TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma, tietokonetekniikka
Pasi Järveläinen

Tutkintotyö

Pasi Järveläinen

FICI-COPY KY:N LÄHIVERKON JA ESITTELYTILAN SUUNNITTELU SEKÄ TOTEUTUS

Työn valvoja: Kai Poutanen

Työn ohjaaja: Fici-Copy Ky, Laila Tuomi

Tekijä:	Pasi Järveläinen
Työn nimi:	Fici-Copy Ky:n lähiverkon ja esittelytilan suunnittelu sekä toteutus
Päivämäärä:	19.04.2006
Sivumäärä:	56 sivua + 12 liitesivua
Hakusanat:	Lähiverkko, Esittelytila, WLAN, Tulostus, Skannaus, Tietoturva
Koulutusohjelma:	Tietotekniikka
Suuntautumisvaihtoehto:	Tietokonetekniikka
Työn valvoja:	Kai Poutanen
Työn ohjaaja:	Laila Tuomi Fici-Copy Ky

Tämän tutkintotyön tavoitteena oli suunnitella ja toteuttaa työn toimeksiantajalle Fici-Copy Ky:lle toimiva ja käyttökelpoinen lähiverkkojärjestelmä sekä laitteiden esittelytilat. Fici-Copy toimii Hämeenlinnan alueella Konica Minoltan jälleenmyyjänä. Lähiverkko kattaa Fici-Copyn toimiston sekä varaston. Lisäksi verkkoon liitetään Konica Minoltan monitoimilaitteita, joiden ominaisuuksia esittelytilassa voidaan testata.

Tutkintotyössä toteutetaan toimistotiloihin lähiverkko, joka korvaa vanhan olemassa olevan verkon kokonaisuudessaan. Työssä selvitetään myös yleisiä lähiverkkotekniikoita ja lähiverkossa olevia aktiivilaitteita sekä palvelimen asennusta ja Konica Minolta monitoimilaitteiden toimintaa esittelytilassa. Myös tietoturva on esillä niin langattoman kuin kiinteänkin verkon toteutuksessa. Lisäksi käsitellään erilaisia verkon nimipalveluja sekä verkon yleistä suunnittelua ja ylläpitoa.

Teoria siirtyy käytäntöön verkon eri toteutusvaiheiden kautta. Verkon asennuksen pohjalta toteutetaan myös uusi toimiva esittelytila Konica Minoltan monitoimilaitteilla.

Author:	Pasi Järveläinen
Name of the Thesis:	Planning and realizing a local area network and showroom to Fici-Copy, LP
Date:	19.04.2006
Number of pages:	56 pages + 12 appendices
Keywords:	Local Area Network, Showroom, WLAN, Printing, Scanning, Data Security
Degree program:	Computer systems engineering
Specialisation:	Computer technology
Supervisor:	Kai Poutanen
Director:	Laila Tuomi Fici-Copy, LP

The objective of this work was to plan and implement a functional local area network system and showroom to the commissioner of this thesis, Fici-Copy, LP. Fici-Copy operates in Hämeenlinna area as a Konica Minolta dealer. Local area network (LAN) covers Fici-Copy´s office and warehouse. Konica Minolta multi functional products are also added to the network. It is possible to test the characteristics of these products in the showroom.

The main purpose of the thesis was to execute a local area network, which completely replaces the old one. Thesis clarifies general local area network techniques and the devices, which are connected to network. Data security is also present when implementing both wireless and landline network. In addition, different name services, planning and maintenance of the network are discussed in the work.

Different implementation phases of the network turn the theory into practise. Also a new functioning showroom with Konica Minolta multi functional products is accomplished on the ground of the net.

ALKUSANAT

Tämä tutkintotyö on tehty toukokuun 2005 ja joulukuun 2005 välisenä aikana Fici-Copy Ky:lle. Olen toiminut kyseisen yrityksen palveluksessa kohta viisi vuotta. Insinöörityöni aihe uuden verkon rakentamisesta sai alkunsa yrityksen johdolta, joka ei ollut tyytyväinen vanhan verkon toimintaan. Sain monilta osin vapaat kädet toteuttaa uuden lähiverkon ja omat kokemukseni vanhasta verkosta auttoivat myös uuden rakentamisessa. Tutkintotyöni perusajatuksena oli saada verkkoratkaisut toteutettua siten, että päivittäisten perustöiden kuten laskutuksen, kirjanpidon ja huoltoseurannan teko olisi mahdollisimman helppoa ja verkko kattaisi yrityksen toimitilat kokonaisuudessaan. Samalla esittelyssä olevien monitoimilaitteiden ominaisuuksien testauksen tulisi olla helppoa sekä kattavaa.

Tampereella 19. huhtikuuta 2006

_____

Pasi Järveläinen

SISÄLLYSLUETTELO

LYHENNELUETTELO

LAN	Local Area Network, Lähiverkko
NetBIOS -nimi	Network Basic Input Output System Names, Tietokoneen nimi lähiverkossa
CSMA/CD	Carrier Sense Multiple Asses / Collision Detection, Vuoronvaraus tekniikka Ethernet verkossa
VLAN	Virtual Local Area Network, Virtuaalinen lähiverkko
TCP/IP	Transmission Control Protocol / Internet Protocol, Ethernet verkossa käytettävä protokolla
IANA	Internet Assigned Numbers Authority, IP-osoitteiden jakamisesta huolehtiva organisaatio
DNS	Domain Name System, Nimipalvelu, joka yhdistää IP-osoitteen nimeen
WINS	Windows Internet Name Service, Nimipalvelu, joka yhdistää NetBIOS-nimen IP-osoitteeseen
DHCP	Dynamic Host Configuration Protocol, Palvelu, joka tarjoaa automaattiset IP-osoitteet
NAT	Network Address Translation, Palvelu, joka muuttaa julkisen IP-osoitteen intraosoitteiksi
MAC	Media Access Control, Verkossa olevan laitteen henkilökohtainen valmistusvaiheessa määritelty osoite

WLAN	Wireless Local Area Network, Langaton lähiverkko
SSID	Service Set ID, Langattoman verkon nimi
WPA	Wireless Fidelity Protected Access, Langattoman verkon salaustekniikka
WEP	Wired Equivalence Privacy. Langattoman verkon salaustekniikka
IEEE	Institute of Electrical and Electronics Engineers, Sähkö-, tietokone- ja tietoliikenneinsinöörien yhdistys, joka kehittää alaansa liittyviä standardeja
SMTP	Simple Mail Transfer Protocol, TCP-pohjainen protokolla, jota käytetään sähköpostin lähettämiseen
SNMP	Simple Network Management Protocol, TCP/IP-verkkojen hallintaan käytettävä protokolla
MIB	Management Information Base, Laitteessa oleva tietokanta, jota SNMP käyttää
OID	Object Identifier, MIB tietokannassa olevien tietojen polku
RAID	Redundant Array of Independent Disks, Tekniikka, jolla parannetaan tietokoneiden vikasietoisuutta tai nopeutta
PCL	Printer Control Language, Tulostus- ja sivunkuvauskieli
PS	PostScript, Tulostus- ja sivunkuvauskieli
SMB	Server Message Block, Protokolla, joka mahdollistaa tiedostojen luku- ja kirjoitusoikeudet

FTP	File Transfer Protocol, Tiedonsiirtoprotokolla
TWAIN	Technology Without An Interesting Name, Standardi, jolla skannerit pystyvät siirtämään tietoa ohjelmasovelluksiin
HDD	Hard Disk Drive, Kovalevy
URL	Uniform Resource Location, Osoitepolku tietokoneessa
LPR	Line Printer Remote, Tulostuksessa käytettävä portti
SATA	Serial ATA, Kovalevyn liityntä
PCI	Peripheral Component Interconnect, Tietokoneen emolevyllä oleva liityntäpaikka lisäkorteille
AGP	Accelerated Graphics Port, Tietokoneen emolevyllä oleva liityntäpaikka näytönohjaimelle

1 JOHDANTO

Lähiverkot ovat arkea yrityksen jokapäiväisessä toiminnassa. Ne kuuluvat olennaisena osana yritysten tiedonsiirtoon niin työntekijöiden- kuin toistenkin yritysten välillä. Lähiverkon käyttötarkoitus määrittelee siinä käytettävät laitteistot sekä ohjelmat. Onkin syytä harkita tarkkaan, kuinka paljon on kannattavaa sijoittaa verkkoon sen tuomaan kokonaishyötyyn nähden, sillä verkko vaatii jatkuvaa ylläpitoa uusien tekniikoiden ja ohjelmien käyttöönotossa. Sen käyttäminen on tehtävä helpoksi, jotta se onnistuu tavalliselta käyttäjältä, jolla ei ole monen vuoden koulutusta tietotekniikasta.

Yhteiskunnan nopea verkottuminen asettaa tiedon turvaamiselle uuden näkökulman. Langattomat verkot ovat yleistyneet nopeasti, monia töitä tehdään etätyönä ja tietoverkkoihin murtautumiset ovat lisääntyneet huomattavasti. Tällöin verkossa liikkuva data on aina syytä salata, ja yrityksen verkoista on tehtävä rakenteellisesti sellaisia, että niihin on vaikea murtautua. Samalla verkkoon liitettävät laitteet ovat tulleet yhä monimutkaisemmiksi ja niihin on tullut paljon uusia ominaisuuksia. On tavallista, että sama laite sekä tulostaa, kopioi, faksaa että skannaa.

Fici-Copy Ky on Hämeenlinnan ja sen lähikuntien kuten esimerkiksi Hattulan, Rengon ja Janakkalan alueella toimiva Konica Minoltan (Konica Minolta Business Partner Finland Oy) jälleenmyyjä. Se on kommandiittiyhtiömuotoinen pk-yritys, joka on perustettu vuonna 2000. Yrityksen toimistotilat sijaitsevat Hämeenlinnan keskustassa. Näihin tiloihin yritys muutti keväällä 2005 lisääntyneet tilantarpeen vuoksi. Yritys toimii IT-alalla myyden sekä huoltaen pääsääntöisesti Konica Minoltan toimistolaitteita. Yritys myy myös erilaisia tietotekniikkalaitteita, sekä rakentaa ja ylläpitää lähiverkkoja. Kaupankäynti keskittyy pääasiassa business to business- eli yrityskauppaan.

2 LÄHIVERKKO

Tietoliikenteessä maantieteellisesti rajatun pienen alueen sisäistä tietoliikennettä sanotaan lähiverkoksi, josta voidaan käyttää myös nimitystä LAN (Local Area Network). Tavallisesti lähiverkko on yhden organisaation hallinnassa, mutta verkko voi olla myös ulkopuolisen tahon vuokraama tai ylläpitämä. /1, s. 4; 2, s.4-7/

Lähiverkko koostuu verkossa olevista erillisistä työasemista, palvelimista, verkon aktiivilaitteista ja kaapeloinnista. Lähiverkon yksi keskeisimmistä tehtävistä on tarjota verkon käyttäjille jaettuja resursseja. Tällaisia ovat esimerkiksi tiedosto-, ohjelmisto- ja oheislaitejaot. Tiedostojen jakamisesta huolehtivat tiedostopalvelimet, jotka jakavat niin sanottuja jaettuja hakemistoja käyttäjille. Tulostuspalvelin on tärkein ja eniten käytetty oheislaitteiden jakoon erikoistunut palvelintyyppi. Palvelin hoitaa tulostimen jaetun tulostusjonon ylläpidon. /1, s. 4; 2, s.4-7/

Nykyaikaisessa lähiverkossa nimi- ja verkonselauspalvelut kuuluvat myös verkon peruspalveluihin. Tieto kulkee lähiverkossa koneelta toiselle niin sanottujen fyysisten osoitteiden perusteella. Näitä osoitteita kutsutaan MAC-osoitteiksi, jotka ovat laitteisiin jo valmistusvaiheessa määriteltyjä yksilöllisiä osoitteita. Tavallisen käyttäjän kannalta MAC-osoitteet eivät sovellu lähetettävän tiedon vastaanottajan määrittämiseen, koska niitä on liian vaikea muistaa. /1, s. 4; 2, s.4-7/

Lähiverkon koneille annetaan yleensä asennusvaiheessa NetBIOS-nimi, jolla fyysisen osoitteen sijaan voidaan koneeseen viitata nimen perusteella. Nimi-osoite-parit ovat talletettuina lähiverkossa palvelimelle, joka on erikoistunut nimi-osoite-parien tallennukseen. Tällöin kaikki muut lähiverkossa olevat koneet voivat hakea aktiivisten koneiden nimi- ja osoitetiedot kyseiseltä palvelimelta. Palvelimelle on tehty myös verkon selauspalveluja, joiden avulla käyttäjät voivat listata verkossa olevan laitekannan. Selauspalvelut myös ryhmittelevät koneet esimerkiksi työryhmittäin tai toimialueittain. /1, s. 4; 2, s.4-7/

2.1 Lähiverkon historia

Ethernetin eli lähiverkkotekniikan historia on kestänyt jo lähes 30 vuotta. Voidaan katsoa, että Ethernet syntyi 1960-luvun lopulla Havaijin yliopistossa keksityn ALOHA-radioverkon pohjalta. Tuonaikaisesta 4 800 bit/s:n tiedonsiirtonopeudesta on tultu nykyiseen 1 000 Mbit/s:n nopeuteen kuparikaapeleilla ja 10 000 Mbit/s:n nopeuteen valokuitukaapeleilla toteutetuissa siirtotekniikoissa. Verkkojen toiminnallinen perusperiaate on kuitenkin sama kuin ALOHA-verkossa. /1, s.9-10/

2.1.1 Ethernet, 10 Mbps

Tiedonsiirtonopeudet ovat kasvaneet jatkuvasti ja nykyään 10 Mbit/s:n verkot ovat jäämässä kokonaan pois. Silti monet uudet aktiivilaitteet tukevat vielä 10 Mbit/s:n tiedonsiirtonopeutta. Alussa 10 Base-2 ja 10 Base-5-verkkoja rakennettiin koaksiaalikaapelilla, mutta uusimmissa 10 Base-T-verkoissa alettiin käyttää kierrettyjä parikaapeleita. Koaksiaalikaapelilla toteutettu verkko oli yleisesti toiminut väylätopologialla, mutta parikaapelissa käytetään tähtitopologiaa, jossa verkon keskipisteenä on jokin aktiivilaite. Parikaapelin pituus saa olla maksimissaan 100 metriä. Käytännössä ristikytkentäkaapilta verkkorasialle on varattu 90 metriä ja ristikytkentä- ja työasemakaapeleille loput 10 metriä. Parikaapelin pitää olla kategorian 3, 4 tai 5 mukaista. Kaapeleilla on omat standardit, joiden mukaan niiden kategoriat määräytyvät. Standardit määrittelevät vähimmäisvaatimukset, jotka kaapelin pitää täyttää, esimerkiksi kaistanleveyden. Kaapelista käytetään yleensä nimenä sen kategoriaa eli esimerkiksi kategorian 5 kaapeli on Cat5. /5, s66/

2.1.2 Ethernet, 100 Mbps

Tämän hetken yleisin lähiverkkokaapelointi on 100 Mbit/s:n siirtonopeuteen pystyvä 100Base-TX. Verkko on myös tähden mallinen ja sen keskipisteenä

toimii usein kytkin. Kaapelin maksimipituus on 100 metriä ja se sisältää työasema- ja ristikytkentäkaapelit. Kaapelointi on toteutettava vähintään kategorian 5 kaapelilla. Cat5-kaapeli on mahdollistanut kaksisuuntaisen tiedonsiirron (full dublex) perinteisen yksisuuntaisen (half dublex) lisäksi. Verkko on yhteensopiva vanhemman 10 Base-T:n kanssa, joten siirtyminen uuteen nopeuteen on käynyt helposti. Kaapelista on tullut myös uusien testausstandardien takia uusi versio, joka on nimeltään Cat5e. Käytännössä se on samaa kaapelia kuin Cat5-kaapeli, mutta täyttää standardivaatimukset. Uusin käytössä oleva kaapeliversio on Cat6-kaapeli, joka antaa entistä pidemmän eliniän kaapeloinnille. Cat6-kaapelin taajuuskaistan ylärajaa on myös nostettu 250 MHz:iin, kun se Cat5e-kaapelissa oli 100 MHz. Taajuuskaistan kasvattaminen on antanut tilaa uusille sovelluksille ja toimintavarmuutta nykyisille. 100 Base-TX käyttää kaapelin neljästä parista vain kahta. /5, s70; 22; 23; 24/

2.1.3 Ethernet, Gigabit

Lähiverkoissa 1 Gbit/s:n siirtonopeudet ovat alkaneet tulla yhä yleisemmiksi. Ennen 1Gbit/s:n nopeutta käytettiin vain verkkojen runkolinjoissa reitittimien ja muiden aktiivilaitteiden yhdistämiseksi, mutta nykyään sitä käytetään jo työasemien liityntänä. Gigabitin tekniikkaan on standardisoitu kaksi eri mallia. Toinen on Cat5e tai Cat6 kuparikaapelissa toimiva 1000Base-T ja toinen on 1000Base-SX, jota käytetään lyhyissä kuituyhteyksissä. 1 Gbit/s:n kaapelointi on myös sitä hitaampiin yhteyksiin yhteensopiva eli samalla kaapeloinnilla voidaan käyttää myös 100 Mbit/s:n ja 10 Mbit/s:n nopeuksia. 1 Gbit/s käyttää parikaapelista kaikkia neljää paria. /22; 23/

2.1.4 Ethernet, 10 Gigabit

10 Gbit/s:n yhteydet on toteutettu valokuiduilla. Standardi on IEEE 802.3ae, joka määrittelee yhteensä seitsemän erilaista mediatyyppiä, jotka kaikki ovat kuituja. Tavoitteena on myös toteuttaa 10 Gbit/s:n nopeus parikaapelissa. IEEE

olettaa saavansa 10GBase-T-standardin ratifioitua heinäkuuhun 2006 mennessä. Tarkoitus on saada 10GBase-T toimimaan Cat6-kaapelissa 55-100 m ja Cat7-kaapelissa vähintään 100 m. /24; 22/

2.2 Arkkitehtuuri

Jonkin aikaa oli samanaikaisesti käytössä kaksi kilpailevaa lähiverkkotekniikkaa, IBM:n kehittämä Token Ring sekä DEC:n, Intelin ja Xeroxin kehittämä Ethernet. Token Ring -verkko perustuu kiertävään tokeniin, joka on valtuus verkon hallintaan eli tällöin tokenin omistama asema voi lähettää tietoa verkkoon. Token-verkossa ei voi tapahtua törmäyksiä, ja sen siirtoon kului paljon aikaa, minkä vuoksi sen käyttö lähiverkoissa jäi toissijaiseksi./1, s12/

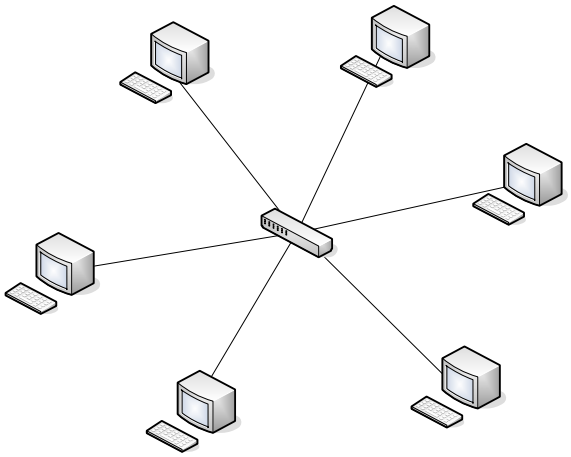
Ethernet-verkko perustuu CSMA/CD-vuoronvarausmenettelyyn. CSMA/CD on kilpavarausmenetelmä, jossa lähettävä asema kuuntelee, onko siirtotie varattu. Jos siirtotie on vapaa, asema alkaa lähettää tietoa. Periaatteessa kaikilla asemilla on oikeus aloittaa lähetys. Kahden aseman samanaikainen tiedonlähetys synnyttää törmäyksen. Lähettävä asema huomaa törmäyksen, odottaa hetken ja lähettää tiedon uudestaan. Lähiverkossa, jossa on useita työasemia, syntyy helposti törmäyksiä. Törmäyksien vuoksi lähiverkon maksimitiedonsiirtonopeus pienenee, mutta tässäkin tapauksessa Ethernet on Token Ring-tekniikkaa nopeampi. /13, s17; 14/

