TAMPEREEN
AMMATTIKORKEAKOULU

TUTKINTOTYÖRAPORTTI

Salesline Oy:n tietoverkon kehityssuunnitelma

Janita Puukkoniemi

Tietojenkäsittelyn koulutusohjelma
Toukokuu 2006
Työn ohjaaja: Rami Lehtinen

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Janita Puukkoniemi

Koulutusohjelma(t) Tietojenkäsittely

Tutkintotyön nimi Salesline Oy:n tietoverkon kehityssuunnitelma

Työn valmistumis-kuukausi ja -vuosi Toukokuu 2006

Työn ohjaaja Rami Lehtinen **Sivumäärä:** 57

TIIVISTELMÄ

Sain tutkintotyön aiheeni toimeksiantona Salesline Oy:ltä. Tutkintotyön tavoitteena on suunnitella kehittyneempi, tietoturvallinen tietoverkkoratkaisu Salesline Oy:lle. Tutkin työssä mahdollisuuksia kehittää Salesline Oy:n lähiverkkoja ja vaihtoehtoisia tapoja liittää toimipisteet yhdeksi loogiseksi tietoverkoksi.

Teoria osuudessa perehdyn palvelinten maailmaan ja niiden toimintaan lähiverkoissa. Käsittelen myös Windows Server 2003- ja FreeBSD-verkkokäyttöjärjestelmiä niitä toisiinsa verraten. Toimipisteiden yhdistämisen teoria keskittyy virtuaalisiin yksityisverkkoihin eli VPN-verkkoihin (Virtual Private Network) ja Secure Shell-ohjelmistoon.

Tutkintotyöni tuloksena annan ratkaisuvaihtoehtoja, joilla Salesline Oy:n tietoverkkoa voitaisiin kehittää ja ilmaisen myös päätelmiäni, millä vertailluista tavoista kehityssuunnitelma olisi kannattavinta toteuttaa.

Avainsanat VPN SSH palvelin tietoturva

TAMPERE
POLYTECHNIC

Author(s)	Janita Puukkoniemi
Degree Programme(s)	Business Information Systems
Title	Network development plan for Salesline Oy
Month and year	May 2006
Supervisor	Rami Lehtinen

Pages: 57

ABSTRACT

I got my thesis subject as an assignment from Salesline Oy. The objective of the thesis is to plan more developed, secure network solution for Salesline Oy. In this thesis I observe the changes to develop the local area network of Salesline Oy and alternative ways to connect their locations to one logical network.

In the theoretical part I get acquinted with the world of servers and their actions in the local area network. I also approach the Windows Server 2003 and FreeBSD network operating systems comparing them to each other. The theory of connecting local area networks concentrates to Virtual Private Networks (VPN) and Secure Shell software.

As a result of this thesis I give alternative options how the network of Salesline Oy could be developed and also express my own conclusions in which ways the development plan would be productive to execute.

Keywords VPN SSH server security

Sisällysluettelo

1. Johdanto

Internet on nykypäivänä suuri osa ihmisten elämää, niin koti- kuin työelämässäkin. Ihmiset käyttävät Internetiä kotona sähköpostin lukemiseen, tiedon hakuun ja viihdyttämiseen. Työssä Internetiä käytetään samoihin tarpeisiin, tosin vähemmän viihdyttämiseen kuin kotona.

Yrityksissä ihmiset saattavat järjestää videokeskusteluita Internetin yli toiseen toimipisteeseen tai asiakkaalle, myös monien yrityksien tilaukset ja laskutus kulkevat nykyään sähköisessä muodossa. Nämä toiminnat sisältävät paljon yritykselle tärkeää ja samalla salaista tietoa. Näiden tietojen välittäminen Internetissä suojaamattomana voi olla hyvinkin haitallista yritykselle ja heidän asiakkailleen. Tietoturva onkin yksi puhuttavimmista aiheista nykypäivänä leviävien viruksien, matojen ja hyökkäyksien takia. Tietoturva tulisi siis säilyttää mahdollisimman korkeana niin yrityksien lähiverkoissa kuten myös yritysten ja toimipisteiden välisissä yhteyksissä.

Toimeksiantajani Salesline Oy on maahantuonti- ja tukkuliikeyritys, joka koki suuria muutoksia vuonna 2004, kun yritys aloitti erään tuotteensa valmistamisen Suomessa. Näihin aikoihin yritys joutui tekemään suuria investointeja ja yritys jakautui kahdelle eri paikkakunnalle.

Tämän tutkintotyöaiheen käynnistäjänä ovat toimineet vanhempieni omistaman yrityksen, Salesline Oy:n, ongelmat tilausten käsittelyssä yrityksen jakauduttua kahteen toimipisteeseen. Ongelmat ovat vain korostuneet yrityksen hankittua kolmannen toimipisteen. Pääongelmiksi ovat osoittautuneet tilausten käsittely, tiedostojen käsittely ja säilyttäminen useammalla tietokoneella ja tärkeiden tietojen välittäminen suojaamattomana sähköpostilla.

Salesline Oy:ltä saamani toimeksiannon perusteella tutkin mahdollisuuksia kehittää toimistojen lähiverkkoja paremmin tarpeita vastaaviksi. Tutkin myös vaihtoehtoisia tapoja liittää toimipisteet yhdeksi loogiseksi tietoverkoksi lisäten toimipisteiden välisen kommunikaation tietoturvallisuutta. Pyrin suunnittelemaan tietoverkon myös taloudellisesti, joten suurten yritysten hyödyntämiä monen palvelimen ja erillisten palomuurikoneiden maailmaan en syvenny. Lyhyesti tutkintotyön tavoitteena on suunnitella Salesline Oy:lle kehittyneempi, tietoturvallinen tietoverkkoratkaisu.

2. Toimeksiantaja

Salesline Oy on avioparin perustama perheyritys, joka maahantuo, valmistaa ja markkinoi kolmea eri tuotetta. Anita ja Vesa Puukkoniemi perusti yrityksen vuonna 1985. Vuosien varrella yritys on myynyt monenlaisia tuotteita Pikkurillistä Tuplasulkaan. Tällä hetkellä yritys myy Sports Lace–kengännauhoja, Aito–lampaanvillapohjallisia ja Kurastoppari–ovimattoja.

Vuonna 2002 yritys koki suuria muutoksia, kun saksalainen yhteistyökumppani päätti lopettaa toimintansa. Tämä tarkoitti myös sitä, että Kurastoppari–ovimaton valmistus lopetettaisiin. Tuotemerkin lopettaminen ei tullut kyseeseenkään, koska Kurastoppari–ovimatto toi suurimman osan liikevaihdosta yritykseen. Ilmoituksen myötä alkoi siis uuden valmistajan metsästys.

Salesline Oy:n omistajat kiersivät pitkin Eurooppaa mattomalliensa kanssa ja toivoivat löytävänsä jonkun, joka osaisi valmistaa tai valmistaisi kyseisenlaatuista mattoa. Karu todellisuus tuli vastaan, kun osa valmistajista sanoi, etteivät pysty eivätkä halua rakentaa sellaista pitkää linjastoa, jonka maton valmistamiseen tarvitaan.

Eräs belgialainen yritys yritti valmistaa samanlaista mattoa kuin Kurastoppari–ovimatto on, mutta harmillisesti tämäkään ei onnistunut. Totuus oli, että kukaan ei enää valmistanut tällaista mattoa, kun yhteistyökumppanimme sen valmistuksen päätti lopettaa.

Vaihtoehdot alkoivat vähentyä ja myös tuotemerkin lopettamista harkittiin pariin otteeseen. Kolmen kuukauden kuluttua saksalainen yhteistyökumppanimme otti yhteyttä ja tarjosi mahdollisuutta ostaa vuosikymmeniä vanhat laitteensa, 50 metriä pitkän linjaston, joilla mattoa oli tehty. Omistajat päättivät, että he ostavat laitteet, mutta sitä ennen heidän on pystyttävä tekemään suuri erä mattoja Saksassa, jotta voisivat taata markkinoiden jatkumisen Suomessa ja saisivat asioiden järjestelyihin tarpeeksi aikaa.

Saksalainen yhteistyökumppani kertoi, että linjaston käyttäminen ei olisi mahdollista Saksassa, koska lämmitykseen käytettävä höyrykattila oli hajonnut. Suomesta käsin kuitenkin selvitettiin, että Saksassa on mahdollisuus vuokrata liikkuva höyrykattilajärjestelmä, jonka voisi liittää vanhan tilalle siksi aikaa, kun Salesline Oy:n työntekijät opettelisivat maton tekoa.

Monien vastoinkäymisien jälkeen maton valmistus onnistui Saksassa, jonka jälkeen koko linjasto purettiin ja rahdattiin Suomeen. Linjasto varastoitiin ensiksi Pirkkalaan varastohalliin, jonka jälkeen alettiin miettiä ja suunnitella linjaston tulevaa olinpaikkaa. Tässä vaiheessa harkittiin uuden hallirakennuksen rakentamista Tampereelle tai lähikuntiin. Investoinnit uuden hallirakennuksen rakentamiseen olisivat kuitenkin olleet niin suuret, että harkittiin myös valmiin hallirakennuksen ostamista tai vuokraamista. Vuokraaminen kuitenkin suljettiin pian pois laskuista, koska linjaston purkaminen ja kasaaminen on niin suuri urakka, että sitä ei haluttaisi tehdä enää uudestaan edes kymmenien vuosien jälkeen.

Oikean kokoisen, 50 metriä pitkän ja ainakin kuusi metriä leveän, hallirakennuksen löytäminen kohtuullisen läheltä vaikutti kuitenkin ylipääsemättömältä. Lähimmäksi osui Orivedeltä löytynyt vanha ruuvitehdas, joka oli kuitenkin päässyt niin heikkoon kuntoon, että remontointikuluilla olisi melkein katettu jo puolet uuden hallin rakentamisesta. Epätoivon keskelle annettiin myös hieman onnea ja valmis halli löytyi, tosin 300 kilometrin päästä, Taipalsaaresta, Lappeenrannan lähikunnasta. Aika alkoi painaa päälle ja tämä halli tuntui ainoalta vaihtoehdolta, joten kaupat hallista tehtiin syyskuussa 2003.

Loka-marraskuun 2003 aikana linjasto siirrettiin Taipalsaareen, jossa se puhdistettiin, hiottiin ja maalattiin ennen paikalle asettamista. Viikkojen työn jälkeen linja oli uudelleen koottu ja testattu. Ensimmäinen kotimainen tuotantoerä valmistettiin Taipalsaaressa toukokuussa 2004.

Tässä vaiheessa yritys jakautui niin sanotusti kahtia, kun toimisto sijaitsi edelleen Tampereella vanhoissa tiloissaan ja tehdas oli Taipalsaaressa. Myöskään työntekijöitä ei ollut vielä tähän mennessä hankittu, kun ei vielä tiedetty, kuinka tuotantoa alettaisiin pyörittää. Tuotannon alkuun saanti oli tärkein asia, koska Saksassa valmistetut tuotteet alkoivat loppua varastosta. Maton pohjaus tehtiin aina kaikkien työntekijöiden voimin, mutta jälkikäsittely jäi omistajien hartioille, koska työntekijöillä oli omat työtehtävänsä ja menonsa Tampereella.

Tässä vaiheessa huomattiin myös puutteet sähköisessä tiedonvälityksessä, kun tilauksia käsitellään ja lähetetään kahdesta eri paikasta. Aina, kun tilaustenkäsittelyohjelmaa aletaan käyttää, pitää soittaa toiseen päähän Suomea ja tiedustella, onko ohjelmaan tehty siellä päässä muutoksia. Jos muutoksia on tehty, tiedot siirretään yrityksen sähköpostin kautta. Tämä on melko turvaton ja epävarma tapa hoitaa

yrityksen asioita, ja siihen omistajat tahtovat parannuksen, minkä vuoksi tämä opinnäytetyö on saanut alkunsa.

Nykyään Salesline Oy:llä on myös kolmas toimipiste, jossa ei ole vielä lähiverkkoa eikä Internet-yhteyttä. Kolmas, Lempäälän, toimipiste tullaan tulevaisuudessa myös verkottamaan ja yhdistämään muihin toimipisteisiin, mutta tällä hetkellä sitä ei tarvitse ottaa huomioon muutoin kuin laajenemismahdollisuuksien osalta.

3. Verkon nykytila

Tällä hetkellä Salesline Oy toimii kahdessa eri toimipisteessä, Tampereella ja Taipalsaaressa. Molemmissa paikoissa käytetään samaa, Tukiset–nimistä, tilausten käsittely- ja laskutusohjelmaa. Ohjelman tietokantoja siirretään tällä hetkellä sähköpostin turvin toimipisteiden välillä, koska ohjelma ei toimi verkkopohjaisesti ja toimipisteiden välille ei ole luotu minkäänlaista verkkolinkkiä.

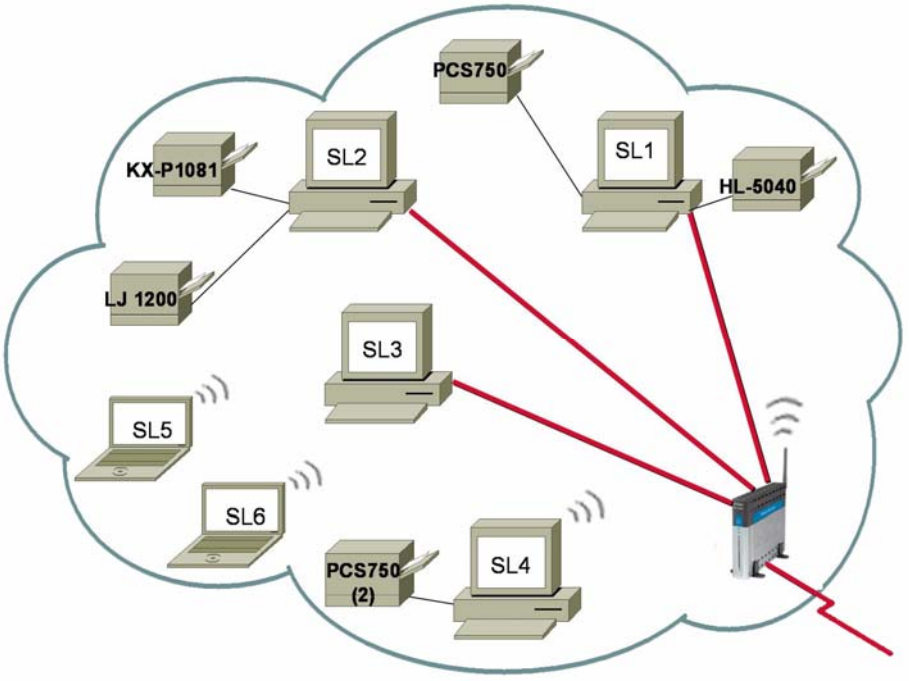
Samankaltainen ongelma esiintyy myös yrityksen toimistossa Tampereella. Tietokoneet ovat verkotettu keskenään D-linkin langattoman ADSL-reitittimen (Asymmetric Digital Subscriber Line) kautta, mutta osa käyttäjistä ei osaa käyttää verkkoresursseja. Myöskään Tukiset–ohjelmaa ei voi käyttää verkossa suoraan, vaan ohjelma on tietokantoineen aina siirrettävä sille koneelle, jolla ohjelmaa haluaa käyttää. Tietoja sijaitsee usealla koneella ja kaikkia pystyy muokkaamaan samanaikaisesti. Tämä aiheuttaa sen, että tiedostot eivät välttämättä ole ajan tasalla jokaisella koneella, jolloin tietoja saattaa kadota.

3.1. Laitteisto

3.1.1. Tampereen toimipiste

Tampereen toimiston tietoverkko koostuu tällä hetkellä neljästä pöytätietokoneesta, kahdesta kannettavasta tietokoneesta ja monista lisälaitteista. Lisälaitteita ovat useat tulostimet, joita on ajan saatossa ostettu miltei jokaiselle tietokoneelle yksi tai kaksi, ja D-Linkin langaton ADSL-reititin. Yksityiskohtaisemmat tiedot Tampereen toimiston tietokoneista ja laitteistosta löytyvät liitteestä 1 ja Taipalsaaren toimiston liitteestä 2.

