

Opinnäytetyö AMK

Tieto- ja viestintäteknikka

2022

Ville Helander

Teollisuusyrityksen lähiverkon dokumentointi

Ville Helander

Teollisuusyrityksen lähiverkon dokumentointi

Toimiva lähiverkko on yrityksen kannalta kriittinen, ja vikatilanteiden ilmaantuessa voi tulla merkittäviä kustannusvaikutuksia. Pahimmillaan pitkäkestoinen verkkovika altistaa tuotannon laitteet häiriöille, sekä, vaarantaa ympäristö- ja työturvallisuutta. Myös lähiverkon ja sen laitteiden tietoturva kärsii, mikäli verkko on huonosti suunniteltu.

Tämän opinnäytetyön tavoitteena oli luoda selkeä dokumentaatio ja kuvata nykytila yrityksessä käytössä olevan tieto- ja automaatioverkkojen rakenteesta sekä tehdä suunnitelma lähiverkon turvallisuuden ja vikasietoisuuden parantamiseksi.

Opinnäytetyö tehtiin tutkimalla lähiverkkoa, sen rakennetta sekä laitteita. Apuna käytettiin yritykseltä saatua dokumentaatiota sekä haastatteleamalla yrityksen IT-osaston työntekijöitä. Lähiverkon jokaisella IP-alueella ajettiin ARP -skannaus, jolla saatiin selkeä kuva lähiverkon laitteiden määrästä. Kytкимиä tarkkailemalla pystyttiin havainnoimaan kuormamääriä.

Saavutetut tulokset antoivat selkeän kuvan verkon laitteista ja rakenteesta sekä toivat esiin kehityskohteita. Opinnäytetyötä tehdessä havaittiin myös se, että valmista isoa verkkoa on huomattavasti monimutkaisempaa suunnitella kuin aloittaa verkon suunnittelu alusta. Tätä vaihtoehtoa ei ollut käytettävissä tässä opinnäytetyössä.

ASIASANAT:

Lähiverkko, dokumentointi, tietoverkko

BACHELOR'S THESIS

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information and Communications Technology

2022 | 23 pages

Ville Helander

Documentation of an industrial company lan

A functional local area network is critical for a company and when the fault situations occur, there may be significant cost effects. At its worst, a long-lasting failure exposes production equipment to interference, and endangers environmental and occupational safety. The security of the local area network and its equipment will also suffer if the network is poorly designed.

The aim of this thesis was to create a clear documentation and to describe the current state of the structure of information and automation networks used in the client company and to make a plan to improve the safety and faults of the local area network.

The thesis was carried out by examining the local are network, its structure and equipment. The documentation from the company was used and the company's IT department employees were interviewed. An ARP scan was conducted in each IP area of the local area network, which provided a clear picture of pieces of equipment in the local area network. By observing the switches, the amounts of loads were observed.

These findings provided a clear picture of the network's equipment and structure, and highlighted areas for improvement and these were documented.

KEYWORDS:

Local area network, documentation, network

SISÄLTÖ

KÄYTETYT LYHENTEET	5
1 JOHDANTO	6
2 LÄHIVERKON MÄÄRITELMÄ	8
2.1 Lähiverkon historia	8
2.2 Lähiverkon laitteet	8
2.3 Lähiverkon kaapelit	9
2.4 Langaton lähiverkko	11
3 YRITYKSEN LÄHIVERKKO	12
3.1 Automaatioverkot	13
3.2 Automaatioverkon laitteet	14
3.3 Tehdasverkko	15
3.4 Tehdasverkon vikasietoisuus	16
3.5 Verkon segmentointi	17
3.6 Segmentoinnin huonot puolet	18
3.7 Segmentoinnin hyvät puolet	18
3.8 Suunnitelma yrityksen verkon parantamiseksi	19
4 LOPUKSI	20
5 LÄHTEET	21

KÄYTETYT LYHENTEET

CAT6	Category 6, kategoria 6
LAN	Local Area Network, lähiverkko
RSTP	Rapid spanning tree protocol, nopea datanvälityssilmukoiden muodostumista ehkäisevä protokolla
STP	Spanning tree protocol, datanvälityssilmukoiden muodostumista ehkäisevä protokolla
VLAN	Virtual local area network, virtuaalinen lähiverkko
WLAN	Wireless local area network, langaton lähiverkko

1 JOHDANTO

Nykyäänkin vielä käytetään yrityksissä paljon erilaisia lähiverkkoja. Myöskään erilaisten pilvipalveluiden lisääntynyt tarjonta ei ole poistanut perinteisen lähiverkon tarvetta. Internetin käyttö yritysten työasemista on ollut arkipäivää jo vuosikymmenet, ja erilaiset tietoturvaohjelmat horjuttavat yritysten verkkoja. Pahimmillaan yrityksen huonosti suunniteltu lähiverkko asettaa erilaiset tuotantonohjausjärjestelmät sekä yrityssalaisuuksia sisältävät asiakirjat suoraan kenen tahansa saataville. Vuosikymmenten kuluessa reilusti laajentunut lähiverkko sekä tuotannon ja erilaisen toimistotyön liittyminen yhä enenemissä määrin verkkoon ja internetiin toi myös tarpeen tehdä perusteellinen selvitys yrityksen lähiverkon nykytilasta.