2.2.1 Topologiat

Koneiden välistä tietoliikennettä voidaan tarkastella kahdella tasolla. Fyysinen taso määrittelee koneiden välisen kaapeloinnin toteutuksen ja looginen taso tiedonkulun koneelta toiselle. Lähiverkossa käytetyin topologia on tähti. Muita topologioita ovat väylä ja rengas. Nykyaikaisessa verkossa käytetään fysikaalisella tasolla tähtikaapelointia, joka toimii loogisella tasolla väylänä. /2, s.68/

Tähti

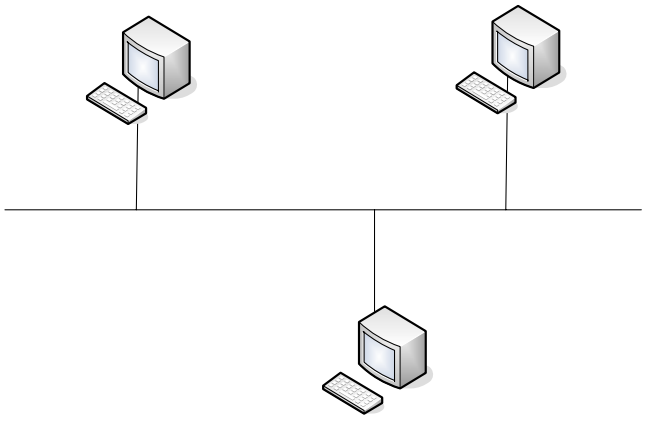
Tähtikytkennässä laitteet ovat toisiinsa yhteydessä yhteisen keskipisteen kautta (kuva 1). Kytkentä muodostaa tähteä muistuttavan kuvion, josta se on saanut nimensä. Tähden keskipisteenä on jokin aktiivilaite, esimerkiksi keskitin (hub), kytkin (switch) tai reititin (router). /2, s.70/



Kuva 1 Tähtirakenne

Väylä

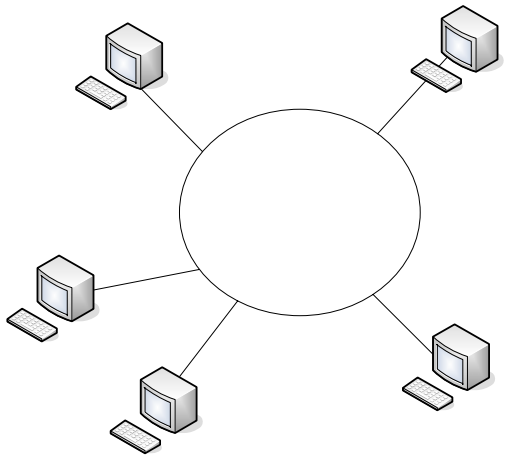
Väylärakenteisessa verkossa kaikki laitteet liittyvät samaan siirtokanavaan (kuva 2). Tieto kulkee väylässä kaikkiin suuntiin ja väylä voi olla teoriassa äärettömän pitkä. Tällöin tietoa ei tarvitse poistaa väylästä. Käytännössä äärettömän pitkä kaapeli saadaan tehtyä kaapelin päätevastuksilla eli terminaattoreilla. /2, s.69/



Kuva 2 Väylärakenne

Rengas

Rengastopologiassa laitteet ovat liitettyinä renkaaksi (kuva 3). Tieto siirtyy tiettyyn suuntaan kulkien vuoron perään jokaisen laitteen läpi. Lähetettävä tieto on poistettava verkosta. Käytännössä lähettävä kone poistaa kehyksen, jos se palaa takaisin siihen. /2, s.69/



Kuva 3 Rengasrakenne

2.2.2 Aktiivilaitteet

Vaimeneminen on signaaleja siirrettäessä merkittävä tekijä. Vaimenemista on sitä enemmän, mitä pidempi käytetty kaapeli on. Haluttaessa kuljettaa signaalia pitkiä matkoja, on sitä välillä vahvistettava. Lähiverkoissa, joissa ei ole reititystä aktiivilaitteella, on kaksi tehtävää: vahvistaa signaalia ja estää jälkitörmäysten synty. /2, s81/

Toistin (hub)

Toistin on laite, joka toistaa sille tulevan signaalin eteenpäin. Ethernet-verkossa toistimet ovat moniporttisia. Toistimen toimintaperiaate on lähettää data kaikkiin muihin portteihin paitsi siihen, mistä se on alun perin tullut. Verkossa olevat koneet voivat verkko-osoitteen perusteella päätellä, onko kyseinen data tarkoitettu juuri tälle koneelle. Toistimien tietoturva on huono, koska signaali lähetetään jokaiseen porttiin. Myös runsasliikenteisessä verkossa toistimen tie-

donsiirtonopeus pienenee huomattavasti verkossa tapahtuvien törmäysten johdosta. /2, s81-82/

Toistimet tukevat usein myös eri nopeuksia. Näitä toistimia kutsutaan DUAL-SPEED-toistimiksi ja ne koostuvat kahdesta toistimesta ja niitä yhdistävästä sillasta. Erinopeuksiset toistimet toimivat itsenäisesti, ja niiden välissä oleva silta välittää liikenteen toistimille. Silta puskuroi dataa, jolloin se voi yhdistää erinopeuksiset toistimet yhteen. Yleensä DUAL-SPEED-toistimissa on automaattinen nopeuden tunnistus eli auto negotiation, jolloin laitteet voivat keskenään sopia välillään käytettävän liikennöintinopeuden. Toistimet tukevat yleensä nopeuksia 10 Mbps ja 100 Mbps. 1Gbps:n yhteyksiä ei toteuteta toistimilla. Toistimet ovat kuitenkin alkaneet hiljalleen jäädä pois lähiverkoista, koska tilalle ovat tulleet kytkimet. /13, s53-54/

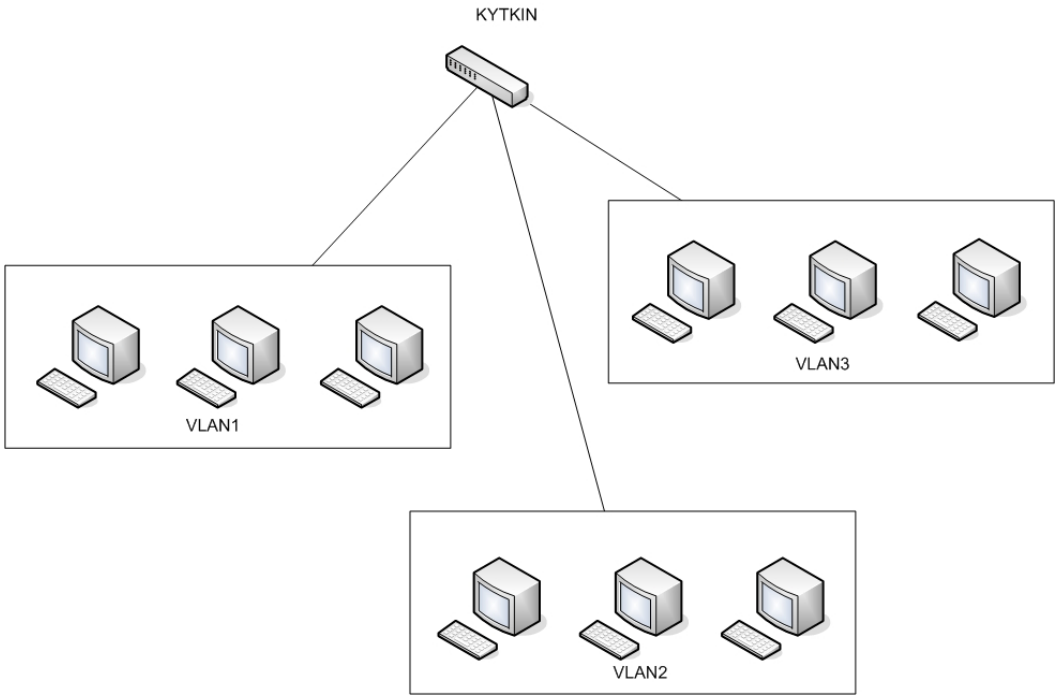
Kytkin (switch)

Verkon ollessa rakenteeltaan tähtiverkko sen tärkein aktiivilaite on kytkin. Kytkin yhdistää toisiinsa verkkoja. Käyttämällä kytkintä tähtikytkentäisessä verkossa voi jokainen työasema perustaa oman verkon, jonka kytkin yhdistää. Käyttämällä aktiivilaitteena kytkintä ei Ethernetissä tällöin ole enää koneille tyypillistä yhteistä väylää. Kytkimen toimintaperiaate on lähettää data ainoastaan siihen porttiin, josta kohdeosoite löytyy. Kytkin opettelee sen porteissa olevien koneiden IP-osoitteet ja tallentaa ne keskusmuistissa olevaan taulukkoon. Tämän ominaisuuden perusteella kytkin osaa tehdä välityspalvelun. /13, s57;2, s84-85/

Kytkimen tietoturva on paljon parempi verrattuna toistimeen, koska data lähetetään ainoastaan sille tietokoneelle, jolle se on tarkoitettu. Lähes kaikki kytkimet tukevat useaa tiedonsiirtonopeutta ja nopeudet ovat tyypillisesti 10 Mbps / 100 Mbps. Lähiaikoina on markkinoille kuitenkin tullut myös 10 Mbps / 100 Mbps / 1 Gbps kytkimiä. Kytkinten mediat voivat myös vaihtua esimerkiksi parikaapelista optiseen kuituun. /13, s57;2, s84-85/

Usein kytkimiin voidaan tehdä erillisiä VLAN-kytkentöjä. Tällöin koneet ovat fyysisesti samassa verkossa, mutta loogisesti ne muodostavat erillisiä verkkoja

(kuva 4). Koneet voivat keskustella ainoastaan samassa VLANissa olevien koneiden kanssa. VLAN-verkot voidaan määritellä kytkimen porttien, protokollan tai Ethernet-osoitteen (MAC-osoitteen) mukaan. VLAN-verkot määritellään kytkimen hallintatyökalulla, joka voi olla esimerkiksi web-selainpohjainen toteutus. /13, s64/



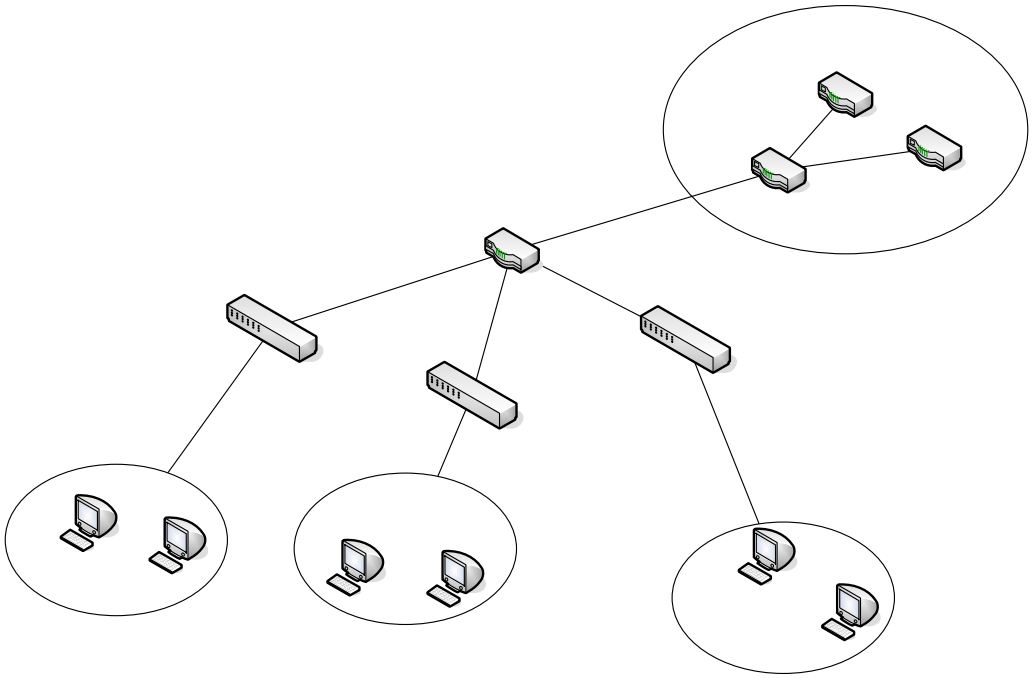
Kuva 4 Virtuaaliverkko VLAN

Lisäksi uusiin kytkinmalleihin on tullut myös reititysominaisuuksia. Näitä kytkimiä kutsutaan L3-kytkimiksi. Kytkimen nimi tulee sen toiminnasta ISO-mallin kolmannella tasolla (Layer 3), eli reitittämisestä. Kytkin pitää reititystaulun lisäksi yllä taulukkoa IP-osoitteista, joihin viimeksi on mennyt dataa. Todennäköisyys, että seuraava datapaketti menee juuri näihin osoitteisiin, on hyvin suuri, joten kytkin vertaa ensin paketin osoitekenttää taulukon arvoihin, ja jollei sen kautta löydy vastaanottajaa, se tekee reitityspäätöksen reititystaulun avulla. /13, s64/

Reititin (router)

IP-verkossa olevat koneet, palvelimet ja työasemat ovat kaikki reitittimiä. Niiden tehtävänä on reitittää TCP/IP-liikennettä. IP-pakettien vastaanottajia on pe-

riaatteessa kolme eli lähettäjä itse, samassa lähiverkkosegmentissä oleva kone ja eri lähiverkkosegmentissä oleva kone. Varsinaisen reitittimen tehtävänä on reitittää kahden eri lähiverkkosegmentissä olevan koneen välistä liikennettä (kuva 5). Reitittimen on tiedettävä tällöin porteissa olevat verkot. Reitittimellä pitää olla myös oletusreitti, johon se voi lähettää ne paketit, joiden verkkoa se ei tunne. Reitittimen sisällä on reititystaulu, jonka avulla reitityspäätökset tehdään. Reititys perustuu koneiden IP-numeroihin, ja reititystaulu voidaan tehdä käsin, jolloin sitä kutsutaan staattiseksi reititykseksi. Dynaamisella reitityksellä tarkoitetaan reitittimien keskenäistä tiedonvaihtoa tuetuista reiteistä. Tämä tehdään yleensä erillistä reititysprotokollaa käyttämällä. Dynaaminen reititys on käyttökelpoinen, kun tarkoituksena on reitittää paljon eri verkkoja, jotka myös muuttuvat jatkuvasti. Tällaisen reitityksen tekeminen käsin olisi lähes mahdotonta. /2, s256-258, 274/



Kuva 5 Lähiverkon reititys

3 TCP/IP-VERKOT

Mahdollisuus yhteydenpitoon erityyppisten laitealustojen ja käyttöjärjestelmien välillä on TCP/IP-verkon parhaimpia ominaisuuksia. Nimi- ja osoitejärjestelmät määrittelevät koneen sijainnin sekä verkon sisällä että verkon sijainnin Internetin sisällä. Nimipalvelut yhdistävät nimet ja osoitteet, mistä muodostuukin TCP/IP-verkon tärkein palvelu. Usein TCP/IP:stä puhutaan protokollana, vaikka se ei varsinaisesti ole protokolla, vaan siihen kuuluu monta eri protokollaa. Nämä protokollat on suunniteltu useisiin eri tarkoituksiin ja ne muodostavat niin sanotun protokollaperheen. /4, s1-2;2, s178/

3.1 TCP/IP-protokollaperhe

TCP/IP-protokollaperhe on suunniteltu Internetin käyttöön. Tehtävänä on tarjota pienille verkoille liikenne- ja viestienvaihtosäännöt. Protokollaperhe voidaan jakaa jäsenprotokolliin käyttötarkoituksen mukaan. Näitä ovat muun muassa sovellus-, kuljetus-, verkko- ja siirtoyhteysprotokolla. /2, s179/

Internet on jatkuvasti muuttuva useiden yksityisten ja julkisten verkkojen muodostama kokonaisuus. Sitä ei varsinaisesti omista kukaan, eikä sillä ole keskitettyä hallintoa tai ylläpitoa. Ainoastaan aivan keskeisimmistä toiminnoista on perustettu erilliset organisaatiot. Tällaisia toimintoja ovat muun muassa IP-osoitteiden hallinta ja domain-nimet. /2, s179;15; 16 /

Internet Assigned Numbers Authority (IANA) on organisaatio, joka vastaa kansainvälisellä tasolla nimien ja osoitteiden jakamisesta. Protokollaperheeseen liitettävien uusien protokollien standardoimisesta huolehtii Internet Engineering Task Force (IETF). Internet on luonteeltaan sellainen, että eri verkoissa olevat koneet voivat olla laite- ja käyttöjärjestelmäalustoiltaan erilaisia. TCP/IP-protokolla on tehty juuri tällaisten erilaisten laitteistojen ja verkkojen väliseen liikennöintiin. /2, s179;15; 16 /

3.2 Nimipalvelut ja IP-osoitteet

Tavallinen käyttäjä haluaa, että yhteyden luominen haluttuun koneeseen olisi mahdollisimman helppoa. Internet-verkossa koneeseen viitataan IP-osoitteella. IP-osoite koostuu neljästä kentästä, jotka määrittelevät sekä verkon että itse koneen. Netid eli verkko-osoite kertoo koneen verkon, ja hostid eli koneosoite kertoo koneen osoitteen verkossa. Huonon muistettavuuden vuoksi IP-osoitteet eivät ole sopivia sellaisenaan koneiden osoitteiksi. Tästä syystä käytetäänkin numeeristen osoitteiden rinnalla kirjaimista koostuvia osoitteita eli niin sanottuja domain-nimiä. Samalla tavoin ne ovat myös hierarkisia, mutta osoitteet voidaan korvata paremmin muistettavalla sanalla. Tällöin tavallisen käyttäjän ei tarvitse tietää varsinaisia IP-osoitteita, vaan hän voi käyttää pelkkiä domain-nimiä. Internetin yksi keskeisimmistä palveluista onkin nimipalvelu, joka yhdistää konenimen vastaavaan IP-osoitteeseen. Internetin alussa verkossa olevia koneita oli niin vähän, että jokaiselle verkossa olevalle koneelle voitiin luoda host-tiedosto. Tiedosto sisälsi taulukon IP-osoitteista ja niitä vastaavista nimistä. Koneiden määrän kasvu johti siihen, että tällaisen tiedoston ylläpitäminen on mahdotonta. Verkon jatkuvan elämisen vuoksi on kehitelty tietokanta, joka huolehtii IP-osoitteiden ja konenimien yhdistämisestä. /2, s185-186; 13, s73/

Ydinpalvelujen lisäksi TCP/IP-verkossa käytetään muitakin peruspalveluja, kuten esimerkiksi Windows-pohjaisissa järjestelmissä NetBIOS-nimipalveluja. Verkon IP-osoitteiden jakoon taas käytetään DHCP-palvelua ja osoitteenmuutokseen NAT-palvelua. /17; 18; 6, s1354/

