsevat kytkinten päivityksen ja siistimmän johdotuksen. Oman haasteensa luo myymälöiden eri-ikäisyys ja -kokoisuus. Osassa myymälöistä laitekaapeissa on myös vanhoja puhelinjohdotuksia. Tämän vuoksi tarkastelussa on otettava vain huomioon pääperiaatteiden luominen laitteistossa, laitekaappien sisällöissä ja dokumentoinnissa.

Tässä työssä perehdytään muutaman vuoden ikäisen, keskikokoisen myymälän (Myymälä D) lähiverkkoon. Myymälässä on talojakamo ja kolme kerrosjakamoa. Talojakamossa on yhteydet internetiin sekä liityntä yrityksen verkkoon. Ensimmäisessä kerrosjakamossa sijaitsee palvelimet, varayhteys, kulunvalvonta ja valaistuksen hallinta. Toisessa kerrosjakamossa on valvontakameroiden ja työasemien kytkimiä sekä muiden toimijoiden yhteyksiä. Kolmannessa kerrosjakamossa on kytkettynä kaksi valvontakameraa talojakamon kytkimeen. Yrityksen langaton lähiverkko (WLAN) jää tämän opinnäytetyön ulkopuolelle ja opinnäytetyössä keskitytään laitekaappien sisällön vakioimiseen ja dokumentointiin. Kuvissa 11-13 on Myymälän D jakamot ennen uudistusta.



Kuva 11. Myymälän D kerrosjakamo 1 ennen uudistusta. (Yritys Oy, 2018)



Kuva 12. Myymälän D kerrosjakamo 2 ennen uudistusta.

Kuva 13. Myymälän D talojakamo ennen uudistusta. (Yritys Oy, 2018)

8.2 **Toteutus**

Kun opinnäytetyö varmistui yrityksen puolelta, oli askelmerkit työn suorittamiseen selvät. Yhteen toimipisteeseen, Myymälä D, tehdään verkon aktiivilaitteiden päivitys etähallittaviin Hewlett Packard Enterprisen (HPE) valmistamiin Aruba 2540 PoE+ 4SFP+ -kytkimiin, joita voidaan hallita Aruba AirWave -hallintaohjelmistolla. Ethernet-kaapelointi laitekaapissa toteutetaan standardeilla kaapeleilla, joiden käyttötarkoitukset merkitään eri väreillä. Tämä nopeuttaa eri järjestelmien ongelmien selvittämistä ja selkeyttää laitekaappien järjestystä.

8.2.1 HPE Aruba 2540 PoE+ 4SFP+ -kytkin

HPE Aruba 2540 kytkin on L2-tason kytkin, joka toimii OSI-mallin toisella eli siirtoyhteyskerroksella. Kytkimessä on 24 tai 48 1Gb Ethernet-porttia, joilla kytkin on yhteydessä ristikytkennän, kerroskaapeloinnin ja kytkentärasioiden kautta työasemiin. Kytkimet on yhdistetty toisiinsa 10Gb valokaapeliyhteydellä. Koska kytkimiin on yhdistetty valvontakameroita sekä langattoman verkon tukiasemia, täytyy kytkimellä olla kyky toimittaa edellä mainittuihin laitteisiin virtaa. Tämän varmistaa PoE (Power over Ethernet), jonka avulla tarvittava virta siirretään laitteille Ethernet-kaapelia pitkin. Näin esimerkiksi valvontakameroiden asennus helpottuu, koska erillistä virtalähdettä ei tarvita. Kytkimellä voidaan muodostaa virtuaalisia lähiverkkoja, jolla voidaan lisätä lähiverkon tietoturvaa rajaamalla eri laitteet

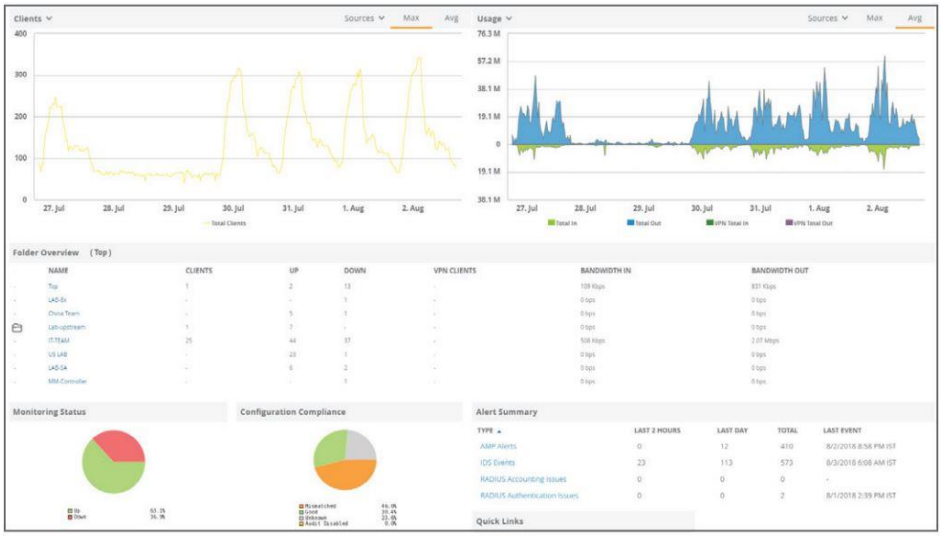
omiin verkkoihinsa. Esimerkiksi kamerat palvelimineen erilleen työasemista ja niiden palvelimesta. (Hewlett Packard Enterprise, n.d.-a) Kuvassa 14 on HPE Aruba 48-porttinen kytkin, jonka vasemmassa laidassa sijaitsevat 10Gb valokuituyhteydet.

