jamk

# Itsehallittavan verkko-oppimisympäristön kehittämistutkimus

## Opinnäytetyö

Teemu Tervo

Opinnäytetyö
Toukokuu 2021
Tekniikan ala
Sähkö- ja automaatiotekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Kuvailulehti**

**Tervo Teemu**

**Itsehallittavan verkko-oppimisympäristön kehittämistutkimus**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 58 sivua

Tekniikan ala. Sähkö- ja automaatiotekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

**Tiivistelmä**

Jyväskylän ammattikorkeakoulun Rajakadun kampuksella oli tarve kehittää teolliseen internetiin liittyvää opetusympäristöä, jotta opiskelijoille voidaan tarjota automaatiotekniikkaan ja tietoverkkoihin pohjautuvaa opetusta. Toimeksiantajalla oli toive tutkia OT-verkkojen rakenteita ja verkkoihin liittyviä hyviä käytänteitä. Tarkoituksena oli luoda oppimisympäristö, jota pystytään hyödyntämään jatkossa osana opintojaksoja. Tutkimuksessa havaittiin, että uuden oppimisympäristön avulla on mahdollisuus lisätä Rajakadun sekä Dynamon kampuksien yhteistyötä tietoverkkoihin liittyvässä koulutuksessa.

Tutkimus aloitettiin perehtymällä teollisen internetin ominaisuuksiin sekä vaatimuksiin. Tietoperusta koottiin aiemmista tutkimuksista, laitemanuaaleista sekä tietoverkkojen kirjallisuudesta. Tutkimuksessa esiintyi kehittämistutkimukselle tyypillisiä piirteitä, kun yhdistettiin kirjallinen tietoperustan analysointi sekä konkreettisen tuotoksen ja kehitysehdotuksien luominen. Tutkimustyötä tehtiin yhteistyössä Siemensin sekä Jyväskylän ammattikorkeakoulun tietohallinnon verkkoasiantuntijoiden kanssa.

Työ aloitettiin asentamalla verkkolaitteet räkkiin ja toteuttamalla tarvittava kaapelointi. Verkon rakennuksen jälkeen tehtiin laitteiden konfigurointi. Lopuksi verkko otettiin käyttöön ja tehtiin tarvittavat toimivuustestaukset. Tutkimuksen tuloksena laboratorioon valmistui itsehallittava lähiverkko, johon liitettiin Siemensin toimittama automaatiolaitteisto. Laitteistoa voidaan ohjata DP69 laboratorion tietokoneilta. Tutkimuksessa analysoitiin uuden ympäristön käyttömahdollisuuksia osana automaatioinsinöörin koulutusta. Lisäksi tunnistettiin lähiverkon tietoturvaan liittyviä riskejä. Uhat pyrittiin minimoimaan parhaiten katsottuja keinoja käyttäen.

Tutkimuksessa tunnistettiin mahdollisuuksia laajentaa verkkoa tulevaisuudessa uusien laitteistojen liittämistä varten. Verkkoympäristön käyttömahdollisuuksia selvennettiin laatimalla alustavia ideoita laboratorioharjoituksia varten. Tutkimuksen tilaajan ymmärrys teollisesta internetistä sekä etäyhteyksien luomisesta kasvoi.

**Avainsanat (asiasanat)**

Teollinen internet, lähiverkko, tietoturva, etäyhteys, Ethernet

**Muut tiedot (salassa pidettävät liitteet)**

-

jamk

**Description**

**Tervo Teemu**

**Design research of a self-managed network learning environment**

Jyväskylä: JAMK University of Applied Sciences, May 2021, 58 pages

Engineering and technology. Degree Programme in Electrical and automation Technology. Bachelors´s Thesis.

Permission for web publication: Yes

Language of publication: Finnish

**Abstract**

The Rajakatu campus of Jyväskylä University of Applied Sciences had a need to develop a teaching environment related to the industrial Internet in order to provide students teaching based on automation technology and information networks. The client wanted to study the structures of OT networks and good practices related to the networks. The purpose was to create a learning environment that can be utilized in the future as part of the study courses. The study found that with the help of the new learning environment, there is an opportunity to increase the cooperation between Rajakatu and Dynamo campuses in training related to information networks.

The research was started by getting acquainted with the features and requirements of the industrial internet. The knowledge base was compiled from previous research, device manuals and the literature of information networks. The study had features typical of development research when combined with a written analysis of the knowledge base and the creation of substantial output and development proposals. The research was carried out in collaboration with Siemens and Jyväskylä University of Applied Sciences' information management network experts.

The work began by installing the network equipment in a rack and implementing the necessary cabling. After building the network, the devices were configured. Finally, the network was commissioned, and the necessary functionality tests were performed. As a result of the research, a self-managed local area network was completed in the laboratory, to which automation equipment supplied by Siemens was connected. The equipment can be controlled from DP69 laboratory computers. The study analyzed the possibilities of using the new environment as part of the training of an automation engineer. In addition, risks related to LAN security were identified. Threats were sought to be minimized using the best viewed means.

The study identified opportunities to expand the network in the future to connect new hardware. The possibilities of using the online environment were clarified by developing preliminary ideas for laboratory exercises. The client’s understanding of the industrial Internet and the creation of remote connections increased.

**Keywords/tags (subjects)**

Industrial internet, local area network, network security, remote access, Ethernet

**Miscellaneous (Confidential information)**

-

**Sisältö**

**Kuviot**

## Käsitteet ja lyhenteet

| | |
|---|---|
| Pienoisjännite | Jännite, jonka suuruus ei yli 50 volttia vaihtojännitettä ja 120 volttia tasajännitettä (TEPA-termipankki 2020). |
| Ethernet | Käytetyin lähiverkkototeutus, joka pohjautuu pilkotun datan (=kehyksien) lähettämiseen (Meyers 2003). |
| VPN | Salattu yksityisverkko. Mahdollisuus yhdistää useita lähiverkkoja julkisen verkon yli langattomasti (Meyers 2003). Verkot voivat sijaita fyysisesti kaukana toisistaan. |
| LAN | Lähiverkko, joka toimii usein organisaation hallinnassa. Lähiverkolla voidaan yhdistää verkkoon kuuluvat laitteet yhdeksi kokonaisuudeksi. (Hämeen-Anttila 2003, 28.) |
| MAC-osoite | 48-bittinen binäärimuotoinen tunniste, jolla identifioidaan jokainen verkkolaite. Käytetään datan lähettämisessä, jolloin pitää varmistua vastaanottajan oikeellisuudesta. (Meyers 2003.) |
| PoE | Power over Ethernet. Jännitteen syöttö Ethernet-kaapelia pitkiä verkkoon liitetylle laitteelle (Mesnik 2016). |
| Redundanssi | Toiminnan varmennus tai vikasietoisuus käyttämällä useita eri laitteita tai järjestelmiä toiminnon suorittamiseksi tai ylläpitoa varten (Adling 2019). |
| MRP | Teollisessa Ethernetissä käytetty protokolla, mikä parantaa laitteiston vikasietoisuutta etsimällä tiedonsiirrolle vaihtoehtoisen reitin vikatilanteen sattuessa (Setup of a Ring Topology Based on “MRP” 2016). |
| IT | IT tarkoittaa tietotekniikkaa tai informaatiotekniikkaa (eng. information technology). IT kattaa tietokoneet, verkkolaitteet sekä tietovarastot. Karkeasti IT-verkolla tarkoitetaan verkkoympäristöä, mikä on kuluttajien käytössä. (Lutkevich 2020.) |

| | |
|---|---|
| OT | OT tarkoittaa operatiivista tekniikkaa (eng. operation technology). Termi käsittää koneet ja laitteet. Termiä käytetään kuvaamaan teollista ympäristöä. (Lutkevich 2020.) |
| Oletusyhdyskäytävä | Tiedonsiirron kulkureitti aliverkkojen välillä. Mahdollistaa yhteyden eri verkkoihin. Oletusyhdyskäytävä (eng. default gateway) on yleisesti alustettu ensisijaiseksi vaihtoehdoksi. (Walker 2021.) |
| VLAN | Virtuaalilähiverkko (eng. Virtual Local Area Network) muodostetaan kiinteästä verkosta tai sen osista. Virtuaaliverkoilla voidaan korvata fyysisiä verkkolaitteita. (Tietotekniikan termitalkoot 2002.) |

# 1 Johdanto

Tässä opinnäytetyössä oli tarkoituksena tutkia teollisuusverkkoon liittyviä normeja sekä hyviä käytänteitä toimivan verkon saavuttamiseksi. Teollisuuslaitokset nojautuvat yhä enemmän tietoverkkoihin, joiden avulla voidaan tehdä huomattavia parannuksia tiedonsiirtoon sekä tiedonhallintaan. Älykkäiden ratkaisujen ansioista teollisuuden laitteistot pystyvät kommunikoimaan keskenään, jolloin tietojen keruu onnistuu hallitusti ja datan analysoinnista saadaan suurin mahdollinen hyöty. Teollisuusympäristössä prosessien valvontaa voidaan myös tehdä etäyhteydellä, jolloin toiminnasta saadaan joustavampaa ja mahdollisiin vikatilanteisiin kyetään reagoimaan nopeammin. Tutkimuksessa analysoidaan IT- sekä OT-verkkojen ominaisuuksia, jolloin tunnetaan molempien ympäristöjen olennaispiirteet. Havaitut osa-alueet ovat tärkeä tuntea verkkoa suunnitellessa, jotta osataan valita oikeanlaisia komponentteja sekä luoda halutunlainen verkko.

## 1.1 Opinnäytetyön tausta ja aiheen rajaus

Opinnäytetyö toteutettiin tukemaan keväällä Jyväskylän ammattikorkeakoululle hankittua Siemensin automaatiolaitteistoa. Laboratoriotiloihin toimitettiin automaatiolaitteisto, josta muokattiin uusi oppimisympäristö tulevia opintojaksoja varten. Uuden ympäristön myötä on mahdollista demonstroida laitteiston etäkäyttöä osana teollista internetiä. Suljettua verkkoa sekä uutta oppimisympäristöä hyödyntäen voidaan kehittää uusia harjoitteita, joissa yhdistyy automaatiotekniikka sekä tietoverkkotekniikka.

Tutkimuksessa käsitellään lähiverkkoihin olennaisesti liittyviä komponentteja, rakenteita sekä lainalaisuuksia yleisellä tasolla. Verkkolaitteiden sekä verkon ominaisuuksien tuntemus on tärkeää, kun suunnitellaan uutta verkkoa. Verkkoihin liittyvä yksityiskohtainen bittitason tieto on rajattu tästä tutkimuksesta pois, eli tutkimuksessa keskitytään verkkolaitteiden valintaan, lähiverkon rakenteeseen, rakennetun lähiverkon konfigurointiin sekä testaukseen.

Työn tutkimuskysymykseksi asetettiin: ”Millä keinoilla ja mitä laitteita käyttäen laboratorioon saadaan luotua tehtaan verkkoa mallintava lähiverkko”? Tutkimuskysymykseen olennaisesti liittyviä apukysymyksiä ovat

- Mitä eroa on IT- ja OT-verkolla?

- Mikä topologia valitaan verkon toteutukseen ja miksi?
- Toimiiko etäyhteys halutulla tavalla?
- Millaiset topologiat, laitteet, protokollat, tietoturvaratkaisut sekä konfiguraatiot ovat soveltuvia OT-verkkoon?

## 1.2 Työn tarpeellisuus ja tavoite

Toimeksiantajan toiveena oli tutkia OT-verkon rakennetta sekä verkkoon liittyviä hyviä käytänteitä. Työssä tutkittiin myös etäyhteyden luomista sekä etäyhteyden toimintaa OT-verkossa. Laitteistoa haluttiin pystyä ohjaamaan paikkaan sitomatta. Uuden laitteiston tarkoituksena on tarjota opiskelijoille uusia laboratorioharjoituksia sekä uusi testausalusta.

Etäkäyttö lisääntyy teollisessa ympäristössä ja yhä useampi laitteisto on sidottuna teolliseen internetiin. Toimeksiantaja koki tämän osion hallitsemisen tärkeäksi nykypäivän automaatioinsinöörille. Opinnäytetyössä tutkittiin teollisuusverkon ominaisuuksia sekä rakennettiin ympäristö vastaamaan vaadittuja lainalaisuuksia ja hyviä käytänteitä, mitkä saatiin tutkimuksessa selville. Tutkimuksen pohjalta oppilaitoksen lehtorit voivat suunnitella tulevaisuuden opintojaksoihin sisältöä, joka liittyy teolliseen internetiin.

Tutkimuksen tuloksena valmistuva lähiverkko pyrittiin rakentamaan alusta asti harkiten, jotta tulevaisuutta varten säilyy laajennusmahdollisuuksia. Räkin layout suunniteltiin harkiten, ja tulevaisuutta ajatellen laitesijoittelussa otettiin huomioon mahdolliset lisälaitteet. Tulevaisuudessa laboratorioon voidaan hankkia lisää automaatiolaitteistoja, joita voidaan ohjata samaa lähiverkkoa käyttäen.

# 2 Tutkimusasetelma

## 2.1 Tutkimusote

Tutkimusotteella ymmärretään strategiaa ja keinoja, joita käyttäen ilmiön tutkiminen suoritetaan. Tyypillisimmät tutkimusotteet ovat kvantitatiivinen tutkimus ja kvalitatiivinen tutkimus.

### 2.1.1 Määrällinen tutkimus

Kvantitatiivinen eli määrällinen tutkimus pohjautuu numeerisuuteen, analyyseihin sekä taulukoihin. Määrällinen tutkimus vastaa muun muassa seuraaviin kysymyksiin: Kuinka moni? Kuinka paljon? Kuinka usein? (Vilkka 2007, 14).

Aineiston keräämiseen kuuluu olennaisesti, että kysymykset ovat strukturoituja ja yksikäsitteisiä eli kysymykset voidaan ymmärtää ainoastaan yhdellä tavalla. Tällä tavoin saadaan tutkimusdataa, joka voidaan esittää numeerisesti. Tutkimustuloksia pystytään käsittelemään analyyttisesti ja niitä pystytään käyttämään erilaisissa laskutoimituksissa (Kananen 2012, 32).

Määrällisessä tutkimuksessa tutkijan rooli on ulkopuolinen havainnoija. Tutkijalla on pieni vaikutus tutkimustuloksiin, koska haastatteluissa ja kyselyissä esitetyt kysymykset ovat yksikäsitteisiä. Laaja tutkimusaineisto korostaa haastateltavan yksilön sekä tutkijan etäistä vuorovaikutusta. (Vilkka 2007, 17.)

### 2.1.2 Laadullinen tutkimus

Kvalitatiivinen eli laadullinen tutkimus pyrkii ymmärtämään kohteena olevaa ilmiötä sekä sen ominaisuuksia. Järvenpään (2006) mukaan laadullisessa tutkimuksessa käsitellään aiheita, joita ei vielä tunneta hyvin eikä aiheeseen liittyviä muuttujia ole vielä tunnistettu. Tutkijan rooli korostuu, koska mitattuja arvoja tärkeämpää on keskustelut ja siten tutkijan omat havainnot. (Järvenpää 2006, 5.)

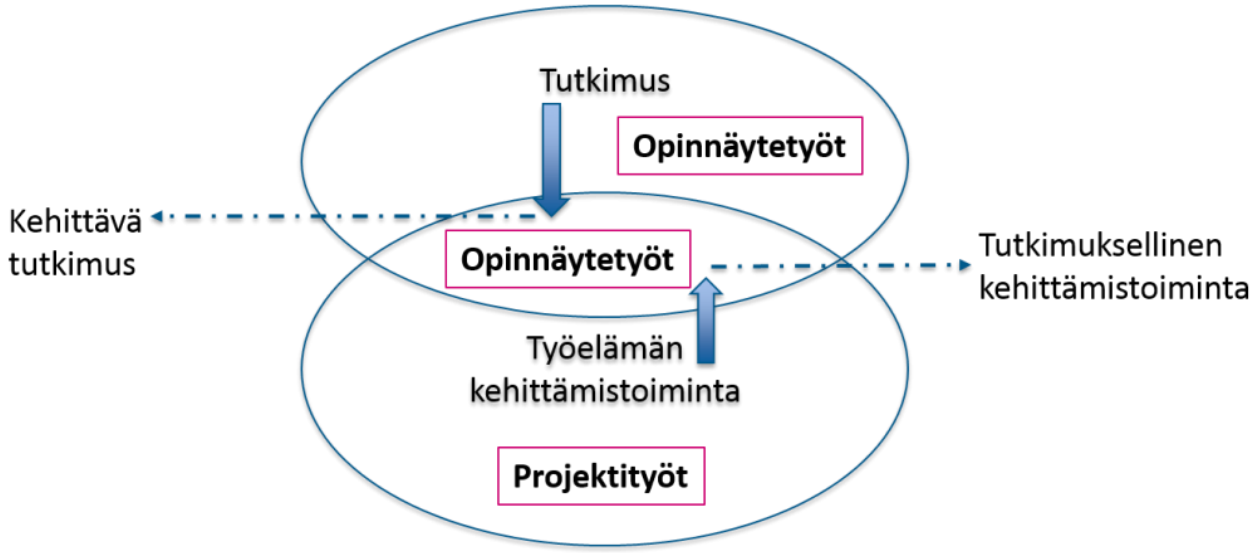
Laadullisessa tutkimuksessa käytetään avoimia kysymyksiä ja tutkimusprosessista puuttuvat, määrälliseen tutkimukseen olennaisesti liittyvät, tiukat säännöt. Avoimemman ohjeistuksen ja menetelmäviitekehyksen puutteen johdosta tutkimuksessa pyritään kuvaamaan ilmiötä ja antamaan mielekäs tulkinta. (Kananen 2012, 29–30.)

## 2.2 Kehittämistutkimus

Kehittämistutkimuksen tarkoituksena on parantaa jotain jo olemassa olevaa prosessia tai palvelun tasoa. Vaihtoehtoisesti kehittämistutkimus voi luoda perustaa myös uusille innovaatioille. Ominaisuuspiirteisiin kuuluu, että tutkimustyö on yleensä moninaista, ja kehittämistutkimusta tehdessä

joutuu monesti tukeutumaan eri tutkimusotteiden menetelmiin. Tämän takia voidaan todeta kehittämistutkimuksen olevan monitasoinen tutkimusmenetelmä, joka tukeutuu sekä kvantitatiivisen että kvalitatiivisen tutkimuksen ominaispiirteisiin. (Kananen 2012, 19.)

Kanasen (2012) mukaan kehittämistutkimus nojaa taustalla oleviin teorioihin, minkä lisäksi kehittämistutkimus vaatii tutkimuksellista otetta. Nämä asiat erottavat tutkimuksen tavanomaisesta projektityöstä. (Kananen 2012, 19–20.) Kehittämistutkimus on tyypillinen tutkimusmenetelmä ammattikorkeakoulun opinnäytetyötä tehtäessä, koska tutkimustyössä yhdistyy käytännön ongelmien ratkaisu, tutkimuksellisuus sekä taustalla oleva teoreettinen tietoperusta (kuvio 1).

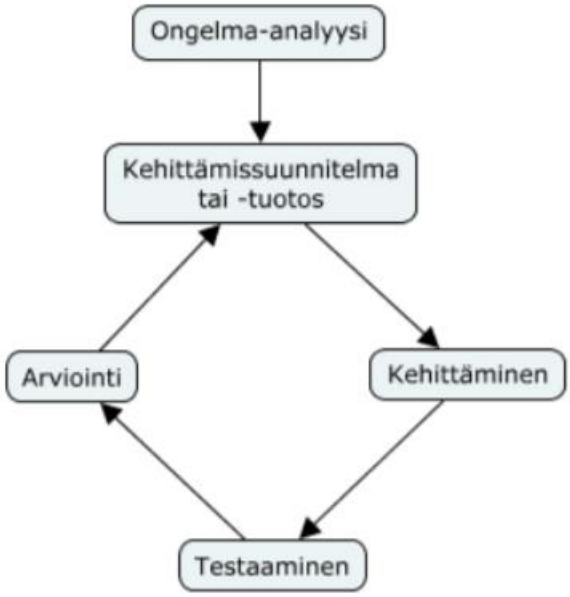



Kuvio 1. Tutkimus ja projektityö yhdistyvät kehittämistutkimuksessa (Tutkimuksellinen kehityshanke opinnäytetyönä vs projektityö N.d.)

