TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

OPINNÄYTETYÖ

VERKON DOKUMENTOINTI

Työn tekijä: Marko Pakarinen
Työn ohjaaja: Arja Kitunen
Työn valvoja: Kari Järvi

Työ hyväksytty: 21. 3. 2010

Kari Järvi
Yliopettaja

OPINNÄYTETYÖN TIIVISTELMÄ

Työn tekijä: Marko Pakarinen	
Työn nimi: Verkon dokumentointi	
Päivämäärä: 3.2.2010	**Sivumäärä:** 35 s.
Koulutusohjelma: Tietotekniikka	**Ammatillinen suuntautuminen:** Tietoverkot
Työn ohjaaja: yliopettaja Kari Järvi, Metropolia Ammattikorkeakoulu **Työn ohjaaja:** Atk-päällikkö Arja Kitunen, Suomen Syöpäyhdistys Ry	

Tässä insinöörityössä esitetään verkon dokumentoinnin perusteita ja hyviä toimintatapoja. Niiden pohjalta on luotu dokumentaatio Suomen Syöpäyhdistykselle. Ensiksi työssä tehdään katsaus verkon suunnittelun perusteisiin, jossa esitetään yleiset periaatteet, joilla verkkoja suunnitellaan.

Suunnittelun perusteiden jälkeen tutustutaan tietoturvan osa-alueisiin lyhyesti sekä tietoturvan toteuttamiseen palvelimissa ja työasemissa. Verkon tietoturvassa esitetään muutama yleisin tekniikka, joilla tietoturvaa voi parantaa.

Edellisten jälkeen siirrytään itse dokumentointiasioiden pariin. Työssä kerrotaan dokumentoinnin hyödyistä ja hyvistä toimintatavoista. Dokumentointiin käytettävistä työkaluista esitetään perustoimisto-ohjelmat, kuten Word ja Excel lyhyesti sekä dokumentointiin varta vasten tarkoitetuista ohjelmista Microsoft Visio ja NetViz.

Työn lopuksi esitellään Suomen Syöpäyhdistykselle tehtyä dokumentointia, joka on pyritty luomaan työssä esiteltyjen dokumentoinnin perusteiden mukaisesti. Dokumentoinnin on tarkoitus auttaa verkon hahmottamisessa sekä muutosten vaikutuksen arvioinnissa, kun verkkoa muutetaan ajan myötä.

Työn tuloksia voi käyttää verkon dokumentoinnin suunnittelussa suuntaviivoina. Tämä työ loi pohjan jatkuvalle verkon dokumentoinnille Suomen Syöpäyhdistyksessä.

Avainsanat: dokumentaatio, dokumentointimenetelmät, verkon suunnittelu, tietoturva

Metropolia

ABSTRACT

Name: Marko Pakarinen

Title: Network documentation

Date: 3.2.2010 **Number of pages:** 35

Department: Information Technology

Study Programme: Information Networks

Instructor: Kari Järvi, Principal Lecturer

Supervisor: Arja Kitunen, IT-manager

This graduate study examines optimal methods and procedures for creating documentation of networks. Based on this, network documentation was created for the Finnish Cancer Organisation and is partly presented in the study.

The study begins with an overview of the fundamentals for network design, which generally set out the principles by which networks are planned. After that, a look is taken on network security and how to improve security on desktops and servers is discussed.

The latter part of the study focuses on the theory of documentation and two of the most common documentation software are presented, i.e. Microsoft Visio and NetViz. After the theory part the documentation which was made for the organisation is presented. It was created according to the principles described above. The aim is to help to outline the network and also to predict the effects of changes as the network will be further developed.

Keywords: documentation, documentation methods, network design

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

1 JOHDANTO

Suurehkon yritysverkon suunnittelu ja ylläpito on iso tehtävä. Suunnittelussa pitää ottaa monia asioita huomioon ja määrittää, mitä ominaisuuksia verkolta vaaditaan. Verkon pitäisi olla toteutettavissa kohtuullisin kustannuksin, ottaen samalla huomioon mahdollisesti kasvavat verkon liikennemäärät. Sen pitää olla myös helposti laajennettavissa. Kun suunnittelut on tehty ja verkko rakennettu, alkaa verkon ylläpitäminen, johon osana kuuluu verkosta tehdyn dokumentaation ylläpitäminen.

Suomen Syöpäyhdistyksessä verkon dokumentaatio oli melko puutteellinen, joten sitä päätettiin parantaa, jotta verkon hahmottaminen ja mahdollisten ongelmakohtien paikantaminen helpottuisi.

Tässä opinnäytetyössä käsitellään verkon suunnitteluun liittyviä asioita, mietitään tietoturvan toteuttamista sekä mitä hyvän dokumentoinnin pitäisi sisältää ja mitä työkaluja sen toteuttamiseen tarvitaan.

Aluksi työssä esitellään verkon suunnitteluun sopiva suunnittelumalli, jolla verkon suunnittelutyön pystyy jakamaan osiin, jolloin suunnittelu helpottuu. Työssä kerrotaan periaatteet, joilla verkko pitäisi toteuttaa ja miten sen toimintaa voi testata.

Tietoverkon suunnittelun periaatteiden jälkeen mietitään laajassa mittakaavassa tietoturvan toteuttamista. Tämän jälkeen tarkastellaan käytännönläheisemmin tietoturvan toteuttamista työasemissa, palvelimissa ja verkossa yleensäkin.

Tietoturva-asioiden jälkeen perehdytään dokumentoinnin toteuttamiseen. Tässä osassa kerrotaan dokumentoinnin hyödyistä ja siitä, miten dokumentointi rajataan niin, että sen ylläpitämisestä ei tule liian suuri taakka verkosta vastaavalle henkilöstölle. Lisäksi esitellään pari dokumentointiin hyvin soveltuvaa ohjelmaa.

Lopuksi esitellään Suomen Syöpäyhdistykselle tehtyä dokumentointia. Kerrotaan, mitä tavoitteita dokumentaatiolle asetettiin ja mitä pohdintoja syntyi dokumentoinnin edetessä. Lisäksi kerrotaan, mitä jatkokehitystä dokumenteille on vielä suunnitteilla.

2 TIETOJÄRJESTELMÄN SUUNNITTELU JA VAIHEJAKOMALLI

Tietoverkkojen merkitys yritysmaailmassa on kasvanut vuosikymmenten saatossa osaksi tuotannollista toimintaa. Tietoverkon vikaantuminen saattaa aiheuttaa liiketoiminnan pysähtymisen, josta voi aiheutua suuriakin kuluja. Käyttökatkosten välttämiseksi on tullut tärkeäksi, että verkosta on ajantasainen dokumentointi ja sen suunnittelussa on riittävästi hyödynnetty vikasietoisuutta lisääviä ja riskejä vähentäviä toimintatapoja.

Tarvittavien toimintojen määrä määrittelee, kuinka paljon alustavaa suunnittelua verkon rakentaminen vaatii. Pienen yrityksen verkko saattaa koostua vain parista verkkolaitteesta ja työasemasta sekä palvelimesta ja sen voi melko helposti saada toimimaan riittävän luotettavasti ilman kovin suurta suunnitteluprosessia ja tarvekartoituksia. Suuremmassa verkossa, joka koostuu sadasta tai useammasta työasemasta ja palvelimesta, suunnitelmallisuus korostuu ja laitteiden valinnassa pitää enemmän miettiä, mitä ominaisuuksia tarvitaan verkon toteuttamiseksi.

Isojen tietoverkkojen suunnittelu on mittava projekti. Suunnitelma edellyttää koko tietojärjestelmän ja organisaation kaikkien toimintojen kartoittamisen. Kattava suunnitelma käsittää kaiken käytettävistä sovelluksista fyysiseen kaapelointiin asti. Kaapeloinnin suunnittelulta vältytään ainakin osittain siinä tilanteessa, että se on valmiiksi tehtynä. Näin on usein kaupunkien vuokrattavissa toimistotiloissa. Sekä uuden verkon että vanhan verkon modernisoinnin suunnittelussa voidaan käyttää systeemityön vaihejakomallia, joka pilkkoo projektin hallittaviin kokonaisuuksiin, joille voidaan sitten asettaa omat aikataulunsa.

Systeemityön vaihejakomallissa tietojärjestelmän rakentaminen jaetaan seitsemään eri vaiheeseen:

- esitutkimukseen
- määrittelyyn
- suunnitteluun
- toteutukseen
- testaukseen
- käyttöönottoon
- ylläpitoon.

Vaiheet eivät välttämättä ole peräkkäisiä, sillä ne jaetaan usein aliprojekteiksi, joiden valmistuminen ei ole riippuvainen toisen vaiheen valmistumisesta. Tällöin määrittely-, suunnittelu- ja toteutusvaiheen töitä voidaan tehdä osittain samanaikaisesti.

Suunnittelutyön jokaiseen vaiheeseen kuuluu tehdyn työn dokumentointi. Dokumentit on huomattavasti helpompi tehdä suunnittelun yhteydessä, kun tehdyt asiat ja yksityiskohdat ovat vielä tuoreessa muistissa. Suunnittelun aikana tehdyt dokumentit luovat pohjan verkon dokumentaatiolle, joka helpottaa verkon valmistuttua sen ylläpitämistä ja päivittämistä. [1, s. 406.]

2.1 Esitutkimus

Esitutkimuksessa kerätään tietoja, joita projektissa tarvitaan ja yleisellä tasolla kartoitetaan projektin sisältö. Projektin käyttöön kerätään eri tietolähteistä noudatettavien standardien kuvaukset ja aiempien tietojärjestelmien dokumentit, jos sellaisia on. Myös erilaiset ohjelmisto- ja laitemanuaalit voivat olla hyödyllisiä suunnittelutyössä. [1, s. 407.]

2.2 Määrittely

Määrittelyvaiheen sisältö riippuu paljolti siitä, ollaanko rakentamassa täysin uutta tietojärjestelmää vai korvataanko aiempi tietojärjestelmä uudella, tehokkaammalla järjestelmällä. Määrittelyvaiheessa selvitetään tietojärjestelmältä vaadittavat ominaisuudet ja määrittelyn apuna tehdään usein tarvekartoituksia kysymällä käyttäjien tarpeista ja toiveista. Peruskäyttäjien huomioon ottamisella määrittelyvaiheessa on myös se hyvä vaikutus, että muutosvastarinta vähenee.

Määrittelyn tärkeimpiä työvälineitä ovat erilaiset analyysit. Täysin uudelle tietojärjestelmälle keskeisimmät analyysit ovat

- tietotarveanalyysi
- tietovarastoanalyysi
- tietovuoanalyysi.

Vanhan järjestelmän päivityksen tapauksessa tehdään edellisten lisäksi

- ongelma-analyysi
- syy-seuraus-analyysi.

Tietotarve-, tietovarasto- ja tietovuoanalyysit selvittävät muun muassa, minkälaisia tietoja järjestelmään syötetään ja mitä tietoja otetaan ulos ja kenellä tai millä organisaation osalla pitää olla pääsy tietoihin. Tämän lisäksi pohditaan eri tallennustapoja näille tiedoille ja selvitetään, miten tieto kulkee organisaatiossa eri toimintaprosessien sisällä sekä niiden välillä.

