VAASAN YLIOPISTO

TEKNIIKAN JA INNOVAATIOJOHTAMISEN YKSIKKÖ

OHJELMISTOTEKNIIKKA

Vesa Rantala

TIETOLIIKENTEEN DYNAAMINEN REITITYS KAIVOSTEOLLISUUDEN TIETOVERKKOINFRASTRUKTUURISSA

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten
Vaasassa 23.4.2018.

Työn valvoja	Professori Jouni Lampinen
Työn ohjaaja	DI Pirkka Tukeva

ALKUSANAT

Tämä diplomityö on tehty Seinäjoella toimivalle Exertus Oy:lle. Osoitan suuret kiitokset Juha Viitaselle ohjauksesta ja mielenkiintoisista keskusteluista, jotka tarjosivat arvokkaita näkökulmia diplomityötä varten. Suuret kiitokset myös Kimmo Hautalalle, joka tarjosi asiantuntevia neuvoja tietoliikennetekniikkaan liittyvissä asioissa. Lisäksi kiitän erityisesti Pirkka Tukevaa, joka auttoi hallinnollisissa asioissa ja asiakasyhteyksissä.

Kiitos professori Jouni Lampiselle diplomityön eteenpäin viemisestä ja rakentavasta palautteesta.

Kiitos perheelleni ja ystävilleni tuesta.

Seinäjoella 22.4.2018
Vesa Rantala

SISÄLLYSLUETTELO

LYHENNELUETTELO

ARP	Address Resolution Protocol, fyysisen osoitteen loogisesta osoitteesta selvittävä tietoliikenneprotokolla
ASCII	American Standard Code for Information Interchange, merkistö
CAN	Controller Area Network, ajoneuvoissa käytettävä automaatioväylä
CIDR	Classless Inter-Domain Routing, luokaton reititys
dBd	Desibeliä verrattuna puoliaaltodipoliantenniin
dBi	Desibeliä verrattuna isotrooppiseen antenniin
dBm	Desibeliä verrattuna milliwattiin
DHCP	Dynamic Host Configuration Protocol, IP-parametrejä jakava tietoliikenneprotokolla
DNAT	Destination Network Address Translation, kohdeosoitteenmuunnos
DNS	Domain Name System, verkkotunnuksen IP-osoitteeksi muuntava nimipalvelujärjestelmä
EIRP	Effective Isotropic Radiated Power, efektiivinen säteilyteho isotrooppisesta antennista
ERP	Enterprise Resource Planning, toiminnanohjausjärjestelmä (ERP-järjestelmä)
FTP	File Transfer Protocol, tiedostonsiirtoon tarkoitettu tietoliikenneprotokolla
HTTP	Hypertext Transfer Protocol, WWW-tekniikassa käytettävä tietoliikenneprotokolla
I/O	Input/Output, sisäänmenoja ja ulostuloja sisältävä liitäntä
IEEE 802.11	Langattomien lähiverkkojen standardi, jonka on standardisoinut Institute of Electrical and Electronics Engineers

IoT	Internet of Things, esineiden internet
IP	Internet Protocol, IP-pakettien siirrosta vastaava tietoliikenneprotokolla
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö
JSON	JavaScript Object Notation, tiedonvälityksessä käytettävä tiedostomuoto
LAN	Local Area Network, lähiverkko
LED	Light-Emitting Diode, hohtodiodi
MAC	Media Access Control, siirtoyhteyden varaava osakerros siirtoyhteyskerroksessa
MQTT	Message Queuing Telemetry Transport, kevyt tuottaja–tilaaja-protokolla
NAT	Network Address Translation, osoitteenmuunnos
OSI	Open Systems Interconnection, tietoliikennejärjestelmien toiminnan kuvaamiseen käytetty kerrosmalli (OSI-malli)
PoE	Power over Ethernet, virransyöttö kierretyllä parikaapelilla Ethernet-lähiverkossa
PWM	Pulse-Width Modulation, pulssinleveysmodulaatio
RARP	Reverse Address Resolution Protocol, loogisen osoitteen fyysisestä osoitteesta selvittävä tietoliikenneprotokolla
ReDi	Remote Diagnostics, Exertus Oy:n kehittämä ja ylläpitämä telematiikkapalvelu
REST	Representational State Transfer, arkkitehtuurimalli ohjelmointirajapinnoille
RS232	Recommended Standard 232, sarjamuotoisen ja asynkronisen tiedonsiirron standardi
SMTP	Simple Mail Transfer Protocol, sähköpostiviestien välitykseen tarkoitettu tietoliikenneprotokolla
SNAT	Source Network Address Translation, lähdeosoitteenmuunnos

SSID	Service Set Identifier, langattomassa lähiverkkotekniikassa käytettävä verkon nimimääritys
TCP	Transmission Control Protocol, yhteydellisen tiedonsiirtotien tarjoava tietoliikenneprotokolla
TFT	Thin-Film Transistor, ohutkalvotransistori
UDP	User Datagram Protocol, yhteydettömän tiedonsiirtotien tarjoava tietoliikenneprotokolla
URL	Uniform Resource Identifier, internetissä käytettävä osoitusmekanismi
USB	Universal Serial Bus, sarjamuotoinen liitäntä
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, langattomissa lähiverkoissa käytettävä salausmenetelmä
WWW	World Wide Web, tiedon jakoon tarkoitettu palvelu internetissä

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Vesa Rantala
Diplomityön nimi: Tietoliikenteen dynaaminen reititys kaivosteollisuuden tietoverkkoinfrastruktuurissa
Valvoja: Professori Jouni Lampinen
Ohjaaja: DI Pirkka Tukeva
Tutkinto: Diplomi-insinööri
Koulutusohjelma: Tietotekniikan koulutusohjelma
Suunta: Ohjelmistotekniikka
Opintojen aloitusvuosi: 2013
Diplomityön valmistumisvuosi: 2018 **Sivumäärä:** 82

TIIVISTELMÄ

Esineiden internet mahdollistaa muun muassa erilaisten työkoneiden liittämisen internetiin. Tämän johdosta työkoneiden käytöstä voidaan kerätä dataa, jota voidaan hyödyntää monilla eri osa-alueilla. Esineiden internet edellyttää kuitenkin pääsyn internetiin ja vaativissa olosuhteissa internet-yhteyttä ei aina ole saatavilla tai se voi olla laadultaan huono. Yhteyden puuttumisesta huolimatta dataa pitäisi silti saada siirrettyä.

Diplomityössä suunnitellaan ja toteutetaan eräänlainen liikkuva välityspalvelin kaivosteollisuudessa käytettäville työkoneille. Työkoneilla on valmius lähettää dataa palvelimelle, mutta syvällä maan alla yhteyttä internetiin ei aina ole saatavilla. Tästä syystä työkoneilla pitäisi nousta maan pinnalle datan lähetystä varten, mikä ei ole kaivostoiminnan kannalta käytännöllistä. Sen sijaan työkoneet voisivat lähettää datansa välityspalvelimelle, joka sitten kuljettaisi datan ylös kaivoksesta ja lähettäisi ne oikealle palvelimelle internetiin. Välityspalvelimen suunnitteluun ja toteutukseen liittyvät keskeisenä osana TCP/IP-protokollaperhe ja osoitteenmuunnos. Osoitteenmuunnoksen avulla välityspalvelin saadaan näyttäytymään oikeana palvelimena työkoneille. Diplomityössä keskitytään välityspalvelinjärjestelmän laitteisto- ja verkkoarkkitehtuuriin ohjelmistoarkkitehtuurin jäädessä pienempään osaan.

Välityspalvelin toteutettiin siten, että se sisältää elementtejä työkoneesta ja oikeasta palvelimesta. Välityspalvelimen verkko rakennettiin yleiskäyttöiseksi siten, että sitä voidaan käyttää tulevaisuudessa myös muissa järjestelmissä sellaisenaan. Lisäksi työkoneissa käytettävään ohjausjärjestelmän ohjelmistoarkkitehtuuriin ei tarvinnut tehdä muutoksia, sillä järjestelmä toteutettiin laitteisto- ja verkkoarkkitehtuuri edellä. Tuloksena syntyi toimiva välityspalvelin, joka voi siirtää dataa langattomasti työkoneilta oikealle palvelimelle internetiin. Lisäksi uuden järjestelmän arkkitehtuuri mahdollistaa sen, että sitä voidaan käyttää myös ilman välityspalvelinta. Näin uuden järjestelmän välityspalvelin ei ole välttämätön kaivostyömaalla, jossa internet-yhteys on muuten helposti saatavilla.

AVAINSANAT: esineiden internet, dynaaminen reititys, välityspalvelin, kaivosteollisuus

UNIVERSITY OF VAASA
School of Technology and Innovations
Author: Vesa Rantala
Topic of the Thesis: Dynamic Routing in Data Network Infrastructure of Mining Industry
Supervisor: Professor Jouni Lampinen
Instructor: M.Sc. (Tech.) Pirkka Tukeva
Degree: Master of Science in Technology
Degree Programme: Degree Programme in Information Technology
Major: Software Engineering
Year of Entering the University: 2013
Year of Completing the Thesis: 2018 **Pages:** 82

ABSTRACT

Internet of Things makes it possible to connect different sorts of work machines to the Internet so that data can be gathered from them. Gathered data can then be used in a wide range of applications. However, Internet of Things requires Internet access and it is not always available in certain environments. Despite the lack of Internet access there is still need to transfer data to the Internet.

The aim of this thesis was to develop a type of mobile proxy server for work machines used in mining industry. Work machines are able to transmit data to a server but in a deep mine Internet connection cannot always be established. Therefore, work machines must be brought out from the mine so that they can establish an Internet connection and transmit their data. In the case of mining this is very impractical procedure. Instead, work machines could transmit their data to a proxy server that would be able to carry the data out of mine and transmit it to the actual server when Internet connection is available. TCP/IP protocol suite and network address translation are key techniques to be used in the proxy server. With the help of network address translation, it is possible to make proxy server act as a real server to the work machines. The thesis focuses on hardware and network architecture while software architecture is discussed only in brief.

The proxy server was implemented so that it contains elements from a work machine and from the real server. Network architecture of the proxy server was developed so that it is general-purpose and can be used with other systems as well in the future. In addition, there is no need to modify the control system used in work machines because of the hardware architecture of the new system. The result of this thesis is functional proxy server which can transfer data wirelessly from the work machines to the real server. The architecture of the new system makes it also possible to use it without the proxy server. If there is no need for proxy server and the Internet connection is available the proxy server can be omitted from the system.

KEYWORDS: internet of things, dynamic routing, proxy server, mining industry

1 JOHDANTO

Internetiin yhdistetään nykyään tavanomaisimmatkin laitteet. Tämä esineiden internet mahdollistaa monia asioita, mutta sen myötä syntyy myös uusia ongelmia ratkaistavaksi. Esineiden internetin esineet voivat olla mitä vain laitteita, jotka voidaan yhdistää internetiin. Yleisesti kuitenkin tarkoitetaan sellaisia laitteita, joita ei ole aiemmin ollut tarkoitus yhdistää internetiin. Tämä rajaa esimerkiksi puhelimet pois esineiden internetistä. Esineiden internetiin voidaan siten katsoa kuuluvan esimerkiksi erilaiset työkoneet. Työkoneiden tapauksessa halutaan yleensä reaaliaikaista dataa sen hetkisestä tilanteesta työmaalla tai käyttötietoja itse työkoneesta. Datan kerääminen työkoneilta toteutuu nykypäivänä melko vaivattomasti hyvien internet-yhteyksien vuoksi. Dataa ei kuitenkaan voida kerätä alueilla, joilla internet-yhteyttä ei ole lainkaan saatavilla tai se on laadultaan huono. Tällaisia alueita voivat olla esimerkiksi erämaat ja kaivokset. Kaukana erämaassa voi kuitenkin olla yhteys satelliitin kautta. Sen sijaan kaivoksissa, jotka ulottuvat syvälle maan alle, ei internet-yhteyttä voida muodostaa, ellei kaivokseen ole sitä varten rakennettu verkkoinfrastruktuuria. Edellä mainittu tilanne on hyvä esimerkki esineiden internetin mahdollistamasta toiminnasta, joka tuo mukanaan uuden ongelman.

1.1 Tausta

Seinäjoella toimiva Exertus oy sai asiakkaaltaan Normet oy:ltä tilauksen kehittää eräänlainen tiedonsiirtojärjestelmä, joka pystyisi keräämään kaivostyökoneiden tuottaman datan ja lähettämään sen eteenpäin internetissä sijaitsevalle palvelimelle. Uusi järjestelmä olisi tarkoitus liittää tällä hetkellä käytössä olevaan ohjausjärjestelmäperheeseen nimeltä Norsmart. Normetin työkoneiden Norsmart-ohjausjärjestelmä voidaan tällä hetkellä kytkeä internetiin ja ohjausjärjestelmä voi lähettää reaaliaikaista dataa työkoneesta internetissä sijaitsevalle palvelimelle. Normetin työkoneita käytetään usein kaivoksissa syvällä maan alla, jossa ei aina ole internet-yhteyttä saatavilla riippuen siitä, onko kaivokseen rakennettu tarkoitukseen sopiva verkkoinfrastruktuuri. Verkkoinfrastruktuurin puuttuessa data ei liiku kaivoksen työkoneilta palvelimelle reaaliaikaisesti, eikä välttämättä ollenkaan, jos työkoneet eivät pääse välillä maan pinnalle lähettämään dataa.

Työkoneiden ohjausjärjestelmissä on rajallinen muisti dataa varten ja jossain vaiheessa vanhempaa dataa alkaa tuhoutua uuden tilalta, jos dataa ei saada välillä lähetettyä palvelimelle. Uuden järjestelmän olisi tarkoitus korjata tämä ongelma siten, että kaivoksessa eräänlainen ajoneuvo keräisi työkoneilta niiden tallentaman datan. Tällä ajoneuvolla voitaisiin sitten nousta välillä maan pinnalle, jolloin se voisi lähettää kaikilta työkoneilta keräämänsä datan palvelimelle. Järjestelmän ei kuitenkaan tarvitsisi olla reaaliaikainen. Pääasia olisi se, että data saataisiin talteen, eikä työkoneilla tarvitsisi nousta maan pinnalle pelkästään datan lähetystä varten.

1.2 Tavoitteet

Diplomityössä käsitellään pääasiassa uuden järjestelmän laitteisto- ja verkkoarkkitehtuuria. Päätavoite on rakentaa tietoliikenteen näkökulmasta toimiva tiedonsiirtojärjestelmä kaivostyökoneiden käyttöön siten, että dataa saadaan siirrettyä työkoneilta palvelimelle. Ohjelmistoarkkitehtuuria käsitellään tämän tukena ylemmällä tasolla, mutta yksityiskohtainen tutkimus tähän liittyen rajataan diplomityön ulkopuolelle.

1.3 Rakenne

Ensimmäisenä esitellään järjestelmä, johon tavoitteen mukainen lopputulos on tarkoitus yhdistää. Tämän jälkeen käsitellään asiaan liittyvää teoriaa ja käsitteistöä. Tavoitteen mukaisen järjestelmän arkkitehtuuri ja suunnitelma esitellään ennen itse järjestelmän rakentamista ja testausta. Lopuksi esitellään tulokset ja kehitysideat.

1.4 Exertus oy

Exertus oy on perustettu vuonna 2003 ja on riippumaton palveluyritys, jonka päätavoitteena on auttaa asiakkaita tekemään tuotteistaan älykkäämpiä. Exertuksen ydinosaaminen liittyy CAN-väylällä hajautettujen ohjausjärjestelmien hallintaan. Asiakkaille voi-

daan tarjota pienempiä osa-alueita tai kokonaisvaltainen ohjausjärjestelmä. Palvelukonsepti kattaa myös esisuunnittelun, konsultoinnin, määrittelyn, toteutuksen, koulutuksen ja ylläpidon. (Exertus oy 2018.)

2 OHJAUSJÄRJESTELMÄ

2.1 Arkkitehtuuri

Normetin työkoneissa on käytössä älykäs ohjausjärjestelmä nimeltä Norsmart. Se koostuu Exertuksen kehittämistä ohjausyksiköistä, näytöistä ja työkoneen laitteistosta. Ohjausjärjestelmää varten on ohjausyksiköille räätälöity ohjelmisto, joka sisältää ohjauslogiikan ja käyttöliittymän.

2.1.1 Exertuksen ohjausyksiköt

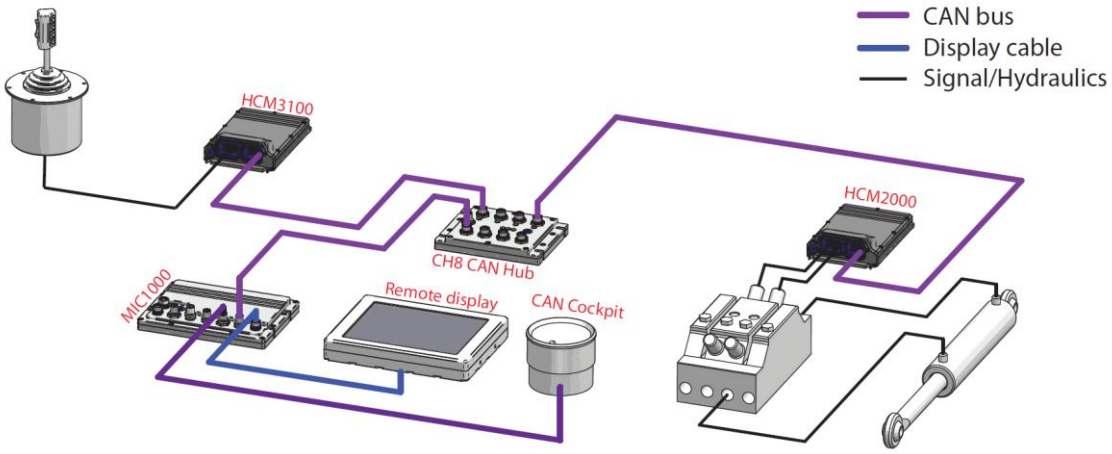
Norsmart-ohjausjärjestelmän ytimenä on Exertuksen kehittämä ohjausyksikkö MIC1100S. Käyttöjärjestelmänä siinä on sulautettu Linux, joka perustuu Debian-jakeluun. Ohjausyksikön I/O-liitännästä löytyy monenlaisia sisäänmenoja ja ulostuloja. Näihin kuuluvat digitaaliset sisäänmenot ja -ulostulot, analogiset sisäänmenot, pulssisisäänmenot ja PWM. Laitteessa on myös Ethernet, USB, RS232, CAN sekä näyttö- ja komposiittivideoliitännät. (Exertus oy 2017a: 2–6.)

Tässä ohjausyksikössä ei ole omaa näyttöä, mutta sen kanssa voidaan käyttää erillistä näyttöä, kuten liitännöistä huomataan. Tähän tarkoitukseen sopivat Exertuksen näytöt RD121S2 sekä kooltaan pienempi RD084S2. Molemmat ovat TFT-näyttöjä ja niiden resoluutio on 800x600 (Exertus oy 2017b: 2, 2017c: 2). MIC1100S voidaan tarvittaessa korvata Exertuksen uudemmilla ohjausyksiköillä, joita ovat MIC2000S ja MID070S.

Ohjausyksikölle voidaan asentaa Exertuksen Guitu-ohjelmalla rakennettu sovellus, jossa on graafinen käyttöliittymä ja ohjauslogiikka. Ohjauslogiikka voidaan ohjelmoida myös suoraan C-ohjelmointikielellä ja sitä käytetäänkin Norsmart-ohjausjärjestelmässä hyvin paljon.

Yleensä tarvitaan myös I/O-moduuleja, sillä yksittäisen ohjausyksikön I/O-liitäntä harvoin riittää kokonaiselle työkoneelle. Moduulit ja ohjausyksiköt ovat yhteydessä toisiin-

sa CAN-väylän kautta. I/O-moduulit ottavat vastaan syötteitä ja ohjaavat työkoneen laitteita sekä lähettävät tietoa ohjausyksikölle ohjausjärjestelmän käyttöön. Esimerkiksi kuvassa 1 ohjaimelta menee tieto sisäänmenoon I/O-moduulille HCM3100, josta tieto menee CAN-väylää pitkin ohjausyksikölle. Sieltä menee tieto I/O-moduulille HCM2000, jonka ulostulo sitten ohjaa hydrauliikkaa. HCM2000 voi vielä lähettää ohjausyksikölle tiedon esimerkiksi männän asennosta sylinterissä. I/O-moduulit eivät ole ohjelmoitavia, vaan niissä on tarvittava ohjelma valmiina. Exertuksella on useita I/O-moduuleita, jotka soveltuvat eri käyttötarkoituksiin.

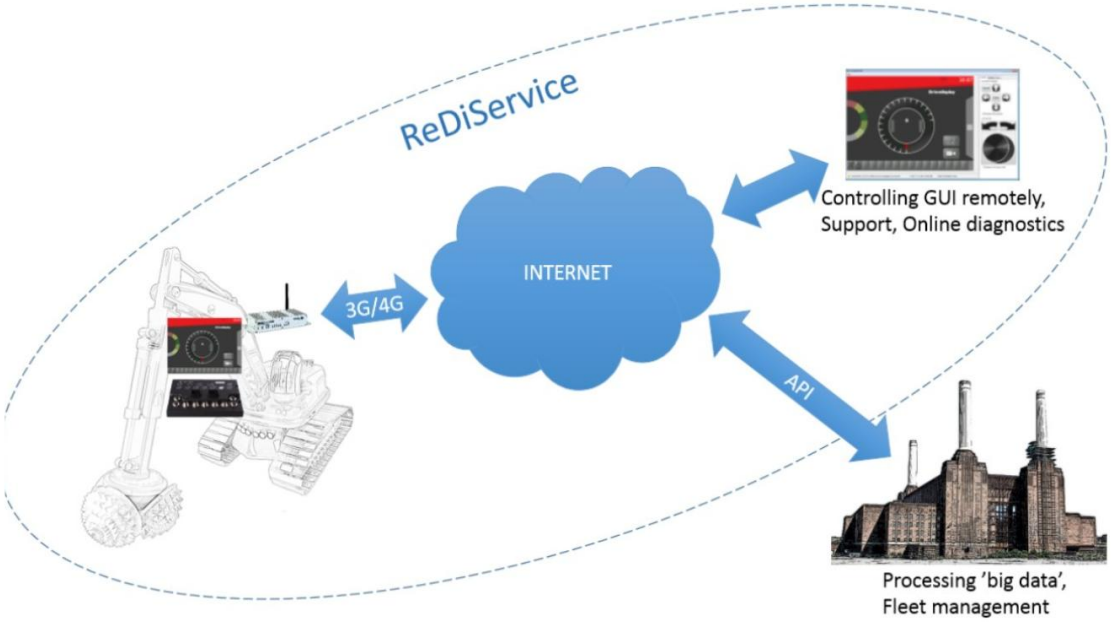


Kuva 1. Norsmart-ohjausjärjestelmän arkkitehtuuri (Exertus oy 2009: 1).

2.2 Tietoliikenne

Diplomityön käytännön osuuden kannalta on oleellista tietää, miten Norsmart-ohjausjärjestelmän tietoliikenne toimii. Tietoliikenteen puolella ohjausjärjestelmässä käytetään Exertuksen kehittämää ja ylläpitämää ReDi-palvelua. Se tarjoaa telematiikkaratkaisuja työkoneisiin, joissa on Exertuksen ohjausjärjestelmä. Se mahdollistaa kaksisuuntaisen tiedonsiirron työkoneen ohjausjärjestelmän ja asiakkaan järjestelmien välillä. Sen avulla voidaan esimerkiksi muodostaa salattu etäyhteys työkoneeseen internetin välityksellä, jolloin työkoneen mahdollisista vikatilanteista saadaan tietoa jo ennen kuin paikan päälle mennään, mikä tietenkin nopeuttaa huoltotoimenpiteitä. Työkoneen kuljettajaa voidaan myös opastaa etäyhteyden avulla, sillä molemmissa päissä nähdään sa-

ma käyttöliittymä. ReDi-palvelu mahdollistaa datan keräämisen työkoneilta ja datan analysoinnin. Tämä big data sisältää tietoja työkoneen käyttöasteesta, eli esimerkiksi siitä kauanko työkone on ollut käynnissä ja kauanko sillä on tehty työtä sen ollessa käynnissä. Näihin liittyvät myös polttoaineen kulutus ja ajettu matka. Lisäksi voidaan tarkkailla työkoneen apulaitteiden kuntoa. (Exertus oy 2016: 2–3.) ReDi-palvelun arkkitehtuuri yleisellä tasolla nähdään kuvasta 2.