3.2.1 DNS

Domain Name System (DNS) on tietokanta, johon on tallennettu IP-osoitteet ja niitä vastaavat nimet. Tietokanta on hajautettu useaan koneeseen ympäri Internetiä. Juuripalvelin sisältää informaatiota, joka koskee ylimmän tason toimialuenimiä, kuten .COM, .EDU ja .GOV. Tämän lisäksi jokaisella Internetin toimialueella on nimipalvelin, joka vastaan omalla toimialueella käytetyistä nimis-

tä ja osoitteista. Kun asiakastietokone tarvitsee tiettyä osoitetta, se lähettää DNS-palvelimelle kyselyn. Jos paikallinen palvelin ei tiedä kyseistä osoitetta, se lähettää kyselyn taas eteenpäin seuraavalle palvelimelle. Tätä ketjua jatketaan, kunnes löytyy sellainen palvelin, joka tietää osoitteen. /5, s243; 2, s185/

3.2.2 WINS

Lähiverkoissa, joissa tiedonsiirtoon käytetään TCP/IP-protokollia, tarvitaan IP-osoitteita vastaavien NetBIOS-nimien selvitystä varten NetBIOS-nimipalvelin. Windows-pohjaisissa verkoissa käytetään Windows Internet Name Services eli WINS-nimipalvelimia. Nimestään huolimatta WINS-palvelua käytetään ainoastaan lähiverkossa. NetBIOS-nimet eivät ole hierarkisia, joten niitä ei voida käyttää Internetissä. NetBIOS-nimijärjestelmässä verkon koneet ilmoittavat muille käyttämänsä NetBIOS-nimen. WINS-palvelimen tietokannassa koneiden NetBIOS-nimet kytketään IP-osoitteisiin. Kirjautuessaan verkkoon kone lähettää palvelinkoneelle rekisteröintipyynnön. Pyyntö sisältää koneen IP-osoitteen sekä NetBIOS-nimen. WINS-palvelin lähettää vastauksen, josta käyvät ilmi palvelimen osoite, rekisteröity nimi sekä rekisteröinnin voimassaoloaika. Windows-verkossa toisen koneen tunnistamiseen käytetään NetBIOS-nimeä. /2, s209-210; 6, s1354/

3.2.3 DHCP-palvelu

DHCP-palvelin helpottaa verkon ylläpitoa sellaisessa verkossa, jossa muutokset ovat yleisiä. Koneet saavat DHCP-palvelimen avulla automaattisesti oikeat IP-osoiteasetukset liittyessään verkkoon. DHCP-palvelua voidaan hyödyntää myös monissa palvelimissa. Tällöin koneen IP-osoite on liitetty koneen MAC-osoitteeseen. Palvelinkone saa näin aina saman IP-osoitteen verkossa. IP-osoitteen ja MAC-osoitteen liittämistä toisiinsa kannattaa käyttää myös työasemissa, jolloin ylläpito helpottuu, kun lokitiedoissa IP-osoite yksilöi aina oikean koneen ja sen käyttäjän. DCHP-palvelimelle voidaan määrittää käytettävät

osoitealueet. Osoitteet määritellään niin sanottuna osoitepoolina. Osoitealueen vapaat IP-osoitteet DHCP-palvelin jakaa eteenpäin DHCP-asiakkaille. DHCP-palvelin määrittää IP-osoitteelle kestoajan, jonka jälkeen osoitevaraus pitää uusia. DHCP-palvelimet eivät jaa tietojaan toistensa kesken. Jos halutaan varmistua, ettei samaa osoitetta jaeta kahteen kertaan, pitää DHCP-palvelimien jakaa eri osoitealueita. Pienissä verkoissa tämänkaltainen tilanne on mahdoton, koska niissä ei käytetä monia DHCP-palvelimia. /2. s240-243; 17/

3.2.4 NAT-palvelu

Usein varsinkin pienillä yrityksillä on vain yksi julkinen IP-osoite, vaikka yrityksen lähiverkossa onkin monia koneita. Jotta kaikki voisivat olla yhteydessä Internetiin, tulee käytössä olla NAT-osoitteenmuutospalvelu. Network Address Translation eli NAT on menetelmä, jolla reititin tai yhdyskäytävä muuttaa sisäverkon osoitteen viralliseksi IP-osoitteeksi. Sisäverkossa käytetään harmaita IP-osoitteita, joita ei ole rekisteröity kenellekään. NAT-osoitteenmuutoksella voidaan lisäksi peittää sisäverkon arkkitehtuuri, mikä tuo verkkoon lisää tietoturvaa, jolloin ulkopuolelta on ainoastaan havaittavissa reitittimen IP-osoite. Tällöin verkossa olevat koneet jäävät näkymättä. Osoitteenmuutos tuo myös ongelmia, sillä monesti käytettäessä kaksisuuntaisia palveluja vaikuttavat monet niistä toimivan vain toiseen suuntaan ja Internetistä takaisinpäin kulkeva liikenne jää usein tulematta. Tämän vuoksi NAT-laitteille voidaan määritellä avoimia yhteyksiä, jolloin laitteet pitävät niistä listaa. Yhteys poistetaan listasta, kun se suljetaan. Yhteyksillä on myös aikaraja, ja käyttämätön yhteys poistetaan listalta tietyn ajan kuluttua. /2, s246; 1, s 196/

3.2.5 IP-osoitteet

Kaikilla Internetiin kytketyillä laitteilla pitää olla oma yksikäsitteinen osoite. TCP/IP-protokollissa käytetään IP-osoitteita. IP-osoite on 32-bittinen standardin mukainen osoite, joka sisältää tiedon koneen verkosta ja siinä olevasta ko-

neesta. Osoite voi olla esimerkiksi muotoa 192.168.1.1. IP-osoite sisältää aina verkko-osoitteen (netid) ja isäntäosoitteen (hostid). Verkko-osoite määrää, mihin luokkaan osoite kuuluu. Kaikki Internetin IP-osoitteet on jaettu osoiteluokkiin, ja nämä luokat määräävät yksittäiselle verkolle suurimman mahdollisen konemäärän. Kansainvälisellä tasolla IP-osoitteiden jaosta vastaa IANA ja kansallisella tasolla jokin Internet-operaattori. /5, s235; 2, s191/

Jokaisella verkkokortilla on oma, kortinvalmistusvaiheessa siihen poltettu MAC-osoite. Jokainen MAC-osoite on siis ainutkertainen, ja se koostuu kuudesta tavusta. Yleensä osoite ilmoitetaan heksadesimaalilukuina, jotka on erotettu toisistaan kaksoispisteellä tai viivalla. Osoitteen kolme ensimmäistä tavua kertovat kortin valmistajan, ja kolme viimeistä tavua ovat kortin ainutkertainen osoite. Ethernet-kehysten osoitekentissä käytetään juuri MAC-osoitetta. IP-osoite vie paketin perille, ja MAC-osoitteen perustella kone voi päätellä, onko datapaketti tarkoitettu juuri sille. Viime aikoina on ollut yleisesti puhetta IP-osoitteiden loppumisesta. TCP/IP:stä onkin tehty uusi versio, joka on ristitty IPv6:ksi. /5, s235; 2, s191/

3.2.5.1 IPv4 ja IPv6

IPv6 mullistaa koko osoitejärjestelmän rakenteen. Kyseinen standardi on vahvistettu jo vuonna 1995. IPv6 yksinkertaistaa TCP/IP-määritysten tekemistä ja tarjoaa tietoturvallisuuden parantamiseen yksinkertaiset menetelmät. Kuitenkaan sitä ei ole otettu vielä laajamittaisesti käyttöön. Ensimmäinen suuri parannus IPv6:ssa on sen 128-bittinen osoitekenttä. IPv4:n osoite on vain 32-bittinen, ja lisäksi osoitteiden luokkajaon vuoksi suurin osa osoitteista jää kuitenkin käyttämättä. IPv6:n osoitteita on 2^128 kpl eli niitä on monta miljardia jokaiselle maapallon neliömetrille. IPv4:ssä on yhteensä osoitteita vain hieman yli neljä miljardia. IP-numeroita ei riitä siis edes kaikille maapallon ihmisille, saati sitten, jos ihmisillä olisi useampi IP-numero käytössä. Tällainen tilanne voi tulla eteen silloin, kun TV-laitteisiin, radioihin, autoihin tai puhelimiin tulee omat IP-numerot. /2, s215; 20, s7/

IP-numeron esitystapa on myös erilainen IPv6:ssa. Osoitteissa yhdistyvät sekä looginen että fyysinen osoite. Näin ollen luokkajakoa ei tarvita. Silti osoitteet ovat hierarkisia ja osoitteen avulla voidaan nopeasti selvittää, mihin verkkoon osoite kuuluu, ja missä verkko sijaitsee maantieteellisesti. IPv6:n IP-numero merkitään seuraavasti: 8000:0000:0000:0000:0123:4567:89AB:CDEF. Tämä voidaan lyhentää jättämällä välissä olevat nollat pois (8000::123:4567:89AB:CDEF). Vanhat IP-osoitteet voidaan kirjoittaa lisäämällä osoitteen alkuun kaksi kaksoispistettä esimerkiksi ::192.168.1.1. /20, s7-10; 2, s216/

Toinen hyvä parannus IPv6:ssa on Ethernet-kehyksen otsikkokentän lyhentäminen. IPv6 on pituudeltaan vain 7 kenttää, kun IPv4 on 13. Lyhyempi otsikkokenttä mahdollistaa entistä nopeamman pakettien käsittelyn reitittimissä, jolloin tiedonsiirto saadaan nopeammaksi. Kolmas parannus on entistä parempi tuki optioille, eli kentät, jotka olivat ennen pakollisia, ovat nyt vaihtoehtoisia. Lisäksi niiden erilainen esittämistapa antaa reitittimille mahdollisuuden hypätä sellaisten optioiden yli, joita ei ole tarkoitettu niille käsittelyyn, jolloin toiminnot nopeutuvat. Neljäs parannus on turvallisuus, jossa käyttäjän yksityisyyttä ja tunnistettavuutta on parannettu. /20, s7-10; 2, s216/

IPv4 ja IPv6 eivät ole keskenään yhteensopivia. Kestää todennäköisesti pitkään ennen kuin IPv6 korvaa kokonaan IPv4:en. Tällä hetkellä on satoja miljoonia koneita, jotka käyttävät IPv4:ää. IP-numeroiden loppumista on ehkäisty ennalta käyttämällä sisäverkoissa erillisiä intranet-osoitteita, joissa julkinen IP-osoite muutetaan NAT-osoitteenmuutospalvelulla useaksi harmaan sarjan intranet-osoitteeksi. Siirtymävälivaiheen ratkaisuksi on esitetty kahta eri vaihtoehtoa. Ensimmäisessä vaihtoehdossa muutetaan IPv6-paketit vanhempaan versioon niissä osin verkkoa, missä ei ole IPv6:n tukea. Toinen vaihtoehto on tunneloida IPv6 paketti IPv4:n paketin sisään ja siirtää se näin eteenpäin IPv4-verkossa. Internetiin liitettävien laitteiden määrä tulee varmasti kasvamaan, ja langattomien laitteiden määrän ennustetaan ohittavan kiinteästi verkkoon liitettyjen laitteiden määrän. IP-osoitteita tarvitaan tällöin lisää. Uuden IP-protokollan käyttöönotosta hyötyisivät varmasti siis ainakin matkapuhelimien ja PDA-laitteiden valmistajat. /21, s58-60; 2, s216/

3.2.5.2 Luokat

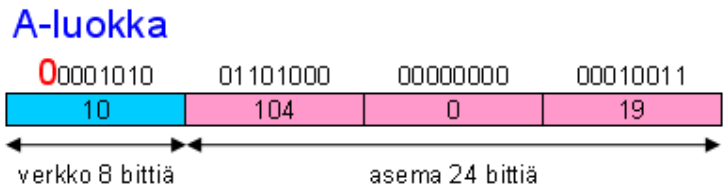
Ensimmäinen osa IP-osoitteesta yksilöi verkon osan (netid) ja toinen verkossa olevan koneen (hostid). Osoiteluokkia on yhteensä viisi kappaletta (taulukko 1.) ja ne on merkitty kirjaimin A-E. Kolme ensimmäistä kirjainta, eli A, B ja C ovat pääluokkia. D- ja E-luokat ovat erikoistapauksia. Tutkimalla osoitteen neljää ensimmäistä bittiä voidaan päätellä, mihin luokkaan osoite kuuluu. Osoite pitää siis muuttaa binääriseen muotoon, jotta sitä voidaan tarkastella. Esimerkkeinä mainittakoon 32-bittinen osoite 192.168.1.1 muutettuna binääriseen muotoon: 1100000 1010100 00000001 00000001, ja 32-bittinen osoite 10.10.10.5 muutettuna binääriseen muotoon: 00001010 00001010 00001010 00000101. /5, s235; 2, s 191/

Taulukko 1. IP-osoitteiden luokkajako

Luokka	**Aliverkon peite**	**Verkon osoite**
A	255.0.0.0	1.0.0.0 - 126.255.255.255
B	255.255.0.0	128.0.0.0 - 191.255.255.255
C	255.255.255.0	192.0.0.0 - 223.255.255.255
D	255.255.255.0	224.0.0.0 - 239.255.255.255
E	—	240.0.0.0 - 255.255.255.255

A-luokka

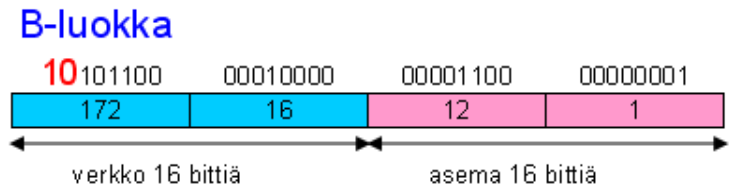
IP-osoitteen ensimmäisen bitin ollessa 0, kuuluu kyseinen osoite A-luokkaan (kuva 6). Verkko-osoite koostuu kahdeksasta ensimmäisestä bitistä. Ensimmäinen bitti kertoo siis luokan ja seitsemän seuraavaa bittiä yksilöivät verkon. Viimeiset 24 bittiä yksilöivät verkossa olevan koneen. Kappalemäärältään verkkoja voi olla teoriassa vain 128 kappaletta, mutta yhteen verkkoon voi liittää yli 16 miljoonaa konetta. Desimaalimuotoisina osoitteet ovat 1.0.0.0-126.255.255.255. Osoite 0.0.0.0 on varattu laitteiden oletusosoitteeksi ennen osoitteen oikeaan arvoon muuttamista. Osoite mahdollistaa koneen käynnistymisen. A-luokan harmaat IP-osoitesarjat ovat välillä 10.0.0.0-10.255.255.255. Nämä sarjat eivät siis ole julkisessa jakelussa, vaan niitä voi käyttää intranet-osoitteina. /5, s237; 2, s 195; 4, s27/



Kuva 6 A-luokan osoitteet

B-luokka

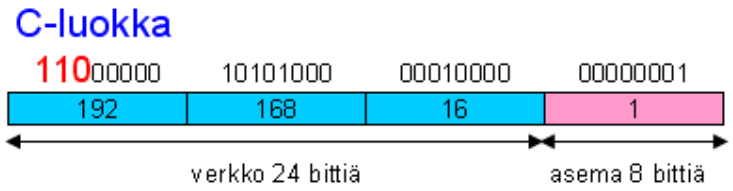
B-luokan osoitteessa kaksi ensimmäistä bittiä ovat muotoa 1 0 (kuva 7). B-luokan osoitteet desimaalimuotoisina ovat siis 128.0.0.0-191.255.255.255 välissä. Verkko- ja koneosoitteet ovat kaksitavuisia eli 16-bittisiä. Eri B-luokan verkkoja on yhteensä 16 384 kappaletta ja jokaisessa voi olla 65 536 kappaletta yksittäistä konetta. Vaikka molempien osoitteet ovat 16-bittisiä, ei verkkoja ja niissä olevia koneita ole samaa määrää. Ero johtuu siitä, että kaikkia mahdollisia osoitearvoja ei voida käyttää, vaan ne ovat muiden luokkien käytössä. B-luokan harmaat sarjat sijoittuvat välille 172.16.0.0-172.31.255.255. /5, s237; 2, s195; 4, s27/



Kuva 7 B-luokan osoitteet

C-luokka

C-luokan osoitteet tunnistaa 1 1 0 -alkuisesta bittijonosta (kuva 8). Desimaalimuotoisina osoitteet voivat olla siis 192.0.0.0-223.255.255.255. Verkko-osoite koostuu tällöin kolmesta tavusta eli yhteensä 24 bitistä, jolloin koneosoitteille jää nyt vain yksi tavu eli kahdeksan bittiä. Yhteen verkkoon ei siis sovi kuin korkeintaan 256 konetta, mutta verkkoja on vastaavasti huomattavasti enemmän eli 2097152 kappaletta. /5, s238; 2, s 195; 4, s27/



Kuva 8 C-luokan osoitteet

D- ja E-luokat

Nämä kaksi viimeistä luokkaa ovat käytössä eri tavalla kuin varsinaiset kolme pääluokkaa. D-luokan osoitteita käytetään monilähetysryhmien käyttöön (multicasting), jossa datapaketit lähetetään yhden isäntäkoneen sijaan useammalle. D-luokan osoitteet alkavat aina bittijonolla 1 1 1 0, joten näin ollen osoitealueeksi tulee 224.0.0.0-239.255.255.255. /5, s238; 2, s 195/

E-luokan osoitteet ovat tällä hetkellä käytössä ainoastaan testiverkoissa, ja ne ovat varattuina tulevaa käyttöä varten. Osoitteet alkavat 1 1 1 1 0-bittijonolla ja osoitealue on 240.0.0.0-255.255.255.255. /5, s238; 2, s 195/

3.2.5.3 Aliverkot

Erityisesti A- ja B-luokkien osoitesarjoissa syntyy usein tilanteita, jolloin koko käytettävissä olevaa osoitesarjaa ei ole mielekästä käsitellä yhtenä kokonaisena verkkona. Tällöin verkko voidaan kutistaa, eli jakaa osiin niin sanotuiksi aliverkoiksi. Ideana aliverkon muodostamisessa on jakaa koneiden osuus osoitteista kahteen yhtä suureen osaan. Jako määritellään aliverkonpeitteellä (subnet mask), joka kertoo, mitkä bitit kuuluvat koneelle ja mitkä aliverkolle. Jotta aliverkkoja voitaisiin laskea, pitää osoitteet muuntaa aina binäärimuotoon. /5, s240;4, s31/

Laitteille asetettaessa osoitteet annetaan lähes poikkeuksetta desimaalimuotoisina. Aliverkonpeite ilmoittaa, kuinka monta bittiä IP-osoitteesta kuuluu verkon osoitteeseen. Usein aliverkonpeitteen verkkobittien kokonaismäärä ilmoitetaan IP-osoitteen perässä /-merkin jälkeen, esimerkiksi 192.168.1.1/24. Kyseinen

merkintä tarkoittaa, että aliverkonpeite on 255.255.255.0, eli 24 ensimmäistä bittiä ovat ykkösiä. /5, s240;4, s31/

Jaettaessa verkko aliverkkoihin, sen peitettä kasvatetaan yhdellä. Tällöin syntyy kaksi uutta erillistä verkkoa. Esimerkkinä mainittakoon 192.168.1.0/24 -verkko-osoite, jossa koneosoitteita on yhteensä 256 kappaletta. Kun tästä verkosta muodostetaan kaksi erillistä aliverkkoa, sen aliverkonpeitettä kasvatetaan yhdellä. Tällöin syntyvät verkot 192.168.1.0/25 ja 192.168.1.128/25. Molemmissa verkoissa on nyt siis 128 kpl osoitteita. Jos halutaan jakaa vielä nämäkin verkot, niin kasvatetaan taas aliverkonpeitettä yhdellä. Niin syntyvät uudet aliverkot 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26 ja 192.168.1.192/26. Kaikissa näissä verkoissa on jokaisessa 64 osoitetta. /5, s240;4, s31/