Kuva 14. HPE Aruba 48-porttinen kytkin. (Hewlett Packard Enterprise, n.d.-a)

8.2.2 Aruba AirWave -hallintaohjelmisto

Aruba AirWave on verkonhallintaohjelmisto, jolla voidaan hallita useampien toimittajien verkkolaitteita. Ohjelmistolla voidaan hallita kytkimiä, langattoman verkon tukiasemia ja päivittää niitä sekä valvoa verkon liikennettä. AirWaven on mahdollista konfiguroida hälyttämään verkon virheistä ja ongelmista sekä suorittaa proaktiivisia verkon huoltotoimenpiteitä. (Hewlett Packard Enterprise, n.d.-b)

Vaikka AirWave on alun perin tarkoitettu langattoman verkon hallintaan, sillä onnistuu myös langallisen verkon hallinta. Ohjelmisto valittiin Yritys Oyn käyttöön, koska toisen mahdollisen ohjelmiston elinkaari oli lopussa ja yritykseen tarvittiin pidemmän ajan ratkaisua verkonhallintaan. Ohjelmiston langallisen verkon hallinta paranee päivitysten myötä ja sille tulee lisää ominaisuuksia. Kuvassa 15 on AirWaven hallintakonsolin etusivu, josta näkee yhdellä silmäyksellä kytkinten ja konfiguraatioiden tilan.



Kuva 15. Aruba AirWave hallintakonsolin etusivu. (Hewlett Packard Enterprise, n.d.-b)

AirWavessa kytkimien konfigurointeja voi tarkastella ja vertailla eri kytkimien konfigurointeja. Kytkimiä joudutaan silti hallitsemaan vielä komentoriviä käyttäen, koska kytkimen konfigurointi ei onnistu AirWaven käyttöliittymän kautta. Kun valmis konfiguraatio on tehty yhdelle kytkimelle, voidaan se jakaa muihin kytkimiin AirWaven avulla.

8.2.3 Verkon aktiivilaitteiden asennus ja kytkentä

Yritys Oyn tietohallinto konfiguroi ja nimesi tarvittavat kytkimet valmiiksi etukäteen ennen asennusta. Kytkimet on merkitty tarrakirjoittimella tunnistamisen helpottamiseksi. Asennustyöhön osallistui yksi henkilö tietohallinnon puolelta. Uusien kytkimien asennus laitekaappeihin suoritettiin valmistelevana toimenpiteenä ennen varsinaista kytkemistä. Samalla selvitettiin mahdollisia ongelmakohtia, jotka tulisi ottaa huomioon ennen myynnin kannalta kriittisten työasemien liittämistä uusiin kytkimiin.

Itse kytkimien asennus laitekaappeihin oli suoraviivainen operaatio, vaikka laitekaapin järjestystä vaihdettiin. Myymälän lisääntynyt kameravalvonta on vaatinut laitekaappeihin lisää kytkimiä valvontakamerakäyttöön ja työn kohteena olevassa myymälässä oli yhdessä jakamossa kolme erikokoista kytkintä valvontakameroille ja yksi muulle lähiverkolle. Nämä korvattiin kahdella HPE Aruba 2540 -kytkimellä, jotka liitettiin toisiinsa valokaapeliyhteydellä.

Kytkinten toiminta ja liittyminen verkkoon varmistettiin ottamalla yhteyttä komentokehotteen Ping-komennolla (Packet Internet Groper) kytkimen IP-osoitteeseen. Lähiverkkoon liitetyltä tietokoneelta lähetetään kytkimelle vastauspyyntö ja jos kytkin vastaa, se on liittynyt verkkoon. Kuvassa 16 on esimerkki Ping-komennosta. Oletuskomennolla lähetetään neljä vastauspyyntöä TCP/IP-protokollan kautta kohteena olevan laitteen IP-osoitteeseen.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=13ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 4ms

