ÄLYPUHELINTEN KESKITETTY HALLINTA YRITYSKÄYTÖSSÄ

Andritz Oy

LAHDEN AMMATTIKORKEAKOULU
Insinööri
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2008
Mike Virtanen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

VIRTANEN, MIKE: Älypuhelinten keskitetty hallinta yrityskäytössä

Tietoliikennetekniikan opinnäytetyö, 56 sivua

Kevät 2008

TIIVISTELMÄ

Työn tavoitteena on esitellä yrityskäyttöön tarkoitetun älypuhelimille suunnatun järjestelmän käyttöönotto ja sen mahdollistamat hyödyt. Järjestelmä perustuu Nokia Intellisync Mobile Suite -tuoteperheeseen, jonka Wireless Email ja OMA Device Manager tulevat yrityksen käyttöön. Lisäksi tavoitteena on luoda yritykselle valmis konsepti, jota seuraamalla uusia matkapuhelimia otetaan yrityksessä käyttöön sekä kehittää ja määrittää parhaimmat tavat joiden avulla tuotetta voidaan hyödyntää yrityksen eduksi.

Intellisync Wireless Email tarjoaa sähköposti-, kalenteri- ja yhteystietopalvelun älypuhelimeen, jolloin työskentely mahdollistuu ilman tietokonetta. Tiedon saatavuuden ja ajantasalla pysyvän kalenterin avulla parannetaan työntekijöiden työpanosta. OMA Device Manager mahdollistaa älypuhelinten hallinnoimisen ja sen avulla puhelimien sisältämä tieto pyritään suojaamaan ulkopuolisilta.

Työssä perehdytään myös älypuhelinten vakioinnin suunnitteluun, jota seuraamalla uudet älypuhelimet lisätään järjestelmään. Vakioinnin avulla puhelimissa on valmiina yrityksen määrittämät asetukset ja niissä käytettävät ohjelmistot sekä varmistus siitä, että puhelin pysyy suojattuna.

Järjestelmän käyttöönotto vaatii palvelinlaitteiston, ohjelmiston ja lisenssit palvelimille, vaadittavat verkkoasetukset, järjestelmään lisättävät puhelimet sekä henkilön, joka käyttöönottaa järjestelmän ja varmistaa sen toimivuuden.

Tulevaisuudessa laajenevan järjestelmän tulee skaalautua hyvin käyttötarpeiden mukaan. Järjestelmästä tulee kehittää mahdollisimman vähätöinen ja yrityksen sisäisen tuen työnjakoa on hyvä miettiä.

Työssä tehty tutkimus on suoritettu Andritz Oy:n pyynnöstä. Tutkimuksen pääkohdat sisältävät Intellisyncin ja OMA Device Managerin vaatimat verkkojärjestelyt sekä tarkemman esityksen niiden käyttöönotosta ja hallinnasta.

Avainsanat: Nokia, Intellisync, Device Manager, älypuhelin, push-email, sähköposti, tietoliikennetekniikka, etähallintajärjestelmä, mobiililaitteet

Lahti University of Applied Sciences
Faculty of Technology

VIRTANEN, MIKE:

Centralized management of smart phones in business use

Bachelor's Thesis in Telecommunications Technology, 56 pages

Spring 2008

ABSTRACT

This thesis deals with the deployment and management of the Nokia Mobility solution. The Mobility solution is made for business use only. The system is based on the Nokia Intellisync Mobile Suite production family. The objective of the thesis was to deploy Wireless Email and OMA Device Manager, which are parts in the product family, for the use of Andritz Oy. The purpose was also to create a concept which will be followed through while adding new smart phones into the system and also to determine the most suitable ways to use this product for the company's advantage.

Intellisync Wireless Email provides smart phones with email, calendar and contacts services. Through availability of information and up-to-date calendar the employees' working efficiency is improved. OMA Device Manager is a remote control system for smart phones and makes it possible to protect the information in the smart phones.

The study also deals with planning a suitable way for adding new smart phones into the system. Company phones will be set with the required settings and all the needed programs. After the phones are set, their protection is verified.

Introduction of the system needs server hardware, software and licences for the servers, network configurations, smart phones which are going to be installed to the system, and a person who will build up the system and ensure its functionality.

The system needs to be scalable for future needs. The system should require as little work as possible and it would be good to think how to distribute different support tasks within the company.

Key words: Nokia, Intellisync, Device Manager, smart phone, push-email, electronic mail, telecommunications technology, remote control system, mobile devices

SISÄLLYS

LYHENNELUETTELO

DMZ	Demilitarized zone. Tietoverkon alue, johon voidaan avata yhteys, mutta jonka sisältä ei oletusarvoisesti voi avata yhteyttä ulko- tai sisäverkkoon.
IMS	Intellisync Mobile Suite. Nokian mobiilisähköpostijärjestelmän keskeinen osa, joka keskustelee mm. sähköpostipalvelimen kanssa.
ISGW	Intellisync Secure Gateway. Nokian Intellisync Mobile Suitea suojaava ohjelmisto, joka toimii matkapuhelimen ja Intellisync Mobile Suiten välillä.
LAN	Local Area Network. Yrityksen sisäinen verkko, joka ei yleisesti näy ulkoverkkoon.
LDAP	Lightweight Directory Access Protocol. Yleinen autentikointiprotokolla käyttäjähakemistoa vastaan.
NBC	Nokia Business Center. Nokian kehittämä sähköpostijärjestelmä, joka korvattiin Intellisyncillä.
RAID-1	Kiintolevyn peilausmenetelmä, jonka avulla sama tieto tallennetaan kahdelle eri kiintolevylle tiedon säilymisen varmistamiseksi.
Sybase	Sybase on kehittänyt kevyen relaatiotietokantamallin matkapuhelinjärjestelmiin, jonka nimi on Adaptive Server Anywhere.
TCP	Transmission Control Protocol. Pakettiliikenteiseen tiedonsiirtoon yleisimmin käytetty yhteydellinen tiedonsiirtoprotokolla.

Tomcat	Apache Foundation:in kehittämä sovelluspalvelin, joka perustuu avoimeen lähdekoodiin. Tomcat on yksi tunnetuimmista web-komponenttialustoista.
WAN	Wide Area Network. Yrityksen ulkopuoleinen verkko, esim. Internet.

1 JOHDANTO

Nykyaikana puhelin on tärkeä työkalu useissa työtehtävissä. Matkapuhelimet ovat yleistyneet niin laajalle, että useimmissa yrityksissä toimihenkilöille tarjotaan työsuhdepuhelinta, jonka avulla hoidetaan työasioita. Matkapuhelimen välityksellä toimivat myynti, markkinointi, huolto kuin tukipalvelutkin. Sähköposti on myös tärkeä palvelu yritysmaailmassa ja sillä kommunikoidaan ja tiedotetaan työasioista. Tiedonkulkua saadaan tehostettua yhdistämällä sähköposti henkilökunnan matkapuhelimiin.

Andritz Oy:llä on toimipisteitä ympäri maailmaa ja osa työntekijöistä joutuu matkustamaan suhteellisen paljon. Andritz Oy käyttää Microsoft Outlook -ohjelmistoa sähköpostiohjelmana, jonka avulla lähetetään sähköpostia ja seurataan kalenteria. Andritz Oy:n IT-osasto on huolestunut yrityksensä työntekijöiden matkapuhelimista ja niissä säilytettävistä tiedoista. Yritykseltä katoaa useita matkapuhelimia vuodessa ja osa niistä myös varastetaan. Matkapuhelin voi sisältää henkilökohtaista ja myös yrityksen liiketoiminnan kannalta tärkeää tietoa, jolloin varastettu puhelin voi aiheuttaa yritykselle rahallista tappiota. Käyttöönotettavalla matkapuhelinten etähallintaohjelmistolla voidaan lukita matkapuhelimen asetuksia sekä puhelin on mahdollista lukita ja nollata etänä, jolloin tietoturvan tasoa saadaan huomattavasti parannettua.

Työn tavoitteena on esitellä yrityskäyttöön tarkoitetun älypuhelimille suunnatun järjestelmän käyttöönotto ja sen mahdollistamat hyödyt. Järjestelmä perustuu Nokia Intellisync Mobile Suite -tuoteperheeseen, jonka Wireless Email ja OMA Device Manager tulevat yrityksen käyttöön. Lisäksi tavoitteena on luoda yritykselle valmis konsepti, jota seuraamalla uusia matkapuhelimia otetaan yrityksessä käyttöön sekä kehittää ja määrittää parhaimmat tavat joiden avulla tuotetta voidaan hyödyntää yrityksen eduksi.

Työn aihepiiri rajataan järjestelmien käyttöönottoon sekä sen ylläpitoon. Työssä ei huomioida järjestelmän käyttöönoton kustannuksia, järjestelmässä käytettäviä matkapuhelimia eikä runkoverkon suunnitteluun ja toteutukseen liittyviä asioita.

2 YRITYS JA SEN TOIMIALA

Andritz Oy on yksi maailman johtavista sellu- ja paperiteollisuuden järjestelmien, laitteiden ja palvelujen toimittajista. Andritz Oy:n tuotealueita ovat puunkäsittely, kuituprosessit, kemikaalien talteenotto ja massankäsittely. Andritz Oy:n liikevaihto on noin 500 miljoonaa euroa ja yhtiön henkilökunnan määrä on noin 1100. Yhtiön pääkonttori sijaitsee Helsingissä. Hallituksen puheenjohtajana toimii Wolfgang Leitner (Andritz AG) ja toimitusjohtajana Harry Rickman. Yhtiön omistaa itävaltalainen Andritz AG. Andritz Oy:n tytäryhtiö on Savonlinna Works Oy. (Andritz 2008a.)

Yritys koostuu 13:sta eri divisioonasta, joita ovat Puunkäsittely-, Kemikaalijärjestelmät-, Kuitulinja-, Talteenotto-, Sellunkuivatus-, Paperin viimeistely-, Paperikone-, Automaatio-, Paperitehdas Service-, Sellutehdas Service-, Kulutusosapalvelut-, Massankäsittely- ja Mekaaninen massa- divisioona. Lisäksi yritys on jaettu viiteen regioonaan, joita ovat Pohjois-Amerikan-, Etelä-Amerikan-, Pohjois-Euroopan-, Keski-Euroopan ja Kiinan ja muun Aasian regioona. (Andritz 2008b.)

Puunkäsittelydivisioona (Wood Processing Division) on johtava kuorimolaitoksien ja -laitteiden toimittaja maailmassa. Tuotevalikoimamme sisältää prosessin tai laitteen jokaiseen puunkäsittelyn vaiheeseen; siitä kun puu saapuu tehtaalle, siihen asti kunnes hake on valmista kemiallisen tai mekaanisen massan valmistukseen. Puunkäsittelydivisioonan pääkonttori on Hollolassa ja sillä on toimipaikat USAssa, Kanadassa ja Brasiliassa. (Andritz 2008c.)

Sellutehdas Service -divisioona käsittää Puunkäsittelydivisioonan ja Sellutehdasdivisioonan palvelu- ja huoltotoiminnot. Pääpaino on tuotannon tehokkuus- ja käytettävyyspalveluissa, joita tuotetaan Andritzin tai muiden laitevalmistajien toimittamille sellutehtaille ja puunjalostuskentille (kulutusosat, varaosat, laitteiden kunnostukset, tehtaiden seisokkityöt, huoltosopimukset ja modernisoinnit). Traditionaalisten service-tuotteiden lisäksi divisioona toimii nykyisin yhdessä asiak-

kaan kanssa tuotannon luotettavuuden ja kokonaisvaltaisen tehokkuuden maksimoimiseksi tuottamalla arvoa lisääviä palveluja ja innovatiivisia ratkaisuja. Sellutehdas Service -divisioona palvelee Andritzin toimittamaa laajaa laitekantaa kaikkialla maailmassa. Osaamiskeskukset ovat Pohjois-Amerikassa ja Euroopassa, mutta paikallisia service-keskuksia on yli 30 paikkakunnalla eri puolilla maailmaa. Sellutehdas Service -divisioonan pääkonttori on Suomessa, Savonlinnassa. Divisioonassa työskentelee 285 henkilöä, joista noin 50 % Pohjois-Amerikassa, 40 % Euroopassa ja loput 10 % muualla maailmassa. Servicen omat tuotantoyksiköt laitekunnostuksiin ovat USA:ssa ja Suomessa. Lisäksi divisioonalla on paikalliset partner-konepajat Uudessa-Seelannissa, Indonesiassa, Etelä-Afrikassa, Brasiliassa ja Portugalissa. (Andritz 2008c.)

Massankäsittelydivisioona toimittaa maailmanlaajuisesti järjestelmiä, laitteita ja palveluja kaikkiin paperinvalmistusprosesseihin, kuten uusiomassan käsittelyyn, massankäsittelyyn, paperikoneen lyhytkiertoon, hylynkäsittelyyn sekä paperitehtaan sisäiseen vedenkäsittelyyn, lietteen ja rejektin käsittelyyn. Divisioonan toimipaikat ovat Grazissa, Itävallassa ja Kotkassa ja huomattavaa toimintaa on myös Kiinassa Foshanissa, USA:ssa Glens Fallsissa, New Yorkin osavaltiossa sekä Japanissa Tokiossa. (Andritz 2008c.)

Kuitulinjadivisioona on yksi maailman johtavista kemiallisen massan valmistuksessa käytettävien systeemien, laitteiden ja prosessien toimittajista. Divisioonan tuotteisiin kuuluvat jatkuvatoimiset keitinsysteemit, pesurit, sihdit, valkaisusysteemit ja niihin liittyvät laitteet. Divisioonan pääkonttori on Kotkassa. Muut toimipaikat ovat Savonlinnassa, USA:ssa Roswell (GA) ja Glens Falls (NY), Japanissa Tokio sekä Brasiliassa Curitiba. (Andritz 2008c.)

Andritz Oy:n kehittyminen ei ole tapahtunut hetkessä. Noin 15 vuotta sitten Andritz oli Suomen osalta huomattavasti pienempi kuin mitä se on nykyään. Yritys kasvoi ensiksi yhdistymällä Konewoodin kanssa Andritz Konewoodiksi ja myöhemmin vuonna 1996 yritys vaihtoi nimekseen Andritz Oy. Tällä hetkellä Andritz Oy työllistää yhteensä noin tuhat henkilöä Kotkassa, Helsingissä, Tampereella, Savonlinnassa, Varkaudessa ja Hollolassa. Näiden tuhannen henkilön lisäksi yritys

käyttää paljon tilapäistä työvoimaa ja tämän lisäksi yritys työllistää satoja alihankkijoita. (Andritz Oy 2008d.)

3 PALVELIMET

3.1 Palvelinhallinta

Lähes jokainen yritys tarvitsee palvelimia, vaikkei yrityksen liiketoiminta olisi sijoittunut informaatioteknologiaan. Tämän vuoksi palvelimien käyttötarve vaihtelee huomattavasti yrityksen tarpeiden mukaan. Palvelinten hallinta on aina jonkin henkilön tai ryhmän vastuulla. Heidän työnsä on tarkkailla, että palvelimet ovat toimintakunnossa ja samalla varmistaa, että niiden laitteistot sekä ohjelmistot pysyvät ajan tasalla. (Takkinen 2003.)

Palvelimet tulisi sijoittaa tilaan, jonne ulkopuolisilta on pääsy estetty. Palvelinhuoneen tilat suunnitellaan niin, että niiden sisään syttynyt tulipalo saadaan sammutetuksi vahingoittamatta muuta laitteistoa. Palvelimissa olevien komponenttien käyttöikä lyhenee, jos ilmanvaihdosta ei huolehdita. Palvelinhuoneen ilmanvaihdon tulee olla tehokas, jolloin palvelimet eivät pääse ylikuumenemaan edes pitkäaikaisessa rasituksessa. (Hosia 2004.)

Palvelimia hallitaan useimmiten etäyhteyksien kautta, jolloin vältetään tarvetta kulkea palvelinhuoneeseen. Palvelinhuoneessa työskennellään ainoastaan silloin, kun tehdään fyysisiä muutoksia palvelimille. Etäyhteyksien ansiosta palvelinten toimintaa voidaan tarkkailla keskitetysti. Palvelimia hallinnoiva henkilö voi korjata ilmenneitä ongelmia suoraan kodistansa milloin tahansa, jolloin hänen ei tarvitse matkata konttorille. (Takkinen 2003.)

Microsoftin tarjoama etäyhteys-palvelu on nimeltään Remote Desktop. Remote Desktop:in avulla käyttäjä voi avata etäyhteyksiä palvelimille, jotka tukevat Remote Desktop protokollaa. Remote Desktop Protocol (RDP) perustuu ITU T.120 protokollaperheeseen ja sen laajennukseen. RDP on monikanavaisuuteen perustuva protokolla, joka sallii useiden virtuaalikanavien välittää tietoa suojatusti palve-

limelta etätyöasemalle. RDP tukee 64000 erinäistä kanavaa tiedonsiirtoon ja huolehtii monipistesiirrosta. (Microsoft msdn 2008.)

RDP käyttää palvelimen näytönohjainta kääntämään (render) ruudun näkymää luomalla käännetystä informaatiosta tietoverkkopaketteja, jotka käyttävät RDP-protokollaa. Nämä paketit lähetetään verkon lävitse etäkoneelle (client). Etäkoneella RDP vastaanottaa käännettävää tietoa ja tulkitsee paketit vastaamaan Microsoft Win32:n graphics device interface:n (GDI) API-kutsuja (Application Programming Interface). Etäkoneelta lähetetyt näppäimistön ja hiiren toiminnot ohjataan suoraan palvelimelle käyttäen palvelimen on-screen näppäimistön ja hiiren ajuria. Kaikki etätyöpöytäistunnossa olevat ympäristömuuttujat, kuten esimerkiksi värien syvyyttä ilmaisevat muuttujat, jotka ovat määritetty RCP-TCP yhteyden asetuksissa. (Microsoft msdn 2008.)

RDP-yhteys on suojattu käyttäen RSA:n Security RC4 salausta, joka on suunniteltu salaamaan tehokkaasti pieniä määriä dataa. Salaus voidaan tehdä joko 56- tai 128-bittisellä avaimella. Kaistanleveyttä pyritään pienentämään käyttämällä tiedon pakkausta, sekä muuttumattomien kuvien ja kuvien osien tallentamista välimuistiin. Ruudulla tapahtuvien muutosten tiedot siirretään ainoastaan tietoverkon läpi, jolloin säästetään huomattavasti kaistanleveyttä ja etähallinnan käyttö mahdollistuu hitaillakin yhteyksillä. (Microsoft msdn 2008.)

Jos verkkoyhteys katkeaa kesken RDP-istunnon, käyttäjän istunto jää odottamaan käyttäjän takaisinkirjautumista. RDP-istuntoa voidaan jatkaa uudesta sijainnista ilman, että istunnon aikana tallennetut tiedot menetettäisiin. RDP:n tarjoama etäyhteys mahdollistaa leikepöydän käytön, jolloin tekstin ja kuvien kopioiminen etäkoneen ja palvelimen välillä on mahdollista. Samalla tavoin tulostus voidaan ohjata etäpalvelimelta etäkoneen tulostimelle. (Microsoft msdn 2008.)

3.2 Sähköpostipalvelimet

3.2.1 Yleistä sähköpostipalveluista

Sähköpostipalveluiden käyttö on yleistynyt kaikkialla tietoverkkojen laajentumisen ansiosta. Sähköpostipalvelut voidaan luokitella kahteen pääkategoriaan sähköpostipalvelimen omistajuuden mukaan.

Tarjolla on ilmaisia sähköpostipalveluita, joiden käyttäjäksi pääsee rekisteröimällä oman sähköpostitunnuksen kyseiselle domain-päätteelle. Palvelut ovat pääosin ilmaisia, mutta niihin voi ostaa lisäosia ja -palveluja, kuten esimerkiksi lisää verkkolevytilaa sähköposteille. Tämän tyyppisiä palveluita tarjoavat operaattorit sekä useat muut yhtiöt. Näitä palveluntarjoajia ja palveluita ovat esimerkiksi Google – Gmail, Microsoft – Hotmail, Yahoo! – Yahoo! Mail, Elisa – Saunalahti, MTV3 – Luukku, Sonera – Sähköposti. (Kotilainen 2007.)

