Oscar Ojala

Tehtaan aliverkon suunnittelu ja toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

16.11.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Oscar Ojala Tehtaan aliverkon suunnittelu ja toteutus 46 sivua + 7 liitettä 16.11.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Marko Uusitalo Toni Virta, IT-insinööri

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa SSAB Europen Hämeenlinnan yksikön elvyttämöalueelle uusi aliverkko. Työssä paneuduttiin verkon keskeisimpiin käsitteisiin verkkosuunnittelussa sekä verkon arkkitehtuurissa. Lisäksi työssä paneuduttiin verkon suunnitteluun liittyvään dokumentointiin.

Työ aloitettiin verkon kartoituksella, josta siirryttiin laiteselvitysten kautta verkon uudelleenkartoitukseen. Näiden vaiheiden jälkeen laadittiin suunnitelma, jonka pohjalta siirryttiin verkon fyysiseen toteutukseen.

Rajatun aikataulun sekä tehdastuotannon vaatimusten takia opinnäytetyötä ei voitu suorittaa loppuun. Puuttumaan jäivät verkkolaitteiden IP-muunnokset vanhasta aliverkosta toiseen sekä käytännön verkkotestaus. Työn lopputuloksena kuitenkin syntyi suunnitelma, jonka pohjalta SSAB Europen henkilöstö voi suorittaa verkon toteutuksen loppuun.

Avainsanat	Tietoverkko, Dokumentointi, Cisco, SSAB, OSI, TCP, IP

Author(s) Title Number of Pages Date	Oscar Ojala Implementation and design of a subnetwork on the factory premises 46 pages + 7 appendices 16 Nov 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Marko Uusitalo, Senior Lecturer Toni Virta, IT Engineer

The objective of this thesis was to design and implement a subnetwork for one of the SSAB Europe's manufacturing sites in Hämeenlinna. The thesis covers the most important concepts of the network in relation to network design and network architecture. In addition to this, the thesis delved into network planning regarding documentation.

The thesis started off by mapping the network. After that, the objective was to locate the missing devices within the network. The next task consisted of composing a plan, which would help in the implementation of the new subnetwork.

Due to the limited time frame of the project as well as the production demands, the thesis could not be finished in time. The plan was to make a migration from the old subnetwork to the new subnetwork along with testing the network. However, because of this work, a plan was devised to amend the incomplete thesis, which acts as a basis for the SSAB staff to accomplish the remaining tasks to finish the implementation.

Keywords	Network, Documentation, Cisco, SSAB, OSI, TCP, IP

Sisällys

Lyhenteet ja termit

ACL	Access Control List tarkoittaa pääsylistaa, jonka avulla voidaan rajoittaa tai sallia verkkoliikennettä aktiivilaitteella.
BPDU	Bridge Protocol Data Unit tarkoittaa kehystä, joka sisältää tietoa Spanning Tree Protocol:sta.
DHCP	Dynamic Host Configuration Protocol tarkoittaa automatisoitua verkko-asetusten jakoa.
DNS	Domain Name System on Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
EIGRP	Enhanced Interior Gateway Routing Protocol on Ciscon kaupallinen reititysprotokolla.
Ethernet	Pakettipohjainen lähiverkkoratkaisu.
Frame Relay	Alueverkkotekniikka, jolla yhdistetään lähiverkkoja toisiinsa.
HDLC	High-Level Data Link Control tarkoittaa synkronista tietoliikenneprotokollaa, joka siirtää bittimuotoista data sarjalinkkien yli.
HSRP	Hot Standby Router Protocol on verkon vikasietoisuutta lisäävä protokolla.
ICMP	Internet Control Message Protocol on virheraportointiprotokolla, jonka avulla verkossa toimivat laitteet voivat raportoida Internet Protokolla -pakettien virheellisestä lähetyksestä.
IGRP	Interior Gateway Routing Protocol on etäisyysvektoriprotokolla, joka on EIGRP:n edeltäjä.
IP	Internet Protocol huolehtii pakettikytkentäisessä verkossa tietoliikennepakettien perille pääsemisestä.

IPAM	IP Address Management on hallintajärjestelmä, jonka avulla voi hallita lähiverkon IP-osoitteita.
IPv4	Internet Protocol version 4 on neljäs versio Internet Protokollasta.
IPv6	Internet Protocol version 6 on kuudes versio Internet Protokollasta.
IPX	Interwork Packet Exchange on verkkoprotokolla Novellilta.
ISL	Cisco Inter-Switch Link on Ciscon suljettu protokolla, joka ylläpitää VLAN-informaatiota Ethernet-kehyksien avulla.
LAN	Local Area Network tarkoittaa maantieteellisesti rajoitetulla alueella toimivaa tietoliikenneverkkoa.
MAC	Media Access Control Address tarkoittaa verkkosovittimen Ethernet-verkossa yksilöivää osoitetta.
MAN	Metropolitan Area Network. Yhden tai useamman kaupungin alueella toimiva tietoliikenneverkko.
NetBIOS	Network Basic Input/Output System on ohjelma, jonka avulla erilaiset tietokoneet voivat kommunikoida keskenään lähiverkossa.
NTP	Network Time Protocol on täsmällinen aikatiedon välittämisprotokolla tietokoneiden välillä.
OSI-malli	Open System Interconnection Reference Model kuvaa tiedonsiirtoprotokollien hierarkkista kokonaisuutta kerrosesityksenä.
OSPF	Open Shortest Path First on avoimiin standardeihin perustuva reitityksprotokolla.
Ping	TCP/IP-protokollan työkalu, joka kokeilee määrätyn laitteen saatavuutta ICMP-paketin avulla.

PPP	Point-to-Point Protocol on digitaalisessa tiedonsiirrossa käytetty suoran yhteyden muodostava protokolla.
PVST+	Per VLAN Spanning Tree Plus on Ciscon kehittämä suljettu Spanning Tree -protokolla.
RFC	IETF-organisaation julkaisema Internetiä koskeva standardi.
RIP	Routing Information Protocol on reititysprotokolla, joka perustuu verkossa tapahtuviin ”hyppymäärien” laskemiseen.
SDH	Synchronous Digital Hierarchy on synkronoituun tiedonsiirtoon käytetty standardi, joka perustuu kaikkien laitteiden samanaikaiseen tahdistukseen.
SNMP	Simple Network Management Protocol on TCP/IP-verkoissa käytetty verkkojen hallintaan soveltuva tietoliikenneprotokolla.
SPX	Sequenced Packet Exchange on käyttäjä/palvelin-ympäristössä toimiva kuljetusprotokolla.
SSH	Secure Shell on salattuun tietoliikenteeseen tarkoitettu protokolla, jonka avulla käyttäjä voi ottaa turvallisen etäyhteyden laitteisiin.
STP	Spanning Tree Protocol on verkkoprotokolla, jonka tarkoituksena on muodostaa “silmukkavapaita” verkkoja.
TCP	Transmission Control Protocol on tietoliikenneprotokolla, joka muodostaa yhteyksiä laitteiden välille.
TCP/IP	Transmission Control Protocol/Internet Protocol on Internetin arkkitehtuurin kuvaamiseen tarkoitettu tietoliikenneverkkojen malli.
Telnet	Yksinkertainen yhteysprotokolla, jonka avulla voi muodostaa etäyhteyksiä laitteisiin.
Token Ring	Valtuudenvälitysverkko, jossa tietoa hallitaan valtuuden kierrättämisellä.

UDP	User Datagram Protocol on tiedonsiirtoon tarkoitettu yhteydetön protokolla.
WAN	Wide Area Network on laajaverkko, joka peittää suuria maantieteellisiä alueita.
WDM	Wavelength Division Multiplexing on kuituliikenteessä käytetty teknologia, jossa siirtoyhteydet jaetaan samassa kuidussa usealle eri aallonpituudelle.
VLAN	Virtual Local Area Network on tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa useampaan loogiseen osaan.
VLSM	Variable-Length Subnet Mask tarkoittaa tekniikkaa, jonka avulla aliverkot voidaan jakaa pienempiin osakokonaisuuksiin.
VOIP	Voice Over Internet Protocol on tekniikka, jonka avulla ääntä voidaan siirtää reaaliaikaisesti IP-protokollan avulla tietoliikenneverkossa.

1 Johdanto

SSAB Oy on vuonna 1918 perustettu ruotsalainen teollisuuskonserni, joka toimii maailmanlaajuisesti 45 maassa. SSAB:n tuoteperheeseen kuuluu pitkälle kehitettyjä terästuotteita, esimerkiksi nauha-, levy- ja putkituotteita sekä erilaisia rakennusratkaisuja. Vuonna 2014 SSAB yhdistyi suomalaisen Rautaruukki Oyj:n kanssa, ja yhteensä yrityksellä on noin 17 300 työntekijää. Yhtiön pääkonttori sijaitsee Tukholmassa. [1.]

Kuva 1. SSAB Europe Hämeenlinnan tehdas [2.]

Tämän opinnäytetyön tavoitteena on uudistaa SSAB Oy:n Hämeenlinnan tehtaan elvyttämöalueen aliverkko. Alueeseen kuuluu elvyttämö, jossa regeneroidaan suolahappoa erinäisiin teräsprosesseihin. Lisäksi alueella on rakennuskunnossapidon yksikkö, sekä tehtaan vedenpuhdistamo. Opinnäytetyössäni tulen kertomaan projektin eri vaiheista, toimintatavoista sekä ratkaisuista, joiden avulla päädyin lopputilanteeseen.

Aloitin opinnäytetyöni keväällä 2015 toisen harjoitteluni ohella. Työssäni pääsin tutustumaan lähietäisyydeltä erilaisiin teräsalan toimintaprosesseihin sekä tehdasympäristön moniin haasteisiin verkkosuunnittelun näkökulmasta.

Työn alkuvaiheet käsittelevät alkuperäisen verkkotopologian kartoitusta tehdasalueella ja eri laitteiden paikantamista. Tämän jälkeen käyn läpi käytännön toteutuksen kautta kytkimien konfiguraatioita ja *on-site* -asennusta. Lopuksi esitellään suunnitelma lopullisesta toteutuksesta vanhan tehdasverkon tilalle. Näiden lisäksi työssä käydään läpi teoriatasolla aiheita tietoverkoista ja siihen liittyvästä suunnittelusta.

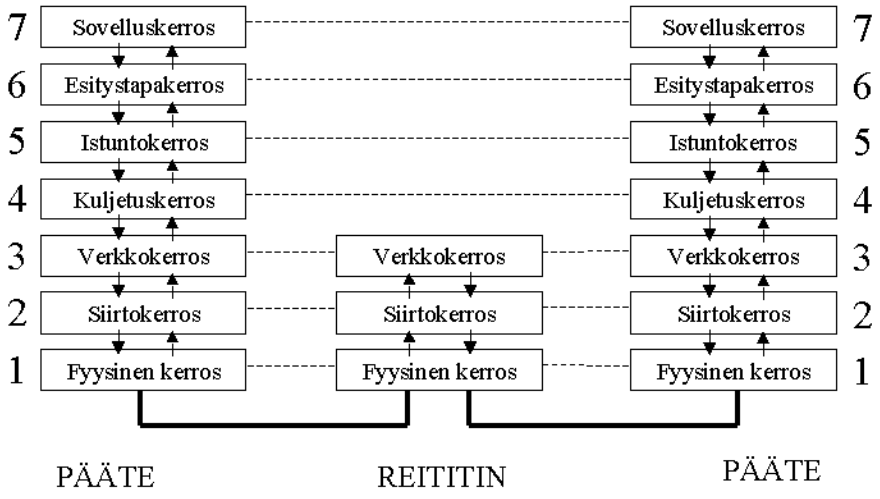
2 Teoria

Tietoverkko määritellään ympäristöksi, jossa kaksi tai useampia laitteita on yhteydessä toisiinsa vaihtaakseen tietoa, kuvaa tai ääntä keskenään. Verkon tiedonsiirtoprotokollia kuvattaessa käytetään viitemallina OSI-mallia, joka kuvaa seitsemässä kerroksessa tietoliikenteen rakenteen, sekä TCP/IP-viitemallia, joka muistuttaa läheisesti edellä mainittua neljässä kerroksessa.

2.1 OSI

OSI *Open Systems Interconnection Reference Model* on ISO:n standardi siitä, miten järjestelmät ovat avoimesti toisiinsa liitettävissä. OSI-malli syntyi alun perin 1970-luvun puolivälissä Honeywell Information Systemsin ryhmän työn pohjalta, kunnes muutamien välivaiheiden jälkeen vuonna 1979 malli sai standardin aseman.

OSI-mallissa tietoliikenneohjelmistot on jaettu seitsemään osaan: neljään yläkerrokseen ja kolmeen alakerrokseen. Periaatteena on, että kerroksen tehtävät on määritelty, mutta toteutustapa on jätetty avoimeksi. Kerroksella on määritelty rajapinta, jonka kautta se kommunikoi ylempien tai alempien kerrosten kanssa. Esimerkiksi kerros voi ottaa vastaan käskyn ylemmältä kerrokselta muodostaa yhteys, jolloin se voi käskeä alempaa kerrosta toimimaan rajanpintansa avulla. Lopuksi alemmilta tasoilta annetaan vahvistus yhteyden muodostamisesta. [3, s. 458.]



Kuva 2. OSI-mallin mukainen rakennekaavio [4.]

Vaikka kuvan 2 mukaisia verkkoja ei käytännössä ole, se auttaa ymmärtämään niiden tehtäviä laitteiden välille muodostetussa avoimessa järjestelmässä. Malli toimii ylläpitohenkilöiden apuna mm. tietoliikennejärjestelmän vikatilanteissa, jolloin vian etsimisestä tulee järjestelmällistä.

Fyysinen kerros

Fyysinen kerros (*physical layer*) on viitemallin alin kerros. Se määrittelee kaapelointiin ja signaalinsiirtoon liittyvät arvot. Tyypillisiä määrityksiä ovat esimerkiksi käytettävät liitin- ja kaapelityypit, signaalien jännitetasot ja vaimennus. Lisäksi, johtokoodaus (*encoding*) kuuluu fyysisen kerroksen tehtäviin. Johtokoodauksessa lähetettävät bitit muunnetaan erilaisiin signaalimuotoihin. Verkon aktiivilaitteista toistimet, mediamuuntimet ja keskittimet kuuluvat fyysisen kerroksen laitteisiin. [5, s. 139.]

