TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUDEN YKSIKKÖ

TUTKINTOTYÖRAPORTTI

IT-JÄRJESTELMÄN KEHITTÄMINEN SEURAKUNTAYMPÄRISTÖSSÄ
Case: Ylöjärven seurakunta

Matti Turunen

Tietojenkäsittelyn koulutusohjelma
Toukokuu 2006
Työn ohjaaja: Harri Hakonen

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUDEN YKSIKKÖ

Tekijä(t): **Matti Turunen**

Koulutusohjelma(t): **Tietojenkäsittely**

Tutkintotyön nimi: **IT -järjestelmän kehittäminen seurakuntaympäristössä Case: Ylöjärven seurakunta**

Työn valmistumis-kuukausi ja -vuosi: **Toukokuu 2006**

Työn ohjaaja: **Harri Hakonen** Sivumäärä: **67**

TIIVISTELMÄ

Tutkintotyöni käsittelee Ylöjärven seurakunnan IT-järjestelmän kehittämistä. Kokonaisuus on laaja. Siihen kuuluvat seurakunnan tietoverkko, verkkoon kytketyt laitteet sekä käytettävät tietojärjestelmät, ohjelmistot ja verkkopalvelut. Erityistä huomiota vaatii toiminta seurakuntaympäristössä, osana valtakunnallista KIRKKO-verkkoa.

Seurakunnassa oli ajankohtaista vanhentuneen tietoverkon uusinta ja laajentaminen uusiin toimipaikkoihin, sekä siirtyminen NT4-toimialueesta Active Directoryn käyttöön. Työssäni kuvaan näiden muutosten suunnittelua, asennusta ja dokumentointia.

Käytössä olleesta IT-järjestelmästä tehtiin laajamittainen kartoitus, jossa kerättiin toiminnan kannalta tarpeelliset tiedot järjestelmän eri osa-alueilta. Tiedot kerättiin pääasiassa käsin. Kerätyn tiedon pohjalta laadittiin selkeä ja helposti ylläpidettävä dokumentaatio. Tätä dokumentaatiota käytettiin suunnittelun pohjana ja sitä ylläpidettiin toteutuksen etenemisen yhteydessä.

Seurakunnan verkossa oli alun perin kaksi toimipistettä. Käytössä oli 25 työasemaa ja kaksi palvelinta. Verkkoa laajennettiin kattamaan viisi toimipistettä. Työasemien määrä kasvoi yli 40:een. Palvelimista toinen päivitettiin ja toinen poistettiin käytöstä. Toimipisteiden lähiverkot toteutettiin kytkimillä ja yhdistettiin toisiinsa sillatuilla WLAN- ja xDSL-yhteyksillä. Käyttöön otettiin VLANit ja verkkoon liitettiin taloautomaatiojärjestelmä.

Active Directory -hakemistopalvelu on Microsoftin palvelinkäyttöjärjestelmien osa. Microsoftin nykyiset toimialueet perustuvat Active Directoryyn. Active Directoryssä hyödynnetään LDAP-standardia. Sen avulla voidaan hallita verkon käyttäjiä, työasemia, käyttöoikeuksia sekä jaettuja resursseja. Nimiosoituksessa käytetään DNS-palvelua. Siirtyminen NT4 -pohjaisista järjestelmistä Active Directoryn käyttöön on yleistä. Tähän on syynä se, että Microsoftin tarjoama NT4-tuki loppui vuosien 2004–2005 vaihteessa.

Dokumentointi on IT-järjestelmien hallinnan ja ylläpidon perusedellytys. Järjestelmien kehittäminenkin perustuu aina olemassa olevaan tietoon järjestelmien nykytilasta. Oikein toteutetulla dokumentoinnilla voidaan varautua erilaisiin uhkiin, kuten tulipalot, varkaudet ja vesivahingot. Dokumentoinnilla myös turvataan toiminnan jatkuminen. Hyvä dokumentaatio sisältää riittävän tarkat tiedot ja kuvauksen järjestelmästä. Mikäli vastuuhenkilöt vaihtuvat, tarvittava tieto on edelleen saatavilla.

Avainsanat: KIRKKO-verkko Tietoverkko Tietojärjestelmä Aktiivihakemisto Dokumentointi

TAMPEREEN
AMMATTIKORKEAKOULU
BUSINESS SCHOOL

Author(s): **Matti Turunen**

Degree Programme(s): **Business Information Systems**

Title: **Developing an IT-system for parish administration - a case study of the Parish of Ylöjärvi**

Month and year: **May 2006**

Supervisor: **Harri Hakonen** Pages: **67**

ABSTRACT

My thesis describes the development of the IT-system used by the parish of Ylöjärvi. The subject is comprehensive. It covers the church's information network and equipment connected to it as well as used information systems, software and network services. Special attention is required in working with a church environment and a part of the nation wide KIRKKO-verkko network.

In the parish of Ylöjärvi it was time to renew the outdated network and expand it to new locations. Also upgrading from NT4-domain to Active Directory was current. In this thesis I describe the planning, installation and documentation of these changes.

IT-system used in the parish was mapped out completely. All necessary information was gathered from different parts of the system. This was mainly done by hand, on-site. A well organized and easily updateable documentation was made from the gathered information. This documentation was the base of planning changes in the system and it was updated throughout the implementation.

Originally the parish's network covered two locations. There were 25 workstations and two servers. The network was extended to cover five locations. The number of workstations crew to over 40. One of the servers was upgraded and the other one removed from the system. The LANs in different locations were build using switches and they were connected together with bridged WLAN- and xDSL-connections. VLANs were implemented and the building automation system was connected to the network.

Active Directory is a part of Microsoft's server operating systems. Today Microsoft's domains are based on Active Directory. Active Directory uses LDAP-standard. It can be used to manage users, workstations, user rights and shared resources in a network. DNS is used for name services. Upgrading from NT4 based system to Active Directory is common. This is because Microsoft ended its support for NT4 at the end of year 2004.

Documentation is a fundamental requirement for administration and maintenance of IT-systems. Developing these systems is always based on information about their current state. Proper documentation can be used to prepare for different kinds of threats, such as fires, thefts and water damages. Documentation also provides security and continuity. A good documentation contains adequate information and descriptions about the system. If the responsible people change, needed information is still available.

Keywords: KIRKKO-verkko, Information network, Information system, Active Directory, Documentation

SISÄLLYSLUETTELO

1 Johdanto

Tutkintotyöni aiheena on Ylöjärven seurakunnan IT-järjestelmän päivityksen suunnittelu ja toteutus. Tarkoitus oli kehittää järjestelmä vastaamaan seurakunnan tarpeita nyt ja tulevaisuudessa. Kokonaisuuteen kuului myös päivitetyn järjestelmän dokumentointi; kuvaus siitä, miten järjestelmän eri osat toimivat ja kuinka ne on asennettu.

Työssäni pyrin myös kuvaamaan tämän tyyppisen projektin eri vaiheet, organisoinnin, etenemisen ja ongelmat. Näitä asioita käsittelen nimenomaan seurakuntaympäristöissä toimittaessa.

Varsinaisen työn suoritin päivätyöni yhteydessä. Toimin kyseisen toteutuksen toimittajan (Tamico Systems Oy) vastuuhenkilönä. Tehtäviini kuului järjestelmän päivityksen suunnittelu, varsinaisten muutosten toteutus ja/tai niiden valvonta sekä dokumentointi. Luonnollisesti hyödynsin tätä yhteyttä tutkintotyössäni.

1.1 Työn tarkoitus ja sisältö

Projektin tarkoituksena oli ”yksinkertaisesti” luoda Ylöjärven seurakunnan käyttöön aiempaa parempi IT-järjestelmä. Tavoitteena oli vastata kaikkien seurakunnan työntekijöiden, hyvinkin erilaisiin, tietoteknisiin tarpeisiin. Tämä järjestelmä (laitteineen, ohjelmistoineen ja käytettyine tekniikoineen) tuli dokumentoida mahdollisimman tarkasti ja yksityiskohtaisesti. Myös käytetyistä asennus- ja päivitysmenetelmistä haluttiin dokumentit.

Tutkintotyöni olen pyrkinyt jäsentämään selkeäksi kokonaisuudeksi. Tavoitteeni oli rakenteeltaan ja etenemiseltään looginen raportti toteutetusta järjestelmästä ja siihen liittyneistä vaiheista. Pyrin tarkkaan ja laajuudeltaan riittävän kattavaan kuvaukseen kyseisestä toteutuksesta.

Työn kohteena ollut järjestelmä sekä siihen kohdistuneet muutokset on esitetty liitteissä 2-5. Liitteistä selviää järjestelmän eri ”kehitysvaiheet” sekä siihen kulloinkin liitettyjen laitteiden määrät.

Tutkintotyöni sisällön on tarkastanut ja hyväksynyt toimeksiantajan edustaja. Työstä on jätetty pois tai muutettu kaikki arkaluontoinen, kyseistä organisaatiota ja/tai järjestelmää koskeva informaatio (toimipaikat, tarkat sijainnit, laite- ja käyttäjänimet, TCP/IP-osoitteet ja -portit, käytetyt laite- ja ohjelmistoasetukset, salaukset jne.). Järjestelmästä on projektin aikana luotu erillinen tekninen dokumentaatio.

1.2 Aiheen valinta ja rajaus

Olin jo pitkään opintojeni edetessä miettinyt sopivaa asiakokonaisuutta tutkintotyöni aiheeksi. Alusta asti minulle oli selvää, että tulisin tekemään opinnäytetyöni jostakin todellisesta projektista. Toteutuksesta, jossa olen mukana työelämässä ja joka liittyy varsinaisiin työtehtäviini hyvin kiinteästi. Alkuvuodesta

2004 tuli ajankohtaiseksi aloittaa suunnittelu IT-järjestelmän kehittämisestä ja päivittämisestä Ylöjärven seurakunnassa. Kyseisen tietojärjestelmän ylläpidossa olen ollut mukana jo pidempään. Tässä vaiheessa oli helppo tehdä päätös työn aihevalinnasta. Kun vielä sekä toimeksiantajani, että työnantajani olivat suostuvaisia (ja jopa tyytyväisiä) ehdotukselleni, oli minulla opinnäytetyön aihe valittuna marraskuussa 2004.

Tutkintotyötä ja varsinaista järjestelmän päivitystä tehtäessä nousi esiin lukuisia eri osakokonaisuuksia. Nämä kaikki liittyivät tavalla tai toisella omana tehtävänäni olevaan kokonaisuuteen. Osittain joudun selkeyden vuoksi sivuamaan näitä IT-järjestelmään ”liittyviä” asioita raportissani. Pyrin kuitenkin rajaamaan työni kokonaisuudeksi, joka käsittelee pääasiassa seurakunnan tietoverkkoa, siinä käytettäviä tietojärjestelmiä sekä niihin kohdistuneita muutoksia ja päivityksiä. Tämä on omaa osaamisaluettani ja mahdollisimman lähellä minun osuuttani ja työkuvaani kyseisen järjestelmän ympärillä.

1.3 Toimeksiantaja esittely

Toimeksiantaja työlleni on Ylöjärven seurakunta. Ylöjärven seurakunta on tyypillinen Tampereen seutukunnan itsenäinen seurakunta (toisin kuin esimerkiksi Tampereen alueella toimiva seurakuntayhtymä, joka on usean eri seurakunnan yhteinen hallinnollinen kokonaisuus). Seurakunta toimii luonnollisesti Ylöjärven kaupungin alueella, kuten Kirkkolaki kunnan ja seurakunnan alueen yhdenmukaisuudesta edellyttää. Seurakunta hoitaa Ylöjärven alueella sille säädetyt yhteiskunnalliset palvelut ja vastuut: väestötietojen ylläpito, hautaustoimi ja hengelliset palvelut. Seurakunta työllistää noin 75-100 henkilöä ja sillä on useita eri toimipaikkoja: toimistoja, kirkkoja, leirikeskuksia ja kerhotiloja.

Ylöjärven seurakunnalla on haasteena jatkuva palveluiden kysynnän kasvu. Sama ongelma on monella muullakin, nopean väestönkasvun omaavan kunnan, seurakunnalla. Kunnan väestömäärä kasvaa, jolloin myös seurakuntalaisten määrä kasvaa. Joudutaan tarjoamaan entistä enemmän erilaisia palveluita, niin seurakuntalaisille, kuin muullekin väestölle. Tämä tarkoittaa jatkuvaa lisäystä henkilöstöön, toimitiloihin sekä muihin resursseihin. Luonnollisesti tämä asettaa oman paineensa myös IT-järjestelmien tehostamiselle ja kehittämiselle.

Seurakunnan IT-järjestelmistä vastaa pääsääntöisesti taloustoimisto. Järjestelmän ylläpitotehtävien parissa työskentelee (sivutoimisesti) yksi ATK-tukihenkilö, sekä talouspäällikkö. Lisäksi ylläpidossa ovat mukana Kirkkoherra (hallinnollisena henkilönä), seurakunnan tiedottaja (www-julkaisujärjestelmän, Intra- ja Extranet:ien osalta), kiinteistöpäällikkö (kiinteistövalvontajärjestelmän osalta) ja kultakin toiminnalliselta alueelta (diakonia-, lähetys-, nuoriso-, lapsi-, musiikkityö, hautaustoimi, jne.) omat yhteyshenkilönsä. Vastuuhenkilöt tuovat esiin kunkin toimialan erityistarpeet ja ongelmat. ATK-tuki on kiinteässä yhteistyössä varsinaista järjestelmien hallintaa ja huoltoa palveluina toimittavien, ulkopuolisten asiantuntijatahojen kanssa.

1.4 Oma roolini

Työskentelen Tamperelaisen IT-palveluyrityksen (Tamico Systems Oy) palveluksessa järjestelmäasiantuntijana. Tätä kautta olen ollut mukana Ylöjärven seurakunnan IT-järjestelmien ylläpidossa jo useita vuosia. Asiakaskuntamme kostuu paikallisista ja kansainvälisistä yrityksistä sekä julkishallinnon organisaatioista. Toimitamme IT-palveluita mm. useille Pirkanmaalaisille seurakunnille. Ylläpito-tiimimme toimialaan kuuluvat IT-infrastruktuurin suunnittelu, toimitukset, käyttöönotto, seuranta ja hallinta sekä kehittäminen. Tutkintotyöhöni liittyvässä projektissa olin mukana alusta loppuun.

1.5 Kehto-projekti

IT-järjestelmän kehittämisprojektin varsinaisille työvaiheille ja suurempien muutosten läpiviemiselle päätettiin jo etukäteen varata riittävästi aikaa. Vaikka kokonaisuuteen liittyviä toimenpiteitä oli osittain jo suoritettu vuoden 2004 aikana, asetettiin varsinaiseksi projektin aikatauluksi vuosi 2005.

Samanaikaisesti seurakunnassa tuli esiin muita kehittämistarpeita, jotka eivät suoranaisesti liittyneet omaan tehtäväalueeseeni. Ne liittyivät kuitenkin tavalla tai toisella tietoverkon tai erilaisten olemassa olevien tietojärjestelmien kehittämiseen. Tällaisina asioita olivat mm. puhelinjärjestelmien kehittäminen, ajanhallinta- ja varausjärjestelmän käyttöönotto, seurakunnan toimitilojen muutokset ja lisääntyminen, käyttäjien toimenkuvien muutokset ja liikkuvuus sekä kiinteistöautomaatiojärjestelmien kehittäminen. Näiden tarpeiden ja menossa olevan IT-järjestelmän kehitystyön johdosta, kaikki Informaatio- ja kommunikaatioteknologioihin liittyvät hankkeet päätettiin ”niputtaa” yhdeksi, laajemmaksi projektiksi: syntyi YSICT-KEHTO 2005 (**Y**löjärven **S**eurakunnan **ICT**:n **KEH**ittäminen ja **TO**iminnallisuus).

Oma tutkintotyöni ja siihen kuuluneet IT-järjestelmien muutokset muodostivat näin osan YSICT–KEHTO -projektia. Projektin pääpiirteet on kuvattu LII-TE1:ssä.

2 Keskeiset käsitteet

AD (*Active Directory*) - Aktiivihakemisto
Windows:n (2000/2003) hakemistopalvelut, jotka sisältävät verkon objekteja koskevat tiedot ja mahdollistavat näiden käyttämisen. Aktiivihakemistopalvelujen ansiosta käyttäjien tarvitsee kirjautua sisään järjestelmään vain kerran, jonka jälkeen he voivat käyttää kaikkia heille julkaistuja verkon palveluita. Verkonhallitsijat näkevät aktiivihakemistossa verkon yhtenä hierarkkisena rakenteena ja voivat sen kautta keskitetysti hallita kaikkia verkon objekteja.

ADSL (*Asymmetric Digital Subscriber Line*)
Asymmetrinen digitaalinen tilaajayhteys. Puhelinjohdoissa käytettyyn kierrettyyn parikaapelitekniikkaan kehitetty laajakaistatekniikka, joka mahdollistaa suuren yhdensuuntaisen tiedonsiirtokapasiteetin tavallisen puhetoiminnan lisäksi.

Aliverkko - Subnetwork
TCP/IP-verkoissa käytetty verkonjakojakotekniikka. Käytäntö jossa laiteosoitteen bittejä varataan niin sanotuksi aliverkko-osoitteeksi, joka kuvaa reitittimen eristämää itsenäistä verkkoa organisaation sisällä. Aliverkottaminen on tarpeellista, jotta suurista A- (24 bittiä laiteosoitetta varten > 16000000 laitetta), B- (16 bittiä laiteosoitetta varten) ja jopa C-luokan (8 bittiä laiteosoitetta varten) verkoista saadaan toteutettua paremmin todellista laitemäärää vastaavia, itsenäisiä kokonaisuuksia.

Aliverkkomaski - Subnet mask
Aliverkkomaski on aliverkkotekniikassa käytetty TCP/IP-osoitteen osa, joka kertoo tietojärjestelmille mitkä bitit laiteosoitteesta yksilöivät laitteen verkon ja mitkä itse laitteen.

ASP (Application Service Provider) - Sovelluspalveluntarjoaja
Palveluntarjoaja joka mahdollistaa organisaatiolle tietyn sovelluksen käytön Internetin tai muun verkkoyhteyden kautta, ilman että organisaatiolla tarvitsee itsellään olla kyseisestä ohjelmistosta mitään palvelin- ja/tai työasemasovelluksia asennettuna. Varsinaiset palvelimet ja sovelluksen vaatimat tietokannat ovat palveluntarjoajan hallinnassa, esimerkiksi palveluntarjoajan laitetilassa ja palveluntarjoaja vastaa niiden ylläpidosta, huollosta, varmistuksista ja päivityksistä sopimuksen mukaisesti, korvausta vastaan. Etuna organisaatiolle tällaisesta ”sovellusvuokrauksesta” ovat pois jäävät laitteistoinvestoinnit sekä ylläpidon ja päivitysten tarve. ASP-palveluita käytettäessä organisaation ja palveluntarjoajan välisen tietoliikenneyhteyden kriittisyys luonnollisesti korostuu. Suomessa ASP-palveluntarjoajina toimivat perinteisesti teleoperaattorit sekä tietotekniikka- ja ohjelmistoalan yritykset.

DHCP (*Dynamic Host Configuration Protocol*)
Protokolla, joka määrittää TCP/IP-asetukset automaattisesti. Sisältää osoitteiden staattisen ja dynaamisen varaamisen ja hallinnan.

DNS (*Domain Name System*)
Yleiskäyttöinen, hajautettu ja toisinnettu nimipalvelu, jota käytetään Internetin ja intranettien isäntäkoneiden nimien muuttamiseen TCP/IP-osoitteiksi.

Frame Relay
ISDN:n LAPD-protokollasta kehitetty pakettivälitteinen protokolla, joka sijoittuu OSI-mallin siirtoyhteyskerrokselle. Frame Relay tarjoaa yksinkertaisen ja tehokkaan tavan siirtää tietoa yleisten verkkojen läpi. Suomessa (varsinkin aiemmin) yleisesti käytetty telepalvelu, jota käytetään esimerkiksi lähiverkkojen yhdistämiseen toisiinsa.

GP (*Group Policy*) - Ryhmäkäytäntö
Ryhmäkäytännöillä tarkoitetaan kokoonpanoasetuksia, jotka määritellään ja liitetään Aktiivihakemiston objekteihin ja tallennetaan ryhmäkäytäntöobjektiin (GPO = Group Policy Object). Ryhmäkäytäntötiedot tallennetaan Aktiivihakemiston ryhmäkäytäntöobjekteihin kahteen paikkaan: säiliöihin (GPC = Group Policy Containers) ja malleihin (GPT = Group Policy Templates). Ryhmäkäytäntöobjekti sisältää toimipaikkoja, toimialueita ja organisaatioyksikköjä koskevat ryhmäkäytäntöasetukset. Ryhmäkäytännöillä voidaan määritellä valmiiksi Windows:n asetukset työasemilla sekä käyttäjän työympäristö näkymineen, ohjelmistoineen ja oikeuksineen.

HDSL (*High bit-rate Digital Subscriber Line*)
Nopea digitaalinen tilaajayhteys. Puhelinjohdoissa käytettyyn kierrettyyn parikaapelitekniikkaan kehitetty laajakaistatekniikka, joka mahdollistaa suurinopeuksisen symmetrisen tiedonsiirtoyhteyden 2-3 kupariparilla tiettyyn etäisyyteen asti. G.HDSL on paranneltu versio HDSL:stä, jolla saavutetaan luotettavammin nopea datayhteys ja yhteys on mahdollista toteuttaa käyttäen ainoastaan yhtä kupariparia.

ISDN (*Integrated Services Digital Network*)
Puhelinverkkoja hyödyntävä digitaalinen monipalveluverkko, joka on tarkoitettu täydentämään perinteisiä telepalveluja. ISDN-verkossa on yhdistettynä puhelu-, data-, telex-, fax-, kuvapuhelin-, radio-, TV-, teletex-, videotex- ym. palveluiden siirto. Suomessa ISDN-tekniikkaa hyödynnetään pääasiassa puhelu-, fax- ja datapalveluihin.

IT / ICT (Information Technology / Information & Communication Technology)
Informaatio teknologialla tarkoitetaan kaikkea tiedon hallintaan ja käsittelyyn sekä sen automatisointiin (ATK) liittyvää tekniikkaa ja käytettyjä laite- ja ohjelmistoratkaisuja.
Informaatio ja kommunikaatio teknologia laajentaa käsitteen kattamaan myös tiedon välittämiseen liittyvät ratkaisut, kuten erilaiset tietoverkot ja esimerkiksi tele- ja puhelinratkaisut.

Keskitin - Hub
Moniporttitoistin, johon verkon työasemat, palvelimet ja oheislaitteet kytketään. Keskitin on ns. tähtipiste, josta verkon tietoliikenneyhteydet eri verkon laitteille lähtevät ja joka välittää yhdestä portista tulevan tietoliikenteen tarkistettuna ja vahvistettuna muihin portteihinsa ja näin muille verkon laitteille.

Kytkin - Switch
Aktiivinen lähiverkon komponentti, joka toimii kuten keskitin (jokaiseen porttiin voidaan kytkeä työasema). Sisältää nopean laitteen sisäisen välityskyvyn ja kykenee sekä jakamaan, että välittämään useiden verkkosegmenttien välisen liikenteen. Kytkin ei toista kaikkia yleislähetyspaketteja kaikille porteille, vaan lähettää paketit ulos ainoastaan siitä portista, johon kohdelaite on kytketty. Kytkintä käytetään lähiverkon siltaamiseen, reitittämiseen ja kuorman jakamiseen.

LAN (*Local Area Network*) - Lähiverkko / paikallisverkko
Maantieteellisesti rajatun alueen sisäistä tietoliikennettä hoitava, suuren siirtokapasiteetin omaava verkko, joka on tavallisesti yhden orgamisaation hallinnassa ja omistuksessa. Verkko koostuu fyysisistä tiedonsiirtoyhteyksistä sekä erilaisista aktiivilaitteista, työasemista, palvelimista ja oheislaitteista ja voi olla sekä fyysisesti, että loogisesti hyvin moniulotteinen.

LDAP (*Lightweight Directory Access Protocol*)
X.500-verkkoprotokollan pohjalta kehitetty, kevyempi ja asiakaslaitteelle yksinkertaisempi sekä vähemmän prosessointia vaativa protokolla, joka suunniteltiin siten, että työpöytäkoneet kykenisivät käyttämään X.500-tyyppisiä hakemistoja ilman että niiden toiminta hidastuu. LDAP-hakemistot käyttävät hajautettua topologiaa, joka on yksinkertaisempi X.500:n verrattuna, mutta kuitenkin yhteensopiva X.500:n kanssa. LDAP-standardin mukaisia hakemistoja käyttävät mm. Microsoftin Aktiivihakemisto, Novell ja Netscape, joten ne kykenevät vaihtamaan tietoja eri hakemistopalvelutoteutusten kesken, riippuen tietysti kuinka eri valmistajat tulkitsevat standardia.

Monitoimitulostin - MFP *(Multi Function Printer)*
Monitoimitulostimessa yhdistyvät verkkotulostimen, kopiokoneen, skannerin ja faksin ominaisuudet. Tällöin saadaan suoraan työasemilta hyödynnettyä esimerkiksi kopiokoneen kaksipuolisuus-, lajittelu-, nidonta- ja rei'itysominaisuudet sekä faksien lähetys- ja vastaanotto-ominaisuudet, riippuen MFP-laitteen ominaisuuksista. Näin käyttäjät voivat tuottaa suoraan mahdollisimman valmiita paperidokumentteja, ilman lukuisia erillisiä työvaiheita. Suurin osa markkinoilla olevista MFP-laitteista perustuu luotettavaan ja toimintavarmaan kopiokonetekniikkaan.

NAT (*Network Address Translation*)
Verkko-osoitteen muunnos on "tulkkaus", joka tehdään reitittimessä (tai muussa reitittävässä laitteessa), joka toimii yhdyskäytävänä eri verkojen välillä. Muunnos toimii niin, että kun lähettävä laite paketoi lähetettävän tiedon ja liittää siihen vastaanottajan ja lähettäjän verkko-osoitteen, purkaa yhdyskäytävä paketin, muuttaa sitä niin, että vastaus lähetetäänkin takaisin sille ja paketoi sen uudelleen sekä lähettää sen vastaanottajalle. Vastauksen tullessa tekee yhdyskäytävä vastaavan muunnoksen päinvastoin ja välittää paketin perille alkuperäiselle lähettäjälle. Käytettäessä NAT-muunnosta yhdyskäytävässä, vältytään paljastamasta varsinaisen loppukäyttäjän todellista verkko-osoitetta vastaanottajalle esimerkiksi Internetissä.

Operaattori (Internetpalveluntarjoaja) - ISP (Internet Service Provider)
Palveluntarjoaja joka tarjoaa tekniset ratkaisut ja fyysiset yhteydet organisaation Internet-yhteydelle, oman lähiverkon ulkopuolelle. ISP-palveluntarjoaja voi tarjota myös muita Internet-palveluita organisaatiolle, kuten www- tai sähköpostipalveluita tai Internetin kautta kulkevia etäyhteyksiä. Suomessa ISP-palveluntarjoajina toimivat perinteisesti teleoperaattorit, kuten Telia-Sonera, Elisa ja Finnet.

Palomuuri - Firewall
Laitteistosta ja ohjelmistosta muodostuva turvajärjestelmä, joka suojaa verkkoa tai sen osaa toisista verkoista, esimerkiksi Internetistä, tulevilta tunkeutujilta ja muilta uhkilta. Kaikki saapuva ja lähtevä liikenne ohjataan palomuurin kautta ja se estää verkon ulkopuolella olevia tietokoneita viestimästä suoraan verkon tietokoneiden kanssa ja päinvastoin. Palomuuri voi myös seurata ver-

kon toimintaa ja tallentaa tiedot tietoliikenteen määristä ja asiattomista yhteysyrityksistä.