Erilaisia selvityksiä on tehty lukuisia vuosien aikana eri yrityksissä ja yhtä oikeaa tapaa lähiverkon konfigurointiin ei koskaan ole ja myös jokaisessa yrityksessä on erilaisia vaatimuksia.

Tämän opinnäytetyön tarkoituksena oli tehdä yrityksen lähiverkosta selvitys, jonka pohjalta voidaan tehdä suunnitelma verkon päivittämiseksi. Verkon päivittämisen tarkoituksena on saada yrityksen lähiverkko turvalliseksi, toimintavarmaksi sekä skaalautuvaksi tulevaisuuden tarpeita varten. Koska verkkoa ei suunnitella alusta asti, ei myöskään dokumentaatiota tehdä muuta kuin segmentoinnin ja vikasietoisuuden osalta.

Työ aloitetaan kartoittamalla verkon nykytila ja tekemällä vertailua siihen, miten verkon tahdotaan tulevaisuudessa toimivan. Työtä jatketaan selvittämällä lähiverkon laitteiden kytkennät ja konfiguroinnit. Näiden tulosten pohjalta pohditaan nykytilan hyviä ja huonoja puolia. Näistä tuloksista muodostetaan yritykselle dokumentti, jota yritys voi käyttää verkon päivittämiseen.

Tietoa kerättiin yrityksen dokumentaatiosta, paikan päältä tutkimalla ja haastatteleamalla yrityksen IT-osaston työntekijäitä, sekä erilaisin verkkoskannauksin. Näiden pohjalta tehtiin päätelmiä, miten verkko kannattaa päivittää sekä miten segmentointi lisäisi verkon hallittavuutta sekä turvallisuutta.

Lähteenä on käytetty alan kirjallisuutta ja yrityksen nykyistä dokumentaatiota. Osa opinnäytetyön kuvista on poistettu toimeksiantajan pyynnöstä.

2 LÄHIVERKON MÄÄRITELMÄ

Lähiverkolla tarkoitetaan yrityksissä tai kotitalouksissa olevaa, reunapalomuurin tai reunareitittimen takana olevaa verkkoa, johon on kytketty useita erilaisia tietoliikennettä tuottavia laitteita. Lähiverkko mahdollistaa laitteiden kytkeytymisen erilaisiin sisäisiin palvelimiin sekä muihin lähiverkkoihin Internetin yli. [1]

2.1 Lähiverkon historia

Tohtori Robert Metcalfen kehittäessä vuonna 1973 konseptin, jossa liitettiin koaksiaalikaapelilla tietokoneita ja maailman ensimmäinen Xeroxin valmistama lasertulostin yhteen, hän keksi nimen Ethernet. Tämä Ethernet mahdollisti pakettien lähettämisen sitä pitkin tietokoneista toiseen sekä tulostimeen. Tätä voidaan pitää nykyisen lähiverkon syntynä. Toisaalta ensimmäisen kaupallisen lähiverkon nimellä asennetun verkon asensi Datapoint yhtiö Chase Manhattan pankille New Yorkissa 1977. Tämä kaupallisen verkon toiminta perustui tunnusväälittämiseen, jolla vältettiin tohtori Robert Metcalfen konseptissa tapahtuvat datapakettien törmäykset. Lähiverkon yleistymisen alkoi vuonna 1983 ja lähiverkon standardiksi muodostui IEEE 802 vuonna 1985. [2]

2.2 Lähiverkon laitteet

Lähiverkot sisältävät mm. kaapeleita, kytkimiä, reitittäjiä sekä muita laitteita joiden avulla päätelaitteet muodostavat yhteyden toisiinsa sekä verkon erilaisiin palveluihin. Laitteet muodostavat yhteyden parikaapelilla, kuitukaapelilla tai langattomasti. Kuvassa 1 esitetään Ubiquitin valmistamia lähiverkkolaitteita. [1]



Kuva 1. Ubiquitin valmistamat lähiverkon kytkimet sekä palomuri. [3]

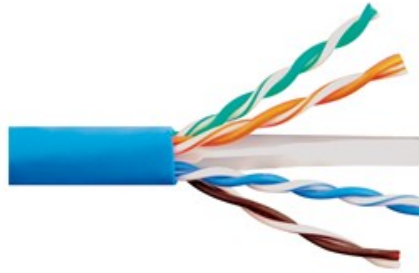
2.3 Lähiverkon kaapelit

Enimmäkseen lähiverkossa käytetään kaapelointina EN 50173 standardin mukaisia parikaapeleita. Kaapelit ovat STP (kuva 2) tai UTP (kuva 3) tyyppisiä. STP eli shielded twisted pair-tyyppiset kaapelit ovat paremmin suojattu ympäristön säteilyjä vastaan.