Siirtoyhteyskerros

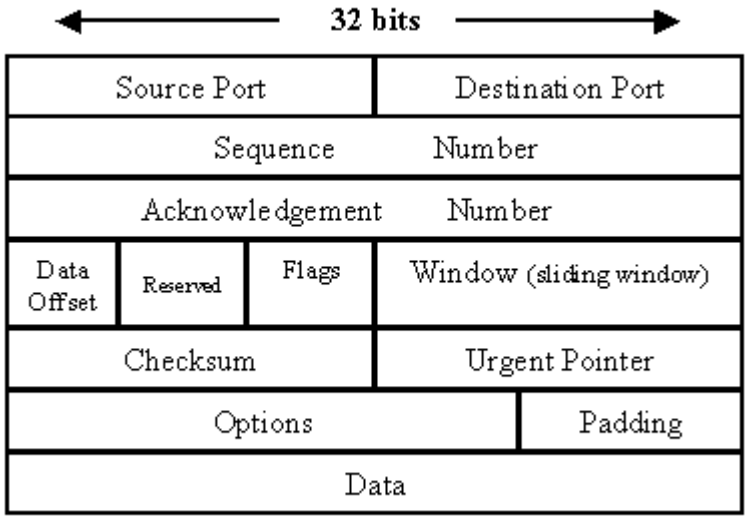
Siirtoyhteyskerros (*data link layer*) määrittelee, miten lähetettävästä datasta muodostetaan kaapelointijärjestelmässä siirrettäviä yksiköitä, kuten kehyksiä tai soluja. Kerroksen tehtävänä on määritellä lähettävän ja vastaanottavan laitteen fyysiset MAC-osoitteet (*Media Access Control*). Lähiverkoissa käytettävät *Ethernet*- ja *Token Ring* -kehysmääritykset ovat siirtoyhteyskerroksen keskeisiä käsitteitä. Siirtoyhteyskerroksella kytkin osaa lukea *Ethernet*-protokollasta laitteiden MAC-osoitteet ja ohjata paketit oikeisiin fyysisiin laiteportteihin osoitteen perusteella. Laajaverkoissa vastaavasti käytettäviä protokollia ovat mm. PPP (*Point-to-Point Protocol*) ja HDLC (*High Level Data Link Control Protocol*), sekä *Frame Relay*. Verkon tärkeimpiin siirtoyhteyskerroksen aktiivilaitteisiin kuuluvat kytkimet, sillat sekä verkkokortit. Näistä aktiivilaitteista puhuttaessa on hyvä tietää, että ne toimivat myös fyysisellä kerroksella. [5, s. 139]

Verkkokerros

Verkkokerros (*Network layer*) määrittelee pakettien reitityksen verkoissa sekä liikennemuotojen priorisoinnin. Verkkokerroksen keskeisin aktiivilaite on reititin. Tehtävien suorittamiseen käytetään yleisimmin IP-protokollaa (*Internet Protocol*) sekä vanhemmissa järjestelmissä Novellin IPX-protokollaa (*Interwork Packet eXchange*). Vaikka reitittimet toimivat verkkokerroksella, suorittavat ne myös fyysisen ja siirtoyhteyskerroksen tehtäviä. [5, s. 139.]

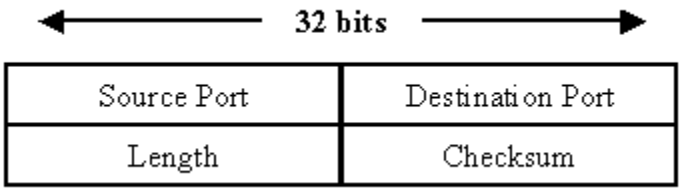
Kuljetuskerros

Kuljetuskerroksen (*transport layer*) tehtävä on reitittää luotettavalla tavalla paketti alkupisteestä loppupisteeseen. Näistä tehtävistä huolehtivat kuljetusprotokollat, kuten TCP (*Transmission Control Protocol*), SPX (*Sequential Packet Exchange*) sekä NetBIOS. Edellä mainittujen protokollien tehtävänä on pilkkoa sovellusten lähettämä datavirta segmenteiksi tai paketeiksi. Lisäksi, kuljetusprotokollien tehtävä on huolehtia yhteyden muodostamisesta ja purkamisesta ohjelmistojen välillä sekä varmistaa lähetetyn datan perille saapuminen kuittauksella (*acknowledgement*) [ks. Kuva 3]. Näiden metodien lisäksi, pakettikoon määritys mukaan lukien, muodostaa tehtäväkokonaisuuden, jota kutsutaan vuonohjaukseksi (*flow control*). [5, s. 139 – 140.]



Kuva 3. TCP-paketin rakenne [6.]

Edellä mainittujen kuljetusprotokollien lisäksi kuljetuskerroksella toimii UDP (*User Datagram Protocol*), jonka tehtävänä on datavirran pilkkominen osiin, mutta se ei ota kantaa muuhun vuonohjaukseen. Tällaista protokollaa kutsutaan yhteydettömäksi protokollaksi. [5, s. 140.] UDP ei kuitenkaan varmista paketin saapumista perille ja tästä syystä pakettien saapumisjärjestys saattaa erota alkuperäisestä järjestyksestä. UDP:n tarkistussummakenttä (*checksum*) kuitenkin mahdollistaa tarkistuksen datan eheydestä [ks. Kuva 4]. UDP:n yleisimpiä palveluita ja protokollia verkossa ovat esimerkiksi nimipalvelu (DNS), aikapalvelu (NTP) sekä dynaaminen IP-osoitteiden jakeluun keskittyvä DHCP-protokolla.



Kuva 4. UDP-paketin rakenne [6.]

Istuntokerros

Istuntokerroksen (*session layer*) tehtäviin kuuluu istunnon ylläpito laitteistojen välillä verkon ylitse. Ylläpitoon kuuluu yhteyden rakentaminen, hallinnointi ja sulkeminen. Mikäli istunto päättyy, esimerkiksi verkkovian takia, istuntokerros mahdollistaa yhteyden palauttamisen ja jatkamisen siitä, mihin ennen vikaa jäätiin (*checkpointing*). [4.]

Esitystapakerros

Esitystapakerros (*presentation layer*) määrittelee, missä muodossa kahden päätelaitteen välinen niin sanottu sanomaliikenne tapahtuu. Kerroksella määritellään erilaisten koodausjärjestelmien avulla, kuinka binäärimerkkijonoina (*binary string*) lähetettävä tieto koodataan (*encode*) ja dekoodataan (*decode*) takaisin alkuperäiseen tietotyyppiin vastaanottavassa sovelluksessa. Nykyisissä lähiverkkojärjestelmissä esitystapakerroksen tehtävistä huolehtii pääasiassa itse käyttöjärjestelmä. [5, s. 140.]

Sovelluskerros

Sovelluskerros (*application layer*) määrittelee sovellusten ja käyttöjärjestelmien toiminnasta ne osat, joita alemmissa kerroksissa ei ole määritelty. Nykyisissä lähiverkkojen sovelluksissa sekä käyttöjärjestelmissä sovellus-, esitystapa- ja istuntokerrosten erottaminen toisistaan ei ole mahdollista, vaan niistä muodostuu ohjelmallinen kokonaisuus. [5, s. 140 – 141.] Sovelluskerros poikkeaa muista kerroksista siinä, että sen ei tarvitse tarjota palveluita ylemmille kerroksille, vaan toimii viimeisenä rajapintana sovelluksen ja tiedonsiirron välillä.

2.2 TCP/IP

TCP/IP-protokollapino on verkon arkkitehtuurin kuvaamisessa käytetty tietoliikenneverkkojen viitemalli. Nimensä TCP/IP on saanut sen kahden pääprotokollan mukaan, TCP:n ja IP:n. Viitemalli voidaan jakaa käyttötarkoituksensa mukaan viiteen kerrokseen: fyysiseen kerrokseen, linkkikerrokseen, verkkokerrokseen, kuljetuskerrokseen ja sovelluskerrokseen. [7.]

OSI-viitemallin tavoin ylemmän protokollan tasot käyttävät alempaa tasoa ja rinnakkaiset tasot ovat keskenään loogisesti yhteydessä toisiinsa. Ylemmän kuljetuskerroksen protokollana toimii TCP ja alemmalla verkkokerroksella IP. Myös yhteydetöntä UDP:ta on mahdollista käyttää kuljetuskerroksella TCP:n kanssa.

TCP/IP-protokollapinon kahdella alimmalla kerroksella, fyysisellä ja siirtokerroksella ei toimintoja varsinaisesti määritellä, vaan niiltä oletetaan tiettyjä asioita, joita esimerkiksi Ethernet-standardit toteuttavat. [8, s. 22.] Protokollapinosta puhuttaessa varsinainen kerrostoiminta alkaa määrittelyineen verkkokerrokselta.

Taulukko 1. TCP/IP-protokollakerrosten vertailu OSI-viitemalliin

OSI	TCP/IP
Sovelluskerros	Sovelluskerros
Esitystapakerros	
Istuntokerros	
Kuljetuskerros	Kuljetuskerros
Verkkokerros	Verkkokerros
Siirtokerros	Siirto- ja fyysinen kerros
Fyysinen kerros	

Kuten taulukosta 1 nähdään, protokollapinon kaksi alinta kerrosta on yhdistetty yhdeksi kokonaisuudeksi, sillä TCP/IP-verkoissa IP-kerroksen (verkkokerroksen) alla voi periaatteessa toimia mikä verkkotekniikka tahansa. Eri verkkotekniikoiden tapauksessa TCP/IP-protokollapinon alimmat kerrokset voivat siis koostua vaikka kuinka useasta protokollakerroksesta. [8, s. 22.]

OSI-mallin tavoin protokollapinon kuljetuskerroksella toimii sekä UDP että TCP. Näistä kahdesta jälkimmäistä käyttävät sovellukset näkevät verkon loogisina yhteyksinä. Jotta tällainen yhteys saadaan muodostettua, tarvitaan soketteja eli IP-osoitteen ja porttinumeron muodostamia kokonaisuuksia. Porttinumeron avulla ylemmän kerroksen sovellusprosessi pystyy välittämään datan oikeaan IP-osoitteeseen. Porttinumeron tarkoituksena on siis määritellä sovelluskerroksen ja TCP:n tai UDP:n välinen osoitteistuksen määritys. TCP:n tehtäväksi jää sokettiparien, eli lähde ja kohde sokettien välisen liikenteen korjaus ja ylläpito.

2.3 IP-protokolla

Internet Protocol (IP) on TCP/IP-mallin tärkein protokolla. IP-kerroksen alapuolella sijaitsevilla kerroksilla voidaan käyttää melkein mitä tahansa tiedon siirtämiseen soveltuvaa protokollaa ja IP-kerroksen yläpuolella olevalla kuljetuskerroksella voidaan käyttää erilaisia kuljetusprotokollia. Toisin sanoen IP tarjoaa muille protokollille rajapinnan, jonka avulla voidaan rakentaa toimiva tietoverkko. [8, s. 43.] IP ei sisällä tarkistusmekanismeja, joiden avulla voitaisiin tarkistaa paketin saapuminen loppupisteeseen, tästä syystä paketin kulkureitillä ei ole väliä. IP:tä onkin kutsuttu tästä syystä niin sanotuksi yhteydettömäksi protokollaksi.

Internet-protokollan tärkeimpänä ominaisuutena pidetään IP-osoitteita. Jokaisella Internetiin kytketyllä laitteella täytyy olla uniikki osoitteensa. Vaikka laitteilla onkin laitevalmistajasta riippuen tietty Mac-osoite, ei se kuitenkaan yksittäisenä ominaisuutena ole kovinkaan luotettava. IP-osoitteen avulla liikenne voidaan ohjata oikeisiin verkon segmentteihin. Voidaan ajatella, että MAC-osoite vastaisi oikeassa elämässä katuosoitetta ja vastaavasti IP-osoite vastaisi postinumeroa. Näiden kahden tiedon perusteella postinjakelukeskuksessa osattaisiin ohjata kirje oikeaan kaupunkiin ja edelleen oikealle kadulle. Vastaavasti, ilman postinumeroa kirje saattaisi päätyä väärään kaupunkiin. [8, s. 53.]

IPv4

IPv4 osoite muodostuu neljästä tavusta eli 32 peräkkäisestä bitistä, joiden arvo on 1 tai 0 riippuen tavun numeraalisesta arvosta. IPv4-osoitteet ilmoitetaan normaalisti desimaalimuodossa, jolloin osoitteiden lukeminen on helpompaa. Desimaalimuotoisessa osoitteiden ilmaisussa jokainen tavu erotetaan toisistaan pisteillä, jolloin jokaiseen oktettiin

jää kahdeksalle bitille arvo, jonka yhteenlaskettu summa voi olla välillä 0…255. IP-osoitteet jaetaan myös kahteen osaan, joista ensimmäinen on verkko-osa ja toinen on laiteosa. Internet-liikenteessä verkon tunniste on tärkeimmässä asemassa. Internetissä kulkeva liikenne on pääasiassa verkkojen välistä liikennettä, jolloin tärkeintä on oikean verkon löytyminen lukuisista osaverkoista.

Taulukko 2. IPv4-osoitteen rakenne

IPv4-osoite	172	16	254	1
Bittijono	10101100	00010000	11111110	00000001
Bittien laskutoimitus	128+0+32+0+8+4+0+0	0+0+0+16+0+0+0+0	128+64+32+16+8+4+2+0	0+0+0+0+0+0+0+1
1 tavu = 8 bittiä				

Taulukosta 2 nähdään, kuinka bittijonona ilmoitettu osoite voidaan muuntaa esimerkkiosoitteeksi 172.16.254.1. Jokainen bittijonossa ilmoitettu ykkönen muunnetaan vastaavaksi arvoksi ja lopuksi summataan yhteen, jolloin lopputuloksena saadaan desimaalimuodossa ilmoitettu osoite.

Koko IPv4-osoiteavaruus on jaettu neljään eri luokkaan A-E kokonsa puolesta 16 miljoonasta osoitteesta aina pienempiin C-luokan osoitteisiin, joita on 254. Oheisessa taulukossa 3 on esitelty nämä osoiteluokat koko IPv4-avaruudessa.

Taulukko 3. Osoiteluokat IPv4-avaruudessa

Osoiteluokat		
Luokka	Osoitealue	Koneiden määrä/verkko
A	000.000.000.000-127.255.255.255	16 miljoonaa
B	128.000.000.000-191.255.255.255	65 534
C	192.000.000.000-223.255.255.255	254
D	224.000.000.000-239.255.255.255	Multicast-osoitteet
E	240.000.000.000-255.255.255.255	Kokeilut

IP-protokollan elinkaaren alkuaikoina IP-osoitteiden ryhmittely tapahtui taulukon 3 mukaisesti. Luokittelun alkuvaiheessa käytössä oli vain luokan A osoitteisto, sillä oletuksena oli, ettei osoitteita tarvitsisi käyttää kuin muutaman suuren verkon käyttöön. Luokan A osoitteisto alkaa 0-bitillä, jota seuraa 7 bittiä verkon osoitteille ja 24 bittiä laitteiden käyttöön, eli kokonaisuudessaan osoitteen pituus on 32 bittiä. Paikallisten verkkojen yleistyessä otettiin käyttöön B- ja C-luokan osoitteet, joista C-luokka oli varattu pienille verkoille

ja B-luokka verkon keskisuurille verkoille. Nykyään osoitteiden luokittelu kuitenkin tapahtuu jakamalla verkon pienempiin aliverkkoihin verkkopeitteen avulla.

Aliverkko

Nykyaikaisissa TCP/IP-verkoissa käytetään IP-osoitteen rinnalla ns. verkkopeitettä (*netmask*), joka määrittelee, mikä osa osoitteen biteistä kuuluu verkolle ja mitkä puolestaan laitteille. Peitteen avulla verkko- ja koneosoitteiden välinen raja voidaan sijoittaa mihin tahansa. Tällaista osoitteiden jakamista kutsutaan luokattomaksi IP-osoitteistukseksi. Tämä mahdollista suurten osoitekokonaisuuksien jakamisen pienemmiksi verkoiksi, eli aliverkotukseksi, ja pienten osoitekokonaisuuksien yhdistämisen suuremmiksi verkoiksi eli yliverkotukseksi. Osoiteluokkia hyödyntämällä organisaatiot voivat jaotella esimerkiksi B-luokan osoiteavaruuden, suuren kokonaisuuden pienemmiksi lohkoiksi sopimaan toimipisteensä tarpeisiin. Tästä syystä lähiverkossa on käytössä useampiakin osoitepeitteitä, jolloin menetelmää kutsutaan nimellä VLSM (*Variable Length Subnet Masking*). [5, s. 195.]

