LÄHIVERKON DOKUMENTOINTI

Tomi Wahlroos

Opinnäytetyö
Huhtikuu 2012
Tietotekniikka
Tietoliikenne

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikenne

TOMI WAHLROOS:
Lähiverkon dokumentointi

Opinnäytetyö 39 sivua, josta liitteitä 2 sivua
Huhtikuu 2012

Tämä opinnäytetyö tehtiin Tampereen ammattikorkeakoulussa tietotekniikan koulutusohjelmassa. Työn tilaaja on PC-Räätäli Ay, joka on tietokoneita sekä niiden oheislaitteita myyvä ja huoltava yritys.

Projekti aloitettiin tammikuussa 2012, kun PC-Räätäli Ay tarvitsi uuden dokumentoinnin verkostaan. Yrityksen verkko ei ole suuri, joten työn tekemiseen meni yksi päivä. Työssä avusti Petteri Wahlroos, koska verkko oli kahdessa eri kerroksessa, mikä hankaloitti kaapeleiden seurantaa yksin.

Työn tarkoitus on opettaa sekä sen tekijälle että tämän opinnäytetyön lukijoille pienyrityksen verkon toimivuutta, sen dokumentointia ja eri laitteiden toimivuutta verkossa. Työssä tutustuttiin hieman paremmin verkon tärkeimpiin palveluihin, joita ovat SNMP- ja DHCP-palvelu

Opinnäytetyö on jaoteltu kolmeen osaan. Ensimmäisenä tarkastellaan verkon dokumentointia ja siihen liittyviä asioita. Dokumentointiosion jälkeen esitellään verkkolaitteita sekä keskeisiä käsitteitä. Viimeisenä on PC-Räätälin verkon esitteleminen kaikkine laitteistoineen. Viimeisessä osiossa käitellään, miksi verkko on jaettu kahteen erilliseen osioon.

Työn liitteissä ovat kuvat verkon topologiasta sekä verkon pohjapiirustuksesta, jossa on näkyvissä verkon laitteistot. Kuvista käyvät ilmi kaikki verkon laitteet, niiden sijainti yrityksessä sekä jokaisen laitteen yhteydet.

Asiasanat: dokumentointi, verkko, opinnäytetyö, tietoliikenne, insinööri

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Information technology
Telecommunications engineering

TOMI WAHLROOS:
Ducumentation of local area network

Bachelor's thesis 39 pages, appendices 2 pages
April 2012

This thesis is made for PC-Räätäli Partnership which sells and repairs computers and theirs accessories. It is a very small company and it has only two owners.

The project started in January 2012 for the reason of PC-Räätäli needing a new documentation of their local area network. The network of PC-Räätäli is very small and therefore the whole work of the documentation itself was done in one day.

The purpose of this project is to teach for its readers the function and the documentation of a local area network. This thesis is divided in three sections: The first one is explains how the network was documented. The second chapter introduces the essential terms that is needed to know when reading this thesis. The final section demonstrates the whole network of PC-Räätäli's and its side network which is called Kk4 network. Kk4 network is made for testing the new features before they are applied to practice.

This thesis introduces thoroughly the devices of the network of PC-Räätäli. The thesis also includes a chapter of network security. At the end of this document there is a network topology image and the layout of the PC-Räätäli's property with network devices as an appendices.

Key words: documentation, network, thesis, telecommunications, engineering

SISÄLLYS

LYHENTEET JA TERMIT

ADSL	Asymmetric Digital Subscriber Line, laajakaistaliittymä
Ay	Avoin yhtiö
DHCP	Dynamic Host Configuration Protocol, IP-osoitteita jakava verkkoprotokolla
FTP	Foiled Twisted Pair, foliosuojattu parikaapeli
IP-osoite	Internet Protocol -osoite, laitteen verkko-osoite
IPv4	Internet Protocol version 4, verkko-osoitteen versio 4
IPv6	Internet Protocol version 6, verkko-osoitteen versio 6
IRC	Internet Relay Chat, pikaviestipalvelu
LAN	Local Area Network, Lähiverkko
MAC-osoite	Media Access Control -osoite, verkkosovittimen osoite
NAT	Network Address Translation, osoitteenmuunnos
PSK	Pre-shared key, esijaettu avain, tunnussana
QoS	Quality of Service, palvelun laatu, verkkoliikenteen priorisointi
S/FTP	Screened Foiled Twisted Pair, suojattu ja folioitu parikaapeli
S/STP	Screened Shielded Twisted Pair, kahdesti suojattu parikaapeli
SNMP	Simple Network Management Protocol, verkkohallinan protokolla
SSH	Secure Shell, protokolla salatun yhteyden muodostamiseen
STP	Shielded Twisted Pair, suojattu parikaapeli
UTP	Unshielded Twisted Pair, suojaamaton parikaapeli
WAN	Wide Area Network, Laajaverkko
WLAN	Wireless Local Area Network, Langaton lähiverkko
VLAN	Virtual Local Area Network, Virtuaalinen lähiverkko
WPA2	Wi-Fi Protected Access II, langattoman verkon tietoturvastandardi
VPN	Virtual Private Network, virtuaalinen sisäverkko

1 JOHDANTO

Työn tarkoitus on opettaa pienyrityksen verkon toimivuutta, sen dokumentointia, eri laitteiden toimivuutta verkossa ja minkä takia verkon eri osat on hyvä jakaa erilleen toisistaan. Työssä pyritään avaamaan kaikki tärkeät käsitteet. Enemmän asiasta kiinnostuneille tämä työ tarjoaa hyvät lähteet alkuperäisiin kirjoituksiin ja tarjoaa myös lisäinformaatiota hyödyllisillä web-osoitteilla.

Tässä opinnäytetyössä laadittu verkkokaavio ja pohjakuva ovat tehty yritykselle korvaamaan heidän päivittämättömän paperiversionsa verkkokaavio. Verkkokaavion eli verkon topologiakuvan tarkoituksena on antaa yritykselle selkeä kuva heidän tämänhetkisestä verkosta. Kuvan tulee olla myös helposti muokattavissa, jotta yritys voi päivittää sitä myöhemmin.

Tämä dokumentti on jaettu kolmeen osioon: aluksi kerrotaan hieman itse dokumentoinnista, jonka jälkeen on katsaus yleisellä tasolla verkossa olevista laitteista sekä keskeisistä käsitteistä. Tämän osion jälkeen päästään varsinaiseen PC-Räätälin verkon tarkasteluun, jossa kerrotaan verkon toiminnasta, kaapeloinnista ja laitteistosta. PC-Räätälin verkon jälkeen otetaan lyhyt katsaus verkossa sijaitsevaan erilliseen verkko-osioon nimeltä Kk4, joka on yhden työntekijän ylläpitämä verkko testi- ja hyötykäyttöön.

Verkosta tehtyjen kuvien lisäksi tämä työ antaa kattavan katsauksen yrityksen verkon palvelimiin sekä verkkolaitteisiin kuten kytkimiin, reitittimiin ja langattomaan verkkoon.

2 VERKON DOKUMENTOINTI

Verkon dokumentointi on tärkeä osa verkon rakentamissa ja ylläpitämissä. Siitä selviää verkon toiminta, laitteet ja muut tarpeelliset tiedot, jotka helpottavat verkon korjaamista ongelmatilanteissa. Mahdolliset laajennukset ovat helpompia toteuttaa, jos verkosta on olemassa kattava dokumentaatio.

Dokumentoinnin tarve tulee erittäin hyvin esiin tilanteissa, joissa pientä verkkoa on hiljalleen laajennettu yhä isommaksi lähes kokonaan yhden ihmisen toimesta. Tällaisessa tilanteessa muut verkon kanssa työtä tekevät eivät tiedä verkon toimintatapoja ilman dokumentointia.

Ennen dokumentin tekemistä on hyvä määritellä laajuuden rajat. Liiallinen tiedon määrä voi tehdä dokumentista raskaan ja vaikeaselkoisen, mutta toisaalta tiedon puute voi tehdä dokumentista käyttökelvottoman.

2.1 Tarve uudelle verkkokaaviolle

Yrityksen verkosta oli aiemmin tehty dokumentointi, jota ei ole päivitetty ajan tasalle. Verkkokaavio on paperitulosteena, joten dokumentin muokattavuus on hankalaa. Paperiversiota muokattaessa lopputulos on yleensä epäselvä.

Dokumentin tarpeellisuus nousi esiin, kun alkuperäisen dokumentin tekijä, ja verkon rakentaja, lähti lomamatkalle. Matkan aikana verkossa tuli ongelmia eivätkä yhteydet toimineet. Vanha päivittämätön dokumentti ei ollut tässä tilanteessa avuksi ja ongelmaa piti ratkoa puhelimitse lomamatkalta.

Uuden dokumentoinnin tarkoituksena on korvata vanha dokumentti. Uuteen dokumenttiin sisällytetään enemmän tietoa ja siitä pyritään saamaan selkeämpi ja helpommin päivitettävä. Sen tarkoitus on olla avuksi tulevissa verkko-ongelmissa ja auttaa ymmärtämään verkon toimintaa siitä tietämättömille.

2.2 Dokumentoinnin laajuuden päättäminen

Verkkokaavion tiedoiksi valittiin laitteet nimineen, verkkokaapelit, IP-osoitteet sekä DHCP-allas. Verkkokaavion lisäksi dokumentti käsittää Microsoft Excel -taulukon, johon listataan laajemmat tiedot kustakin palvelimesta.

Aluksi harkittiin myös käyttäjätunnusten, salasanojen sekä laitteistojen tarkkojen asetusten kirjaamista dokumenttiin, mutta nämä tiedot jätetään tämän opinnäytetyön ulkopuolelle tietoturvasyistä. Yritys voi erittäin helposti lisätä ne myöhemmin valmiiseen dokumenttiin ja mahdollisesti myös verkkokaavioon, mikäli he niin haluavat.

Verkkokaaviosta jätettiin tarkoituksella merkitsemättä kytkimien portit, koska kaikki kytkimet ovat lähes tehdasasetuksilla. Yksi syy, jonka takia verkkoportit eivät ole merkittyinä verkkokaavioon on se, että verkkokaapelien paikat kytkimissä ja reitittimissä saattavat vaihdella sekä uusia huollettavia tietokoneita tulee jatkuvasti lisää.

2.3 Menetelmät dokumentoinnin laatimiseen

Työ tehtiin PC-Räätälin tiloissa ja verkkodokumentointiin käytettiin yhtä kannettavaa tietokonetta, jossa oli dokumentointiohjelma. Verkkokaavion tekemiseen valittiin Network Notepad -sovellus, josta kerrotaan enemmän seuraavassa luvussa. Ohjelmalla lisättiin verkkokaavioon jokainen verkkolaite, joka oli kytkettynä verkkoon sekä kaikki tietokoneet ja kaapelit, joissa oli laitteita. Haastetta toivat kerrostenväliset yhteydet, joita ei pystynyt esteettä seuraamaan. Yläkerrassa johtoa piti nykiä ja alakerrassa katsoa, mikä kaapeleista liikkui.