Ongelma-analyysillä pyritään selvittämään vanhan tietojärjestelmän puutteita: miksi järjestelmä ei toimi riittävän tehokkaasti, mitä puutteita sen ylläpitämissä tiedoissa on, onko järjestelmässä tietoturvaongelmia jne. Syy-seuraus-analyysillä pyritään löytämään ne seikat, jotka aiheuttavat aiemman tietojärjestelmän puutteet ja heikkoudet.

Määrittelyvaiheen tarkoituksena on löytää vastaus kysymykseen: ”Mitä ominaisuuksia tietojärjestelmällä pitää olla?”. [1, s. 407.]

2.3 Suunnittelu

Suunnitteluvaiheessa etsitään eri ratkaisumalleja määrittelyssä asetettujen ominaisuuksien saavuttamiseksi. Toteutustapoja voi olla useita. Koska tietojärjestelmät ovat nykyisin hyvin monimutkaisia, voi olla, että kaikkia määrittelyssä asetettuja vaatimuksia ei voida täyttää, koska jonkun halutun ominaisuuden toteuttamisella voi olla epäsuotuinen vaikutus johonkin toiseen ominaisuuteen.

Suunnitteluvaiheeseen kuuluvat myös kustannus-hyöty-analyysit, joilla arvioidaan eri ominaisuuksien toteutuksien taloudellista järkevyyttä.

Ratkaisuvaihtoehtoja arvioidaan usein nelikenttäanalyysiksi kutsutulla SWOT-analyysillä (Strenghts, Weaknesses, Opportunities, Threats), jolla haetaan kunkin ratkaisun vahvuudet ja heikkoudet (nykyhetki) sekä mahdollisuudet ja uhkakuvat (tulevaisuus).

Suunnittelussa kannattaa valita kansainvälisiin standardeihin perustuvia ratkaisuja aina, kun se on mahdollista, koska niiden käyttö helpottaa eri tietojärjestelmien yhteistoimintaa. [1, s. 409.]

2.4 Toteutus

Toteutusvaiheessa aloitetaan varsinainen tietojärjestelmän ja verkon rakentaminen. Joitakin suunnitelmien yksityiskohtia saatetaan joutua vielä muuttamaan toteutusvaiheessa.

Toteutusvaiheen aikana luodaan myös dokumentointia, johon kirjataan tehdyt asetukset ja tarpeen mukaan kommentoidaan niitä. Dokumenttien ei ole kuitenkaan tarkoitus toimia asennusohjeina, vaan dokumentin lukijan oletetaan tietävän, mistä dokumentoidut asetukset löytyvät. [1, s. 410.]

2.5 Testaus

Testausvaiheessa varmistetaan järjestelmien toiminta. Testaus voidaan jaotella toiminnalliseen, määrityksenmukaisuus- ja standardinmukaisuustestaukseen. Toiminnallisella testauksella varmistetaan esimerkiksi asennettujen laitteiden ja kaapelointien toiminta. Määrityksenmukaisuustestauksessa katsotaan, onko asetetut vaatimukset saavutettu. Standardinmukaisuustestauksessa käytetään standardien omia testistandardeja hyväksi. Ne määrittelevät, millaiset testitulokset ovat hyväksyttäviä.

Testauksessa tehdään myös kuormitusanalyyseja verkolle ja testataan tietoturvallisuutta erilaisilla tietoturvaskannereilla ja hakkereiden käyttämillä sovelluksilla. Oman verkon testauksessa hakkereiden työkalut eivät ole laittomia.

Tietoverkkojen testaamiseen käytetään yleensä liikenne- ja kuormitusanalyysiä. Verkkoa kuormitetaan joko erillisillä kuormituksen simulointiohjelmilla tai käyttämällä tietojärjestelmiä ruuhkakäyttöä vastaavalla intensiteetillä. Testin aikana suoritetaan liikenneanalyysiä, jonka avulla nähdään, tarjoaako verkko määritysten mukaisen kapasiteetin ja kuinka paljon tiedonsiirtovirheitä tapahtuu.

Myös verkon tietoturvallisuutta voi testata erilaisilla tietoturvaskannereilla ja hakkereiden käyttämillä sovelluksilla, joita löytyy runsaasti Internetistä. Niiden käyttö oman verkon testaamisessa ei ole laitonta. [1, s. 410.]

2.6 Käyttöönotto

Käyttöönottovaiheessa tietojärjestelmä otetaan tuotantokäyttöön. Vaiheeseen kuuluu tarkkailujakso, ja monesti uuden tietojärjestelmän rinnalla käytetään jonkin aikaa myös vanhaa järjestelmää, jolloin molempiin järjestelmiin syötetään samat tiedot. Tällä menetelmällä varmistetaan uuden järjestelmän toiminta. Huonona puolena on, että kahta järjestelmää yhtä aikaa ylläpidettäessä se sitoo henkilöstöä lähes kaksinkertaisen määrän. [1, s. 411.]

2.7 Ylläpito

Projekti päättyy käyttöönottovaiheeseen, jonka jälkeen alkaa järjestelmän ylläpitäminen. Ylläpitämiseen kuuluu rutiininomainen ylläpito sekä projektin aikana luotujen dokumenttien päivitys, kun muutoksia järjestelmään on tehty. [1, s. 411.]

3 TIETOVERKOISTA

3.1 Kaapelit

Kaapelointikustannuksessa ei ole järkevää säästää siksi, että ne ovat keskimäärin vain 5 % lähiverkon kokonaiskustannuksista. Säästäminen voi siis tarkoittaa sitä, että 95 %:n osuudella hankittu osa verkosta ei toimi. Kaapeloinnin tulee palvella vähintään 10 vuotta, joten kasvavat tiedonsiirtotarpeet pitää huomioida.

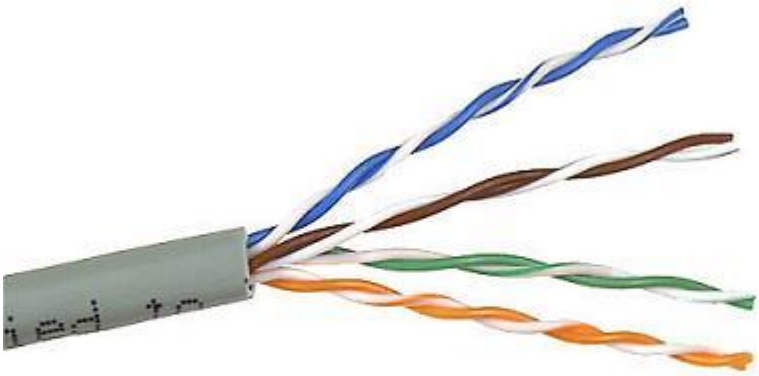
Kaapelointien toteutuksissa noudatetaan yleensä jotain standardia, koska standardien käyttö säästää aikaa - pyörää ei tarvitse keksiä uudestaan. Toimistotilojen kaapelointien suunnittelussa käytetään siihen tarkoitettua standardia EN 50173-1, joka määrittelee kaapeloinnin rakenteen ja kokoonpanon, toteutusvaihtoehdot ja erilaiset suorituskykyvaatimukset. Muita yleisessä käytössä olevia standardeja ovat EN 50173-2, jota käytetään teollisuuskiinteistöihin, ja EN 50173-3 asuinkiinteistöille.

3.1.1 Parikaapelit

Kerroskaapeloinnissa on pitkään ollut käytössä Cat 5 -standardin mukainen kaapelointi, jolla yhdistetään verkon aktiivilaitteet ja työasemat. Cat 6 on vuodesta 2002 lähtien ollut yleisin Suomessa asennettava kaapelointistan-

dardi. Nousukaapeloinneissa on tänä päivänä lähes poikkeuksetta käytössä optinen kuitu.

Parikaapeleissa on kahdeksan johdinta, jotka muodostavat toistensa ympäri kiertäviä johdinpareja. Parikierrolla estetään häiriöiden syntymistä, ja jokaisella parilla on erisuuruinen parikierto, jolla estetään häiriöiden siirtymistä parista toiseen. Parikaapeleita on useita eri tyyppiä: on suojaamattomia ja suojattuja. Suojatuissa kaapeleissa kaapeli ja parit voidaan ympäröidä metallivaipalla, jolla saavutetaan paras suoja ulkoisia häiriöitä vastaan. Suojaustarvetta voi olla, jos kaapelointi menee läheltä voimakkaita magneettikenttiä muodostavia laitteita, kuten muuntajia. Parikaapeli voi olla maksimissaan 100 metriä ilman toistimia tai muita verkkolaitteita välissä. Tätä pidemmissä kaapeleissa tapahtuu jo liikaa signaalin vaimenemista. Kuvassa 1 on esitetty Cat5e-tyypin kaapeli.



Kuva 1. Parikaapeli

3.1.2 Optinen kuitu

Optinen kuitu on parikaapeleihin verrattuna ominaisuuksiltaan huomattavasti parempi, mutta kalliimpi. Se ei ole altis häiriöille sähkömagneettisissa kentissä, ja signaalin vaimeneminen on parikaapeleita vähäisempi, mikä mahdollistaa pidemmät yhtämittaiset kaapelivedot jopa 2000 metriin asti. Optisia

kaapeleita käytetään tavanomaisesti runkoverkoissa ja aluekaapeloinneissa, mutta niiden käyttö on yleistynyt myös kerrostalokaapeloinneissa.

Optisia kuituja on kahta tyyppiä: monimuoto- ja yksimuotokuituja. Monimuotokuiduissa käytetään LED-lähettimiä, jotka hajoittavat sädettä enemmän kuin laser-lähettimet. Valonsäteet kulkevat monimuotokuidussa useaa reittiä. Tämä ilmiö rajoittaa suurinta mahdollista käytettävää taajuutta eli kaistanleveyttä, koska kun pulssit leviävät liikaa, alkaa tiedonsiirrossa tapahtua virheitä.

Yksimuotokuidussa valo etenee yhdessä muodossa, mutta siinäkään ei vältytä kokonaan pulssien levenemiseltä kromaattisen dispersion takia. Tästä huolimatta yksimuotokuiduissa saavutetaan parempi kaistanleveys kuin parhaimmassakaan monimuotokuiduissa. Yksimuotokuiduissa käytetään aina laser-lähetintä. Kuvassa 2 on esimerkki optisesta kaapelista.

Kuva 2. Valokuitukaapeli

3.2 Reititys ja verkon aktiivilaitteet

Kaikki IP-verkon koneet, palvelimet ja työasemat ovat käytännössä reitittimiä. Ne reitittävät TCP/IP-liikennettä oman lähiverkkosegmentin muille koneille tai oletusyhdyskäytävänä toimivalle reitittimelle. Varsinaisten reitittimien tehtävä on ohjata lähiverkkosegmenttien välistä liikennettä sekä ohjata oman verkon ulkopuolelle suuntautuva liikenne oikeaan laajaverkkoon.