2.4 IPv6

IPv4 osoitteiden loppuminen on asettanut haasteen nykypäivän yhteiskunnalle. Vuonna 1992 yleistynyt Internetin käyttö on aiheuttanut IPv4 osoiteavaruuden tyrehtymisen, eikä uusia julkisia osoitteita enää jakelevalta taholta juurikaan julkaista. Vuonna 1994 ongelmaan ryhdyttiin kehittelemään ratkaisua IETF:n (*Internet Engineering Task Force*) toimesta. Tuloksena syntyi uusi Internet-protokolla, joka nykyisin tunnetaan nimellä IPv6. Ensimmäinen versio uudesta *protokollasta* julkaistiin vuonna 1995, ja se sisällytti vain muutamia parannuksia IPv4-protokollaan nähden, joista tärkeimpänä pidettiin laajennettua osoiteavaruutta. Muita merkittäviä parannuksia protokollaan olivat muun muassa yksinkertaistettu otsikko.

IPv6:n kehitys

Yritysmaailman negatiivinen asenne IPv6-protokollaa kohtaan on kuitenkin hidastanut kehitystyötä. Lisäkustannuksia aiheuttava migraatio IPv4 verkosta IPv6 verkkoon ei ole houkutteleva vaihtoehto päättäjien mielessä, sillä miksi muuttaa jotain, mikä toimii, ja riskeerata siten koko verkon toiminta. Lisäksi välittömän hyödyn vastine rahalle ei ole välittömästi havaittavissa siirryttäessä IPv6-verkkoon, eikä näin ollen ole näennäisesti järkevää resurssien käyttöä. Tulevaisuudessa kuitenkin IPv6:n käyttöönotto on välttämätön, sillä yhä pienempien laitteiden kommunikoidessa verkon yli asettaa se vaatimuksen laajemmalle osoiteavaruudelle ja näin ollen ajaa yrityksen väistämättä pois IPv4:n käytöstä. Näin ollen on vain ajan kysymys, milloin yritykset siirtyvät uudempaan protokollaan. Toisena hidastavana tekijänä on universaalisti pidetty uusia tehokkaita tapoja säästää osoitteita IPv4-ympäristössä. Muun muassa NAT, CIDR ja DHCP ovat olleet suurimmassa roolissa. NAT osoitteenmuunnos mahdollistaa useiden laitteiden samanaikaisen yhden julkisen osoitteen käytön ja näin ollen sisällyttää sisäänsä monia laitteita, jotka muutoin tarvitsisivat useita osoitteita. DHCP taas mahdollistaa julkisten osoitteiden vuokraamisen niitä tarvitseville isäntälaitteille määräaikaisella sopimuksella. Tämä tekniikka kierrättää osoitteita, jolloin käyttämättömien osoitteiden ”hukkaaminen” vähenee. Luokattoman reitityksen ansiosta luokkiin perustuva IP-allokaatio vähenee, jolloin julkisten IP-osoitteiden jakelu muuntautuu vähemmän osoitetilaa vieväksi toimintatavaksi, joka skaalautuu nykypäivän verkkotilavaatimuksiin.

IPv6-osoite

IPv6-osoitteet muodostuvat 128 bitistä, ja osoitteita on olemassa 2^{128} (eli $3{,}4\times10^{38}$ kappaletta). Käytännössä luku on kuitenkin pienempi, sillä osa IP-osoitteista on varattu muuhun käyttöön tai poistettu käytöstä kokonaan. Tällaisia muuhun käyttöön varattuja osoitteita ovat muun muassa yksityisiin verkkoihin tarkoitetut osoitteet.

IPv6-osoitteet voidaan tyyppinsä perusteella luokitella kolmeen osaan:

- **Unicast**-osoitteet muodostavat suurimman osan kaikista osoiteavaruuteen kuuluvista osoitteista. Se on yksittäinen verkkoliittymän osoite, johon lähetetyt paketit toimitetaan lyhintä reittiä pitkin.

- **Anycast**-osoite on useammalle verkkoliittymälle suunnattu osoite. Kaikki Anycast-liittymät kuuluvat samaan fyysiseen verkkoon, jolloin niillä on sama aliverkon osoite. Paketti, joka on osoitettu Anycast-osoitteeseen, toimitetaan reitti-protokollan määräämälle lähimmälle koneelle.

- **Multicast**-osoitteet muistuttavat läheisesti Anycast-osoitteita, sillä ne ovat myös verkkoliittymäjoukon osoitteita. Erilaisen niistä tekee se, että multicast-osoitteeseen lähetetty paketti välitetään jokaiselle liittymäjoukon laitteelle, näin ollen korvataan IPv4:n broadcast-osoitteet.

IPv6-osoitteiden esitystavat

IPv6-osoitteiden ollessa 128-bittisiä niiden esitystapa eroaa lyhyemmistä 32-bittisistä IPv4-osoitteista. IPv6:n esitystavassa osoite jaotellaan kahdeksaan 16-bitin heksadesimaalilukuun. Muunnos suoritetaan esimerkin mukaisesti:

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Jolloin muunnettaessa heksadesimaalimuotoon osoitteeksi muodostuu:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Tämän jälkeen osoitetta voidaan tiivistää, jotta sitä on helpompi tulkita ihmissilmällä. Osoitteen sisällä oleville nollille on erilaisia tiivistyssääntöjä, joita soveltamalla saadaan osoite siistimpään muotoon. Viidennessä kolumnissa lukujono 0063 voidaan lyhentää, jolloin osoite näyttää seuraavalta:

2001:0000:3238:DFE1:**63**:0000:0000:FEFB

Jos osoitteet sisältävät useammassa kolumnissa pelkkiä nollia, voidaan niiden muoto tiivistää peräkkäisten ”::”-merkkien avulla oheiseen muotoon:

2001:0000:3238:DFE1:63**::**FEFB

On syytä huomata, että edellisen tiivistystoimenpiteen suorittaminen on mahdollista vain kerran, sillä useampien nollien tiivistys eri kohdista aiheuttaa sen, ettei osoitetta ole enää mahdollista purkaa alkuperäiseen muotoon. Jos osoitteessa kuitenkin on toisen kolumnin tapaan useampia pelkkiä nollia sisältäviä kohtia, on mahdollista tiivistää ne yhteen nollaan:

2001:**0**:3238:DFE1:63::FEFB

Kuten esimerkistä huomataan, alkuperäisessä muodossaan IPv6-osoitteet voivat olla pelottavia, mutta käytännössä tiivistystoimenpiteiden jälkeen osoitteet muistuttavat näennäisesti hyvin paljon IPv4-osoitteita. [9.]

IPv6:n autokonfiguraatio ja NDP

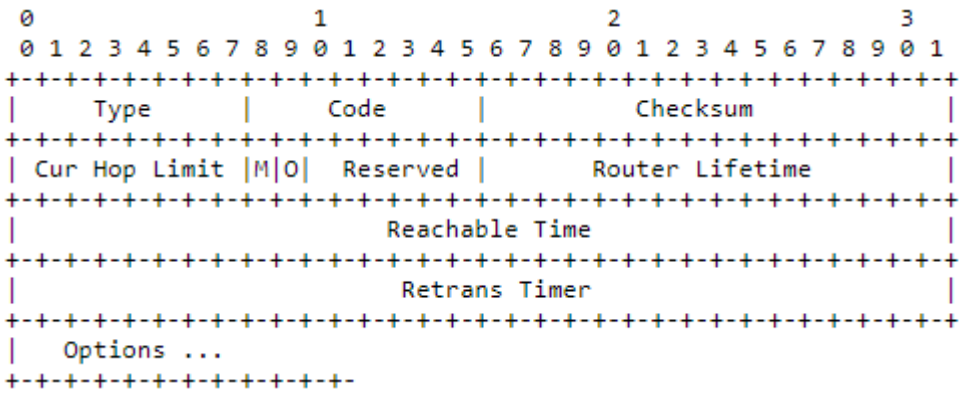
Suuren osoiteavaruutensa lisäksi IPv6:lla on ominaisuuksia, jotka ovat mainitsemisen arvoisia koko protokollan ymmärtämisen kannalta.

IPv4-verkoissa käyttäjien automatisoitu osoitteiden hallinta perustuu DHCP-protokollaan. Vastaavaa toimintaa IPv6-verkoissa tarjoaa DHCPv6-protokolla, jota suurimassa määrin palveluntarjoajat käyttävät verkoissaan. On myös kuitenkin mahdollista hyödyntää tilatonta automaattikonfiguraatiota (SLAAC), joka yhdistää käyttäjän IPv6-verkkoon automaattisesti määrittäen *link-local*-osoitteen. Osoitteen perusteella verkkolaite voi suorittaa kyselyn, jonka avulla se saa tiedot lähireitittimistä sekä muista parametreista, joita verkkoliikenne edellyttää.

Tilattomassa automaattikonfiguraatiossa laitteen osoite muodostuu kahdesta osasta. Ensimmäinen 64-bitin osa IPv6-osoitteessa kuuluu reitittimen mainostamalle osalle, eli prefiksille. Kaikilla samaan verkkoon kuuluvilla liittymillä on sama 64-bitin osa. Osoitteen toinen osa muodostuu laitteen 48-bittisen MAC-osoitteen perusteella, joten näin ollen kaikkien verkossa toimivien laitteiden osoite on uniikki. Jotta osoitteen 64-bitin vaatimus täyttyisi, osoitteeseen lisätään myös 16-bitin pituinen täyteheksadesimaali FFFE. Ensimmäinen 24-bittinen laitevalmistajakohtainen tunniste (*Organizationally Unique Identifier*) on jokaiselle tietyn valmistajan laitteelle sama. Tämän jälkeen osoitteeseen määritellään täyteheksadesimaali, jota seuraa 24-bitin uniikki laitetunniste.

Edellä käsitelty automaatiokonfiguraatio kuitenkin asettaa tietoturvallisesta näkökulmasta haasteita, sillä osoitteen jälkiosa ei käytännössä muutu käyttäjän siirtyessä esimerkiksi kotiverkosta julkiseen verkkoon. RFC4941 määrittelee uudenlaisen tavan käsitellä käyttäjien osoitteita satunnaisalgoritmin avulla, jolloin yksittäisten laitteiden seuranta muuttuu lähes mahdottomaksi. Satunnaisgeneraatiossa hyödynnetään MD5-algoritmia, joka muodostaa 128-bittisen tiivisteen alkuperäisestä satunnaisesta historiallisesta arvosta (määritelty RFC4941:ssä). Automaatiokonfiguraatiossa tätä hyödynnetään ottamalla ensimmäiset 64 bittiä tiivisteestä ja muuntamalla jonon seitsemäs bitti nollaksi, jolloin tuloksena saadaan osoitteen loppuosa. Duplikaattiosoitteiden välttämiseksi osoitetta verrataan aikaisemmin luotuihin osoitteisiin ja näin varmistetaan laitteen uniikki osoite. MD5-tiivistysalgoritmin toinen osa säilytetään seuraavalle laitteelle satunnaisluvun muodostuksessa. Tapauksissa, joissa historiallista satunnaislukua ei ole tallennettu käytettäväksi, laite hyödyntää MD5-algoritmissa satunnaisdataa osoitteen loppuosan muodostamiseksi. [10.]

Käytännössä se, millä tavalla laite itselleen IP-osoitteen määrittelee, riippuu reitittimen mainostukseen käytettävän paketin sisällöstä.



Kuva 5. Reitittimen mainostusviestin rakenne IPv6-formaatissa [11.]

Laiteen IP-konfiguraatioon vaikuttaa kuvan 5 paketissa olevat parametrit ”M” ja ”O”. Parametri ”M” (*Managed Address*) määrittelee, käytetäänkö laitteella DHCPv6-ominaisuutta. Arvoksi voidaan määritellä ”1”, jolloin laite käyttää DHCPv6-osoitteensa määrittelyyn. Vastaavasti arvolla ”0” laite määrittelee itselleen osoitteen esimerkiksi tilattoman autokonfiguraation avulla. Parametri ”O” (*Other Configuration*) määrittelee IP-osoitteistuksen muita ominaisuuksia, kuten nimipalvelimen tietoja. Edellä mainittujen lisäksi pa-

ketti sisältää ”L”- ja ”A”-parametrit, joiden avulla määritellään lisäominaisuuksia osoitteistuksen yhteyteen. ”L” ilmoittaa laitteelle, että samalla osoiteprefiksillä kommunikoivat muut laitteet kuuluvat samaan aliverkkoon ja kehottaa niitä kommunikoimaan verkossa toimivien kytkinten välityksellä. ”A”-parametri ilmoittaa laitteelle MAC-osoitteen käytöstä autokonfiguraation yhteydessä. Laite siis käyttää saamaansa reititinprefiksiä käsi kädessä oman laiteosoitteensa kanssa.

Automaattikonfiguraation toiminta perustuu NDP-protokollaan (*Neighbor Discovery Protocol*), joka toimii verkon siirtoyhteystasolla. NDP:n avulla voidaan paikantaa muita verkon laitteita osoitteiden tai laitteen tilan perusteella, kuten esimerkiksi nimipalvelimia sekä reitittimiä. NDP-protokollan avulla voidaan myös tarkistaa mahdollisia osoitteiden päällekkäisyyksiä. NDP:n toiminta muistuttaa läheisesti IPv4:n avulla toimivia ARP- ja ICMP-protokollia, mutta toimintaa on paranneltu edeltäjäänsä verrattuna.

3 Lähiverkon arkkitehtuuri

Lähiverkolla (LAN) tarkoitetaan maantieteellisesti rajatun alueen sisäistä tietoliikennettä toteuttavaa ja suureen siirtokapasiteettiin pystyvää verkkoa. Verkko on tavallisesti yhden organisaation hallinnassa, mutta joissain tapauksissa verkko saattaa olla kolmannen osapuolen osittain vuokraama tai ylläpitämä. [3, s. 348.] Verkon toiminnan mahdollistavia, fyysisen kerroksen laitteita, ovat mm. kaapelit, kytkimet ja reitittimet. SSAB:n Hämeenlinnan yksikön lähiverkossa toimii useita laitteiden huollosta ja ylläpidosta huolehtivia alihankkijoita. Lisäksi, tehtaan alueella toimivat alihankkijat voivat hyödyntää lähiverkkoa tarpeidensa mukaan erilaisten, organisaation määrittelemien, käytäntöjen linjaamana.

Alueverkko (MAN) on nopea lähiverkkoja yhdistävä kaupunki- tai kampusalueen dataverkko. Koska alueverkko yhdistää monia lähiverkoja, on sen suorituskyvyn oltava riittävä. Useimmiten yksityisissä kampusverkoissa käyttäjä ja ylläpitäjä kuuluvat samaan organisaatioon, mutta laajoissa julkisissa alueverkoissa sekä rakennuttaja että ylläpitäjä, yleensä palveluntarjoaja, kuuluvat eri organisaatioon kuin käyttäjät. [12, s. 12.] Alueverkot on useimmiten toteutettu *Ethernet*-, SDH- ja WDM-tekniikalla valokuituyhteyksiä käyttäen, liikennöintinopeus on tyypillisesti noin 10 Gpbs.