Kehittämistutkimus keskittyy kehittämään tutkimuskohdetta ja siihen liittyvää ympäristöä. Tutkimuksen päätavoitteena on tutkimuskohteeseen liittyvän teorian luominen. Kehittämistutkimuksissa kehitettyjä teorioita pyritään voimakkaasti yleistämään kohti suurempaa mittakaavaa. (Pernaa 2013, 5.)

Kuviossa 2 esitetään kehittämistutkimukselle tyypillinen syklinen eteneminen. Kehittämistutkimus aloitetaan aina tekemällä ongelma-analyysi, jonka pohjalta arvioidaan kehittämisen tarpeet, mahdollisuudet sekä haasteet (Pernaa 2013, 6). Ongelma-analyysin tekeminen on välttämätöntä, koska kehittämistarve muodostuu konkreettisesta ongelmasta.

Seuraavaksi laaditaan kehittämissuunnitelma, jonka mukaan aletaan tehdä varsinaista tutkimusta. Kehittämistutkimus koostuu tutkimussykleistä (kuvio 2). Kun toteutus jaetaan sykleihin, konkreettista tutkimusta pystytään jaksottamaan sekä suunnitelmaa kehittämään. Tässä kehittämistutkimuksessa luodaan useita tutkimussyklejä, jotta voidaan tarkastella verkon rakentamisen etenemistä sekä palata tarvittaessa muokkaamaan kehittämissuunnitelmaa.




Kuvio 2. Kehittämistutkimuksen eteneminen (Kehittämistutkimus: TVT:n tehokas integrointi matematiikan digitaaliseen ylioppilaskokeeseen valmistautumisessa 2017)

## 2.3 Tietoperusta

Tutkimuksen tietoperusta koostuu pääosin ammattikirjallisuudesta, internetjulkaisuista, artikkeleista sekä muista opinnäytetöistä. Aineistoa kerätessä lähdekritiikkiin kiinnitetään erityistä huomiota, jotta pystytään toteamaan faktojen oikeellisuus. Verkkolaitteiden valmistajan manuaalia käytetään aineistona laitevalintoja tehtäessä. Laitteita valitessa voidaan vertailla teoriatietoa valmistajan datalehtien tietoihin. Lähiverkon topologian valintaa ja laitteiden konfigurointia varten

haastatellaan Jyväskylän ammattikorkeakoulun tietohallinnan edustajaa sekä Siemensin verkkoasiantuntijaa. Haastatteluista saatuja tietoja arvioidaan sekä analysoidaan. Tiedoista tehtyjen päätelmien perusteella tehdään topologian lopullinen valinta.

Tietoliikenteeseen ja tietoverkkoihin liittyviä opinnäyte-, sekä gradutöitä on tehty aiemminkin. Monissa tutkimuksissa otetaan kantaa verkon rakenteeseen sekä tiedonsiirtoprotokolliin. Salminen (2006) sekä Itkonen (2018) ovat tehneet vastaavaa tutkimustyötä tämän tutkimuksen aihepiireihin liittyen, joten heidän tutkimuksistaan saatuja tuloksia käytetään osana tämän tutkimuksen tietoperustaa.

Salminen (2006) analysoi gradutyössään ”Teollisuus-Ethernetin teknistaloudellinen selvitys sähkötukkukaupan näkökulmasta” Ethernetin käyttöä teollisessa ympäristössä. Salminen vertailee työssään Ethernetin eroavaisuuksia toimisto- ja teollisuusympäristössä sekä vertailee käyttökelpoisia laitteita teollista ympäristöä ajatellen.

Itkonen (2018) tutkii teollisuuden tietoverkkoja osana hänen opinnäytetyötään ”Teollisuustietoliikenneverkot osana suunnitteluprosessia”. Tietoverkot muuttuvat jatkuvasti monimutkaisemmiksi, joten aihe on otettava entistä vakavammin huomioon teollisuuslaitoksia suunnitellessa (Itkonen 2018). Tutkimuksessaan Itkonen ottaa kantaa verkon rakenteeseen sekä verkkoon liittyviin laitteisiin yleisellä tasolla.

Tutkimusaineiston oikeellisuutta tarkastellaan vertailemalla aiemmin tehtyjen tutkimuksien keskeisimpiä tuloksia tämän tutkimuksen havaintoihin sekä tuloksiin. Aineistoa analysoidaan tekemällä sisältöanalyysiä sekä tekemällä yhteenvetoja tietoperustasta ja tutkimuksen aikana hankitusta tiedosta. Sisältöanalyysia tehdessä keskitytään aineiston aiheisiin ja teemoihin (Vuori n.d). Lopullinen analyysi tehdään tutkimuksen tuloksena syntyneen oppimisympäristön pohjalta, minkä avulla arvioidaan tutkimuksen onnistumista.

## 2.4 Tutkimuksen eettisyys

Tutkimusta tehdessä noudatetaan hyviä tieteellisiä käytänteitä. Helinin, Spoofin, Jäppisen & Launisen (2012) mukaan tutkimuksessa tulee esittää rehellisyyttä, huolellisuutta sekä tarkkuutta. Tutkimusta tehdessä täytyy vaalia avoimuutta tutkimustulosten suhteen sekä käyttää eettisesti kestäviä

tiedonkeruu- sekä analysointimenetelmiä. Muiden tutkijoiden tekemää työtä kunnioitetaan viittaamalla heidän julkaisuihinsa asiaan kuuluvalla tavalla.

Tässä tutkimuksessa pyritään käyttämään julkaisujen alkuperäisiä lähteitä, jotta varmistutaan tiedon oikeellisuudesta sekä kyetään puntaroimaan lähteen luotettavuutta. Myös aiemmin hankittua tietoa käyttämällä analysoidaan tutkimuksen lähteiden hyvyyttä. Muiden tutkijoiden julkaisuihin viitatessa käytetään ensisijaisesti referointia. Sitaatteja pyritään välttämään ja niitä käytetään ainoastaan, kun on välttämätön tarve. Lopullisesta tutkielmasta pyritään tekemään mahdollisimman läpinäkyvä, jolloin työ kestää eettistä tarkastelua.

Tutkimuksella on myös suuri vaikutus tulevaisuudessa lisättävien automaatiolaitteistojen kyberturvallisuuteen sekä suurien laitteiden osalta myös henkilöturvallisuuteen. Verkkolaitteistoa on mahdollisuus laajentaa tulevaisuudessa, joten on ensisijaisen tärkeää tehdä tutkimustyö huolella alusta loppuun asti. Seurauksien laajuus korostaa tutkijan vastuuta sekä perusteltua tarvetta tehdä tutkimus käyttäen hyviä eettisiä periaatteita. Täten työssä tarvitaan erityistä huolellisuutta sekä lähdeaineistoon liittyvää kriittisyyttä, jolloin varmistutaan oikeista työmetodeista.

# 3 Ethernet

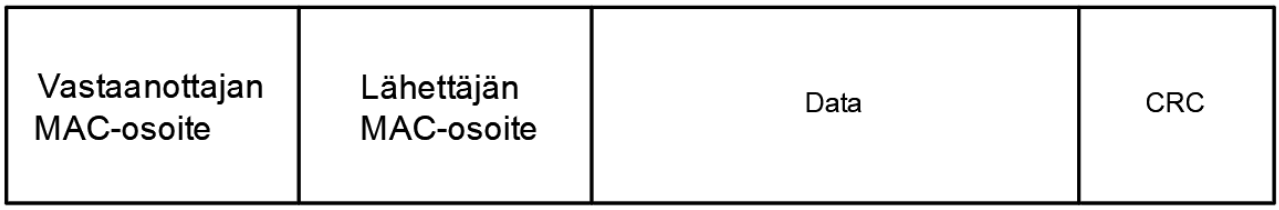
Ethernetin suosio on kasvanut huomattavasti viime vuosina. Olemassa olevista tietoliikenneverkoista noin 90–95 % pohjautuu Ethernetiin. Ethernet valtaa markkinoita yksinkertaisen rakenteen, laitteiden edullisuuden sekä jatkuvan kehitystyön johdosta. (Jaakohuhta 2005.) Tässä työssä Ethernet-verkkotekniikan tutkiminen on olennaista, koska Ethernet on tutkimuksessa tarkasteltavan verkon tiedonsiirtoväylän ratkaisuna.

## 3.1 Ethernetin ominaispiirteet

Xerox esitteli Ethernetin alkuperäisen version Yhdysvalloissa 1970-luvulla. Ensimmäinen versio pohjautui paksuun koaksiaalikaapeliin, joka toimi Ethernet-väylänä. Väylään pystyi liittämään maksimissaan 100 solmua eli laitetta, jolloin tiedonsiirtonopeus oli maksimissaan 3Mb/s. Nykyaikana Ethernetin nopeus voi olla useita gigabittejä sekunnissa ja kaapelointi on toteutettu joko parikierretyllä kuparikaapelilla tai valokuidulla. Kehitys on ollut äärimmäisen nopeaa. (Jaakohuhta 2005.)

Ethernetin liikennöinti perustuu paketteihin eli kehyksiin sekä MAC-osoitteisiin. Ethernetissä liikkuva data on pilkottu pieniin kehyksiin, jotka kulkevat kaikille järjestelmään liitetyille laitteille. Laitteiden verkkokortit osaavat kasata kehykset, jolloin siirretystä datasta muodostuu yhtenäinen kokonaisuus. (Meyers 2003.) Verkkokortit myös valitsevat vastaanotetuista kehyksistä ne, joiden MAC-osoite täsmää vastaanottavan laitteen kanssa. MAC-osoite on tunniste, jonka avulla paketit identifioidaan oikeille laitteille. Verkkokortit vastaanottavat paketit, jotka on niille tarkoitettu. Jos MAC-osoite ei täsmää, paketti pyyhkiytyy pois.

Yksinkertainen kehys on esitetty kuviossa 3. Kehys koostuu vastaanottajan ja lähettäjän MAC-osoitteista. Näiden tietojen pohjalta tiedetään mistä paketti on tulossa ja mihin se on menossa. Paketti sisältää myös lähetettävää dataa sekä CRC-tiedon, jonka avulla tarkastetaan, että paketissa oleva data saapuu oikein. (Meyers 2003.)




Kuvio 3. Kehyksen yleismalli

Ethernetin nopeudet ovat kasvaneet vuosikymmenten kuluessa moninkertaisiksi alkuperäisiin nopeuksiin verrattuna. Jaakohuhdan (2005) mukaan Ethernetit voidaan jaotella seuraavasti

- 10 Mbs, 10Base-T, koaksiaalikaapeli / suojaamaton parikaapeli
- 100 Mbs, Fast-Ethernet, kierretty parikaapeli
- 1000 Mbs, 1000Base-T / Gigabit-Ethernet, valokuitu
- 10000 Mbs, 10Gbe, valokuitu.

Ethernet on syrjäyttänyt monet kilpailijat, joten Ethernet on pystynyt valtaamaan suurimman osan uusista verkoista. Token Ring- sekä FDDI-verkot ovat jääneet vuosien saatossa Ethernetin jalkoihin. Ethernet on laajentunut nopeasti myös teollisuusympäristöihin laitteiden yleistyessä ja nopeuksien kasvaessa. (Jaakohuhta 2005.) Ethernetin suuren suosion perustana ovat suuret liikennöintinopeudet, kattavat tukipalvelut sekä edulliset laitteet ja järjestelmät (Pyyskänen 2006, 78). Taiponen

(2006) esittää tutkimuksessaan Ethernetin eduiksi myös erinomaisen laitetarjonnan sekä laitteiden yhteensopivuuden eri valmistajien välillä.

## 3.2 IT- ja OT-verkon erot ja yhtäläisyydet

Taiponen (2006) on listannut toimintaympäristöjen eroavaisuudet kolmitasoiseen taulukkoon. Taulukossa vertaillaan tyypillisimpiä yhtäläisyyksiä sekä eroavaisuuksia kahden ympäristön välillä. Vertailtavat piirteet ovat laitteiden asentaminen, tiedonsiirtovaatimukset sekä ympäristön asettamat vaatimukset laitteistolle.

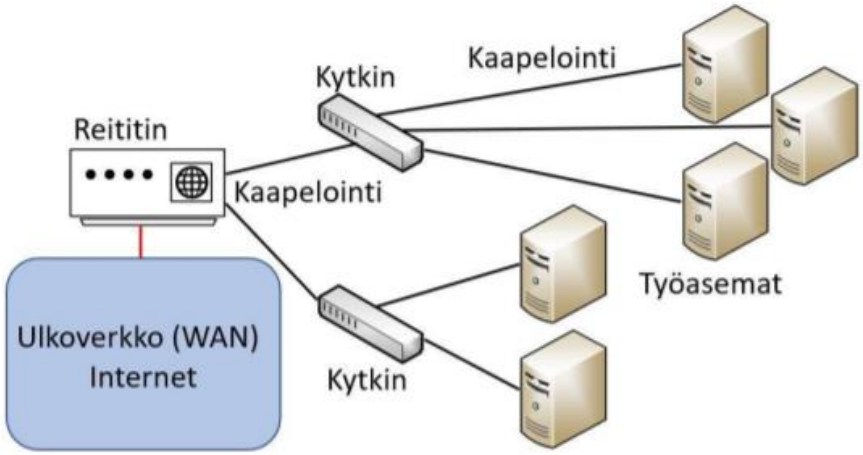
Toimistoympäristö on asennusta ajatellen melko stabiili. Asennukset ovat kiinteitä, verkon topologia on usein puumainen, verkkolaitekaapelit tulevat valmistajalta kasattuina ja työpäätteet ovat standardisoituja. Verkkolaitteiden jännitteensyöttö on tyypillinen 230 voltin vaihtojännite. Ethernetin rakentaminen sisätiloihin on suoraviivaista. Teollisuusympäristössä vaatimukset ovat huomattavasti suuremmat. Käytössä olevat järjestelmät määrittävät asennustavan sekä kaapeloinnin. Puutopologian sijaan teollisuudessa käytetään rengas- tai väylätopologiaa, jolloin verkkoon saadaan lisättyä redundanttisuutta sekä toimintavarmuutta. Laitteiden jännitteensyöttö on yleensä 24 volttia tasajännitettä tai 48 volttia PoE. (Taiponen 2006, 25.)

Toimistoympäristön tiedonsiirto on yleensä syklittäistä ja siirrettävät paketit ovat huomattavan suuria. Tiedonsiirto ei täten ole jatkuvaa. Verkon toimintavarmuudelle on keskisuuri vaatimus eli verkko voi aika-ajoin kaatua, mutta siitä ei koidu suurta vahinkoa. Teollinen Ethernet taasen ei saa kaatua, koska verkon toiminnan on oltava jatkuvaa. Teollisessa ympäristössä siirrettävät paketit ovat pieniä, mutta verkossa liikennöidään koko ajan. (Taiponen 2006, 25.) Toimistoverkkoa ja teollista verkkoa ei siis saa sekoittaa keskenään.

Toimistoympäristö on ihanteellinen laitteiden asennukselle. Toimistossa lämpötila on yleensä stabiili, jos jäähdytys toimii suunnitellusti. Ulkoista kuormitusta ei siistissä sisäympäristössä yleensä ole. Teollisessa ympäristössä verkkolaitteet altistuvat korkeille lämpötiloille sekä eri prosessiaineille. Mahdollisia riskin aiheuttajia ovat myös pöly, lika, kosteus, tärinä, iskut, kemialliset aineet ja UV-säteily. (Taiponen 2006, 25.)

# 4 Lähiverkko

Lähiverkko eli LAN (eng. Local Area Network) on tietoliikenneverkko, joka toimii tietyllä maantieteellisesti rajatulla alueella (Hämeen-Anttila 2003, 28). Lähiverkko on tarkoitettu lähekkäin sijoitettujen tietokoneiden ja verkkolaitteiden yhdistämiseen. Lähiverkko voidaan rakentaa esimerkiksi yrityksen toimitiloihin. Yksikertainen lähiverkko on esitetty kuviossa 4.




Kuvio 4. Havainnekuva lähiverkon rakenteesta (Lähiverkon vakiointi yrityksen useaan toimipisteeseen 2019)

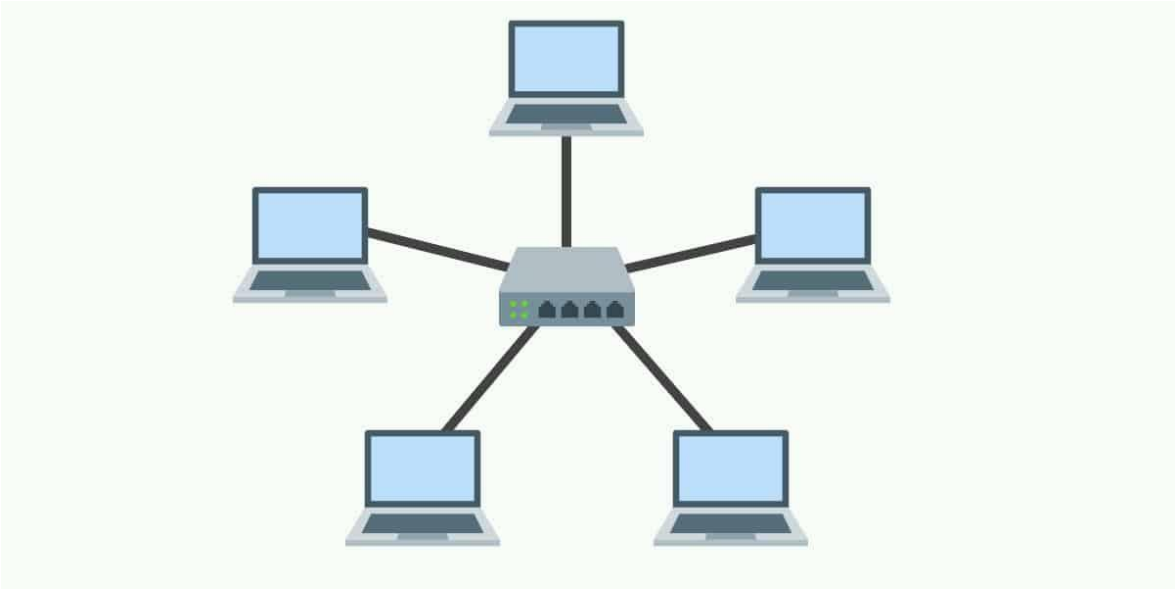
## 4.1 Verkkotopologiat

Verkkotopologia käsittää verkkolaitteiden liityntätavan toisiinsa nähden. Eri topologioilla on erilaisia ominaisuuksia sekä heikkouksia, joten topologioiden tunteminen on tärkeää verkkoa suunnitellessa. Topologiat voidaan jakaa kahteen pääryhmään: kaksipisteyhteyksiin ja monipisteyhteyksiin (Granlund 2007). Tämän tutkimuksen kannalta oleellinen ryhmä on monipisteyhteydet. Topologiat voidaan jakaa vielä fyysiseen sekä loogiseen topologiaan. Fyysinen topologia tarkoittaa sitä miltä verkko konkreettisesti näyttää käyttäjälle. Looginen topologia taasen kertoo, kuinka verkko toimii sähköisesti. (Meyers 2003, 69.)

### 4.1.1 Tähtitopologia

Tähtikytkennässä (kuvio 5) laitteet muodostavat yhdessä aktiivilaitteen kanssa tähteä muistuttavan verkon. Verkon jokainen laite on kytketty tähden keskipisteeseen, joka voi olla keskitin, reititin tai kytkin (Hakala & Vainio 2005).