C:\>
```

Kuva 16. Komentokehotteessa suoritettu Ping-komento, jossa kaikki vastauspyynnöt saivat vastauksen.

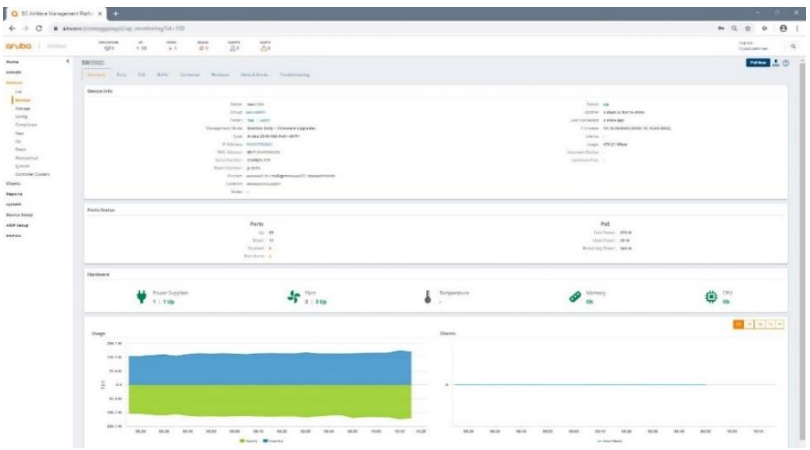
Kytkinten yhteyksien varmistamisen jälkeen kytkettiin valvontakamerat uusiin kytkimiin väliaikaisesti vanhoilla kaapeleilla. D myymälän valvontakameroista osa ei toiminut ennen kytkimen vaihtoa, mutta osa toimimattomina olleista kameroista alkoi toimia uuteen kytkimeen liitettäessä.

Seuraava vaihe, eli asiakaspalvelun kannalta tärkeimmät työasemat, toteutettiin aamulla ennen myymälän avaamista. Etukäteen oli selvitetty kassojen ja palvelutiskin ristikytkentöjen paikat, joten kytkentä onnistui ripeästi ja myymälän aukiolon ulkopuolella. Tämän jälkeen kameroiden vanhat, värikoodaamattomat kaapelit korvattiin värikoodatuilla. Kun kameroita kytkettiin, Aruban kytkin meni virrantoimituksen (PoE) vikatilaan. Samassa kytkimessä olevien kassojen yhteydet toimivat, mutta valvontakameroiden eivät. Tämä korjaantui kytkimen uudelleenkäynnistyksellä, kun varmistettiin, että kassahenkilöstö oli tietoinen lyhyestä katkoksesta.

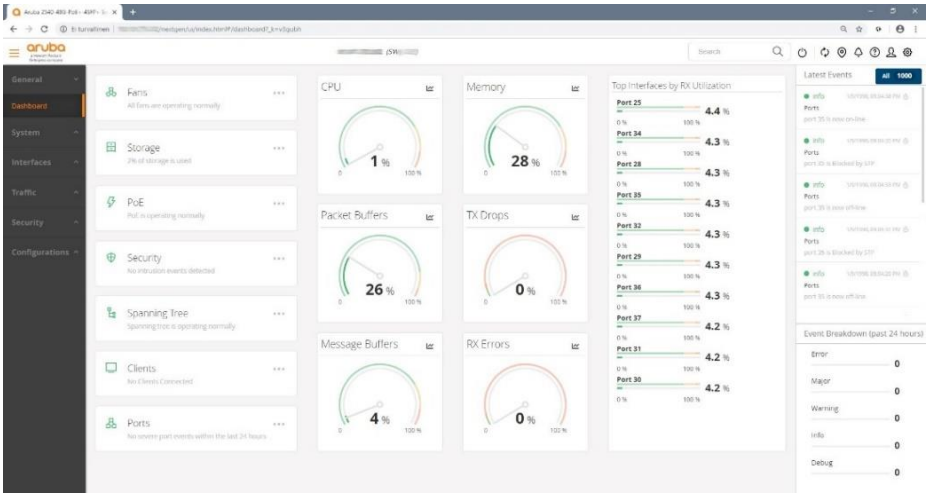
Työasemien ja kameroiden kytkemisen jälkeen suoritettiin muiden toimittajien verkkojohtojen vaihto sekä järkevöitettiin laitekaappien virransaanti. Laitekaappeihin asennettiin uudet varavirtalähteet, joiden tilaa voidaan tarkkailla verkon yli. Vanhat varavirtalaitteet olivat alimitoitettuja uusille kytkimille ja muille laitteille. Kaikki virtajohdot nimettiin tarrakirjoituslaitteella näiden tunnistamisen helpottamiseksi.

8.2.4 Myymälän D kytkinten lisääminen Aruba AirWave -hallintaohjelmaan

AirWaven hallintakonsolin tunnukset saatiin tietohallinnolta ja myymälän kytkimet lisättiin järjestelmään IP-osoitteen perusteella myymälän omaan kansioon. AirWavessa näkee kytkimen perustiedot, tilan, porttien kytkennät ja tilan, virtuaaliset lähiverkot, virrankulutuksen jne. Kuvassa 17 on Myymälän D kerrosjakamo 1 kytkimen perustiedot. Kytkimiä voidaan hallita myös yrityksen verkossa olevalta työasemalta suoraan IP-osoitteen perusteella. Esimerkiksi VLAN-määritykset tulee tehdä suoraan kytkimen kautta, joko komentokehotteella tai IP-osoitteen kautta internet selaimella, ei AirWavessa. Kuvassa 18 on yhteys suoraan työasemalta kytkimeen IP-osoitteella.

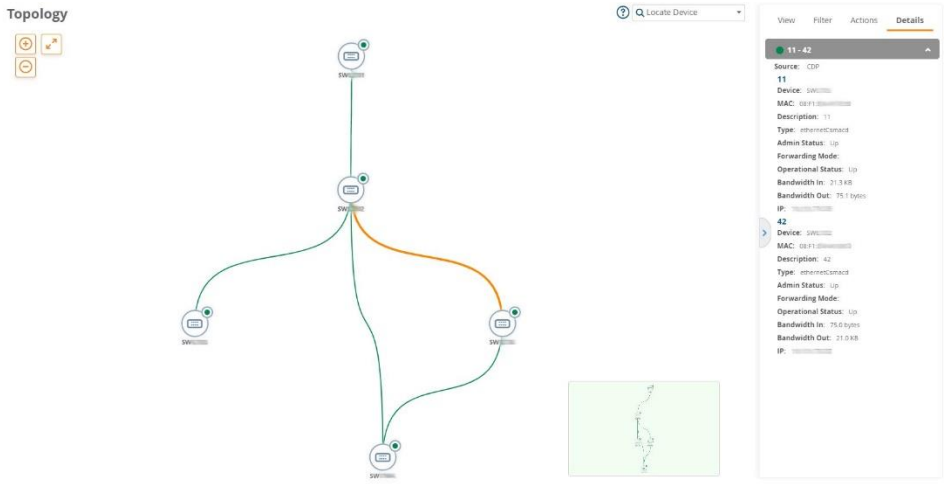


Kuva 17. Kerrosjakamo 1 kytkimen perustiedot AirWavessa.



Kuva 18. Kerrosjakamo 1 kytkimen näkymä suoraan IP-osoitteella.