Laajaverkolle tyypillinen ominaisuus on ulottuminen maantieteellisesti paikkakunnalta toiselle, joissain tapauksissa myös valtion rajojen ulkopuolelle. Laajaverkko on tavallisesti teleoperaattorin omistama palveluverkko, jonka avulla asiakkaiden maantieteellisesti erillään olevat toimipisteet voidaan yhdistää toisiinsa. Palveluverkot toteutetaan usein yhdistelemällä erilaisia tekniikoita kuhunkin tilanteeseen sopivalla tavalla. Tällaisia tekniikoita ovat esimerkiksi edellä mainitut *Ethernet* sekä WDM. [3, s. 679.] SSAB:n organisaatioverkko toimii hyvänä esimerkkinä, joka sisällyttää kaikki edellä mainitut verkkojen tyypit. Hämeenlinnan tehtaan lähiverkko on yhteydessä muiden yksiköiden lähiverkkoihin mm. Raahessa ja Helsingissä muodostaen laajaverkon. Nämä lähiverkot ovat edelleen yhteydessä muiden maiden konttoreihin Ruotsissa, Puolassa ja Amerikassa muodostaen laajaverkon usean maan välille.

3.1 Kaapelointi

Kaapelointi on tietoliikenneverkon osa, jossa päätelaitteet kuten työasemat, palvelimet ja tulostimet liitetään verkkolaitteiden välityksellä toisiinsa. Kaapelointi toimii tiedonsiirtotienä verkkolaitteiden ja päätelaitteiden välillä.

Kaapelointi *Ethernet*-verkoissa toteutetaan useimmiten symmetrisillä parikaapeleilla tai valokaapeleilla. Kaapelia kutsutaankin useasti mediaksi ja tarkemmin sanottuna siirtomediaksi tai siirtotieksi. Jokaisesta kaapelityypistä on useita versioita, esimerkiksi valokaapelit voidaan isompana kokonaisuutena jaotella yksi- ja monimuotokuituihin ja edelleen asennustarpeiden mukaan ulko- ja sisäasennuskuituihin. [13, s. 35.]

Yleiskaapelointi

Yleiskaapeloinnin tarkoituksena on toteuttaa tarkoituksenmukainen ja tehokas tietoliikenneverkko, joka on järjestelmäriippumaton kaapelointiratkaisu. Standardi koskee symmetristä kuparikaapelointia tai optista kaapelointia. Suomessa yleiskaapelointistandardi tunnetaan tarkemmin nimellä SFS EN 50173-1.

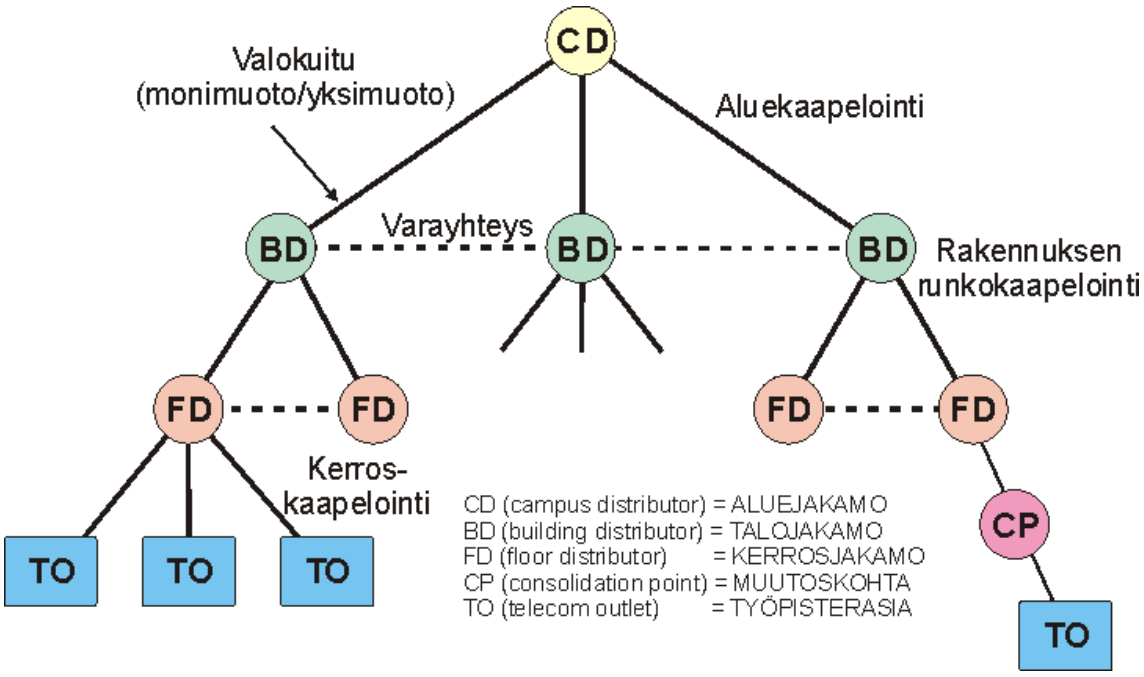
Standardi koostuu kolmesta toiminnallisesta osasta, joita yhdistelemällä voidaan muodostaa toimiva kokonaisuus yrityksen tietoliikenneverkon rungoksi.

- **Nousukaapelointi** tarkoittaa kaapelointia, joka ulottuu talojakamosta yhteen tai useampaan kerrosjakamoon. Nousukaapelointiin kuuluu aluekaapeloinnin tapaan kaapelointi, päätteet sekä kytkennät. Parikaapeleissa ei myöskään saa olla jatkoksia. Nousukaapeloinnin enimmäispituus on 500 metriä.

- **Kerroskaapelointiin** kuuluu kaapelit, jotka viedään kerrosjakamosta yhteen tai useampaan työpisterasiaan. Kerroskaapelointi käsittää kerroskaapelit, ristikytkennät, työpisterasiat sekä kerrosjakamoissa sijaitsevat kaapeleiden päätteet. Kaapeloinnin enimmäispituus on 90 metriä.

- **Aluekaapelointi,** joka ulottuu aluejakamosta useampiin talojakamoihin. Aluekaapelointiin kuuluu aluekaapeleiden lisäksi niiden päätteet jakamoissa sekä ristikytkennät aluejakamossa. Aluekaapeleiden avulla voidaan myös yhdistää talojakamot suoraan keskenään. Aluekaapeloinnin sekä kerrosjakamon välinen kaapelipituus ei saa ylittää 2000 metriä.

Kuvassa 6 esitellään valokuidulla toteutettu kolmen rakennuksen lähiverkko. Kuvasta nähdään yleiskaapeloinnin suunnittelussa käytetty hierarkkinen toteutus sekä jakamossa tähtiperiaatteella toteutettu kaapelointi, joka pätee jokaisessa jakamossa.



Kuva 6. Yleiskaapeloinnin periaatekuva [13, s. 51.]

Yleiskaapelointistandardin kuvassa 6 osoitettu kaavio on kuitenkin joustava. Kaapeloitavan alueen koko ja sijainti vaikuttavat kunkin yleiskaapelointistandardin osa-alueen käyttöön. Esimerkiksi alueen ollessa pieni, yhden rakennuksen käsittävä kokonaisuus, ei aluekaapelointia silloin tarvita. Jotkut rakennukset saattavat kuitenkin pienestä maantieteellisestä koostaan huolimatta vaatia aluekaapelointia välimatkojen kasvaessa liian suuriksi. Uuden verkon suunnittelijoiden velvollisuus siis on, että kaikki rakenteelliset ja maantieteelliset seikat otetaan suunnitteluvaiheessa huomioon.

3.2 Valokuitukaapeli

Valokaapeli on muovista tai lasista valmistettu kuitu, jonka tarkoituksena on siirtää dataa valon avulla. Valokaapelia on kahta tyyppiä: yksimuotokuitua (*single mode*) ja monimuotokuitua (*multi mode*). Erona näillä kaapelityypeillä on ytimen halkaisijan suuruus, joka vaikuttaa valon käyttäytymiseen kuidun sisällä. Lisäksi kuitujen signaalin lähetykseen käytetty liitin eroaa toisistaan, yksimuotokuidun signaalilähetin hyödyntää laserlähetystä ja monimuotokuidussa lähetykseen voidaan käyttää LED-lähettimen lisäksi VCSEL-lähetintä. VCSEL-lähetin sijoittuu ominaisuuksiltaan LED- ja laserlähettimen välimaastoon, mutta on huomattavasti vastaavia lähettimiä halvempi vaihtoehto kuitukaapeloinnissa.

Yksimuotokuidun ytimen halkaisija on noin 9 mikrometriä ja monimuotokuidun yleisimmin 50 mikrometriä. Vanhemmissa monimuotokuiduissa ytimen halkaisija on 62,5 mikrometriä. Yksimuotokuituja useimmiten hyödynnetään aluekaapeloinnissa sen parempien siirto-ominaisuuksien takia. Monimuotokuituja vastaavasti hyödynnetään lyhyen matkan siirtoyhteyksiin lähiverkoissa.

Valokuitukaapeleista puhuttaessa monimuotokuidut luokitellaan kaistanleveytensä perusteella kolmeen kategoriaan: OM1, OM2 ja OM3. Yleiskaapelointistandardissa SFS-EN 50173-1 näille kaapeleille on määritelty suurin vaimennus ja pienin kaistanleveys. Yksimuotokuiduista puhuttaessa kategoriasta käytetään nimitystä OS1. [5, s. 117–119; 13, s. 63.]

3.3 Keskitin

Keskittimen tehtävänä on jakaa yhdeltä tulojohdolta saamansa signaali useisiin menoportteihin. Passiivinen keskitin on verkon yksinkertaisin laitetyyppi. Se jakaa ulostuloliikenteen kaikkiin liityntöihinsä sisällöstä riippumatta. Aktiivinen keskitin voi sen sijaan suodattaa liikennettä ja vahvistaa signaaleja toistimen tavoin. Kytkevä keskitin toimii hyvin samankaltaisesti kytkimeen nähden, sillä se välittää liikenteen vain kohteena oleviin portteihin. Keskittimen suurin ongelma on yleislähetysalueiden suuruus, tästä syystä yrityksissä on siirrytty nykyaikaisempiin kytkinpohjaisiin verkkoratkaisuihin, sillä yleislähetysalueiden kasvaessa, verkkoon kohdistuu tavallista suurempi kuorma lähetteiden vie-

dessä kaistanleveyttä. Nykyaikaisissa verkkoratkaisuissa ei kuitenkaan keskittimiä juurikaan käytetä, sillä hinnanlaskun seurauksena kytkimistä on tullut keskeisin laite verkkoinfrastruktuurista puhuttaessa.

3.4 Kytkin

Verkon keskeisin osa on kytkin, joka yhdistää pakettikytkentäisiä verkon osia, jolloin muodostuu yhtenäinen siirtoyhteystasolla toimiva verkko. Kytkin tallentaa saapuvan paketin MAC-osoitteen ja portin kytkimen osoitetauluun ja vertaa paketin vastaanottajan MAC-osoitetta taulun tietoihin ja ohjaa eteenpäin oikeaan porttiin. Jos osoitetaulusta ei löydy vastaanottajan tietoja tai kyseessä on *multicast*- tai *broadcast*-lähete, paketti ohjataan kaikkiin portteihin. Jos paketilla on sama lähettäjä ja vastaanottaja, paketti hävitetään. Tämä on olennainen osa varmistettaessa verkon turvallisuus ja toimivuus, sillä kyseiset paketit mahdollistavat verkon väärinkäytön ja kuormittavat kytkintä tarpeettomasti. [14, s. 33.]

VLAN

Fyysinen lähiverkko muodostuu loppukäyttäjien laitteista, kaapeleista ja verkkolaitteista. Kaikki verkon loppukäyttäjälaitteet vastaanottavat toistensa lähettämät yleislähetysviestit, toisin sanoen ne muodostavat yhden fyysisen lähiverkon.

Fyysisen lähiverkon lailla virtuaalinen lähiverkko eli VLAN (*Virtual Local Area Network*) muodostuu kaikista samaan yleislähetysalueeseen kuuluvista loppukäyttäjälaitteista. Kytkimelle konfiguroidaan VLAN siten, että tietyt fyysisen kytkimen portit kuuluvat ennalta määriteltyihin VLAN:hin. Näin kytkimen avulla muodostetaan yleislähetysalueita, jotka välittävät kehyksensä vain samaan VLAN:iin kuuluvien laitteiden välillä. Tämä vähentää verkon kuormitusta tilanteissa, joissa yleislähetysalueet ovat kasvaneet yrityksen koon takia liian suuriksi. Yleisimpiä virtuaalilähiverkkojen tyyppejä ovat *Data*, *Default*, *Native*, *Voice* sekä *Management*.

- **Default VLAN** sisältää kaikki kytkimen portit, joita ei ole ennalta konfiguroitu. Default VLAN:ia ei voi poistaa eikä nimetä uudelleen. Tietoturvallisista syistä on suositeltavaa, ettei tähän VLAN:iin määritellä portteja.

- **Data VLAN** on yleisin edellä mainituista viidestä VLAN:sta. Kaikki normaali käyttäjäliikennöinti kulkee tämän VLAN:n kautta.

- **Voice VLAN** on VOIP-laitteille tarkoitettu kanava, jonka avulla IP:n yli kulkevaa puhelinliikennettä voidaan luokitella ja priorisoida QoS-käytäntöjen avulla.

- **Native VLAN** on 802.1Q-trunkeissa esiintyvä VLAN, jonka liikenne välitetään normaaleina ethernet-kehyksinä ilman 802.1Q-tunnistetta.

- **Management VLAN** on tarkoitettu järjestelmänvalvojan liikenteen ohjaamiseen. Rajapinnan avulla voidaan suorittaa erilaisia muutoksia kytkinten asetuksissa, sillä VLAN:lle asetetaan oma IP-osoite sekä aliverkon peiteosoite. Tämä mahdollistaa kytkimeen kirjautumisen esimerkiksi SSH:n avulla.

Virtuaalilähiverkkojen tarkoituksena on jakaa fyysinen lähiverkko loogisiin kokonaisuuksiin, joiden laatimiseen sovelletaan ”*principle of least privilege*”-ajattelumallia. Sen tarkoituksena on tarjota loppukäyttäjille pääsy ainoastaan niihin tietoihin, joita se työnsä suorittamiseen tarvitsee. Esimerkiksi, palkanlaskennan toimihenkilöiltä evätään pääsy tuotannon virtuaalilähiverkkoon ja päinvastoin. Tällöin arkaluontoinen materiaali on suojassa väärinkäytöksiltä ja omalta osaltaan vahvistaa yrityksen tietoturvaa. Tämän lisäksi työtehtävien muutos yrityksen sisällä ei aiheuta sitä, että käyttäjän tulisi fyysisesti muuttaa työpisteeltään toiselle, sillä virtuaalilähiverkot mahdollistavat resurssien jaon sijainnista riippumatta. Tämä ei myöskään aiheuta rajoituksia sille, mihin uusia työntekijöitä sijoitetaan yrityksen sisällä.