RAS (*Remote Access Service*) - Etäkäyttöpalvelu
Microsoft Windows:n palvelu, joka mahdollistaa tietokoneen ja/tai tietojärjestelmän etäkäytön. Tyypillisimmin palvelua tarjoaa etäkäyttöpalvelin, johon otetaan yhteys tavallisen modeemin, ISDN-modeemin tai VPN-yhteyden avulla.

Reititin - Router
Aktiivinen lähiverkon komponentti, joka huolehtii sanomien välityksestä (reitityksestä) verkossa. Reititin voi välittää liikennettä verkon eri osien, eri aliverkkojen tai täysin eri verkkojen (esimerkiksi lähiverkon ja Internetin) välillä.

Silta - Bridge
Aktiivinen lähiverkon komponentti, joka puskuroi ja suodattaa liikenteen lävitseen. Siltoja käytetään sekä lähekkäisten verkkojen, että kaukana erillään olevien verkkojen yhdistämiseen. Silta generoi lähiverkon paketit uudelleen, jolloin Ethernet -verkon pituussääntö katkeaa.

SNMP (*Simple Network Management Protocol*)
TCP/IP-protokolla verkkojen valvontaa varten. Perustuu pyyntöihin ja vastauksiin, joilla agentit, eli pienet apuohjelmat, seuraavat verkon liikennettä ja laitteiden toimintaa, keräävät niistä tietoa ja tallentavat ne hallintatietokantaan (MIB). Erillinen hallintakonsoli pyytää nämä tiedot agenteilta säännöllisesti ja jos jokin arvo on asetetun rajan ylä- tai alapuolella voi tuoda hälytyksen näyttöön tai lähettää sen vastuuhenkilölle vaikkapa tekstiviestinä tai sähköpostina.

TCP/IP (*Transmission Control Protocol / Internet Protocol*)
Teollisuusstandardin mukainen protokollaperhe, joka mahdollistaa tiedonsiirron sekarakenteisissa verkkoympäristöissä. Nykyisin useimmat verkot tukevat nimenomaan TCP/IP:tä. TCP/IP on kuljetustason protokolla, joka koostuu useiden istunto tasolla toimivien protokollien pinosta. Siihen kuuluu reititettävä yritysverkkoprotokolla sekä pääsy Internetin resursseihin. TCP on OSI-mallin mukaiselle kuljetuskerrokselle (4) sijoittuva luotettava protokolla järjestettyjä tietoja varten. IP on OSI-mallin mukaiselle verkkokerrokselle (3) sijoittuva reititettävä yhteydetön protokolla pakettien välittämistä varten (yhteydetön CLNS-palvelu). IP toimii aliverkkojen yli ja edellyttää aliverkoilta ainoastaan keskinäisen tiedonsiirron, ilman varmennuksia.

TCP/IP-address - TCP/IP-osoite
Yksittäisen laitteen käyttämä TCP/IP-osoite, joka mahdollistaa halutun tietoliikenteen ohjaamisen kyseiselle laitteelle.

Toimialue - Domain
Windows-verkossa oleva joukko tietokoneita ja käyttäjiä, joilla on yhteinen tietokanta ja suojauskäytännöt. Nämä tiedot on tallennettu ohjauspalvelimeksi määritellyn tietokoneen tietokantaan, jonne on määritelty myös toimialueen yksilöllinen nimi.

UDP (*User Datagram Protocol*)
Yhteydetön protokolla, jonka tehtävä on siirtää tiedot lähteestä kohteeseen TCP/IP-verkoissa.

Verkkoprotokolla - Protocol
Käytäntö jonkin toimenpiteen suorittamiseen: Tietoliikenteessä tarkoitetaan menettelyä, jolla eri laitteet keskustelevat keskenään.

Verkkotopologia - Topology
Tietokoneiden, kaapeleiden ja muiden osien järjestys verkossa.

VDSL (*Very high data rate Digital Subscriber Line*)
Erittäin nopea digitaalinen tilaajayhteys. Puhelinjohdoissa käytettyyn kierrettyyn parikaapelitekniikkaan kehitetty laajakaistatekniikka, joka mahdollistaa suurinopeuksisen symmetrisen tiedonsiirtoyhteyden lyhyillä, muutaman kilometrin, matkoilla.

VLAN (*Virtual Local Area Network*) - Virtuaalinen lähiverkko
Virtuaalisessa lähiverkossa erotetaan toisistaan verkon fyysinen ja looginen rakenne. Virtuaaliverkko on oma reititysalueensa, jonkin fyysisen LAN:n tai WAN:n sisällä.

VPN (*Virtual Private Network*) - Näennäinen yksityisverkko
Joukko julkiseen verkkoon, esimerkiksi Internetiin, kytkettyjä tietokoneita, jotka viestivät keskenään käyttäen salaustekniikkaa. Salaus estää ulkopuolisia sieppaamasta ja ymmärtämästä tietokoneiden välisiä viestejä. Näennäinen yksityisverkko toimii kuin tietokoneiden välillä olisi yksityinen kaapelointi ja tarjoaa organisaatioille mahdollisuuden saattaa eri toimipaikkojensa tietojärjestelmät yhteen.

WAN (*Wide Area Network*) - Alueverkko / laajaverkko
Tietokoneverkko, jonka tietokoneet ovat fyysisesti kaukana toisistaan ja yhdistettyinä toisiinsa (verkkoon) tietoliikennelinkeillä.

WLAN (*Wireless Local Area Network*) - Langaton lähiverkko verkko
Langaton lähiverkko on radiotaajuuksiin perustuva tekniikka verkkoyhteyden muodostamiseksi ilman fyysistä kupariyhteyttä. WLAN-verkot toimivat yleisimmin vapailla 2,4GHz taajuusaluille ja ne on standardoitu IEEE802.11x –standardeissa. Nykyiset WLAN-tekniikat hyödyntävät useita eri liikennöintinopeuksia (11 Mbps, 54 Mbps, 108 Mbps…) ja niissä on käytettävissä useita eri tietoturva- ja salaustekniikoita (MAC-suodatus, SSID, WEB, WPA, VPN…).

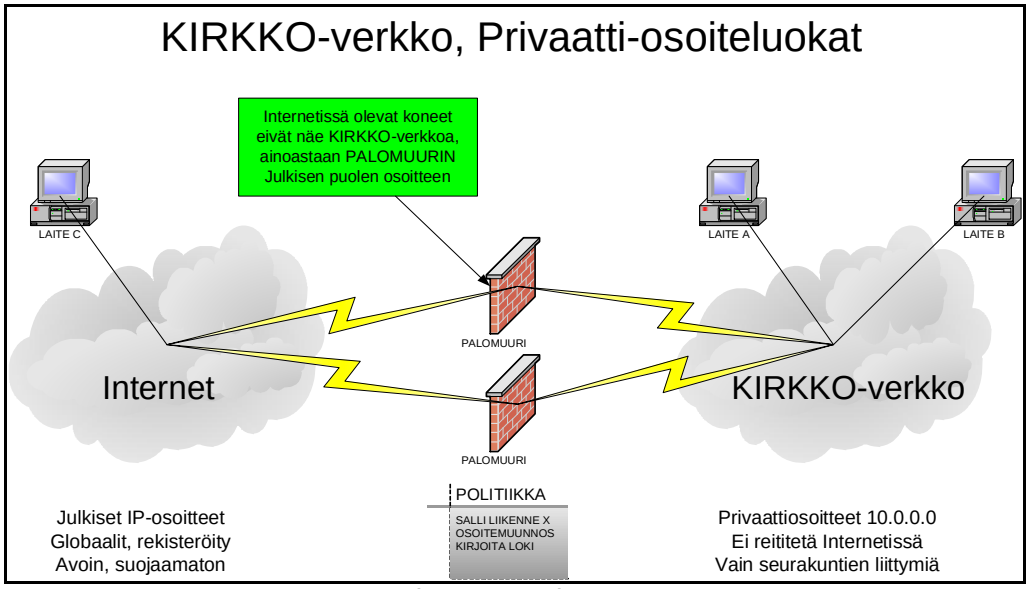
X.500
ISO:n (International Standard Organization - Kansainvälinen standardisointijärjestö) ja ITU:n (International Telecommunications Union-Kansainvälinen telekommunikaatiounioni (aiemmin CCITT)) yhdessä kehittämä Standardijoukko, jonka tarkoituksena oli luoda maailmanlaajuinen valkoisten sivujen puhelinluettelopalvelu. X.500-standardijoukko pitää sisällään useita standardeja, joihin kuuluu mm. nimeämistapoja ja verkkoliikenneprotokollia. X.500-protokolla kehitettiin tarkoituksena mahdollistaa erilaisten informaatiovarastojen yhdistäminen. Tämän johdosta X.500-hakemisto on rakenteeltaan erittäin hierarkkinen, selkeä ja järjestelmällinen, mikä käyttäjän näkökulmasta vaikeuttaa tietojen hallintaa ja näyttämistä. X.500-protokolla ei koskaan saavuttanut suurempaa suosiota, koska sen nimeämismenetelmä on erittäin monimutkainen. Kun sitä käsiteltiin byrokraattisesti eri komiteoissa ja sen protokollista väiteltiin ja niitä hiottiin, syntyi Internet joka otti käyttöönsä TCP/IP:n.

3 KIRKKO-verkko

(KIRKKO-verkon puitesopimukset.)

KIRKKO-verkko on kaikkien Suomen seurakuntien yhteinen tietoverkko. KIRKKO-verkko syntyi 1990-luvulla tarpeesta rakentaa kaikki seurakunnat kattava tietoverkko kirkon viranomaistehtävien, kuten väestötietojärjestelmien ylläpidon, hoitoa varten. Samalla rakentui infrastruktuuri, joka toimii tukena kaikissa seurakuntien toiminnoissa. KIRKKO-verkkoa hyödynnetään taloudenhoidossa, hallinnossa, viestinnässä ja erilaisten palveluiden tarjonnassa. Kirkon viranomaistehtävien johdosta KIRKKO-verkko on luokiteltu ns. viranomaisverkoksi. Tämä luo verkolle omat erityisvaatimuksensa. Kirkko ja sen eri seurakunnat ovat sitoutuneet noudattamaan valtionhallinnon tietoturvamääräyksiä ja -ohjeistuksia. KIRKKO-verkon toimintaa ohjaa, valvoo ja kehittää kirkon oma tietohallinto, joka vastaa KIRKKO-verkosta kokonaisuudessaan.

KIRKKO-verkossa käytetään sellaisia IP-osoitteita, jotka kuuluvat ns. privaattiosoiteluokkaan. Tämä takaa sen, että käytettävissä on riittävän paljon osoitteita systemaattisen ja hyvin hallinnoitavan verkon toteuttamiseen. Verkon sisäiset osoitteet on erotettu julkisista Internet-osoitteista palomuurilla ja NAT-muunnoksella. Verkon sisällä olevat privaatti A-luokan osoitteet (10.x.x.x/8) muodostavat yhtenäisen verkon. Reititysmielessä verkon sisällä oleva kone pääsee kaikkiin sisäverkon palveluihin ja internetissä oleviin palveluihin. Internetissä oleva laite sen sijaan pääsee vain internetiin tai sellaisiin kohteisiin, jotka sijaitsevan julkisissa IP-osoitteissa (kuva 3.1).

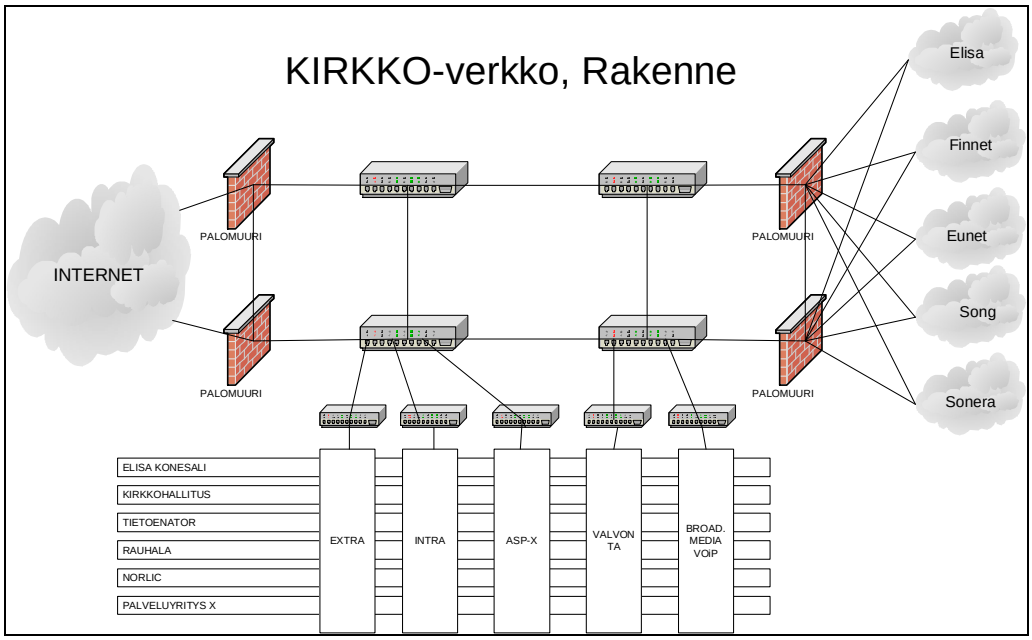


Kuva 3.1 KIRKKO-verkon IP-osoiteavaruus

Pienimmillään seurakunnan lähiverkko on vain yksi mikro. Laajimmillaan seurakunnan suljettu ja sisäinen lähiverkko kattaa kaikki seurakunnan toimipisteet. Toisaalta seurakunnan eri toimipisteissä voi olla myös useita erillisiä lähiverkkoja, jotka on kukin erikseen liitetty KIRKKO-verkkoon. Laitteiden IP-numerot ovat KIRKKO-verkon kokonaisuuteen sopivia yksityisiä 10.0.0.0-sarjaan kuuluvia numeroita. Kullekin lähiverkolle on aliverkottamalla varattu omat privaatti C-luokan osoitteet (10.x.x.x/24). Lähiverkon toimipisteet yhdistetään toisiinsa kullakin paikkakunnalla tarkoituksenmukaisimmalla tavalla.

Jos lähiverkon alustana käytetään esimerkiksi monien eri osapuolten yhteisiä kuntaverkkoja, seurakunnan toimipisteet ”tunneloidaan” suljetuksi ja sisäiseksi, muista osapuolista erillään olevaksi kokonaisuudeksi paikallisesti valitulla teknologialla.

KIRKKO-verkkoliittymä on se liittymä, jolla em. lähiverkko kytketään varsinaiseen, kaikki seurakunnat kattavaan, KIRKKO-verkkoon. Liittymän voi toimittaa vain KIRKKO-verkon puitesopimusoperaattori. Tyypillisessä tapauksessa yksi puitesopimusoperaattoreista toimittaa kaikki lähiverkon liittymät seurakunan eri toimipisteisiin. Niistä muodostetaan loogisesti yhtenäinen WAN-verkko, joka sisältää myös yhteyden KIRKKO-verkon palveluihin ja sen tietoturvarajapintaan (kuva 3.2).



Kuva 3.2 KIRKKO-verkon rakenne

Yksittäinen seurakunta tai seurakuntayhtymä vastaa määrätyn itsehallinnon mukaisesti itse käytössään olevista tietoverkoista ja niitä hyödyntävistä tietojärjestelmistä. Sopimus lähiverkon rakentamisesta ja ylläpidosta tehdään paikallisesti seurakunnan ja valitun rakentajan välille. Lähiverkon rakentajana voi olla muukin taho kuin KIRKKO-verkon puitesopimusoperaattori. Seurakunnan lähiverkkoon ei rakenneta omia paikallisia Internet-yhdyskäytäviä (Internet-palomuureja tai VPN-yhdyskäytäviä). Olisi suuri riski sille, että joku ulkopuolinen tunkeutuisi niiden kautta ensin seurakunnan lähiverkkoon ja sitä kautta muualle KIRKKO-verkkoon.

Se paikallinen seurakunta tai seurakuntayhtymä, joka vastaa mm. paikallisten sopimusten teosta lähiverkon rakentajan ja ylläpitäjän kanssa, vastaa myös lähiverkon kustannuksista ja sen tietoturvasta sekä käyttäjien paikallisesta tuesta ongelmatilanteissa. Omistajana on aina seurakunta tai seurakuntayhtymä. Omistajana ja vastuullisena ei voi olla esimerkiksi joku paikallinen atk-yritys tai operaattori, koska ne eivät ole kirkkolain mukaisia kirkon hallintoon kuuluvia organisaatiota. Omistaja voi ulkoistaa joitakin lähiverkon palveluja paikalliselle ATK-yritykselle, mutta se vaatii omistajan ja atk-yrityksen välistä selkeää sopimista. Lopullinen vastuu mm. tietoturva-asioista on kuitenkin aina omistajalla.

4 Yleistä tietojärjestelmistä

Tietojärjestelmissä on lähtökohtaisesti erilaisia ongelmia ja rajoituksia, sekä niiden historiasta johtuvia seikkoja, jotka melkeinpä pakottavat tekemään tiettyjä teknisiä ratkaisuja jatkossa. Tässä luvussa käsittelen niitä tekniikoita ja menetelmiä, jotka vaativat yksityiskohtaisempaa tarkastelua projektissamme.

Käyttäjien määrän kasvu ja käsiteltävän tiedon lisääntyminen vaativat jatkuvasti lähiverkoilta enemmän tehoa. Ongelmia aiheuttavat hallinnan puute sekä vakioimattomat ympäristöt ja laitteet.

Tänä päivänä yksi merkittävä muutokseen ajava tekijä on NT4-käyttöjärjestelmän auttamaton vanheneminen. Siihen saatava tuki loppui vuosien 2004–2005 vaihteessa. On siirryttävä uudempaan tekniikkaan.

4.1 Ethernet-verkot

Ethernet-lähiverkon topologiaa voidaan kuvailla joko fyysisenä tai loogisena. Fyysinen topologia kuvailee verkon siirtotien ja siihen yhdistettyjen laitteiden todellisen sijoittelun. Looginen topologia käsittelee verkon läpi kulkevia loogisia tiedonsiirron polkuja. Ethernet–verkoissa tulee huomioida niitä koskevat rajoitukset. Näitä ovat käytetyn siirtotien pituus ja nopeus, yhdistävien laitteiden ominaisuudet, sallittujen laitteiden lukumäärä ja siirtotien varausmekanismi.

Käytettyjä topologioita ovat väylä ja tähti sekä niiden yhdistelmät, puu ja hierarkkinen tähti. Väylätopologiassa kaikki työasemat ja laitteet jakavat yhteisen kaapelin. Sitä pidetään vanhentuneena, eikä sen käyttöä suositella. Tähtitopologiassa kukin työasema liitetään yhden kaapelin varrelle joka on kytketty suoraan verkon keskipisteenä toimivalle laitteelle, keskittimelle. Kaiken datan täytyy kulkea tämän keskittimen kautta. Topologiaa voidaan kasvattaa käyttämällä verkon eri segmenttejä yhdistäviä laitteita, kuten reitittimiä ja kytkimiä. (Ogletree 2001: 138-143.)

4.1.1 Lähiverkon aktiivilaitteet

(Ogletree 2001: 99-103.)

Keskitin (moniporttitoistin) toimii toistamalla kaiken sisään tulevan liikenteen ulos muista porteista, jolloin kaikki keskittimeen liitetyt solmut (tässä tapauksessa siis kaikki verkon laitteet) kuulevat kaikki lähiverkossa lähetetyt paketit. Keskitin on monin tavoin väylätopologiaverkkoa parempi siinä mielessä, että kaapelointi on keskitetty, eikä kaapelikatkos kaada koko lähiverkkoa. Tästä huolimatta, yksinkertainen passiivinen keskitin ei vähennä millään tavalla lähiverkon kokonaisliikennettä.

Kytkin toimii kuin keskitin, jossa jokaiseen porttiin voidaan yhdistää työasema. Erona on kuitenkin se, että kytkin ei toista kaikkia yleislähetyspaketteja kaikille muille porteille. Tämän sijaan kytkin lähettää paketin ulos vain siitä portista, johon kohdelaite on yhdistetty. Sillan tapaan kytkin oppii yksittäisten laitteiden

sijainnin tutkimalla pakettien lähdeosoitteen, kun työasema suorittaa lähetyksen ensimmäistä kertaa. Kun kytkin on rakentanut työasemaosoitetaulun, sen ei enää tarvitse lähettää paketteja kaikille porteille.

Jos verkossa käytetään keskittimiä ja siinä on verkkoliikenneongelmia, kytkin todennäköisesti parantaa verkon suorituskykyä. Useimmissa tapauksissa kytkin on erinomainen verkon päivitystapa muihin päivitysvaihtoehtoihin verrattuna. Tietyissä tilanteissa kytkin ei paranna suorituskykyä kovinkaan paljoa. Esimerkiksi pieni osastolähiverkko, jossa jokainen työasema on yhdistetty kytkimeen, jonka porttiin puolestaan on liitetty palvelin. Koska kaikki tätä palvelinta käyttävät työasemat ovat samassa paikassa palvelimen kanssa, kytkimen vuoksi vain yksi työasema kerrallaan voi käyttää palvelinta. Tällä tavoin saavutetaan suunnilleen sama läpimeno kuin sijoittamalla palvelin ja työasemat keskittimelle. Jos kuitenkin kasvatetaan kytkimeltä palvelimelle yhdistettyjen porttien lukumäärää, tilanne muuttuu. Niin pitkään, kun palvelin itsessään omaa riittävästi kapasiteettia, läpimeno kasvaa ja käyttäjät huomaavat palvelimen vastaavan nopeammin. Yleisesti ottaen kytkin toimii parhaiten yhdistäessään useita käyttäjiä useisiin resursseihin. Esimerkissä yksittäinen palvelin vastaa useita resursseja, koska se on yhdistetty kytkimeen useiden polkujen kautta.

4.1.2 VLAN-verkot

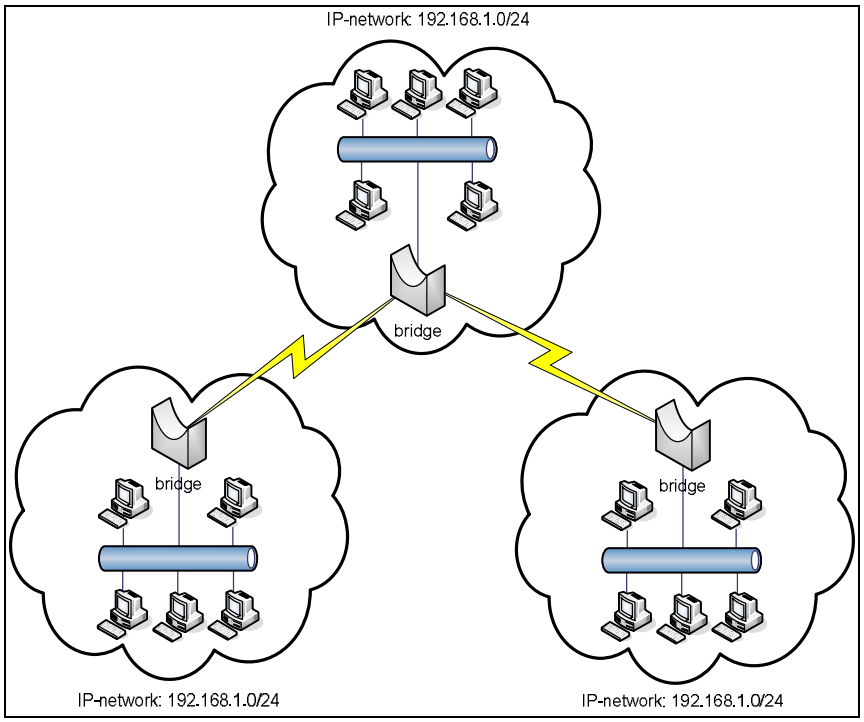
Virtuaalisessa lähiverkossa (VLAN) erotetaan toisistaan verkon fyysinen ja looginen rakenne. Virtuaaliverkko on käytännössä oma reititysalueensa. Useita VLAN:eja voidaan käsitellä täysin omina verkkoinaan, jonkin fyysisen LAN:n tai WAN:n sisällä. Tämä vaatii verkon aktiivilaitteilta (kytkimet, reitittimet) VLAN-tukea, niin että ne voivat keskinäisessä tietoliikenteessään erotella eri verkkoihin tarkoitetut paketit niihin lisätyn VLAN-tagin perusteella.

4.1.3 WAN-yhteydet

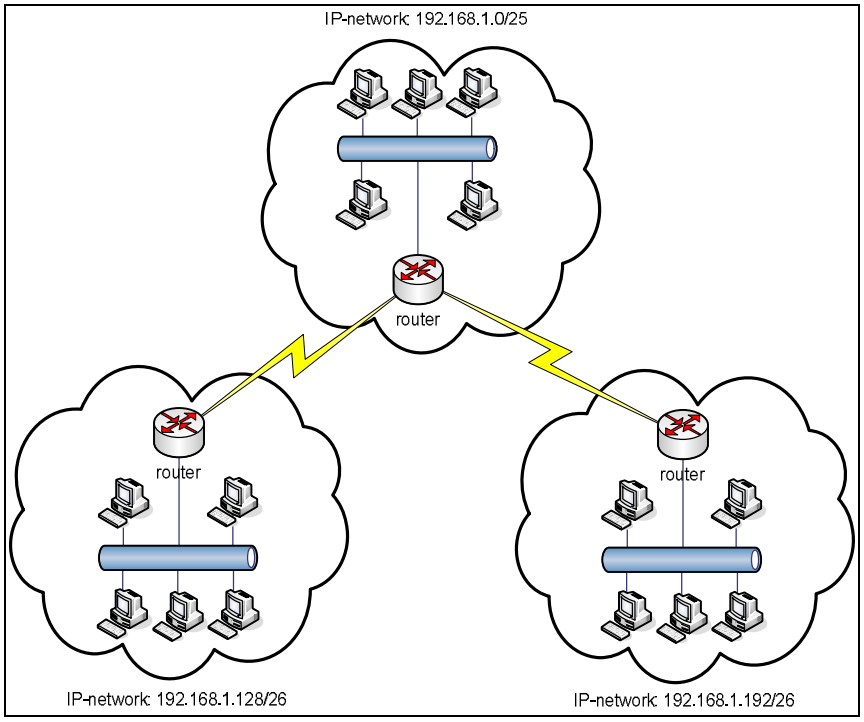
Jokainen Ethernet-verkko omaa kaksi perustekijää: kaapelin ulottuvuudella on rajansa ja lähiverkkoon voidaan liittää vain tietty määrä laitteita. Tästä syystä tulee usein tarpeelliseksi laajentaa verkkoa yhdistämällä se toiseen. Suurempien verkkojen rakentaminen on mahdollista, yhdistämällä yksittäisiä verkkoja toisiinsa siltojen ja reitittimien avulla.

Silta on yksinkertainen laite, joka on varustettu pienellä määrällä älykkyyttä. Se toimii siirtoyhteystasolla ja tekee muutakin kuin vain vahvistaa saapuvaa signaalia ja lähettää sen ulos muista porteista. Siirtoyhteystasolla lähiverkon laitteet erotetaan toisistaan MAC-osoitteen (Media Access Control) avulla. Silta kerää nämä arvot ylläpitämäänsä tauluun. Näin se oppii mitkä laitteet ovat kytkettyinä mihinkin portteihin ja osaa tehdä päätöksiä sisään tulevien pakettien lähettämisestä muille porteille. Silta ei ota kantaa käytettiin verkkoprotokollaan, vaan välittää liikenteen lävitseen. TCP/IP-verkoissa tämä tarkoittaa saman IP-verkon laajentumista siltayhteyden ylitse (kuva 4.1). (Ogletree 2001: 93-104.)