Tähtikytkentä sietää kohtuullisesti vikatilanteita, koska kaapelirikko katkaisee ainoastaan yhden yhteyden ja se ei vaikuta muun verkon toimintaan. Vianmääritys on myös muihin topologioihin verrattuna helpompaa. Ongelmatilanteissa on nopeaa selvittää mikä laite on lakannut toimimasta, ja koska keskuslaitteita on vain yksi, laitteiston päivitys on helppoa. (Hämeen-Anttila 2003, 31.) Toisaalta koko verkko on riippuvainen yhdestä keskuslaitteesta, joten keskuslaitteen suorituskyky sekä toimintavarmuus ovat ensisijaisen tärkeitä.



Kuvio 5. Tähtitopologia (Network Topology: 6 Network Topologies Explained & Compared 2020)

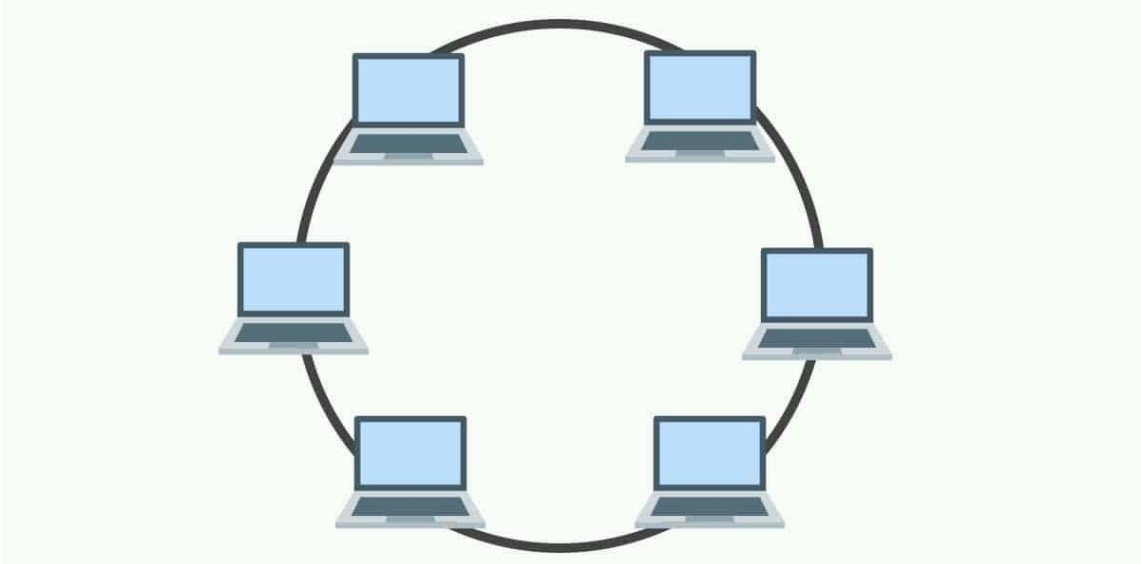
### 4.1.2 Rengastopologia

Rengastopologiassa (kuvio 6) verkkoon liitetyt laitteet muodostavat rengasmaisen asetelman. Edellinen laite lähettää signaalin aina seuraavalle laitteelle, joka vastaanottaa signaalin ja lähettää sen taas eteenpäin. Signaali kulkee renkaassa niin kauan kuin se saavuttaa tavoitellun laitteen. Rengastopologia on herkkä vikaantumiselle. (Pyyskänen 2007, 28.) Yksikin vika voi kaataa koko

verkon eli renkaan toimintavarmuus on heikko. Rengasasetelmassa myös vianmääritys on hankalaa. Vikaantunut laite on hankala paikantaa, koska rengas voi olla poikki mistä kohdasta tahansa. Laitteiden lisääminen tai poistaminen tuottaa myös hankaluuksia, koska laitteet täytyy sammuttaa, jotta muutostyö tai huolto voidaan toteuttaa.

Rengastopologia oli yleisesti käytössä Token Ring -teknologiaa käytettäessä. Nykyisin Ethernet on vallannut suurimman osan verkkojen markkinaosuudesta. Toimistoympäristöön rakennetut Ethernetit ovat joko puumaisia tai tähtiväyläverkkoja. Tästä syystä rengastopologian käyttö on erittäin vähäistä verkkoja rakennettaessa. (Meyers 2003.) Teollisessa ympäristössä Ethernetiä rakennetaan vielä renkaaseen käyttäen MRP-protokollaa, jolloin verkon redundanttisuus kasvaa ja verkoista saadaan toimintavarmoja (Adling 2019).

MRP-protokollaa käytettäessä rengasverkon vikasietoisuus paranee. MRP-protokollan käyttö on yleistä teollisuus- sekä prosessiautomaatiossa. Tällä protokollalla suurin saavutettu etu on redundanttisuuden kasvattaminen. Protokolla mahdollistaa nopean uudelleenreitityksen vian sattuessa, jolloin verkkoliikenne ei katkea. (Setup of a Ring Topology Based on “MRP” 2016, 5.) MRP-protokollaa sekä verkkolaitteiden konfigurointia tutkitaan tarkemmin luvussa 5.4.



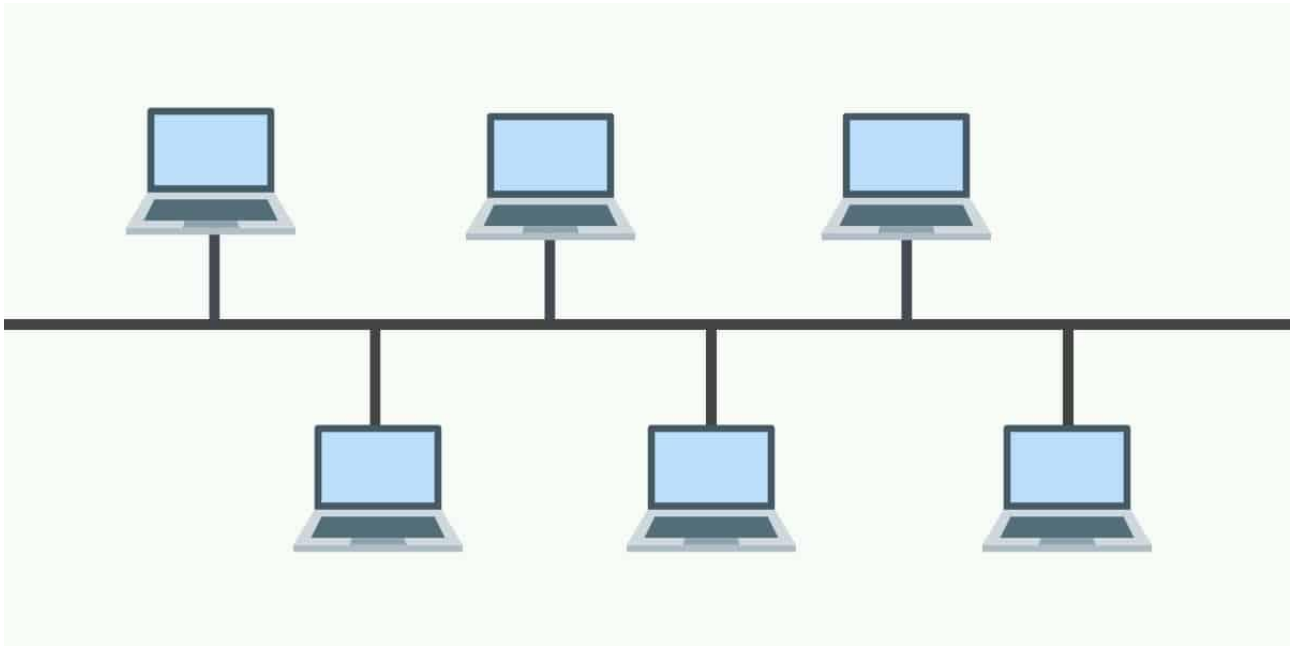
Kuvio 6. Rengastopologia (Network Topology: 6 Network Topologies Explained & Compared 2020)

### 4.1.3 Väylätopologia

Väylätopologiassa (kuvio 7) verkon laitteet yhdistetään samaan runkokaapeliin. Verkkoliikenne kulkee kaikkien laitteiden kautta ja data päätyy lopulta halutulle väylän laitteelle.

Verkon muokkaaminen on helppoa, koska haaroja voidaan poistaa mistä vain ja laitteiden lisääminen onnistuu asentamalla uusi laite sekä väyläpala päätevastuksen tilalle. Väylän pituutta voidaan kasvattaa asentamalla verkkoon vahvistin, joka vahvistaa verkossa kulkevaa signaalia sähköisesti. (Pyyskänen 2007, 27.)

Väyläratkaisun haasteena on verkon ruuhkautuminen. Kaikki laitteet voivat aloittaa lähetyksen vapaasti, jolloin verkossa tapahtuu törmäyksiä. Törmäyksestä toipumiseen vaaditaan omat toimenpiteet, mikä hidastaa liikennettä verkossa. (Granlund 2007, 79.) Väyläratkaisussa on lisäksi riskinä runkokaapelin vaurioituminen, mikä saattaa kaataa koko verkon.



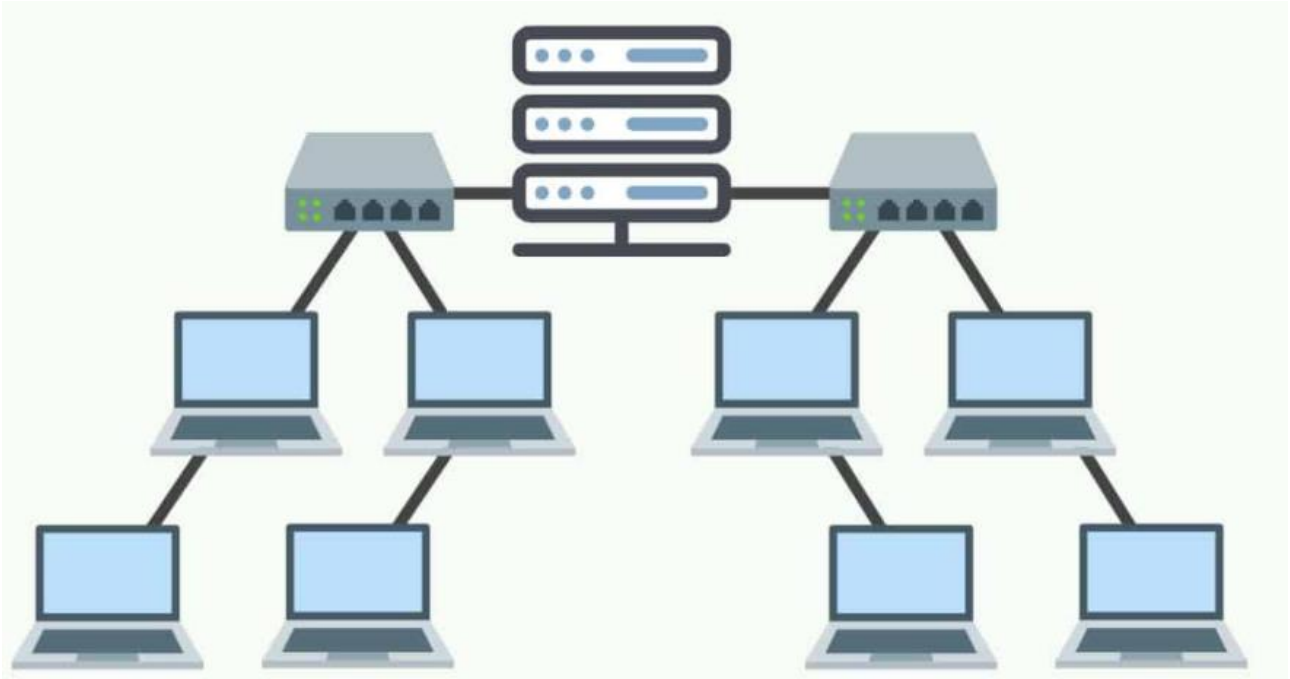
Kuvio 7. Väylätopologia (Network Topology: 6 Network Topologies Explained & Compared 2020)

### 4.1.4 Puutopologia

Puutopologia (kuvio 8) muistuttaa väyläverkon rakennetta. Puuverkon väylät ovat yhdistetty yhdeksi verkoksi käyttäen päätevahvistinta. Puuverkko toimii myös samoin kuin väyläverkko eli jokaista väyläkaapelia koskee samat rajoitukset ja lainalaisuudet. (Pyyskänen 2007, 30.)

Puuverkon heikkous on liikennöinti. Kuten väyläverkossakin, ainoastaan yksi laite voi liikennöidä kerrallaan puuverkossa, mikä voi aiheuttaa verkkoon ruuhkautumista. Päätelaitteeksi voi hankkia useampi kanavaisen lähettimen, mutta tämä ratkaisu nostaa huomattavasti laitteiston kustannuksia. Verkon haavoittuvia osia ovat kaapeloinnit sekä päätelaite. Jos kaapeli katkeaa tai päätelaite hajoaa, verkko saattaa pahimmassa tapauksessa lopettaa toimintansa. (Pyyskänen 2007, 30.)

Puuverkkoja on laajalti käytössä sekä toimisto- että teollisuusympäristössä, koska puumainen rakenne sallii rakentaa monimutkaisia verkkoja. Puuverkot ovat yleistyneet tietoverkkotekniikassa, koska absoluuttisia topologiavaihtoehtoja ei ole juuri käytössä. Useat verkot koostuvat monesta eri topologiaratkaisusta. Puuverkkojen etuina ovat monimutkaiset rakenteet, helpot muutostyöt sekä nopea vianetsintä.



Kuvio 8. Puutopologia (Network Topology: 6 Network Topologies Explained & Compared 2020)

## 4.2 Lähiverkon laitteet

Verkon suunnittelua aloittaessa on olennaista tuntea tyypillisimmät verkkolaitteet. Laitetuntemus nopeuttaa suunnittelua. Kun tiedetään laitteiden ominaisuudet ja suorituskyky, suunnittelua pystytään tekemään huomattavasti selkeämmin. Järkevillä toimilaiteratkaisuilla pystytään luomaan tehokkaampi verkko sekä säästämään toteutuskuluissa.

### 4.2.1 Toistin ja keskitin

Toistin eli vahvistin on verkkoon liitettävä laite, jonka tehtävänä on vahvistaa heikentynyttä verkkosignaalia puuttumatta signaalin sisältöön. Signaalia vahvistamalla voidaan suunnitella pidempiä kaapelointeja. Toistimessa voi olla yksinkertaisimmillaan liitännät yhdelle sisään tulevalle signaalille sekä vahvistetulle ulostulosignaalille. Useiden ulostulojen omaavia toistimia kutsutaan moniporttitoistimiksi. Näissä yksi sisään tuleva signaali vahvistetaan ja jaetaan useisiin ulostuloihin. (Hämeen-Anttila 2003, 45.)

Jaakohuhtan (2005, 95) mukaan keskitin (eng. hub) tarkoittaa napapistettä, joka jakaa lähiverkkoa työasemille samalla vahvistaen signaalin vahvuutta. Toistin sekä keskitin saatetaan ymmärtää samana laitteena, mutta oleellinen ero on se, että keskitin voi sisältää usean toistimen. Keskittimiä käytetään usein tähtiverkkoa rakennettaessa (Pyyskänen 2007, 32).

### 4.2.2 Kytkin

Kytkintä käytetään yhdistämään lähiverkon osia (kuvio 4). Lähiverkkojen tehostaminen onnistuu korvaamalla keskitin kytkimellä. Kytkimen etuna on verkkoliikenteen nopeuden säilyvyys. Saapuvan verkkoliikenteen nopeus on yhtä suuri kuin lähtevän verkkoliikenteen. Tämä johtuu muun muassa kytkimen nopeasta taustaväylästä. (Jaakohuhta 2005, 137.)

Kytkin pystyy suodattamaan verkkoliikennettä. Tulevan paketin MAC-osoite tallentuu kytkimen osoitetauluun. Kytkin vertaa sisään tulevien pakettien MAC-osoitteita muistissa oleviin osoitteisiin, minkä jälkeen paketti lähetetään oikeaan porttiin. Jos vastaanottajan osoitetta ei löydy, sisään tuleva paketti lähetetään kaikkiin portteihin. Vastaavasti jos lähettäjä- ja vastaanottajaosoite on sama, paketti hävitetään. (Pyyskänen 2007, 33.)

### 4.2.3 Reititin

Tietoliikenneverkkojen yhdistäminen onnistuu käyttämällä reititintä. Reititin on aina yhteydessä kahteen eri verkkoon. Kuviossa 4 on esitetty lähiverkon rakenne, jossa reititin on yhdistetty ulkoverkkoon eli Internetiin sekä lähiverkon kytkimiin.

Reititin on ylemmän tason laite eli se on verkkohierarkiassa korkeammalla kuin kytkin. Tämä tarkoittaa sitä, että kytkin ei voi olla yhteydessä ulkoverkkoon toisin kuin reititin. Edellytyksenä reitityksen toiminnalle on laitteiden IP-osoitteet (ks. luku 4.4), joiden avulla reitittimet lähettävät ja vastaanottavat paketteja protokollien mukaan. (Kurose & Ross 2013.)

Reitittimiin on ohjelmoitu protokollia eli käytänteitä, joiden algoritmeja noudattamalla reititin valitsee sopivimman reitin paketin kuljetukselle. Reititin voi esimerkiksi etsiä lyhimmän tai nopeimman reitin protokollan mukaan. Protokollaan voi olla konfiguroituna vaihtoehtoisen reitin hakeminen, jos oletusreitti ei ole käytettävissä. (Kurose ym. 2013.)

## 4.3 Lähiverkon tietoturva

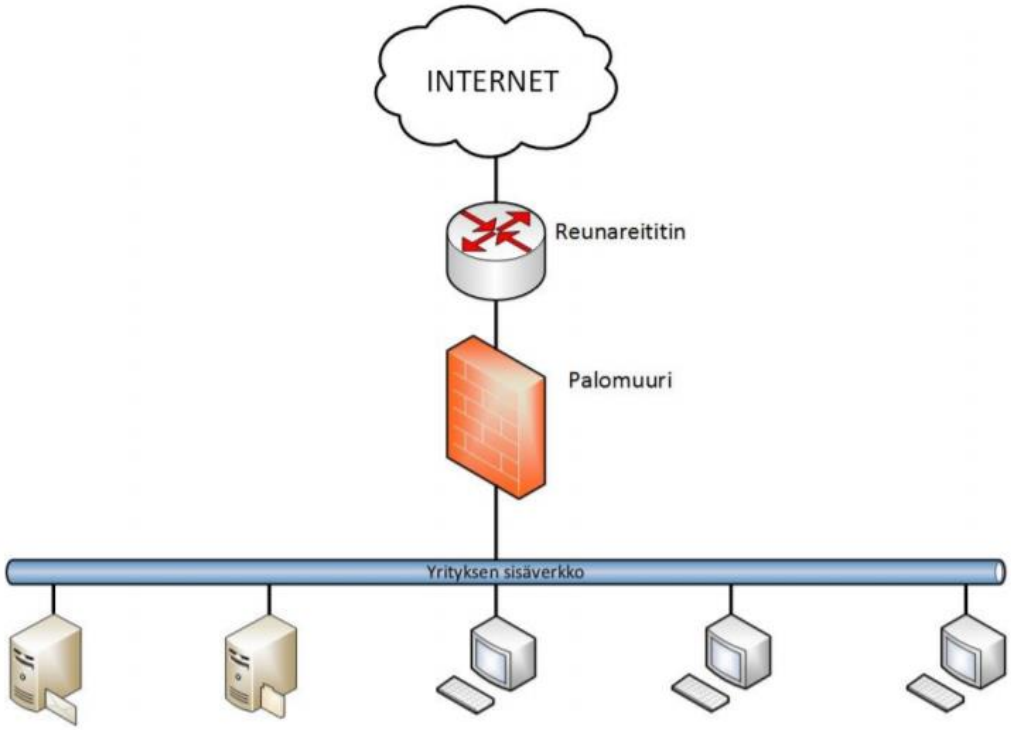
Tieto- ja laiteverkot ovat yhä merkittävämmässä roolissa osana yksityisten käyttäjien sekä yritysten arkipäivää. Arkaluontoiset tiedot, kuten pankkitunnukset tai yrityksien dokumentit, liikkuvat verkossa tai ovat tallennettuina erilaisiin pilvipalveluihin. Näitä tietoja on syytä varjella ja tästä syystä tarvitaan tietoturvaa parantavia työkaluja.