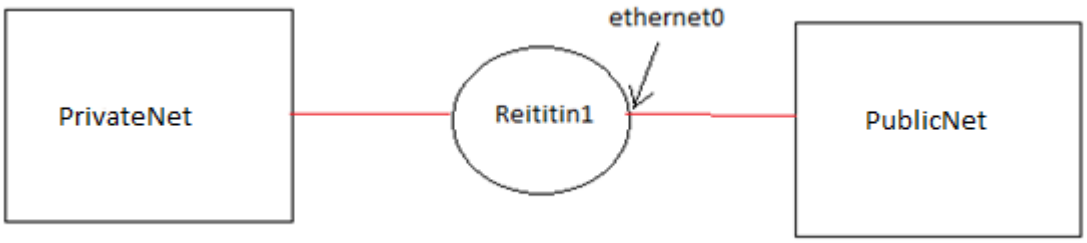
3.5 Reititin

Reitittimet ovat verkkokerroksen protokollariippuvaisia laitteita, jotka välittävät paketteja aliverkkojen välillä. Reitittimien protokollat huolehtivat verkkotopologiatietojen muutoksista toisten reitittimien välillä ja huolehtivat pakettien oikean reitin valinnasta. Lisäksi pääsylistojen (*ACL, Access List*) avulla reititin voi suodattaa liikennettä esimerkiksi protokollan tai lähdeosoitteen mukaan. Pääsylistojen konfigurointi reititetyssä verkossa on tärkeää tietoturvan näkökulmasta, vanhentuneiden protokollien käyttöä tulisi välttää ja tietoturvallisessa ajattelutavassa käyttäjien pääsyä tulisi rajoittaa vain tarpeellisiin tietoihin pääsyyn. Ohessa esimerkkinä yksinkertaisen pääsylistan konfigurointi reitittimellä,

tarkoituksena estää vanhentuneen Telnet-protokollan käyttö verkkojen välillä tietoturvasyistä.

```
Hostname Reititin1

!

interface ethernet0

ip access-group 102 in

!

access-list 102 deny tcp any any eq 23

access-list 102 permit ip any any
```

Esimerkkikonfiguraatio 1. Pääsylista, joka rajoittaa Telnet-yhteyksiä sisäverkkoon (PrivateNet)



Kuva 7. Pelkistetty verkkotopologia liittyen esimerkkikonfiguraatioon 1.

Kuvassa 7 on esitetty verkkotopologia julkisen ja yksityisen verkon välillä. Tarkoituksena rajoittaa pääsyä ulkoisesta verkosta sisäiseen. TCP-protokollalla toimiva Telnet on vanhentunut ja aiheuttaa tietoturvauhkia, sillä liikennöintiä ei ole salattu millään tavalla. Nykyaikaisissa verkoissa suositellaankin käytettäväksi vähintään SSH2-protokollaa, joka käyttää epäsymmetristä salaustekniikkaa liikenteen suojaamiseen.

Esimerkkikonfiguraatiosta 1 voidaan huomata, että pääsylistan avulla kaikki TCP-liikenne, joka vastaa Telnetin käyttämää porttinumeroa 23 on estetty yhtymäkohdassa ethernet0 reitittimille. Konfiguraatiosta huomaamme myös, että pääsylistana on käytetty pidennettyä 100–199 numeroalueella toimivaa pääsylistaa. Pääsylistoja konfiguroitaessa on syytä muistaa, että yksinkertaisemmat 1-99 alueella toimivat pääsylistat sijoitetaan mahdollisimman lähelle lopullista määränpäätä, sillä nämä pääsylistat rajoittavat liikennettä lähdeosoitteen perusteella. Vastaavasti pidennetyt pääsylistat, kuten kuvasta 7 huomataan, on tärkeä sijoittaa mahdollisimman lähelle lähdeosoitetta.

Reitityksellä tarkoitetaan mekanismeja, joilla IP-paketti löytää lähteestä kohteeseen paketista löytyvien osoitetietojen avulla. IP-reititys jakautuu loogisesti kahteen eri prosessiin: IP-pakettien mekaaniseen välitykseen reitittimen sisääntuloliitännästä oikeaan ulosmenevään liitäntään reititystaulun perusteella sekä protokolliin, joilla reititystaulujen tietoja välitetään IP-verkon reitittimien kesken. IP-paketit liikkuvat verkossa reitittimeltä toiselle niin sanottujen ”hyppyjen” avulla, jokaisella reitittimellä siis tulee olla tieto siitä, mihin suuntaan kyseinen paketti täytyy lähettää, jotta se päätyy sille tarkoitettuun verkkoon. Ajatus siis on, että reititystauluissa, joiden avulla paketteja ohjataan, ei koskaan ole tietoa paketin kokonaismatkasta kohteeseen. Reitittimien käytössä olevia yleisimpiä protokollia ovat RIP, RIPv2, EIGRP ja OSPF.

RIP ja RIPv2

RIP ja RIPv2 (*Routing Information Protocol*) ovat etäisyysvektoriprotokollia, jotka käyttävät etäisyyden mittana hyppyjen lukumäärää. Kahden reitittimen välinen hyppy lasketaan yhdeksi hypyksi. Reititin lähettää 30 sekunnin välein päivitysviestejä naapurireitittimille. Jos naapuri ei vastaa 3 minuutin kuluessa, niin reitti asetetaan etäisyydeltään äärettömäksi, jonka jälkeen se poistetaan kokonaan reititystaulusta. [8, s. 90–91.]

EIGRP ja IGRP

IGRP on Cisco Systemsin kehittämä etäisyysvektorialgoritmi. Reitin paremmuuden ilmoittaman metriikan oletusarvona on segmenttiviiveiden ja polun alhaisimman siirtonopeuden käänteisarvon summa. Lisäksi IGRP huomioi linkkien luotettavuuden ja kuormituksen algoritmissaan. Näiden tekijöiden painoarvoja voidaan manuaalisesti muuttaa, mutta reitityssilmukoiden välttämiseksi verkon kaikissa reitittimissä suositellaan käytettäväksi samoja painoarvoja.

EIGRP on Ciscon reititysprotokolla, joka on korvannut IGRP:n nykyaikaisissa verkoissa. Se käyttää samaa reititysmetriikkaa kuin aikaisempi versio, mutta reittien laskentaa ja tietojen välittämistekniikkaa on uudemmassa versiossa paranneltu. EIGRP myös levittää nopeasti tiedon verkossa tapahtuvista muutoksista ja päivittää reititystaulut sen mukaisesti. [12, s. 211.]

OSPF

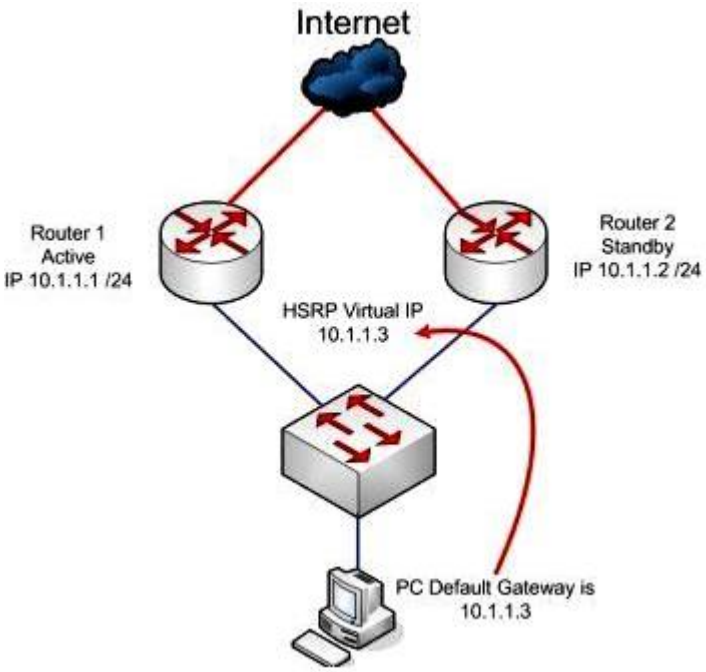
Edellä mainittujen etäisyysvektoriprotokollien lisäksi sisäisissä verkoissa on käytössä niin sanottuja linkin tila -reititysalgoritmeja (*Link State*). Näissä algoritmeissa reitittimet muodostavat hajautetun topologiatiedon verkoista ja reitittimistä. Ajatuksena on, että reitittimet aluksi kertovat naapuriverkoistaan kaikille saman alueen reitittimille. Linkin tila -reititysalgoritmit soveltuvat parhaiten suurempiin verkkokokonaisuuksiin, sillä verkon topologiamuutokset levittyvät nopeasti kaikille alueen reitittimille. Yleisin näistä algoritmeista on OSPF (*Open Shortest Path First*).

OSPF on valmistajariippumaton reititysprotokolla, joka käyttää optimaalisen reitin valintaan Dijkstra-algoritmia. Reitittimet lähettävät verkossaan linkin tila -viestejä muille saman hierarkia-alueen reitittimille, tästä syystä OSPF toimiikin hierarkkisessa verkossa parhaiten. Ylin hierarkiataso on autonominen järjestelmä, joka on kokoelma pienemmistä loogisista verkkoalueista, joilla on yhteinen reititysstrategia. Verkkoalueen reitittimillä on sama topologiatietokanta, eikä tämä tieto näy määriteltyjen alueiden ulkopuolelle. Tästä syystä OSPF tarvitsee vähemmän reititystietoja, mikä parantaa reitittimien suorituskykyä, ja samalla lisää tietoturvaa tiedon ollessa hajautettuna reitittimien välillä. Verkon jaottelu lisää myös verkon stabiiliutta, sillä muutokset yhden alueen sisällä eivät heijastu muille alueille. [12, s. 211–214.]

HSRP

HSRP-protokolla on Ciscon kehittämä vikasietoisuusprotokolla, jonka tarkoituksena on varmistaa verkkoyhteyksien toimivuus lähiverkossa, mikäli yhteys päätoimiseen reitittävään laitteeseen menetetään. HSRP-ryhmään kuuluu kaikki HSRP-instanssissa toimivat reitittävät laitteet. Konfiguroitaessa ryhmää reitittäville laitteille määritellään normaali IP-osoite laitteiden tunnistukseen lähiverkossa sekä virtuaalinen IP- ja MAC-osoite. Virtuaalinen HSRP-ryhmän IP-osoite toimii lähiverkon aktiivilaitteiden oletusyhdyskäytävänä,

jonka avulla liikennöinti muihin verkkoihin onnistuu. MAC-osoite määräytyy virtuaalilaitteelle automaattisesti, joten sitä ei tarvitse itse konfiguroida.



Kuva 8. HSRP-topologia ja toiminta [15.]

Kuvan 8 mukaisesti lähiverkon aktiivilaite hyödyntää näennäisen yhden virtuaalilaitteen IP:tä oletusyhdyskäytävänään, vaikka taustalla toimii kaksi reititintä.

HSRP-protokollan toiminta perustuu instanssissa toimivien laitteiden väliseen HELLO-pakettien lähetykseen, joita laite lähettää *multicast*-osoitteen sekä UDP-portin 1985 välityksellä. Primäärilaite lähettää tasaisin väliajoin paketteja *standby*-laitteille, jolloin oletuksena laitteet säilyttävät roolinsa. Jos *standby*-laite ei saa tietyn ajan kuluessa HELLO-paketteja, se olettaa yhteyden primäärilaitteeseen katkenneen ja asettaa itsensä uudeksi päätoimiseksi HSRP-ryhmän laitteeksi. Päätelaitteet eivät näe verkon rakenteessa tapahtuvia muutoksia, jolloin liikennöinti voi jatkua katkeamatta. Tämä on tärkeä ominaisuus katkeamattomassa tehdastuotannossa.

Laitteiden roolit määritellään konfiguraatiossa prioriteettinumeroiden avulla. Korkeimman prioriteettinumeron omaava laite määräytyy primäärilaitteeksi, jolloin kaikki muut ryhmän laitteet ovat odotustilassa eivätkä osallistu pakettien välitykseen. HSRP-protokollan etuna on myös laitemäärä, sillä käyttäjä ei ole rajoitettu pelkästään kahden laitteen käyttöön, vaan ryhmässä voi olla useampia laitteita. Tämä mahdollistaa skaalautuvan vikasietoisen ratkaisun reitittävien laitteiden toiminnan varmistamiseksi.

3.6 Yhdyskäytävä

Yhdyskäytävä on laite, jonka tärkeimpänä tehtävänä on yhdistää eri protokollia käyttävät verkot keskenään toisiinsa. Laite suorittaa tarvittaessa protokollamuutokset, jotta verkkojen toiminta keskenään olisi mahdollista. Esimerkiksi TCP/IP-verkkojen SMTP-sähköpostiprotokollan sanomia voidaan muuntaa yhdyskäytävän avulla X.25-verkon X.400-sähköpostijärjestelmän ymmärtämään muotoon. Yhdyskäytävän oleellisin ero siltaan nähden on se, että yhdyskäytävä voi yhdistää ylempien tasojen eri teknologioita käyttäviä verkkoja toisiinsa. TCP/IP-verkossa toimivan yhdyskäytävän täytyy siis olla sekä IP-reitin, että siihen yhdistyneen erilaista verkkoprotokollaa käyttävän verkon vastaava laite. [8, s. 31.]

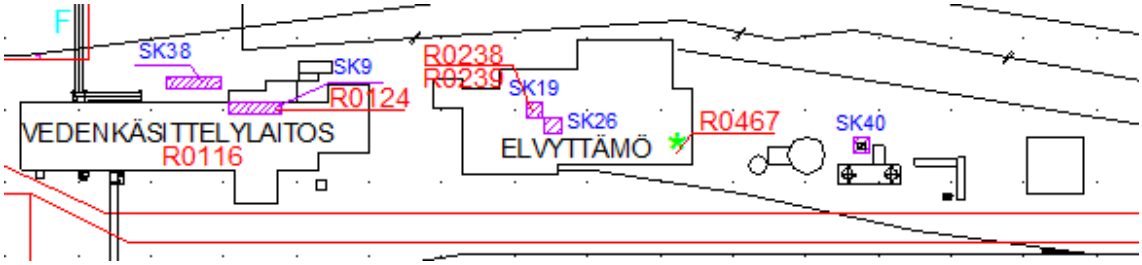
3.7 Palomuuri

Palomuuri sijaitsee tyypillisesti yksityisen yrityksen verkon osan ja julkisen verkon rajalla. Palomuurin tehtävänä on suodattaa liikennettä ja estää esimerkiksi asiattomien henkilöiden pääsy joihinkin sisäverkon osiin, jotka saattavat sisältää arkaluontoista tietoa. Palomuuri voi myös toimia toiseen suuntaan eli sillä voidaan estää pääsy sisäverkosta joihinkin julkisen verkon osiin, esimerkiksi tietyille verkkosivustoille. Palomuurin tehokkuus perustuu tiedon suodattamiseen useammalta protokollapinon kerrokselta. Mitä useamman kerroksen tietoa palomuuri voi lukea, sitä paremmin laite pystyy lukemaan ja suodattamaan läpi kulkevaa tietoa paketeista. Yksinkertaisimmillaan palomuuri voi suodattaa paketteja IP-osoitteiden perusteella, vaikkakaan tietoturvallisesta näkökulmasta se ei ole kovin tehokasta. [8, s. 32.]

4 Verkon dokumentointi ja rakenne

4.1 Yleistä dokumentoinnista

Hämeenlinnan SSAB Oy:n tehdasalueen koko on 55 hehtaaria, joista noin 13 hehtaaria on rakennusalaa. Tässä työssä keskitymme tehtaan elvyttämöalueen aliverkon uusimiseen, joka näkyy kuvasta 9.