Kaapeleiden ja laitteiston tutkimisen jälkeen verkkokaavio lopulta valmistui. Yrityksen henkilökunta auttoi hieman kertomalla hankalimpien kaapeleiden ja laitteiden sijainnit sekä IP-osoitteet ja laitteiden tiedot.

Verkkokaavion valmistumisen jälkeen tehtiin taulukko, laitteista ja niiden IP-osoitteista, Microsoftin Excel-ohjelmalla. Kiinteistön pohjapiirustukseen sijoitettiin myös laitteet, jotta dokumentointi olisi mahdollisimman havainnollistava.

2.4 Työssä käytetyt ohjelmistot

Ohjelmisto valittiin sen perusteella, mikä niistä pystyisi suoriutumaan mahdollisimman hyvin verkon dokumentoinnista, eli tekemään laitteiden kuvat ja niiden välille linkit, joita pystyi itse määräämään ja hallitsemaan. Tärkeinä ominaisuuksina oli myös ohjelman ilmaisuus ja helppokäyttöisyys. Useiden ohjelmien testauksen jälkeen päädyttiin Network Notepadiin, joka on erittäin pienikokoinen, ilmainen ja toimiva verkkodokumentointiohjelma Windows-ympäristöihin.

Network Notepad -sovellukseen voi tutustua ja sen voi ladata seuraavasta osoitteesta: http://www.networknotepad.com/. Ohjelma on ilmainen ja pienen kokonsa ansiosta sen voi nopeasti ladata testikäyttöön.

Muita käytettyjä ohjelmia ovat Microsoft Paint ja Office, joista jälkimmäisellä on tehty tämä opinnäytetyö kuten myös IP-taulukko. Kiinteistön pohjapiirustuksen hahmotteluun käytettiin Microsoftin Paintia, mutta lopullinen versio pohjapiirustuksesta teetettiin Expotec Oy:llä. Lopulliseen versioon käytettiin AutoCAD-ohjelmistoa, jolla saatiin mahdollisimman viimeistelty lopputulos.

3 LÄHIVERKON KESKEISET KÄSITTEET

Tämä luku avaa termejä, joita käytetään itse työn selvittämisessä luvussa 4. Käsitteisiin ei syvennytä kuin sillä tasolla, joka on tarpeellista itse työn ymmärtämisen kannalta. Avattavia termejä ovat erilaiset verkkolaitteet, palvelut ja peruskäsitteitä liittyen verkkoliikenteeseen.

3.1 Reititin

Reititin on laite, joka yhdistää eri verkkoja ja ohjaa niiden välistä liikennettä. Reitittimissä on yleensä vain muutama verkkoportti ja niissä on monipuolisemmat verkkoliikenteen reititysominaisuudet kuin kytkimissä. Reitittimen ominaisuuksiin kuuluu toiminta isoissa verkoissa ja eri verkkoprotokollien hallinta. Internet koostuu monista reitittimistä, jotka ohjaavat liikennettä operaattoreilta toiselle sekä myös operaattorin omissa verkoissaan. (Lauri Suoranta 2008.)

Reitittimiä on eri hintaisia ja eri kokoisiin verkkoihin. Pienyrityksiin tai kotitalouksiin sopii hyvin erittäin halpa reititin, jossa on perusominaisuudet. Koti- ja pienyritysverkossa yleensä suurin osa verkkoliikenteestä on verkkoon sisään tulevaa liikennettä ja lähtevä liikenne on hyvin vähäistä. Tästä syystä halvemmillakin laitteistoilla pärjätään, joissa on perusasetukset reititykselle ja verkkoliikenteen rajoittamiselle. Suurissa verkoissa siirretään suuria määriä tietoa ja verkkoliikenne voi paikoittain olla ruuhkaista. Tällaisissa verkoissa tarvitaan tehokkaampia reitittimiä, joissa on paljon muistia sekä hyvät suorittimet, jotta reititys ei hidastuisi.

3.2 Kytkin

Kytkin ohjaa liikennettä saman lähiverkon sisällä. Myös kytkimissä on suuria eroja niiden hallittavuuden ja toimintojen osalta. Monessa pienyrityksessä ja kotitaloudessa riittää hyvin halvempi kytkin, johon ei juuri pysty asetuksia laittamaan, mutta se ohjaa liikenteen erittäin pienellä vaivalla koneelta toiselle. Kytkimen valinnassa on paljon samoja piirteitä kuin edellä mainitussa reitittimen valitsemisessa. Sekä kytkin että reititin siirtävät verkkoliikennettä, ja jos tiedon määrä kasvaa suureksi, niin tällöin tarvitaan

kalliimpia laitteita. Isommissa verkoissa tarvitaan monipuolisempia kytkimiä, joihin voidaan asettaa virtuaalisia lähiverkkoja, erilaisia suojauksia liikenteelle, parempaa tietoturvaa ja niissä on yleensä enemmän verkkoporttipaikkoja. Kytkimet pystyvät tunnistamaan verkkoliikenteen lähettäjät ja vastaanottajat, jolloin kytkin osaa lähettää tietovirran oikealle laitteelle. (Microsoft Corporation.)

3.3 Palvelin

Palvelin on tietokone, joka nimensä mukaisesti palvelee toisia tietokoneita ja käyttäjiä omilla palveluillaan. Palvelin on yleensä pelkkä tietokoneen keskusyksikkö, johon on asennettu erilliset palvelinohjelmistot. Palvelimilla on yleensä varmuuskopioita, tiedoston jakamista, web-sivustoja tai mitä tahansa muuta, johon halutaan monelta koneelta pääsy. Joissakin tilanteista tietokoneesta tai palvelimesta voidaan tehdä kytkin tai reititin, johon voidaan lisäksi asentaa palomuuri.

3.4 Työpiste

Työpiste on tietokone, jolla tehdään töitä ja se on osana yrityksen tietoverkkoa. Työpiste on yleensä myös yhteydessä palvelimiin ja mahdollisesti myös Internetiin. Usein työt ja tiedostot sijaitsevat palvelimilla, josta työpisteelle voidaan siirtää työtiedostot tai niitä käytetään suoraan palvelimelta. Työpisteiden koneet saavat IP-osoitteensa yleensä automaattisesti DHCP-palvelimelta. Tietototurvasyistä työpisteiltä voidaan rajoittaa pääsy toisiin verkkoihin tai laitteisiin.

3.5 Palomuuri

Palomuuri suodattaa verkossa tai laitteessa kulkevaa verkkoliikennettä. Palomuurin voi tehdä laitteistolla tai ohjelmistolla. Kotikäytössä ja pienyrityksissä ohjelmistolla tehty palomuuri on yleensä riittävä. Se asennetaan tietokoneelle tai erilliselle palvelimelle, joka mahdollisesti toimii myös reitittimenä. (Viestintävirasto 1 2007.)

Ohjelmistolla toteutettu palomuurin asentaminen on nopeampaa eikä vaadi kovinkaan paljon asiantuntemusta. Varsinkin Windows-tietokoneissa on valmiiksi asennettuna ja toiminnassa oleva palomuuri, joten sen käyttöönotto ei vaadi mitään tietokoneen käyttäjältä. Monille niin sanotuille peruskäyttäjille tämä ratkaisu on täysin riittävä ja se suojaa käyttäjän tietokonetta melko hyvin erilaisilta haittatekijöiltä.

Laitteistolla tehty palomuuri eli ns. rautapalomuuri on tehty yleensä reitittimellä, joka estää ja sallii tietynlaista verkkoliikennettä. Myös kytkimellä pystytään tekemään tietoturvaratkaisuja, joita voidaan pitää palomuurin tapaisina, kuten virtuaaliset lähiverkot. Virtuaalisilla lähiverkoilla voidaan erottaa esimerkiksi samassa kytkimessä kiinni olevat työasemat ja palvelimet toisistaan, etteivät ne näe toisiaan suoraan lähiverkossa.

Tässä opinnäytetyössä keskitytään vain tietokoneisiin, joissa on ohjelmistolla toteutetut palomuurit. Tässä opinnäytetyössä dokumentoitavassa verkossa ei ole varsinaisia reitittimiä, joihin voisi palomuuriasetuksia asentaa, ja ainoa hallittava Ciscon kytkin on lähes oletusasetuksilla.

3.6 Parikaapelit

Parikaapelia käytetään Ethernet-lähiverkoissa. Kaapeleiden tyyppiin viitataan yleensä kategorialla esimerkiksi Cat5 ja Cat6 sekä myös liittimen tyypillä kuten RJ45, jota käytetään Ethernet-lähiverkossa.

Jotta parikaapelin siirtonopeus ja laatuvaatimukset täyttyvät, on kaapelille asetettu tiettyjä ehtoja. Yhden kokonaisen kanavan pituudeksi on asetettu enintään 100 metriä, jolloin molempiin päihin on asetettu 5 metrin laitekaapeli sekä 90 metrin pituinen linkki. Asennuksissa on hyvä myös ottaa huomioon kaapelin taivutukseen asetetut ohjeet. Parikaapelia ei pitäisi taittaa pienemmälle mutkalle kuin 10 · kaapelin halkaisija ja varsinkin 90° tiukat käännökset kaapelissa voivat vahingoittaa kaapelia. (Tampereen sähköpalvelu Oy, 5-6.)

Kanavalle asetettu 100 metrin enimmäispituuden voi kuitenkin ylittää ja linkki voi silti toimia, mutta tällöin kaapelointi pitää tehdä erittäin huolellisesti. Yhteys toimii ja linkis-

sä kulkee verkkoliikenne, vaikka kaapeli ei täyttäisikään kaikkia määritettyjä spesifikaatioita, mutta linkki voi toimia hitaammin tai siinä voi olla muita häiriöitä.

3.6.1 Kategoriat

Nykyään Cat5e ja Cat6 ovat kategorioista yleisimmät. Uudemman Cat6-kategorian käyttö on lisääntynyt yhä useammassa verkossa. Kategoriat ovat standardeja, joissa määritellään kaapelin siirtonopeus sekä erilaisia vaimennuksia, ylikuulumisia ja muita häiriötekijöitä. Alla on taulukko, jossa on jokaisen kategorian nimellinen siirtonopeus.

Tällä hetkellä yleisimmässä käytössä ovat Cat5, Cat5e sekä Cat6, koska näillä kaapeleilla päästään suurimpiin tiedonsiirtonopeuksiin (taulukko 1). Näiden lisäksi on olemassa Cat7, mutta sen standardi ei ole vielä valmis.