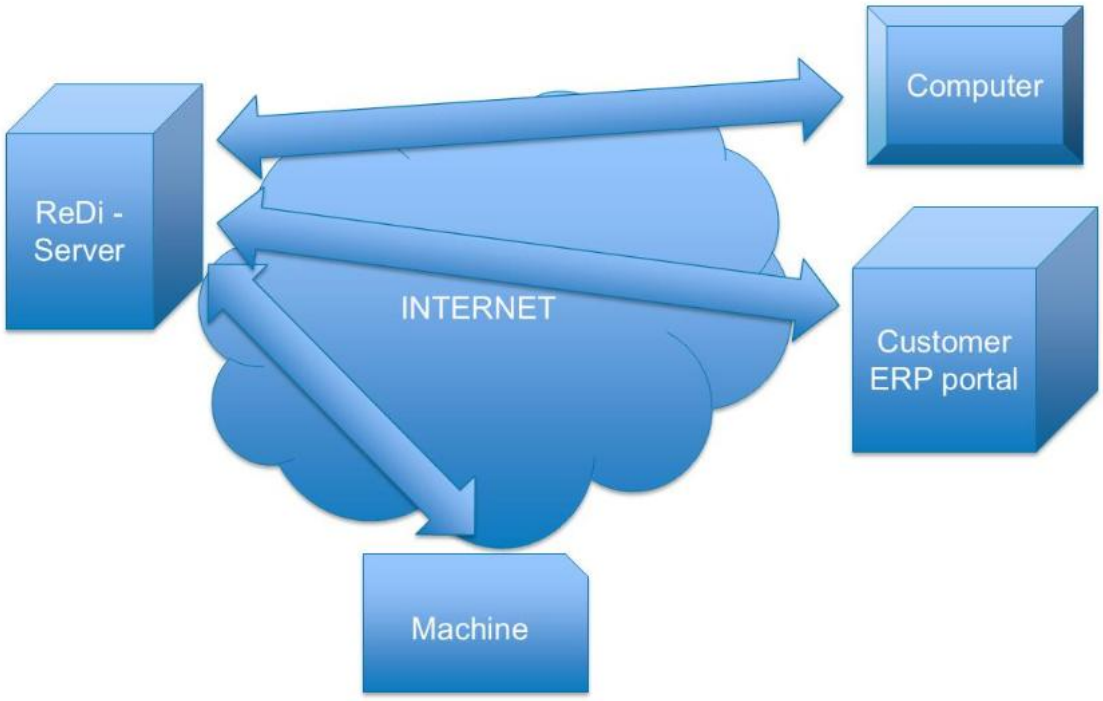


Kuva 2. Exertuksen ReDi-palvelun arkkitehtuuri (Exertus oy 2016: 3).

2.2.1 REST-palvelin

Kuvassa 3 on nähtävillä tarkempi kuvaus ReDi-palvelusta. Kuvasta nähdään, että tieto kulkee työkoneen ja ReDi-palvelun palvelimen välillä. Palvelimelta on yhteys asiakkaan ERP-järjestelmään ja toimistotietokoneille. Palvelinta ylläpitää Exertus ja sen tarkoituksena on käsitellä työkoneelta tulevaa raakaa dataa siten, että se saapuu asiakkaan järjestelmään oikeassa muodossa ohjelmointirajapinnan kautta (Exertus oy 2016: 2). ReDi-palvelun avulla saadaan tietoa myös järjestelmän toimivuudesta, sillä ReDi-palvelun ja sen palvelimen toiminta pysyy lähestulkoon aina samanlaisena. Jos tiedon kulku vikaantuu, voidaan palvelimen avulla rajata vika työkoneen ohjausjärjestelmään tai asiakkaan ERP-järjestelmään. ReDi-palvelun palvelin on rakennettu REST-

arkkitehtuurin mukaisesti ja se on tarkoitettu datan keräämiseen kaikenlaisilta työkoneilta. Koska kyseessä on REST-arkkitehtuurin mukainen palvelin, niin sitä voidaan käyttää sellaisenaan ilman muutoksia kaikilla Exertuksen ohjausjärjestelmillä.



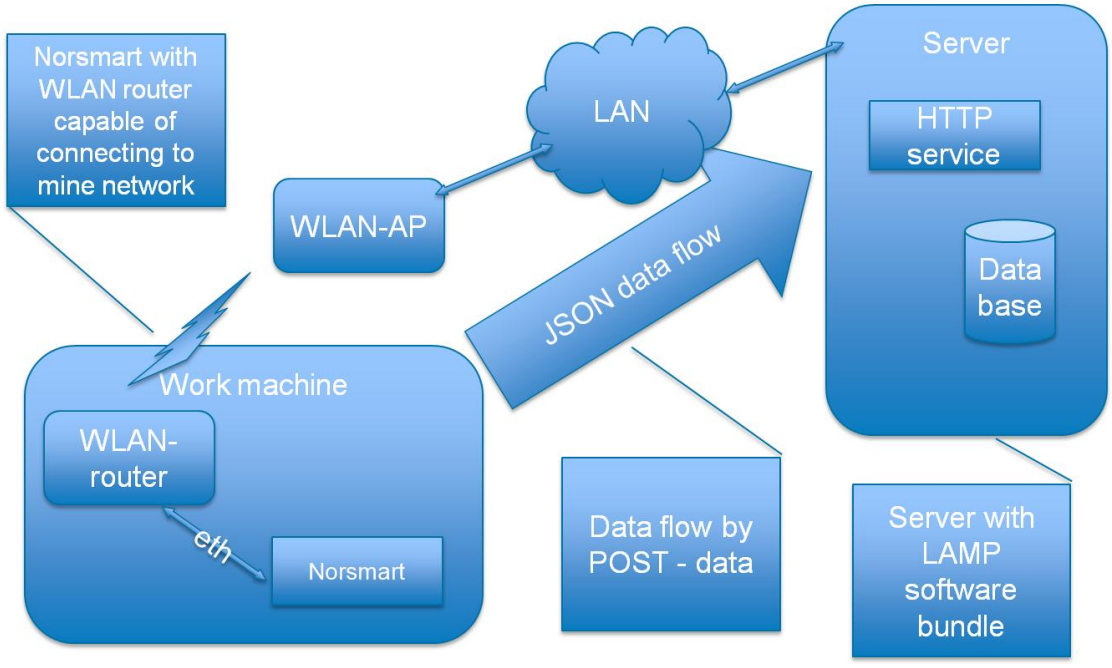
Kuva 3. Yhteydet Exertuksen ReDi-palvelussa (Exertus oy 2016: 2).

REST-ohjelmointirajapinnan periaatteita ovat hyvä suorituskyky, skaalautuvuus, yksinkertaisuus, siirrettävyys ja muokattavuus (Yellavula 2017: 9). REST-rajapintaan liittyviä rajoitteita ovat asiakas–palvelin-malliin perustuva arkkitehtuuri, yhtenäinen rajapinta, kerroksittainen järjestelmä, välimuisti, tilattomuus ja ladattava koodi. Näiden rajoitteiden katsotaan täyttävän WWW:n kehitykselle asetetut vaatimukset. Edellä mainitut rajoitteet täytyy siis löytyä järjestelmästä, jotta sitä voidaan kutsua REST-arkkitehtuurin mukaiseksi. (Massé 2011: 2–5.) REST-rajapinnassa tietojen lähetys ja vastaanotto ovat hyvin yksinkertaisia toimenpiteitä, sillä jokainen REST-rajapinnan kutsu liittyy URL-osoitteeseen ja HTTP-metodeihin, joista yleisimmin käytössä ovat GET, POST, PUT, PATCH, DELETE ja OPTIONS (Yellavula 2017: 11–12).

Myöhemmässä vaiheessa käytämme Exertuksen REST-palvelinta yhteyden testaamiseen. Yhteyttä testataan lähettämällä palvelimelle dataa POST-metodilla. Palvelin vastaa POST-pyyntöön sen perusteella hyväksyykö se vastaanottamansa datan. Jos palvelin hyväksyy datan, palvelin tallentaa sen tietokantaan ja lähettää vastauksen pyynnön lähettäjälle, jossa se kertoo toiminnon onnistuneen. Jos taas data on vääränlaista, palvelin ei tallenna sitä ja ilmoittaa pyynnön lähettäjälle, että data ei ole oikeassa muodossa. Muita REST-rajapinnan mukaisia HTTP-metodeja ei tällä kertaa tarvita.

2.2.2 Työkone

ReDi-palvelussa tieto liikkuu siis työkoneen ohjausjärjestelmästä Exertuksen REST-palvelimelle ja sieltä edelleen asiakkaan järjestelmiin. Tarkastellaan tiedon kulkua Normetin työkoneen Norsmart-ohjausjärjestelmästä ReDi-palvelun REST-palvelimelle. Pääpiirteet järjestelmän tästä osasta nähdään kuvasta 4.



Kuva 4. Tietoliikenne Norsmart-ohjausjärjestelmässä (Exertus oy 2013: 6).

Ohjausjärjestelmä kerää dataa työkoneesta sitä varten rakennettuun rengaspuskuriin. Dataa voidaan varastoida hetkellisesti pitkäänkin, jos internet-yhteyttä ei ole saatavilla

ja dataa ei pystytä lähettämään. Rengaspuskurin koko on siitä huolimatta rajallinen ja jossain vaiheessa vanhempaa dataa alkaa kadota, jos työkone on ollut pitkään ilman internet-yhteyttä. Työkoneen ohjausjärjestelmään on yhdistetty Ethernetillä standardin IEEE 802.11 mukainen langaton reititin tai silta tilanteesta riippuen. Näin työkoneen ohjausjärjestelmä voi yhdistyä kaivoksen tai tehtaan langattomaan verkkoon. Tämä langaton verkko taas on yhdistetty internetiin ja sitä kautta data kulkee ReDi-palvelun REST-palvelimelle. Työkoneen ohjausjärjestelmä kokoaa lähetettävän datan JSON-formaatin mukaiseen tekstitiedostoon. (Exertus oy 2013: 6–8.) JSON-formaatti helpottaa datan käsittelyä myöhemmin, sillä siitä on muodostunut eräänlainen de facto -standardi IoT-alalla (Korotkevitch 2016: 241). Yhteenvetona ReDi-palvelun palvelin on siis REST-arkkitehtuurin mukainen palvelin, jonne työkoneen ohjausjärjestelmä lähettää datan JSON-muodossa käyttäen POST-metodia (Exertus oy 2013: 6–8).

3 TIETOLIIKENNETEKNIIKAT

Diplomityössä keskitytään laitteistoon ja verkon suunnitteluun, joten on tarpeellista käydä läpi suunnittelussa ja toteutuksessa tarvittavien tekniikoiden teoriaa. Tähän liittyvät erityisesti erilaiset tietoliikenneprotokollat. Seuraavaksi käsiteltäviä tekniikoita tullaan soveltamaan uuden järjestelmän rakentamisessa.

3.1 OSI-malli

OSI-malli on ISO:n määrittelemä standardi ja se tulee sanoista Open Systems Interconnection. Sen tarkoituksena on ollut tarjota laitevalmistajille ja käyttäjille sellainen ympäristö, jossa järjestelmät olisivat yhteensopivia ja kykenisivät kommunikoimaan keskenään. Tähän tavoitteeseen ei ole päästy, eikä sen mukaisia järjestelmiä ole juurikaan käytössä. OSI-mallia käytetään kuitenkin tietoliikennejärjestelmien toiminnan kuvaamiseen, johon se sopii erityisen hyvin ja se onkin laajasti käytössä tässä tarkoituksessa. (Kaario 2002: 18; Hakala & Vainio 2005: 138.)

OSI-mallissa tietojärjestelmälle on määritelty seitsemän eri perustehtävää ja ne kuvataan kerroksina. Kerrokset yhdestä kolmeen liittyvät laitteistoon ja niiden käyttämiin protokolliin. Näitä kerroksia kutsutaan alakerroksiksi. Ylemmät kerrokset seitsemänteen kerrokseen asti sen sijaan määrittelevät asiakas–palvelin-sovelluksen toiminnan ohjelmallisesti. (Hakala & Vainio 2005: 138.) Käydään kerrokset läpi yksitellen alimmasta kerroksesta ylimpään kerrokseen.

Alin kerros on nimeltään fyysinen kerros. Se hoitaa bittien fyysisen käsittelyn, eli sen avulla määritellään sähköiset arvot signaalinsiirtoon. Fyysisellä kerroksella verkon aktiivilaitteita ovat esimerkiksi keskitin ja toistin. (Hakala & Vainio 2005: 139.)

Siirtoyhteyskerros määrittelee, miten datasta rakennetaan siirrettäviä yksiköitä, kuten kehyksiä ja soluja. Siirtokerros määrittelee myös lähettävän ja vastaanottavan osapuolen

fyysiset laiteosoitteet eli MAC-osoitteet. Siirtokerroksen laitteita ovat esimerkiksi verkkokortti, silta ja kytkin. (Hakala & Vainio 2005: 139.)

Kolmas kerros eli verkkokerros määrittelee tietoliikenteen reitittämisen. Tämä kerros ei välitä verkon fyysisestä rakenteesta ja tekniikasta, kunhan tieto vain kulkee alempien kerrosten kautta. Protokolla, jota tällä tasolla yleisesti käytetään, on IP. Tämän kerroksen tärkein laite on reititin, joka reitittää IP-paketit kohdeverkkoon. (Hakala & Vainio 2005: 139.)

Neljäs kerros ja samalla ylemmän kerroksen ensimmäinen kerros tunnetaan nimellä kuljetuskerros. Tähän kerrokseen liittyvät keskeisesti kuljetusprotokollat, joista yleisimpiä ovat TCP ja UDP. TCP on yhteydellinen protokolla, ja UDP on yhteydetön protokolla. Tällä tasolla protokollien tehtävänä on tehdä sovellusten tietovirroista pienempiä yksiköitä eli paketteja. Tiedon pilkkominen, pakettikoon määritys ja kuittaus muodostavat yhdessä kokonaisuuden nimeltä vuonohjaus, jonka yhteydelliset protokollat ottavat huomioon. Lisäksi yhteydellistä protokollaa käytettäessä tämä kerros huolehtii yhteyden muodostamisesta ja purkamisesta. Yhteydetön protokolla huolehtii tietovirran pilkkomisesta, mutta ei muusta vuonohjauksesta. (Hakala & Vainio 2005: 139–140.)

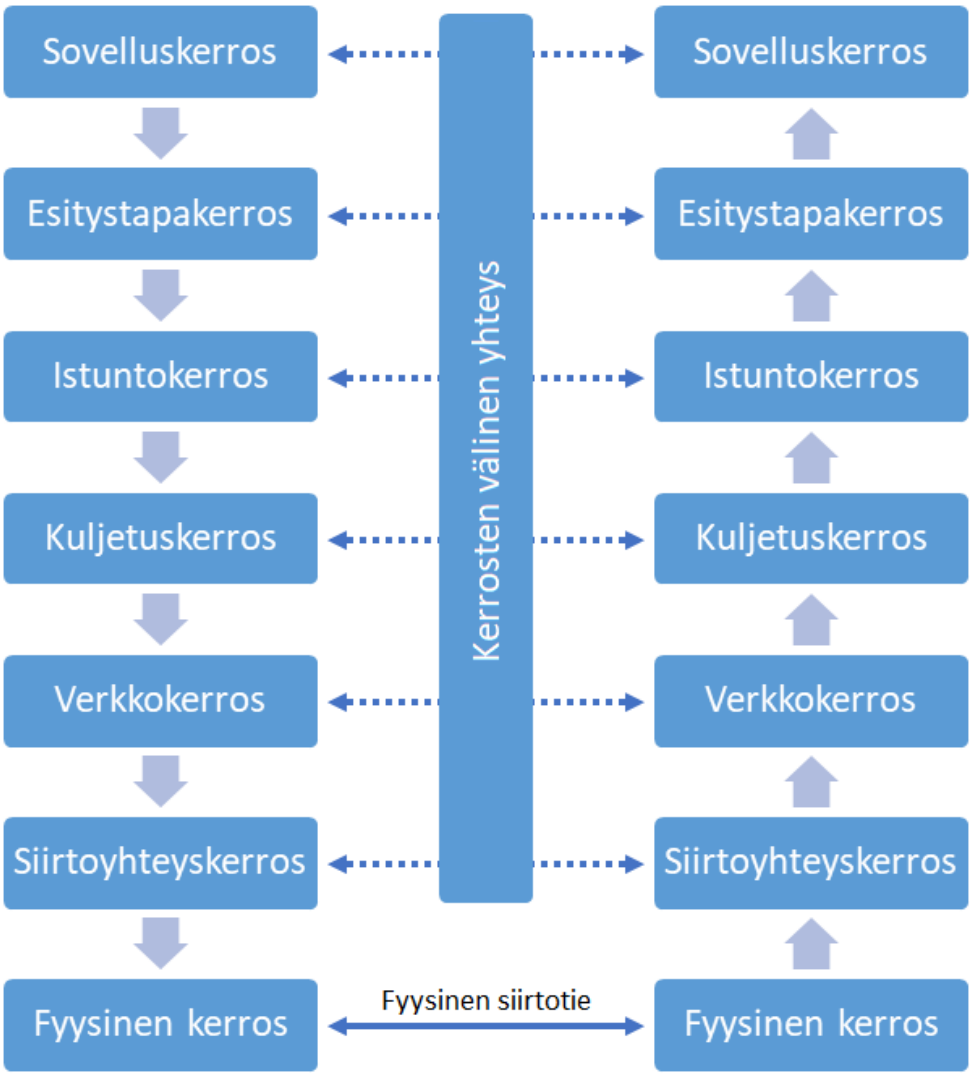
Istuntokerros huolehtii käyttöoikeuksien tarkistuksesta ja muista järjestelmän suojauksista. Sen tehtäviin kuuluu tarjota kirjautumisrutiinit ja salausmenetelmät sekä huolehtia lukituksista. Nykyään monista istuntokerroksen tehtävistä huolehtii käyttöjärjestelmä. (Hakala & Vainio 2005: 140.)

Esitystapakerros määrittelee muodon asiakkaan ja palvelimen väliselle sanomaliikenteelle. Näitä ovat erilaiset koodausjärjestelmät, kuten esimerkiksi merkistö ASCII. Myös tämän kerroksen tehtävistä suurin osa hoidetaan nykyään käyttöjärjestelmässä. (Hakala & Vainio 2005: 140.)

Mallin ylin kerros on sovelluskerros, joka määrittelee sovellusten ja käyttöjärjestelmien toimintojen ne osat, joita alemmissa kerroksissa ei ole määritelty. Se on siten rajapinta sovelluksia varten. Tavanomaisia palveluja ovat esimerkiksi Telnet, FTP ja SMTP. Ku-

ten edellä mainittiin, on istunto-, esitystapa- ja sovelluskerros nykyään ohjelmallinen kokonaisuus käyttöjärjestelmissä, eikä niiden erottaminen ole aina mahdollista. (Hakala & Vainio 2005: 140–141.)

Kerrosten nimet ja niiden välinen liikenne nähdään kuvasta 5. Kuvassa on havainnollistettu tietovuo lähettäjältä vastaanottajalle. Loogisella tasolla tieto siirtyy samantasoisten kerrosten välillä, kun taas fyysisellä tasolla tieto kulkee ainoastaan fyysisten kerrosten välillä. Ylemmästä kerroksesta alempaan tieto siirretään sen sijaan palvelupyynnöillä. Sanomaa vastaanotettaessa esitetään lukupyyntö alemmalle kerrokselle, jolloin saadaan kuittauksena vastaanotettu sanoma. (Granlund 2007: 10.)



Kuva 5. Tiedon siirto OSI-kerrosmallissa (Granlund 2007: 11).

3.2 TCP/IP-protokollaperhe

TCP/IP-protokollaperheestä puhuttaessa on hyvä eritellä yksittäiset protokollat TCP ja IP, sillä usein tätä protokollien yhdistelmää kutsutaan virheellisesti yhdeksi protokollaksi. Yhdessä TCP ja IP muodostavat siis TCP/IP-protokollaperheen. Lisäksi tähän protokollaperheeseen kuuluu myös muita jäsenprotokollia sovellus-, kuljetus-, verkko- ja siirtoyhteysprotokollista. TCP/IP-verkossa toiminnan lähtökohtana on verkkojen välinen tietoliikenne, eikä esimerkiksi yksilölliset laitteiden osoitteet. Hierarkkiset nimi- ja osoitejärjestelmät määrittelevät sekä verkon että laitteen sijainnin verkossa ja reitityksen avulla tieto liikkuu eri arkkitehtuurien mukaisten osaverkkojen välillä. Osoitteina käytetään loogisia osoitteita, jotka on määritelty laitteille ohjelmallisesti. Itse laitteet sijaitsevat sitten jossain verkossa, jossa on käytössä fyysiset laiteosoitteet eli MAC-osoitteet. (Hakala & Vainio 2005: 178.) Loogisen osoitteen ja MAC-osoitteen välisestä muunnoksesta huolehtivat protokollat ARP ja RARP (Kaario 2002: 63).

3.2.1 TCP/IP-protokollapino

Koska TCP/IP-protokollaperhe liittyy jollain tapaa kaikkiin OSI-mallin kerroksiin, on sillä myös OSI-mallin kaltainen kerrosmalli eli TCP/IP-protokollapino. Siihen kuuluu viisi kerrosta, jotka ovat fyysinen-, siirto-, verkko-, kuljetus- ja sovelluskerros. Näistä kahta ensimmäistä kerrosta voidaan kuvata myös yhtenä kerroksena, sillä kuten OSI-mallin yhteydessä mainittiin, verkkokerroksen alla voi olla melkein mikä verkkotekniikka tahansa. Täten TCP/IP-protokollaperhe toimii oikeastaan verkkokerrokselta ylöspäin, sillä fyysisen kerroksen ja siirtokerroksen asioita ei suoraan määritellä. TCP/IP-protokollapinon kerroksien suhde OSI-mallin kerroksiin nähdään kuvasta 6. Kuten kuvasta havaitaan, niin TCP/IP-protokollapinon kerrokset voivat vastata useampaa kerrosta OSI-mallista. Esimerkiksi sovelluskerros käsittää jopa kolme kerrosta OSI-mallista. TCP/IP-protokollapino helpottaa siis TCP/IP-protokollaperheen käsittelyä, kun sitä voidaan verrata OSI-malliin. (Kaario 2002: 21–22.)

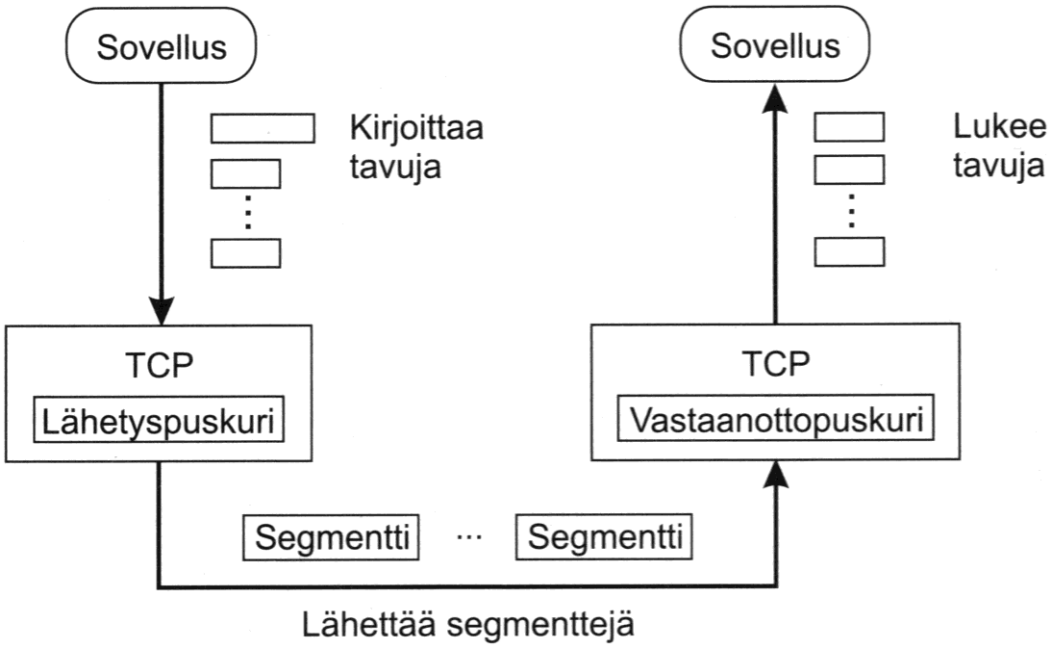
Kuva 6. TCP/IP-protokollapinon kerrosten suhde OSI-mallin kerroksiin (Kaario 2002: 22).

3.2.2 TCP

Transmission Control Protocol eli TCP on yhteydellinen tietoliikenneprotokolla, joka tarjoaa sovelluksille luotettavan kuljetuspalvelun. Luotettavuus tarkoittaa tässä tapauksessa sitä, että TCP kykenee varmistamaan tiedon perillemenon ja korjaamaan mahdolliset virheet tiedonsiirrossa. Yhteydellisyys tarkoittaa sitä, että TCP:n kuljetuspalvelu on aina kahden pisteen välistä palvelua. Tämä tarkoittaa myös sitä, että osapuolten välillä neuvotellaan yhteyden muodostamisesta ja purkamisesta. TCP käsittelee tavuvirtaa, eli TCP-kerroksen yläpuolella oleva sovellusprosessi kirjoittaa tavuja TCP:lle lähetystä varten. TCP voi varastoida tavuja puskureihin. Lähetyspuskurista TCP lähettää segmenttejä, jotka eivät välttämättä ole samankokoisia sovelluksen kirjoittamien palasten kanssa. (Kaario 2002: 166.) Kuvasta 7 nähdään, kuinka TCP lukee tavuja ja lähettää segmenttejä.

TCP:n yläpuolella olevat sovellusprosessit tunnistetaan porttinumeroilla. Niiden avulla yksi TCP-prosessi voi palvella useita sovelluksia samaan aikaan. TCP osaa myös valvoa verkon suorituskykyä ja voi säätää lähetysnopeuttaan sen mukaan. Käytännössä lähettä-

jä tarvitsee siis tiedon siitä, kuinka paljon vastaanottaja voi vastaanottaa tietoa. (Kaario 2002: 166.)