### 4.3.1 Palomuuri

Palomuuri on tietoturvalaite, joka toimii sisäisen ja ulkoisen verkon rajapinnassa (kuvio 9). ”Palomuuri tutkii liityntäänsä saapuvan liikenteen ja soveltaa siihen tiettyjä sääntöjä, käytännössä sallien tai estäen liikenteen kyseisten sääntöjen perusteella.” (Thomas 2005, 161.) Näin ollen palomuuri tekee päätöksen verkkoliikenteen sallimisesta ulkoverkosta sisäverkkoon tai päinvastoin. Palomuuri kerää tietoja verkkoliikenteestä muistiin, jolloin se oppii tunnistamaan turvalliset verkkosivustot.

Palomuureja on eri tasoisia: henkilökohtaisia, monitoimisia, pienille ja keskisuurille yrityksille suunnattuja sekä suuryrityksille suunnattuja. Henkilökohtaisia palomuureja käytetään kuluttajatasolla

yleensä henkilökohtaisissa tietokoneissa turvaamaan verkossa liikkumista. Monitoimipalomuurit ovat yleensä valmiiksi integroituina reitittimiin. Tällaiset laitteet sopivat käyttäjille, jotka jakavat laajakaistaa esimerkiksi kotona useiden laitteiden käyttöön. Yrityskäyttöön kohdistetut palomuurit ovat järeitä ja niissä on suuri muistikapasiteetti. Yritysten palomuureissa on paljon liityntöjä, koska yritysverkoissa on usein monia käyttäjiä. (Thomas 2005, 171.)



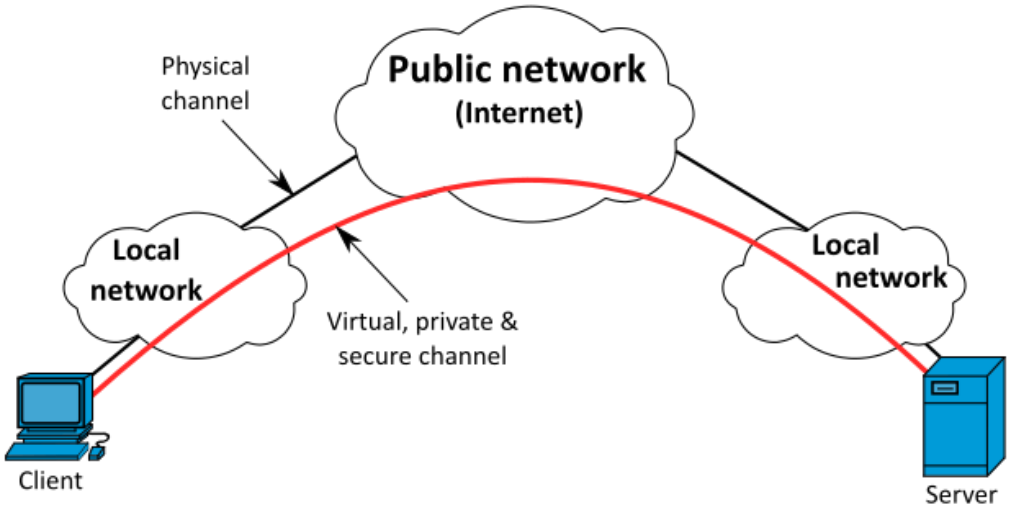

Kuvio 9. Palomuurin sijanti verkossa (Aktiivisen IPCop-palomuurin yliheitto 2015)

Palomuurien ongelmana on se, ettei kaikkia uhkia voida todeta ajoissa, koska uusia haittaohjelmia luodaan verkkoon jatkuvasti. Hakkereita voidaan hidastaa, mutta palomuurit eivät kuitenkaan takaa täydellistä suojausta. Verkon käyttäjien kannalta palomuuri saattaa joskus hankaloittaa työskentelyä, jos palomuuri estää käyttämästä harmitonta sivustoa luullessaan sitä uhkaksi.

### 4.3.2 VPN

VPN (eng. Virtual Private Network) eli virtuaalinen yksityisverkko on yksinkertainen ja turvallinen tapa luoda yhteys lähiverkkoon Internetin tai muun verkon kautta. Kuviossa 10 on esitetty VPN toiminta yksinkertaistettuna. Käyttäjä voi ottaa yhteyden toiseen lähiverkkoon VPN-tunnelin kautta, jolloin VPN-yhteys salaa käyttäjän IP-osoitteen sekä GPS-tiedon (Andreasson & Koivisto 2013).

Näin ollen verkon käyttö on turvallista. Ilman VPN:ää yhteys pitää luoda Internetiin ilman salausta, jolloin käyttäjä on alttiina uhkille ja hänen verkkoliikennettään voidaan monitoroida.




Kuvio 10. VPN-yhteys ja Internet-yhteys (Teleworking: VPN and other recommendations 2020)

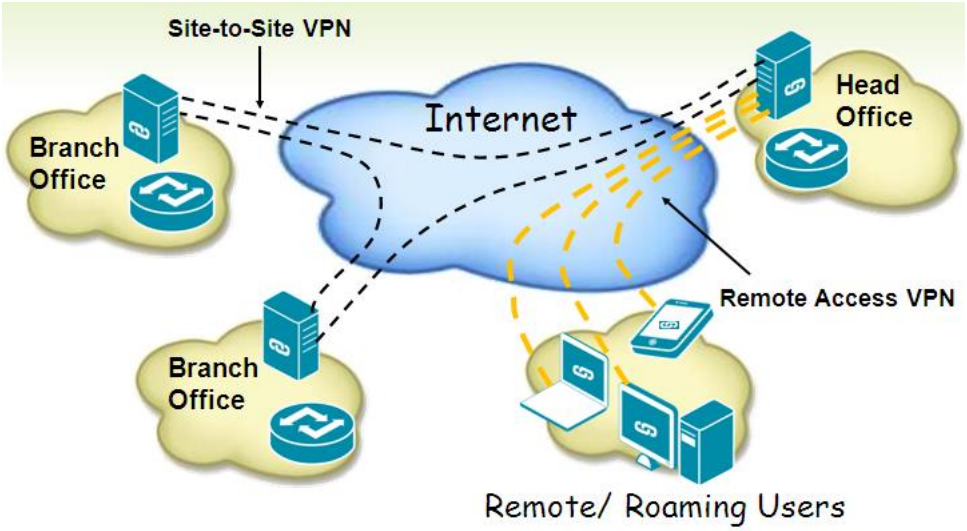
VPN on hyödyllinen yritysmaailmassa, kun työskennellään samassa lähiverkossa. Käyttäjä voi käyttää lähiverkkoa sijainnista riippumatta hyödyntäen VPN:ää. VPN voidaan rakentaa fyysisen verkon sijaan, jolloin saadaan isoja kustannussäästöjä, kun ei tarvitse rakentaa tai ylläpitää varsinaista verkkoa (Kurose ym. 2013). VPN:n muita etuja ovat nopeus, turvallinen verkkoliikenteen salaus sekä liikuteltavuus.

Thomas (2005) on jakanut VPN-verkot kolmeen eri kategoriaan. VPN-verkkojen tyyppejä ovat

- VPN-etäyhteysverkko
- Toimipisteiden välinen VPN-verkko
- VPN-extranet -verkko.

Tämä on suora esimerkki, kuinka virtuaalisia yksityisverkkoja kannattaa jaotella yritysmaailmassa. VPN-etäyhteysverkko kuvastaa yksittäisen käyttäjän, mobiililaitteen tai esimerkiksi tietokoneen yhdistämistä etäyhteydellä yrityksen lähiverkkoon. Tällä tavoin päästään tarkastelemaan esimerkiksi yrityksen verkkolevylle tallennettuja tiedostoja. Toimipisteiden välinen VPN-verkko kuvastaa

eri toimistojen välistä salattua yhteyttä Internetin yli. VPN-extranet -verkko mahdollistaa esimerkiksi asiakkaiden ja toimittajien toiminnan yhteisessä verkossa. Tämä helpottaa työskentelyä, jos tehdään tiiviisti yhteistyötä ja pyritään saavuttamaan samoja päämääriä. (Thomas 2005, 238.) Kuviossa 11 esitetään verkkojen jaottelua piirretyssä muodossa.




Kuvio 11. VPN-verkkojen tyyppejä

### 4.3.3 Fyysinen suojaus

Andreassonin sekä Koiviston mukaan tietoturvaa miettiessä on tärkeää ottaa huomioon verkkolaitteiden fyysinen suojaus. Tällä tarkoitetaan sitä, että laitehuoneisiin, jakamoihin ja muihin verkon tärkeisiin laitetiloihin ei ole ulkopuolisilla pääsyä. Näin voidaan estää, etteivät ei-halutut henkilöt pääse käsiksi verkon haavoittuviin osiin ja täten vahingoittamaan verkkoa tai levittämään haittaohjelmia. (Andreasson & Koivisto 2013.)

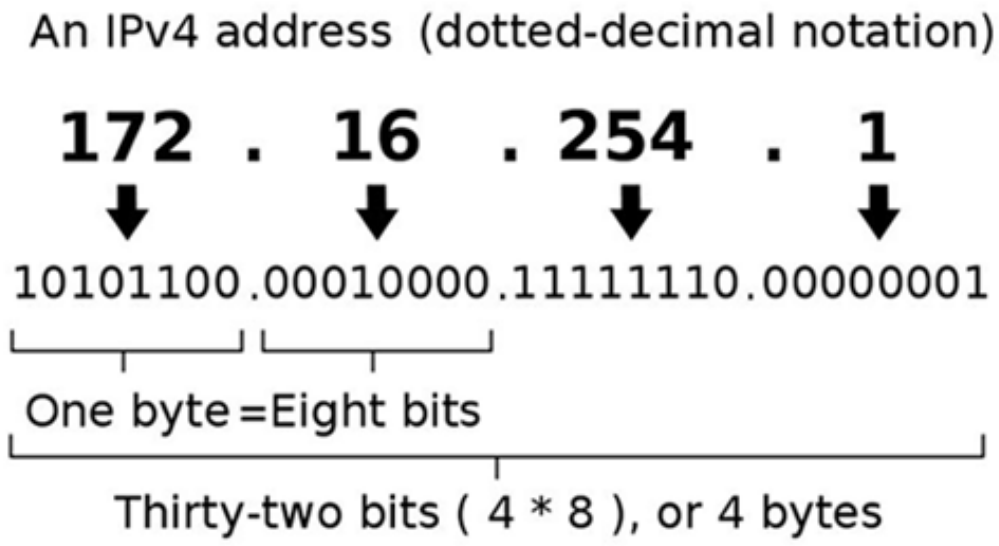
Thomasin mukaan yksinkertaisin tapa suorittaa fyysinen suojaus on lukita ovet. Monissa eri rakennuksissa velvoitetaan pitämään henkilökorttia esillä, jolloin voidaan nopeasti todeta vierailun asianmukaisuus. (Thomas 2005, 371.) Lisäksi Andreasson sekä Koivisto korostavat, että rikollisuuden lisäksi fyysisellä suojauksella ymmärretään myös esimerkiksi tulipaloilta ja vesivahingoilta suojautumista. Onnettomuuksilta suojautumista voidaan parantaa muun muassa kiinnittämällä huomiota laitteiston sijoitteluun rakennuksessa sekä asentamalla tilaan tunnistimia, esimerkiksi paloilmaisimia. (Andreasson & Koivisto 2013.)

## 4.4 Internet Protocol

Jokaisella Internetiin liitetyllä verkkolaitteella on IP-osoite. Jotta verkkoliikenne Internetissä onnistuu, jokainen laite tulee identifioida omalla osoitteella. IP-osoitteen avulla esimerkiksi reitittimet osaavat ohjata datapaketit oikeille laitteille.

Tutkimuksen kannalta on oleellista tuntea IPv4-osoitteen rakenne sekä miten IPv4-osoite määrittyy. Tästä syystä IP-protokollaa tarkastellaan yleiseltä, käyttäjälle olennaiselta, tasolta. IPv6-osoitteen tarkastelua ei tehdä tässä tutkimuksessa.

IPv4-protokollan mukaan erilaisia IP-osoitteita voi olla noin 4,3 miljardia ($256^4$ = 4 294 967 296). IP-osoitteet koostuvat neljästä eri numerosta, jotka ovat erotettu pisteillä (kuvio 12). Jokainen luku on kooltaan kahdeksan bitin eli yhden tavun kokoinen. IP-osoite on siis suuruudeltaan 32 bittiä eli neljä tavua. Yhteen tavuun mahtuu numeroarvoja lukuun 256 asti. (Odom 2005, 217.) Kuviossa 12 esitetään, kuinka binääriset arvot muutetaan ensin lukuarvoiksi ja sen jälkeen IP-osoitteeksi.




Kuvio 12. IPv4-osoitteen määritys (IPv4 2020)

IPv4-protokollan IP-osoitteet voidaan jaotella verkkoluokkiin. Verkkoluokat ovat A, B, C, D ja E. Kolme ensimmäistä luokkaa ovat kaikkein olennaisimmat. Verkkoluokat jakaantuvat kuvion 13 mukaisesti.

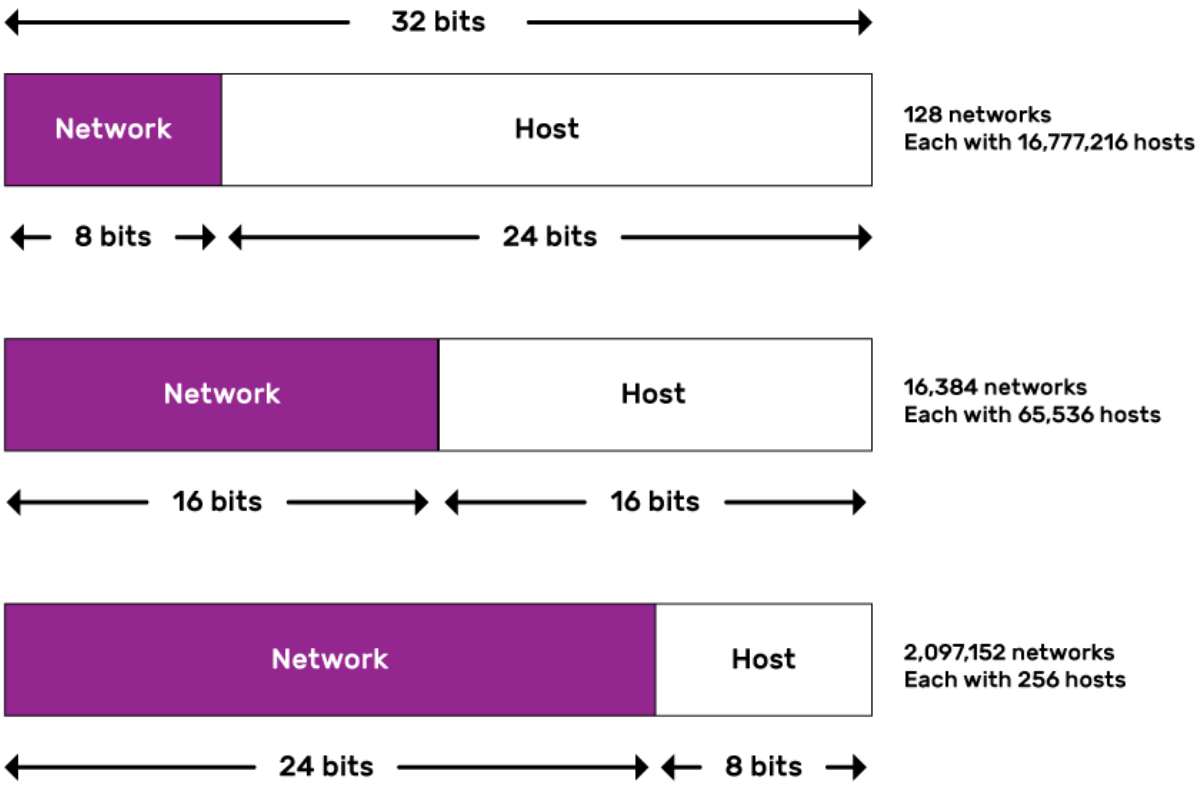
| Address Class | Bit Pattern of First Byte | First Byte Decimal Range | Host Assignment Range in Dotted Decimal |
|---|---|---|---|
| A | 0xxxxxxx | 1 to 127 | 1.0.0.1 to 126.255.255.254 |
| B | 10xxxxxx | 128 to 191 | 128.0.0.1 to 191.255.255.254 |
| C | 110xxxxx | 192 to 223 | 192.0.0.1 to 223.255.255.254 |
| D | 1110xxxx | 224 to 239 | 224.0.0.1 to 239.255.255.254 |
| E | 11110xxx | 240 to 255 | 240.0.0.1 to 255.255.255.255 |

Kuvio 13. IPv4 verkkoluokat (IP addressing concept N.d)

IP-osoitteet koostuvat verkko-osasta sekä isäntäosasta. Verkkoluokka määrittää prefiksin eli osoitteen alkuosan. Alkuosa vaihtelee verkkoluokittain ja esiintyy IP-osoitteessa ensimmäisinä lukuina. (Hunt 1998, 25.) Kotikosken (2021) mukaan verkko- ja isäntäosien tavujen määrä on jaoteltu seuraavasti

- A-luokka
  - Verkko-osa yksi tavu ja isäntäosa kolme tavua
- B-luokka
  - Verkko-osa kaksi tavua ja isäntäosa kaksi tavua
- C-luokka
  - Verkko-osa kolme tavua ja isäntäosa yksi tavu.

Kuviossa 14 on myös esitetty osoiteluokkien rakenteet sekä verkkojen ja kytkettävien laitteiden määrät. Verkko-osasta pystytään tutkimaan kuinka monta verkkoa kyseissä verkkoluokassa voi olla. Isäntäosa taasen kertoo verkkoon liitettävien laitteiden määrän. (Hunt 1998, 25.) Täten voidaan todeta, että A-luokan verkkoja on melko vähän, mutta ne ovat todella laajoja. C-luokan verkkoja on toisaalta todella paljon, mutta niihin voidaan liittää huomattavasti vähemmän verkkolaitteita.




Kuvio 14. Verkkoluokkien määräytyminen (Internet Protocol (IP) Addresses N.d)

## 4.5 Aliverkon peite

Kuten luvussa 4.4 todettiin, verkkoja on olemassa rajallinen määrä. IP-osoitteiden verkko-osan mukaan määräytyvät verkkojen koot ovat samassa verkkoluokassa aina samankokoisia. Tosielämässä fyysiset verkot ovat yleensä aina eri kokoisia, joten aina tarvitaan eri määrä IP-osoitteita. Aliverkon peitteen avulla pystytään rajaamaan vakiomuotoisia verkkoja pienempiin kokonaisuuksiin, jolloin IP-osoitteita ei mene hukkaan. (Hakala ym. 2005, 196.) Kuviossa 15 on esitetty IP-osoitealueet sekä luokitellut aliverkkojen peitteet. Käytössä voi olla esimerkiksi A-luokan verkko, mikä on todella suuri. Tätä verkkoa voidaan rajata käyttämällä esimerkiksi C-luokan aliverkon peitettä, jos verkosta halutaan rajata pieni osa. IP-osoitteita ja aliverkon maskeja voi rajata parhaiten katsomallaan tavalla tarpeiden mukaan.