TAULUKKO 1. Verkkokaapeleiden nopeudet (Cisco Systems, Inc)

Kategoria	Nopeus
Cat2	4 Mbit/s
Cat3	10 Mbit/s
Cat4	16 Mbit/s
Cat5	100 Mbit/s
Cat5e	1000 Mbit/s (1 Gbit/s)
Cat6	1000 Mbit/s (1 Gbit/s)

Seuraavan sivun kuvassa 1 on tarkemmin esitetty kaapeleiden standardit ja niiden vaatimukset kaapelille. Cat7:n standardi ei ole vielä valmis ja siksi sen standardi on vasta esitys. (Tec Datawire.)

Cat5, Cat5e, Cat6 and Cat7 Patch Cable Performance Specification Chart				
Parameter	**Cat5 Patch Cables and Class D** with additional requirements TSB95 and FDAM 2	**Cat5e Patch Cables** ('568-A-5)	**Cat6 Patch Cables Class E** (Performance at 250 MHz shown in parentheses)	**Proposed Cat7 Patch Cables Class F** (Performance at 600 MHz shown in parentheses)
Specified frequency range	1-100 MHz	1-100 MHz	1-250 MHz	1-600 MHz
Attenuation	24 dB	24 dB	21.7 dB (36 dB)	20.8 dB (54.1 dB)
NEXT	27.1 dB	30.1 dB	39.9 dB (33.1 dB)	62.1 dB (51 dB)
Power-sum NEXT	N/A*	27.1 dB	37.1 dB (30.2 dB)	59.1 dB (48 dB)
ACR	3.1 dB	6.1 dB	18.2 dB (-2.9 dB)	41.3 dB (-3.1 dB)**
Power-sum ACR	N/A	3.1 dB	15.4 dB (-5.8 dB)	38.3 dB (-6.1 dB)**
ELFEXT	17 dB (new requirement)	17.4 dB	23.2 dB (15.3 dB)	ffs***
Power-sum ELFEXT	14.4 dB (new requirement)	14.4 dB	20.2 dB (12.3 dB)	ffs***
Return loss	8 dB* (new requirement)	10 dB	12 dB (8 dB)	14.1 dB (8.7 dB)
Propagation delay	548 nsec	548 nsec	548 nsec (546 nsec)	504 nsec (501 nsec)
Delay skew	50 nsec	50 nsec	50 nsec	20 nsec

KUVA 1. Kategorioiden spesifikaatiot (Tec Datawire)

3.6.2 Suojaus

Kategorioiden lisäksi parikaapeleiden suojauksella on suuri merkitys. Parikaapeleille on tehty erilaisia suojauksia, mutta suojaamattomiakin kaapeleita on saatavilla. Mitä paremmin kaapeli on suojattu, sitä paremmin se täyttää standardin vaatimat spesifikaatiorajat. Kaapelin signaaliin häiriöitä aiheuttavat muun muassa erilaiset sähkölaitteet, valaisimet ja kaapelit.

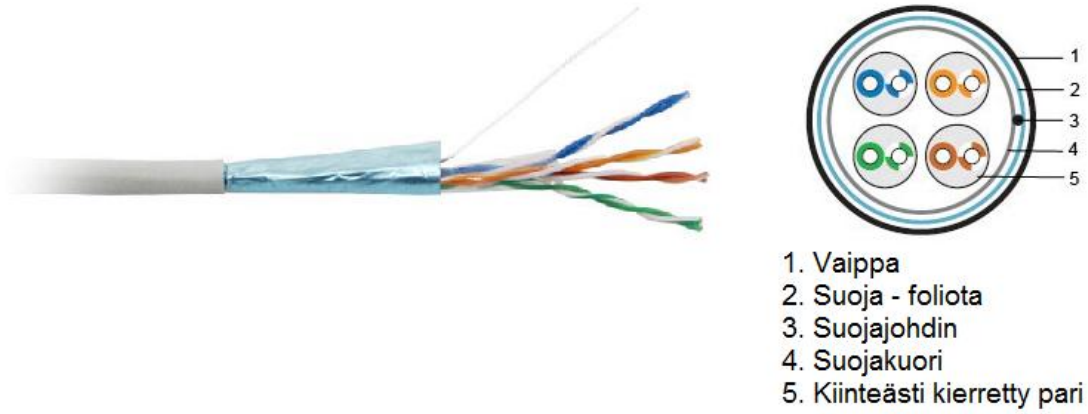
Oikealla asennuksella sekä hyvälaatuisilla liittimillä voidaan estää lisähäiriöitä kaapelissa, mutta kaapelin omat suojaukset ovat erittäin tärkeitä. Suurimmassa osassa nykyajan parikaapeleissa parit ovat kierrettyinä toistensa ympärille, mikä vähentää häiriöitä, jotka aiheutuvat kaapelista itsestään. Ulkoisilta sekä muiden kierrettyjen parien häiriöiltä suojaa yleensä folio. Folio voidaan kiertää kolmella eri tavalla kaapeleiden ympärille: kaikkien parien ympärille, jokaisen erillisen parin ympärille tai sekä että. Seuraavaksi esitellään lyhyesti eri kaapelityypit havainnollistavien kuvien kanssa.

Suojaamaton kierretty parikaapeli eli UTP (Unshielded Twisted Pair) on yleensä halvin ja vähiten suojattu parikaapeli, kuten nimestäkin voi päätellä. Sitä voidaan hyvin käyttää

tietokoneen verkkokaapelina ja paikoissa, joissa ei tarvita pitkiä verkkokaapeleita eikä mahdollisista häiriöistä ole merkittävää haittaa. Se onkin todennäköisesti suosituin kaapeli koti- ja pienyritysverkoissa matalan hinnan ja helpon käsiteltävyyden takia. (kuva 2)

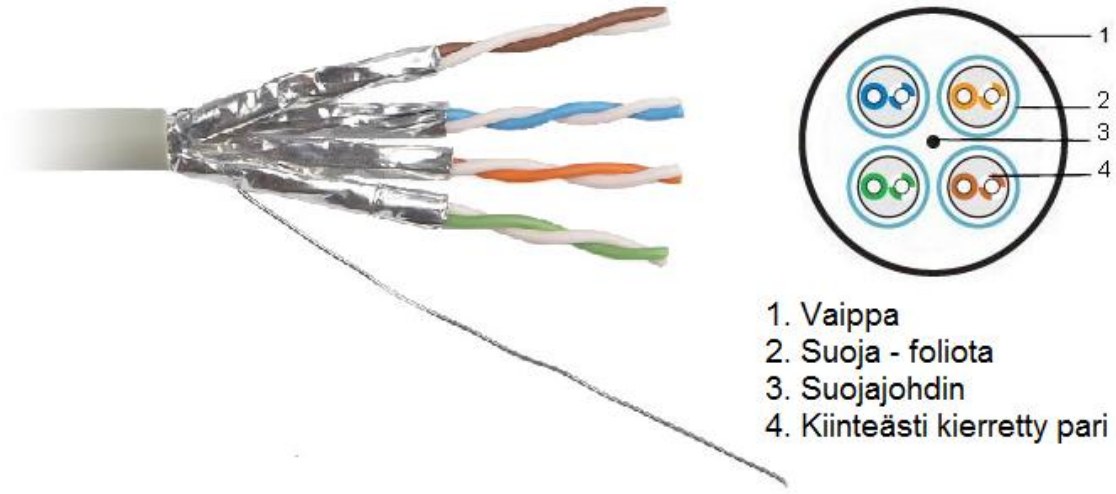
KUVA 2. UTP-kaapeli ja sen poikkileikkaus (Hyperline 1, muokattu)

Foliolla suojattu parikaapeli eli FTP (Foiled Twisted Pair) on hieman kalliimpi kuin suojaamaton kaapeli. Se suojaa paremmin ulkoisilta häiriöiltä folion ansiosta. Folio on kierrettynä kaikkien parien ympärille. (kuva 3)



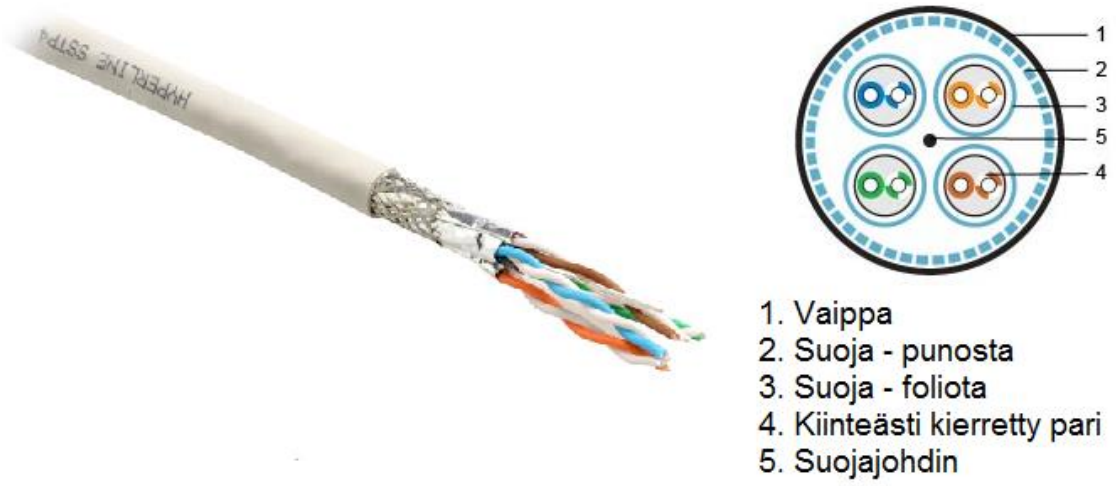
KUVA 3. FTP-kaapeli ja sen poikkileikkaus (Hyperline 2, muokattu)

Suojattu parikaapeli eli STP (Shielded Twisted Pair) antaa hyvän suojan sekä ulkoisia häiriöitä että kaapelin omien parien aiheuttamiin häiriöihin. Jokainen kierretty pari on suojattu foliolla, joten parit eivät pääse häiritsemään toisiaan yhtä paljon kuin suojaamattomassa. (kuva 4)



KUVA 4. STP-kaapeli ja sen poikkileikkaus (Hyperline 3, muokattu)

Parhain mahdollinen suojaus on käyttää sekä foliosuojausta kaapelin vaipassa että jokaisen parin ympärillä. Tällaisia sanotaan SFTP- (Screened Foiled Twisted Pair) tai SSTP-kaapeleiksi (Screened Shielded Twisted Pair). Nämä kaapelit ovat huomattavasti kalliimpia kuin suojaamattomat. Tällaisten kaapeleiden käsiteltävyys on huonompi, koska suurten suojausten takia kaapelit ovat jäykkiä, eivätkä ne taivu kovin helposti rullalle. Kaapelin heikompi käsiteltävyys vaikeuttaa hieman asennustöitä ja tekee kaapeleista hankalia työpöytäkäytössä ja toimistoissa. Kaapelit sopivatkin parhaiten pitkille matkoille reitittimien tai kytkimien väliseen liikenteeseen. (kuva 5)



KUVA 5. SFTP- ja SSTP-kaapeleiden poikkileikkaus (Hyperline 4, muokattu)

3.7 ADSL-yhteys

DSL on lyhenne sanoista Digital Subscriber Line. ADSL tarkoittaa epäsymmetristä DSL-linjaa eli Asymmetric Digital Subscriber Line. Siirtonopeus on pääasiassa suurempi lataamaan kuin lähettämään internetiin. (Diane Teare 2010, 442.)