Verkon looginen rakenne saadaan suoraan hallintaohjelmistosta, jolloin voidaan tarkastella eri kytkinten välisiä yhteyksiä. Asennusten yhteydessä huomattiin, että kaksi kytkintä oli yhteydessä toisiinsa tarpeettomasti, kuten kuvasta 19 voidaan päätellä. Oranssilla värillä näkyy ylimääräinen yhteys kytkinten välillä. Tämä vanha kameraserverin yhteys poistettiin, koska kytkimet yhdistyvät joka tapauksessa valokaapelilla. Näin kytkinten välille ei tule ylimääräisiä yhteyksiä, jotka voivat joissain tapauksissa haitata toimintoja. AirWaven päivitysten myötä mahdollisesti myös muut laitteet saadaan loogisen rakenteen kuvaukseen, jolloin yhdellä silmäyksellä nähdään koko verkon rakenne.



Kuva 19. Verkon looginen rakenne kytkinten osalta.

8.2.5 Dokumentointi

Dokumentointi on tärkeä osa lähiverkon vakiointia. Kunnollisella dokumentaatiolla helpotetaan paikallisen IT-tuen ja tietohallinnon IT-tuen työtä. Kun jokaisen verkkouudistuksen läpikäyneen toimipisteen

dokumentaatio on saatavilla yrityksen intranetistä, voi IT-tuki helposti tarkistaa kytkennät ja laitteet. Näin ollen dokumentaation päivitys on helppoa, kun ne löytyvät yhdestä paikasta toimipistekohtaisesti.

Osana dokumentointia on sähköpiirustukset, joissa näkyy jakamoiden kytkentärimojen yhteydet laiterasioihin, joissa työasemat, kamerat yms. ovat kytkettynä. Kylläkään tämän osalta sähköpiirustukset eivät ole täysin ajan tasalla, koska erilaisia kytkentöjä on jouduttu tekemään jälkikäteen, eikä niitä ole dokumentoitu.

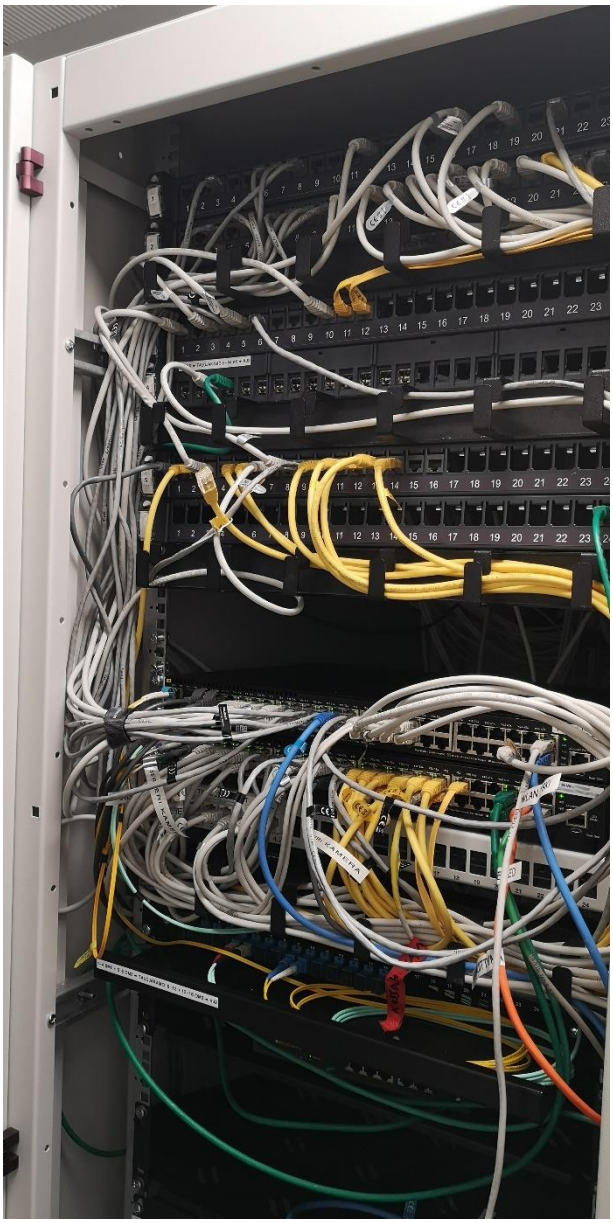
Kuvassa 20 on esitetty malli, jolla kytkennät dokumentoidaan taulukkolaskentaohjelmalla. Taulukossa on esitetty kytkimen nimi, malli, fyysinen sijainti ja IP-osoite. Kytkennät on lueteltu porteittain värikoodattuna laitetyypin mukaan, sijainti ristikytkentäpaneelissa, virtuaalinen lähiverkko (VLAN), fyysinen sijainti sekä lisätieto. Lisätieto on suuntaa antava, koska laitteiden kytkentöjä voidaan joutua muuttamaan ja vaatii päivittämistä.

Kytkin	SWXXXXX				
Malli	HPE Aruba 2540 48 PoE+				
Sijainti	Kerrosjakamo 2				
IP-osoite	XXX.XXX.XXX.XXX				
Porttinro	Laite	Ristikytkentä	VLAN	Sijainti	Lisätieto
1	Liittymä	KJ2 1-3	30		Pääliittymä
2	INY	KJ2 4-24	100	KJ2	Veikkaus
3	WLAN	KJ2 4-23	30	KJ2	Sisäverkko
4					
5	Kamera	KJ2 2-22	40	Kassat	Kassa1
6	Sisäverkko	KJ2 1-3	30	Kassat	Kassa1
7	Kamera	KJ2 2-23	40	Kassat	Kassa2
8	Sisäverkko	KJ2 1-4	30	Kassat	Kassa2
9	Kamera	KJ2 2-24	40	Kassat	Kassa3
10	Sisäverkko	KJ2 1-5	30	Kassat	Kassa3
11					