3.2.5.3 Yliverkot

Usein ei ole enää yhtään sopivaa B-luokan osoitesarjaa vapaana tai koneita ei ole niin paljon, että se kattaisi koko B-luokan. Tässä tilanteessa haluttaisiin koneita yhteen verkkoon enemmän kuin yhteen C-luokkaan mahtuu, jolloin voidaan käyttää kahta peräkkäistä C-luokan osoitesarjaa. Käytettäessä useita osoitesarjoja erillisinä verkkoina on verkkojen välillä käytettävä reititintä. Reitittimen käyttö kuitenkin hidastaa verkon toimintaa. Tästä syystä voidaan joukko peräkkäisiä C-luokan osoitesarjoja yhdistää yhdeksi lähiverkoksi, jota kutsutaan yliverkoksi. /2, s200/

Aliverkotuksen yhteydessä muutettiin koneosoitteen bittejä verkko-osoitteen biteiksi, mutta yliverkotuksessa taas tehdään toiminnot päinvastaisesti, eli osa verkko-osoitteen biteistä muutetaan koneosoitteen biteiksi. Toisin sanoen verkon peitettä pienennetään. Verkko-osoitteiden täytyy myös olla peräkkäisiä ja niiden tulee olla oikeassa kohdassa osoitesarjaa, sillä muuten yliverkotus ei onnistu. /2, s200/

4 LANGATON LÄHIVERKKO

Kaikissa kohteissa kiinteän verkon rakentaminen ei ole aina mahdollista, joten langaton lähiverkko on ongelmaan sopiva ratkaisu. Langattomasta lähiverkosta käytetään nimitystä WLAN, joka tulee englannin kielen sanoista Wireless Local Area Network. Langaton verkko on rakennuskustannuksiltaan edullinen ja se mahdollistaa aivan uudentyyppisten päätelaitteiden ja sovellusten käyttöönoton. Liikkuvuus on hyödyksi nykyaikaisessa toimistoympäristössä, jossa työtä ei aina tehdä tietyssä paikassa. Langaton verkko tarjoaa pääsyn samoihin tiedostoihin ja palveluihin verkon tukiasemien kantavuusalueella. /7, s18-19;2, s152; 12. s538/

Osa langattomista verkoista on luvanvaraisia, koska ne käyttävät lupaa vaativia radiokanavia. Näitä ei kuitenkaan ole kovinkaan montaa ja ne hankitaan yleensä langattomia verkkopalveluita tarjoavalta yritykseltä. Yleisin käytössä oleva langaton lähiverkko perustuu IEEE 802.11 -standardiin, eikä se tarvitse erityistä lupaa. IEEE 802.11 -standardissa on monia eri versioita, jotka kertovat langattoman verkon nopeuden. Tällä hetkellä on käytössä 802.11g-versio, joka pystyy 54 Mbps:n tiedonsiirtonopeuteen. Käytössä on kuitenkin vielä paljon 11 Mbps:n 802.11b-standardin laitteita. Langattoman verkon todellinen hyötynopeus ei kuitenkaan ole näin suuri, vaan se on todellisuudessa noin 10–50% nimellisnopeudesta. /2, s152;13, s66/

Lupavapaat langattomat verkot toimivat mikroaaltoalueella. Käytettävät taajuudet ovat Euroopassa 2,4 GHz ja 5,0 GHz. Alueella toimii myös paljon muita laitteita esimerkiksi Bluetooth-laitteet, mikroaaltouunit ja tutkat. Nämä laitteet tuottavat häiriötä langattomalle verkolle. Mikroaallot eivät myöskään läpäise kiinteitä esteitä kovinkaan hyvin, vaan heijastuvat niistä, mikä aiheuttaakin usein ongelmia tukiasemien sijoittelun suunnittelun kannalta. Tukiasemien eri sijoituspaikkoja siis kannattaa asennusvaiheessa kokeilla. Toisaalta samat materiaalit jotka estävät mikroaaltojen kulun heijastavat aaltoja monessa tilanteessa. Tällöin voidaan heijastumista käyttää hyödyksi tukiasemien sijoittelussa. Myös

tietoturva paranee, jos verkko ei kanna kovinkaan pitkälle rakennuksen ulkopuolelle. /2, s152;8, s111/

4.1 Suojaus

Tietoturva on tullut esille yhä suuremmassa määrin puhuttaessa nykyajan lähiverkosta. Varsinkin lähiverkon ollessa langaton on syytä laittaa tietoturva-asetukset kuntoon, sillä verkko ei pysy talon rakenteiden sisällä. Kuka tahansa voi siis liittyä suojaamattomaan verkkoon. Langattomiin verkkoihin on suunniteltu useita erilaisia suojauskäytäntöjä sekä liikenteen salakuuntelun, että verkon luvattoman käytön ehkäisemiseksi. Hakkereiden kehittämiä vakoilutyökaluja on saatavissa Internetistä runsaasti, jolloin potentiaalisia salakuuntelijoita ja luvattomia käyttäjiä on runsaasti. Langattoman verkon suojaaminen tehdään tukiasemaa konfiguroimalla. /2, s167/

Verkon suojaamiseksi kannattaa ensin muuttaa tukiaseman salasana. Salasanan pitäisi olla tarpeeksi pitkä, ja siinä on hyvä olla sekä isoja ja pieniä kirjaimia että numeroita. Toinen hyvä suojausmenetelmä on käytössä oleva verkon nimen piilottaminen. Verkon nimeä kutsutaan Service Set ID:ksi eli SSID:ksi. Piilottamalla SSID-verkko ei näy ulkopuolelle, jos esimerkiksi Windowsin langaton verkko-toiminnolla yritetään etsiä liitettäviä verkkoja. Verkkoon voi siis liittyä vain tietämällä sen nimen. Toiminto on hyvä silloin, kun verkkoon ei liitetä usein uusia koneita. Tukiasemaan voidaan myös määritellä, mitkä verkkolaitteet saavat siihen liittyä, jolloin siihen tehdään niin sanottu MAC-suodatus, jolloin tukiasemaan voidaan muodostaa yhteys vain sen listaan määrätyillä MAC-osoitteilla. Tämäkin toiminto on tehokas verkossa, jossa uusia liitettäviä laitteita ei tule usein. /10/

Edellä esitetyt toimenpiteet toimivat vain verkon luvattoman käytön estossa, mutta itse dataa ei ole vielä salattu, jolloin ilmassa liikkuvaa dataa voi asiaan perehtynyt henkilö helposti lukea. Onkin suositeltavaa käyttää myös tässä tilanteessa jonkinlaista salausta. Salaamiseen kannattaa käyttää joko WEP- tai

WPA-salausta, joista WPA (Wireless Fidelity Protected Access) on ehdottomasti suositeltavampi. Ensimmäinen WLAN-verkkojen salaamiseen kehitetty WEP (Wired Equivalence Privacy) tarjoaa perusturvaa, mutta se on helposti murrettavissa siitä löydettyjen tietoturva-aukkojen takia. Salausta kannattaa käyttää vain silloin, kun tukiasema tai siihen liitettävä laite ei ole WPA-yhteensopiva. WPA-salauksessa salausavainta vaihdetaan jatkuvasti jolloin tunkeutuja ei pysty selvittämään verkkoliikennettä. WEP-salauksessa käytetään vain yhtä salausavainta. Tallentamalla riittävästi verkkoliikenteen dataa voidaan tietokonetta hyväksikäyttäen laskea käytettävä avain. /10/

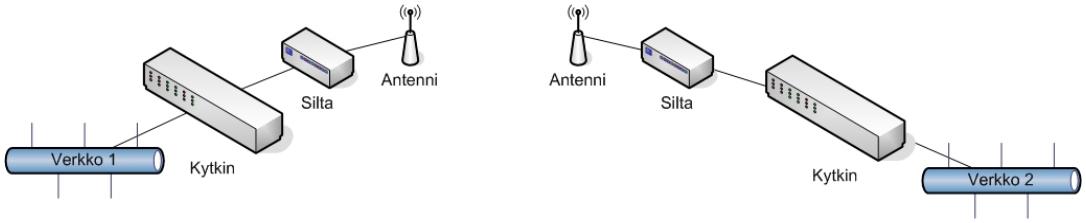
Uusimmista laitteista saattaa löytyä jo WPA:takin kehittyneempi WPA2-salaus. Moniin vanhoihin tukiasemiin ja langattomiin verkkokortteihinkin voidaan päivittää uusi WPA2-salaus ajuripäivityksillä. Salauksen saa käyttöön tukiaseman asetuksista, johon määritellään salausavain. WPA:ssa on käytössä kaksi erilaista kirjautumismenetelmää. WPA-PSK:ssa salausavain kirjoitettaan tukiasemalle, kun taas tavallisessa WPA:ssa salausavain haetaan erilliseltä palvelimelta. Salausavaimeksi kannatta määritellä vähintään 14:sta merkistä koostuva satunnainen sarja. Avainta on myös suositeltavaa vaihtaa säännöllisin väliajoin. /10;9/

4.2 Aktiivilaitteet ja antennit

Peruskomponentteina langattomassa lähiverkossa ovat langattomat verkkokortit sekä tukiasemat. Näiden lisäksi tukiasema sisältää yleensä langattoman etäsillan tai langattoman reitittimen. Tukiasema on keskeisin komponentti langattomassa lähiverkossa ja sitä hankittaessa ensisijaisena valintakriteerinä voidaan pitää tukiaseman tukemia WLAN-standardeja. Kannattaa siis valita sellainen tukiasema, jota suurin osa yrityksen laitteista tukee. Usein tukiasemat tukevat monia eri standardeja. /2, s157/

Etäsiltoja käytetään rakennettaessa langaton lähiverkko esimerkiksi kahden eri rakennuksen välille langaton lähiverkko. Siltoja käytetään myös yhdistämään kahta erillistä langallista verkkoa (kuva 9). Esimerkiksi häiriötilanteessa voi-

daan kahden verkon kytkimet yhdistää helposti langattomalla sillalla. Käytettäessä etäsiltaa pitää molempiin laiteisiin määritellä linkin toisessa päässä olevan laitteen MAC-osoite. Monipistesiltoja voidaan käyttää langattomien verkkojen yhdistämiseen toisiinsa. Monipistesilta ylläpitää yhteyttä moniin eri verkkoihin samanaikaisesti. /2, s157/



Kuva 9 Kahden lähiverkon yhdistäminen etäsillan avulla.

Langattomissa lähiverkoissa voidaan käyttää myös langattomia reitittimiä, jotka mahdollistavat reitityksen kiinteän ja langattoman verkon välillä. Lisäksi tarvitaan vielä langattomat verkkokortit, joiden valintaan vaikuttavat suurimmaksi osaksi käytössä oleva WLAN-standardi. On myös suositeltavaa kiinnittää huomiota kortin herkkyyteen, joka määrittelee signaalin pienimmän tehon jota kortti voi vastaanottaa. Tukiasemissa on yleensä valmiina antennit ja niihin voidaan tarvittaessa liittää ulkopuolinen antenni, jolla saavutetaan parempi kuuluvuus. Antennin muodostama suuntakuvio määrittelee sen käytön. Yleensä sisätiloissa kannattaa käyttää ympärille säteilevää antennia, jonka säteilynkuvio on pallon muotoinen. Tällöin saadaan aikaan suurempi peittoalue. Esimerkiksi langattomien etäsiltojen kytkemisessä toisiinsa kannattaa käyttää suunta-antennia, joka keskittää lähetystehon tiettyyn suuntaan. Usein puhutaan myös suuntakuviosta tai keilasta. Kapein keila ja suurin teho haluttuun suuntaan saadaan joko lautasantennilla tai putkiantennilla. On olemassa myös sektori- ja paneeliantenneja, joka rajoittavat signaalin etenemistä ei-toivottuihin suuntiin. Kuitenkin näiden antennien signaalin vahvistus toivottuun suuntaan on pieni. /2, s157-166;7, s63/

5 VERKON SUUNNITTELU

Lähiverkkoa rakennettaessa ei ole helppo määrittää, mitä kaikkea täytyy ottaa suunnittelussa huomioon, sillä lähtökohdat voivat olla hyvinkin erilaiset. Vanhaa verkkoa laajennettaessa rasitteena on vanha tekniikka, kun taas uudessa verkossa pitää ottaa huomioon kaikki muutoksen aiheuttamat riskitekijät. Suunnittelu voidaan jakaa seitsemään eri vaiheeseen, jotka ovat esitutkimus, määrittely, suunnittelu, toteutus, testaus, käyttöönotto ja ylläpito. Vaiheet eivät välttämättä etene juuri tässä järjestyksessä, sillä varsinkin määrittely-, toteutus- ja suunnitteluvaiheet menevät usein osittain päällekkäin. /2, s406/

Esitutkimus

Ensimmäisessä vaiheessa selvitetään ja kerätään projektissa tarvittavat tietolähteet. Näitä ovat muun muassa vanhan verkon dokumentointi ja käytössä olevien tietojärjestelmien selvittäminen. Esitutkimusvaiheessa kartoitetaan yleisellä tasolla koko projektin sisältö, jonka perusteella tehdään alustavat aikataulut. /2, s407/

Määrittely

Tietoverkkoon vaadittavat ominaisuudet selvitetään määrittelyvaiheessa, johon liittyvät myös erilaiset alkukartoitukset ja analyysit. Vaiheen sisältöön vaikuttaa myös se, ollaanko laajentamassa tai uudistamassa vanhaa järjestelmää vai tehdäänkö kokonaan uusi. Tässä vaiheessa kysytään järjestelmän ylläpitäjien ja käyttäjien mielipiteitä ja toiveita, ja selvitetään esimerkiksi työasemien määrät, siirrettävien datojen määrät, virtuaaliverkkojen-, langallisten- ja langattomien yhteyksien tarve. /2, s407/

Suunnittelu

Suunnitteluvaiheessa etsitään ratkaisuja määrittelyvaiheessa asetettujen tarpeiden saavuttamiseksi. Erilaisten vaihtoehtojen tarkastelu kuuluu suunnitteluvaiheeseen, mutta kaikkia toiveita ei aina pystytä toteuttamaan. Suunnitteluvaiheeseen kuuluu myös taloudellisten hyötyjen tarkastelu, jossa pitää selvittää, mitkä ominaisuudet halutaan saavuttaa taloudellisesti järkevällä panostuksella. Selvi-

tykseen kuuluu myös perinteisten laite- ja ohjelmistokustannusten lisäksi ottaa huomioon mahdolliset käyttö- ja ylläpitokustannukset. /2, s409/

Toteutus

Toteutusvaiheessa alkaa varsinainen tietoverkon rakentaminen. Toteutus tehdään suunnittelun perusteella, mutta usein toteutusvaiheessa joudutaan muuttamaan joitakin suunnittelun yksityiskohtia. Toteutusvaiheen dokumentointi on tärkeää mahdollisten jatkolaajennusten ja ylläpidon helpottamiseksi. Dokumenttien pitäisi sisältää tehdyt asetukset ja niistä mahdolliset kommentoinnit. /2, s410/

Testaus

Verkon varsinainen testaus suoritetaan tässä vaiheessa. Toiminnallisella testauksella tarkoitetaan verkkoon asennettujen kaapeleiden, laitteiden ja ohjelmistojen toiminnan tarkastamista. Moniin verkon osiin liittyy oma testistandardi, esimerkiksi kaapeloinnilla on omat mittalaitteet, jotka määrittelevät testitulosten hyväksyttävyyden. /2, s410/

Käyttöönotto

Käyttöönottovaiheessa uusi tietojärjestelmä otetaan käyttöön. Usein uuden rinnalla käytetään myös vanhaa järjestelmää, sillä se on turvallinen tapa ottaa käyttöön uusi järjestelmä. Mahdollisia eroavaisuuksia huomattaessa voidaan korjaukset tehdä siten, että varsinainen liiketoiminta ei kuitenkaan katkea, vaikka se sitookin työhön lähes kaksinkertaisen työpanoksen. /2, s411/

Ylläpito

Verkon suunnitteluprojekti päättyy käyttöönottovaiheeseen. Tämän jälkeen alkaa verkon ylläpito. Ylläpidon aikana laaditaan aina dokumentit järjestelmään tehdyistä muutoksista. Tällaisia dokumentteja voivat olla esimerkiksi aktiivilaitteiden konfigurointimuutokset, käyttäjätilien ja -tunnusten asetusten sekä ristikytkentätaulukon muutokset. Ylläpitovaiheessa pidetään yllä myös lokitietoja sekä liikenne- ja kuormitusseurantaa. /2, s411/

6 LÄHIVERKON YLLÄPITO

Kaikilla verkon laitteilla ja ohjelmilla on tietty elinkaari. On tärkeää tietää milloin on aika päivittää järjestelmää. Tähän auttavat erilaiset hallinta- ja verkonvalvontaohjelmat. Ohjelmilla voidaan seurata verkon liikennettä ja selvittää mahdollisia verkon pullonkauloja. Ohjelmat auttavat myös erilaisissa vikatilanteissa, jolloin on mahdollista paikantaa vika nopeasti. Tätä kautta vika voidaan myös korjata ilman verkon pitkäaikaista toimintakatkosta. /5, s19/

6.1 SNMP ja verkonhallintaohjelmistot

Ylläpidolle on tärkeää tietää verkossa olevien laitteiden tilasta. SNMP-protokolla antaakin tähän hyvät mahdollisuudet ja se on vakiintunut verkonhallintatietojen keräämisessä. TCP/IP-pohjaisissa verkonhallinnan avulla hallittavissa laitteissa on SNMP-agentti, joka kerää tietoja laitteen toiminnoista. Tietojen kerääminen suoritetaan hallintaohjelmilla. /1, s312-313; 2, s323/

Hallintaohjelman ja laitteen välillä käytetään SNMP-protokollaa. SNMP on sovellustason protokolla joka määrittää, miten sovellusohjelma suorittaa kyselyt agentin MIB-tietokannalta sekä sen, miten agentti vastaa. Agentti voi myös itse lähettää viestejä hallintaohjelmalle. Yleensä tietylle tapahtumalle on ennalta määritelty jokin kynnysarvo, jolloin agentti tietää lähettää viestin. Tällainen arvo voi olla esimerkiksi jokin virhetilanne tai tulostimen väriaineen vähyys. SNMP-hallintaohjelmista on myös olemassa yleisiä malleja, joita voi käyttää kaikkien SNMP:tä tukevien laitteiden hallintaan. Monilla laitevalmistajilla on myös valmiiksi tietylle laitteelle räätälöity SNMP-hallintaohjelma, jolloin laitteesta voidaan saada hyvinkin erilaisia tietoja. /1, s312-313; 2, s323/

MIB-tietokanta määrittelee kaikki tiedot, jotka laite pitää sisällään. MIB määrittelee tietojen tyypit ja ne muuttujat, joilla hallintaohjelma voi vaikuttaa laitteen toimintaan. Tietokanta on standardisoitu puumaiseksi rakenteeksi, jossa osa puun sisältämistä tiedoista on pakollisia eli ne löytyvät kaikista SNMP-

laitteista. Tällöin voidaan käyttää yleisiä hallintaohjelmia laiteriippumattomasti. MIB-puurakenteen tietoihin viitataan OID:llä. Näiden lisäksi laitteiden valmistajilla on omia järjestelmäkohtaisia tietoja. Hallinta-asema suorittaa MIB-tietokannasta tietojen kyselyn, johon agenttilaite vastaa. Jos kyseistä tietoa ei voida palauttaa, ilmoittaa agentti virheestä. /1, s315; 2, s325/

