A technical prestudy on Seamless roaming for mobile Internet at Martinsson Information Systems AB

Abstract

Seamless roaming is an abstraction over the Internet connection. The users no longer need to care about how he or she is connected. That is entirely handled by the system that automatically selects the most appropriate network available without the user even noticing it. Is this a suitable business area for Martinsson, a company focused on infrastructure and server based computing? The technologies needed for seamless roaming have been examined, and systems from the world-leading companies Columbitech and IP Unplugged have been evaluated. The investigation shows that the technology is very interesting and it will be important in the future. Though, it is yet too immature to be deployed in larger scale by Martinsson, but it is advisably to closely follow the market development and maybe initiate some field testing in cooperation with customers that is aware of the system's limitations.

Sammanfattning

Seamless roaming är en abstraktion över Internetuppkopplingen. Användarna behöver inte längre bry sig om hur han eller hon faktiskt är uppkopplade, utan det hanteras helt och hållet av systemet som automatiskt väljer det mest lämpliga nätet. Är detta ett lämpligt affärsområde för Martinsson, ett bolag som i första hand är fokuserat på infrastruktur och serverrelaterade tjänster? De nödvändiga teknikerna samt två system för Seamless roaming från de världsledande företagen Columbitech och IP Unplugged har utvärderats. Undersökningen visar att tekniken är intressant och kommer att spela en viktig roll i framtiden. Dock är tekniken fortfarande för omogen för att rullas ut i större skala till Martinssons kunder. Man bör dock följa marknadens utveckling noga och kanske inleda testverksamhet i samarbete med kunder som är medvetna om systemens begränsningar.

Summary

The purpose of this master thesis is to investigate the possibilities for Martinsson to start up a business focus area around the concept of mobility. The investigation is not limited to technical requirements. The investigation also includes market potential and the maturity of technology, and how well the technology complies with the Martinsson business philosophy.

The investigation has basically been conducted in four steps. Initially, the company has been examined. Then the bearer technologies on the market have been evaluated, and from the knowledge acquired a specific area of technology has been selected for a deeper technical study. Then a recommendation based on the technical investigation and external market investigation has been issued to Martinsson.

Martinsson is a consultant company that successfully has endured the harsh times of the IT industry without being forced to painful reductions. This is because Martinsson has always been careful and unwilling to take high risks. The company works mainly with mature technology and desires to establish stable partnerships with manufacturers and other companies, and focuses on the building of stable and cost-efficient infrastructure in cooperation with it's partners. The most important partners are *Microsoft*, *Citrix* and *Cisco Systems*. Martinsson profiles itself as a server specialist, and believes that thin clients that connect to servers is a very cost-effective IT infrastructure. Internally, Martinsson is organized in 8 focus areas. In each area, Martinsson desires to be one of the top three actors in Sweden. The areas are *IP Communication, Security, Storage and Data Protection, Server Based Computing, Databases and Messaging* and *Directory Services*.

The bearer technologies that have been investigated and evaluated are WLAN (802.11), HiperLAN, GSM / GPRS and UMTS (3G). The conclusion of the investigation is that HiperLAN can be sorted out, at least for the near future. UMTS is not a reality in Sweden for some time to come, and from a IP perspective, it is not very different from GSM and GPRS. GPRS is still also an immature technology and gives unreliable access to the internet. It should not be trusted for business-critical applications that rely on an always-present internet connection. WLAN is the most mature technology for mobile internet access, and even though the mobility aspect of WLANs can be questioned, it is the only technology mature today. The main problems with WLANs are the security flaws, and WLANs cannot be trusted to be secure without additional security measures like VPNs. Since Martinsson build infrastructure, a mobile infrastructure based on WLAN with support from other carriers that gives the customers less problems and solves the security problems would be an approach that complies with the company philosophy.

Seamless roaming is the very front of technology, and is an abstraction over internet connection. Seamless roaming means that the user does not have to care about how he (or she) is connected. The system always and automatically chooses the best connection available. Two Swedish companies, Columbitech and IP Unplugged build systems for seamless roaming and they are described as world-leading in media, for example the paper *Ny Teknik*. They are both developing systems for seamless roaming that include VPNs. These systems have been theoretically examined and their throughput, roaming characteristics and usability have been tested.

Columbitech's system is called Columbitech Wireless Suite, and is a software-only solution that consists of three major parts. A VPN server called Columbitech Enterprise Server, an optional load balancing server called Columbitech Gatekeeper and a user client that plugs into the user's computer as a virtual network adapter. The client and the enterprise server try to keep up a TCP connection between them and automatically select the best network available. The virtual NIC (*Network Interface Card*) however, always reports an active connection to the user applications. Loss of the real connection appears only as network disturbances. The system also deploys additional functionality, including strong encryption, data compression and certificate handling. Columbitech's system is easy to install and configure and gives good throughput. Unfortunaly, the system lacks in stability and the

roaming is not fully seamless. Roaming works significantly better in a pure LAN/WLAN environment than in GPRS environments.

IP Unplugged's system has a structure similar to that of Columbitech WVPN. It consists of the Roaming Gateway, Roaming Server and Roaming Client components. The Roaming Gateway is a VPN Server and Firewall. The Roaming Client plugs into the user's computer as a virtual NIC and the Roaming Server is a management server that can handle large numbers of users and Roaming Gateways. The system is based on standard components and uses IPsec and Mobile IP. System requirements are high which affects throughput, but the system is stable and easy to manage, and roaming works well in LAN and WLAN environments. Roaming to GPRS is slow, due to the long connection times to GPRS.

The market predictions from Columbitech, IP Unplugged and Gartner all draw a bright future for mobility. IP Unplugged mentions the report "*Mobile Intranets Towards the Wireless Enterprise*" from Ovum that claims that the world market will be worth $2.000.000.000 in 2006. Columbitech means that seamless roaming is a necessarity in a future heterogeneous network environment. The users should not need to worry about security or internet connection. The user should just be connected. Columbitech wants to supply application developers with an always-connected API. Gartner claims that WLANs are going to be much more common and a natural part of mobile operators's networks in the future. VPNs are gaining more trust among users and will replace other private connections like leased lines. The main problems are integration and security, according to Gartner.

The conclusion is that mobility is an important part the future Internet infrastructure, and a Martinsson cannot ignore this development. Seamless roaming is a part of a wireless infrastructure, and would fit well into Martinsson's focus on infrastructure.

Both the systems of Columbitech and IP Unplugged works over GPRS today, but they are not smooth and add little value under such circumstances. However, as a tool mainly for roaming in LAN/WLAN environments, the systems are fairly good. Columbitech's WVPN has good performance, but is too unstable to be offered to Martinsson's customers. IP Unplugged's system however is stable enough and it would be possible to offer it to test customers that are aware of the limitations. The market must be watched closely.

.

Förord

Arbetet har utförts på Martinsson Information Systems AB i Umeå. Detta examensarbete har genomförts under HT-2002 på 20p D-nivå och ingår som del i civilingenjörsprogrammet för teknisk datavetenskap 180p.

Huvudsyftet med examensarbetet har varit att undersöka marknaden för mobil kommunikation och möjligheten för Martinsson att erbjuda kunder tjänster inom området mobilitet. Arbetet har i huvudsak gått ut på att studera Martinssons organisation, tekniken på den mobila marknaden samt testning och utvärdering av tekniken Seamless Roaming.

Under examensarbetets gång har vi fått tillfälle att lära känna många trevliga personer både internt inom Martinssons organisation samt hos de företag som ställt upp med utbildning, materiel och support till vårt arbete. Tillsammans har alla varit starkt bidragande till att arbetet flutit på.

Ett speciellt tack skulle vi vilja rikta till våra handledare Conny Björnehall från Martinsson och Thomas Nilsson från Umeå Universitet för att dom alltid ställt upp och svarat på våra frågor.

Vi vill också tacka John Rehnberg på IP Unplugged samt Ola Jonsson och David Ranner från Columbitech för att dom ställde upp med sina respektive produkter för Seamless Roaming samt det stöd vi erhöll under testningen. Vi vill också passa på att tacka Cisco, Gartner, Umeå Energi och Umdac för deras bidrag när vi satte upp vår testmiljö.

Slutligen skulle vi vilja tacka samtliga anställda på Martinsson i Umeå för att ni alltid hjälpt till de gånger då vi stött på problem samt att vi fick tillfället att lära känna er samt bli en del i kontorsgemenskapen.

Författare: Per Pettersson, Fredric Rylander
Institutionen för Datavetenskap, Umeå Universitet

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Mobilitet är något som diskuteras väldigt mycket idag och utvecklingen går snabbt framåt. Mobiltelefoner finns idag i var mans hand och GSM-tekniken är en fullkomlig succé. Gick det att förutspå den utvecklingen för tio år sedan? Via GPRS går det att ha en ständig Internetuppkoppling till sin mobiltelefon, laptop eller handdator. Samtidigt har teleoperatörerna förbundigt sig att snabbt bygga ut tredje generationens mobiltelefonnät, 3G, över hela landet.

Även WLAN figurerar i diskussionen. Telia bygger ut ett nät av WLAN-hotspots, *Telia Homerun*, på flygplatser, hotell och caféer över hela Sverige. WLAN blir allt vanligare både i hem och företag. Ett flertal standarder och tekniker diskuteras, t.ex. IEEE 802.11b, 802.11a, 802.11g och även HiperLAN.

Det är med andra ord uppenbart att vi går mot en allt högre grad av mobilitet. Frågan är bara hur framtidens mobilitet ser ut.

Martinsson Informationsystem AB är ett IT-företag som i första hand arbetar med infrastruktur. Företaget bygger nät, sätter upp servrar, skrivare och mycket annat. Martinsson har ingen egen utveckling, utan strävar istället efter att etablera djupa samarbeten med marknadens övriga aktörer och marknadsföra deras produkter samt installera väl fungerande standardprodukter till fast pris. Målet har hela tiden varit att ha en stabil ekonomi och en verksamhet som genererar vinst och samtidigt som man undvikit att kasta sig in i okända områden allt för fort. Detta har kanske inte fått Martinsson att framstå som ett häftigt och glamoröst IT-företag, men man har klarat sig igenom IT-krisen utan större problem och idag tillhör Martinsson de populärare arbetsgivarna i Sverige. En undersökning från företaget Universum (http://www.universum.se) säger att Martinsson är på plats 65 bland Sveriges attraktivaste arbetsgivare enligt Lars Pettersson, Martinssons VD.