Kun sähköpostia hyödynnetään liiketoiminnassa, tulee sähköpostin sisällön eheyden ja tiedon salaaminen tärkeäksi osaksi koko sähköpostijärjestelmää. Liiketoiminnan kannalta ei ole järkevää sallia ulkopuolisille oikeuksia päästä käsiksi lähetettyihin ja vastaanotettuihin sähköposteihin. Varmistaakseen sähköpostien yksityisyyden ja parantaakseen luotettavuuden tunnetta asiakkaissa, yrityksen kannattaa perustaa oma sähköpostipalvelin käyttöönsä. Yrityskäyttöön suunnatut sähköpostiohjelmistot tarjoavat useasti myös lisäpalveja, kuten kalenterin, kontaktitietojen organisoinnin sekä pikaviestintäominaisuudet. Lisäpalvelujen avulla yritys voi parantaa henkilöstön tuottavuutta, sekä joissain tapauksissa saada säästöjä. (Kalliala, Maunuksela-Malinen & Saloniemi 2004.)

Sähköpostipalvelimiin löytyy ohjelmistoja useilta eri valmistajilta, mutta yrityskäytössä yleisimpiä ovat Microsoftin Exchange, Novellin GroupWise ja IBM:n Lotus Notes. Sähköpostin lukemiseen tarvitaan sopiva ohjelmisto, joka liikennöi

yrityksessä olevan sähköpostipalvelimen kanssa. Sähköpostiin avataan usein pääsy myös web-sivuston kautta, joskin lisäpalveluiden käyttö on tällöin mahdotonta. (Scoble 2005.)

3.2.2 Microsoft Exchangen kehitys

Microsoft Exchange on oletettavasti yleisin käytössä oleva sähköpostijärjestelmä. Microsoft Exchangen ensimmäinen versio julkaistiin vuonna 1996, joka oli nimeltään Exchange Server 4.0. Exchange Server 4.0 oli päivitys Microsoft Mail 3.5:lle, joka oli Microsoftin edeltävä sähköpostijärjestelmä. Microsoft Exchange Server 4.0 oli täysin uusi X.400-pohjautuva pääte – palvelin tyyppinen järjestelmä. Järjestelmä käytti yhtä ainoata tietokantaa, joka tuki myös X.500 hakemistopalveluita. Tästä hakemistopalvelusta muodostui lopulta Microsoftin Active Directory palvelu, joka on LDAP-yhteensopiva hakemistopalvelu. (Microsoft Technet 2008.)

Exchange Server päivittyi versioon 5.0 toukokuussa vuonna 1997. Exchange Serverin uusin ominaisuus oli Exchange Administrator console, joka avasi pääsyn ensimmäistä kertaa SMTP-pohjautuviin verkkoihin. Exchange 5.0 pystyi kommunikoimaan suoraan palvelimien kanssa käyttämällä internet mail -standardia. Samalla julkaistiin Outlook Web Access, jonka avulla käyttäjä voi kirjautua sähköpostiinsa web-sivun kautta. (Microsoft Technet 2008.)

Exchange 5.5 julkaistiin saman vuoden marraskuussa ja sitä myytiin kahtena eri versiona. Standard Edition sisälsi tuen 16 Gt:n tietokannalle, aivan kuten aikaisemmat versiot Exchange Serveristä. Enterprise Edition sisälsi tuen 16 Tt:n tietokannalle. Exchange 5.5 oli myös yhteensopiva muiden sähköpostijärjestelmien kanssa joita olivat cc:Mail, Lotus Notes ja Novell GroupWise. Exchange 5.5 mahdollisti kahden palvelimen clusteroinnin, jolloin kaksi sähköpostipalvelinta voitiin asettaa rinnakkain verkkoon. Lisäksi Exchange 5.5 julkisti useita uusia ominai-

suuksia, kuten kalenteritуen Outlook Web Accessiin sekä IMAP ja LDAP v3 päätteet. (Microsoft Technet 2008.)

Exchange Server 2000 julkaistiin vuonna 2000 ja se ratkaisi useita rajoituksia edeltävistä versioistaan. Exchange Server 2000 kasvatti tietokannan maksimikokoa ja nosti clusterin koon kahdesta neljään palvelimeen. Toisaalta Microsoft vaati yrityksen verkolta täyden tuen Microsoftin Active Directorylle, jota ei vaadittu edeltäjältään Exchange 5.5. Exchange Server 2000 ei sisältänyt sisäistä Directory Serviceä. Pikaviestinnälle lisättiin tuki, mutta myöhemmin se irrotettiin omaksi kokonaisuudeksi. Pikaviestintäpalvelu kantaa nykyjään nimeä Microsoft Office Live Communication Server. (Microsoft Technet 2008.)

Exchange Server 2003 julkaistiin syyskuussa vuonna 2003. Exchange Server 2003 sisältää useita yhteensopivuustiloja, joiden avulla käyttäjät voidaan muuttaa uuteen järjestelmään. Tämä hyödyntää suuria yrityksiä, joiden jaetut Exchange Server ympäristöt eivät salli pitkää järjestelmän alhaallaoloaikaa, jolloin järjestelmä olisi pois käytöstä. Yhteensopivuustilojen avulla järjestelmä voidaan pitää käynnissä, jolloin vältytään pitkältä toimintakatkolta. Katkon pituus muodostuisi järjestelmän täydellisestä siirtymisestä uuteen järjestelmään, ennen kuin palvelua voitaisiin käynnistää. Yksi pääominaisuus Exchange Server 2003:ssa on sen parannettu vikaantumisesta palautuminen. Parannellun vikaantumisesta palautumisen mahdollistaa toiminto, jonka avulla palvelimen sallitaan lähettää ja vastaanottaa sähköpostia, samalla kun sen sisältämää viestitietokantaa palautetaan varmuuskopioista. (Microsoft Technet 2005.)

Exchange Server 2003:n mukana tehtiin selvä jako, siten että Exchange sisältää ainoastaan sähköpostin ja kalenteritoiminnon. Muut Microsoftin tuotteet myydään erikseen, mutta ne ovat toistensa kanssa yhteensopivia ja täten järjestelmästä saadaan laajempi kokonaisuus lisäämällä siihen uusia palveluita. Uusia palveluja ovat muun muassa Office, Office Live communication Server, Live Meeting ja Sharepoint. (Microsoft Technet 2005.)

3.3 Tietokannat

Tietokanta on toisiinsa liittyvistä tiedoista kerätty kokoelma. Tietokanta tallennetaan matriisitaulukkoon, joka yksinkertaisimmillaan koostuu sarakkeista ja riveistä. Tietokanta voi sisältää myös tiedon syvyydestä, jolloin taulukosta tulee kolmiulotteinen. (ODBC 2008.)

Tietokantoja käytetään lähes jokaisella sovellusalueella. Niihin tallennettava tieto on hyvin järjestetty ja usealle käyttäjälle ja laitteelle voidaan antaa mahdollisuus muokata samaa tietokantaa. Tällä tavoin tietokannan tarjoamia etuja saadaan tehostettua. (ODBC 2008.)

3.3.1 Sybase Adaptive Server Anywhere

Adaptive Server Anywhere (ASA) on Sybase:n kehittämä tietokannan hallintajärjestelmä. Sybasen ominaisuuksista löytyy toimintojen eheyden tarkistaminen, automaattinen järjestelmän palautus ja tallennettavan tiedon eheyden tunnistus, liipaisimet (triggers) ja tallennettavat proseduurit. (Owen 2003.)

ASA ei ole rajoitettu käytettäväksi ainoastaan pienissä työpöytä sovelluksissa, vaan se tukee yli 100 samanaikaista käyttäjää. ASA on suunniteltu tarvitsemaan vähän huoltoa. Adaptive Server Anywhere osaa kasvattaa automaattisesti tietokannan kokoa ja muokata sitä toimimaan tehokkaammin. Lisäksi se osaa hyödyntää poistetun tilan uudelle tiedolle. ASA:lla käytetään yleisesti useiden gigatavujen kokoisia tietokantoja. (Owen 2003.)

3.3.2 Microsoft SQL

Tietojärjestelmissä olevaa tietoa halutaan hyödyntää entistä tehokkaammin. Kuukausittain ajetut raportit eivät enää riitä, vaan nykyään raportteja tulee saada minä päivänä tahansa. Ruudulta halutaan nähdä reaaliaikaisesti tilauskannan kehitys ja tulevaisuutta ennustetaan käyttämällä olemassa olevaa tietomassaa. Tiedon halu-

taan olevan käytössä rikkaassa muodossa niin, että tieto soveltuu mahdollisimman suoraan päätöksenteon pohjaksi. Tavoitteena on saada aikaan parempia päätöksiä ja nopeampia tuloksia. (Microsoft SQL 2008.)

Kahdennetut tietokantapalvelimet ja tietokannat olivat aikaisemmin vain suurten yritysten ja suurten järjestelmien toteutuksia. Ei välttämättä siksi, että korkeaa käytettävyyttä ei tarvittaisi pienemmissä yrityksissä ja pienemmissä sovelluksissa, vaan koska se ei ollut kustannusmielessä perusteltavissa. Monet järjestelmät palvelevat työntekijöitä, asiakkaita ja kumppaneita kellon ympäri seitsemän päivää viikossa. Tietokannan ollessa tuotannossa siihen on pystyttävä tekemään tarvittavat hallintatoiminnot, kuten varmistukset ja indeksoinnit. (Microsoft SQL 2008.)

Microsoft SQL Server 2005 on kustannustehokas ja monipuolinen tietojenhallinta- ja -analysointiratkaisu, jonka avulla yrityksen tieto- ja analysointisovellusten turvallisuus, skaalautuvuus ja käytettävyys ovat aiempaa parempia ja näiden sovellusten luonti, käyttöönotto ja hallinta ovat entistä helpompaa. SQL Server 2005 auttaa yritystoiminnan kolmella keskeisellä osa-alueella: yritystietojen hallinnassa, kehittäjien tuottavuudessa ja liiketoimintalogiikassa. (Moonsoft 2008.)

3.4 Virtualisointi

Virtuaalipalvelimet ovat jatkaneet yleistymistään yrityksissä ja niihin tarjottavat laitteistot ja ohjelmistot ovat kehittyneet huomattavasti menneistä vuosista. Virtualisoinnilla pyritään säästämään yrityksen kuluja, sekä samalla yksinkertaistamaan ja helpottamaan palvelinten hallintaa. (Purho 2007.)

Virtualisointi perustuu ajatukseen, jossa palvelimiin sijoitettu laskentateho keskitetään yhteen isoon keskuspalvelimeen, jonka sisällä ajetaan palvelimia virtuaalisesti. Resurssien keskittämisestä on etua varsinkin silloin, kun yrityksessä käytetään palvelimia, jotka tarvitsevat hetkellisesti paljon laskentatehoa. Virtualisoinnin ideaalitapauksessa virtualisoitavat palvelut tarvitsevat paljon laskentatehoa hetkellisesti ja muuna aikana toimivat vain tyhjäkäynnillä. Tämän tapainen palvelu on

esimerkiksi varmuuskopiointi, joka useimmiten suoritetaan yön aikana. Varmuuskopiointi suoritetaan haluttuna ajankohtana, jonka jälkeen palvelin jää odottamaan seuraavaa varmuuskopiointiajankohtaa. (Purho 2007.)

Virtualisointi on konsolidointitekniikka, jonka avulla ohjelmat voidaan siirtää fyysiseltä palvelimelta virtuaalikoneisiin. Virtuaalikoneita voi olla yksi tai useampi yhdellä fyysisellä palvelimella. Virtualisointikäyttöjärjestelmistä tunnetuimpia ovat tällä hetkellä VMware ESX ja Microsoftin Hyper-V. (Microsoft it showcase 2005.)

Virtuaalipalvelimia voidaan luoda ja hallita laitteistoympäristön rajoissa eivätkä laitteistomuutokset vaikuta virtuaalipalveluihin. Menettelyllä saavutetaan laiteinvestointien korkeampi käyttöaste, sovellusten ja laitteiden elinkaaren hallinnan helpottuminen ja tärkeimpänä nopeampi reagointi liiketoiminnan tarpeiden muutoksiin. (Suomen tietoveljet Oy 2006.)

3.5 Varmuuskopiointi

Palvelimien ylläpidosta huolehtivan tulee varautua tilanteisiin, joissa palvelin hajoaa fyysisesti tai palvelimen sisältämät tiedot katoavat. Palvelimissa käytetyt kiintolevyt vikaantuvat ja levyllä oleva data voi muuttua lukukelvottomaksi, vaikkei palvelimen laitteisto hajoaisi. Varmuuskopioinnilla voidaan välttää tiedon menetys ja se mahdollistaa järjestelmän nopean palauttamisen toimintakuntoon. (Soinsaari 2007.)

Varmistuakseen siitä, että järjestelmä voidaan palauttaa nopeasti alkutilaansa, siitä tulee ottaa varmuuskopioita riittävän usein. Varmuuskopiointiin on tarjolla useita ohjelmia, joiden avulla voidaan suorittaa varmuuskopiointi automaattisesti ja halutulla tapaa. Varmuuskopiointi voidaan tehdä joko osittain, ohjelmakohtaisesti, käyttöjärjestelmäkohtaisesti tai osio-/kiintolevykohtaisesti. (Soinsaari 2007.)

Varmuuskopiointi tehdään useimmiten nauha-asemien avulla. Nauha-aseman käyttö ei ole kuitenkaan ainoa vaihtoehto, vaan varmuuskopiot voidaan tallentaa kiintolevyille, optisille tallennusmedioille tai flash-muistille. (Soinsaari 2007.)

Varmuuskopio voidaan tallentaa tallennusmedialle kolmella eri tapaa. Tallennettavasta kohteesta voidaan tehdä Full Backup, joka tallentaa tiedon kokonaisuudessaan. Incremental Backup tallentaa edellisestä varmuuskopiosta muuttuneet tiedot. Tämä säästää huomattavasti tallennustilaa, mutta tiedostojen palauttaminen muodostuu työlääksi. Incremental Backupissa palautus tulee suorittaa läpi koko varmuuskopiosarjan, aina Full Backupista lähtien. Tästä syystä jokainen Incremental Backup tallenne on tärkeä. (The Tech FAQ 2008a.)

Differential Backup tallettaa Full Backup:sta tapahtuneet muutokset, jolloin jokainen yksittäinen Differential Backup sisältää muutokset Full Backup tilaan. Tämä poistaa muiden varmuuskopioiden tarpeellisuuden, mutta käyttää enemmän tallennustilaa kuin Incremental Backup, koska alkuperäiseen Full Backup:iin verrattuna sama tieto tallennetaan joka kerta uudestaan uuteen Differential Backup:iin. (The Tech FAQ 2008b.)

Varmuuskopiointiohjelmistot voivat tarjota lisäparannuksia varmuuskopiointiin. Ohjelmallisesti voidaan verrata varmuuskopioitavia tietoja toisiinsa ja täten saman tiedoston tallentaminen usealta käyttäjältä voidaan välttää. (Soinsaari 2007.)

4 TIETOLIIKENNEVERKOT

Tietoliikenneverkot ovat valloittaneet lähes koko maailman ja niissä kulkevan liikenteen määrä kasvaa entisestään. Verkoista tulee nopeampia ja tämä aiheuttaa haasteita palveluntarjoajille, jotka pyrkivät palvelemaan asiakkaitaan parhaansa mukaan.

Tietoliikenneverkot voivat toimia joko langattomasti tai langallisesti. Langattomasti toimivia tietoverkkoja ovat esimerkiksi GSM-verkot ja satelliittilinkit. Langattomat tietoverkot hyödyntävät maanpäällisiä tietoliikenneverkkoja. Maanpäälliset tietoliikenneverkot voidaan luokitella karkeasti sijaintinsa ja käyttökohteensa mukaan kolmeen eri alueeseen. Näitä alueita ovat Wide Area Network, Local Area Network ja Demilitarized Zone. (Granlund 1999, 34, 43.)

4.1 GSM-verkot

GSM-teknologian kehitys aloitettiin 1980-luvun lopulla. Se perustuu digitaaliseen tiedonsiirtoon, toisin kuin sitä edeltänyt NMT-teknologia, joka toimi analogisesti. GSM-verkko on solukkopuhelinverkko, jonka solut voivat olla hyvin erimuotoisia ja kokoisia. Olennaista solukkoverkossa on, että vierekkäiset solut eivät käytä samaa taajuusaluetta, vaan niiden välillä on vähintään yhden solun ”suojaväli”. (Hämeen-Anttila 2003, 101.)

GSM 900 -taajuudet jakautuvat kolmeen luokkaan. Perus-GSM (standard tai primary) eli P-GSM toimii uplink-suunnassa 890 – 915 MHz taajuusalueella ja 935 – 960 MHz taajuudella downlink-suuntaan. Uplink-suunta tarkoittaa puhelimesta tukiasemalle lähetettyä siirtosuuntaa ja downlink-suunta tukiasemalta puhelimeen lähettämää siirtosuuntaa. P-GSM järjestelmässä on yhteensä 124 taajuutta eli 25 MHz taajuuskaista, joka yleensä jaetaan kilpailevien operaattorien kesken. (Penttinen 1999, 78.)

Laajennettu GMS (extended) eli E-GSM on määritetty uplink-suuntaan alueelle 880 – 915 MHz ja downlink-suuntaan 925 – 960 MHz alueelle. GSM-spesifikaatiot määrittävät myös rautateiden käyttöön R-GSM:n, joka käyttää taajuusalueenaan 876 – 915 MHz uplink-suuntaan ja 921 – 960 MHz downlink-suuntaan. E-GSM ja R-GSM kuuluvat GSM 900 järjestelmään. (Penttinen 1999, 78.)

GMS 900:n lisäksi on olemassa DCS 1800 -versio (Digital Cellular System for 1800 MHz), joka toimii useasti PCN-verkossa (Personal Communications Network). DCS 1800 käyttää taajuusalueinaan 1710 – 1785 MHz (uplink) ja 1805 – 1880 MHz (downlink). DCS 1800:n taajuuskaista on 75 MHz siirtosuuntaa kohden ja sisältää 374 taajuutta. (Penttinen 1999, 79.)

Amerikkalaisten käyttämä GSM-verkko toimii PCS 1900 -verkossa. PCS-järjestelmä koostuu useista taajuuslohkoista 1900 MHz:n alueelta sisältäen kapea- ja laajakaistaisia järjestelmiä. Kaikki GSM-järjestelmät perustuvat samoihin spesifikaatioihin. Erot ovat pääasiassa radiorajapinnan tehotasoissa, kanavien lukumäärissä ja taajuusalueissa. GSM Association on määrittänyt verkoille yhtenäiset nimet GSM 900, GSM 1800 ja GSM 1900. (Penttinen 1999, 79.)

GSM-järjestelmien taajuus- eli kanavaväli on 200 kHz. Taajuusalueiden alussa on yhden kanavan suojaetäisyys, joten ensimmäinen käytettävä P-GSM-taajuus on 890,2 MHz. Lähetys- ja vastaanottotaajuudet on jaettu kahdeksan aikavälin eli TDMA-kehyksen (Time Division Multiple Access) jaksoihin. Koska GSM-järjestelmä käyttää useita radiokanavia, kyseessä on TDMA:n ja FDMA:n (Frequency Division Multiple Access) yhdistelmä. (Penttinen 1999, 79.)

Nykyisen GSM-teknologian avulla kukin puhelu käyttää 16 kbps aikavälin. Varsinainen hyötykuorma GSM-tekniikalla on 9600 bps, koska mm. virheenkorjaus vaatii osan kaistanleveydestä. (Hämeen-Anttila 2003, 102.)