Reitittimet ovat kehittyneempiä laitteita. Ne toimivat korkeammalla verkkomallissa. Siinä missä sillat toimivat siirtoyhteyskerroksella, reitittimet toimivat verkkokerroksella ja käyttävät protokollaosoitteita, kuten TCP/IP-osoitteita. Reitittimet luvat taulun osoitteista ja tekevät tämän avulla päätöksen liikenteen välittämisestä toisille porteille. TCP/IP-verkoissa tämä mahdollistaa verkkojen aliverkottamisen ja liikenteen välittämisen eri TCP/IP-osoiteavaruudet omaavien verkkojen välillä (Kuva 4.2). Aliverkottaminen mahdollistaa verkon laitteiden lukumäärän kasvattamisen sekä reititettävän tiedon rajoittamisen. (Ogletree 2001: 93-104.)



Kuva 4.1 Sillattu, samaa aliverkkoa oleva WAN-verkko



Kuva 4.2 Reititetty ja aliverkoilla erotettu WAN-verkko

4.2 Windows 2000 Server

Windows 2000 on monikäyttöinen käyttöjärjestelmä, joka sisältää tuen asiakas-, palvelin- ja vertaisverkkoja varten. Windows 2000 tuoteperheen suunnittelussa on lähdetty siitä, että se skaalautuu aina pienistä verkoista suuriin yritysverkkoihin asti. Windows 2000 sisältää kattavan Internet- ja sovellustuen, joka perustuu NT 4.0 Server:n menestykseen Internetiä hyödyntävänä, sovelluskeskeisenä palvelinkäyttöjärjestelmänä. (Microsoft Windows 2000 Training Kit: 2-6.)

Microsoft on julkaissut Windows 2000 tuoteperheessä viisi erilaista käyttöjärjestelmää. Työasemakäyttöjärjestelmäksi tarkoitetun Windows 2000 Professionalin sekä palvelinkäyttöjärjestelmiksi tarkoitetut Windows 2000 Server (tiedosto-, tulostus-, sovellus- sekä web-palvelinalusta), Windows 2000 Advanced Server (tehokkaampi, laajennetut käytettävyys- ja skaalautuvuusominaisuudet sisältävä sovelluspalvelin tietokantakeskeiseen työhön), Windows 2000 Datacenter server (erikoisversio, laajoihin ja raskaaseen tietojen käsittelyyn sekä konsolidaatiota, kuormantasausta ja klusterointia vaativiin prosesseihin) sekä Windows 2000 Small Business Server (Erityisesti pieniin ympäristöihin suunniteltu, laajennettavuudeltaan rajoitettu versio, johon on paketoitu mukaan Fax, Modem, ISA Server 2000, Exchange 2000 Server ja SQL Server 2000 palvelut).

Windows 2000 Server:n ominaisuuksia ja etuja ovat:

- Automaattiset sovellusten asennus- ja päivitystoiminnot sekä keskitetyt asetus- ja kokoonpanomääritykset
- Käyttöoikeuksien tarkistaminen ennen kuin verkon resursseja voidaan käyttää
- Paikallisen ja verkkotason tietoturva sekä tiedostojen, kansioiden, kirjoittimien ja muiden resurssien käytön seuranta
- Tuki Kerberos-protokollalle ja julkisen avaimen salaukselle (PKI)
- Aktiivihakemistopalvelut, jotka tallentavat verkon resursseja, kuten käyttäjätilejä, sovelluksia, laitteita ja tietoturvaa koskevat tiedot
- Aktiivihakemistopalveluiden hallinta, valvonta ja turvaus
- Moniprosessorituki (SMP) neljälle prosessorille sekä tuki järjestelmöprosessien ja ohjelmien moniajolle
- Yleisten verkkoprotokollien tuki
- Mahdolliset yhteydet Novell NetWare:en, Unix:iin/Linux:iin ja AppleTalk:iin
- Tuki puhelinverkkoyhteyksille (256 samanaikaista istuntoa) sekä etäkäyttöpalveluille (RAS)
- Mahdollistaa paikallisen LAN-verkon, intranet:n ja Internet:n resurssien turvallisen yhdistämisen
- Microsoft Internet Information Server (IIS) Web-palvelinalusta
- Mahdollistaa muokattujen järjestelmänhallintatyökalujen luonnin vakiokäyttöliittymään (MMC)
- Mahdollistaa kolmannen osapuolen järjestelmänhallintatyökalujen sisällyttämisen vakiokäyttöliittymään
- Tuki USB-sarjaliikenneväylälle
- Tuki automaattisesti asentuville PnP-laitteille

(Microsoft Windows 2000 Training Kit: 2-6.)

4.3 Active Directory

Aktiivihakemistopalvelut on integroitu Windows Serveriin (2000/2003) ja ne tarjoavat käyttäjien liiketoiminnassaan tarvitseman hierarkian, laajennettavuuden, skaalattavuuden ja hajautetun suojauksen. Aktiivihakemistopalvelujen avulla käyttäjät saavat käyttöönsä hakemistopalvelut, jotka liittyvät saumattomasti sekä Internet- että Intranet-ympäristöön. Sen avulla voi käyttää hakemistopalveluja sekä tietolähteenä, että järjestelmänhallinnallisten palvelujen lähteenä. Aktiivihakemistoissa integroituvat Internetin nimiavaruuskäsite ja käyttöjärjestelmän hakemistopalvelut.

Aktiivihakemistopalvelut mahdollistavat kaikkien julkaistujen palveluiden, kuten tiedostojen, oheislaitteiden, tietokoneliitäntöjen, tietokantojen, Internetyhteyksien, käyttäjien, palveluiden ja muiden objektien, keskitetyn hallinnan. Se käyttää DNS:ää (Domain Name System) paikannuspalveluna, järjestelee toimialueen objektit organisaatioyksiköistä (Organizational Unit, OU) muodostuvaksi hierarkiaksi ja mahdollistaa useiden toimialuiden liittämisen puurakenteeksi. Järjestelmänhallinta yksinkertaistuu, koska käytössä ei ole PDC- (Primary Domain Controller) ja BDC (Backup Domain Controller) -palvelimista muodostuvaa rakennetta, kuten Windows NT 4.0 Serverissä. (Microsoft Windows 2000 Training Kit: 239-240.)

4.3.1 Active Directory - toimialueiden tyypit

Microsoftin Aktiivihakemistosta on tällä hetkellä saatavilla 4 erilaista tyyppiä, ns. toiminnallisuustasoa ja ne ovat riippuvaisia käytettävästä palvelimen käyttöjärjestelmästä (2000/2003). Toiminnallisuustasot ovat Windows Server 2000 mixed mode, Windows Server 2000 native mode, Windows Server 2003 interim mode ja Windows Server 2003 mode. Toiminnallisuustasot ovat hierarkkisia ja toimialuetasoa voidaan nostaa tarvittaessa. Toiminnallisuustasoa muutettaessa on selvitettävä muutoksen vaikutus, sillä kun toiminnallisuustaso on kerran muutettu, paluu entiseen ei enää ole mahdollinen.

Windows Server 2000 mixed mode tarjoaa tuen kaikille ohjainpalvelin versioille Windows NT4:stä alkaen (Windows NT4-palvelin ei voi kuitenkaan toimia toimialueen ohjauskoneena) ja käytössä ovat vain aktiivihakemiston peruspalvelut. Tässä tilassa Windows 9x-työasematkin toimivat verkossa ja käyttäytyvät kuin olisivat jäsenenä Windows NT4-toimialueella.

Windows Server 2000 native mode tukee ohjainpalvelimena ainoastaan Windows 2000 ja Windows 2003-palvelimia. Toimialueella voi ottaa käyttöön edistyksellisempiä ominaisuuksia, kuten laajennettavuus ja universaalit ja sisäkkäiset ryhmät.

Windows Server 2003 interim mode on välitila, joka on tarkoitettu käytettäväksi siirryttäessä Windows NT4:stä suoraan Windows 2003-ympäristöön. Tämä tila ei tue lainkaan Windows 2000:a, mutta muilta osin kaikki toiminnot vastaavat Windows 2000 mixed mode:a.

Windows Server 2003 mode on mahdollista ottaa käyttöön, kun kaikki palvelimet toimialueella on päivitetty Windows Server 2003:ksi. Tässä tilassa ei

tueta muita ohjainpalvelimia. Windows Server 2003 mode:ssa on mahdollista ottaa käyttöön aktiivihakemiston uusimmatkin lisäominaisuudet.

4.3.2 Active Directoryn arkkitehtuuri

Aktiivihakemistopalvelut voidaan jakaa seuraaviin pääosiin: tietomalli (data model), laajennettava kaava (extensible schema), suojausmalli ja hallintomalli. Lisäksi aktiivihakemistopalveluihin liittyy useita muita käsitteitä, kuten globaali luettelo (global gatalog), nimiavaruus ja nimeämiskäytännöt.

Aktiivihakemiston tietomalli on peräisin X.500:n tietomallista. Se sisältää objekteja, jotka edustavat järjestelmän eri osia. Jokainen objekti kuvataan attribuuteilla ja objekteista muodostuva kokoelma määritellään kaavassa. (Microsoft Windows 2000 Training Kit: 247.)

Aktiivihakemiston laajennettava kaava sisältää muodollisen määritelmän Aktiivihakemiston sisällöstä ja rakenteesta. Se Määrittelee attribuutit, luokat ja luokkien ominaisuudet. Kaava määrittelee jokaiselle objektiluokalle, mitä attribuutteja luokan ilmentymillä on oltava, mitä lisäattribuutteja sillä voi olla ja mikä objektiluokka voi olla toisen luokan yläluokka. Aktiivihakemiston kaava on laajennettavissa, mikä tarkoittaa, että siihen voidaan määritellä uusia hakemisto-objekteja ja attribuutteja ja olemassa oleville objekteille voidaan määritellä uusia attribuutteja. Kaava toteutetaan ja tallennetaan Aktiivihakemistoon (globaaliin luetteloon) ja sitä voidaan päivittää dynaamisesti. Näin ollen sovellus voi laajentaa kaavaa uusilla attribuuteilla ja luoda sekä käyttää niitä välittömästi. Kaavan päivitykset suoritetaan luomalla tai muokkaamalla hakemistoon tallennettuja kaavaobjekteja. Kuten kaikki muutkin Aktiivihakemiston objektit, myös kaavaobjektit on suojattu käytönvalvontaluetteloilla (ACL), joten vain valtuutetut käyttäjät voivat muuttaa kaavaa. (Microsoft Windows 2000 Training Kit: 240-247.)

Hakemisto on osa Windows 2000 Trusted Computing Base -rakennetta ja siten myös Windows 2000:n suojaininfrastruktuuria. Trusted Computing Base on joukko käyttöjärjestelmän osia, jotka panevat täytäntöön käyttöjärjestelmän suojakäytännöt. Kaikki Aktiivihakemiston objektit on suojattu käytönvalvontaluetteloilla (ACL), joiden avulla varmistetaan, että Aktiivihakemiston objekteihin tai attribuutteihin kohdistuvat muutokset ovat laillisia. (Microsoft Windows 2000 Training Kit: 247.)

Vain valtuutetut käyttäjät voivat suorittaa Aktiivihakemistoon järjestelmänhallintaa. Riittävät valtuudet omaava järjestelmänvalvoja voi valtuuttaa jonkun käyttäjistä suorittamaan määrättyjä, tiettyihin objekteihin ja luokkiin kohdistuvia toimenpiteitä. Tätä kutsutaan delegoiduksi järjestelmänhallinnaksi (delegated system administration, DSA). Delegoitu järjestelmänhallinta mahdollistaa tehtävien jakamisen ja valtuuksien delegoinnin ilman, että on tarpeen myöntää käyttäjille ylimääräisiä oikeuksia järjestelmään. DSA eristää käyttäjän hakemiston tietojen fyysisestä tallennusformaatista ja mahdollistaa hakemiston helpon käyttämisen sekä lisää järjestelmän turvallisuutta. (Microsoft Windows 2000 Training Kit: 247-248.)

Globaali luettelo on toimialuepuun (joukko toimialueita, jotka muodostavat yhteisen toimialuehierarkian) tai toimialuemetsän (joukko toimialuepuita, jotka

ovat hierarkian osia) objekteja koskevien tietojen keskeinen säilytyspaikka. (Microsoft Windows 2000 Training Kit: 242.)

Aktiivihakemistopalvelut, aivan kuten kaikki muutkin hakemistopalvelut tarkoittavat nimiavaruutta. Nimiavaruus on tahansa rajallinen alue, jonka avulla nimet voidaan selvittää. Tämä tarkoittaa prosessia, jossa nimen perusteella etsitään objekti tai tieto, jota nimi tarkoittaa. Aktiivihakemiston nimiavaruus perustuu DNS:ään, joten se mahdollistaa yhteistoiminnan Internet-teknologioiden kanssa. (Microsoft Windows 2000 Training Kit: 243.)

Aktiivihakemistossa kaikki objektit tunnistetaan nimellä. Aktiivihakemistopalveluissa käytetään useita nimämiskäytäntöjä: yksittäiset nimet (distinguished names), suhteelliset nimet (relative distinguished names), globaalit nimet (globally unique identifiers) ja käyttäjien ensisijaiset nimet (user principal names). Aktiivihakemisto on LDAP-hakemistopalvelu, mikä edellyttää, että hakemisto-objektien nimet on muodostettu tavalla, joka vastaa nimeämisstandardin määrittävän RFC:n (Request For Comments) vaatimuksia. (Microsoft Windows 2000 Training Kit: 244-246.)

4.3.3 LDAP

(Microsoft Windows 2000 Training Kit: 239-240.)

Aktiivihakemiston ydinprotokollana käytetään LDAP-protokollaa (Lightweight Directory Access Protocol), joka mahdollistaa toimimisen käyttöjärjestelmärajojen yli erilaisia nimiavaruuksia integroimalla. Se pystyy hallitsemaan sovelluskohtaisia ja muita NOS-pohjaisia (Network Operating System-verkkokäyttöjärjestelmä) hakemistoja ja tarjoaa näin yleiskäyttöisen hakemiston, jonka avulla voidaan vähentää monien erillisten nimiavaruuksien järjestelmänhallinnalle aiheuttamaa kuormaa ja kustannuksia.

Aktiivihakemisto ei ole X.500-hakemisto. Sen sijaan se käyttää yhteysprotokollana LDAP-protokollaa ja tukee X.500:n tietomallia ilman, että järjestelmien on kannettava X.500:n koko yleiskuorma. Tuloksena on järjestelmien väliset korkean tason yhteiset toiminnot, jotka tukevat erilaisia heterogeenisia verkkoja.

4.3.4 DNS-nimiavaruus ja toimialuerakenne

Aktiivihakemistopalvelun toteutukseen liittyy useita tekijöitä, jotka ovat osa suunnitteluprosessia. Ensiksi on suunniteltava DNS -nimiavaruus. Nimiavaruus sisältää toimialuehierarkian, globaalin luettelon, luottamussuhteet ja replikoinnin. Lisäksi nimiavaruus sisältää organisaatioyksiköt (OU).

Aktiivihakemiston nimiavaruus määrittää yrityksen ylimmän tason toimialuenimen. Se käsittää Windows–toimialueet, toimialueen ohjauspalvelimet, organisaatioyksiköt, luottosuhteet ja toimialuepuut. Eräs päätös, joka on tehtävä, kun Aktiivihakemistopalveluita toteutetaan, on se, tehdäänkö erillinen sisäinen nimiavaruus palomuurin sisäpuolella ja ulkoinen nimiavaruus palomuurin ulkopuolella vai yhdistetäänkö ne. Yksinkertaistettuna kysymys on siitä, onko

Aktiivihakemiston nimiavaruus sama kuin Internet–toimialuenimi, joka organisaatiolla mahdollisesti on. (Microsoft Windows 2000 Training Kit: 257-261.)

Sen lisäksi, että päätetään, käytetäänkö sisäisessä ja ulkoisessa verkossa samaa vai erillistä nimiavaruutta, on olemassa muita muuttujia, jotka vaikuttavat nimiavaruuden arkkitehtuuriin. Organisaatiot ja niiden rakenne muuttuvat jatkuvasti ja on kyettävä muuttamaan nimiavaruuden rakennetta mahdollisimman pienin kustannuksin ja huomaamatta. Tavoitteena on sellainen arkkitehtuuri, joka on skaalautuva, mukautuu muutoksiin, pystyy tekemään eron sisäisten ja ulkoisten resurssien välillä ja kykenee suojaamaan yrityksen tiedot.

Nimiavaruuden arkkitehtuurin tulisi edustaa organisaation rakennetta, mutta samalla sen tulisi olla järjestelmänhallinnallisesti ositettavissa tavalla, jonka Aktiivihakemistopalveluihin perustuvan verkon hallitseminen vaatii. Rakenteen tulee olla skaalautuva ja laajentuva organisaatiossa ja hallinnassa tapahtuvien muutosten varalta. (Microsoft Windows 2000 Training Kit: 257-261.)

Eräs tapa toteuttaa tällainen rakenne on asettaa toimialueet kolmeen kerrokseen:

- Juuritoimialue (esim. microsoft.com)
- Ensimmäinen toimialuekerros (esim. europe.microsoft.com)
- Toinen toimialuekerros (esim. fi.europe.microsoft.com)
    - alitoimialue (esim. sales.fi.europe.microsoft.com)

4.3.5 Organisaatioyksiköt

(Microsoft Windows 2000 Training Kit: 263-266.)

Organisaatioyksikköjen (OU) tulisi heijastaa yrityksen liiketoiminnan rakennetta. Organisaatioyksikköjä voidaan luoda, kun halutaan delegoida pienempiä käyttäjäryhmiä, ryhmiä ja resursseja koskevia järjestelmänhallinnallisia oikeuksia. Myönnetyt järjestelmänhallinnalliset oikeudet voivat olla täydellisiä tai rajoitettuja. Koska ylimmän tason organisaatioyksikköjen alapuolella voi olla muita organisaatioyksikkötasoja, voidaan käyttää niin yksikkökohtaista jaottelua, kuin on tarpeen. Nämä objektit tulee järjestellä loogiseksi rakenteeksi, joka sopii yrityksen toimintatapaan ja rakenteeseen. Organisaatioyksiköt perivät ylemmän toimialueen tai organisaatioyksikön suojauskäytännöt, ellei nimenomaan toisin määritetä.

Organisaatioyksiköiden ansiosta käyttäjille ei tarvitse antaa hallinnollisia oikeuksia toimialuetasolla.. Oikeudet voidaan myöntää organisaatioyksikkötasolla ja siirtää näin yksinkertaisemmat hallintatoimet pois järjestelmänvalvojien harteilta. Organisaatioyksiköt lisäävät turvallisuutta, koska ne mahdollistavat julkisten resurssien rajoitetun näkyvyyden käytönvalvontaluetteloiden avulla: käyttäjät näkevät vain ne objektit, joihin heillä on käyttöoikeus.

Yrityksen organisaatioyksikköjä luotaessa tulee noudattaa seuraavia yleisohjeita:

- Organisaatioyksikköjen tulee mahdollistaa järjestelmänhallinnan delegointi
- Organisaatioyksikkörakenteen tulee mahdollistaa yksikköjen järjestelmänvalvojien tehokas työskentely
- Organisaatioyksikköihin voidaan liittää suojauskäytäntöjä

- Organisaatioyksiköiden avulla voidaan laajentaa tai rajoittaa julkaistujen resurssien näkyvyyttä tietyille käyttäjille
- Organisaatioyksikkörakenteen tulisi olla vakaa. Organisaatioyksikköjen avulla lisätään kykyä mukautua yrityksen vaihtuviin tarpeisiin
- Organisaatioyksikköihin ei tulisi luoda liian monia objekteja

Kun organisaatioyksikkörakennetta ryhdytään suunnittelemaan, on organisaatioyksiköille ja objekteille annettava nimet, jotka ovat hierarkkisia, yhdenmukaisia, staattisia ja kyllin yleisiä minkä tahansa toimialueen käyttöön. Organisaatioyksikön objektien määrä kannattaa pitää mahdollisimman pienenä, jotta haku- ja siirtymiskyselyt eivät aiheuttaisi pullonkauloja. Kun organisaatioyksikkörakenne on luotu, se mahdollistaa tulevat uudelleen järjestelyt mahdollisimman vähillä objektien siirroilla.

On tärkeää päättää, millaiselta pohjalta organisaatioyksikköhierarkiaa lähdetään suunnittelemaan. Seuraava luokittelu tarjoaa erilaisia tapoja määrittää organisaatioyksikköhierarkia:

- Järjestelmänhallinta- tai objektiperusteiset organisaatioyksiköt
- Maantieteelliset organisaatioyksiköt
- Liiketoimintoihin perustuvat organisaatioyksiköt
- Osastokohtaiset organisaatioyksiköt
- Projektikohtaiset organisaatioyksiköt

4.3.6 Toimipaikat

Myös järjestelmän fyysiseen rakenteeseen on tärkeää kiinnittää huomiota, jotta Aktiivihakemistopalveluita tukeva Windows-verkko voidaan toteuttaa menestyksellisesti. Windows-verkon fyysisen rakenteen rajat määrittää toimipaikka. Toimipaikka muodostuu yhdestä tai useasta IP-aliverkosta, jotka on yhdistetty nopeilla linkeillä. Toimipaikan rajat ovat usein samat kuin lähiverkon (LAN) tai nopean laajaverkon (WAN) rajat.

Aktiivihakemiston replikointijärjestelmässä voidaan määrittää, mitä replikoidaan lähiverkon linkkien kautta ja mitä replikoidaan hitaiden WAN-linkkien kautta. Toimipaikan sisäinen liikenne on tavallisesti suurempi kuin toimipaikkojen välinen liikenne. Se miten toimipakat rakennetaan vaikuttaa Windowsiin kahdella tavalla:

- Sisään kirjautuminen työasemiin: Kun käyttäjä kirjautuu sisään, Aktiivihakemistoa tukevat asiakkaat yrittävät löytää toimialueen ohjauspalvelimen samasta toimipaikasta, jossa käyttäjän tietokone on.
- Hakemiston replikointi: Toimialueiden välillä tapahtuva hakemistoreplikoinnin aikataulu voidaan konfiguroida erikseen toisin kuin toimipaikan sisällä tapahtuvassa replikoinnissa.

(Microsoft Windows 2000 Training Kit: 266-268.)

Aktiivihakemiston toimipaikat eivät kuulu nimiavaruuteen. Kun paikallista nimiavaruutta tarkastellaan, nähdään tietokoneita ja käyttäjiä, jotka on ryhmitelty toimialueiden ja organisaatioyksiköiden mukaan, mutta ei toimipaikkojen mukaan. Toimipaikkarakenne on tallennettu hakemiston eri osaan. Toimipaikat sisältävät vain tietokoneobjekteja ja toimipaikkojen välisen replikoinnin konfiguroinnissa käytettäviä yhteysobjekteja.

Kun aliverkot ryhmitellään toimipaikoiksi, on otettava huomioon aliverkkojen välisten linkkien nopeus. Seuraavassa yleisohjeita siitä, kuinka aliverkkoja yhdistetään toimipaikoiksi:

- Vain sellaiset aliverkot, joiden välillä on nopeat ja luotettavat verkkoliitännät, tulee yhdistää. ”Nopea” verkkoliitäntä tarkoittaa, että käytettävissä on ainakin 512 kilobittiä kaistanleveyttä. On järkevää harkita jopa paljon nopeampien linkkien käyttämistä yhtä toimipaikkaa varten.
- Toimipaikat tulee konfiguroida siten, että replikointia tapahtuu vain sellaisena aikana, jolloin se ei haittaa verkon muuta liikennettä.

(Microsoft Windows 2000 Training Kit: 266-268.)

Aktiivihakemistopalvelut ylläpitävät erikseen toimialueen rakennetta ja toimipaikan rakennetta. Toimialue voi sisältää useita toimipaikkoja ja toimipaikka voi sisältää useita toimialueita tai osia useista toimialueista. Suunnittelemalla toimipaikat oikein varmistutaan siitä, että replikointiliikenne ei tuki linkkejä, että Aktiivihakemistopalvelut ovat ajan tasalla ja että asiakastietokoneet käyttävät resursseja, jotka ovat niitä lähinnä. Toimipaikkoja suunniteltaessa on harkittava, mitä toimialueen ohjauspalvelimia aliverkoissa olevien työasemien tulee käyttää. Jotta työasema kirjautuisi vain määrättyihin ohjauspalvelimiin, toimipaikat tulee määrittää siten, että kyseiset ohjauspalvelimet kuuluvat samaan toimipaikkaan kuin työasema. Kannatta miettiä, mihin toimialueen ohjauspalvelimet sijoitetaan, koska jokaisen ohjauspalvelimen on otettava osaa hakemiston replikointiin yhdessä muiden ohjauspalvelinten kanssa. (Microsoft Windows 2000 Training Kit: 266-268.)

Pääsääntöisesti haarakonttorista kannattaa tehdä oma toimipaikka Aktiivihakemistoon, riippuen sen koosta (työasemien määrästä). Kun työasemia on yhdestä viiteen, ei luoda toimipaikkaa, vaan suoritetaan käyttäjien tunnistus hitaan linkin kautta, jota ei varata replikointiliikenteelle. Kun työasemia on enemmän kuin viisi, luodaan toimialue, jolloin toimialueen ohjauspalvelimet sijoitetaan paikallisesti ja käyttäjien tunnistus tehdään toimipaikan sisällä. Replikointiliikenne voidaan määrittää tapahtuvaksi hitaiden linkkien kautta, hiljaisina aikoina. (Microsoft Windows 2000 Training Kit: 266-268.)

4.3.7 Ohjauspalvelinroolit

Aktiivihakemistossa kaikki ohjauspalvelimet (DC) ovat periaatteessa keskenään samanarvoisia. Kaikki hallintatoimenpiteet voidaan suorittaa millä tahansa ohjauspalvelimella, mistä ne replikoituvat muihin aktiivihakemiston palvelimiin. On kuitenkin tiettyjä, toimialuetta tai toimialuemetsää koskevia toimenpiteitä, joita voi suorittaa vain tietyiltä, nimetyiltä, ohjauspalvelimilta. Näitä erityistehtäviä tai ”rooleja” (FSMO (Flexible Single Master Operation)) hoitavia palvelimia kutsutaan toimintopalvelimiksi (Operations Masters). Nämä toiminnot ovat järjestelmän toiminnan kannalta kriittisiä ja siksi niiden tulee sijaita verkossa sellaisella palvelimella jonka toiminta on stabiilia ja varmennettua.

Ohjauspalvelinroolit ovat aina toimialue tai toimialuemetsä kohtaisia ja yksi palvelin vastaa kunkin niiden toiminnasta, joten mikään muu tietokone ei voi hoitaa kyseistä tehtävää. Rooleja on viisi erilaista ja ne ovat Primary domain controller (PDC) emulator, Schema master, Domain naming master, Relative identifier (RID) master ja Infrastructure master. Näistä rooleista Schema master ja Domain naming master ovat koko toimialuemetsää koskevia ja loput koko toimialuetta koskevia palveluita.

Ohjauspalvelinroolien lisäksi ohjainpalvelimien joukosta löytyy myös Global catalog -palvelimia, jotka ylläpitävät globaalia hakemistoa (yleistä luetteloa) Active Directory:sta. Globaali hakemisto pitää sisällään koko Active Directory-tietokannan. Oletuksena se asentuu ensimmäiselle palvelimelle, mutta Global catalog -palvelimiksi voidaan asentaa useita toimialueen ohjauspalvelimia, lisäämään vikasietoisuutta ja kuormantasausta. Suositeltavaa on asentaa ainakin yksi Global catalog -palvelin kuhunkin toimipisteeseen, jossa on oma ohjauspalvelin. (Microsoft Windows 2000 Server Administrator's Companion: 435-443.)

Primary domain controller (PDC) emulator -roolin palvelin käyttäytyy kuten NT4 Primary Domain Controller -palvelin toimialueilla joissa on NT4 Backup Domain Controller -palvelimia tai työasemia ilman Windows 2000/XP-käyttöjärjestelmää. Se emuloi NT4-toimialueen pääohjauskonetta ja huolehtii replikointipyynnöt NT4-varaohjauspalvelimilta (Mixed Mode-toimialueella). Koska hallinta tapahtuu Aktiivihakemistossa, välittää PDC emulator tapahtuneet muutokset NT4-palvelimille ja mikäli käyttäjä ei pysty kirjautumaan toimialueelle, tarkistaa kirjautumista hoitava palvelin PDC emulator:lta onko kyseinen tili lukittu. PDC emulator -palvelin toimii toimialueen pääselaajana tietokoneiden selauspalveluille ja huolehtii toimialueen kellojen synkronoinnista. (Microsoft Windows 2000 Server Administrator's Companion: 435-436.)