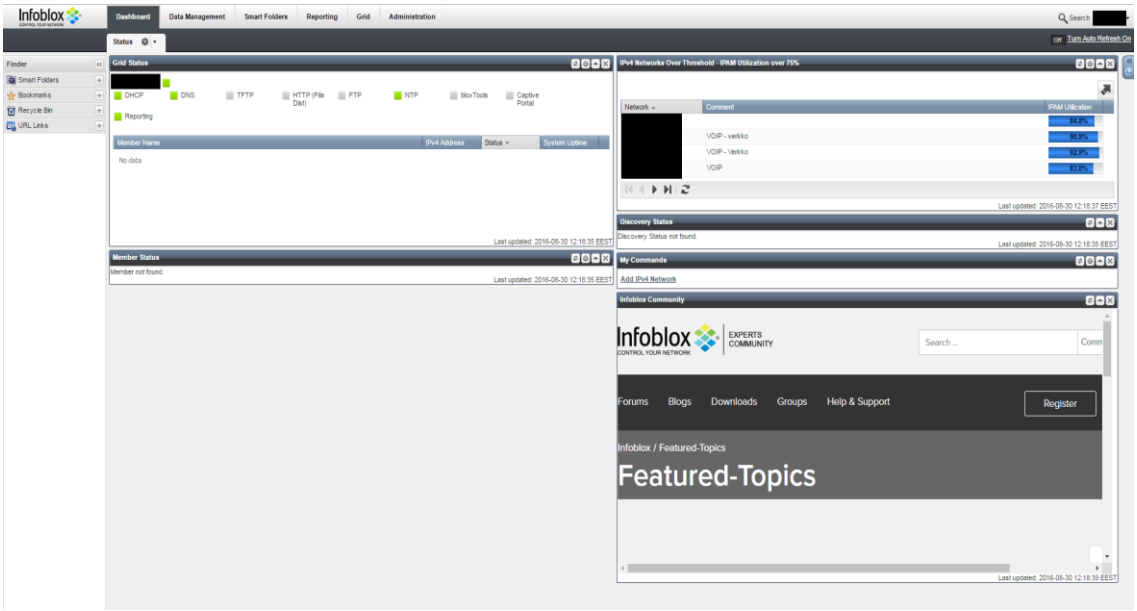
Kuva 9. Tehtaan elvyttämöalue

IT-henkilöiden lisäksi sähköteknikkojen vastuulla on tehtaalla suoritettavien johtokytkentöjen tekeminen. Sähköpuolen henkilöstöllä ei kuitenkaan ole pääsyä tehtaalla käytettävään dokumenttiin, joka kartoittaa kaikki tehtaalla olevat verkkokytkennät. Tästä syystä dokumentti saattaa vääristää nykyistä tilannetta, ja työssäni ensimmäisenä tehtävänä keskityin nykyisen aliverkon kartoittamiseen, jotta saisin kokonaiskuvan verkkolaitteista sekä kytkennöistä.

Työssä on käytetty dokumentointityökaluna netViz-ohjelmaa, jonka avulla pystytään yksityiskohtaisesti kartoittamaan yrityksen käytössä oleva verkko. Ohjelmiston avulla voidaan laatia koko tehtaan kattava topologia, josta nähdään esimerkiksi IP-osoitteiston lisäksi kaapelimerkinnät sekä ristikytkentäpaneelien molemmat päät lähiverkossa. On syytä kuitenkin huomata, että IP-osoitteistus on verkkodokumentissa vain suuntaa antava osa, sillä yrityksessä käytetään yksityiskohtaiseen IP-osoitteiden hallintaan IPAM-ohjelmistoa *(IP Address Management*). Kuva 9 on piirretty netViz-ohjelman avulla, josta nähdään aliverkon maantieteellinen sijainti. Yksinkertaistuksen takia kuvasta on jätetty pois alueen itäpuolella sijaitseva tehdasrakennus ja länsipuolella sijaitseva putkitehdas, jotka jäävät tämän opinnäytetyön ulkopuolelle.

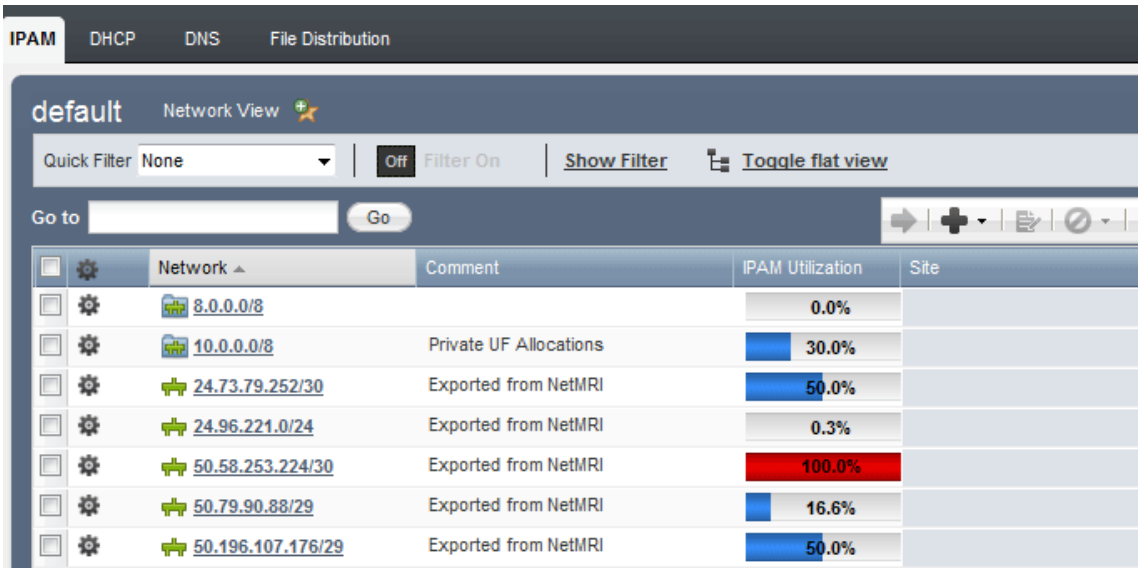
4.2 Infoblox

Nykyaikaisten IP-verkkojen kasvaessa ja BYOD-ajatuksen (*Bring Your Own Device*) yleistyessä IP-verkon hallintaan kohdistuu jatkuvasti enemmän paineita, jolloin keskitetyn verkon hallinnan kysyntä on kasvanut. IPAM eli IP-osoitteiden hallinta tarkoittaa yksityisten IP-osoitteiden jakelua, suunnittelua, hallintaa, raportointia ja niiden seurantaa IP-osoiteavaruudessa. IP-osoitteiden automatisoitu hallinta voi parhaimmassa tapauksessa nopeuttaa ja yksinkertaistaa IP-osoitteiden käsittelyä, jonka ansiosta yrityksen kustannukset sekä virheellisen konfiguraatioiden määrä laskevat. Infobloxin tarjoama IPAM on sisäänrakennettu DNS- ja DHCP-palveluihin, jolloin erillisten laitteiden tai sovelluksien tarvetta ei käyttöönotossa ole. IPAM:n hallinta onnistuu web-käyttöliittymän avulla, jolloin hallinta yksinkertaistuu ja tieto keskitetään helposti saataville. [16.].



Kuva 10. Infoblox-etusivun näkymä

Kuvan 10 mukainen kokonaisnäkymä verkon tilasta aukeaa kirjauduttaessa selaimella Infoblox-käyttäjäliittymään. Kokonaisnäkymä ilmaisee verkon eri palveluiden tilan joko vihreänä tai punaisena. Etusivulta nähdään myös lyhyesti eri verkkojen allokaatiotilanne riippuen vapaiden osoitteiden määrästä kyseisessä verkossa. Kuvasta 11 nähdään yksityiskohtaisempi aliverkkojen tilanne suhteessa vapaisiin IP-osoitteisiin.



Kuva 11. Infoblox IPAM-verkkonäkymä [17.]

Jokaisesta aliverkosta on mahdollista avata yksityiskohtaisempi näkymä, joka auttaa käyttäjää IP-osoitteiden hallinnassa halutussa aliverkossa. Lisäksi verkkonäkymään on mahdollista lisätä jokaisen laitteen kohdalle kommentti, joka on vapaamuotoinen informaation lähde muille IP-hallinnan käyttäjille. Vapaamuotoinen kommenttikenttä kuitenkin aiheutti työssäni ongelmia, sillä osassa laitteista oli vanhentunut tietokenttä, tai sitä ei ollut ollenkaan.

Infoblox IPAM sisältää ominaisuuden, joka automaattisesti tunnistaa verkossa olevia laitteita ja näiden MAC-osoitteita. IP-hallinnan automaattinen tunnistus perustuu ylläpitäjän määrityksestä riippuen ICMP-protokollaan, eli ping-viesteihin, tai TCP SYN -viesteihin. ICMP-viesteihin vastaavan laitteen tiedonanti on rajallinen, sillä laitteesta nähdään vain IP-osoite sekä aktiivisuus verkossa. TCP SYN -viestit antavat vastaavasti laitteen MAC-osoitteen sekä IP-osoitteen. [18.] Päädyin työssäni hyödyntämään TCP SYN -pohjaista laitteiden tunnistusominaisuutta, sillä laitteiden MAC-osoitteiden avulla pystyin siirtymään laitteiden tunnistusprosessissa eteenpäin hyödyntäen Efecte-ohjelmistoa.

4.3 Efecte

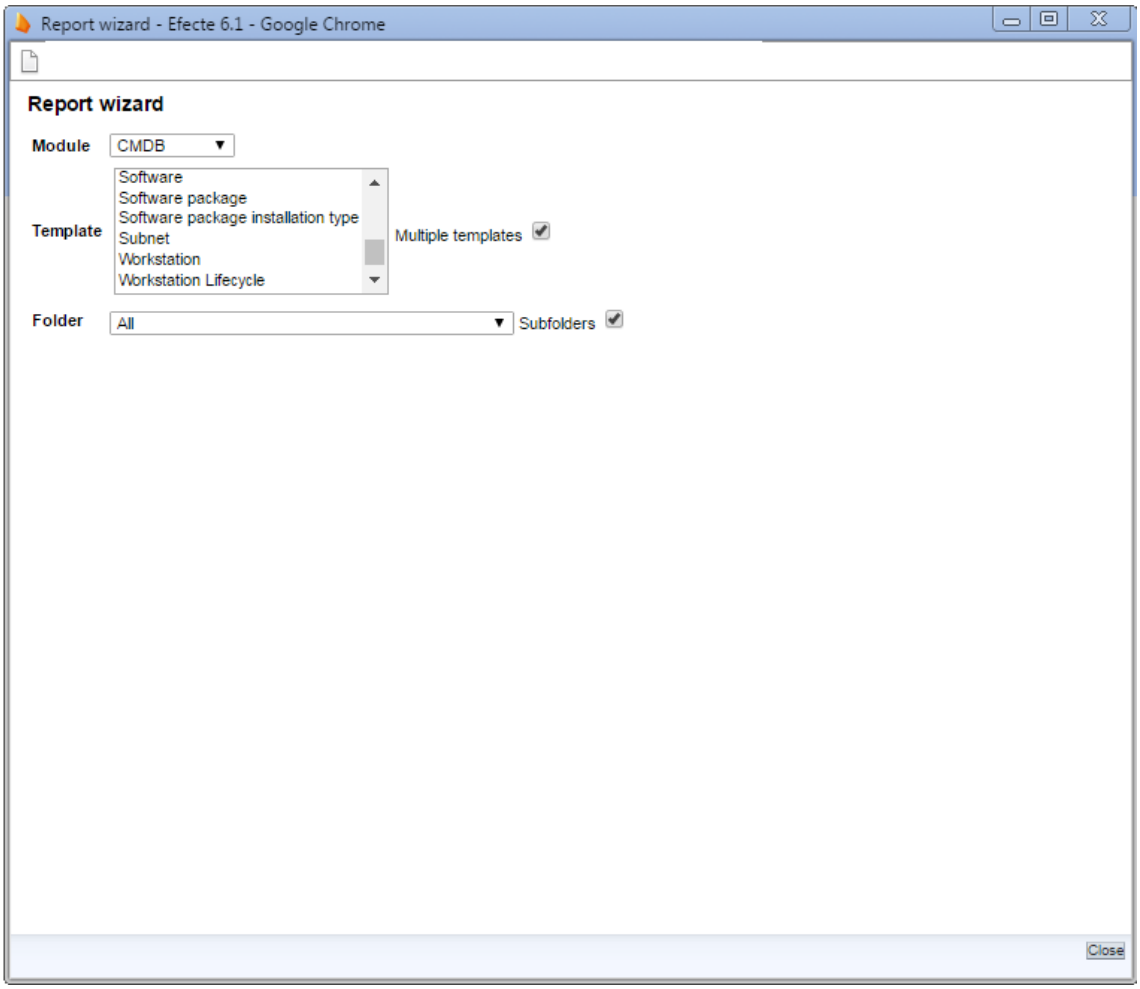
Efecte Oy

Efecte on 1998 perustettu ohjelmistoyhtiö, joka kehittää pilvipohjaisia palvelunhallinta-, itsepalvelu sekä identiteetinhallintaohjelmistoja organisaatioiden toiminnan tehostamiseksi. Yrityksen pääkonttori sijaitsee Espoossa ja työllistää noin 70 ihmistä. Toimipisteitä on Suomen lisäksi Ruotsissa, Tanskassa ja Saksassa. [19.].

Efecte Asset Management

Efecte Asset Management on tarkoitettu yrityksen laitteiden hallintaan. Inventointityökalun avulla IT-henkilöstö voi ylläpitää tarkkaa listaa yrityksen nykyisistä käyttökelpoisista ja romutetuista laitteista, sekä työpisteiden käyttöjärjestelmistä ja lisensseistä. Lisäksi ohjelman avulla pystytään seuraamaan päätelaitteille asennettuja ohjelmia sekä tehdä laajoja ohjelmistopäivityksiä halutuille laitteille. Ohjelmisto on kortistomuotoinen rekisteri, jonka avulla ylläpitäjät voivat suunnitella organisaation laitehankintoja, lisenssisopimuksia sekä päivitysratkaisuja. Jokaisen laitteen yksilöllisestä kortista ylläpitäjät voivat selvittää yksittäisten laitteiden IP-osoitteen, MAC-osoitteen, omistajan, käyttäjän sekä sijainnin yrityksessä. Laitteen paikannus kuitenkin edellyttää tietoa organisaation verkkotopologiasta. Ohjelmiston kokonaisvaltainen käyttö onnistuu selaimen avulla, jolloin ylläpidollinen taakka myös vähenee.

Dokumentaatiovaiheen toisessa osassa tehtävänäni oli selvittää kahden aliverkon, Sinkityslinjan ja Elvyttämön laitteisto. Efecten konfiguraatiohallinntatietokannan (*Configuration Management Database*) avulla onnistuin suorittamaan yksityiskohtaisen haun, joka suodatti organisaation laitteiston sekä IP-osoitteiden että Mac-osoitteiden perusteella. Tuloksena Efecte loi listan, joka ilmoitti jokaisen laitteen nimen, omistajan sekä nykyisen tilan. Näiden tietojen avulla rakensin listauksen molempien verkkojen laitteista, jolloin kokonaisuutena valmistui taulukko, joka listasi laitteiden nimien ja IP-osoitteiden lisäksi nykyisen tilan sekä sijainnin.