Nykyään käytetään CAT6-, CAT6a- ja CAT7-kategorioiden kaapeleita. Nämä kaapelit mahdollistavat jo 10 Gt:n siirtonopeuden. CAT6 mahdollistaa 10 Gt:n siirtonopeuden 55 m:iin saakka ja CAT6a ja CAT7 100 m:n matkalle. Taulukossa 1 näkyy yhteenvetona nykyisten Ethernet-kaapeleiden kategorioita ja niiden eroavaisuuksia.



Kuva 2. CAT6 STP kaapeli [4]



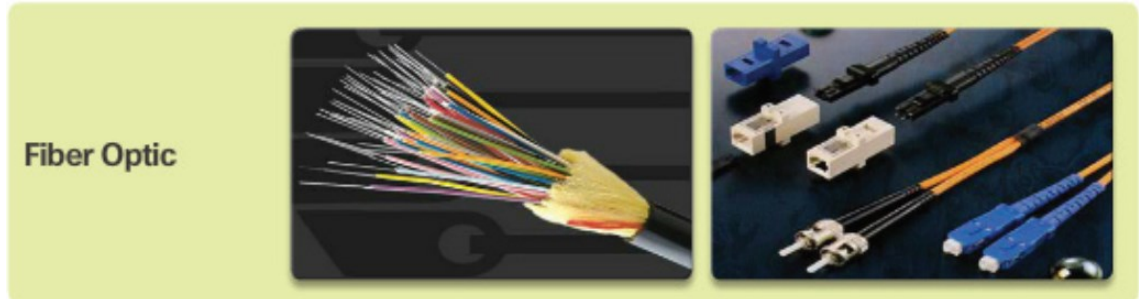
Kuva 3. Cat6 UTP kaapeli [5]

Taulukko 1. Tietoa yleisimmistä Ethernet-kaapeleista.

Kategoria	Kaistan- leveys	Nopeus	Pituus	Liitäntä
CAT6	250 MHz	10Gbps	100m (1Gbps) 55m (10Gbps)	RJ45
CAT6a	500 MHz	10Gbps	100m	RJ45
CAT7	600 MHz	10Gbps	100m	GG45

Tietoa voidaan siirtää myös kuitukaapeleita pitkin. Kuitukaapelit koostuvat ohuista lasi- tai muoviputkista joissa valo etenee valonnopeudella pulsseittain.

[6]



Kuva 5. Kuitukaapeleita erilaisilla liittimillä [6]

Kuitukaapeleiden etuna tavallisiin Ethernet-kaapeleihin on niiden häiriöttömyys sähkömagneettisille kentille sekä yksittäisen vedon pituus. Teollisuusympäristössä matkat voivat olla pitkiä sekä sähkökäyttöisille isoille tuotantolaitteille tulee isoja sähkökaapeleita joista voi syntyä sähkömagneettisia kenttiä.

2.4 Langaton lähiverkko

Langaton lähiverkko eli WLAN toimii kuten langallinen, mutta ilmateitse sähkömagneettisen säteilyn avulla. WLAN käyttää 2,4 GHz:n sekä 5 GHz:n taajuuksia yhteytenä. Nykyään on käytössä enimmäkseen 802.11n- ja 802.11ac-standardien mukaisia laitteita. [7]

WLAN tarjoaa helpon tavan tuoda lähiverkko saataville usealle asiakkaalle samalla kerralla. Useamman tukiaseman ympäristössä pitää kiinnittää huomiota päällekkäisiin kanaviin, jotta langaton lähiverkko toimisi mahdollisimman hyvin.