Reititystapa voi olla staattinen tai dynaaminen. Staattisessa reitityksessä lähettävä kone tutkii omasta reititystaulustaan, mistä IP-paketin vastaanottaja löytyy. Perusvaihtoehtoja on kolme: vastaanottaja on lähettäjä itse, vastaanottaja on samassa lähiverkkosegmentissä tai vastaanottaja on eri segmentissä kuin lähettäjä. Kun kyseessä on kehyksen lähettäminen oman segmentin koneelle, ARP-protokolla selvittää, mikä MAC-osoite vastaa vastaanottajan IP-osoitetta. Staattisen reitityksen ylläpito tapahtuu manuaalisesti.

Dynaamisessa reitityksessä käytetään erilaisia protokollia, joilla verkon reitittimet jakavat tietoa yhteyksistään toisille verkon reitittimille. Protokollat voi karkeasti jakaa kahteen ryhmään: sisäisiin reititysprotokolliin, jotka soveltuvat hyvin esimerkiksi yrityksen sisäverkon toteutukseen ja ulkoisiin reititysprotokolliin, joita käyttävät suurten Internet-operaattoreiden reitittimet Internetin osaverkkojen välisessä liikenteessä. Osa protokollista perustuu Internet-standardeihin, mutta niiden lisäksi on reititinvalmistajien, kuten Cisco Systemsin kehittämiä protokollia. Standardiprotokollien hyvä puoli on siinä, että ne toimivat eri valmistajien reitittimiä käyttävissä verkoissa, mutta ne usein häviävät suorituskyvyltään ja luotettavuudeltaan reititinvalmistajien protokollille. Reititinvalmistajien protokollien käyttö sitoo organisaation hankkimaan reitittimensä samalta valmistajalta. Jokaisella protokollalla on kuitenkin omat hyvät ja huonot puolensa. Tästä syystä mikään protokolla ei ole saavuttanut määräävää asemaa markkinoilla.

Sisäiset reititysprotokollat voidaan jakaa karkeasti kolmeen pääryhmään: etäisyysvektoriprotokolliin (Distance Vector Protocol), linkkitilaprotokolliin (Link State Protocol) ja näiden yhdistelmään, josta käytetään nimitystä hybridiprotokolla (Hybrid Protocol). [1, s. 256, 274.]

3.2.1 Etäisyysvektoriprotokollat

Etäisyysvektoriprotokollassa reitin valinta tapahtuu pääasiassa aliverkkojen välissä olevien reitittimien lukumäärän perusteella. Yhteyden muodostuksessa valitaan polku, johon kuuluu mahdollisimman vähän reitittimiä. Reititin tietää, kuinka kaukana siitä eri verkkosegmentit ovat polun varrella olevien reitittimien määrällä ilmaistuna, sekä karkeasti, missä suunnassa reitittimeen itseensä nähden ne sijaitsevat. Reitittimellä ei kuitenkaan ole käsitystä verkon topologiasta, sillä niillä ei ole käytössään reittikarttaa. Etäisyysvektoriprotokollat saattavat myös kerätä jonkin verran tietoa aliverkkojen välisten yhteyksien nopeudesta, kuormituksesta ja virhealttiudesta.

Etäisyysvektoriprotokollien parhaana ominaisuutena pidetään niiden yksinkertaista rakennetta. Ne eivät sanottavasti kuormita reitittimen prosessoria eivätkä vaadi yleensä suurta määrää keskusmuistia. Niihin liittyy kuitenkin runsaasti myös heikkouksia. Ne kuormittavat usein verkkoa säännöllisillä reititystaulupäivityksillä tai yhteyden testaamiseen käytettävillä viesteillä. Suurin heikkous on kuitenkin se, ettei niiillä ole tietoa verkon topologiasta. Tämä saattaa aiheuttaa ns. reitityssilmukoiden syntymisen. Niissä reititin lähettää paketteja katkennutta yhteyttä pitkin saatuaan joltakin toiselta reitittimeltä vanhentuneen tiedon reitin olemassaolosta. Muun muassa RIP, IGRP, EGP ja BGP ovat etäisyysvektoriprotokollia. [1, s. 274 - 275.]

3.2.2 Linkkitilaprotokollat

Linkkitilaprotokollat ylläpitävät verkon reitittimillä yhtenevää tietoa verkon rakenteesta. Kaikilla reitittimillä on käytössään verkon topologian kertova reittikartta. Mika Vainio ja Mika Hakala selittävät kirjassaan *Tietoverkon rakentaminen* linkkitilaprotokollien toiminnan havainnollisesti seuraavanlaisesti:

> Sitä voisi verrata hyvään reaaliaikaiseen tiekarttaan, jossa kaupunkien (aliverkot) väliset eritasoiset tiet (yhteydet) näkyvät nopeusrajoituksineen (siirtokapasiteetti), liikennemäärineen (kuormitus) ja tietöineen (virheiden määrä). Reititin valitsee käytettävän polun kuten kesälomamatkaa suunnitteleva autoilija: eri vaihtoehtoja verrataan nopeusrajoitusten, ruuhkien tai tietöiden määrän perusteella.

Reitittimen määrityksissä siirtokapasiteettia, kuormitusastetta tai virheiden määrää voidaan painottaa eri tavoin ja etsiä näiden tietojen perusteella paras mahdollinen reitti useiden vaihtoehtoisten reittien joukosta. Jonkin yhteyden katkeaminen tai tukkeutuminen aiheuttaa verkon kaikkien reitittimien

reittikarttojen välittömän päivittymisen, jolloin reitityssilmukoita ei pääse syntymään. Linkkitilaprotokollia ovat mm. OSPF ja IS-IS. [1, s. 275.]

3.3 Kytkimet

Kytkimet (engl. switch) ovat OSI-mallin kerroksella 2 (siirtoyhteyskerros) toimivia laitteita. Niitä käytetään reitittimien tapaan kytkemään tietokonelaitteita toisiinsa. Kukin tietokone liitetään kytkimeen Ethernet-kaapelilla, ja tietokoneesta toiseen lähetetyt tiedot kulkevat kytkimen kautta. Kytkimet pystyvät tunnistamaan vastaanottamiensa tietojen tarkoitetun kohteen ja lähettävät tiedot vain niihin tietokoneisiin, joiden on tarkoitus vastaanottaa ne, poikkeuksena jakeluviestit (broadcast).

Kytkimen liikenteenohjaus toimii siten, että kehyksen saapuessa kytkimelle kytkin tallentaa sen lähettäjän MAC-osoitteen ja portin kytkimen osoitetauluun. Tämän jälkeen kytkin vertaa kehyksessä olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää kehyksen oikeaan porttiin. Kytkimet voivat lähettää ja vastaanottaa tietoja samanaikaisesti (full-dublex).

Kytkimet eroavat reitittimistä siinä, että ne tuntevat vain fyysiset osoitteet (MAC-osoitteet) ja kehysten ohjaus tapahtuu niiden avulla. Reitittimet puolestaan ohjaavat tietopaketit oikeaan kohteeseen loogisten IP-osoitteiden avulla. Tästä syystä kytkimeen liitettyjen työasemien on kuuluttava samaan lähiverkkosegmenttiin ja eri lähiverkot liitetään toisiinsa reitittimien avulla.

4 TIETOTURVAN TOTEUTTAMINEN

Tietoturvasta huolehtiminen on jälkiteollisessa yhteiskunnassa tärkeää. Perusajatuksena on, että organisaation tärkein omaisuus on tieto, joka halutaan pitää luotettavana, saada nopeasti ja oikeassa muodossa ja on ainoastaan oikeiden henkilöiden saatavilla.

Tietoturvallisuus pilkotaan usein helpommin käsiteltäviin osiin, joiden avulla dokumenttien rakennetta voidaan selkeyttää. Tavallisin tapa on jakaa tietoturvallisuus osa-alueisiin, näitä ovat

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöturvallisuus
- tietoaineistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus. [2, s. 10.]

4.1 Tietoturvan osa-alueet

Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella tarkoitetaan sitä, että tietoturvan kehitys ja johtaminen on jatkuva prosessi ja sitä pyritään ylläpitämään. Myös yhteydenpito eri turvallisuudesta vastaaviin elimiin organisaation sisällä sekä sen ulkopuolella toimiviin viranomaisiin kuuluu siihen. Tärkeätä on erityisesti lainsäädännön ja erilaisten yksityisoikeudellisten sopimusten, kuten lisenssisopimusten ja palvelusopimusten, vaikutusten arviointi organisaation tietoturvakäytäntöihin. [2, s. 10 - 11.]

Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluu rakennuksen tilojen ja laitteiden suojaaminen erilaisilta uhkilta, kuten ilkivallalta ja murroilta, sekä ympäristöuhkilta, kuten vesi- ja palovahingoilta tai sähkö- ja lämmitysjärjestelmien toimintahäiriöiltä. Fyysisen turvallisuuden ylläpito kuuluu yleensä kiinteistöhuollon ja vartiointialan ammattilaisille, mutta tietojenkäsittelyn ja tietohallinnon ammattilaisten on syytä osallistua fyysisen turvallisuuden suunnitteluun ja ylläpitoon ainakin omien tilojensa osalta. Esimerkiksi palvelintilojen fyysisen suojauksen on oltava korkeatasoinen. [2, s. 11.]

Henkilöturvallisuus

Henkilöturvallisuudella varmistetaan tietojärjestelmän käyttäjien toimintakyky ja rajataan heidän oikeuksiaan organisaation tietojen käyttöön. Toimintakyky varmistetaan esimerkiksi varamiesjärjestelyillä ja riittävän koulutustoiminnan järjestämisellä. [2, s. 11.]

Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmistamiseen ja palauttamiseen sekä tuhoamiseen liittyvät toimet. Aineistoihin kuuluvat myös manuaalisen tietojenkäsittelyn asiakirjat sekä automaattisen tietojenkäsittelyn tulosteet.

Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen kuuluvat käytettyihin ohjelmistoihin liittyvät seikat, kuten ohjelmistojen testaus, jolla varmistetaan muun muassa

- sovellusten sopivuus suunniteltuun käyttötarkoitukseen
- ohjelmistojen keskinäinen yhteensopivuus
- toiminnan luotettavuus ja virheettömyys.

Lisäksi ohjelmistoturvallisuuteen kuuluvat ohjelmistoversioiden ja lisenssien hallinta. [2, s. 11 - 12]

Laitteistoturvallisuus

Laitteistoturvallisuuteen liittyvät tietokoneiden ja muiden laitteiden toiminnan testaus ja huoltaminen tarvittaessa. Myös laitteiden kulumiseen ja vanhentumiseen pitää varautua sekä minimoida sähköiskujen ja muiden loukkaantumisvaarojen mahdollisuudet. [2, s. 12.]

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen, kuten lähi- ja laajaverkkoyhteyksien sekä muiden viestinjärjestelmien turvallisuudesta.

Vaikka edellä lueteltu jaottelu on melko keinotekoinen siinä mielessä, että kaikki osa-alueet vaikuttavat toisiinsa ja niissä on runsaasti yhteisiä tekijöitä, auttaa jaottelu silti tietoturvan suunnittelussa. [2, s. 12.]

4.2 Palvelimien ja työasemien tietoturva

4.2.1 Työasematurvallisuus

Työasemien käytön turvallisuus on riippuvainen käyttäjän osaamisesta ja motivaatiosta. Käyttäjän tulee osata hyödyntää organisaation tuotannossa käytettäviä ohjelmistoja ja saada tarvittaessa koulutusta ja ohjeistusta ohjelmien oikeaan käyttöön. Myös laitteiden ja verkkopalveluiden käytössä tarvitaan ohjeistusta.