Kuvasta 1 selviää, kuinka tietokoneet ja laitteet ovat verkotettu toisiinsa. Nimet ja numeroinnit eivät vastaa yrityksessä käytettyjä tietokoneiden nimiä. SL 1 on eniten käytössä oleva tietokone tehokkuutensa ja tietokoneeseen liitettyjen tulostimien takia. Yrityksen eniten käytetyimmät tiedostot löytyvät SL 1 tietokoneesta. Tälle tietokoneelle usein työntekijät jonottavat, koska ovat oppineet käyttämään sitä sujuvasti.



Kuva 1. Tampereen toimiston tämän hetkinen verkottuminen.

SL 2 on tietokone, jolla käsitellään enimmäkseen Tukiset-ohjelmaa. Tämä johtuu siitä, että tämän tietokoneen perään on liitetty Panasonic KX-P1081-matriisikirjoitin, jota käytetään ainoastaan Tukiset-ohjelmasta tulostettaessa. Tukiset-ohjelma ei myöskään ymmärrä verkkotulostimia, joten SL 2 tietokoneen perään on lisätty myös HP LaserJet 1200-tulostin, jolla tulostetaan yrityksestä lähetettävät laskut.

SL 3 tietokone on vuosien saatossa jäänyt vähimmälle käytölle. Kyseistä tietokonetta käytetään lähinnä Internetissä surffailuun, mutta senkin se suorittaa tehottomuutensa takia hitaasti. Yleensä, jos jokin muu tietokone on vapaana, työntekijät valitsevat jonkin tehokkaamman tietokoneen Internetin käyttöön.

SL 4 tietokoneella työskennellään lähinnä sähköpostin lukemisen ja lähettämisen sekä web-sivuston tekemisen ja päivittämisen kanssa. Tällä tietokoneella tehdään myös paljon markkinointimateriaalin suunnittelua ja kuvien sähköiseen muotoon siirtoa, jonka vuoksi yksi HP PSC 750 monitoimitulostin on liitettynä tähän koneeseen.

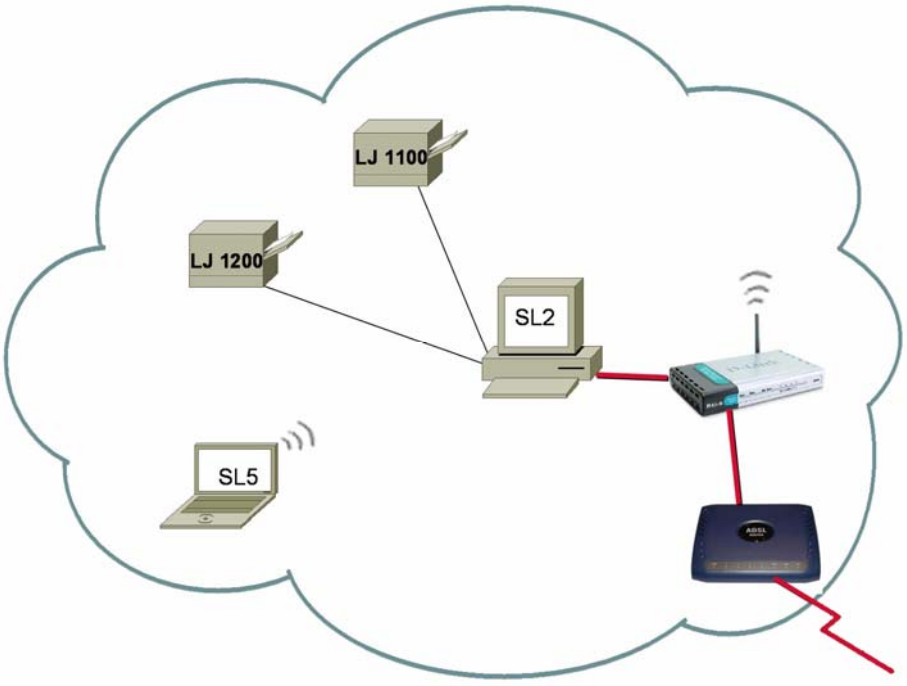
SL 5 on kannettava tietokone, joka on viimeinen tietokonehankinta. Kyseinen kannettava ostettiin syksyllä 2004 paikkaamaan edeltäjänsä SL 6:n tehtävää, koska SL 6 kannettavan tietokoneen toiminta oli työntekoa haittaavaa. SL 6 saattoi kesken ohjelman käytön, esimerkiksi tekstin kirjoittamisen, pysähtyä eikä suostunut tekemään enää mitään.

Eteenpäin pääsi vain uudelleen käynnistämällä tietokoneen. SL 6:ta on tarkasteltu ja tutkittu Salesline Oy:n puolesta useaan otteeseen, mutta vikaa kyseisestä tietokoneesta ei ole löytynyt. SL 6 on toiminnallisuutensa vuoksi jätetty lähinnä Internet-käyttöön, mutta odottaa ammattilaisen tarkempaa tutkailua.

Kaikki tietokoneet yhdistää toisiinsa D-Linkin Wireless ADSL Router eli langaton ADSL-reititin. SL 1, SL 2 ja SL 3 on liitetty reitittimeen straight-through eli suoralla Cat5 Gigabit Ethernet-kaapeleilla. SL 4 on yhdistetty langattomasti D-Linkin langattomalla USB-adapterilla. SL 5 omaa sisäisen langattoman verkkokortin, jonka avulla se liittyy verkkoon. SL 6 yhdistyy kannettavalle tarkoitetulla D-Linkin 54 megabitin PC-kortilla.

3.1.2. Taipalsaaren toimisto

Kuten kuvasta 2 selviää, Taipalsaaren tietoverkko koostuu yhdestä pöytätietokoneesta (SL 2) ja yhdestä kannettavasta tietokoneesta (SL 5). Se sisältää myös ADSL-modeemin ja langattoman tukiaseman, joilla saadaan yhteys Internetiin ja tietokoneiden välille. Verkossa on myös kaksi tulostinta. Nämä laitteet eivät kuitenkaan ole aina Taipalsaaren toimistossa, vaan ne siirretään tarpeen tullen Tampereen toimistoon. Ainoastaan HP LaserJet 1100-lasertulostin, ADSL-modeemi ja langaton tukiasema ovat siellä aina.

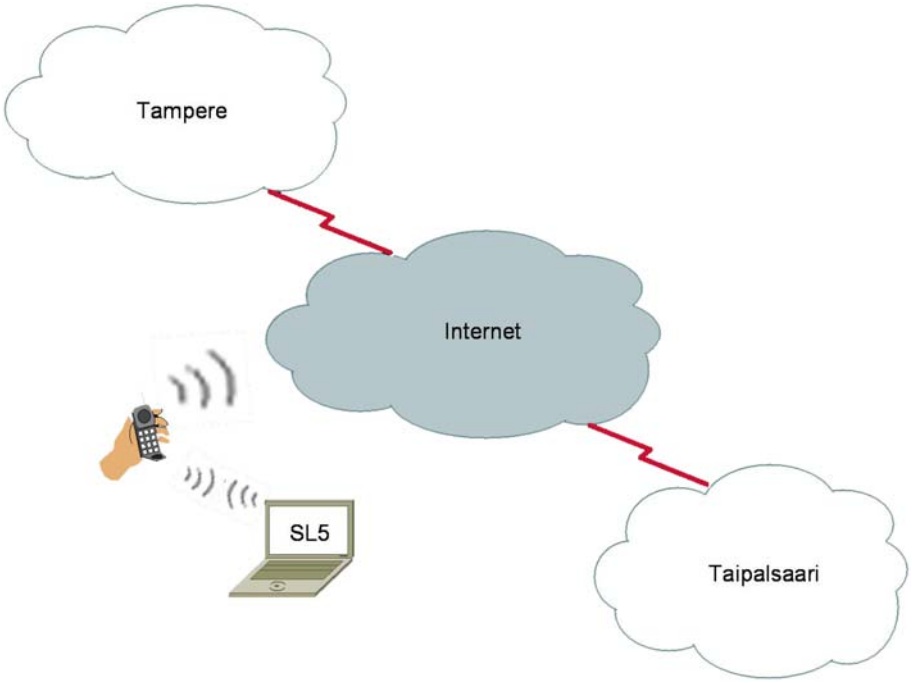


Kuva 2. Taipalsaaren toimiston tämän hetkinen verkottuminen.

Tietokoneet ovat yhdistettynä toisiinsa D-Linkin DI-624+ langattomalla reitittimellä. A-Linkin ADSL-modeemi mahdollistaa Internet-yhteyden muodostamisen. SL 2 on liitetty D-Linkin tukiasemaan suoralla Cat5 Gigabit Ethernet-kaapelilla. SL 5 yhdistyy verkkoon sisäisellä langattomalla verkkokortilla. Tulostimet ovat yhdistettynä SL 2 tietokoneeseen. HP LaserJet 1100-tulostin on liitetty perinteisellä tulostinkaapelilla ja HP LaserJet 1200 USB-kaapelilla.

3.1.3. Etätyöntekijä

Kuvasta 3 voidaan nähdä, kuinka toimipisteet ovat erillään toisistaan, samoin kannettava tietokone SL 5, josta on mahdollisuus päästä Internetiin GPRS-yhteydellä (General Packet Radio Service). SL 5 ottaa yhteyden matkapuhelimeen Bluetooth-teknologian avulla. Matkapuhelimella muodostetaan yhteys Internetiin GPRS:llä ja tällä tavoin SL 5:llä voidaan ladata esimerkiksi sähköpostit.



Kuva 3. SL 5 yhdistyy Internetiin GPRS:n avulla, toimipisteet ovat yhdistetty ADSL:n avulla.

3.2. Kehityskohdat

Kehityskohteita on niin toimiston verkossa kuin toimipisteiden välillä. Toimiston verkko tulisi muuttaa asiakas/palvelinpohjaiseksi. Verkossa olisi yksi tiedostopalvelin, jolla kaikki tiedostot sijaitsisivat ja niitä käytettäisiin kyseiseltä

palvelimelta. Vain yhden käyttäjän kerrallaan pitäisi voida käyttää tiedostoja, jotta päällekkäisyyksiltä vältytään. Tällä estetään tiedostojen siirtäminen, moninkertaistuminen ja tietojen katoaminen.

Toimipisteiden välille tulisi kehittää turvallinen, yksityinen linkki, jonka kautta voitaisiin olla yhteydessä toimiston verkkoon ja tulevaan tiedostopalvelimeen. Vaihtoehtoja näyttäisi löytyvän useampiakin, sovelluspohjaisista palveluista käyttöjärjestelmien omiin lisäpalveluihin. Tutkailen virtuaalista yksityisverkkoa eli VPN:ää (Virtual Private Network) ja salattua SSH-yhteyttä (Secure Shell) yksityisen linkin luomiseksi toimistoverkkojen välille.

4. Lähiverkon kehityssuunnitelma

Lähiverkon ongelmia pohtiessani päädyin asiakas/palvelin-ratkaisuun. Tällä ratkaisulla pystytään poistamaan moninkertaistuvat tiedostot ja estettäisiin tietojen katoaminen. Tämän ratkaisun toteuttamiseen tarvitaan palvelimelle soveltuva käyttöjärjestelmä ja tietysti itse palvelinkone. Palvelimen päätarkoituksena olisi tiedostojen säilyttäminen.

4.1. Asiakas/palvelin-malli

Petteri Järvisen IT-tietosanakirjan mukaan asiakas/palvelin on ”tietojärjestelmä, joka on hajautettu niin, että osa siitä toimii tavallisessa mikrossa (yleensä graafinen käyttöliittymä) ja osa (esimerkiksi tietokanta) isommassa koneessa, joko palvelimessa tai perinteisessä keskuskoneessa. Mikrojen ja keskuskoneen yhteistyö tapahtuu lähiverkon välityksellä” (Järvinen 2001: 49).

4.1.1. Verkkokäyttöjärjestelmä

Keoghin mukaan verkko toimii samalla tavalla kuin tietokone. Tietokone on vain laatikko, joka sisältää elottomia kytkimiä. Kun tietokoneeseen ladataan ohjelmisto, esimerkiksi Windows tai vastaava, tietokone herää henkiin. Sama pätee verkkoon. Verkko on myös kasa erilaisia kaapeleita, verkkokortteja ja muita osia, kunnes siihen asentaa verkkokäyttöjärjestelmän. Tämä mahdollistaa tiedon siirron verkon sisältämiä osia pitkin. (Keogh 2001: 223.)

Verkkokäyttöjärjestelmä on vähän kuin tietokoneessa toimiva käyttöjärjestelmä. Verkkokäyttöjärjestelmä huolehtii siitä, että tieto virtaa verkoissa ja antaa asiakkaille, jotka ovat liitettynä verkkoon, mahdollisuuden käyttää verkossa mahdollisesti sijaitsevien palvelimien verkkoresursseja kuten tiedostoja ja tulostimia. (Keogh 2001: 223.)

Verkkokäyttöjärjestelmässä on kaksi osaa, asiakasohjelma ja palvelinohjelma. Asiakkaiden levyasemiin asennetaan asiakasohjelmat ja palvelimiin palvelinohjelmat. Yhdessä nämä ohjelmat muodostavat turvallisen tavan, jolla asiakkaat voivat käyttää palvelimen resursseja. (Keogh 2001: 225.)

Verkkokäyttöjärjestelmän välitysohjelmalla asiakasohjelma lähettää verkkoresurssien käyttöpyynnöt verkkoon.

Välitysohjelma seuraa asiakaskoneen resurssipyyntöjä ja ohjaa verkkopalvelujen pyynnöt verkkoon. Välitysohjelman lähettämät pyynnöt vastaanottaa ja käsittelee palvelinohjelma. (Keogh 2001: 225.)

4.1.2. Tiedostopalvelin

Tiedostopalvelin on verkon tietokone, jossa säilytetään tiedostoja. Se on kuin kiintolevy, jota kaikki verkon käyttäjät voivat hyödyntää. Tiedostopalvelimen kiintolevylle voi tallentaa ja sieltä voi noutaa tiedostoja jokainen, jolla on yhteys kyseiseen verkkoon ja oikeus käyttää tiedostopalvelinta. Hyvänä esimerkkinä voit tallentaa tiedostopalvelimelle taulukkolaskentaohjelman tiedoston ja ystäväsi voi avata kyseisen tiedoston omalla tietokoneellaan. (Keogh 2001: 226.)

Tiedostopalvelin ja verkko toimivat yksi yhteen verkossa olevan tietokoneen kanssa. Voit tallentaa tiedostopalvelimelle tietoja ja lukea niitä avain samalla tavalla kuin tietokoneen omalta kiintolevyltä tai levykkeeltä. (Keogh 2001: 227.)

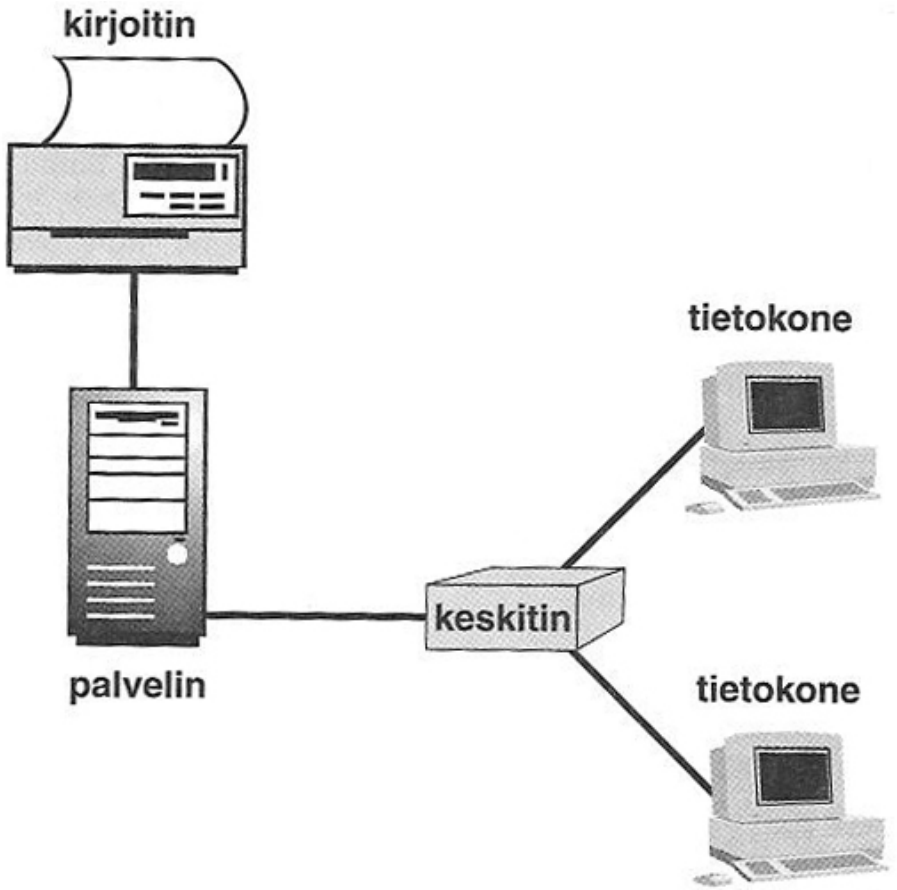
Windowsin Resurssinhallinta-ohjelma tietää, mitkä levyasemat ovat paikallisia ja mitkä verkkoresursseja. Esimerkiksi, jos asema I on verkkoresurssi, kyseiselle asemalle menevät käyttöpyynnöt siirretään välitysohjelmalle, joka pyytää verkkokäyttöjärjestelmää toteuttamaan tiedostonsiirron. (Keogh 2001: 227.)