4.1.1 GPRS

GPRS tulee sanoista General Packet Radio Service. GPRS tukee langattomia yhteyksiä IP-pohjaisiin verkkoihin luomalla saumattoman yhdyskäytävän esimerkiksi Internetiin. Tämä muutos on GPRS:n osalta siirtyminen piirikytkentäisistä yhteyksistä pakettipohjaisiin yhteyksiin. Pakettipohjainen ratkaisu tuo samalla uuden hinnoittelumahdollisuuden. Piirikytkentäisissä verkoissa laskutettiin asiakasta puhutun ajan mukaan, mutta pakettipohjaisissa verkoissa hinnoittelu perustuu siirretyn datan määrään. GPRS:n maksimi tiedonsiirtonopeus on 171,2 kbps. (Hämeen-Anttila 2003, 103.)

GRPS-verkko vaatii GSM-verkolta lisäkomponentteja, koska piirikytkentäisiä palveluja tarjoava verkko tulee mahdollistaa tarjoamaan pakettikytkentäisiä yhteyksiä. Uusia verkkoelementtejä ovat GPRS-tukisolmu (SGSN) ja GPRS-yhdyskäytävä (GGSN). GPRS-tukisolmu tietää matkapuhelimen sijainnin ja välittää matkapuhelimen ja GSN:n (GPRS Support Node) välistä pakettiliikennettä. GGSN tekee pakettien muunnoksen IP- ja X.25-protokollapaketeiksi ja lähettää ne toisiin verkkoihin. (Hämeen-Anttila 2003, 104.)

4.1.2 EDGE

EDGE (Enhanced Data Rates for GSM Evolution) toi merkittäviä parannuksia GSM:n toiseen vaiheeseen. Koska teknologia perustuu jo olemassa olevaan GSM-verkkoon, uusia verkkoelementtejä ei tarvita. EDGE on tarkoitettu operaattoreille, joilla ei ole 3G-lisenssiä, mutta jotka kuitenkin haluavat tarjota asiakkailleen kilpailukykyisiä langattoman multimedian palveluita. EDGE:n standardiin kuuluu kaksi merkittävää palvelua: EGPRS (Enhanced General Packet Radio Service) ja ECSD (Enhanced Circuit Switched Data). (Hämeen-Anttila 2003, 105.)

EDGE käyttää uutta modulointimenetelmää, jolloin alkuperäinen 0,3 GMSK (Gaussian Minimum Shift Keying) vaihtuu 8-PSK-modulaatioon (8 Phase Shift

Keying). EDGE:ä voidaan periaatteessa käyttää myös puhepalveluiden parantamiseen. (Penttinen 1999, 282.)

EDGE:n tarjoaa nopeamman liikennöintinopeuden kuin GPRS tai HSCSD. EDGE pystyy siirtämään tietoa 64 kbps jokaisella aikavälillä. Maksimissaan EDGE voi käyttää kahdeksaa aikaväliä, jolloin maksimaalinen tiedonsiirtonopeus kasvaa 384 kbps. Jos EDGE-tietoverkkoa ei ole saatavilla, käytetään tiedonsiirtoon GRPS-verkkoa. EDGE tarjoaa parhaan nopeusluokan 2.5 G verkkoon, joka tullaan lopulta päivittämään 3G verkoksi. (Landmark Internet Ltd 2008.)

4.1.3 UMTS

UMTS (Universal Mobile Telecommunications System) on GSM:n seuraajaksi kehitetty kolmannen sukupolven, eli 3G:n (3rd Generation) matkapuhelinjärjestelmä. Euroopassa käytetään järjestelmälle nimitystä UMTS ja maailmanlaajuisesti se tunnetaan nimellä IMT-2000 (International Mobile Telecommunications 2000). UMTS:n suunnittelu alkoi 1990-luvulla. UMTS:n ensimmäiset päätökset maailmanlaajuisista taajuusvarauksista tehtiin ITU:ssa (International Telecommunication Union) jo vuonna 1992. ITU vastaa UMTS:n eli IMT-2000:n maailmanlaajuisesta suunnittelusta ja sen tarkoituksena on mahdollistaa maailmanlaajuisesti päätelaitteiden yhteensopivuus. (Verkkouutiset 1998.)

UMTS-solun koko määräytyy aktiivisen käyttäjämäärän mukaan. UMTS:n tiedonsiirtonopeus on maksimissaan 384 kbps ja sen vasteaika on noin 200 millisekuntia. UMTS:ia edeltäneissä GPRS- ja EDGE-tekniikoissa viive vaihteli 500 millisekunnista kolmeen sekuntiin. UMTS-verkon tiedonsiirtonopeutta voidaan moninkertaistaa käyttämällä HSDPA-tekniikkaa. HSDPA voi saavuttaa 3,6 Mbps tiedonsiirtonopeuden tavallisella antennilla olevaan matkapuhelimeen. Tulevaisuudessa paremmilla antenniratkaisuilla saavutetaan jopa 14,4 Mbps tiedonsiirtonopeus. (Nortel 2005.)

4.2 Johdolliset tietoliikenneverkot

Johdollisissa tietoliikenneverkoissa kaapelit muodostavat yhteyden päätelaitteiden välille. Yleisimpiä kaapelityyppejä ovat parikierretty johdin, koaksiaalikaapeli ja valokuitu. Koaksiaalikaapelin käyttö on poistumassa tietoliikenneverkoista ja sen korvaajaksi on tullut parikierretty kaapeli. Parikierretty kaapeli soveltuu hyvin lähiverkkojen kaapelointiin. Pidemmille etäisyyksille käytetään valokuitua, joka samalla mahdollistaa nopeammat linkkinopeudet. (Granlund 1999, 34.)

IP-protokollaan pohjautuvat tietoliikenneverkot ovat pakettikytkentäisiä, joissa siirrettävä tieto jaetaan paketteihin. Kukin paketti sisältää vähintään tiedon kohdeosoitteesta sekä muita käytettävään protokollaan liittyviä tietoja. Koaksiaaliverkot olivat verkkotopologialtaan rengas- ja väyläkytkentäisiä. Nykyään käytössä olevat parikaapeli- ja kuituyhteydet käyttävät tähtikytkentäistä verkkotopologiaa. (Granlund 1999, 52.)

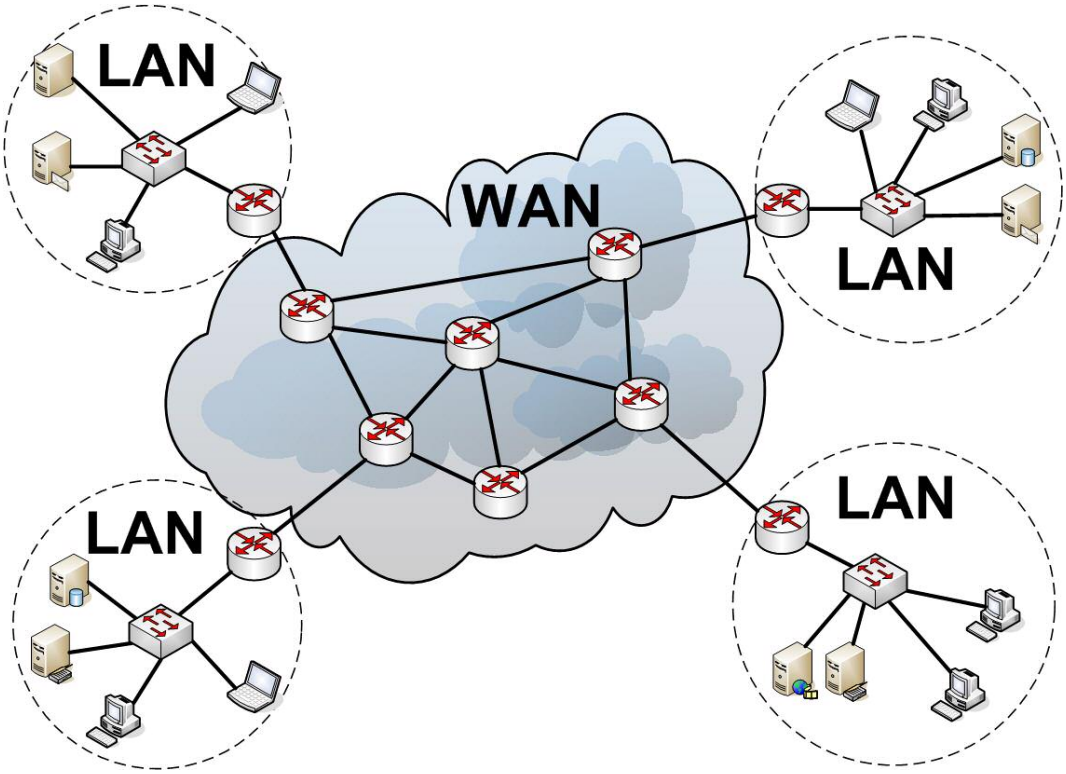
4.2.1 Wide Area Network

Wide Area Network (WAN) on tietoverkko, joka käsittää laajalle alueelle kattavan alueen. WAN-verkolla tarkoitetaan verkkoa, joka yltää mantereelta toiselle. WAN-verkot muodostuvat reititin-verkoista, jotka kattavat koko maailman. Näistä reitittimistä muodostuu hyvin laaja runkoverkko, jonka kautta pienemmät verkot voivat liikennöidä toisten verkkojen kanssa. (Pääkkönen 2002.)

WAN-verkkoon voidaan ajatella sisältyvän CAN- (Campus Area Network) ja MAN-verkot (Metropolitan Area Network). WAN-verkko on mahdollistanut Internetin toimimisen, jonka välityksellä on mahdollista luoda yhteyksiä ympäri maailmaa. (Pääkkönen 2002.)

WAN-verkon ylläpito ei olisi mahdollista luoda ilman hyvää yhteistyötä palveluntarjoajien (ISP, Internet Service Provider) kesken ja täten heidän panoksensa verkon toimivuuteen on hyvin suuri. Palveluntarjoajat sopivat keskenään reitittimissään käytetyt reititysprotokollat sekä linkkinopeudet. Heidän vastuullensa jää

myös linkkiyhteyksien luonti, eli kaapelien veto maan ja meren yli. WAN-verkko ei näy verkkoon kytkeytyneille laitteille millään tapaa, vaan se käyttäytyy aivan kuin normaali yhteys käyttäjän päätteeltä kohdepäätteelle. (Pääkkönen 2002.)

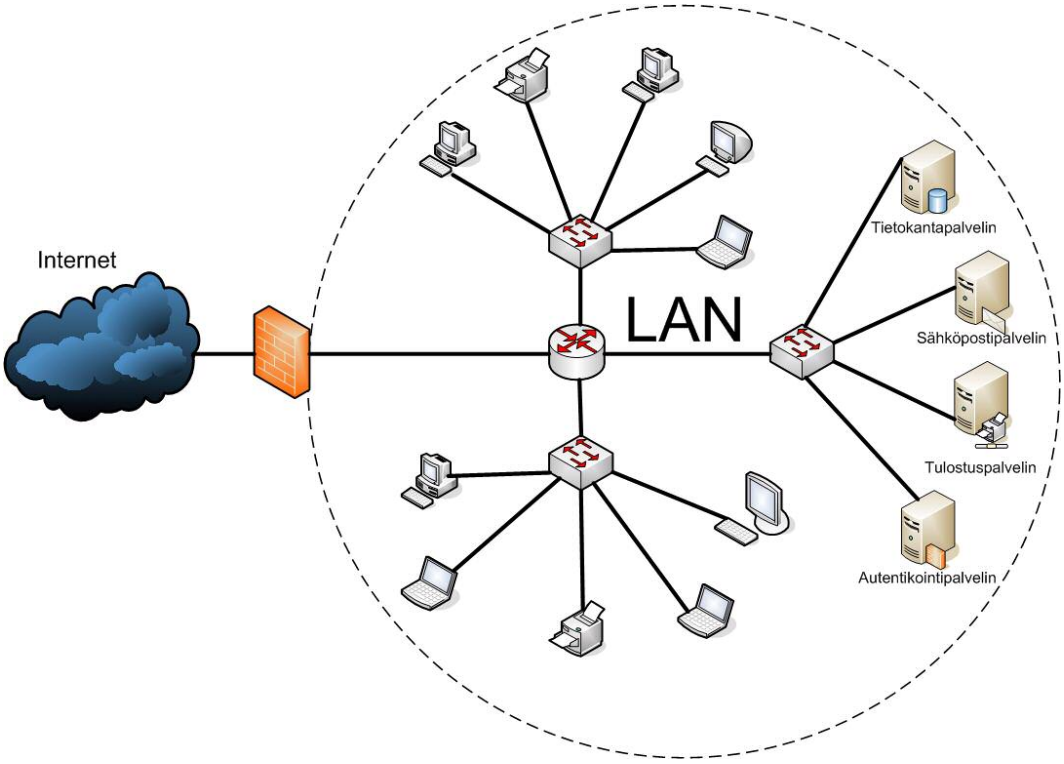


KUVIO 1. Wide Area Network

4.2.2 Local Area Network

Local Area Network (LAN) on lähiverkko, joka kattaa maantieteellisesti pienen alueen tietokoneita ja palvelimia. LAN-verkko vastaa kooltaan rakennuksen kokoa. LAN-verkkoja löytyy maailmasta todennäköisesti eniten, koska palveluntarjoajat antavat niin kotikäyttäjille, kuin myös yrityksille ainoastaan yhden IP-osoitteen, jolla voidaan liikennöidä ulkoverkkoon eli WAN-verkkoon päin. Tästä syystä yritykset ja kotikäyttäjät liittyvät Internetiin yleisesti reitittimen tai palomuurin kautta. Reititin toimii verkkojen välisenä linkittäjänä ja täten LAN-

verkossa käytetään eri IP-avaruutta, kuin millä ulkoverkossa liikennöidään. LAN-verkkoon voidaan ajatella sisältyvän myös PAN-verkot (Personal Area Network), joiden hallinnointi on yleensä yhden henkilön vastuulla. (Koivisto 1997.)



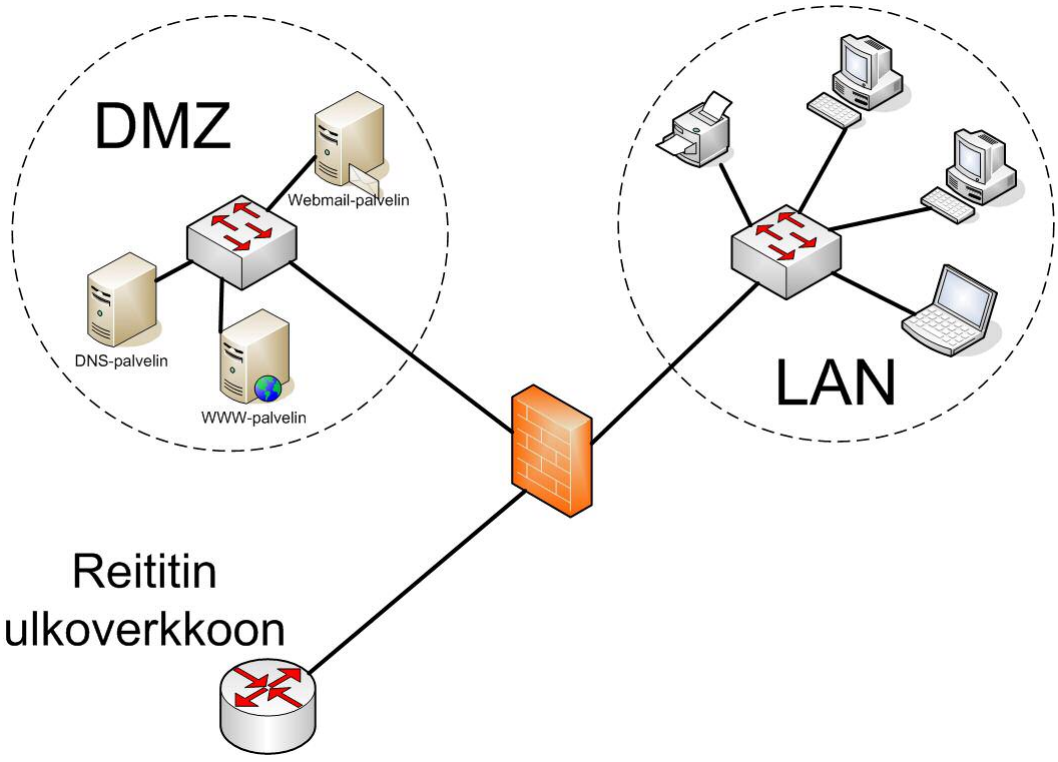
KUVIO 2. Local Area Network eli lähiverkko

4.2.3 Demilitarized Zone

Demilitarized Zone (DMZ) on eräänlainen lisäverkko yrityksen sisällä. DMZ-alueen sisältä ei ole millään laitteella oikeuksia aloittaa yhteydenmuodostusta ulko- tai sisäverkkoon. DMZ-alueella olevat laitteet saavat kuitenkin vastata yhteydenottoihin. DMZ-alueelle lisätään palvelimia, jotka halutaan näkymään verkosta ulospäin, kuten esimerkiksi www-palvelin ja FTP-palvelin. DMZ-alueelle on syytä sijoittaa kaikki palvelimet, joihin tulee päästä ulkoverkon kautta. Aluetta voi käyttää myös proxynä yhteyksien välillä, mutta se ei ole enää yleistä. (Grönholm 2002.)

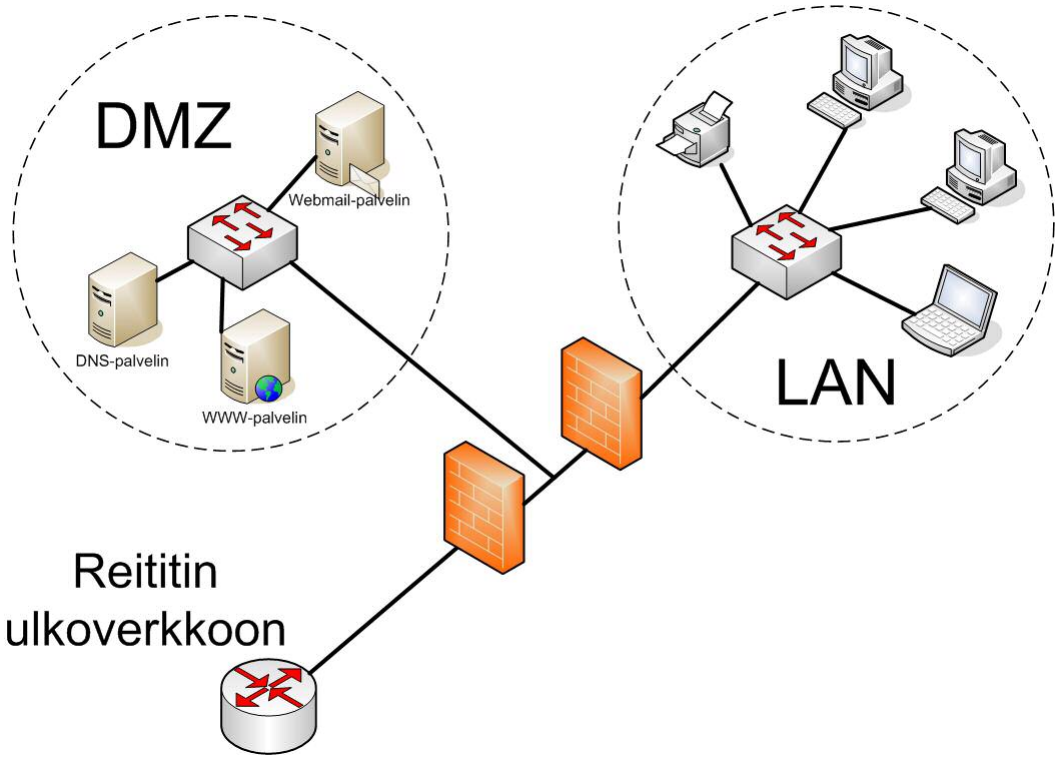
DMZ-alueelle murtautuminen ei tarkoita sitä, että yrityksen sisäverkkoon voitaisiin päästä tunkeutumaan. Tämä johtuu siitä, että DMZ-alueelta on kielletty laitteiden yhteyksien muodostaminen niin sisä- kuin ulkoverkkoonkin. Jos murtautuja on kuitenkin päässyt DMZ-alueen palvelimelle, hän voi lukea ja poistaa palvelimen sisältä löytyviä tietoja. (Grönholm 2002.)