12	Sisäverkko	KJ2 1-10	30	Palvelu	Tiski1
13	Sisäverkko	KJ2 1-11	30	Palvelu	Tiski2
14	Sisäverkko	KJ2 1-12	30	Palvelu	Tiski3
15	Kamera	KJ2 2-18	40	Palvelu	Tiskit
16					

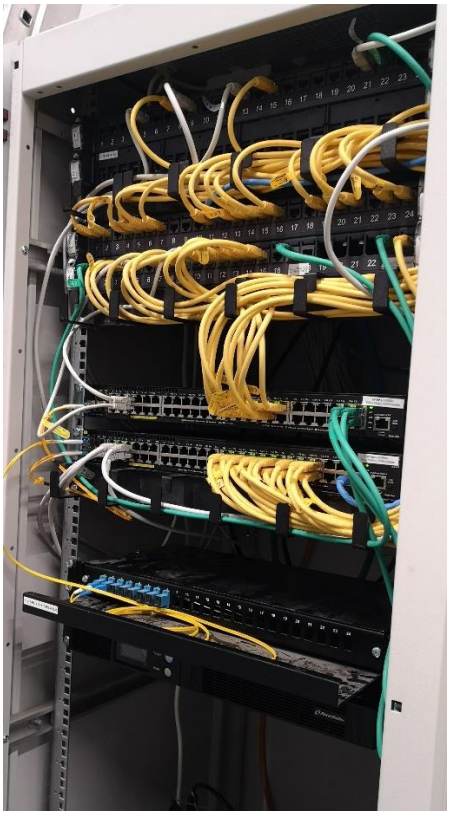
Kuva 20. Kytkimen porttien dokumentointimalli.

9 TULOKSET

Myymälän D verkkolaitteiden uusiminen ja laitekaappien sisällön vakiointi onnistui. Laitekaappien sisältö on yksinkertaistettu ja uusittu kytkimet etähallittaviin HPE Aruba 2540 -kytkimiin. Toimipisteen eri järjestelmät on jaettu omiin virtuaalisiin verkkoihinsa kytkimissä ja verkkoihin liittyvät laitteet on kytketty värikoodauksen mukaisesti. Laitekaapin johdotuksen värikoodausta muutettiin alkuperäisestä suunnitelmasta johtuen myymälässä kolmannen osapuolen käyttämien johdotusten takia. Näin ollen ulkopuolisten toimijoiden Ethernet-johtoja ei tarvinnut vaihtaa. Kuvissa 21-23 on Myymälän D jakamoita uudistuksen jälkeen.



Kuva 21. Myymälän D kerrosjakamo 1 uudistuksen jälkeen.



Kuva 22. Myymälän D kerrosjakamo 2 uudistuksen jälkeen.

Kuva 23. Myymälän D talojakamo uudistuksen jälkeen.

Jo nyt verkon ongelmien selvittäminen on helpompaa laitekaappien selkeyden vuoksi. Eräässä ongelmatapauksessa tietohallinnon IT-tuki lähetti sähköpostilla kuvan laitekaapista, josta vian aiheuttanut erillinen kytkin voitiin helposti tunnistaa ja käynnistää uudelleen ongelman ratkaisemiseksi. Myös toimimattomien valvontakameroiden etsintä verkosta helpottui, koska kameroiden hallintaohjelmasta saadaan toimimattoman kameran MAC-osoite ja sen avulla löydettiin kytkimen oikea portti AirWavesta.

Lähiverkon vakioiminen ja verkkolaiteuudistus ei sujunut täysin ongelmitta. Muutamien kytkentöjen muuttamien aiheutti odottamattomia ongelmia, jotka onneksi saatiin ratkaistua pikaisesti. Tämä oli oman oppimisen kannalta opinnäytetyön parasta antia, kun ongelmaa pääsi itse selvittämään. Jatkossa näihin asioihin osaa kiinnittää huomiota seuraavien toimipisteiden lähiverkon vakioinnissa.

Opinnäytetyössä käytetty lähdemateriaali on osin yli kymmenen vuoden ikäistä. Lähiverkkojen perusperiaatteet ovat kuitenkin säilyneet samoina. Lähinnä tietoliikenteessä oleva tiedonmäärän lisääntyminen on kasvattanut standardien päivityksien myötä verkkojen nopeuksia. Myös verkkojen tietoturva on pääpiirteissään pysynyt muuttumattomana. Dokumentoinnin ja verkonhallinnan osalta kehittyneiden ohjelmistojen käyttö on helpottanut molempia vuosien varrella.

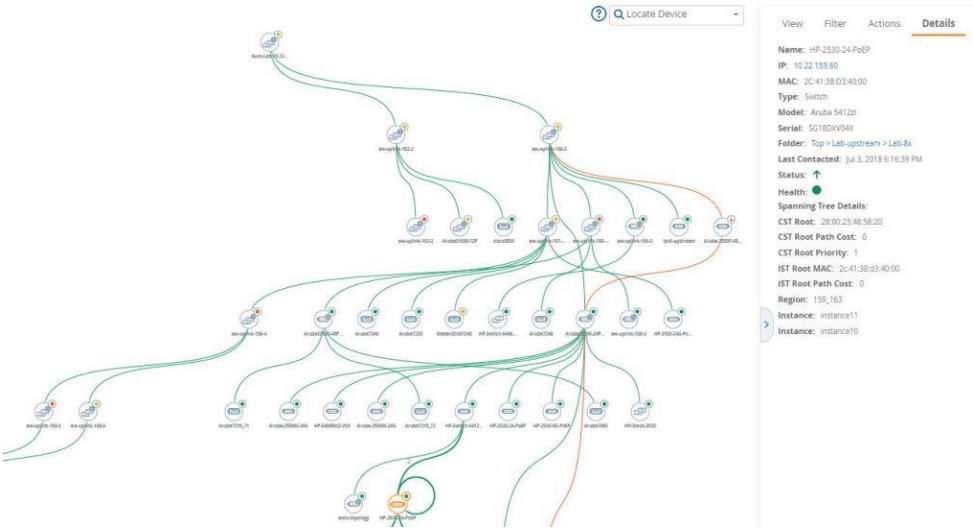