Schema master -palvelin ylläpitää Aktiivihakemiston kaavaa (schema) koko toimialuemetsän laajuisesti ja on vastuussa sen levittämisessä koko metsän alueella. Tämä rooli on oletusarvoisesti ensimmäisellä asennetulla palvelimella. Schema master ylläpitää luetteloa kaikista mahdollisista luokista ja attribuuteista, jotka määrittelevät Aktiivihakemiston objekteja. Kun kaavaa päivitetään tai siihen tehdään muutoksia (esimerkiksi asennetaan ohjelmistoja joiden täytyy tehdä muutoksia/lisäyksiä kaavan luokkiin tai attribuutteihin) tulee Schema master -palvelimen olla tavoitettavissa verkosta ja lisäksi kaavaa muutettaessa tulee olla riittävät oikeudet kyseiseen palvelimeen. (Microsoft Windows 2000 Server Administrator's Companion: 437-438.)

Domain naming master -palvelin huolehtii toimialueiden lisäyksistä ja poistoista toimialuemetsässä. Tämä rooli on erittäin tärkeä toimialueiden eheyden ylläpitämiseksi. Toimialueita ei voi lisätä tai poistaa mikäli tätä roolia hoitava palvelin ei ole tavoitettavissa. Lisäksi Domain naming master -palvelin käsittelee myös ulkoisiin hakemistoihin kohdistuvat viittaukset. Domain naming master -palvelimen pitää olla myös Global catalog-palvelin, koska se tarkistaa globaalista hakemistosta jokaisen lisättävän toimialueen nimen yksilöllisyyden. (Microsoft Windows 2000 Server Administrator's Companion: 438-439.)

Relative identifier (RID) master -palvelin pitää huolen että jokaisella toimialueen objektilla on yksilöllinen suojaustunniste (SID). Suojaustunniste kostuu kahdesta osasta: kaikille toimialueen objekteille yhteisestä alkuosasta ja yksilöllisestä RID-tunnisteesta. RID master -palvelin huolehtii että kaikilla toimialueen ohjauspalvelimilla on riittävästi RID-tunnisteita, joista ne voivat muodostaa toimialueen eri objekteille SID-suojaustunnisteita. (Microsoft Windows 2000 Server Administrator's Companion: 439-441.)

Infrastructure master -palvelin tallentaa muutokset, joita toimialueen objekteihin kohdistuu. Kaikki muutokset kirjataan ensin Infrastructure master -palvelimeen, josta ne replikoidaan muihin ohjauspalvelimiin. Sen tehtävänä on huolehtia objekteista ja niiden viittauksista toisiin objekteihin, esimerkiksi

objektin jäsenyyksistä eri ryhmissä. Infrastructure master -palvelinta ei tulisi asentaa samaan palvelimeen joka on Global catalog -palvelin, ellei sitten kaikki toimialueen palvelimet ole Global catalog - palvelimia. Tämä siitä syystä, että toimiakseen kunnolla se ei saisi sisältää tietoa objekteista, jotka eivät ole osa toimialuetta. (Microsoft Windows 2000 Server Administrator's Companion: 441-442.)

Haluttaessa tai tarvittaessa ohjauspalvelin rooleja voidaan siirtää palvelimelta toiselle tai kyseisen toimintopalvelimen ollessa kokonaan poissa käytettävistä roolit voidaan myös kaapata toiselle palvelimelle. Apuna näissä toimenpiteissä käytetään Active Directory Schema -, Active Directory Users and Computers-ja Active Directory Domains and Trusts-työkaluja.

4.3.8 Ryhmäkäytännöt

Ryhmäkäytännöillä (group policies) tarkoitetaan kokoonpanoasetuksia, jotka voidaan liittää Aktiivihakemiston objekteihin. Ryhmäkäytännöt tekevät mahdolliseksi käyttäjien työpöytäympäristöjen järjestelemisen ja hallinnan keskittämisen. Niiden avulla voidaan määrittää, mitä ohjelmia käyttäjät voivat käyttää, mitkä ohjelmat näkyvät ja millaisia valintoja käynnistysvalikossa on käytettävissä. Ryhmäkäytännöt vaikuttavat käyttäjätileihin, ryhmiin ja tietokoneisiin ja niitä voidaan lisäksi määrittää organisaatioyksikkö- tai toimipaikkatasolla.

Ryhmäkäytäntö sisältää asetukset, joilla hallitaan Aktiivihakemiston objektin tai sen aliobjektien käyttäytymistä. Nämä asetukset tallennetaan ryhmäkäytäntöobjekteihin (group policy object, GPO) kahteen paikkaan: Aktiivihakemiston objektiin nimeltä ryhmäkäytäntöjen säiliö (group policy container, GPC) ja kansiorakenteeseen nimeltä ryhmäkäytäntöjen mallit (group policy template, GPT). Ryhmäkäytäntöobjektien rakenne jää suurimmalta osin näkymättömiin. (Microsoft Windows 2000 Training Kit: 377-407.)

Ryhmäkäytäntöjen avulla voi laatia käyttäjille valmiin työpöytäympäristön, joka voi sisältää mukautetun käynnistysvalikon, valmiiksi asennetut ohjelmat ja tiedostoja, kansioita sekä Windows-asetuksia koskevat käyttöluvat. Ryhmäkäytännöt voivat lisäksi vaikuttaa käyttäjätileille ja ryhmille myönnettyihin oikeuksiin. Toimipaikkaan, toimialueeseen tai organisaatioyksikköön voidaan liittää yksi tai useita ryhmäkäytäntöobjekteja. Yhteen ryhmäkäytäntöobjektiin voidaan liittää useita Aktiivihakemistossa olevia säiliöitä ja yhteen säiliöön voi liittyä useampia kuin yksi ryhmäkäytäntöobjekti. Ryhmäkäytännön voimassaoloalue määräytyy turvaryhmän jäsenyyden kautta. Jos ryhmäkäytäntötietoja on vähän ja ne muuttuvat harvoin, ne tallennetaan ryhmäkäytäntöjen säiliöön, jos tietoja on paljon ja ne voivat muuttua usein, ne tallennetaan ryhmäkäytäntöjen malliin. (Microsoft Windows 2000 Training Kit: 377-407.)

Ryhmäkäytännöt vaikuttavat useisiin verkon komponetteihin ja Aktiivihakemiston objekteihin. Aktiivihakemistossa on käytettävissä seuraavat ryhmäkäytäntötyypit:

- Software Settings: Vaikuttaa sovelluksiin, joita käyttäjällä on lupa käyttää. Sovellusten asennus voidaan automatisoida kahdella tavalla:

    - Sovellusten liittäminen käyttäjiin (application assignment), joka asentaa tai päivittää tietokoneen sovelluksen automaattisesti tai tarjoaa käyttöön sovelluksen, jota ei voi poistaa.
    - Sovellusten julkaiseminen (application publishing), jossa julkaistaan sovellukset Aktiivihakemistossa. Tämän jälkeen sovellus näkyy niiden komponenttien luettelossa, jotka käyttäjä voi asentaa (ja poistaa) ohjauspaneelin lisää/poista sovellustoiminnolla.
- Scripts: Määritettyjä scriptejä ja komentotiedostoja, jotka suoritetaan tiettyyn aikaan (järjestelmän käynnistys tai sulkeminen tai käyttäjän kirjautuminen sisään tai ulos). Näillä automatisoidaan toistuvia tehtäviä (kuten verkkoasemien liittäminen).
- Security Settings: Mahdollistaa tiedostojen ja kansioiden käytön rajoittamisen, tilin käyttörajoitusten määrittämisen, paikallisten käytäntöjen määrittämisen, palvelujen toiminnan hallinnan, rekisterin ja tapahtumalokin käytön rajoittamisen ja julkisen avaimen käytön sekä IP - turvakäytäntöjen (IPSec) määrittämisen.
- Administrative Templates: Rekisteriperusteiset ryhmäkäytännöt, joiden avulla määritetään työpöydän käyttäytymistä ja ulkoasua ohjaavat asetukset.
- Etäasennuspalvelut (Remote Installation Services, RIS): Hallitsee etäasennusasetuksia, jotka näkyvät käyttäjälle, kun hän käynnistää ohjatun Client Installation-toiminnon.
- Kansion uudelleenohjaus (Folder Redirection): Mahdollistaa Windows:n erityiskansioiden uudelleenohjauksen verkkoon vaihtoehtoiseen paikkaan, jossa niitä voidaan hallita keskitetysti.

(Microsoft Windows 2000 Training Kit: 377-407.)

Käyttäjien käyttöympäristöä voidaan ryhmäkäytäntöjen avulla parantaa seuraavasti:

- Lisäämällä tai poistamalla sovelluksia käyttäjien käynnistysvalikoista.
- Mahdollistamalla sovellusten jakelu niin, että käyttäjät voivat helposti löytää sovelluksia verkosta ja asentaa niitä.
- Sijoittamalla tiedostoja tai pikakuvakkeita sopiviin paikkoihin verkossa tai tiettyihin tietokoneissa oleviin kansioihin.
- Käynnistämällä tehtäviä tai ohjelmia automaattisesti, kun tietokone käynnistetään tai suljetaan tai käyttäjä kirjautuu sisään tai ulos.
- Lisäämällä tietojen luotettavuutta, saatavuutta ja turvallisuutta uudelleen ohjaamalla kansioita sopiviin paikkoihin verkossa.

Ryhmäkäytäntöjen suurimmat edut syntyvät suoraan kustannussäästöistä. Todelliset omistamisen kustannukset (total cost of ownership, TCO) tarkoittavat kustannuksia, jotka syntyvät hajautetun tietoverkon käytöstä ja ylläpidosta. Tutkimusten mukaan suurin osa näistä kustannuksista aiheutuu menetetystä työajasta. Työajan menetykset taas syntyvät tavallisesti käyttäjän virheestä, siitä, että käyttäjä muuttaa järjestelmän kokoonpanotiedostoja ja tekee tietokoneen toimintakelvottomaksi. Menetyksiä aiheuttavat myös lukuisat tarpeettomat ohjelmat ja ominaisuudet. Kustannuksia voidaan vähentää ryhmäkäytäntöjen avulla, luomalla käyttäjille työtehtävien ja kokemuksen mukaan räätälöity, hallittu työympäristö. (Microsoft Windows 2000 Training Kit: 377-407.)

5 Seurakunnan järjestelmän lähtötilanne

Ylöjärven seurakunnan tietojärjestelmä on alun perin toteutettu 1990-luvun puolen välin jälkeen, Microsoftin tuotteiden pohjalta. Järjestelmää on myöhemmin laajennettu tarpeiden mukaan. Tässä luvussa käsittelen järjestelmää sellaisena kuin se oli ennen projektissamme toteutettuja muutoksia (LIITE3). Osittain kuvaan järjestelmää jo aiemmalta ajalta (LIITE2), jotta projektin tarpeet ja lähtökohdat tulisivat mahdollisimman selväksi.

Ensimmäinen vaihe päivitysprojektissamme oli järjestelmän kartoitus ja dokumentointi. Tiedot kerättiin ja tarkistettiin vuoden 2004 aikana, ennen varsinaisen päivitysprojektin alkua. Lähtötilanteen selvittäminen ei sinänsä ollut kovin haasteellinen, eikä ongelmallinen työvaihe. Ylläpidossa mukana olleille henkilöille järjestelmän tila ja siinä olevat ongelmat olivat tuttuja ja dokumentaatio oli pääosin olemassa.

Pitkään ennen varsinaista järjestelmän päivitystä oli tiedossamme ollut tarve kyseiselle operaatiolle. Normaalin ylläpitotoiminnan yhteydessä tehdyissä ratkaisuissa olimme jo varautuneet tulevaan projektiin. Uudet työasemat oli vakioitu tiettyyn mallisarjaan vuonna 2001. Työasemakäyttöjärjestelmien testaus ja vakiointi oli suoritettu Windows 2000 Professional:n osalta vuonna 2001 ja Windows XP Professional:n osalta vuonna 2003. Vuosina 2001–2004 oli työasemia tarvittaessa korvattu vakioiduilla laitteilla, joita voitaisiin hyödyntää jatkossakin.

Lisäksi teimme jo ennen vuotta 2005 joitakin varsinaisia järjestelmän muutostöitä, joita käsittelen työssäni. Muutokset johtuivat aina akuutista tarpeesta ja niissä huomioitiin edessä oleva järjestelmän kokonaisvaltainen muutos. Merkittävimpiä toimenpiteitä olivat Windows 2000 Server -palvelimen asennus tietokantapalvelimeksi keväällä 2003, TOIMIPAIKKA3:n liittäminen verkkoon sillatulla WLAN-yhteydellä syksyllä 2004 sekä useiden MFP-tulostinten (kopiokoneiden) liittäminen verkkoon vuosina 2003–2004.

5.1 Järjestelmän kartoitus

Järjestelmän kartoitus toteutettiin olemassa olevan dokumentaation pohjalta. Kävimme läpi kaikki tietojärjestelmään kytketyt laitteet, sekä niissä käytetyt sovellukset. Kartoitusvaiheessa tarkistettiin jokainen työasema, oheislaite, verkon aktiivilaite ja palvelin (merkki, malli ja sarjanumero, hankintapäivämäärä ja takuutiedot sekä käyttöjärjestelmien ja ohjelmistojen versiot ja asennetut päivitykset). Nämä tiedot päivitettiin dokumentaatioon, joka samalla muutettiin hyödynnettävämpään muotoon.

Kartoitus ja dokumentointi vaativat paljon eri paikkoihin sijoitettujen laitteiden luona tapahtunutta työtä. Emme käyttäneet mitään keskitettyä kartoitusmenetelmää (analysointiohjelmisto tms.), vaan päädyimme tekemään kartoitustyön fyysisesti paikanpäällä. Halusimme tarkistaa kunkin laitteen fyysisen toimintaympäristön ja siitä mahdollisesti aiheutuvat ongelmat tai riskit. Kartoitukseen osallistui useita projektissa mukana olleita henkilöitä, joten dokumentoinnin yhdenmukaisuuden ja versionhallinnan merkitys korostui. Kartoitustyön ohella

selvitimme myös kunkin käyttäjän ja laitteen kohdalla esiin tulleet ongelmakohdat ja tarpeet tulevaa päivitystä ajatellen.

5.1.1 Palvelimet

Järjestelmän ohjauspalvelimena toimi Windows NT 4.0 Server -palvelin SERVER#1. SERVER#1 oli asennettu vuonna 1997 ja sitä oli aktiivisesti ylläpidetty koko elinkaaren ajan. Siihen oli päivitetty kaikki tarpeelliset tietoturva- ja ohjelmistopäivitykset ja sen laajennuskapasiteetti oli käytetty loppuun. SERVER#1-palvelin toimi seurakunnan toimialueen ohjauspalvelimena, tulostuspalvelimena ja tiedostopalvelimena, sähköpostipalvelimena sekä varmistuspalvelimena.

Järjestelmään oli asennettu myös Windows 2000 Server -palvelin: SERVER#2. SERVER#2 oli asennettu toimialueelle jäseneksi, ilman ohjauspalvelinrooleja. Palvelimella sijaitsi Status -ohjelmiston käyttämä Solid SQL-palvelin. SERVER#2:ta käytettiin ainoastaan tietokantapalvelimena.

SERVER#1-palvelimen todettiin tulleensa elinkaarensa loppuun. Sen ohjaama NT4-toimialue rajoitti seurakunnan tietojärjestelmän kehittämistä.

5.1.2 työasemat

Työasemat olivat myös osittain vanhentuneita ja laitekanta oli erittäin kirjava. Käyttöjärjestelminä oli aiemmin käytetty MS Windows 95/98 sekä MS Windows NT 4.0 Workstation versioita. Osa työasemista oli ehditty jo uusia (Windows 2000 tai XP), mutta suuri osa oli vielä vanhempaa laitekantaa.

Kartoitusvaiheessa verkkoon oli liitetty 19 työasemaa. Etäkäytön avulla järjestelmään oli yhteydessä 6 työasemaa, seurakunnan eri toimipaikoista.

5.1.3 Lähiverkko

Lähiverkko kattoi projektimme alussa kaksi seurakunnan toimipistettä: PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA2:n. Seurakunnan käytössä oli KIRKKOverkon C-luokan (10.x.x.x/24) IP-verkko. Verkon runkona toimivat 1990-luvulla hankitut keskittimet. Ne olivat eri laitevalmistajien 10Base-T-standardin mukaisia (tiedonsiirtokapasiteetiltaan 10Mb/s) laitteita.

Fyysinen lähiverkkokaapelointi oli rakennettu 1990-luvun lopulla sekä PÄÄTOIMIPAIKKA:an, että TOIMIPAIKKA2:een. Kaapelointi oli toteutettu CAT-5e-standardin mukaisesti ja siitä oli olemassa mittauspöytäkirjat. Muissa toimipaikoissa ei ollut varsinaista verkkokaapelointia, eikä paikallisia lähiverkkoja.

5.1.4 Sillattu WAN-verkko

Verkossa olleiden kahden toimipaikan lähiverkot oli yhdistetty toisiinsa sillatulla yhteydellä. Toimipaikat käyttivät yhteistä IP-osoiteavaruutta, jakoivat yhteiset palvelut ja näkyivät käyttäjille yhtenä laajaverkkona. Verkkojen yhdistämisessä oli käytetty hyväksi sillattua HDSL-yhteyttä. Yhteys oli hankittu vuokrapalveluna operaattorilta. Vuokrattu yhteys sisälsi tarvitut 2 kupariparia (4 johdinta) toimipaikkojen välillä, sekä käytetyt päätelaitteet Ethernet-rajapinnalla. Yhteyden nopeus oli 512/512Kbps. kuukausikustannus tällä, ”kuristetulla” nopeudella oli vähintäänkin ”merkittävä”.

5.1.5 Etäyhteydet

Muita seurakunnan toimipaikkoja ei ollut yhdistetty varsinaiseen tietoverkkoon. Niissä sijainneet työasemat olivat yhteydessä verkkoon modeemilla, käyttäen SERVER#1-palvelimeen asennettua RAS-etäkäyttöpalvelua (Remote Access Service). Modeemiyhteyksiä käytti osa työntekijöistä etätyöhön kotoaan ja sitä hyödynnettiin myös huolto- ja ylläpitotehtävissä.

5.1.6 Muut verkkoon kytketyt laitteet

Seurakunnassa oli käytössä lukuisia työasemiin kytkettyjä, henkilökohtaisia, mustesuihku- ja lasertulostimia. Verkkoon oli asennettu 4 lasertulostinta sekä 3 MFP-tulostinta (kopiokonetta).

Tietoverkkoa ei hyödynnetty muuhun kuin PC-verkon tarpeisiin.

5.2 Käytetyt ohjelmistot

Työasemissa käytettiin pääasiassa Microsoft Office-ohjelmistoja (vanhemmissa Office 97-versiota ja uudemmissa XP/2003-versioita) ja Status-toiminnanohjausohjelmistoa. PDF-dokumenttien tuottamiseen käytettiin PDF-XChange -ohjelmistoa ja lukuun Adobe Acrobat reader -ohjelmistoa. Joissakin työasemissa käytettiin erinäisiä kuvankäsittelyohjelmistoja sekä hengellisen työn erityisohjelmistoja: Labora, MikroRabbi, Capella. Käytettyjen ohjelmistojen tietokannat ja niillä tuotetut dokumentit sijaitsivat palvelimella. Sähköpostiohjelmana käytettiin Microsoft Outlook-ohjelmistoa, yhdessä Microsoft Exchange-palvelimen kanssa. Kaikissa työasemissa oli F-Securen Anti-Virus -ohjelmisto.

5.2.1 Microsoft Office

Perus toimisto-ohjelmistoina käytettiin Microsoftin Office -ohjelmistoja. Ohjelmistoja käyttivät kaikki käyttäjät normaaliin asiakirjahallintaan. Seurakunta on hankkinut kaikki Office-lisenssit erillisinä OEM-lisensseinä (vain uuden lait-

teen yhteydessä hankittava lisenssi), työasemahankintojen yhteydessä. Käytössä ei ole ollut yhtenäistä ja keskitettyä lisensointisopimusta. Seurakunnan käyttöön on vakioitu pienyrityksille suunnattu SBE (Small Business Edition)-versio Microsoft Office paketista, joka sisältää vain perusohjelmistot (Word, Excel, PowerPoint, Outlook).

5.2.2 Microsoft Exchange

Seurakunnan käytössä oli MS Exchange 5.5 -sähköpostipalvelin. Se oli aikoinaan hankittu sisäistä sähköpostiliikennettä ja tiedottamista varten. Palvelimessa oli täysin oma, organisaation sisäinen, nimiavaruus käytössä. Tilien hallinta oli yhtenäinen käytössä olleen NT4 -toimialueen kanssa.

Kirkkohallitus on hankkinut Internet - yhteydet ja sähköpostijärjestelmän oman toimintansa tukemiseen. Yleiseksi tavaksi on muodostunut avata työntekijöille ns. henkilökohtaisia sähköpostiosoitteita, yleensä muotoa: etunimi.sukunimi@työnantaja.fi. Tällainen on käytäntö Kirkkohallituksessakin. Järjestelmät on hankittu ensisijaisesti työasioiden hoitamista varten ja työntekijät sitoutuvat noudattamaan niiden käytöstä annettuja ohjeita ja pelisääntöjä. Sillä on oikeus määrätä työntekijöiden sähköpostin ja tietoverkon käytöstä. Oikeus perustuu työvälineiden ja laitteiden omistusoikeuteen sekä työnjohto- ja valvontavaltaan. (Sähköpostin ja Internetin käytön pelisäännöt kirkkohallituksessa.)

Myös Ylöjärven seurakunnassa oli otettu käyttäjien käyttöön valtakunnallisia Internet-sähköpostitilejä ja niihin kuuluvia etunimi.sukunimi@evl.fi -muotoisia sähköpostiosoitteita. Nämä tilit oli asennettu aina käyttäjäkohtaisesti. Tämä tarkoitti sitä, että kullakin Internet-sähköpostitilin omaavalla käyttäjällä oli määriteltynä paikallisesti, oman työasemansa sähköpostiohjelmaan (Outlook), Exchange-yhteyden lisäksi myös erillinen Internet-sähköpostitili. Internet-sähköpostitilin viestit luettiin erikseen ja tallennettiin, tässä tapauksessa ainoastaan tietosäilönä toimivaan, Exchange-palvelimeen. Viime vuosien aikana lähes kaikille seurakunnan työntekijöille oli otettu käyttöön Internet-sähköposti. Tämä aiheutti sähköpostien ylläpidossa suuria ongelmia. Sähköpostien kaikenlainen keskitetty hallinta oli täysin mahdotonta ja kaikki asetukset piti määritellä käyttäjäkohtaisesti, paikan päällä.

5.2.3 Status

Seurakunnan tärkeimpänä operatiivisena ohjelmistona käytetään Status-toiminnanohjausjärjestelmää. Ohjelmisto on julkishallinnon, kuten kuntien ja seurakuntien, yleisesti käyttämä. Ohjelmistolla hoidetaan seurakunnan tarjoamien julkisten palveluiden ohjaus ja seurakunnan tukitoimien hallinta. Ohjelmistoa käytetään muun muassa taloushallintoon, väestötietojen ylläpitoon, henkilöstöhallintaan sekä hautaustoimen ohjaukseen.

Status-ohjelmistossa käytetään Solid SQL-tietokantahallintajärjestelmää. Ohjelmisto oli tietokantoineen asennettuna SERVER#2-palvelimelle. Ohjelmistosta on erilliset tiedonsiirtoyhteydet muun muassa rahaliikennettä ja väestötietoja varten.

5.3 Virustorjunta

Kirkkoverkossa on suositukset käytettävistä virustorjuntaohjelmistoista sekä keskitetyt hankintasopimukset eri toimittajien kanssa.

Virustorjunta oli toteutettu käyttämällä työasemissa ja palvelimissa F-Secure Anti-Virus -ohjelmistoja. Ohjelmistot olivat paikallisesti työasemille asennettuja. Pääsääntöisesti ne oli ylläpidetty kohtalaisella tasolla, versioiden ollessa melko uusia kaikissa työasemissa. Toisaalta versiokirjo oli varsin laaja eri työasemien välillä.

5.4 Keskitetyt varmistukset

Seurakunnan tietojärjestelmän varmistaminen oli toteutettu keskittämällä kaikki käytettävä tieto palvelimille ja varmistamalla se sieltä keskitetysti ja automatisoidusti varmistusnauhoille.

Varmistaminen oli suoritettu palvelimelta SERVER#1, johon tiedot oli tallennettu. Varmuuskopioinnissa käytettiin ARCServe Backup 8.5-ohjelmistoa. Tiedot varmistettiin palvelimelle asennettuun 24GB:n tallennuskapasiteetin omaavaan varmistusnauhuriin. Varmistuksessa nauhalle kopioitiin kaikki tiedostot ja hakemistorakenne sekä NT4-toimialueen rakenne ja käytännöt (system state). Varmistus suoritettiin jokaisena arki-iltana. Näin saatiin luotettava ja täydellinen varmuuskopio jokaiselle rutiinissa käytetylle varmistusnauhalle. Tällä mahdollistettiin tietojen hallittu palauttaminen kultakin nauhalta erikseen. Palautus oli mahdollista niin yksittäisten tiedostojen, kuin koko järjestelmänkin (full restore / emergency restore) osalta. SERVER#2-palvelimella sijainnut Solid SQL - tietokanta varmistettiin verkon kautta, osana SERVER#1-palvelimen varmistusrutiinia. Palvelimilla sijainneet tietokannat (MS Exchange ja Solid SQL) ajettiin automatisoidusti alas varmistuksen alkaessa ja nostettiin taas ylös kopioinnin päätyttyä. Tällä tavoin myös ko. tietokannat saatiin varmistettua, vaikkakin se aiheutti tietokantoihin käyttökatkon itse varmistuksen ajaksi.

5.5 Aiemmat muutokset ja akuutit toimenpiteet

Vuonna 2002 työasemakanta oli jaettu tiettyihin ryhmiin. Iän, käyttötarpeen, käyttöjärjestelmän ja kriittisyyden suhteen oli laadittu elinkaarimalli, jossa kukin työasema vaihtuisi uuteen tietyn kierron mukaisesti. Myös laitteiden mallisarjat oli vakioitu (2001) ja käyttöjärjestelmäksi valittu MS Windows XP (2003). Tätä mallia käyttäen oli osa järjestelmän työasemista jo vaihtunut ajanmukaisiksi. Uudet tai rikkoutuneiden tilalle hankitut työasemat olivat vakioinnin mukaisia. Päivitysprojektin käynnistyessä päätettiin elinkaarikierron

mukaista uusintaa nopeuttaa vanhimpien laitteiden osalta niin, että saisimme päivityksen yhteydessä aikaiseksi yhdenmukaisen laiteympäristön.

SERVER#1 -palvelimen prosessointi- ja levytilakapasiteetin oli käynyt riittämättömäksi seurakunnan toiminnanohjaukseen käytetyn Solid SQL-tietokannan vaatimuksille. Tästä syystä oli keväällä 2003 asennettu järjestelmään erillinen MS Windows 2000 Server -palvelin; SERVER#2. SERVER#2 oli asennettu toimialueelle jäseneksi, ilman mitään ohjauspalvelinrooleja. Siihen oli siirretty pelkästään SQL-tietokantapalvelut SERVER#1:ltä. Päivitysprojektimme valmistelevana toimenpiteenä, siirrettiin syksyllä 2004 SERVER#2-palvelimelle lisää palveluita ja SERVER#1:n kuormitusta kevennettiin entisestään. SERVER#2:lle siirrettiin tulostuspalvelut, suurin osa levyjaoista sekä DNS-palvelut (DHCP- ja WINS-palvelut säilyivät SERVER#1:llä).