Käyttäjäkohtaista turvallisuutta toteutetaan käyttöoikeuksien rajaamisella ja käyttäjän tunnistamisella. Käyttöoikeuksien pitää olla riittävät, että käyttäjä pystyy työskentelemään sujuvasti. Tämä ei kuitenkaan tarkoita, että käyttäjällä pitäisi olla pääkäyttöoikeudet. Yleisesti ottaen käyttäjälle annetaan ensin peruskäyttöoikeudet. Tarpeen mukaan annetaan mahdollisesti muita lisäoikeuksia. Lisäoikeuksia voidaan tarvita sovellusten ja laitteiden käytössä.

Oikeuksien käyttöä voidaan valvoa auditoinnilla, joka on oletuksena Windows-käyttöjärjestelmissä poissa päältä. Auditointi tallentaa logi-tiedostoon muun muassa kirjautumis-, levynkäyttö- ja ohjelmankäyttötietoja. [2, s. 124 - 138.]

4.2.2 Palvelinturvallisuus

Palvelimet rakennetaan jotain tiettyä tarkoitusta varten. Palvelimet, joihin palveluita keskitetään, voivat olla joko pieniä tai järeitä. Pienissä palvelimissa on se hyvä puoli, että niitä on helppo päivittää kuormituksen kasvaessa. Järeissä palvelimissa sen sijaan tekniikka on usein vikasietoisempaa. Nykyään hyödynnetään myös virtuaalipalvelimia, joilla voidaan saavuttaa molempien ratkaisujen hyötyjä.

Palvelimilla on tärkeää tietoa, joka voi muuttua useasti. Tästä syystä tiedon varmistus on tärkeää. Tietoa voidaan tallentaa yksittäisille cd- tai dvd-levyille, ulkoisille kiintolevyille, varmistusnauhoille tai nauharobotille. Yleisimmät varmistustavat on esitetty taulukossa 1. [2, s. 144.]

Taulukko 1. Yleisimmät varmistustavat [2, s. 144]

Varmistustavat (Microsoft Backup)	
Tapa	**Toiminto**
Normal	Varmistetaan valittu tieto ja merkitään se varmistetuksi
Incremental	Varmistetaan valittu tieto, varmistetaan edellisestä varmistuksesta muuttunut tieto ja merkitään se varmistetuksi
Differential	Varmistetaan valittu tieto, varmistetaan edellisestä varmistuksesta muuttunut tieto, varmistettua tietoa ei merkitä varmistetuksi
Copy	Varmistetaan valittu tieto, varmistettua tietoa ei merkitä varmistetuksi
Daily	Varmistetaan päivän aikana muuttunut tieto

4.3 Verkon turvallisuus

Verkon turvallisuus koostuu monesta osasta. Tietoliikenteen yleisiä turvamenettelyjä ovat muun muassa palomuurit ja virtuaalisten lähiverkkojen käyttäminen tietojärjestelmiin pääsyn rajoittamiseksi. Luvatonta pääsyä verkkoon voi estää myös siten, että käyttämättömät liitinrasiat on irrotettu ristikytkentäpaneeleista ja aktiivilaitteiden käyttämättömät portit on suljettu. [2, s. 182 - 183.]

4.3.1 Palomuurit

Palomuurit voivat olla ohjelmistoja tai laitteita. Niiden tarkoitus on estää asiattomien pääsy verkkoon tai sen osaan. Palomuureja on pääasiassa kolmea eri perustyyppiä: pakettisuodattimia, välityspalvelimia ja sovellustason yhteyskäytäviä. Kotikäyttäjille tavallisimmat palomuurit ovat pakettisuodattimia, jotka hylkäävät liikennettä lähde- ja kohdeosoitteiden sekä sovellusten käyttämien porttinumeroiden perusteella. Internetissä välityspalvelimet toimivat tiedon varastoina, joilla voidaan vähentää verkon kuormitusta. Intranetissä välityspalvelimilla voidaan rajoittaa sisäverkosta pääsyä ulkoverkkoon, jolloin joillekin sivustoille pääsy voidaan kokonaan estää sisäverkosta. Välityspalvelimet mahdollistavat myös käyttäjän luotettavan tunnistuksen ennen yhteyden avaamista.

Sovellustason yhdyskäytävät (Application Level Gateway) ovat tietoturvamielessä tehokkaimpia palomuureja. Tällainen palomuuri tutkii kaiken lävitseen kulkevan liikenteen. Kun epäilyttäviä paketteja havaitaan, niitä ei lähe-

tetä eteenpäin, vaan ne aiheuttavat hälytyksen, joka välitetään palomuurin käyttöhenkilöstölle. Paketit on myös mahdollista tallentaa tarkempaa analyysia varten. Koska tämän kaltainen palomuuri vaatii paljon prosessointitehoa, se näkyy laitteiden korkeissa hinnoissa. [2, s. 187 - 188.]

4.3.2 NAT

NAT on osoitteenmuunnostekniikka, jolla ulkoisia IP-osoitteita säästetään ja jolla sisäverkon IP-osoitteita voidaan piilottaa. Tekniikka kehitettiin alunperin, kun huomattiin, että tulevaisuudessa IPv4-osoitteita ei riittäisi jokaiselle koneelle. IPv6:lle tekniikka ei ole tarpeellinen, koska sen osoiteavaruus on valtava. NAT muuttaa lähettäjän yksityisen IP-osoitteen julkiseksi IP-osoitteeksi, kun liikenne kulkee sisäverkosta ulos ja toisinpäin sisään tullessa. NAT:sta huolehtiva reititin pitää lähettäjistä kirjaa ja tunnistaa ne TCP/IP-yhteyksissä käytetyistä IP-osoite-porttinumero-parista. [2, s. 215.]

4.3.3 VPN

Tietoturvallinen työskentely kotoa käsin on mahdollista VPN:n avulla, jolla yhteys muodostetaan yksittäisen koneen ja etäkäyttöpalvelimen välille. VPN:llä voidaan yhdistää myös eri toimipisteiden verkkoja toisiinsa tietoturvallisesti. Yhteys on salattu ja sillä on omat protokollat, joilla alkuperäinen paketti kapseloidaan. Uusi kapselointi sisältää muun muassa tiedot lähettäjästä ja vastaanottajan IP-osoitteen. [2, s. 284 - 285.]

5 DOKUMENTOINNIN TEORIAA

5.1 Dokumentoinnin hyödyt

Dokumentoinnin hyödyt tulevat ilmeisiksi siinä vaiheessa, kun tietoverkko on kasvanut muutaman koneen ja palvelimen kokonaisuutta laajemmaksi. Ajan tasalla olevat dokumentoinnit helpottavat verkon hallintaa ja sen kehittämisprosessia sekä nopeuttavat palautumista häiriötilanteista. Kun verkkoon on tarkoitus tehdä suuria muutoksia ja päivityksiä, dokumentointi helpottaa ja nopeuttaa suunnitteluprosessia, koska on helpompi arvioida muutosten vaikutus nykyiseen tietojärjestelmään.

Dokumentointi nähdään usein vain aikaa vievänä kulueränä tai sen puuttumista perustellaan sillä, että kaikki aika on mennyt järjestelmän ylläpidon rutiineihin. Todellisuudessa dokumentoinnin kulut ja sen tekemiseen kulunut aika saadaan monin kerroin takaisin, kun säästetään aikaa ongelmatilanteissa tiedon keruuvaiheelta tai vältytään kokonaan joltain ongelmalta, jota ei osattaisi odottaa ilman dokumentointia. Joissakin tapauksissa katkokset tietojärjestelmän toiminnassa voivat keskeyttää jopa koko liiketoiminnan, joten erityisesti näissä tilanteissa nopea ongelmanratkaisu on tärkeää. Dokumentointi helpottaa kokonaisuuden hahmottamista. Jos dokumentointia ei ole aikaisemmin tehty, voi dokumentointi tuoda päivänvaloon selviä ongelmakohtia tai tietoturvariskejä.

Jotta dokumenteista on mahdollisimman paljon hyötyä, niiden pitää olla tarkkuudeltaan riittävän tarkkoja ja niiden pitää olla ajan tasalla. Tätä varten henkilöstölle pitää kouluttaa dokumenttien laatimista ja niiden versioimista, ja organisaatiossa tulisi olla yhtenäinen dokumentointikäytäntö.

Tehokkaimmin dokumentointi tapahtuu, kun se aloitetaan jo projektin suunnitteluvaiheessa. Tällöin on mahdollista nähdä tulevat ongelmat jo etukäteen ja tehdä vaadittavat muutostyöt jo ennen ongelmien syntymistä. [3, s. 4.]

5.2 Dokumentoinnin tarkkuus ja rajaus

Tietoliikenneverkon dokumentoinnista vastaavan on päätettävä, millä tasolla dokumentointi toteutetaan. Liian tarkkaa dokumentaatiota ei yleensä pystytä ylläpitämään riittävällä tasolla. Lisäksi on huolehdittava, että dokumentoinnin ylläpitoon ei saa kulua liiaksi aikaa. Hyvä sääntö on, että dokumenttien tulee tuottaa enemmän kuin kuluttaa. Tärkeää olisi dokumentoida liiketoiminnan kannalta kriittiset komponentit sellaisella tasolla, että tarvittaviin jatkotoimenpiteisiin voidaan ryhtyä riittävän nopeasti. Dokumentoinnin syvyyden tason tarve on yrityskohtaista. Se riippuu järjestelmän koosta ja rakenteesta, sekä mahdollisten vikojen oletetuista haitoista. Yleensä dokumentointi toteutetaan sekä fyysisellä että loogisella kuvauksella.

Jaakohuhdan (Tietojärjestelmien luotettavuus, 2003) mukaan verkosta kannattaa dokumentoida

- kaapelointi (mittauspöytäkirjat)
- johtotiet
- jakamot
- kytkimet, reitittimet, palomuurit (aktiivilaitteet)
- verkkolaitteiden konfiguraatiot
- WLAN-tukiasemat
- palvelimet
- varusohjelmistot
- sovellukset
- UPS-järjestelmät
- varmistusmenetelmät
- käytetyt työvälineohjelmat
- työasemat, tulostimet yms. (päätelaitteet)
- liitännät.

Näiden lisäksi Jaakohuhta lisää vielä

- laitteen MAC-osoitteen
- laitteen IP-osoitteen
- verkkolaitteiden käyttöjärjestelmäversiot
- sovellusohjelmien versiot
- laitteen mahdolliset DNS-, NetBIOS- ja Novell-nimet
- laitetyypin, merkin ja mahdolliset versiot

- muut tiedot, joita tarvitaan suunnittelua tai laiteinventointia varten.

Dokumentoida kannattaa myös komponenttien maahantuojat ja toimittajat sekä varaosien ja palveluiden saatavuus. [4, s. 114 - 115.]