Kuva 7. Tavujen kirjoittaminen ja lukeminen (Kaario 2002: 166).

3.2.3 IP

Internet Protocol eli IP välittää paketteja verkkojen osasta toiseen. Luonteeltaan se on yhteydetön protokolla, eli verkkokerroksen tasolla ei pidetä kirjaa olemassa olevista yhteyksistä, sillä se jätetään ylempien kerrosten protokollien hoidettavaksi. IP:n hyvä suorituskyky perustuu siihen, että se ei suorita vuonohjausta eikä virheenkorjausta. IP-liikenne on luonteeltaan pakettiliikennettä, missä kaikki paketit välitetään erikseen riippumatta siitä, mitä reittiä edellinen paketti on kulkenut. IP:n tehtäviä ovat muun muassa pakettien osioiminen, liikenteen reititys IP-osoitteen avulla ja peruspaketin koon määritys. (Anttila 2001: 114.)

On hyvä erottaa käsite IP-osoite itse protokollasta, sillä kuten aiemmin mainittiin, niin IP reitittää liikennettä IP-osoitteen avulla. Tällä hetkellä on käytössä versiot IPv4 ja IPv6. Näistä IPv4 on vanhempi ja edelleen laajasti käytössä. Diplomityössä käsitellään ainoastaan IPv4-osoitteita, joten käydään läpi IPv4-osoitteen rakennetta. IPv4:n mukai-

nen IP-osoite lukuna muodostuu 32 bitistä ja tavallisesti se esitetään neljän desimaaliluvun sarjana pisteillä erotettuna. Pisteillä erotetut luvut ovat arvoltaan välillä 0–255. (Anttila 2001: 87.) Internetin osoiteavaruus on jaettu viiteen eri luokkaan, joita ovat A, B, C, D ja E. Kullakin luokalla on tietty määrä osoitteita. (Anttila 2001: 88–90.) Nykyään puhutaan kuitenkin luokattomista IP-osoitteista. Luokattomuuden tarjoaa erityinen CIDR-tekniikka. (Anttila 2001: 109–110.)

IP-osoitteiden käyttöön liittyy tärkeänä osana aliverkotus. Aliverkotus on tärkeää erityisesti julkisten IP-osoitteiden yhteydessä, sillä niitä on käytössä hyvin rajallinen määrä. Siksi tällaiset osoitteet olisi hyvä jakaa mahdollisimman tehokkaasti käytössä olevien laitteiden kesken. Jos esimerkiksi yritys tarvitsee julkiset IP-osoitteet kymmenelle laitteelle, niin ei ole järkeä antaa yrityksen käyttöön kokonaista C-luokan osoiteavaruutta, joka käsittäisi 254 osoitetta. Aliverkotus hoidetaan yleisimmin erillisen aliverkon maskin avulla. Aliverkon maski peittää kohdeosoitteesta tietyn osan. Aliverkon maskin avulla IP-osoitteesta nähdään sen verkko-osa, sillä aliverkon maskin kohdalla peiton kohde on IP-osoite ja peitettävä kohde on osoitteen laiteosuus. Kun laite haluaa kommunikoida toisen laitteen kanssa, niin laite tekee oman ja vastapuolen osoitteen välillä binäärisen XOR-operaation. Tästä saatavaan tulokseen tehdään binäärinen AND-operaatio aliverkon maskin kanssa. Mikäli AND-operaation tulos on nolla, niin vastaanottajalaite sijaitsee samassa verkossa ja paketti voidaan lähettää käyttäen lähiverkon menetelmiä. Mikäli tulos ei ole nolla, niin vastaanottaja sijaitsee jossain toisessa verkossa ja paketti lähetetään reitittimelle, josta paketti reititetään eteenpäin kohti oikeaa verkkoa. (Anttila 2001: 96–99.) Aliverkon maski voi olla esimerkiksi 255.255.255.0. Tällöin esimerkiksi laite, jonka IP-osoite on 10.3.2.2, sijaitsee verkossa 10.3.2.0. Toisin sanoen aliverkon maskin nolla-bitit kertovat mikä osa osoitteesta voi muuttua. Esimerkissämme verkossa on siis käytössä IP-osoitteet 10.3.2.1–10.3.2.254 osoitteen 10.3.2.255 ollessa levitysviestiosoite. Verkko-osoite ja aliverkon maski yhdistetään nykyään CIDR-tekniikan merkintätavan mukaisesti. Edellä mainittu esimerkkiverkko 10.3.2.0 ja aliverkon maski 255.255.255.0 kirjoitettaisiin CIDR-merkintätavan mukaisesti muotoon 10.3.2.0/24, missä kauttamerkin jälkeinen luku kertoo ykkösbittien määrän aliverkon maskissa (Anttila 2001: 110).

Diplomityön kannalta oleellista on tietää mitä IP-osoitteita voidaan käyttää yksityisessä verkossa eli lähiverkossa, sillä julkisiin internet-osoitteisiin ei oteta nyt kantaa. Jos tarkastellaan IP-osoitteita internetin näkökulmasta, niin on olemassa tiettyjä osoitteita, joita ei voida käyttää julkisina IP-osoitteina internetissä. Taulukossa 1 on listattu erikoiskäyttöön varatut verkot ja siitä nähdään yksityisille verkoille varatut verkko-osoitteet, joita ovat 10.0.0.0/8, 172.16.0.0/12 ja 192.168.0.0/16. Tätä kannattaa soveltaa myös toiseen suuntaan. Toisin sanoen lähiverkossa, josta on yhteys internetiin, ei kannata käyttää sellaisia IP-osoitteita, jotka ovat oikeita osoitteita internetissä. Lähiverkoissa kannattaakin käyttää juuri lähiverkoille tarkoitettuja osoitteita taulukon 1 mukaisesti.

Taulukko 1. Erikoiskäyttöön varatut osoitteet (Internet Assigned Numbers Authority 2017).

Address Block	**Name**
0.0.0.0/8	"This host on this network"
10.0.0.0/8	Private-Use
100.64.0.0/10	Shared Address Space
127.0.0.0/8	Loopback
169.254.0.0/16	Link Local
172.16.0.0/12	Private-Use
192.0.0.0/24	IETF Protocol Assignments
192.0.0.0/29	IPv4 Service Continuity Prefix
192.0.0.8/32	IPv4 dummy address
192.0.0.9/32	Port Control Protocol Anycast
192.0.0.10/32	Traversal Using Relays around NAT Anycast
192.0.0.170/32, 192.0.0.171/32	NAT64/DNS64 Discovery
192.0.2.0/24	Documentation (TEST-NET-1)
192.31.196.0/24	AS112-v4
192.52.193.0/24	AMT
192.88.99.0/24	Deprecated (6to4 Relay Anycast)
192.168.0.0/16	Private-Use
192.175.48.0/24	Direct Delegation AS112 Service
198.18.0.0/15	Benchmarking
198.51.100.0/24	Documentation (TEST-NET-2)
203.0.113.0/24	Documentation (TEST-NET-3)
240.0.0.0/4	Reserved
255.255.255.255/32	Limited Broadcast

On olemassa hyviä käytäntöjä siitä, miten eri osoitteet kannattaa jakaa laitteiden kesken. Kuten taulukosta 1 nähdään, niin laitteen osoite ei saa olla 0 tai 255, sillä 0 tarkoittaa verkkoa itseään, eikä näin ole yksittäinen laite ja 255 on levitysviestiosoite, jonka kautta lähetetään viesti yleislähetyksenä kaikille verkon laitteille. Käytäntö laitteiden osoitteille voi olla millainen tahansa, sillä sen tarkoitus on helpottaa ihmisten työtä uusia asennuksia tehtäessä ja virhetilanteita selvitettäessä. Esimerkiksi reitittimille, palvelimille ja asiakaslaitteille jaettavat osoitteet voidaan määritellä alkavan jostain tietystä luvusta. Kuvitellaan, että käytössä on aiemmin mainitun verkon 10.3.2.0/24 IP-osoitteet 10.3.2.1–10.3.2.254, jolloin osoitteen viimeinen desimaaliluku muuttuu. Tällöin esimerkiksi reitittimille ja hallittaville kytkimille voidaan antaa osoitteet 1–10, palvelimille osoitteet 200–254, asiakaslaitteille osoitteet 100–199 ja varalle jää vielä osoitteet 11–99. (Anttila 2001: 94.)

3.3 DHCP

Dynamic Host Configuration Protocol eli DHCP on tietoliikenneprotokolla, jonka tärkein tehtävä on antaa IP-osoite verkkoon kytkeytyvälle työasemalle. Yleensä DHCP antaa myös muita IP-parametrejä. Näitä ovat esimerkiksi aliverkon maski, yhdyskäytävä, nimipalvelimien IP-osoitteet ja verkkotunnus. Työasema voi pyytää näitä parametrejä DHCP-palvelimelta, jossa on DHCP-palvelu toiminnassa. DHCP-palvelu ei ole verkossa välttämätön, sillä tarvittavat parametrit voidaan asettaa työasemalle myös käsin, mutta työasemien määrän kasvaessa tämä muuttuu hyvin epäkäytännölliseksi. Siksi DHCP onkin erityisen kätevä suuressa verkossa, jossa työasemat ovat satunnaisesti käynnissä ja niiden sijainti vaihtelee. Tästä huolimatta DHCP on yleisesti käytössä jo ihan pienissäkin verkoissa, sillä sen käyttöönotto on helppoa ja hyöty on suuri. DHCP-palvelin voi sijaita reitittimellä, mutta suuremmissa verkoissa sitä varten kannattaa olla oma palvelimensa. (Anttila 2001: 201–202.)

DHCP-palvelin voi määritellä IP-osoitteen työasemalle kolmella tavalla, joita ovat automaattinen määrittely, dynaaminen määrittely ja määrittely käsin. Automaattinen määrittely tarkoittaa sitä, että osoitetta pyytävälle työasemalle annetaan osoite määrittele-

mättömäksi ajaksi. Dynaamisessa määrittelyssä osoite annetaan määritellyksi ajaksi. Käsin määriteltäessä verkon ylläpitäjä asettaa palvelimen antamaan kiinteitä IP-osoitteita tietyille työasemille niiden MAC-osoitteiden perusteella. Voidaan määritellä esimerkiksi työasema, jonka MAC-osoite on 00-00-0c-a0-a2-10 saamaan aina IP-osoite 10.3.2.10. Käsin määrittely on hyödyllistä silloin, kun tietylle työasemalle halutaan antaa aina sama osoite, mutta halutaan sen saavan muita mahdollisesti muuttuvia parametrejä DHCP-palvelimelta. Tavallisesti käytetään dynaamista määrittelyä, sillä siinä osoitteet voivat palautua tietyn ajan kuluttua takaisin jaettavien osoitteiden joukkoon. Jos esimerkiksi verkossa, jossa työasemia on enemmän kuin jaettavia IP-osoitteita käytettäisiin automaattista määrittelyä, osoitteet loppuisivat jossain vaiheessa kesken ja viimeisinä käynnistetyt työasemat eivät saisi enää osoitteita ollenkaan. Dynaamisella määrittelyllä tämä onnistuu, kunhan kaikki työasemat eivät ole yhtä aikaa päällä. (Anttila 2001: 203.)

3.4 DNS

Domain Name System eli DNS on nimipalvelujärjestelmä, joka muuntaa verkkotunnuksen (domain) IP-osoitteeksi. Jos esimerkiksi halutaan vierailla osoitteessa univaasa.fi, niin DNS muuntaa verkkotunnuksen univaasa.fi IP-osoitteeksi 193.166.120.2. Pelkkä verkkotunnus ei siis toimi yksinään, vaan sen takaa löytyy aina IP-osoite, jonka avulla varsinainen yhteys muodostetaan. (Järvinen 2003: 166.) Verkkotunnukset taas helpottavat lähinnä osoitteiden muistamista, sillä nimet painuvat numerosarjoja helpommin mieleen (Anttila 2001: 231). Nimipalvelun toiminta perustuu nimipalvelimiin (domain name server), jotka tietävät verkon sisällä olevien laitteiden verkkotunnukset ja niitä vastaavat IP-osoitteet. Jos nimipalvelin ei pysty selvittämään sille saapunutta pyyntöä, se lähettää pyynnön toiselle nimipalvelimelle ja tätä jatkuu, kunnes oikea palvelin löytyy ja vastaava IP-osoite selviää. (Järvinen 2003: 166.) Internetin verkkotunnuksista kirjaa pitävät nimipalvelimet sijaitsevat tietenkin internetissä, mutta myös lähiverkossa voidaan ylläpitää omaa nimipalvelinta ja omia lähiverkon sisäisiä verkkotunnuksia. Tällainen verkkotunnus voisi olla esimerkiksi mailsrv1.koti.local, jonka IP-osoite lähiverkos-

sa olisi esimerkiksi 10.3.2.200 ja tämän verkkotunnus löytyisi ainoastaan lähiverkosta. (Hakala & Vainio 2005: 226–228.)

3.5 NAT

Muun muassa reitittimen ominaisuuksiin kuuluva osoitteenmuunnos eli NAT muuntaa lähiverkon yksityiset IP-osoitteet yksilöllisiksi ulkoisiksi IP-osoitteiksi. Näin esimerkiksi monen lähiverkon laitteen IP-osoitteet saadaan näkymään internetiin yhtenä IP-osoitteena. Tällöin lähiverkon sisäisessä liikenteessä voidaan käyttää lähiverkon osoiteavaruuteen kuuluvia osoitteita ja ulkopuolelle, eli yleensä internetiin suuntautuvissa yhteyksissä käytetään sitten julkista osoitetta. Samasta syystä NAT parantaa myös tietoturvaa toimiessaan eräänlaisena palomuurina, joka piilottaa lähiverkon osoitteet ulkomaailmalta. Lisäksi lähiverkon laitteella on ulkoinen osoite vain silloin, kun yhteys on muodostettu ulkomaailmaan osoitteenmuunnoksen kautta. (Ballew 1998: 237–239.)

Osoitteenmuunnos toimii yleensä siten, että kun lähiverkon laite ottaa yhteyden esimerkiksi internetiin, NAT antaa sen käyttöön IP-osoitteen. Kun laite lähettää paketin, NAT korvaa sen lähiverkon IP-osoitteen dynaamisesti allokoidulla ulkoisella IP-osoitteella. Kun tällä samalla osoitteella varustettu paketti palaa takaisin, NAT tekee käänteisen osoitteenmuunnoksen, eli korvaa ulkoisen osoitteen alkuperäisellä sisäisellä osoitteella. Kun laite lopettaa yhteyden, NAT vapauttaa ulkoisen osoitteen muiden laitteiden käyttöön. (Ballew 1998: 237–238.)

Osoitteenmuunnos voidaan tehdä neljällä tavalla, joita ovat menetelmät yhdestä yhteen, yhdestä moneen, monesta yhteen ja monesta moneen. Yhdestä yhteen tarkoittaa sitä, että yksi lähiverkon IP-osoite muunnetaan yhdeksi julkiseksi IP-osoitteeksi. Yhdestä moneen puolestaan tarkoittaa sitä, että jokaiselle, yhdestä lähiverkon osoitteesta lähtevälle yhteydelle annetaan oma julkinen osoite. Monesta yhteen on tapa, jossa lähiverkon osoitteet muunnetaan aina yhdeksi ja samaksi julkiseksi osoitteeksi. Monesta moneen tarkoittaa nimensä mukaisesti sitä, että lähiverkon osoitteita muunnetaan tietyn julkisen osoiteavaruuden sisältämiksi osoitteiksi. (Gheorghe 2006: 91.)

Edellä esitelty osoitteenmuunnos on niin sanottu täysimääräinen osoitteenmuunnos (Full NAT). Osoitteenmuunnoksen tavanomaisimmissa käyttökohteissa sitä käytetään juuri täysimääräisenä. Täysimääräinen osoitteenmuunnos koostuu kahdesta eri osoitteenmuunnoksen alalajista. Näitä ovat lähdeosoitteenmuunnos (SNAT) ja kohdeosoitteenmuunnos (DNAT). Lähdeosoitteenmuunnos muuntaa ainoastaan tietyn lähdeosoitteen joksikin tietyksi osoitteeksi, joka määritetään käsin. Jos esimerkiksi reitittimessä on pelkkä lähdeosoitteenmuunnos käytössä, niin pakettia lähetettäessä lähiverkon osoite muunnetaan käsin määritellyksi julkiseksi osoitteeksi, mutta paketin palatessa reitittimelle julkista osoitetta ei muunneta takaisin lähiverkon osoitteeksi. Tällöin paketti ei pääse takaisin lähdeosoitteeseensa. Masquerade on lähdeosoitteenmuunnoksen erityistapaus, joka toimii muuten kuten lähdeosoitteenmuunnos, mutta se ei muunna lähiverkon osoitetta käsin määritetylle julkiselle osoitteelle, vaan reitittimen ulkoisen verkkosovittimen osoitteelle, joka voi vaihdella. Kohdeosoitteenmuunnos muuntaa tietyn kohdeosoitteen joksikin tietyksi osoitteeksi. Periaate on sama kuin lähdeosoitteenmuunnoksessa, mutta muunnos tehdään nyt vain toiseen suuntaan. Jos reitittimessä on pelkkä kohdeosoitteenmuunnos käytössä, niin julkisesta verkosta tulevat paketit pääsevät kohdeosoitteenmuunnoksessa määritettyyn osoitteeseen, mutta paketit eivät voi palata takaisin, sillä osoitetta ei muunneta takaisin. Yhdessä lähdeosoitteenmuunnos ja kohdeosoitteenmuunnos muodostavat siis täysimääräisen osoitteenmuunnoksen, jolloin osoitteenmuunnos toimii molempiin suuntiin ja yhteys voidaan muodostaa osoitteenmuunnosta käyttäen. (Gheorghe 2006: 92–96.)

4 SUUNNITTELU

4.1 Nykyinen tiedonsiirtojärjestelmä

Nykyinen järjestelmä tietoliikenteen näkökulmasta koostuu työkoneesta ja ReDi-palvelun REST-palvelimesta suhteella monesta yhteen, eli työkoneita on monta ja REST-palvelimia yksi. Järjestelmän tiedonsiirrossa käytetään standardin IEEE 802.11 mukaista langatonta lähiverkkoa (WLAN), mikä tunnetaan myös nimellä Wi-Fi. Työkoneen ohjausyksikköön on kytketty standardin mukainen langaton silta, joka yhdistyy kaivoksen tai tehtaan langattomaan lähiverkkoon, jos sellainen on saatavilla. Tätä kautta työkoneen ohjausyksikkö on yhteydessä internetiin ja REST-palvelimelle. Ongelmaksi muodostuu kuitenkin se, että langatonta lähiverkkoa ei ole läheskään aina saatavilla tai sen kantama ei riitä sinne asti, missä työkoneita käytetään.

Myös matkapuhelinverkkoa voidaan hyödyntää. Tällöin internet-yhteys ei ole pelkän langattoman lähiverkon varassa. Siitä huolimatta tällainen ratkaisu auttaa vain silloin, kun työkoneet ovat maan päällä. Koska Normetin työkoneita käytetään usein haastavissa olosuhteissa syvällä maan alla, niin edellä mainitut tekniikat eivät toimi sellaisenaan. Edes matkapuhelinverkoista ei ole hyötyä maan alla, sillä signaali ei pääse kiven ja maa-aineksen läpi. Tätä voidaan verrata tilanteeseen, jossa puhelimeen puhutaan mentäessä ison tunnelin läpi junalla ja yhteys katkeaa. Normetin työkoneet ovat lähes aina vielä paljon syvemmällä kuin tällaiset tunnelit, joten yhteys ei varmasti toimi kumpaankaan suuntaan. Tilanne on samanlainen langatonta lähiverkkoa käytettäessä. Langattoman lähiverkon yhteys on usein vielä huomattavasti heikompi kuin yhteys matkapuhelinverkon välityksellä, sillä lähetysteho on pienempi. Lisäksi taajuus voi olla suurempi, jolloin signaali vaimenee voimakkaammin.

Koska työkoneiden kanssa käytetään tavallisesti langatonta lähiverkkoa, on vaihtoehtoja pääasiassa kaksi. Helpompi tapa on se, että jos kaivos sijaitsee esimerkiksi tehtaan lähellä ja tehtaalla on langaton lähiverkko, niin työkoneella voidaan silloin tällöin nousta maan pinnalle, jolloin verkkoon voidaan liittyä. Tämä on tosin melko epäkäytännöllistä,

jos kaivoksesta täytyy nousta pelkästään sen takia. Tämä riippuu toki siitä, millainen työkone on kyseessä, mutta sellaisia työkoneita, jotka muuten olisivat paljon maan alla, ei ole kannattavaa tuoda ylös vain yhteyden takia. Toinen vaihtoehto on rakentaa kaivokseen oma verkkoinfrastruktuuri, joka tarjoaa langattoman lähiverkon kaivoksen sisällä. Tämä edellyttää kaapeleiden vetämistä kaivokseen ja useiden langattomien siltojen tai langattomien reitittimien asennusta kaivoksen kokoluokasta riippuen. Tämä on kallista, sillä se vie aikaa ja resursseja, mutta toisaalta siinä saavutetaan suuri hyöty tietoliikenteen reaaliaikaisuudella.

4.2 Uusi tiedonsiirtojärjestelmä

Tarkoituksena on kehittää sellainen järjestelmä, jonka avulla kaivoksen työkoneiden tuottama data saadaan siirrettyä ReDi-palvelun REST-palvelimelle. Koska vaatimuksena on ainoastaan datan saaminen palvelimelle, niin tiedonsiirron reaaliaikaisuudesta voidaan luopua. Tällöin data voidaan siirtää tallennusvälineen avulla yhteydettömästi. Yhteydettömällä tiedonsiirrolla tarkoitetaan tässä tapauksessa sitä, että kun data lähtee työkoneelta, se ei heti pääse palvelimelle. Itse asiassa data ei välttämättä koskaan pääse oikealle palvelimelle, vaikka työkoneen ohjausjärjestelmän näkökulmasta data onkin lähetetty onnistuneesti. Tarkoitus tietenkin olisi, että data pääsee aina palvelimelle asti. Tästä johtuen voidaan käyttää termiä yhteydetön tiedonsiirto, koska ylemmällä tasolla nähdään vain työkone ja REST-palvelin. Tällä tasolla työkone lähettää dataa ja palvelin vastaanottaa tätä dataa, mutta lähetys ja vastaanotto tapahtuvat selvästi eri aikoina. Se, mitä tapahtuu tällä välillä, ei ole osapuolten tiedossa. Alemmalla tasolla osakokonaisuuksissa tiedonsiirto on toki yhteydellistä johtuen käytetyistä menetelmistä ja protokollista.

Yksinkertaisin esimerkki tällaisesta tapauksesta on ulkoisen tallennusmedian, kuten esimerkiksi USB-muistin käyttäminen. USB-muistia voitaisiin kuljettaa työkoneen ja palvelimen välillä ja sitä voisi käyttää siihen valtuutettu kaivostyöntekijä. Työkoneen päässä ohjausjärjestelmään kiinnitettäisiin USB-muisti, jolloin data siirtyisi USB-muistille. Tämän jälkeen USB-muisti kuljetettaisiin fyysisesti palvelimelle ja data siir-

rettäisiin sinne. Tällaista järjestelmää kutsutaan leikkisästi nimellä sneakernet. Siinä data siirretään fyysiselle tallennusmedialle paikassa A ja kuljetetaan sellaisenaan paikkaan B, jossa data puretaan tallennusmedialta. (Ulz, Pieber, Steger, Haas & Matischek 2017: 261.) Tällaisenaan järjestelmä on kuitenkin erittäin kömpelö, sillä USB-muistia ei kannata kuljettaa mahdollisesti maasta toiseen palvelimelle asti. Itse palvelimen sijaintia ei edes tarkasti tiedetä työkoneen päässä, sillä palvelinta ylläpitää Exertus. Täten datan kuljettaminen palvelimelle on mahdotonta. Sen sijaan USB-muistia voitaisiin kuljettaa työkoneen ja internetiin kytketyn tietokoneen välillä, jolloin USB-muistilla oleva data siirrettäisiin ensin tietokoneeseen, josta data sen jälkeen siirtyisi internetin välityksellä palvelimelle. Huonona puolena tässä on edelleen se, että USB-muisti pitäisi aina kiinnittää fyysisesti kaikkiin työkoneisiin erikseen. Tämä vie tietenkin paljon aikaa, jos työkoneita pitää etsiä kaivoksesta ja mahdollisesti pitää kirjaa niistä työkoneista, joista data on jo siltä erää siirretty USB-muistille. Lisäksi työkoneen toiminta pitää joissakin tapauksissa pysäyttää hetkellisesti tai ainakin noudattaa äärimmäistä varovaisuutta, jotta USB-muisti päästään kiinnittämään työkoneen ohjausyksikköön. Tämän jälkeen USB-muisti pitäisi vielä viedä sellaiseen paikkaan, jossa on tietokone ja internet-yhteys. Tällaisia paikkoja saattaa olla vain tehtaassa tai toimistossa, joka voi olla pitkänkin matkan päässä.