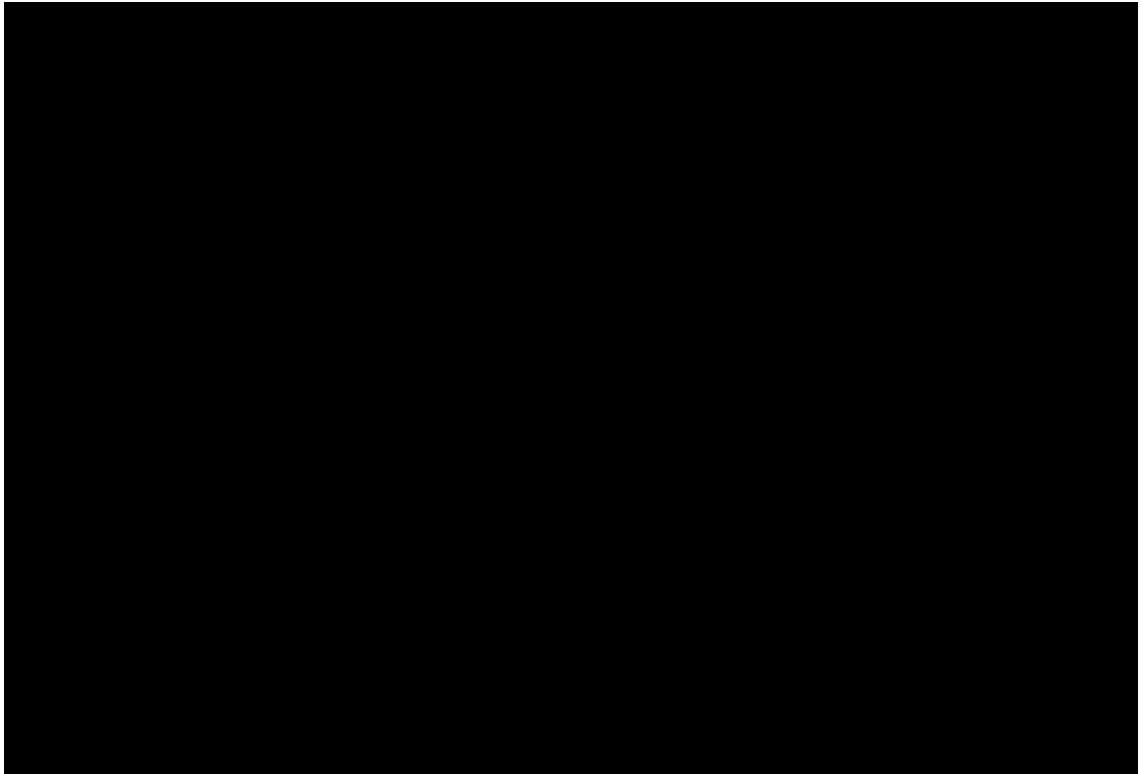
[8]

3 YRITYKSEN LÄHIVERKKO

Yrityksen lähiverkossa on käytössä useita eri IP-alueita. IP-alueet ovat kooltaan /24 verkkoja joten yhteen verkkoon on käytettävissä 254 eri osoitetta. Laitteiden määrän kasvaessa on uusia ip-alueita otettu käyttöön. Verkkojen kokoa ei kuitenkaan ole kasvatettu vaan uudet verkot ovat myös /24 kokoisia. Samassa verkossa voi olla tietokoneita, palvelimia, IOT-laitteita ja tulostimia. Verkoista on pääsy internetiin palomuurin läpi ja laitteet voivat keskustella toisensa kanssa, eikä verkkoja ei ole segmentoitu tietoturvan kannalta mitenkään.

Lähiverkossa on käytössä erilaisia kytkimiä, joilla eri osastojen laitteet on liitetty toisiinsa. Nykyinen lähiverkko (kuva 6) ja IP-alueet toimivat kaikki yhteen, eikä lähiverkkoa ole segmentoitu mitenkään erottelemalla eri tyyppiset laitteet toisistaan. Nykyisellään lähiverkko toimii kyllä hyvin, eikä uusia laitteita lisätessä tarvitse juuri miettiä miten ne verkkoon kytkeytyy. Myös vikaantuneen kytkimen vaihto on helppo tehdä sekä uudet fyysiset kytkennät, kun ei erillisiä kytkimien porttikonfiguraatioita tarvita. Huonona puolena tällaisessä verkossa on se, että kaikkien laitteiden hallintaportaalit ovat myös samassa verkossa ja kaikkien verkon käyttäjien saavutettavissa. Vaikka hallintaportaalit on suojattu salasanoilla, voi laitteissa olla tietoturva-aukkoja, jotka mahdollistavat laitteen hallintaportaaliiin pääsyn myös niiltä kenellä ei siihen normaalisti oikeuksia ole. Tällaisia aukkoja myös erilaiset haittaohjelmat käyttävät hyödykseen. Mahdollisessa vikatilanteessa tai verkon asiakkaiden selvittäminen on hankalampaa, koska ARP-kyselyt eivät välity kuin layer 2-tasolla, jolloin eri ip-alueella olevia laitteita ei havaita.

Automaatioverkkojen laitteet on fyysisesti erotettu tehdasverkosta, joten tehdasverkon ja automaatioverkon sekoittuminen ei ole suurena vaarana.



Kuva 6. Yritykseltä saatu kuva verkon fyysisestä topologiasta.

3.1 Automaatioverkot

Tuotannonohjausjärjestelmät toimivat omissa fyysisissä verkoissaan, joihin ei ole suoraa pääsyä mistään yrityksen verkoista. Automaatioverkot on segmentoitu ja eristetty suoralta pääsylvä tehdasverkosta. Automaatioverkkoihin pääsee ainoastaan erillisen palomuurin läpi, johon on määritetty sallitut ip-osoitteet. Automaatioverkkoihin ei ole monellakaan käyttäjällä tarvetta päästä. Automaatioverkko tulee laitteiston toimittajalta, joten tässä työssä ei tutkita niitä kovinkaan syvällisesti.