Aliverkon peitteen toinen tärkeä tehtävä on kertoa, onko IP-osoite paikallinen vai etäosoite. Voidaan todeta, että IP-osoitteet ovat paikallisia, jos niillä on sama verkko-osa eli ne ovat osana samaa verkkoa. Etäosoitteet sijaitsevat eri verkoissa. Tämä vaikuttaa erityisesti verkkoliikennöintiin. (Meyers 2003, 311.) Jos lähettävä kone havaitsee vastaanottavan koneen olevan oman aliverkon ulkopuolella, lähetys tapahtuu oletusyhdyskäytävän (eng. default gateway) kautta. Oletusyhdyskäytävänä voi olla esimerkiksi reititin tai palomuuri. Jos laitteet ovat samassa aliverkossa, lähetys tapahtuu verkon sisällä.

IP addresses classes and Default subnet mask

| Class | IP address ranges | Default subnet mask |
|---|---|---|
| A | 0.0.0.0 to 127.255.255.255 | 255.0.0.0 |
| B | 128.0.0.0 to 191.155.255.255 | 255.255.0.0 |
| C | 192.0.0.0 to 223.255.255.255 | 255.255.255.0 |
| D | 224.0.0.0 to 239.255.255.255 | Not applicable |
| E | 240.0.0.0 to 255.255.255.255 | Not applicable |

Kuvio 15. IP-osoitealueet sekä aliverkot peitteet

Aliverkon peitteet voidaan esittää kahdella eri tavalla. Tyypillisin tapa on muuntaa aliverkon peite binäärimuotoon, jolloin luvusta on helppo laskea nollat ja ykköset. Binäärimuoto on oleellinen, koska numeroiden avulla aliverkon peitteestä voidaan tutkia verkko- ja isäntäosien pituudet. Ykköset ovat aina verkko-osaa ja nollat ovat aina isäntäosaa. (Meyers 2003, 311.) Esimerkiksi peitteessä 11111111.11111111.11111111.00000000 verkko-osa on 255.255.255.0, koska kolme ensimmäistä tavua muodostavat jokainen luvun 255. Viimeinen tavu muodostaa luvun nolla.

Aliverkon peitteet voidaan esittää myös pistedesimaalimuodossa, kuten IP-osoitteetkin. Esimerkiksi verkon 201.23.45.123/24 IP-osoite on 201.23.45.123 ja aliverkon peite on 255.255.255.0. (Meyers 2003, 312.) Kauttaviiva kertoo, kuinka monta ykköstä binäärimuotoisessa esityksessä on. Kun luvun 24 jakaa kolmella, saadaan luku kahdeksan. Tämä vastaa binäärilukuna arvoa 255 eli aliverkon peitteen verkko-osaksi muodostuu yllä mainittu 255.255.255.0.

Jaetaan esimerkin vuoksi C-luokan verkko 205.40.100.0/24 kahdeksi aliverkoksi. /24 vastaava aliverkon peite on binäärimuodossa 11111111111111111111111100000000. Isäntätunnuksessa on kahdeksan bittiä ja kaikkien arvo on nolla. Aliverkkoja luodessa aliverkon peitettä täytyy jatkaa oikealle, jolloin isäntäosa pienenee. Tämä tarkoittaa sitä, että verkkojen koko kutistuu. (Meyers 2003, 314–318.) Aliverkon peitettä jatketaan oikealle yhdellä bitillä. Isäntäosaan jää seitsemän bittiä eli verkon koko on tällöin 128. Ensimmäinen uusi verkkotunnus on 11001101.00101000.01100100.00000000 = 205.40.100.0/25. Tämä verkko kattaa osoitteet välillä 205.40.100.0 ja 205.40.100.127. Toinen uusi verkkotunnus on 11001101.00101000.01100100.10000000 = 205.40.100.128/25. Tämä verkko kattaa osoitteet välillä 205.40.100.128 ja 205.40.100.255. Muunnoksessa luotu aliverkon peite on 255.255.255.128.

# 5 Tutkimuksen toteutuminen

## 5.1 Käytössä oleva laitteisto

Opinnäytetyön verkkolaitteisto on Siemensin valmistama. Laboratorion automaatiolaitteisto koostuu myös Siemensin komponenteista. Käytettäessä saman valmistajan laitteita vältytään ylimääräisiltä laiterajapinnoilta, jolloin konfigurointi ja käyttöönotto helpottuu. Tarvittava parametrointi saadaan tehtyä TIA Portalilla eli laitteiden asetukset voidaan vaihtaa käyttäen yhtä ohjelmistoa.

Tutkimukseen hankittavat verkkolaitteet ovat uusia. Jännitelähde on kuitenkin purettu vanhasta räkistä eli se on ollut jo aiemmin käytössä. Tutkimuksessa täytyy analysoida jännitelähteen ominaisuuksia, jolloin voidaan varmistua, että laite soveltuu myös osaksi uutta kokonaisuutta.

### 5.1.1 Siemens SCALANCE XC208

Tutkimuksessa luotavan verkon kytkimeksi valikoitui Siemensin SCALANCE XC208 (kuvio 16). SCALANCE-sarjan kytkin valittiin tutkimuksen komponentiksi, koska automaatiolaitteisto koostuu kokonaisuudessaan Siemensin valmistamista komponenteista. Konfigurointi helpottui, kun kaikki laitteet ovat saman valmistajan tekemiä. (Adling 2019.) Tulevaisuudessa verkon laajentaminen on myös vaivattomasti toteutettavissa, kun laitteiden osalta ei ole eri valmistajien välisiä rajapintoja.

XC208-kytkimet suositellaan kytkemään renkaaksi ja parametroimaan MRP-protokolla käyttöön. Tällöin verkon vikasietoisuus lisääntyy. Vikatilanteessa kytkimet pystyvät määrittämään uudelleenreitityksen 200 millisekunnin kuluessa. Sama protokolla voidaan parametroida käyttöön kaikille tutkimuksen verkkolaitteille. (Adling 2019.)


Kuvio 16. Siemens SCALANCE XC208 (6GK5208-0BA00-2AC2 2019)

Tietoturva on myös otettu huomioon XC208-kytkimessä. Asetusten muuttamista varten käyttäjän täytyy syöttää oikea salasana. Toinen vaihtoehto on käyttää pääsylistoja (eng. ACL = Access Control List). Listoille on määritetty käyttäjät, joille on annettu oikeudet kytkimen asetusten muokkaamiseen. (Adling 2019.) Kolmas vaihtoehto tietoturvan lisäämiseen on kytkeä tarpeettomat portit pois käytöstä, jolloin ulkopuolisilla henkilöillä ei ole pääsyä kytkimen sisälle. Ylimääräiset portit voidaan myös lukita fyysisillä lukoilla, jolloin tarpeeton pääsy saadaan evättyä. (Network security 2020.)

XC208-kytkimessä on kahdeksan RJ-45 -liityntää. Tämä määrä riitti tutkimuksessa rakennettavan verkon tarpeisiin. Osa porteista jäi kuitenkin vapaaksi ja niitä voidaan hyödyntää esimerkiksi tulevaisuudessa verkkoa laajentaessa. Kytkin tukee Ethernet-protokollaa ja kytkin konfiguroidaan TIA Portalilla, joten voidaan todeta, että kytkin sopii tarkasteltavien osa-alueiden osalta tutkimukseen. (Data sheet 6GK5208-0BA00-2AC2 2019.)

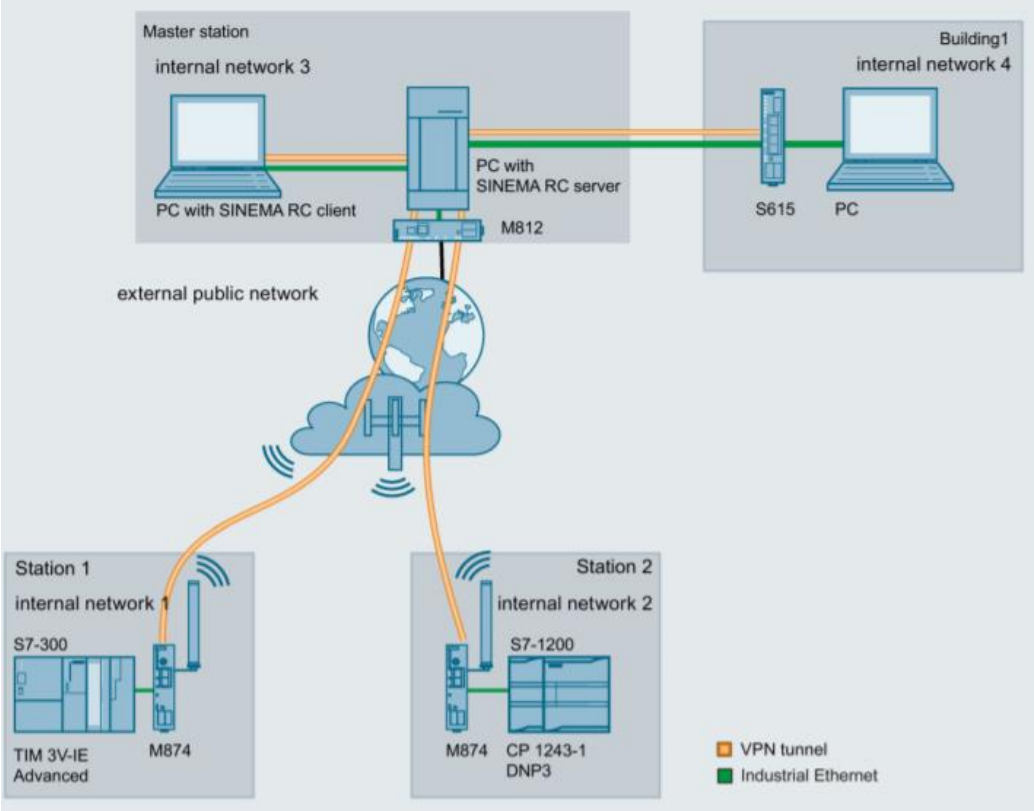
### 5.1.2 Siemens SCALANCE S615

Tutkimuksen verkkoon valittiin reitittimeksi Siemens SCALANCE S615 (kuvio 17). Reitittimessä on viisi RJ-45 -porttia. Neljä porttia on ulospäin suuntautunutta verkkoliikennettä varten. Yksi porteista on sisään tulevaa liikennettä varten. (Network security 2020.) S615-reititin on suunniteltu toimimaan samassa verkossa muiden Siemensin verkkolaitteiden kanssa eli soveltuu käytettäväksi XC208-kytkimen sekä SC636-2C -palomuurin kanssa.


Kuvio 17. Siemens SCALANCE S615 (6GK5615-0AA00-2AA2 N.d)

S615-reitittimen tietoturvassa olennaisimpana osana on VPN ja salattu verkkoliikenne. Tällä keinolla pyritään lisäämään etäyhteyksiä sekä turvaamaan tiedonsiirtoa. Etäyhteys vähentää huoltoaikoja, kun voidaan tehdä ennakkohuoltoa sekä valvontaa. Reitittimen tietoturvaan liittyy myös vahvat salasanat ja NAT (eng. Network Address Translation) eli IP-osoitemuunnos. (Industrial Ethernet Security SCALANCE S615 Web Based Management 2020.)

S615-reititintä käytettäessä voidaan hyödyntää Siemensin SINEMA RC -yhteyttä. Tällä yhteydellä kyetään tekemään huolloista, verkkoliikenteen monitoroinnista sekä valvonnasta huomattavasti joustavampia. (Operating instructions 2015.) Kuviossa 18 on esitetty, kuinka SINEMA RC -serveriltä voidaan ottaa VPN:än kautta yhteys reitittimiin ja täten ohjata sekä monitoroida laitteita turvallisesti. Tämä mahdollistaa laitteistojen etäoperoinnin paikkaan sitomatta.




Kuvio 18. SINEMA RC (Configuration manual 2020)

### 5.1.3 Siemens SCALANCE SC636-2C

SCALANCE SC636-2C -palomuuri (kuvio 19) on prosessiteollisuudessa käytettävä verkkolaite, jonka tehtävänä on suojata teollisuudessa tapahtuvaa tiedonsiirtoa (Data sheet 6GK5636-2GS00-2AC2

2019). Palomuuri analysoi verkkoliikennettä verkon sisäisten ja ulkoisten osien rajapinnassa. SC636-2C on valittu tutkimuksessa käytettäväksi palomuuriksi.

Kuvio 19. Siemens SCALANCE SC636-2C (6GK5636-2GS00-2AC2 2020)

Palomuurin tietoturva perustuu vahvan salasanan luomiseen sekä NATiin. Ylimääräiset verkkoliitynnät voidaan sulkea fyysisillä lukoilla, jotka käyvät RJ-45 -liityntään. (Network security 2020.) Kuviossa 20 on esitetty RJ-45 -liittimeen sopiva lukko. Lukoilla voidaan estää ulkopuolisten pääsy verkkolaitteen liityntöihin. Lukkojen käyttö on yksinkertaista, koska niiden asentamiseen ei vaadita työkaluja. (IE RJ45 port lock n.d.) RJ-45 -lukkojen hinta on noin 50 €/kappale. Portteja jää vapaaksi yhteensä noin 15 kappaletta, jolloin lukkojen yhteishinnaksi tulisi 750 €.

SC636-2C -palomuuri tukee OpenVPN-yhteyttä (Network security 2020). Tämä mahdollistaa etäyhteyden luomisen verkkoon käyttämällä laboratoriossa olevaa tietokonetta, joka on yhteydessä oppilaitoksen lähiverkkoon. VPN-yhteys on tärkeä osa tutkimuksessa rakennettavaa verkkoa sekä etäkäyttöä. Palomuuriin voidaan ottaa yhteys käyttämällä SINEMA RC -yhteyttä, jolloin voidaan monitoroida palomuurin toimintaa sekä tarvittaessa muuttaa asetuksia. Palomuurin ominaisuudet täyttävät tutkimuksen asettamat vaatimukset.


Kuvio 20. Siemensin RJ-45- lukko (IE RJ45 port lock N.d)

### 5.1.4 Powernet ADC5723

Jännitelähdettä valittaessa tärkein huomioon otettava asia on sisään- ja ulostulevan jännitteen suuruus. ADC5723-jännitelähde (kuvio 21) muuntaa 230V vaihtojännitteen 24V tasajännitteeksi. Luvuissa 5.1.1 sekä 5.1.2 esitellyt verkkolaitteet tarvitsevat 24V tasajännitteen toimiakseen (Data sheet 6GK5208-0BA00-2AC2 2019; Data sheet 6GK5636-2GS00-2AC2 2019).


Kuvio 21. Jännitelähde ADC5723 (ADC5000 SERIES 2017)

Jännitelähteen valintaperusteena toiseksi tärkein ominaisuus on jännitelähteen tuottama teho. Teholukeman täytyy olla suurempi kuin verkkolaitteiden vaatima teho, jotta laitteet toimivat. Verkkolaitteiden ottotehot ovat

- XC208-Kytkin
  - tehontarve: 4.2W (Data sheet 6GK5208-0BA00-2AC2 2019)
- SC636-2C-Palomuuri
  - tehontarve: 9.6W (Data sheet 6GK5636-2GS00-2AC2 2019)
- S615-reititin
  - tehontarve: 3W (Operating instructions 2015).

Kytkimiä on kaksi kappaletta, palomuureja on yksi kappale ja reitittimiä on myös yksi kappale. Täten kokonaistehon tarve on

$$4.2W + 4.2W + 9.6W + 3W = 21W.$$

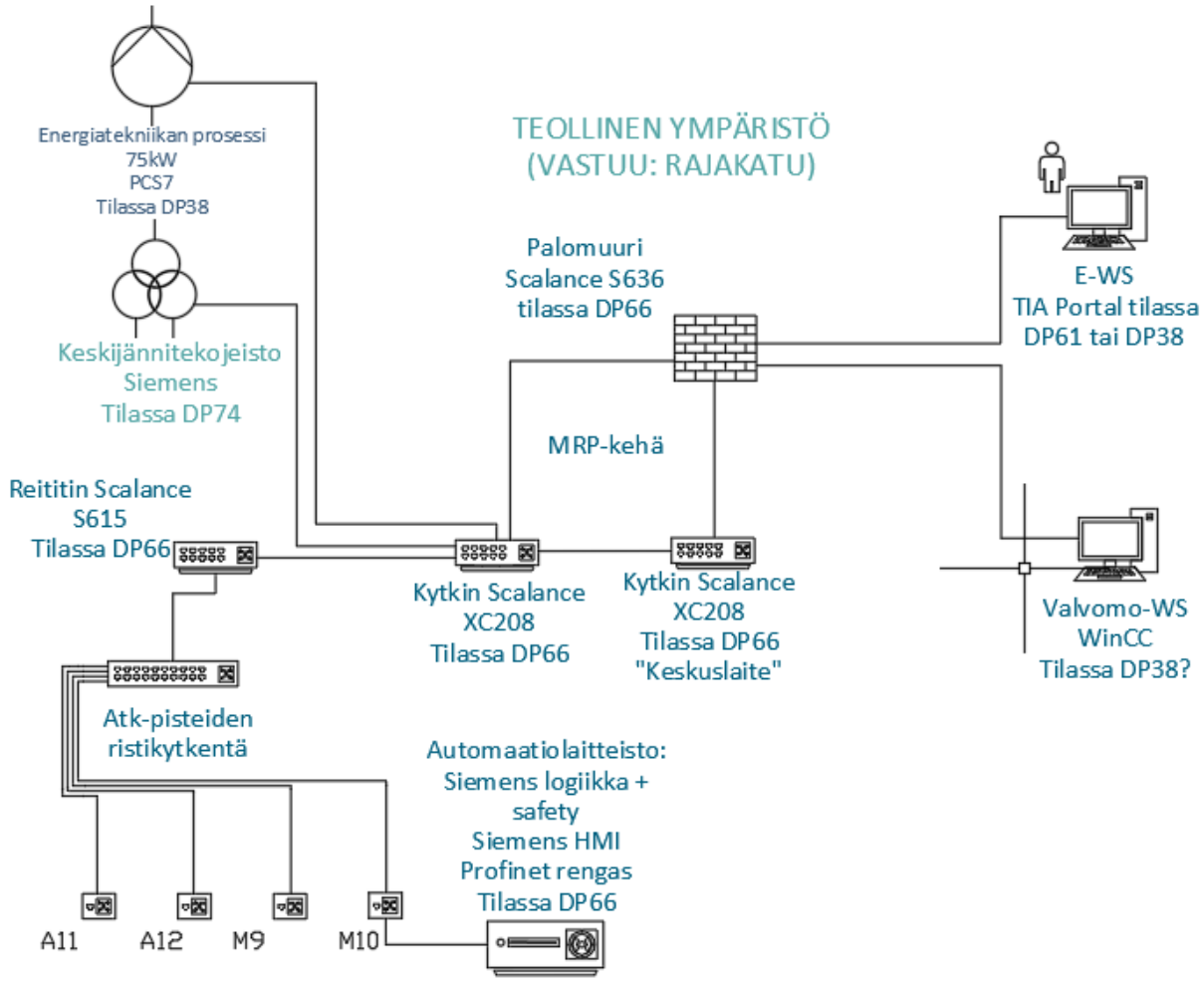
Jännitelähteen tuottama teho on 60W (Data sheet/User manual 2017). Voidaan todeta, että 60W > 21W, joten jännitelähteen tuottama teho riittää kattamaan verkkolaiteiden ottaman tehon. Jännitelähde asennetaan DIN-kiskoon, mikä on soveliain asennustapa tutkimuksessa käytettävään laiteräkkiin (Data sheet/User manual 2017). Jännitelähteen muuntama jännite sekä tehontuotto ovat tarvittavan suuruiset, joten todetaan, että jännitelähde soveltuu tutkimukseen.