Suomessa suuressa suosiossa oleva ADSL-liittymä on laajakaistayhteys, joka on jatkuvasti yhteydessä palveluntarjoajaan. DSL-yhteydet käyttävät puhelinlankoja, jonka takia DSL on Suomessa erittäin suosittu ja sen saa lähes jokaiseen talouteen, jossa on puhelin. ADSL-käyttää samaa kaapelia kuin lankapuhelimet, joka tulee jokaiseen taloon omana erillisenä kaapelina. Tästä syystä yhteyttä ei jaeta muiden saman alueen käyttäjien kesken. (SuomiCom.)

DSL-yhteys on erittäin hyvä kotikäyttöön sekä pienemmille yrityksille, koska sen siirtonopeudet ovat melko hyvät eikä se kuitenkaan ole merkittävän kallis. Vanha ADSL-tekniikka pääsee suurimmillaan 8 Mbit/s latausnopeuteen ja 1Mbit/s lähetysnopeuteen (Diane Teare 2010, 447). Vanhan ADSL-tekniikan lisäksi nykyään operaattoreilla on nopeampia ADSL2+-yhteyksiä. Ne pystyvät jopa 24Mbit/s latausnopeuteen.

3.8 IP-osoitteet

IP-osoitteet ovat tietoverkossa olevien laitteiden osoitteita, samantapaisia kuin kiinteistöillä ovat katuosoitteet. Jokaisella verkon laitteella on oma identtinen IP-osoite, jolla laitteet tunnistavat toisensa. Laitteille voidaan asettaa itse IP-osoitteet tai jokin muu laite antaa DHCP:n avulla verkkoon liittyvälle laitteelle automaattisesti IP-osoitteen. (CSC — Tieteen tietotekniikan keskus Oy.)

IP-osoitteiden jakamisesta ja hallinnoimisesta vastaa IANA eli Internet Assigned Numbers Authority. IANA jakaa muun muassa IP-osoitteita operaattoreille, jotka voivat jakaa niitä eteenpäin omille asiakkailleen. IANA:a hallitsee ICANN (Internet Corporation for Assigned Names and Numbers). Lisätietoa IANA:sta ja sen toiminnasta osoitteesta: http://www.iana.org/about/. (Internet Assigned Numbers Authority; CSC — Tieteen tietotekniikan keskus Oy.)

IPv4-osoitteiden rajallisen määrän takia tarvitaan osoitteenmuunnos eli NAT. Osoitteenmuunnoksen avulla voidaan säästää useita julkisia osoitteita ja saadaan hieman lisättyä tietoturvaa. Osoitteenmuunnoksesta kerrotaan tarkemmin luvussa 3.9.

IP-osoitteista on myös olemassa uudempi IPv6-standardi, mutta koska PC-Räätälin verkossa ei ole käytössä IPv6:sta, ei sitä ole mielekästä tässä opinnäytetyössä käsitellä. Lisätietoa IPv6:sta voi lukea esimerkiksi Wikipedian sivuilta, jossa on perusasiat selvitettynä sekä annettu osoitteen muodosta havainnollistava esimerkkikin. Osoite artikkeliin: http://fi.wikipedia.org/wiki/IPv6.

IP-osoitteita on kahta eri tyyppiä, joista julkiset osoitteet ovat internetissä reititettäviä osoitteita ja sisäverkon osoitteet ovat lähiverkkoihin tarkoitettuja osoitteita.

3.8.1 Julkiset osoitteet

Verkkolaitteet saavat julkiset osoitteet yleensä palveluntarjoajalta. Palveluntarjoajan sopimuksissa on yleensä asetettu IP-osoitteiden lukumäärä sekä se, onko osoitteet kiinteitä vaiko dynaamisia. Kiinteä eli staattinen IP-osoite ei vaihdu siinä missä dynaaminen IP-osoite saattaa ajoittain vaihtua verkkolaitteella.

Julkinen IP-osoite asetetaan yleensä reitittimelle tai modeemille, jotka toimivat yhteyden ohjaajina sisäverkon ja operaattorin verkon välillä. Julkinen IP-osoite voidaan jakaa eteenpäin sisäverkon laitteille, jos reititin tai modeemi on siltaavassa tilassa. Julkisella IP-osoitteella varustettu verkkolaite näkyy internetiin, minkä takia siihen saadaan helposti muodostettua yhteys. Yleensä julkisille palvelimille, johon halutaan taata Internetistä pääsy, annetaan julkinen IP-osoite nopean ja helpon yhteyden varmistamiseksi.

Operaattori voi sopimuksesta riippuen antaa yhden tai useamman julkisen IP-osoitteen. Nykyään monessa kotitaloudessa ja pienyritysten verkoissa on enemmän laitteita kuin operaattorilta saatavia julkisia IP-osoitteita. Julkisten osoitteiden loppuessa kannattaa käyttöön ottaa sisäverkon osoitteet.

3.8.2 Sisäverkon osoitteet

Sisäverkon osoitteet on tarkoitettu käytettäväksi vain lähiverkoissa, eikä niitä saa reitittää internetiin. Sisäverkon osoitteet käännetään osoitteenmuunnoksen avulla julkisiksi osoitteiksi. Sisäverkon osoitteille ei ole asetettu rajoitteita, vaan niitä saa kuka tahansa käyttää niin paljon kuin haluaa, koska niillä on vain paikallinen merkitys. Sisäverkon osoitteita saa myös jakaa vapaasti aliverkkoihin ja osoitteet voidaan määrätä itse kiinteiksi tai asettaa DHCP-palvelimen avulla automaattisesti.

Taulukossa 1 on listattuna sisäverkon IP-osoitteet. Monessa kotitalouksiin tarkoitetuissa reitittimissä ja langattomissa tukiasemissa on yleensä käytössä 192.168.0.0-verkko. Myös verkot 172.16.0.0 ja 10.0.0.0 ovat usein käytössä ja erilaisilla verkko-osoitteilla saadaan luontevasti eroteltua verkot toisistaan. Niiden hahmottamisesta tulee nopeaa ja helppoa (taulukko 1).

TAULUKKO 1. Sisäverkon osoitteet

Alku	Loppu	Aliverkon peite
10.0.0.0	10.255.255.255	/8
172.16.0.0	172.31.255.255	/12
192.168.0.0	192.168.255.255	/16

Esimerkkinä voidaan miettiä verkkoja 192.168.1.0 ja 192.168.2.0, jotka ovat yhden rakennuksen sisäverkon osoitteet kahdelle omalle kerrokselleen. Ajatellaan, että yläkerrassa on toimisto, jonka laitteet käyttävät verkkoa 192.168.2.0 ja alakerran toimiston laitteet käyttävät verkkoa 192.168.1.0. Näiden verkkojen lisäksi voidaan haluta erottaa palvelimet omaan verkkoon, jonka huomaa helposti jo laitteiden IP-osoittesta ja tällöin voidaan esimerkiksi palvelimille käyttää omaa verkkoa 172.16.0.0.

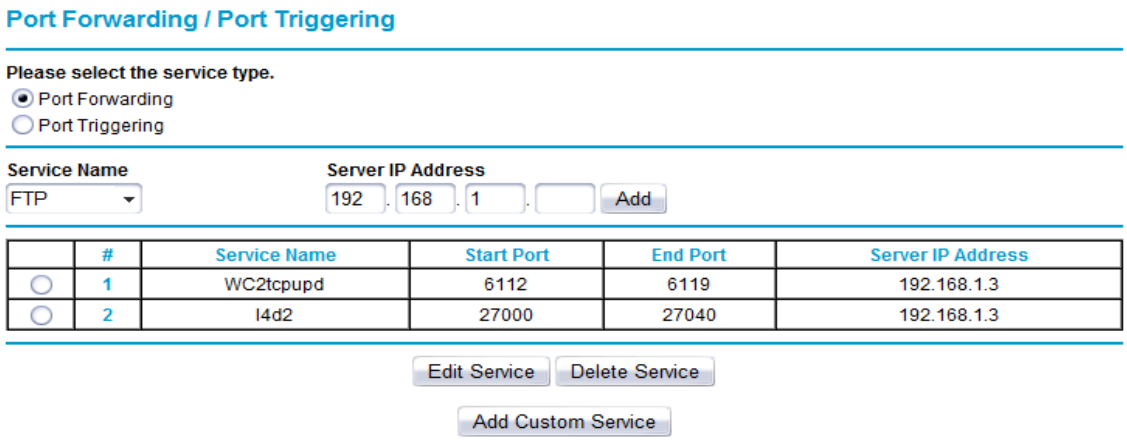
Sisäverkon osoitteiden hankaluus on niiden näkymättömyys Internetistä. Jos yhteys halutaan muodostaa Internetistä sisäverkossa olevaan palvelimeen, tarvitaan tätä varten porttiohjaus osoitteenmuunnoksen avulla.

3.9 Osoitteenmuunnos

Verkon tietoturvaa lisää osoitteenmuunnos eli NAT (Network Address Translation), jolla verkon sisäiset harmaan alueen IP-osoitteet muutetaan julkiseksi IP-osoitteeksi reitittimessä. Vaikka alunperin NAT tehtiin säästämään IPv4-osoitteita, niin se luo myös erittäin hyvän tietoturvan, koska verkon ulkopuolelta käsin kohdekoneen osoitetta ei tiedetä ja siihen käsiksi pääseminen on erittäin vaikeaa.

Mikäli yritysverkossa on osoitteenmuunnos käytössä, eikä heillä ole palvelimilla julkisia IP-osoitteita, tällöin heidän on tehtävä porttien ohjaaminen eli port forwarding, jotta ulkomaailmasta saapuvat yhteydet osaavat mennä oikeaan palveluun, kuten web-palvelimelle tai sähköpostipalvelimelle. Port forwarding tehdään asettamalla tietty sisäinen IP-osoite tietylle portille julkisessa IP-osoitteessa. Esimerkiksi tähän kelpaavat web- ja SSH-palvelut. Web-palveluun saapuvat yhteyspyynnöt tulevat julkisen IP-osoitteen porttiin numero 80 ja tällöin ne ohjataan web-palvelimen sisäiseen IP-osoitteeseen. SSH-palvelupyynnöt puolestaan tulevat porttiin numero 22, jolloin ne ohjataan omalle SSH-palvelimen sisäiselle IP-osoitteelle. Tällä tavalla jokaiselle laitteelle ja palvelulle saadaan oma sisäinen osoite, jolloin tullaan toimeen vain muutamalla julkisella osoitteella.