4.1.3. Tulostuspalvelin

Keogh kertoo kirjassaan, että ohjelma nimeltään Tulostuksenhallinta yhdistää kirjoittimen nimen verkkokirjoittimeen samaan tapaan kuin paikallinen kirjoitin ilmoitetaan. Tämä liitos luodaan tietokoneen Ohjattu kirjoittimen asennus-toiminnolla verkon ylläpitäjän toimesta. (Keogh 2001: 227.)

Kirjoitinta valittaessa Tulostuksenhallinta tietää, onko kirjoitin liitetty suoraan tietokoneeseeni vai onko kyseessä verkkokirjoitin. Jos kyseessä on verkkokirjoitin, Tulostuksenhallinta lähettää kaikki sille tarkoitetut pyynnöt välitysohjelmalle, joka välittää ne käyttöjärjestelmän käsiteltäväksi. Jos verkkokirjoitin on kytketty tulostuspalvelimeen, se vastaanottaa asiakirjoja pyynnöstä, laittaa ne tulostusjonoon ja lähettää ne verkkokirjoittimelle. (Keogh 2001: 227.)

Paikalliselle kirjoittimelle tulostaminen on erilaista kuin verkkokirjoittimelle, koska kirjoitin määrää asiakirjojen tulostusjärjestyksen. Tulostuspalvelin tallentaa käyttäjiltä saapuvat asiakirjat väliaikaisesti spool-nimiseen muistiin. (Keogh 2001: 232.)



Kuva 4. ”Verkkokirjoitin jaetaan useiden verkkoasiakkaiden kesken.” (Keogh 2001: 233.)

4.1.4. Palvelinohjelma

Palvelinohjelmistolla on kolme päätehtävää: koordinoi verkkoresurssien käyttöä, antaa resurssien käyttöoikeuden ja vastaa käyttöoikeuksien antamisesta vain sellaisille asiakkaille, joilla on oikeus käyttää resurssia tietyllä tavalla. (Keogh 2001: 228.)

Palvelinohjelmisto verkonhallintatehtävään kuuluu verkon käyttöoikeuksien myöntäminen käyttäjätunnuksen perusteella. Käyttöoikeuksien myöntäminen tapahtuu käyttäjän kirjautuessa verkkoon. (Keogh 2001: 229.)

Kirjautumisprosessi kulkee seuraavasti: kirjauduttaessa verkkoon tietokoneen välitysohjelma pyytää kirjautumista kirjautumisruudun avulla, joka pyytää verkkokäyttäjätunnustasi ja salasanaa. Jokaiselle käyttäjälle on oma tunnuksensa ja salasanansa, jotka verkon ylläpitäjät ovat määritelleet. Kirjautumistietojen antamisen jälkeen välitysohjelma välittää tiedot ensisijaisen verkkopalvelimen tarkistettavaksi. Tiedot verrataan tiedostossa oleviin käyttäjiin, ja tietojen täsmätessä palvelin antaa käyttöoikeuden verkkoresursseihin. (Keogh 2001: 229.)

Kaikkiin verkkoresursseihin ei ole kaikilla oikeuksia. Verkon ylläpitäjä hallinnoi verkonhallintaohjelmalla resurssien, kuten kirjoittimien tai tiedostopalvelimen, käyttöoikeuksia. Verkonkäyttäjiä voidaan myös luoda tai poistaa verkonhallintaohjelmalla. (Keogh 2001: 229.)

4.2. Verkkokäyttöjärjestelmät

Verkkokäyttöjärjestelmiä on kymmeniä, joten on tarpeen selvittää, minkälainen verkkokäyttöjärjestelmän tulisi olla, jotta sitä voitaisiin hyödyntää vielä tulevaisuudessakin yrityksen kohdatessa uusia muutoksia. Jo nyt on tiedossa, että vanha Tukiset-ohjelma tullaan jossakin vaiheessa päivittämään nykyaikaisempaan järjestelmään, joten sekin tulisi ottaa huomioon.

Useimmiten taloushallinnon ohjelmat vaativat Windows-verkkokäyttöjärjestelmän, jolloin tietysti olisi helpoin päätyä parhaimpaan Windows-verkkokäyttöjärjestelmään. Nämä verkkokäyttöjärjestelmät ovat kuitenkin lisensseiltään kohtuullisen kalliita ja tämän tyyppistä verkkokäyttöjärjestelmää ei vielä tarvita. Pitää ottaa myös huomioon, että tulevaisuudessa taloushallinnon ohjelmalle kannattaisi varata oma palvelin niin tehokkuuden kuin tietoturvallisuudenkin nimissä.

Verkkokäyttöjärjestelmän toiminnallisuuksien tulisi olla tavallisen käyttäjän näkökulmasta kuin palvelinverkkoa ei olisikaan olemassa. Tarkoituksena on siis, että tiedostopalvelin näkyy yhtenä levyasemana käyttäjän tietokoneessa, jolloin käyttäjän on helppo omaksua se käyttöönsä. Myös tulostustoiminnot tulisi näkyä käyttäjälle kuin ne olisivat suoraan omassa tietokoneessa kiinni.

4.2.1. Microsoft Windows Server 2003

”Windows Server 2003-tuoteperhe on nopeasti muuttuvilla markkinoilla toimiville yrityksille tarkoitettu teknisten ratkaisujen pohja. Windows Server 2003 muodostaa ainutlaatuinen tietojenkäsittely-ympäristön kaikenkokoisille yrityksille.” (Microsoft 2005)

Windows Server 2003 perustuu Windows 2000-käyttöjärjestelmään. Windows Server 2003:n sisältyy asiakkaiden arvostamat perusominaisuudet, kuten toiminnan luotettavuus, suojaus ja skaalattavuus. Windows Server-tuoteperhettä on parannettu ja laajennettu, jotta yritykset voivat hyödyntää kaikkia .NET.toimintoja. (Microsoft 2005)

Windows Server 2003-perhe sisältää seuraavat neljä tuotetta:

- Windows Server 2003 Web Edition
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datcenter Edition

(Microsoft 2005)

Näistä lähemmin tutkin Windows Server 2003 Standard Edition-versiota, koska se vastaa parhaiten lähiverkon tarpeita.

Windows Server 2003 Standard Edition verkkokäyttöjärjestelmällä voidaan nopeasti ja helposti toteuttaa yrityskohtaisia ratkaisuja. Tämä palvelin soveltuu kaikenkokoisten yritysten päivittäiseen käyttöön. (Microsoft 2005)

Windows Server 2003 Standard Edition:

- tukee tiedostojen ja tulostinten jakamista
- sisältää suojatut Internet-yhteydet
- mahdollistaa keskitetyn sovellusten käyttöönoton
- sisältää monipuoliset työntekijöille, yhteistyökumppaneille ja asiakkaille tarkoitetut yhteiskäyttötoiminnot
- tukee kaksisuuntaista symmetristä moniprosessointia ja 4 gigatavun muistia
  (Microsoft 2005)

4.2.2. FreeBSD

”FreeBSD on vapaa BSD-pohjainen Unixin kaltainen tietokoneen käyttöjärjestelmä. FreeBSD-projekti on erityisesti keskittynyt luomaan tehokasta käyttöjärjestelmää Intel- ja AMD-yhteensopiville tietokoneille. FreeBSD on myös pohjana Applen Macintosh-tietokoneiden Mac OS X-käyttöjärjestelmälle.” (Wikipedia 2005)

FreeBSD tarjoaa kehittyneitä verkkotyöskentely-, suorituskyky-, turvallisuus- ja yhteensopivuusominaisuuksia, jotka puuttuvat tänä päivänä muista käyttöjärjestelmistä, myös parhaista kaupallisista. FreeBSD on ideaali Internet tai Intranet palvelin. Se tarjoaa järeitä verkkopalveluita raskaidenkin kuormien alla ja käyttää muistia tehokkaasti säilyttääkseen hyvän vastausajan tuhansille yhtäaikaisille käyttäjäprosesseille. (FreeBSD 2005)

Prosessori-Uutisten mukaan FreeBSD-projektiryhmä on julkaissut uuden version avoimen lähdekoodin käyttöjärjestelmästään, joka haastaa Linuxin, Sun Solariksen ja Windowsin organisaatio- ja yrityskäytössä. Uusimman FreeBSD 6.0 luvataan olevan luotettava, skaalautuva ja turvallinen ympäristö avoimen lähdekoodin ohjelmistoille. Tärkeimpiä uudistuksia on monisäikeinen tiedostojärjestelmä, joka nostaa merkittävästi levyn käsittelyn nopeuksia paikallisilla levyillä, raid-kokoonpainoilla, verkkolevyillä ja tallennusverkoissa. Suorituskykytestien mukaan käyttöjärjestelmä päihittää Linuxin raa’assa tiedonsiirron käsittelynopeudessa. (Prosessori-Uutiset 2005)

Samba on suosittu avoimen lähdekoodin ohjelmapaketti, joka tarjoaa tiedosto- ja tulostinpalveluita Microsoft Windows asiakkaille. Tällaiset asiakkaat voivat yhdistyä ja käyttää FreeBSD tiedostoavaruutta kuin se olisi paikallinen levyasema, tai FreeBSD tulostimia kuin ne olisi paikallisia tulostimia. (FreeBSD Handbook 1999: 695)

Sivuston www.samba.org:n mukaan Samba koostuu kahdesta avainohjelmasta. Nämä ohjelmat ovat smbd ja nmbd. Niiden tehtävänä on toteuttaa neljä nykyaikaista CIFS (Common Internet File System) peruspalvelua, jotka ovat tiedosto- ja tulostuspalvelut, tunnistaminen ja valtuutus, nimenselvitys sekä palvelutiedotus (selailu). (Samba: An Introduction 2001)

Tiedosto- ja tulostinpalvelut ovat CIFS:n kulmakivi. Nämä tarjoaa smbd, SMB Daemon. Smbd hoitaa myös jakamis- ja käyttäjätilan tunnistamisen ja valtuuttamisen. Tämä tarkoittaa

sitä, että voit suojata jaetut tiedostot ja tulostuspalvelut salasanan taakse. Jakamistilassa, helpoin ja vähiten suositeltu tapa, salasana voidaan antaa jaetulle hakemistolle tai tulostimelle. Tämä salasana annetaan kaikille, joilla on lupa käyttää jakoa. Käyttäjätilan tunnistamisessa jokaisella käyttäjällä on oma käyttäjänimi ja salasana ja ylläpitäjä voi hyväksyä tai kieltää pääsyn yksilökohtaisella tasolla. (Samba: An Introduction 2001)

Kahta muuta CIFS:n osaa, nimenselvitystä ja selailua, hoitaa nmbd. Nämä kaksi palvelua pohjimmiltaan sisältää NetBIOS nimilistan hallinnan ja jakelun. (Samba: An Introduction 2001)

Nimenselvitys ymmärtää kaksi muotoa: lähetys (broadcast) ja pisteestä pisteeseen (point-to-point). Kone voi käyttää näistä vain toista tapaa tai molempia tapoja riippuen sen asetuksista. Lähetysselvitys on lähimpänä alkuperäistä NetBIOS mekanismia. Periaatteessa asiakas, joka etsii palvelua nimeltä Trillian, huutelee ”Trillian! Missä olet?” ja odottaa vastausta sen nimiseltä koneelta, jolla on IP-osoite (Internet Protocol). Tämä voi aiheuttaa jonkin verran lähetysliikennettä, mutta se on rajoitettu lähiverkkoihin, joten siitä ei ole paljoa haittaa. (Samba: An Introduction 2001)

Toinen nimenselvitystyyppi sisältää NBNS (NetBIOS Name Service) palvelimen käytön. NBNS toimii kuin vanhan puhelinkopin seinä. Koneet jättävät nimensä ja numeronsa (IP-osoite) muiden nähtäväksi. Asiakkaat lähettävät heidän NetBIOS nimensä ja IP-osoitteensa NBNS palvelimelle, joka säilyttää tietoa yksinkertaisessa tietokannassa. Kun asiakas haluaa keskustella toisen asiakkaan kanssa, se lähettää toisen asiakkaan nimen NBNS palvelimelle. Jos nimi on listalla, NBNS palvelin palauttaa IP-osoitteen. NBNS tunnetaan nykyään paremmin Microsoftin julkaisemalla nimellä Windows Internet Naming Service (WINS). (Samba: An Introduction 2001)

Asiakkaat eri verkoissa voivat jakaa saman NBNS palvelimen, toisin kuin lähetyksessä, joten pisteestä pisteeseen mekanismi ei ole rajoitettu paikalliseen lähiverkkoon. Monella tapaa NBNS on samankaltainen kuin DNS (Domain Name Service), mutta NBNS nimilista on melkein kokonaan dynaaminen ja siellä on muutama kontrolli, jotka varmistavat, että vain valtuutetut asiakkaat voivat rekisteröidä nimiään. (Samba: An Introduction 2001)

Selailu tässä merkityksessä ei tarkoita tuntemaamme Internet selailua vaan selattavaa listaa palveluista, joita tietokoneet verkossa tarjoavat. Lähiverkossa osallistuvat tietokoneet

valitsevat paikallisen isäntäselaimen eli Local Master Browserin (LMB). Valittu tunnistaa itsensä ilmoittamalla erityisen NetBIOS nimen. LMB:n tehtävä on pitää listaa saatavilla olevista palveluista, ja tämä on se lista, joka tulee näkyviin Windowsissa ”Verkkoympäristö” nappia painamalla. (Samba: An Introduction 2001)

LMB:n lisäksi on olemassa Domain Master Browsereita (DMB) eli toimialueen isäntäselaimia. DMB:t järjestää selauslistoja pitkin NT toimialueita, jopa reititetyistä verkoista. NBNS:n avulla LMB löytää DMB:nsä vaihtaakseen ja yhdistääkseen selauslistoja. Vaikka selauslistoja on levitetty kaikille isännille NT toimialueessa, valitettavasti synkronointiajat ovat hieman harallaan. Voi kestää yli puoli tuntia saada kaukainen verkko näkyviin Verkkoympäristössä. (Samba: An Introduction 2001)

4.3. Palvelintietokone

Tässä luvussa perehdyn tarkemmin palvelintietokoneeseen liittyviin vaatimuksiin. Verkkokäyttöjärjestelmät tarvitsevat niille soveltuvan alustan toimiakseen tehokkaasti.

Microsoft Server 2003 Standard Edition laitteistovaatimukset ovat seuraavanlaiset:

- Suorittimen vähimmäisnopeus 133 MHz
- Suositeltava suoritinnopeus 550 MHz
- Random Access Memory (RAM)-muistin vähimmäismäärä 128 Mt
- Suositeltava RAM-muistin vähimmäismäärä 256 Mt
- RAM-muistin enimmäismäärä 4 Gt
- Usean suorittimen tuki 1 tai 2
- Asennuksen edellyttämä levytila 1,5 Gt
- (Microsoft 2005)

FreeBSD:n laitteistovaatimukset ovat räätälöity eri alustoille, monet laitteet ovat tuettu (tai merkityksellisiä) ainoastaan tietyille prosessoreille tai rakenteille. (FreeBSD 2005)

FreeBSD:n uusimman 6.0-RELEASE version tuetut prosessorit ja emolevyt i386-alustalle ovat seuraavanlaiset:

- IBM PC yhteensopiva kone
- i386 yhteensopiva kannettava
- i386 yhteensopiva prosessori vaihtuvalla pisteellä
- Intelin prosessorit tuettuja 80486:sta alkaen

- i386 yhteensopiva AMD-prosessori ja Duron-prosessori
- emolevyt käyttäen ISA-, VLB-, EISA-, AGP- ja PCI-laajennusväyliä tuettuja
- symmetrinen multiprosessori (SMP) yleisesti tuettu

FreeBSD 6.0-RELEASE tukee myös monia muita laitteita, esimerkiksi Ethernet-verkkokortteja, langattomia verkkorajapintoja, äänilaitteita, USB-laitteita, ja niin edelleen, jotka on lueteltu merkeittäin ja malleittain FreeBSD:n kotisivuilla osoitteessa www.freebsd.org.