## 5.2 Verkon rakenne ja topologia

Hämäläinen (2021) sekä Pyykkö ja Torvinen (2021) esittävät eriävät näkemykset tutkittavan verkkoympäristön topologioille. Hämäläinen ehdottaa topologiavalinnaksi kahdennettua tähtiverkkoa. Tähtiverkko olisi käyttäjäystävällisin ja toimintavarmin ratkaisu. Verkkokaapeleiden kahdennus toisi myös lisää luotettavuutta verkon toiminnalle vikatilanteissa. (Hämäläinen 2021.) Pyykkö ja Torvinen (2021) puolestaan korostavat rengastopologian etuja käytettäessä Siemensin valmistamia verkkolaitteita. Siemensin laitteet tukevat MRP-protokollaa, joka on teollisessa ympäristössä yleisesti käytössä oleva protokolla. Pyykkö ja Torvinen painottavat MRP-protokollan uudelleenreititysominaisuutta kytkettäessä laitteet renkaaseen. Verkkolaitteet osaavat etsiä vikatilanteen sattuessa tiedonsiirrolle vaihtoehtoisen reitin 200 millisekunnin kuluessa, jolloin tietoliikenne ei ehdi katketa. (Pyykkö & Torvinen 2021; Setup of a Ring Topology Based on “MRP” 2016, 4.)

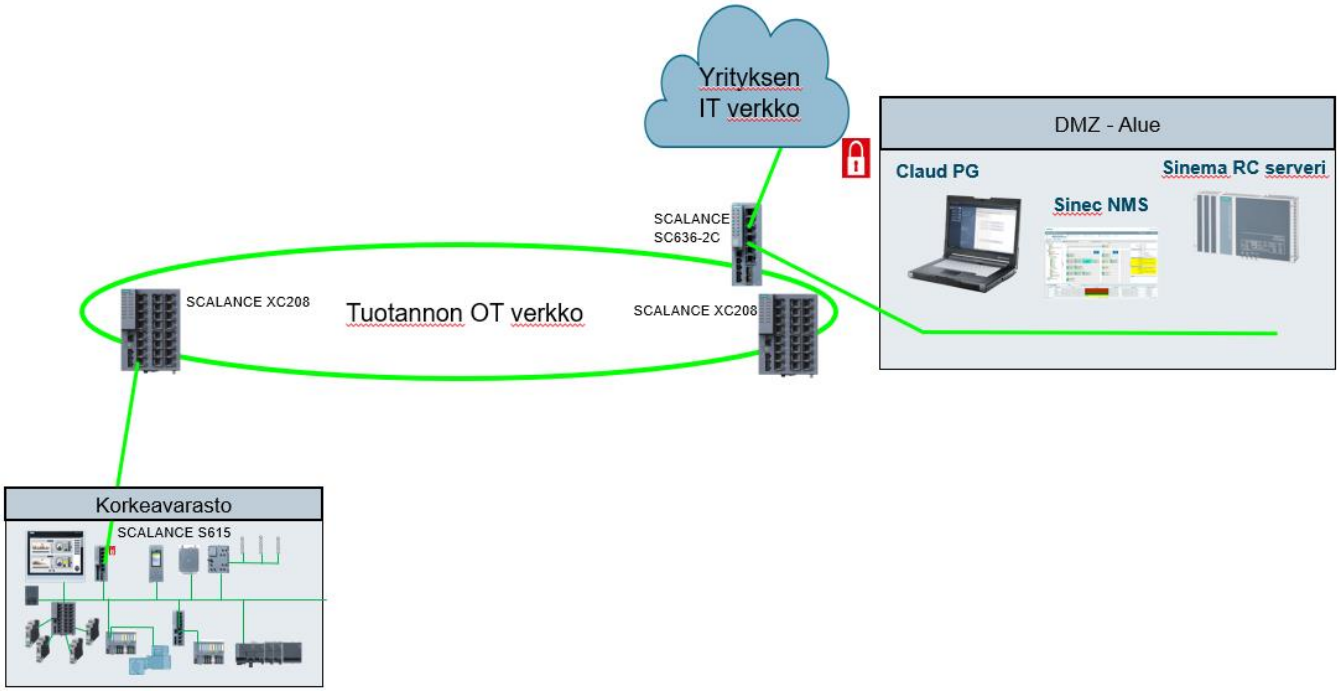
Tutkimuksessa rakennettavan verkon topologiaksi valitaan rengasverkko (ks. luku 3.1.2), koska työssä pyritään mukailemaan OT-verkkoa. Rengastopologia on teollisessa ympäristössä yleisesti käytetty verkkotyyppi. Rengasverkon etuja ovat pienet kustannukset, yksinkertainen layout, nopea uudelleenreititys vikatilanteessa sekä standardisoidut protokollat laitevalmistajien kesken, jolloin voidaan yhdistää eri valmistajien laitteita. Yhteensopivien laitteiden täytyy olla standardin IEC 62439 mukaisia. (Setup of a Ring Topology Based on “MRP” 2016, 4–5.)

Siemensin laitemanuaalin mukaan verkkolaitteet tukevat kaikkia topologioita, mutta rengastopologia soveltuu tutkimukseen parhaiten. (Network security 2020.) Useiden topologiamahdollisuuksien ansioista verkon rakennetta voidaan kuitenkin halutessa muokata ilman että tarvitsee hankkia kokonaan uusia komponentteja. Tästä johtuen laboratoriossa voidaan tulevaisuudessa analysoida erilaisten verkkoratkaisujen käyttäytymistä sekä ominaisuuksia. Tämänhetkinen verkkorakenne on esitetty kuviossa 22. Yhtenäiset viivat ovat toteutuvia ratkaisuja. Katkoviivoilla esitettyjä laitteita analysoidaan ja yhdistetään verkkoon mahdollisesti tulevaisuudessa.




Kuvio 22. Tietoverkon rakenne

Tutkimuksen verkko koostuu neljästä eri osasta (kuvio 23). Korkeavarasto-osuus kattaa automaatiolaitteiston sekä SCALANCE S615 -reitittimen. Tuotannon OT -verkko käsittää laboratoriotilassa olevan verkkoräkin komponentit ja kaapeloinnin. Kuviossa 23 näkyy myös räkkilaitteiden keskinäinen kytkentä eli topologia. DMZ-alue toimii eteisverkkona tutkimuksen lähiverkolle. Itkonen (2018) on tutkinut opinnäytetyössään DMZ-alueen merkitystä osana teollisuusverkkoa. Hän toteaa, että eteisverkon tehtävänä on toimia puskurina sisäisen ja ulkoisen verkon välillä. DMZ-alueella on suuri merkitys tietoturvan parantamisessa sekä verkkoliikenteen valvonnassa. (Itkonen 2018, 38–39.) Yrityksen IT -verkko edustaa Jyväskylän ammattikorkeakoulun Rajakadun kampuksen omaa lähiverkkoa. Jokaiselle alueelle määritetään omat IP-osoitealueet. Laitteiden konfigurointia tutkitaan tarkemmin luvussa 5.4.




Kuvio 23. Verkon osat

## 5.3 Verkon rakennus

### 5.3.1 Alkuvalmistelut

Verkon rakentaminen aloitettiin kartoittamalla tilanne laboratoriossa. Aluksi tarkastettiin tutkimusta varten hankittavat laitteet sekä laboratorion tilat, joihin verkko on tarkoituksena rakentaa. Laboratoriossa oli valmiina Metso DNA -laitekaappi, josta muokattiin alusta verkkolaitteille. Oppilaitoksen lähiverkossa olevia atk-pisteitä valjastettiin myös osaksi tutkimuksen verkkoa kytkemällä ne irti oppilaitoksen verkosta. Samalla laboratorion yleistä layoutia muokattiin, jolloin käyttäjän on helpompi työskennellä räkin ympäristössä ja mahdollisten harjoitusten tekeminen onnistuu. Tilan muokkauksessa otettiin huomioon myös automaatiolaitteisto, joka vaati huomattavasti tilaa. Kuvissa 24 näkyy laboratorion uusi layout. Vasemmalla olevalle verkkoräkille sekä oikean reunan automaatiolaitteistolle on esteetön pääsy.

Kuvio 24. Laboratorion uusi layout

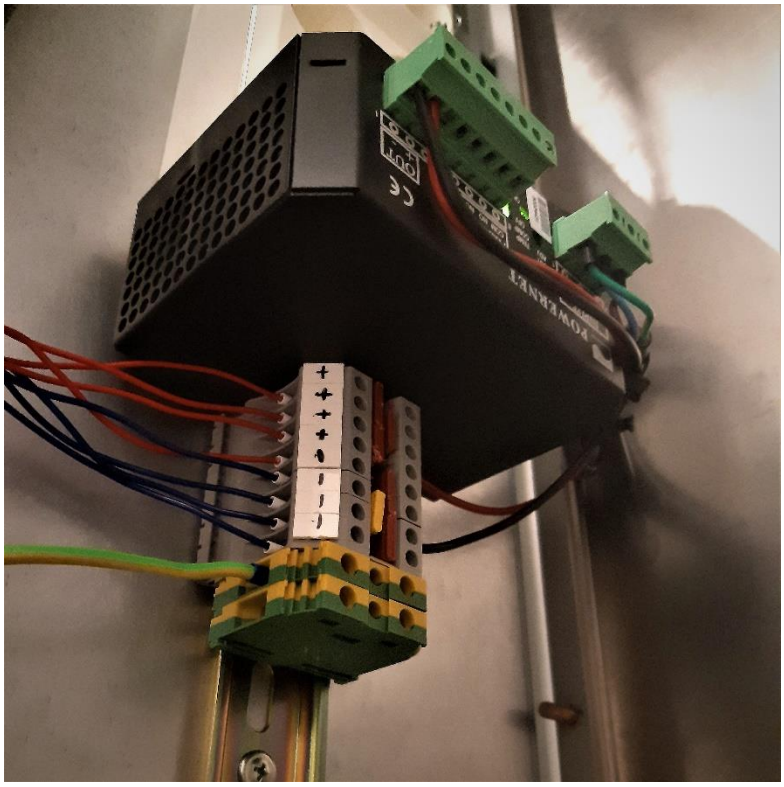
Metso DNA -laitekaappi soveltuu tutkimuksen tarpeisiin. Kaappiin oli jäänyt paljon erilaisia atk-laitteita sekä keskusyksiköitä, jotka olivat tarpeettomia. Ennen kuin laitekaapin layoutia voitiin suunnitella, kaappi täytyi siivota ja tarpeettomat laitteet piti siirtää pois. Lopulta kaappiin jäi ainoastaan yksi käytössä oleva Valmet DNA -järjestelmään liittyvä kytkin. Jyväskylän ammattikorkeakoulun henkilökunnan kanssa päätettiin, että kyseinen kaappi rakennetaan täysin verkkoliikennettä varten. Täten kaappiin ei asenneta laitteita, jotka eivät liity tietoliikenteeseen.

### 5.3.2 Laitteiden asennus ja jännitekaapelointi

Kaappiin asennettavia verkkolaitteita oli yhteensä neljä kappaletta ja jännitelähteitä oli yksi kappale. Verkkolaitteet asennettiin kaappiin omaksi kokonaisuudeksi keskelle räkkiä, jolloin vapaata tilaa jäi runsaasti tulevaisuutta varten ja verkkokaapeleiden ei tarvinnut olla kovin pitkiä. Kuviossa 25 on esitetty siistitty räkki.

Kuvio 25. Verkkolaiteräkki valmiina kaapelointiin

Jännitelähde oli aiemmin käytössä samassa räkissä. Aiempi asennus oli tehty huolimattomasti ja kosketussuojaus ei ollut riittävä. 230 voltin vaihtojännite oli kytketty riviliittimille. Kytkentä oli tehty heikosti, koska osa johtimista oli paljaina. Tällaisessa kytkennässä on riskinä, että käyttäjä saa vaarallisen sähköiskun. Vanha kytkentä purettiin ja vaarallinen vaihtojännite kytkettiin suojattuun pistorasiaan, jolloin kosketussuojaus täyttyi vaihtojännitteen osalta. Pistorasia kytkettiin syöttämään jännitelähdettä, jonka ulostuleva 24 voltin pienoisjännite kytkettiin riviliittimiin. Riviliittimiä tosin ei pystytty täysin suojaamaan kosketukselta, mutta Hongan, Korhosen ja Tammisen (2019, 4) mukaan pienoisjännitteen sekä virran suuruus ovat niin pienet, ettei käyttäjälle sähköiskun tilanteessakaan aiheudu hengenvaaraa. Lisäksi johtimien päät holkitettiin ja kytkettiin huolellisesti, jolloin sähköiskun vaara pieneni. Sähköiskujen mahdollisuus pyrittiin minimoimaan. Kuviossa 26 näkyy riviliittimet sekä jännitelähde.



Kuvio 26. Tasajännitelähteen kytkentä

Jännitelähteen asennuksen jälkeen räkki oli valmiina kaapelointia varten. Kuvioissa 26 ja 27 näkyy kuinka 24 voltin tasajännite on kytketty riviliittimiltä verkkolaitteille. Kaapelointi toteutettiin käyttämällä KLMA 4x0.8+0.8 -kaapelia. Kaapelista erotettiin ainoastaan punainen sekä sininen johdin käyttöön, koska ne edustavat yleisesti plus- ja miinusnapoja.

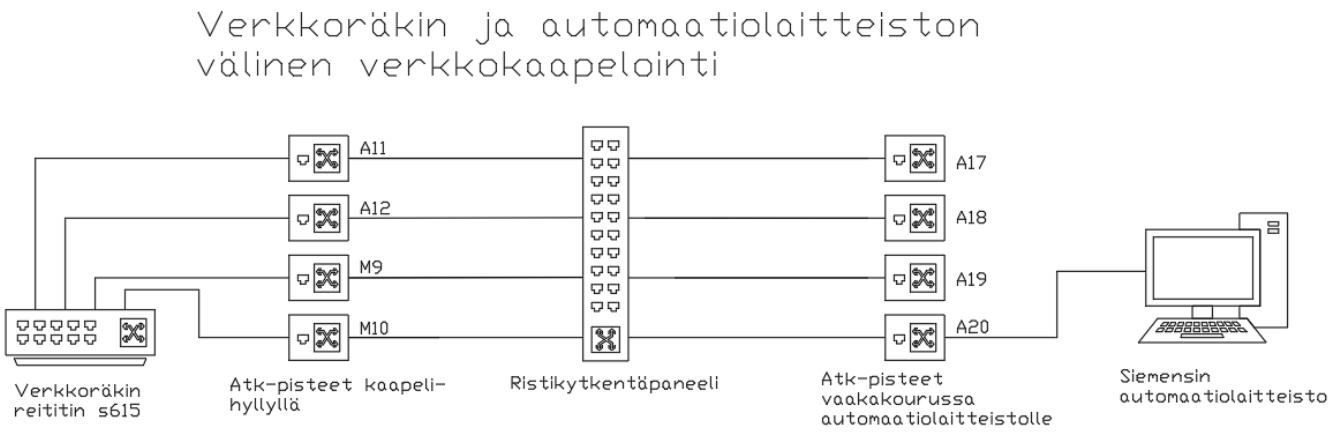
Kuvio 27. Verkkolaitteiden asennus ja kaapelointi

### 5.3.3 Ristikytkentä sekä verkkokaapelointi kentällä

Hämäläisen (2021) mukaan verkkokaapeleiden kytkentä tulee suorittaa ristikytkentäkaapilla. Tällöin kaikki liikenne kulkee ristikytkennän kytkimen kautta. Jyväskylän ammattikorkeakoulun tietohallinnolla on myös parempi käsitys laboratorion verkon rakenteesta, kun laboratorioon ei ole tehty omia kytkentöjä vaan kaikki muokkaukset on tehty sovitusti ja ristikytkentäpaneelin kautta. (Hämäläinen 2021.)

Laboratorion kaapelihyllyllä oli neljä ylimääräistä atk-pistettä. Nämä pisteet kytkettiin osaksi suljettua verkkoa. Verkkoliityntää varten riittää yksi piste, mutta vikaantumiset huomioon ottaen valittiin useampi piste. Verkkoräkin reitittimeltä lähtevät neljä kaapelia kytkettiin atk-pisteisiin. Atk-

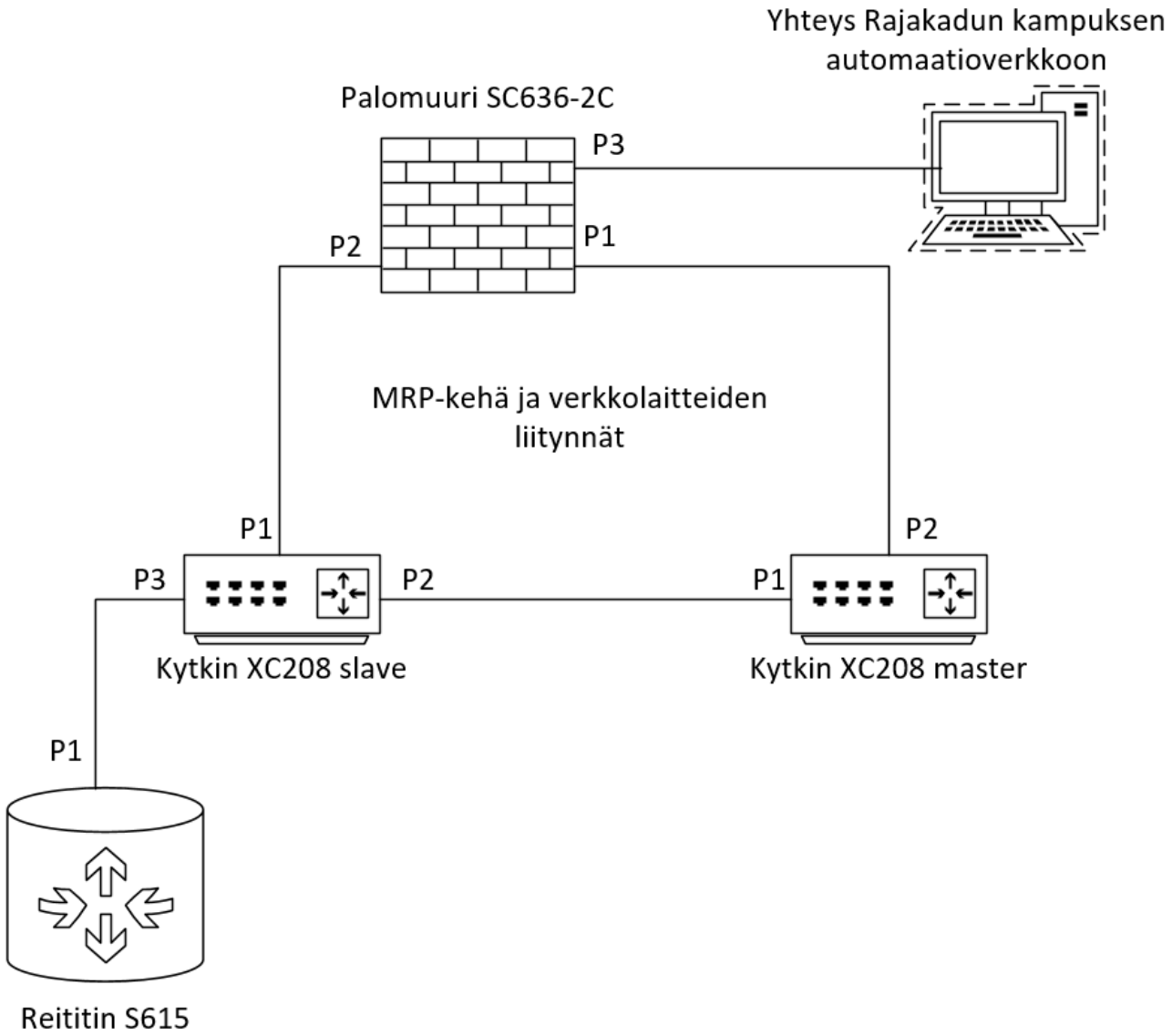
pisteet sekä varsinaiset atk-rasiat yhdistettiin ristikytkentäpaneelissa yhteen, jolloin saatiin muodostettua yhtenäinen reitti. Näin saatiin luotua verkkoräkiltä yhteys atk-pisteiden ja ristikytkennän kautta automaatiolaitteistoon lähellä oleville rasioille, joista saatiin kaapelilla yhteys automaatiolaitteistoon. Laboratorion verkkokaapelointitoteutus on esitetty kuviossa 28.