Kuvassa 6 on esimerkki porttiohjauksesta, joka on tehty Netgearin valmistamalle WLAN-reitittimelle. Kuvassa näkyy palvelu nimeltä l4d2, jolle on asetettu portit 27000-27040. Julkiseen IP-osoitteeseen kohdistuvat yhteyspyynnöt, jotka koskevat edellä mainittuja portteja, lähetetään edelleen laitteelle, jonka IP-osoite on 192.168.1.3.



KUVA 6. Porttiohjaus

3.10 DHCP-palvelu

DHCP (Dynamic Host Configuration Protocol) on ratkaisu, jolla laitteille saadaan asetettua automaattisesti verkkoasetukset. Verkossa täytyy olla DHCP-palvelin, joka yleensä on verkon reititin, modeemi tai erillinen palvelin. Jos kiinteää IP-osoittetta ei ole asetettu laitteelle, niin se saa DHCP-palvelimen kautta IP-osoitteen, aliverkon peitteen sekä oletusyhdyskäytävän. Näiden lisäksi voidaan myös antaa tiedot nimipalvelimista. (Microsoft Oy, 2007.)

DHCP-palvelu on hyvä ratkaisu verkon ylläpitäjälle, koska sillä vältytään laitteiden verkkoasetusten tekemiseltä. Laitteet osaavat itse hakea omat asetuksensa, kun ne kytketään verkkoon kiinni, jossa on DHCP-palvelin.

Microsoftin tukisivustolla on seikkaperäinen selvitys DHCP:n toiminnasta sekä heidän DHCP:tä tukevista Windows-käyttöjärjestelmistä. Osoite Microsoftin tukisivustolle: http://support.microsoft.com/kb/169289.

3.11 VPN-yhteys

VPN on yksityinen virtuaalinen sisäverkko. Lyhenne VPN tulee sanoista Virtual Private Network. VPN on ratkaisu, jolla yhdistetään erilliset verkot toisiinsa tai yksittäinen etäkäyttäjä verkkoon. VPN:llä luodaan niin sanottu tunneli julkisen verkon eli internetin ylitse. Tämän tunnelin tarkoitus on turvata yhteys ja pitää tieto muuttumattomana tunnelin päästä päähän. (Viestintävirasto 2 2007.)

VPN voidaan toteuttaa joko ohjelmalla tai laitteistolla. Ohjelmistolla toteutettu VPN vaatii sekä käyttäjälle että palvelimelle oman ohjelman, jonka kautta yhteys muodostetaan. Laitteistolla toteutettu VPN on suoraan asennettuna esimerkiksi reitittimeen, jolloin käyttäjät eivät tarvitse erillistä ohjelmistoa, eivätkä edes huomaa käyttävänsä VPN-yhteyttä.

VPN-tunnelissa käyttäjät todennetaan, yhteys salataan ja siinä voidaan käyttää PPTP-protokollaa (Point to Point Tunneling Protocol). Nämä toimenpiteet yhdessä tekevät

VPN-yhteydestä erittäin luotettavan ja suositun yhteysmuodon, jota käytetään paljon etäyhteyden muodostamisessa. (Viestintävirasto 2 2007.)

4 DOKUMENTOITAVIEN VERKKOJEN ESITTELY

Seuraavissa kappaleissa esitellään sekä varsinainen PC-Räätälin pääverkko sekä Kk4-testiverkko. Verkkojen esittelyssä käydään läpi hieman erilaisia palveluita ja laitteita, joita verkkoon on asennettuna. Näiden lisäksi otetaan pieni katsaus verkon vikasietoisuuteen sekä tulevaisuuden suunnitelmiin laajennettavuudessa.

Lopussa on liitteenä kuvat verkon topologiasta sekä verkon pohjakuva, josta on nähtävillä jokaisen laitteen sijainti yrityksessä. Kuvat voivat auttaa verkon hahmottamista samalla kun tätä tekstiä luetaan. (liite 1 ja 2.)

4.1 PC-Räätälin verkko

Verkko on täysin Ethernet-verkko. Siinä on yksi reititin, joka on tehty Linux-tietokoneesta, sekä 12 kytkintä. Kytkimistä yksi on Ciscon valmistama ja se on ainoa hallittava kytkin, johon voidaan määritellä edistyneempiä asetuksia. Sitä käytetään silti lähes perusasetuksilla. Loput kytkimistä ovat halvempia peruskytkimiä, jotka sopivat hyvin koti- ja pienverkkoihin. Ne ovat kytkettyinä verkkoon täysin alkuperäisasetuksilla ja toimivat vain liikenteen ohjaajina ilman asetusten muutoksia.

4.1.1 Verkon kaapelointi ja sen selvittäminen

Verkkokaapeleina toimii sekaisin vanhoja Cat5-kaapeleita sekä hieman uudempien standardien Cat5e- sekä Cat6-kaapeleita. Vanhat kaapelit eivät ole vielä haitaksi, koska osa kytkimistä eivät kykene uusien standardien suuriin siirtonopeuksiin. Kaapelointia ei ole tehty seinien sisään tai kouruihin kuten uusissa nykyaikaisissa ratkaisuissa, vaan kaapelit on vedetty suoraan kytkimeltä tai reitittimeltä seuraavalle laitteelle mahdollisimman lyhyttä reittiä seinien viertä tai pöytiä pitkin. Kaikki kaapelit ovat hyvin näkyvillä, joten niitä on vaivaton seurata. Tärkeimpiin kaapeleihin on laitettu merkintä, jotta ne tunnistetaan.

Kaapelointi ja kytkimien käyttö vaikuttaa hieman sekavalta, kun verkkoa katsoo ensimmäisen kerran. Verkkoa on laajennettu vähitellen ja tarpeen mukaan, jonka vuoksi se näyttää epäselkeältä. Verkko toimii kuitenkin erittäin hyvin yrityksen tarpeisiin nähden.

Verkon kytkimistä löytyy myös paljon verkkokaapeleita, joissa ei ole laitteita kiinni. Näihin kaapeleihin laitetaan yleensä huollettavat tietokoneet kiinni tai muita väliaikaisia projekteja, jotka tarvitsevat verkkoyhteyden. Näitä yksittäisiä irrallisia verkkokaapeleita ei ole otettu huomioon verkkokaaviossa.

4.1.2 IP-osoitteiden jakaminen DHCP-palvelun avulla

Verkossa on käytössä DHCP ja se on asennettuna Untangle-palvelimelle. Verkon osoite on 192.168.0.0, jossa DHCP-palvelin jakaa laitteille osoitteita. DHCP-palvelin antaa verkossa työkoneille laiteosoitteet 192.168.0.1-49 ja korjattaville asiakaskoneille osoitteet 192.168.0.50-254.

Työkoneiden IP-osoitteista poikkeavat kiinteät osoitteet, jotka ovat asetettu palvelimille ja verkkolaitteille. Palvelimilla on hyvä olla kiinteät IP-osoitteet, jotta niihin saadaan muodostettua yhteys helposti ja laitteet pystyvät aina keskustelemaan toistensa kanssa.

4.1.3 Katsaus verkon palvelimiin

Verkossa on käytössä viisi palvelinta, joista yksi toimii reitittimenä. Palvelimien nimet ovat Fanta, Kesoil, SparcStation, Unity ja Untangle. Jokaiselle palvelimelle on asetettu oma kiinteä IP-osoite.

Suurimmassa osassa palvelimista on käytössä Linux-käyttöjärjestelmä. Kesoil- ja Fanta-palvelimissa on Linux-pohjainen Ubuntu-jakelu ja Untanglessa on Debian-jakelu. Yksi palvelimista on todella vanha ja se on Sun Microsystemsin tekemä SparcStation, joka oli alunperin työkone. SparcStationissa on käytössä NetBSD-käyttöjärjestelmä, jolla on korvattu alkuperäinen Sun Microsystemsin kehittämä SunOS-käyttöjärjestelmä.

Untangle-palvelin toimii verkossa palomuurina ja reitittimenä. Se sijaitsee ensimmäisenä laitteena kiinni ADSL-modeemissa suojaten muuta verkkoa. Untanglen reititinsovellukselle ei ole asetettu muita liikenteen ohjaamisen ominaisuuksia kuin DHCP-palvelu sekä reitti ADSL-modeemin kautta internetiin.

Fanta-pääpalvelimessa ovat asiakasrekisteri sekä levykuvat asennettavista ohjelmistoista. Fanta on kiinni gigabitin siirtonopeuteen kykenevässä kytkimessä, jotta levykuvien nopea saanti olisi taattu. Täten huollettavien tietokoneiden asennusajat lyhenevät.

SpacrStation-palvelimella on IRC-palvelu ja sen sovellukseksi on valittu ircd. IRC-palvelinta käytetään internetkeskusteluohjelman käyttämiseen.

Unity-palvelimella toimiva web-palvelin on toteutettu Apache2-sovelluksella. Web-palvelimella on yrityksen työntekijöiden omia kotisivuja, ohjekirjoja ja hyödyllisiä linkkejä. Yrityksen varsinaiset kotisivut ovat ulkoistettu yrityksen verkon ulkopuolelle.

Yritykseen on myös tehty oma kameravalvonta ja sitä ylläpitää Linux-palvelin, joka on nimetty vanhan huoltoasemaketjun Kesoilin mukaan. Kameravalvonnasta vastaa yrityksen kehittämä oma ohjelma, jonka pohjana on motion-sovellus.

Alla olevassa taulukossa on IP-osoitteen mukaan listattu verkon palvelimet järjestykseen. Listasta käy ilmi palvelinten nimet, mihin toimintaan palvelimet on tehty, niiden käyttöjärjestelmät ja niiden ytimet, laitteiston tiedot sekä lähiverkon IP-osoitteet (taulukko 3).

TAULUKKO 3. PC-Räätälin palvelimet

Nimi	Toiminta	Käyttöjärjestelmä	Kernel	Prosessori	RAM	Kiintolevy	IP-osoite
Untangle	Palomuuri/GW	Debian	2.6	N/A	N/A	N/A	192.168.0.1
Fanta	Pääpalvelin	Ubuntu	2.6.32-38	i3 540	6GB	6TB(RAID1)	192.168.0.11
Kesoil	Kameravalvonta(CCTV)	Ubuntu	2.6.32-39	P4 2.6GHz	1GB	1.5TB	192.168.0.14
SparcStation	IRCD	NetBSD	3.0 GEN	SPARC 110	142MB	2GB SCSI	192.168.0.19
Unity	Web-palvelin	Debian	2.4.27-4	P3 500MHz	250MB	30GB+NFS	192.168.0.42

4.1.4 Tietoturvaratkaisut suojaavat verkkoa

Turvallisuudesta vastaa palomuurilla varustettu tietokone Untangle. Koko verkko on samassa lähiverkossa, jolloin jokaiselta tietokoneelta pääsee mille tahansa laitteelle. Tietysti tätä estää käyttäjänimet ja salasanat, jotka ovat konekohtaisia.