Att mobilitet är något som är på kraftig frammarsch har givetvis inte gått Martinsson förbi. Frågan är bara hur Martinsson ska förhålla sig till det och hur företaget ska agera. Är marknaden tillräckligt mogen att ge sig in på? Finns det möjlighet för Martinsson att bli en leverantör av mobila tjänster?

2. Syfte

2.1. Målbeskrivning

Det övergripande syftet med arbetet är att undersöka om hur Martinsson ska förhålla sig till den expanderade mobila marknaden för datatjänster.

Företaget Martinsson är organiserat med en mängd standardiserade bastjänster i botten som man erbjuder sina kunder. Utöver detta finns åtta så kallade fokusområden där målet är att vara en av de tre främsta aktörerna i Sverige. Dessa fokusområden ska vara mer tekniskt avancerade än vanliga bastjänster och allt eftersom tekniken utvecklas övergår fokusområdenas tjänstepaket till att vara bastjänster och nya tjänster inom fokusområdena tillkommer.

Det praktiska målet för det här arbetet har avgränsats till att undersöka de tekniska och marknadsmässiga förutsättningar för att skapa ett nytt fokusområde: *Mobility och* ge en rekommendation för hur Martinsson bör agera i frågan. Några rekommendationer som skulle kunna vara tänkbara är att helt ignorera området, köpa upp något företag, bygga upp en egen kompetens, initiera samarbete med någon aktör eller att avvakta men bevaka marknaden. Frågor som ska beaktas är bland annat kundnyttor, integrationsmöjligheter med Martinssons nuvarande system och teknologins tekniska och marknadsmässiga mognad.

2.2. Frågeställningar

Målen ger naturligt upphov till ett flertal frågor som måste besvaras.

- Hur fungerar Martinsson internt, vilka tjänster erbjuds kunderna, vilka leverantörer samarbetar företaget med och vilka system används?
- Hur ser den mobila marknaden ut, var går den tekniska frontlinjen, hur mogen är teknologierna tekniskt och marknadsmässigt?
- Finns det delar av den mobila marknaden av som passar Martinsson och vilka är detta i så fall?
- Hur ska Martinsson agera?

2.3. Syfte för vetenskaplig fördjupning

Efter att Martinsson och omvärlden undersökts tillkommer ännu ett syfte. Tekniken Seamless roaming ska undersökas och Columbitechs och IP Unpluggeds produkter ska utvärderas. Den frågeställning som ska besvaras är främst om någon av dessa produkter är intressanta för Martinsson.

3. Metodbeskrivning

3.1. Övergripande metodbeskrivning

Arbetet delades in i fyra tidsmässiga faser med olika innehåll. Den första fasen gick ut på att studera Martinssons teknik och organisation. Den andra fasen var en omvärldsanalys, den tredje var en teknisk fördjupning och den fjärde var en sammanställnings- och rapportskrivningsfas.

3.2. Fas 1 - Undersökning av Martinsson

Den första fasen gick ut på att studera företaget Martinsson internt - Martinssons organisationsmodell med bastjänster och fokusområden. Utredningen har också beaktat hur konsulterna jobbar mot kunder och vilka erbjudanden som ges, Martinssons företagsfilosofi och profil, vilka de viktigaste samarbetspartnerna är, vilken teknik som används och hur den interna projektmodellen ProMIS ser ut.

Informationen som behövs till dessa undersökningar har inhämtats från Martinssons interna informationsdatabas och genom intervjuer med anställda. En rapport har skapats om varje fokusområde och denna rapport har sedan granskats och godkänts som korrekt av ansvarig för respektive fokusområde.[1]

3.3. Fas 2 - Omvärldsundersökning

Fas 2 var en analys av omvärlden och de databärartekniker som används. Dels har de bärartekniker som idag används för trådlös dataöverföring studerats, samt vilka som väntar inom en snar framtid. Detta har givit en bra grund för olika teknikers tekniska och marknadsmässiga mognad och vi har fått en god överblick över vilka företag och organisationer som är intressanta och var teknikens frontlinje går. Kunskaperna som inhämtats i denna omvärldsundersökning, samt resultaten från fas 1, har legat till grund för beslutet om hur fas tre och fyras utformning.

Informationen till denna omvärldsanalys måste vara färsk och därför är Internet den källa som varit absolut viktigast. För teknisk information är olika standardorganisationers webbplatser, såsom ETSI och IEEE men även vissa företags webbplatser värdefulla. Marknadsmognad är något svårare att vetenskapligt bedöma än tekniska fakta och därför har mindre vetenskapliga källor fått användas i detta fall. Exempel är tidningsartiklar, större tekniska webbmagasin och handelsplatser.

3.4. Fas 3 – Teknisk fördjupning

Den tredje fasen var en teknisk fördjupning. I detta fall har vi satt upp testsystem med lösningar för Seamless Roaming både för Columbitech och IP Unplugged. Båda systemen har prestandatestats tekniskt. Vi har även noterat hur funktionaliteten i systemen upplevts. Den bakomliggande teknikens för- och nackdelar har undersökts. Leverantörerna har även fått ta del av resultaten och gett sina kommentarer till dem, samt berättat vilka förbättringar som ska göras på produkterna inom den närmsta framtiden.

3.5. Fas 4 – Marknadinformation och rekommendation

[1] Fokusområdesrapporterna har bifogats som appendix.

Till den slutgiltiga sammanställningen har sedan extern marknadsinformation hämtats in. Columbitech och IP Unplugged har fått ge sin syn på marknaden, kundnyttor och försäljningsargument. Vi har även inhämtat prognoser och analyser från analysföretaget Gartner. Utifrån vår tekniska undersökning och de externa marknadsanalyserna har vi givit en rekommendation till Martinsson hur vi anser att företaget bör agera.

4. Avgränsningar

Ämnesmässigt så kommer undersökningen att till en början ha en väldigt flytande avgränsning, då syftet i den andra fasen är orientering i moderna trådlösa databärartekniker som kan vara relevanta för mobilitet. Detta innebär i dagsläget både teknikfamiljer för trådlösa nätverk (802.11 och HiperLAN) och teknik för mobiltelefoni (GSM/GPRS och UMTS). Eftersom det övergripande syftet med undersökningen är att undersöka mobilitet ur ett Martinsson-perspektiv så har vi också valt bort tekniker som inte är vanligen förekommande, eller som vi inte ansett relevanta, i Sverige. Det innebär att tekniker som WCDMA2000, iMode, RadioLAN med flera har valts bort. Mobitex har också valt bort eftersom det i Sverige inte kan erbjuda tillräckligt bra prestanda och i första hand kan anses vara ett system för fordonsbruk.

Den tekniska fördjupningen har också begränsats av det marknadsperspektiv vi har valt. Det innebär att vi har lagt en större vikt på hur systemen fungerar tekniskt ur en användarsynvinkel än en ingenjörssynvinkel.

5. Martinsson

5.1. Bakgrund och historik

Martinsson kommer ursprungligen av en mängd lokala företag som slogs ihop till en organisation. Dock fanns betydande brister i samordningen mellan kontoren och de tjänster som erbjöds var knutna till lokala kontor. Utvecklingen ledde till att ett antal fokusområden skapades med tjänster som alla kontor skulle kunna erbjuda. Annat kvalitetsarbete, som införandet av ProMIS, följde också. Under IT-krisen har Martinsson hela tiden lyckats göra positivt resultat tack vara fokusering på kvalitet och expansion i långsamt tempo.

På grund av problem inom bolaget, som sysslade med infrastruktur, Lotus Notes och affärssystemsutveckling valde ledningen år 2000 att dela upp bolaget. Infrastrukturbiten blev nya Martinsson, Notesdelen blev, efter flera namnbyten, Datavis och affärssystemsutvecklingen blev Navigera. I augusti 2002 köpte Martinsson upp den större konkurrenten IMS som nu har införlivats i verksamheten. I dagsläget (december 2002) har Martinsson ungefär 550 anställda på 19 lokalkontor i Sverige [Arvidsson 2002, personlig kommunikation].

5.2. Mål, visioner och affärsidé

Huvudmålet för Martinsson är att skapa ett så stort mervärde som möjligt för kunden på genomförd investering. Företaget strävar också efter att vara bland de tre bästa i Sverige inom sina fokusområden.

Martinsson beskriver sin affärsidé: "Våra kvalificerade och engagerade medarbetare levererar i samarbete med marknadsledande aktörer server och serverrelaterade tjänster med helhetsansvar som ger våra kunder ökad konkurrenskraft" [Martinsson 2003].

5.3. Organisationsstruktur

Martinsson består av 19 lokalkontor vilka leds centralt av VD och styrelse i en vertikal struktur. Alla kontor har en platschef och minst en konsultchef. Horisontellt mot kontorsstrukturen finns fokusområdesstrukturen, som är att betrakta som en slags kompetensstruktur. Alla konsulter jobbar inom ett fokusområde och alla fokusområden leds och drivs av en AI (affärsingenjör) som ska garantera områdets fortlevnad och jobbar direkt under den tekniske chefen. Affärsingenjörens uppgift är att hitta nya produkter och skapa fler tjänster för företagets kunder. Fokusområdet är inte konsultens formella arbetsgivare, utan konsulten är anställd av sitt lokalkontor men har ett fokusområde som sin primära inriktning. Det praktiska arbetet bedrivs till stor del på lokal nivå utanför fokusområdet, men man strävar efter att lägga så mycket som möjligt av arbetet inom fokusområdet. Om ett kontor har behov av specialkompetens inom något av fokusområdena som saknas lokalt kallas kompetensen in från andra kontor, vilket gör att alla Martinssonkontor får tillgång till all kompetens inom organisationen. Organisationsstrukturen är i princip densamma som hos Cisco.

Konsulterna som jobbar är antingen seniorkonsulter, systemkonsulter eller teknikkonsulter med arbetsuppgifter av olika karaktär. Konsulterna börjar oftast som teknikkonsulter och kan sedan vidareutveckla sig. För de konsulter som vill satsa lite extra på kompetensutveckling finns möjligheten att bli CMG (*Commando Martinsson Grön*), inom något område. Som CMG får konsulten lägga ner en stor del av sin tid på kompetensutveckling. CMG:n förväntas tillhöra toppförmågorna inom sitt område. En CMG kan bistå vid särskilt komplicerade uppdrag och jobbar med att vidareutveckla sitt fokusområde vid sidan av det dagliga arbetet. *”Commando Martinsson Grön”* kommer av att den som började bygga upp CMG-strukturen varit militär innan anställningen på Martinsson.