Vuosina 2003–2004 oli tulostusta tehostettu, uusimalla seurakunnan käytössä olleet kopiokoneet verkkoon liitetyillä MFP-tulostimilla.

Kartoituksen jälkeen kävimme lävitse olemassa olevan laitekannan ohjelmistoversiot ja niiden päivitystilanteen. Keräämiemme tietojen pohjalta tehtiin uusi, ”ylläpidollinen”, kierros järjestelmään kytkettyjen laitteiden parissa. Tämän yhteydessä saatettiin kaikkien laitteiden (työasemat, oheislaitteet, palvelin) käyttöjärjestelmien, ohjelmistojen ja ajureiden versiot ja päivitykset yhdenmukaisiksi ja viimeisimmälle mahdolliselle tasolle. Näin saimme yhtenäiset työkalut kaikille järjestelmän käyttäjille sekä selkeän lähtökohdan järjestelmän kehittämiselle.

Ennen verkkoon tehtyjä muutoksia sen liikennettä seurattiin protokolla-analysointiin tarkoitetulla Ethereal-ohjelmistolla. Tavoitteena oli karsia pois kaikki turha verkkoliikenne. Saatujen tulosten perusteella, tarkistettiin laitepäivitysten yhteydessä niiden verkkoasetukset. Käytöstä poistettiin kaikki muut verkkoprotokollat paitsi TCP/IP. Lisäksi joidenkin laitteiden ”tarkistuspakettien” lähettämisen aikavälejä kasvatettiin.

6 Seurakunnan järjestelmän päivitys ja käyttöönotto

Tässä luvussa kuvaan varsinaisia työvaiheita ja käyttämiämme menetelmiä tietojärjestelmän päivityksen yhteydessä. Vertailen eri toteutustapojen etuja ja haittoja keskenään sekä esitän perusteluja niille ratkaisuille, joihin lopulta päädyimme. Käyn läpi projektissa esiin nousseita ongelmia, teknisiä ratkaisuja sekä käytännön työhön liittyviä huomioita.

Projekti haluttiin toteuttaa mahdollisimman yksinkertaisesti ja kustannustehokkaasti. Eri työvaiheita tehtiin vaiheittain vuonna 2005. Asennustyöt pyrittiin suunnittelemaan siten, että ne vaikuttaisivat käyttäjien normaaliin työskentelyyn mahdollisimman vähän. Ratkaisuissa tuli huomioida useita käyttäjien tarpeista esiin nousseita asioita joita aiempi järjestelmä ei mahdollistanut.

Ensin päivitimme eri toimipaikkojen paikalliset lähiverkot ja niiden väliset WAN-yhteydet. Tämän jälkeen suoritimme varsinaisen AD:n käyttöön siirtymisen. Lopuksi teimme ohjelmisto asennuksia sekä erilaisia testauksia. Toimipaikkojen verkkojen ja niiden välisten yhteyksien päivittäminen tehtiin toimipaikkakohtaisesti, 1-3 päivän mittaisina osaprojekteina. Eniten varsinaisia asennus- ja muutostöitä vaatinut, AD:n käyttöönotto, toteutettiin ennalta sovittuna ajankohtana. Muutos tehtiin kolmen päivän aikana, keskiviikon ja perjantain välillä (LIITE4-5). Tuolloin järjestelmässä oli käyttökatko keskiviikkoillasta torstaiaamuun. AD:n käyttöönotossa oli mukana kuusi henkilöä.

6.1 Verkon päivitys

Ylöjärven seurakunnalla on toimintaa ja henkilökuntaa useissa eri toimipisteissä. Lähes kaikki toiminta vaatii tänä päivänä tuekseen myös erilaisia tietojärjestelmiä. Tietojärjestelmien tulee olla käytettävissä käyttäjällä pääsy verkon resursseihin mistä tahansa.

Verkon aktiivilaitteiden ja tietoliikenneyhteyksien osalta todettiin muutosten olevan tarpeellisia. Aiemmin ainoastaan ”PÄÄTOIMIPAKKA” ja TOIMIPAIKKA2 olivat yhdistettyinä toisiinsa. Muista toimipisteistä käytettiin tieverkon modeemiyhteyden avulla. Tavoitteena oli saada lähiverkot kaikkiin toimipaikkoihin ja yhdistää ne kiinteällä verkkoyhteydellä PÄÄTOIMIPAIKKA:an. Aiemmin käytetyt etäkäyttöpalvelut haluttiin poistaa käytöstä. Verkon toteutuksessa käytetyt tekniikat ja laitteet haluttiin vakioida.

Lähiverkon kaapelointi todettiin riittävän hyväksi PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA2:n osalta. Näissä runkokaapelointi oli toteutettu CAT5e-standardin mukaisesti. Lähiverkot oli alun perin 1990-luvulla rakennettu tähtimäisiksi ja suunniteltu käytettäviksi keskittimien avulla. Lähiverkojen tähtitopologian todettiin olevan hyvä ja kehittämiskelpoinen ratkaisu, eikä sitä haluttu muuttaa. Uusina toteutettavien TOIMIPAIKKA3:n, TOIMIPAIKKA4:n ja TOIMIPAIKKA5:n lähiverkkojen toteutuksissa päädyttiin myös käyttämään CAT5e-standardin mukaista kaapelointia. Verkoista saatiin yhdenmukaiset ja toteutus oli kustannustehokas. Vaihtoehtoisia tekniikoita (CAT6:sta, valokuituyhteyksiä tai WLAN-toteutuksia) ei edes harkittu. Toimipaikkoihin rakennettiin yleiskaapelointi sekä ristikytkentätilat. Kaapeloinnin osalta dokumentointiin sisällytettiin ko. urakoista vaaditut mittauspöytäkirjat. Myös vanhat yleiskaapeloinnit

mittautettiin uudelleen. Ristikytkennät purettiin ja rakennettiin uudelleen. Rakennetuissa ristikytkennöissä otimme käyttöön kytkentäkaapelien värikoodauksen sekä kaapelien merkintäpannat. Työasemien LAN-liitännöissä käytimme harmaita kaapeleita (VLAN_1), tulostimilla sinisiä (VLAN_1), palvelimella punaista (VLAN_2 = DMZ), tietoliikenneyhteyksissä keltaisia (kaikki VLANit) ja taloautomaatiojärjestelmässä vihreitä (VLAN_3).

WAN-yhteyksien suunnittelu aloitettiin sopivien yhdistämistekniikoiden kartoituksella. Selvitimme yleisten WAN-tekniikoiden soveltuvuuden seurakunnan käyttöön. Vertailtaviksi tekniikoiksi valitsimme yleisesti käytössä olevat tekniikat: kupari-/valokaapeli Ethernet, ADSL, HDSL, VDSL, Frame relay ja WLAN. Vertailua suoritettiin myös eri laitteiden/valmistajien välillä. Vertailussa huomioitiin: ominaisuudet, asennus, hallittavuus, ylläpito ja tuki, skaalautuvuus, luotettavuus, kustannukset. Tarkempaa tarkastelua vaati WAN-yhteyksissä käytettävän tekniikan lisäksi se, käytettäisiinkö sillattuja vai reititettyjä yhteyksiä (Kuva 5.1 ja 5.2). Sillattujen yhteyksien etuna on selvästi helpompi käyttöönotto ja yksinkertaisempi hallinta. Olemassa oleva järjestelmä laajentuu uusiin toimipaikkoihin, ilman suuria muutostöitä. Reititetyillä yhteyksillä on mahdollista eri verkkojen aliverkottaminen ja reititettävän tiedon hallittavuus. Näin voidaan luoda tietoturvallisempi ja hallittavampi verkko sekä säästää ”hitaan” WAN-yhteyden kaistaa ainoastaan oleelliseen tietoliikenteeseen.

Yhteydet päädyttiin toteuttamaan sillattuina. Tämä ratkaisu oli todettu toimivaksi ja se oli sekä käyttäjille, että ylläpitäjille, tuttu. Ratkaisussa voitiin säilyttää olemassa oleva KIRKKO-verkon aliverkkoavaruus, jossa tiettyjä IP -osoitteita oli ”sidottu” tiettyihin palveluihin. Lisäksi voitiin helposti, ilman muutoksia, hyödyntää olemassa olevia keskitettyjä palveluita (kuten DHCP), koko verkon alueella. Mahdollisuus muuttaa toteutetut sillatut yhteydet reititetyiksi ja erottaa toimipaikat toisistaan aliverkoilla otettiin huomioon laitevalinnoissa ja WAN-yhteyksiä asennettaessa.

6.1.1 Kytkimet

Verkon laitteet oli yhdistetty toisiinsa 10Mbps suorituskyvyn omaavin keskittimin. Tämä oli selkeä ongelma jo pelkästään suorituskykynsä puolesta. Lähiverkon keskittimet päätettiin korvata tämän päivän suorituskyvyn omaavilla ja standardien mukaisilla kytkimillä. Näin verkko tulisi segmentoitua järkevästi ja tarpeeton verkkoliikenne saataisiin pois kuormittamasta verkkoa. Hankittavat kytkimet haluttiin vakioida tiettyihin malleihin. Vakioinnilla pyrittiin takaamaan yhteensopivuus sekä mahdollisten vika- ja ongelmatilanteiden nopea korjaus.

Kytkinten ominaisuuksille asetettiin seuraavat vaatimukset: helppo asennus/käyttöönotto, automaattinen yhteysnopeuden tunnistus (10/100Mbps), mahdollisuus 1000Mbps yhteyksiin, hallittavuus, mahdollisuus erottaa loogisesti eri verkot toisistaan (VLAN -tuki), liikenteen priorisointi (QoS) sekä mahdollisuus SNMP-protokollaan perustuvaan valvontaan.

Jokaiseen toimipaikkaan asennettiin aiemmin määritellyn mukainen kytkin. Aiemmin käytössä olleet keskittimet (PÄÄTOIMIPAIKKA ja TOIMIPAIKKA2) korvattiin kytkimillä. Uusiin toimipaikkoihin (”TOIMIPAIKKA3-5”) rakennettiin lähiverkot kytkinten avulla. Jokaisen toimipaikan hankinnat tehtiin erikseen, hinta-/laatuvertailun pohjalta. Kytkimiä hankittiin kahdelta eri laitevalmistajalta.

6.1.2 Sillatut xDSL-yhteydet

Tämän päivän kustannustehokkaimpia ja käytetyimpiä WAN-tekniikoita ovat erilaiset DSL-yhteydet. Niiden suurin etu on mahdollisuus hyödyntää jo olemassa olevaa puhelinkaapelointia. Suurimmassa osassa WAN-yhteyksiä päädyimme käyttämään eri DSL-tekniikoita. Päätelaitteet hankittiin seurakunnalle ja ainoastaan tarvittavat kupariyhteydet vuokrattiin operaattoreilta. Näin saatiin aikaiseksi merkittäviä kustannussäästöjä lyhyessä ajassa. Hankittuihin päätelaitteisiin otettiin myös takuun laajennukset, jolloin niissä ilmenneet ongelmat kuuluvat laitetakuun piiriin koko käyttöiän. DSL-päätelaitteet määriteltiin silta-tilaan, jolloin ne vain siirtävät IP-paketit hitaamman kupariyhteyden ylitse ja muodostavat ne uudelleen. Päätelaitteet asennettiin toimipaikkojen ristikytkentätiloihin, kytkinten yhteyteen. Hintavertailun pohjalta laitteita hankittiin kahdelta eri laitevalmistajalta. Kaikki hankittujen laitteiden ominaisuuksiin kuuluu VLAN-tuki.

PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA4:n välinen yhteys toteutettiin VDSL-yhteytenä. Toimipaikkojen välinen lyhyt etäisyys (alle 1km kaapelia) mahdollisti tekniikan käytön. Sillä saavutettiin yli 12Mbit/s yhteys. Yhteys rakennettiin yksi parista johdinta käyttäen. Yhteydessä hyödynnettiin seurakunnan omaa, olemassa olevaa puhelinkaapelointia.

PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA2:n sekä TOIMIPAIKKA5:n väliset yhteydet toteutettiin G.HDSL-tekniikalla. Yhteyksiä varten vuokrattiin operaattorilta suorat kuparipariyhteydet kyseisten toimipaikkojen ristikytkentätilojen välille. Myös näissä yhteyksissä käytettiin yksi parista johdinta. Etäisyyksien pysyessä kohtuullisina, saavutettiin kyseisillä yhteyksissä yli 2,5Mbit/s nopeus.

6.1.3 WLAN-silta

PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA3:n välille päädyimme rakentamaan sillatun WLAN-yhteyden. Kyseiseen toimipaikkaan vaadittiin hieman nopeampaa yhteyttä, eikä käytettävissä ollut tarkoituksenmukaista puhelinkaapelointia. WLAN-sillalla saavutimme 11Mbit/s symmetrisen yhteyden. WLAN-yhteyden mahdollisti toimipaikkojen välinen etäisyys ja rakennusten sijainti maastossa.

WLAN-tukiasemiksi valitsimme täysin ulkokäyttöön suunnitellut, ainoastaan siltayhteyksiin tarkoitetut laitteet. Laitteet olivat 802.11b-standardin mukaisia, 2,4GHz taajuusalueella toimivia WLAN-tukiasemia.

Yhteyden päädyimme toteuttamaan rakentamalla kaksi erillistä WLAN-siltayhteyttä ja tekemällä toimipaikkojen välille ns. toistinaseman. Tämä toistinasema sijoitettiin kolmanteen seurakunnan toimipisteeseen, PÄÄTOIMIPAIKKA:n ja TOIMIPAIKKA3:n välille. Toistinasemalla WLAN-tukiasemat liitettiin toisiinsa ristiin kytketyllä kaapelilla. Näin saatiin muodostettua suora tietoliikenneputki WLAN-yhteyksien ylitse. Toistinasemana käytetyssä toimipaikassa ei asennushetkellä tarvittu verkkoyhteyksiä, mutta tukiasemaparien väliin on tarvittaessa mahdollisuus kytkeä kytkin, josta kyseisen toimipaikan tar-

vitsemat verkkoyhteydet saadaan rakennettua. WLAN-tukiasemat asennettiin toimipaikkojen katoille rakennettuihin antennitukiin ja niistä kaapeloitiin suorat CAT5e-standardin mukaiset yhteydet ristikytkentätiloihin. Kaapeloinnissa käytettiin erikoisvalmisteista, -50 °C pakkasta kestävää kaapelia.

WLAN-tukiasemaparit määriteltiin käyttämään eri kanavia, jotta ne eivät häiritsisi toisiaan. Tukiasemat asennettiin käyttämään tiettyä WLAN-tunnusta ja niihin asetettiin MAC-osoitteiden tunnistus. Näin varmistettiin että tukiasemat keskustelevat vain keskenään. Tukiasemat määriteltiin kahdeksi pariksi niin, että kummassakin parissa oli päätukiasema (AP) ja asiakastukiasema (AC). Asiakastukiasemat määriteltiin hakemaan asetuksensa automaattisesti omalta päätukiasemaltaan, eikä asetuksia tarvinnut määritellä kuin kerran kumpaankin tukiasemapariin. tietoturvallisuuden takaamiseksi tukiasemien välinen tietoliikenne määriteltiin kahteen kertaan salatuksi. Ensin epäsymmetrisesti (avainpareilla) ja sitten symmetrisellä IPsec VPN-salauksella (3DES/AES).

6.1.4 VLAN-verkot

Asennettuihin kytkimiin määriteltiin seuraavat virtuaaliverkot: VLAN_0 hallinta, VLAN_1 LAN, VLAN_2 DMZ (palvelin) ja VLAN_3 taloautomaatio. Hallintaverkon määrittelimme erikseen, koska halusimme saada verkon aktiivilaitteiden (kytkimet, sillat) hallintaa varten oman IP-osoiteavaruuden. Palvelinta varten luotiin oma verkko ja taloautomaatio erotettiin omaksi verkokseen. Näitä verkkoja varten määriteltiin tietyt portit kustakin kytkimestä. Lisäksi kytkinten välillä, siltayhteyksien ylitse, kulkevaa tietoliikennettä varten määriteltiin kytkimiin tietyt portit. Nämä portit siirtävät kaikkien VLAN-verkkojen liikenteen VLAN-tunnuksin merkattuna. Muut kytkinten portit määriteltiin normaaliin lähiverkkoon VLAN_1.

6.1.5 Taloautomaatiojärjestelmä IP-verkkoon

Omana kokonaisuutenaan oli tietoverkon hyödyntäminen myös taloautomaatiojärjestelmän tarpeisiin. Kyseistä toteutusta varten seurakunnan lähiverkkoon määriteltiin erillinen VLAN-verkko. Järjestelmälle on varattu täysin erillinen IP-osoiteavaruus. Järjestelmään kuuluvat laitteet on kytketty kyseiseen VLAN-verkkoon määriteltyihin portteihin kytkimissä.

Taloautomaatiojärjestelmä on muusta tietoverkosta täysin erillään oleva järjestelmä. Siihen kuuluu ohjausjärjestelmä (logiikka) sekä valvomo-PC. Valvomo-PC on yhdistetty ohjausjärjestelmään sarjaliitännällä (RS-232) ja sillä ohjataan järjestelmän asetuksia sekä valvotaan hälytyksiä. Valvonta-PC:lle on oma etähallintajärjestelmä. Ohjausjärjestelmä hyödyntää RS-485-standardin mukaista sarjaliikennettä. Tällä sarjaväylällä ohjausjärjestelmä on yhdistetty kiinteistöjen eri taloautomaatiolaitteisiin (lämmitys, ilmastointi, lukitukset jne.). Näillä laitteilla on kullakin oma väyläosoitteensa ja niiden omat logiikat voivat sisältää erilaisia arvoja mittaavia antureita sekä ohjauksia.

Jokaiseen toimipaikkaan on rakennettu sarjakaapeliväylä, johon toimipaikan taloautomaatiolaitteet on kytketty. Aiemmin eri toimipaikkojen sarjakaapeliväylät oli yhdistetty ohjausjärjestelmään modeemiyhteyksillä. Ainoastaan

PÄÄTOIMIPAIKKA:n sarjakaapeliväylä oli ns. jatkuvassa valvonnassa ja siitä saatiin tilatiedot ja hälytykset välittömästi. Muiden toimipaikkojen osalta tilojen tarkistus tehtiin ajastetuilla yhteyksillä, tietyn rutiinin mukaisesti ja ohjaustoimenpiteet suoritettiin erikseen.

Toteutetussa ratkaisussa perinteiset modeemiyhteydet korvattiin mediamuuntimilla (”IP-modeemeilla”), jotka muuntavat RS-485 muotoisen sarjaliikenteen IP-liikenteeksi ja takaisin. Samalla modeemiyhteyksien vaatimat analogiset puhelinliittymät voitiin lopettaa. Järjestelmän vaatima sarjaliikenteen liikennöintinopeus on säädettävissä 1200-115000bit/s välillä. Käytimme liikennöintiin 9600bit/s nopeutta ja sen siirtäminen rakennetun WAN-verkon yli onnistui hyvin eikä verkossa havaittu merkittävää kuormitusta. Näin voitiin olemassa olevaa, aina aktiivista, tietoliikenneyhteyttä hyödyntää myös taloautomaation käytössä. Samalla saatiin etätoimipaikkojen taloautomaatiojärjestelmät ajantasaisen valvonnan piiriin.

6.2 Palvelimet

Päivitystä suunniteltaessa tavoitteena oli mahdollisimman helppo siirtymä vanhasta järjestelmästä uuteen. Tarkoitus oli luoda mahdollisimman selkeä, yksinkertainen ja helposti ylläpidettävä kokonaisuus. Suurin huomio ja tärkeimmät ratkaisut kohdistuivat luonnollisesti palvelimiin sekä toimialueen päivittämiseen.

Järjestelmään kohdistuvista päivityksistä haluttiin tehdä käyttäjille mahdollisimman huomaamattomia. Tuleva järjestelmä haluttiin rakentaa niin, että verkon ja palvelimen resurssien käyttäminen tai järjestelmänhallinta ei vaatisi käyttäjiltä tai ylläpitoon osallistuvilta henkilöiltä juurikaan lisäkoulutusta. Näin ollen, päätyminen Microsoft Windows:n käyttöön ja Active Directory -hakemistopalveluun perustuvaan toimialueeseen oli itsestään selvä.

Muina vaihtoehtoina palvelimien osalta tarkasteltiin mahdollisuutta Novell- tai Linux-järjestelmiin. Todettiin, että vastaavan tyyppisistä Novell-järjestelmistä oli yleisesti pikemminkin pyrkimys siirtyä muihin järjestelmiin. Linux palvelinten käyttöjärjestelmänä todettiin enemmänkin mahdolliseksi tulevaisuuden ratkaisuksi. Linuxilla voitaisiin kyllä hoitaa seurakunnan tarvitsemat tietojärjestelmäpalvelut, mutta järjestelmän käyttöönotto vaatisi huomattavaa panostusta käyttäjien ja ylläpitäjien koulutukseen. Tarkemman selvityksen jälkeen todettiin Linux-järjestelmiä käytettävän seurakunnissa lähinnä ”perinteisesti” www- ja sähköposti-palvelimina sekä erilaisten opetusluokkien Internet-työasemina. Vaihtoehtona Linux sivuutettiin tarvittavan ylläpitokoulutuksen, epävarman laitteistoyhteensopivuuden sekä liiallisen ulkopuolisen tuen tarpeen johdosta.

6.2.1 Windows 2000 Server

Palvelinten päivittämisessä otettiin lähtökohdaksi kartoittaa yksinkertaisin ja kustannustehokkain tapa saada järjestelmä ajanmukaiseksi. Pyrimme hyödyntämään jo olemassa olevat laitteistot tulevassa järjestelmässä mahdollisimman tehokkaasti. Aktiivihakemistopalvelun käyttöön siirryttiin, jo olemassa

olevaa Windows 2000-palvelinta hyödyntäen. Kyseistä palvelinta oli aiemmin käytetty ainoastaan sovelluspalvelimena ja se poistui tästä tehtävästä kun palvelimella sijainneet tietokannat siirtyivät seurakunnan oman verkon ulkopuolelle. Seurakunnalla oli siis jo olemassa tarvittava laitteisto sekä ohjelmistolisenssit vaadittua muutosta varten ja nämä haluttiin hyödyntää. Päätökseen vaikuttivat niin kustannustehokkuus kuin järjestelmään kohdistuvien muutosten organisointi ja aikataulutus.

6.2.2 Vaihtoehtona Windows Server 2003

Palvelimen käyttöjärjestelmän vaihtoehtona tarkasteltiin myös uudempaa ja kehittyneempää Microsoftin palvelinkäyttöjärjestelmää, Windows 2003 Server:iä. Tämä oli toteutettavan järjestelmän osalta ainoa todellinen vaihtoehto.

Windows Server 2003:n etuina Windows 2000 Server:iin verrattuna ovat: parannetut Active Directory -hakemistopalvelut, laajemmat käyttäjäasetusten ja verkon resurssien ylläpidon ja hallinnan työkalut, nykyaikaisemmat ja kehittyneemmät sovellus- ja web-palvelin ominaisuudet, tietoturvallisemmat verkkopalvelut, kehittyneemmät terminaali- ja etäkäyttöominaisuudet sekä käyttäjäryhmien yhteiset työtilat.

Näitä ominaisuuksia ei kuitenkaan nähty välttämättöminä tai erityisen tarpeellisin. Niillä ei koettu saavutettavan merkittävää hyötyä tai riittävää kustannustehokkuutta järjestelmän tai sen käyttäjien kannalta.

Tulevaisuutta ja järjestelmän kehitystä ajatellen, siirtyminen käyttämään Windows 2003 Server (tai tulevia Windows 2003 Server R2 tai Windows ”Vista” Server) -ympäristöä on erittäin yksinkertaista, nopeaa ja käyttäjille huomaamatonta. Tämän mahdollistaa Microsoftin Aktiivihakemistoon perustuva toimialuerakenne, jota myös Microsoftin uudemmat palvelinkäyttöjärjestelmät käyttävät.

6.3 Active Directoryyn siirtyminen

Aktiivihakemistoon päivittäminen, valmiita työkaluja käyttäen, tarjosi helposti toteutettavan vaihtoehdon siirtymiselle olemassa olevasta NT4-järjestelmästä huomattavasti kehittyneempään ja monipuolisempaan järjestelmään. Näin päästiin hyödyntämään aktiivihakemiston ominaisuuksia, sekä sen tuomaa dynamiikkaa, skaalautuvuutta ja helppoa päivitettävyyttä.

Aktiivihakemiston LDAP:n ja X.500:n tietomallin tuki antaa mahdollisuuden integroida järjestelmä tulevaisuudessa muihin tietojärjestelmiin, kuten Novell, UNIX tai Linux -pohjaisiin järjestelmiin. Vaikka päätyminen Active Directory -ratkaisuun olikin alusta asti hyvin selvää, koettiin tämä projektissa merkittävänä etuna. Integroinnin mahdollisuuden merkitystä lisää se, että laajempana strategisena tavoitteena valtakunnallisesti on pyrkimys kehittää yhteistyötä ja yhteisiä toimintamalleja eri seurakuntien sekä seurakuntien ja muun julkishallinnon, kuten kuntien, kesken. Tämän tavoitteen saavuttamisessa tietojärjestelmät ja niiden yhteensopivuus tulevat varmasti olemaan merkittävässä roolissa.

Aktiivihakemistoon siirtyminen toteutettiin täysin uuden Aktiivihakemiston asennuksena SERVER2-palvelimeen. Ennen asennusta SERVER2-palvelin poistettiin vanhalta NT4-toimialueelta, jonka jäsen se oli ollut. Lisäksi palvelimen nimi vaihdettiin, kuvaamaan paremmin sen tulevaa tehtävää. Palvelimelta poistettiin aiemmin käytössä ollut DNS-palvelu. Vanhan toimialueen toimintaan tämä ei vaikuttanut, koska siinä oli käytössä myös WINS-nimipalvelu.

6.3.1 Toimialueen asennus

Toimialueen asennus suoritettiin ajamalla Aktiivihakemiston asennusvelho (dcpromo.exe). Asennusvelhossa asennusvaihtoehdoksi valittiin täysin uuden toimialueen ja toimialuemetsän asennus ja SERVER2-palvelin määriteltiin olevan asennettavan toimialueen ensimmäinen palvelin. Toimialueen nimiavaruudeksi määriteltiin ”domain.local”. Toimialue määriteltiin asennusvaiheessa Windows Server 2000 mixed mode:en.

Koska Ylöjärven seurakunnan päivitetty järjestelmä päädyttiin toteuttamaan yhden palvelimen varaan, kaikki ohjauspalvelinroolit asennettiin luonnollisesti tähän palvelimeen. Tulevaisuudessa, kun kuormitus kasvaa ja halutaan lisätä vikasietoisuutta, on todennäköistä että järjestelmään joudutaan lisäämään uusia palvelimia. Tässä vaiheessa tulee myös ohjauspalvelinroolien jakaminen harkittavaksi uudelleen.

Aktiivihakemiston asennuksen jälkeen SERVER2-palvelimelle asennettiin myös DHCP-palvelin. DHCP-palvelimeen määriteltiin uuden toimialueen nimi, työasemien käyttöön tarkoitettu osuus IP-osoiteavaruudesta, reitittimen IP-osoite ja DNS-palvelimen osoite. ”SERVER1” -palvelimella ollut aiempi DHCP-palvelu ajettiin alas.