Untanglessa palomuurina toimii Linuxin Netfilter. Palomuurissa on käytössä myös NAT, johon on asetettu avoimiksi porteiksi seuraavat: 22/TCP (SSH), 80/TCP (HTTP), 85/TCP (MIT-ML-Dev), 443/TCP (HTTPS) ja 6667/TCP (IRC). Ulosmenevälle liikenteelle Untanglessa ei ole asetuksia. (netfilter.org.)

Verkossa on Ciscon hallittava kytkin, johon voisi tehdä tietoturvaa parantavia asetuksia, kuten virtuaalisen lähiverkon eli VLANin. Kytkimelle ei kuitenkaan ole asennettu tietoturvaa parantavia asetuksia, vaan kytkin on lähes kokonaan vakioasetuksilla. Kytkimeen on kuitenkin asennettu SNMP-palvelu käyttöön. Se mahdollistaa laitteiston etätarkkailun, joka on hyödyllinen mahdollisissa vikatilanteissa. Tästä kerrotaan lisää myöhemmin luvussa 4.2.3, jossa on katsaus Kk4-verkon SNMP-palveluun.

Untangle-palvelimen palomuuriin on asennettuna VPN-tunneli. Palvelimen kautta jokainen OpenVPN-ohjelman asentanut etäkäyttäjä saa muodostettua yhteyden sisäverkon palvelimiin. Untangle on ainoa palvelin, johon VPN tarvitsee asentaa, koska Untangle on samassa verkossa muiden palvelimien kanssa, joten näiden väliset yhteydet toimivat ilman VPN-tunnelia.

4.1.5 Yhteydet internetiin verkosta

Tällä hetkellä yrityksessä on ADSL2+-yhteys, joka on kytkettynä taloyhtiön puhelinkeskuksessa valokuituun. Yhteys mahdollistaa 20Mbit/s latausnopeuden lähetysnopeuden jäädessä vain 0,7Mbit/s. Yhteyden päivittämistä on kaavailtu valokuituyhteyteen tai mahdollisesti ottamalla 3G-modeemi ADSL-liittymän rinnalle.

Valokuituyhteyden ansiosta yritys saisi erittäin nopeat lataus- ja lähetysnopeudet sekä pienen viiveen internetiin. Yhteys tulisi taloyhtiön kautta, joten hinta olisi melko edullinen verrattuna yhteyden tuomiin etuihin. Taloyhtiöllä ei vain vielä ole täysiä valmiuksia

valokuituyhteydelle. Tampereen Puhelin on asentanut valokuidun taloyhtiön puhelinkeskukseen asti, mutta taloyhtiöllä on vain ADSL-yhteyksiä tukevat laitteistot kytkettynä talon sisäiseen kaapelointiin.

Erittäin taloudellisena vaihtoehtona toimisi 3G-yhteys ADSL-yhteyden rinnalle. Sillä saadaan lähinnä kaistanleveyttä suurennettua, mutta yhteyden viiveelle internettiin sillä ei juuri ole merkitystä. Tästä kerrotaan enemmän hieman myöhemmin luvussa 4.8 laajennettavuus.

4.1.6 Langaton lähiverkko lisää joustavuutta

Langaton verkko on osa varsinaista yrityksen verkkoa ja tarkoitettu kannettavien tietokoneiden yhteyksiä varten. Langaton verkko tarjoaa työntekijöiden kannettaville työkoneille joustavuutta ja helpon pääsyn verkkoon.

Salauksena toimii WPA2-PSK, eli avain on ennalta määritetty. Langattoman verkon nopeus on 54Mbit/s, joka on 802.11g-standardin mukainen. Laitteet tukevat myös 802.11b-standardia, joka on hieman vanhempi ja hitaampi.

Jokaisessa langattomassa reitittimessä on osoitteenmuunnos päällä, ja jokaisella niistä on oma langattoman verkon verkko-osoite 192.168.1.0. Langaton verkko on siis eri verkossa kuin yrityksen kiinteä verkko, jonka takia osoitteenmuunnos on pakollinen, jotta laitteet voivat muodostaa yhteyden toistensa kanssa.

Langattoman verkon laitteet eivät kykene näkemään tai hakemaan kiinteässä verkossa olevia palvelimia eikä niiden osoitteita. Langattomasta verkosta voidaan muodostaa yhteys kiinteän verkon palvelimiin, jos niiden IP-osoitteisiin yhdistetään suoraan.

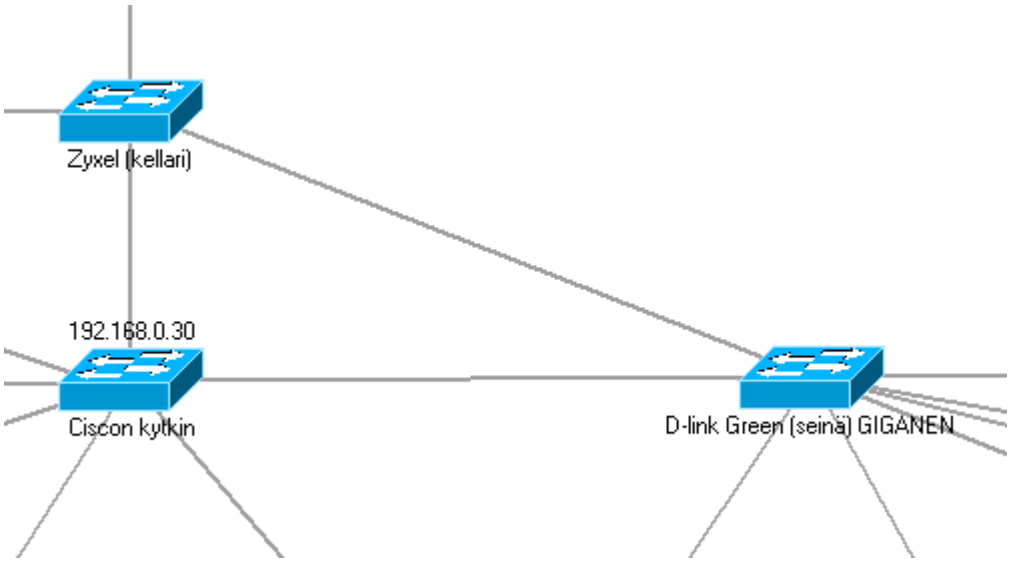
4.1.7 Verkon vikasietoisuus ongelmatilanteissa

Yrityksessä ei ole tällä hetkellä lainkaan varavirtalähteitä (UPS - Uninterruptible Power Supply), joten sähkökatkoksen aikana kaikki laitteet sammuvat. Verkko on myös vain

yhden palveluntarjoajan ja yhden reititinmodeemin varassa, joten laiterikko tai ongelmat palveluntarjoajalla katkaisevat yhteydet Internetiin täysin.

Sisäverkon vikasietoisuutta lisää useamman kytkimen käyttö, jotka ovat toisiinsa yhteydessä. Usean kytkimen käyttö voi myös tulla ongelmaksi. Tällä hetkellä verkko toimii hyvin ilman ongelmia, mutta kytkinten välille voi muodostua niin sanottuja yleislähetysmyrskyjä jotka voivat hidastaa verkkoa ja kytkimiä. Spanning tree -protokollaa käyttämällä kytkimet osaisivat keskustella sekä muodostaa pää- ja varareitin. Spanning tree -protokolla on tehty kytkentäiseen verkkoon . Sen tarkoituksena on poistaa silmukat verkosta muodostamalla yhden pääreitin ja muut reitit ovat poissa päältä toimien varareitteinä. (IEEE 802.1d STP.)

Alla olevassa kuvassa on PC-Räätälin verkkokaaviosta kuva kolmesta kytkimestä. Ciscon kytkin on ainoa kytkin verkossa, joka tukee spanning tree -protokollaa. Spanning tree -protokollan puute kahdesta muusta kytkimestä voi aiheuttaa ongelmia verkossa. Yleislähetykset voivat jäädä kiertämään kytkinten välille, joka aiheuttaa verkon hidastumista (kuva 7).



KUVA 7. Kytkimet ja reitityssilmukka

Vikasietoisuutta lisää myös se, että yrityksellä on varastossa kytkimiä. Uusi kytkin saadaan nopeasti tilalle, jos verkosta sellainen hajoaa. Asetuksiakaan ei tarvitse kovin paljoa tehdä, koska kytkimet ovat lähes vakioasetuksilla. Vähäisten asetuksien takia uuden kytkimen verkkoon asentamiseen onnistuu nopeasti.

4.1.8 Mahdolliset laajennettavuudet tulevaisuudessa

Verkko on melko pieni, mutta pienen yrityksen tarpeisiin sopivan kokoinen ja toimiva. Kytkimiä verkossa on jo reilusti ja porttipaikkojakin riittää, mutta ongelmana on kytkimien hitaat liitännät, mikä ilmenee hitaana siirtonopeutena. Vaikka verkkokaapelit kykenevät gigabitin siirtonopeuteen, niin vain neljä kytkimistä tukevat gigabitin siirtonopeutta ja loput ovat tukevat vain 100 Mbit/s siirtonopeuteen asti.

Kiinteistössä on ADSL2+-yhteys, joka on hieman liian hidas yrityksen tarpeisiin ja hintakin on melko tyyris siirtonopeuteen nähden. Valokuituyhteyttä on mietitty ADSL-yhteyden korvaajaksi, mutta kuten aiemmin todettiin luvussa 4.1.1, valokaapelille ei ole vielä taloyhtiöllä tarvittavaa laitteistoa.

Nettiyhteyden kapasiteettia ja vikasietoisuutta saataisiin lisättyä yhdistämällä ADSL:n kanssa 3G-modeemi. 3G-yhteyden hinta on nykyään niin alhainen, että se olisi taloudellinen ja nopea tapa saada lisäkaistaa. Mobiiliyhteyksien kapasiteetti on melko hyvä, vaikka viiveet ovat suuret ja heittelehtivät melko paljon. Viiveen merkitys on tosin pieni, kun yhteys yhdistetään ADSL:n kanssa. Verkossa on IP-puhelin, joka vaatii yhteydeltä reaaliaikaisuutta ja pienen viiveen. Pelkkä ADSL-yhteys kykenee tähän riittävän hyvin, joten 3G-yhteyden viiveelle jää hyvin pieni merkitys.