Säljare kan antingen resa runt och besöka kunder på plats, eller vara innesäljare på något kontor som kommunicerar med sina kunder via telefon. Kontoren har även koordinatörer som fördelar arbeten som kommer in. Martinsson eftersträvar även att alla kunder ska ha en "huskonsult" från det lokala kontoret som kontaktperson [Arvidsson 2002, personlig kommunikation].

5.4. ProMIS och projekt

ProMIS är ett policydokument för hur affärer ska genomdrivas som har utvecklats till en enkel projektmall. Syftet är att garantera kunderna kvalitet och skapa likformighet över hela landet. Viktiga verktyg är tydlig terminologi, fasta roller, avstämningsdokument och acceptansprotokoll. ProMIS definierar ett par tydliga roller:

- Kundansvarig säljare är den som är ansvarig för kunden och ska ha en långsiktig strategi för kunden
- Affärsägare är den som är ansvarig för att affären och ska se till att den fullföljs.
- Leveransansvarig är den som operativt ser till att arbetet genomförs.
- Beställare är den som å kundens vägnar förhandlar fram en affär.

ProMIS påminner till stora delar om Ericssons projektmodell PROPS och kan beskrivas som en kraftigt förenklad modell av denna, säger Jonas Emilsson [Emilsson 2002-10, personlig kommunikation].

5.5. Kunderbjudanden och affärstänkande

5.5.1. Kvalitet och partnerrelationer

Martinsson satsar på att erbjuda kvalitet både i personal och produkter och därför jobbar företaget i långsiktiga partnerförhållanden med leverantörer, genom att uppnå så hög partnerstatus hos leverantörerna som möjligt. En högre status hos en leverantör brukar ofta innebära bra rabatter på hårdvara, mjukvarulicenser och utbildning. Martinsson satsar även på att konsulterna ska vara kvalificerade inom sina områden och därför läggs det ned både tid och pengar på att konsulterna ska skaffa sig så mycket certifikat som möjligt.

5.5.2. Standardlösningar och fastpristjänster

Martinsson strävar efter att till stor del sälja standardiserade lösningar till kunderna. Tjänster paketeras in i olika standardpaket som i så hög utsträckning som möjligt har ett fast pris. Kunden får då en tydlig specifikation på vad som ingår i paketet. En stor del av paketen utgörs av "workshops" som går ut på att gå igenom kundens IT-miljö för att identifiera problem, behov och möjliga lösningar. Dessa workshops är ordentligt subventionerade och Martinsson tjänar inga pengar på dem, men förhoppningen är att de ska leda till att Martinsson får sälja in andra produkter och tjänster till kunderna istället.

Strävandet efter ett standardiserat utbud faller väl samman med strävandet efter partnerrelationer, då ett mindre urval av lösningar leder till bättre koncentration av företagets kompetens. Martinsson strävar också efter att erbjuda en större andel tjänster till fast pris.

5.5.3. Serverfokus

Martinsson profilerar sig som en expert på serverbaserad databehandling och hela organisationen är inriktad på att främja ett centraliserat arbetssätt hos kunderna. Martinsson tror att detta leder till lägre kostnad för IT-verksamheten än vad en decentraliserad struktur gör.

5.5.4. Helhetssyn och driftåtaganden

Martinsson vill gärna befria kunden från ansvaret över IT-driften, på olika nivåer och erbjuder därför ett flertal tjänster inom området. Exempel är fjärrövervakning, uppställning av kunders maskiner i Martinssons drifthall i Eskilstuna, "huskonsulter" som sitter ute hos kund och även fullskaliga åtaganden för IT-driften.

5.6. IP Communication

Motivet för fokusområdet IP Communication är att erbjuda kunderna experthjälp med utveckling och design av kommunikationslösningar och att ”lägre driftskostnader, bättre informationsskydd och högre tillgänglighet” ska bli resultatet. Eftersom det är allmänt känt att driftavbrott kan bli mycket kostsamma så är det rimligt.

I utbudet ingår LAN, WAN, WLAN, brandväggar, VPN, IDS (*Intrusion Detection Systems*) och managementverktyg. Martinsson gör även analyser av kundernas kommunikationsmiljö för att kunna ge råd i samband med investeringar. Företaget samarbetar med några stora aktörer. Cisco är den största leverantören av utrustning. Teletjänster köpes i första hand in från Telia Sonera.

Området är mycket intressant ur ett mobilitetsperspektiv då det byggs stora trådlösa IP-nät. GSM, UMTS/3G och alla WLAN-hotspots som byggs ger upphov till nya affärsmöjligheter. Eftersom säkerheten i trådlösa nätverk och på bärbara enheter är under all kritik borde stora möjligheter att bygga säker infrastruktur, t.ex. via VPN, föreligga [IDG 2002]. För att kunna jobba smidigt i en heterogen nätverksmiljö krävs också någon slags roaming mellan olika nätverk. [2]

5.7. Security

Att säkerhet är viktigt, i många fall avgörande, för en verksamhet står utan tvivel. Trots detta är säkerheten tydligt eftersatt i många organisationer. Kunskapen är ofta låg och många saknar ett helhetsperspektiv.

Martinssons recept på ett lyckat uppdrag hos en kund är att i första hand få ledningen för företaget att förstå att en helhetssyn på säkerhet är viktigt samt att en intern organisation skapas för att driva frågan. Därefter bör ett policydokument tas fram och en riskanalys göras. Först när en analys är klar kan olika lösningar tas fram i syfte att se vilka som passar företaget bäst. Virusskydd, krypteringsskydd, brandväggsinstallation, e-postfiltrering, operativsystemssäkerhet och säkerhetskopiering är exempel på verktyg som används. Efter att lösningarna implementerats är det också viktigt med utbildning av anställda samt efterkontroller.

Det är ingen tvekan om att säkerhet är en viktig aspekt på i princip all dataanvändning och i mobila system måste detta verkligen beaktas då dessa system i många fall är mycket osäkra. Säkerheten kan mycket väl bli en huvudfråga i ett framtida mobilt fokusområde. [3]

[2] Fokusområdet finns djupare beskrivet i appendix A.
[3] Fokusområdet finns närmare beskrivet i appendix B

5.8. Storage & Data Protection

Några centrala faktorer vid datalagring är hög informationsintegritet, hög tillgänglighet och snabb åtkomst. Då mängderna med lagrad data snabbt ökar tycker Martinsson att ett skalbart system också är viktigt. Martinssons svar på dessa krav brukar vara ett SAN (*Storage Area Network*). Företaget jobbar även med backup och installerar nya backupsystem, likväl som man servar och ser över gamla backupsystem. Compaq, IBM, StorageTek (www.storagetek.com), ADIC (www.adic.com) och Overland (www.overlanddata.com) på är partners på hårdvarusidan. På mjukvarusidan pågår samarbete med Veritas (www.veritas.com) , Legato (www.legato.com) och IBM.[4]

5.9. Server Based Computing

Martinsson menar att en tunna klienter som jobbar mot en central server oftast är en mycket kostnadseffektiv lösning. Behovet att förnya arbetsstationerna minskar och administrationen blir mycket enklare. Systemen blir klientoberoende, vilket gör det möjligt att jobba från flera olika plattformar.

Martinsson profilerar sig som Citrix-partner och har, som ett av tre svenska företag, uppnått högsta partnerstatus hos Citrix. Citrix produkter, då särskilt Citrix Metaframe, är en mycket viktig del i Martinssons sortiment. Citrix Metaframe består primärt av en server och klienter som kopplar upp sig mot denna och kör applikationerna där och skärmuppdateringar skickas till klienten. Protokollet är anpassat för låga bandbredder och mobil användning och anpassar kvalitén på presentationen efter tillgänglig bandbredd och döljer långa svarstider för användaren. Ett stort problem är dock att de små skärmarna på mobila enheter ofta gör applikationerna svåranvända.

Martinsson ser Citrix som en central del av mobilitet, i och med att de går att använda mobilt på uppkopplingar med låg genomströmningskapacitet, som t.ex. GSM, idag. Detta verkar vara en riktig iakttagelse och Citrix bör fungera utmärkt över framtida mobila system. Kanske kan en komplettering med VPN och Roaming vara bra och säkerheten måste givetvis beaktas.[5]

5.10. Databases & Messaging

Databaser och meddelandesystem är en viktig del i en IT-infrastruktur och det är naturligtvis viktigt att lösningarna är säkra och väl fungerande. Martinsson har inom detta område specialiserat sig på Microsoftprodukter såsom Exchange, SQL Server och Cluster Server. Lotus Notes ingår också i utbudet, men partnern heter Microsoft.

Området har relativt få mobilitetsaspekter. Visserligen bör användare t.ex. kunna läsa sina mail mobilt men om övriga system görs mobilt tillgängliga följer mailen med på köpet.[6]

5.11. Systems Management

Systems Management handlar om styrning, kontroll och övervakning av datorsystem. Här arbetar Martinsson med övervakning av kunders system. Övervakningen sker främst på distans och när något går fel får Martinsson ett larm. Scriptade installationer är en annan viktig del av området och ger möjlighet att skapa anpassade standardinstallationer vilket ofta förenklar administrationen.

[4] Fokusområdet finns djupare beskrivet i appendix C
[5] Fokusområdet finns djupare beskrivet i appendix D
[6] Fokusområdet finns djupare beskrivet i appendix E

Martinssons partners är Compaq och IBM och från dessa levereras både hård- och mjukvara. Martinssons största tjänstepaket finns inom detta område, Tivoli Enterprise, består av ett flertal "managers" som ska kunna integreras med varandra. Martinsson är ett av två svenska företag med högsta partnerstatus hos Tivoli. Den andra är Cygate (www.cygategroup.com), en av Martinsson konkurrenter. En annan konkurrent, främst inom Tivoli Storage, är EnjoyIT (www.enjoyit.se).

Området är i dagsläget av mindre intresse ur ett mobilitetsperspektiv. Tivoli har stöd för mobil övervakning vilket kan vara intressant. Övervakning av mobila affärssystem kan också vara intressanta men frågan är hur mycket det skiljer sig från att övervaka fasta system.[7]

5.12. Directory Services

Katalogtjänster går i grunder ut på att samla behörighetsinformation för flera system på ett ställe. Då en organisation har många system som användare måste komma åt finns det säkerhetsrisker och administrativa problem. Användare måste komma ihåg flera olika identiteter och lösenord och tvingas till flera inloggningar. Systemadministratörerna måste dela ut behörigheter på flera olika system. Detta leder ofta till uppskrivna lösenord, glipor i behörigheterna och en onödigt arbete. En katalogtjänst ger en bättre översikt över behörigheter, enklare administration och mindre besvär för användarna.