6.3.2 DNS-nimipalvelut

Aktiivihakemistossa päädyttiin eriytettyyn sisäiseen DNS-nimiavaruuteen oli helppo ja selkeä ratkaisu. Painavimpana syynä oli KIRKKO-verkon rakenne, sekä siihen kuuluvat verkko- ja nimipalvelut. Lisäksi käytössä olevat ulkoiset DNS - nimiavaruudet eriytyivät niin selkeästi omiin käyttötarkoituksiinsa (evl.fi, jonka kautta hoidetaan valtakunnallisesti seurakuntien sähköpostin ja Internet-/Intranet-nimipalvelut sekä ylojarvi.seurakunta.net, jonka kautta on hoidettu seurakunnan omat Internet-palvelut), että päätyminen erilliseen, täysin sisäiseen käyttöön tarkoitettuun, nimiavaruuteen oli luontevinta.

Ylöjärven seurakunnalle riittää nykytilanteessa täydellisesti yksi toimialue, joten suunnitteluvaiheessa päätettiin seurakunnan tietojärjestelmää varten ottaa käyttöön vain yksitasoinen toimialuerakenne, juuritoimialue. Uusi toimialue haluttiin nimiavaruutensakin puolesta erottaa vanhasta, käytössä olleesta NT4-toimialueesta ”TOIMIALUE”, joten Aktiivihakemiston toteutuksessa päätettiin käyttää ”domain.local”-nimiavaruutta.

Aktiivihakemiston asennuksen yhteydessä asennettiin uudelleen myös DNS-palvelin. DNS-palvelin asennettiin myös Aktiivihakemiston asennusvelhon avulla ja asennuksessa käytettiin oletusarvoja ja DNS-palvelin asennettin Aktiivihakemistoon integroiduksi. DNS-palvelimen hallinnoimaksi nimiavaruudeksi tuli toimialueen mukaisesti ”domain.local” (Forward Lookup Zone) ja IP-osoiteavaruudeksi seurakunnan käytössä oleva C-luokan (10.x.x.x/24) IP-verkko (Reverse Lookup Zone).

Koska asennettu DNS-palvelin hallinnoi ainoastaan seurakunnan sisäistä nimiavaruutta, määriteltiin siihen myös ulkoiset DNS-nimipalvelimet (forwarders). Näille nimipalvelimille ohjataan kaikki nimikyselyt joihin ei löydy vastausta järjestelmän omasta DNS-palvelimesta (kaikki seurakunnan lähiverkon ulkopuoliset osoitteet). Ulkopuolisina DNS-palvelimina käytettiin KIRKKO-verkon julkisia DNS-palvelimia (operaattori).

DNS-palvelimessa sallittiin osoitetietojen automaattinen päivittyminen (Dynamic Updates). Tällöin kukin työasema päivittää omat tietonsa DNS-palvelilla saadessaan IP-osoitteen DHCP-palvelimelta.

DNS-palvelimeen määriteltiin käsin myös joukko erillisiä DNS-nimiosoituksia, joilla viitataan joko järjestelmän sisäisiin tai ulkoisiin palveluihin. Nämä osoitukset toteutettiin sisäisiin palveluihin aliaksilla ja ulkoisiin A-tietueilla. Erikseen luotujen nimiosoitusten tarkoituksena on luoda järjestelmään dynaamisuutta ja helpottaa käytettyihin sovelluksiin tulevaisuudessa kohdistuvia muutoksia.

6.3.3 Luottosuhteet

Toimialueiden välisen hakemistotietojen sekä datan siirron onnistumiseksi uuden ja vanhan toimialueen välille muodostettiin molemmin suuntaiset luottosuhteet. Näin varmistettiin käyttöoikeuksien riittävyys tiedonsiirtojen yhteydessä. Luottosuhteet määriteltiin molempiin palvelimiin niin, että kumpikin luotti toisiinsa ja oli toisen luottama (trusted, trusting). Aktiivihakemistoon siirtymisen jälkeen, kun vanha palvelin ja toimialue oli poistettu verkosta, poistettiin nämä määritykset uudelta palvelimelta.

6.3.4 ADMT

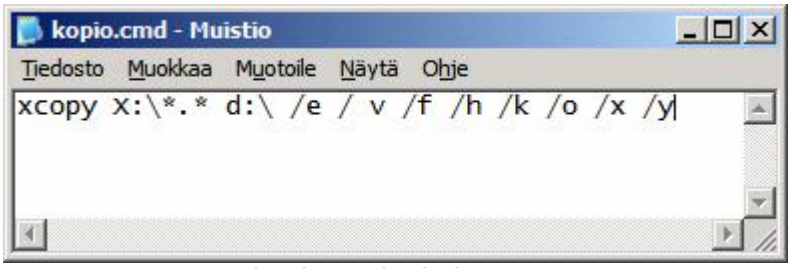
Aktiivihakemiston asennuksen ja luottosuhteiden luonnin jälkeen oli aika siirtää käyttäjätietokanta vanhalta toimialueelta uudelle. Toimenpiteessä käytimme Microsoftin ADMT2 (Active Directory Micration Tool)-apuohjelmaa. Ohjelma asennettiin SERVER2-palvelimella ja ajettiin siinä.

ADMT:ssä määritellään lähde- ja kohdetoimialueet sekä siirrettäväksi halutut tiedot toimialuehakemistosta. Toimialuetietojen siirron yhteydessä voidaan määritellä käyttäjät, ryhmät ja tietokonetilit siirrettäviksi vanhoine salasanoineen ja UID-tunnuksineen. (Microsoft Active Directory Migration Tool (ADMT) version 2.0 Release Notes 2005.)

Siirrettäväksi valittiin ainoastaan käyttäjät ja ryhmät. Tietokonetilejä emme halunneet siirtää, koska joutuisimme joka tapauksessa käymään työasemat lävitse ja tarkistamaan ne. Oli yksinkertaisempaa luoda jokaiselle työasemalle uusi tietokonetili, varmasti oikealla nimellä. ADMT:n ajo tapahtui melko nopeasti käsiteltävällä käyttäjämäärällä, eikä siirrossa ilmennyt virheitä.

6.3.5 Datan siirto

Varsinainen datan siirto suoritettiin komentojonon avulla. Siirsimme ”SERVER1”-palvelimen dataosiolla (D:\) sijainneet hakemistorakenteet ja tiedostot, kokonaisuudessaan, SERVER2 palvelimen vastaavalle osiolle. Kopiointia varten ”SERVER1”:n kyseinen osio yhdistettiin SERVER2:een X:\ - asemaksi. Kopiointi suoritettiin Windows:n XCOPY-komennolla. Apuna käytettiin tarvittavia, käyttöoikeudet ja tiedostomääritteet siirtäviä, attribuutteja. Komennosta tehtiin kuvassa 6.1 esitetty kopio.cmd-tiedosto SERVER2-palvelimen C:\ - aseman juureen. Tiedosto ajettiin SERVER2-palvelimelta, AT-komennolla ajastettuna (AT 16:30 /interactive ”c:\kopio.cmd”). Tämä siksi että kopiointi saatiin suoritettua SYSTEM-käyttäjänä. Näin varmistuttiin riittävistä käyttöoikeuksista käyttäjien henkilökohtaisiin tiedostoihin. Kopioinnissa siirrettiin useampi gigatavu tietoja, joten siirto ajoitettiin muutospäivien väliseksi illaksi/yöksi. Kopioinnin jälkeen luotiin SERVER2-palvelimelle tarvittavat verkkojaot käsin ja poistettiin vastaavat jaot ”SERVER1”-palvelimelta. Kopioinnin jälkeen tiedostojen käyttöoikeuksia testattiin ”pistokoemaisesti” ja verkkojakojen toimivuus varmistettiin.



Kuva 6.1 kopio.cmd - tiedosto

6.4 Toimialueen määritykset

Toimialueen asetusten määrittelyyn käytettiin normaaleja Windows Server 2000 Aktiivihakemiston hallintatyökaluja. Joidenkin asetusten helpottamiseksi palvelimelle asennettiin Windows Server 2000 Active Directory Schema:n laajennuspaketti Windows XP:tä varten (Internet) sekä Windows 2000 Support Tools - paketti (Windows 2000 Server-asennus CD).

6.4.1 Toimipaikat

Koska seurakunnan eri toimipaikkojen väliset WAN-yhteydet toteutettiin sillattuina ja kaikissa toimipaikoissa oli käytössä sama IP-osoiteavaruus, ei Aktiivihakemistoon määritelty kuin yksi toimipaikka (”domain.local”). Määrittely teh-

tiin ”Active Directory Sites and Services”-työkalulla, jossa oletustoimipaikka nimettiin uudelleen toimialueen mukaan.

Ratkaisua puolsi etätoimipaikkojen suhteellisen pienet (alle 10 työaseman) käyttäjämäärät sekä melko nopeat (2-15Mbps) WAN-yhteydet. Ei myöskään haluttu hankkia ja asentaa useita ohjauspalvelimia, eri toimipisteisiin. Ratkaisulla menetettiin eräitä työasemien hallintaa Aktiivihakemistossa helpottavia menetelmiä. Toisaalta tilannetta korvattiin luomalla organisaatioyksikkörakenne toimipaikkojen mukaiseksi. Mikäli toimipaikkojen välinen liikenne muutetaan tulevaisuudessa reititetyksi ja IP-osoiteavaruudet erotetaan toisistaan, on Aktiivihakemiston toimipaikkarakenne helppo muuttaa vastaamaan uutta tilannetta.

6.4.2 Organisaatioyksiköt

Organisaatioyksikkörakenne päädyttiin toteuttamaan käyttämällä yhdistelmää liiketoimintoihin (seurakunnan tapauksessa toimialat kuten hallinto, talous, nuorisotyö, lapsityö, diakonia jne.) perustuvista yksiköistä sekä maantieteellisistä (toimipaikat) yksiköistä. Tämä yhdistelmä kuvaa parhaiten seurakunnan organisaatiota ja toimintaa. Näin saavutetaan järjestelmän käytettävyyttä tukeva organisaatioyksikkörakenne. Tätä perusrakennetta päätettiin täydentää tarvittaessa järjestelmänhallinnallisilla organisaatioyksiköillä sekä tapauskohtaisesti projektikohtaisilla organisaatioyksiköillä.

Seurakunnan järjestelmän perustuessa yhteen yksitasoiseen toimialueeseen, haluttiin organisaatiorakennekin pitää mahdollisimman yksinkertaisena ja yksiselitteisenä. Halusimme myös mahdollisuuden hallita käyttäjien työympäristöä toimialan mukaan, riippumatta siitä mistä käyttäjät järjestelmään kirjautuvat.

Loimme Aktiivihakemiston hallintaan (Active Directory Users and Computers) yhden ”perus” organisaatioyksikön nimeltä ”domain”. Tämän alle loimme yksiköt ”laitteet” ja ”käyttäjät”. ”Laitteet”-yksikön alle loimme jokaiselle toimipaikalle oman yksikön, jonka alle kyseisen toimipaikan laitteet sijoitettiin. ”Käyttäjät”-yksikön alle loimme seurakunnan eri toimialoille omat yksikkönsä, joihin sijoitimme kyseisten toimialojen käyttäjätunnukset sekä toimialakohtaiset ryhmät.

Eri organisaatioyksiköiden hallintaa ei delegoitu käyttäjille. Hallintaa voi suorittaa ainoastaan pääkäyttäjätunnuksilla, joilla on pääsy koko Organisaatioyksikköhierarkiaan.

6.4.3 Käyttäjätunnukset ja -ryhmät

Käyttäjien hallintaa vanhassa NT4-toimialueessa oli tehty normaalina ylläpitotyönä siihen asti, kunnes Aktiivihakemistoon siirtyminen toteutettiin. Tästä syystä uudelle toimialueelle siirretyt käyttäjätilit, niihin liittyvät profiilit sekä käyttäjäryhmät olivat ajan tasalla. eikä niihin tarvinnut tehdä mitään muutoksia.

6.4.4 Ryhmäkäytännöt

Tietojärjestelmän perusasetuksia haluttiin hallita keskitetysti. Tähän käytettiin Aktiivihakemiston ryhmäkäytäntöjä. Ryhmäkäytännöt suunniteltiin toteutettaviksi hierarkkisesti niin, että yleiset käytännöt ovat voimassa toimialuetasolla kaikille ja yksityiskohtaisemmat määritellään organisaatioyksikkötasoilla. Määrittelimme ryhmäkäytännöt ohjaamaan järjestelmässä olevien laitteiden asetuksia sekä käyttäjien työympäristöjen määrityksiä.

Toimialueen oletuspolitiikkaan (Default Domain Policy) määriteltiin muutamia perusasetuksia: työasemille kirjautumisen asetukset, tietoturvapäivitysten asetukset ja salasanan vaatimukset. Muut määritykset tehtiin ”domain”-organisaatioyksikköön liitettyyn ”toimialueen asetukset”-ryhmäkäytäntöön. Tähän ryhmäkäytäntöön määriteltiin halutut, kaikkia toimialueen käyttäjiä ja työasemia koskevat asetukset: käyttäjien työpöytien asetukset, profiilien oletushakemistot, käytettävät verkon resurssit sekä Windows:n palomuuri-, virransäästö ja lukitusasetukset. Lisäksi teimme muutamia tiettyjä asetuksia ohjaavia ryhmäkäytäntöjä, jotka liitettiin toimipaikka- tai toimialakohtaisiin organisaatioyksiköihin. Näillä ohjattiin mm. liikkuvien profiilien latautumista etätoimipaikoissa ja offline-tiedostojen käyttöä.

6.5 Ohjelmistoasennukset

Tietojärjestelmän päivityksen yhteydessä oli ajankohtaista käydä lävitse myös seurakunnalla käytössä oleva sovellusohjelmistokanta. Tarkistimme eri ohjelmistojen versio- ja päivitystilanteen sekä käytettyjen ohjelmistojen yhdenmukaisuuden. Tarkistus suoritettiin niin palvelimessa kuin työasemissakin.

Heti Aktiivihakemiston asennuksen sekä toimialuetietojen ja datan siirron jälkeen suoritimme uusien ohjelmistoversioiden asennukset palvelimelle. Tämä oli kriittistä suorittaa välittömästi Aktiivihakemiston asennuksen jälkeen, jotta vanhat palvelut voitiin ajaa alas ja poistaa verkosta ja uudet palvelut olivat heti käytettävissä kun työasemat liitettiin toimialueelle.

6.5.1 Microsoft Exchange 2000 + ExMerge

Seurakunnan käytössä olleen Microsoft Exchange 5.5 -palvelimen päivittäminen ja käytön tehostaminen oli yksi päivitysprojektin haasteellisimmista osista. Selvää oli, että sähköpostipalvelimen käyttöä haluttiin jatkaa ja kehittää jo pelkästään sinne kertyneen historiatiedon johdosta. Kysymys kuului: miten oman sähköpostipalvelimen käyttöä voitaisiin tehostaa ja parantaa? Voisiko omaa sähköpostipalvelinta käyttää paremmin yhdessä seurakuntien valtakunnallisen sähköpostipalvelimen kanssa ja saada hyödynnettyä @evl.fi -päätteiset sähköpostiosoitteet omassakin järjestelmässä?

Aiemmin SERVER#1-palvelimella sijainneen Microsoft Exchange 5.5 -palvelimen tietojen säilyttäminen ja niiden luotettava siirtäminen uudelle palvelimelle oli itsestään selvää. Koska uusi SERVER#2-palvelin oli Windows 2000-käyttöjärjestelmällä varustettu, tuli myös päivitetyn MS Exchange-

palvelimenkin versioksi MS Exchange 2000. Muihin sähköpostipalvelimiin vaihtamista ei koettu mieleiseksi vaihtoehdoksi, eikä niitä näin ollen edes harkittu.

Echange-palvelimen päivittämiseksi NT4-palvelimelta Windows 2000-palvelimelle ja 5.5 -versiosta 2000 - versioon on olemassa eri vaihtoehtoja:

- Siirto (Move)
    - Olemassa olevaan toimialueeseen asennetaan uusi Windows/Exchange 2000-palvelin ja tilit siirretään siihen
- Keinu-päivitys (swing upgrade)
    - Olemassa olevaan toimialueeseen asennetaan uusi Windows/Exchange 2000-palvelin ja tilit siirretään siihen. Vanha palvelin tyhjennetään, asennetaan uudelleen Windows/Exchange 2000-palvelimeksi ja tilit siirretään takaisin
- Päälle asennus (in-place upgrade)
    - Olemassa oleva Echange 5.5-palvelin (sp3/sp4) päivitetään Exchange 2000-palvelimeksi
- ExMerge
    - Erillinen apuohjelma
    - Kopioi Exchange 5.5-palvelimen tilien sisältö .PST - tiedostoiksi ja lue ne uuteen Exchange 2000-palvelimeen
    - Voidaan käyttää siirrettäessä tilejä toimialueelta toiseen
- Siirtovelho (Migration Wizard)
    - Erillinen apuohjelma
    - Tarkoitettu tilien siirtoon eri toimialueiden välillä.
    - Tarkoitettu käytettäväksi ADMT-työkalun kanssa

(A comparison of the migration methods for migrating from Exchange Server 5.5 to Exchange Server 2003 or to Exchange 2000 Server.)

Palvelimelle asennettiin “puhdas” asennus Microsoft Exchange 2000-sähköpostipalvelimesta. Tämä loi palvelimelle tyhjän Exchange-tietokannan ja integroi Exchange-palvelun Aktiivihakemistoon. Näin Aktiivihakemiston hallintaan (Active Directory Users and Computers) saatiin tarvittavat Exchange-palvelun määritykset (objektikohtaiset välilehdet siirretyille käyttäjille ja ryhmille). Aktiivihakemistoon liitetty Exchange-palvelu käyttää nimiosoitukseensa oletuksena Aktiivihakemiston toimialuetta. Näin ollen osoitteet olivat oletuksena muotoa ”%tunnus%@domain.local”. Koska kaikkien käyttäjien käytössä oli valtakunnallinen etunimi.sukunimi@evl.fi -sähköpostiosoite, Exchange-palvelimen nimiavaruus muutettiin tähän muotoon. Muodon ollessa sama kuin jo käytössä olevassa valtakunnallisessa palvelussa, ei seurakunnan omaa sähköpostipalvelinta voi käyttää julkisena palvelimena vaan se palvelee ainoastaan seurakunnan sisäisessä verkossa. Tämän lisäksi integraatioon tarvittiin erillinen POP3 - yhdyskäytävä (Quantum Exchange Connector), jolla postit siirrettäisiin Exchange tietokantaan.

Seuraavaksi luotiin kullekin käyttäjälle oma, tyhjä, tili ja määriteltiin käyttäjäryhmistä jakelulistat. Tämän jälkeen käytettiin Microsoftin ExMerge-apuohjelmaa, luomaan vanhan Exchange 5.5-palvelimen tietokannassa olevista sähköpostilaatikoista *.PST-tiedostot. Nämä tiedostot sisälsivät käyttäjäkohtaisesti kaikki vanhan Exchange-palvelimen tilien sisältämät viestit, yhteystiedot, kalenterimerkinnät ja muut tietokantaan tallennetut tiedot. *.PST-tiedostot voitiin tämän jälkeen ”lukea” tilikohtaisesti suoraan uuteen Exchange-palvelimeen luotuihin tyhjiin tileihin. Näin saatiin vanha sähköpostihistoria siirtymään täydellisenä uudelle palvelimelle.

Edellä kuvattu menettely vaati kyseessä olleella käyttäjämäärällä muutaman tunnin manuaalisen työn. Vaihtoehtoisena Exchange-tietokannan siirtotapana olisi ollut vanhan Exchange-palvelimen päivitys. Tällöin tietojen siirto olisi tapahtunut automaattisesti. Siinä vanha NT4-palvelin olisi pitänyt päivittää osaksi aktiivihakemistoa. Tähän ei haluttu lähteä, koska vanhentunut palvelimen oli poistumassa järjestelmästä. Siihen kohdistuvien asennusten epäonnistumisen riski koettiin liian suureksi ja tässä vaiheessa projektia hyvin kriittiseksi.

6.5.2 Quantum Exchange Connector

Asennettua Microsoft Exchange 2000-palvelinta haluttiin hyödyntää myös seurakuntien valtakunnallisten @evl.fi -päätteisten tilien lukemiseen. Jotta uuteen Exchange-palvelimeen saataisiin keskitetysti ladattua sähköpostiviestit järjestelmän ulkopuoliselta sähköpostipostipalvelimelta, tarvittiin palvelimeen erillinen yhdyskäytäväohjelmisto (connector). Tämä on Exchange-palvelimen eräänlainen agentti, joka lataa viestit Exchange-tietokantaan tietystä ulkopuolisesta lähteestä. Valitsimme käytettäväksi POP3-protokollan sen yksinkertaisuuden ja selkeyden johdosta. Tällöin saamme ladattua viestit omaan tietokantaan, eikä tarvitse välittää esimerkiksi ulkopuolisista levytilarajoituksista.

Tekniikka on yleisimmin käytössä pääsääntöisesti pienissä organisaatioissa, jotka eivät halua tai voi ylläpitää omaa julkista sähköpostipalvelinta. Microsoft tarjoaa omaa Excange POP3 Connector -apuohjelmaansa ainoastaan pienyrityksille suunnatun Windows Small Business Server-tuoteperheen osana. Jouduimme hakemaan ratkaisun kolmannen osapuolen ohjelmistoista. Suoritetun vertailun pohjalta, valitsimme käyttöön Quantum Software Solutions:n Exchange Connector 3.3-ohjelmiston.

Exchange Connector 3.3-ohjelmisto asennettaan palvelimelle, jossa se integroituu Exchange-palvelimeen yhdyskäytäväksi. Ohjelmisto asentuu palveluksi (service), joka käynnistyy automaattisesti palvelimen käynnistyksen yhteydessä. Tämän jälkeen ohjelmistoon määritellään ulkopuoliset sähköpostitiliasetukset ja niitä vastaavat Exchange-tilit, jonne viestit välitetään (LIITE 6). (Exchange Connector.)

Ohjelmistoon määriteltiin lisäksi asetus, joka säilyttää uudet viestit ulkopuolisessa palvelimessa kaksi viikkoa. Näin mahdollistettiin uusien sähköpostien luku myös julkisen WEBMAIL-palvelun kautta, esimerkiksi kotoa

Ohjelmiston asennus sekä käyttöönotto olivat nopeita ja sen hallinta on varsin yksinkertaista. Toisaalta se tuo oman ylläpidollisen työnsä normaaleihin käyttäjien lisäyksiin ja poistoihin.

6.5.4 STATUS

Tietojärjestelmän päivityksen yhteydessä päätettiin Status-ohjelmiston osalta liittyä mukaan Tampereen seudun seurakuntien yhteisen sovelluspalvelimen käyttöön. Seurakunnan oman järjestelmän päivityksessä ei tarvinnut Status-ohjelmiston osalta suunnitella muuta, kuin Solid SQL-tietokantojen siirto ulko-

puoliselle sovelluspalvelimelle ja tarpeettomien tiedostojen poistaminen seurakunnan omalta palvelimelta. Statuksen käyttöä jatkettiin tämän ASP-palvelun (Application Service Provider – sovelluspalveluntarjoaja) kautta. Omalle palvelimelle ei tarvinnut siirtää tai asentaa mitään tietokannan tai ohjelmiston osia. Ainoastaan ohjelmiston käynnistykseen tarvittavat tiedostot tuli säilyttää seurakunnan omassa järjestelmässä.

Palvelimelle luotiin kansio, joka jaettiin toimialueelle nimellä \\SERVER2\STATUS$. Tämä yhdistetään tarvittavien käyttäjien käyttöön verkkoasemaksi S:\ kirjautumiskomentosarjan avulla. Käyttöoikeudet kyseiseen kansioon myönnettiin järjestelmänvalvojien lisäksi ainoastaan erilliselle Status-ryhmälle. Kansio sisältönä on ainoastaan ohjelmiston käynnistävä *.exe-tiedosto sekä kaksi määrittelytiedostoa: *.ini ja *.prm. Näistä *.ini-tiedostossa määritellään käytettävä tietokantapalvelimen IP-osoite ja tietokannan käyttämä TCP-portti sekä polku josta *.prm-tiedosto löytyy. *.prm-tiedostossa määritellään käytettävä protokolla (TCP) sekä ohjelmiston käyttämä väliaikaistiedostojen työkansio ja prosessin nimi. *.ini-tiedostossa käytettiin tietokantapalvelimen kohdalla DNS-nimeä ”PALVELIN”, joka ohjataan oikeaan IP-osoitteeseen SERVER2-palvelimen DNS-palvelussa. Mikäli tietokantapalvelimen osoite myöhemmin muuttuu, voidaan sen sijainnin kertova osoitus korjata helpolla DNS-muutoksella. Tämän lisäksi jaettiin työasemille ohjelmiston käynnistävät pikakuvakkeet haluttuihin paikkoihin (työpöytä, käynnistä - valikko) työasema-asennusten yhteydessä.

6.5.5 F-Secure

Suojautuminen vahingollisilta viruksilta on välttämätön paha nykyisissä verkoissa. Kannattaa valita ohjelmisto, joka päivittää virusten tunnistetiedot automaattisesti. Vaikka olisitkin piilossa organisaation palomuurien takana, kannattaa työasemille hankkia myös palomuuriohjelmisto, joka estää muiden paitsi määriteltyjen TCP/IP-porttien käytön. (Microsoft 2001: 160.)

Koska seurakunnalla oli jo F-Securen tuotteet käytössä ja lisensointisopimus olemassa, ei muita vaihtoehtoja virustorjuntaan edes harkittu. F-Securen ohjelmistojen käyttöä päätettiin tehostaa ja niiden eri ominaisuuksia hyödyntää laajemmin.

Työasemille F-Securen tuotteista valittiin virustorjunnan lisäksi palomuurin, sähköpostitarkistuksen ja haittaohjelmien torjunnan sisältävä F-Secure Client Security 6.01-ohjelmisto. Palvelimelle asennettiin F-Secure Anti-Virus 5.52 for Windows Servers. Lisäksi palvelimessa päätettiin ottaa käyttöön ns. ”gateway”-, eli ”yhdyskäytävä” -tuotteista F-Secure Anti-Virus for Exchange 6.40. Ohjelmisto tarkistaa MS Exchange-sähköpostipalvelimen läpi kulkevat viestit. Palvelimelle päätettiin asentaa F-Secure Policy Manager Server for Windows 6.01-hallintapalvelin sekä palvelimen hallintakonsoli. Hallintapalvelimella määritellään kaikkien järjestelmään asennettujen F-Secure-tuotteiden asetukset. Lisäksi hallintapalvelimella suoritetaan kaikkien järjestelmän F-Secure-tuotteiden asennukset ja päivitykset. Internetistä ladataan viruskuvaustiedostot ainoastaan palvelimelle. Palvelin hoitaa niiden keskitetyn jakelun verkkoon. Näin säästetään huomattavasti ylläpitotyötä ja tietoliikennekapasiteettia. Hallintapalvelimen ja työasemien välisessä tietoliikenteessä päädyttiin tehokkuus ja tietoturva syistä käyttämään http-protokollaa, perinteisen verkkojaon sijaan.

F-Secure Policy Manager Server asennettiin käyttämään http-protokollaa tietoliikenneyhteyksiin ja ohjelmistojen päivityksiin. Hallintaan ja raportointiin käytettävät TCP-portit muutettiin oletusarvoista eriäviksi. Ohjelmiston hallintaa varten hyväksyttiin hallinta-konsolin käyttäminen ainoastaan palvelimelta, jonne myös konsoli asennettiin (hallinta palvelimen etähallintayhteyden kautta). Asennuksen jälkeen palvelimeen tuotiin (import) tarvittavat F-Securen työasema- ja palvelinohjelmistojen *.jar-asennuspaketit. Asennuspaketit tarvitaan ohjelmistojen keskitettyä asennusta sekä asennettujen ohjelmistojen hallintaa varten.