4.2 Kk4-verkko

Kk4-verkko on yhden yrityksen työntekijän ylläpitämä testiverkko, joka sijaitsee PC-Räätälin tiloissa ja on yhteydessä internetiin yrityksen ADSL-yhteyden kautta. Se on rakennettu testi- ja hyötykäyttöön. Verkossa koekäytetään uusia ominaisuuksia ja palveluita ennen kuin ne laitetaan PC-Räätälin varsinaiseen verkkoon. Tällä varmistetaan, etteivät uudet palvelut tai ominaisuudet aiheuta ongelmia yrityksen verkossa.

Kk4-verkko on erillään PC-Räätälin verkosta ja Kk4-verkon verkko-osoite on 192.168.100.0. Verkossa on DHCP- ja SNMP-palvelin sekä muita palvelimille asennettuja sovelluksia. Verkko on rajattu erikseen yrityksen verkosta tietoturvasyistä, jotta

testaamattomat ohjelmat ja palvelut eivät aiheuttaisi tietoturvareikiä. Ne voivat myös tehdä palvelimista epävakaita tai jopa sekoittaa ne täysin.

4.2.1 DHCP-palvelu ja kiinteät IP-osoitteet

Kk4-verkossa on pelkkiä palvelimia ja jokaiselle niistä on määrätty MAC-osoitteen mukaan kiinteä IP-osoite, jonka DHCP-palvelin antaa laitteille. Tällä hetkellä DHCP:stä ei ole kovinkaan paljon hyötyä, kun jokaiselle verkossa olevalle laitteelle on annettu kiinteä IP-osoite. DHCP on myös laitettu antamaan osoitteita 50-100 väliltä laitteille, joita verkkoon on mahdollista laittaa tarpeen tullen.

4.2.2 Palvelimet hyöty- ja testikäyttöön

Verkossa on kuusi palvelinta. Niitä ovat Irwin-reititinpalvelin, Shell-palvelin Tulppaani, Allonen-varmuuskopiopalvelin, Cacti-palvelin CCT sekä Leijona, jossa on TTD-pelipalvelin. Näiden lisäksi verkkoon tuli uusi palvelin nimeltä Palsu, joka ylläpitää LFS-autosimulaattoripalvelinta.

CCT-palvelimen Cacti-sovellus mahdollistaa SNMP:tä hyväksikäyttäen muiden koneiden tilantarkkailun ja siten lisää verkon ja laitteiden vikasietoisuutta, kun mahdolliset laitehajoamiset voidaan ennaltaehkäistä. Seuraavassa kappaleessa selvitetään enemmän SNMP:stä.

Kk4-verkkoon lisättiin 6.3.2012 uusi palvelin nimeltä Palsu. Se ylläpitää Live For Speed -autosimulaattoripalvelinta eli LFS-palvelinta. Se on ainoa palvelin Kk4-verkossa, jonka käyttöjärjestelmänä ei ole Linux-jakelu. Palsun palvelut toimivat Windows XP -ympäristössä, koska LFS-palvelinohjelmistoa ei ole vielä tehty Linuxille yhteensopivaksi.

Taulukosta selviää, kuinka Palsu on ainoa Windows-käyttöjärjestelmää käyttävä tietokone, muiden palvelimien pohjautuessa Linux-pohjaiseen Debian-jakeluun (taulukko 4).

TAULUKKO 4. Kk4-verkon palvelimet

Nimi	Toiminta	Käyttöjärjestelmä	Kernel	Prosessori	RAM	Kiintolevy	IP-osoite
Irwin	Palomuuri/GW	Debian	2.6.32-5	P(D) E2160	1GB	72GB	192.168.100.1
Tulppaani	Shell	Debian	2.6.32-5	P4 2.4GHz	3GB	1.5TB(RAID1)	192.168.100.10
Allonen	Varmuuskopiointi	Debian	2.6.32-5	Athlon 2GHz	512MB	1.5TB	192.168.100.11
cct	Cacti	Debian	2.6.26-2	Celeron 1.5	512MB	72GB	192.168.100.12
Leijona	OpenTTD	Debian	2.6.32-5	P4 3.2Ghz	1.5GB	15GB+NFS	192.168.100.20
Palsu	LFS	Win XP Pro	5.1.2600	P4 3.0GHz	1GB	120GB+CIFS	192.168.100.21

4.2.3 Tietojen keräämistä SNMP-palvelun avulla

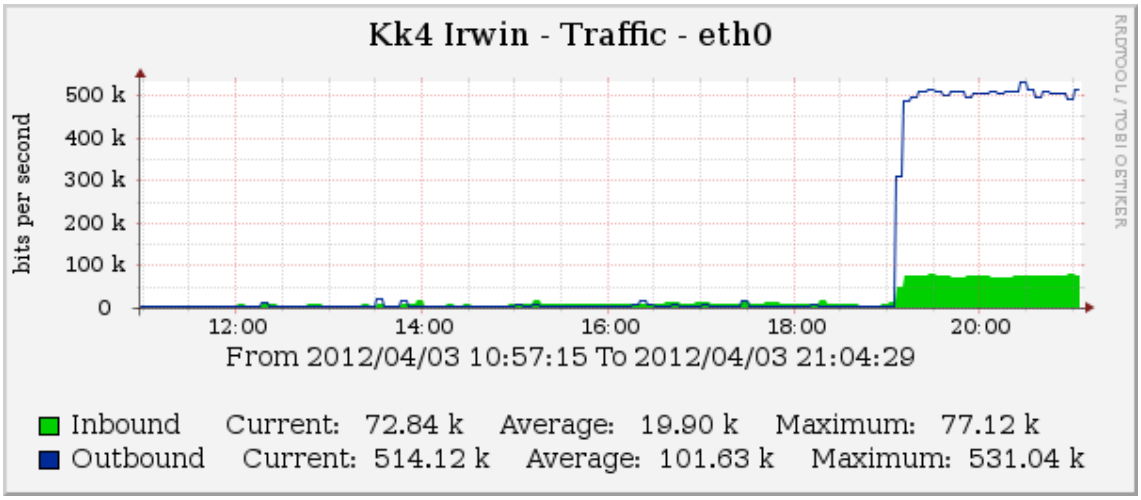
Tässä kappaleessa esitellään hieman verkossa toimivaa Cacti-palvelinta, jolla voidaan monitoroida muita palvelimia ja verkkolaitteita. Palvelimeen on asennettuna Cacti-ohjelma, joka pyytää kohdekoneilta tietoja SNMP:n avulla niiden laitteistosta ja halutuista tiedoista. Alla on kuvakaappaus Cacti-ohjelmasta CCT-palvelimelta.

Kuvassa 8 näkyy verkkotietoja halutuista laitteista. Tietoja ovat: IP-osoite, viive, edellinen yhteyskatkos sekä luotettavuus. Näillä tiedoilla pystytään hyvin tarkkailemaan, jos verkossa ilmenee ongelmia. Edellisestä yhteyskatkoksesta ja luotettavuudesta nähdään, kuinka hyvin laite pysyy toimintakunnossa ja onko itse verkko toiminut oikein. Viiveen muutoksista voidaan nähdä, jos laitteessa tai verkossa muodostuu solmukohtia. Usein myös itse reitittimen tai modeemin ohjelmisto voi mennä sekaisin ja aiheuttaa viiveitä tai katkoksia.

KUVA 8. SNMP-tietoja (Petteri Wahlroos 1, muokattu)

Näiden tietojen lisäksi voidaan myös yksittäisiä koneita tarkastella tarkemmalla tasolla. Seuraavissa kuvissa on esimerkiksi otettu SNMP-tietoja Irwin-palvelimesta. Ensimmäisessä kuvassa on kuvaaja palvelimen verkkoliikenteestä (kuva 9).

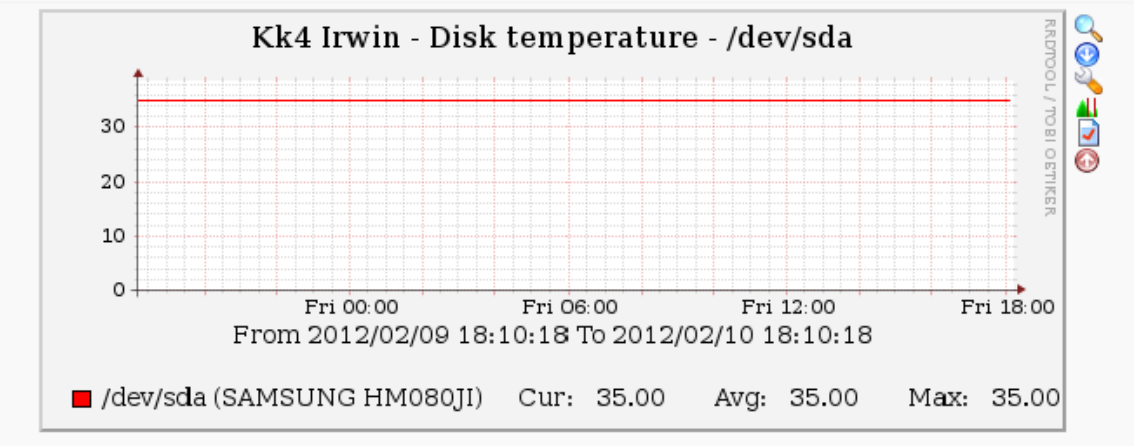
Alla olevassa kuvassa näkyy palvelimen läpimenevä verkkoliikenne kokonaisuutena sekä sisään- että ulospäin. Kuvassa sininen kuvaaja on ulospäin oleva liikenne, eli sisäverkosta internetiin ja vihreä kuvaaja on liikenne sisäänpäin sisäverkkoon Internetistä. Kuvassa näkyy hyvin kuinka siirtonopeudet kasvavat, kun tiedonsiirto aloitetaan noin kello 19. (kuva 9).