Koska työkoneet kykenevät langattomaan tiedonsiirtoon, niin eikö kannattaisi hyödyntää sitä myös tässä yhteydettömässä tiedonsiirrossa? Tiedonsiirtoa ei tarvitse välttämättä tehdä oikeasti yhteydettömänä pelkkien tallennusvälineiden avulla, kuten edellä kuvattiin. Työkoneen langaton datasiirtolaite tarvitsee vain samanlaisen liityntäpisteen, kuin olisi normaalissakin tapauksessa käytettäessä esimerkiksi tehtaan langatonta lähiverkkoa.

Edellä mainittua ajatusta jalostamalla, voitaisiin kehittää eräänlainen liikkuva tietokone, johon olisi kytketty kaksi langatonta reititintä, joista toinen on asennettu tukiasemaksi ja toinen tavalliseksi asiakkaaksi. Työkoneessa olisi tällöin langattoman sillan sijaan myös langaton reititin asiakastilassa, joka voisi liittyä liikkuvan tietokoneen tukiasemaan ja lähettää datan sinne. Sieltä data lähetettäisiin oman asiakastilassa olevan reitittimen avulla edelleen tehtaan langattoman lähiverkon tukiasemalle sitten, kun tällainen verkko

on saatavilla. Sieltä data pääsee internetiin ja edelleen oikealle palvelimelle. Tällä tavoin data saataisiin siirtymään automaattisesti langatonta tekniikkaa hyödyntämällä. Näin dataa keräävää tietokonetta voitaisiin vain liikutella kaivoksessa lähellä työkoneita ja kun data on kerätty, noustaan ylös ja lähetetään data palvelimelle.

Tällaisen liikkuvan tietokoneen voidaan ajatella olevan eräänlainen välityspalvelin, joka muodostaa koko järjestelmästä osittaisen viivesietoisen verkon (delay-tolerant network). Siinä dataa siirretään ainoastaan yksi solmuväli kerrallaan (hop-by-hop), jolloin solmulle saapunut viesti tallennetaan pysyväismuistiin odottamaan reititystä uuteen solmuun (store-and-forward). Solmut voivat myös liikkua fyysisesti paikasta toiseen, jolloin ne kuljettavat viestejä mukanaan (store-carry-and-forward). (Dunkels, Alonso, Voigt, Ritter & Schiller 2004: 146; Syrjänen 2007: 7.) Tässä tapauksessa liikkuva solmu on siis välityspalvelin ja se voi olla internet-yhteyden ulottumattomissa hyvinkin pitkän ajan. Tällöin viive tiedonsiirrossa kasvaa moninkertaiseksi verrattuna perinteiseen, millisekunteja kestävään päästä–päähän-yhteyteen, johon esimerkiksi internet perustuu. Tässä tapauksessa puhutaan minuuteista tai jopa tunneista. Tällöin on käytännöllistä siirtää toimitusvastuu työkoneelta aina välityspalvelimelle (custody transfer), jolloin työkoneen ei tarvitse saada tietoa oikealta palvelimelta viestin perillemenosta. Riittää, että välityspalvelin ilmoittaa työkoneelle olevansa oikea palvelin ja vastaanottaneensa tämän viestin. (Fall 2003: 31–32; Syrjänen 2007: 7.)

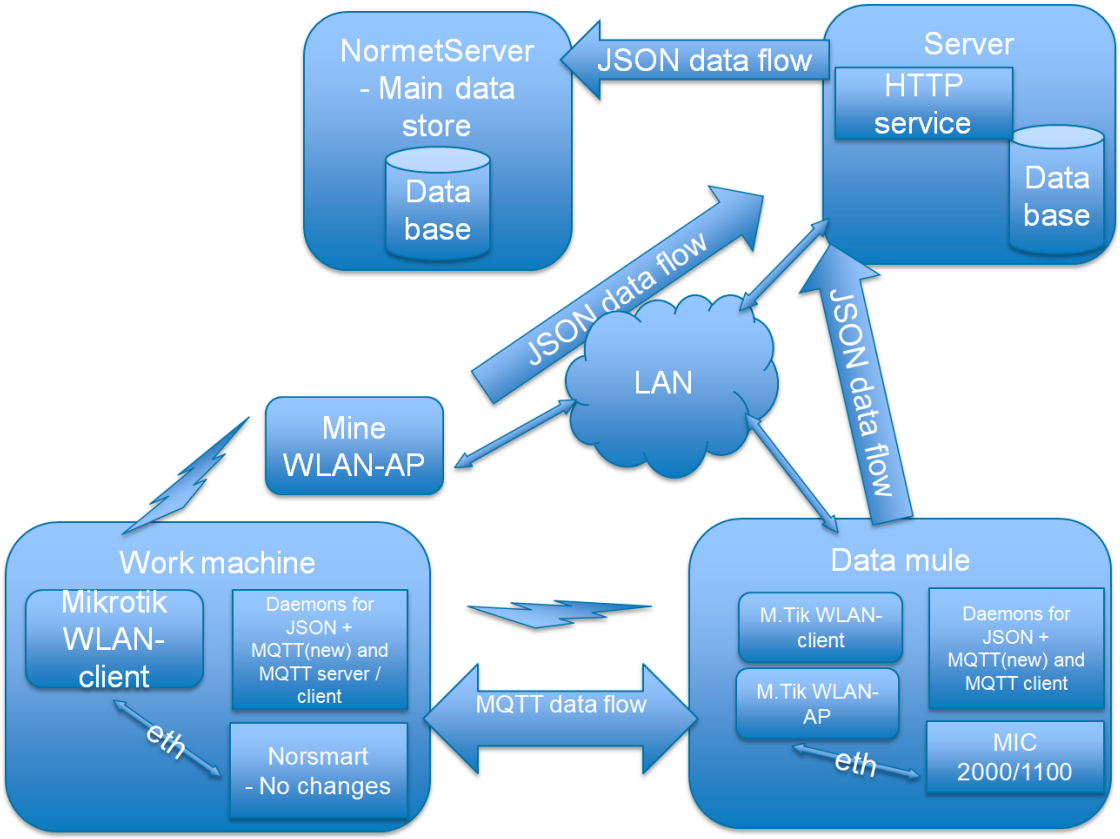
Edellä mainitut tekniikat edellyttävät kuitenkin sitä, että viivesietoisen verkon solmulla on tarkoitukseen sopiva ohjelmisto sekä oma, verrattain suurikin tietovarasto riippuen käyttötarkoituksesta. Vaatimus tietovarastosta laitteistotasolla toteutuu diplomityön aikana, mutta tulevat ohjelmistoratkaisut määrittävät lopulta sen, perustuuko järjestelmä täysin viivesietoiseen verkkoon. Viivesietoisessa verkossa myös lähettäjällä ja vastaanottajalla pitää olla tarkoitukseen sopiva ohjelmisto, sillä viivesietoinen verkko on sovellustason kateverkko (overlay network), jossa siirretään viestinippuja (bundle) tarkoitukseen sopivalla protokollalla (Syrjänen 2007: 6). Viivesietoinen verkko toimii siten olemassa olevien protokollapinojen yläpuolella. Esimerkiksi internet-liikenteeseen se rakennettaisiin TCP/IP-protokollaperheen päälle. (Fall 2003: 30.)

4.2.1 Arkkitehtuuri yleisellä tasolla

Uusi järjestelmä toimii siis eräänlaisena liikuteltavana välityspalvelimena, joka ottaa vastaan työkoneelta lähetetyn datan ja lähettää sen edelleen eteenpäin oikealle palvelimelle. Tiedonsiirto näiden kolmen osan välillä hoidetaan langattomia lähiverkkoja käyttämällä, jolloin toimenpiteet saadaan automatisoitua mahdollisimman pitkälle ennen varsinaisia ohjelmistoratkaisuja.

Järjestelmästä olisi tarkoitus tehdä sellainen, että se kykenee toimimaan myös sellaisenaan ilman välityspalvelintakin, jolloin välityspalvelinta ei ole pakko käyttää, jos internet-yhteys on muuten aina helposti saatavilla. Näin järjestelmä kykenee toimimaan myös entiseen tapaan, eikä välityspalvelin sulje mitään toimintoja ulkopuolelle. Tässä mielessä järjestelmä muodostaa kokonaisuutena eräänlaisen dynaamisen reitityksen tietoliikenteelle, sillä järjestelmän tulee mukautua kumpaankin tilanteeseen automaattisesti. Käytännössä tämä tarkoittaa sitä, että kaivostyökoneet lähettävät dataa joko välityspalvelimelle tai oikealle palvelimelle ja valinta näiden kahden välillä tehdään itsenäisesti ilman ulkopuolista toimijaa.

Kuvasta 8 nähdään uuden tiedonsiirtojärjestelmän arkkitehtuurikuvaus yleisellä tasolla. Kuvassa näkyy myös suunniteltuja laitteisto- ja ohjelmistoratkaisuja, mutta tässä vaiheessa kuvasta kannattaa huomioida erityisesti kolme laatikkoa: Work machine, Data mule ja Server. Nämä kolme osaa ovat uuden järjestelmän pääosat. Nykyisen järjestelmän muodostavat Work machine eli kaivostyökone ja Server eli tässä tapauksessa ReDi ja sen REST-palvelin. Tähän on nyt siis tarkoitus lisätä kolmas osa eli välityspalvelin, joka on kuvassa markkinointisyistä nimellä Data mule. Kuvan kaaviota kannattaa verrata erityisesti kuvan 4 samantyyliseen kaavioon, jossa näytetään nykyisen järjestelmän arkkitehtuurikuvaus. Jos kuvan 8 järjestelmästä pudotetaan välityspalvelin pois, niin järjestelmä toimii kuten kuvassa 4. Itse asiassa järjestelmä toimii ensisijaisesti aina kuten kuvassa 4, sillä järjestelmän on tarkoitus toimia siten, että kun välityspalvelin on työkoneiden lähellä, niin järjestelmästä tulee kuvan 8 kaltainen, mutta muussa tapauksessa tiedonsiirtojärjestelmä toimii kuten kuvassa 4.



Kuva 8. Uuden tiedonsiirtojärjestelmän tietoliikenne Norsmart-ohjausjärjestelmässä (Exertus 2013: 7).

4.3 Verkkoarkkitehtuuri

Uusi järjestelmä koostuu siis kolmesta osakokonaisuudesta, joita ovat työkone, REST-palvelin ja välityspalvelin. Suunnitellaan seuraavaksi näiden kolmen osakokonaisuuden verkkoarkkitehtuurit. Verkkoarkkitehtuurin näkökulmasta on hyvä tarkastella kaikkia kolmea osaa aluksi erikseen ja lopuksi yhdistää ne yhdeksi kokonaisuudeksi. Sanottakoon vielä, että REST-palvelimen verkkoarkkitehtuuri on tietenkin jo olemassa, mutta käydään se silti läpi ylemmällä tasolla, sillä se helpottaa kokonaiskuvan muodostamista.

4.3.1 Työkone

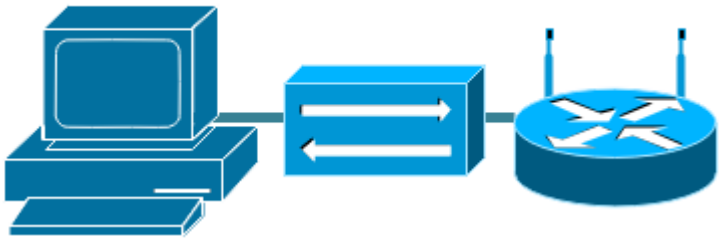
Työkone on järjestelmän yksinkertaisin kokonaisuus verkkoarkkitehtuurin näkökulmasta, sillä laitteiston puolesta se koostuu sulautetulla Linux-käyttöjärjestelmällä varuste-

tusta ohjausyksiköstä ja langattomasta reitittimestä. Ohjausyksikkö on aina jokin Exertuksen ohjausyksiköistä. Ohjausyksikköön kiinnitetään langaton reititin Ethernetkaapelilla. Täten tällä osakokonaisuudella on oma langallinen lähiverkko eli LAN. Langallisen lähiverkon puolella reitittimen DHCP-palvelin antaa ohjausyksiköllе IP-osoitteen, joka on samassa aliverkossa reitittimen langallisen verkkosovittimen eli Ethernet-sovittimen kanssa. DHCP-palvelimen antaman IP-osoitteen sijaan voitaisiin käyttää myös kiinteää IP-osoitetta ohjausyksikössä, jolloin se olisi aina sama. Ongelmaksi muodostuu kuitenkin se, että jos ohjausyksikkö vaihdetaan toiseen, sille pitäisi asettaa IP-osoite, aliverkon maski ja yhdyskäytävä aina käsin. Tästä ei toki olisi suurta vaivaa, mutta koska se ei tuo etua, niin on parempi jättää asia DHCP-palvelimen hoidettavaksi.

Langaton reititin toimii asiakastilassa, eli se on niin sanottu langaton asiakas (wireless client). Tämä tarkoittaa sitä, että langaton reititin pystyy yhdistymään tukiasemaan (access point) niin kuin mikä tahansa langattomalla verkkosovittimella varustettu laite, kuten esimerkiksi tietokone tai älypuhelin. Tässä tapauksessa se vain sattuu olemaan langattomaksi asiakkaaksi asennettu reititin, sillä ohjausyksikössä ei ole langatonta verkkosovitinta. Koska langaton reititin yhdistyy tukiasemaan, reitittimen langaton verkkosovitin saa IP-osoitteen ja muut tarvittavat IP-parametrit tukiaseman DHCP-palvelimelta. Täten sen IP-osoite voi vaihdella paljonkin riippuen siitä, monenko eri tukiaseman alueella työkone liikkuu. Tällä ei sinänsä ole merkitystä, sillä langaton asiakas saa aina internet-yhteyttä varten tarvittavat asetukset automaattisesti tukiasemalta.

Reitittimen langattoman verkkosovittimen ja Ethernet-sovittimen välinen liikenne toteutetaan käyttämällä osoitteenmuunnosta. Tässä tapauksessa käytetään täysimääräistä osoitteenmuunnosta, sillä osoite pitää saada muunnettua molempiin suuntiin. Täysimääräistä osoitteenmuunnosta käytettäessä tarvitaan lähdeosoitteenmuunnos ja kohdeosoitteenmuunnos. Täysimääräisen osoitteenmuunnoksen avulla oman yksityisen lähiverkon laitteen IP-osoite muunnetaan joksikin julkiseksi IP-osoitteeksi. Tässä tapauksessa osoitteenmuunnos toimii siten, että reititin muuntaa lähdeosoitteenmuunnoksen avulla langallisen lähiverkon puolella olevan ohjausyksikön IP-osoitteen näyttäytymään langattomalle lähiverkolle sillä osoitteella, jonka reitittimen langaton verkkosovitin saa tu-

kiaseman DHCP-palvelimelta. Tästä syystä lähdeosoitteenmuunnos on itse asiassa masquerade, koska langattoman verkkosovittimen IP-osoite voi vaihdella. Ohjausyksikön IP-osoite ei nyt siis näy langattoman lähiverkon puolella. Langallisen lähiverkon näkökulmasta langaton lähiverkko on julkinen verkko, vaikka oikeasti julkinen verkko eli internet onkin vasta tehtaan tukiaseman oman osoitteenmuunnoksen takana. Kohdeosoitteenmuunnoksen avulla reititin muuntaa langattoman verkkosovittimen IP-osoitteen takaisin ohjausyksikön IP-osoitteeksi. Tämä pitää kuitenkin järjestellä siten, että langattoman verkon puolelta ei voida ottaa yhteyttä mihinkään tiettyyn kohdeosoitteeseen langallisen lähiverkon puolella. Edellä suunniteltu työkoneen verkkoarkkitehtuuri nähdään kuvasta 9. Siinä työkoneen ohjausyksikkö on kiinnitetty langattomaan reitittimeen, joka toimii asiakastilassa. Osoitteenmuunnos on sijoitettu näiden kahden välille kuvaamaan sitä, että langallisen lähiverkon puolella on työkoneen oma verkko ja langattoman lähiverkon puolella on työkoneen näkökulmasta julkinen verkko.

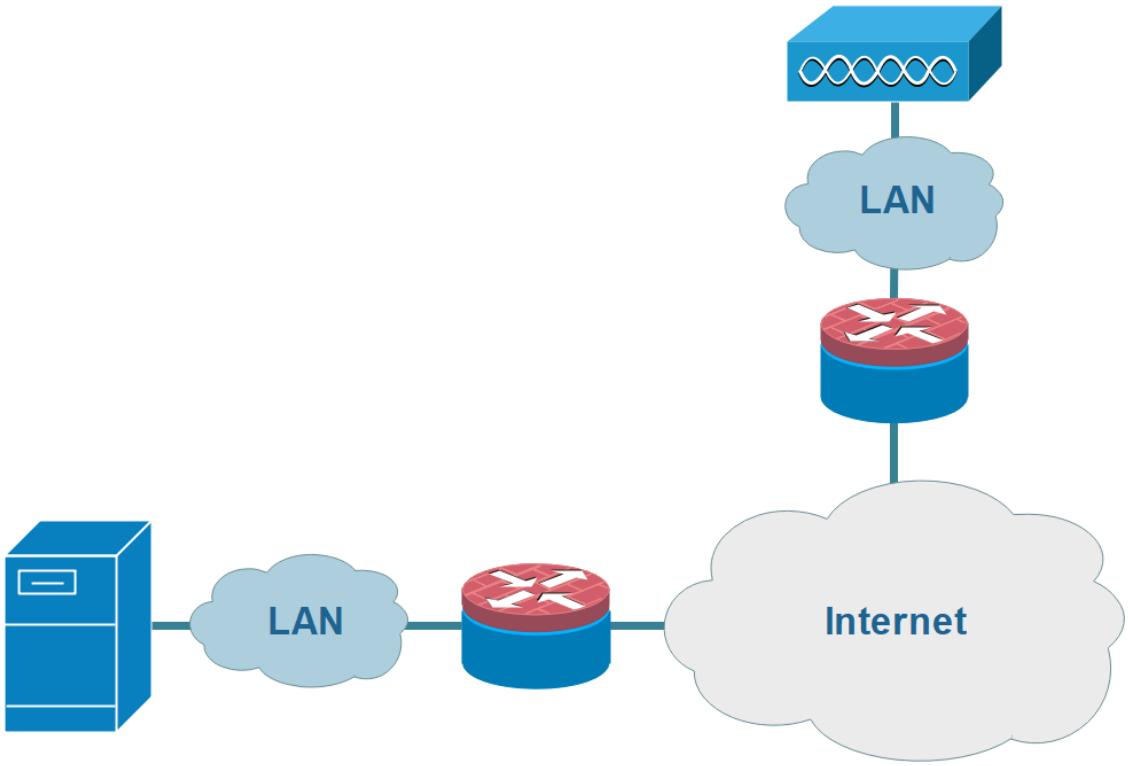


Kuva 9. Työkoneen verkkoarkkitehtuuri.

4.3.2 ReDi

Käsitteellä ReDi tarkoitetaan diplomityössä Exertuksen palvelua kokonaisuudessaan. Verkkoarkkitehtuurin näkökulmasta ReDi on REST-palvelin, joka sijaitsee internetissä. Laajennetaan ReDi koskemaan nyt myös tehtaan langattoman verkon tarjoavaa tukiasemaa, johon työkoneet yhdistyvät. Edellä mainittu tilanne on kuvattu kuvassa 10. Siinä REST-palvelin ja tukiasema ovat yhdistettyinä internetiin, jolloin tukiasemalta on yhteys REST-palvelimelle. Nämä voitaisiin pilkkoa pienemmiksikin osakokonaisuuksiksi, mutta kun tarkastellaan tulevaa järjestelmää kokonaisvaltaisesti, niin työkoneen ja

välityspalvelimen kannalta on samantekevää missä palvelin sijaitsee ja miten palvelin on kytketty internetiin, kunhan sinne pääsee tukiaseman kautta.



Kuva 10. Laajennettu ReDi-palvelun verkkoarkkitehtuuri.

ReDi-palvelun REST-palvelin sijaitsee siis internetissä ja sillä on julkinen IP-osoite. Tämä osoite on palvelimella kiinteä. Palvelimella on myös oma verkkotunnus, mutta sitä ei tarvita uuden tiedonsiirtojärjestelmän suunnittelussa tai toteutuksessa, sillä tulevassa järjestelmässä ei ole sellaisia komponentteja, jotka erityisesti vaatisivat verkkotunnuksen käyttöä tällä hetkellä. Laitteiston kanssa voidaan aivan hyvin käyttää pelkkiä IP-osoitteita, sillä verkkotunnukset on tarkoitettu ensisijaisesti ihmisille, jotta osoitteiden muistaminen olisi helpompaa.

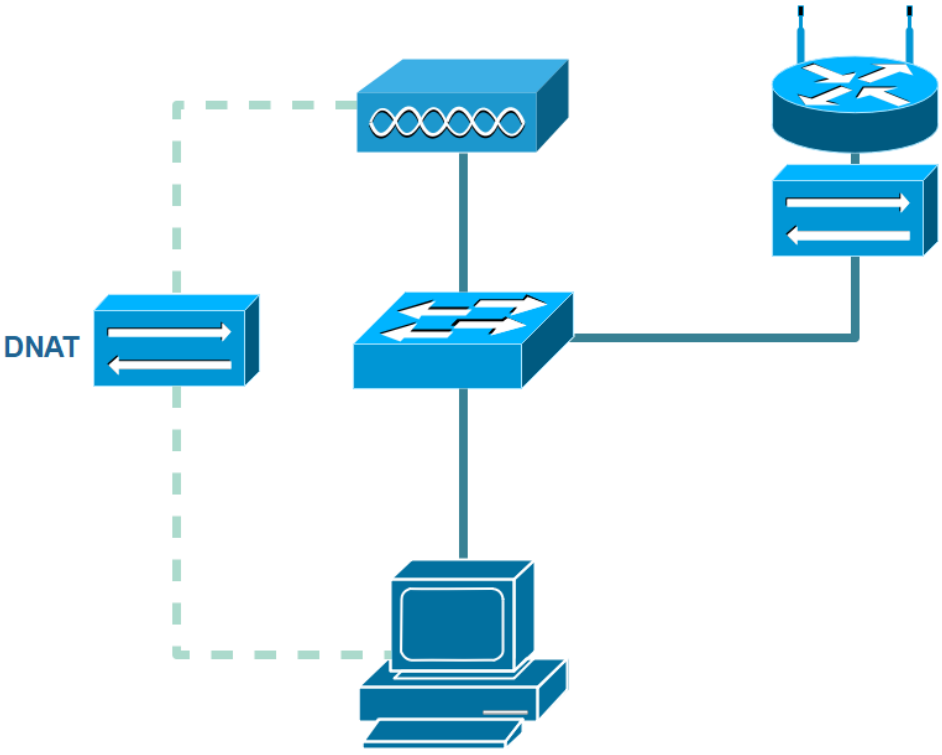
Kuvassa 10 näkyvä tukiasema ei ole mikään tietty tukiasema, vaan se kuvaa yleisesti tukiasemaa, johon työkoneet ja myöhemmin myös välityspalvelin voivat yhdistyä. Se voi olla siis mikä tahansa tukiasema missä tahansa, kunhan se on yhteydessä internetiin ja kaivostyökoneet voivat käyttää sitä. Tämän tukiaseman DHCP-palvelimen pitää

myös olla toiminnassa, jotta se voi jakaa IP-parametrit siihen liittyville asiakkaille. Muuten järjestelmä ei toimi.

4.3.3 Välityspalvelin

Välityspalvelimen verkkoarkkitehtuuri on näistä kolmesta osakokonaisuudesta suurin. Tietenkin ReDi on siinä mielessä suurin, että se on kiinni internetissä, mutta internet onkin siinä vain välikappaleena, joten siinä mielessä välityspalvelimen verkko on monimutkaisempi.

Välityspalvelin on ikään kuin työkone ja ReDi yhdistettynä, sillä välityspalvelimen täytyy sisältää elementtejä molemmista osista, jotta järjestelmä toimii kokonaisuutena. Tästä syystä välityspalvelimella on kaksi langatonta reititintä, joista toinen on välityspalvelimen oma tukiasema ja toinen oma langaton asiakas. Kuvassa 11 tukiasemareititin on kuvattu samalla tavalla kuin kuvassa 10 ja asiakasreititin on kuvattu samalla tavalla kuin kuvassa 9.



Kuva 11. Välityspalvelimen verkkoarkkitehtuuri.

Tukiasemaa tarvitaan siksi, että työkoneet voivat tarvittaessa yhdistyä siihen langattomasti ja lähettää dataa aivan kuten ne tekisivät yhdistyessään tehtaan tukiasemaan. Langatonta asiakasta puolestaan tarvitaan siihen, että välityspalvelin voi itse yhdistyä tehtaan tukiasemaan ja lähettää työkoneilta vastaanotetun datan oikealle palvelimelle. Järjestelmään tarvitaan myös tietokone, joka varastoi työkoneilta vastaanotetun datan sekä hoitaa myöhemmin palvelimen toimintoja ja mahdollisesti myös muita ohjelmistoteknisiä toimintoja. Tässä voidaan käyttää samanlaista ohjausyksikköä, jota työkonekin käyttää, sillä siinä on tarkoitukseen hyvin sopiva Linux-käyttöjärjestelmä. Edellä mainittujen laitteiden lisäksi tarvitaan vielä verkkokytkin, joka yhdistää edellä mainitut kolme laitetta. Kuvasta 11 nähdään kuinka verkkokytkin yhdistää välityspalvelimen ohjausyksikön, tukiaseman ja asiakastilassa olevan langattoman reitittimen.