Hallintapalvelimeen luotiin Aktiivihakemiston organisaatioyksikkörakennetta vastaava ”puumainen” rakenne. Rakenteessa pyrittiin yhteneväisyyteen Aktiivihakemiston kanssa. Siinäkin haluttiin erotella eri toimipaikoissa sijaitsevat laitteet. Tämän jälkeen määriteltiin ”peruspolitiikka”, jossa asetettiin kaikkia asennettavia F-Secure-ohjelmistoja koskevat asetukset: tietoliikenne, aikavälit, torjunta- ja tarkistusmenetelmät, hälytys- ja raportointiasetukset, automattiset päivitykset ja palomuurisäännöt. Palomuuriasetuksissa peruslähtökohta oli kaikkien TCP- ja UDP-porttien liikenteen kieltäminen ja ainoastaan todella tarvitun liikenteen salliminen. Palomuurit määriteltiin hyväksymään yleisesti käytetty tietoliikenne (http, https, icmp, pop3, smtp jne.) työasemista ulospäin sekä ylläpitäjien tarvitsema tietoliikenne sisäänpäin. Hallintapalvelimeen kohdistuvassa tietoliikenteessä, F-Securen ohjelmistot määriteltiin käyttämään DNS-palvelimeen määriteltyä nimiosoitusta (alias) ”FSECURE”, palvelimen IP-osoitteen sijaan. Näin mahdollistettiin palvelun dynaaminen siirtäminen toiselle palvelimelle myöhemmin tulevaisuudessa.

Lopuksi asennettiin torjuntaohjelmistot työasemille. Asennukset suoritettiin ryhmissä, toimipaikka kerrallaan. Asennukset tehtiin keskitetysti, hallintakonsolin ”push installation”-toiminnolla.

6.5.6 ARCserve

Päivitettyyn järjestelmään toteutettiin toiminnaltaan aiemman kaltainen, mutta nykyaikaisempi, tehokkaampi ja kapasiteetiltaan riittävä varmistusjärjestelmä. Järjestelmää päivitettäessä kaikki tieto keskitettiin SERVER#2-palvelimelle. Palvelimeen oli jo sen hankinnan yhteydessä asennettu AIT-nauhuri. Nauhuria päätettiin käyttää varmuuskopioinnissa, niin kauan kuin sen 70 GB:n tallennuskapasiteetti riittäisi seurakunnan tarpeisiin. Koska SERVER#1-palvelin poistui kokonaan järjestelmän päivityksen yhteydessä, vapautui siinä käytössä ollut ARCserve-ohjelmiston lisenssi. Lisenssi päivitettiin uusimpaan 11.5 versioon ja hyödynnettiin SERVER#2-palvelimessa. Varmistusohjelmiston valinnassa ei suoritettu lainkaan vertailua eri tuotteiden välillä. Päädyimme suoraan käyttämään luotettavaksi osoittautunutta ARCserveä, joka oli entuudestaan ylläpitäjille tuttu.

Käyttöön otettiin aiempaa huomattavasti laajempi nauhakierto. Kopioinnissa käytettävien nauhojen määrää lisättiin. Mahdollisia palautuspisteitä on käytettävissä edellisestä päivästä lähtien, päivittäin, aina kuukauden takaiseen tilanteeseen asti ja siitä kuukausittain taaksepäin. Lisäksi päädyttiin ottamaan erillisiä ”arkistovarmistuksia”, aina kun järjestelmään tai palvelinympäristöön kohdistuu joitakin muutoksia tai asennuksia. Varmuuskopioinnin tilasta, sekä varmistusten onnistumisesta tai tapahtuneista virheistä, määriteltiin järjestel-

mään erilliset lokitiedostot, sekä raportit. Raportit lähetetään automaattisesti, sähköpostilla, varmuuskopioinnista vastaaville pääkäyttäjille. Näin varmuuskopioinnin seuranta helpottui huomattavasti.

ARCserve:en asennettiin lisäksi kaksi erillistä agenttia (Agent for Microsoft Exchange ja Agent for Microsoft Exchange Premium addon) MS Exchange palvelinta varten. Näillä voidaan MS Exchange-tietokanta varmistaa niin, että itse tietokannasta ja siellä sijaitsevista yksittäisistä sähköpostilaatikoista saadaan erilliset varmuuskopiot, ajamatta itse Exchange-palvelua alas.

Solid SQL-tietokanta siirrettiin seurakunnan verkon ulkopuolelle, joten sen varmistamiseen ei enää tarvitse kiinnittää huomiota.

Varmuuskopiointirutiini määriteltiin kopioimaan kaikki palvelimella sijaitsevat tiedostot, Aktiivihakemiston tietokannan sekä Exchange-palvelimen tiedot ajastetusti varmistusnauhalle joka arki-ilta kello 23:00. Varmuuskopiointi asetettiin käyttämään mitä tahansa nauha-asemassa olevaa nauhaa, välittämättä sen sisällöstä. Operaatio alustaa nauhurissa olevan nauhan ennen kopiointia. Varmuuskopiointi ajetaan täydellisenä jokaisella kopiointikerralla (ainakin toistaiseksi, kun käsiteltävä data mahtuu kokonaisuudessaan yhdelle nauhalle ja kopiointi ehditään suorittamaan yöaikana). Tällöin jokaisesta nauhasta voidaan suorittaa täydellinen järjestelmän palautus (vrt. vain muuttuvien tietojen kopiointi).

6.6 Työasemat ja oheislaitteet

Työasemien kohdalla käyttöjärjestelmän valinta oli itsestään selvä Microsoft Windows. Vakiointi oli suoritettu jo aiemmin. Perusteina valinnalle oli olemassa oleva infrastruktuuri, käytettyjen ohjelmistojen perustuminen Windows-alustalle sekä käyttäjien osaamisen taso. Kuten aiemmin totesin, päivitysprojektin käynnistyessä päätettiin elinkaarikierron mukaista uusintaa nopeuttaa. Vielä käytössä olleet Windows 9x- ja NT4-työasemat korvattiin Windows XP-työasemilla. Käytössä olleet Windows 2000-työasemat päätettiin hyödyntää elinkaarensa loppuun.

Tulostinten osalta päätimme päivitysprojektin yhteydessä siirtyä mahdollisimman kokonaisvaltaisesti verkkotulostinten käyttöön. Perusteena oli lähinnä tulostuskustannusten aleneminen sekä saavutettava tulostinten keskitetty hallinta. Muutos tarkoitti useiden, erilaisiin tarkoituksiin soveltuvien, tulostinten hankintaa ja asennusta eripuolille järjestelmää. Henkilökohtaisista tulostimista päätimme luopua, muutamaa poikkeusta lukuun ottamatta, kokonaan.

Muiden, mahdollisesti tarvittavien, oheislaitteiden osalta päätimme suorittaa hankinnat ja asennukset käyttäjäkohtaisesti.

Työasemien asennuksessa toimittiin laaditun suunnitelman mukaisesti. Uusittaviksi valitut työasemat poistettiin käytöstä ja tilalle asennettiin uudet ja säilyvien työasemien päivitykset ja ohjelmistot tarkistettiin viimeisimmälle mahdolliselle tasolle. Nämä toimenpiteet suoritettiin Aktiivihakemistoon siirtymisen yhteydessä, liitettäessä työasema uudelle toimialueelle. Kaiken datan ja käyttäjäprofiilien sijaitessa verkossa, ei työasemien poistamisen tai toimialueen vaihdon yhteydessä tarvinnut huolestua tiedon häviämisestä. Työasemia voitiin käsitellä ikään kuin ”tyhminä päätteinä”.

Seurakunnan työasemavakiointi on rakennettu ns. merkkikoneiden ympärille. Käytössä ovat laitevalmistajan tarjoamat levykuvat (image) käyttöjärjestelmistä. Levykuvat sisältävät kaikki kyseisissä laitteissa tarvittavat ajurit ja apuohjelmat. Halusimme käyttää näitä olemassa olevia asennuksia, joten käsittelimme jokaista työasemaa erikseen. Emme käyttäneet mitään malliasennuksen levittämiseen tarkoitettua menetelmää.

6.6.1 Microsoft Office

Järjestelmän päivitystä suunniteltaessa tehtiin kartoitus käytössä olevista ja tarvittavista MS Office-lisensseistä. selvitimme myös keskitetyn lisensointisopimuksen aiheuttamat kustannukset ja sopimuksella saavutettavat edut. Lisensointisopimukseen siirtymisestä koituvien kustannusten johdosta, päädyttiin pitäytymään aiemmin käytössä olleessa OEM-lisenssien hankintamallissa. Käytössä olevat (ja jatkossa hankittavat) Office versiot päätettiin kuitenkin vakioida ainoastaan kahteen eri versioon: MS Office XP SBE SP3 ja MS Office 2003 SBE SP2. Näin haluttiin minimoida käytössä olevien ohjelmisto- sekä päivitysversioiden mahdolliset yhteensopimattomuudet ja taata kaikille käyttäjille mahdollisimman kattava tuki.

Järjestelmän päivityksen yhteydessä määriteltiin seurakunnan verkkoon MS Office-ohjelmistojen yhteiset työryhmäkansiot. Lisäksi Office-ohjelmistojen korjauspäivitykset päädyttiin sijoittamaan verkkoon. Työasemien päivityksen yhteydessä tarkistimme MS Officea koskevien asetusten ja päivitysten tilan ja suoritimme tarvitut, korjaavat, toimenpiteet.

6.6.2 Työasemien siirtäminen uuteen toimialueeseen

Uuden toimialueen ollessa käytettävissä, voitiin työasemat liittää siihen. Asennus suoritettiin kunkin työaseman luota paikallisesti. Työasemille kirjauduttiin paikallisella pääkäyttäjätunnuksella. Komentoriviltä tarkistettiin ”ipconfig /all”-komennolla DHCP-asiakkuuden olevan käytössä. Verkkoyhteyksien toimivuus testattiin ”ping www.evl.fi”-komennolla. Tämän jälkeen muutettiin/asetettiin työaseman käyttämän toimialueen nimeksi ”domain.local” ja tarkistettiin, että työaseman nimi on sovitun nimeämiskäytännön mukainen. Hyväksymällä nämä asetukset ja suorittamalla vaaditun uudelleenkäynnistyksen, liittyi työasema uuteen toimialueeseen. Toimenpiteessä kului aikaa noin 5-20 minuuttia työasemaa kohden. Asennuksen jälkeen työasema jätettiin päälle ja se oli valmis käyttäjän käytettäväksi tai ylläpitäjien etähallittavaksi.

Pääsääntöisesti kaikki käyttäjät omaavat Aktiivihakemistossa ”peruskäyttäjän” oikeudet ja saavat verkon käyttöoikeudet niiden käyttäjäryhmien mukaan, joihin kuuluvat. Tämä mahdollistaa kenen tahansa käyttäjän kirjautumisen mille tahansa toimialueen työasemalla ja pääsyn verkkoon omilla oikeuksillaan. Osalle käyttäjistä piti kuitenkin erikseen määritellä oman työasemansa paikalliset tehokäyttäjän tai järjestelmänvalvojan oikeudet. Tämä oli tarpeen tiettyjen ohjelmistojen käyttö- ja/tai päivitystarpeiden johdosta. Näin toimittaessa otettiin tietoinen tietoturvariski, käytettävyyden parantamiseksi.

6.6.3 Ohjelmistoasennusten automatisointi

Ohjelmistoasennusten automatisointiin emme käyttäneet mitään erillistä ohjelmistopakettien jakelumenetelmää. Tämä siksi, että Office-ohjelmistopaketit oli erikseen asennettu jokaiseen työasemaan ja muut ohjelmistot olivat asennuksiltaan erittäin yksinkertaisia.

Asennukset suoritettiin komentosarjan avulla. Komentosarja oli liitetty tietyn ylläpitotunnuksen kirjautumiskomentosarjaksi. Työaseman toimialueelle liittämisen jälkeen, kirjauduttiin työasemalle em. tunnuksella. Tällöin komentosarja kopioi tarvittavat hakemistot, tiedostot, rekisterimerkinnät ja pikakuvakkeet sekä käynnisti asennuspaketit. Lopuksi komentosarja käynnisti työaseman uudelleen, minkä jälkeen asentaja tarkasti välittömästi asennusten onnistumisen.

6.6.4 Automaattiset päivitykset

Microsoftilla on julkinen Microsoft Update-Internetpalvelu, jonka kautta voi automaattisesti päivittää Windows ja Office-tuotteiden tietoturvapäivitykset tietokoneelleen. Päivitykset ladataan Windows:n ”Automaattiset päivitykset”-toiminnolla. Päivitykset haluttiin saada, välittömästi niiden julkaisun jälkeen, levitettyä kaikkiin työasemiin. Ryhmäkäytäntöjen avulla automaattiset päivitykset asetettiin pakotetusti päälle kaikkiin työasemiin.

Järjestelmään ei haluttu asentaa mitään keskitettyä päivitysten jakeluohjelmistoa (Microsoftin SUS-palvelua tai muuta kolmannen osapuolen ohjelmistoa). Tähän päädyttiin työasemien suhteellisen pienen lukumäärän ja päivityspalvelun vaatiman ylläpidon johdosta. Haittana jokaisen työaseman erikseen tapahtuvassa päivittymisessä on päivitysten hallitsemattomuus sekä tietoliikennekaistojen kuormittuminen. Jokainen työasema lataa samat päivitykset erikseen, eikä asennettaviin päivityksiin voida vaikuttaa. Seurakunnan tietojärjestelmän kohdalla näitä asioita ei koettu kovinkaan suuriksi ongelmiksi.

Tietojärjestelmän päivitysprojektimme aikana Microsoft julkaisi uuden version keskitetystä päivitysten jakelupalvelusta, WSUS:n (korvaa SUS:n). Harkitsimme tätä vaihtoehtona päivitysten jakelusta työasemille, mutta päädyimme odottamaan mahdollista seurakuntien yhteistä toteutusta palvelusta.

6.6.5 Microsoft Baseline Security Analyzer 2

Työasemien asennuksen jälkeen niiden tietoturvan tilasta (asetusten oikeellisuutta) ja päivitysten onnistumisesta haluttiin saada tietoa. Tässä päädyttiin käyttämään Microsoftin vasta projektimme aikana julkaisemaa Baseline Security Analyzer 2-ohjelmistoa. Ohjelmistolla voidaan tarkistaa työaseman (2000/XP) tietoturvan taso verkon ylitse. Tarkistusten perusteella saadaan työasemien tilasta kuvassa 6.2 esitetyn kaltaiset raportit

Computer name: [redacted]
IP address: [redacted]
Security report name: testiraportti
Scan date: [redacted]
Scanned with MBSA version: 2.0.5029.2
Catalog synchronization date: [redacted]
Security update catalog: Microsoft Update
Security assessment: [redacted]

Security Update Scan Results

Score	Issue	Result
✓	Office Security Updates	No security updates are missing. What was scanned Result details
✓	Windows Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✱	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
ⓘ	Windows Firewall	Windows Firewall is disabled and has exceptions configured. Windows Firewall is disabled or has exceptions on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (1 of 8) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
✓	Password Expiration	All user accounts that were scanned do not have non-expiring passwords. What was scanned Result details

Kuva 6.2 Osa MS BSA 2-ohjelmiston testiraportista

Ohjelmisto asennettiin palvelimelle sekä yhdelle ylläpidon työasemalle, koska näistä oli tietoliikenne sallittu kaikkiin verkon työasemiin. Verkon työasemat tarkistettiin toimipaikkakohtaisissa ryhmissä. Saaduista raporteista selvisi lähinnä se, että kyseisten työasemien tietoliikenne toimii, tietoturvapäivitykset ovat onnistuneesti asentuneet ja perustietoturva-asetukset (kuten paikallisten tunnusten salasanat ja eri ohjelmistojen käynnistämät palvelut) ovat kunnossa.

6.7 Etähallinta

Järjestelmän toiminnan ja ylläpidon kannalta oleellista on pääkäyttäjien nopea pääsy käsiksi ongelmatilanteisiin. Tämän johdosta koko järjestelmän kattava etähallinta oli yksi päätavoitteistamme. Ylläpitäjien keskitetyn etähallinnan alle asennettiin kaikki järjestelmään kytketyt laitteet: kytkimet, sillat, tulostimet, työasemat ja palvelin. Etähallinnassa on käytössä useita menetelmiä ja ohjelmistoja. Muiden kuin tietokoneiden osalta yhteydet otetaan joko selaimella tai terminaalilla tai käytetään SNMP-hallintaa. Tietoturvamielessä halusimme rajata etähallinnan mahdolliseksi ainoastaan tiettyjen ylläpitäjien toimesta. Hallintaa suoritetaan tietyiltä laitteilta, joko seurakunnan omista tiloista tai seurakunnan ulkopuoliselta kumppanilta käsin. Tämä toteutettiin käyttäjätunnistuksilla, sallittujen IP- ja MAC-osoitteiden luetteloilla sekä palomuurisäännöillä.

6.7.1 Palvelimen etähallinta

Palvelimen etähallinnassa päädyttiin käyttämään Microsoft Windows:n omaa etätyöpöytäominaisuutta. Vaihtoehtoisesti käytetään myös DameWare-etähallintaohjelmistoa, jonka client-ohjelmisto palvelimelle asennettiin.

Etäkirjautuminen palvelimelle määriteltiin sallituksi ainoastaan tietyille ylläpito-tunnuksille, joilla etähallintaa suoritetaan.

6.7.2 Työasemien etähallinta

Työasemien etähallinta päätettiin toteuttaa kuten palvelimenkin. Etätyöpöy-täyhteydet sallittiin työasemilta (Windows XP), toimialueen oletuspolitiikkaan määritellyn ryhmäkäytännön avulla. Lisäksi asennettiin tarvittaessa (Windows 2000) DameWare client -etäkäyttöohjelmisto.

Palvelimesta poiketen, työasemien etäkäyttöön vaikuttaa työasemiin asennet-tu F-Securen palomuuriohjelmisto. Palomuuri estää oletusarvoisesti kaikki ul-kopuoliset yhteydet. Etäkäyttöä varten määriteltiin F-Secure Policy Mana-ger:iin ylläpitäjien työasemien liikenteen sallivat palomuurisäännöt koskemaan kaikkia järjestelmän työasemia.

6.8 Etäyhteydet / etätyö

Aiemmin käytössä olleet suorat etäkäyttöyhteydet seurakunnan tietojärjestel-mään poistettiin kokonaan käytöstä. Käyttöön otettiin julkisessa Internetistä olevat palvelut ajanhallinnan sekä sähköpostin osalta. Näillä toimenpiteillä py-rittiin toteuttamaan Kirkkohallinnon antamaa tietoturvaohjeistusta.

7 Järjestelmän dokumentointi

Kaikessa tietokoneisiin liittyvässä vianetsinnässä voidaan toimia kahdella tapaa. Yksi lähestymistapa on reaktiivinen: tukihenkilöstö odottaa, kunnes heille raportoidaan varsinaisista ongelmista, ennen kuin niiden ratkaisemiseksi tehdään jotain. Koska verkot tehdään, ne eivät synny itsestään, ja koska ne kasvavat ajan mittaan kokien useita muutoksia, joita useat henkilöt ovat tehneet, tämä lähestymistapa on tuomittu epäonnistumaan.

Huomattavasti parempi toimintatapa vianselvityksessä on proaktiivinen lähestymistapa. Tämä tarkoittaa sitä, että verkon fyysisistä ja loogisista ominaisuuksista kerätään tietoja ja ne toimitetaan tukihenkilöstölle ja käyttäjille ennen varsinaisten ongelmien ilmaantumista. Proaktiivinen lähestymistapa ei oleta verkon pysyvän aina kunnossa. Sen sijaan ymmärretään, että ongelmien ajoittainen esiintyminen on tiettyyn rajaan asti normaalia.

Kaikenkokoisten verkkojen ongelmien ennakoiminen ja välttäminen, sekä ratkaisujen helppo toteuttaminen riippuvat siitä, onko saatavilla tarkoin kuvaavia dokumentteja, jotka edustavat käytettäviä työkaluja ja tekniikoita. Näistä dokumenteista esimerkkeinä verkon topologiaa kuvaavat kartat, FAQ-dokumentit, jotka auttavat liikkumaan verkossa ja käyttämään sen resursseja, järjestelmälliset ongelmanratkaisuproseduurit ja projektien dokumentaatiot. (Ogletree 2001: 8.)

7.1 Tavoitteena toiminnan turvaaminen ja järjestelmän kehitys

Yleensä dokumentoinnin merkitys paljastuu vasta siinä vaiheessa, kun verkon toiminnassa alkaa esiintyä ongelmia tai esimerkiksi avainhenkilö ei enää olekaan käytettävissä.

Jatkuvuuden turvaaminen on yrityksissä yksi tärkeimpiä dokumentoinnin perusteita. Yrityksen on varauduttava siihen, ettei sen avainhenkilöillä oleva tietotaito katoa missään olosuhteissa. Tietojärjestelmien ja tietoverkon käyttöön liittyvä dokumentointi on hyvä tehdä siten, että esimerkiksi vastuuhenkilöiden vaihtumisen yhteydessä uudet asiantuntijat voivat perehtyä järjestelmiin riittävän helposti ja nopeasti.

Kehittämistyö perustuu aina reaaliaikaiseen tietoon systeemin nykytilasta. Ilman nykytilan tuntemista suunnittelutyö muodostuu hankalaksi. Verkkoa laajennettaessa hyvä dokumentaatio auttaa oikeiden ratkaisujen löytämisessä sekä antaa paremmat mahdollisuudet suunnitella tulevia tietoteknisiä ratkaisuja. Dokumentointi on myös perusedellytys verkon tehokkaalle hallinnalle ja ylläpidolle. Yrityksessä, jonka lähiverkkoa ei ole dokumentoitu, uusien verkon hallinnointijärjestelmien käyttöönotto saattaa osoittautua vaikeaksi tai jopa hyödyttömäksi, mikäli saatua tietoa ei kyetä kohdentamaan oikeaan osoitteeseen. (Sepänmaa 2004: 18.)

7.2 Dokumentointityökalut

Kyseisen järjestelmän dokumentointityössä käytettiin hyväksi useita eri työkaluja. Näillä työkaluilla tätä informaatiota myös päivitettiin aina sen muuttuessa. Tuotettuihin dokumentteihin sisällytettiin tietoa tarvittaessa kuvaruutukaappauksina.

Oleellisimmat käytetyt työkalut olivat:
- MS Office
    - o MS Word (sanalliset kuvaukset, asennus- ja käyttöohjeet, luettelot, laitteiden konfiguraatiotiedot…)
    - o MS Excel (taulukot, listat, graafiset kuvaukset…)
    - o MS PowerPoint (ohjeet, graafiset esitykset, kaaviot…)
- MS Visio (graafiset esitykset, vuokaaviot, kaaviokuvat, sijoittelukuvat…)
- F-Secure Policy Manager Server (Virustorjunnan ”tilannekuva” ja asennustiedot)
- HP Systems Insight Manager (laiteinformaatio, tilaseuranta/SNMP -valvonta)
- AD:n hallintatyökalut (Active Directoryn rakenne ja määritykset)
- PDF-XChange Pro 3.0

7.3 Dokumentaation luonti ja hallinta

Dokumentaatio luotiin ensimmäisenä työvaiheena koko projektissa. Tuolloin siihen koottiin mukaan kaikki jo olemassa oleva tieto järjestelmästä. Tietojen paikkansa pitävyys tarkistettiin. Luodut dokumentit tallennettiin dokumenttien hallintaan käyttämäämme järjestelmään. Järjestelmä tallentaa dokumentit tietokantaan ja huomio versioinnin automaattisesti. Projektin edetessä jokainen työvaihe ja muutos päivitettiin dokumentaatioon. Jokaisen dokumenttiin tehdyn muutoksen jälkeen tallennettiin siitä uusi versio suojatussa PDF-muodossa. Samalla dokumenttihistoria suojattiin, eikä muutoksia voinut tehdä kuin viimeisimpään versioon (työversio). Näin pystyttiin hallitsemaan ja seuraamaan projektin etenemistä ja järjestelmässä tapahtuneita muutoksia. Tarvittaessa voitiin tarkistaa myös vanhaa, jo muuttunutta, tietoa. Kukin henkilö tallensi dokumentit tietokantaan omalla tunnistetiedollaan. Näin saatiin kerättyä tieto myös dokumentaation muutoksista ja kunkin muutoksen tekijästä.

Dokumentaatiotyössä on sovellettavilta osin käytetty hyväksi Annamarin Sepänmaan vuonna 2004 Tampereen Ammattikorkeakoululle tutkintotyönään tekemää mallia Tampereen seurakuntayhtymän tietoverkon dokumentoinnista ja pyritty kehittämään siinä käytettyjä menetelmiä eteenpäin.

Dokumentaatio koostuu seuraavista erillisistä dokumenteista:
- Sanallinen kuvaus järjestelmästä (”yleiskuvaus”)
- Verkkokaavio jokaisesta lähiverkosta
- Verkkokaavio laajaverkosta ja ulkopuolisista yhteyksistä
- Sijoittelukuva jokaisesta lähiverkosta/toimipaikasta
- Kaaviokuva jokaisesta virtuaaliverkosta yhteyksineen
- Sijoittelukuva jokaisesta ristikytkennästä/laitekaapista
- ristikytkentäluettelo jokaisesta ristikytkennästä/laitekaapista
- Kaaviokuva jokaisesta kytkimestä; kytkennät

- Laiteluettelo; yksityiskohtaiset laitetiedot
- Käyttäjäluettelo; yksityiskohtaiset käyttäjätiedot
- Ryhmäluettelo; yksityiskohtaiset ryhmätiedot (laiteet, käyttäjät, GPO:t)
- Ohjelmistoluettelo; käytettyjen ohjelmistojen tiedot ja asetukset, käytettävät versiot, asennus- ja päivitysohjeet.
- Verkkoasetukset: IP-verkot, niiden asetukset ja käyttö
- Laitteiden asennuskuvaukset; ”perusasennuskuvaus” kullekin järjestelmän laitteelle (image, asetukset, nimeäminen, ohjelmistot, päivitykset…)
- Yhteystiedot; eri osa-alueiden tarpeelliset yhteystiedot ja lisäinformaatio

Lisäksi dokumenttien hallintajärjestelmään on tallennettu erikseen eri laitevalmistajien ja ohjelmistotoimittajien ohjekirjoja ja manuaaleja, runkoverkkojen mittauspöytäkirjat ja toimipaikkojen sähkösuunnitelmat sekä muita vastaavia asiakirjoja.

7.3 Dokumenttien tietoturva ja turvaluokitukset

Organisaation toiminnan kannalta tärkeiden tietojen tallettaminen ja niiden turvallisesta säilyttämisestä huolehtiminen ovat osa tietoturvapolitiikkaa. Oikealla tavalla toteutettu dokumentointi luo yritykselle turvallisuutta sellaisten onnettomuuksien varalle kuten ilkivalta, tulipalo ja vesivahingot. Pahimmassa tapauksessa vahinko saattaa olla korvaamaton.

Dokumentoitavat asiat riippuvat yksilöllisesti yrityksien tai yhteisöjen tarpeista. Yleisenä sääntönä voidaan pitää, että mikäli tiedon menettäminen aiheuttaa taloudellisia menetyksiä, tulisi se tieto dokumentoida. Jokaisen yrityksen tai yhteisön tulisi laatia oma **tietoturvasuunnitelma**. Oikein määritelty ja suoritettu dokumentointi on merkittävä osa tietoturvapolitiikkaa. (Sepänmaa 2004: 18-19)

Dokumentointi tulisi yrityksissä määritellä eri turvaluokkiin, jotta kyetään luomaan käsittelysäännöstö erilaiselle tiedolle. Määrittelyperusteena käytetään dokumenttien aiheuttamaa uhkaa tietoturvalle. Neljä turvaluokkaa ovat:
- Julkiset tiedot (public)
- Sisäiset tiedot (internal)
- Luottamukselliset tiedot (confidential)
- Salaiset tiedot (secret)

(Sepänmaa 2004: 18-19)

Luokituksessa tulee määritellä dokumentin käsittely, säilytys, viestittäminen ja hävittäminen. Turvaluokituksen piiriin tulee ottaa myös yrityksen ulkopuolelta tulevat dokumentit. (Sepänmaa 2004: 18-19)

Ylöjärven seurakunnan tietojärjestelmää koskevat dokumentit on tallennettu dokumenttien hallintaan käytettävään järjestelmään. Järjestelmään on pääsy vain nimetyillä, järjestelmän ylläpitotehtäviä suorittavilla, henkilöillä. Järjestelmässä käytetään ns. vahvaa tunnistusta (vrt. verkkopankit).