Martinsson jobbar med två olika katalogtjänster, Microsofts Active Directory och Novells NDS (*Novell Directory Service*). AD finns bara på Windows 2000-plattformen medan NDS finns på många plattformar.

Området är av uppenbar vikt för mobilitet. En mobil terminal måste ha samma möjligheter att utnyttja en katalogtjänst som stationära terminaler. Om den mobila terminalen har en IP-adress borde detta dock inte vara ett problem.[8]

[7] Fokusområdet finns djupare beskrivet i appendix F
[8] Fokusområdet finns djupare beskrivet i appendix G

6. Tekniken på marknaden

6.1. Beskrivning

För att förstå hur de tekniska lösningarna som används idag fungerar och vilken inverkan de innovativa teknikerna som är på gång kommer att ha på marknaden för mobilitet har bärarteknikerna som finns på marknaden idag noga studeras.

Teknikerna utvecklas i en rasande fart och ska en produkt eller lösning tillhandahållas bör man se till att den är gångbar oavsett vilken typ av bärare för mobil dataöverföring som för tillfället finns på marknaden. Det bör också tas i beaktande vilken konkurrerande teknik som väntar runt hörnet och vad den tekniken kan innebära för produkten eller tjänsten som ska erbjudas. Med anledning av detta har vi tittat på ett par bärartekniker som används idag samt även studerat ett par tekniker som kan komma att spela en stor roll för den framtida mobila utvecklingen de närmsta åren.

När vi studerat de olika teknikerna har vi främst tittat på de tjänster som företag kan erbjuda sina kunder samt vilken överföringskapacitet de har. Vi har även tittat på teknikens mognadsgrad, framtidsutsikter samt konkurrenssituationen.

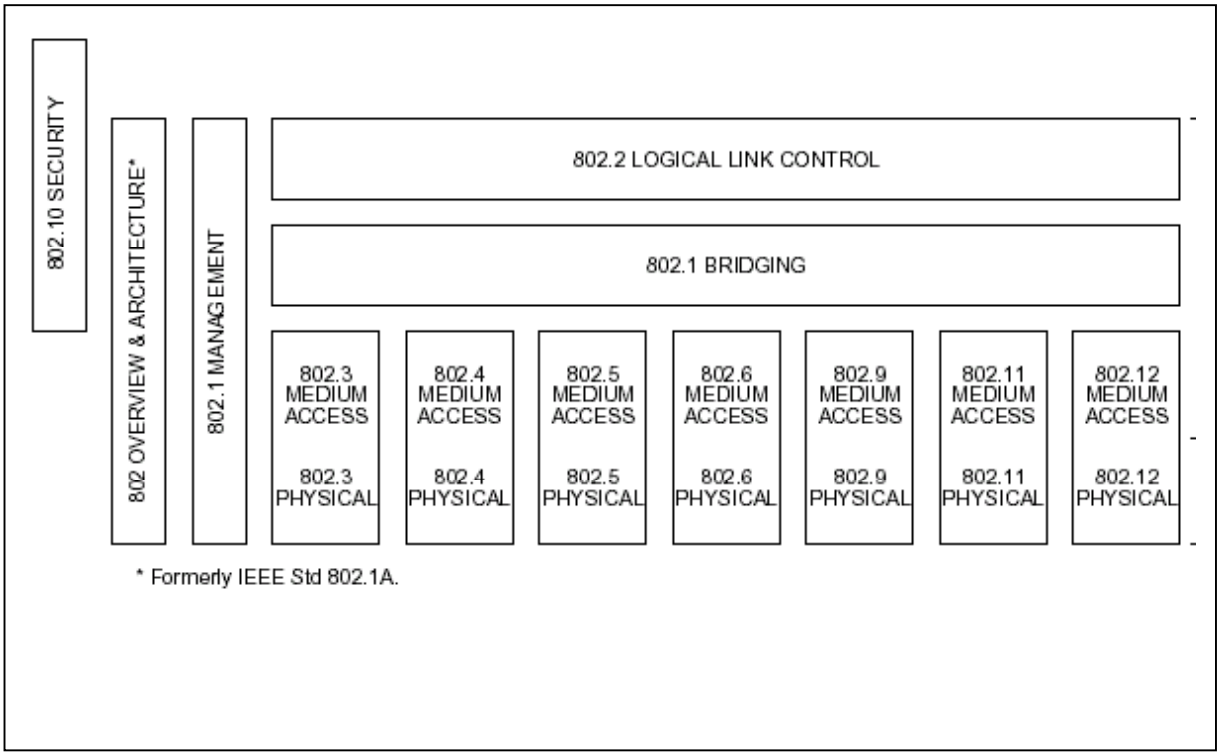
6.2. 802.11

De trådlösa nät som idag används som trådlösa kontors- eller hemmanätverk kallas WLAN (*Wireless Local Area Network*) och det är enbart sådana nät den här rapporten behandlar. De WLAN som normalt byggs idag består dels av en fast infrastruktur bestående av accesspunkter kopplade till en gateway eller brygga som kopplas mot annan infrastruktur, dels består de av mobila stationer, oftast datorer med WLAN-kort.

802.11 är en del av IEEE 802-standarden (Figur 1) som är en familj av standarder för LAN och MAN (*Metropolitan Area Network*). Familjen innefattar ett flertal standarder och tillägg till standarder. 802.11 definierar upp det fysiska lagret och MAC-lagret för WLAN-delen av 802-standarden (Figur 2). Inom 802.11 finns tre olika fysiska lager. Det grundläggande som vidareutvecklats med 802.11b, 802.11a och 802.11g. Kombinationerna av 802.11/802.11b och 802.11a/802.11h är de utrustningsstandarder som i första hand kommer att behandlas eftersom dessa är de dominerande på marknaden idag och de som troligen kommer att dominera marknaden för 802.11-produkter under den närmaste framtiden [Keene 2002].

Fysiska lager i 802.11:

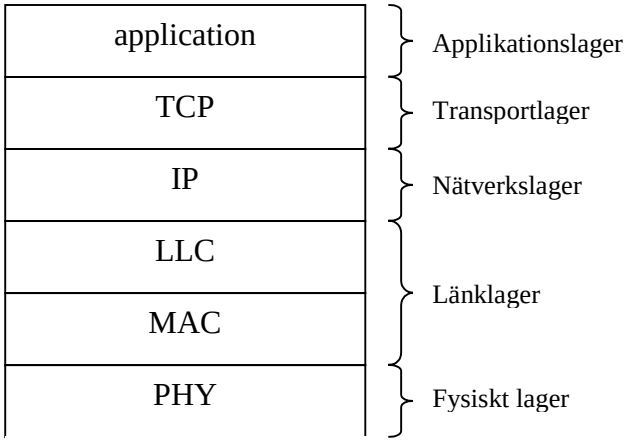
- Grundläggande med DSSS, 2,4 GHz
  - 802.11b (11 Mbit/s)
- Vidareutvecklat fysisk lager, 2,4 GHz
  - 802.11g (54 Mbit/s)
- 5 GHz-lagret
  - 802.11a (54 Mbit/s)
  - 802.11h (54 Mbit/s)



Figur 1. 802-standarden Källa: [IEEE 802.11 1999]

6.2.1. WECA / Wi-Fi

WECA (*Wireless Compability Alliance*, www.weca.net) är en organisation som arbetar för främjandet av trådlösa nät. WECA står bakom Wi-Fi-märkningen, en kvalitetsstämpel som betyder att utrustningen har testats utförligt och är kompatibel med 802.11-standarden. WECA certifierar även 802.11b- och 802.11a-utrustning [WECA 2002], vilket innebär att 802.11a-utrustning kan få Wi-Fi-stämpeln. 802.11b-utrustning kallas även ibland för Wi-Fi.



Figur 2. Protokollstacken i 802.11. Efter förlaga i [Schiller 2000].

6.2.2. 802.11

802.11-tekniken är en standardspecifikation för WLAN av IEEE som sätter upp specifikationer både för PHY-laget (fysiskt lager) och MAC-lagret (länklager). Det fysiska lagret kan använda RF-teknik (Radio) antingen som FHSS (*Frequency Hopping Spread Spectrum*) eller DSSS (*Direct Sequence Spread Spectrum*) [Champness]. Här används det licensfria ISM-bandet (*Industrial, Scientific, Medical*) som ligger vid 2.4 GHz. Även ett PHY-lager för IR finns.

802.11 är en relativt enkel teknik som skulle kunna kallas för ett trådlöst Ethernet med ett delat medium. En viktig skillnad är att Ethernet använder CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) medan 802.11 använder sig av CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Detta beror på att i ett vanligt Ethernet kan alla höra alla och därmed upptäcks en kollision. Därför är det okej att bara sända rakt ut i mediet utan att kolla om det är ledigt eller inte och sedan sända om ifall det skulle bli en kollision. I ett trådlöst nät kan inte alla höra alla och därmed kan inte alla kollisioner upptäckas. Därför är det bättre att använda Collision Avoidance, som går ut på att lyssna av mediet tills det är ledigt och sedan sända.

6.2.2.1. 802.11b

802.11b är en vidareutveckling av 802.11 DSSS i det fysiska lagret som höjer kapaciteten till 11 Mbit/s [IEEE 802.11b 1999]. Denna standard kallas 802.11 High Rate och det är denna standard som normalt menas när det talas om WLAN. 802.11 High Rate använder 8-bits CCK (*Complementary Code Keying*) samt några frivilliga funktioner för att förbättra prestandan.

6.2.2.2. 802.11a

Standarden 802.11a beskriver ett nytt fysiskt lager som jobbar i 5 GHz-bandet och ska tillåta datahastigheter på upp till 54 Mbit/s. Eftersom 5-GHz-bandet inte är fritt måste standarden vara förenlig med olika lagstiftningar [IEEE 802.11a 1999] kap 17). Lagret ska vara förenligt med existerande MAC-lager och vara en accessteknologi för data, röst och bildöverföring [IEEE 1997]. Tekniken har likheter med HiperLAN, men kommer att bli tillståndspliktig i EU eftersom den saknar effektreglering [PTS].

6.2.2.3. Övriga 802.11-standarder

802.11-teknologin är inte anpassad efter alla länder. 802.11d ska utöka den så att den passar olika regeldomäner (i praktiken länder) och beskriver även en mekanism för Roaming mellan olika regeldomäner [IEEE 802.11d 2001].