DMZ-alue voidaan luoda monella eri tapaa. Kaksi yleisintä tapaa luoda DMZ-alue on käyttää yhtä tai kahta palomuuria. Yhtä palomuuria käytettäessä, palomuurista tulee löytyä kolme eri verkkoliitäntää. Niiden avulla käytetään esimerkiksi porttia Eth0 ulko-verkolle (WAN), Eth1 DMZ-alueelle ja Eth2 sisäverkolle (LAN). DMZ-alueelle on hyvä käyttää omaa IP-osoite avaruutta, jolloin LAN- ja DMZ-verkko eivät mene helposti sekaisin. Tämän tyyppinen ratkaisu vaatii paljon tehoa palomuurilta, koska sen tulee hallita sisä- ja ulkoverkosta tuleva liikenne. DMZ-alueelta lähtevät yhteydenmuodostukset tulee oletusarvoisesti estää. (Newman 1999.)



KUVIO 3. DMZ-verkko käytettäessä yhden palomuurin ratkaisua

Kahta palomuuria käyttämällä, saadaan helpotettua palomuurille kohdistuvaa rasitusta. Lisäksi palomuureissa ei tarvitse olla kuin kaksi verkkoliitäntää. DMZ-alueena on jälleen hyvä käyttää omaa aliverkkoa, koska se selventää järjestelmän ymmärtämistä ja helpottaa palomuurin sääntöjen suunnittelua. Kahden palomuurin järjestelyssä heikompitehoinen palomuuri sijoitetaan sisäverkon ja DMZ-alueen välille. Tehokkaampi palomuuri sijoitetaan DMZ-alueen ja ulkoverkon välille, koska liikenne ulkoverkosta DMZ-alueelle, sekä sisäverkosta ulkoverkkoon vaatii paljon tehoa. Palomuurien väliltä tulee löytyä yhteys, jolloin ulkoverkosta tuleva liikenne voidaan ohjata myös suoraan sisäverkkoon DMZ-alueen sijaan. Ulkoverkon puoleisen palomuurin tulee sallia liikenne DMZ-alueelle, mutta tarkistaa huolellisesti sisäverkkoon tuleva liikenne. Sisäverkon puoleisen palomuurin tulee varmistua siitä, että DMZ-alueelta ei sallita yhteyden muodostuksia sisäverkkoon. Samalla sisäverkon puoleisen palomuurin tulee varmistaa sisäverkkoon tuleva liikenne oikeelliseksi. (Newman 1999.)



KUVIO 4. DMZ-verkko käytettäessä kahden palomuurin ratkaisua

4.3 LDAP

LDAP on kehittynyt CITT:n (International Telegraph and Telephone Consultative Committee) ja ISO:n (International Organization of Standards) kehittämästä hakemistopalvelusta, jota voitiin käyttää käyttöympäristöstä riippumatta. Julkaistu standardi oli X.500, joka koostui useista eri suosituksista ja viittasi moniin muihin ISO:n standardeihin. X.500:n hyviä puolia olivat monipuolinen tietomalli, yleiskäyttöisyys ja laajennettavuus. Asiakkaan ja hakemistopalvelun välillä liikennöitiin käyttämällä DAP-protokollaa (Directory Access Protocol). DAP:in heikkous oli siinä, että se tarvitsi koko protokollapinon käyttöä, jonka vaatimia resursseja ei kaikista käyttöympäristöistä kuitenkaan löytynyt. Tämän takia kehitettiin asiakkaan ja hakemistopalvelimen välille kevyempi protokolla, joka sai nimekseen LDAP (Lightweight Directory Access Protocol). (Salakoski 2002.)

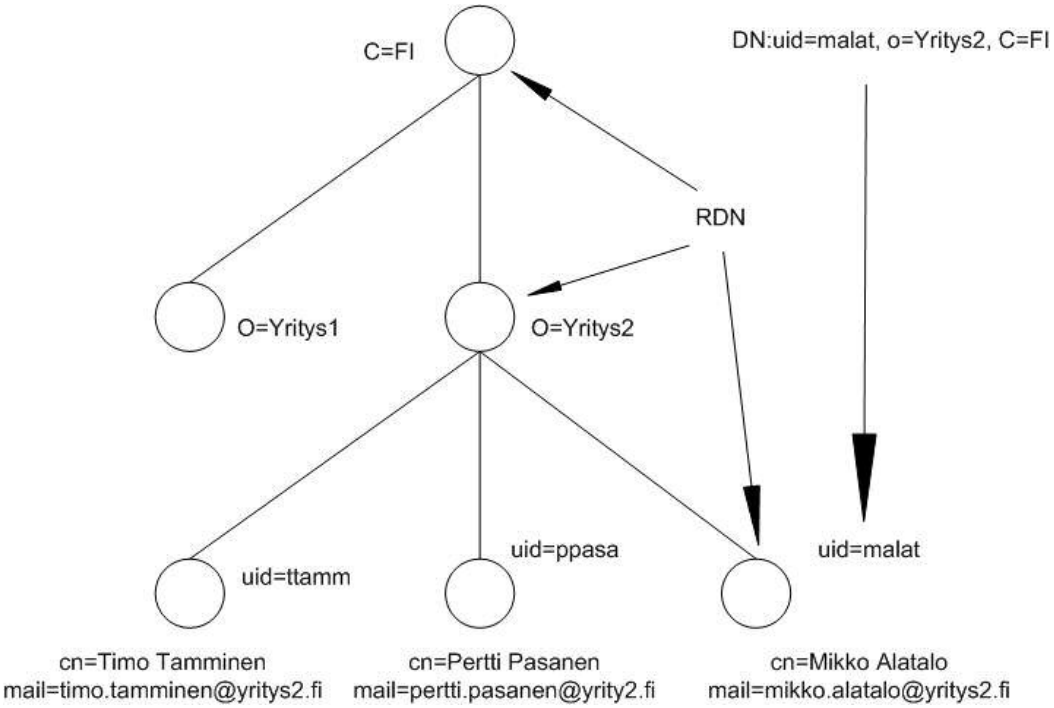
LDAP määrittelee asiakkaan ja hakemistopalvelimen välille käytettävän yhteisen kielen. Aluksi asiakas lähettää yhteyden alustuspyynnön (bind request) palvelimelle, johon sisältyy asiakkaan tunnistautumistiedot. Jos tunnistautuminen onnistuu, asiakas voi suorittaa haluamiaan operaatioita, kuten esimerkiksi tietojen hakua. Kun asiakas päättää sulkea yhteyden palvelimelle, lähettää se yhteyden lopetuspyynnön (unbind request). (Salakoski 2002.)

LDAP sisältää neljä eri mallia joilla hakemiston käyttöä ohjataan. Ensimmäinen niistä on tietomalli. Siinä määritetään hakemistoon talletettavien attribuuttien tyypit sekä attribuuteista koostuvat tietueet (entry). Yksittäinen tietue kuvaa isompaa asiakokonaisuutta, kuten henkilöä tai yritystä. Tietueeseen kuuluvat attribuutit kuvaavat itse tietueen ominaisuuksia eli esimerkiksi henkilön nimeä. Attribuutit voivat sisältää yhden tai useamman arvon. (Salakoski 2002.)

Attribuutit luokitellaan käyttäjäattribuutteihin ja toiminnallisiin attribuutteihin. Käyttäjäattribuutit ovat tavallisia attribuutteja, joiden arvoa voidaan muokata. Toiminnallisia attribuutteja ovat määrättyyn tarkoitukseen käytetyt attribuutit, jotka ohjaavat hakemiston toimintaa tai kuvaavat hakemiston tilaa. (Salakoski 2002.)

Hakemiston skeemaa kuvaa se, minkä olioluokkien tyyppiä voidaan tallentaa hakemistoon ja sen mitä attribuutteja siihen sisältyy. Kun hakemistoon tehdään muutoksia tai lisätään uusi tietue, palvelin tarkistaa ensiksi hakemiston skeemasta valitun tietotyypin. Jos muokattava tietue on skeeman mukainen, operaatio suoritetaan palvelimella. Jos se ei jostain syystä ole skeeman mukainen, palvelin palauttaa operaatiosta virheilmoituksen. Skeema tulee sisältää joitakin yleisiä olioluokkia, attribuutteja ja syntakseja. (Salakoski 2002.)

Toinen malli hakemiston ohjauksesta liittyy nimeämiseen. Siinä määritetään kuinka tietueet nimetään ja organisoidaan puumaiseen hakemistorakenteeseen. Tietueiden järjestys hakemistopuussa perustuu niiden yksikäsitteisiin nimiin. Tietueen yksikäsitteinen nimi (Distinguished Name, DN) muodostuu tietueen nimestä yhdistettynä hakemistopuun edeltäviin nimiin. Tämän takia nimi koostuu useasta paikallisesti yksikäsitteisestä nimestä (Relative Distinguished Name, RDN), joiden pitää olla yksikäsitteinen vain sisarus-tietueittensa kanssa. Ainoa poikkeus puumaiselle rakenteelle on alias-tietue, joka viittaa toiseen tietueeseen palvelimen hakemistopuusta. (Salakoski 2002.)



KUVIO 5. LDAP-hakemistopuun rakenne

Kolmas malli hakemiston ohjauksesta on toimintomalli, joka kuvaa LDAP-hakemistoon tehtävät operaatiot. Näitä toimintamallin sisältämiä toimintoja on kolmea eri tyyppiä, joita ovat tunnistautumis-, kysely- ja päivitysoperaatiot. (Salakoski 2002.)

Tunnistautumiseen käytetään bind-, unbind- sekä abandon-operaatioita. Bind-operaatiolla asiakas tunnistautuu ja avaa yhteyden LDAP-palvelimelle. Unbind-operaatiolla yhteys suljetaan. Abandon-operaatiolla asiakas voi keskeyttää bind-operaation, jos asiakas kyllästyy odottamaan vastausta. (Salakoski 2002.)

Kyselyoperaatioita on kahta eri tyyppiä. Compare-operaatiolla voidaan tehdä kysely hakemistopalvelimelle jonkin attribuutin tietystä arvosta. Search-operaatiolla vuorostaan saadaan tieto, jos haettavaa attribuuttia ei löydy edes koko hakemistosta. Tällaisessa tilanteessa search-operaatio palauttaa vastauksena tiedon, että attribuutilta ei löydy kysyttyä arvoa. (Salakoski 2002.)

LDAP määrittelee neljä eri päivitysoperaatiota, joilla LDAP-hakemiston tietoja muutetaan. Näitä operaatioita ovat add, delete, modify ja modify RDN. Add-operaatiolla lisätään uusia tietueita hakemistoon, syöttämällä tietueen parametreihin yksikäsitteinen nimi ja siihen liitettävät attribuutit. Delete-operaatiolla saadaan poistettua tietueita hakemistosta. Poistettaessa tietueita tulee varmistua siitä, ettei tietueelta löydy lapsia. Modify-operaation avulla voidaan muokata tietueen attribuutteja. Tietueen siirto toiseen paikkaan hakemistopuussa tapahtuu käyttämällä modify-RDN-operaatiota. Modify-RDN-operaatiota käytettäessä siirrettävän tietueen alipuu siirtyy mukana. Päivitysoperaatiota ei voida suorittaa osittain, vaan se onnistuu joko kokonaan tai ei ollenkaan. (Salakoski 2002.)

Neljäs malli hakemiston ohjauksesta on LDAP-turvallisuusmalli, joka perustuu bind-operaatioon. LDAP on yhteydellinen protokolla, jossa asiakas ensiksi autentikoituu, sen jälkeen suorittaa operaationsa ja lopuksi sulkee yhteyden. Jos autentikointia ei suoritetta, niin palvelin käsittelee asiakasta anonyyminä, jolloin asiakas ei yleensä saa mitään oikeuksia. (Salakoski 2002.)

LDAP versio 3:n autentikointi voidaan suorittaa kahdella eri tavalla. Yksinkertainen tunnistus ei ole yleisesti suositeltava, koska käyttäjätunnus ja salasana lähetetään palvelimelle selkokielisenä. Turvallisempi tapa on SASL-tunistus, jossa palvelin ja asiakas sopivat yhteisen autentikointi- tai salausprotokollan. Tällöin palvelin suojaa yhteyden asiakkaan pyytämällä protokollalla, jos protokolla on palvelimen puolesta tuettu. (Salakoski 2002.)

4.4 Symbian OS

Älypuhelimet ovat uuden sukupolven matkapuhelimia, joista löytyy kämmentietokoneista muistuttavia ominaisuuksia. Älypuhelimilla voidaan suorittaa yksinkertaista tekstinkäsittelyä, taulukkolaskentaa, esitysgrafiikkaa sekä käyttää internetiä. (Älypuhelimet 2008.)

Pääkriteeri matkapuhelinten ja älypuhelinten luokittelussa on puhelimen käyttöliittymä. Tavallinen matkapuhelin sallii ainoastaan tehdä muutoksia asetuksiin, mutta älypuhelimeen voidaan asentaa ulkopuolisia sovelluksia. Puhelimeen voidaan ohjelmoida omia sovelluksia tai niitä voidaan ladata verkko- tai mobiilipalveluista. Älypuhelinten käyttöjärjestelmistä yleisimpiä ovat Symbian OS, Microsoft Windows Mobile, Palm, Brew, SmartPhone sekä Mobile Linux, joista yleisin on Symbian OS. (Älypuhelimet 2008.)

Symbian perustettiin vuonna 1998 yhteistyössä Ericssonin, Motorolan, Nokian ja Psionin kanssa. Symbian:ista omistaa enemmistöosan Nokia (47,9 %) ja toiseksi eniten Symbian:ista omistaa Ericsson (15,6 %). Symbian OS on Symbian Ltd:n kehittämä käyttöjärjestelmä, joka on tarkoitettu pienitehoisille ja vähäisillä resursseilla toimiville laitteille. Symbian on kuuluisin matkapuhelinkäyttöjärjestelmänä ja siitä on kehitetty useita eri versioita. (Symbian 2008a.)

Symbian OS pohjautuu mikrokernel-arkkitehtuuriin. Itse kernel huolehtii vain aktiivisen säikeen vaihtamisesta, muistinsuojauksesta sekä viestinvälityksestä eri prosessien välillä. Kaikki muu toiminnallisuus hoidetaan erillisissä server-

prosesseissa, joita käytetään asynkronisesti lähettämällä näille viestejä, eikä perinteiseen tapaan funktiokutsun tapaisilla järjestelmäkutsuilla. (Symbian 2008b.)

Symbian OS on kirjoitettu C++-kielellä, mutta se ei käytä C++-kielen standardikirjastoja, vaan toteuttaa omat kirjastonsa näiden tilalle. Symbian OS:n käyttämät kirjastot on suunniteltu alusta lähtien kuluttamaan mahdollisimman vähän muistia ja ne ovat jossain määrin matalamman tason kirjastoja kuin standardin C++:n kirjastot. Koska kirjastot ovat standardi C++:n kirjostoja matalammalla tasolla, niiden käyttäminen on vaikeampaa ja siten kirjastojen käyttäminen hidastaa ja hankaloittaa käyttöjärjestelmän sovellusten ohjelmointia. (Symbian 2008b.)

5 NOKIAN MATKAPUHELINJÄRJESTELMÄ

5.1 Nokia Business Center

Nokia toi markkinoille Nokia Business Centerin (NBC) vuonna 2005. NBC:n välityksellä älypuhelin saa muodostettua yhteyden yrityksen sisällä sijaitsevaan MS Exchange -palvelimeen. Järjestelmän päätehtävä on luoda käyttäjille tiedon saatavuus, jolloin käyttäjät eivät ole sidottuja työskentelemään tietokoneella ennalta määrätyssä sijainnissa. Sovellus oli ensimmäinen palvelu, joka oli suunnattu yrityksen työntekijöille. Aiemmin kännykkäsähköpostit oli avattu ainoastaan yrityksen johdolle käyttäen apunaan vpn-tunnelointia tai SSL-salausta, jota NBC:tä edeltänyt Nokia Secure Access System (NSAS) käytti. NBC tukee MS Exchangea ja IBM:n Lotus Notesia. (Lehto 2005.)

NBC:n myötä Nokia ryhtyi kilpailemaan RIM BlackBerryn, IBM:n, Smartner-Sevenin ja Viston kanssa mobiilisähköpostijärjestelmistä. Sähköpostissa käytetään push-toimintoa, jolloin käyttäjän ei tarvitse itse tarkistaa uusia sähköpostejaan. (Lehto 2005.)

Push Email on yleistynyt nimike tekniikalle, joka mahdollistaa sähköpostin vastaanoton mobiililaitteeseen ilman, että kyseessä oleva laite käy hakemassa tai tarkistamassa vastaanotettuja sähköposteja sähköpostipalvelimelta. Mobiililaitteessa oleva asiakasohjelma on näennäisesti valmiustilassa ja tarkistaa yhteyden palvelimeen aika ajoin. Sähköpostin saapuessa palvelin lähettää puhelimeen ainoastaan viestin otsikkotiedon. Kun puhelin vastaanottaa otsikkotiedon, puhelimen asiakasohjelmisto avaa yhteyden palvelimeen ja lataa sähköpostin sisällön. (Microsoft Solution Finder 2008.)

Push Emailin etuja ovat operaattoririippumattomuus, hyvä tietoturvan taso salauksen ansiosta, helppo käyttöönotettavuus, sekä käytön helppous. Ainoa kriteeri palvelun toimivuudelle on Internet-yhteyden saaminen esimerkiksi GRPS- tai

WLAN-yhteydellä. GPRS-yhteys aiheuttaa kuitenkin kuluja erityisesti ulkomailla samalla lyhentäen akun varausta, koska yhteyden ylläpitokin kuluttaa akkua. (Microsoft Solution Finder 2008.)

5.2 Nokia Intellisync Mobile Suite tuoteperhe

Nokia osti yhdysvaltalaisen Intellisync -nimisen yrityksen marraskuun 16. päivä vuonna 2005. Intellisync oli alustariippumattomien langattomien viestintä- ja matkapuhelinsovellusten markkinajohtaja. Yritysoston ansiosta Nokia kohensi yritysratkaisujen kehitys-, käyttöönotto ja hallintaratkaisutarjonnan markkinoiden kattavimmaksi kokonaisuudeksi. Nokian tavoitteena on pyrkiä tarjoamaan asiakkailleen palvelu, jonka avulla yritykset saavat turvallisen pääsyn sähköpostiin. (Nokia Lehdistötiedotteet 2005.)

Intellisync on toimittanut maailmanlaajuisesti eri operaattoriverkkoihin osan suurimmista langattomista sähköpostiratkaisuista, joissa hyödynnetään laajaa laitevalikoimaa ja eri sovellusalustoja. Yritys on yritysmobiliteettisovellusten ja mobiiliiratkaisujen edelläkävijä. Intellisync mahdollistaa teknologiallaan tiedon ja tiedostojen synkronoinnin eri ohjelmistojen välillä täsmällisesti ja turvallisesti. (Nokia Lehdistötiedotteet 2005.)

Intellisync korvasi Nokian aiemmin markkinoilla olleen Nokia Business Centerin. Nokia Business Centerin kehitystoiminta on lopetettu, eikä tuotetta enää markkinoida. Nokia tarjoaa kuitenkin yhä tukea entisille asiakkailleen Nokia Business Centeriä koskevissa asioissa. (Nokia Lehdistötiedotteet 2005.)

Nokia Intellisync Mobile Suiten tuoteperhe koostuu viidestä yksittäisestä osuudesta, joita ovat Wireless Email, Device Management, File Sync, Application Sync ja Call Connect. (Nokia 2008a.)

Nokia Intellisync Wireless Email mahdollistaa sähköposti-, kalenteri-, yhteys- ja muiden tietojen haun johtavilta groupware/sähköpostipalvelimilta, mukaan lukien

Microsoft Exchange ja Lotus Domino. Nokia Intellisync Wireless Email toimii melkein kaikissa mobiililaitteissa, joita ovat Windows Mobile-, Symbian-, BREW- ja Palm OS-pohjaiset laitteet. (Nokia 2008a.)