Usein verkonhallinnassa käytetään laitteiden tai ohjelmistojen omia hallinta-ominaisuuksia. Verkon kasvaessa voi hallinnasta kuitenkin tulla työlästä, jolloin on kannattavaa hankkia yhtenäinen hallintaympäristö. Pääsääntöisesti se on yleinen kaupallinen sovellus. /1, s309/

6.2 Varmuuskopiointi ja RAID

Varmuuskopioinnilla tarkoitetaan tiedostojen kopioimista käytössä olevasta järjestelmästä toiseen. Varmuuskopio voidaan ottaa täysin eri mediaan esimerkiksi CD- tai DVD-levylle tai magneettikaseteille. Varmuuskopioon on syytä merkitä arkistointimerkinnät ja se on syytä siirtää tälle tarkoitettuun tilaan esimerkiksi paloturvalliseen kaappiin. Ottamalla työasemien ja palvelimien tiedostoista säännöllisesti varmuuskopiot estetään näin tietojen katoaminen erilaisten häiriöiden sattuessa. Häiriöitä voivat olla muun muassa kiintolevyhäiriöt, virtakatkokset, laitteisto-ongelmat tai virusten aiheuttamat ongelmat. /6, s677/

Varmuuskopiot suositellaan ottamaan ainakin käyttäjien työtiedostoista, sillä usein nämä sijaitsevat verkon palvelimella tai hajautettuina käyttäjän omalle työasemalle. On kannattavaa ottaa varmuuskopiot myös erilaisten palvelinpalveluiden ja niiden käyttämien tietokantojen tiedostoista. On kuitenkin olemassa myös erilaisia rutiineja, joiden avulla varmuuskopiointi on mahdollista automatisoida. Otetut varmuuskopiot on myös syytä testata, jotta voidaan varmistua siitä, että tiedot pystytään tarvittaessa palauttamaan. /6, s677/

RAID-tekniikalla pyritään parantamaan tietokoneen vikasietoisuutta tai nopeutta. Tekniikan avulla voidaan yhdistää monia kiintolevyjä yhdeksi loogiseksi le-

vyksi. Levyt voidaan myös laittaa peilaamaan toisensa, jolloin toisen levyn rikkoutuessa voidaan tiedot palauttaa toiselta levyltä. RAID-tekniikka voidaan jakaa eri tasoihin. Seuraavaksi esittelen nämä tasot. /26; 6, s26/

RAID0

RAID0-taso sisältää lomituksen, jossa yhden levyn data jaetaan kahdelle eri levylle. Levyille tapahtuvat luku- ja kirjoitustoimenpiteet voidaan suorittaa samanaikaisesti, jolloin toimenpiteisiin kuluva kokonaisaika pienenee merkittävästi. Huono puoli on se, että toisen levyn rikkoutuessa menetetään kaikki olemassa oleva data. /26; 6, s26/

RAID1

RAID1-taso tekee datan lomituksen eli peilauksen, jossa kahdelle kiintolevylle tallennetaan sama data. Toisen kiintolevyn rikkoutuessa voidaan toisesta kiintolevystä palauttaa data takaisin. Usein rikkoutuneen kiintolevyn vaihto onnistuukin niin sanotusti lennossa eli konetta ei tarvitse sammuttaa kiintolevyn vaihdon yhteydessä lainkaan. Tällöin koneen suorittamat palvelut eivät myöskään katkea. Huono puoli on se, että kiintolevytilaa hukataan kaksinkertainen määrä. Kiintolevyjen ollessa erikokoiset, vain pienemmän levyn tilan verran voidaan käyttää myös isompaa levyä. Näin ollen levytilaa hukkaantuu. /26; 6, s26/

RAID01

RAID01–taso on edellisten tasojen yhdistelmä. RAID01-tasossa kiintolevyjä täytyy olla minimissään neljä kappaletta. Tallennettu data kyetään palauttamaan takaisin rikkoutuneesta levystä, jos peilissä on yksi ehjä levy. /26; 6, s26/

RAID5

RAID5-tekniikka toimii XOR-tarkistussummilla, jossa osa kiintolevyn kapasiteetistä varataan tarkistussummia varten. Levyn rikkoutuessa voidaan data palauttaa laskemalla muiden levyjen tarkistussummat, eli tiedot saadaan muista levyissä. Kiintolevyjen minimimäärä on viisi kappaletta. Tämä ohjelmilla toteutettu vikasietoisuusmenetelmä ei ole yhtä tehokas ja luotettava kuin laitteistolla toteutetut RAID0- ja RAID1-tekniikat. /26; 6, s802/

7 TIETOTURVA

Tietopääoma on nykyaikaisen yrityksen arvokkainta omaisuutta. Sen saatavuus, oikeellisuus ja luottamuksellisuus on turvattava mahdollisimman pitkälle. Usein varaudutaan mahdollisiin ulkopuolisiin uhkiin kuten Internetistä tuleviin viruksiin haittaohjelmiin, mutta unohdetaan se, että suurin osa vakavista tietoturvariskeistä on oman yrityksen sisällä. Täydelliseen tietoturvaan ei koskaan päästä. On myös hyvä muistaa, että ylläpidosta koituvat kustannukset eivät saisi kasvaa turvallisuudesta saatavia hyötyjä suuremmaksi. /2, s342

7.1 Verkkoon kohdistuvat uhkat

Tietoturvallisuudessa on kolme keskeistä tekijää, jotka ovat luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuus on sitä, että vain ne henkilöt, joilla on tietoon käyttöoikeus, voivat käyttää sitä. Käytännössä tämä tarkoittaa sitä, että ohjelmille, kansioille tai tiedostoille voidaan määrittää käyttäjäoikeudet. Kansioihin ja tiedostoihin ei pääse käsiksi, jos käyttäjällä ei ole voimassaolevaa käyttäjätunnusta ja siihen henkilökohtaista salasanaa. Eheydellä tarkoitetaan sitä, että järjestelmässä olevat tiedot eivät pääse muuttumaan virheellisiksi. Käytännössä tässä tilanteessa on kuitenkin varauduttava ulkopuolisen tietojen tahalliseen tai tahattomaan muuttumiseen. Tahattomasti tiedot voivat muuttua jonkin käyttäjän virheellisen ohjelman käytön, laitevirheiden, ohjelmointi- tai tiedonsiirtovirheiden vuoksi. Palomuureilla ja käyttäjän tunnistuksella pyritään estämään tahallista tietojen muuttamista. Tahatonta muuttamista voidaan välttää käyttämällä esimerkiksi yhteydellisiä protokollia esimerkiksi TCP/IP:tä. /2, s342

Käytettävyys tarkoittaa sitä, että tarvittava tieto on saatavissa kohtuullisessa ajassa ja se on käyttökelpoisessa muodossa. Käytettävyyttä voi parantaa huolehtimalla riittävästä verkon kaistanleveydestä sekä varayhteyksistä. Nämä kolme tekijää ovat keskeisimmät tekijät tietoturvassa. Lisäksi monesti puhutaan pääsynvalvonnasta ja kiistämättömyydestä. Pääsynvalvonnalla tarkoitetaan sitä,

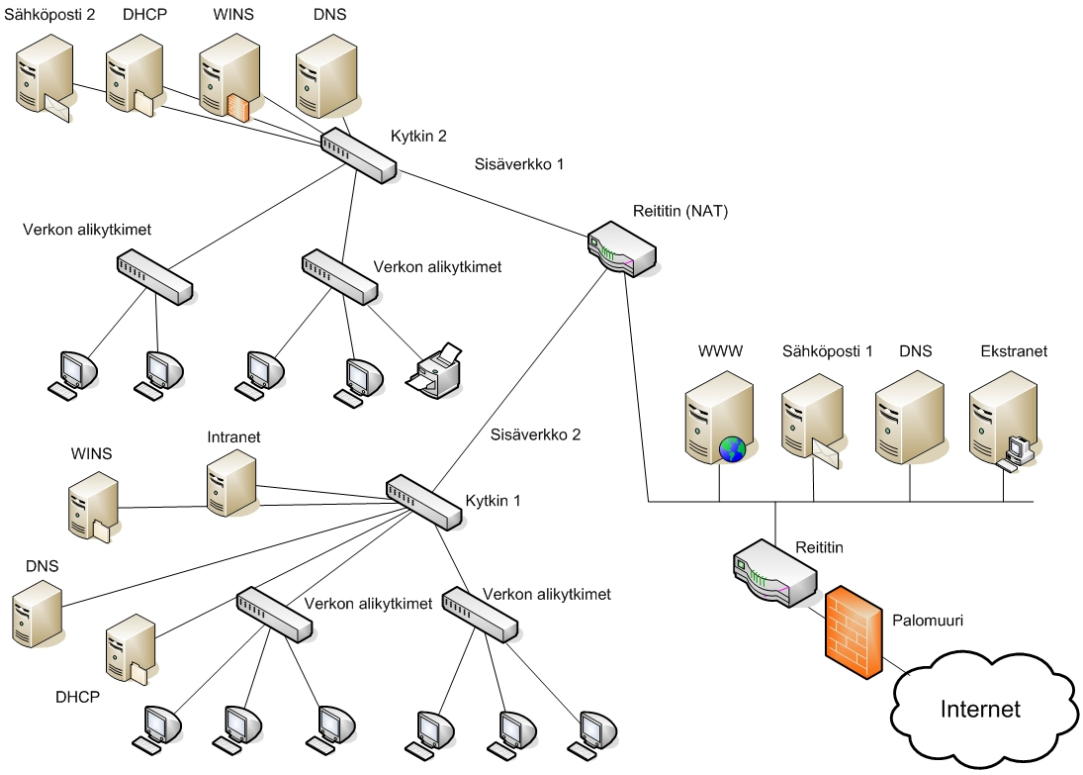
millä kaikilla tavoilla käyttäjiä tunnistetaan ja joilla rajoitetaan pääsyä tietojärjestelmiin. Kiistämättömyydellä tarkoitetaan sitä, että järjestelmien ja tietojen käytöstä jää luotettava merkintä lokitietoihin. /2, s342/

Yleisin verkkoon kohdistuva uhka on tiedon estyminen, jolloin verkossa olevat aktiivilaitteet, verkkokortit tai kaapelointijärjestelmä vikaantuvat. Näin ollen haluttuihin tietoihin tai palveluihin ei päästä käsiksi. Tiedonsaanti voi olla myös tahallisesti estettyä, jolloin ulkopuolinen taho kuormittaa verkkoa tietoisesti. Tyypillisesti tietoverkot on suojattu palomuurilla ulkopuolisilta hyökkäyksiltä, joka estää varsinaisen tunkeutumisen verkkoon. Tämän takia hakkerit pyrkivätkin kuormittamaan verkon ulkopuolisia julkisia palvelimia. Palvelimien ja aktiivilaitteiden mahdollisten ohjelmointivirheiden takia on mahdollista, että niiden suojaus voidaan kiertää palvelun kaatuessa. Koko suojauksen periaatteena on kuitenkin se, että käyttäjillä on ainoastaan välttämättömimmät oikeudet tarvitsemiinsa tietoihin ja laitteisiin. /2, s342-343/

7.2 Rakenteellinen tietoturva

Verkon toiminnan kannalta on tärkeää estää mahdollisten liikenteen pullonkaulojen syntyminen, sekä samalla estää pääsy ulkopäin. Jos ulkopuolelta halutaan päästä käsiksi sisäverkkoon, on sen tapahduttava suojattuja yhteyksiä pitkin. Kuvassa 10 on esitetty keskikokoisen yrityksen verkon periaatekuva. Liikenteen pullonkaulat pyritään estämään liittämällä palvelimet ja tehotyöasemat suoraan verkossa oleviin kytkimiin. Tavalliset työasemat ovat liitettyinä erillisten paikallisten kytkinten kautta pääkytkimeen. Kytkimiin on suositeltavaa tehdä myös VLAN-määritykset siten, että molemmat verkot muodostavat oman erillisen virtuaaliverkon. Lisää turvallisuutta saadaan aikaan myös määrittelemällä useampia eri virtuaaliverkkoja kuhunkin kytkimeen. Kummassakin sisäverkossa on omat DNS- ja WINS-palvelimet, jotka vastaavat vain sisäverkkojen kautta tuleviin nimikyselyihin. Sisäverkossa onkin suositeltavaa käyttää NAT-osoitteenmuutospalvelua, joka tehdään reitittimessä. DHCP-palvelin kannattaa kuitenkin säilyttää varalla vaikka käytettäisiin NAT-palvelua, koska tällöin voi-

daan keskitetysti tehdä kaikkien erillisten työasemien TCP/IP-asetukset. ./2, s344-345/



Kuva 10 Keskikokoisen organisaation verkon periaatekuva

Ennen kuin päästään yksityiskohtaisesti suunnittelemaan verkon suojausta, on siis tiedettävä verkon rakenne, mihin segmenttiin tai aliverkkoihin palvelut kuuluvat, mitä kaapelointijärjestelmiä käytetään sekä millaiset aktiivilaitteet ovat käytössä. Kaikki Internetissä olevat julkiset palvelut on sijoitettu pakettisuodattimena toimivan reitittimen erottamaan omaan segmenttiin, johon kuuluvat koneet voivat joutua ulkopuolisen hyökkäyksen kohteeksi, mutta niiden tilapäinen toimimattomuus ei häiritse yrityksen perustoimintaa. Myös ensimmäinen SMTP-sähköpostipalvelin on sijoitettu tähän heikosti suojattuun segmenttiin. Sen tehtävä on vastaanottaa postia ja lähettää se edelleen sisäverkossa olevalle palvelimelle. Sisäverkosta lähtevät postit käyttävät toista palvelinta vain läpikulkupalvelimena välittäessään postia Internetiin ja ainoastaan postia vastaanottava palvelin rekisteröidään julkiselle DNS-palvelimelle. Postipalvelimen lisäksi tähän julkiseen segmenttiin liitetään julkinen DNS-palvelin, joka huolehtii

vain etusegmenttiin kuuluvien laiteiden DNS-nimistä. Siinä ei saa olla sisäverkkoon kuuluvien koneiden tietoja. WWW-palvelimet ja ekstra-palvelimet kuuluvat myös etusegmenttiin, jonka turvaaminen perustuu pakettisuodatukseen, eli niiden porttien sulkemiseen joita ei julkisissa palveluissa käytetä. /2, s344-345/

7.3 Palomuurit ja virustentorjuntaohjelmat

Palomuuri on tullut tavalliselle Internetin käyttäjällekin tutuksi. Sitä kaupataan yleensä virustentorjuntaohjelmistojen mukana. Käsitteenä sana palomuuri on epämääräinen. Sillä voidaan tarkoittaa erityyppisiä ohjelmia tai laitteistoja, joiden tehtävänä on estää mahdolliset väärinkäytökset verkossa. Toimintansa puolesta palomuurit voidaan jakaa kolmeen eri tyyppiin. Ensimmäinen on pakettisuodin, joka hylkää liikennettä kohde- ja lähdeosoitteen sekä sovellusten porttinumeroiden perusteella. Toinen tyyppi on välityspalvelin, joka avaa käyttäjän puolesta palveluun tarvittavan yhteyden. Välityspalveluun on etukäteen määritelty, mistä laitteista voi yhteyden ottaa, jolloin käyttäjä voidaan tunnistaa luotettavasti. Huono puoli on se, että ainoastaan ennalta määriteltyjä palveluita voidaan käyttää ja muita palveluita käytävä liikenne hylätään. /2, s347/

Kolmas tyyppi on yhdyskäytävä, jota pidetään tietoturvamielessä kaikkein tehokkaimpana. Se tutkii sisällön jokaisesta paketista, joka kulkee asiakas- ja palveluohjelmistoissa. Virusohjelmiston tavoin se ilmoittaa epäilyttävästä paketista. Näitä paketteja ei lähetetä edelleen eteenpäin, vaan usein ne tallennetaan jatkotutkimuksia varten. Kaikki yhdyskäytävän läpi kulkevat paketit tarkastetaan, joten se vaatii laitteistolta suurta prosessoritehoa. Nämä kaikki kolme palomuuritekniikkaa vaativat pakettisuodatusmenetelmien tuntemusta, koska hyväksyttävä liikenne on määriteltävä käyttämällä pakettisuodatuksen perustietoja, kuten lähde- ja kohdeosoitteita sekä palveluiden käyttämät porttinumeroita. /2, s347/

Viruksista on tullut PC-koneen käyttäjälle riesa. Internetiin kytketty suojaamaton kone voi olla hyökkäyksen kohteena jo muutaman minuutin jälkeen. Tämän vuoksi on suositeltavaa käyttää virustentorjuntaohjelmistoja, joiden lisäksi tulee

olla oikein määritelty palomuuri. Yrityksissä nämä asiat on pääsääntöisesti hoidettu hyvin, mutta kotikäyttäjiltä suojaukset saattavat puuttua. Se on riski myös yritykselle, koska työntekijät voivat tuoda kotoaan viruksia työpaikan verkkoon. Tämän vuoksi isoissa yrityksissä on usein niin kattavat virustentorjuntalisenssit, että samat virustentorjunta-ohjelmat voidaan asentaa myös työntekijöiden kotikoneille. Käytännössä kaikki virustentorjuntaohjelmistot käyvät päivittämässä tietokantansa uusista viruksista automaattisesti Internetistä ja ohjelmat tarkistavat tietokoneen taustalla verkkoliikenteessä liikkuvia paketteja. Ohjelma antaa hälytyksen, jos liikenteestä löytyy kyseenalainen paketti, joka vie resursseja ja tehoja koneelta. Käyttöjärjestelmistä ja sovellusohjelmissa löytyy jatkuvasti tietoturva-aukkoja, jotka mahdollistavat haittaohjelmien pääsyn koneelle. Ohjelmien valmistajat päivittävätkin tuotteitaan usein, joten uusimmat päivitykset on syytä hakea sopivin väliajoin. Osa ohjelmista käy automaattisesti itse hakemassa päivitykset Internetistä. Useimmat virukset käyttävät leviämistienään sähköpostia, joten sähköpostin suodattamisesta on tullut yhä suurempi osa virustentorjuntaa. Samalla voidaan poistaa roskapostit. /25/

7.4 IOS-pohjainen pakettisuodatus

Reitittimissä ja niihin liitetyissä verkoissa ja laitteissa käyttöoikeudet määritellään pääsylistojen (Access List) avulla. Listoja käytetään erilaisten päivitystietojen rajoittamiseen sekä varsinaisiin palomuuritoimintoihin. Access-listat voidaan jakaa kahteen ryhmään, jotka ovat vakiolista (IP standard) ja laajennetut listat (IP extended). Vakiolistaa voidaan käyttää rajoittavana listana, joka määrittelee mistä osoitteista esimerkiksi reitittimen reittipäivityksiä haetaan. Vakiolistassa taas määritellään, mistä osoitteista liikenne hyväksytään. Laajennettuja listoja käyttämällä sallittu liikenne voidaan määrittää tarkemmin. Tähän voidaan käyttää sekä lähde- että kohdeosoitteita, erilaisia protokollatyyppejä, lähde- ja kohdeportteja sekä yhteyden muodostamiseen käytettävää suuntaa. Listoja ei lueta kokonaan läpi, vaan lukeminen lopetetaan heti kun löydetään ehto, joka täyttää määritykset. Ehtojen määrittely kannattaakin tehdä huolella, jotta ne menisivät toivotulla tavalla. /2, s348/

8 CASE FICI-COPY

Lähiverkon rakennusprojekti sai alkunsa vuoden 2005 toukokuussa, jolloin Fici-Copy Ky muutti uusiin tiloihin. Tiloissa oli jo valmiina lähiverkkokaapelointi, mutta sitä oli tarvetta laajentaa. Yrityksen toiveena projektissa oli, että verkon yhteyteen saataisiin kopiokoneiden ominaisuuksia varten esittelytilat. Samalla lähiverkon ylläpitoa oli tarkoitus helpottaa.