4.4. Varmuuskopiointi

Tieto voi kadota tai vahingoittua monella tavalla, kuten esimerkiksi laitteiden hajotessa, ilkivallan, viruksien ja matojen sekä jopa luonnonmullistuksien seurauksina. Tiedon katoaminen on mahdollista parhaiten suojatuissakin tietovarastoissa. (Keogh 2001: 269.)

Tietojen kadotessa ensimmäiseksi pitää suorittaa tiedon palautus, jotta organisaatio tai yritys pysyy toimintakykyisenä. Tieto voidaan palauttaa joko luomalla se uudestaan tai kopioimalla se toisesta lähteestä. (Keogh 2001: 269.)

Tiedon uudelleenluonti on huonoin vaihtoehto tiedon palautuksessa, koska se on aikaa vievää ja uudelleenluonnin aikana saattaa tietoon tulla virheitä. Monesti tiedon uudelleenluonti ei myöskään ole mahdollista. Paras palautuskeino on tiedon kopiointi. Tällöin palautettu tieto vastaa tietoa, joka oli palvelimella ennen ongelmien syntymistä. (Keogh 2001: 269 - 270.)

Witherspoonien mukaan on tehtävä ero luotettavien ja epäluotettavien varmuuskopioiden välillä. Jälkeenpäin on paha jossitella, että varmistukset on tehty huolimattomasti tai huonolle medialle. He luetteloivat myös asiat, jotka huomioimalla varmuuskopioista ja palautuksista on hyötyä.

- Varmistuksista on hyötyä vain mikäli myös palautus onnistuu. Palautusmenetelmä tulee testata säännöllisesti.

- Joukko valittuja tiedostoja kannattaa palauttaa koemielessä säännöllisesti tähän varattuun paikkaan palvelimella.

- Varmistettaessa kriittisiä tietoja tulee käyttää varmuuskopioinnin optioita, joka tarkistaa heti kirjoittamisen jälkeen sen onnistumisen. Lisäksi tulee tarkistaa kaikki aiotut tiedostot ovat varmasti tallentuneet varmistusmedialle.

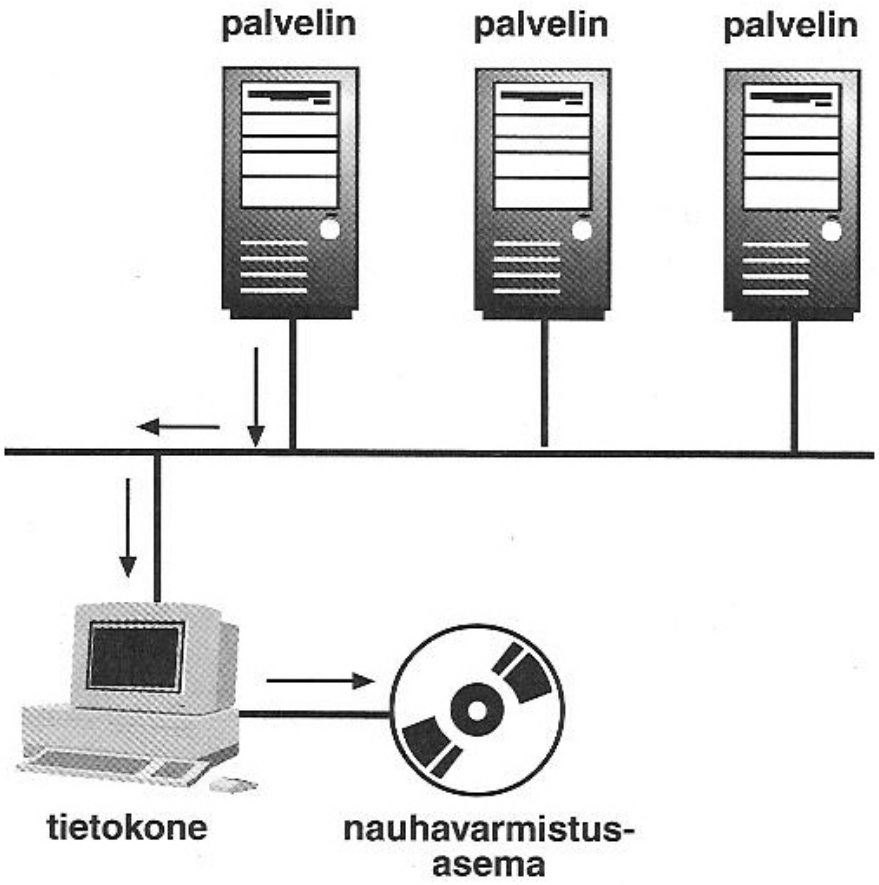
- Varmuuskopioiden on aina oltava ajan tasalla. Niiden tekoon tulee laatia erillinen aikataulu, jota noudatetaan täsmällisesti.

- Kannattaa muistaa, että myös luotettavilla varmuuskopioilla on rajoituksensa. Data saattaa olla vanhentunutta ja käyttäjät saattavat varmistaa tarpeetonta dataa sisältäviä levyjä.

- Tietyt varmuuskopiot voi olla viisasta säilyttää muualla täysin omissa tiloissaan. Tämä turvaa datan säilyvyyden, vaikka itse verkko tuhoutuisi pahimmassa tapauksessa esimerkiksi tulipalossa.

- Tietokonevirus voi saastuttaa sekä palvelimen että kaikki varmuuskopiot. Palvelimen levyille on tehtävä virustarkistus aina ennen varmistuksia.
  (Witherspoon 1996: 365 – 366).

Jotta tiedon palauttaminen voitaisiin tehdä kopioimalla, alkuperäinen tieto on pitänyt kopioida johonkin tallennusmediaan kuten nauhalle, CD:lle tai levykkeelle. Tätä kutsutaan tiedon varmuuskopioinniksi (Kuva 5). Yleisin varmuuskopiointimenetelmä on nauha tai CD-varmuuskopiointi. Tällä keinolla kaikki tieto ja tiedostot, kuten ohjelmat, kopioidaan säännöllisesti nauhalle tai CD:lle. (Keogh 2001: 270.)



Kuva 5. ”Verkon ylläpitäjä voi palauttaa datan, koska hän varmuuskopioi sen säännöllisesti.” (Keogh 2001: 270.)

Varmuuskopiointiratkaisuja on monia, joista William R. Stanek mainitsee kirjassaan seuraavaa:

- Nauha-asemat ovat yleisimmin käytettyjä varmuuskopiointilaitteita. Niissä tiedot tallennetaan kaseteille, joissa on magneettinen nauha. Magneettiset nauhat ovat melko edullisia, mutta eivät täysin luotettavia. Nauhat voivat katketa tai venyä. Ne voivat myös menettää tietoja ajan mittaan. Nauhojen tallennuskapasiteetti vaihtelee keskimäärin 4 gigatavusta 10 gigatavuun. Muihin ratkaisuihin verrattuna nauha-asemat ovat melko hitaita. Niiden merkittävin myyntivaltti on edullinen hinta.

- Digitaaliset nauha-asemat ovat monessa tapauksessa syrjäyttäneet perinteiset nauha-asemat suositeltavina varmuuskopiointilaitteina. Laajamittaiseen käyttöön soveltuvat esimerkiksi DLT- (Digital Linear Tape) tai Super DLT-nauhurit. DLT IV-nauhojen pakkaamattomat tallennuskapasiteetit ovat 35 Gt ja 40 Gt (70 Gt ja 80 Gt

pakattuna). Suurten yritysten kannattaa tutkia LTO- (Linear Tape Open) ja AIT- tekniikoita (Advanced Intelligent Tape). LTO-nauhoilla on tyypillisesti 100 Gt pakkaamatonta tallennuskapasiteettia (200 Gt pakattuna). AIT-3-nauhojen tallennuskapasiteetti on 100 Gt pakkaamatta (260 Gt pakattuna).

- Automaattiset nauhanvaihtojärjestelmät käyttävät automaattisesti useita nauhoja laajentaen siten tallennuskapasiteettia huomattavasti. Nauhat vaihdetaan automaattisesti varmuuskopioinnin ja palautuksen aikana. Useimmat nauhanvaihtojärjestelmät käyttävät digitaalista tallennustekniikkaa (DAT, DLT, LTO tai AIT). Tyypilliset DLT-asemat voivat tallentaa jopa 45 gigatavua tunnissa, ja nopeuttaa voidaan edelleen parantaa hankkimalla nauhakirjastojärjestelmä, joka käyttää useita asemia. Tällä tavoin voidaan tallentaa usealle nauhalle samanaikaiseksi. Useimmat LTO- ja AIT-asemat tallentavat yli 100 gigatavua tunnissa, ja useita asemia käytettäessä päästään satoihin gigatavuihin tunnissa.

- Optiset jukeboksit muistuttavat automaattisia nauhanvaihtojärjestelmiä. Ne käyttävät nauhojen sijaan MO-levyjä (Magneto Optical). Ne vaihtavat levyjä tarpeen mukaan automaattisesti, mutta niiden haittapuolena on korkea hinta.

- Vaihdettavia levyjä, kuten Iomega Jazia (1 Gt ja 2 Gt-versiot) käytetään paljon varmuuskopiointiin. Vaihdettavat levyt ovat nopeita ja helppokäyttöisiä varmistettaessa yksittäistä asemaa tai yksittäistä järjestelmää. Laajemmassa käytössä kustannukset ovat kuitenkin suuremmat kuin perinteisiä nauha-asemia tai digitaalisia nauha-asemia käytettäessä.

- Kiintolevyt ovat nopein tapa varmuuskopioida ja palauttaa tietoja. Niiden avulla voidaan usein tehdä muutamassa minuutissa se, mihin nauha-asemalta voi kulua tunteja. Jos yritys tarvitsee hyvin nopeaa palautusratkaisua, mikään ei voita kiintolevyjä. Kiintolevyillä toteutettu varmuuskopiointiratkaisu on kuitenkin suhteellisen kallis verrattuna nauhakirjastojärjestelmiin.
  (Stanek 2003: 357).

4.4.1. Varmuuskopiointi Microsoft Windows Server 2003:ssa

Microsoft Windows Server 2003:ssa on varmuuskopiointiohjelma nimeltään Backup. Ohjelmalla voidaan tehdä varmuuskopioita sekä paikallisesta että etäjärjestelmästä. Ohjelmalla on mahdollista arkistoida tiedostoja ja kansioita sekä myös palauttaa ne. Tehtävämanagerin avulla varmuuskopiointi voidaan myös automaattisesti ajoittaa. (Stanek 2003: 358).

Jotta varmuuskopioiden tekeminen ja palauttaminen olisi mahdollista, käyttäjällä on oltava valtuudet ja käyttöoikeudet sen tekemiseen. Täydet valtuudet varmuuskopioinnin tekoon ja palauttamiseen mistä tiedostosta tahansa on Järjestelmänvalvoja- ja Varmuuskopiointioperaattori-ryhmien jäsenillä. (Stanek 2003: 359.)

Varmuuskopioinnin voi tehdä Backup-ohjelman ohjatulla toiminnolla tai ohjelmasta löytyvältä Backup-välilehdellä. Ohjelmassa pystyy valitsemaan tekeekö varmuuskopioin kaikista tietokoneen tiedostoista, tietyistä valituista tiedostoista vai vain järjestelmän tilatiedoista. Ohjelmassa pystyy valitsemaan myös käytetäänkö varmuuskopiotiedostoa vai tietovälinettä, kuten esimerkiksi nauhaa tai levyä. (Stanek 2003: 360 – 365.)

4.4.2. Varmuuskopiointi FreeBSD:ssä

FreeBSD:ssä on kolme merkittävää varmuuskopiointiohjelmaa, jotka ovat dump(8), tar(1) ja cpio(1). Perinteisiä UNIX-varmuuskopiointiohjelmia ovat dump ja restore. Ne toimivat asemalla levylohkokokoelmana, tiedosto-, linkki- ja hakemistoabstraktion alla, jotka tiedostojärjestelmä on luonut. Dump varmuuskopioi koko tiedostojärjestelmän laitteeseen. (FreeBSD Handbook 1999: 456 – 457.)

Dump ohjelmalla ei pysty varmuuskopioimaan vain osaa tiedostojärjestelmästä tai hakemistopuuta, joka käsittää enemmän kuin yhden tiedostojärjestelmän. Dump ei myöskään kirjoita tiedostoja ja hakemistoja nauhalle, mutta kirjoittaa raakadatalohkoja, jotka sisältävät tiedostoja ja hakemistoja. Varmuuskopiointi on mahdollista suorittaa verkon yli toisen tietokoneen nauha-asemaan. Dump ja restore-ohjelmilla on myös mahdollista käyttää turvallisempaa tapaa SSH:n yli. (FreeBSD Handbook 1999: 457.)

Tar toimii yhteistyössä tiedostojärjestelmän kanssa; se kirjoittaa tiedostoja ja hakemistoja nauhalle. Tar ei tue kaikkia asetuksia, jotka ovat saatavilla cpio(1):ssa , mutta se ei vaadi epätavallista putkilinjaa, jota cpio käyttää. Tar tukee etälaitteita käyttäen samaa syntaksia kuin rdump. (FreeBSD Handbook 1999: 457.)

Cpio(1) on alkuperäinen UNIX tiedostojen vaihto-ohjelma magneettiselle medialle. Cpio:lla on asetuksia (monien muiden joukossa) suorittamaan tavuvaihtoa, kirjoittamaan paljon erilaisia tiedostomuotoja ja johtamaan dataa muihin ohjelmiin. Viimeinen ominaisuus tekee cpio:sta erinomaisen vaihtoehdon asennusmedialle. Cpio ei tue varmuuskopiointia verkon yli. (FreeBSD Handbook 1999: 458.)

Vuosien aikana on syntynyt monia versioita tar ja cpio-ohjelmista, jotka ovat hieman yhteensopimattomia. On luotu uusi hyötyohjelma arkistointiin nimeltään Pax. Pax pyrkii lukemaan ja kirjoittamaan monia cpio ja tar tiedostomuotoja sekä sen omia uusia tiedostomuotojaan. Sen käskyt muistuttavat enemmän cpio:ta kuin tar:ia. (FreeBSD Handbook 1999: 458.)

Amanda (Advanced Maryland Network Disk Archiver) on ennemmin asiakas/palvelin-ympäristön varmuuskopiointijärjestelmä kuin yksittäinen ohjelma. Amanda palvelin varmuuskopioi yksittäiselle nauha-asemalle kaikki tietokoneet, joissa on Amanda asiakasohjelma ja verkkoyhteys Amanda palvelimeen. Yleinen ongelma kohteissa, joissa on paljon laajoja levyjä, on ajan pituus, joka vaaditaan varmuuskopioimaan data suoraan nauhalle, joka ylittää tehtävälle varatun ajan. Amanda selvittää tämän ongelman. Amanda voi käyttää ”levyn viivästystä” varmuuskopioidakseen monia tiedostojärjestelmiä samaan aikaan. Amanda luo ”arkistosettejä”: ryhmä nauhoja, joita käytetään aikajakson yli luodakseen täydellisiä varmuuskopioita kaikista tiedostojärjestelmistä, jotka ovat Amandan konfiguraatiotiedostossa. ”Arkistosetti” sisältä myös yölliset lisävarmuuskopioinnit kaikista tiedostojärjestelmistä. Vahingoittuneet tiedostojärjestelmän palauttaminen vaatii viimeisimmän täydellisen varmuuskopioinnin ja lisävarmuuskopiot. (FreeBSD Handbook 1999: 458.)