Kuvio 28. Verkkokaapelointi räkin reitittimeltä automaatiolaitteistoon

## 5.4 Konfigurointi

Konfigurointi aloitettiin kytkemällä räkin verkkolaitteet topologian mukaisesti Ethernet-kaapeleilla. Kuviossa 29 on esitetty kaapeleiden kytkentä sekä käytetyt RJ-45 -portit. Siemensin verkkolaitteet ovat jo valmiiksi parametroitu käyttämään ensimmäisiä liityntäportteja. Oletusparametrointi helpottaa konfigurointia sekä vähentää virheiden mahdollisuutta. Kytkennät tehtiin porteille P1-P2, koska ne ovat oletusvalintoina MRP-kehää varten (Pyykkö & Torvinen 2021). Konfigurointia tehdessä MRP-kehään kytkettiin ylimääräinen Ethernet-kaapeli, jonka kautta laitteille asetettiin parametrit tietokoneelta.



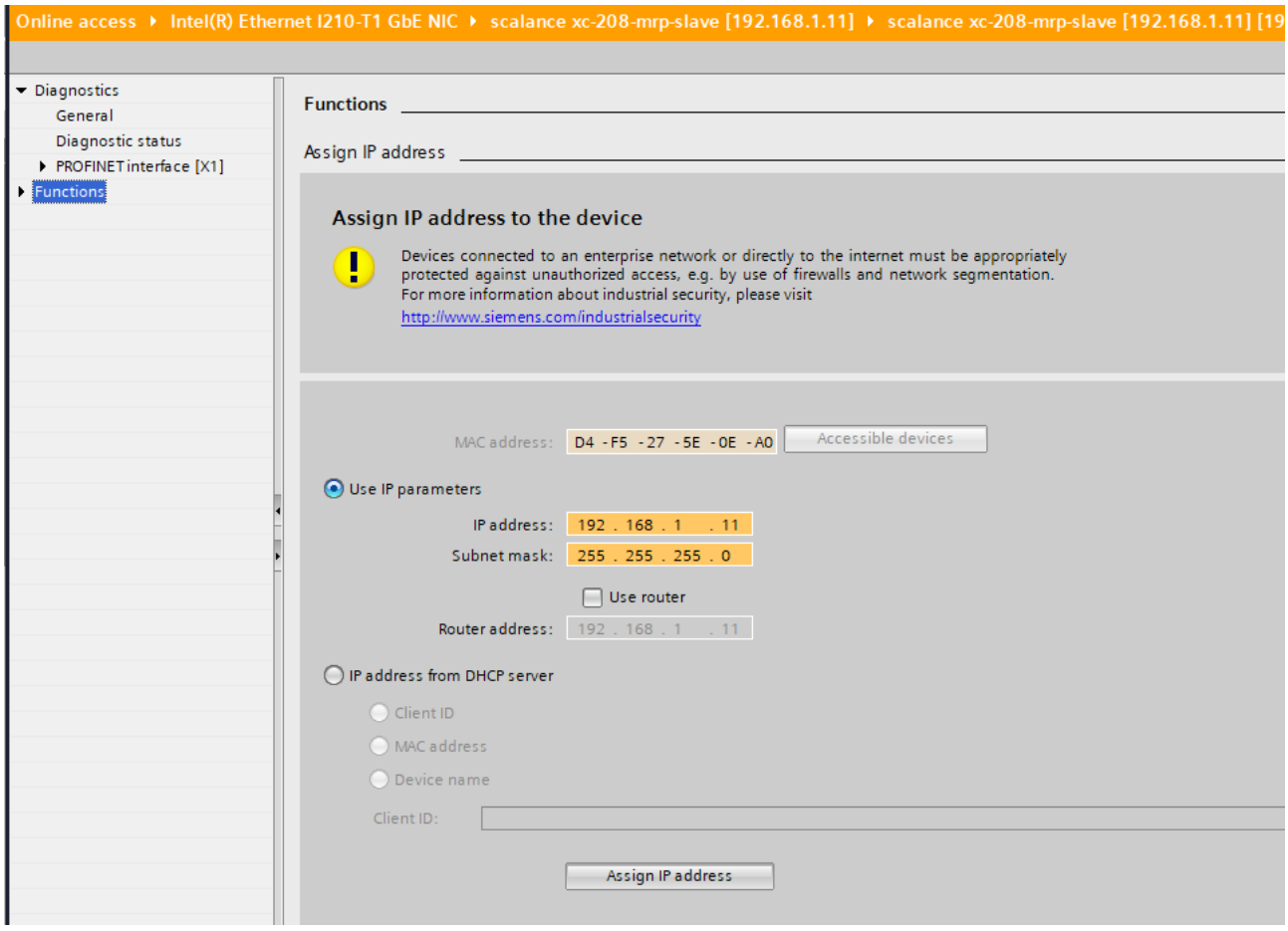

Kuvio 29. Verkkolaitteiden liitynnät

Ensimmäiset asetettavat parametrit olivat laitteiden IP-osoitteet. Verkkolaitteilla ei ole oletuksena IP-osoitteita. Tämä vaihe suoritettiin ensimmäiseksi, jotta saatiin luotua yhteys laitteisiin. Kun IP-osoitteet oli asetettu, laitteiden parametreja voitiin muokata selaimen kautta. (Learn-/Training Document 2019.)

Pyykkö ja Torvinen (2021) ovat määrittäneet verkoille seuraavat IP-osoiteavaruudet

- Korkeavarasto 192.168.0.x /24
- OT-verkko 192.168.1.x /24
- IT-verkko 192.168.2.x /24
- DMZ-alue 192.168.3.x /24.

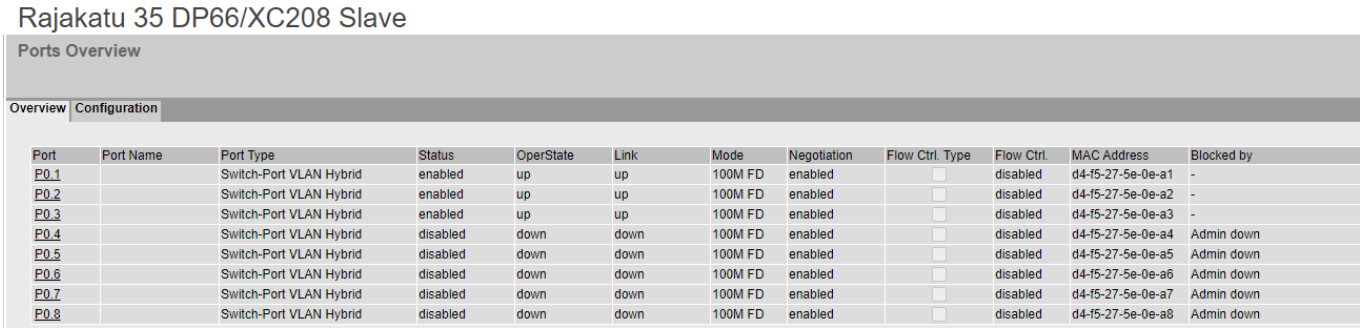
Hämäläinen (2021) määritti lisäksi testausta varten Rajakadun automaatioverkosta IP-osoitteen. Määritettyä IP-osoitetta voidaan hyödyntää laboratorion sisäisessä testauksessa. IP-osoitteet asetettiin laitesijaintien mukaan, kuten kuviossa 23 on esitetty. Samassa verkossa sijaitsevien laitteiden IP-osoitteiden alkuosat ovat aina samat, mutta viimeinen numero erottaa laitteet toisistaan. Osalle laitteista jouduttiin asettamaan kahden tai useamman verkon IP-osoite. Esimerkiksi S615-reitittimelle jouduttiin asettamaan sekä korkeavaraston että OT-verkon IP-osoite, koska laite sijaitsee molemmissa verkoissa. Kuviossa 30 näkyy XC208-slave -kytkimelle asetettu IP-osoite.




Kuvio 30. XC208 slaven IP-osoite

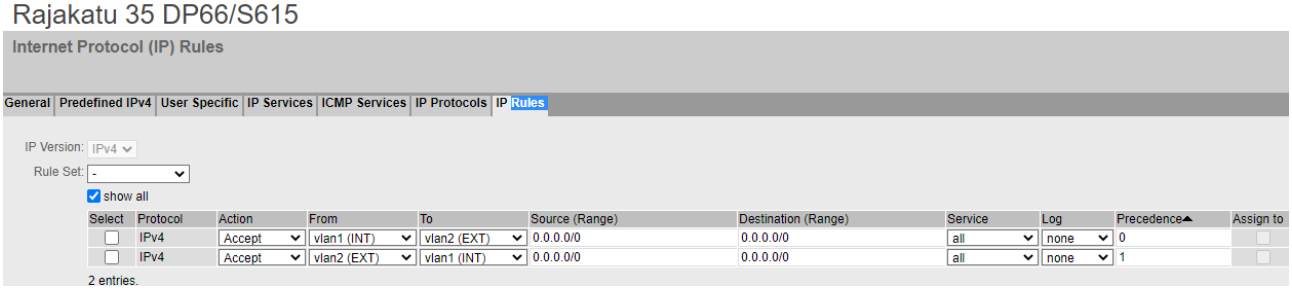
IP-osoitteiden jälkeen määritettiin käyttöön MRP-kehä sekä laitteiden hierarkia. Yksi XC208-kytkin määritettiin MRP-masteriksi ja muut kehään liitetyt laitteet määritettiin MRP-slaveiksi. Näin ollen yksi kytkin valvoo ja ohjaa kehässä tapahtuvaa tietoliikennettä sekä korjaa reititystä vikatilanteessa. Samalla määritettiin myös topologiaan liittyvät verkkoportit. Siemensin verkkolaitteissa MRP-oletusportit ovat yleisesti P1 ja P2, joten niitä ei tarvinnut muuttaa. (Pyykkö & Torvinen

2021.) Seuraavaksi täytyi huomioida muut käyttöön tulevat portit. Esimerkiksi XC208 slave -kytkimen P3-portti tuli käyttöön, jotta saatiin yhteys S615-reitittimelle. Muut vapaat portit voitiin kytkeä pois käytöstä. Kuviossa 29 näkyy käytössä olevat portit ja kuviossa 31 on esitetty XC208 slave -kytkimen porttien tilat.




Kuvio 31. XC208 slaven -porttien määrittely

Palomuurien parametreja täytyi myös muokata testausta varten. Aluksi parametroitiin S615-reititin, johon sisältyy myös palomuuri. Reititin toimii osana korkeavaraston verkkoa sekä OT-verkkoa. Näin ollen palomuuriin asetettiin molempien verkkojen IP-osoitteet. (Configuration manual 2020, 33.) Koska kyseessä oli testivaihe, kaikki verkkoliikenne sallittiin palomuurin läpi. Tämä helpotti yhteyden luomista, koska verkkoliikenteellä oli vähemmän esteitä. SC636-2C -palomuurin parametreja muokattiin myöhemmässä vaiheessa. Kuviossa 32 näkyy liikenteen rajoittamattomuus molempiin suuntiin testausvaiheessa.




Kuvio 32. S615-kytkimen palomuurin tietoliikenne

Kun perusparametrit olivat asetettu, yhteyttä pystyttiin testaamaan Siemensin TIA Portalilla. Automaatiolaitteisto oli valmiina käyttöön ja sovellusohjelma oli jo valmiiksi ladattuna logiikkaan. Testausta varten logiikka sekä käyttöpaneeli täytyi asettaa online-tilaan, jolloin päästiin käyttämään laitteiston käyttöpaneelia tietokoneelta käsin. Käyttöpaneelin näkymä on kuvion 33 mukainen.

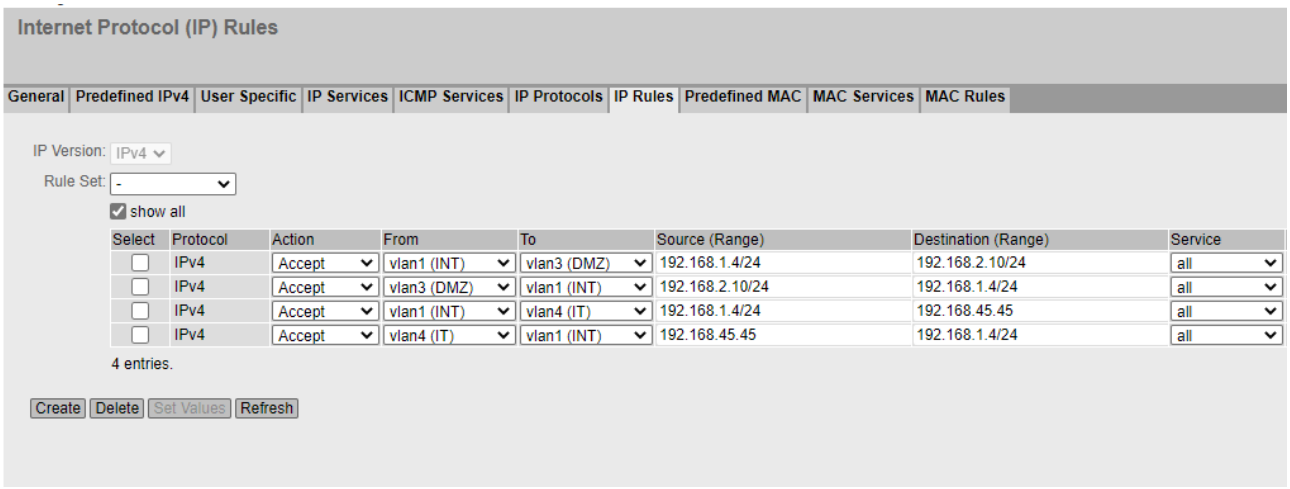

Kuvio 33. Automaatiolaitteiston käyttöpaneeli

## 5.5 Etäyhteys

Etäyhteys räkkiin luotiin Rajakadun kampuksen automaatioverkosta. Tähän verkkoon on kytketty kaikki laboratorioissa DP69 sekä DP66 olevat verkkolaitteet. Haluttiin, että kaikilta automaatioverkossa olevilta tietokoneilta oli yhteys Ethernetin kautta räkkiin. Aluksi Hämäläinen (2021) valitsi tutkimusta varten automaatioverkosta vapaan IP-osoitteen. Tämä osoite on kiinteä ja tarkoitettu ainoastaan verkon ja räkin väliselle verkkoliikenteelle. Seuraavaksi etsittiin DP66-laboratoriosta vapaa atk-rasia. Tämä piste toimii linkkinä SC-636-2C -palomuurin sekä Rajakadun kampuksen verkkoräkin välillä. Palomuuri kytkettiin atk-rasiaan Ethernet-kaapelilla. Rasialta lähtevä kaapeli kytkettiin räkin kytkimeen. Täten jokaiselta laboratorion tietokoneelta oli pääsy räkin palomuuriin,

mutta automaatioverkon ulkopuolelta räkkiin ei saa luotua yhteyttä. Palomuuriin pääsee yhdistymään, kun luo tietokoneelta yhteyden kiinteään IP-osoitteeseen, joka on varattuna palomuurille.

Palomuurin parametreja täytyi muuttaa, jotta liikenne kahden verkon välillä toimii. Palomuuriin täytyi luoda kaksi uutta VLANia sekä sallia verkkoliikenne palomuurin lävitse. Yksi palomuurin verkkoliitynnöistä täytyi myös konfiguroida ainoastaan automaatioverkon yhteyttä varten. VLANit luotiin ennalta määritettyjen IP-osoitealueiden mukaisesti (kuvio 34). Sisäverkon IP-osoitteeksi valittiin palomuurin oma IP-osoite sisäverkon IP-osoitealueelta. Automaatioverkon IP-osoitteeksi valittiin tietohallinnon määrittämä kiinteä IP-osoite. IT-verkon IP-osoite korvattiin automaatioverkon osoitteella yhteyden testaamista varten. Tämän jälkeen määritettiin rajoittamaton liikenne näiden VLANien välillä. Tietoturvan kannalta rajoittamaton liikenne ei ole kannattava ratkaisu, mutta räkki on vielä rakennusvaiheessa, joten liikennöintisäännöt voidaan luoda myöhemmin. Toisaalta tietoturvariskejä ei tässä konfiguraatiossa ole, koska liikennöinti tapahtuu suljetussa sisäverkossa. Lopuksi automaatioverkkoon lähtevälle liikenteelle täytyi määrittää oma portti, jonka kautta verkkoliikenne kulkee.




Kuvio 34. SC636-2C -palomuurin verkkoliikennesäännöt

# 6 Tutkimuksen tulokset

## 6.1 Laitteiston rakennus

Verkkolaitteisto saatiin rakennettua verkkolaitteiden osalta suunnitelmien mukaisesti. Kaikki verkkolaitteet sovitettiin räkkiin ilman ongelmia. Laitteiden sijoittelussa otettiin huomioon myös mahdollisesti tulevaisuudessa lisättävät komponentit. Laitelisäyksiä varten nykyiset laitteet asennettiin kompaktisti ja laitteet muodostavat oman selkeän kokonaisuuden. Räkin kaapelointi tehtiin mahdollisimman siististi, jotta muokkaukset ja lisäykset saadaan tehtyä ongelmitta. Myös laitteiston uudet käyttäjät sisäistävät räkin kytkennät sekä toiminnan nopeasti, kun ulkoasu on selkeä.

Tietohallinnon kanssa tehtiin yhteistyötä S615-reitittimen sekä automaatiolaitteiston välisen kaapeliyhteyden rakentamisessa. Kaapelointien yhdistäminen tehtiin ristikytkennässä, jolloin kaikki yhteydet kulkevat kampuksen verkkoräkin kautta. Kaikki yhteydet kulkevat kootusti yhden pisteen kautta, eikä laboratorioissa ole hallitsemattomia yhteyksiä. Ristikytkennästä tehtiin tarkat dokumentaatiot, jolloin tietohallinto pysyy ajan tasalla oppilaitoksen lähiverkon kytkennöistä.

Laitteet kytkettiin kehään ja käytettiin MRP-protokollaa, jolloin verkon toimintavarmuus kasvoi. Kehä sekä verkkolaitteet saatiin toimimaan ja yhteys automaatiolaitteistoon saatiin alustavasti luotua laboratorion automaatioverkosta. Räkki on täten toimintakuntoinen ja verkkolaitteiden parametrointi onnistui. DMZ-aluetta ei tosin saatu luotua. Tutkimuksen resurssit alkoivat olla vähissä ja DMZ-alueen luominen olisi vaatinut ylipääsemätöntä ponnistelua. DMZ-alueen luomista varten täytyy tehdä lisää yhteistyötä Piippukadun kampuksen henkilökunnan kanssa, jotta yhteys Rajakadulle voi toteutua. Ympäristön luominen vaatii myös päätöksiä henkilökunnan tasolla.

## 6.2 Tietoturvaratkaisuiden toteutuminen

Tietoturva oli tärkeä teema osana tutkimusta. Ympäristöstä pyrittiin luomaan erittäin turvallinen kyberuhkia vastaan. Tällä tavoin estetään verkkolaitteiden käyttö ulkopuolisilta. Hyviä tietoturvaan liittyviä normeja mukaillen luotu ympäristö toimii myös opetusvälineenä tulevilla opintojaksoilla. Tietoturvan merkitystä ei voi väheksyä teollisuudessa, kun käytössä olevat laitteistot ovat tärkeissä rooleissa osana esimerkiksi yhteiskunnan toimintaa ja infrastruktuuria.