Vaikka verkkoarkkitehtuurin näkökulmasta laitteisto onkin jo selvillä, niin tarvitaan silti vielä eräitä tekniikoita, jotta järjestelmä toimii oikein. Kysymys on erityisesti siitä, miten työkone pystyy lähettämään datansa välityspalvelimelle siten, että työkone luulee välityspalvelimen olevan oikea palvelin. Tämä voidaan ratkaista siten, että välityspalvelimen tukiasemassa käytetään kohdeosoitteenmuunnosta. Voidaan puhua eräänlaisesta mies välissä -hyökkäyksestä (man-in-the-middle attack), jossa kahden pisteen välissä on vihamielinen hyökkääjä, joka kaappaa osapuolten liikenteen. Tässä tapauksessa välissä ei ole vihamielinen hyökkääjä, vaan mies välissä -hyökkäyksen periaatetta käyttävä itsenäinen välityspalvelin, jonka kautta data kulkee.

Kohdeosoitteenmuunnos toimii siten, että sille määritetään IP-osoite, joka näkyy ulkoverkolle ja IP-osoite, joka ohjaa tähän ulkoverkolle näkyvään IP-osoitteeseen tulevat paketit oikeaan paikkaan sisäverkossa. Tämän avulla välityspalvelimen ohjausyksikkö saadaan näyttäytymään REST-palvelimen IP-osoitteella välityspalvelimen tukiaseman puoleiselle langattomalle lähiverkolle. Tämän johdosta ohjausyksiköllä täytyy olla aina sama IP-osoite. Siksi sille kannattaa määrittää kiinteä IP-osoite, sillä jos ohjausyksikön IP-osoite muuttuu, kohdeosoitteenmuunnos ei enää ohjaa liikennettä tähän muuttuneeseen osoitteeseen. Kohdeosoitteenmuunnos on merkitty kuvaan 11 tukiaseman ja ohjausyksikön välille.

Lisäksi kun käytetään TCP-yhteyttä, niin kohdeosoitteenmuunnosta käytettäessä pitää perille saapuneen paketin tietää reitti takaisin lähettäjälle, sillä kohdeosoitteenmuunnos ei sitä kerro. Tässä tapauksessa ohjausyksikön täytyy kertoa paluupaketille reitti takaisin, eli kertoa mistä pääsee siihen langattomaan lähiverkkoon, jossa paketti oli ennen kohdeosoitteenmuunnosta. Toisin sanoen ohjausyksikkö reitittää paketin tukiasemareitittimen Ethernet-sovittimelle, josta se pääsee langattoman lähiverkon puolelle, jonka jälkeen paketti tietääkin jo reitin takaisin lähettäjälle. Välityspalvelimen langattomana asiakkaana toimiva reititin puolestaan tarvitsee täysimääräisen osoitteenmuunnoksen samaan tapaan kuin työkoneenkin langaton reititin.

Koska välityspalvelimen ohjausyksiköllä on kiinteä IP-osoite, niin välityspalvelimen lähiverkossa ei ole ollenkaan tarvetta DHCP-palvelulle, sillä myös molemmilla reitittimillä on kiinteät IP-osoitteet. Ainoastaan tukiaseman täytyy jakaa IP-osoitteita siihen liittyville työkoneiden reitittimille, joten tukiaseman langattoman verkon puolella täytyy olla DHCP-palvelu toiminnassa.

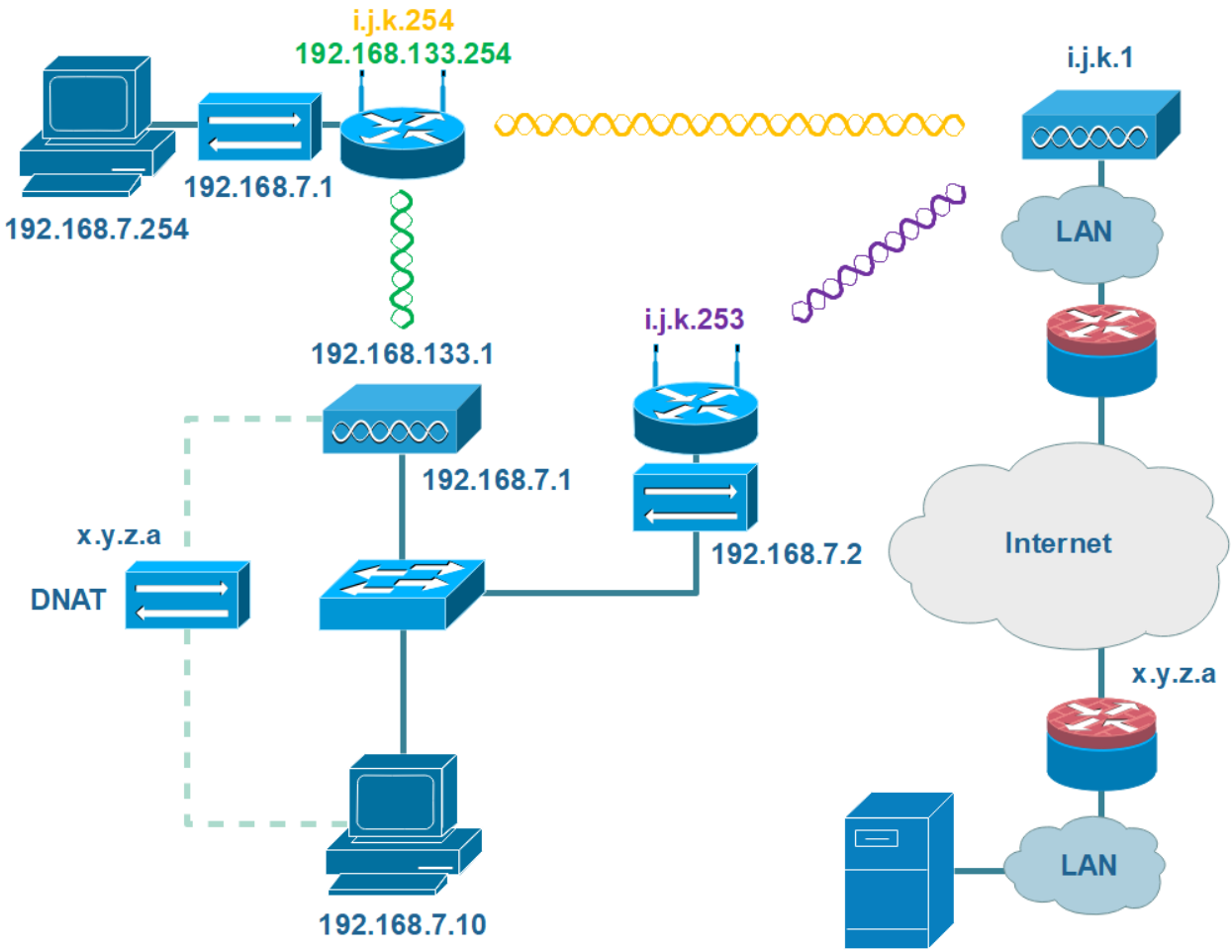
4.3.4 Kokonaisuus

Edellä esiteltiin kolme osakokonaisuutta, joista uusi tiedonsiirtojärjestelmä koostuu. Nyt yhdistetään nämä osat yhdeksi kokonaiseksi järjestelmäksi, joka voi toimia sekä välityspalvelimen kanssa että ilman sitä. Tässä vaiheessa mukaan tulevat myös laitteiden IP-osoitteet. Esitetyt IP-osoitteet ovat ainoastaan esimerkkejä, eikä niitä tulla käyttämään järjestelmän tuotantoversiossa.

Järjestelmän lähiverkoissa tullaan käyttämään aliverkon maskia 255.255.255.0, jolloin käytössä ovat aina osoitteet 1–254 ja levitysviestiosoitetta varten on osoite 255. Vaikka lähiverkoissa ei tule olemaan näin monta laitetta, on kyseinen verkon koko silti hyvä ratkaisu. Ensinnäkin se yksinkertaistaa osoitteiden käsittelyä, kun esimerkiksi ylläpitovaiheessa tietyn lähiverkon kokoa ei tarvitse erikseen selvittää, vaan tiedetään, että verkon koko on kaikkialla sama. Lisäksi tämän kokoinen verkko tekee uusien laitteiden lisäämisestä helppoa. Jos verkkoon pitäisi myöhemmin lisätä laitteita ja verkko olisikin liian pieni, niin verkon kokoa täytyisi kasvattaa. Nyt kun verkon koko on tarpeeksi suu-

ri, niin laitteita voidaan huoletta lisätä montakin, jos sille on tarvetta. Liian suuresta verkosta ei muutenkaan ole mitään haittaa, sillä kyseessä on yksityinen lähiverkko.

Kuvasta 12 nähdään uuden järjestelmän verkkoarkkitehtuuri kokonaisuutena, johon on yhdistetty edellä mainitut osakokonaisuudet IP-osoitteineen. Myös osakokonaisuuksien väliset langattomat yhteydet näkyvät kuvassa.



Kuva 12. Uuden järjestelmän verkkoarkkitehtuuri kokonaisuudessaan.

Kuvassa näkyvistä langattomista yhteyksistä täytyy huomata se, että työkone voi olla yhdellä kertaa yhdistyneenä vain yhteen tukiasemaan, eli käytössä on joko oranssi yhteys tai vihreä yhteys. Tämän johdosta kannattaa huomata myös se, että järjestelmän on tarkoitus toimia kahdessa tapauksessa eli välityspalvelimen kanssa ja ilman sitä. Tarkastellaan näitä kahta tilannetta tarkemmin. Aloitetaan yksinkertaisemmasta tilanteesta eli

tilanteesta ilman välityspalvelinta. Tätä tilannetta voidaan havainnollistaa kuvassa 12 siten, että jätetään välityspalvelin huomiotta, jolloin työkone käyttää oranssia yhteyttä. Työkoneen ohjausyksikössä toimiva ohjausjärjestelmä on nyt tallentanut dataa työkoneen liikkeistä ja nämä tiedot pitäisi saada lähetettyä ReDi-palvelun REST-palvelimelle. Ohjausyksiköllä on oma IP-osoite, jonka se on saanut työkoneen langattomalla reitittimellä sijaitsevalta DHCP-palvelimelta. Työkoneen langallinen lähiverkko on 192.168.7.0/24. Tällöin aliverkon maski on 255.255.255.0, jolloin jaossa oleva osoiteavaruus on 192.168.7.1–192.168.7.254 osoitteen 192.168.7.255 ollessa levitysviestiosoite. Reitittimen Ethernet-sovittimella on kiinteä IP-osoite 192.168.7.1. DHCP-palvelimet voivat antaa IP-osoitteita joko osoiteavaruuden alku- tai loppupäästä. Sovitaan, että tämän diplomityön aikana DHCP-palvelin antaa osoitteita aina osoiteavaruuden loppupäästä. Koska levitysviestiosoite on tässä tapauksessa 192.168.7.255, niin ensimmäinen vapaa osoite, jonka DHCP-palvelin antaa työkoneen ohjausyksikölle, on 192.168.7.254.

Työkoneen reitittimen langaton verkkosovitin saa langattoman lähiverkon osoitteensa nyt tässä tapauksessa tehdasverkon tukiaseman DHCP-palvelimelta. Sen osoiteavaruus ei ole tässä tapauksessa tiedossa ja se voi vaihdella eri tukiasemilla, joten käytetään tässä verkkoa i.j.k.0/24. Koska määrittelimme tämän verkon aliverkon maskiksi 255.255.255.0, niin voimme olettaa, että tukiaseman langattoman verkkosovittimen IP-osoite on silloin i.j.k.1. Työkoneen reitittimen langaton verkkosovitin saa tukiaseman DHCP-palvelimelta osoitteen i.j.k.254. Näin tukiasema ja työkoneen reitittimen langaton verkkosovitin ovat samassa langattomassa lähiverkossa.

Tehtaan tukiasema on yhdistetty internetiin. Miten tehdasverkko on tukiaseman jälkeen suunniteltu, ei ole tämän diplomityön kannalta merkityksellistä. Tässä tapauksessa riittää ainoastaan tieto siitä, että tukiasemalta on yhteys internetiin. Tilanne on kuvattu palomuurilla ja reitittimellä kuvissa 10 ja 12. Todellisuudessa tehtaan sisäinen verkko saattaa olla hyvinkin paljon monimutkaisempi kuin kuvissa, mutta sillä ei ole nyt merkitystä. Palomuurit saattavat toki rajoittaa liikennettä esimerkiksi sulkemalla portteja, mutta tällaiset tilanteet ovat erikoistapauksia ja ne voidaan ratkaista asiakkaan kanssa erikseen.

Tehdasverkon tukiasemalta on siis yhteys internetiin ja sitä kautta ReDi-palvelun REST-palvelimelle. REST-palvelimen julkinen IP-osoite on x.y.z.a. Jos tarkastellaan palvelimen sijaintia sen lähiverkossa, niin tilanne on sama kuin tehdasverkon tapauksessa, eli se ei ole tiedossa eikä sillä ole järjestelmän toiminnan kannalta edes merkitystä. Tässä tapauksessa riittää tieto REST-palvelimen julkisesta IP-osoitteesta. Nyt koko ketju työkoneen ohjausyksiköltä REST-palvelimelle on tiedossa. Nyt kun TCP-paketti lähtee työkoneen ohjausyksiköltä osoitteesta 192.168.7.254, se etenee reitittimen Ethernet-sovittimelle osoitteeseen 192.168.7.1. Tässä kohdassa osoite muunnetaan käyttäen lähdeosoitteenmuunnosta. Tässä vaiheessa poistutaan työkoneen lähiverkosta 192.168.7.0/24 ja siirrytään tehdasverkon langattomaan lähiverkkoon i.j.k.0/24, jolloin paketti etenee verkon yhdyskäytävään tukiasemalle osoitteeseen i.j.k.1. Tästä paketti siirtyy tehtaan langalliseen lähiverkkoon ja sieltä internetiin. Internetin kautta paketti päätyy lopulta REST-palvelimelle osoitteeseen x.y.z.a. Paluupaketti menee perille samaa reittiä kuin tullessakin. Lähdeosoite näyttää kuitenkin nyt osoitteenmuunnoksen johdosta osoitetta i.j.k.254, mutta reititin osaa kääntää paketin kohdeosoitteenmuunnoksen avulla takaisin. Tästä paketti palaa takaisin ohjausyksikölle osoitteeseen 192.168.7.254.

Nyt kun tiedetään, miten järjestelmä toimii ilman välityspalvelinta, voidaan toimintaa tarkastella välityspalvelimen kanssa. Tämä tilanne nähdään kuvasta 12 siten, että käytetään vihreää- ja violettia yhteyttä. Lähtötilanne on työkoneen päässä sama lähiverkon osalta, eli ohjausyksikkö saa osoitteen 192.168.7.254 DHCP-palvelimelta ja työkoneen reitittimen Ethernet-sovittimen IP-osoite on 192.168.7.1 verkon ollessa 192.168.7.0/24.

Tässä vaiheessa tilanne muuttuu aiempaan, sillä nyt työkoneen reitittimen langaton verkkosovitin saa osoitteensa välityspalvelimen tukiasemalta. Käytämme välityspalvelimen tukiaseman langattomassa lähiverkossa verkkoa 192.168.133.0/24. Tällöin aliverkon maski on 255.255.255.0 ja osoiteavaruus on siten 192.168.133.1–192.168.133.254, jolloin levitysviestiosoite on 192.168.133.255. Tukiaseman langattoman verkkosovittimen IP-osoite on 192.168.133.1. Tukiaseman DHCP-palvelin antaa työkoneen reitittimen langattomalle verkkosovittimelle osoitteen 192.168.133.254. Käytetään välityspalvelimen sisällä verkkoa 192.168.7.0/24, vaikka samannimistä verkkoa käytetään myös

työkoneen sisällä. Periaatteessa voitaisiin käyttää jotain muutakin verkkoa, mutta korostetaan tällä sitä, että vaikka verkoilla on sama osoite, niin ne ovat kuitenkin täysin eri verkkoja, koska verkot on eristetty toisistaan. Muutenkin työkoneita on oikeasti monta ja niillä kaikilla on käytössään samanniminen verkko. Koska kaikkialla on käytössä samanniminen verkko, niin ylläpito helpottuu jonkin verran.

Koska suunnitelman mukaan välityspalvelimen ohjausyksiköllä on kiinteä IP-osoite, niin välityspalvelimen langallisessa lähiverkossa ei ole tarvetta DHCP-palvelulle, sillä myös reitittimien Ethernet-sovittimilla on kiinteät IP-osoitteet. Koska verkko on 192.168.7.0/24, niin laitteilla on käytössä jälleen 254 osoitetta. Osoitteet voitaisiin jakaa mielivaltaisesti laitteiden kesken, mutta selkeyden vuoksi määritetään tukiasemareitittimen Ethernet-sovittimelle osoite 192.168.7.1 ja asiakasreitittimen Ethernet-sovittimelle osoite 192.168.7.2. Osoite 192.168.7.2 eli asiakasreitittimen Ethernet-sovitin pitää määrittää välityspalvelimen ohjausyksikön yhdyskäytäväksi, sillä ainoastaan asiakasreitittimen kautta on pääsy internetiin. Lisäksi määritetään ohjausyksikölle osoite 192.168.7.10. Ainoa sovitin, joka saa osoitteen DHCP-palvelimelta, on langattomana asiakkaana toimivan reitittimen langaton verkkosovitin. Se yhdistyy tehtaan tukiasemaan ja saa sieltä osoitteensa.

Nyt jos TCP-paketti on lähdössä työkoneelta ja yhteyttä internetiin ei ole, mutta välityspalvelin on kantaman sisällä, niin työkoneen langattomana asiakkaana toimiva reititin yhdistyy välityspalvelimen tukiasemaan ja saa sieltä osoitteen 192.168.133.254. Paketti kulkee nyt työkoneen ohjausyksiköltä osoitteesta 192.168.7.254 työkoneen langattoman reitittimen Ethernet-sovittimelle osoitteeseen 192.168.7.1. Reitittimessä tehdään lähdeosoitteenmuunnos ja paketti lähtee välityspalvelimen tukiaseman langattomalle verkkosovittimelle osoitteeseen 192.168.133.1. Kun paketti saapuu välityspalvelimen tukiaseman langattomaan verkkosovittimeen, niin tukiasemana toimivalle reitittimelle määritelty kohdeosoitteenmuunnos (DNAT kuvissa 11 ja 12) muuntaa välityspalvelimen ohjausyksikön osoitteen näyttäytymään REST-palvelimen osoitteena. Tämä tarkoittaa sitä, että osoite 192.168.7.10 muunnetaan osoitteeksi x.y.z.a.

Kohdeosoitteenmuunnoksen käytössä on kuitenkin se ongelma, että se ei kerro paluupaketille reittiä takaisin, joten yhteys ei vielä toimi. Paketin pitäisi löytää verkko 192.168.133.0/24, jossa se oli viimeksi. Ainoa osoite, jonka takaa tämä verkko löytyy, on tukiasemana toimivan reitittimen Ethernet-sovittimen osoite 192.168.7.1. Koska määrittelimme välityspalvelimen langallisen lähiverkon yhdyskäytäväksi langattomana asiakkaana toimivan reitittimen Ethernet-sovittimen eli osoitteen 192.168.7.2, niin paketti yrittäisi normaalisti sitä kautta löytää reittiä takaisin, mikä ei tietenkään ikinä onnistu. Jos langallisen lähiverkon yhdyskäytäväksi olisikin määritetty tukiaseman Ethernet-sovittimen osoite 192.168.7.1, niin paketti löytäisi verkon 192.168.133.0/24 sen takaa, mutta silloin välityspalvelimen internet-yhteys ei toimisi, koska osoite 192.168.7.2 ei ole yhdyskäytävänä. Tässä tilanteessa paketille pitää siis kertoa minkä osoitteen kautta tähän verkkoon pääsee. Lisätään siis verkko 192.168.133.0/24 ohjausyksikön reititystauluun ja osoite 192.168.7.1 yhdyskäytäväksi tähän verkkoon. Nyt paketti pääsee verkkoon 192.168.133.0/24. Tästä verkosta löytyy osoite 192.168.133.254, jossa tehdään kohdeosoitteenmuunnos ja paketti pääsee takaisin työkoneen ohjausyksikölle osoitteeseen 192.168.7.254.

Nyt työkone on saanut paketin lähetettyä onnistuneesti ”REST-palvelimelle” eli oikeasti välityspalvelimen ohjausyksikölle ja voidaan ajatella, että paketti on tallennettu ohjausyksikölle. Tässä vaiheessa ohjausyksikön tuleva ohjelmisto suorittaisi toimenpiteitä, joiden jälkeen paketti voitaisiin lähettää oikealle palvelimelle sitten, kun välityspalvelimella on internet-yhteys käytettävissä. Koska yhdyskäytäväksi on määritetty asiakasreitittimen Ethernet-sovittimen osoite 192.168.7.2, niin paketti yrittää tämän kautta löytää reittiä REST-palvelimelle. Tämä onnistuu tietenkin vain silloin, kun reitittimen langaton verkkosovitin on yhteydessä tehtaan tukiasemaan. Tällöin paketti lähtee ohjausyksiköltä osoitteesta 192.168.7.10 ja etenee osoitteeseen 192.168.7.2. Sieltä paketti etenee edelleen reitittimen lähdeosoitteenmuunnoksen jälkeen tehtaan langattomaan lähiverkkoon i.j.k.0/24, sillä välityspalvelimen asiakasreitittimen langaton verkkosovitin on saanut tehtaan tukiaseman DHCP-palvelimelta osoitteen i.j.k.253. Nyt paketti pääsee tehtaan tukiaseman langattomalle verkkosovittimelle osoitteeseen i.j.k.1 ja sieltä edelleen tehtaan langalliseen lähiverkkoon. Tästä eteenpäin tilanne on sama, kuin tilanteessa ilman välityspalvelinta, jolloin paketti kulkee internetin kautta REST-palvelimelle osoittee-

seen x.y.z.a. Paluupaketti kulkee samaa reittiä vastakkaisessa järjestyksessä takaisin välityspalvelimen ohjausyksikölle. Välityspalvelimen asiakasreitittimen kohdeosoitteenmuunnoksen avulla paluupaketti pääsee ohjausyksikölle.

4.4 Laitteistoarkkitehtuuri

Uuden järjestelmän laitteistoa tarkasteltaessa pitää ottaa huomioon vain työkoneen ja välityspalvelimen laitteisto, sillä ReDi-osuuden laitteistoon ei voida tässä tapauksessa vaikuttaa millään tavalla – eikä tarvitsekaan. Suunniteltavaksi jää siten työkoneen ja välityspalvelimen laitteisto. Uusi järjestelmä ReDi pois lukien koostuu Exertuksen ohjausyksiköistä, langattomista reitittimistä ja verkkokytkimestä. Aiemmin kuvatun suunnitelman mukaan välityspalvelimeen tarvitaan yksi ohjausyksikkö, kaksi langatonta reititintä ja nämä yhdistävä verkkokytkin. Tiedonsiirron näkökulmasta työkoneen laitteisto koostuu yhdestä ohjausyksiköstä ja yhdestä langattomasta reitittimestä. Koska välityspalvelimessa ja työkoneissa käytetään samoja reitittimiä, niin ei ole tarpeen käydä niitä erikseen läpi.

4.4.1 Reititin

Reititin on verkkokerroksen laite, joka hallitsee IP-tason protokollat. Se osaa reitittää IP-paketit kohdeverkkoon. (Kaario 2002: 31.)

Uudessa järjestelmässä käytettävä reititin on merkiltään Mikrotik ja malliltaan Metal. Metal-sarja on vahvistettu mallisarja, eli se on vedenpitävä ja kestää iskuja. Lisäksi se pystyy toimimaan suurella lämpötilavälillä. Ominaisuuksiltaan reititin on todella monipuolinen, sillä siitä löytyy todella paljon eri toimintoja. (Mikrotik 2017a.) Reitittimen asetuksien säätämiseen voidaan käyttää internet-selaimella toimivaa Webfig-ohjelmaa (Mikrotik 2012) tai Windows-käyttöjärjestelmällä toimivaa Winbox-ohjelmaa (Mikrotik 2018). Edellä mainitut säätötyökalut ovat graafisia. Myös Telnet-ohjelmaa voidaan käyttää, jolloin kaikki tehdään komentokehotteessa (Mikrotik 2007).