Kyselyn mukaan yhtenä haasteena lähiverkossa pidettiin lisäkoulutuksen tarvetta. Eri toimipisteiden lähiverkon vakioimisen toteutuksen yhteydessä voidaan paikallinen IT-tuki kouluttaa lähiverkon osalta. Paikallisen IT-tukihenkilöiden kanssa voidaan kiertää jakamot, tärkeimmät työasemat, esitellä luotua dokumentaatiota sekä opastaa kytkentöjen tekemisessä.

Tavoitteena on, ettei lähiverkkoon voida lisätä työasemia, tulostimia tai valvontakameroita ilman, että tietohallinnon puolelta avataan kytkimen portti ja liittäisi sen oikeaan virtuaaliseen lähiverkkoon. Näin ollen verkkoon lisätty laite päätyisi suoraan oikeaan virtuaaliseen lähiverkkoon, eikä näin ollen voisi aiheuttaa mahdollisia tietoturvaongelmia. Verkon tietoturva paranee, kun laitteita ei voi kytkeä esimerkiksi vihamielisen tahon toimesta lähiverkkoon.

Kytkinten etähallinnalla päästään näkemään tietohallinnon puolelta porttikohtaisesti, onko kyseinen portti aktiivinen ja lähettääkö se virtaa PoEn kautta. Tällä voidaan rajata ongelma tiettyyn porttiin ja sitä kautta kytkettyyn laitteeseen. AirWave-hallintaohjelmaan voidaan asettaa hälytyksiä, joilla valvotaan esimerkiksi kytkinten toimintaa.

Verkosta olisi hyvä tehdä myös looginen ja fyysinen kuvaus. Koska yrityksellä on yli 30 toimipistettä, olisi dokumentoinnin helpottamiseksi kannattavaa harkita verkon suunnitteluun ja dokumentointiin tarkoitettua ohjelmaa. AirWavessa langattomasta lähiverkosta voidaan luoda loogisia ja

fyysisiä kuvauksia tukiasemien tasolle saakka, kuten kuvassa 24. Tämän ominaisuuden toivoisin tulevan myös langalliselle lähiverkolle päivitysten myötä.



Kuva 24. Aruba AirWaven topologia näkymä. (Hewlett Packard Enterprise, n.d.-b)

10 YHTEENVETO

Opinnäytetyön tavoitteena oli luoda yhtenäinen ohjeistus lähiverkon vakioimiselle. Erikokoiset toimipisteet voidaan mallissa ottaa huomioon, koska malli perustuu laitekaappien sisällön yhtenäistämiseen sekä johdotuksen selkeyttämiseen ja värikoodaukseen. Näin ollen malli on skaalautuva ja voidaan helposti toteuttaa erikokoisissa toimipisteissä.

Lähiverkon hallintamallina olisi paikallisten IT-tukihenkilöiden avustamana tietohallinnon kautta tapahtuva hallinta. Tietohallinto voi hallita kytkimiä ja avata tarvittaessa niiden portteja suoraan oikeaan virtuaaliseen lähiverkkoon. Tämä lisää tietoturvaa, koska ylimääräisiä laitteita ei voida kytkeä lähiverkkoon tietohallinnon tietämättä. Dokumentointi säilytetään Yritys Oyn intranetissä toimipistekohtaisesti ja päivitetään keskitetysti. Myymälän D lähiverkon fyysinen tietoturva on hyvällä tasolla, johtuen toimipisteen iästä. Kulunvalvonta toimii, valvontakameroita on riittävästi ja laitekaapit ovat lukittuja tai sijaitsevat lukitussa tilassa. Muiden myymälöiden tilannetta täytyy tarkastella toimipistekohtaisesti.