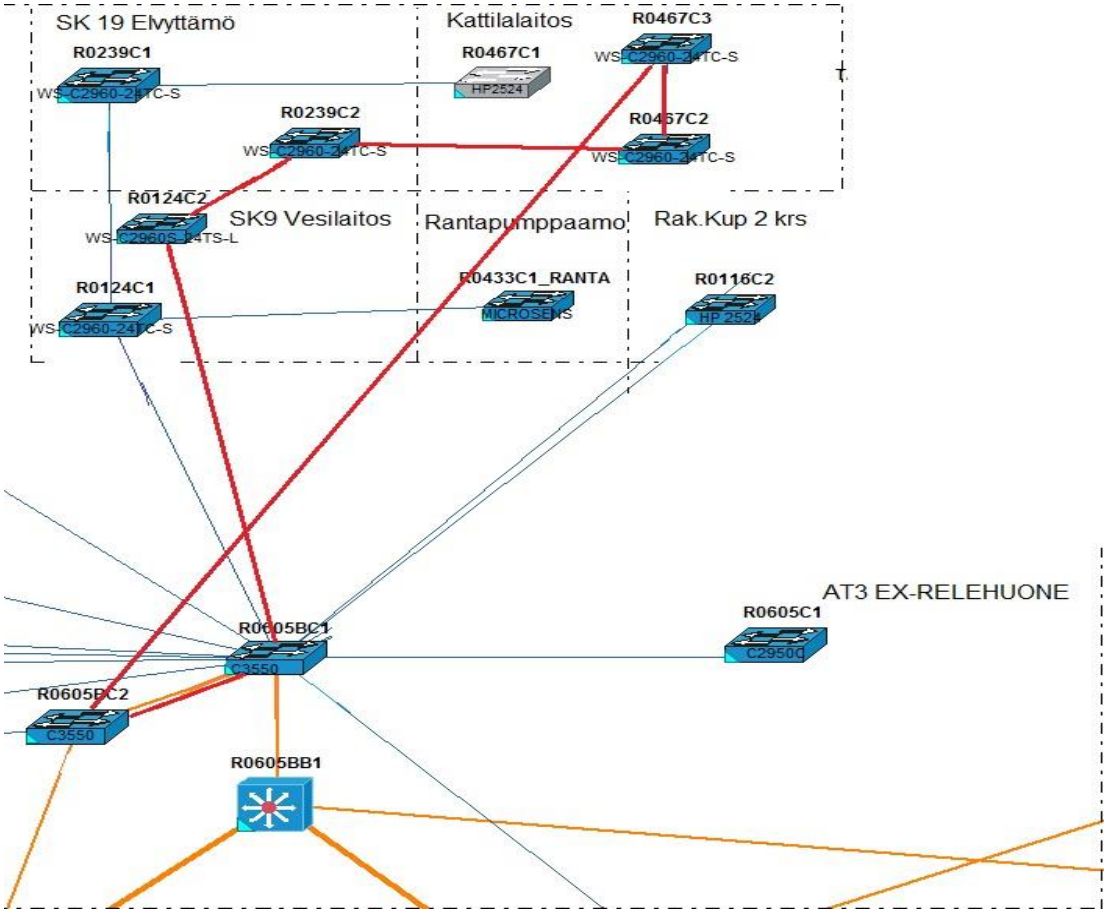
Kuva 12. Efecte CMDB report wizard -näkymä

Kuvan 12 raporttiavustajan avulla Efecten konfiguraationhallintatietokannasta voidaan suodattaa käyttäjälle halutut tiedot yksityiskohtaiseksi listaukseksi. Suodatusmahdollisuuksiin kuuluu mm. aliverkon ja laitepäätteiden valinta. Suodatusmahdollisuuksien määrä on käytännössä rajaton, jolloin tietokannasta on mahdollista kerätä todella yksityiskohtaista tietoa. Suodatusmahdollisuuksien tarkkuus kuitenkin perustuu käytännössä ylläpitäjien organisointiin. Puutteellisesti täytettyjen korttien suodatus johtaa raportointiavustajan virheellisiin listauksiin, jolloin tärkeiden laitteiden huomaaminen saattaa olla mahdotonta ohjelman avulla.

4.4 Hämeenlinnan tehtaan verkko

Verkon kartoituksen jälkeen tehtäväksi tuli suunnitella järkevä ratkaisu kahden aliverkon erittelylle. Lähtökohtana opinnäytetyöhöni oli suoraviivaistaa ja selkeyttää nykyisen aliverkon IP-allokaatio ja erotella kaksi nykyisin sekoittunutta aliverkkoa toisistaan. Tehtaalla sijaitsevan Sinkityslinjan aliverkko on aikojen saatossa sekoittunut Elvyttämön kanssa. Aliverkon kartoitusvaiheessa huomasin, että pelkän Elvyttämön laitteiston kartoitus ei ollut järkevää, sillä nykyisen aliverkkoratkaisun takia sinkityslinjan laitteisto oli syytä ottaa huomioon uuteen verkkoon siirryttäessä.

Dokumentointivaiheen jälkeen laadin netViz-ohjelmalla pohjapiirroksen siitä, kuinka nykyisen verkon rinnalle rakennettaisiin uudella aliverkon tunnisteella kulkeva verkko.



Kuva 13. Pohjapiirros nykyisen verkon rinnalle.

Kuvasta 13 ilmenee uuden aliverkon topologia, joka on merkitty punaisella viivalla. Tämän lisäksi kuvasta nähdään, mihin yksikköön uusi laitteisto tullaan asentamaan. Kattilalaitoksen HP:n kytkin erotetaan nykyisestä verkosta laitteiston vanhan iän takia ja on näin ollen tarpeeton uudessa verkossa. Tämän muutoksen lisäksi koko topologia määritellään uudelleen ja nykyisten kytkimien rinnalle tuodaan uudet kytkimet, jolloin muutostyön suorittaminen on yksinkertaista laitteiden konfiguraatioiden ollessa identtiset. Tehdastuotannon ollessa jatkuvaa on erityisen tärkeää, että kaikki verkossa suoritettavat muutostyöt ovat mahdollisimman lyhytkestoisia. Pitkät tuotantokatkokset verkon häiriötilanteissa vaikuttavat huomattavasti koko tehtaan tuottavuuteen puhdistamoalueen ollessa tärkeässä roolissa tuotantoketjussa.

Topologian tärkein ominaisuus on vikasietoisuus laitehäiriön tapahtuessa. Yhden laitteen tai linkin hajoaminen ei aiheuta tietoliikennekatkosta, sillä liikenne pääsee kulkemaan *Layer3*-kytkinten *R0605BC1 ja R0605BC2* kautta, jotka sijaitsevat R0605-kaapissa tehdasrakennuksessa. Näiden laitteiden välille on rakennettu kahden linkin käsittävä yhteys, jolloin vikatilanteessa tietoliikenne jatkuu ehjäksi jääneen linkin kautta. Edellä mainittuihin kytkimiin on myös konfiguroitu HSRP-protokolla (*Hot Standby Router Protocol*) toimimaan tilanteissa, joissa yhteys kytkimeen katkeaa. Tämä tarkoittaa sitä, että kytkimen R0605BC1:n ollessa niin sanottu aktiivinen kytkin, ja R0605BC2:n ollessa standby-kytkin, omaksuu BC2 aktiivisen kytkimen roolin, jos yhteys BC1-kytkimeen katkeaa. Tämän lisäksi runkoverkon kautta kulkeva liikenne on kovennettu muodostamalla *R0605BB1*, *R0422BB1* ja *R0066BB1* kytkinten välille rengasmallin mukainen yhteys.

5 IP-osoitesuunnitelma

Jokaisen hyvän verkkosuunnitelman perustana on huolella laadittu IP-osoitesuunnitelma. Suunnittelussa tulisi ottaa huomioon verkon nykyinen vaatimustaso sekä tulevaisuuden muutostyöt, jotka saattavat vaikuttaa siihen. Verkon dokumentoinnin ja laitekartoituksen jälkeen siirryin opinnäytetyössäni suunnitteluvaiheeseen, joka toimii perustana käytännön toteutusvaiheelle.

Lähtökohtana IP-suunnitelmalle oli aliverkon kokoon keskittyvä osoiteavaruuden rajaaminen. Jo työn alkuvaiheessa selvisi, että verkkoon tultaisiin lisäämään useita lisälaitteita olemassa olevien rinnalle. Tästä syystä päädyimme /25-aliverkkopeitteen kokoiseen, 126 osoitetta sisältävään verkkoon.

Suunnitelman seuraavassa vaiheessa tehtävänä oli IP-osoitteiden allokointi laitteille IPAM:n avulla. Salassapitovelvollisuuden sekä tietoturvallisuuden takia IP-osoitesuunnitelman yksityiskohdat on rajattu julkisen opinnäytetyön ulkopuolelle. Salatussa liitteessä 3 on kuvattu IP-osoitteiden lisäksi laitteille määritellyt nimet, MAC-osoitteet, kommenttikentät sekä valmistajat. IP-osoitteiden varaus mahdollistaa yksityiskohtaisen sekä järjestelmällisen dokumentin työn toteutusta varten, jotta mahdollisten päällekkäisten laiteosoitteiden konfiguraation riski pienenee huomattavasti.

6 Laitekonfiguraatio

Osoitesuunnitelman jälkeen työssäni siirryin laitekonfiguraatioon. Kaikkiin kytkimiin tultaisiin asettamaan seuraavat parametrit:

- tarvittavat palvelut (*service*)
- *errdisable recovery*
- *spanning tree protocol* (*STP*)
- *virtual local area network* (*VLAN*)
- porttiasetukset vaatimuksista riippuen.
- kytkimen hallintaan vaadittavat parametrit
- pääsylistat (*ACL*)
- *simple network management protocol* (*SNMP*)
- *network time protocol* (*NTP*)

6.1 DHCP ja oletusyhdyskäytävä

Hämeenlinnan tehtaan verkko käyttää reititykseen OSPF-protokollaa, joka on jaettu kolmeen alueeseen. Verkon runko, jota kutsutaan nimellä *Backbone*, muodostaa ensimmäisen alueen. Tuotantoverkko muodostaa tehtaan toisen OSPF-alueen, joka käsittää tehtaan tuotantoympäristössä toimivat laitteet sekä kytkimet. Toimistoverkko on kolmas OSPF-alue, joka nimensä mukaisesti sisältää tehtaan toimistoverkon laitteet. Elvyttämöalue kuuluu tehtaan tuotantoverkon piiriin, jossa DHCP-palvelut eivät ole käytössä. Tästä syystä kaikille aliverkon laitteille tullaan asettamaan staattiset IP-osoitteet, joten konfiguraatiossa ei tulla käyttämään DHCP-palveluita.

Elvyttämöalueen aliverkko yhdistyy *Backbone*-alueeseen oletusyhdyskäytävän kautta, joka sijaitsee itse tehdasrakennuksen jakelukeskuksessa. IP-allokaatiossa määritelty osoite xxx.xxx.xxx.xxx on tunniste R0605BC1-kytkimeen, joka mahdollistaa tiedonkulun muihin verkkoihin. Oletusyhdyskäytävän määrittely yksinkertaisuudessaan tehdään seuraavasti:

```
ip default-gateway xxx.xxx.xxx.xxx
```

6.2 Errdisable recovery

Konfiguraatioissa on huomioitu tehdastuotannon tarpeet. Yhteyksien jatkuvaan toimivuuteen perustuvan *errdisable recovery all* -parametrin avulla yhteyden palautuminen vikatilanteesta on automaattinen. Kuitenkaan tämä ei ole pysyvä ratkaisu, vaan vikatilanteen sattuessa ylläpidon tehtävänä on selvittää ongelman lähtökohta ja korjata tilanne. Parametrin tarkoituksena on toimia kokonaisvaltaisen tuotannon pysäytyksen estäjänä. Ilman kyseistä konfiguraatioita tukihenkilöiden pitäisi jokaisen ongelmatilanteen jälkeen tehdä manuaalinen portin alasajo *shutdown*-komennon avulla, sekä nostaa portti takaisin toimintavalmiuteen *no shutdown* -komennolla. Tästä syystä konfiguraatiossa huomioitiin myös aikaintervalli, jolla kytkimen portit palautuvat virhetilastaan. Oletusarvoisesti kytkimen portit pyrkivät palautumaan virhetilasta 300 sekunnin välein. Yrityksen yleisen konfigurointiohjeistuksen mukaisesti kytkimille määritellään 60 sekunnin aikaintervalli, jonka aikana portti voi palautua vikatilanteesta. Tämä antaa tukihenkilöille joustavamman vasteajan ongelmatilanteisiin, eikä tuotanto pahimmassa tapauksessa pysähdy.

6.3 Porttiasetukset

Porttikohtaisten konfiguraatioiden määrittely oli myös suuressa roolissa työtä tehdessä. Vanhempien laitteiden asetuksissa oli määritelty porttinopeuksia käytöstä poistuneiden laitteiden mukaan. Uuteen verkkoon liitettävien laitteiden vaatimusten tarkistuksen jälkeen selvisi, ettei vanhan konfiguraation mukaisia *half duplex* -asetuksia enää tarvittu, joten jokainen portti toimisi jatkossa *full duplex* -asetuksella. Näiden lisäksi tehdasympäristön vaatimusten mukaisesti laitteiden yhteyksien palautumisen tulisi olla mahdollisimman nopeaa, joten porttiasetuksiin määriteltiin *spanning-tree portfast* -parametri. Tiedossa myös oli, ettei näihin portteihin koskaan yhdistettäisi toista kytkintä, joten haitallisten silmukoiden muodostuminenkaan ei olisi uhka.

Kytkinten välinen liikenne kulkee kuitukaapeleiden kautta, joten konfiguraatiossa otettiin huomioon kuituliittimien lisääminen kytkinten GigabitEthernet-portteihin. Porteissa hyödynnetään Ciscon SFP-moduuleita, jotka tarjoavat kustannustehokkaan ratkaisun kuitukaapeloinnille. Kytkimessä on kaksi GigabitEthernet-porttia, jotka ovat niin sanottuja ”combo”-portteja. Tämä tarkoittaa sitä, että näihin portteihin voidaan asentaa joko moduulin avulla kuituyhteys, tai sitten RJ45-kaapelia käyttäen normaali yhteys muihin laitteisiin. Combo-porttien käytössä on syytä huomata, etteivät kuituportit toimi samanaikaisesti kupariporttien kanssa.

Verkkoympäristössä hyödynnetään LC (*Lucent Connector*) Duplex/FC (*Fix Connector*) liittimillä varustettua monimuotokuitua, joka tukee suuren volyymin tietoliikennettä lyhyellä matkalla. Kytkimiin asennettavien kuituliittimet tukevat LC-kytkentää ja tietoliikennekaapeissa olevat kuitukytkentäpaneelit FC-kytkentää.

Porttiasetukset tapahtuvat käskyillä:

```
interface FastEthernet0/1-24
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet0/1
 description xxx
 switchport mode access
 media-type sfp
 duplex full

interface GigabitEthernet0/1-2
 description xxx
 switchport mode access
 media-type sfp
 duplex full
```

Parametri media-type sfp mahdollistaa kuituliittimen tunnistuksen GigabitEthernet-portissa.

6.4 VLAN

VLAN-konfiguraatiossa otettiin huomioon opinnäytetyöni tarkoitus. Aliverkkojen sekoittuminen keskenään sekä IP-osoitteiden puutteen takia vanhasta VLAN:sta siirryttiin Elvyttämölle tarkoitettuun VLAN:iin. Uuteen aliverkkoon siirtyminen vapauttaa vanhasta IP-osoitteita uuteen käyttöön ja mahdollistaa tulevaisuudessa uusien laitteiden lisäämisen sinkityslinjoille. Vanhan aliverkon tapaan uuteen, Elvyttämölle tarkoitettuun aliverkkoon, laadittiin 128 osoitteen kokoinen osoiteavaruus, sillä laitemäärien takia ei ole suotavaa pienentää sen kokoa. Lisäksi tulevaisuuden laiteinvestoinnit lisäävät IP-osoitteiden tarvetta, joten skaalautuva verkko on tärkeä. VLAN-asetukset toteutettiin seuraavilla käskyillä:

```
vlan 2329
 name 2329

interface FastEthernet0/1-24
 switchport access vlan 2329
interface GigabitEthernet0/1-2
 switchport access vlan 2329


interface Vlan2329
 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
 no ip route-cache
```

6.5 SNMP ja pääsylistat

SNMP eli *Simple Network Management Protocol* on valmistajariippumaton verkonhallintaprotokolla, joka määrittelee verkonhallintaohjelmiston toiminnot, sekä selittää, miten raportti on määritelty ja lähetty. Standardi myös määrittelee viestin muodon vastaanottavalle laitteelle samalla yrittäen korjata virheitä tai välttää virhetiloja. [3, s. 574.]