802.11e går ut på att förbättra det nuvarande MAC-lagret i 802.11 med QoS, samt att nyttja 802.11b och 802.11a för att skapa nätverk med högre prestanda som lämpar sig för trådlös video, ljud och annan mediadistribution [IEEE 1997]. [Parks 2001] påpekar också att standarden kommer att vara helt bakåtkompatibel med äldre 802.11b och 802.11a-utrusning.

802.11f är ett försök att standardisera hur accesspunkter fungerar för att möjliggöra kommunikation mellan accesspunkter från olika leverantörer för att skapa bättre distributionssystem [IEEE 1997].

802.11g ska vidareutveckla de fysiska lagret i 802.11b för att förbättra prestandan och samtidigt behålla kompatibilitet [IEEE 1997].

802.11h går ut på att förbättra 802.11 MAC och 802.11a med funktonalitet för network management och spectrum/power control främst för 5 GHz-trafik i licensband som kan kräva sådant. Man vill även

ha bättre kontroll på kanalerna [IEEE 1997]. Detta gör att 802.11h med största säkerhet kommer att bli fri att använda i EU eftersom de funktioner som gör 802.11a tillståndspliktigt finns i 802.11h [PTS].

802.11i går ut på att förbättra säkerhets- och authenticeringsmekanismer i 802.11 MAC [IEEE 1997]. Alternativ till WEP (*Wired Equivalent Privacy*) ska införas [Keene 2002].

6.2.2.4. Marknadsacceptans

802.11b är den standard som i praktiken används idag. Sökmotorn Altavista ger vid en sökning den 1/10 -02 322.470 träffar vid en sökning på 802.11b, jämfört med 61578 träffar för 802.11a, 9987 träffar för HiperLAN och 3433 träffar för Hiperlan2 och en översiktlig genomläsning av produktlistan på datorbutiken.com visar även att de accesspunkter och NIC:s (*Network Interface Card*) som säljs är 11 Mbit/s 802.11-produkter.

802.11a verkar vara nästa steg i utvecklingen. Produkter finns att köpa i dag. Enligt [Sony 2001] säljer Sony accesspunkter för 400$ och nätverkskort för 180$. D.v.s. den prisnivå som inte för så länge sedan kunde ses på 802.11b-utrustning. 802.11a saknar mekanismer för effektbegränsning, dynamisk frekvensval och har dålig frekvensspridning vilket gör att den kommer att vara tillståndspliktig att använda i EU (men fritt tillåten i USA). 802.11h har dock korrigerat dessa problem och denna utrustning kommer troligen att vara fri att använda inom EU. Detta innebär att 802.11h ur ett användarperspektiv kommer att upplevas på samma sätt som 802.11a [PTS].

6.2.2.5. Kapacitet och QoS-egenskaper

802.11b har en kapacitet på 11 Mbit/s. Detta betyder inte att en användare får en genomströmning på 11 Mbit/s. Protokoll och signalering lägger till ett signifikant overhead, vilket medför att den maximala genomströmningen för en ensam användare på en accesspunkt hamnar på ca 6 Mbit/s under goda förhållanden enligt [Geier 2002]. Blir det fler användare måste dessa dela på de 11 Mbit/s som finns. Dessutom är det ett känt faktum att vanliga Ethernet-nätverk (CSMA/CD) fungerar dåligt vid högre belastningar från många användare eftersom random access används samt att omsändning sker vid kollisioner. 802.11 påminner om Ethernet till sin grundläggande princip om ett delat medium och därför kommer liknande problem att finns i 802.11b.

Ett allvarligt problem i alla trådlösa nät är att paketförlusten pga. störningar ligger högt över paketförlusterna i trådbundna nät. [Schiller 2000] talar om 1.000.000 gånger så många fel som i fiberkabel. Detta kan allvarligt påverka prestandan. Det s.k. "TCP over wireless"-problemet är ett utmärkt exempel på detta. I ett trådbundet IP-nät är dataförlusterna p.g.a. störningar små - det är mycket troligare att ett förlorat paket beror på trafikstockning (congestion) i näten eftersom IP slänger paket vid congestion. TCP-protokollets congestion control (trafikstockningskontroll) är anpassat för trådbundna nät och antar automatiskt att ett borttappat paket beror på congestion och sänker drastiskt överföringshastigheten vilken sedan långsamt ökar igen. Detta fungerar bra i trådbundna nät där antagandet är sant, men i trådlösa nät hade en annan hantering varit mycket bättre. Resultatet kan bli usla TCP-prestanda under dåliga sändningsförhållanden.

Eftersom 802.11b i MAC-lagret använder sig av CSMA/CA och exponential backoffs när mediet är upptaget [Schiller 2000] innebär det att när en station vill sända lyssnar den av mediet och om det är ledigt sänder den. Är det inte ledigt väntar den en tidsperiod och försöker igen. För varje misslyckat försök ökas väntetiden (congestion windows), men inte högre än till ett maxvärde (cwmax), innan ett nytt sändningsförsök görs. Tekniken aldrig kan garantera någon som helst maximal överföringstid eller genomströmning. 802.11-standarden som består av PHY och MAC-lager kan som en följd av detta aldrig garantera någon som helst QOS vad gäller genomströmning eller maximal sändningstid. Däremot går det med hjälp av högre lager ge t.ex. leveransgaranti. TCP är ett utmärkt exempel på detta.

Ett annat problem som förtjänar att nämnas är risken för störningar. Eftersom 802.11b använder det fria ISM-bandet på 2.4 Ghz finns det risk att andra licensfria sändare kan störa trafiken. [Molta 2001] räknar upp trådlösa telefoner och bluetooth-apparater som möjliga störningskällor. Vanliga mikrovågsugnar ligger också i samma frekvensområde och borde kunna orsaka störningar.

802.11a definierar endast ett nytt fysiskt lager till 802.11-standarden. Det fysiska lagret, som sänder i 5 GHz-området. Lagret höjer datahastigheten till maximalt 54 Mbit/s men i övrigt används samma MAC-lager som i 802.11b. Det innebär att det är samma overhead som i 802.11b och bandbredden måste delas. [Molta 2001] gör en mindre undersökning av datagenomströmning som bekräftar detta då en genomströmning på 27.1 Mbit/s uppmäts. Några nya QoS-mekanismer finns inte implementerade i 802.11a.

Den möjlighet till QoS som verkar ligga närmast till hands för 802.11 är den som skapas i standarden 802.11e och som kommer att fungera tillsammans med både 802.b och 802.11a-utrustning. Därmed är det en rimlig slutsats att även 802.11h kommer att kunna ta del av samma stöd för QoS.

6.2.3. Säkerhetsaspekter

Ett radionät har ur säkerhetssynpunkt betydligt sämre grundförutsättningar än ett trådbundet nät. Radiovågor sprids, så att lyssna av trafiken på ett trådlöst nät är betydligt enklare än att bryta sig in i ett trådbundet nät. Vem som helst sända till nätet och det är mycket enklare att störa ut ett trådlöst nät än ett trådbundet. Kopparkabel och ändutrustningar för fiber kan visserligen störas, men det är långt ifrån lika enkelt som att störa ett trådlöst nät. Fiberkablar är mycket svåra att störa. En fördel med trådlösa nät är dock robustheten. Vid t.ex. en jordbävning kan kablage slitas sönder medan ett trådlöst nät fortfarande fungerar [Schiller 2000].

För att hantera några av dessa problem har 802.11 två huvudsakliga skydd: En krypterande inkapsling, WEP (*Wired Equivalent Privacy*) ska simulera samma säkerhet som i ett trådbundet nät. En authenticeringsalgoritm, *Shared Key Authentication*, ska simulera fysisk accesskontroll genom att hindra icke-authenticerad åtkomst [Walker 2001]. Tyvärr lider dessa system av fundamentala designfel. [BGW 2001] menar att detta beror på att systemen utvecklats utan allmän insyn och testning och därför har dessa fel kunnat gå igenom. En öppen prövning skulle med största säkerhet ha avslöjat dem.

Felen ger mycket stora konsekvenser på säkerheten i näten. Enligt [Walker 2001] uppnås inget av designmålen med säkerhetsmekanismerna. En angripare kan relativt enkelt ändra i krypterade paket [Walker 2001], passivt dekryptera trafik baserat på statistik analys, lura accesspunkter i syfte att dekryptera trafik och skicka in trafik från icke-authenticerade stationer i syfte att dekryptera trafik, enligt [BGW 2001]. [Walker 2001] hävdar att en angripare efter en dags trafikanalys har fått in tillräckligt med data för att dekryptera nätverkstrafiken i realtid med en dictionary-attack.

Arbete pågår inom IEEE för att förbättra säkerheten och 802.11i är en ansträngning för att införa alternativ till WEP. Hur långt detta har kommit i dagsläget är oklart, men troligen är det en bit kvar eftersom WEP knäcktes under 2001. Det bör noteras att användandet av de inbyggda säkerhetssystemen i 802.11 är frivilligt och om de inte är påslagna så är näten helt vidöppna för intrång.

6.3. HiperLAN

6.3.1. Beskrivning av tekniken

HiperLAN (*High Performance Radio Local Area Network*) är en familj av standarder som utvecklats av ETSI (*European Telecommunications Standards Institute*, http://www.etsi.org/). De fyra standarder som finns är HiperLAN/1, HiperLAN/2, HiperLAN/3 (numera HIPERACCESS) och HiperLAN/4 (numera HIPERLINK) och de är skapade för olika sorters nät. Deras gemensamma nämnare är integrationen av tjänster för tidskänslig dataöverföring [Schiller 2000].

6.3.1.1. HiperLAN/1

Standarden HiperLAN/1 skapades av ETSI 1996 som ett WLAN med stöd för ad-hoc-nät och infrastrukturbaserade nät. Standarden stödjer forwardingmekanismer, topology discovery, kryptering och energibesparingsfunktionalitet samt de funktioner för dynamiskt frekvensval som krävs för att utrustningen ska få användas licensfritt i Europa [PTS 2002-06]. Datahastigheten är 23.5 Mbit/s. Tyvärr har tekniken inte fått något kommersiellt genomslag. Enligt [Hayes 2000] fanns det 1999 i praktiken inga HiperLAN/1-produkter på marknaden och IEEE vill använda frekvensbanden som reserverats för HiperLAN/1 till 802.11a och HiperLAN/2 istället. En sökning på nätet efter HiperLAN/1-produkter idag (oktober 2002) ger få träffar och [Judge 2001] talar om kollapsen bakom HiperLAN. Det verkar som HiperLAN/1 har hamnat på teknologins soptipp.