Nokia Intellisync Device Management -laitehallinnan avulla hallitaan kattavasti ja kustannustehokkaasti mobiiliratkaisuiden käyttöönottoa tehokkaalla ja tietoturvan huomioivalla hallintaratkaisulla. Nokia Intellisync Mobile Suite:n Device Management tukee kaikkia muita älypuhelinalustoja Symbiania lukuun ottamatta. (Nokia 2008a.)

Nokia Intellisync File Sync -tiedostonsynkronointiratkaisu on ratkaisu yrityksen tietojen ja sovellusten tuomiseksi liikkuvien työntekijöiden käyttöön. Työntekijöiden tiedostot synkronisoituvat kämmenlaitteeseen, kannettavaan tietokoneeseen ja pöytätietokoneeseen. (Nokia 2008a.)

Nokia Intellisync Application Sync -ratkaisu on yksinkertaistettu, automaattinen informaation jakelu, päivitys ja haku, joka mahdollistaa koko organisaation pysymisen ajan tasalla yritystietojen ja -dokumenttien suhteen. Ratkaisu on luotettava ja läpinäkyvä loppukäyttäjälle. Application Sync -ratkaisu tarjoaa dokumenttien seurantamahdollisuuden, jolloin valvonnasta ja oikeudellisista seikoista on helpompi huolehtia. (Nokia 2008a.)

Nokia Intellisync Call Connect mahdollistaa Nokia E-sarjan matkapuhelinten siirtämisen VoIP-puheluiksi. VoIP-ratkaisulla voidaan tehostaa puhelimen käyttöä puhelimeen tarjottavilla lisäpalveluilla ja samalla pienennetään matkapuhelinkuluja. (Nokia 2008a.)

KUVIO 6. Nokia Intellisync Mobile Suiten sisältämät osat (Nokia 2007a.)

5.2.1 Intellisync Mobile Suite Wireless Email

Intellisync Mobile Suite:n Wireless Email tarjoaa käyttäjille pääsyn Microsoft Outlook:in tarjoamiin palveluihin matkapuhelimen välityksellä. IMS-palveluun tarjotaan kahdentyyppisiä käyttäjälisenssejä. Base-client tarjoaa rajoituksettoman määrän käyttäjiä, mutta näyttää ainoastaan 3-päivän sähköpostit eikä tarjoa sähköpostin lisäksi muita palveluita. Pro-client tarvitsee erikseen ostetut lisenssit jokaista käyttäjää kohden. (Computerlinks 2008.)

Pro-clientille tarjottavia palveluita ovat sähköpostien, kalenterimerkintöjen ja kontaktitietojen synkronisointi matkapuhelimeen. Ohjelmistosta löytyy myös merkinnät (notes), tehtävät (tasks) sekä matkapalvelu (travel information). Matkapalvelua voidaan hyödyntää Intellisyncissä, jos yritys on tilannut itselleen sitä koskevan palvelun. Palvelun avulla voidaan lähettää käyttäjille esimerkiksi säätietoja kohdealueesta. Lisäksi sovelluksesta löytyy nimihakutoiminto, jonka avulla voidaan hakea yksittäisen henkilön yhteystietoja LDAP-palvelimelta. Tällöin saadaan sel-

ville tietoja haettavasta henkilöstä, kuten puhelinnumero, konttori, titteli sekä osasto johon henkilö kuuluu. Nämä henkilötiedot tulee olla määritelty AD/LDAP:iin. (Computerlinks 2008.)

Lisäksi käyttäjälle voidaan tarjota pääsy verkkolevylle. Verkkolevylle voidaan tallentaa tiedostoja väliaikaisesti ja niiden lataaminen takaisin puhelimeen GPRS-yhteyden avulla. Verkkolevyn käyttö soveltuu hyvin niihin tapauksiin, kun puhelimeen asennetaan uusi versio Intellisync:stä, eikä muunlainen tietojen talteen ottaminen onnistu. Verkkolevyä ei voida hyödyntää puhelimen ohjelmistopäivityksen varmuuskopiointiin. (Computerlinks 2008.)

5.2.2 Intellisync:in järjestelmävaatimukset

Intellisync Mobile Suite (IMS) ja Intellisync Secure Gateway (ISGW) toimivat Microsoft Windows Server-käyttöympäristöissä, joista suositeltavin käyttöjärjestelmä on Windows Server 2003. Ohjelmistoa asennettaessa tulee tietää mihin kaikkeen järjestelmä sidotaan. IMS sisältää sisäinen Sybase:n Adaptive Server Anywhere tietokantatuen, jossa tiedot tallennetaan IMS-palvelimelle. IMS-palvelin voidaan yhdistää myös ulkoiseen tietokantapalvelimeen, joista tuetaan Oracle:n Microsoft:in SQL-tietokantaapalvelimia. Nokia Intellisync Wireless Email ei tue Oraclea. Oraclen tietokantaa voidaan käyttää File Sync, Application Sync tai Device Management palveluun, mutta Wireless Email on tuettu ainoastaan ulkopuoliselle Microsoft SQL-tietokannalle. (Nokia 2007b.)

Tietokanta suositellaan eriytettäväksi IMS-palvelimesta, jos palvelimen käyttäjien lukumäärä kasvaa yli 100 käyttäjään. Eriytetty tietokanta säästää IMS-palvelimen prosessorikuormaa, jolloin se pystyy palvelemaan käyttäjiä tehokkaammin. Käytettävän tietokannan siirtäminen vaatii järjestelmän uudelleenasennuksen, koska ulkoinen tietokanta ei voi olla samantyyppinen kuin sisäinen. Tästä syystä käyttäjämäärä on hyvä arvioida jo etukäteen ja samalla varautua tuleviin muutostarpeisiin. (Nokia 2007b.)

Käyttäjien tunnistamisessa voidaan käyttää järjestelmän paikallisia käyttäjätunnus – salasana -pareja tai ulkoista LDAP-tunnistusta, kuten esimerkiksi Microsoftin Active Directorya. Käytettäessä ulkoisia tunnuksia asennuksessa tulee esittää käyttäjätili, joka voi sitoa (bind) tilejä LDAP-palvelimelta. Tätä tiliä käytetään uusien käyttäjien lisäämiseen Intellisynciin esimerkiksi AD:sta. Tämän tilin muuttaminen jatkossa on mahdollista. Lisäksi asennuksessa tulee esitellä ISGW:n osoite, jos sitä käytetään tässä järjestelmässä. ISGW:n lisääminen jatkossa on myös mahdollista. (Nokia 2007b.)

TAULUKKO 1. Intellisync Mobile Suite palvelimen minimivaatimukset (Nokia 2007b.)

Table 5 Server Minimum Requirements for Nokia Intellisync Mobile Suite

	Nokia Intellisync Mobile Suite	Wireless Email	Device Mgmt	File Sync	RealSync Server	Application Sync
HARDWARE						
Processor	Pentium III 900MHz	•	•	•	•	•
Hard Disk Space	5 GB free disk space	•	•	•	•	•
Memory	1 GB RAM	•	•	•	•	•
SOFTWARE						
Operating System	Windows Server 2000 (SP4) Windows Server 2003 (SP1)	•	•	•	•	•
Browser	IE 6.0 or later	•	•	•	N/A	•
Other	MS TCP/IP Protocol network environment	•	•	•	•	•
	Microsoft Management Console 1.2	•	•	•	•	•
Supported Databases (see the following page for additional information)	SQL Server 2000 (SP3) SQL Server 2005	• Plus: Sybase Adaptive Server Anywhere 9.0.1	• Plus: Oracle 9i Sybase Adaptive Server Anywhere 9.0.1	• Plus: Oracle 9i Sybase Adaptive Server Anywhere 9.0.1	•	• See *Nokia Intellisync Application Sync Certifications List*
OTHER REQUIREMENTS						
Permissions	Local Admin	•	•	•	•	Domain Admin
Open port 443	Open port 443 from IMS server to Internet for communication with the license server	•	•	•	•	•
Latency between IMS server and other backend server, database, or file system	36 milliseconds or less	*	*	*	*	*

• Indicates minimum requirements for Nokia Intellisync Mobile Suite

5.3 OMA Device Manager

5.3.1 OMA – Open Mobile Alliance

Open Mobile Alliance on kansainvälinen organisaatio, joka suunnittelee avointa markkinointipainotteista yhteensopivuusmäärittelyjen globaalia hyväksymistä. OMA perustettiin kesäkuussa vuonna 2002 yhteistyössä johtavien matkapuhelinoperaattoreiden, -laitteiden ja -verkkojen toimittajien, IT-yhtiöiden, sekä sisällön- ja palveluidentarjoajien kesken. (Open Mobile Alliance 2006.)

Device Management Working Group:in päämäärä on määrittää protokollat ja mekanismit, joiden avulla laitteita voidaan hallita. Hallinnan vaatimuksiin sisältyvät mahdollisuudet asetusten määrittämiseen laitteisiin, asennusten ja päivitysten asentaminen laitteisiin, laitteissa olevan hallintatiedon korjaaminen, sekä kyky laitteista luotujen tapahtumien ja virheiden prosessointiin. (Open Mobile Alliance 2008.)

5.3.2 Mobiililaitteiden tietoturvallisuus

Matkapuhelin on tarkoitettu pääosin puheluiden soittamista varten, mutta yhä enemmän älypuhelimet yleistyvät markkinoilla. Älypuhelimia voidaan hyödyntää muuhunkin kuin pelkästään puheluiden soittamiseen, jolloin niistä syntyy useasti huomaamaton tietoturvariski. Matkapuhelimeen tallennetaan usein yrityksen sisäistä tietoa ja salasanoja, joita ulkopuolinen voi hyödyntää omaksi edukseen ja samalla heikentää yrityksen toimintaa.

OMA Device Manager (OMA DM) on Nokian itse kehittämä lisäys Intellisync-tuoteperheeseen, jolla pyritään parantamaan matkapuhelinten tietoturvaa. OMA DM on tarkoitettu ainoastaan Symbian-pohjaisten mobiililaitteiden hallintaan. Intellisync tarjoaa tuen Windows Mobile, Palm, Brew, SmartPhone, PC, Tablet PC alustaisille mobiililaitteille. OMA DM:in kautta Nokian matkapuhelimia voi-

daan etähallita ja määrittää asetuksia lukkoon niin, ettei käyttäjä voi tahallisesti tai tahattomasti heikentää niiden suojausta. (Computerlinks 2006a.)

OMA DM:in avulla työntekijältä varastettu matkapuhelin voidaan lukita tai nollata etänä. Palvelun avulla puhelimeen voidaan asentaa myös ohjelmistoja ja niiden päivityksiä, ilman että käyttäjä pystyy niitä estämään. Käyttäjältä ei kysytä tehtävään vahvistusta, vaan ohjelmat asennetaan puhelimeen huomaamattomasti. (Nokia 2008b.)

OMA DM:in tarjoamat edut vaikuttavat lupaavilta ja tarjoavat uusia näkymiä mobiililaitteiden hyödyntämiseen. Välillä kuitenkin liikutaan tietoturvan harmaalla alueella, koska ohjelma mahdollistaa henkilöiden tekemisten vakoilemisen. Tämän takia etähallittavien puhelinten omistajille tulee tiedottaa, että heidän puhelimen käyttöään voidaan tarkkailla. (Nokia 2008b.)

TAULUKKO 2. Osa OMA DM:in tuetuista laitteista sekä niihin mahdollistetut ominaisuudet (Computerlinks 2006b.)

	E60, E61, E70, E50 S60 3.0 Symbian OS 9.1	9500, 9300, 9300i S80 Symbian OS 7.0	N71, N80, N91 S60 3.0 Symbian OS 9.1	N70, N90, 6630 6680, 6681, 6682 S60 2.x/Symbian OS 8.0
Built-in device features and supported applications				
IAP provisioning, GPRS/WLAN	✓ / ✓ 1)	✓ / ✓ 1)	✓ / ✓ 1)	✓ / -
OMA DM / DS settings	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
VoIP and SIP settings	✓	-	-	-
Bookmarks	✓	✓	✓	✓
Native Email client settings	✓	✓	✓	✓
App. install and settings mgmt - Nokia Business Center - Symantec AV/PFW - Pointsec device encryption - Cisco SCCP	 ✓ ✓ 2) ✓ 2) ✓	 ✓ ✓ 2) ✓ 2) -	 - - - -	 - - - -
Application installation	✓	✓	-	-
Inventory, basic	✓	✓	✓	✓
Corporate Policy (TARM)	✓	-	-	-
Lock and lock settings	✓	-	-	-
Wipe	✓	-	-	-
Application installation	✓	✓	-	-
Extended features				
Inventory, extended	✓	✓	-	-
File transfer	✓	✓	-	-
Connection manager	✓	✓	-	-

1) For WLAN capable devices: E60, E61, E70, 9500, 9300i, N80, N91
2) Depending on availability or 3rd party applications

OMA Device Manager tuo myös näkymän etäkäyttäjän näytöltä hallintaohjelmaan, jolloin puhelimen käyttäjää voidaan opastaa ja samalla seurata miten hänen

puhelimensa käyttäytyy. Tulevassa OMA DM:n versiossa parannetaan puhelimen toimintojen hallintaa, jolloin esimerkiksi digikameran käyttö voidaan estää. (Computerlinks 2006b.)

5.4 Fyysiseen verkkoon tehtävät muutokset

5.4.1 Intellisync:in vaatimat verkkomuutokset

Intellisync vaatii muutamia verkkoresursseja toimiakseen. Vähimmäisvaatimus on yhteys sähköpostipalvelimeen. Tällöin käyttäjien tunnistautuminen tapahtuu IMS-palvelimella. Jos yritykseltä löytyy tunnistautumispalvelin, on sen käyttö suotavaa. Nokia Intellisync ohjelmisto sisältää sekä ISGW- ja IMS-ohjelmistot. Tämän takia ISGW-palvelimen käyttö on suotavaa, jos ISGW-palvelimelle tarvittava laitteisto on helposti saatavilla.

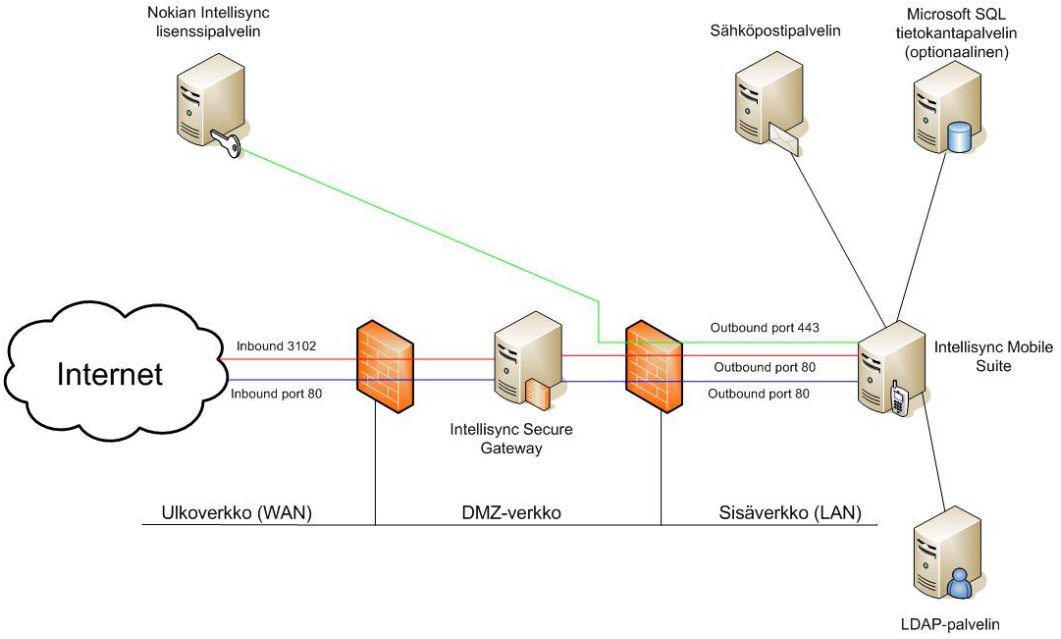
Intellisync voidaan sijoittaa verkkoon usealla eri tavalla. Minimivaatimuksena IMS sijoitetaan joko yrityksen sisäverkkoon tai DMZ-alueelle. Jos IMS sijoitetaan sisäverkkoon, tulee palomuurista sallia yhteydet suoraan IMS palvelimelle. Tämän tyyppinen ratkaisu ei ole suositeltava, koska palvelimelle murtautuneella on pääsy suoraan yrityksen sisäverkkoon. Turvallisempi vaihtoehto on sijoittaa IMS-palvelin DMZ-verkkoon. Tällöin IMS-palvelimelta sallitaan yhteydenotot LDAP- ja sähköpostipalvelimelle. Tämäkään vaihtoehto ei ole tietoturvallinen, koska IMS-palvelimeen voidaan mahdollisesti tunkeutua jonkin tietoturva-aukon avulla ja sieltä voidaan pyrkiä sisään sähköpostipalvelimelle tai LDAP-palvelimelle tai muuten vain häiritä verkkoliikennettä. (Nokia 2007b.)

Turvallisin tapa on käyttää ISGW -palvelinta ulkoverkon ja IMS-palvelimen välillä. Tällöin ISGW sijoitetaan DMZ-verkkoon ja IMS-palvelimelta avataan yhteys ISGW:lle. Palomuuriin tulee avata yhteydet ISGW:lle, joka vastaa yhteyden muodostuksiin. ISGW:n ei sallita muodostaa yhteyksiä ulko- tai sisäverkkoon. Tällä tavoin ISGW toimii eräänlaisena väliporttina IMS-palvelimen ja ulkoverkon välillä. (Nokia 2007b.)

Kun järjestelmässä käytetään ISGW-palvelinta, tarvittava tietoliikenne käyttää ainoastaan kolmea TCP-porttia ulkoverkosta sisäänpäin. Näitä portteja ovat http (80), https (443) ja oma valinnainen portti network push:lle. Network push käyttää oletuksena porttinumeroa 3102, mutta se voidaan uudelleen määrittää suoraan IMS-palvelimen admin consolesta. ISGW liikennöi IMS:in kanssa käyttämällä TCP porttia numero 80. (Nokia 2007b.)

Palomuurissa DMZ- ja LAN-verkon välille tarvitaan sallia ainoastaan TCP 80-porttiliikenne IMS-palvelimelta ISGW:lle. Ulkoverkosta ISGW:lle tulee sallia TCP portit 80, 443 ja 3102 eli push-toiminnolle valittu portti. Tilallinen palomuuri sallii vastauspakettien siirron lähettämisen ennalta muodostettuihin yhteyksiin. (Nokia 2007b.)

ISGW:n käyttöönotto vaikuttaa mobiililaitteiden yhteysasetuksiin niin, että laitteet tulevat muodostamaan yhteydet ISGW:lle IMS:in sijaan. Palvelua käyttävät eivät voi kuitenkaan tietää sitä, joten he olettavat liikennöivänsä IMS:n kanssa vaikka oikeasti ovatkin yhteydessä ISGW:hin. ISGW:n käytön ainoa heikkous on siinä, jos se jostain syystä lakkaa toimimasta. Kun ISGW ei toimi, niin Intellisync ei pysty palvelemaan asiakkaitaan. ISGW:n tilaa tulee käytännössä tarkkailtua harvoin, joten sen toimimattomuus jää helposti huomaamatta. (Nokia 2007b.)