Konfiguraatiotiedosto sisältää varmuuskopioiden ja verkkoliikenteen seurannan, jota Amanda synnyttää. Amanda käyttää mitä tahansa yllä mainituista ohjelmista kirjoittaakseen datan nauhalle. (FreeBSD Handbook 1999: 458.)

FreeBSD Handbook:ssa suositellaan käyttämään Dump-ohjelmaa säilyttämään kaiken datan ja kaikki UNIX:n tiedostojärjestelmän erikoisuudet. (FreeBSD Handbook 1999: 459.)

5. Toimipisteiden välinen tiedonsiirto

5.1. Virtual Private Network

Virtual Private Network eli virtuaalinen yksityisverkko on virtuaalisien piirien verkko, joka kuljettaa yksityistä liikennettä. Virtuaalinen piiri on yhteys, joka on rakennettu lähettäjän ja vastaanottajan välille, jossa sekä istunnon reitti ja kaista on varattu dynaamisesti. VPN voidaan luoda kahden tai useamman lähiverkon välille tai etäkäyttäjien ja lähiverkon välille. (Kosiur 1998: 19.)

Internet-pohjainen VPN käyttää avointa, Internetin ”rakentamaa” infrastruktuuria datan siirtämiseen yrityksen toimipaikkojen välillä. Yritykset, jotka käyttävät Internet VPN:ää ottavat yhteyksiä palveluntarjoajan paikallisiin yhteyspisteisiin, nimeltään Points-of-Presence (POPs), ja antavat palveluntarjoajan varmistaa, että data on siirretty tarkoitettuihin paikkoihin Internetin kautta jättäen loput yhteyden yksityiskohdat palveluntarjoajan verkolle ja Internet infrastruktuurille. (Kosiur 1998: 23.)

Linkki, joka on luotu tukemaan annettua yhteyssessiota paikkojen välille, on dynaamisesti muodostettu verkon kuormaa vähentämällä; kiinteät linkit eivät ole osa Internet VPN:n rakennetta. Toisin sanoen, kaistaa, jota tarvitaan sessiossa, ei varata ennen kuin sitä tarvitaan ja se vapautetaan muuhun käyttöön kun sessio on lopetettu. (Kosiur 1998: 23 - 24.)

Koska Internet on julkinen verkko, jossa suurin osa datasta on siirretty avoimesti, Internet VPN sisältää ehdon datan salaamiselle lähetettäessä VPN pisteiden välillä. Tämä suojaa dataa luvattomien osapuolten salakuuntelulta ja peukaloinnilta. Myös lisähyötynä, Internet VPN tukee turvallista yhteyttä liikkuville työntekijöille monilla soittosarjayhteyksillä, joita palveluntarjoaja tyypillisesti tarjoaa asiakkailleen heidän POP:aansa. (Kosiur 1998: 24.)

5.1.1. Internet VPN:n hyödyt

Internet VPN:n hyötyjä ovat suorat ja epäsuorat rahan säästöt, joustavuus ja skaalautuvuus.

Suurin rahan säästö tapahtuu verrattaessa Internet VPN:ää perinteiseen VPN:ään. Perinteinen VPN rakennetaan käyttäen

tariffiperustaisia, vuokrattuja T1- ja T3-linkkejä, joiden rakenne sisältää asennusmaksun, kuukausimaksun ja kilometrimaksun. (Kosiur 1998: 25.)

Internet VPN:ää voi käyttää kiinteällä laajakaistaliittymällä, joka sisältää vain kuukausimaksun. Mobiilikäyttäjät voivat ottaa yhteyden matkapuhelimella Internetiin ja käyttää tätä kautta Internet VPN:ää, jolloin kustannukset kerääntyvät GPRS-yhteyden kuukausi- ja tiedonsiirtomaksuista.

Joustavuus tulee esiin, kun yrityksen ei tarvitse tukea samaa mediaa ja nopeutta jokaisessa paikassa, koska pisteestä pisteeseen (Point-to-Point)-linkit eivät ole osa Internet VPN:ää. Tämä vähentää laite- ja tukikustannuksia. (Kosiur 1998: 31.)

Skaalautuvuus voidaan Internet VPN:ssä jakaa kahteen luokkaan, maantieteelliseen ja kaistaleveyden skaalautuvuuteen. Maantieteellisellä skaalautuvuudella tarkoitetaan Internet VPN:ssä sitä, että toimistot, ryhmät, etätyöläiset ja mobiilityöntekijät voivat olla osana VPN:ää missä tahansa, missä palveluntarjoaja tarjoaa POP:n. Tämä skaalautuvuus voi olla myös dynaamista; kenttätoimisto asiakkaan tiloissa voidaan yhdistää helposti paikalliseen POP:iin muutamassa minuutissa ja yhtä helposti poistaa VPN:stä, kun sitä ei enää tarvita. (Kosiur 1998: 32.)

Kaistaleveyden skaalautuvuus osoittaa sen, että kaistaleveyden voi valita tarpeen mukaan. Kotitoimistossa saatetaan tarvita T1- tai jopa T3-yhteyttä, mutta sivutoimisto pärjäisi soittosarjamodeemi- tai ISDN-linjalla (Integrated Services Digital Network). Jos sivutoimiston tarve suuremmalle kaistaleveydelle kasvaa, sitä voidaan nostaa puhelinlinjasta 56-kilobittiseen tai ISDN -yhteyteen tai ISDN:stä T1:seen. Verkko voi kasvaa tarpeiden mukaan, koska linkit eivät ole kiinteitä paikkojen välillä. Laitepäivityksiä ei tarvitse tehdä joka paikkaan tukemaan yhden paikan muutoksia. (Kosiur 1998: 32.)

5.1.2. Tunnelointi

Palveluntarjoajan ja Internetin infrastruktuurin piilottaminen VPN sovelluksesta on tehty mahdolliseksi konseptilla nimeltään tunnelointi. Tunnelointi luo erityisen yhteyden kahden loppupisteen välille. Tunnelin luomiseksi lähettäjä kapseloi pakettinsa IP-paketeiksi kulkeakseen läpi Internetin. VPN:ssä kapselointi saattaa sisältää alkuperäisen paketin salaamisen ja uuden IP-etuliitteen lisäämisen pakettiin. Vastaanottajan päässä oletusyhdyskäytävä poistaa IP-etuliitteen ja purkaa

salauksen paketista tarvittaessa, ja lähettää alkuperäisen paketin määränpäähänsä. (Kosiur 1998: 40.)

Tunnelointi antaa luvan datavirtojen ja käyttäjäinformaation välitykseen jaetun verkon yli virtuaalisen putken sisällä. Tämä putki tekee reititetystä verkosta totaalisesti näkymättömän käyttäjille. (Kosiur 1998: 40.)

Tunnelit on jaettu kahteen eri tyyppiin, pysyviin tai väliaikaisiin. Mutta staattiset tunnelit, kuten ensimmäistä usein kutsutaan, ovat vähän käytössä VPN:ssä, koske ne sitovat kaistaleveyttä, vaikka sitä ei käytettäisikään. Väliaikaiset, tai dynaamiset, tunnelit ovat paljon kiinnostavampia ja käytännöllisempiä VPN:lle, koska niitä voidaan luoda tarvittaessa ja lopettaa, kun niitä ei enää tarvita. Dynaamiset tunnelit eivät vaadi jatkuvaa varausta kaistaleveydestä. (Kosiur 1998: 40.)

Tunnelit voivat koostua kahden tyyppisistä loppupisteistä, joko yksittäisestä tietokoneesta tai lähiverkosta varustettuna turvallisella oletusyhdyskäytävällä, joka voisi olla reititin tai palomuuri. Vain kahta kombinaatiota näistä loppupisteistä on yleensä käytetty suunnitellessa VPN:ää. Lähiverkosta lähiverkkoon tunnelointi, turvallinen oletusyhdyskäytävä molemmissa päissä, toimii rajapisteenä tunnelin ja yksityisen lähiverkon välillä. Käyttäjät kummassakin lähiverkossa voivat käyttää tunnelia näkymättömästi kommunikoidessaan toisilleen. Asiakkaalta lähiverkkoon tunnelointityyppi on rakennettu mobiilikäyttäjälle, joka haluaa olla yhteydessä yrityksen lähiverkkoon. Asiakas käynnistää tunnelin luonnin omalta laitteeltaan vaihtaakseen liikennettä yrityksen verkossa. Tehdäkseen näin käyttäjä käynnistää tietyn asiakas-sovelluksen tietokoneellaan kommunikoidakseen oletusyhdyskäytävän kanssa, joka suojaa lähiverkkoa. (Kosiur 1998: 41.)

5.1.3. Yksityisyys

Peruskäytössä yksityinen VPN:ssä tarkoittaa, että tunneli kahden käyttäjän välillä VPN:ssä näkyy yksityisenä linkkinä, vaikka se kulkeekin jaetun median yli. Yrityskäytössä, etenkin lähiverkosta lähiverkkoon linkeissä, yksityinen tarkoittaa enemmän kuin edellä mainittu. Sen pitää tarkoittaa turvallisuutta, joka on vapautta urkkijoista ja peukaloinnilta. Nykypäivän Internet on iso pilvi yhdistettyjä verkkoja, joissa suurin osa liikenteestä siirretään avoimena tai salaamattomana tietona. Päävaatimus Internet-pohjaisen VPN:n luomiselle on turvallisuus. VPN:n täytyy täyttää neljä kriittistä funktiota

varmistaakseen turvallisuuden tiedolle. Nämä funktiot ovat seuraavat:

- Autentikointi – varmistaa, että data tulee siitä lähteestä, mistä väittää tulevansa.
- Pääsykontrolli – estää luvattomia käyttäjiä saamasta lupaa verkkoon.
- Luottamuksellisuus – estää ketään lukemasta tai kopioimasta tietoa, kun se kulkee Internetin läpi.
- Datan koskemattomuus – varmistaa, ettei kukaan peukaloi tietoa, kun se kulkee Internetin läpi. (Kosiur 1998: 41 – 42.)

5.1.4. Salaus

Vaikka tunnelit helpottavat datan lähetystä Internetin yli, käyttäjien autentikointi ja datan koskemattomuuden säilyttäminen riippuu salausmenetelmistä kuten digitaalinen allekirjoitus ja salaus. Nämä menetelmät käyttävät jaettuja salaisuuksia, joita kutsutaan avaimiksi. Niitä pitää käsitellä ja jakaa varovasti, joka lisää VPN:n hallintatehtäviä. (Kosiur 1998: 42.)

Kaksi suurta luokkaa protokollia tekee VPN:stä mahdollisen Internetissä. Ensiksi ovat protokollat, jotka määrittelevät, kuinka paketit salataan ja tunnelit luodaan kuten myös, kuinka paketit on turvattu. Toiseksi, koska turvallisuusprotokollat usein sisältävät salaisuuksien vaihdon lähettäjän ja vastaanottajan välillä VPN:ssä, protokollia tarvitaan hoitamaan näiden salaisuuksien hallinta ja muita autentikointitapoja. (Kosiur 1998: 44.)

Neljää protokollaa on alun perin ehdotettu VPN:n ratkaisumalliksi. Kolme niistä toimii OSI-mallin toisella kerroksella: Layer2 Forwarding (L2F), Point-to-Point Tunneling Protocol (PPTP) ja Layer2 Tunneling Protocol (L2TP). Ainoa kolmannen kerroksen VPN protokolla on IP Security (IPSec). (Kosiur 1998: 44 - 45.)

L2F

L2F on Cisco Systemsin kehittämä mekanismi, joka muodostaa UDP (User Datagram Protocol)-kapseloituja tunneleita etäkäyttölaitteiston ja sen reitittimien välille. L2F on kuitenkin

poistumassa oleva protokolla ja Perlmutterin ja Zarkowerin mukaan ”siirtynyt eläkkeelle” standardin määrittely asemasta, vaikka monien verkkolaitteiden valmistajien keskuudessa se on jonkinlainen de facto-standardi. Perlmutter ja Zarkower kuitenkin uskovat L2TP:n syrjäyttävän L2F:n, koska ne ovat hyvin samanlaisia, mutta eivät ole yhteensopivia, L2TP on standardi toimialalla ja Ciscokin on alkanut tuomaan markkinoille L2TP:tä (Perlmutter & Zarkower 2001: 125 - 126.)

PPTP

PPTP on protokolla, joka kuljettaa Remote Access Service-etäyhteyden (RAS) salattuna Internetin yli. Muut verkon käyttäjät eivät pysty seuraamaan tietoliikennettä, koska se on salattu. PPTP:llä yrityksien sisäiset lähiverkot voidaan yhdistää yhdeksi loogiseksi verkoksi. PPTP:llä voidaan yhdistää myös liikkuvat käyttäjät oman yrityksen verkkoon tietoturvan vaarantumatta. (Järvinen 2001: 538.)

L2TP

L2TP protokolla on PPTP:n ja L2F:n yhdistelmä (Perlmutter & Zarkower 2001: 125). L2TP:llä on tiettyjä rajoituksia, mutta se on myös laaja-alaisesti tuettu eli on olemassa useita sitä tukevia IETF-määritysluonnoksia (Internet Engineering Task Force), jotka suosittelevat L2TP:hen ehdotettuja parannuksia. Näihin parannuksiin kuuluvat esimerkiksi ehdotukset standardi-MIB:eistä (Management Information Blocks), palvelunlaatuun liittyvät ehdotukset (QoS) ja niin edelleen. (Perlmutter & Zarkower 2001: 134.)

IPSec

IPSec ei varsinaisesti ole protokolla, vaan protokollien kokoelma. Kokoelma on määritelty IETF:n RFC-asiakirjoissa (Request for Comments) ja määrittelyluonnoksissa (Draft Specification). IPSec tarjoaa IP-paketeille koskemattomuutta ja luottamuksellisuutta. IPSec koostuu kolmesta perustekijästä, jotka kaikki tekevät siitä hyödyllisen VPN-protokollana: todennus (pakettitasolla, eikä käyttäjätasolla), salaus ja avaimenhallinta. (Perlmutter & Zarkower 2001: 106.)

- Todennus – varmistetaan, että datan lähettäjät ovat niitä, joita he antavat ymmärtää olevansa ja että lähetetty data on yhtäläinen vastaanotetun datan kanssa.

- Salaus – dataa sekoitetaan siten, että se on käsittämätöntä niille, joilla ei ole oikeaa avainta hallussaan.

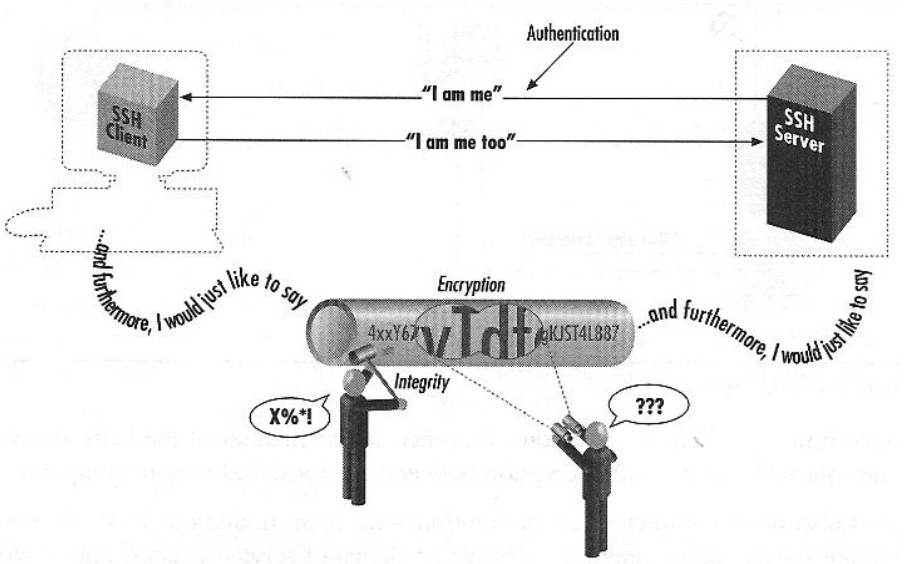
- Avaimenhallinta – toimenpide, jossa sovitaan tai neuvotellaan salattu avainarvo lähettäjän ja vastaanottajan välille.
(Perlmutter & Zarkower 2001: 106 - 107.)