5.3 Hyvän dokumentoinnin tunnusmerkit

Hyvän dokumentoinnin tunnusmerkit vaihtelevat hieman riippuen siitä, millainen tavoite dokumentille on asetettu. Yleisesti hyvän dokumentoinnin piirteitä oletetaan Jaakohuhdan (Tietojärjestelmien luotettavuus, 2003) mukaan olevan:

- helposti (edullisesti) ylläpidettävä
- havainnollinen ja helposti tulkittava
- dokumentointiraja tunnettu
- syvyystaso (tarkkuus)
- hallintaraja
- asianomaisten helposti saaatavissa
- viittaukset muihin dokumentteihin
- taloudellinen
- organisaaation sisällä yhdenmukainen
- mahdollisuus käyttää organisaation valmiiksi luomia osia dokumentointiin, kuten esimerkiksi sähköisessä muodossa olevia pohjapiirustuksia, johtoteitä ja niin edelleen
- käytetyt symbolit mahdollisimman pitkälle standardien mukaisia
- ei ole ristiriidassa organisaation muun dokumentoinnin kanssa. [4, s. 117.]

5.4 Dokumentoinnin tarve

Dokumentoinnin tarpeellisuudelle voidaan löytää useita perusteita. Karkean jaottelun mukaan voidaan löytää ainakin neljä perustetta huolehtia, että yrityksen tuotantoympäristö on dokumentoitu asianmukaisesti:

- jatkuvuuden turvaaminen
- kehityksen mahdollisuus
- turvallisuudesta huolehtiminen
- ongelmien ratkaiseminen. [5, s. 3.]
-

Jatkuvuus

Jatkuvuuden turvaaminen on yrityksille erittäin tärkeätä. Tämän merkitys on sitä suurempi, mitä harvemman henkilön osaamisen ja tietämisen varassa jokin osa verkosta on. Jos tällainen avainhenkilö joutuu onnettomuuteen tai siirtyy pois organisaatiosta, niin tärkeätä tietoa voidaan menettää. [5, s. 3.]

Kehitys

Tuotannon ja järjestelmien kehittäminen perustuu täysin ajan tasalla olevaan tietoon. Jos järjestelmistä oleva tieto on vanhentunutta tai sitä ei ole lainkaan, on järjestelmän kehittämisen suunnittelu hankalaa tai jopa mahdotonta. [5, s. 4.]

Turvallisuus

Hyvin toteutettu ja asianmukaisesti säilötty dokumentointi luo yritykselle turvaa erilaisien onnettomuuksien varalle, joita voivat olla vesivahingot, tulipalo ja ilkivalta. Dokumentointi auttaa onnettomuustilanteessa nopeasti palautumaan alkuperäiseen tilanteeseen ja se sisällytetään osaksi hyvin toteutettua tietoturvapolitiikkaa. [5, s. 4.]

Ongelmien ratkaiseminen

Dokumentointi nopeuttaa ratkaisujen löytämisessä ongelmatilanteissa ja säästää täten aikaa ja vapauttaa tiedon etsintään käytetyn työpanoksen itse ongelman ratkaisuun. Hyvin tehty dokumentointi tuottaa suoranaista taloudellista hyötyä, kun ongelmatilanteissa arvokasta työaikaa ei kulu tiedon etsintään. [5, s. 4.]

5.5 Dokumentointiprojekti

Periaatteessa dokumentointityö tulisi aloittaa jo tietojärjestelmän suunnitteluprosessin aikana, jolloin rakennettujen järjestelmien tiedot ja asetukset voi samalla kirjoittaa ylös muistiin. Usein dokumentointi on kuitenkin syystä tai toisesta jäänyt tekemättä, tai dokumentointi on epätäydellistä. Tässä osassa pyritään hahmottamaan ja antamaan vinkkejä siitä, kuinka dokumentointiprojektia voisi lähteä toteuttamaan. Tulee kuitenkin muistaa, että ei ole yhtä oikeata tapaa toteuttaa dokumentointia, vaan tarpeet ja toteutustavat voivat vaihdella riippuen siitä, minkälainen tietojärjestelmä on kyseessä.

Ennen dokumentoinnin aloittamista tulee päättää, mitä kaikkea dokumentointiin sisällytetään. Dokumentointistandardin tulisi olla yhtenäinen koko organisaatiossa. Kuten aiemmin mainittiin, nyrkkisääntönä on, että liiketoiminnan kannalta keskeisimmät osat tulisi dokumentoida. Keskeisiä osia ja tietoja ovat mm. palvelimet, verkkolaitteiden asetukset ja varmistusmenetelmät.

Kun dokumentointi aloitetaan, kannattaa aloittaa tietojärjestelmän pääpiirteiden kartoittamisesta ja edetä sitten yksityiskohtaisempien tietojen keruuseen. Tietojärjestelmästä hahmottaa nopeasti yleisen rakenteen, kun loogiset ja fyysiset kartat on luotu verkosta. Karttojen teon jälkeen voi ryhtyä keräämään tietoa tietojärjestelmän toiminnallisista osista, kuten palvelimista ja verkkolaitteista. Dokumentoitaessa yhden tarkkuustason lisäys voi kuitenkin lisätä dokumentoitavan tiedon määrää todella paljon, joten pitää puntaroida, onko kyseisen tiedon dokumentointi oleellista ja onko niiden tietojen ajan tasalla pitäminen liian työlästä, jolloin se todennäköisesti jää tekemättä.

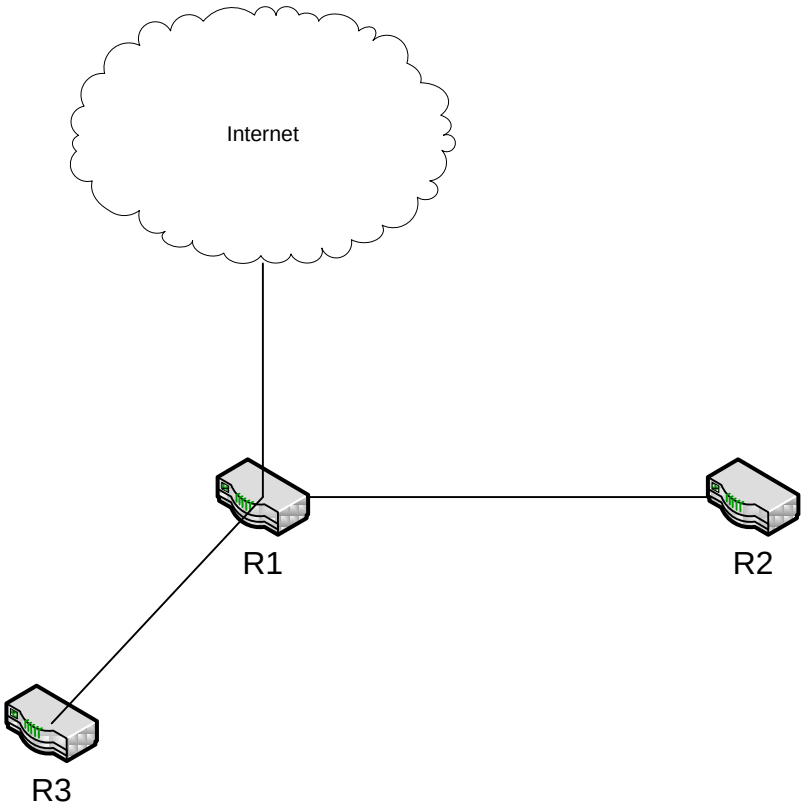
Oleellisimpia dokumentoitavia tietoja laitteista ovat mm. IP-osoitteet, laitteen malli ja huoltotiedot. Dokumenttien rakenne tulisi olla sellainen, että niitä on helppo ylläpitää ja ne ovat havainnollisia. [6.]

5.6 Verkkokartat

Verkkokarttoja on pääasiassa kahdenlaisia: loogisia karttoja, jotka kuvaavat verkon toimintaa ja fyysiset kartat, joihin on tarkkaan merkitty eri laitteiden sijainnit. Karttoja tehdessä pitäisi käyttää standardoituja merkkejä ja laitteiden merkintätapoja, jotka ovat yhtenäisiä laitteiden kanssa. Tämä helpottaa laitteiden tyypin ja sijainnin hahmottamisessa kartoista.

Looginen verkkokartta

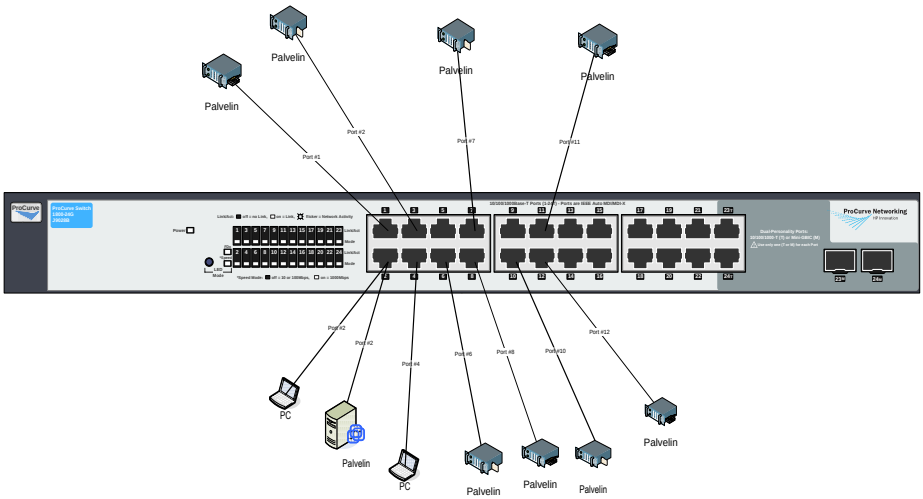
Loogiseen karttaan kuvataan verkko pääpiirteissään, eli fyysistä karttaa yksinkertaisemmin. Kartasta tulisi pystyä nopeasti hahmottamaan yleiskuva verkon toteutuksesta ja miten verkkoliikennettä ohjaavat laitteet ovat kiinni toisissaan. Karttaan piirrettäviä laitteita ovat reitittimet, kytkimet ja muut verkkolaitteet sekä palvelimet. Laitteiden väliset kaapelityypit on myös hyvä merkitä karttaan. Kartan voi piirtää joko käsin tai erillisellä piirtoon soveltuvalla ohjelmistolla. Kuvassa 3 on esitetty yksinkertainen looginen kuvaus.



Kuva 3. Looginen kartta

Fyysinen verkkokartta

Fyysiseen karttaan on tarkoitus merkitä tarkasti kaikki verkkolaitteet, kuten työasemat, tulostimet, kytkimet ja reitittimet. Fyysisen kartan pohjana käytetään yleensä rakennuksen pohjapiirustusta, josta on karsittu verkkokuvauksen kannalta epäolennaiset merkit pois. Fyysisestä kuvauksesta pitäisi pystyä heti näkemään kaapeleiden sijainnit pohjapiirustuksessa. Fyysinen kuvaus tulisi luoda toimitilan rakentamisen yhteydessä. Kuvassa 4 on esitetty yksittäisen kytkimen fyysinen kuvaus.