8.1 Esitutkimus

Fici-Copyn verkkoon kuuluu neljä kiinteää työasemaa ja kaksi kannettavaa tietokonetta, jotka ovat verkossa satunnaisesti. Lisäksi esittelytiloissa on markkinoilla kulloinkin olevia kopiokonelaitteita. Varsinaista palvelinta ei vanhassa verkossa ollut, vaan sen tehtäviä hoiti yksi työasemista. Yhteys Internetiin on luotu ADSL-tekniikan avulla, eli verkossa on ADSL-reititin. Puhelinyhteydet on toteutettu ISDN-tekniikalla.

8.2 Määrittely

Uusissa toimitiloissa on siis valmiiksi pohjalla lähiverkkokaapelointi, jota voidaan käyttää hyödyksi. Liitteessä 12 on esitetty toimiston pohjapiirustus, josta näkyvät sekä vanhat että uudet rasiat. Kaapelointi on tehty kategorian Cat5e kaapelilla ja liittimillä, joten myös verkon laajennuksen tulee täyttää Cat5e-standardin vaatimukset. Työasema joka toimii palvelimena on ylikuormitettu, mikä näkyy palveluiden hitautena. Tiedostot taas sijaitsevat jokaisen koneen omilla kiintolevyillä, mikä vaikeuttaa osaltaan yhteisten tiedostojen lukua. Tulostimet ovat myös asennettuna paikallisesti jokaiseen koneeseen, joten niiden ylläpito on vaikeaa. IP-osoitteiden jakamisesta järjestelmässä vastaa DHCP-palvelin, joka sijaitsee ADSL-reitittimellä. Käytössä on NAT-palvelu, joka muuttaa julkisen osoitteen harmaisiin sarjoihin. Varmuuskopiointi tapahtuu tiedostojen kopioinnilla toisiin työasemiin ja satunnaisilla cd-taltioinneilla. Fici-

Copylla on myös käytössään varasto joka sijaitsee samassa rakennuksessa, mutta sinne ei ole käyntiä toimiston tiloista. Verkkoyhteys on saatava toimimaan myös sillä, jotta kannettavilla tietokoneilla pääsee varastosta käsinkin verkkoon. Verkossa olevilla työasemilla käyttöjärjestelminä toimivat Windows XP Professional ja Windows 2000.

8.3 Suunnittelu

Tieto uusiin toimitiloihin muuttamisesta laittoi alulle uuden verkon suunnittelun. Silloin oli selvää, että vanha tietojärjestelmä on korvattava uudella. Verkossa olevien yhteisten tietojen saatavuus oli saatava helpommaksi ja tiedot oli myös turvattava mahdollisen laitteistovian takia. Samoin palvelimen lisääminen verkkoon oli suunniteltu jo ennalta.

8.3.1 Kaapelointi

Verkon kaapeloinnit toteutetaan suojaamattomalla Cat6-standardin vaatimukset täyttävillä kaapeleilla ja liittimillä. Suojausta ei tarvita, koska kaapelointi tulee tavalliseen toimistotilaan eikä siellä ole suuria häiriölähteitä. Kaapeli ei myöskään ole merkittävästi kalliimpaa kuin Cat5e kaapeli. Toimistotilan rasiat ovat niin sanottuja tuplarasioita, eli niissä on kaksi verkkoliitinpaikkaa. Työpisteille, joissa on kiinteät puhelimet, voidaan toista kaapelia käyttää puhelimen kytkentään, jolloin ei tarvita erillisiä puhelinpistokkeita. Vanhassa verkossa olleita aktiivilaitteita voidaan hyödyntää myös uudessa verkossa. ADSL-reititin ja 16-porttinen 10/100 Mbit/s kytkin toimivat hyvin myös uudessa verkossa.

Uuden verkon pitää kattaa myös eri tilassa sijaitsevavarasto, joten lattiaan on tehtävä läpivienti tai käytettävä langatonta verkkoa. Langattoman verkon rakentaminen on taloudellisesti kannattavampaa, joten verkon tukiasemaksi valitaan D-linkin DI-624+. Kyseisessä tukiasemassa on kaikki tarpeelliset toiminnot, jotta suojattu langaton verkko voidaan rakentaa. Uusia rasioita tehdään kuusi

kappaletta, joista viiteen tulee tuplarasia. Yhteen rasiaan tulee vain yksi liitin WLAN-tukiasemalle. Näin verkko laajenee 11 uudella verkkoliitäntäpisteellä, jotka tulevat työasemien sekä esittelytilan laitteiden läheisyyteen. Lisäksi yksi rasia on varattu WLAN-tukiasemalle.

8.3.2 Palvelimen valinta

Vanha palvelimena toiminut työasema saa väistyä ja tilalle ostetaan nykyaikainen toimistopalvelin. Palvelimeksi valittiin Fujitsu Siemens:in Primergy Econel, joka on niin sanottu kevyt toimistopalvelin. Toimistopalvelimissa on myös koneen käyntiääni saatu hiljaiseksi käyttömukavuuden parantamiseksi. Keveydestään huolimatta Primergy Econel -palvelimessa on virheen korjaavat muistit sekä raid-peilaukset ja palvelin on suunnattu yhtäaikaisesti tiedosto-, tulostus- ja sähköpostipalvelimeksi. Palvelimen valintaan vaikuttivat eniten sen tuki monille eri käyttöjärjestelmille, sekä yrityksen tarpeisiin riittävät ominaisuudet, joiden lisäksi myös hinta oli kohtuullinen.

Palvelin on varustettu pentium-4 -tason suorittimella. Muistia voidaan myös laajentaa tarpeen mukaan neljään gigatavuun asti ja kovalevytilaa asentaa yhteensä 640 gigatavua. Kovalevyiksi voidaan asentaa neljä SATA-levyä. Vakiona koneessa on 512 megatavua muistia, mutta sitä kasvatetaan yhteen gigatavuun. Kovalevynä vakiona oli 80 gigatavuinen SATA-levy, joka korvataan kahdella 160 gigatavuisella SATA-levyllä, jotka on tarkoitus asentaa peilaaviksi. Palvelimessa on myös DVD-ROM- ja levykeasema sekä kuusi USB 2.0 paikkaa. Lisäksi laajennusmahdollisuuksia on yksi PCI Express 8x- ja neljä PCI Express 1x liitäntäpaikkoja, jotka korvaavat vanhat AGP- ja PCI-korttipaikat. Palvelimelle ei tule omaa näyttöä, näppäimistöä tai hiirtä, vaan palvelimen hallinta suoritetaan etänä toiselta koneelta. Mahdollisen vikatilanteen sattuessa siihen kuitenkin liitetään omat hallintalaitteet.

Palvelimen käyttöjärjestelmäksi valitaan Windows 2003 Server, joka on uusin Windows-tuoteperheen palvelinkäyttöjärjestelmä. Windows on yleisesti käytös-

sä toimistoympäristöissä ja siihen on lähes aina olemassa toimivat tulostin- ja muut ajurit saatavilla. Fici-Copylla olisi ollut valmiiksi lisenssit Windows 2000 Serveriä varten, mutta verkkoa varten päätettiin kuitenkin hankkia uudempi käyttöjärjestelmä. Fici-Copy on Microsoft-tuotteiden jälleenmyyjä ja kuuluu Microsoftin ”Partner Program”-ohjelmaan, joka mahdollistaa ”Microsoft Action Pack Subscription”-ohjelmistopaketin ostamiseen ja käyttämisen yrityksen omissa koneissa. Pakettiin kuuluvat kaikki toimistoissa tarvittavat ohjelmistot käyttöjärjestelmistä asiakirjojen muokkausohjelmiin. Samalla päivitetyksi tulevat siis muutkin käytettävät ohjelmat.

Palvelimelle on tarkoitus asentaa huollon seurantaohjelma sekä laskutusohjelma, jotka ovat olleet vanhassa työasemapalvelimessa. Yhteiset tiedostot on tarkoitus tallettaa palvelimen levylle, josta ne on kaikkien helppo hakea. Tiedon varmistus toteutetaan kiintolevyjen peilauksella sekä ajastetuilla varmuuskopioinneilla. Windows 2003 Server on tarkoitus määrittää toimimaan verkon toimialuepalvelimena (domain controller). Palvelimelle on tarkoituksena myös asentaa verkkoskannauksessa tarvittavat ohjelmat, sekä FTP-skannaukseen tarvittava FTP-palvelu. Verkkotulostimien ajurit asennetaan myös palvelimelle. Varmuuskopioinnit datasta suoritetaan joka yö, jolloin ennalta määrätyt tiedostot kopioidaan toiselle työasemalle tai ulkoiselle kiintolevylle. Palvelin toimii siis tulostin-, tiedosto-, ohjelma- ja FTP-palvelimena.

8.3.3 IP-osoitteiden jako

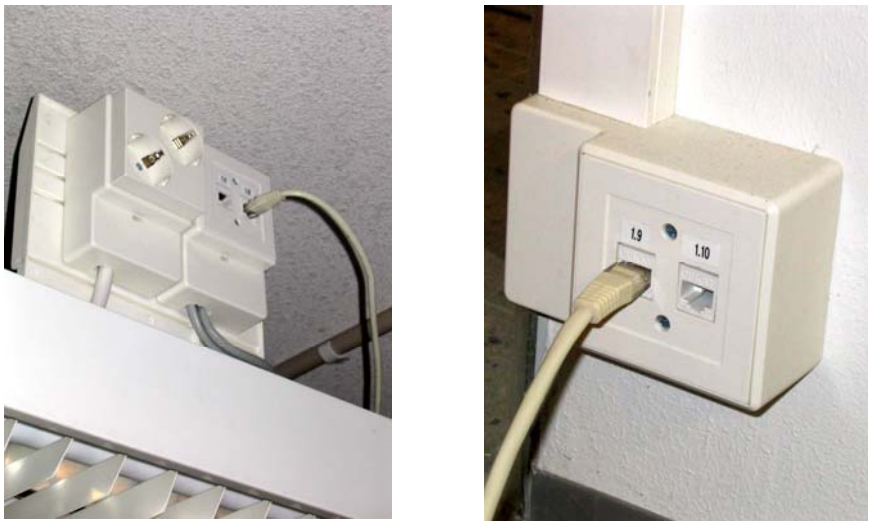
IP-osoitteiden jakaminen suoritetaan DHCP-palvelun avulla NAT-palvelun ollessa edelleen käytössä. Windows 2003 Serveriin olisi mahdollista asentaa DHCP-palvelu, mutta virhetilanteiden takia se on syytä pitää edelleen ADSL-reitittimellä. Palvelimen kaatuessa toimivat siis ainakin Internet-yhteydet. DHCP-palvelin määritellään antamaan työasemille ja palvelimelle IP-osoitteet staattisesti, eli työasemat saavat aina saman IP-osoitteen. Kopiokoneisiin osoitteet voidaan määritellä käsin, tai hakea dynaamisesti DHCP-palvelimelta.

8.4 Toteutus

Verkon suunnittelun ollessa valmis päästään varsinaiseen toteutusvaiheeseen. Verkon osat asennetaan vaiheittain muutaman kuukauden kuluessa, joten kaikki asennukset eivät tapahdu samanaikaisesti. Suunnitelma oli kuitenkin koko ajan tiedossa ja se ei muuttunut projektin aikana merkittävästi. Toimitilaan muuttamisen yhteydessä toukokuussa 2005 tehtiin verkon kaapeloinnin laajennus, jossa oli käytössä aluksi vanha järjestelmä. Langaton lähiverkko asennettiin samaan aikaan kun palvelin eli lokakuussa 2005. Palvelimen asennuksen jälkeen vanha palvelin on varalla verkossa, jos jostain syystä uusi palvelin ei toimisi.

8.4.1 Kaapelointi

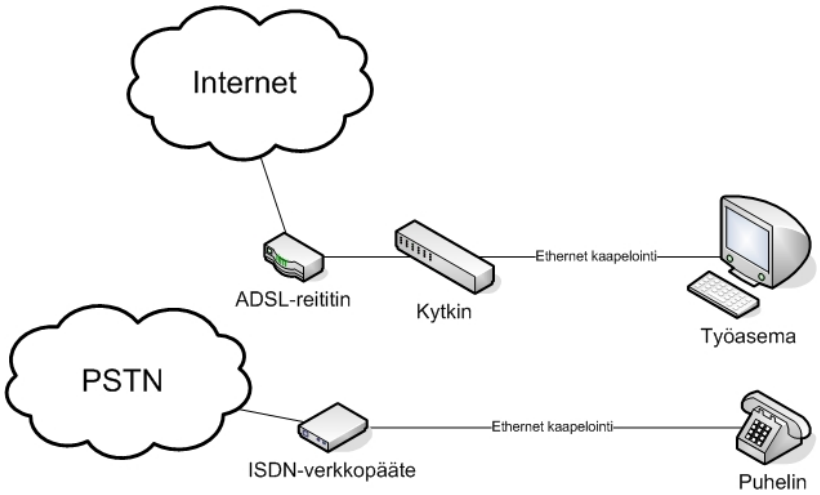
Verkon toteutus aloitetaan uusien verkkorasioiden asennuksella. Asennuksessa käytetään pinta-asennusrasioita, joten varsinaista johtokourua ei tarvitse asentaa (kuva 11). Kaapeleiden vedot viedään välikaton kautta, josta ne tuodaan alas liimalistan avulla. Neuvotteluhuoneeseen rasia sijoitetaan katossa olevaan lamppukiskoon (kuva 11). Rasioita asennetaan siis kuusi kappaletta, joista yhteen tulee vain yksi liitin. Tähän rasiaan liitetään WLAN-tukiasema.



Kuva 11 Lamppukiskoon ja seinään kiinnitetyt rasiat

8.4.2 Aktiivilaitteiden liittäminen

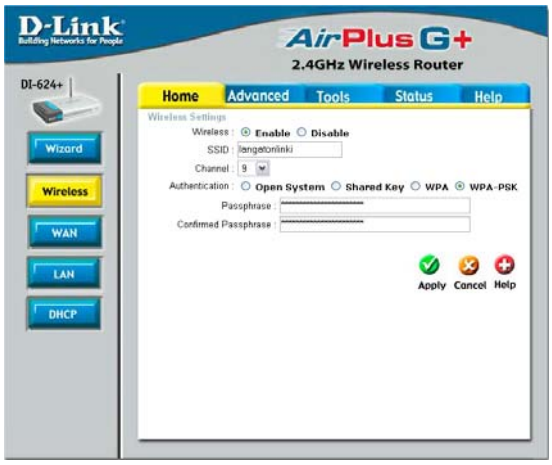
Rasioiden asennuksen jälkeen on testattava niiden toiminta. Aluksi testaus tehdään Fluken Nettool -laitteella, joka kertoo oleelliset verkkotiedot esimerkiksi kaapeleiden oikeista kytkennöistä. Myöhemmin tehdään myös tarkempi mittaus verkolle. Kaapeloinnin olleessa valmis voidaan verkon aktiivilaitteet kytkeä siihen (kuva 12). ADSL-reitittimeltä menee tällöin yhteys kytkimeen, joka jakaa yhteyden. Puhelimet kytketään ISDN-verkkopäätteen perään. Ethernet-kaapelointi mahdollistaa lähiverkon ja puhelinverkon käyttämisen samoissa kaapeleissa. ADSL-reitin toimii DCHP-palvelimena, joka jakaa IP-osoitteet verkkoon. ADSL-reitittimessä on myös NAT-palvelu, joka määritellään käyttöön. NAT-palvelu määritellään niin, että se jakaa C-luokan harmaan sarjan 192.168.200.0 osoitteita. Reitittimen IP-osoitteeksi määritellään 192.168.200.254. Työasemille ja palvelimille määrätään DHCP antamaan osoitteet väliltä 192.168.200.1-10. Loput osoitteet ovat vapaassa käytössä, ja niitä voidaan antaa muun muassa verkossa oleville kopiokoneille ja verkkotulostimille.



Kuva 12 Periaatekuva työasemien ja puhelimien kytkemisestä

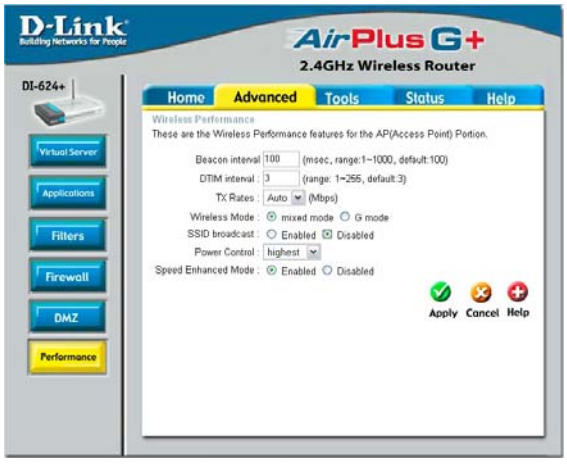
Kuten jo aiemmin mainittiin, WLAN-tukiasemaksi valittiin D-linkin DI-624+ (nopeus 54 Mbit/s), koska kyseisen valmistajan muut tuotteet ovat tuttuja ja asetusten määrittely on niihin helppoa. Ensimmäisenä toimenpiteenä vaihdettiin tukiaseman salasana. Tukiaseman asennuksessa piti myös määritellä oletusar-

voisena ollut DHCP-palvelu pois päältä, jolloin tukiasema hakee IP-osoitteet ADSL-reitittimeltä. Langaton verkko-ominaisuus kytkettiin päälle ja verkolle annettiin SSID-nimi sekä asennettiin suojaus. Suojauksena käytetään WPA-PSK suojausta, jolloin suojausavain määritellään itse tukiasemaan (kuva 13).



Kuva 13 Langattoman lähiverkon määritykset

Lisäksi tukiasemaan otettiin käyttöön MAC-osoitteiden suodatus, johon määritellään kahden kannettavan tietokoneen MAC-osoitteet. Ainoastaan näillä kahdella koneella on mahdollista on siis mahdollisuus liittyä langattomaan verkkoon. Log-tiedostojen seurannan helpottamiseksi tiedostot lähetetään sähköpostilla ylläpitäjälle, joka voi seurata niistä mahdollista langattoman verkon väärinkäyttöä. Langattoman verkon ollessa valmis, sen SSID piilotetaan yleisestä jaosta (kuva 14).



Kuva 14 SSID:n piilottaminen

8.4.3 Palvelimen konfigurointi

Palvelimen asennus aloitetaan lisämuistien asennuksella sekä kiintolevyjen vaihdolla. Tämän jälkeen on vuorossa käyttöjärjestelmän asennus. Fujitsu-Siemens on kehittänyt helpon tavan asentaa käyttöjärjestelmä, ja palvelimen mukana tulevilla käynnistyslevyillä on helppo määritellä asetukset. Ensin valitaan asennettava käyttöjärjestelmä, jonka jälkeen käyttöön tulevat valittua järjestelmää vastaavat ohjeet. Fujitsu-Siemensin levyllä tulevalla ohjelmalla on mahdollista myös muun muassa osioida kiintolevyt sekä määrittää kiintolevyjen RAID-tasot. Käyttöjärjestelmän asennukseen kuluu aikaa muutama tunti, jonka aikana syötetään palvelimelle järjestelmänvalvojan tunnukset ja käyttöjärjestelmän ohjelmistoavaimia. Kun käyttöjärjestelmä on asennettu, on se syytä päivittää. Internet-verkkoon konetta on kuitenkin riski laittaa, jos siinä ei ole ajan tasalla olevaa virustentorjuntaohjelmaa. Virustentorjunta hoidetaan Fici-Copyllä F-Securen ohjelmistoilla, joissa on oma versio palvelimia varten. Samalla päivitetään kaikkiin työasemiin F-Securen virustentorjunta- ja palomuuriohjelmistot. Palvelimelle asennetaan myös F-Secure Policy Manager Console ohjelma, jolla voidaan hallita kaikkia F-Securen ohjelmia verkossa.