Verkon sisäisiltä uhkilta ympäristö suojattiin palomuureilla sekä vahvoilla salasanoilla. VPN-yhteyttä ei vielä kyetty luomaan, mutta tulevaisuudessa se tulee olemaan tärkeässä roolissa osana verkkoympäristön tietoturvaa. Palomuureilla estetään ei-toivottu verkkoliikenne, jolloin kyberuhkien vaara vähenee. Palomuurien liikenne on tällä hetkellä rajattu ennalta määritettyjen IP-osoitteiden välille, jolloin yhteyttä ei voi luoda mistä IP-osoitteesta tahansa. Verkkolaitteiden konfiguraation muutokset ja parametrointi estettiin luomalla vahvat salasanat, jotka pidetään henkilökunnan tiedossa.

Fyysiset uhat poissuljetaan pääsääntöisesti lukitsemalla laboratorion sekä verkkoräkin ovet. Laboratorion ovet ovat normaalisti lukossa. Laboratorion varaajalla on aina vastuu ympäristöstä, joten vastuuhenkilö pitää huolen, ettei laboratorioon pääse kukaan ulkopuolinen. Verkkolaitteisiin pääsy voidaan estää hankkimalla luvussa 5.1.3 esitettyjä RJ45-lukkoja. Lukot asennetaan RJ45-liityntöihin, jolloin verkkolaitteeseen ei voi liittää ylimääräisen verkkokaapelia. Ylimääräiset verkkoliitynnät kytkettiin varmuuden vuoksi pois käytöstä muuttamalla laitteiden parametreja.

## 6.3 Laitteisto osana uutta oppimisympäristöä

Uutta ympäristöä voidaan hyödyntää opintojaksoilla demonstroitaessa teollisen internetin merkitystä teollisessa ympäristössä sekä osana automaatiotekniikkaa. Uusista järjestelmistä pyritään luomaan entistä älykkäämpiä, jolloin tarvitaan tietotekniikkaa. Rakennetulla ympäristöllä voidaan esittää, kuinka tiiviisti tieto- sekä automaatiotekniikka liittyvät toisiinsa. Ilman tietotekniikkaa automaatiolaitteistoa voitaisiin käyttää ainoastaan laitteiston ohjauspaneelista, mutta verkkoympäristön ansiosta laitteistoa voi ohjata toiselta PC:ltä ja tulevaisuudessa myös oppilaitoksen ulkopuolelta. Automaatiotekniikan tutkinto-ohjelman opintojaksoilla ei käsitellä ollenkaan teollisuuden tietoverkkoja tai verkkoihin liitettäviä laitteita. Tämän tutkimuksen tarkoituksena oli tarkastella mahdollisuuksia kehittää tietoverkkotekniikan tuntemusta. Rakennettu verkkoympäristö toimii valmiina alustana tietoverkkotekniikan opetuksen kehittämistä varten.

Tässä opinnäytetyössä tutkittiin tietoturvan merkitystä kyberuhkien torjumiseen sekä tietoturvan roolia teollisuusverkoissa. Tietoturva on jaoteltu sisäisien- sekä ulkoisien uhkien torjumiseen. Uusi verkkoympäristö on rakennettu hyväksi havaittuja tietoturvaratkaisuja mukaillen. Turvallista verkkoa voidaan käyttää oppilaitoksessa ilman tietoturvauhkia. Vaarattomassa ympäristössä toimiessa

on helppo demonstroida hyviä tietoturvaan liittyviä normeja sekä verkkojen yleisiä haavoittuvuuksia. Tämän työn tärkeimmiksi tietoturvakomponenteiksi lukeutuvat palomuurit, koska ne ovat osana useaa verkkoa ja mahdollistavat verkkoliikenteen ulkoverkosta lähiverkkoihin.

Erilaisten topologioiden rooli korostui tutkimusta tehdessä. Topologioita on monta erilaista ja niitä voidaan myös yhdistellä. Jokaisella vaihtoehdolla on luonnollisesti omat edut sekä heikkoudet. Toimistoympäristöissä ja teollisuusympäristöissä tarpeet ovat erilaisia, joten topologioiden valintaan tulee kiinnittää erityistä huomiota. Rengastopologiaa ei esimerkiksi käytetä enää paljon IT-verkoissa, mutta OT-ympäristöissä rengasverkkoja rakennetaan edelleen. Tutkimuksen verkko rakennettiin renkaaseen, koska Siemensin laitteet tukevat MRP-protokollaa, jonka avulla rengasverkosta saa luotua luotettavan. Laboratorion verkkoympäristöllä voidaan havainnollistaa MRP-protokollan toimintaa. Katkaisemalla kehän verkkokaapeli verkkoliikenteen tulisi jatkua, mutta liikenne ohjataan kulkemaan ehjää kaapelia pitkin.

Räkkiin valikoitui useita erilaisia verkkolaitteita. Laboratorion lähiverkko on pieni versio suuresta teollisuusverkosta. Täten jokaisella räkin laitteella on tärkeä tehtävä ja jokaista verkkolaitetta tarvitaan, jotta on edellytys luoda halutunlainen ympäristö. Tutkimuksen verkkolaitteet ovat luotu puhtaasti teollisuusympäristöön soveltuvaksi, joten ne sopivat täysin myös tutkimukseen. Opintojaksoilla voidaan tulevaisuudessa vertailla toimistoympäristöön ja teollisuuteen sijoittuvien laitteiden ominaisuuksia sekä ympäristön asettamia vaatimuksia. Myös laitteiden konfigurointia on suositeltavaa havainnollistaa laboratorion laitteilla. Verkko on konfiguroitu yksinkertaisille parametreille, joita on helppo muokata. Muokattavia parametreja on vain muutama, joten parametrien avulla on helppo esittää, miten verkon käyttäytyminen muuttuu parametreja vaihtamalla.

VPN-yhteys luodaan tulevaisuudessa. Tällöin opiskelijat voivat luoda yhteyden verkkoon sijainnista riippumatta. Tällä hetkellä yhteyden voi luoda kaikkialta automaatioverkosta, mikä auttaa jo huomattavasti tulevia parannuksia ajatellen. Etäyhteys on myös yleinen ratkaisu teollisuusverkoissa, kun on tarvetta esimerkiksi monitoroida laitteita tai tutkia järjestelmiä vikatilanteissa.

# 7 Pohdinta

Opinnäytetyön tavoitteena oli tutkia uuden oppimisympäristön luomista Jyväskylän ammattikoulun laboratorioon sekä analysoida tietotekniikan ja automaatiolaitteiden yhdistämistä teollisessa

ympäristössä. Älykkäät laitteet sekä teollinen internet ovat yleistyneet kiihtyvällä tahdilla jo muutaman vuosikymmenen ajan, minkä vuoksi tutkimusta alun perin päätettiin alkaa tekemään. Uusi oppimisympäristö mahdollistaa opiskelijalle uutta tietoa ja ymmärrystä työelämää varten. Tietoverkko-osaamisen tärkeys on korostunut entisestään automaatioinsinöörin työtehtävissä.

Tutkimusta tehdessä haluttiin korostaa hyviä eettisiä periaatteita niin kirjallisen analysoinnin kuin konkreettisen työn osalta. Verkon rakentaminen täytyi tehdä hyviä normeja noudattaen, jotta oppimisympäristöstä saatiin käyttäjän kannalta turvallinen. Lisäksi huolellisella työskentelyllä ja suunnittelulla saatiin luotua vakaa perusta tulevaisuudessa tehtäville lisäasennuksille sekä laajennuksille. Kyberuhkiin suhtauduttiin myös vakavasti, jotta ulkopuoliset eivät pääse käsiksi lähiverkkoon ja sen laitteisiin.

Tutkimuksessa ei päästy täysin alkuperäisiin tavoitteisiin. VPN-yhteys jäi puuttumaan, joten yhteyttä räkkiin ei voitu muodostaa automaatioverkon ulkopuolelta. Toisaalta VPNän ja DMZ-alueen luominen olisi vaatinut suuria ponnisteluja ja mittavia palavereita tutkijan sekä Jyväskylän ammattikorkeakoulun henkilökunnan toimesta. Tutkimuksessa resurssit eivät yksinkertaisesti riittäneet. Nykyinen ympäristö toimii lähes yhtä hyvin, joten toimeksiantaja oli tyytyväinen ympäristöön sekä sen käytettävyyteen. Tutkimuksen tuloksiin saatiin kartutettua myös paljon uutta tietoa teollisiin verkkoihin liittyen. Näitä tietoja hyödyntäen Jyväskylän ammattikorkeakoulu pystyy kehittämään opetuksen laatua sekä laajentamaan opintojaksotarjontaa tietoverkkojen osalta.

Lähiverkkoa voidaan käyttää oppimisympäristönä osana opintojaksoja. Uudella laitteistolla voidaan demonstroida teollisuusverkon toimintaa sekä automaatiolaitteiston ohjausta suljetun verkon kautta. Tulevaisuudessa laitteistosta voidaan esimerkiksi erottaa yksittäisiä komponentteja ja analysoida niiden toimintaa. Verkkolaitteiden konkreettinen esittäminen tullee olemaan hyvä harjoitus teoriaopetuksen lisäksi. Eri verkkolaitteiden parametreja voidaan vaihtaa ja niiden perusteella voidaan analysoida laitteiden toimintaa. Tällä tavoin verkkolaitteiden parametrit tulevat opiskelijoille tutuiksi ja laitteiden tuntemus paranee. Verkon topologian muuttaminen on myös mahdollinen esimerkkiharjoitus. Tällä tavoin voidaan tuoda esille eri topologioiden edut ja haitat. Mielestäni tutkimuksen tärkein saavutus on kuitenkin tuoda markkinoilla olevat teollisuusympäristöön soveltuvat verkkolaitteet lähelle opiskelijoita sekä lehtoreita, jolloin tietoverkkotekniikkaa voidaan liittää entistä tiiviimmin osaksi automaatioinsinöörin koulutusta.

Tutkimuksen tuloksena syntynyttä oppimisympäristöä voidaan vielä parantaa tulevaisuudessa. Tutkimuksessa oli tarkoituksena tutkia oppimisympäristön perustamiseen liittyviä asioita ja luoda lähiverkko, jota voidaan laajentaa. Kaikissa jo nyt käytössä olevissa verkkolaitteissa on kaksi liitynt-tää jännitteen syötölle. Tulevaisuudessa räkkiin on suositeltavaa asentaa toinen jännitelähde, joka toimii varasyöttönä verkkolaitteille. Jännitelähteen syöttö kannattaa asentaa sähkökeskuksessa toiselle sulakkeelle, jolloin saadaan lisättyä toimintavarmuutta. Jyväskylän ammattikorkeakoulun laboratoriotiloissa on yksi UPS-yksikkö. Laite voidaan liittää tulevaisuudessa osaksi verkkoympäris-töä. UPS-yksikkö on akusto, joka tuottaa virtaa esimerkiksi sähkökatkon aikana. Sähkökatkojen ai-heuttamia vahinkoja voidaan vähentää käyttämällä UPS-yksikköä, jolloin verkossa tapahtuvaa lii-kennettä voidaan jatkaa hetken aikaa. Lyhytkin toiminta-ajan lisäys on tärkeä, jotta verkon liikenne saadaan lopetettua hallitusti.

Laboratoriotiloissa on myös muita automaatiolaitteistoja, joita voidaan liittää osaksi ympäristöä. Esimerkiksi energiatekniikan laboratorioissa on laitteistoja, jotka olisivat hyvä lisä osaksi oppimis-ympäristöä. Myös uusia verkkolaitteita voidaan lisätä räkkiin, jos verkkoa halutaan laajentaa. Alus-tavat työt tehtiin huolella, jotta jatkossa tapahtuvalle kehitystyölle taataan laadukas lähtökohta.

Tutkimusta tehdessä hankalin työvaihe oli verkkolaitteiden konfigurointi. Verkkolaitteisiin ei ole paljoakaan tutustuttu automaatiotekniikan opintojaksoilla, joten parametrien asettaminen tuntui hankalalta. Onneksi muutettavia parametreja ei ollut monia, minkä ansiosta tutkimus eteni jouhe-vasti. Toisaalta uudet laitteet ja sekä ominaisuuksien muokkaaminen kehittivät minua osaajana. Verkkoympäristön ymmärtäminen kokonaisuutena oli myös aluksi hankalaa. Tietohallinnolla sekä Siemensin asiantuntijoilla oli hieman eri näkemys asiasta, joten en saanut aluksi luotua itselleni selkeää ideaa kokonaisuudesta. Tutkimusta tehdessä opin erityisesti paljon uutta tietoa lähiver-koista sekä tietoliikenteestä. Opin myös paljon teollisesta internetistä sekä laitteiden verkottami-sen hyödyistä. Kehityin myös huomattavan paljon kirjoittajana, koska tutkimuksen tekeminen vaa-tii tieteellistä otetta sekä tietoperustan oikeellisuuden todentamista.

# Lähteet

Adling, A. 2019. Industrial communication. Siemensin SCALANCE-kytkinten laitemanuaali. Viitattu 14.3.2021. https://assets.new.siemens.com/siemens/assets/api/uuid:8bc97741-9b9b-4a19-8f65-feaf80911d09/004945-scalancex-whitepaper-06-en-screen.pdf.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Configuration manual. 2020. Siemensin S615-reitittimen käyttöönottomanuaali. Viitattu 16.3.2021. https://cache.industry.siemens.com/dl/files/632/109751632/att_1028499/v1/PH_SCALANCE-S615-WBM_76.pdf.

Data sheet 6GK5208-0BA00-2AC2. 2019. Siemensin SCALANCE XC208-kytkimen datalehti. Viitattu 14.3.2021. https://www.nexinstrument.com/assets/images/pdf/6GK5208-0BA00-2AC2.pdf.

Data sheet 6GK5636-2GS00-2AC2. 2020. Siemensin SCALANCE SC636-2C-palomuurin datalehti. Viitattu 14.3.2021. https://www.west-l.ru/uploads/tdpdf/6gk5636-2gs00-2ac2_eng_tds.pdf.

Data sheet/User manual. 2017. Powernetin laitemanuaali ADC5000-sarjan jännitelähteille. Viitattu 14.3.2021. https://powernet.fi/wp-content/uploads/2018/11/ADC50001.pdf.

Granlund, K. 2007. Tietoliikenne. Jyväskylä: Docendo.

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

Helin, M., Spoof, S-K., Jäppinen, S. & Launis, V. 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Tutkimuseettinen neuvottelukunta. Viitattu 17.3.2021. https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf.

Honka, E., Korhonen, J. & Tamminen, J. 2019. Sähköturvallisuus. Sähköalojen työalatoimikunnan laatima työturvallisuusohje 28.10.2019. Viitattu 24.3.2021.https://ttk.fi/files/4823/STO2_Sahkoturvallisuus_korjattu.pdf.

Hunt, G. 1998. TCP/IP-verkonhallinta. Helsinki: Suomen Atk-kustannus.

Hämeen-Anttila, T. 2003. Tietoliikenteen perusteet. Jyväskylä: Docendo.

Hämäläinen, K. 2021. Tietoverkkotopologiat. Sähköpostiviesti 3.3.2021. Vastaanottaja T. Tervo. Jyväskylän ammattikorkeakoulun tietohallinnan edustajan opastus verkon rakennukseen.

IE RJ45 port lock. N.d. Siemensin tuotekatalogi verkossa. Viitattu 3.4.2021. https://mall.industry.siemens.com/mall/en/us/Catalog/Products/10303300.

Itkonen, A. 2018. Teollisuustietoliikenneverkot osana suunnitteluprosessia. Opinnäytetyö, AMK. Metropolia ammattikorkeakoulu, automaatiotekniikka. Viitattu 1.3.2021. https://www.theseus.fi/bitstream/handle/10024/142096/Itkonen_Aku.pdf?sequence=1&isAllowed=y .

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. Helsinki: Edita Prima.

Järvenpää, E. 2006. Laadullinen tutkimus. SoberIT jatko-opintoseminaari. Viitattu 27.2.2021. https://www.cs.tut.fi/~ihtesem/k2007/materiaali/luento4.pdf.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kotikoski, S. 2021. IP-osoitteet. Sähköpostiviesti. 5.3.2021. Vastaanottaja T. Tervo. Jyväskylän ammattikorkeakoulun tietotekniikan lehtorin opastus opiskelijalle IP-osoitteiden määritystä varten.

Kurose, J. & Ross, K. 2013. Computer Networking A Top-down approach Sixth Edition. E-kirja. New Jersey: Addison-Wesley. Viitattu 28.2.2021. https://eclass.teicrete.gr/modules/document/file.php/TP326/%CE%98%CE%B5%CF%89%CF%81%CE%AF%CE%B1%20(Lectures)/Computer_Networking_A_Top-Down_Approach.pdf.

Learn-/Training Document. 2019. Siemensin konfigurointiopas XC208-kytkimelle sekä S7-1500 -logiikalle. Viitattu 10.4.2021. https://www.automation.siemens.com/sce-static/learning-training-documents/tia-portal/security/sce-142-100-industrial-ethernet-xc208-r1906-en.pdf.

Lutkevich, K. 2020. IT/OT Convergence. Artikkeli SearchITOperations-verkkosivuilla. Viitattu 3.4.2021. https://searchitoperations.techtarget.com/definition/IT-OT-convergence.

Mesnik, B. 2016. How Power Over Ethernet Works. Verkkojulkaisu. Viitattu 28.3.2021. https://kintronics.com/how-power-over-ethernet-works/.

Meyers, M. 2003. Verkot+-sertifikaatti. Helsinki: Edita Prima.

Network security. 2020. Siemensin verkkolaitteiden opas. Viitattu 14.3.2021. https://pdf.directindustry.com/pdf/siemens-industrial-communication/network-security/50160-941106.html#open1712884.

Odom, W. 2005. Tietoverkot perusteet. Helsinki: Edita Prima.

Operating instructions. 2015. Siemensin S615-reitittimen asennusmanuaali. Viitattu 29.3.2021. https://cache.industry.siemens.com/dl/files/909/109475909/att_841005/v1/BA_SCALANCE-S610_76.pdf.

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. Artikkeli. Viitattu 27.2.2021. https://tuhat.helsinki.fi/ws/files/127650174/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf.

Pyykkö, T. & Torvinen, V. 2021. Lähiverkon rakentaminen teollisuusympäristöön. Teams-palaveri 2.4.2021. Siemensin yrityksen asiantuntijoiden kanssa.

Pyyskänen, S. 2007. Teollisuuden laiteverkot. Johdatus väylätekniikkaan. Helsinki: Suomen automaatioseura ry.

Setup of a Ring Topology Based on “MRP”. 2016. Siemensin manuaali rengasverkon rakentamiseen. Viitattu 2.4.2021. https://cache.industry.siemens.com/dl/files/614/109739614/att_891688/v3/109739614_MRP_DOKU_V10_en.pdf.

Taiponen, A. 2006. Teollisuus-Ethernetin teknistaloudellinen selvitys sähkötukkukaupan näkökulmasta. Gradutyö. Lappeenrannan teknillinen yliopisto. Sähkötekniikan osasto. Viitattu 28.3.2021. https://lutpub.lut.fi/bitstream/handle/10024/30404/nbnfi-fe200902241195.pdf?sequence=1&isAllowed=y.

TEPA-termipankki. 2020. Haku sanalla pienoisjännite. Viitattu 28.3.2021. https://termipankki.fi/tepa/fi/haku/pienoisj%C3%A4nnite.

Thomas, T. 2005. Verkkojen tietoturvaperusteet. Helsinki: Edita Prima.

Tietotekniikan termintalkoot. 2002. Haku sanalla VLAN. Viitattu 27.4.2021. http://www.tsk.fi/tsk/termitalkoot/fi/node/266.

Vilkka, H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Helsinki: Tammi. Viitattu 1.3.2021. https://trepo.tuni.fi/bitstream/handle/10024/98723/Tutki-ja-mittaa_2007.pdf?sequence=1&isAllowed=y.

Vuori, J. N.d. Laadullinen sisällön analyysi. Artikkeli Tietoarkiston sivustolla. Viitattu 28.2.2021. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/.

Walker, D. 2021. What is a default gateway? Artikkeli ITPro-verkkosivuilla. Viitattu 3.4.2021. https://www.itpro.co.uk/network-internet/30327/what-is-a-default-gateway.