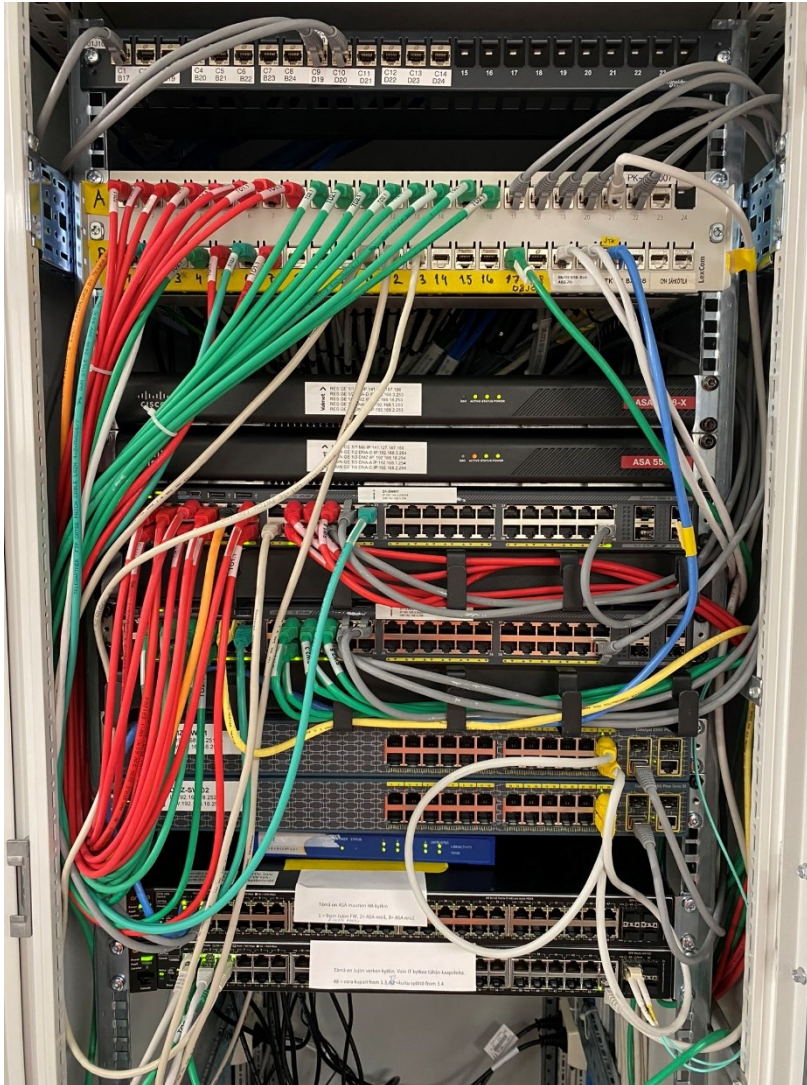
Automaatioverkon toimivuus on kriittinen, koska se ohjaa tuotannon laitteita ja rikkoutuessaan voi aiheuttaa merkittäviä taloudellisia haittoja. Myös työturvallisuus, sekä ympäristöturvallisuus voi kärsiä automaatioverkon toimintahäiriössä.

Automaatioverkot on rakennettu vikasietoisiksi ja yhden lähiverkon laitteen, esimerkiksi kytkimen rikkoutuminen ei aiheuta vielä suurta haittaa.

Automaatioverkon valvonta tapahtuu pääsääntöisesti laitteen toimittajan kautta, eikä yritykseen ole rakennettu automaatioverkon valvonnalle mitään tarkoitukseen mukaista valvontaa. [9]

3.2 Automaatioverkon laitteet

Automaatioverkon laitteet koostuvat eri-ikäisistä, yleensä Ciscon valmistamista laitteista. Laitteina on eri kokoiset kytkimet sekä ASA-palomuurit.



Kuva 7. Automaatioverkon laitteita rakkikaapissa.

3.3 Tehdasverkko

Tehdasverkolla tarkoitetaan yrityksen muuta verkkoa paitsi automaatioverkkoa. Tehdasverkkoon on kytketty yrityksen palvelimet, työasemat, tulostimet sekä IOT-laitteet. Tehdasverkko on tehty ethernet-kaapeleilla sekä monimuotokuiduilla. Kuidun etuna on pidemmät vetomatkat, mikä on hyödyksi teollisuuslaitoksessa kun välimatkat ovat pitkiä. Tehdasverkkoa käytetään myös langattomilla laitteilla, joten yritykseen on tehty langaton verkko toimimaan 2,4 GHz sekä 5 GHz taajuuksilla. Langaton verkko muodostetaan 802.11n ja 802.11ac standardien mukaisilla tukiasemilla. Langattomia asiakkaita ei ole merkittäviä

määriä, mutta niiden toimivuus on kuitenkin tärkeää yrityksen toiminnan sujuvuuden varmistamiseksi.