Konfiguraatiossa määritellään laitteille pääsylistojen avulla palvelimet, joilta laitteet voivat lataa tai siirtää ennalta määriteltyjä asetuksia. Tämän lisäksi määritellään tiedonsiirtoprotokolla, jota kytkimet käyttävät asetusten siirtoon ja tallennukseen. SNMP-konfiguraatio toteutettiin seuraavilla parametreilla:

```
access-list 10 permit xxx.xxx.xxx.xxx
access-list 10 permit xxx.xxx.xxx.xxx
```

```
snmp-server view backup ccCopyEntry included
snmp-server community RTT view backup RW 10
snmp-server community production RO
snmp-server tftp-server-list 10
snmp-server host xxx.xxx.xxx.xxx production
snmp-server host xxx.xxx.xxx.xxx production
snmp-server file-transfer access-group 10 protocol tftp
snmp ifmib ifindex persist
```

6.6 NTP

NTP tulee sanoista *Network Time Protocol*. Se on UDP-pohjainen protokolla täsmällisen aikatiedon välittämiseen laitteiden välillä verkossa. NTP:n tarkoituksena on synkronoida kaikki verkossa olevat laitteet keskenään, jotta aikapohjaiset toiminnot toimisivat halutulla tavalla. Näitä ovat muun muassa lokitiedostojen muodostaminen. Verkon laitteet päivittävät kellonsa NTP-palvelimen kautta, jonka konfiguroiminen tapahtuu seuraavalla tavalla:

```
ntp clock-period 36029338
ntp server xxx.xxx.xxx.xxx
```

Manuaalista *ntp clock-period* määritystä ei vaadita, sillä kytkin asettaa sen itse.

6.7 STP

STP eli *Spanning Tree Protocol* tärkeimpänä tehtävänä voidaan pitää niin sanottujen silmukoiden muodostumista verkossa. Kun laitteita kytketään ristiin, verkkoon voi muodostua silmukoita, joissa data jää kulkemaan laitteiden välillä loputtomasti aiheuttaen verkolle kuormitusta ja pahimmassa tapauksessa pysäyttäen sen kokonaan. Protokollan avulla voidaan laskea edullisin reitti, jotka pitkin data voi kulkea paikasta A paikkaan B. Protokolla sulkee tarpeettomat yhteyden siirtäen ne *blocking*-tilaan, jolloin kaikki data on linkissä estetty mutta voi vastaanottaa BPDU-paketteja. BPDU-pakettien vastaanotto on elintärkeää, sillä osallistuminen verkkomuutoksen yhteydessä suoritettavaan Root-kytkimen valintaan ei muuten onnistuisi. Esimerkiksi kahdennetussa yhteydessä toinen linkeistä poistuu käytöstä ja tulee ainoastaan käyttöön silloin, kun primäärilinkki syystä tai toisesta lakkaa toimimasta siirtyen *forwarding*-tilaan. Konfiguraatio suoritetaan seuraavalla tavalla:

```
spanning-tree mode rapid-pvst

interface GigabitEthernetx/x
 description xxx
 switchport access vlan 2329
 switchport mode access
 duplex full
 spanning-tree link-type point-to-point
```

Rapid-PVST+ tulee sanoista *Rapid Per-VLAN Spanning Tree+* ja tarkoittaa sanansa mukaisesti protokollaa, joka ylläpitää jokaisesta verkossa konfiguroidusta VLAN:sta oman *Spanning Tree* -instanssinsa. Rapid-PVST+ -protokollan tärkeimpänä ominaisuutena voidaan pitää kuorman jakamista verkossa sekä reagointia topologiamuutoksiin lyhyellä aikavälillä verrattuna edeltäjiinsä. Kytkinten välille on konfiguraatiossa luotu *point-to-point*-linkit, jolloin laiteviasta voidaan toipua nopeasti topologian muuttuessa. Laitevian tapahtuessa protokolla käynnistää äänestysprosessin, jonka avulla määritellään uusi Root-kytkin omalle instanssillensa. Rapid-PVST+:ssä tämä kestää noin yhden sekunnin verran ja on näin ollen mainiosti soveltuva ratkaisu tuotantoympäristöön. Protokolla tukee sekä ISL- (*Cisco Inter-Switch Link*) että 802.1Q-pakettikapselointia. Edellisissä kohdissa mainitut STP-konfiguraatiot on jätetty pois selkeyden vuoksi.

7 Verkon toteutus

Verkon toteutuksen alkuvaiheessa ilmeni ongelma, jonka takia opinnäytetyötäni jouduttiin rajaamaan uudelleen. Tehdastuotannon ollessa ympärivuorokautista tietoliikenteen pitää olla katkeamatonta elvyttämöalueelta muihin verkkoihin. Tämä aiheuttaa sen, ettei aliverkkovaihdosta voida toteuttaa sellaisenaan ennen kuin alueella suoritetaan tuotannon seisakki, joko vuosihuollon tai hallitun sähkökatkoksen aikaan. Tästä syystä työni ei tule käsittelemään laitteiden IP-osoitteiden vaihdoksia tai verkkotestausta. Työssä ei myöskään tulla esittelemään valmista verkkoa, sillä tuotantoyksikön pysäytys vaatisi kattavan aikataulusuunnitelman, eikä määräaikaisen työsuhteeni aikana tällaisen laatiminen ollut ajallisesti mahdollista.

Työn uudelleenrajaus ei kuitenkaan vaikuttanut toteutuksen ensimmäisiin vaiheisiin, sillä ongelmista huolimatta uuden aliverkon kytkinten asennus ei vaikuttaisi sen hetkiseen verkkoon millään tavalla. Laitteiden asennustyöt suoritettiin nykyisten laitteiden rinnalle, jotta tulevaisuudessa, kun toimeksianto uuteen aliverkkoon siirtymisestä tapahtuu, voidaan kytkennälliset toimenpiteet suorittaa nopeasti laitekaapeleiden paikkaa vaihtamalla. Tämä tarkoittaa sitä, että vaihdoksen yhteydessä ristikytkentäpaneelista tulevien laitekaapeleiden paikkaa siirretään vanhasta kytkimestä rinnalle asennettuun kytkimeen.

Laiteasennuksien lisäksi jokaiseen uuteen kytkimeen asennettiin SFP-moduuli, jonka avulla kuitukaapeleiden kytkentä tietoliikennekaapin yläosassa sijaitsevaan kuitupaneeliin mahdollistui.

Uudesta työn rajauksesta huolimatta kytkinasennuksien lisäksi kuitukytkennät pystyttiin toteuttamaan suunnitelmien mukaan, jolloin työn tuloksena syntyi uuden aliverkon runko ja siihen sovellettava, liitteen 3 mukainen, IP-osoitesuunnitelma lopulliseen toteutukseen.

8 Tietoverkon kehittäminen

Verkon palvelevuuden hallinta yritysympäristössä on merkitykseltään suuri. Aiheena se ei kuitenkaan ole aina täysin yksiselitteinen, sillä hallinnan painopisteet määräytyvät organisaatioiden välillä hyvin yksilöllisesti. Kokemukset sekä havainnot määrittelevät yleensä toimintaperiaatteita, joita organisaation sisällä noudatetaan. On kuitenkin olemassa hyvän toiminnan periaatteita, joiden avulla organisaation toimintaa pystytään kehittämään parempaan suuntaan.

Aktiivinen riskien kartoittaminen on tärkeässä osassa ennakoivassa toiminnassa uhkakuvia vastaan. Laiterikoista sekä tietoturvamurroista palautuminen on huomattavasti tehokkaampaa, kun tiedetään riskitilanteeseen liittyvät toimintatavat. Tällainen ajatustapa edistää myös toimintaa työympäristön muilla osa-alueilla, sillä sitä ei ole sidottu vain informaatioteknologiaan. Tämän lisäksi retroaktiivisen raportointisysteemin kehitys on tärkeässä roolissa, sillä tapahtumien jälkeinen asian läpi käynti auttaa varautumaan tulevaisuudessa paremmin samanlaisiin riskeihin ja samalla niihin kohdistuvia korjaustoimenpiteitä voidaan käynnistää heti ongelman ilmaannuttua.

Riskien kartoituksen yhteydessä henkilöstön tietoturva-ajattelua tulisi kehittää. Nyky-yhteiskunnan suurimpiin uhkiin lukeutuu tietomurrot yrityksiä vastaan, jolloin rahalliset vahingot saattavat nousta hyvinkin suuriksi. Tietoliikennetason muutoksien lisäksi esimerkiksi yksilön omaa tietoturvaa ei tulisi jättää huomioimatta. Ajatusmallin siirros ”tutusta ja turvallisesta” tulisi suunnata kohti järkevää ja kestävää ajattelua. Käytännössä tämä tarkoittaa sitä, ettei esimerkiksi laitesalasanoja tulisi luovuttaa kuin niille, jotka niitä oikeasti tarvitsevat. Verkkolaitteita konfiguroitaessa on suositeltavaa hyödyntää ulkoista todennuspalvelinta (*Radius*), jolloin normaalitilanteessa ylläpidollisia tehtäviä suorittava henkilö käyttäisi omia henkilökohtaisia käyttäjätunnuksiaan sisäänkirjautumiseen. Paikallisten käyttäjätunnuksia tulisi siis käyttää ainoastaan silloin, kun todennuspalvelin ei jostain syystä toimi, jolloin ylläpitäjien on silti mahdollista paikallisesti kirjautua verkkolaitteille.

Ylläpidollisista tehtävistä puhuttaessa on lisäksi hyvä huomioida lokitiedostojen tärkeys muutostöitä tehdessä. Lokipalvelimet toimivat elintärkeänä työkaluna vikatilanteissa, joissa esimerkiksi muutostyön seurauksena etäyhteys konfiguroitavaan laitteeseen on katkennut. Vikatilanteeseen vastaavan henkilön on tässä tapauksessa yksinkertaisimmillaan tarkistettava viimeisimmät kyseiseen laitteeseen tehdyt muutokset lokipalvelimelta ja toimia niiden mukaisesti. Lokitiedostoista saadaan myös selville viimeisimpien

muutosten tekijä, jolloin väärinkäsityksiltä voitaisiin välttyä. Tulevaisuudessa muutosten tekijää voidaan ohjeistaa toimimaan oikeaoppisesti vikatilanteiden välttämiseksi.

Verkkotasolla kehityksen suuntaa tulisi ohjata kohti uudempaa laitteistoa. Monissa nykypäivän yrityksissä tukeudutaan edelleen vanhempaan laitteistoon, mikä tarkoittaa sitä, ettei lähitulevaisuudessa kyseisille laitteille implementoida vaatimusten tasoista tietoturvaa tai tukea vikatilanteissa.

9 Yhteenveto

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa SSAB:n Hämeenlinnan tehtaan elvyttämöalueelle uusi aliverkko. Työn painopisteenä oli koko alueen uudelleen kartoitus käyttämällä monia erilaisia dokumentointitekniikoita sekä ohjelmistoja. Teoriatason tutkimus auttoi työssäni ymmärtämään verkon monimuotoisuutta sekä haasteita, joita erilaisten tekniikoiden yhdisteleminen saattaa aiheuttaa. Tehdasympäristön huomiointi oli myös mielekäs lisä työnkuvaan, sillä koulussa läpikäydyt asiat yhdistettynä työssä opittuun tietoon muodostivat mielenkiintoisen lähtökohdan toimeksiannon asettamiin vaatimuksiin.

Jälkeenpäin ajateltuna työssäni olisin voinut kiinnittää huomiota enemmän aikataulutukseen ja ennakoida verkon käyttöönottoon liittyviä ongelmia, kuten esimerkiksi taukoamaton tuotanto tehdasympäristössä.

Kokonaisuutena pidän opinnäytetyötäni kuitenkin onnistuneena, vaikka täydellistä toteutusta aliverkosta ei saatu vietyä loppuun. Puuttumaan jäi verkon laitteiden staattiset IP-vaihdokset, jotka IT-henkilöstö voi laatimani IP-osoitesuunnitelman avulla viimeistellä. Verkon testaus voidaan myös suorittaa ennen lopullista uuteen aliverkkoon siirtymistä verkkolaitteiston ollessa valmiiksi asennettuna.

Lähteet

1 SSAB. Verkkodokumentti. https://fi.wikipedia.org/wiki/SSAB. (Luettu 13.3.2017).

2 SSAB Europe Oy. Verkkodokumentti. https://www.ssab.com/company/about-ssab/sites-all-over-the-world. (Luettu 13.3.2017).

3 Jaakohuhta, Hannu. 2011. Tietotekniikan sanakirja. Helsinki: Redame.fi.

4 Colliander, Andreas. 1999. Verkkodokumentti. http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Essays/essee_OSI.html (Luettu 13.3.2017).

5 Hakala, Mika & Vainio, Mika. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy.

6 Mullins, Michael. Verkkodokumentti. http://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/. (Luettu 20.3.2017).

7 TCP/IP-viitemalli. 2017. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/TCP/IP-viitemalli. (Luettu 15.3.2017).

8 Kaario, Kimmo. 2002. TCP/IP-verkot. Jyväskylä: Docendo Finland Oy.

9 IPv6 Address tutorial. Verkkodokumentti. https://www.tutorialspoint.com/ipv6/ipv6_address_types.htm (Luettu 26.6.2017).

10 RFC 4941. Verkkodokumentti. https://tools.ietf.org/html/rfc4941. (Luettu 18.10.2017).

11 RFC 4861. Verkkodokumentti. https://tools.ietf.org/html/rfc4861. (Luettu 28.6.2017).

12 Puska, Matti. 2000. Lähiverkkojen Tekniikka. Jyväskylä: Gummerus Kirjapaino Oy.

13 Jaakohuhta, Hannu. 2005. Lähiverkot – Ethernet. Helsinki: Edita Prima Oy.

14 Pyyskänen, Seppo. 2007. Teollisuuden laiteverkot: Johdatus väylätekniikkaan. Helsinki: Picaset Oy.

15 Redundancy with HSRP. Verkkodokumentti. http://www.techrepublic.com/article/ensure-cisco-router-redundancy-with-hsrp/. (Luettu 29.6.2017).

16 Infoblox. Verkkodokumentti. https://www.infoblox.com/products/ipam-dhcp. (Luettu 23.4.2017).

17 University of Florida. Verkkodokumentti. https://net-services.ufl.edu/provided-services/dns-dhcp/infoblox-reference/getting-started.html. (Luettu 24.4.2017).

18 Infoblox. Verkkodokumentti. https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-whitepaper-ip-address-management.pdf. (Luettu 24.4.2017).

19 Efecte. Verkkodokumentti. https://fi.wikipedia.org/wiki/Efecte. (Luettu 24.4.2017).

Projektisuunnitelma

Aloitus

- Alueen kartoitus
- Verkkokuvien päivitys ajan tasalle
- Laitteiden kartoitus alueella
- Kytkinten konfiguraation tarkistus

Suunnittelu

- Kytkinten porttien takana olevien laitteiden kartoitus
- NetViz – kaavion tekeminen
- Aliverkon suunnittelu
- IP-osoitteiden allokaatio
- Tietoturvallisuus

Toteutus

- Uusien kytkinten konfiguraatio
- Kytkentöjen tekeminen
- Laitteiden IP-osoitteiden muutos
- IPAM