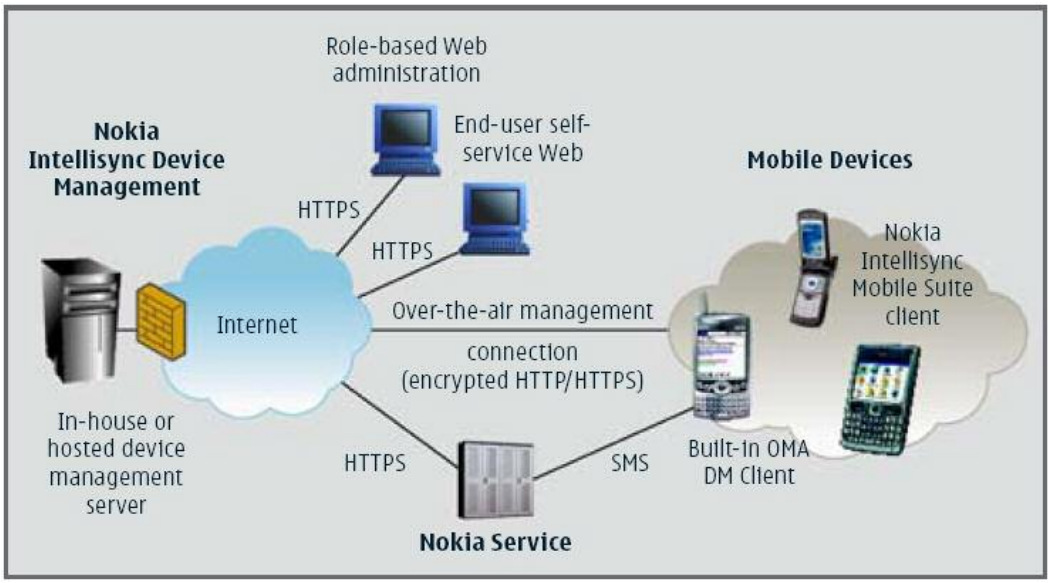
KUVIO 7. Verkkokuva Intellisync-ratkaisusta Secure Gatewayn kanssa (Nokia 2007b.)

KUVIOssa 7 sininen viiva kuvaa data-liikennettä, punainen viiva push-liikennettä ja vihreä viiva Intellisync Mobile Suiten yhteyttä Nokian lisenssipalvelimelle. Kun uusia käyttäjiä lisätään IMS-palvelimelle, palvelin tarkistaa että vapaita lisenssejä löytyy lisenssipalvelimelta. Jos lisenssipalvelin vastaa kyselyyn kieltävästi eli ostetut lisenssit ovat loppuneet, käyttäjän lisääminen peruutetaan ja ilmoitetaan syyksi lisenssien loppumista.

5.4.2 OMA Device Managerin vaatimat verkkomuutokset

OMA DM:n verkko vaatii vähemmän suunnittelua kuin Intellisync-verkon perustaminen. OMA DM sijoitetaan DMZ-verkkoon, josta TCP portin 443 liikenne tulee sallia ans1.nokia.com ja ans2.nokia.com palvelimille. Nokian ans1- ja ans2 -palvelimet luovat järjestelmälle tarvittavan tekstiviestipalvelun. Matkapuhelinverkon välityksellä voidaan lähettää hallinnoitaviin puhelimiin tekstiviestejä, jotka käskevät puhelinta muodostamaan yhteyden OMA Device Manager -palvelimelle. (Nokia 2007c.)

Ulkoverkkoon tulee OMA DM:lle avata TCP portit 80 ja 443. Sisäverkosta palvelimelle avattavia portteja ovat etähallinta ja tarvittaessa LDAP-autentikointi. (Nokia 2007c.)



KUVIO 8. OMA Device Managerin verkkokuva (Nokia 2007c.)

6 MATKAPUHELINJÄRJESTELMÄN HYÖDYNTÄMINEN

6.1 Järjestelmän tavoitteet

Puhelimia unohdetaan ja niitä varastetaan yllättävän paljon maailmanlaajuisesti. Suomessa pääkaupunkiseudulla tutkimukseen osallistuneisiin takseihin unohdettiin puolen vuoden aikana noin 3600 matkapuhelinta, 110 kämmenmikroa ja 50 kannettavaa tietokonetta. Pääkaupunkiseudun asukit lukeutuvat tuhansista kadotetuista laitteista huolimatta tutkimuksen maltillisempiin hukkaajiin: esimerkiksi Kööpenhaminassa takseihin unohdettiin vastaavana aikana lähes 12 000 matkapuhelinta. Lontoossa takseihin jäi jopa yli 60 000 puhelinta ja 5000 kannettavaa tietokonetta puolen vuoden aikana. (Karvonen 2005.)

Tutkimuksen luvut ovat hälyttäviä sikäli, että vuonna 2001 tehtyyn tutkimukseen verrattuna esimerkiksi Lontoossa kadotettiin yli 70 prosenttia enemmän kannettavia tietokoneita ja 350 prosenttia enemmän kämmenmikroja kuin kolme vuotta sitten. (Kotilainen 2005.)

Andritz Oy:n päämäärä on ottaa käyttöönsä sähköpostijärjestelmä, joka palvelee yrityksen omia työntekijöitä ja sijaitsee yrityksen sisäisissä tiloissa. Järjestelmä tulee olla yrityksen omassa hallinnassa, jolloin ulkopuolisilla ei ole pääsyä yrityksen sisäiseen verkkoon. Tällöin järjestelmän ylläpito toimii ilman tarpeetonta viivettä, koska järjestelmästä vastataan yrityksen sisällä. Vikatilanteet saadaan korjatuksi nopeasti, koska järjestelmän osat ja niiden sijainti tunnetaan.

Matkapuhelinjärjestelmältä ei vaadita lisäominaisuuksia, koska tarjottavat lisäominaisuudet eivät tue yrityksen toimintaa. Tarjolla olevista lisäominaisuuksista voidaan hyödyntää muita osuuksia tulevaisuudessa, jos niille löydetään tarvetta. Nokian tarjoaman järjestelmän osa-alueet maksavat ja täten niiden hankinta on turhaa, koska muille osa-alueille ei ole tällä hetkellä käyttötarvetta.

Andritz Oy:llä on kokemusta Nokia Business Centeristä (NBC), joka on Nokian vanhempi mobiili-email-järjestelmä. NBC:llä saatiin välitettyä sähköpostit suojatusti kommunikaattoreihin. Kanadalainen yritys RIM (Research In Motion) on julkaissut NBC:iä vastaavan mobiili-email-järjestelmän, joka tukee BlackBerry-älypuhelimia, sekä myös muita matkapuhelimia BlackBerry Connect -ohjelmiston avulla.

BlackBerry on Yhdysvalloissa suosittu älypuhelinmerkki, joka valmistaa kämmentietokoneita. BlackBerry:n mobiili-email järjestelmä vaatii BlackBerry Enterprise Solution:in asentamista yrityksen tiloihin.

Nokian tietoturvallinen ratkaisu antoi paljon painoarvoa uutta järjestelmää suunniteltaessa, koska RIM BlackBerry -sähköpostijärjestelmän on todettu sisältävän tietoturva-aukkoja. Lisäksi käyttäjälisenssien siirtäminen NBC:stä Intellisync Mobile Suite:n Wireless Email -järjestelmään tarjosi aihetta siirtyä uuteen järjestelmään. Nokian tarjoama ratkaisu tukee BlackBerry-älypuhelimia sekä myös muita puhelinmerkkejä, jolloin järjestelmä soveltuu laajaan käyttöön.

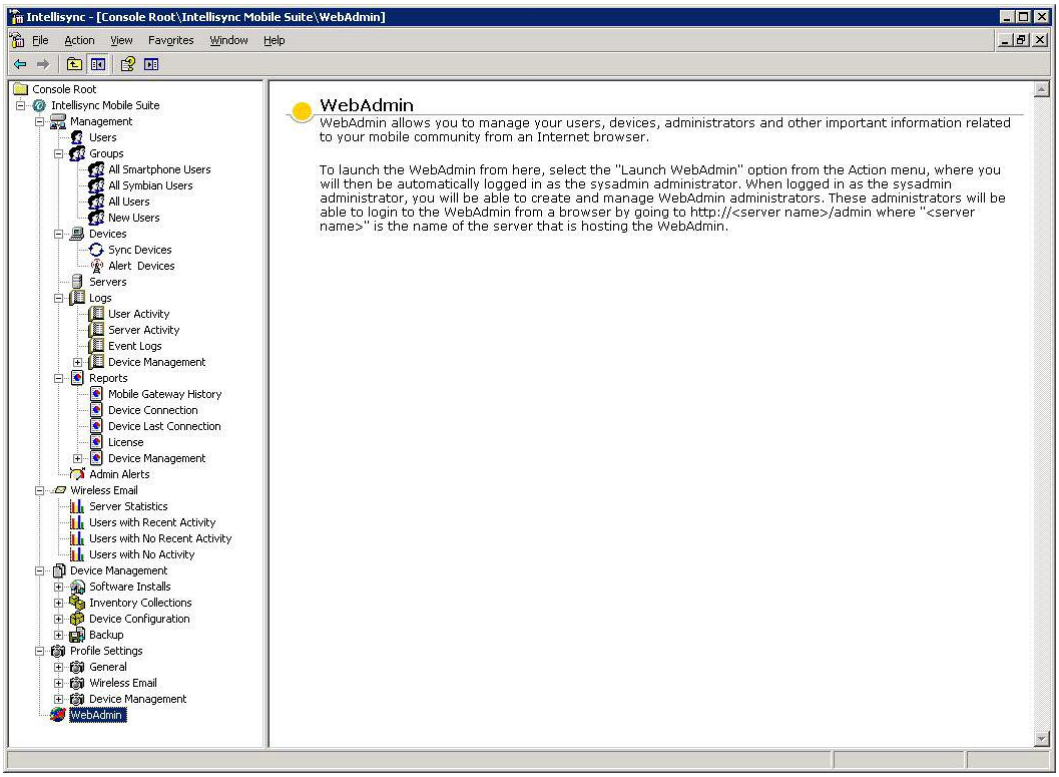
Järjestelmää varten tulee laatia selvät säännöt, joiden mukaan uusia matkapuhelimia ostetaan, asetuksia muokataan ja puhelinta käytetään ilman tietoturvauhkia. Järjestelmän laajennettavuus tulee huomioida ja sen toiminnallisuutta tulee tarkkailla. Matkapuhelinjärjestelmää käyttäville henkilöille tulee tarjota tukea ja jakaa tukipalvelut henkilöstön kesken.

6.2 Järjestelmän käyttöönotto

6.2.1 IMS Wireless Email:in yhteydenmuodostus

Kun palvelimelle asennetut ohjelmistot on asennettu ja palvelimet on sijoitettu verkkoon, tulee varmistaa IMS-palvelimen yhteys LDAP-palvelimelle sekä sähköpostipalvelimelle. Yhteyksien viive voidaan tarkistaa IMS-palvelimen Admin Consolesta löytyvästä WebAdmin-sivulta.

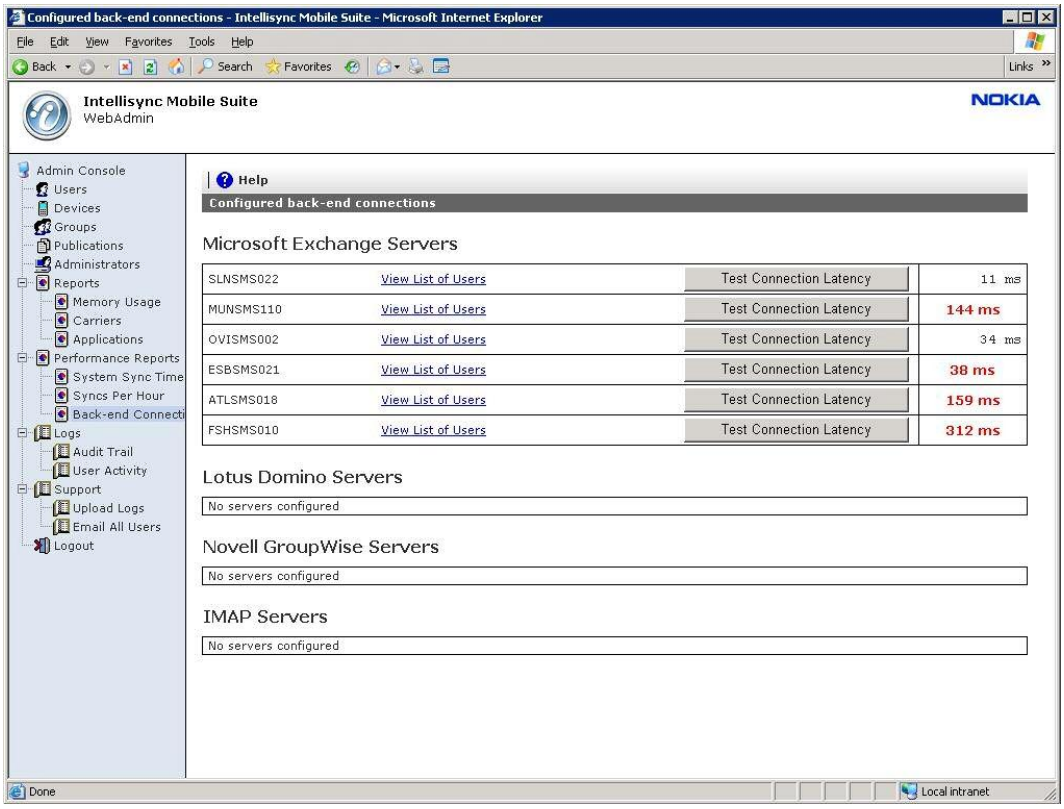
WebAdmin-sivun Back-end Connection -valikosta voidaan mitata viive IMS- ja sähköpostipalvelinten väliltä. Viiveen voi tarkistaa myös komentokehotteesta ping-komennolla. On kuitenkin muistettava, että kohdepalvelin on voitu estää vastaamasta ping-kyselyihin.



KUVIO 9. IMS-palvelimen Admin Console

Nokian suositus viiveestä on alle 36 ms, mutta järjestelmä voi toimia vielä 300 ms viiveelläkin. Liian suuri viive aiheuttaa kuitenkin erinäisiä ongelmia ja virheitä matkapuhelimien synkronoinnissa. Viiveen pienentäminen on mahdollista käyttämällä nopeampia tietoliikenneyhteyksiä tai lyhentämällä IMS- ja sähköpostipalvelimen välistä matkaa. Jos yritysverkossa käytetään useampia sähköpostipalvelimia, voidaan useampia IMS-palvelimia ottaa käyttöön. Useamman IMS-palvelimen käyttö tarvitsee toimiakseen ISGW-palvelimen, johon IMS-palvelimet ovat yhteydessä. Usean IMS-palvelimelle on tarvetta, jos yrityksen sähköpostipalvelimia on eri mantereilla.

IMS-palvelimelle kerääntyy nopeasti uusia käyttäjiä, koska useat käyttäjät ovat halukkaita kokeilemaan palvelun tarjoamia etuja. Kun käyttäjätilejä lisätään ja käyttäjät muokkaavat henkilökohtaisia asetuksiaan, varmuuskopioita olisi hyvä ottaa lähes viikoittain.



KUVIO 10. WebAdmin-sivuston Back-end Connection valikko

Itse Intellisync-järjestelmästä varmuuskopion ottaminen on helppoa. Jos Intellisync käyttää sisäistä Sybase-käyttäjätietokantaa, varmuuskopion ottaminen ei ole kuitenkaan niin helppoa, koska Intellisync varaa tietokannan itselleen eikä siitä tällöin saada varmuuskopiota. Helpoin ratkaisu varmuuskopioiden ottamiseen on käyttää ulkoista tietokantaa, jolloin tietokannan varmuuskopiot sisältävät myös tietokanta-palvelimesta otettavat varmuuskopioihin. Jos ulkoista tietokantaa ei käytetä, tulee IMS-palvelimelta sammuttaa Intellisync Mobile Suite ja Adaptive Server Anywhere – MOBILE palvelut. Kun palvelut on sammutettu, voidaan kopioida koko Intellisync Mobile Suite -asennuskansio talteen. Kun asennuskansio

on kopioitu, käynnistetään IMS-palvelimelta sammutetut palvelut käänteisessä järjestyksessä.

6.2.2 Intellisync Secure Gateway:n käyttöönotto

ISGW-palvelimeen asennetaan ainoastaan Intellisync Secure Gateway -ohjelmisto Windows käyttöjärjestelmän lisäksi. Secure Gateway -ohjelmiston asentamiseen tarvitaan ainoastaan palvelimen paikalliset järjestelmänvalvoja-tunnukset. IMS-palvelin muodostaa uloslähtevän http-yhteyden ISGW:n porttiin 80. Tämä uloslähtevä yhteys ohjaa synkrointiliikenteen ISGW:ltä IMS-palvelimelle ja samalla pienentää verkon riskiä haavoittua. Mobiililaite kommunikoi suoraan ISGW:n porttiin 80. Vastaanotettaessa sisään tulevaa synkronointiliikennettä tarkistetaan liikenteen yhdenmukaisuus ja paikkansapitävyys, jonka jälkeen liikenne reititetään IMS-palvelimelle.

Kaikki yhteydet mobiililaitteen ja IMS-palvelimen välillä vaativat tunnistautumisen, joka suojataan oletusarvoisesti 128-bittisellä AES-salauksella. Kaikki ISGW:lle tuleva liikenne tarkastetaan. Tarkistuksen avulla varmistetaan, että liikenne vastaa odotettua formaattia. Formaatista eroavat paketit hylätään ja ainoastaan sallitut paketit käsitellään ISGW:llä ja ohjataan IMS-palvelimelle.

6.2.3 Intellisyncin käyttöönotto ja laitevaatimukset älypuhelimissa

Intellisync Mobile Suite asennetaan älypuhelimeen siihen sopivalla asennuspaketilla. Asennuspaketit luodaan halutuille älypuhelinalustoille IMS-palvelimen Admin Consolesta. Intellisync-ohjelmistopaketti asennetaan puhelinmerkille sopivalla tavalla. Nokian älypuhelimiin asennuspaketin voi ladata verkon kautta tai käyttää Nokia PC Suite-ohjelmistoa paketin asentamiseen tietokoneelta. Intellisync-ohjelmisto ei tarvitse paljoa suoritustehoa älypuhelimesta ja tästä johtuen se toimii sujuvasti vanhimmissa älypuhelimissa.

TAULUKKO 3. Intelisync Mobile Suiten minimilaitevaatimukset älypuhelimelta (Nokia 2007b)

Table 4 Client Minimum Requirements for Nokia Intellisync Mobile Suite

	PC Client	Pocket PC Client	SmartPhone	Palm OS Client	Symbian
HARDWARE					
Processor Type	Pentium	Supported processor type: ARM - XScale			
Hard Disk Space	64 MB				
Memory	64 MB RAM	32 MB RAM	32 MB RAM	8 MB RAM	32 MB RAM
SOFTWARE					
Operating System	• Windows Server 2000 • Windows Server 2003 • Windows XP	• Microsoft Windows Mobile Pocket PC 2003 and 2003SE • Windows Mobile 5.0	• Microsoft Windows Mobile Pocket PC 2003 and 2003SE • Windows Mobile 5.0	Palm OS 4.0 up to 5.4	• Symbian OS 7.0 • Symbian OS 8.0 • Symbian OS 9.1 (specifically for E61 S60 3rd Edition)
Browser	Microsoft Internet Explorer 6.0 or later				
Other	Microsoft TCP/IP protocol network environment	ActiveSync 4.1 or later (on desktop or laptop)	ActiveSync 4.1 or later (on desktop or laptop)	HotSync 6.0.1 or later (on desktop or laptop)	Symbian 2nd Ed: UIQ, S60, S80 Symbian 3rd Ed: E61 S60, UIQ

6.2.4 OMA DM:n käyttöönotto

OMA DM 8.5 vaatii käyttöjärjestelmäkseen Linuxin. Linux-julkaisuista RedHat on ainoa tuettu vaihtoehto. Asennus ei vaadi graafista käyttöliittymää (X), mutta ohjelmiston asennus helpottuu graafisella puolella. Graafinen puoli ei vaadi asennuksessa eritysosaamista RedHat:istä, toisin kuin konsolipuolen asennus. Asennettaessa OMA DM konsolista, tulee käyttäjän tietää käyttöjärjestelmänsä hakemistopolut ja peruskomennot. Edellinen versio OMA DM:stä 2.04 voitiin asentaa myös Windows 2003 Serveriin.

Kun OMA DM otetaan käyttöön ensimmäistä kertaa, järjestelmänvalvojan tulee suunnitella tulevaisuutta koskeva konsepti, jota puhelimet tulevat seuraamaan. Ensimmäinen tärkeä asia OMA Device Managerista on tehtävien toiminnallisuus.