6.3.1.2. HiperLAN/2

HiperLAN/2 är en WLAN-standard som är baserad på ATM och skulle kunna liknas vid ett trådlöst ATM på samma sätt som 802.11 kan liknas vid trådlöst Ethernet [GHAR 2002]. En av tankarna bakom HiperLAN/2 är att näten ska vara ett komplement till 3G-näten och kunna ta över från UMTS/WCDMA-näten som databärare i hotspots där användarna ska kunna få extra hög kapacitet. När användarna går utanför hotspotens räckvidd ska andra nät ta över [Bergljung 2002]. Det är, som bekant, den vision om 4G som råder i dagsläget - en mängd nät med roaming emellan. Detta gör att nätet stödjer QoS och roaming mellan olika nät. Datahastigheten ligger på 56 Mbit/s. Den främsta konkurrenten på marknaden är 802.11a men HiperLAN/2 har bättre prestanda (ca 3,5 ggr högre genomströmning i praktiken enligt [Bergljug 2002]) och egenskaper. Marknadsläget är dock oklart, inga eller extremt få produkter verkar finnas att köpa idag och risk finns att HiperLAN/2 blir utslaget [GHAR 2002].

6.3.1.3. HIPERACCESS

HIPERACCESS är en specifikation för ett snabbt accessnätverk/BRAN (*Broadband Radio Area Network*) som ska vara den sista länken mellan operatörer och kunders egna nät. Näten är tänkta att vara stationära och fungera som ersättare till t.ex. kabelmodem. Datahastigheten uppgår till 25 Mbit/s och räckvidden är 5 km. [Schiller 2000]. Frekvensområdet är 40,5 - 43,5 GHz [ETSI h1]. I en pressrelease [ETSI 2002] hävdar dock ETSI att hastigheten ska nå upp emot 100 Mbit/s. HIPERACCESS stödjer, liksom HiperLAN/2, ATM:s trafikklasser [Schiller 2000]. Tekniken är mindre intressant ur ett mobilitetsperspektiv och kommer därför inte att behandlas ytterligare.

6.3.1.4. HIPERLINK

HIPERLINK är en teknik för att skapa trådlösa point-to-point-länkar mellan två noder, t.ex. HiperLAN2-noder eller HIPERACCESS-noder. Datahastigheten är 155 Mbit/s och räckvidden 150 m. Frekvensbanden ligger vid 17 GHz. Inget arbete på standarden har påbörjats ännu [ETSI h1]. Även HIPERACCESS stödjer, liksom HiperLAN/2, ATMs trafikklasser [Schiller 2000]. Denna teknik är ej heller intressant ur ett mobilitetsperspektiv och kommer ej att behandlas vidare.

6.3.2. Tekniska egenskaper

6.3.2.1. Marknadsacceptans

HiperLAN2 global forum är en sammanslutning av organisationer som jobbar för att driva på utvecklingen för HiperLAN2. Tyvärr ser det mörkt ut för HiperLAN2 i kampen mot dess största konkurrent, 802.11a. Trots extensivt sökande på nätet har vi inte lyckats hitta några HiperLAN/2-produkter på marknaden ännu. Det närmaste en produkt vi hittat är en demonstration av HiperLAN/2 som Panasonic höll på CeBIT 2002 [Bergljung 2002]. [GHAR 2002] hävdar dessutom att Ericsson dragit sig ur HiperLAN2 Global Forum och numera stödjer 802.11a. 802.11a har problem med att den kräver tillstånd i Europa, men enligt [PTS 2002-06] är 802.11a-utrustning som arbetar i frekvensbandet 5150-5250 MHz, har en maximal uteffekt på 200 mW och endast används inomhus icke tillståndspliktigt i Sverige sedan den 1:a januari 2002. 802.11h-standarden ska modifiera 802.11a att den blir helt fri att använda och om sådana produkter kommer ut på europamarknaden före HiperLAN/2 är det rimligt att anta att det blir problem för HiperLAN/2. [GHAR 2002] hävdar också att 802.11a har bättre förtroende hos användarna som redan är vana vid 802.11b och en starkare marknadsförande organisation bakom sig.

6.3.2.2. Kapacitet och QoS-egenskaper

Datahastigheten i det fysiska lagret ligger på 54 Mbit/s i HiperLAN/2. Det betyder dock inte att det är den genomströmning som ges vid vanlig sändning av data, utan ett signifikant overhead finns alltid.

[Bergljug 2002] visar en prestandajämförelse mellan HiperLAN/2 och 802.11a. Vid jämförelsen skickas 512 byte stora paket med en datahastighet av 54 Mbit/s. HiperLAN/2 får då en genomströmning på 42 Mbit/s medan 802.11a endast kommer upp i 12 Mbit/s. Detta beror på två saker. 1) HiperLAN/2 har bättre genomströmning än 802.11a i grunden och 2) Genomströmningen i 802.11a beror på paketstorleken. Om datahastigheten sätts lägre blir skillnaden mellan 802.11a och HiperLAN/2 mindre. Överlag kan det dock sägas att HiperLAN/2 har en mycket bra genomströmning oavsett datahastighet.

HiperLAN/2 har inbyggt stöd för ATMs trafikklasser vilket innebär att stöd för QoS finns. Systemet är kretskopplat (circuit switched) liksom ATM och vanliga telefonnät. Motsatsen är paketkopplade (packet switched) nätverk som Ethernet och IP. Varje koppling kan tilldelas specifika bandbredder, delays, error rates och prioritetsnivåer vilket gör HiperLAN/2 ytterst lämpat för applikationer som kräver vissa tjänstegarantier för att kunna fungera bra, exempelvis IP-telefoni och telekonferenser.

6.3.2.3. Säkerhetsaspekter

[Johnsson 1999] hävdar att HiperLAN/2 har stöd för både authenticering och kryptering. Både accesspunkterna och de mobila terminalerna kan authenticera varandra, men systemet är inte inbyggt i HiperLAN/2, utan istället måste en extern funktion som t.ex. en katalogtjänst användas. Den kryptering som troligen kommer att används DES eller 3DES.

6.3.2.4. Kompabilitet och användarevänlighet

HiperLAN/2 är inte kompatibelt med 802.11a även om de fysiska lagren liknar varandra. HiperLAN/2 är dock designat för att samverka med en mängd andra nätverkstyper såsom Ethernet, ATM, GRPS, UMTS och IEEE 1394 (FireWire). För att uppnå detta användes ett konvergenslager i HiperLAN/2-stacken [Bergljug 2002].

6.4. GSM / GPRS

6.4.1. Beskrivning av tekniken

GSM är en standard för digital mobiltelefoni. Utvecklingen av GSM startade 1982 då CEPT (*Conference of European Posts and Telegraphs*) startade en grupp kallad *Groupe Speciale Mobile* för att utveckla ett mobilt telefonsystem. I början på 80-talet fanns det ett flertal analoga system runt om i Europa med varierande kvalité. Det denna grupp fick till uppgift var att skapa ett mobilt system som kunde erbjuda en bra ljudkvalité, låg kostnad både för installation och underhåll och möjlighet att enkelt utöka antalet tjänster. 1989 tog ETSI *(European Telecommunication Standards Institute)* över ansvaret att utveckla GSM vidare och förkortningen GSM fick en ny betydelse, Global System for Mobile communications [GSM 1995].

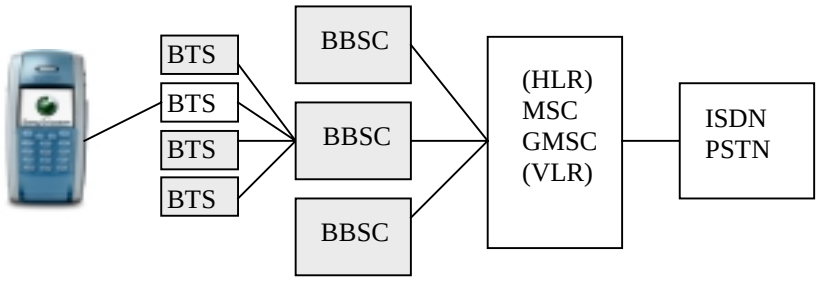
Det första kommersiella GSM nätverket lanserades år 1991 och är idag den snabbast växande mobilstandarden. I mitten av 90-talet hade tekniken lanserats i ett 60-tal länder och med över 5.4 miljoner. GSM-nät finns idag i över 169 länder och beräkningar visar på att antalet användare uppgår till 787,5 miljoner. I slutet av år 2003 beräknas antalet GSM-användare uppgå till 805,3 [GSM 2003].

GSM använder sig av TDMA (*Time Division Multiple Access)* vilket innebär att en kanal delas in i så kallade TDMA-frames som i sin tur delas in i åtta tidsluckor. Detta gör att upp till åtta användare kan utnyttja samma frekvensområde.

En annan tänkbar teknik för att dela på mediet är FDMA (*Frequency Division Multiple Access)* , som används för att dela upp ett frekvensband i flera mindre frekvensband som inte överlappar varandra i ett område.

6.4.2. Komponenter

Ett GSM-nätverk består av ett antal komponenter med olika funktionalitet:



Figur 3: Förenklad schematisk bild över ett GSM-nät

En basstation är en stationär radiosändare som har förbindelse med det fasta nätet (via tråd, kabel, optofiber eller radiolänk) och håller kontakt över radio med mobila enheter i sitt närområde, som brukar kallas en cell. Genom att ha många basstationer med angränsande celler går det att åstadkomma ett stort, yttäckande nät. När en mobilterminal flyttar sig mellan olika basstationer inom en operatörs nät kallas det handover, medan växlingen mellan operatörers nät kallas roaming. Figur 3 visar en schematisk bild över ett GSM-nät. Basstationen består av två delar, BTS (*Base Transceiver Station*) och BSC, *Base Station Controller*. BTS är den del av basstationen som sänder och tar emot signaler från terminaler. BSC håller koll på ett flertal BTS och sköter handover mellan BTS.

För att en mobil terminal ska fungera måste den ha ett SIM-kort. SIM-kortet gör det möjligt att identifiera sig mot operatören och innehåller en del parametrar, däribland användarens IMSI,

International Mobile Subscriber Identity, som unikt identifierar SIM-kortet. SIM-kortet skyddas av en fyra siffrors PIN-kod och en av fördelarna är att detta kort enkelt kan byta terminal genom att flytta kortet.