5.2. Secure Shell

Secure Shell, tutummin SSH, on Tatu Ylösen kehittämä protokolla, jolla taataan salattu tiedonsiirtoyhteys epäluotettavan verkon, kuten Internet, yli. Yhteyden avaus välitetään RSA:lla salattuna, muu data voidaan salata monella vaihtoehtoisella symmetrisellä salaustekniikalla. (Järvinen 2001: 628.)

SSH on suosittu, tehokas, ohjelmistopohjainen lähestymistapa tietoverkkoturvallisuuteen. Kun dataa lähetetään tietokoneelta verkkoon, SSH automaattisesti salaa sen. Datan saavuttaessa tarkoitetun vastaanottajansa, SSH automaattisesti purkaa salauksen. Tämä on läpinäkyvä salaus: käyttäjät voivat toimia normaalisti tietämättään, että heidän kommunikaationsa on turvallisesti salattu verkossa. (Barrett & Silverman 2001: 2.)

SSH protokolla käsittää autentikoinnin, salauksen ja datan koskemattomuuden verkon yli, kuten kuvasta 6 voi nähdä. (Barrett & Silverman 2001: 4.)



Kuva 6. Autentikointi, salaus ja koskemattomuus. (Barrett & Silverman 2001: 4.)

- Autentikointi - Luotettavasti selvittää jonkun henkilöllisyyden. Yritettäessä kirjautua sisään etäkoneeseen, SSH pyytää digitaalista todistetta henkilöllisyydestä. Jos testi läpäistään, sisäänkirjautuminen onnistuu, muutoin SSH hylkää yhteyden.

- Salaus - SSH sekoittaa dataa, jolloin se on käsittämätöntä muille paitsi tarkoitetulle vastaanottajalle. Tämä suojaa dataa, kun se ylittää verkon.

- Koskemattomuus - Takaa, että data on koskematon saapuessaan perille matkattuaan verkon yli. Jos kolmas osapuoli saa kiinni ja muokkaa dataa matkalla, SSH havaitsee tämän.
  (Barrett & Silverman 2001: 4.)

Lyhyesti SSH luo verkkoyhteyksiä tietokoneiden välille vahvalla vakuudella, että yhteyden molemmat päät ovat alkuperäisiä. Se takaa myös, että data saapuu yhteyksien yli muokkaamattomana ja lukemattomana. (Barrett & Silverman 2001: 5.)

5.2.1. Yksityisyys (Salaus)

Yksityisyys tarkoittaa datan suojaamista paljastuksilta. Tyypilliset tietokoneverkot eivät takaa yksityisyyttä; kaikilla joilla on pääsy verkkolaitteisiin tai tietoverkkoon liitettyihin työasemiin voivat lukea kaikkea dataa, joka kulkee verkossa. Vaikka nykyaikaisesti kytketyt tietoverkot ovat vähentäneet tätä ongelmaa lähiverkoissa, se on silti vielä vakava asia; salasanoja varastetaan säännöllisesti tällaisten nuuskimishyökkäyksien kautta. (Barrett & Silverman 2001: 42.)

SSH antaa yksityisyyttä salaamalla dataa, joka kulkee tietoverkon yli. Tämä pisteestä pisteeseen salaus pohjautuu sattumanvaraisiin avaimiin, jotka ovat turvallisesti neuvoteltu kyseiselle istunnolle ja tuhotaan, kun istunto päättyy. SSH tukee laajaa valikoimaa salausalgoritmeja istuntodatalle sisältäen sellaiset salakirjoitukset kuin ARC-FOUR, Blowfish, DES, IDEA ja 3DES. (Barrett & Silverman 2001: 42.)

ARC-FOUR (RC4)

RC4 on Ron Rivestin kehittämä salausalgoritmi. Algoritmi oli pitkään RSA Data Security Inc:n tuotesalaisuus, kunnes lähdekoodi vuoti julkisuuteen Internetin kautta. RC4 on nopea

jonosalaaja, jossa avaimen pituus on valittavissa. Salausalgoritmi perustuu S-taulukkoon, jossa numeroarvot sekoitetaan ja käytetään sen jälkeen viestitavujen salaamiseen XOR-operaatiolla. (Järvinen 2001: 563.) Koska RC4 on RSA Data Security Inc:n tuotemerkki, joten nimi ”ARCFOUR” on liitetty julkisesti paljastuneeseen versioon algoritmista (Barrett & Silverman 2001: 96).

Blowfish

Blowfish on Bruce Schneierin kehittämä nopea symmetrinen salausalgoritmi, joka salaa tietoa 64 bitin lohkoissa. Avaimen pituuden voi valita 32 ja 448 bitin väliltä. Blowfish on nopea, luotettava ja sen lähdekoodi on vapaasti saatavilla. Tämän takia Blowfish on levinnyt laajaan käyttöön. (Järvinen 2001: 79.)

DES

Data Encryption Standard (DES) on 1970-luvun alussa IBM:n kehittämä salausalgoritmi. Se perustuu 56 bitin avaimeen, jolla tietoa koodataan 64 bitin lohkoissa. Samaa avainta käytetään sekä salaamiseen että purkamiseen, koska avain on symmetrinen. (Järvinen 2001: 151.)

IDEA

International Data Encryption Algorithm (IDEA) on Sveitsissä 1990-luvulla kehitetty symmetrinen salakirjoitusmenetelmä. Se perustuu 128-bittiseen avaimeen. Esimerkiksi PGP:ssä (Pretty Good Privacy) käytetään kyseistä menetelmää varsinaisen viestitekstin salaamiseen. (Järvinen 2001: 281.)

3DES

Triple-DES tai 3DES on muunnos DES:stä, jossa on pyritty parantamaan turvallisuutta pidentämällä avaimen pituutta. On todistettu, että DES funktio ei muodosta ryhmää avaimiensa päälle, joka tarkoittaa, että moninkertainen salaus yksittäisillä avaimilla voi nostaa turvallisuutta. 3DES salaa selkokielisen tekstin kolmella DES algoritmimuunnoksella käyttäen kolmea eri avainta. Tehokas avain pituus 3DES:ssä on 112 bittiä, valtava ero 56 bitin DES avaimeen. (Barrett & Silverman 2001: 96.)

5.2.2. Koskemattomuus

Koskemattomuus tarkoittaa varmuutta, että toisesta päästä verkkoa lähetetty data saapuu muuntelemattomana toiseen päähän. SSH:n taustalla olevalla kuljetustasolla, TCP/IP:llä (Transmission Control Protocol Internet Protocol), on koskemattomuustarkistus, joka havaitsee tietoverkosta johtuvat muutokset, kuten sähkömelu, pakettien katoaminen johtuen liiallisesta liikenteestä, ja niin edelleen. Siitä huolimatta nämä tavat ovat tehottomia tahallista peukalointia vastaan ja nokkela hyökkääjä voi huijata niitä. Vaikka SSH salaa datavirran niin, että hyökkääjä ei pysty helposti muuttamaan tiettyjä kohtia saadakseen tietyn lopputuloksen, TCP/IP:n koskemattomuustarkistus yksinään ei pysty estämään hyökkääjän tahallista roskan pumppaamista istuntoon. (Barrett & Silverman 2001: 42.)

SSH 2 protokolla käyttää salaustekniikkaa koskemattomuustarkistuksessa, joka vahvistaa, että lähetettyä dataa ei ole muunnettu ja, että se oikeasti tulee toisesta päästä yhteyttä. SSH 2 käyttää tähän tarkoitukseen avaimellista sekoitusalgoritmia, joka perustuu MD5:een ja SHA-1:een, jotka ovat hyvin tunnettuja ja laajasti luotettuja algoritmeja. Toisaalta SSH 1 käyttää verraten heikompaa menetelmää: 32 bittistä jaksottaista tarpeettomuustarkistusta (Cyclic Redundancy Check CRC-32) salaamattomaan dataan joka paketissa. (Barrett & Silverman 2001: 43.)

5.2.3. Autentikointi

Autentikointi tarkoittaa toisen henkilöllisyyden vahvistamista. Kaikki SSH yhteydet sisältävät kaksi autentikointia: asiakas vahvistaa SSH palvelimen henkilöllisyyden (server authentication) ja palvelin vahvistaa käyttäjän henkilöllisyyden (user authentication). Palvelimen autentikointi varmistaa, että SSH palvelin on aito, eikä huijari, suojaamassa hyökkääjiä vastaan, jotka pyrkivät uudelleenohjaamaan verkkoyhteyden toiseen tietokoneeseen. Palvelimen autentikointi suojaa myös ”man-in-the-middle”-hyökkäyksiä vastaan, jossa hyökkääjä on läpinäkymättömästi tietokoneesi ja palvelimen välillä teeskennellen asiakasta toiseen suuntaan ja palvelinta toiseen huijaten molempia puolia ja lukien kaiken liikenteen. (Barrett & Silverman 2001: 43.)

SSH tukee autentikointia salasanalla, salaten salasanan, kun sen matkustaa tietoverkon yli. Tämä on valtava kehitys muihin

vastaavanlaisiin etäohjelmaprotokolliin (Telnet, FTP) verrattuna, jotka yleensä lähettää salasanan selkokielisenä tietoverkon yli, jossa kuka tahansa riittävällä verkkoyhteydellä voi varastaa sen. Silti se on vain yksi salasana autentikaatio, joten SSH mahdollistaa toisen tehokkaamman ja paremmin hallittavamman mekanismin; käyttäjäkohtaisen julkisen avaimen allekirjoituksen ja kehitellyn rlogin-tyylisen autentikoinnin, jossa isännän henkilöllisyys vahvistetaan julkisella avaimella. Lisäksi monet SSH toteutukset tukevat muita järjestelmiä kuten Kerberos, RSA Securityn SecurID osoitus, S/Key kertakäyttöinen salasana ja Pluggable Authentication Modules (PAM) järjestelmä. SSH asiakas ja palvelin päättävät, mitä autentikointimekanismia käyttävät pohjautuen heidän asetuksiinsa. SSH 2 voi myös vaatia moninkertaisia autentikointimuotoja. (Barrett & Silverman 2001: 44.)

5.2.4. Valtuutus

Valtuutus tarkoittaa päätöstä mikä kukakin voi tehdä ja mitä ei. Se selviää autentikoinnin jälkeen, koska oikeuksia ei voi myöntää ennen kuin tietää kenelle niitä myöntää. SSH palvelimilla on monia tapoja rajoittaa asiakkaan toimintaa. Pääsyä interaktiivisiin sisäänpääsyistuntoihin, TCP-portin ja X Window:n edelleenvälittämiseen, avainagentin edelleenvälittämiseen, jne. voidaan kontrolloida, vaikka näitä kaikkia ominaisuuksia ei ole kaikissa SSH toteutuksissa, ja ne eivät ole aina niin yleisiä tai joustavia kuin käyttäjä haluaisi. Valtuutusta voidaan kontrolloida palvelinlaajuisella tasolla tai asiakaskohtaisesti riippuen käytetystä autentikointimenetelmästä. (Barrett & Silverman 2001: 44 – 45.)

5.2.5. Edelleenvälitys (Tunnelointi)

Edelleenvälitys tai tunnelointi tarkoittaa toisen TCP-pohjaisen palvelun, kuten Telnet tai IMAP (Internet Message Access Protocol), kapselointia SSH istunnon sisällä. Tämä tuo SSH:n turvallisuusedut muihin TCP-pohjaisiin palveluihin. Esimerkiksi tavallinen Telnet yhteys lähettää käyttäjänimen, salasanan ja muut istunnon tiedot selkokielellä. Edelleenvälittämällä Telnetin SSH:n läpi, kaikki data salataan ja koskemattomuus tarkistetaan automaattisesti ja autentikoimiseen voidaan käyttää SSH suosituksia. (Barrett & Silverman 2001: 45.)

SSH tukee kolmea edelleenvälittämisen tyyppiä. Yleinen TCP portin edelleenvälitys toimii edellä mainitusti kaikilla TCP-palveluilla. X edelleenvälitys sisältää lisäominaisuuksia X

protokollan (esimerkiksi X Window:n) turvaamiseksi. Kolmas tyyppi, agentin edelleenvälittäminen, sallii SSH asiakkaan pääsyn SSH:n julkisiin avaimiin etätietokoneissa. (Barrett & Silverman 2001: 45.)

5.2.6. OpenSSH

OpenSSH on joukko verkkoyhteystyökaluja, joilla otetaan yhteys etätietokoneeseen turvallisesti. Sitä voidaan käyttää suoraan vastaavien ohjelmien tilalla kuten rlogin, rsh, rcp ja telnet. Lisäksi mikä tahansa TCP/IP yhteys voidaan tunneloida tai edelleenvälittää turvallisesti SSH:n kautta. OpenSSH salaa kaiken liikenteen tehokkaasti eliminoiden salakuuntelun, yhteyden kaappaamisen ja muut verkkotason hyökkäykset. (FreeBSD Handbook 1999: 394.)

OpenSSH:ta ylläpitää OpenBSD projekti ja se perustuu SSH v1.2.12:sta sisältäen viimeisimmät ongelmakorjaukset ja päivitykset. Se on yhteensopiva molempien SSH 1 ja SSH 2 protokollien kanssa. OpenSSH on sisältynyt FreeBSD:hen versiosta 4.0. lähtien. (FreeBSD Handbook 1999: 394.)

OpenSSH:n Internet-sivujen mukaan OpenSSH on tarkoitettu vain Unix- ja Linux-pohjaisille käyttöjärjestelmille, joten seuraavassa kappaleessa käsittelen vastaavanlaista ohjelmaa, joka on tarkoitettu Windows-käyttöjärjestelmille. (OpenSSH 2005)

5.2.7. PuTTY

PuTTY on vapaa avoimen lähdekoodin ohjelmisto, jota käytetään Windows-käyttöjärjestelmissä Unix-koneiden merkkipohjaiseen etäkäyttöön. PuTTY tarvitsee toimiakseen ainoastaan exe-tiedoston, jota ei tarvitse erikseen asentaa vaan se on helposti haettavissa PuTTY:n virallisilta Internet-sivuilta osoitteesta www.chiark.greenend.org.uk/~sgtatham/putty/. (Wikipedia 2005)

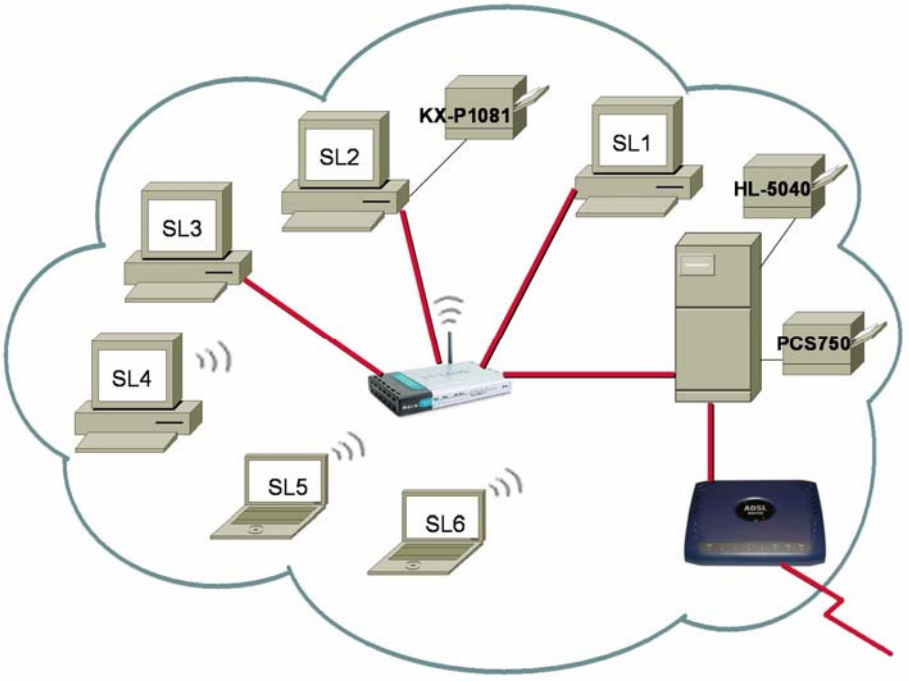
6. Ratkaisuehdotukset

6.1. Tampereen toimipisteen kehityssuunnitelma

Lähiverkko tulisi toteuttaa asiakas/palvelin-mallia hyödyntäen. Tähän malliin perustuen tietoverkossa olisi yksi palvelin, joka toimisi tiedosto- ja tulostinpalvelimena. Palvelimella hallittaisiin myös käyttäjätunnuksia ja niiden oikeuksia käyttää verkkoresursseja.