3.4 Tehdasverkon vikasietoisuus

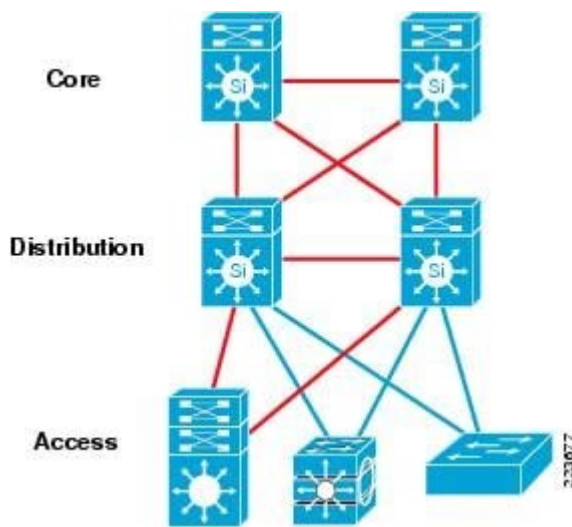
Tehdasverkon suunnittelun lähtökohtana ei ole ollut vikasietoisuus osittain rakennuksen koon, iän sekä tarpeen vuoksi. Suunnittelussa ei myöskään ole ollut aina käytettävissä tarvittavaa osaamista verkkotekniikkaan. Myös eri-ikäiset kytkimet tuovat haasteita suunnitteluun.

Verkossa on käytössä spanning tree -protokolla, jolla saadaan ohjattua liikennettä haluttujen kytkimien kautta. [9] Viime aikoina on lisätty myös kaapelointeja, joilla on saavutettu joitain vikasietoisia reittejä, mutta määrä on kokonaisuudessaan kuitenkin sen verran pieni, ettei niillä saada koko verkkoa vikasietoiseksi.

Vikasietoisuuden parantamiseksi voidaan ottaa eri lähtökohtia. Vikasietoisuutta voidaan parantaa lisäämällä kytkimiä, lisäämällä kaapelointeja kytkinten väliin tai tekemällä näitä molempia. Paras vikasietoisuus saadaan, kun tehdään näitä molempia ja lisätään kytkimiä sekä kaapelointeja niin paljon, että saadaan tehtyä verkko kuvassa 8 näkyvän Ciscon 3-kerrostoimintamallin mukaan. Tässä toimintamallissa on looginen verkko jaettu kolmeen eri kerrokseen ja kerroksien väliset reitit ovat vikasietoisia. [10]

Vikasietoiseen verkkoon pitää konfiguroida käyttöön RSTP eli Rapid Spanning Tree Protocoll. RSTP:llä voidaan konfiguroida päälinja, jota käytetään normaalissa tilanteessa, sekä varalinja, joka voidaan ottaa käyttöön mikäli yhteys päälinjassa menee poikki. Tällaisessä käytössä pitää huomioida verkon kuorma, ettei itse linjanopeus tule pullonkaulaksi. Myös kaikkien kytkimien pitää tukea RST -protokollaa jotta ominaisuus on käytössä koko verkossa ja toimii kuten on tarkoitettu. [11]

Spanning Tree -protokollasta on olemassa myös muita variaatioita, mutta tässä työssä ei paneuduta muihin versioihin.

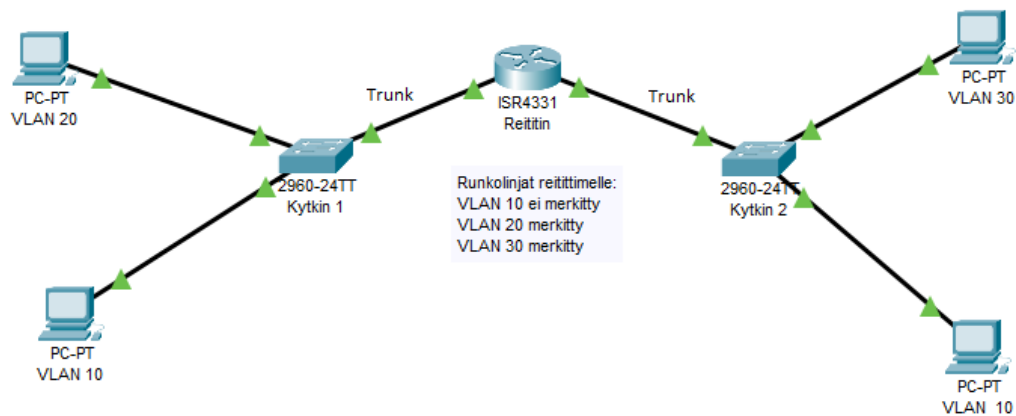


Kuva 8. Cisco 3 - tier toimintaperiaatekuva. [10]

3.5 Verkon segmentointi

Yhtenä merkittävänä turvallisuutta lisäävänä tekijänä voidaan pitää verkon segmentointia. Loogisen topologian segmentoinnilla tarkoitetaan verkkojen jakamista eri verkkoihin riippumatta siitä missä verkko fyysisesti sijaitsee. Tämä tehdään VLAN, eli virtuaalilähiverkko tekniikalla. Virtuaalilähiverkon käyttöönotto vaatii tuen kaikilta kytkimiltä, sekä reitittimiltä. Segmentoinnin jälkeen voidaan reittejä määrittellä reitittimiltä sekä kytkimiltä. Virtuaalisia lähiverkkoja voidaan konfiguroida 4096 kappaletta, jolloin niiden käytöllä voidaan tehdä hyvinkin monimutkaisia verkkoja. Kuvassa 9 esitetään eri VLAN verkkojen kulkua lähiverkossa. Trunk-linjaa pitkin kulkevat kaikki eri VLAN:t ja kytkimiltä 1 ja 2 kulkevat vain erikseen asetetut VLAN:t [12]