Mikrotik Metal-reitittimiä on saatavilla eri taajuusalueille standardin 802.11b/g/n mukaisesti. Vaihtoehtoja ovat Metal 2, Metal 5, Metal 52 ja Metal 9. Mallin numero viittaa langattoman verkon taajuuteen. Metal 2:n taajuus on 2,4 Ghz ja Metal 5:n taajuus on 5 GHz. Metal 52-mallissa molemmat taajuudet ovat valittavissa, jolloin voidaan käyttää joko 2,4 GHz:n taajuutta tai 5 GHz:n taajuutta. Metal 9 on erityinen 900 MHz:n malli. Mikrotik Metal-reitittimiin saa tarvittaessa hyvinkin suuren lähetystehon riippuen taajuudesta ja tiedonsiirtonopeudesta. Suurimmillaan voidaan käyttää jopa 32 dBm:n eli noin 1585 mW:n lähetystehoa. (Mikrotik 2017a.) Lähetystehoa määriteltäessä on huomioitava maakohtaiset lähetystehorajoitukset, eli mikä on suurin sallittu lähetysteho kyseessä olevalla taajuusalueella. Esimerkiksi Suomessa standardin 802.11b/g/n mukaisen datasiirtolaitteen suurin sallittu efektiivinen säteilyteho isotrooppisesta antennista on 100 mW taajuusalueella 2400–2483,5 MHz (Viestintävirasto 2018: 10). Käytännössä tämä tarkoittaa sitä, että jos antennin vahvistus on 0 desibeliä isotrooppiseen antenniin verrattuna, niin lähetysteho voidaan asettaa arvoon 100 mW. Jos taas antennin vahvistus on suurempi, täytyy lähetystehoa vastaavasti pienentää, jotta efektiivinen säteilyteho ei ylity. (Williams, Graham, Layer & Osenkowsky 2007: 1632.) Antennin vahvistus voidaan merkitä desibeleinä isotrooppiseen antenniin verrattuna tai puoliaaltodipoliantenniin verrattuna. Näitä merkitään yksiköillä dBi ja dBd. 0 dBd:n vahvistus vastaa 2,14 dBi:n vahvistusta. Antennia varten reitittimestä löytyy jykevä N-liitin. Diplomityössä käytetään antenneina 6 dBi:n ympärisäteileviä vertikaaliantenneja, jotka toimitettiin reitittimien mukana.

Mikrotik Metal-reititin käyttää PoE-tekniikkaa, jossa laitteen tarvitsema virta syötetään parikaapelin avulla eli samalla kaapelilla, missä data kulkee (Mikrotik 2017a). Tässä on se hyvä puoli, että reitittimelle kulkee vain yksi kaapeli, jossa kulkee sekä data että virta. Tämä mahdollistaa ennen kaikkea sen, että reititin voidaan sijoittaa mahdollisimman ylös samalle korkeudelle kuin mihin antenni sijoitettaisiin. Näin antenni voidaan kiinnittää suoraan reitittimeen, jolloin reitittimen ja antennin välistä siirtolinjaa eli tässä tapauksessa koaksiaalikaapelia ei tarvita ollenkaan. Näin reitittimeltä lähtevä radioteho saadaan hyödynnettyä mahdollisimman tehokkaasti suoraan antennissa ja tehohäviöt ovat mahdollisimman pienet. Parikaapelissa sen sijaan virta ja erityisesti data liikkuvat samanpituisella matkalla huomattavasti tehokkaammin. Parikaapelilla voi olla pituutta

enimmillään 100 metriä (Maniktala 2013: 39). Työkoneen tapauksessa tehohäviö koaksiaalikaapelissa ei olisi kuitenkaan kovin mittava, sillä puhutaan muutamista metreistä työkoneen sisältä ulkopuolelle, mutta sekin kuitenkin vaikuttaa jonkin verran näin suurilla taajuuksilla. Lisäksi erilaisten kaapeleiden vähentäminen helpottaa asennusta yleisesti.

4.4.2 Verkkokytkin

Verkkokytkin on siirtoyhteyskerroksen laite. Se välittää eri lähdeporteista eri kohdeportteihin kulkevaa liikennettä samanaikaisesti liityntöjensä välillä. (Kaario 2002: 30).

Verkkokytkimenä käytetään asennusvaiheessa ZyXEL-merkkistä GS-108B-mallin verkkokytkintä, jossa on kahdeksan porttia. Tätä ei tulla käyttämään tuotantoversiossa, vaan siinä tullaan käyttämään jotain vahvistettua verkkokytkintä, joka sopii paremmin kyseessä oleviin olosuhteisiin. Tässä vaiheessa ei ole väliä mitä verkkokytkintä käytetään, sillä verkkokytkimen toiminta pysyy samanlaisena, vaikka merkki tuleekin vaihtumaan.

4.4.3 Ohjausyksikkö

Välityspalvelimessa tullaan käyttämään MID070S-ohjausyksikköä. Se on Exertuksen kehittämä, sulautetulla Linux-käyttöjärjestelmällä varustettu ohjausyksikkö, jossa on myös oma näyttö ja navigointinäppäimistö. Diplomityön kannalta ohjausyksikön tärkeimmät ominaisuudet ovat juuri Linux-käyttöjärjestelmä ja Ethernet-liitäntä. Ohjausyksikön Linux sisältää ainoastaan komentorivikäyttöliittymän. Lisäksi Linuxissa käytetään Busybox-ohjelmaa, joka sisältää yleisimmät UNIX-työkalut pieneen kokoon pakattuna. Komentotulkkina on Almquist shell.

Työkoneessa käytetään diplomityön aikana MIC1100S-ohjausyksikköä. Normetin työkoneissa käytetään muitakin ohjausyksiköitä, mutta tässä vaiheessa ei ole väliä mitä ohjausyksikköä käytetään, sillä kaikista löytyy Linux-käyttöjärjestelmä ja Ethernet-

liitäntä, joita nyt tarvitaan. Tässä ohjausyksikössä ei siis ole omaa näyttöä, mutta siihen voi halutessaan kytkeä erillisen näytön.

Koska ohjausyksiköiden Linux on Debian-pohjainen, niin verkkoasetusten määrittämiseen voidaan käyttää tiedostoa /etc/network/interfaces. Tämän tiedoston avulla voidaan esimerkiksi määritellä käyttääkö Linux kiinteitä IP-parametrejä vai saako se ne DHCP-palvelimelta. (LaCroix 2015: 57–61.) Tiedoston manuaalisivulta löytyy perustietoa tiedoston käytöstä. Manuaalisivun saa näkyviin Linuxissa komennolla man 5 interfaces. Pakatusta tiedostosta /usr/share/doc/ifupdown/examples/network-interfaces.gz löytyy lisäksi esimerkkejä interfaces-tiedostosta.

4.5 Ohjelmistoarkkitehtuuri

Välityspalvelimen ohjelmistoarkkitehtuuri ei ole kovin suuressa osassa tässä diplomityössä, sillä pääpaino on juuri verkkoarkkitehtuurissa. Koska välityspalvelimen tekniikka suunnitellaan verkkolaitteisto edellä, niin ohjelmisto voidaan myöhemmin räätälöidä tarpeen mukaan.

5 ASENNUS

Uutta järjestelmää lähdetään rakentamaan siten, että se jaetaan pienempiin osakokonaisuuksiin sen mukaan mistä ja mihin dataa lähetetään yhdellä kertaa. Tällaisia tapauksia ovat yhteydet työkoneelta REST-palvelimelle, työkoneelta välityspalvelimelle ja välityspalvelimelta REST-palvelimelle.

Vaikka toteutuksessa keskitytään laitteisto- ja verkkoarkkitehtuurin rakentamiseen, niin järjestelmän tuotantoversio rakennetaan laitteiston osalta Normetin toimesta. Tässä käytävä toteutus on siten edelleen suunnitelma lopullista laitteistokokoonpanoa silmällä pitäen ja tähän eivät sisälly esimerkiksi akku ja latauskomponentit. Tarkoitus onkin rakentaa toimivaksi todettu verkkolaitteisto lopullista tuotetta varten.

Vaikka Mikrotik-reitittimien asennus olisi havainnollisempaa tehdä Winbox-ohjelmalla graafisesti, niin käytetään siitä huolimatta Telnet-ohjelmaa asetuksien asettamiseen, sillä sen käyttö on huomattavasti tehokkaampaa. Asetuskomennot voidaan liittää osaksi tekstiä, mikä vie vähemmän tilaa kuin kuvien käyttö. Komennot on muodostettu Discherin (2011: 66–98, 160–167, 209–219) ja Burgessin (2011: 80–105, 124–168, 202–212) kirjoissa esitettyjen teorioiden ja esimerkkien pohjalta. Huomautettakoon vielä, että reitittimille on tehty tehdasasetusten palautus ja kaikki vakiona tulevat asetukset on otettu pois käytöstä.

Asennuksen yhteydessä tarvitaan tehtaan langattoman verkon SSID ja WPA2-avain. Koska nämä eivät ole tiedossa ja muuttuvat toimijasta riippuen, sovitaan tässä, että asennuksen yhteydessä tehtaan langattoman verkon SSID on factory ja WPA2-avain IJK12kji. Myös välityspalvelimen tukiasema käyttää WPA2-todennusta. Olkoon sen avain XYZ98zyx ja SSID proxy. Edellä mainitut avaimet ja SSID:t ovat esimerkkejä, eikä niitä tulla käyttämään järjestelmän tuotantoversiossa. Sovitaan myös, että koko järjestelmässä käytetään kaikissa langattomissa reitittimissä 2,4 GHz:n taajuutta, joten Mikrotik-reitittimen täytyy olla malliltaan Metal 2 tai Metal 52.

Ohjausyksiköiden asentamisessa käytetään niiden Linux-käyttöjärjestelmiä. Ohjausyksiköiden asennus kattaa verkkoasetusten määrittämisen.

5.1 Työkone

Aloitetaan asentaminen työkoneen laitteistosta. Tähän sisältyvät ohjausyksikön ja langattoman reitittimen asennus. Työkoneen laitteistosta asennetaan ensimmäisenä ohjausyksikkö, jonka jälkeen reititin asennetaan langattomaksi asiakkaaksi.

5.1.1 Ohjausyksikkö

Suunnitelman mukaan työkoneen ohjausyksikkö saa IP-parametrit reitittimen DHCP-palvelimelta. Ohjausyksikön verkkoasetustiedostossa on tavallisesti DHCP-asetus vakiona päällä, mutta tarkistetaan, että asetukset ovat oikein. Koska kyseessä on Debian-pohjainen Linux, niin asetukset ovat tiedostossa /etc/network/interfaces ja tiedoston pitäisi olla seuraavanlainen:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

Aluksi siinä määritetään sisäinen verkkosovitin (lo) takaisinkaiutusosoitteeksi. Sen jälkeen määritetään Ethernet-sovitin (eth0) saamaan IP-parametrit DHCP-palvelimelta. Näin ohjausyksiköltä lähtevä liikenne reitittyy oikein ja yhteys toimii odotetusti, sillä IP-osoite, aliverkon maski ja yhdyskäytävä tulevat ohjausyksiköllе reitittimen DHCP-palvelimelta.

5.1.2 Reititin

Työkoneen ohjausyksiköltä tulee siis olla yhteys internetiin tai vaihtoehtoisesti välityspalvelimeen. Ideana onkin tehdä langattomana asiakkaana toimivaan reitittimeen kaksi profiilia, joista toinen on tarkoitettu tehtaan langattomaan lähiverkkoon ja toinen väli-

tyspalvelimen langattomaan lähiverkkoon. Tarvitaan siis tiedot tehtaan langattomasta lähiverkosta ja välityspalvelimen langattomasta lähiverkosta. Näiden avaimet ja SSID:t sovittiin aiemmin.

Aloitetaan reitittimen asennus langattomasta verkkosovittimesta. Siinä reitittimen langaton verkkosovitin asetetaan toimimaan asiakastilassa, jolloin se voi yhdistyä tukiasemaan. Taajuudeksi asetetaan aiemmin sovittu 2,4 GHz. Langaton verkkosovitin asennetaan seuraavalla komennolla:

```
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n \
    channel-width=20/40mhz-Ce \
    default-authentication=no disabled=no \
    frequency=auto mode=station ssid=""
```

Luodaan tämän jälkeen turvallisuusprofiilit langattomille lähiverkoille, joita tässä tapauksessa ovat välityspalvelimen tukiaseman tarjoama langaton lähiverkko ja tehtaan langaton lähiverkko. Molemmille verkoille tarvitaan omat turvallisuusprofiilit ja niille annetaan yksilölliset nimet, joita tarvitaan asennuksen myöhemmässä vaiheessa. Annetaan profiileille nimet proxySP ja factorySP. Turvallisuusprofiilissa määritetään todennusmenetelmä, joka on molemmille verkoille aiemmin sovittu WPA2. Lisäksi asetetaan aiemmin sovitut WPA2-avaimet. Luodaan profiilit seuraavalla komennolla:

```
/interface wireless security-profiles
add authentication-types=wpa2-psk eap-methods="" \
    group-ciphers=tkip,aes-ccm \
    management-protection=allowed mode=dynamic-keys \
    name=proxySP supplicant-identity="" \
    unicast-ciphers=tkip,aes-ccm wpa2-pre-shared-key=\
    XYZ98zyx
add authentication-types=wpa2-psk eap-methods="" \
    group-ciphers=tkip,aes-ccm \
    management-protection=allowed mode=dynamic-keys \
    name=factorySP supplicant-identity="" \
    unicast-ciphers=tkip,aes-ccm wpa2-pre-shared-key=\
    IJK12kji
```

Verkkoja varten tarvitaan lisäksi profiilit yhteysluetteloon. Yhteysluettelossa kerrotaan minkä nimiseen langattomaan verkkoon reititin yrittää yhdistyä ja mitä turvallisuusprofiilia juuri kyseisessä toimenpiteessä käytetään. Yhteysluettelon profiileja varten tarvitaan langattomista lähiverkoista SSID ja turvallisuusprofiilin nimi. SSID on tehtaan esimerkkiverkossamme factory, ja vastaava turvallisuusprofiilin nimi factorySP. Välityspalvelimen SSID puolestaan on proxy ja vastaava turvallisuusprofiilin nimi on proxySP. Yhteysluettelon profiiliin pitää määrittää myös yhteyden voimakkuusväli. Tällä tarkoitetaan väliä, jolla nyt kyseessä oleva asiakasreititin yrittää yhdistyä kyseiseen langattomaan verkkoon. Vastaavasti jos kyseiseen verkkoon ollaan yhdistyneenä ja signaalin voimakkuus ei ole tällä välillä, yhteys katkaistaan. Voimakkuusväli annetaan desibelimilliwatteina. Käytetään molemmissa verkoissa väliä -70–120. Edellä mainitut asetukset lisätään seuraavalla komennolla:

```
/interface wireless connect-list
add interface=wlan1 security-profile=proxySP \
    signal-range=-70..120 ssid=proxy
add interface=wlan1 security-profile=factorySP \
    signal-range=-70..120 ssid=factory
```

Huomautettakoon, että yhteysluetteloon voi lisätä haluamansa määrän profiileja, joilla on prioriteetti. Tässä tapauksessa prioriteetti määräytyy profiilin luontiajan mukaan, eli tämä reititin yrittäisi ensisijaisesti liittyä välityspalvelimen langattomaan verkkoon ja jos se ei onnistu, niin se yrittää liittyä tehtaan verkkoon. Lisäksi jos reititin on yhdistynyt toissijaiseen verkkoon, yhteyttä ei katkaista, vaikka ensisijainen verkko tulisikin kuuluviin. Jos yhteysluetteloon haluttaisiin lisätä profiileja, täytyy kaikille luoda myös omat turvallisuusprofiilit.

Määritetään seuraavaksi IP-asetukset reitittimelle. Reitittimen Ethernet-sovitin sijaitsee ohjausyksikön kanssa samassa lähiverkossa ja kuten ohjausyksiköstä aiemmin kerrottiin, se saa IP-osoitteensa ulkoiselta DHCP-palvelimelta. Suunnitelman mukaan verkko, jossa työkoneen laitteet sijaitsevat on 192.168.7.0/24. Reitittimen Ethernet-sovittimelle määritetään osoite 192.168.7.1, joka on verkon yhdyskäytävä. DHCP-palvelin asetetaan jakamaan osoitteita tästä verkosta, jolloin mahdolliset osoitteet ovat välillä 192.168.7.2–192.168.7.254. Sen sijaan reitittimen langaton verkkosovitin saa asiakkaana osoitteensa

ulkoiselta DHCP-palvelimelta eli joko tehtaan tukiasemalta tai välityspalvelimen tukiasemalta. Se pitää siten määrittää DHCP-asiakkaaksi. IP-asetukset määritetään seuraavalla komennolla:

```
/ip pool
add name=default-dhcp \
    ranges=192.168.7.2-192.168.7.254
/ip dhcp-server
add address-pool=default-dhcp disabled=no \
    interface=ether1 name=defconf
/ip address
add address=192.168.7.1/24 interface=ether1 \
    network=192.168.7.0
/ip dhcp-client
add comment=defconf dhcp-options=hostname,clientid \
    disabled=no interface=wlan1
/ip dhcp-server network
add address=192.168.7.0/24 gateway=192.168.7.1
```

Suunnitelman mukaan työkoneen reitittimen Ethernet-sovittimen ja langattoman verkkosovittimen välille tarvitaan osoitteenmuunnos. Koska kyseessä on täysimääräinen osoitteenmuunnos, niin tarvitaan lähdeosoitteenmuunnos ja kohdeosoitteenmuunnos. Näistä lähdeosoitteenmuunnos on vielä tarkemmin masquerade, koska käytetään langatonta verkkosovitinta, jolloin lähdeosoitetta ei muuteta miksikään yksittäiseksi IP-osoitteeksi. Mikrotik-reitittimillä täysimääräinen osoitteenmuunnos toteutetaan siten, että lähdeosoitteenmuunnos määritetään reitittimen osoitteenmuunnosasetuksiin ja kohdeosoitteenmuunnos reitittimen palomuuriasetuksiin. Luodaan lähdeosoitteenmuunnos seuraavalla komennolla:

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=wlan1
```

Kuten edellä mainittiin, määritetään kohdeosoitteenmuunnos tässä tapauksessa palomuuriasetuksiin. Näin kohdeosoitteenmuunnos saadaan toimimaan oikein paluupaketeille. Varmistetaan palomuurilla myös se, että esimerkiksi langattomasta lähiverkosta ei ole suoraa pääsyä langallisen lähiverkon laitteille. Tarvittavat asetukset palomuuriin asetetaan seuraavalla komennolla:

```
/ip firewall filter
add chain=input comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=input comment=\
    "defconf: drop all from WAN" in-interface=wlan1
add chain=forward comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=forward comment=\
    "defconf: drop invalid” connection-state=invalid
add action=drop chain=forward comment=\
    "defconf:  drop all from WAN not DST-NATed" \
    connection-nat-state=!dstnat \
    connection-state=new in-interface=wlan1
```

Työkoneen reititin on nyt asennettu langattomaksi asiakkaaksi ja sille on asetettu tarvittavat tiedot, joilla se voi muodostaa yhteyden langattomiin lähiverkkoihin.

5.2 Välityspalvelin

Nyt kun työkoneen verkko on rakennettu, voidaan lähteä rakentamaan välityspalvelimen verkkoa. Välityspalvelimen tapauksessa asennetaan ohjausyksikkö ja kaksi langatonta reititintä, joista toinen asennetaan tukiasemaksi ja toinen langattomaksi asiakkaaksi. Edetään asennuksessa tiedonkulun suunnan mukaan eli kun järjestelmää käytetään, paketti saapuu ensimmäisenä tukiasemareitittimelle, josta se etenee ohjausyksikölle ja sieltä edelleen asiakasreitittimelle. Ensimmäisenä asennetaan reititin tukiasemaksi, jonka jälkeen tehdään tarvittavat asetukset ohjausyksikköön ja lopuksi asennetaan jäljelle jäänyt reititin langattomaksi asiakkaaksi.

5.2.1 Tukiasemareititin

Aloitetaan välityspalvelimen tukiaseman asennus määrittämällä turvallisuusprofiili, sillä sitä tarvitaan langattoman verkkosovittimen asentamiseen. Määritetään ensinnäkin turvallisuusprofiilin nimi. Sen ei tarvitse olla sama kuin työkoneella, mutta käytetään tässä silti samaa nimeä, joka on siis proxySP, sillä se kuvaa hyvin kyseessä olevaa profiilia.

Lisäksi määritetään käytettävä todennusmenetelmä, joka on tässä tapauksessa WPA2. Asetetaan myös WPA2-avain, jonka tukiasemaan liittyvän asiakkaan täytyy tietää. Tämä on sama avain, joka määritettiin työkoneenkin reitittimelle. Edellä mainitut toiminnot asennetaan seuraavalla komennolla:

```
/interface wireless security-profiles
add authentication-types=wpa2-psk eap-methods="" \
    group-ciphers=tkip,aes-ccm \
    management-protection=allowed mode=dynamic-keys \
    name=proxySP supplicant-identity="" \
    unicast-ciphers=tkip,aes-ccm wpa2-pre-shared-key=\
    XYZ98zyx
```

Seuraavaksi tehdään määritykset langattomaan verkkosovittimeen. Tehdään reitittimestä tukiasema siten, että muutetaan reitittimen toimintatila tukiasemaksi. Riippuen Mikrotik Metal-mallista, taajuus voidaan valita tässä vaiheessa. Aiemmin sovimme koko järjestelmän kattavaksi taajuudeksi 2,4 GHz, joten käytetään sitä. Valitaan tukiasemalle SSID, joka tässä tapauksessa on proxy. Tässä vaiheessa valitaan myös tukiaseman lähetysteho. Tukiasemaa asennettaessa täytyy ottaa huomioon lähetystehon suuruus. Langattomaksi asiakkaaksi asennettaessa lähetystehoasetusta ei oteta huomioon, sillä tieto tarvittavasta lähetystehosta tulee tukiasemalta. Kuten standardin IEEE 802.11 mukaisista datasiirtolaitteista aiemmin mainittiin, suurin sallittu lähetysteho Suomessa on 100 mW (EIRP). Reitittimessä lähetystehon voisi asettaa käsin desibelimilliwatteina, jolloin 100 mW olisi 20 dBm. Koska antennina käytetään 6 dBi:n antennia, täytyy lähetysteho mitoittaa sen mukaan. Tätä ei kuitenkaan tarvitse itse laskea, sillä reitittimessä on automaattinen laskuri tätä varten. Sille asetetaan maa ja antennin vahvistus, jonka yksikkö on dBi. Näiden parametrien perusteella reititin osaa itse mitoittaa tarvittavan lähetystehon, sillä reitittimellä on tieto maakohtaisista lähetystehorajoituksista. Tässä ei kuitenkaan oteta huomioon siirtolinjassa tapahtuvia häviöitä, jotka voisi periaatteessa vähentää antennin vahvistuksesta. Tällöin reitittimestä lähtevä teho kasvaisi. Tässä tapauksessa antenni on kuitenkin kiinnitetty suoraan reitittimeen, joten tätä ei tarvitse huomioida. Muutenkin siirtolinjan pitäisi olla hyvin pitkä, jotta sen aiheuttama häviö voitaisiin vähentää antennin vahvistuksesta, sillä antennin vahvistusasetukseen voidaan asettaa vain

kokonaislukuarvoja. Edellä mainittujen seikkojen perusteella langaton verkkosovitin asennetaan seuraavanlaisella komennolla:

```
/interface wireless
set [ find default-name=wlan1 ] antenna-gain=6 \
    band=2ghz-b/g/n channel-width=20/40mhz-Ce \
    country=finland disabled=no frequency=auto \
    mode=ap-bridge security-profile=proxySP ssid=proxy
```

Tämän jälkeen määritetään IP-asetukset. Suunnitelman mukaan langallinen lähiverkko on 192.168.7.0/24 ja langaton lähiverkko on 192.168.133.0/24. Verkkosovittimien IP-osoitteet ovat edellä mainituissa verkoissa 192.168.7.1 ja 192.168.133.1. Lisäksi langattomassa lähiverkossa täytyy olla DHCP-palvelu toiminnassa, joten määritetään DHCP-palvelin antamaan osoitteita asiakkaille siten, että osoiteavaruus on 192.168.133.2–192.168.133.254. Tällöin asennuskomento on seuraavanlainen:

```
/ip pool
add name=dhcp ranges=192.168.133.2-192.168.133.254
/ip dhcp-server
add address-pool=dhcp disabled=no interface=wlan1 \
    name=dhcp1
/ip address
add address=192.168.7.1/24 interface=ether1 \
    network=192.168.7.0
add address=192.168.133.1/24 interface=wlan1 \
    network=192.168.133.0
/ip dhcp-server network
add address=192.168.133.0/24 gateway=192.168.133.1
```

Määritetään seuraavaksi osoitteenmuunnos. Suunnitelman mukaan tässä tulee käyttää kohdeosoitteenmuunnosta, joka muuntaa osoitteen x.y.z.a ohjausyksikön osoitteeksi 192.168.7.10. Tässä tapauksessa sallitaan vain TCP-yhteydet. Tämä asetetaan seuraavalla komennolla:

```
/ip firewall nat
add action=dst-nat chain=dstnat dst-address=x.y.z.a \
    protocol=tcp to-addresses=192.168.7.10
```

Reitittimen palomuuriin tarvitaan lisäksi oikeanlaiset asetukset, joilla mahdollistetaan reitittimen oikeanlainen toiminta verkkojen osalta. Asetukset palomuuriin asetetaan seuraavalla komennolla:

```
/ip firewall filter
add chain=input comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=input comment=\
    "defconf: drop all from WAN" in-interface=wlan1
add chain=forward comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=forward comment=\
    "defconf: drop invalid” connection-state=invalid
add action=drop chain=forward comment=\
    "defconf:  drop all from WAN not DST-NATed" \
    connection-nat-state=!dstnat \
    connection-state=new in-interface=wlan1
```

Reititin on nyt asennettu tukiasemaksi.

5.2.2 Ohjausyksikkö

Välityspalvelimen verkkoarkkitehtuurin näkökulmasta ohjausyksiköllе täytyy asettaa kiinteä IP-osoite ja yhdyskäytävä. Lisäksi täytyy kertoa reitti ohjausyksiköltä tukiaseman puoleiselle langattomalle lähiverkolle. Tiedostossa /etc/network/interfaces verkkoasetukset ovat normaalisti seuraavanlaiset:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

Siinä määritetään sisäinen verkkosovitin (lo) takaisinkaiutusosoitteeksi. Lisäksi määritetään Ethernet-sovitin (eth0) saamaan IP-parametrit DHCP-palvelimelta. Suunnitelman mukaan välityspalvelimen lähiverkossa ei käytetä DHCP-palvelua ollenkaan, vaan ohjausyksikölle ja reitittimille asetetaan kiinteät IP-osoitteet. Ohjausyksikön verkkoasetuksia täytyy muokata siten, että sille tulee kiinteä IP-osoite, joten asetetaan tiedostoon

IP-osoitteeksi suunniteltu 192.168.7.10. Lisäksi täytyy määrittää aliverkon maski, joka tässä tapauksessa on 255.255.255.0. IP-osoitteesta ja maskista käyttöjärjestelmä laskee käytettävän verkon (192.168.7.0/24) ja levitysviestiosoitteen (192.168.7.255) automaattisesti, joten niitä ei tähän tarvitse erikseen asettaa. Yhdyskäytävä sen sijaan merkitään tiedostoon. Suunnitelman mukaan ohjausyksikön yhdyskäytäväksi tulee 192.168.7.2. Näillä asetuksilla ohjausyksikkö pystyy lähettämään paketin eteenpäin yhdyskäytävälle, mutta tukiasemana toimivan reitittimen kohdeosoitteenmuunnoksen kautta tulleet paketit eivät vielä löydä reittiä takaisin lähettäjälle. Asetetaan tiedostoon reitti verkkoon 192.168.133.0/24, joka löytyy osoitteen 192.168.7.1 takaa. Näin paketit osaavat takaisin siihen verkkoon, jossa olivat ennen kohdeosoitteenmuunnosta. Muokkauksien jälkeen interfaces-tiedosto näyttää seuraavanlaiselta:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
  address 192.168.7.10
  netmask 255.255.255.0
  gateway 192.168.7.2
  up route add -net 192.168.133.0/24 gw 192.168.7.1
```

5.2.3 Asiakasreititin

Välityspalvelimen sisällä verkko on nyt rakennettu tukiaseman ja ohjausyksikön välille. Vielä täytyy asentaa jäljelle jäänyt reititin langattomaksi asiakkaaksi välityspalvelimen verkkoon. Jotta välityspalvelimen reititin voidaan asentaa asiakastilaan, tarvitaan tiedot tehtaan langattomasta lähiverkosta. Tarvittavia tietoja ovat jälleen SSID, käytettävä todennusmenetelmä, todennusmenetelmän mukainen avain ja langattoman verkon taajuus.