Taipalsaaren toimipisteellä olevat A-Linkin ADSL-modeemi ja D-Linkin langaton tukiasema vaihdettaisiin päittäin Tampereen toimipisteen D-Link langattoman ADSL-reitittimen kanssa. Näin voidaan hyödyntää olemassa olevia laitteita eikä tarvitse sijoittaa uusiin laitteisiin.

Tampereen toimipisteessä tietokoneet liitettäisiin lähiverkoksi D-Linkin langattoman reitittimen kautta. Myös palvelin olisi liitettynä tähän reitittimeen, jolloin työasemilta saataisiin yhteys palvelimeen. Kaikki Internetiin suuntaavat yhteydet työasemilta kulkisivat palvelimen kautta A-Linkin ADSL-modeemille ja sen kautta Internetiin. Tällöin palvelin toimisi palomuurina niin sisään kuin uloskin menevissä yhteyksissä.



Kuva 7. Tampereen toimipiste tulevaisuudessa.

6.2. Palvelin

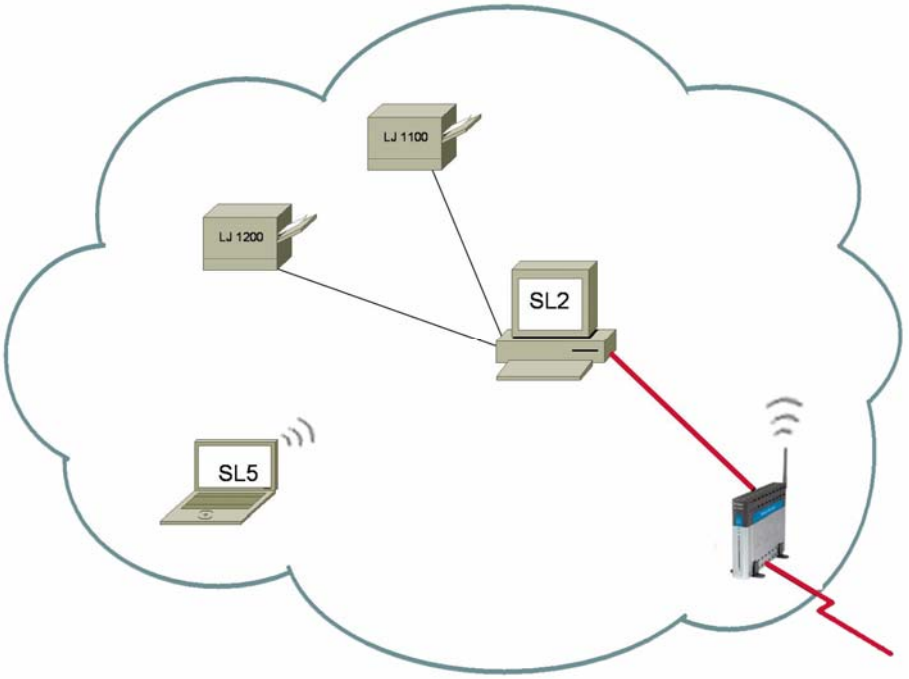
Palvelimella olisi monta tehtävää, kuten tiedostojen jako, tulostinpalvelut, palomuuraus ja reititys. Tiedostojen jako toimisi niin, että palvelin näkyisi yhtenä levyasemana, esimerkiksi Z-asemana, lähiverkon tietokoneissa. Tämä on mahdollista toteuttaa molemmilla, FreeBSD ja Windows Server 2003, käyttöjärjestelmillä. Haluttu asema tai kansio jaetaan verkkokäyttäjien käyttöön ja lisätään verkkosijainti työasemiin.

Palvelin toimisi myös tulostinpalvelimena lähiverkossa. Palvelimeen olisi liitettyinä kaksi kirjoitinta, Brother-merkkinen HL-5040-laserkirjoitin ja HP:n PSC750-monitoimikirjoitin. Ajatus siitä, että HP PSC 750:llä voisi myös siirtää tietoa sähköiseen muotoon jokaiselta työasemalta, näytti mahdottomalta. HP:n asiakastuen mukaan tämä on kuitenkin mahdollista erillisen lisälaitteen, HP JetDirect Print Server:n, avulla.

Palvelin suorittaisi myös varmuuskopioinnin joko tallentavalle CD- tai DVD-asemalle. DVD-levylle mahtuu paljon enemmän tietoa kuin CD-levylle, joten se olisi käytössä helpompi suurien varmuuskopiointimäärien kopioimiseen. Varmuuskopiointi suoritettaisiin päivittäin tärkeimmille ja usein muuttuville tiedostoille. Tiedostojärjestelmän ja muut tiedot varmuuskopioitaisiin viikoittain.

6.3. Taipalsaaren toimipisteen kehityssuunnitelma

Taipalsaaren toimipisteen lähiverkko toteutettaisiin Tampereen toimipisteestä vaihdetulla D-Linkin langattoman ADSL-reitittimen avulla. Tietokoneet liitetään kyseiseen reitittimeen langattomasti ja olemassa olevilla Cat5-kaapeleilla. Muutoin Taipalsaaren lähiverkko pysyy samanlaisena kuin tälläkin hetkellä.



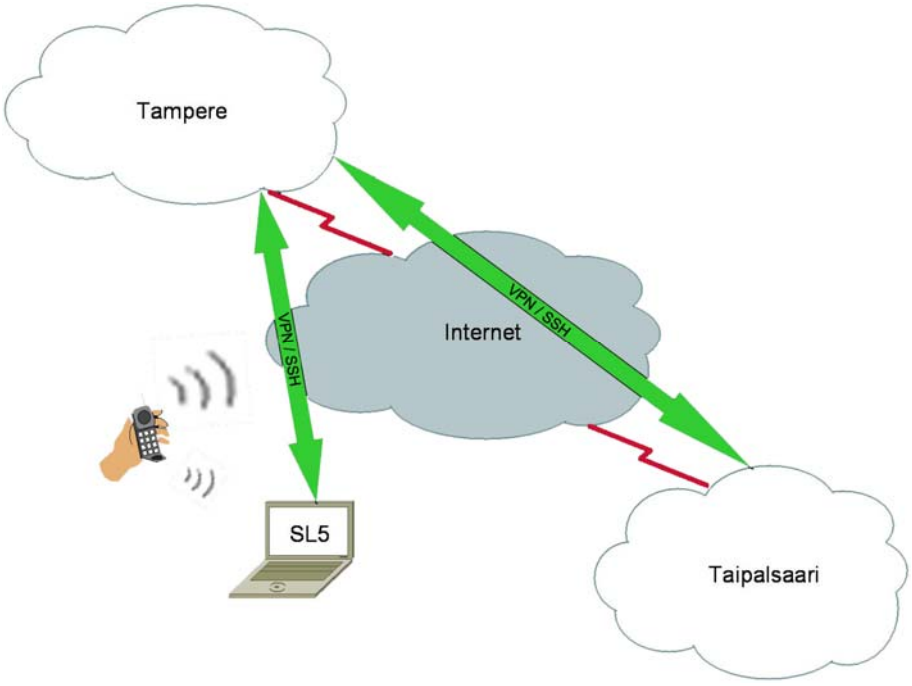
Kuva 8. Taipalsaaren toimipiste tulevaisuudessa.

6.4. Toimipisteiden yhdistämissuunnitelma

Tiedonsiirto Tampereen ja Taipalsaaren toimipisteiden välillä voidaan luoda tietoturvallisesti hyödyntäen joko VPN-tekniikkaa tai SSH-protokollaa. Tiedonsiirto Tampereen toimipisteen ja mobiilikäyttäjienkin välille voidaan toteuttaa samalla tavalla.

VPN-tekniikkaa hyödynnettäessä mobiilikäyttäjä tai Taipalsaaren lähiverkon käyttäjä ottaa yhteyden Tampereen toimipisteessä sijaitsevaan palvelimeen. Tämä tapahtuu helposti palvelimeen avatun VPN-palvelun avulla, jolloin erillisiä VPN-reitittimiä tai muita lisälaitteita ei tarvitse käyttää. Käyttäjätunnusten perusteella palvelin joko hyväksyy tai kieltää yhteyden luonnin onnistumisen. Koska kaikki tieto ja tiedostot säilytetään kyseisellä palvelimella, yhteyttä ulkomaailmasta lähiverkkoon ei sallita. Yhteyden luominen palvelimeen tapahtuu automaattisesti käyttäjän kirjautuessa tietokoneelleen.

SSH:ta käytettäessä yhteys Tampereen toimipisteeseen ei tapahdu automaattisesti käyttäjän kirjautuessa sisään tietokoneeseensa. Tässä tapauksessa käyttäjä tarvitsee PuTTY-nimisen SSH-asiakasohjelmiston, jotta yhteys Tampereen toimipisteellä sijaitsevaan SSH-palvelimeen onnistuisi. Käyttäjän autentikointi tapahtuu käyttäjän ottaessa yhteyttä palvelimeen.



Kuva 9. Salattu yhteys toimipisteiden ja mobiilikäyttäjien välillä.

7. Loppuarviointi

Tässä tutkintotyössäni olen pyrkinyt laatimaan Salesline Oy:n tietoverkon kehityssuunnitelman ja esittämään erilaiset ratkaisuvaihtoehdot toteutuksen pohjaksi. Valitsin kaksi erilaista verkkokäyttöjärjestelmää vertailtavaksi, Windows Server 2003 yleisyyden, tunnettuuden ja helppokäyttöisyyden, FreeBSD:n taloudellisuuden vuoksi. FreeBSD ei ollut minulle lainkaan tuttu järjestelmä, joten sitä oli mielenkiintoista tutkia. Ratkaisuvalintaa miettiessä ja tehtäessä kannattaa kuitenkin pohtia, onko tärkeää, että järjestelmä on helppokäyttöinen vai taloudellinen. Taloudellinen vaihtoehto voi helposti tulla kalliiksi, jos sen käyttöön kuluu paljon aikaa ja asiantuntevaa palvelua joutuu pyytämään alan asiantuntijoilta. Windows Server 2003 vaikuttaa tavalliselta Windows-käyttöjärjestelmältä, jolla on vain monia lisäominaisuuksia. Käyttäjän on helppo omaksua kyseisen verkkokäyttöjärjestelmän käyttö, jos on käyttänyt Windowsia aikaisemmin ja tämä saattaa vähentää käytettyä aikaa ja alan asiantuntijoiden avun tarvetta.

Ensin alkuun suosittelisin käyttämään CD- tai DVD-varmistusta, jos varmuuskopioitavia tiedostoja ei ole laajoja määriä. Myös päivittäin muuttuvat tiedot on helppo kopioida omalle CD- tai DVD-levylleen. Nauhavarmistuslaitetta kannattaa harkita, jos varmuuskopioitavia tiedostoja on hyvin paljon, mutta myös otettava huomioon, että nauhakasetit ovat melko kalliita ja itse varmuuskopiointi saattaa kestää jopa tunteja. Varmuuskopiointi tulisi suorittaa tai ajastaa suoriutumaan automaattisesti joka päivä töiden päätteeksi, jolloin työntekijät eivät enää muuttaisi tiedostoja. Aika ajoin tulisi myös poistaa turhia tiedostoja tietovarastoista, jotta ei varmistettaisi tarpeetonta dataa.

VPN- ja SSH-yhteyksien tietoturvallisuus on erittäin hyvä ja täten täyttää omalta osaltaan vaatimukset. Näidenkin vertailukohteiden välillä nousee esiin helppokäyttöisyys ja käyttäjäystävällisyys. VPN-yhteyksien muodostaminen ja ylläpitäminen vaikuttavat olevan helpommin toteutettavissa kuin SSH:ssa. VPN-yhteyden luonnin jälkeen käyttäjän ei tarvitse huolehtia tietoturvallisuudesta. SSH-yhteyksissä käytetään erillisiä ohjelmia, joiden kautta käyttäjä käyttää tietoturvallista yhteyttä. SSH:n käyttö täten vaikuttaa hyvin epäkäytännölliseltä käyttäjän näkökulmasta katsottuna.

Projektin mahdollisena toteuttajana itse valitsisin Windows Server 2003-käyttöjärjestelmän verkkokäyttöjärjestelmäksi juuri helppokäyttöisyyden vuoksi. Myös kyseiseen käyttöjärjestelmään sisältyy tehokas VPN-ratkaisu, jota voi

hyödyntää tiedonsiirtoyhteyttä rakennettaessa. VPN:ään päätyisin juuri Windows-integraation ja myös helppokäyttöisyyden vuoksi. SSH:n toteuttaminen vaatisi erillisien ohjelmien käyttöä ja niiden automatisointi käyttäjän kirjautuessa tietokoneelleen saattaa aiheuttaa erilaisia ongelmia.

Tutkintotyön tekeminen oli erittäin haastavaa ja monella tavalla hyvin kasvattavaa. Itsekurin ja motivaation ylläpitäminen oli ajoittain hyvin vaikeaa, mutta päättäväisyydellä sain aina vietyä tutkintotyötä eteenpäin. Alkuun tuntui, että aihe saattaisi olla liian laaja, mutta olen mielestäni pystynyt hyvin käsittelemään aiheeseen liittyvät keskeiset asiat. Kirjallisuuden etsiminen tuotti ongelmia, koska aiheesta tuntui löytyvän suhteellisen vähän tietoa. Varsinkin vertailukohteena olleesta FreeBSD-verkkokäyttöjärjestelmästä tuntui löytyvän hyvin vähän tietoa. Kaikki kyseisestä järjestelmästä löytynyt tieto on Internet-lähteistä ja suurin osa viralliselta FreeBSD.org-sivustolta.

Lähteet

Barrett, Daniel J. & Silverman, Richard E. 2001. SSH, the Secure Shell: The Definitive Guide. California: O'Reilly & Associates, Inc.

FreeBSD 2005. Kotisivut. [online][viitattu 12.1.2006]. http://www.freebsd.org/releases/6.0R/hardware.html

FreeBSD 2005. Kotisivut. [online][viitattu 4.1.2006]. http://www.freebsd.org/about.html

FreeBSD Handbook 1999. Kotisivut. [online] [viitattu 12.1.2006]. ftp://ftp.freebsd.org/pub/FreeBSD/doc/en_US.ISO8859-1/books/handbook/book.pdf.zip

Järvinen, Petteri 2001. IT-tietosanakirja. Jyväskylä: Docendo Finland Oy.

Keogh, Jim 2001. Verkkotekniikat: tehokas hallinta. Helsinki: Edita Oyj.

Kosiur, Dave 1998. Building and Managing Virtual Private Networks. New York: John Wiley & Sons, Inc..

Microsoft 2005. Kotisivut. [online] [viitattu 11.1.2006]. http://www.microsoft.com/finland/products/windowsserve2003/evaluation/overview/default.asp

Microsoft 2005. Kotisivut. [online] [viitattu 11.1.2006]. http://www.microsoft.com/finland/products/windowsserve2003/evaluation/choosing/default.asp

OpenSSH 2005. Kotisivut. [online] [viitattu 5.4.2006]. http://www.openssh.com/users.html

Perlmutter, Bruce & Zarkower, Jonathan 2001. VPN – Virtuaaliset yksityisverkot. Helsinki: Edita Oyj.

Prosessori-Uutiset 2005. Kotisivut. [online] [viitattu 11.1.2006]. http://www.prosessori.fi/uutiset/tulosta.asp?id=47878

Samba: An Introduction 2001. Kotisivut. [online][viitattu 12.1.2006]. http://us3.samba.org/samba/docs/SambaIntro.html

Stanek, William R. 2003. Microsoft Windows Server 2003 – Asiantuntijan käsikirja. Helsinki: Edita Prima Oy.