OMA DM 2.0.4 versiossa luodaan tehtäviä (tasks), jotka tekevät puhelimessa määrätynlaisen toiminnallisuuden. Nämä tehtävät ovat aktiivisia, eivätkä ole kertaluontoisia. Aktiivisuudella tarkoitetaan sitä, että kun tehtävän avulla

taluontoisia. Aktiivisuudella tarkoitetaan sitä, että kun tehtävän avulla asennettu ohjelma on suoritettu loppuun, tehtävä jää silti käyttäjän tietoihin. Jos tehtävän avulla asennettu ohjelma poistetaan puhelimesta, OMA DM suorittaa tehtävän uudestaan ja uudelleen asentaa ohjelman matkapuhelimeen. OMA DM:in avulla voidaan varmistua siitä, että puhelimen ohjelmistot säilyvät puhelimissa. OMA DM 8.5:ssä luodaan julkaisu (publication) joka sisältää toimintoja (actions). OMA DM 8.5:n toiminnot vastaavat OMA DM 2.0.4:n tehtäviä.

Koska tehtävät toimivat vastaavalla tavalla, niitä ei tule poistattaa käyttäjiltä. Tehtävien hallinnointi tapahtuu ryhmien avulla. Käyttäjäryhmään asetetaan halutut tehtävät ja kun käyttäjä lisätään kyseiseen ryhmään, käyttäjä saa tehtävikseen ryhmälle asetetut tehtävät. Kun käyttäjätilejä luodaan järjestelmään, heille tulee syöttää vähintään nimi, lyhyt tunnus ja puhelinnumero. Näiden tietojen avulla käyttäjät yksilöidään toisistaan.

Puhelimeen tulee suorittaa kaksi toimintoa, ennen kuin puhelimeen voidaan lähettää tehtäviä. Ensimmäinen toiminto on lähettää puhelimeen sertifikaatti. Sertifikaatin avulla luodaan puhelimen ja OMA DM -palvelimen välille luottosuhde. Ilman luottosuhdetta matkapuhelin ei luota lähteeseen, eikä suorita sille määritettyjä käskyjä. Toinen toiminto on asentaa puhelimeen DM-profiili. DM-profiili yksilöi puhelimen, jolloin puhelin voidaan erottaa muista puhelimista. DM-profiilin avulla puhelinta voidaan etähallita, vaikka puhelimen SIM-kortti vaihdettaisiin.

Matkapuhelin voidaan ottaa etähallittaviksi ajamalla siihen kolme tehtävää. Ensimmäinen tehtävä mahdollistaa puhelimeen lähetettävien ohjelmien asennuksen. Asennus kysyy varmistusta käyttäjältä, joten toisena lähetettävä tehtävä poistaa käyttäjältä varmistamisen. Kolmannella tehtävällä lukitaan edellä tehdyt asetukset, jolloin käyttäjä ei voi poistaa OMA DM:in oikeuksia.

Nokian Intellisync tukee usean tyyppisiä älypuhelimia aina Nokian malleista muiden puhelinvalmistajien malleihin. Tuettujen puhelinten määrä on todella laaja,

mutta rajaamalla käytettävien puhelinmerkkien ja -mallien määrää pienemmäksi, saadaan ohjeistuksesta yhtenevä ja vähennetään yrityksen IT-tuen tarvetta.

Tuettavaksi matkapuhelinmerkiksi valittiin Nokia, koska yrityksellä on jo ennestään ollut Nokian matkapuhelimia käytössä. On myös todennäköistä, että Nokian sovellukset toimivat parhaiten Nokian valmistamissa tuotteissa. Nokialta löytyy eri tuoteperheitä, jotka on suunnattu määrättyihin käyttötarpeisiin. Näistä yleisimpiä ovat N-sarja ja E-sarja. Matkapuhelinjärjestelmään valittiin Nokia E-sarjan puhelimet, koska E-sarja on suunnattu yrityskäyttöön.

Nokian E-sarja puhelimissa on valmiina pdf-, doc- ja xls-lukijat, eli yleisimmät tiedostoformaatit voidaan avata. Puhelimiin tullaan asentamaan Intellisync ja OMA Device Manager, joiden lisäksi F-secure tullaan asentamaan uusiin älypuhelimiin. F-secure suojaa puhelimissa GSM- ja Bluetooth-verkoissa liikkuvilta viruksilta ja madoilta.

6.2.5 Järjestelmän muokkaaminen yrityksen tarpeiden mukaiseksi

Puhelimen omistaja ei yleensä huomaa unohtamaansa tai häneltä varastettua puhelinta kovinkaan nopeasti. Tämän takia varkaalla on mahdollisuus tehdä useita asioita matkapuhelimelle, ennen kuin työntekijä edes ilmoittaa kadonneesta puhelimesta. Puhelinta tulisi pyrkiä suojaamaan jo ennalta, ennen kuin mitään haitallista on vielä ehtinyt tapahtua. Helpoin tapa estää pääsy tekstiviesteihin ja muihin salattaviin tietoihin on lukita puhelin. Tavallinen näppäinlukko ei suojaa varkaudelta, mutta puhelimeen asetettava automaattilukitus suojaa puhelinta ulkopuolisilta. Suojakoodin tulee olla vähintään 4 merkkiä pitkä ja ilman tätä suojakoodia puhelimen lukitusta ei saa auki. Tällöin puhelimen sisältämiin tietoihin ei voida päästä käsiksi.

Puhelinten suojaustasoa parannettiin kolmella tapaa. Ensimmäiseksi puhelimet asetettiin vakioasetuksille, jotka vastasivat yrityksen tietoturvapolitiikkaa. Näitä

asetuksia ovat muun muassa puhelimen käyttökieli ja ulkopuolisten SIM-korttien käyttökielto. Matkapuhelin lukittuu, jos siihen asenetaan toinen SIM-kortti.

Vakioasetusten jälkeen puhelimeen asennetaan yrityksessä käytettävät ohjelmistot puhelimen sisäiseen muistiin. Ohjelmistoja ei asenneta puhelimen muistikortille, koska muistikortille tallennettujen tietojen suojaus voidaan mahdollisesti murtaa käyttämällä tietokoneisiin saatavia salauksenmurto-ohjelmia.

Ensimmäinen ohjelmisto on Nokia Intellisync:in Wireless Email, jolla tarjotaan käyttäjälle mahdollisuus lähettää ja vastaanottaa sähköpostia, sekä seurata kalenteria ja hallita muita tehtäviä. Toinen ohjelmisto on OMA Device Manager, joka mahdollistaa puhelimen etähallinnan.

OMA Device Managerin yksi tärkeä tehtävä on asettaa puhelimen automaattilukitus päälle. Asetus on pysyvä, eikä asetusta voida poistaa käytöstä. Suojakoodin kysely ei suojaa puhelinta, ellei se ensiksi lukkiudu. Tämän takia OMA DM:ssa luotuun tehtävään asetetaan automaattilukituksen intervalliksi 15 minuuttia. Puhelimen käyttäjällä on mahdollisuus lyhentää lukitusaikaa, mutta lukitusajan pidentäminen yli 15 minuuttiin ei ole sallittu.

Lopuksi matkapuhelimeen asennetaan F-secure:n virustorjuntaohjelmisto. Virustorjuntaohjelmisto suojaa matkapuhelinta verkossa leviäviltä madoilta ja viruksilta. F-secure:n virustorjuntaohjelmisto päivittyy automaattisesti verkon kautta, jolloin puhelimien virusturvan oletetaan pysyvän ajan tasalla.

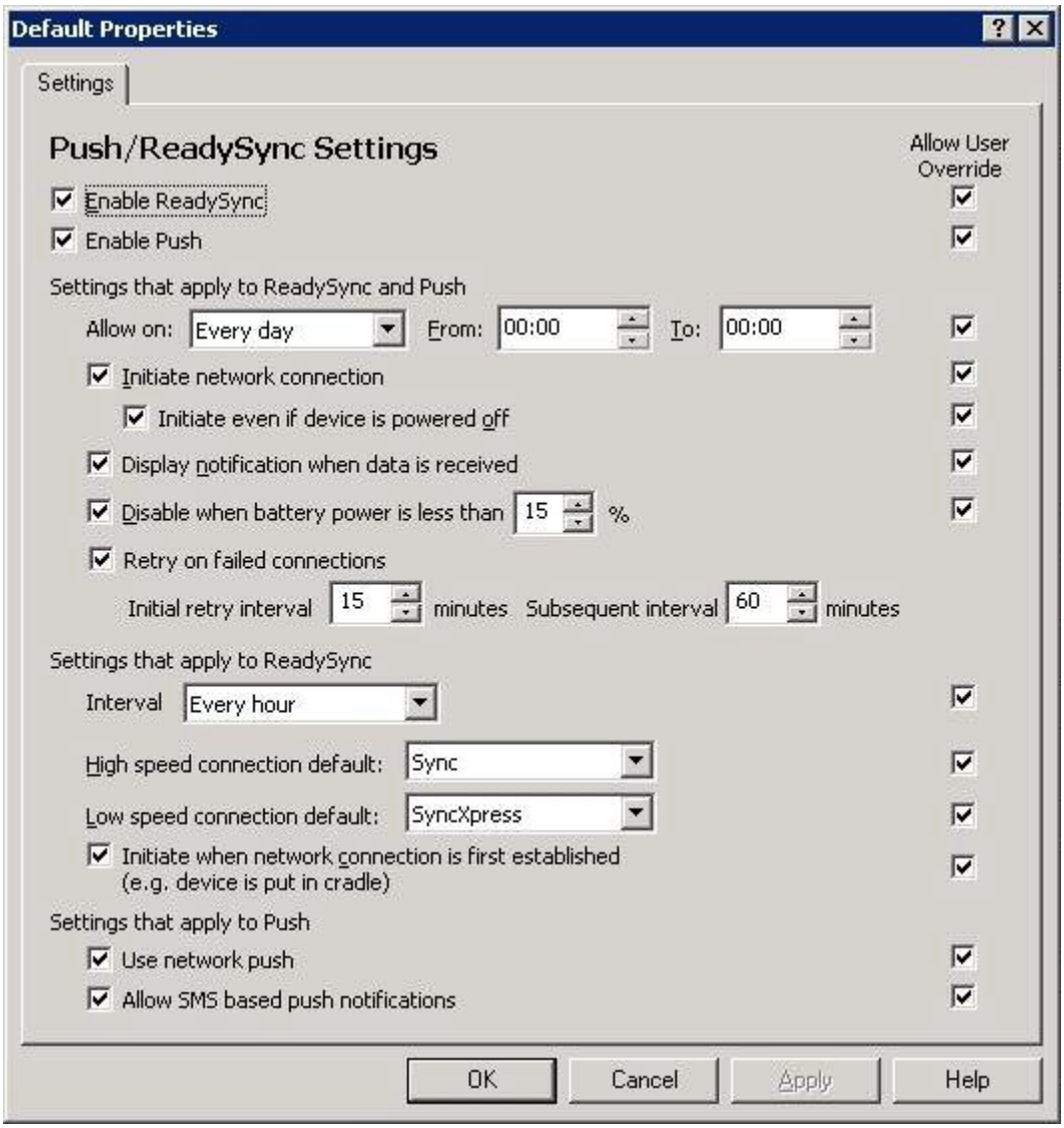
6.3 Järjestelmässä esiintyneet ongelmat

Käyttäjien ohjeistaminen ohjelmiston käyttöön osoittautui oletettua vaikeammaksi, koska käyttäjien osaamisen taso vaihtelee suuresti yrityksen sisällä. Käyttäjille on hyvä tarjota koulutusta puhelimen ja siinä olevan ohjelmiston käyttöön. Koulutuksen lisäksi käyttäjille on tärkeätä jakaa koulutusta koskevat ohjeet, jolloin ongelmatilanteissa käyttäjä pystyy etsimään apua jaetuista ohjeista.

Ajoittain ongelmia syntyy myös älypuhelimien takia. Yrityskäytössä olevia matkapuhelimia sammutetaan melko harvoin ja tämän takia puhelimet ovat usein päällä viikkoja. Kun matkapuhelimen muisti alkaa loppua kesken, syntyy erikoisia ongelmia. Nokian älypuhelimet saattavat lakata joko osittain tai kokonaan toimimasta. Useimmissa tapauksissa ongelmasta selvitään, kun puhelin sammutetaan ja sen sisältämä akku irrotetaan puhelimesta muutamaksi minuutiksi ennen puhelimen uudelleenkäynnistystä.

Älypuhelinten akun kesto lyheni noin 20 – 50 % järjestelmää käyttäneillä henkilöillä. Useat järjestelmässä mukana olleet henkilöt olivat tottuneet lataamaan puhelintaan kerran viikossa, mutta järjestelmän toimiessa puhelimen akku kesti ainoastaan muutamia päiviä. Akun kulutus johtuu siitä, että puhelin on koko ajan yhteydessä IMS-palvelimeen. Puhelimen ollessa online-tilassa, yhteyden tila varmistetaan lähettämällä kysely puhelimesta IMS-palvelimelle noin 10 minuutin välein. Jos puhelin vastaanottaa kyselyynsä vastauksen IMS-palvelimelta, voidaan olettaa, että yhteys puhelimen ja IMS-palvelimen välillä toimii. Akun varaus laskee nopeasti, jos käyttäjä vastaanottaa paljon sähköpostia, jolloin puhelin lataa tietoa lähes jatkuvasti GPRS-yhteyden avulla.

Akun kestoa pyrittiin parantamaan muokkaamalla synkronisointiin liittyviä asetuksia. IMS-palvelimen asetuksista poistettiin ajoitettu synkronisointi käytöstä. Tällöin puhelin käyttää Push-tekniikkaa apunaan ja synkronoituu aina sähköpostia lähettäessä ja vastaanottaessa. Samalla käyttäjiä ohjastettiin sulkemaan Intellisync-sovellus ajalta, jolloin he eivät lukisi sähköpostiaan.



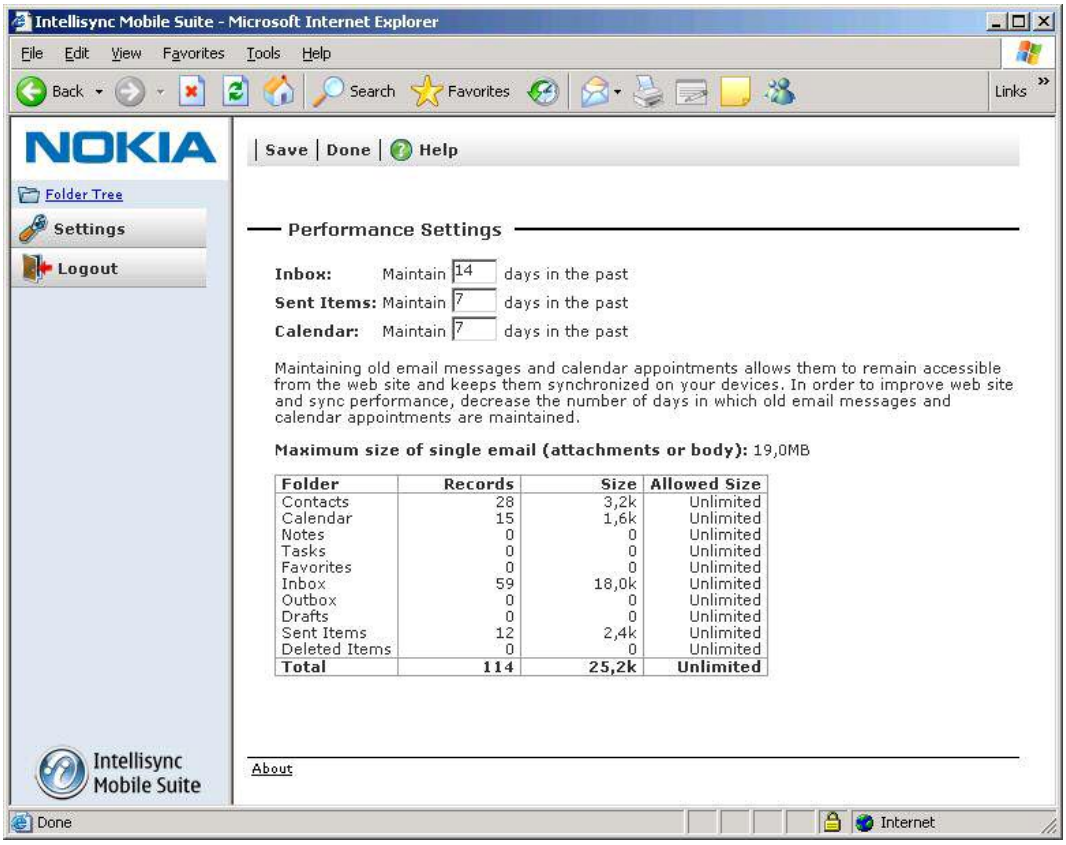
KUVIO 11. IMS Wireless Email -palvelimen Push ja ReadySync asetukset

Osa järjestelmän käyttäjistä kiertää maailmaa ja heidän tärkein työkalunsa on ajan hallinta kalenterin avulla. Kalenteria seuraaville henkilöille on tärkeää, että kalenterimerkinnät pysyvät ajan tasalla. Kyseisille henkilöille sähköpostin lähettäminen ja vastaanottaminen on toissijainen asia. Kalenteria seuraavat henkilöt eivät hyödy push-toiminnosta, koska he pyrkivät pitämään ainoastaan kalenterimerkinnät ajan tasalla Intellisync-järjestelmässä.

Jos käyttäjä tekee Outlookiin kalenterimerkinnän seuraavalle aamulle, mutta ei vastaanota sähköpostia ennen seuraavaa päivää, puhelimeen ei synkronoidu kalen-

terimerkintää ja puhelin ei muistuta kalenterimerkinnästä. Välttääkseen kyseistä tilannetta ReadySync tulee asettaa takaisin päälle.

Viive aiheuttaa ongelmia järjestelmän toimintaan. Viiveestä johtuvien ongelmien ratkaiseminen vaati useasti pidempiaikaisia testejä. Ylipitkän viiveen takia älypuhelimiin saadaan haettua kontakteja ja henkilöhaku-toimintoa voidaan käyttää, mutta sähköpostien nouto ei onnistu. Epäonnistuminen sähköpostien siirtoon johtuu liian pitkästä aikavälistä, koska palvelin voi palvella yhtä puhelinta ainoastaan sille määritetyn aikavälin ajan. Pienentämällä synkronoitavan tiedon määrää järjestelmä saadaan toimimaan liian pitkällä viiveelläkin. Synkronoitavaa tietoa pienennetään vähentämällä synkronoitavien päivien määrää käyttäjäkohtaiselta Intellisync Mobile Suite web -sivulta. Web-sivulle kirjautuminen tapahtuu muodostamalla yhteys IMS- tai ISGW-palvelimen verkko-osoitteeseen, riippuen käytettävästä matkapuhelinjärjestelystä.



KUVIO 12. Käyttäjäkohtaiset synkronointiasetukset

7 YHTEENVETO JA POHDINTAA

Nokian tarjoama ratkaisu mobiililaitteille tarjoaa yrityksille laajan kokonaisuuden, jonka avulla mobiililaitteita voidaan käyttää tehokkaammin, tietoturvallisemmin ja järjestelmän avulla voidaan luoda säästöjä. Intellisync-ympäristön selviä etuja ovat tiedon saatavuuden parantuminen, sekä laaja tuki älypuhelimille.

Andritz Oy:llä on kokemusta Nokia Business Centeristä (NBC), joka on Nokian vanhempi mobiili-email-järjestelmä. NBC:llä saatiin välitettyä sähköpostit suojatusti kommunikaattoreihin. Nokia vaihtoi vanhat NBC Professional clientit Intellisync Mobile Suite:n Wireless Email clientteihin, jolloin yksi vanha NBC Professional client vastaa yhtä Intellisync Mobile Suite:n Wireless Email clienttiä. Toinen syy Nokia Intellisync-järjestelmän käyttöönotolle on yrityksessä käytettävien Nokia-merkkisten älypuhelinten määrä. Voidaan olettaa, että Nokian kehittämä järjestelmä toimii varmemmin Nokian älypuhelimilla.