Kuva 4. Yksittäisen kytkimen kuvaus

5.7 Teknisten laitteiden dokumentointi

Isossa verkossa saattaa olla monenlaisia laitteita. Yksittäisistä laitteista kerättävään dokumentaatioon pitäisi sisältyä ainakin seuraavat dokumentit:

- laitteiden käyttöohjeet
- tekniset tiedot
- laitepäiväkirja sisältäen hankinta-ajankohdan, muutoshistorian, takuut, määräaikaishuoltojen ajankohdat ja ylläpitävän yrityksen yhteystiedot
- vastuuhenkilöiden yhteystiedot
- ongelmatilanteiden ratkaisuohjeet.

Verkon aktiivilaitteista, kuten reitittimistä ja kytkimistä tulisi dokumentoida asetukset tai ottaa varmuuskopiot. [5, s. 6.]

6 DOKUMENTOINTIMENETELMÄT

Dokumentoinnista on hyötyä, vain jos se pidetään ajan tasalla. Niinpä dokumentteja pitääkin päivitellä aina tarpeen tullen. Jotta päivitysprosessi käy helposti, pitää dokumentoinnin olla helposti muokattavissa, jotta koko dokumentaatiota tai sen osaa ei tarvitse kokonaan piirtää uusiksi.

6.1 Dokumentointitapojen muuttuminen

Ensimmäisten verkkojen rakentamisen aikoihin tehtiin myös ensimmäiset dokumentit. Nämä olivat usein verkkojen rakentajien käsin piirtämiä verkkokarttoja ja eri dokumentointitapoja oli varmasti yhtä monta kuin dokumentoijiakin.

Käsin piirretyt dokumentit ovat kuitenkin huonosti muokattavissa. Siksi siirryttiin nopeasti käyttämään toimisto-ohjelmia, kuten Wordia ja Exceliä. Näiden avulla saatiin aikaan helposti muokattavia olevia dokumentteja.

Suurin muutos dokumentoinnin saralla tapahtui 1990-luvulla, kun juuri verkon dokumentointiin tarkoitetut ohjelmat alkoivat yleistyä. Näistä kaksi esimerkkiä ovat Microsoft Visio ja NetViz.

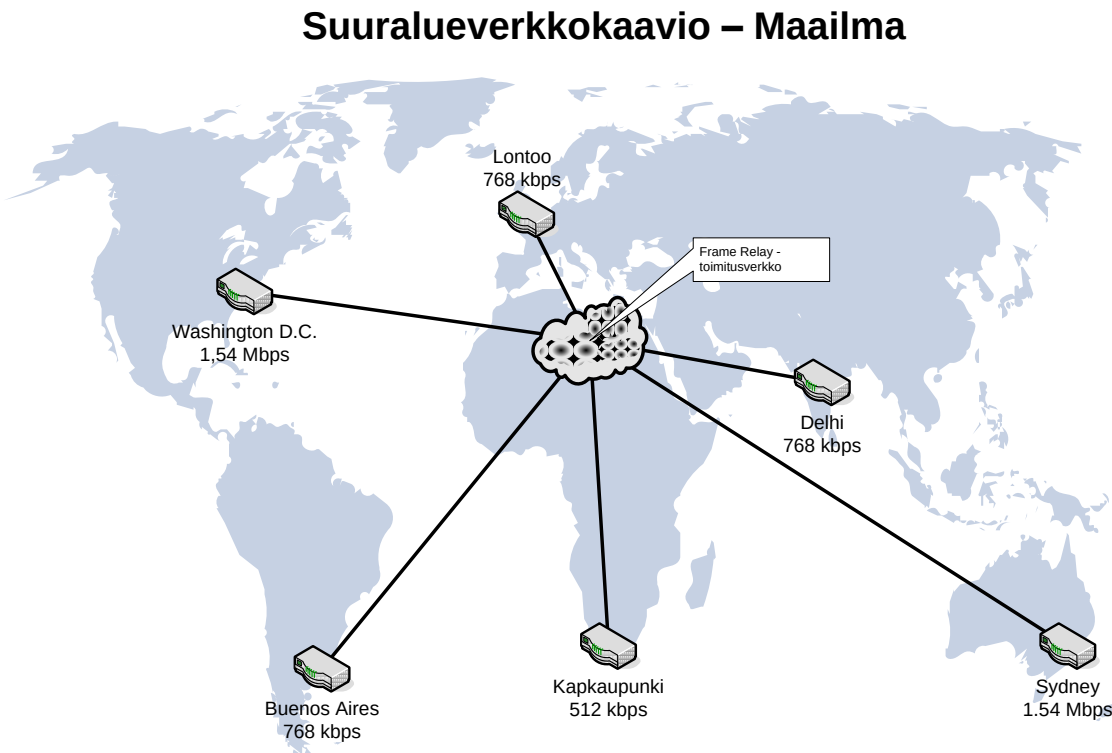
6.2 Perinteiset toimisto-ohjelmat

Mikäli verkko ei ole kovin laaja ja monimutkainen, niin dokumentointiin saattavat riittää perustoimisto-ohjelmat kuten Word ja Excel. Vaikka Wordia ei kovin yleisesti käytetä verkon dokumentoinnissa, voi sillä silti luoda yksinkertaisia palikkakaavioita. Excelillä on mahdollista luoda taulukoita ja tietokantatyylisiä listoja. Listat voivat sisältää koneiden IP-osoitteita, tietoa niiden sijainnista rakennuksessa ja vaikka tietoa, mihin verkon aktiivilaitteeseen se on kytköksissä.

Hyvänä puolena perinteisissä toimisto-ohjelmissa on se, että ne löytyvät nykyään jokaisesta yrityksestä. Dokumentoinnin teko pelkästään näillä välineillä on mahdollista, ja jos tulos on tyydyttävä, ei ole perustetta hankkia erillisiä dokumentointiohjelmia. Usein nämä eivät kuitenkaan riitä ja on syytä harkita varsinaisen dokumentointityökalun hankkimista. [3, s. 9.]

6.3 Dokumentointiohjelmat

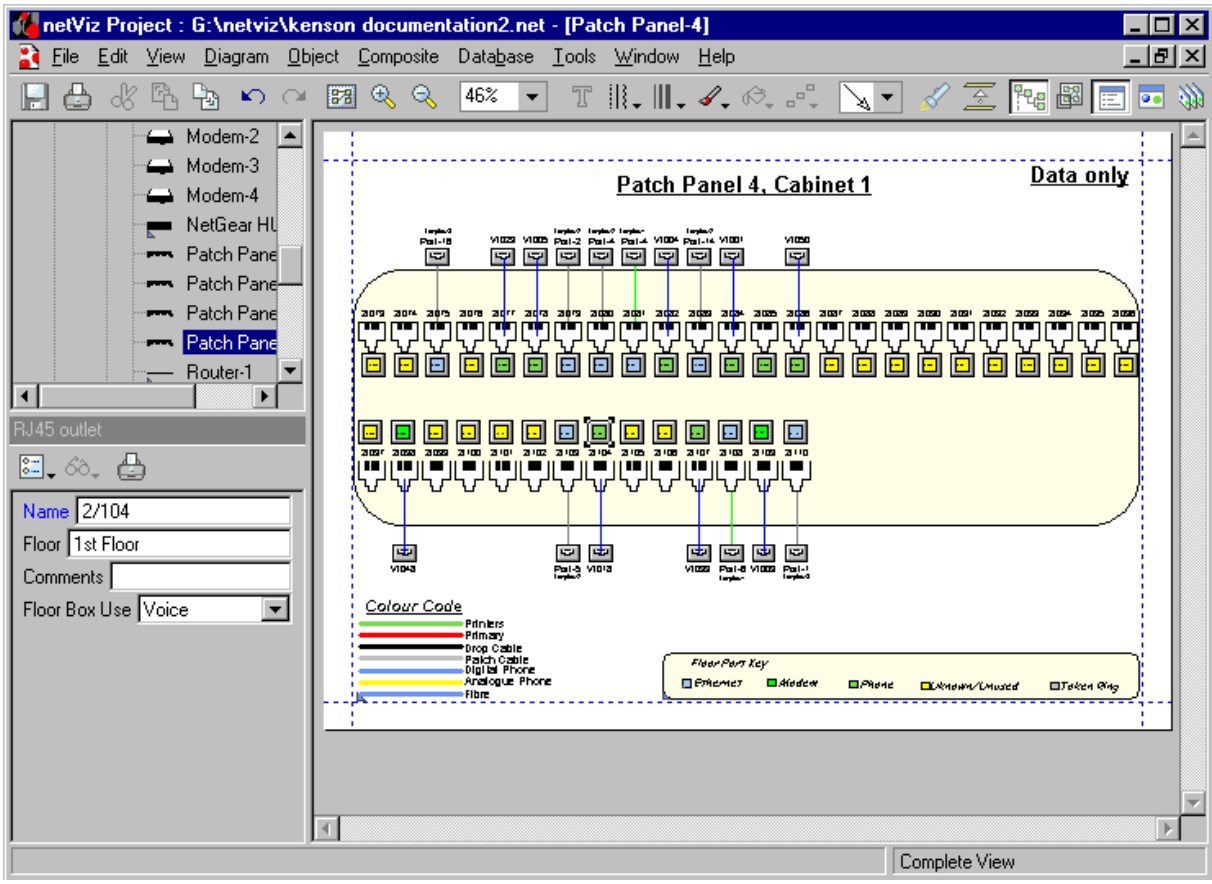
Kevyeen verkkokuvien piirtämiseen soveltuu hyvin Microsoftin Visio, jonka hyviä puolia ovat sen helppokäyttöisyys ja selkeys. Visiolla voi luoda myös muita havainnekuvia ja suunnitteludiagrammeja. Visioon on saatavilla suuri valikoima erilaisia ikoneja havainnoimaan eri laitteita ja niitä pystyy luomaan myös itse. Isojen verkkojen käsin piirtäminen Visiolla on kohtalaisen työlästä. Urakkaa voi kuitenkin helpottaa ylimääräisillä ohjelmilla, jotka ovat erikoistuneet verkon rakenteen tutkimiseen ja kuvaamiseen. Esimerkiksi Solarwinds Lansurveyor on verkon kuvausohjelma, josta kuvat pystyy siirtämään myös suoraan Visioon. Seuraava kuva esittää WAN-verkon kuvausta, ja se on toteutettu Visiolla (kuva 5).



Kuva 5. Visiolla tehty WAN-verkon kuvaus

Järeämpään dokumentointiin voi käyttää Netviz-ohjelmaa. Netviz loistaa laajan dokumentoinnin jäsentämisessä. Esimerkiksi rakennuksen kaapeloinnista voi laatia yleisluontoisen runkodokumentin, jossa kutakin kerrosta kuvaavaa solmua napsauttamalla päästään kerroskohtaisen kaapeloinnin kuvaukseen. Myös loogisten näkymien luonti on mahdollista siten, että yhdellä näkymällä kuvataan kaapelointi ja aktiivilaitteet, toisella työasemat ja palveli-

met. Netviz on alunperin kehitetty nimenomaan verkon dokumentointiin, mutta sillä voi tehdä monenlaisia muita kuvauksia. Organisaatiokaaviot, tietokantakuvaukset ja prosessikaaviot lienevät näistä yleisimpiä. Seuraava kuva esittää ristikytkentäpaneelin kuvausta, joka on tehty NetVizillä (kuva 6).