Wikipedia 2005. Kotisivut. [online] [viitattu 11.1.2006]. http://fi.wikipedia.org/wiki/FreeBSD

Wikipedia 2005. Kotisivut. [online] [viitattu 5.4.2006].
http://fi.wikipedia.org/wiki/PuTTY

Wikipedia 2006. Kotisivut. [online][viitattu 11.4.2006].
http://en.wikipedia.org/wiki/Advanced_Intelligent_Tape

Wikipedia 2006. Kotisivut. [online][viitattu 11.4.2006].
http://en.wikipedia.org/wiki/Linear_Tape_Open

Wikipedia 2006. Kotisivut. [online][viitattu 11.4.2006].
http://en.wikipedia.org/wiki/Magneto-optical_drive

Wikipedia 2006. Kotisivut. [online][viitattu 18.4.2006].
http://fi.wikipedia.org/wiki/SHA-1

Wikipedia 2006. Kotisivut. [online][viitattu 18.4.2006].
http://fi.wikipedia.org/wiki/Unix

Wikipedia 2006. Kotisivut. [online][viitattu 18.4.2006].
http://fi.wikipedia.org/wiki/XOR

Witherspoon, Graig & Coletta 1996. Tehokas client/server-verkko. Jyväskylä:
Gummerus.

Liitteet

Liite 1. Tampereen toimiston laitteisto

Pöytätietokoneet:

SL1:

- MSI K7N2-emolevy
- 1,8 GHz AMD Athlon 2200+-prosessori
- 512 Mt RAM-muisti
- 150 Gt kiintolevy
- 3Com EtherLink XL 10/100 PCI-verkkokortti
- Microsoft Windows XP Professional-käyttöjärjestelmä

SL 2:

- ASRock-emolevy
- 2,4 GHz Intel Celeron-prosessori
- 512 Mt RAM-muisti
- 80 Gt kiintolevy
- Realtek RTL8139/810x Family Fast Ethernet NIC-verkkokortti
- Microsoft Windows XP Professional-käyttöjärjestelmä

SL 3:

- 2 MHz GenuineIntel Pentium-prosessori
- 32 Mt RAM-muisti
- 2 x 1 Gt kiintolevy
- Intel EtherExpress PRO/10+ -verkkokortti
- Microsoft 98 Second Edition-käyttöjärjestelmä

SL 4:

- MSI K7N2 Delta-emolevy
- 1,24 GHz AMD Athlon-prosessori
- 1 Gt RAM-muisti
- 40 Gt ja 60 Gt kiintolevyt
- D-Link AirPlus DWL-120+ Wireless USB Adapter-langaton verkkokortti
- NVIDIA nForce MCP Networking Controller-verkkokortti
- Microsoft Windows XP Professional-käyttöjärjestelmä

Kannettavat tietokoneet:

SL 5:

- 1,6 GHz Intel Pentium M-prosessori
- 512 Mt RAM-muisti
- 60 Gt kiintolevy
- Intel PRO/Wireless 2200BG Network Connection-langaton verkkokortti
- Broadcom NetXtreme Gigabit Ethernet-verkkokortti
- Microsoft Windows XP Professional-käyttöjärjestelmä

SL 6:

- 1,06 GHz Intel Celeron CPU 1066MHz-prosessori
- 248 Mt RAM-muisti
- 20 Gt kiintolevy
- D-Link AirPlus XtremeG+ DWL-G650+ Wireless Cardbus Adapter-langaton verkkokortti
- Intel PRO/100 VE Network Connection-verkkokortti
- Microsoft Windows XP Professional-käyttöjärjestelmä

Verkkolaitteet:

- D-Link DSL-G604T Wireless ADSL Router-reititin

Kaapelit:

- 4 kpl suora Cat5 Gigabit Ethernet-kaapeli
- puhelinkaapeli

Liite 2. Taipalsaaren toimiston laitteisto

Pöytätietokoneet:

SL 2:

- ks. Liite 1. SL 2

Kannettavat tietokoneet:

SL 5:

- ks. Liite 1. SL 5

Verkkolaitteet:

- D-Link WLAN DI-614+-langaton tukiasema
- A-Link RoadRunner 44B-modeemi
-

Kaapelit:

- 2 kpl suora Cat5 Gigabit Ethernet-kaapeli
- puhelinkaapeli

Sanasto

ADSL (Asymmetric Digital Subscriber Line)
Vanhaa puhelinkaapelia käyttävä tiedonsiirtotekniikka, joka pohjautuu tyypillisen tietoverkonkäytön epäsymmetrisyyteen: suurin osa verkkoyhteyden aikana siirretystä tiedosta kulkee palvelimesta käyttäjälle ja paluukanavassa kulkevat vain Internet-osoitteet tai käyttäjän antamat komennot. (Järvinen 2001: 24.)

AGP (Accelerated Graphics Port)
Erityisesti 3D-näytönohjaimien käyttöön tarkoitettu nopea grafiikkaväylä. (Järvinen 2001: 18.)

AIT (Advanced Intelligent Tape)
Sonyn kehittämä nopea, suurikapasiteettinen magneettinen nauhaformaatti. (Wikipedia 2006)

AT-väylä
16-bittinen väylästandardi, jota Yhdysvalloissa usein kutsutaan nimellä ISA (Industry Standard Architecture eli teollisuusstandardi. Tämä tarkoittaa, että se on kaikkien valmistajien hyväksymä yleinen standardi, jonka jatkokehitystä ei kukaan voi ohjailla. (Järvinen 2001: 53 - 54.)

Bluetooth
Ericssonin hankkeesta alkunsa saanut lyhyen kantaman langaton verkko. Alun perin suunniteltu matkapuhelimen ja korvakuulokkeen väliseen tiedonsiirtoon. (Järvinen 2001: 80.)

CIFS (Common Internet File System)
Verkkotekniikka, joka mahdollistaa toisessa koneessa olevien tiedostojen lukemisen ja kirjoittamisen Internetin yli. (Järvinen 2001: 121.)

CRC-32 (Cyclic Redundancy Check)
Varmistusmenetelmä, jolla varmistetaan tiedonsiirron oikeellisuus. (Järvinen 2001: 130.)

DAT (Digital Audio Tape)
Digitaalinen nauhuri, jota käytetään varmuuskopioinnissa. (Järvinen 2001: 141.)

DLT (Digital Linear Tape)
Nauhavarmistustekniikka, DAT:n lailla perustuu digitaalitekniikkaan. (Järvinen 2001: 163.)

DMB (Domain Master Browser)
Toimialueen isäntäselain, joka järjestää selauslistoja NT toimialueilla, jopa reititetyistä verkoista. (Samba: An Introduction 2001)

DNS (Domain Name Service)
Nimipalvelu, joka muuntaa koneen nimen IP-osoitteeksi. (Järvinen 2001: 166.)

EISA (Extended Industry Standard Architecture)
32-bittinen AT-väylälaajennus, joka mahdollistaa nopeiden lisäkorttien kehittämisen ja saman laajennusväylän jakamisen usealle prosessorille. Poistunut läheskokonaan paikallisväylien yleistymisen vuoksi. (Järvinen 2001:190.)

FTP (File Transfer Protocol)
Internetissä toimiva tiedostojen siirto-ohjelma. FTP käyttää tiedonsiirtoon porttia 21. (Järvinen 2001: 229.)

GPRS (General Packet Radio Service)
GPRS-tekniikka mahdollistaa pakettimuotoisen datasiirron GSM-verkoissa. (Järvinen 2001: 242.)

IETF (Internet Engineering Task Force)
Internetin käytännön kehittämisestä huolehtiva elin, joka toimii työryhmissä. (Järvinen 2001: 282.)

IP-osoite
Tietokoneen, joka on TCP/IP-verkossa, 32-bittinen osoite. (Järvinen 2001: 299.)

ISA (Industry Standard Architecture)
Ks. AT-väylä

ISDN (Integrated Services Digital Network)
Digitaalinen puhelinverkko, joka kehitettiin analogisen verkon korvaajaksi. (Järvinen 2001: 302.)

Kerberos
Todennuspalvelu, joka takaa luotettavan käyttäjien ja palvelinten tunnistuksen ja sisältää myös viestiliikenteen salauksen. (Järvinen 2001: 330.)

LMB (Local Master Browser)
Paikallinen isäntäselain, jonka verkossa olevat tietokoneet valitsevat. Sen tehtävä on pitää listaa saatavilla olevista palveluista. (Samba: An Introduction 2001)

LTO (Linear Tape Open)
Vaihtoehtoinen magneettinauhaformaatti patentoidulle Digital Linear Tape:lle (DLT). (Wikipedia 2006)

MD5 (Message Digest 5)
Algometri, joka laskee tekstistä 128-bittisen tunnusluvun. Tekstiä muutettaessa luku muuttuu. (Järvinen 2001: 402.)

MIB (Management Information Blocks)
Hallintainformaation tietokanta, joka sisältää puumaisen tietokannan laitteen staattisista ja dynaamisista toiminnoista. (Perlmutter & Zarkower 2001: 229.)

MO-levy (Magneto Optical)
Magneetto-optinen levy, jota käytetään magneetto-optisissa asemissa. (Wikipedia 2006)

NBNS (NetBIOS Name Service)
Ks. Windows Internet Naming Service (WINS)

NetBIOS
Lähiverkkopalveluiden joukko, joka on tarkoitettu sovelluksille. Näihin palveluihin kuuluu esimerkiksi yhteyden luonti tietokoneiden välille ja tiedon siirto tietokoneiden välillä. (Järvinen 2001: 448.)

OSI-malli
Malli määrittelee puitteet erilaisten tietoliikennejärjestelmien yhteensovittamiseksi. Se rakentuu seitsemästä kerroksesta, jotka keskustelevat vain ala- ja yläpuolisten kerroksien kanssa. (Järvinen 2001: 480.)

Paikallisväylä
Paikallisväylä yhdistää prosessorin ja oheislaitetta ohjaavan lisäkortin. Prosessori ja väylä toimivat samalla kellotaajuudella ja väylä on yhtä leveä kuin prosessorin dataväylä. VLB oli ensimmäinen yleiskäyttöinen paikallisväylä. (Järvinen 2001: 490.)

PAM (Pluggable Authentication Modules)
Yleinen kehys autentikointiin, valtuutukseen ja tiliöintiin. Ohjelmat ottavat yhteyden PAM:iin suorittaakseen kyseisiä funktioita jättäen järjestelmänvalvojalle vapauden konfiguroida yksittäisiä ohjelmia käyttämään erilaisia autentikointitapoja dynaamisten kirjastoiden avulla. (Barrett & Silverman 2001: 131.)

PCI (Peripheral Component Interconnect)
Paikallisväylästandardi, joka määrittelee korttiliittimen muodon ja toimintajänniteet. (Järvinen 2001: 502.)

PGP (Pretty Good Privacy)
Salausohjelma, jolla voidaan salata ja allekirjoittaa sähköpostit ja tiedostot. PGP käyttää useita salausalgoritmeja, jotka ovat symmetrisiä. (Järvinen 2001: 513.)

POP (Point-Of-Presence)
Internet-operaattorin laitetila, johon kuluttajille ja yrityksiin myydyt kiinteät yhteydet päättyvät. Nimitystä käytetään myös eri kaupungeissa tai telealueilla olevista paikallisista soittonumeroista, joihin asiakas ottaa modeemiyhteyden välttyäkseen kalliilta kaukopuheluilta. (Järvinen 2001: 530.)

QoS (Quality of Service)
"Verkon kyky taata kahden pisteen välille ennalta määrätty siirtonopeus ja muita yhteyden laatuun liittyviä parametreja (Järvinen 2001: 554)."

RAM-muisti (Random Access Memory)
Osa keskusmuistia, jota voidaan lukea ja kirjoittaa. Käyttöjärjestelmä, sovellukset ja sovelluksien työtila ovat RAM-muistissa käytön aikana. Sähkön katketessa RAM-muistin sisältö tyhjenee. (Järvinen 2001: 693.)

RAS (Remote Access Service)
RAS mahdollistaa etäkäyttäjän kytkeytymisen verkkoon lähiverkon ulkopuolista tietoliikenneyhteyttä hyödyntäen. Se on verkkokäyttöjärjestelmän tarjoama palvelu. (Järvinen 2001: 569.)

RFC (Request For Comments)
Dokumentteja, jotka määrittelevät Internetin tekniset standardit. Standardien lisäksi RFC:iden joukosta löytyy myös ohjeita, yhteenvetoja ja suosituksia. (Järvinen 2001: 573.)

S/Key
Kertakäyttöinen salasanajärjestelmä, jota ainoastaan OpenSSH tukee SSH autentikointitapana. Yhteyttä muodostettaessa palvelu antaa järjestysnumeron ja avaimen, jotka syötetään salaisen fraasin kanssa salasanalaskimeen paikallisella tietokoneella. Laskin tuottaa kertakäyttöisen salasanan, jolla käyttäjä voi kirjautua palveluun. (Barrett & Silverman 2001: 175.)

SecurID
Laitteistopohjainen autentikointimenetelmä, jossa käyttäjä tarvitsee SecurID-kortin autentikoituakseen. Kortissa on mikrosiru, joka ilmoittaa väliajoin vaihtuvan luvun. Autentikoitaessa luku syötetää salasanan kanssa. (Barrett & Silverman 2001: 174.)

SHA-1 (Secure Hash Algorithm)
Kryptograafinen salausmenetelmä, jota käytetään useissa ohjelmissa. SHA-1 on toinen versio SHA-menetelmästä. SHA-2 on yleisnimitys neljälle SHA-algoritmin varianteille. Kaksi ensimmäistä versiota on pystytty jo murtamaan. (Wikipedia 2006)

SMP (Symmetric Multiprocessing)
Symmetrinen multiprosessointi tarkoittaa ohjelmien ajamista tietokoneessa, jossa on kaksi tai useampi tasa-arvoinen prosessori. Ohjelmia ja niiden osia voidaan jakaa eri prosessorien suoritettavaksi käyttöjärjestelmän avustuksella. Kaikki prosessorit pystyvät suorittamaan kaikkia tehtäviä eivätkä ole erikoistuneet tiettyihin tehtäviin, jolloin prosessointi on symmetristä. (Järvinen 2001: 642.)

SSH (Secure Shell)
Protokolla, joka takaa salatun tiedonsiirtoyhteyden epäluotettavan verkon yli. (Järvinen 2001: 628.)

T1
Yhdysvalloissa yleisesti käytetty tietoliikennenopeus. Euroopan vastine T1:lle on E1 (2 Mbit/s). (Järvinen 2001: 651.)

T3
Yhdysvalloissa käytetty tietoliikenneverkon standardinopeus (44,736 Mbit/s). (Järvinen 2001: 652.)

TCP/IP(Transport Control Protocol Internet Protocol)
Protokollaperhe, jolla tietokoneet siirtävät tietoa toisilleen ja täten muodostaa koko Internetin perustan. Protokollan TCP-osa järjestää tiedon paketeiksi, IP-osa huolehtii pakettien toimittamisesta oikeaan paikkaan Internetissä. (Järvinen 2001: 659.)

Telnet
Merkkipohjainen pääteyhteys, jolla käyttäjä voi ottaa yhteyden mihin tahansa verkossa olevaan Unix-koneeseen edellyttäen, että käyttäjällä on käyttäjätunnus ja salasana kyseiseen järjestelmään. (Järvinen 2001: 663.)

UDP (User Datagram Protocol)
Yksinkertainen tiedonsiirtotapa, joka ei sisällä virheenkorjausta. TCP/IP-protokollaan kuuluvaa UDP:tä käytetään useimmiten silloin, kun tiedonsiirtotarpeet ovat pieniä ja ohjelmat pystyvät huolehtimaan virhetilanteiden käsittelystä itse. (Järvinen 2001: 698.)

Unix
Laitteistoriippumaton käyttöjärjestelmä, josta on polveutunut jo useampia eri versioita. Näitä käyttöjärjestelmiä käytetään keskuskoneissa, palvelimissa ja tehokkaissa työasemissa. (Wikipedia 2006)

WINS (Windows Internet Naming Service)
Staattisen nimen dynaamisesti vaihtuvaan IP-osoitteeseen yhdistävä palvelu. (Järvinen 2001: 758.)

VLB (VESA Local Bus)
Ensimmäinen yleiskäyttöinen paikallisväylätekniikka, joka on melko yksinkertainen, koska se jakaa prosessorin omia datalinjoja suoraan lisäkorteille. (Järvinen 2001: 732.)

VPN (Virtual Private Network)
Tekniikka, jossa maantieteellisesti erillään sijaitsevat lähiverkot yhdistetään Internetin kautta toisiinsa niin, että ne näyttävät muodostavan yhden loogisen kokonaisuuden. (Järvinen 2001: 729.)

XOR-operaatio (eXclusive OR)
Looginen operaatio, jonka merkitys on "toinen ja vain toinen on tosi". Tietotekniikassa operaatiota käytetään usein salaamiseen. (Wikipedia 2006)