Nokia Intellisync Mobile Suite Wireless Email vapauttaa käyttäjänsä työkoneen äärestä ja mahdollistaa työskentelyn lähes kaikkialta. OMA Device Manager parantaa älypuhelinten tietoturvaa usealta osalta, mutta puhelimen sisältö jää yhä suojaamatta. Mobiililaitteiden kryptaukseen erikoistunut Pointsec tarjoaa palvelua, jolla älypuhelinten sisältö voidaan salata. Nokian Intellisync-ympäristö tukee Pointsecin ratkaisua, mutta ei ainakaan vielä tarjoa omaa salausratkaisua älypuhelimiin.

Työn tavoitteena on esitellä yrityskäyttöön tarkoitetun älypuhelimille suunnatun järjestelmän käyttöönotto ja sen mahdollistamat hyödyt. Järjestelmä perustuu Nokia Intellisync Mobile Suite -tuoteperheeseen, jonka Wireless Email ja OMA Device Manager tulevat yrityksen käyttöön. Lisäksi tavoitteena on luoda yritykselle valmis konsepti, jota seuraamalla uusia matkapuhelimia otetaan yrityksessä käyttöön sekä kehittää ja määrittää parhaimmat tavat joiden avulla tuotetta voidaan hyödyntää yrityksen eduksi.

Järjestelmän käyttöönotto sisältää neljä työvaihetta. Ensimmäisessä työvaiheessa järjestelmä asennetaan palvelimille, avataan järjestelmää koskevat tietoliikenneyhteydet ja muokataan ohjelmiston asetukset yrityksen infrastruktuurin mukaiseksi. Toisessa työvaiheessa muokataan IMS-palvelimen käyttäjäkohtaiset asetukset ja luodaan OMA Device Manager:iin tehtävät, joiden avulla älypuhelimet voidaan lisätä keskitettyyn hallintaan, sekä samalla pakotetaan puhelinten asetukset yrityksen määritysten mukaisiksi. Kolmannessa vaiheessa puhelimiin asennetaan Intellisync- ja OMA DM-ohjelmistot, sekä F-secure:n virustorjunta. Lopuksi järjestelmästä tarjotaan koulutusta ja tukea loppukäyttäjille.

Järjestelmän käyttöönotto on hyödyksi yritykselle. Intellisync Wireless Email tarjoaa käyttäjille mahdollisuuden työskennellä missä tahansa päin maailmaa. Tällöin älypuhelimella voidaan hallita sähköpostit, ajanhallinta sekä puhelut. Sähköpostipalvelun avulla käyttäjät voivat säästää puhelinlaskun suuruudessa, koska osa asioista on selvempi selittää kuvin kuin sanoin. OMA Device Manager:in avulla älypuhelinten asetukset voidaan määrittää yrityksen käytäntöjen mukaisiksi, puhelimiin voidaan asentaa ohjelmia ja päivityksiä käyttäjää häiritsemättä ja puhelin voidaan lukita tai sen sisältö tyhjentää hätätilanteessa. F-secure:n avulla varmistetaan puhelinten suojaaminen verkoissa leviäviä viruksia ja matoja vastaan.

Työssä onnistuttiin hyvin ja järjestelmästä saatiin toimiva ratkaisu. Järjestelmänhallinta on jaettu vastuualueisiin, joita hoitavat eri työntekijät. Järjestelmää koskeva koulutus on jäänyt vähäiseksi, mutta tulevaisuudessa sitä tullaan parantamaan.

Järjestelmän ylläpitäminen ei tarvitse kokopäiväistä työtä, mutta ongelmatapauksissa järjestelmää hallinnoivan tulee ymmärtää koko järjestelmän toimintamekanismit. Järjestelmän virheilmoitukset kertovat ajoittain hyvin selkeästi mistä ongelma johtuu, mutta usein virheilmoitukset eivät selvennä lainkaan syytä ongelmaan. Virheilmoituksiin ei ole saatavilla selvennyksiä, joten järjestelmässä esiintyneiden ongelmien ratkaiseminen muuttuu huomattavasti haasteellisemmaksi.

Järjestelmän virheilmoitukset johtuvat useasti liian pitkästä viiveestä IMS- ja sähköpostipalvelimen välillä. Järjestelmän toimivuuden kannalta on järkevintä sijoit-

taa useita IMS-palvelimia sähköpostipalvelinten lähelle. Ratkaisu on edullinen, koska Nokia ei laskuta IMS-palvelinten määrän mukaan, vaan laskutus on riippuvainen järjestelmään lisättävien käyttäjälisenssien määrästä. Tästä syystä jokaisen IMS-palvelimen tulee olla yhteydessä Nokian lisenssipalvelimeen.

Jos Intellisync-järjestelmä laajennetaan tulevaisuudessa yrityksen maailmanlaajuiseksi ratkaisuksi, jolloin sähköpostipalvelimet sijaitsevat ympäri maailmaa, tulee IMS-palvelimet sijoittaa sähköpostipalvelinten läheisyyteen. Tällöin jokaisen IMS-palvelimen hallinta tulee jakaa usean henkilön vastuulle, joista jokainen huolehtii yksittäisen IMS-palvelimen käyttäjätileistä. Käyttäjätili valitaan IMS-palvelimelle sähköpostipalvelimelle tallennetun sähköpostitilin mukaan, jolloin viive sähköpostipalvelimelta käyttäjäkohtaiselle IMS-palvelimelle on mahdollisimman pieni. Globaalissa ratkaisussa älypuhelimet muodostavat yhteyden ISGW-palvelimelle, jonka kautta liikenne ohjataan käyttäjän sähköpostipalvelimeen yhteydessä olevaan IMS-palvelimeen. Virtualisoinnilla voidaan näin ollen säästää laitekuluissa, koska IMS-palvelin voidaan virtualisoida kohdeympäristöönsä käyttämällä VMware-ohjelmistoa.

Loppukäyttäjille matkapuhelinjärjestelmän käyttöönotto nopeuttaa sähköposteihin vastaamista, koska sähköpostin saapuminen muistuttaa tekstiviestin vastaanottamista. Tekstiviesteihin vastataan useasti nopeasti ja niiden käyttö muistuttaa ajoittain pikaviestintää. Tulevaisuudessa sähköposti voi muuttua yhä interaktiivisemmaksi, jolloin viestejä lähetetään käyttäjien kesken tiheään tahtiin. Tällöin alkuperäisen sähköpostin käsite hämärtyy ja työntekijät kommunikoivat keskenään sähköpostin välityksellä lähes reaaliaikaisesti.

Järjestelmän pitkäaikainen toimivuus varmistetaan jakamalla järjestelmän tukitoiminnot eri tasoille. Yrityksen IT-tuki tarjoaa alimman tason tukea, joka auttaa loppukäyttäjiä perusongelmissa. Järjestelmän ylläpitäjä vastaa ongelmiin, joihin IT-tuki ei pysty tarjoamaan ratkaisua. IT-tuen työtarvetta saadaan vähennettyä, kun käyttäjille tarjotaan matkapuhelinjärjestelmää koskeva koulutus. Koulutuksessa käyttäjille jaettava materiaali sisältää vastaukset yleisimpiin matkapuhelin ongelmiin.

Opinnäytetyö opetti näkemään älypuhelinten uusia käyttömahdollisuuksia ja perusteli kuinka tietoturvan tasoa voidaan parantaa. Samalla työ opetti näkemään älypuhelinten jatkuvan kehityksen ja tulevaisuuden tuomat lisähaasteet.

LÄHTEET

Andritz, 2008a. Andritz Oy perustiedot [verkkojulkaisu]. 2008 Andritz Oy [viitattu 4.4.2008]. Saatavissa: http://finland.andritz.com/aboutus/aboutus_perustiedot.cfm

Andritz, 2008b. Divisioonat ja lyhenteet [verkkojulkaisu]. 2008 Andritz Oy [viitattu 4.4.2008]. Saatavissa: http://finland.andritz.com/aboutus/aboutus_divisions.cfm

Andritz, 2008c. Divisioonaprofiilit [verkkojulkaisu]. 2008 Andritz Oy [viitattu 4.4.2008]. Saatavissa: http://finland.andritz.com/aboutus/aboutus_division_profiles.cfm

Andritz, 2008d. ANDRITZIN HISTORIAA MARKKU HÄNNISEN KOKOAMANA [verkkojulkaisu]. 2008 Andritz Oy [viitattu 4.4.2008]. Saatavissa: http://finland.andritz.com/aboutus/aboutus_andritz historiaa.cfm

Computerlinks, 2006a. Nokia IntelliSync Device Management (OMA DM) Symbian-laitteille julkistettu [verkkojulkaisu] Computerlinks Oy [viitattu 25.3.2008]. Saatavissa: http://www.computerlinks.fi/html/np.php?contentid=2925

Computerlinks, 2006b. Managing OMA DM compliant devices [verkkojulkaisu] Computerlinks Oy [viitattu 25.3.2008]. Saatavissa: http://www.computerlinks.de/open/upload/Intellisync%20DM_Managing%20OMA%20DM%20compliant%20devices_May06.pdf

Computerlinks, 2008. Nokia IntelliSync Wireless Email + Device Management saatavissa [verkkojulkaisu] Computerlinks Oy [viitattu 26.3.2008]. Saatavissa: http://www.computerlinks.fi/html/np.php?contentid=2741

Granlund, K. 1999. Tietoliikenne. Jyväskylä: Teknolit Oy

Grönholm, K. 2002. DMZ (demilitarized zone) [raportti]. Lappeenrannan teknillinen korkeakoulu [viitattu 11.3.2008]. Saatavissa: http://www.it.lut.fi/kurssit/01-02/010626000/linux/dmz-kaj_gronholm.pdf

Hosia, A. 2004. Tietojärjestelmän jatkuvuudenhallinta prosessimallin avulla [verkkojulkaisu]. Teknillinen korkeakoulu [viitattu 12.1.2008]. Saatavissa: http://www.tml.tkk.fi/Publications/Thesis/hosia.pdf

Hämeen-Anttila, T. 2003. Tietoliikenteen perusteet. Jyväskylä: Docendo Finland Oy

Kalliala, A., Maunuksela-Malinen P. & Saloniemi M. 2004. Kuusi ensiaskelta tietotekniikan hyödyntämisessä [verkkojulkaisu]. TIEKE Tietoyhteiskunnan kehittämiskeskus ry [viitattu 18.1.2008]. Saatavissa: http://www.tieke.fi/mp/db/file_library/x/IMG/12423/file/Kuusiensiaskelta-opas.pdf

Karvonen, T. 2005. Pointsec: liikesalaisuudet unohtuvat taksin takapenkille [verkkolehti]. itviikko.fi [viitattu 22.3.2007]. Saatavissa: http://www.itviikko.fi/page.php?page_id=46&news_id=2005370

Koivisto M. 1997. Lähiverkot [verkkojulkaisu]. Internetix [viitattu 16.1.2008]. Saatavissa: http://www.internetix.fi/opinnot/opintojaksot/6tekniikkatalous/lahiverkko/index.htm

Kotilainen, S. 2005. Liikesalaisuudet unohtuvat taksin takapenkille [verkkolehti]. Tietokone.fi [viitattu 22.3.2007]. Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=22862&tyyppi=1

Kotilainen S, 2007. Ilmainen sähköposti on miljoonabisnes [verkkojulkaisu]. Taloussanomat [viitattu 20.1.2008]. Saatavissa: http://www.taloussanomat.fi/ITviikko/2007/01/18/Ilmainen+s%E4hk%F6posti+on+miljoonabisnes/20071399/109

Landmark Internet Ltd, 2008. GPRS (General Packet Radio Service), HSCSD & EDGE [verkkojulkaisu}. Landmark Internet Ltd [viitattu 2.4.2008]. Saatavissa: http://www.mobile-phones-uk.org.uk/gprs.htm

Lehto, T. 2005. Nokia työntää Exchange-postit yritysten puhelimiin [verkkolehti]. Tietokone.fi [viitattu 22.3.2007]. Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=24682

Microsoft msdn, 2008. Remote Desktop Protocol (Windows) [verkkojulkaisu]. Microsoft.com [viitattu 23.3.2008]. Saatavissa: http://msdn2.microsoft.com/en-us/library/aa383015.aspx

Microsoft it showcase, 2005. Improving IT effiency at Microsoft Using Virtual Server [verkkojulkaisu]. Microsoft.com [viitattu 22.3.2008]. Saatavissa: http://www.microsoft.com/technet/itshowcase/content/virtualserver2005twp.mspx

Microsoft Solution Finder, 2008. Over the Air Push Email solution for Smartphones [verkkojulkaisu]. Microsoft Solutionfinder [viitattu 29.3.2007]. Saatavissa: https://solutionfinderbeta.microsoft.com/SDK/Solutions/SolutionDetailsView.aspx?solutionid=685a77f84e434c18890c9ef2f34c079d&partnerid=ea85a9d2-24ca-48e0-a237-648dc712a704

Microsoft SQL Server -sovellusalusta, 2008. SQL Server -sovellusalusta [verkkojulkaisu]. Microsoft.com [viitattu 27.3.2008]. Saatavissa: http://www.microsoft.com/finland/servers/sql/cases/default.mspx

Microsoft Technet, 2005. New Mobility Features in Exchange Server 2003 SP2 [verkkojulkaisu]. Microsoft.com [viitattu 24.3.2008]. Saatavissa: http://technet.microsoft.com/fi-fi/library/aa995996(en-us).aspx

Microsoft Technet, 2008. Microsoft's Migration to Microsoft Exchange Server - The Evolution of Messaging within Microsoft Corporation [verkkojulkaisu]. Microsoft.com [viitattu 24.3.2008]. Saatavissa: http://www.microsoft.com/technet/archive/itsolutions/intranet/build/exchgdep.mspx?mfr=true

Moonsoft, 2008. Microsoft SQL Server 2005 [verkkojulkaisu]. Microsoft.com [viitattu 27.3.2008]. Saatavissa: http://www.moonsoft.fi/products/000362.aspx

Newman, D. 1999. Benchmarking Terminology for Firewall Performance [verkkolehti]. RFC.net [viitattu 12.1.2007]. Saatavissa: http://rfc.net/rfc2647.html

Nokia, 2007a. Nokia Intellisync Mobile Suite [verkkojulkaisu]. Nokian internetsivut [viitattu 21.3.2008]. Saatavissa: http://business.nokia.fi/NOKIA_BUSINESS_26/Europe/Products/Mobile_Software/sidebars/pdfs/MobileSuite_Datasheet_EMEA.pdf

Nokia, 2007b. Nokia Intellisync Mobile Suite Installation Guide [verkkojulkaisu]. Asennusohje [viitattu 21.3.2008].

Nokia, 2007c. Nokia Intellisync Device Management [verkkojulkaisu]. Nokian internetsi-vut [viitattu 21.3.2008]. Saatavissa: http://business.nokia.fi/NOKIA_BUSINESS_26/Europe/Products/Mobile_Software/sidebars/pdfs/DeviceMgt_Datasheet_EMEA.pdf

Nokia, 2008a. Nokia Intellisync Mobile Suite [verkkojulkaisu]. Nokian verkkosivut [viitattu 21.3.2008]. Saatavissa: http://business.nokia.fi/A4272067

Nokia, 2008b. Nokia Intellisync Device Management [verkkojulkaisu]. Nokian verkkosivut [viitattu 21.3.2008]. Saatavissa: http://business.nokia.fi/A4272110

Nokia Lehdistötiedotteet, 2005. Nokia ostaa Intellisyncin [verkkojulkaisu]. press.nokia.fi [viitattu 21.3.2008]. Saatavissa: http://press.nokia.fi/PR/200511/1021664_4.html

Nortel, 2005. HSDPA and beyond. [verkkojulkaisu]. Nortel Networks [viitattu 2.4.2008]. Saatavissa: http://faculty.stut.edu.tw/~cwycwy/951/N9490006.pdf

ODBC, 2008. ODBC [verkkojulkaisu] Hämeen ammattikorkeakoulu [viitattu 12.2.2008]. Saatavissa: http://trade.hamk.fi/integraatio/odbc.htm

Open Mobile Alliance, 2006. Interoperability in an Expanding World: Creating new mobility, connectivity and seamless service opportunities in Vietnam [verkkojulkaisu] Open Mobile Alliance [viitattu 21.3.2008]. Saatavissa: http://www.openmobilealliance.org/document/0507_mobilevietnam_jarialvinen1.pdf

Open Mobile Alliance, 2008. DEVICE MANAGEMENT WORKING GROUP CHARTER [verkkojulkaisu] Open Mobile Alliance [viitattu 2.4.2008]. Saatavissa: http://www.openmobilealliance.org/Technical/DM.aspx

Owen, D. 2003. Sybase FAQ: 2/19 - ASA [verkkojulkaisu]. doc.rz.ifi.lmu.de [viitattu 29.3.2008]. Saatavissa: http://doc.rz.ifi.lmu.de/FAQ/databases/sybase-faq/part2/index.html

Penttinen, J. 1999. GSM-tekniikka. Porvoo: WSOY – kirjapainoyksikkö.

Purho, J. 2007. Diplomityö: Työasemapalvelun kehittäminen virtualisoinnin avulla [verkkojulkaisu]. Teknillinen korkeakoulu [viitattu 21.2.2008] Saatavissa: www.netlab.hut.fi/opetus/s383310/07-08/Purho_161007.ppt

Pääkkönen, M. 2002. Runkoverkkojen toteutus ethernet tekniikoilla [verkkojulkaisu]. Jyväskylän yliopisto [viitattu 15.1.2008] Saatavissa: http://tisu.it.jyu.fi/terabitti/Documents/Eth_raportti.pdf

Salakoski, I. 2002. LDAP – Lightweight Directory Access Protocol [seminaariraportti]. Helsingin yliopisto [viitattu 11.3.2008]. Saatavissa: http://www.helsinki.fi/~salakosk/ldap.pdf

Scoble, A. 2005. Microsoft ups maximum storage for standard Exchange Server 2003 in SP2 [verkkojulkaisu]. Computerworld.com [viitattu 11.1.2008]. Saatavissa: http://blogs.computerworld.com/node/295

Soinsaari, T. 2007. Mikroyrityksen Windows-pohjainen tietojärjestelmä [verkkojulkaisu]. Insinöörityö [viitattu 10.1.2008]. Saatavisa: https://oa.doria.fi/bitstream/handle/10024/6024/Soinsaari.Tuomas.pdf?sequence=1

Suomen tietoveljet Oy, 2006: Palvelimien konsolidointi [verkkojulkaisu]. Suomen tietoveljet Oy [viitattu 12.1.2008]. Saatavissa: http://www.saimaasoftware.fi/tuotegalleria.jsp?sivu2=KONSULTOINTI&product=12

Symbian, 2008a. Symbian Fast Facts Q4 2007 [verkkojulkaisu]. Symbian [viitattu 12.4.2008]. Saatavissa: http://www.symbian.com/about/fastfacts/fastfacts.html

Symbian, 2008b. Symbian Developer Fast Facts [verkkojulkaisu]. Symbian [viitattu 12.4.2008]. Saatavissa: http://www.symbian.com/developer/fastfacts/index.html

Takkinen, S. 2003. Tietoturvan perusteita [verkkojulkaisu]. Jyväskylän Yliopisto [viitattu 17.1.2008]. Saatavissa: http://www.cs.jyu.fi/~kolli/verkkotekniikka/luennot/www-tietoturva.pdf

The Tech FAQ, 2008a. What is an incremental backup? [verkkojulkaisu]. The Tech FAQ [viitattu 20.3.2008]. Saatavissa: http://www.tech-faq.com/incremental-backup.shtml

The Tech FAQ, 2008b. What is a differential backup? [verkkojulkaisu]. The Tech FAQ [viitattu 20.3.2008]. Saatavissa: http://www.tech-faq.com/differential-backup.shtml

Verkkouutiset, 1998. Suomeen 3-4 laajakaistaista matkapuhelinverkkoa [verkko-julkaisu]. Verkkouutiset [viitattu 2.4.2008]. Saatavissa: http://www.verkkouutiset.fi/arkisto/Arkisto_1998/2.lokakuu/UMTS3898.HTM

Älypuhelimet, 2008: Älyä puhelimessa ? [verkkojulkaisu]. Älyä puhelimessa ? [viitattu 27.3.2008]. Saatavissa: http://www.alypuhelimet.com/