Hallittaviin kytkimiin voidaan määrittellä portteja, joissa on sallittu vain tietty tai tietyt virtuaaliset lähiverkot. Portteja voidaan myös konfiguroida trunk eli runkoportiksi, jolloin kaikki erinumeroiset virtuaalilähiverkot voivat edetä siinä. Virtuaaliverkon tunnus lisätään Ethernet-kehykseen, jonka perusteella kytkin tunnistaa sen. [12]



Kuva 9. Virtuaaliset lähiverkot fyysisessä verkossa.

3.6 Segmentoinnin huonot puolet

Segmentoinnin huonona puolena voidaan pitää verkon monimutkaistumista sekä hallinnan vaikeutumista. Segmentointin ollessa käytössä, pitää verkon hallintaa viedä kytkinten porttitasolle. Mikäli verkkoyhteys menee toiseen aliverkkoon pitää tiedustella reitittimeltä saakka, jolloin kuorma verkossa kasvaa enemmän.

3.7 Segmentoinnin hyvät puolet

Segmentoinnilla pystytään turvallisesti erottelemaan eri verkkojen liikenne toisistaan. Tietyissä tapauksissa on tärkeää, että eri verkkojen liikenne ei sekoitu, eikä verkosta toiseen ole pääsyä automaattisesti. Esimerkiksi eri laitteiden hallintaportaalien liikenne on hyvä laittaa omaan virtuaaliverkkoon, jonka jälkeen voidaan luoda palomuurisäännöt, joilla sallitaan vain tietyistä ylläpidon koneista pääsy hallintaverkkoon.

Erikokoisten virtuaaliverkkojen lisäys onnistuu helposti, kun verkot eivät ole riippuvaisia toisistaan. Hyvänä puolena voidaan pitää koko verkon turvallisuuden parantumista. Kun verkko on järkevästi ja tarkoituksenmukaisesti segmentoitu, mahdollisessa tietomurrossa ei päästä kaikkiin verkkoihin käsiksi. Myöskään

haittaohjelmat ja tiedostoja kryptaavat madot, eivät pääse kaikkiin tiedostoihin käsiksi.

3.8 Suunnitelma yrityksen verkon parantamiseksi

Tutkittuani yrityksen verkkoa sekä päätelaitteita, selvisi, että vaikka yrityksen verkon toimivuus on tärkeää, ei sitä ole kuitenkaan huomioitu suunnittelussa kovinkaan tarkasti. Verkko on laajentunut tarpeen mukaan ilman vikasietoisuuden lisäämistä. Tämä on toisaalta ollut helppo sekä kustannustehokas tapa. Yrityksen toimitilat ovat kuitenkin isot ja välimatkat kasvavat helposti, jolloin kaapeleiden veto on hankalampaa sekä kalliimpaa. Myöskään tehdasverkossa jonkin alueen katkos esimerkiksi johdon katkeamisen seurauksena, ei aiheuta välitöntä tuotannon menetystä eikä muutakaan välitöntä vakavaa haittaa.

Verkon parantaminen kannattaa aloittaa uusimalla vanhimpia kytkimiä uusiin sekä päivittämällä alle 1 Gb/s linjat nopeammiksi. Kytkimiä tulisi lisätä vikasietoisuuden parantamiseksi. Verkon segmentointi ottamalla virtuaaliset lähiverkot käyttöön, pitäisi suunnitella tarkasti myös tulevaisuuden tarpeita pohtien. Tietoturvaan tulisi panostaa ja verkon reititys miettiä tarkasti. Tärkeää olisi erottaa kaikkien kytkimien ja muiden verkkolaitteiden hallintaverkko johon on rajattu pääsy.

Aliverkotus tulisi suunnitella uudelleen käyttäen siihen varattuja standardin RFC-1918 osoitteistoa. Nämä osoitteet eivät reitity lähiverkon ulkopuolella. Kytkinten lukumäärä on sen verran iso, että niiden yhteinen kontrolleri helpottaisi myös asetusten tekoa. [13]

Loogisen topologian piirtäminen helpottaisi vikatilanteiden selvitystä. Looginen topologia piirretään toimeksiantajalle kun toimeksiantajan kanssa on saatu tehtyä VLAN jaottelut. Opinnäytetyötä tehdessä ei tämä jaottelu valmistunut, joten sitä ei voida liittää keskeneräisenä työhön. Rakkikaappien ristikytkennät olisi hyvä merkitä selkeästi ja rakkikaapit järjestellä siten, että olisi selkeästi näkyvillä kytkimen portit ja ristikytkentäpaneeli.