Päivitysten ollessa ajantasalla voidaan palvelimelle alkaa määrittelemään asetuksia. Palvelin toimii toimialueen hallintakoneena, joten sitä varten on asennettava Domain Controller (Active Directory), johon määritellään toimialueen nimi ja muut tarvittavat asetukset. Samalla luodaan toimialueeseen liittymiseen tarvittavat käyttäjätunnukset. Tämän jälkeen kaikkien työasemien asetuksia muutetaan siten, että ne liittyvät haluttuun toimialueeseen. Verkkoyhteyksien toimiessa voidaan palvelimelta jakaa kansioita, joihin voidaan siirtää kaikki yhteiset tiedostot, ja samalla määritellä kansioon käyttöoikeudet. Huollonseuranta- ja laskutusohjelmasta otetaan lisäksi vanhasta palvelimesta varmuuskopiot, jotka voidaan siirtää uuteen koneeseen.

Ennen kuin varmuuskopioituja tiedostoja voidaan siirtää vanhalta palvelimelta, pitää kaikkien ohjelmien olla asennettuina ja tarvittavat ympäristömuuttujat määriteltyinä valmiiksi. Työasemille täytyy lisäksi luoda kuvakkeet, joilla huol-

lonseuranta- ja laskutusohjelmia voidaan käyttää. Tulostimia varten asennetaan myös ajurit sekä skannauksia varten vaadittavat ohjelmat ja sallitaan palvelimen etähallintaan määrätyt käyttäjäoikeudet. Palvelimen varmuuskopiointi voidaan ajastaa halutuista tiedostoista Windows 2003 Serverin omalla varmuuskopiointiohjelmalla. Jokaöisen varmuuskopioinnin lisäksi otetaan myös kerran viikossa koko järjestelmästä kopio ulkoiselle kiintolevylle.

8.5 Esittelytilan laitteiden konfigurointi

Fici-Copyn esittelytilaan tulee esittelyyn aina sillä hetkellä markkinoilla olevia kopiokoneita sekä vaihdossa tulleita huollettuja koneita. Kopiokoneet ovat digitalisoituneet, ja niistä löytyy monia eri digitaalisuuden mukanaan tuomia toimintoja. Tämä tarkoittaa muun muassa sitä, että kopiokoneissa on lähes aina mahdollisuudet peruskopioinnin lisäksi tulostukseen, skannaamiseen ja faksin lähettämiseen. Osassa malleista nämä toiminnot löytyvät jo vakiona, mutta joissain malleissa ne ovat saatavana lisäominaisuutena. Värikopiokoneet ovat tulleet myös entistä vahvemmin haastamaan perinteiset mustavalkokopiokoneet, koska niiden käyttökustannukset on saatu lähelle mustavalkokonetta. Samalla ne mahdollistavat myös väriskannauksen. Esittelytilassa on tarkoitus tehdä mahdolliseksi testata koneissa olevia toimintoja. Toiminnot tulisi tehdä siten, että ne kävisivät mahdollisimman monelle eri konemallille.

8.5.1 Tulostusominaisuudet

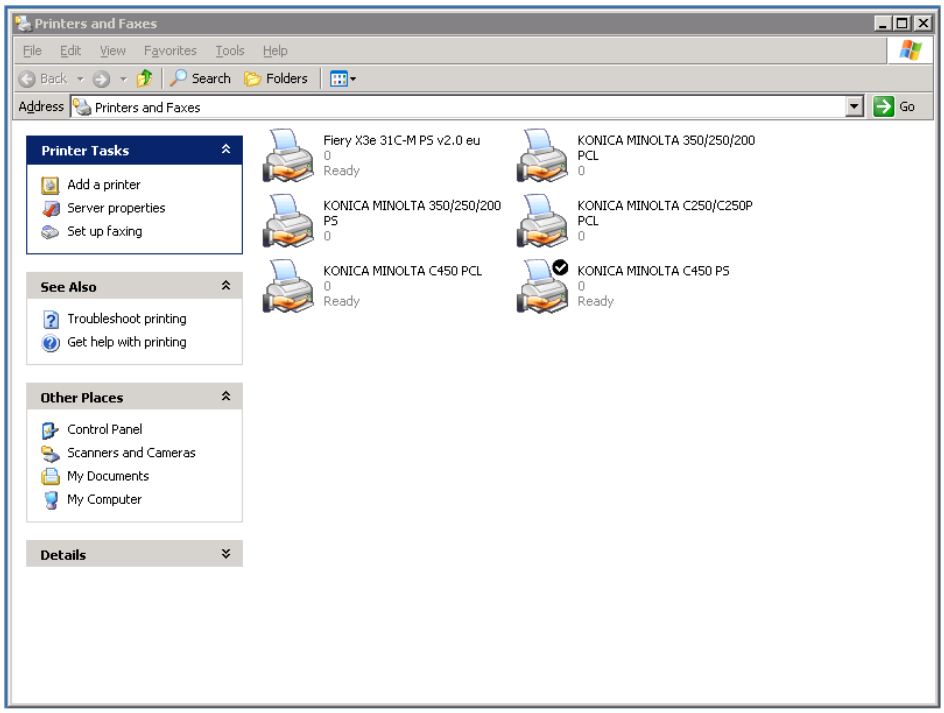
Windows 2003 Serverissä on tulostuspalvelin, joka tarjoaa ja hallitsee verkkoon jaettuja tulostimia, tulostusjonoja ja kirjoitinten laiteohjaimia. Käytännössä kaikista Windows-käyttöjärjestelmistä on mahdollista tehdä tulostuspalvelin. Kopiokoneet liittyvät verkkoon oman verkkokortin kautta, jolloin on mahdollista tehdä tulostinpalvelimelta suoraan TCP/IP-portti, jonka kautta tulostaminen tapahtuu. Harvemmin tämänkokoisissa laitteissa tulostusta hoidetaan USB- tai LPT-tulostusportin kautta. Osassa kopiokoneista on oma tulostuspalvelin, eli tu-

lostimen liittyessä tiettyyn toimialueeseen tai työryhmään on siihen mahdollista tulostaa suoraan ilman erillistä palvelinta. /6, s1009/

Tulostinten lisäämiseksi on Windowsissa olemassa oma ”Add Printer Wizard”, jonka avulla lisääminen on helppoa. Tulostuspalvelimeen liitettävä tulostin lisätään paikallisena kirjoittimena (Local Printer) ja sille luodaan Wizardissa uusi Standard TCP/IP-portti, johon määritellään tulostimen IP-osoite sekä annetaan portille oma nimi. Tämän jälkeen luodun portin asetuksia voidaan muuttaa, kuten esimerkiksi valita erilaisten laitetyyppien omat standardit. Jos tulostusportin asetukset ovat jo etukäteen tiedossa, on mahdollisuus valita myös mukautettu vaihtoehto (Custom). Portin asetuksista pystytään määrittelemään tulostusprotokolla, joka voi olla LPR- tai RAW-muotoa. RAW-tulostusprotokollassa tulostettava data käsitellään tietokoneessa valmiiksi. Pääsääntöisesti kopiokoneissa käytetään LPR-muotoa, jolloin tulostin muokkaa tulosteen itse oikeanlaiseen muotoon. Tällä tavalla tulostuksiin voidaan käyttää muun muassa kaksipuolisuus- tai vihkotoimintoja. LPR-asetuksiin valitaan LPR-jonon nimi, joka on lähes aina PRINT. Haluttaessa käyttää verkonhallintaohjelmia voidaan asetuksiin määritellä SNMP-tila käyttöön. Portin asetusten ollessa kunnossa, kysyy Wizard tulostimen ajuria. Vaikka Windows 2003 käyttöjärjestelmässä on lähes 4000 eri tulostinajuria valmiina, niin kopiokoneiden kaltaisiin monitoimilaitteisiin listasta ei lähes poikkeuksetta löydy sopivaa ajuria. Tämän vuoksi laitevalmistajat toimittavat mukana tulostinajurit. Soveltuvan ajurin asennuksen ollessa valmis, pitää järjestelmään vielä kuitenkin lisätä mahdolliset lisälaiteasetukset kuten kaksipuolisuusyksikkö, viimeistelijä tai lisäpaperikasetit sekä jakaa tulostin muille verkonkäyttäjille. /6, s824/

Kopiokoneet tukevat yleensä PCL- ja PS-tulostuskieliä. PCL (Printer Control Language) on HP:n kehittämä tulostimenohjauskieli ja PS (PostScript) on kehitetty laitteistoriippumattomaksi sivunkuvauskieleksi. On myös mahdollista, että osa ohjelmista tukee vain toista kuvauskieltä. PS-tulostinajuria käytetään yleisemmin paikoissa, joissa tehdään painotuotteita, sen paremman laitteistoyhteensopivuuden vuoksi. /6, s845/

Esittelyverkon tulostus on toteutettu Windows 2003 -palvelimelle (kuva 15), sillä tällä tavoin tulostusjonojen hallinta helpottuu sekä käyttäjien aiheuttamien virheiden todennäköisyys pienenee, kun asetuksia pääsee muuttamaan vain järjestelmän ylläpitäjä. Kopiokoneen laitteiston muuttuessa on helpompaa käydä lisäämässä oikeat asetukset suoraan palvelinkoneelle, kuin käydä lisäämässä asetus jokaiselle työasemalle erikseen. Käyttämällä tulostuspalvelinta voidaan tulostimet jakaa myös helposti kaikille verkon käyttäjille. Esittelyverkossa koneet vaihtuvat usein. Vaihdon tapahtuessa vanhojen tulostusjonojen poistaminen on helppoa suoraan palvelinkoneelta, jolloin myös vanhat koneet poistuvat järjestelmästä. Kun kopiokone tukee molempia tulostuskieliä (PCL ja PS), asennetaan siihen molemmat ajurit. Asiakas voi tällöin päättää itse esittelytilanteessa, kumpaa tulostinkieltä käytetään.

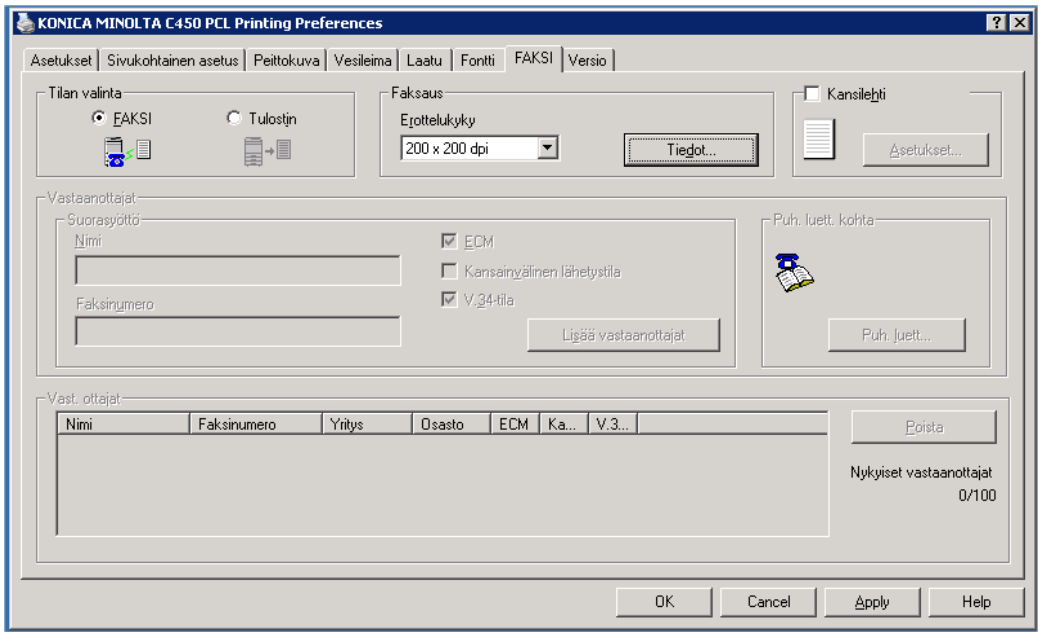


Kuva 15 Windows 2003 palvelimen tulostimet

8.5.2 Faksiominaisuudet

Laitteiden keskittäminen on taloudellisesti kannattavaa ja tilaa säästävää. Kopiokoneet mahdollistavat myös faksien lähetyksen suoraan koneelta. Mahdollis-

ta on myös lähettää niin sanottuja verkkofakseja, eli lähiverkon työasemalta voidaan lähettää suoraan faksi sitä ensin paperiversioksi tulostamatta. Konica Minoltan uusimmissa kopiokonemalleissa on PCL-tulostinajuriin lisätty verkkofaksiominaisuus (kuva 16), jossa koneeseen asennettu faksikortti toimii yhdyskäytävänä puhelinverkkoon ja faksin lähettäminen onnistuu samalla tavalla kuin tulostus. Tulostinajurista valitaan tällöin faksi toiminto ja syötetään käsin vastaanottajan puhelinnumero tai valitaan se ennalta laaditusta puhelinluettelosta. Tämän jälkeen voidaan faksi niin sanotusti tulostaa. Puhelimet käyttävät samoja kaapelointeja, joita käytetään lähiverkossa. Puhelinkeskukset sijaitsevat ristikytkentäkaapeissa, joten faksia varten ei tarvitse enää vetää omia kaapeleita, vaan siihen riittää ainoastaan vapaa lähiverkkorasiapistoke. Tavallisesti kaapelointi tehdään niin sanotulla siamilaisella kaapelilla, jossa kaksi kaapelia on kiinni toisissaan. Usein toinen näistä kaapeleista on varattu juuri puhelinliikenteelle. Esittelyverkossa uusien koneiden kohdalla pelkkä PCL-tulostinajurin asennus mahdollistaa jo verkkofaksin käytön, kun taas vanhemmissa koneissa pitää asentaa erillinen apuohjelma tätä varten. Lisäksi on myös Internet-faksi, joka lähettää skannatut dokumentit sähköpostitse vastaanottajan postipalvelimelle. Sieltä asiakirjat ohjautuvat laitteelle, joka pystyy tulostamaan I-faksilla lähetettyjä tiedostoja. /11, s17/



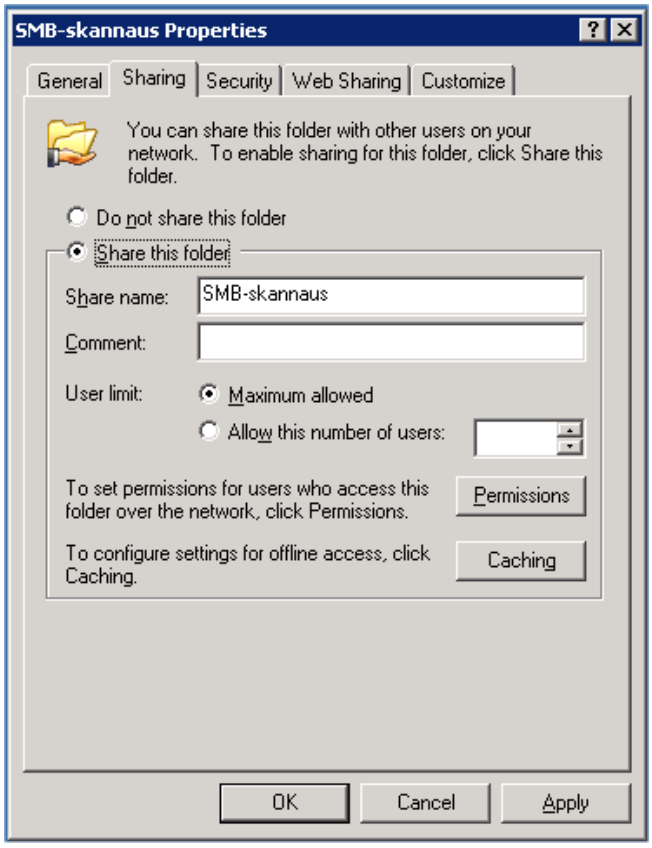
Kuva 16 Konica Minoltan C450 PCL-ajurin faksiominaisuus

8.5.3 Skannausominaisuudet

Asiakirjojen skannaamisesta on tullut luonnollinen osa yrityksen päivittäistä työtä. Paperilla olevat dokumentit skannataan ja arkistoidaan digitaalisina mahdollista myöhempää jakelua ja tulostusta varten. Erilaisia skannaustapoja on useita, joista tavallisimpia ovat skannaus SMB-protokollaa käyttäen, skannaus FTP-palvelimelle, skannaus sähköpostiin, skannaus kopiokoneen kiintolevylle ja TWAIN-skannaus. Lisäksi on olemassa näiden skannausten yhdistelmiä, kuten esimerkiksi URL-skannaus ja HDD-TWAIN-skannaus.

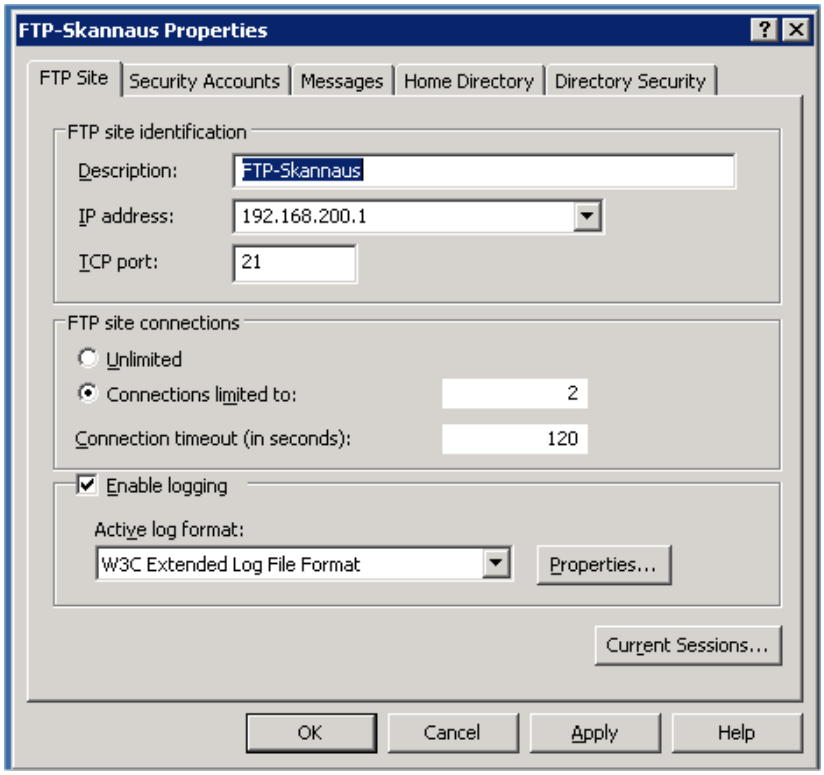
Skannaus SMB:llä (Server Message Block) on vaihtoehto FTP-siirtotekniikalle. SMB-protokolla mahdollistaa tiedostojen luku- ja kirjoitusoikeuden sekä antaa välineet verkkopalveluiden käyttöön. Skannatessa tiedostoon pidetään SMB-protokollaa turvallisempana käyttää kuin FTP-yhteyttä, sillä SMB salaa käytetyt tunnukset, eikä niitä voida tällöin jäljittää verkon kautta. SMB-protokollassa kopiokoneelle määritellään SMB-palvelimen osoite sekä kansion polku, johon skannaukset lähetetään. Palvelimelle on määriteltävä myös kopiokoneen käyttäjätunnukset, jotta kopiokoneella olisi oikeus kirjoittaa kyseiseen kansioon. SMB-palvelimena voi toimia mikä tahansa Windows-käyttöjärjestelmällä toimiva kone.