Pienessä ajassa on havaittu laitekaappien ja kytkentöjen selkeyttämisellä etuja lähiverkon ongelmien selvittämisessä ja paikantamisessa. Kuka tahansa toimipisteen henkilökunnasta voi tarvittaessa selvittää ongelmia tietohallinnon avustuksella, kun laitekaappien sisältö on selkeä ja tarvittavat kohteet on nimikoitu. Tämä lisää tuottavuutta sekä myymäläympäristössä, että tietohallinnossa, kun aikaa jää muihin toimintoihin. Myymälän IT-tukihenkilöt hoitavat IT-lähituen oman työnsä ohella. Esimerkiksi varastotyöntekijän, joka toimii paikallisena IT-tukihenkilönä, toimitusten purkutehokkuus paranee, kun lähiverkon ongelmien selvitetään nopeammin. Tietohallinnossa puolestaan voidaan keskittyä muihin palvelupyyntöihin. Myös myynnin keskeytykset tulevat lyhentymään.

Oman oppimisen kannalta työ on ollut antoisa. Eniten opin erilaisten ongelmien ja niiden ratkaisemisten kautta. Opinnäytetyö on ollut osa verkkolaitteiden uudistusprojektia, ja tämä on lisännyt ymmärrystä laajemmasta kokonaisuudesta yrityksessä. Projekti on vasta alussa, joten päässen osallistumaan siihen myös jatkossa.

Toiminnassa olevan myymälän verkkoon tehtävät muutokset olisi helpoin järjestää myymälän ollessa suljettu. Tällöin järjestelmien testaaminen vie enemmän aikaa, koska ongelma ei ilmene välittömästi, toisin kuin myymälän auki ollessa. Oman haasteensa lähiverkon vakioimiselle luo myymälöiden lukumäärä. Tietohallinnolla ei ole resursseja suorittaa vakiointia lyhyellä aikavälillä kaikkiin toimipisteisiin. Tähän työhön tulisi osoittaa lisäresursseja, palkata harjoittelijoita tai ulkoistaa työ. Kun malli vakioinnille on luotu, voidaan työ suorittaa myös muiden, kuin tietohallinnon henkilöstön toimesta.

LÄHTEET

Granlund, K. (2007). *Tietoliikenne*. Jyväskylä: WSOYpro.

Hakala, M., & Vainio, M. (2005). *Tietoverkon rakentaminen*. Jyväskylä: Docendo Finland Oy.

Hewlett Packard Enterprise. (n.d.-a). Aruba 2540 48G PoE+ 4SFP+ Switch. Retrieved October 14, 2019, from https://www.arubanetworks.com/products/networking/switches/2540-series/

Hewlett Packard Enterprise. (n.d.-b). Data sheet Aruba AirWave. Retrieved October 20, 2019, from https://www.arubanetworks.com/assets/ds/DS_AW.pdf