KUVA 9. Irwinin verkkoliikenne (Petteri Wahlroos 2)

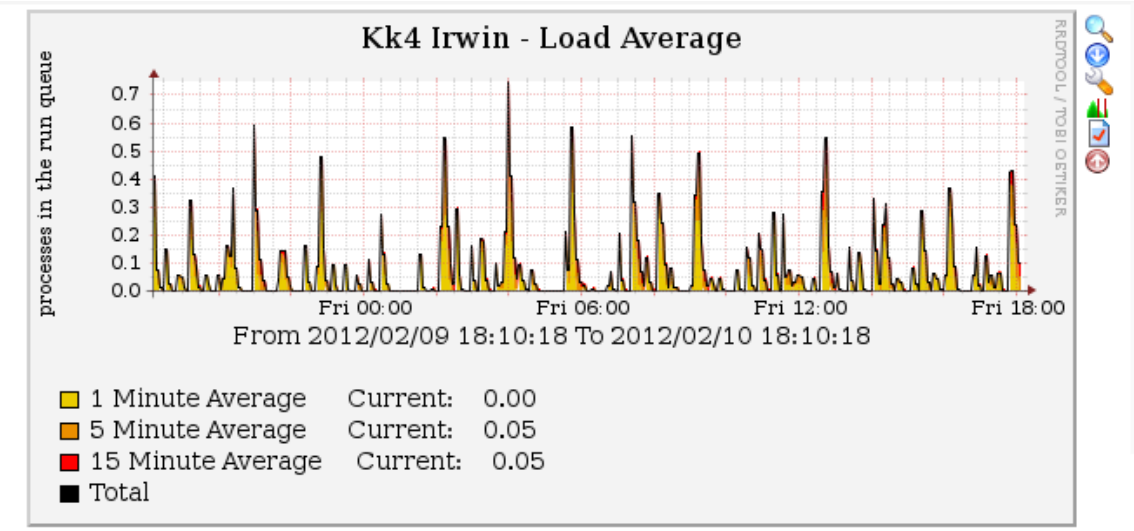
SNMP:llä voidaan tutkia muitakin tietoja kuin laitteen verkkotietoja, kuten ruuhkaa, liikennettä ja viiveitä. Sillä voidaan myös laitetasolla tutkia ja seurata palvelimen kuntoa ja tilaa. Alla olevissa kuvissa on tietoja palvelimen kiintolevyn lämpötilasta sekä tietokoneen kuormituksesta (kuvat 10 ja 11).

Kiintolevyn lämpötilakuvaajasta voidaan helposti huomata vikatilanteet. Näin niihin pystytään ennakoimaan ja vaihtamaan uusi toimiva kiintolevy viallisen tilalle ennen kuin hajoava levy aiheuttaa vahinkoa järjestelmälle (kuva 10).



KUVA 10. Irwinin kiintolevyn lämpötila (Petteri Wahlroos 2, muokattu)

Alla oleva kuva havainnollistaa, kuinka paljon tietokoneella on kuormaa. Kuorma ei ole vain prosessorin suorittamat työt vaan koko tietokoneen laitteiston rasitus. Jos prosesseja jää kovalevylle tai RAM-muistiin prosessoitavaksi, niin nekin nostavat load averagea eli keskivertokuormitusta (kuva 11).



KUVA 11. Irwinin-palvelimen rasitus (Petteri Wahlroos, muokattu)

5 POHDINTA

Verkkokaavio onnistui erittäin hyvin ja auttaa yritystä mahdollisissa tulevissa verkko-ongelmissa. Kaavio on selkeä ja helppolukuinen. Tähän opinnäytetyöhön laitettiin hieman muokattu versio siitä, koska alkuperäisen verkkokaavion asetelma oli liian leveä opinnäytetyön sivuasetteluun. Verkkokaavio on siis tiivistetty Microsoft Wordin takia.

Pohjakuva oli kuvista vaikeampi, koska moni laite sijaitsee samassa paikassa, joten kuvan saaminen selkeäksi oli hankalaa. Siinä kuitenkin onnistuttiin hyvin ja kuvasta saa selville tärkeimmät asiat helposti.

Suuri osa lähteistä on erittäin luotettavista internetsivuista, tunnetuista yrityksistä ja oppikirjallisuudesta. Tekstistä suuri osa on opinnäytetyön kirjoittajan omista opinnoista omaksumiaan tietoa.

Topologiakuvan eli verkkokaavion tekeminen oli melko helppoa vaikka olikin aikaa vievää. Työssä tarvittiin kaksi henkilöä, jotta kerroksesta toiseen ulottuvat kaapelit saatiin selville ja merkittyä työhön oikein.

Isommassa verkossa olisi voinut käyttää verkkokaapeleiden mittaustyökaluja. Niillä olisi saanut selville kaapeleiden kunnon ja kaikki standardissa olevat vaatimukset. Tässä työssä mittauksia ei kuitenkaan ollut tarpeellista tehdä.

LÄHTEET

Lauri Suoranta. 2008. Reititin ohjaa perille. Tietokone. Luettu 20.3.2012. http://www.tietokone.fi/lehti/tietokone_5_2008/reititin_ohjaa_perille_841

Microsoft Corporation. Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla? Luettu 20.3.2012. http://windows.microsoft.com/fi-FI/windows-vista/How-do-hubs-switches-routers-and-access-points-differ

Viestintävirasto. 2007. Palomuuri. Luettu 20.3.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html

CSC — Tieteen tietotekniikan keskus Oy. IP-osoitteiden hallinnointi. Luettu 20.3.2012. http://www.csc.fi/hallinto/funet/palvelut/dns/ip

Internet Assigned Numbers Authority. Introducing IANA. Luettu 22.2.2012. http://www.iana.org/about/

Tampereen sähköpalvelu Oy. Parikaapelointi. Luettu 22.2.2012. http://www.tsp.fi/pdfs/parikaapelointi.pdf

Microsoft Oy. DHCP (Dynamic Host Configuration Protocol) Basics. 27.2.2007. Luettu 22.2.2012. http://support.microsoft.com/kb/169289

Cisco Systems, Inc. CCNA: Network Media Types. 14.3.2003. Luettu 22.2.2012. http://www.ciscopress.com/articles/article.asp?p=31276

Tec Datawire. Cat5, Cat5e, Cat6 and Cat7 Patch Cables. Luettu 22.2.2012. http://www.tecdatawire.com/catspec.html

Hyperline 1. Luettu 2.4.2012. http://www.hyperline.com/catalog/cable/utp-c6-patch-gy.shtml

Hyperline 2. Luettu 2.4.2012. http://www.hyperline.com/catalog/cable/ftp-c5e-s.shtml

Hyperline 3. Luettu 2.4.2012. http://www.hyperline.com/catalog/cable/stp4_c6_solid_indoor.shtml

Hyperline 4. Luettu 2.4.2012. http://www.hyperline.com/catalog/cable/sstp4_10gbe_solid_indoor.shtml

SuomiCom. Laajakaistavertailu auttaa sinua valitsemaan tarpeisiisi sopivan laajakaistan. Luettu 30.3.2012. http://www.suomicom.fi/laajakaistavertailu.php

Viestintävirasto. 2007. VPN. Luettu 2.4.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html

netfilter.org. The netfilter.org project. Luettu 22.2.2012. http://www.netfilter.org/

IEEE 802.1d STP (Spanning tree -protokolla) Luettu 20.3.2012. http://www.tlu.ee/~matsak/telecom/lasse/spanning_tree_algorithm/ieee_8021d_stp_spanning_tree_protokolla.html

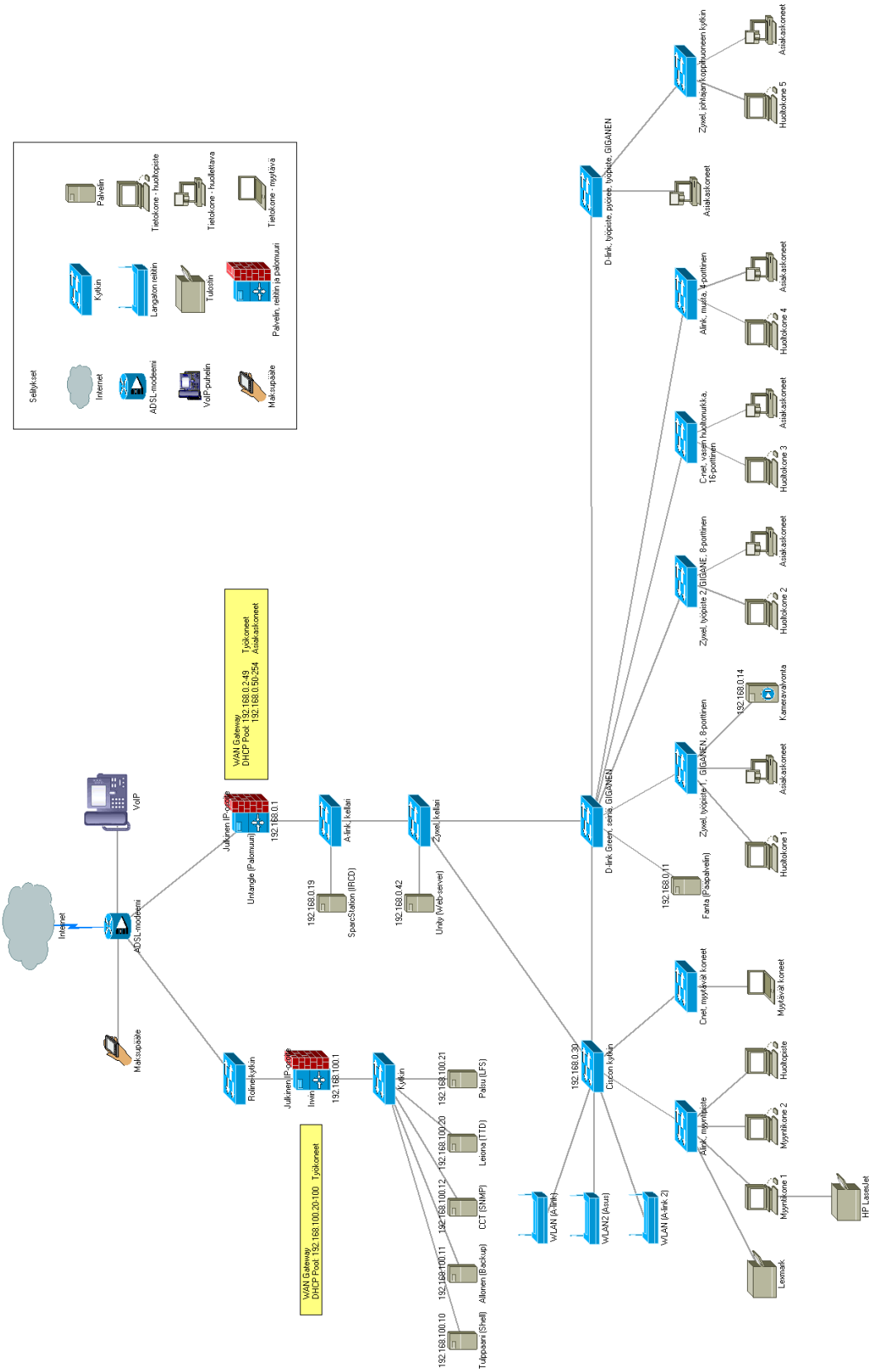
Petteri Wahlroos 1. Luettu 22.2.2012. http://kk4.fi/u/1328890507_cct.png

Petteri Wahlroos 2. Luettu 22.2.2012. http://kk4.fi/u/irwingraph.png

Diane Teare. 2010. Cisco Systems, Inc. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Cisco Press: Indianapolis, USA 2010. ISBN-13: 978-1-58705-882-0

LIITTEET

Liite 1. PC-Räätälin verkkokaavio



Liite 2. PC-Räätälin verkon pohjakuva