Seurakunnan tietojärjestelmää koskeva dokumentaatio on luokiteltu kokonaan joko sisäisiksi tai luottamuksellisiksi dokumenteiksi (vaikka ne osittain sisältävät myös täysin julkista tietoa). Salaisiksi luokitellut dokumentit ovat seurakunnan vastuuhenkilöiden hallinnassa, erillään tietojärjestelmän ylläpidollisesta materiaalista.

8 Työn arviointi

Ylöjärven seurakunnan IT-järjestelmän kehittäminen oli kokonaisuudessaan erittäin mielenkiintoinen ja haastava projekti. Tämän tyyppinen järjestelmän kehittäminen ja päivittäminen on alati jatkuva prosessi, eikä se ole koskaan täysin valmis. Tästäkin syystä oli haasteellista määritellä ja rajata tietyn laajuinen kokonaisuus erilliseksi projektiksi ja tutkintotyöksi. Pääsin soveltamaan toteutuksessa useita oman mielenkiintoni ja ammattitaitoni osa-alueita sekä selvittämään ja ratkaisemaan useita esiin nousseita ongelmakohtia ja tarpeita. Koin tutkintotyön tekemisen mieleiseksi ja opettavaksi. Siitä oli minulle hyötyä sekä opinnoissani, että ammatillisesti.

Työtä tehdessä saimme muodostettua useita erilaisia yhteistyö- ja projektityöskentelymenetelmiä, jotka osoittautuivat erittäin onnistuneiksi ja tehokkaiksi. Jälkeenpäin on korostettava sitä, kuinka moniulotteinen ja haastava tämän kaltainen (koko järjestelmää koskeva) pitkäjänteinen päivitysprojekti on. Todellista työmäärää ja erilaisia työvaiheita on erittäin vaikea arvioida etukäteen.

8.1 Työn tulokset

Työn tuloksena oli Ylöjärven seurakunnan nykyinen IT-järjestelmä, joka on moderni, dynaaminen ja helposti hallittava. Järjestelmä kattaa kaikki organisaation tämän hetkiset tarpeet ja siinä on huomioitu myös tulevaisuuden kehitysvaatimukset sekä jatkuva kasvu kaikilla toiminnan aloilla (LIITE5). Käytössä on aiempaan verrattuna lähes kaksinkertainen määrä laitteita sekä uusia ohjelmistoja ja palveluja.

Kartoitimme järjestelmän ongelmakohdat, viat sekä puutteellisuudet ja saimme ne korjatuiksi tai vähintäänkin hallittaviksi. Keräsimme tietoomme järjestelmän riskit ja haavoittuvuudet niin tietoturvan, kuin käytettävyyden osalta. Saimme luotua turvallisen ja tehokkaan IT-ympäristön. Järjestelmän käytön ja toiminnan kannalta tärkeät riskitekijät on tiedostettu ja toimintatavat, niin normaalioloissa, kuin ongelmatilanteissa, ovat selvillä. IT-järjestelmä on kokonaisuudessaan dokumentoitu. Kaikilla dokumentaatiota käyttävillä ja/tai päivittävillä henkilöillä on (tarpeellisilta osin) pääsy dokumentteihin ja heidän tiedossaan on dokumentoinnissa käytetyt menetelmät ja esitystavat.

Tutkintotyöni raportti on myös tärkeä osa projektin tuloksia. Se kertoo seurakuntaympäristössä käytössä olevan tietojärjestelmän päivittämiseen liittyvät erilaiset menetelmät, tekniikat ja työvaiheet. Raporttia voidaan hyödyntää dokumenttina tehdystä työstä, sekä ”ohjeistuksena” ja ”mallina” tehtäessä vastaavia toimenpiteitä jatkossa. Uskon raportistani olevan hyötyä niin toimeksiantajalle kuin työnantajalleni, mahdollisesti muillekin vastaavien järjestelmien parissa työskenteleville.

8.2 Tavoitteiden saavuttaminen

Saavutimme kaikki IT-järjestelmän päivitysprojektille asetetut tavoitteet vähintäänkin toivotulla tasolla. Käytettävyys ja erilaiset tarpeet järjestelmän toiminnan suhteen on huomioitu. IT-järjestelmää ja tietoverkkoa voidaan hyödyntää monipuolisesti erilaisiin käyttötarkoituksiin. Näin saavutetaan mahdollisimman suuri hyötyarvo olemassa olevalle infrastruktuurille ja kustannustehokkuutta tehdyille investoinneille.

Lisäksi vuoden 2005 aikana saatiin Ylöjärven seurakunnassa toteutettua lähes kaikki YSICT-KEHTO -projektille asetetut tavoitteet ja nekin joita ei vielä ole saavutettu, ovat hyvässä vauhdissa valmistumassa.

Tutkintotyöni suhteen saavutin asettamani tavoitteet työn sisällöstä, laajuudesta ja tasosta. Haasteita raportin laatimiseen aiheutti projektin laajuus ja sen pitkä ajallinen kesto. Vaikeuksia taasen muun työ- ja siviilielämän aiheuttama ajan puute.

8.3 Jatkokehitys

Mikään tietojärjestelmä ei ole koskaan täysin valmis. Tekemämme työn pohjalta Ylöjärven seurakunnan IT-järjestelmän kehitystyö ja siihen kohdistuvat muutokset ja parannukset ovat nyt entistä paremmin hallittavissa. Tulevina haasteina tietojärjestelmän osalta ovat varmaankin alati jatkuvien laitteisto- ja ohjelmistopäivitysten lisäksi erilaiset järjestelmäintegraatiot ulkoisten tahojen kanssa sekä uudet ja kehittyvät teknologiat, kuten mobiilitekniikat, PushMail ja VOIP.

Ylöjärven seurakunnan IT-järjestelmän parissa on varmasti runsaasti ylläpito- ja kehitystyötä tulevaisuudessakin. Järjestelmän laajuudesta ja monipuolisuudesta johtuen esiin nousee taatusti erilasia osakokonaisuuksia, joita voidaan kehittää ja ottaa käyttöön omina projekteinaan. Kehitysprojektimme aikana muodostuneet toimintamallit ja työtavat, sekä toteuttamamme tekniset ratkaisut tulevat osaltaan helpottamaan näitä tulevia töitä.

8.4 Loppusanat ja kiitokset

Kiitokset perheelle ainaisesta jaksamisesta. Ilman en olisi tähän pystynyt.
Kiitokset Eskolle. Ilman esimerkkiäsi en alalla olisi.
Kiitokset Tarjalle, Soinnulle, Erkille ja koko seurakunnan väelle. Kanssanne on hyvä tehdä töitä.
Kiitokset Vexille, Hannulle ja koko TEAMille. Teitte sen mahdolliseksi.
Kiitokset Harrille sitkeästä ohjauksesta, työni tiimoilta sekä koko TAMKin väelle antoisista opinnoista.
Kiitokset myös kaikille niille joille se kuuluu, enkä Teitä mainitse. Tiedätte kyllä itse. Pahoitteluni unohduksesta.

Tuulet ovat suotuisia niille, jotka tietävät mihin ovat menossa

LÄHTEET

Ogletree, Terry 2001. Inside Verkot. Jyväskylä: IT Press.

Microsoft 2000. Microsoft Windows 2000 Server Administrator's Companion. Redmont, Washington: Microsoft Press.

Microsoft 2000. Microsoft Windows 2000 Training Kit. Jyväskylä: IT Press.

Microsoft Active Directory Migration Tool (ADMT) version 2.0 Release Notes. [online] [viitattu 3.12.2005]. http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp

A comparison of the migration methods for migrating from Exchange Server 5.5 to Exchange Server 2003 or to Exchange 2000 Server. [online] [viitattu 3.12.2005]. http://support.microsoft.com/kb/327928/en-us

Exchange Connector. [online] [viitattu 3.12.2005].
http://www.quantumsoftware.com.au/ProductsServices/ExchangeConnector.aspx

Sähköpostin ja Internetin käytön pelisäännöt kirkkohallituksessa. [online] [viitattu 3.12.2005]. http://www.evl.fi/kkh/hao/atk/ohje/pelisaannot-KKH-2005.pdf

KIRKKO-verkon puitesopimukset. [online] [viitattu 3.12.2005].
http://www.evl.fi/tietohallinto/verkkosopimus/

Sepänmaa, Annamari 2004. Seurakuntayhtymän tietoverkon dokumentointi, Tutkintotyö. TAMK.

LIITTEET

LIITE1: YSICT–KEHTO-projektikuvaus

YSICT-KEHTO

Ylöjärven seurakunnan informaatio- ja kommunikaatioteknologian KEHITTÄMINEN ja TOIMINNALLISUUS

Development and functionality of Information and communication technology in the Evangelical Lutheran Church of Ylöjärvi

VISIOT (5 visiota):

- **Luoda eri teknologioista käyttäjäkuntaa mahdollisimman tehokkaasti ja yksilöllisesti palveleva infrastruktuuri**
- **Parantaa ja kehittää käyttäjien osaamista, pyrkimyksenä saada mahdollisimman suuri hyöty olemassa olevasta infrastruktuurista**
- **Kehittää seurakuntien tietojärjestelmiä vastaamaan erilaisiin nykyhetken ja tulevaisuuden tarpeisiin**
- **Rakentaa tietojärjestelmät mahdollisimman helposti ja kustannustehokkaasti johdettaviksi, hallittaviksi ja ylläpidettäviksi**
- **Toteuttaa kokonaisvaltainen ICT-infrastruktuurin kehittäminen ja ylläpito mahdollisimman korkealaatuisesti**

PÄÄFOKUKSET (kehityksen pääpaino organisaatiotasolla kohdistuu…):

ROI (Return Of Investment)
Kuinka pian investoinnit ”maksavat” itsensä takaisin
TCE (Total Customer Experience)
Käyttäjän ”käyttökokemus” / tyytyväisyys (hyötyarvo)
TCO (Total Cost of Ownership)
Todelliset elinkaarikustannukset (sis. piilokustannukset)

Pääfokukset järjestelmien kehittämisen näkökulmasta:

Reachability	Tavoitettavuus: Laitteet, verkot, palvelut, soveltuvuus käyttöön…
Availability	Käytettävyys: Laitteiden kunto, ohjelmistoversiot, päivitykset, huoltokatkot…
Scalability	Skaalautuvuus: Kasvunvara, mahdolliset relaatiot, integraatiot…
Manageability	Hallittavuus: Vakaus, ylläpidon määrä, koulutustarpeet, kustannustehokkuus…

Projektin läpiviennin perustana EFQM Excellence Model

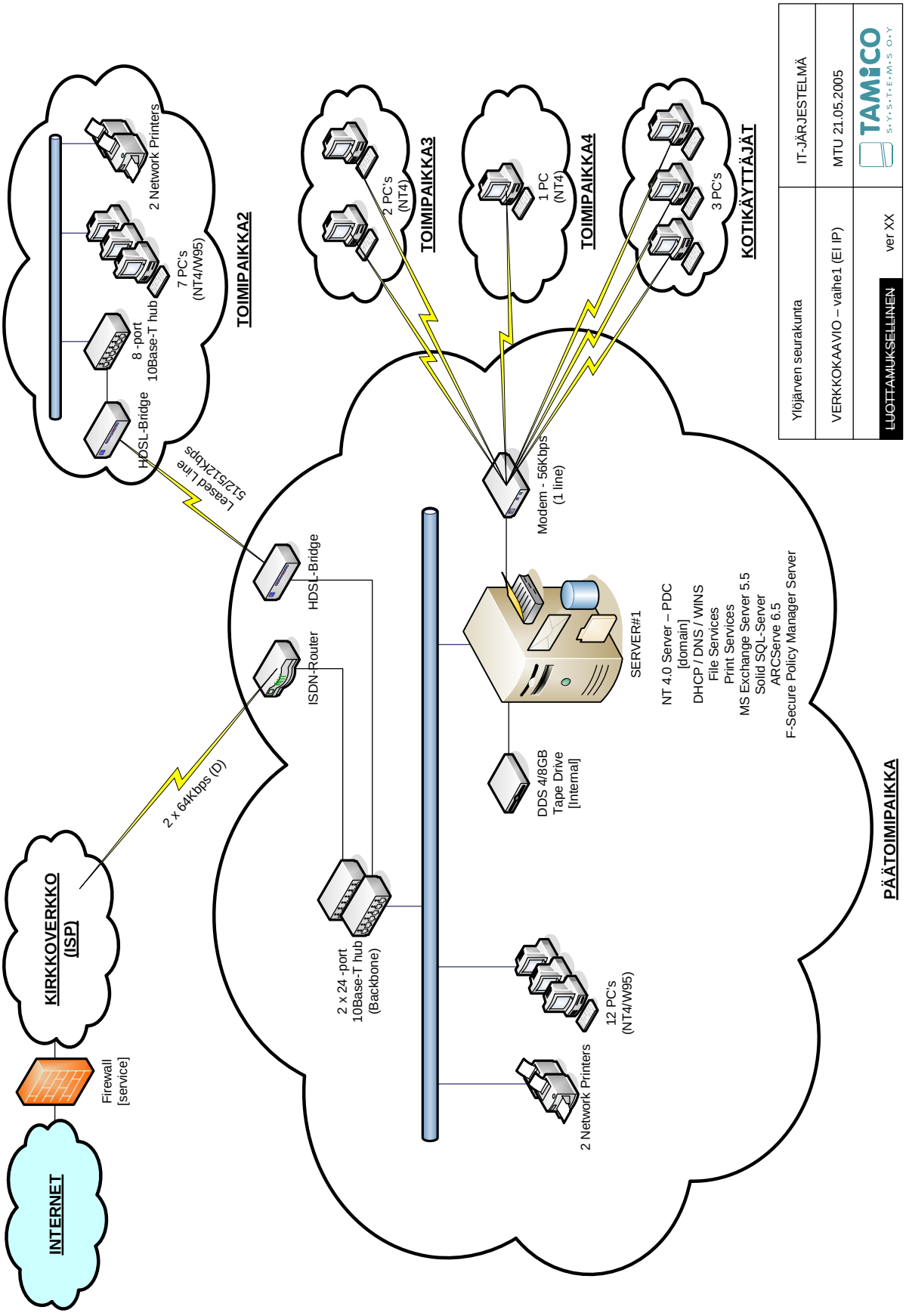
TUTKA-arviointilogiikka

- Tulokset
- Toimintatavat
- Käytännön soveltaminen
- Arviointi ja parantaminen
- Erinomaisuuden tunnuspiirteet
- Tuloshakuisuus
- Asiakassuuntautuneisuus
- Johtajuus ja päämäärätietoisuus
- Prosesseihin ja tosiasioihin perustuva johtaminen
- Henkilöstön kehittäminen ja osallistuminen
- Jatkuva oppiminen, parantaminen ja innovatiivisuus
- Kumppanuuksien kehittäminen
- Yhteiskunnallinen vastuu

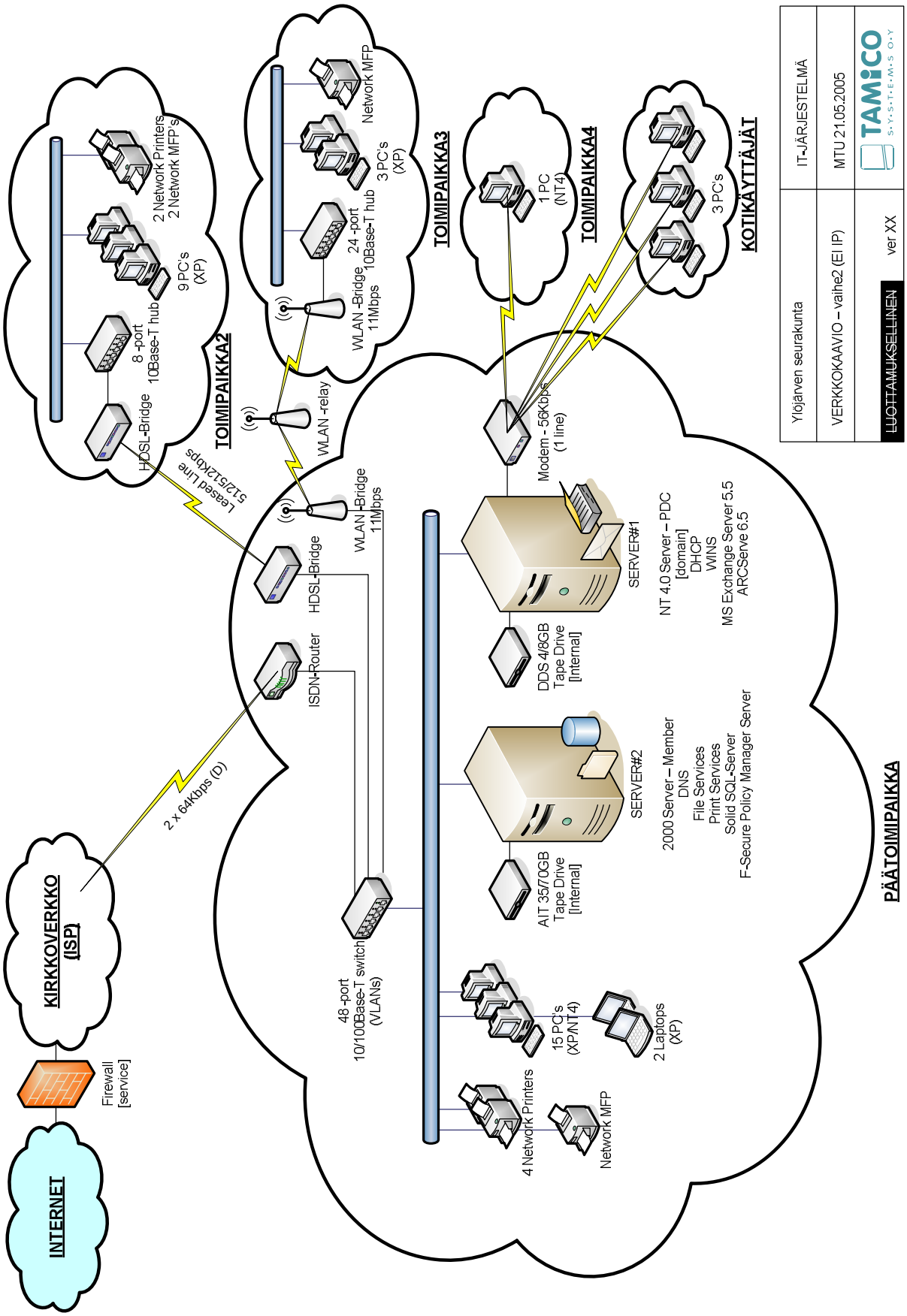
Tavoitteet:

- **Kartoittaa ICT-toimintoihin liittyvät tarpeet ja tyydyttää ne**
  - Yksilöiden / Yksiköiden / Organisaation tarpeet
    - Koulutustarpeet
    - Laitteistotarpeet
    - Ohjelmistotarpeet
    - Liikkuvuus
    - Toimitilat
  - Järjestelmän tarpeet
    - Dokumentointi tarpeet
    - Tietoturvan kehittäminen (tietoturvastrategia / -ohjeistus / -käsikirja)
    - Toimintavarmuuden ylläpito (99,9% => 87,6h / vuosi)
    - Käytettävyyden kehittäminen
    - Toiminnallisuuden kehittäminen (tietohallintostrategia + 5–vuotissuunnitelma 2005-2010)
  - Tulevaisuuden tarpeet
    - WLAN –yhteydet
    - “vierailijaverkot”
    - Varausjärjestelmät
    - Sähköpostijärjestelmien uudistukset
    - Päivitykset, muutokset
    - AD –migraatiot / luottosuhteet
    - Verkkojen yhdistäminen/sulautuminen muihin tahoihin
    - Kiinteistövalvontajärjestelmän kehittäminen
  - Hankinnat / hankintajärjestelmät
    - Kartoitukset
    - Tutustumiset
    - Raportoinnit
    - Kilpailutukset
    - TELE –liikenteen kokonaisratkaisu
      - VOIP
      - GSM / GPRS / 3G

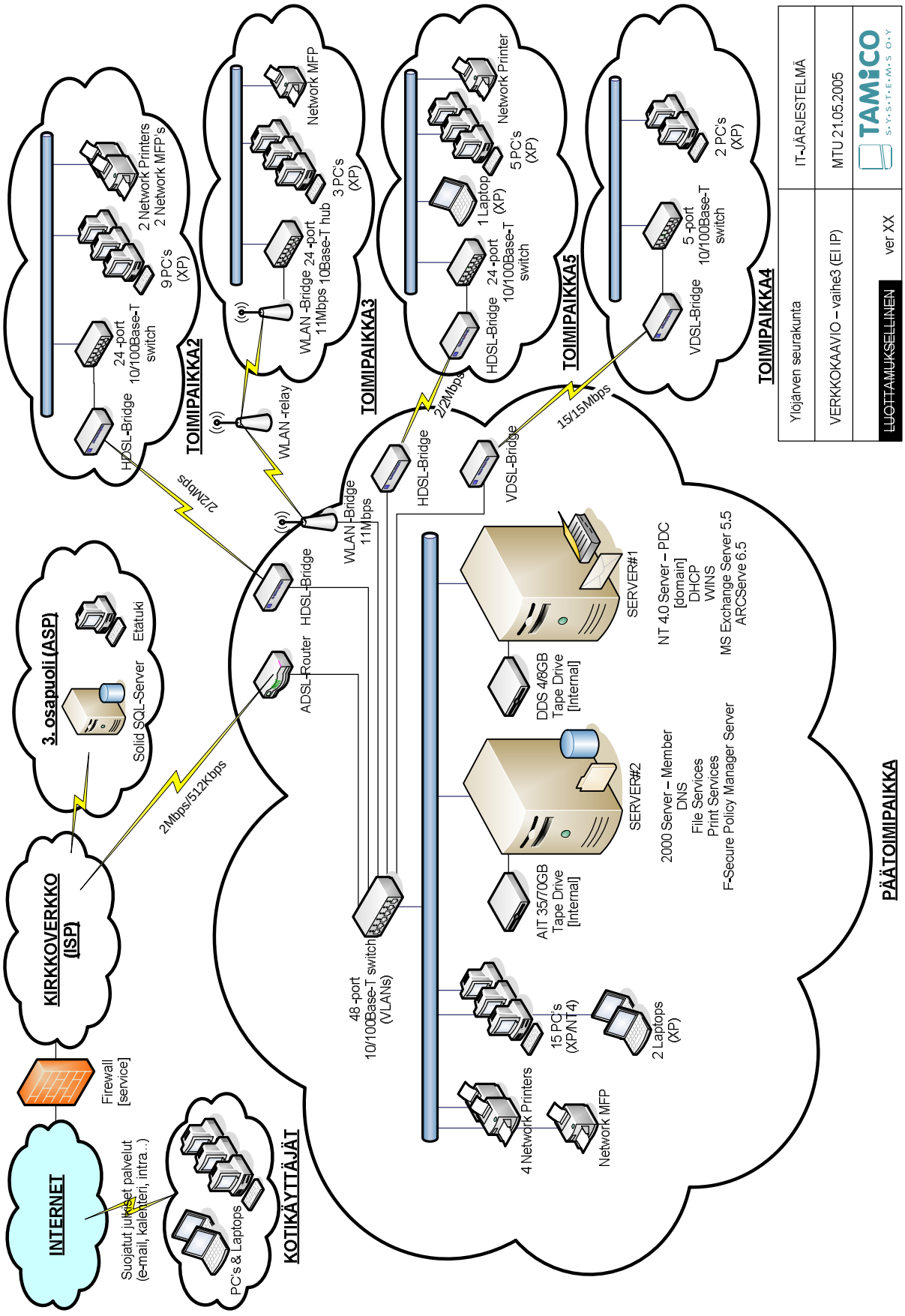
LIITE2: VERKKOKAAVIO-vaihe1



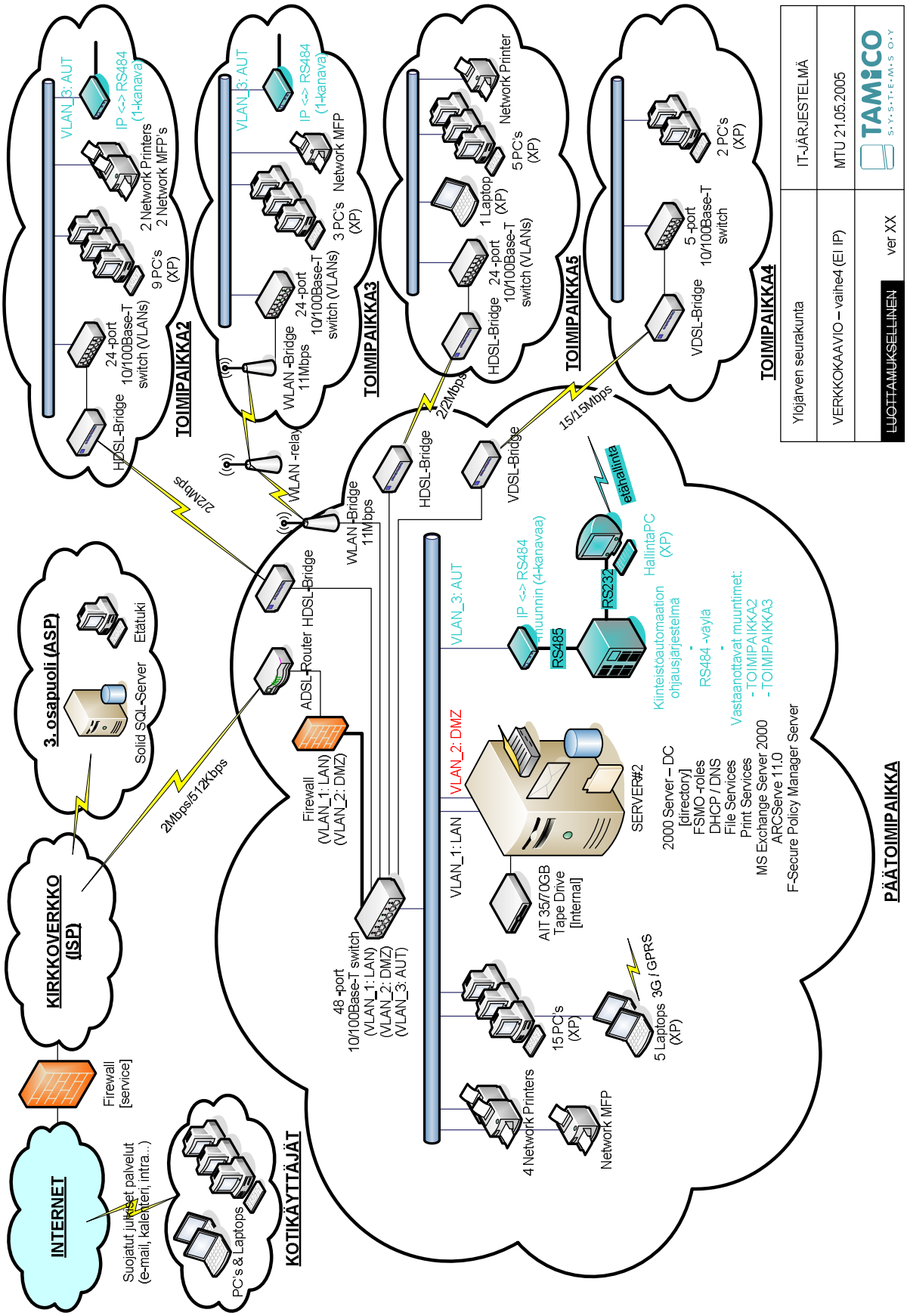
LIITE3: VERKKOKAAVIO-vaihe2



LIITE4: VERKKOKAAVIO-vaihe3



LIITE5: VERKKOKAAVIO-vaihe4



LIITE6: Quantum Software Solutions Exchange Connector-asetukset