Jaakohuhta, H. (2005). *Lähiverkot - Ethernet* (4. painos). Helsinki: Edita Publishing Oy.

Kaario, K. (2002). *TCPIP-verkot*. Jyväskylä: Duocendo.

Valtionvarainministeriö. (2010). Sisäverkko-ohje. Retrieved September 26, 2019, from http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/name.jsp

Vänskä, O. (2012). Nyt se sitten kävi: ipv4-osoitteet loppuivat koko Euroopasta. Retrieved October 2, 2019, from Tietoviikko website: https://www.tivi.fi/uutiset/nyt-se-sitten-kavi-ipv4-osoitteet-loppuivat-koko-euroopasta/f92e160c-73e3-3d30-b524-a971104f66cd

Wendell, O. (2005). *Tietoverkot perusteet* (J. Holttinen, Ed.). Helsinki: Edita Publishing Oy.

Yritys Oy. *Tietohallinto*. , (2018).

Liite 1

KYSELY PAIKALLISESTA LÄHIVERKOSTA

Kysely paikallisesta lähiverkosta

Kyselyn tarkoituksena on selvittää eri myymälöiden lähiverkkoratkaisun tila ja paikallisen IT-tuen mahdollisen koulutuksen tarve.
Kysely toteutetaan anonyyminä, eli vastaajia ja vastauksia ei voida yhdistää.

Teen opinnäytetyötä Hämeen ammattikorkeakoulussa tietojenkäsittelyn koulutusohjelmassa aiheena "Lähiverkon vakiointi yrityksen useassa toimipisteessä käytettäväksi". Opinnäytetyön tarkoituksena on luoda malli ja dokumentointi vakioidulle lähiverkolle verkkohäiriöiden selvittämiseen kuluvan ajan minimoimiseksi ja lähiverkkojen ylläpidon helpottamiseksi.
Itse työskentelen yrityksessä paikallisena IT-tukihenkilönä ja palveluvastaavana.

Kiitos jo etukäteen vaivannäöstäsi!

Jussi Salminen

1. Miten arvioisit paikallisten järjestelmien ja lähiverkon toimivuutta tällä hetkellä?

	1	2	3	4	5
1=ei toimi ... 5=toimii, ei ongelmia	○	○	○	○	○

2. Mitä toivoisit lähiverkolta?

3. Millainen on lähiverkon käytettävyys oman työn näkökulmasta?

	1	2	3	4	5
1=huono ... 5=hyvä	○	○	○	○	○

4. Millaisia haasteita lähiverkossa on tällä hetkellä?

- ☐ Verkko kaatuu
- ☐ IT-tukeen ei saa yhteyttä
- ☐ Päivitysten jälkeen verkko ei toimi odotetusti
- ☐ Lisäkoulutuksen tarve
- ☐ Mahdollisen ongelman selvitys kestää
- ☐ Joku muu, mikä?

5. Tunnen oman yksikköni lähiverkon rakenteen

- ◯ Kyllä
- ◯ En

6. Hallitsen lähiverkon tietoturvan perusteet

- ◯ Kyllä
- ◯ En

7. Arvioi tällä hetkellä lähiverkon ongelmien selvittämiseen kuluva aika

- ◯ 0 - 10 min
- ◯ 11-30 min
- ◯ 31- 60 min
- ◯ yli 60 min

8. Mitä ajatuksia lähiverkon käytäntöjen yhtenäistäminen/vakioiminen herättää?

9. Kuulun

- ◯ Paikalliseen IT-tukihenkilöstöön
- ◯ Tietohallintoon
- ◯ Muuhun

Lähetä