Kansioiden jakaminen verkossa tekee koneesta SMB-palvelimen (kuva 17). Skannausasetukset määritellään jo skannausvaiheessa kopiokoneelta. Asetuksista voidaan määritellä muun muassa skannattavan dokumentin koko, skannauksen resoluutio, kaksipuoleisuus, värit ja tiedostomuoto. Lisäksi sillä pystytään määrittelemään myös alkuperäisen dokumentin tyyppi, esimerkkeinä mainittakoon muun muassa teksti, kuva, kartta, pistematriisi, tulostettu kuva tai valokuva. Tiedostomuotoina käytetään ainoastaan TIFF-, PDF- tai JPG-muotoa, joista PDF-tiedostoon on mahdollista skannata monisivuinen dokumentti. Dokumenttien jatkokäsittely tapahtuu yleensä kuvankäsittely- ja tekstintunnistusohjelmilla. Valmis tiedosto siirretään SMB:n avulla jaettuun kansioon. /11, s5; 27/



Kuva 17 SMB-kansion jakaminen Windows 2003 palvelimella

FTP-skannaus on periaatteeltaan sama kuin SMB-skannaus, mutta dokumentit tallennetaan jaetun kansion sijaan FTP-palvelimelle. Palvelin voi olla yrityksen oma tai ulkopuolisen ylläpitämä. Skannattu dokumentti voidaan hakea FTP Client -ohjelmalla. Yleisimmin käytetty tapa on kuitenkin jakaa kansio johon skannattiin, jolloin käyttäjä voi hakea tiedostot suoraan verkon läpi. Tämä onnistuu ainoastaan silloin, kun FTP-palvelin on samassa verkossa muiden koneiden kanssa. Kopiokoneen mukana tulee Konica Minoltan kehittämä PageScope Cabinet -ohjelmisto, jonka avulla tavallinen työasema voidaan tarvittaessa mukauttaa FTP-palvelimeksi. Tällöin kopiokoneeseen pitää vain määritellä FTP-palvelimen osoite sekä kansio johon skannataan. Lisäksi tarvitaan myös käyttäjätunnukset, jotta FTP-palvelimelle voidaan kirjautua, vaikkakin kirjautuminen on mahdollista tehdä myös tuntemattomana ilman käyttäjätunnuksia. Tietoturvasyistä on kuitenkin kannattavampaa käyttää käyttäjätunnuksia. Esittelyverkossa FTP-palvelimeksi määriteltiin Windows 2003 -palvelin, koska kyseisessä käyttöjärjestelmässä on vakiona FTP-palvelintoiminto (kuva 18). /11, s11; 27/



Kuva 18 FTP-palvelimen määrittely Windows 2003 -palvelimella

Palvelimen asetuksissa määritellään toiminnoille nimi sekä palvelimen IP-osoite ja TCP-portti, joiden lisäksi kopiokoneelle luodaan käyttäjätili ja määritellään FTP-juurikansio. Directory Security -kohdasta sallitaan myös verkon työasemien pääsy FTP-palvelimelle. Määritykset tehdään IP-osoitteen perusteella. Tietoturvasyistä muut IP-numerot on estetty. /11, s11/

Sähköpostiin skannaaminen on yleistynyt skannausmuotona. Siinä kopiokone lähettää sähköpostia suoraan siihen määriteltyihin osoitteisiin, ja skannattu dokumentti tulee sähköpostin liitteeksi. Liitteet voivat olla joko TIFF-, PDF- tai JPG-muodossa. Skannauksen ainoa merkittävä rajoitus on liitetiedostojen enimmäiskoko, kun taas FTP- ja SMB-skannauksessa ei ole tiedoston enimmäiskokoa. Sähköpostiin skannaaminen on suorin tapa siirtää dokumentit vastaanottajan PC:lle. Kopiokoneelle pitää määritellä yrityksen lähtevän sähköpostipalvelimen nimi (SMTP-palvelin). Konica Minoltan kopiokoneiden etähallinta perustuu myös sähköpostien lähettämiseen. Tällöin kopiokoneeseen pitää määritellä myös oma sähköpostitili. /11, s3; 27/

Koneen kovalevylle skannaaminen eli HDD-skannaaminen vaatii kopiokoneeseen luonnollisesti kovalevyn. Useimmissa konemalleissa se on vakiona ja kaikissa suuremmissa koneissa lisävarusteena. Kiintolevylle voidaan luoda käyttäjälaatikoita, joihin käyttäjät voivat skannata dokumentteja, jolloin kiintolevy toimii väliaikaisena tiedostopalvelimena. Käyttäjälaatikoihin voidaan määritellä myös salasanat, jolloin tiedostot pysyvät salassa. Käyttäjälaatikosta voidaan tiedostot hakea kopiokoneen mukana tulevalla PageScope Box Operator-ohjelmalla, tai HDD-TWAIN-ajurilla. Ajuri toimii samalla tavalla kuin perinteinen TWAIN-ajuri, mutta se hakee tiedot kopiokoneen kovalevyltä. Esittelytilassa HDD-TWAIN-ajuri asennetaan jollekin työasemista. /11, s7; 27/

TWAIN-skannaus on yleisin skannaustapa pienillä tasoskannereilla. Isojen asiakirjojen skannaamiseen sitä pidetään hieman monimutkaisena. Skannaus tapahtuu tietokoneelta, josta skanneri pystyy siirtämään tietoa ohjelmasovelluksiin. Esimerkiksi kuvankäsittelyohjelmasta käynnistetään TWAIN-ajuri, joka skannaa kopiokoneessa olevat dokumentit. Dokumentit on siis käytävä asentamassa kopiokoneeseen ensin ja tämän jälkeen on palattava tietokoneelle skannaamaan. Usein kopiokone voi olla kaukana käyttäjästä, jolloin käyttäjä joutuu kulkemaan edestakaisin tietokoneen ja kopiokoneen väliä. TWAIN-skannauksen suurin etu on skannattujen kohteiden siirto mihin tahansa TWAIN-yhteensopivaan ohjelmaan. Esittelytilassa TWAIN-ajuri asennetaan jollekin verkon työasemista, mistä se on helppo esitellä asiakkaille. /11, s9; 27/

URL-skannaus vaatii toimivan FTP- ja sähköpostiskannauksen. URL-skannauksessa dokumentit skannataan FTP-palvelimelle ja vastaanottajille ilmoitetaan erikseen sähköpostitse FTP-palvelimen sijainti. Varsinaiset URL-asetukset määritellään suoraan kopiokoneelle. URL-skannaus on hyvä ratkaisu kookkaiden asiakirjojen jakeluun, sillä siinä yhdistyvät sekä FTP-skannauksen että sähköpostiskannauksen edut, sillä sovellus pystyy käsittelemään suuriakin tiedostoja ja ilmoittamaan niistä vastaanottajalle sähköpostitse. Sähköpostiin tulee tällöin linkki, josta tiedoston voi hakea. Esittelytilassa on mahdollisuus URL-skannaukseen FTP-palvelimen ja sähköpostitilien takia, mutta skannatun tiedoston pystyy hakemaan vain lähiverkon koneilta, koska FTP-palvelimelle pääsy on evätty muista. FTP-palvelu ei näy verkosta ulospäin. /11, s15; 27/

8.6 Testaus

Lähiverkon testaus aloitetaan kaapelointitestauksella, jossa apuvälineenä käytetään Fluken NetTool-mittalaitetta. NetTool kertoo verkosta perustietoa muun muassa kaapelin johdinparien kytkennöistä. NetTool olisi itsessäänkin riittävä mittauslaite verkkotoimintaa varten, mutta verkko päätettiin mitata vielä Fluken DSP-4100-mittalaitteella, missä on automaattinen testaus Cat5e-standardille. Tällöin mittauksista saadaan kattavammat. Mittauslaitteita on kaksi, joista hallintalaitteella käynnistetään mittaukset ja etälaite, joka toimii kaapelin toisessa päässä. Osa mittauksesta tehdään kumpaakin suuntaan, eli etälaite suorittaa samat mittaukset kuin hallintalaite. Mittalaitteen päivityksellä sekä mittapäiden vaihdolla voidaan mitata myös muita kategorioita. Uusien verkkorasioiden mittaustulokset on esitetty liitteissä 1-11. Tuloksista nähdään mitatut ominaisuudet sekä vaihtelurajat. Ensimmäisenä tuloksissa on johtokartta (Wire Map), joka näyttää miten johdinparit on kytketty ja ovatko ne standardin mukaisia (PASS). Seuraavaksi näkyy jokaisen parin mitattu pituus (Length), jossa raja-arvona on 94 metriä (standardipituus). Kaapelin yhteispituus saa olla yhteensä 100 metriä, kun siihen lasketaan myös työasema- ja ristikytkentäkaapelit. Kolmannessa vaiheessa mitataan etenemisviive (Prop. Delay) ja viiveenvääristymä (Delay Skew) sekä parien impedanssit (Impedance) ja vaimentumiset (Attenuation). Vaimentumisen mittaamiseen on käytetty 100 MHz taajuutta, joka on Cat5e -standardin taajuuskaistan yläraja. Muut mittaukset kuten heijastus- ja ylikuuluvuusmittaukset on tehty kaapeleille molemminpuolisesti. Hallintalaitteen tulokset on merkitty Main Results -merkinnöin ja etälaitteen Remote Results -merkinnöin.

Langattoman verkon testauksessa yhdistettiin kannettava tietokone lähiverkkoon langattoman verkkokortin kautta, sekä syötettiin verkon SSID-nimi sekä WPA-salausavain. Tämän jälkeen kone yhdistettiin langattomaan verkkoon. Verkkoyhteys toimii, jos tietokone saa DHCP-palvelimelta oikean IP-osoitteen. Palvelimen asetuksia testataan liittämällä jokin työasema palvelimen ylläpitämään toimialueeseen. Liittyminen vaati uusien käyttäjätunnusten ja salasanojen käyttöä. Toimialueeseen liittymisen jälkeen voidaan testata toimivatko palvelimeen muun muassa asennetut laskutus- ja huollonseurantaohjelmat.

8.7 Käyttöönotto

Verkon käyttöönotto toteutetaan kolmessa osassa. Ensimmäisessä osassa otetaan käyttöön lähiverkkokaapelointi, jossa pyöritettiin vanhaa järjestelmää. Kaapelointi toimi odotetusti, eikä siinä ollut ongelmia. Toisessa vaiheessa lisätään palvelin verkkoon. Samalla muuttuvat kirjautumiskäytännöt sekä kaikki muutkin verkkotoiminnot. Vanha työasemapalvelin jätetään toimimaan uuden palvelimen rinnalla ongelmien varalta. Alussa ongelmia odotetusti aiheuttivat uudet virustentorjunta- ja palomuuriohjelmat, mutta palomuurinohjelman asetusten muokkaamisen jälkeen saatiin verkkoyhteydet toimimaan. Huoltoseurannan tulostuskäytäntöä jouduttiin myös muuttamaan, ja palvelimen LPT1-porttiin oli lisättävä lasertulostin. Tämä tulostin on ainoastaan käytössä huoltoseurantaohjelman raporteille. Lisää odotettuja ongelmia aiheuttavat myös käyttäjien väärät kirjautumiset, jolloin verkkoyhteydet eivät toimi. Esittelylaitteiden ominaisuuksien esittely onnistuu kuitenkin käyttäjille pidettävän käyttökoulutuksen jälkeen.

Kolmannessa vaiheessa vanha työasemapalvelin sammutetaan ja siitä otetaan varmuuskopioinnit mahdollista myöhempää käyttöä varten. Samalla tehdään käyttäjien toivomia muutoksia verkkoon, kuten luodaan uusia verkkolevyjä sekä lisätään käyttäjäoikeuksia.

8.8 Ylläpito

Verkon ylläpito alkoi heti palvelimen liittämisen yhteydessä, jolloin IP-osoitteiden muutokset ja muut verkon tilastot dokumentoitiin. Mahdollisessa vikatilanteessa on tällöin hyvät edellytykset palauttaa järjestelmän tiedot, koska varmuuskopiot otetaan säännöllisesti sekä palvelimen kiintolevyt on peilattu. Ylläpito jatkuu verkossa koko ajan ja mahdolliset muutokset järjestelmään kirjataan säännöllisesti.

9 YHTEENVETO

Tietokoneverkot ovat tulleet pysyvästi helpottamaan ihmisten elämää, ja uusien käyttömahdollisuuksien vuoksi verkolta tullaan vaatimaan koko ajan nopeampia yhteyksiä. Jatkuva kehitys vaatii myös verkon säännöllistä päivitystä ja ylläpitoa luoden samalla lisää työpaikkoja. Tämän päivän yrityksessä on lähes poikkeuksetta jonkinlainen verkkojärjestelmä, joka voi pienimmillään olla yksi tietokone ja Internet-yhteys tai suurimmillaan jopa tuhansien ympäri maapalloa sijoittuneiden laitteiden kokoisuus. Verkon pohjimmaisena tavoitteena on kuitenkin yrityksen tai ihmisen päivittäisen tiedonsiirron helpottaminen.

Tutkintotyössä suunniteltiin ja toteutettiin lähiverkko alle kymmenen henkilön yritykselle. Työn tarkoituksena oli asentaa verkkoon toiminnot päivittäiseen käyttöön, sekä laatia esittelytilan laitteille omat määritykset asiakasesittelyjä varten. Työskentelen itse kyseisessä yrityksessä, joten vanhassa verkossa olleet viat olivat tuttuja. Verkon suunnittelu- ja toteutusprojekti kesti yhteensä noin puoli vuotta aloitettuna toukokuussa 2005 ja valmistuen joulukuussa 2005. Verkko on ollut käytössä joulukuusta 2005 lähtien eikä siinä asennuksen jälkeen ole ilmennyt suurempia ongelmia. Palvelimeen asennettu toimialuetoiminto osoittautui hyväksi vaihtoehdoksi, sillä näin tiedostojen käyttö on helpompaa ja jakotoiminnot toimivat luotettavasti. Esittelytilojen helppous on saanut kiitosta niin työntekijöiden kuin asiakkaidenkin taholta. Suurin puute on ollut keskittyminen ainoastaan Windows-työasemien esittelyyn. Pääsääntöisesti yrityksillä on käytössään Microsoftin käyttöjärjestelmät, mutta varsinkin kuvankäsittelyyn ja taitto-ohjelmiin käytössä ovat usein Macintosh-koneet. Samoin tulostimia tulee usein Unix- tai Linux-koneille.

Projektin edetessä syntyy usein uusia ideoita. Tutkintotyön kirjoitushetkellä toteutuksen alla onkin jo kopiokoneiden etähallintajärjestelmä, jonka on tavoitteena valmistua kesällä 2006. Tarkoitus on saada asiakkailla olevista kopiokoneista etänä tietoja helpottamaan huollon toimintaa. Lisäksi suunnittelussa ovat huollonseurantaohjelman etäkäyttö, sekä erillisen tiedostopalvelimen asennus.

LÄHTEET

Painetut lähteet:

1. Jaakonhuhta, Hannu: Lähiverkot – Ethernet 4. uudistettu painos. IT Press. Helsinki 2005. 380 s.
2. Hakala, Mika – Vainio, Mika: Tietoverkon rakentaminen 1. painos. Docendo Finland Oy. Porvoo 2005. 428 s.
3. Keogh, Jim: Verkkotekniikat tehokas hallinta. IT Press. Helsinki 2001. 391 s.
4. Hunt, Graig: TCP/IP verkonhallinta. O'REILLY/Suomen STK-kustannus. Helsinki 1998. 604 s.
5. Ogletree, Terry: Inside Verkot. IT Press/Edita. Jyväskylä 2001. 901 s.
6. Kivimäki, Jyrki: Windows 2003 Server - Tehokas hallinta. Readme.fi. Helsinki 2005. 1424 s.
7. Puska, Matti: Langattomat lähiverkot. Talentum. Helsinki 2005. 294 s.
8. Puska, Matti: Lähiverkkojen tekniikka –Pro Training. satku.fi. Jyväskylä 2000. 348 s.
9. Seppälä, Kimmo – Brandt, Andrew: Langaton turvasi kaipaa päivitystä. Mikro PC 2/2006, s.14
10. Tuurala, Antti: Salaa aaltosi. MikroBitti 2/2006, s. 91-93
11. Skannausopas. Konica Minolta Business Solutions Europe GmbH: Saksa 2005. s. 22
12. Kiianmies, Matti: Windows XP tehokaskäyttö 4.uudistettu painos. IT Press. Helsinki 2005. 846 s.

Sähköiset lähteet:

13. Kallionpää, Risto, lab.ins. [PPT] Luentomoniste, tietokoneverkot S4277-12, S4277-12.ppt, syksy 2005, Tampereen ammattikorkeakoulu
14. Wikipedia. [www-sivu]. [viitattu 13.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Token_Ring

15. IANA. [www-sivu]. [viitattu 20.3.2006] Saatavissa:

http://www.iana.org/

16. IETF. [www-sivu]. [viitattu 20.3.2006] Saatavissa: http://www.iana.org/
17. Wikipedia. [www-sivu]. [viitattu 20.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/DHCP/
18. Wikipedia. [www-sivu]. [viitattu 20.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Nat
19. IANA. [www-sivu]. [viitattu 22.3.2006] Saatavissa: http://www.iana.org/
20. Kallionpää, Risto, lab.ins. [PDF] Luentomonisteet, tietokoneverkkojen jatkokurssi S4278-4, IPv4vsIPv6.pdf, syksy 2005, Tampereen ammattikorkeakoulu
21. Kallionpää, Risto, lab.ins. [PPT] Luentomonisteet, tietokoneverkkojen jatkokurssi S4278-4, IPv4-6.ppt, syksy 2005, Tampereen ammattikorkeakoulu
22. Wikipedia. [www-sivu]. [viitattu 27.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Ethernet
23. Wikipedia. [www-sivu]. [viitattu 27.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Cat5
24. Kerman. [www-sivu]. [viitattu 28.3.2006] Saatavissa: http://www.kerman.fi/Q & A_Index.htm
25. MikroBitti, [www-sivu]. [viitatut 28.3.2006] Saatavissa: http://www.mbnet.fi/jutut/perusohjelmat/virus.html
26. Wikipedia. [www-sivu]. [viitattu 29.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/RAID
27. Konica Minolta Business Partner Finland. [PDF]. Bizhub C450 Verkkoskanneritoiminnot. C450_Verkkoskanneritoiminnot_1-1-1_FIN.pdf, Saatavissa Konica Minolta jälleenmyyjät ja Konica Minolta Business Partner Finland.

LIITTEET

Liite 1 Verkkorasian 1.1 mittauspöytäkirja

Liite 2 Verkkorasian 1.2 mittauspöytäkirja

Liite 3 Verkkorasian 1.3 mittauspöytäkirja

Liite 4 Verkkorasian 1.4 mittauspöytäkirja

Liite 5 Verkkorasian 1.5 mittauspöytäkirja

Liite 6 Verkkorasian 1.6 mittauspöytäkirja

Liite 7 Verkkorasian 1.7 mittauspöytäkirja

Liite 8 Verkkorasian 1.8 mittauspöytäkirja

Liite 9 Verkkorasian 1.9 mittauspöytäkirja

Liite 10 Verkkorasian 1.10 mittauspöytäkirja

Liite 11 Verkkorasian 1.11 mittauspöytäkirja

Liite 12 Fici-Copy Ky:n toimiston pohjapiirros