4 LOPUKSI

Työn tavoitteeksi otettiin tehdasverkon nykytilanteen dokumentointia, sekä uudelleensuunnittelu. Tehdessäni tätä työtä huomasin kuitenkin, että koko verkon uudelleen suunnittelu vaatisi enemmän aikaa kuin on järkevää käyttää tässä työssä. Myöskään koko verkon uudelleensuunnittelun toteutus ei onnistu kerralla, tuotannon luonteen vuoksi. Tästä johtuen otettiin työn tarkoituksiksi saada verkon rakenteesta selkeä alkutilanne ja löytää nykyisen verkon hyvät ja huonot puolet.

Työn tulosten perusteella voidaan verkon uudelleensuunnittelua jatkaa, nykytilanteen ollessa hyvin selvillä. Hyvänä puolena nykytilanteessa on uusien laitteiden tuonti verkkoon sekä kytkinten konfigurointien vaivattomuus. Myös laajennus on helppoa lisäämällä kytkimiä ja liittämällä nämä suoraan olemassa oleviin kytkimiin.

Verkon segmentointi toisi hyviä etuja nimenomaan tietoturvamielessä. Segmentoitujen verkkojen välinen liikenne kulkisi palomuurin kautta, jolloin liikenteen rajoituksia pystyisi käyttämään. Samalla myös erilaisia tietoturvatarkastuksia liikenteelle olisi mahdollista tehdä. Kaikki verkon laitteet eivät myöskään tarvitse pääsyä internetiin, jolloin laitteiden rajaus toisi myös tietoturvaa lisää.

Tämän työn jälkeen on selkeämpää lähteä toteuttamaan verkon päivitystä tekemällä taulukon, jossa ilmenee eri segmentoidut virtuaalilähiverkot, niiden reitit sekä ip-avaruudet. Haastavin työ on erotella verkon eri asiakkaat oikeisiin virtuaalilähiverkkoihin. Myös matkat eri kytkinten välillä on pitkiä eikä kaapeleiden veto aina ole helppoa teollisuusympäristössä.

5 LÄHTEET

- [1] Cisco, "What is a lan," 2022. [Online]. Available: <https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html#~what-it-is>. [Haettu 14 Tammikuu 2022].
- [2] CompTIA, "What is local area network," 2022. [Online]. Available: <https://www.comptia.org/content/guides/what-is-a-local-area-network>. [Haettu 14 Tammikuu 2022].
- [3] Ubiquiti, "Marketing material," Ubiquiti, 7 Toukokuu 2022. [Online]. Available: <https://www.ui.com/marketing/#unifi-switch>. [Haettu 7 Toukokuu 2022].
- [4] ComputerCableStore, "1000ft cat6 shielded network cable solid stp blue riser cmr pvc," ComputerCableStore, 7 Toukokuu 2022. [Online]. Available: <https://www.computercablestore.com/1000ft-cat6-shielded-network-cable-solid-stp-blue-riser-cmr-pvc>. [Haettu 7 Toukokuu 2022].
- [5] ComputerCableStore, "solid cat6e utp 350 mhz riser cable blue 1000ft," ComputerCableStore, 7 Toukokuu 2022. [Online]. Available: <https://www.computercablestore.com/solid-cat6e-utp-350-mhz-riser-cable-blue-1000ft>. [Haettu 7 Toukokuu 2022].
- [6] Cisco, "Introduction to Networks v6 Companion Guide," tekijä: *Introduction to Networks v6 Companion Guide*, Indiana, Cisco Press, 2022, pp. 44-45.
- [7] W. D. A. Coleman David D., CWNA Certified Wireless Network Administrator Study Guide, 6th Edition, Sybex, 2021.
- [8] Metis Oy, "WLAN 2,4 GHz taajuusalueen käyttö," Metis Oy, 3 Tammikuu 2018. [Online]. Available: <https://metis.fi/fi/2018/01/2dot4-kanavat/>. [Haettu 21 Toukokuu 2022].
- [9] IT-päällikkö, Interviewee, *Automaatioverkot yrityksessä*. [Haastattelu]. 28 Maaliskuu 2022.
- [10] Cisco, "CCNP and CCIE Enterprise Core Official Cert Guide," tekijä: *CCNP and CCIE Enterprise Core Official Cert Guide*, Kalifornia, Cisco Press, 2020, p. 597.
- [11] Cisco, "CCNP and CCIE Enterprise Core Official Cert Guide," tekijä: *CCNP and CCIE Enterprise Core Official Cert Guide*, Kalifornia, Cisco Press, 2020, pp. 52-53.
- [12] E. J. Seifert Rich, *The All-New Switch Book: The Complete Guide to LAN Switching Technology*, Second Edition, John Wiley & Sons, Inc, 2008.

- [13] Internet Engineering Task Force, "Address Allocation for Private Internets," Internet Engineering Task Force, 1996.
- [14] Cisco, "CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide," tekijä: *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*, Kalifornia, CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide Premium Edition eBook and Practice Test, 2020.