För att sköta kommunikationen mellan två mobila terminaler används ett subsystem kallat NSS (*Network and Switching Subsystem*). Systemet innehåller bland annat databaser för att lagra information om mobila användare och består av följande komponenter:

- MSC, *Mobile Switching Center,* används för att leda en signal genom nätverket från en användare till en annan.
- GMSC, *Gateway Mobile Switching Center* sköter kopplingen till andra typer av nätverk så som det fasta nätet eller en annan operatörs nät.
- HLR, *Home Location Register*. När en viktig databas som håller reda på information om en användare. När en mobil terminal kopplas på är det här den registreras och om användaren är giltig kan han sedan börja utnyttja nätverket.
- VLR, *Visitor Location Register*, när en mobil terminal rör sig till en ny BTS frågar VLR efter användarens information från HLR. Processen kallas handover och gör det möjligt för HLR att skicka en inkommande signal till rätt BTS.

6.4.3. Tjänsteutbud

En mycket viktig tjänst som GSM kan erbjuda är det nödnummer som gör det möjligt att kalla på räddningstjänsten, ambulans eller polisen. Detta nummer har högsta prioritet i GSM-nätet vilket gör att den kan avbryta andra pågående samtal för att komma fram. Samma nummer (112) kan också användas över hela Europa och kopplar automatiskt upp sig till närmsta räddningstjänst och är helt gratis.

En av de största och snabbast växande tjänsterna inom GSM är SMS (*Short Message Service)* som går ut på att skicka korta textmeddelanden (upp till 160 tecken) mellan mobiltelefoner. SMS lanserades i mitten på 90-talet men intresset var svalt. Inte förrän 1999 började antalet SMS-meddelanden ta fart. Antalet har ökat från 150 miljoner 1999 till 473 miljoner 2000 och hela 1,02 miljarder meddelanden 2001 [PTS 2002:11].

I Västeuropa beräknar bedömare att det kommer skickas 186 miljarder sms-meddelanden och antalet beräknas bli 365 miljarder under 2006. Ökningstakten kommer dock minska under kommande år då MMS *(Multimedia Messaging Service)* väntas ta över vartefter telefoner med stöd för MMS införs [CS 2002].

SMS-tjänsten, som till en början endast fungerade för att skicka enkla textmeddelanden, har idag ett flertal andra användningsområden tjänsten [PTS 2002-08].

- Ringsignaler och logtyper kan sändas och tas emot.
- Spel, enligt en undersökning spelar 36% av användarna spel på sin mobil och en del av dessa spel är SMS-baserade.
- Interaktiva tjänster, röstning via SMS i samband med TV-program är troligen den vanligaste interaktiva tjänsten.
- Tjänster som talar om var närmaste apotek, blomsteraffär, bank och restaurang finns att tillgå.
- Nummerupplysning.
- Nyheter, väder och sportresultat.
- Påminnelser, omkring 250 personer dör varje år och mer än hälften av alla astmatiker i Sverige tar inte sin medicin enligt ordination. Ett SMS påminner patienten då det är dags att ta den. Enligt en utvärdering av denna tjänst anser 41% sig var hjälpta av tjänsten [PTS 2002-08].

SMS är en tjänst som endast erbjuder meddelanden byggt på text. EMS, *Enhanced Message Service*, däremot är en förbättrad version av SMS som erbjuder möjlighet att även skicka bilder, ljud, animationer och olika typsnitt. EMS kan också använda sig av samma infrastruktur som SMS använder idag. Nästa steg i utvecklingen av SMS-tjänster är MMS, *Multimedia Message Service*, som förutom att ha EMS möjligheter, även kommer kunna skicka video. Operatörer som i framtiden tillhandahåller EMS eller MMS kan också ta mer betalt per meddelande då dom sänder större datamängder vilket ger ett mervärde till användaren [EMS 2001]. MMS kräver dock högre överföringskapacitet än SMS för att fungera bra och är därför mer lämplig i kommande 3G-nät.

Dessa tjänster underlättar för en fortsättning inom den mobila marknaden då man kan se tjänsterna som en introduktion till mer avancerade funktioner i 3G. Användarnas kunskap ökar och det kan vara en viktig del för övergången från dagens GSM-system till UMTS.

En teknik som erbjuder tjänster via GSM-nätet är WAP (*Wireless Application Protocol)* som gör det möjligt att med mobiltelefonen surfa på Internet i textformat. Några andra tjänster som går att använda idag är att skicka email och handla med aktier. För att få detta att fungera krävs en relativt ny telefon med stöd för WAP. WAP-protokollen liknar i stor utsträckning de redan befintliga Internetstandarderna XML, IP samt UDP och är optimerade för små terminaler med begränsad bandbredd som exempelvis mobiltelefoner. WML (*Wireless Markup Language)* används för att skapa sidor som kan användas genom WAP-protokollen.

6.4.4. Tekniska egenskaper

6.4.4.1. Kapacitet och QoS-egenskaper

I det ursprungliga GSM-nätet kunde data sändas med en hastighet av 9,6 kbps och i början av 90-talet räckte det till mer än väl. Men allt eftersom trafiken och behovet av snabbare överföringshastigheter har ökat har det visat sig att kapaciteten inte räcker till i dagens GSM. Några operatörer idag kan erbjuda upp till 14.4 kbps. En möjlighet för att öka överföringskapaciteten finns idag och kallas GPRS (*General Packet Radio Service)* och med denna teknik är det möjligt att komma upp till en teoretisk hastighet kring 115 kbps genom att uppgradera befintliga GSM-nät.

GPRS bygger på paketkopplad kommunikation och möjlighet att utnyttja sändarkapaciteten mellan basstation och terminalen på ett nytt sätt. Istället för att ockupera en hel trafikkanal under hela uppkopplingstiden, skickas data istället i små paket när det behövs. Användaren utnyttjar bara kapacitet när information laddas hem eller skickas, vilket gör ständig uppkoppling möjlig. Med det vanliga GSM-systemet får varje användare tilldelat en tidslucka i en TDMA-frame vilket gör att i de fall användaren är ensam på basstationen används endast en åttondel av kapaciteten. I GPRS däremot kan du få mellan en åttondel till hela kapaciteten i en TDMA-frame. Detta gör att det teoretiskt går att komma upp till åtta gånger hastigheten för vanliga GSM vilket blir 115,2 kbps istället för 14,4 kbps.

I GPRS är det möjligt att specificera en viss QoS (*Quality of Service)* genom att skapa ett antal profilklasser som användare delas in i. Den ena klassen *Reliability* delas användare in i grupper vilken nivå av feltolerans som dom tål. Den andra klassen *Delay* avgör hur mycket försening kommunikationen tål innan det ställer till problem för användaren.

HSCSD (*High Speed Circuit Switched Data)* är en föregångsteknik till GPRS som även den bygger på att använda fler än en tidslucka per TDMA-frame. Denna teknik gör det möjligt att använd tre luckor istället för en vilket gör att hastigheten kan komma upp till 57,6 kbps. HSCSD är dock endast till för data och inte för samtal.

En annan teknik för att förbättra kapaciteten i existerande GSM-nät är EDGE (*Enhanced Data GSM Environment*) som gör det möjlig att komma upp i 384 kbps genom att uppgradera mjukvaran och

hårdvaran i det nät som finns idag. Om GSM kallas andra generationens mobilsystem (2G) kallas GPRS motsvarande 2,5G och EDGE 2,75G. Både GPRS och EDGE utgör en möjlighet för operatörer att fortsätta utnyttja befintligt GSM-nät i en framtida UMTS (3G) satsning. En skillnad gentemot GPRS är att EDGE kräver uppgradering av hårdvaran och tar därmed längre tid och blir kostsammare att införa. En av anledningarna att EDGE kommer upp i höga hastigheter är att det finns en mycket effektiv hantering av paketförluster och annan felhantering [Ericsson 2002].

Dagens GSM-nät är baserat på olika frekvenser beroende på var i världen nätet är installerat. Detta är en nackdel ur användarens perspektiv då frekvensen som används i Europa är 900 och 1800 MHz och 1900 MHz i USA vilket göra att en mobiltelefon från USA inte fungerar i Europa och vice versa. Dessa frekvenser delas upp i block om 200 KHz, där varje block kallas för en kanal. GSM använder sig av full duplex vilket innebär att det både går att sända och ta emot signaler samtidigt. När man pratar om GSM vid 900 MHz betyder det egentligen att signaler sänds i frekvensområdet 890-915 MHz och tas emot i frekvensområdet 935-960 MHz.

6.4.4.2. Säkerhetsaspekter

Vad gäller säkerheten i dagens GSM-telefoner ger en digital signal ett bättre skydd mot avlyssning än tidigare analoga tekniker tack vare kryptering. GSM-tekniken använder sig, förutom kryptering, också av ett flertal frekvenser då en signal sänds vilket gör att den blir svårare att avlyssna.

Identifiering av användaren sköts genom en hemlig nyckel lagrad i SIM-kortet och hos ett speciellt identifieringscenter. Identifieringscentret skickar ett slumpvärde till användarens terminal och med hjälp av nyckeln lagrad i SIM-kortet skickar terminalen tillbaka ett svarsvärde beräknat enligt en viss algoritm. När svarsvärdet kommer tillbaka utför identifieringscentret en liknande beräkning på slumpvärdet och användarens hemliga nyckel och om det värdet stämmer överens med svarsvärdet från användare är användaren identifierad. Användarens SIM-kort använder sedan samma slumpvärde och nyckel för att skicka och ta emot data krypterat. För att ytterligare undvika att signalen blir avlyssnad ändras detta slumvärde kontinuerligt [GSM 2002].

6.5. UMTS

6.5.1. Beskrivning av tekniken

När GSM-näten i början av 90-talet startades upp räckte kapaciteten i näten till mer än väl och funktionen att kunna ringa mobilt var fullt tillräcklig. Men allt eftersom fler användare skaffat mobiltelefon och blivit mer tekniskt kunniga har ett behov av fler tjänster och bättre kapacitet kommit att öka allt mer. GSM är i första hand en teknik som riktar sig till rösttrafik, men i och med att SMS (*Short Message Service)* införts och blivit en populär tjänst har mängden datatrafik ökat. Medan GSM är ett system byggt för rösttrafik är UMTS (*Universal Mobile Telecommunications System)* ett system anpassat både för samtals- och datatrafik.