Kuva 6. Ristikytkentäpaneelin kuvaus NetVizillä

Netviziin voi tuoda tietoja tekstitiedostoista, Excel-taulukoista tai muista odbc-tietokannoista. Yhteydet ovat kaksisuuntaisia, ja koko kuvauksen sisältämän datan voi säilyttää ulkoisessa, esimerkiksi verkonhallintaohjelman ylläpitämässä tietokannassa. [7.]

7 SUOMEN SYÖPÄYHDISTYKSEN TIETOJÄRJESTELMÄ

Ennen dokumentointiprojektin aloittamista valmiina dokumentointina oli tekstitiedostomuodossa tehty listaus verkon laitteista, niiden nimistä ja IP-osoitteista. Dokumentista selvisivät myös käytetyt IP-avaruudet ja mitkä alueet on varattu palvelimille, tulostimille ja työasemille. Tämän dokumentin lisäksi oli Visiolla tehty kuvaus laitekehikon sisällöstä, joita yhdistyksen tästä toimipisteestä löytyy vain yksi. Yhdistyksen omat järjestelmät oli rakennettu toimitilaan keväällä 2008. Rakennuksen yleiskaapelointi on Elisan rakentama ja kaapelit ovat tyyppiä Cat 6. Järjestelmät oli saatettu toimintakuntoon mahdollisimman nopeasti järjestön muuttaessa tilaan. Koska järjestön IT-osasto on pieni, ei dokumentointia tehty rakentamisen yhteydessä. Dokumentoinnin toivottiin tuovan ilmi puutteita ja mahdollisia haavoittuvuuksia verkon rakenteessa ja antamaan selkeän yleiskuvan verkon rakenteesta.

Koska Suomen Syöpäyhdistyksen on pääasiassa lahjoituksien varassa toimiva ei-kaupallinen organisaatio, varat menevät etupäässä tutkimusten tekoon ja muiden toimintojen rahoittamiseen. Tästä syystä verkon infrastruktuurin suunnittelun periaatteena on ollut käyttää edullisimpia toimivia ratkaisuja verkon toteutuksessa. Toimintamalli on yhdistyksen tapauksessa ollut toimiva, koska verkko muuttuu harvoin ja laajentamistarpeet ovat vähäiset.

Rakennuksessa on myös Integralin toimittama VoIP-toteutus ja wlan-järjestelmä. Koska VoIP on kokonaan ulkoistettu järjestelmä ja wlan on eristetty sisäverkosta, päätettiin ne jättää dokumentoinnin ulkopuolelle.

7.1 Palvelimet ja virtualisointi

Suomen Syöpäyhdistyksessä on vuoden 2009 aikana virtualisoitu suuri osa palvelimista kolmelle VMWare:a pyörittävälle koneelle. Palvelintenn lisäksi on virtualisoitu toimisto-ohjelmia kuten Excel.

Palvelinten virtualisoinnissa on kyse ohjelmasta, joka toimii joko suoraan ns. raudan päällä tai käyttöjärjestelmän alaisena. Palvelimet on käytännössä parempi toteuttaa ensiksi mainitulla tavalla, mutta käyttöjärjestelmässä ajettavat virtuaalikoneet ovat käytännöllisiä, kun halutaan esimerkiksi testata uutta käyttöjärjestelmää ennen sen varsinaista käyttöönottoa. Virtuaalikone emuloi fyysisiä laitteita, kuten emolevyä ja prosessoria, ja virtuaalikoneessa pyörivä

käyttöjärjestelmä näkee laitteet kuin ne olisivat oikeasti olemassa. Tämä mahdollistaa useiden virtuaalikoneiden ajamisen samalla koneella. Virtuaalikoneita pyörittävän palvelimen kannattaakin olla mahdollisimman järeä, jotta se jaksaa ajaa niitä useita. Virtualisoinnin hyötyjä on palvelimien keskittämisen helpottuminen, yhdenmukaisten koneiden luonti helpottuu huomattavasti ja virtuaalikoneita on nopea kopioida. Virtualisoinnilla pääsee samalla eroon vanhoista koneista. Virtualisoinnilla on myös mahdollista luoda vikasietoinen palvelin, josta on kaksi kopiota; toisen palvelimen vikaantuessa varalla oleva palvelin ottaa heti tehtävät hoitaakseen ilman että käyttäjä huomaa minkäänlaista katkosta.

Suomen Syöpäyhdistyksessä palvelimet on virtualisoitu VMWare ESX 4:lla. Yhteensä VMWare-palvelimia on kolme kappaletta ja niissä kussakin on 20 GB keskusmuistia ja kaksi kappaletta neliytimellistä Xeon-prosessoria, joiden kellotaajuudet ovat 2,5 GHz. Palvelinten levytilan tarpeista vastaa kaksi HP:n DL360-verkkotallennusjärjestelmää. Yhteensä niissä on 12 TB kovalevytilaa.

Ohjelmien virtualisointi on toteutettu Xenocodella, jolla ohjelman voi pakata yhdeksi käynnistystiedostoksi. Nämä virtualisoidut ohjelmat toimivat Windows-käyttöjärjestelmissä eikä niiden käyttö aiheuta konflikteja muiden asennettujen sovellusten kanssa. [11.]

7.2 Kytkimet

Yhdistyksen käytössä olevat kytkimet ovat HP ProCurve 1800-24G-mallisia. Niitä on yhteensä kymmenen. Kytkimet ovat selaimen kautta hallittavia. Kytkin tukee VLAN:a, tekniikkaa, jolla voidaan pilkkoa verkkoa pienempiin osiin ja näin lisätä tietoturvaa ja parantaa verkon suorituskykyä. Laite tukee myös Link Aggregation Control -protokollaa (LACP), jolla on mahdollista yhdistää usea yhden kytkimen fyysinen portti yhdeksi loogiseksi portiksi, jolloin kaistanleveys ja vikasietoisuus kasvaa esimerkiksi palvelimen ja kytkimen välisissä yhteyksissä, kun käytössä on kaksi verkkokorttia.

Laitteesta puuttuu kuitenkin tuki Spanning Tree -protokollalle (STP), joten kovin korkeaa vikasietoisuutta ei voi saavuttaa runkoverkolle pelkästään näitä kytkimiä käyttämällä. Syöpäyhdistykselle näillä kytkimillä saavutettu toimivuus on kuitenkin ollut riittävä. Kuva kytkimestä ja sen perustiedot esittävä taulukko löytyvät seuraavalta sivulta (kuva 8 ja taulukko 2). [10]

Kuva 8. HP ProCurve 1800-24G.

Taulukko 2. Kytkimen perustiedot.

HP ProCurve 1800-24G	
Porttien lkm:	24
Tuetut standardit	Ethernet 10Base-T, 100Base-TX, 1000Base-T
Mitat (cm):	17.12 x 44.25 x 4.39
Paino:	1.96 kg

7.3 VOIP

VOIP-järjestelmä on Integralin rakentama ja ylläpitämä. Järjestelmässä on noin 90 puhelinta. Kytkinlaitteina on viisi kappaletta HP ProCurve 2610-24-PWR:ia

7.4 WLAN

WLAN muodostaa oman verkkonsa, eikä se ole suoraan yhteydessä sisäverkkoon. Näin on tehty, jotta tietoturvan toteutus olisi mahdollisimman yksinkertaista. WLAN ei myöskään ole kovin tärkeä työntekijöille työn tekemisen kannalta. Lähinnä sitä tarjotaan vierailijoille käytettäväksi ja sähköpostien lukemiseen.

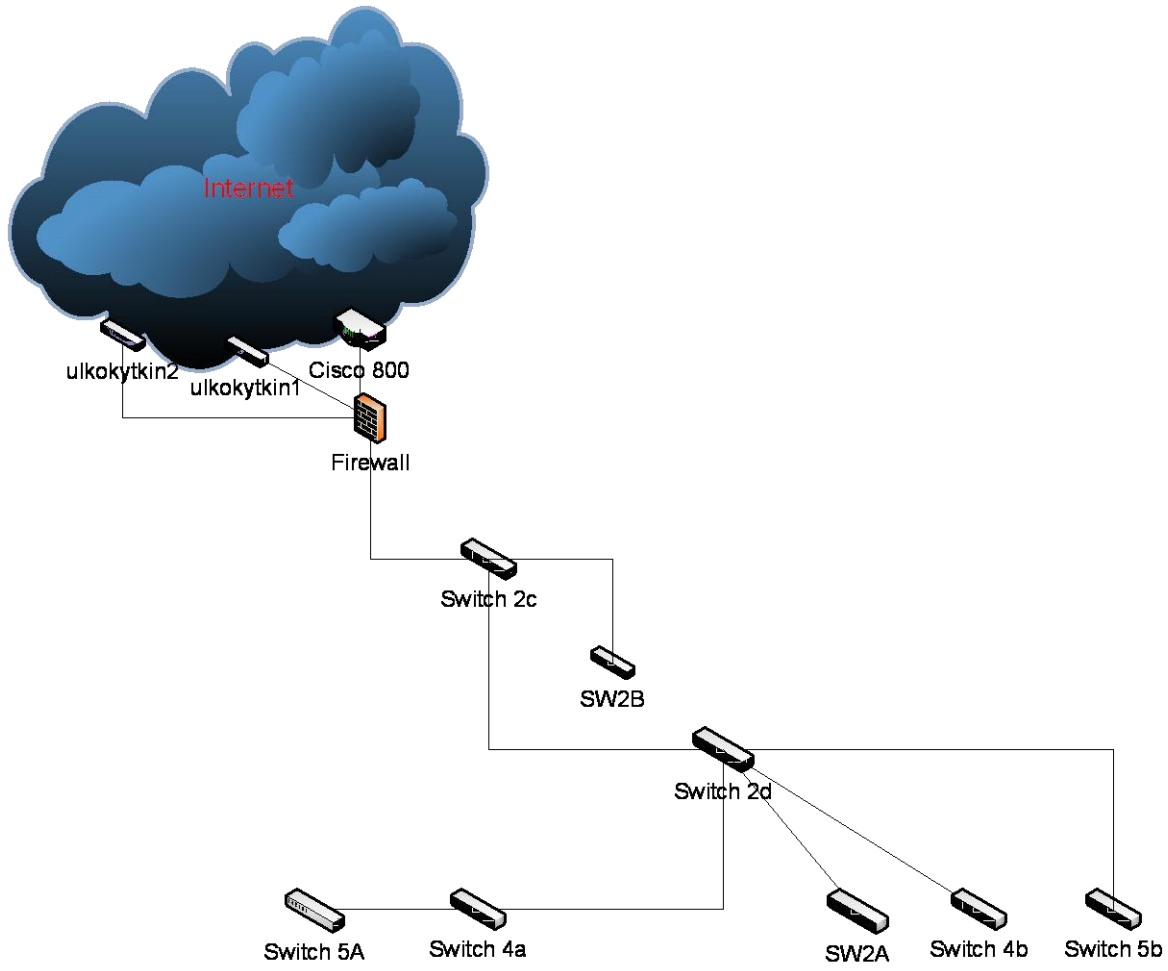
8 DOKUMENTOINNIN TULOS

8.1 Laiteluettelo

Kattavan listauksen verkon laitteista jo ennestään antanutta dokumenttitiedostoa suunniteltiin parannettavaksi siten, että laitteista kerättäisiin myös MAC-osoitteet ja sarjanumerot ja tulevaisuudessa kirjattaisiin myös laitteiden hankintapäivät. Koska dokumentti toimii hyvin eräänlaisena inventaariolistana hankituista laitteista, päätettiin dokumenttiin lisätä myös työasemat ja niistä päätettiin dokumentoida vähintään työaseman nimi ja sarjanumerot sekä kenen käytössä laite on. Excel-muotoinen dokumentointi mahdollistaa myös tietojen integroinnin tulevaisuudessa karttojen kanssa, mutta tämänkaltaista linkittämistä ei ole vielä tehty.