Aloitetaan reitittimen asennus määrittämällä langattoman verkkosovittimen asetukset. Reitittimestä tehdään nyt langaton asiakas tukiaseman sijaan, eli se voi liittyä langattomaan lähiverkkoon aivan kuten työkoneenkin reititin. Tässä vaiheessa asetetaan myös toimintataajuus, joka esimerkkiverkossamme on 2,4 GHz. Nämä asetukset asetetaan seuraavalla komennolla:

```
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n \
    channel-width=20/40mhz-Ce \
    default-authentication=no disabled=no \
    frequency=auto mode=station ssid=""
```

Seuraavaksi luodaan turvallisuusprofiili tehtaan verkkoa varten. Tässä voidaan käyttää täsmälleen samaa profiilia, jota käytettiin toisena profiilina työkoneen reitittimessä. Annetaan profiilille nimeksi tässäkin tapauksessa factorySP. Lisäksi määritetään todennusmenetelmäksi jälleen WPA2 ja avaimeksi sama avain kuin työkoneenkin tapauksessa. Luodaan turvallisuusprofiili seuraavalla komennolla:

```
/interface wireless security-profile
add authentication-types=wpa2-psk eap-methods="" \
    group-ciphers=tkip,aes-ccm \
    management-protection=allowed mode=dynamic-keys \
    name=factorySP supplicant-identity="" \
    unicast-ciphers=tkip,aes-ccm wpa2-pre-shared-key=\
    IJK12kji
```

Tehtaan langatonta lähiverkkoa varten tarvitaan vielä profiili yhteysluetteloon. Yhteysluettelon profiilia varten tarvitaan SSID ja turvallisuusprofiilin nimi. SSID on esimerkkiverkossamme factory, ja turvallisuusprofiilin nimi on factorySP. Yhteysluettelon profiiliin pitää määrittää myös signaalin voimakkuusväli desibelimilliwatteina eli väli, jolla asiakasreititin yrittää yhdistyä kyseessä olevaan langattomaan lähiverkkoon. Käytetään tässä tapauksessa väliä -70–120. Nämä asetukset lisätään seuraavalla komennolla:

```
/interface wireless connect-list
add interface=wlan1 security-profile=factorySP \
    signal-range=-70..120 ssid=factory
```

Toisin kuin työkoneen tapauksessa, nyt yhteysluettelossa on vain yksi profiili. Tämä tarkoittaa yksinkertaisesti sitä, että langaton asiakas yrittää yhdistyä vain tähän verkkoon ja jos sitä ei ole saatavilla, yhteyttä ei muodosteta mihinkään.

Seuraavaksi määritetään IP-asetukset. Reititin sijaitsee fyysisesti välityspalvelimen lähiverkossa, joka on 192.168.7.0/24. Suunnitelman mukaan langattoman verkkosovittimen osoitteeksi tulee 192.168.7.2. DHCP-palvelinta ei tarvita, sillä välityspalvelimen

langallisessa lähiverkossa kaikilla laitteilla on kiinteä IP-osoite. Sen sijaan langattomana asiakkaana langattoman verkkosovittimen pitää saada osoitteensa tukiasemalta, joten asetetaan langaton verkkosovitin DHCP-asiakkaaksi. Edellä mainitut asetukset asetetaan seuraavalla komennolla:

```
/ip address
add address=192.168.7.2/24 interface=ether1 \
    network=192.168.7.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no \
    interface=wlan1
```

Suunnitelman mukaan välityspalvelimen asiakasreitittimen Ethernet-sovittimen ja langattoman verkkosovittimen välille tarvitaan täysimääräinen osoitteenmuunnos. Tässä tapauksessa tämä luodaan samalla tavalla kuin työkoneenkin tapauksessa, eli lähdeosoitteenmuunnos määritetään osoitteenmuunnosasetuksiin ja kohdeosoitteenmuunnos palomuuriasetuksiin. Määritetään lähdeosoitteenmuunnos seuraavalla komennolla:

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=wlan1
```

Palomuuriin asetetaan kohdeosoitteenmuunnos, kuten edellä mainittiin ja lisäksi perusasetukset, jotka estävät suoran pääsyn verkosta toiseen. Asetetaan palomuuriasetukset seuraavalla komennolla:

```
/ip firewall filter
add chain=input comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=input comment=\
    "defconf: drop all from WAN" in-interface=wlan1
add chain=forward comment=\
    "defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=forward comment=\
    "defconf: drop invalid” connection-state=invalid
add action=drop chain=forward comment=\
    "defconf:  drop all from WAN not DST-NATed" \
    connection-nat-state=!dstnat \
    connection-state=new in-interface=wlan1
```

Välityspalvelimen toinen reititin on nyt asennettu langattomaksi asiakkaaksi ja sillä on tarvittavat tiedot, joilla se voi liittyä tehtaan langattomaan lähiverkkoon.

6 TESTAUS

Nyt kun kaikki laitteet on asennettu suunnitelman mukaisesti, niin tietoliikennettä voidaan testata. Testataan tietoliikenteen toimivuutta ohjausyksiköiden välillä, jolloin voidaan olettaa, että myös reitittimet toimivat oikein, sillä ne ovat ohjausyksiköiden välissä. Myös REST-palvelin voidaan ottaa mukaan testaukseen, jolloin yhteys internetiin tulee testattua samalla. Ensimmäisessä testitapauksessa testataan yhteys työkoneen ohjausyksiköltä REST-palvelimelle. Tämän jälkeen testataan yhteys työkoneen ohjausyksiköltä välityspalvelimen ohjausyksikölle. Viimeisenä testataan yhteys välityspalvelimen ohjausyksiköltä REST-palvelimelle. Näin kuvassa 12 näkyvät reitit on käyty läpi. Edellä mainituissa tapauksissa tulevat testatuiksi langalliset lähiverkot ja välityspalvelimen osoitteenmuunnoksen- sekä reitityksen oikeanlainen toiminta.

6.1 Työkoneelta lähtevä tietoliikenne

Työkoneelta lähtevien yhteyksien testaamisessa lähtöpiste on työkoneen ohjausyksikkö. Aluksi testataan yhteyden toimivuus REST-palvelimelle ja internetiin. Data kulkee työkoneen ohjausyksiköltä työkoneen langattomaksi asiakkaaksi asennetulle reitittimelle, joka on liittynyt tehtaan langattomaan lähiverkkoon ja tästä verkosta on pääsy internetiin.

Ennen varsinaisen yhteyden kokeilua on kuitenkin syytä testata reitittimen yhteysluettelon toiminta. Tämä tarkoittaa sitä, että reitittimen langaton verkkosovitin todella liittyy yhteysluettelossa oleviin langattomiin verkkoihin. Tämän testaamiseen tarvitaan siten luettelossa mainittu langaton verkko ja koska nyt testataan yhteyttä internetiin ja REST-palvelimeen, tarvitaan tehtaan langaton lähiverkko. Jotta tätä verkkoa voitaisiin simuloida, tarvitaan sen SSID ja WPA2-avain. Yhteysluettelossa määriteltiin tehdasverkon SSID:ksi factory ja WPA2-avaimeksi IJK12kji. Nyt tarvitaan vielä tukiasema, jolla on edellä mainittu SSID ja avain. Lisäksi tukiasemalta pitää olla yhteys internetiin, sillä simuloimme oikeaa tehtaan langatonta lähiverkkoa. Myös taajuus täytyy olla sama kuin reitittimessä eli tässä tapauksessa 2,4 GHz. Koska tukiasemalle ei ole muita erityisiä

vaatimuksia, voidaan yksinkertaisesti käyttää esimerkiksi älypuhelimesta löytyvää tukiasematoimintoa. Asetetaan oikea SSID, WPA2-avain ja taajuus. Yhdistyminen voidaan havaita Winbox- tai Webfig-ohjelman Quick Set-välilehdeltä. Samalta välilehdeltä nähdään myös langattoman lähiverkon muita tietoja, joita ovat esimerkiksi SSID ja signaalin voimakkuus. Yhdistyminen voidaan havaita myös ilman ohjelmia reitittimessä olevien LED-valojen avulla. Nyt kun tukiasema käynnistetään, niin langaton asiakasreititin yhdistyy tukiasemaan. Voidaan siis todeta, että ainakin tehtaan verkkoon liittyminen toimii automaattisesti.

Nyt voidaan kokeilla itse yhteyden toimivuutta työkoneen ohjausyksiköltä REST-palvelimelle, joka sijaitsee internetissä osoitteessa x.y.z.a. Yhteyttä voidaan kokeilla kätevästi lähettämällä POST-pyyntö REST-palvelimelle, sillä palvelin antaa vastauksen sen mukaan, hyväksyykö se sille lähetetyn datan. Palvelin ottaa vastaan vain tietyntyyppistä JSON-dataa, mutta lähetämme tässä vain yleistä tekstimuotoista dataa sen sijaan. POST-pyyntö voidaan lähettää esimerkiksi Linuxin komentokehotteessa ohjelmalla cURL. Lähetyskomento on seuraavanlainen:

```
curl --connect-timeout 5 –s –X POST \
--data "yhteyskokeilu" x.y.z.a/jsonimport.php
```

Kun pyyntö lähetetään, niin REST-palvelin vastaa lähettämällä seuraavanlaisen merkkijonon:

```
>>>R,ERS,DATANOTVALID<<<
```

Palvelin ei siis huolinut vastaanottamaansa dataa, eikä siten tallentanut sitä tietokantaan. Se ei ollut tarkoituskaan, vaan tärkeintä on se, että palvelin lähetti vastauslähetyksen, jolloin voidaan olla varmoja siitä, että yhteys ohjausyksiköltä palvelimelle ja internetiin toimii.

Seuraavaksi testataan yhteys työkoneen ohjausyksiköltä välityspalvelimen ohjausyksikölle. Tässä tapauksessa data kulkee ensin työkoneen ohjausyksiköltä reitittimelle, joka puolestaan on yhdistyneenä välityspalvelimen tukiasemaan. Tukiaseman kohdeosoit-

teenmuunnoksen kautta data kulkee edelleen välityspalvelimen ohjausyksikölle. Myös tässä tapauksessa testataan aluksi reitittimen yhdistyminen välityspalvelimen langattomaan lähiverkkoon yhteysluettelon avulla. Nyt tukiasemana toimii välityspalvelimen oma tukiasema. Kun työkoneen reititin ja välityspalvelimen tukiasemana toimiva reititin käynnistetään, niin huomataan, että työkoneen reititin yhdistyy tukiasemaan automaattisesti, joten yhteysluettelon mukainen yhdistyminen toimii odotetusti.

Nyt voidaan kokeilla yhteyden toimivuutta välityspalvelimen ohjausyksikölle. Tätä voidaan testata yksinkertaisesti Linuxista löytyvällä ohjelmalla nimeltä Netcat. Sitä voidaan käyttää TCP- ja UDP-yhteyksien muodostamiseen. Tässä tapauksessa välityspalvelimen ohjausyksikkö asetetaan kuuntelemaan TCP-yhteyksiä tietystä portista. Työkoneen ohjausyksiköltä voidaan sitten lähettää TCP-paketti ”REST-palvelimelle” ja samaan porttiin, jota ohjausyksikkö kuuntelee. Asetetaan välityspalvelimen ohjausyksikkö kuuntelemaan TCP-yhteyksiä portista 50000 seuraavalla komennolla:

```
nc –l 50000
```

Työkoneen ohjausyksiköltä lähetetään viesti ”REST-palvelimelle” osoitteeseen x.y.z.a eli oikeasti ohjausyksikölle porttiin 50000 seuraavalla komennolla:

```
echo "yhteyskokeilu" | nc -v –w 5 x.y.z.a 50000
```

Nyt kun paketti lähetettiin työkoneen ohjausyksiköltä, niin välityspalvelimen ohjausyksikön Netcat tulostaa viestin ”yhteyskokeilu” ja työkoneen ohjausyksikön näytölle tulostuu seuraavanlainen ilmoitus:

```
Connection to x.y.z.a 50000 port [tcp/*] succeeded!
```

Voidaan siis todeta, että yhteys toimii odotetulla tavalla.

Koska työkoneen reitittimen yhteysluettelossa on kaksi profiilia, niin on paikallaan testata vielä yhteysluettelon toiminta kokonaisuudessaan. Toisin sanoen testataan asiakasreitittimen automaattinen yhdistyminen saatavilla oleviin langattomiin lähiverkkoihin. Tätä voidaan testata siten, että annetaan työkoneen reitittimen yhdistyä näkyvissä ole-

vaan lähiverkkoon, jonka jälkeen käynnistetään toinen tukiasema. Tämän jälkeen sammutetaan ensimmäinen tukiasema, mikä simuloi kyseisen verkon katoamista. Tällöin reitittimen tulisi yhdistyä automaattisesti jäljellä olevan tukiaseman langattomaan lähiverkkoon, sillä se on ainut verkko, joka on kuuluvissa sillä hetkellä. Tämän jälkeen tehdään vielä sama toimenpide vastakkaisessa järjestyksessä, eli käynnistetään sammutettu tukiasema ja sammutetaan se tukiasema, johon reititin on nyt yhdistyneenä. Nyt reitittimen tulisi yhdistyä takaisin alkuperäiseen langattomaan lähiverkkoon, sillä se on nyt ainoa verkko, joka on käytettävissä. Tätä voidaan testata aiemmin käytetyillä tukiasemilla eli välityspalvelimen tukiasemalla ja älypuhelimella simuloidulla tehtaan tukiasemalla. Käynnistetään tehtaan tukiasema, jolloin huomataan, että työkoneen reititin liittyy tämän tukiaseman verkkoon muutaman sekunnin viiveellä. Sitten laitetaan välityspalvelimen tukiasema päälle ja sammutetaan tehdasverkko. Reititin kadottaa yhteyden tehdasverkkoon ja siirtyy etsimään verkkoja, jolloin se löytää välityspalvelimen langattoman verkon ja liittyy siihen. Nyt käynnistetään tehdasverkko uudelleen ja sammutetaan välityspalvelimen tukiasema. Myös tällä kertaa tapahtuu samoin, eli yhteys katkaistaan ja löydetään uusi verkko, johon liitytään. Voidaan siis todeta, että yhteysluettelo toimii odotetusti ja työkone voi suunnitelman mukaisesti liittyä sekä välityspalvelimen langattomaan lähiverkkoon että tehtaan langattomaan lähiverkkoon.

6.2 Välityspalvelimelta lähtevä tietoliikenne

Välityspalvelimelta yhteydet lähtevät ohjausyksiköltä. Data kulkee aluksi välityspalvelimen langattomalle asiakkaalle, joka on yhdistynyt tukiasemaan. Tukiasemalta on sitten yhteys internetiin ja REST-palvelimelle. Tilanne muistuttaa työkoneen ensimmäistä testitapausta, joten myös tässä tapauksessa voidaan käyttää samoja menetelmiä yhteyden testaamiseen. Aluksi testataan kuitenkin yhteysluettelon toiminta. Koska välityspalvelimen langattomana asiakkaana toimiva reititin muodostaa yhteyden tehtaan langattomaan verkkoon työkoneen reitittimen tavoin, voidaan simulointi tehdä käyttäen samaa tukiasemaa kuin työkoneenkin tapauksessa, sillä tehdasverkko on molemmissa tapauksissa täsmälleen sama. Käynnistetään välityspalvelimen asiakasreititin ja tehdasverkon

simuloitu tukiasema älypuhelimesta. Langaton asiakas yhdistyy tukiasemaan automaattisesti, joten todetaan yhteysluettelon toimivan oikein.

Yhteyden toimivuus REST-palvelimelle voidaan testata samalla menetelmällä kuin työkoneenkin tapauksessa, eli lähetetään POST-pyyntö seuraavalla komennolla:

```
curl --connect-timeout 5 –s –X POST \
--data "yhteyskokeilu" x.y.z.a/jsonimport.php
```

REST-palvelin vastaa samanlaisella viestillä kuin työkoneenkin tapauksessa eli seuraavanlaisella merkkijonolla:

```
>>>R,ERS,DATANOTVALID<<<
```

Palvelin ei siis edelleenkään huolinut sille tulevaa dataa ja lähetti vastauksena viestin, joka kertoo, että data ei ole oikeassa muodossa. Voimme kuitenkin todeta yhteyden toimivan, sillä saimme palvelimelta vastauksen.

7 TULOKSET

Tuloksena syntyi toimiva järjestelmä tulevaisuuden ohjelmistoratkaisuja varten. Uuden järjestelmän tärkein ominaisuus on se, että sen avulla on mahdollista siirtää dataa kaivostyömaan työkoneelta palvelimelle internetiin, vaikka työkoneella itsellään ei ole internet-yhteyttä lainkaan käytettävissä. Tiedon siirron puolestaan mahdollistaa järjestelmässä toimiva välityspalvelin, joka sisältää elementtejä sekä tehtaan langattomasta lähiverkosta että työkoneen verkkoarkkitehtuurista. Välityspalvelin uskottelee työkoneille olevansa oikea Exertuksen ReDi-palvelun REST-palvelin internetissä. Tämän ansiosta työkoneilla käytössä olevaan ohjausjärjestelmään ei tarvitse tehdä lainkaan muutoksia tähän liittyen.

Eräs järjestelmän vahvuus on sen dynaamisuus. Järjestelmän välityspalvelinta ei ole nimittäin pakko käyttää, jos sellaiselle ei ole mitään tarvetta. Jos esimerkiksi kaivokseen on rakennettu oma verkkoinfrastruktuuri, niin ei ole mitään järkeä käyttää välityspalvelinta kaivoksessa. Pahimmassa tapauksessa tämä vain hidastaisi datan siirtoa ja välityspalvelimeksi valjastettu ajoneuvo olisi vain tiellä. Järjestelmään ei tarvitse tehdä edes muutoksia liittyen välityspalvelimen käyttöön. Samat asetukset käyvät järjestelmään, jossa käytetään välityspalvelinta sekä järjestelmään, jossa ei käytetä välityspalvelinta. Tämä helpottaa myös järjestelmän asentamista ja ylläpitoa. Esimerkiksi jos järjestelmää halutaan kokeilla aluksi ilman välityspalvelinta, voidaan näin helposti tehdä. Järjestelmällä on siitä huolimatta täysi valmius käyttää välityspalvelinta, jos sellaista myöhemmin tarvitaan.

Uusi järjestelmä rakennettiin internetin perustana olevaa TCP/IP-protokollaperhettä käyttäen. Tämän ansiosta järjestelmään voidaan räätälöidä hyvin monenlaisia ohjelmistoratkaisuja, sillä TCP/IP-protokollaperheen mukaisia tekniikoita on runsaasti saatavilla ja niitä voidaan soveltaa monilla eri tavoilla. Välityspalvelimen ytimenä voidaan katsoa olevan osoitteenmuunnos. Juuri sen avulla välityspalvelin saadaan näyttäytymään työkoneille oikean palvelimen IP-osoitteella. Tällä tavoin yhteydellisestä TCP:stä tehtiin periaatteessa yhteydetön protokolla, sillä dataa voidaan siirtää TCP-yhteyden avulla työkoneelta oikealle palvelimelle yhteydettömästi tulevien ohjelmistoratkaisujen avulla.

Näin TCP:stä saadaan käyttöön sen hyvät puolet, joita ovat esimerkiksi luotettavuus ja valmiiden ohjelmistoratkaisujen määrä. Uudessa järjestelmässä käytettävää osoitteenmuunnosta toivoisi tekniikkana sovellettavan muuhunkin kuin sen alkuperäiseen tarkoitukseen eli IPv4-osoitteiden säästämiseen. Tämä liittyy juuri täysimääräiseen osoitteenmuunnokseen, mutta lähde- ja kohdeosoitteenmuunnoksen käyttöä erikseen voitaisiin tällä hetkellä hyödyntää enemmänkin erilaisissa IPv4-osoitteisiin perustuvissa verkoissa.

Yksi lähitulevaisuuden visio järjestelmän ohjelmistoarkkitehtuuriin liittyen on MQTT-protokollan käyttö järjestelmän tiedonsiirrossa. MQTT on esineiden internetin tiedonsiirtoon sopiva yksinkertainen tuottaja–tilaaja-protokolla. Se sopii hyvin alhaisen kaistanleveyden- ja korkean viiveen verkkoihin, joissa laitteilla on pienet resurssit. Kuten nykyisessäkin järjestelmässä käytössä oleva JSON-formaatti, myös MQTT-protokolla on muodostumassa de facto -standardiksi IoT-alalla. (Hassan, Khan & Madani 2018: 200.) MQTT-protokollan avulla uuden järjestelmän verkon toimintaa päästään testaamaan pienellä vaivalla, sillä MQTT toimii TCP/IP-protokollaperheen päällä (Gastón 2017: 9–10). Jos MQTT-protokollan toimivuus järjestelmässä todetaan myöhemmin käyttökelpoiseksi, voidaan sitä soveltaa myös aiemmin mainitun viivesietoisen verkon toteutuksessa, jos sellainen päätetään kehittää.

Järjestelmän yksittäisten laitteiden suorituskykyä sivuttiin nopeasti testauksen yhteydessä. Käytännössä järjestelmässä käytettävät langattomat reitittimet toimivat hyvin nopeasti. Jos reitittimet ovat päällä, niin ne pystyvät liittymään automaattisesti langattomaan lähiverkkoon noin viidessä sekunnissa siitä kun langaton verkko tulee kuuluviin. Aika ei juuri kasva tilanteessa, jossa reititin kadottaa yhteyden sen hetkiseen langattomaan verkkoon ja liittyy toiseen kuuluvissa olevaan langattomaan verkkoon. Tässä kestää alle kymmenen sekuntia. Jos reititin ei ole päällä, niin käynnistyksestä verkkoon liittymiseen menee noin puoli minuuttia.

7.1 Kehitysideat

Vaikka uusi järjestelmä mahdollistaa monenlaisten ohjelmistoratkaisujen käytön jo nyt, niin järjestelmän verkkoarkkitehtuuria voidaan edelleen kehittää. Kuten aiemmin mainittiin, voidaan reitittimien yhteysluetteloon lisätä useita profiileja. Jos kaivoksen ja tehtaan alueella on esimerkiksi useita langattomia lähiverkkoja, voidaan näille kaikille tehdä profiilit yhteysluetteloon, jolloin reitittimet voivat yhdistyä kaikkiin verkkoihin ja internet-yhteyden saatavuus alueena laajenee. Tätä voidaan soveltaa myös tilanteeseen, jossa välityspalvelimia olisi kaksi tai jopa enemmän. Tällainen järjestely voi olla tarpeen, jos kaivostyömaa on todella suuri ja siellä on paljon kaivostyökoneita eri alueilla. Tästä olisi lisäksi se hyöty, että kaikkien työkoneiden data ei olisi yhdessä paikassa ja välityspalvelimessa olevan ohjausyksikön kuormaa saataisiin tasattua. Diplomityön tuloksena syntynyt järjestelmä suunniteltiin siten, että välityspalvelimia on yksi ja työkoneita monta, mutta teoriassa järjestelmän pitäisi toimia myös monella välityspalvelimella pienin muutoksin. Tämä vaatisi uuden välityspalvelinprofiilin yhteysluetteloon. Tämän perusteella monen välityspalvelimen järjestelmässä kaikilla välityspalvelimilla olisi oma SSID ja oma WPA2-avain. Tätä puolestaan voitaisiin jalostaa edelleen siten, että kaikille välityspalvelimille asetettaisiin sama SSID ja WPA2-avain kuin tehtaan langattomalla lähiverkolla. Työkoneen reitittimen yhteysluetteloon tulisi täten vain yksi profiili, joka kattaisi tehtaan langattoman lähiverkon ja välityspalvelimet. Vaikka tehtaalla olisi useita langattomia lähiverkkoja, niin silloinkin edellä mainittua tilannetta voitaisiin käyttää soveltuvilta osin. Yhdellä profiililla työkoneiden reitittimet yhdistyisivät oletettavasti aina vahvimman signaalin verkkoon riippumatta siitä, onko verkko välityspalvelimen vai tehtaan. Tämä vaatii kuitenkin lisätutkimuksia varsinkin tietoturvan näkökulmasta. Tästä syystä järjestelmä suunniteltiin siten, että välityspalvelimen tukiasema tarjoaa aivan oman langattoman lähiverkkonsa omalla salausavaimella, jotta se ei vaaranna tehtaan langatonta lähiverkkoa ja sen salausavainta.

Tietoturvaan liittyen lisätutkimusta vaativat myös reitittimien palomuuriasetukset. Diplomityön toteutusvaiheessa reitittimiin asennettiin yksinkertaiset palomuuriasetukset. Nämä asetukset ovat periaatteeltaan sellaiset, että palomuuri sallii vain sellaiset yhteydet, jotka on erikseen sallittu palomuurin asetuksissa. Tämä tarjoaa riittävän tietoturvan

järjestelmälle, mutta asetukset saattavat olla liian tiukat joihinkin sovelluksiin. Palomuurin asetukset vaativatkin laajaa tutkimusta, jossa pohditaan tietoturvan ja helppokäyttöisyyden suhdetta. Palomuuriasetusten perustana on käytetty Discherin (2011: 66–88) kirjassa esitettyjä suosituksia perustavanlaatuisesta palomuurista. Mikrotikin (2017b) verkkosivuilla olevaa esimerkkiä palomuurin perusasetuksista on myös sovellettu tässä tapauksessa. Palomuuriasetuksia kannattaakin lähteä kehittämään näiden pohjalta ottaen samalla huomioon tulevien ohjelmistoratkaisujen vaatimukset. Tietoturvaan liittyy tietenkin muitakin asioita, kuin pelkkä palomuuri. Palomuureilla estetään pääsy verkosta toiseen verkkoon. Toisin sanoen palomuuri on ulkoisia uhkia varten. Tilanne kuitenkin muuttuu oleellisesti, jos tietomurto tapahtuu paikallisesti. Tästä syystä on äärimmäisen tärkeää estää reitittimien luvaton käyttö myös paikallisesti. Tällaisessa tilanteessa voidaan hyödyntää Mikrotik-reitittimen kirjautumisominaisuutta. Reitittimelle voidaan luoda käyttäjätunnus ja salasana kirjautumista varten. Jos kirjautumistiedot eivät ole tiedossa, asetuksia ei pääse muokkaamaan. Oletuksena reitittimissä on käyttäjä admin, jonka salasana on tyhjä. Kun oma käyttäjätunnus on luotu, on oletuskäyttäjä syytä poistaa kokonaan. Näitä asetuksia ei käyty läpi toteutusvaiheessa, sillä ne eivät liity tietoliikenteen toimintaan toisin kuin palomuuri. Edellä kuvattu uuden käyttäjän lisäys ja oletuskäyttäjän poisto voidaan tehdä siten, että muutetaan oletuskäyttäjän nimi ja salasana (Mikrotik 2017c). Seuraavanlaisella komennolla muutettaisiin oletuskäyttäjän nimeksi Maintenance ja salasanaksi 1k3e7TQ0r:

```
/user set 0 name=Maintenance
/user set 0 password="1k3e7TQ0r"
```

Mikrotikin (2017c) verkkosivuilta löytyy myös muita tietoturvaan liittyviä asetuksia, joiden avulla reitittimestä saadaan turvallisempi.

DNS ei ollut vaatimuksena uudessa järjestelmässä, sillä laitteiston näkökulmasta IP-osoitteen käyttäminen on suoraviivaisempaa. DNS kuitenkin toimii työkoneen reitittimessä suoraan tällä hetkellä. Toisin sanoen työkoneen reitittimen voi kytkeä omaan tietokoneeseen ja selata sen avulla internetiä normaalisti verkkotunnuksia käyttäen. Tämä johtuu siitä, että työkoneen ohjausyksikkö ja myös edellä mainittu tietokone saavat IP-parametrit reitittimen DHCP-palvelimelta. Välityspalvelimessa DNS ei toimi suoraan,

mutta sen saa toimimaan siten, että määrittää nimipalvelimen osoitteen ohjausyksikölle käsin. Tulevaisuudessa ReDi-palvelun REST-palvelimen IP-osoite saattaa muuttua, jos palvelin vaihdetaan toiseen. Jos palvelin ja IP-osoite vaihtuvat useamminkin, niin silloin kannattaa siirtyä käyttämään nimipalvelua koko järjestelmässä. Tällöin osoitteena voitaisiin käyttää aina samaa verkkotunnusta muuttuvan IP-osoitteen sijaan, mikä helpottaa järjestelmän ylläpitoa. Siinä tilanteessa välityspalvelimelle pitäisi lisätä tuki nimipalvelulle.

Edellisten asioiden lisäksi on aiheellista pohtia välityspalvelimen reititystä. Toteutuksessa välityspalvelimen ohjausyksikölle asetettiin kiinteät IP-parametrit kohdeosoitteenmuunnosta varten ja DHCP-palvelu ei ole käytössä välityspalvelimen langallisessa lähiverkossa. Tämä ratkaisu on hyvä siinä mielessä, että se on yksinkertainen ja aina samanlainen laitteiston vaihtuessakin. Kiinteiden IP-parametrien asettamiseen tarvitaan kuitenkin pääkäyttäjän oikeudet ohjausyksikön Linuxissa, mutta se ei ole suuri ongelma tässä tapauksessa. Tulevaisuuden ohjelmistoratkaisut saattavat nekin vaatia pääkäyttäjän oikeuksia, joten kiinteiden IP-parametrien asettamisesta ei tule ylimääräistä taakkaa.

Välityspalvelimen langallisessa lähiverkossa voitaisiin siitä huolimatta käyttää DHCP-palvelua, koska sen avulla esimerkiksi DNS saataisiin toimimaan automaattisesti. Kuten edellä pohdittiin, niin DNS vaatii tällä hetkellä kiinteän määrittelyn välityspalvelimen ohjausyksikölle, jos sitä haluttaisiin käyttää. Välityspalvelimen langattomana asiakkaana toimivalla reitittimellä voitaisiin ottaa DHCP-palvelin käyttöön. Tämän johdosta verkkotunnus ja myös muut IP-parametrit saataisiin asetettua automaattisesti ohjausyksikölle. Ongelmaksi muodostuu se, että ohjausyksikön IP-osoite täytyy olla aina sama, jotta kohdeosoitteenmuunnos toimii oikein. Tämä voidaan kuitenkin ratkaista monellakin eri tavalla. Reitittimen DHCP-palvelimelle voidaan esimerkiksi tehdä sellainen asetus, joka yhdistää aina saman IP-osoitteen ennalta määriteltyyn MAC-osoitteeseen. Kyseessä on tällöin käsin määritys, kuten teoreettisessa viitekehyksessä aiemmin mainittiin. Tämän MAC-osoitteen omistaja olisi sitten välityspalvelimen ohjausyksikkö. Tällöin juuri tämä ohjausyksikkö saisi aina saman IP-osoitteen reitittimen DHCP-palvelimelta. Haittapuolena on se, että jos ohjausyksikkö joudutaan vaihtamaan, pitää reitittimen DHCP-asetuksiin määrittää uuden ohjausyksikön MAC-osoite. Parempi rat-

kaisu DHCP-palvelun käyttöön olisi sellainen, jossa reitittimen DHCP-palvelin antaa ohjausyksikölle satunnaisen IP-osoitteen, jolloin tuo IP-osoite yhdistettäisiin siis ohjausyksikön fyysiseen Ethernet-sovittimeen, aivan kuten normaalisti tapahtuukin. Fyysisen Ethernet-sovittimen lisäksi Linuxiin voitaisiin luoda virtuaalinen verkkosovitin, jolle määritetään IP-osoitteeksi se osoite, jonka kohdeosoitteenmuunnos vaatii. Virtuaalinen verkkosovitin voitaisiin luoda ohjelmallisesti aina ohjausyksikön käynnistyessä. Tämä vaatii kuitenkin jälleen pääkäyttäjän oikeudet, mutta kuten aiemmin todettiin, ei siitä ole erityistä haittaa tässä vaiheessa. Todennäköisesti paras ja ehkä yllättäväkin ratkaisu DHCP-palvelun käyttöönottamiseksi, olisi määrittää DHCP-palvelimen jaettavien IP-osoitteiden osoiteavaruus yhden osoitteen suuruiseksi. Tällöin DHCP-palvelin antaa aina tuon yhden ja saman IP-osoitteen ohjausyksikölle riippumatta siitä, mikä sen MAC-osoite on.

Kaikissa edellä mainituissa tapauksissa, joissa DHCP-palvelua käytettäisiin, on se ongelma, että reititys välityspalvelimen ohjausyksiköltä tukiaseman tarjoamaan langattomaan lähiverkkoon ei toimi kohdeosoitteenmuunnoksen tapauksessa, sillä ohjausyksikön reititystaulussa ei ole nyt käsin asetettua reittiä tuohon verkkoon. Reititys voidaan kuitenkin kierrättää ohjausyksikön yhdyskäytävän kautta, koska DHCP-palvelua käytettäessä ohjausyksikkö saa yhdyskäytävän IP-osoitteen DHCP-palvelimelta, joka toimii asiakasreitittimessä. Yhdyskäytävä on siis välityspalvelimen langattomana asiakkaana toimivan reitittimen Ethernet-sovitin. Tällöin yhdyskäytävänä toimivan reitittimen reititystauluun lisätään reitti siihen verkkoon, jossa oltiin ennen kohdeosoitteenmuunnosta. Tämä verkko löytyy siis tukiasemana toimivan reitittimen takaa. Tällä järjestelyllä TCP-paketti pääsee takaisin. Kuvitellaan nyt, että paketti tulee kohdeosoitteenmuunnoksen kautta välityspalvelimen ohjausyksikölle, joka on saanut DHCP-palvelimelta yhdyskäytäväkseen langattomana asiakkaana toimivan reitittimen Ethernet-sovittimen IP-osoitteen. Tämän reitittimen reititystaulun säännön mukaan sama verkko, jossa paketti oli ennen kohdeosoitteenmuunnosta, löytyy tukiasemana toimivan reitittimen Ethernet-sovittimen IP-osoitteen takaa. Näin reititykseen tulee yksi hyppy lisää, mutta yhteys saadaan toimimaan. Tämän ja viimeiseksi ehdotetun DHCP-asetuksen johdosta välityspalvelimen ohjausyksikössä voidaan käyttää vakiona olevia verkkoasetuksia, joita myös työkoneen ohjausyksiköllä käytetään. Toisin sanoen ohjausyksikön verkkoasetuksia ei

tällöin tarvitse muuttaa lainkaan, jolloin laitteisto- ja verkkoarkkitehtuurin näkökulmasta ainoat asennettavat laitteet ovat reitittimet.

Reititykseen liittyen välityspalvelimen reititystä voitaisiin kehittää vielä siten, että välityspalvelin toimisi langattoman lähiverkon toistimena. Välityspalvelin toimii toistimena tilanteessa, jossa työkone ei yllä tehtaan langattomaan lähiverkkoon, mutta välityspalvelin on näiden kahden välissä siten, että välityspalvelin yltää tehtaan langattomaan lähiverkkoon ja työkone yltää välityspalvelimen tarjoamaan langattomaan lähiverkkoon. Näin työkoneelta voisi olla suora ja reaaliaikainen yhteys välityspalvelimen verkon kautta tehtaan langattomaan lähiverkkoon ja sitä kautta myös REST-palvelimelle. Tällainen toiminnallisuus on periaatteessa jo olemassa, mutta se vaatii rinnalleen tiettyjä ohjelmistoratkaisuja. Nämä ratkaisut ovat lähinnä sellaisia, että työkoneelta tullut data tallennetaan välityspalvelimen ohjausyksikölle, josta se sitten luetaan ja lähetetään heti kohti tehtaan langatonta lähiverkkoa. Teoriassa tällainen järjestelmä ei ole reaaliaikainen, mutta tietyillä ohjelmistoratkaisuilla viive saadaan käytännössä hyvin pieneksi. Oikeana langattoman verkon toistimena välityspalvelin osaisi reitittää datapaketin suoraan tehtaan verkkoon, jolloin tallennusvaihe jäisi kokonaan pois. Paitsi että tällainen järjestely olisi täysin reaaliaikainen, se vähentäisi ohjausyksikön kuormitusta, koska ideaalitilanteessa reitityksen hoitaisivat yksin reitittimet. Koska välityspalvelimen luonteeseen kuuluu sen monipuolinen liikuteltavuus, eikä niinkään paikallaan olo, niin toistinominaisuus ei siten ole tarpeellinen vielä tässä vaiheessa. Muutenkin edellä esitetty tilanne, jossa työkone ei yltäisi tehtaan langattomaan verkkoon ja välityspalvelin yltäisi, on harvinainen. On kuitenkin aiheellista pohtia tällaistakin skenaariota tulevaisuuden varalle.

Yhteenvetona kehitysideoista voidaan todeta, että tuloksena syntyneen järjestelmän asetukset eivät tällä hetkellä häviä lainkaan esitetyille kehitysideoille, sillä kyse on lähinnä yksityiskohdista ja tulevaisuuden mahdollisuuksista. Juuri tulevaisuuden ratkaisuja silmällä pitäen, on hyvä pohtia erilaisia tekniikoita. Edellä esitetyt tulevaisuuden ideat eivät muutenkaan toimi sellaisenaan, vaan ne vaativat sekä teoreettisia että käytännönläheisiä lisätutkimuksia, jotta niitä voidaan alkaa soveltaa.

8 JOHTOPÄÄTÖKSET

Diplomityön tuloksena syntynyt järjestelmä on hyvä pohja tulevaisuuden innovatiivisille ohjelmistoratkaisuille, joita voidaan helposti kehittää järjestelmän TCP/IP-pohjaisuutta hyödyntäen. Tulevaisuudessa järjestelmästä voidaan tehdä esimerkiksi aiemmin mainitun viivesietoisen verkon kaltainen. Se voidaan aluksi räätälöidä tietyn tilanteen vaatimusten mukaisesti tai siitä voidaan tehdä jopa kokonaan yleiskäyttöinen. Kokonaan yleiskäyttöinen järjestelmä vaatii kuitenkin paljon kehitystyötä ja siksi alussa onkin tärkeää testata järjestelmää yksinkertaisemmilla tekniikoilla, kuten esimerkiksi MQTT-protokollalla. Tämä jo senkin takia, että järjestelmän toimintaa saadaan testattua kattavammin diplomityössä käydyn suppean testauksen lisäksi. Yksinkertaiset ja helposti toteutettavat tekniikat ohjelmistokehityksen alkuvaiheessa nopeuttavat myös järjestelmän käyttöönottoa sen luonnollisessa käyttöympäristössä. Testaus olisikin hyvä saada laajennettua toimiston ulkopuolelle, sillä kirjoituspöydän ääressä tehdyt testit eivät aina vastaa tilannetta kentällä.

Laitteisto- ja verkkoarkkitehtuurin näkökulmasta uutta järjestelmää voitaisiin hyvin käyttää muissakin käyttökohteissa kuin kaivosteollisuudessa, joka itsessään on hyvin vaativa kohde. Muita käyttökohteita voisivat olla oikeastaan mitkä tahansa kohteet, joissa internet-yhteyttä ei ole saatavilla, mutta dataa haluttaisiin siitä huolimatta siirtää internetin välityksellä. Vasta tulevaisuudessa nähdään millaiseksi MQTT-protokollan, viivesietoisen verkon ja mahdollisesti muiden protokollien ja tekniikoiden kombinaatioksi tämän diplomityön tuloksena syntynyt järjestelmä kehittyy ja missä kaikkialla sitä tullaan käyttämään.

LÄHDELUETTELO

Anttila, Aki (2001). *TCP/IP-tekniikka.* 2. painos. Helsinki: Helsinki Media. 471 s. ISBN 951-832-061-6.

Ballew, Scott M. (1998). *IP-verkkojen hallinta Ciscon reitittimillä.* 1. painos. Espoo: Suomen Atk-kustannus oy. 343 s. ISBN 951-762-644-4.

Burgess, Dennis (2011). *Learn RouterOS.* 2. painos. Lulu Press. 448 s. ISBN 978-1-105-06959-8.

Discher, Stephen (2011). *RouterOS by Example.* 1. painos. ISP Services. 300 s. ISBN 978-0-615-54704-6.

Dunkels, Adam, Juan Alonso, Thiemo Voigt, Hartmut Ritter & Jochen Schiller (2004). Connecting Wireless Sensornets with TCP/IP Networks. Teoksessa: *Wired/Wireless Internet Communications,* 143–152. Toim. Langendoerfer, Peter, Mingyan Liu, Ibrahim Matta & Vassilis Tsaoussidis. Berliini: Springer-Verlag. International Conference on Wired/Wireless Internet Communications, WWIC 2004, Frankfurt/Oder, Saksa, 4.–6.2.2004. ISBN 978-3-540-24643-5.

Exertus oy (2009). Norsmart Architecture. PowerPoint-esitys alkuperäisen Norsmart-ohjausjärjestelmän arkkitehtuurista.

Exertus oy (2013). Norsmart 3. PowerPoint-esitys uudesta Norsmart 3 -ohjausjärjestelmästä.

Exertus oy (2016). ReDiService Overview [verkkodokumentti]. [Viitattu 4.3.2018]. Tietoa Exertuksen ReDi-palvelusta. Saatavissa: http://www.exertus.fi/files/Tiedostot/TechDoc_ReDiService.pdf

Exertus oy (2017a). MIC1100S Technical Data Sheet [verkkodokumentti]. [Viitattu 4.3.2018]. Tietoa Exertuksen MIC1100S-ohjausyksiköstä. Saatavissa: http://www.exertus.fi/files/Tiedostot/TechDoc_MIC1100S.pdf

Exertus oy (2017b). RD121S2 Technical Data Sheet [verkkodokumentti]. [Viitattu 4.3.2018]. Tietoa Exertuksen RD121S2-näytöstä. Saatavissa: http://www.exertus.fi /files/Tiedostot/TechDoc_RD121S2.pdf

Exertus oy (2017c). RD084S2 Technical Data Sheet [verkkodokumentti]. [Viitattu 4.3.2018]. Tietoa Exertuksen RD084S2-näytöstä. Saatavissa: http://www.exertus.fi /files/Tiedostot/TechDoc_RD084S2.pdf

Exertus oy (2018). Yritys | Exertus [verkkodokumentti]. [Viitattu 4.3.2018]. Tietoa yrityksestä. Saatavissa: http://www.exertus.fi/?lang=fi&id=127&page=Yritys

Fall, Kevin (2003). A Delay-Tolerant Network Architecture for Challenged Internets. Teoksessa: *SIGCOMM '03: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 27–34. Toim. Feldmann, Anja, Martina Zitterbart, Jon Crowcroft & David Wetherall. New York: ACM. SIGCOMM Conference 2003, Karlsruhe, Saksa, 25.–29.8.2003. ISBN 1-58113-735-4.

Gastón, Hillar C. (2017). *MQTT Essentials - A Lightweight IoT Protocol.* 1. painos. Packt Publishing. 280 s. ISBN 978-1-78728-781-5.

Gheorghe, Lucian (2006). *Designing and Implementing Linux Firewalls with QoS using netfilter, iproute2, NAT, and L7-filter.* 1. painos. Packt Publishing. 278 s. ISBN 1-904811-65-5.

Granlund, Kaj (2007). *Tietoliikenne.* 1. painos. Jyväskylä: Docendo oy. 487 s. ISBN 978-951-0-32821-7.

Hakala, Mika & Mika Vainio (2005). *Tietoverkon rakentaminen.* 1. painos. Jyväskylä: Docendo oy. 428 s. ISBN 951-846-263-1.

Hassan, Qusay F., Atta ur Rehman Khan & Sajjad A. Madani (2018). *Internet of Things. Challenges, Advances, and Applications.* 1. painos. CRC Press. 436 s. ISBN 978-1-4987-7851-0.

Internet Assigned Numbers Authority (2017). IANA IPv4 Special-Purpose Address Registry [verkkodokumentti]. [Viitattu 27.3.2018]. Saatavissa: https://www.iana.org /assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

Järvinen, Petteri (2003). *IT-tietosanakirja.* 1. painos. Jyväskylä: Docendo oy. 844 s. ISBN 951-846-184-8.

Kaario, Kimmo (2002). *TCP/IP-verkot.* 1. painos. Jyväskylä: Docendo oy. 396 s. ISBN 951-846-107-4.

Korotkevitch, Dmitri (2016). *Pro SQL Server Internals.* 2. painos. Apress. 830 s. ISBN 978-1-4842-1963-8.

LaCroix, Jay (2015). *Mastering Linux Network Administration.* 1. painos. Packt Publishing. 260 s. ISBN 978-1-78439-959-7.

Maniktala, Sanjaya (2013). *Power over Ethernet Interoperability.* 1. painos. McGraw-Hill. 480 s. ISBN 978-0-07-179826-6.

Massé, Mark (2011). *REST API Design Rulebook.* 1. painos. O'Reilly Media. 116 s. ISBN 978-1-449-31050-9.

Mikrotik (2007). Telnet Server and Client [verkkodokumentti]. [Viitattu 17.3.2018]. Tietoa Telnet-ohjelman käytöstä Mikrotik-reitittimessä. Saatavissa: https://mikrotik.com/testdocs/ros/3.0/admin/telnet.pdf

Mikrotik (2012). Manual:Webfig [verkkodokumentti]. [Viitattu 17.3.2018]. Tietoa selainpohjaisesta Webfig-ohjelmasta ja sen käytöstä. Saatavissa: https://wiki.mikrotik.com/wiki/Manual:Webfig

Mikrotik (2017a). Metal [verkkodokumentti]. [Viitattu 17.3.2018]. Yleistä tietoa Mikrotik Metal-reitittimestä. Saatavissa: https://i.mt.lv/routerboard/files/metal2-171002090102.pdf

Mikrotik (2017b). Tips and Tricks for Beginners and Experienced Users of RouterOS: Basic router protection based on connection state and IP address type by using Firewall [verkkodokumentti]. [Viitattu 25.3.2018]. Saatavissa: https://wiki.mikrotik.com/wiki/Tips_and_Tricks_for_Beginners_and_Experienced_Users_of_RouterOS#Basic_router_protection_based_on_connection_state_and_IP_address_type_by_using_Firewall

Mikrotik (2017c). Manual:Securing Your Router [verkkodokumentti]. [Viitattu 19.4.2018]. Ohjeita Mikrotik-reitittimen tietoturvan kehittämiseen. Saatavissa: https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

Mikrotik (2018). Manual:Winbox [verkkodokumentti]. [Viitattu 17.3.2018]. Tietoa Winbox-ohjelmasta ja sen käytöstä. Saatavissa: https://wiki.mikrotik.com/wiki/Manual:Winbox

Syrjänen, Seppo (2007). *Viivesietoisten verkkojen nykytila ja tulevaisuuden haasteet.* Helsingin yliopisto. Tietojenkäsittelytieteen laitos. Pro Gradu -tutkielma.

Ulz, Thomas, Thomas Pieber, Christian Steger, Sarah Haas & Rainer Matischek (2017). Sneakernet on Wheels: Trustworthy NFC-based Robot to Machine Communication. Teoksessa: *2017 IEEE International Conference on RFID Technology Application (RFID-TA),* 260–265. IEEE. International Conference on RFID Technology and Applications, RFID-TA 2017, Varsova, Puola, 20.–22.9.2017. ISBN: 978-1-5386-1833-2.

Viestintävirasto (2018). Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä [verkkodokumentti]. [Viitattu 18.3.2018]. Saatavissa: https://www.viestintavirasto.fi/attachments/maaraykset/Maarays_15AM.pdf

Williams, Edmund A., Graham A. Jones, David H. Layer & Thomas G. Osenkowsky (2007). *National Association of Broadcasters Engineering Handbook.* 10. painos. Focal Press. 2120 s. ISBN 978-0-240-80751-5.

Yellavula, Naren (2017). *Building RESTful Web Services with Go.* 1. painos. Packt Publishing. 316 s. ISBN 978-1-78829-428-7.