8.2 Verkon rakenne

Koska verkkokarttoja ei ollut ennestään piirrettynä, oli niiden luonti tärkeysjärjestyksessä korkealla. Kartat toteutettiin Visiolla, jonka lisenssi oli hankittu dokumentointityötä varten. Kartat olisi voinut toteuttaa myös esimerkiksi NetViz:llä, mutta sen todettiin jo heti alussa olevan turhan järeä työkalu tämän ympäristön dokumentointiin. Ensiksi lähdettiin kartoittamaan verkkoa loogiselta tasolta eli selvitettiin, minkälainen verkon rakenne on pääpiirteissään. Tämä verkkokartta esittää ainoastaan kytkimet, reitittimen ja palomuurin. Symboleina käytettiin Vision omia valmiita symboleita. Seuraava kuva on kytkimet esittävä looginen kuvaus (kuva 9).



Kuva 9. Verkon looginen kuvaus

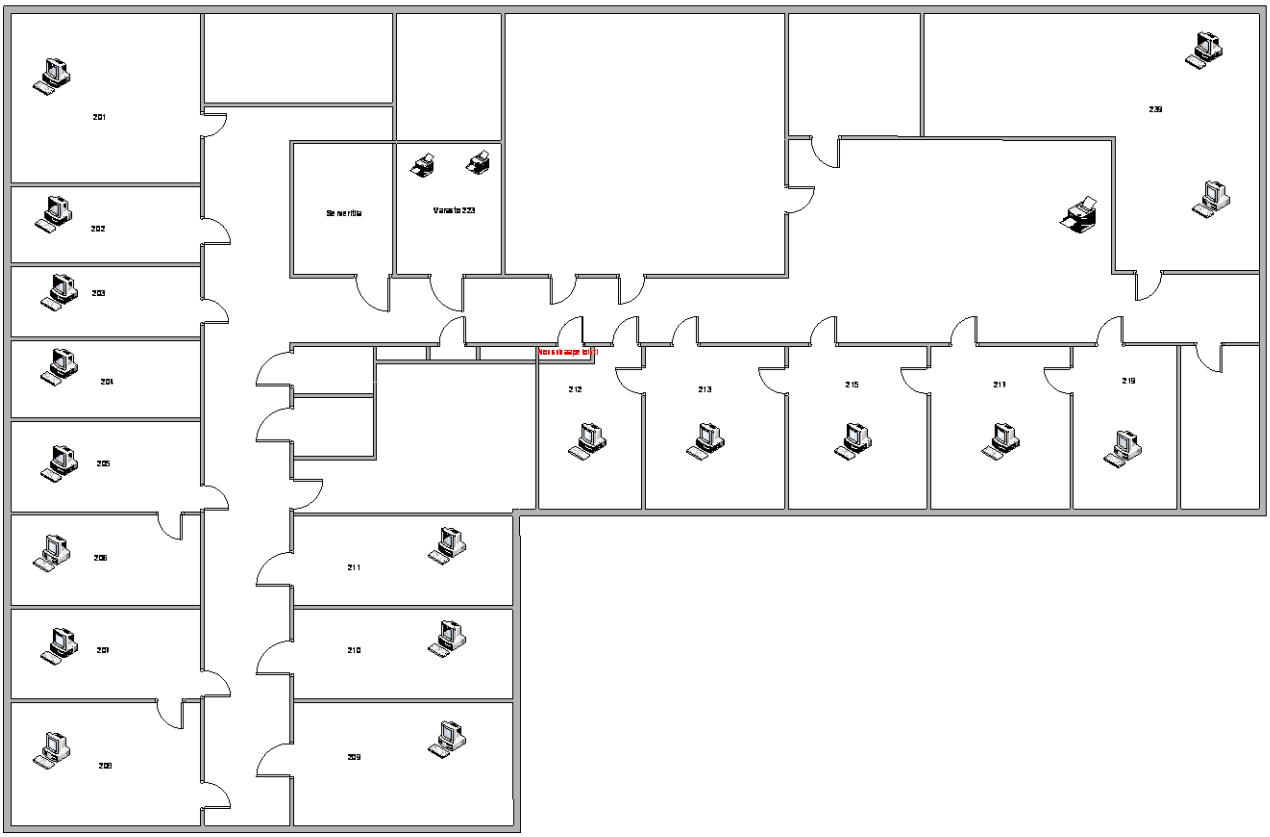
Sisäverkon runko koostuu kahdeksasta HP ProCurve 1800-24G -kytkimestä. Niillä on yksilölliset nimet ja nimistä selviää, missä kerroksessa kytkin sijaitsee. Esimerkiksi SW2D-kytkin sijaitsee toisessa kerroksessa ja on neljäs kytkin tässä kerroksessa. Kaksi samanmallista kytkintä sijaitsee palvelinten kanssa samassa kehikossa. Niille ei ole annettu erityistä nimeä, ja ne vastaavat palvelimien liikenteestä. Sisäverkko on suojattu palomuurilla. Ulkomaailman liikenne kulkee Cisco 800 -reitittimen kautta, jonka toiminnasta vastaa TDC Song.

Suurin osa sisäverkon liikenteestä kulkee kytkimien 2d ja 2c kautta. Verkko on altis lähes koko toiminnan halvaannuttavalle katkokselle siinä tapauksessa, että toinen näistä kytkimistä hajoaa. Kytkimet eivät tue Spanning Tree-protokollaa, joten varayhteyksiä ei pysty kytkinten välille luomaan. Verkkoa tullaan todennäköisesti muuttamaan tulevaisuudessa siten, että hankitaan sisäverkkoon oma reititin. Näin sisäverkkoa pitäisi saada jo vikasietoisem-

maksi ilman liian suuria laitekustannuksia. Ulkoverkon vikasietoisuutta parannettiin työn aikana jo siten, että hankittiin 2 MB:n varayhteys 24Onlinelta.

8.3 Fyysinen kartta

Loogisen kartan lisäksi piirrettiin fyysinen kartta. Kartan pohjana käytettiin talon pohjapiirrosta, joka piirrettiin mittasuhteiltaan silmämääräisenä Visiolla uudelleen yksinkertaistettuna. Kartan piirtoa varten piti selvittää työasemien nimet, käyttäjät ja niiden sijainnit. Tämän vaiheen aikana dokumentoitiin myös työpisterasiat ja kytkentäpaneelit. Kartan on tarkoitus esittää kaikkien verkossa olevien työasemien ja tulostimien sijainnit. Palvelimia ei ole merkitty erikseen karttaan, koska ne sijaitsevat kaikki samassa tilassa. Karttaan olisi merkitty myös kaapelien vetoreitit, jos näistä olisi ollut tarkkaa tietoa saatavilla. Tämän sijaan tyydyttiin merkitsemään vain nousukaapelikuilun sijainnit. Karttaa on tulevaisuudessa tarkoitus parantaa siten, että koneiden tiedot päivittyisivät suoraan erillisestä taulukkotiedostosta. Seuraavassa kuvassa on esitetty rakennuksen toisen kerroksen kuvaus (kuva 10).



Kuva 10. Kerroksen 2 fyysinen kuvaus

8.4 Kytkentäpaneelien dokumentointi

Talossa on 17 ristikytkentäpaneelia ja niissä kussakin on 24 porttia. Rakennuksen toisessa kerroksessa on yhdeksän paneelia. Eri kerroksissa olevien kytkinten kytkennät menevät niiden kautta samoin kuin kytkennät työasemille, WLAN:lle, VOIP:lle ja PSTN:lle.

Jokaisen kerroksen paneeleista luotiin dokumentit ja niistä kerättiin seuraavanlaisia tietoja:

- mikä paneelin portti on kyseessä
- kuinka pitkä kaapeli on kytkettynä (m)
- kaapelin väri
- kaapelin malli
- mihin laitteeseen paneeli on tilassa kytkettynä
- mihin laitteen porttiin se on kiinnitetty
- mihin rakennuksen kerrokseen kytkentä toisessa päässä tulee
- mihin huoneeseen/tilaan
- kenen huone on kyseessä
- mikä laite on kyseessä.

Jokaisesta kytkimestä luotiin Visiolla kuva, josta ilmenee, mikä laite on missäkin portissa kiinni. Kytkinten hallintasivun kautta ei saa paljoa tietoa porteista, joten tietoa kerättiin SMNP:tä hyödyntävillä ohjelmilla sekä muun dokumentoinnin yhteydessä kerätyistä tiedoista.

9 YHTEENVETO

Työssä käytiin läpi tietojärjestelmän suunnitteluun, ylläpitoon ja dokumentointiin liittyviä asioita. Tarkoituksena oli tutustua tietojärjestelmän suunnitteluun sekä sen ylläpitotehtäviin, dokumentoinnin kannalta. Suomen Syöpäyhdistykselle dokumentoinnin toteuttaminen vaati ensiksi hyviin dokumentointitapoihin perehtymistä. Tämän jälkeen piti päättää, mitä asioita olisi tämän tietojärjestelmän dokumentoinnin kannalta oleellisinta dokumentoida. Lopputuloksena syntyi helposti ylläpidettävä ja havainnollinen kuvaus verkosta ja sen järjestelmistä, jota on helppokäyttöisten työkalujen ansiosta helppo laajentaa tarpeen tullen.

VIITELUETTELO

[1] Hakala, Mika - Vainio, Mika, *Tietoverkon rakentaminen.* Porvoo, Docendo. 2005.

[2] Hakala, Mika - Vainio, Mika - Vuorinen, Olli, *Tietoturvallisuuden käsikirja.* Porvoo, Docendo. 2006.

[3] Saine, Jussi, *Verkon dokumentointi.*

[4] Jaakohuhta, Hannu, *Tietojärjestelmien luotettavuus.* Edita. 2003.

[5] Pasanen, Kari*, Turun ammattikorkeakoulun tietoverkon aktiivilaitteiden dokumentointi, 2002.*

[6] Kaapeloinnin dokumentointi [verkkodokumentti] [Viitattu:kesällä 2009] Saatavissa: http://www.tlu.ee/~matsak/telecom/lasse/documentation_of_cabling/index.html.

[7] NetViz esittely [verkkodokumentti] [Viitattu: 31.7.2009] Saatavissa: http://www.tietokone.fi/lukusali/artikkelit/2002tk11/verkkopikis_netviz.htm.

[8] HP ProCurve Switch 1800 Series http://www.procurve.com/products/switches/HP_ProCurve_Switch_1800_Series/overview.htm.

[9] Tietoa Xenocodesta. [Viitattu: 21.11.2009] http://en.wikipedia.org/wiki/Xenocode.