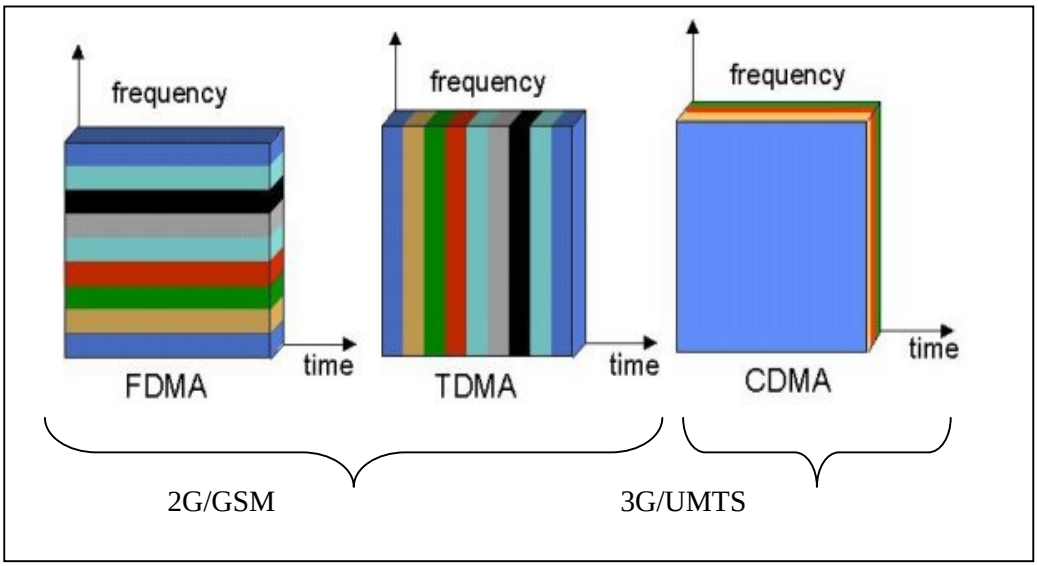
GSM, där G står för *Global*, var i början tänkt att bli ett globalt mobilsystem där en terminal skulle fungera över hela världen där det fanns täckning. Detta blev dock aldrig verklighet då länder beslutade att använda olika frekvensområden för GSM-systemet vilket medförde att en svensk mobiltelefon ej fungerar i tex. USA. Det finns dock en teknik kallad dualband som gör det möjligt att använda sig av två olika frekvenser i samma telefon.

UMTS är en av teknikerna kring tredje generationens mobilsystem och efterföljaren till GSM. Tekniken innebär att IP-baserade tjänster kombineras med mobil access till Internet. Avsikten är att användarna ska kunna koppla upp sig, oavsett var de befinner sig, från sin bärbara terminal och utöver vanlig telefoni även få tillgång till datakommunikation och multimedia.

3G innebär att en användare ständigt kan vara uppkopplad, vilket gör att exempelvis e-post omedelbart kommer att kunna laddas ner i terminalen. Meningen är att 3G ska kunna erbjuda multimedia och dataöverföringstjänster med en teoretisk hastighet på 144kbit/s i ett fordon som rör sig fort, 384 kbit/s i ett fordon som rör sig långsamt och 2 Mbps om terminalen är stationär. UMTS ingår som en del i ITU:s (*International Telecommunications Unions)* IMT-2000 familj.

ITU är en internationell oberoende organisation där myndigheter och den privata sektorn kan arbeta tillsammans för att styra telekommunikationens utveckling och tjänsterna som erbjuds. Organisationen startades redan år 1865 då det fanns ett behovet av samordning mellan olika telegrafsystem. ITU har sedan dess verkat för att standardisera tekniker och utrustning mellan regioner [ITU 2002]. 1999 godkände ITU 3G som en industriell standard. Den fick namnet IMT-2000 (*International Mobile Telecommunications-2000*) och består bland annat av de tre CDMA-teknikerna CDMA2000, WCDMA och TD-SCDMA [3G 2001]. Dessa tre tekniker har sitt ursprung i CDMA (*Code Division Multiple Access*).

CDMA (*Code Division Multiple Access*) används för att sprida signalen över en större bandbredd, se figur 4. Varje signal får också en egen identifierare som ser till att rätt signal når mottagaren. Att sprida ut signalen över fler frekvenser gör att fler mobilanvändare kan använda systemet samtidigt. Signalen blir mindre känslig för störningar, kräver mindre energi och den har också den fördelen att det blir svårare att avlyssna. Tekniken utvecklades teoretiskt redan under andra världskriget av militären men det tog över 40 år innan tekniken kunde användas praktiskt i civilt bruk [CDG 2002].



Figur 4: Visar sändningstekniker som används för mobila system [UMTS W].

Företaget som insåg CDMA:s potential var Qualcomm (www.qualcomm.com) som grundades 1985. Det första kommersiella CDMA-nätet installerades 1995. Vid denna tidpunkt hade många länder i världen redan ett fungerande GSM-nät. Medan GSM utvecklades i Europa utvecklades CDMA i USA vilket medförde att GSM blev starkare i Europa än i USA. En viktig skillnad mellan teknikerna är att Qualcomm tar en avgift för varje produkt som är baserad på CDMA-teknik medan GSM är en öppen standard. Detta har gjort att GSM lättare fått genomslag i övriga världen [Salami 2002].

I nästa generations mobilsystem kommer CDMA-tekniken utgöra grunden i de olika tekniker som ingår i IMT-2000. En av dessa är CDMA2000 som bygger vidare på en 2G-teknik kallad CDMA-One. Med CDMA2000 är det möjligt att bygga vidare på existerande CDMA-One-nät vilket har gjort att CDMA2000-nät finns kommersiellt på marknaden redan idag. Hösten 2000 installerades det första 3G-nätet i Sydkorea och tekniken som användes var just CDMA2000. Genom att använda befintlig infrastruktur har CDMA2000 fått en konkurrensfördel gentemot UMTS som använder WCDMA.

UMTS är ett system utvecklat av ETSI (*European Telecommunication Standardisation Institute)* för att utgöra Europas förslag till tredje generationens mobilsystem. UMTS har även blivit en av teknikerna som accepterats av ITU att ingå i IMT-2000. Utvecklingen drivs av 3GPP, *3rd Generation Partnership Project,* som är ett projekt där tillverkare, operatörer och standardiseringsorganisationer gemensamt tar fram en standard för UMTS. Till 3GPP har ett stort antal organisationer och tillverkare runt om i världen anslutit sig vilket gör att UMTS har god chans att bli det dominerande 3G-systemet i framtiden.

UMTS består rent tekniskt av tre delar: User Equipment, UTRAN och Core Network. User Equipment är helt enkelt de mobilterminaler som stödjer UMTS och dess frekvensområde. Core Network sköter switching och routing av datapaket i systemet medan UTRAN (*UMTS Terrestial Radio Access Network)* sköter överföringen av data mellan en terminal och Core Network. Mellan UTRAN och Core Network används ATM (*Asynchronous Transfer Mode)* som gör det möjligt att sända synkron eller asynkron data i ett kretskopplat eller paketkopplat nät. I UTRAN används WCDMA (*Wideband Code Division Multiple Access*) som radio interface. WCDMA har två grundläggande tillstånd: FDD (*Frequency Division Duplex*) och TDD (*Time Division Duplex)*. FDD är optimerad för att täcka ett stort område medan TDD är optimerad för att täcka mindre områden med högre belastning. Båda tillstånden klarar hastigheter upp till 2 Mbps.

Kina har nyligen beslutat att införa en teknik kallad TD-SCDMA (*Time Division Synchronous Code Division Multiple Access*) som kombinerar TDMA-tekniken med avancerade CDMA-komponenter. Hastigheten i nätet varierar från 1,2 kbps upp till 2 Mbps och terminalerna och basstationerna har smarta antenner som riktar in signalen vilket gör att risken för störning minskar [TD-SCDMA 2002].

6.5.2. Tekniska egenskaper

6.5.2.1. Kapacitet och QoS-egenskaper

UMTS erbjuder multimedia och dataöverföringstjänster med en teoretisk hastighet på minst 144kbit/s. Kvaliteten ska vara jämförbar med den fasta telefonin. UMTS har fyra QoS-klasser [UTMS 2002]:

- conversational class – tidskritiska applikationer eller tal som kräver realtid.
- streaming class – Strömmande media så som video som kräver realtid.
- interactive class – Web-surfning, best effort.
- background class – Email, fax som inte är tidskritiska, best effort.

Förutom dessa QoS-klasser går det även att få QoS när det gäller trafiken och dess egenskaper. Exempel på dessa är:

- Maximum BIT-rate
- Guaranteed BIT-rate
- Delivery order
- Transfer delay
- Traffic priority

6.5.2.2. Säkerhetsaspekter

Säkerheten inom UMTS bygger vidare på säkerheten inom GSM där några områden har förbättrats. Användarens identitet, var han befinner sig och att han inte kan spåras är något som garanteras i UMTS. När det gäller säkerheten i nätverket har den indelats i fem områden [UMTS 2003]:

- Network access security – skyddar från otillåten access till nätet och de tjänster som erbjuds.
- Network domain security **–** Erbjuder säkerhet när data överförs från en domän till en annan.
- User domain security – erbjuder säkerhet i överföringen mellan användare och basstation.
- Application domain security – Sköter säkerheten mellan applikationer som utbyter data mellan domäner.
- Visibility and configurability of security – Informerar användaren om vilket typ av säkerhet som för närvarande används samt den säkerhetsnivå som rekommenderas för en viss typ av tjänst.

6.5.3. 802.11

802.11b är den WLAN-teknik som är absolut störst idag och produkterna är tillgängliga till konkurrenskraftiga priser. Tyvärr är dock kapaciteten dålig - de 11 Mbit/s i delad kapacitet som erbjuds ligger långt ifrån den prestanda som trådbundna nät kan erbjuda. 100 Mbit/s switchat Ethernet är vanligt idag och Gigabit Ethernet är på ingående. TCP-över-wireless-problemet ger försämrade prestanda över trådlösa förbindelser, vilket påverkar alla tjänster som använder TCP, t.ex. vanligt surfande över http. Ett trådlöst nät kan idag inte ens komma i närheten av den prestanda som finns i ett modernt Ethernet. Jämför man med trådlösa nät ligger ett 802.11b-näts datahastighet på 11 Mbit/s långt över de 115.2 kbit/s som GPRS kan ge, 384 kbit/s som EDGE-tekniken ger och de 2 Mbit/s som det talas om i UMTS. Man ska komma ihåg att dessa tekniker också använder ett delat medium.

Prestandaförbättringar är på gång och 802.11a säljs till rimliga priser i USA. Om 802.11a kommer att användas inom EU kommer det krävas licens. 802.11h-standarden kan lösa det problemet och ge 54 Mbit/s även i EU. En konkurrerande teknik är det europeiska HIPERLAN (*High Performance LAN*) som ligger i samma hastighetsklass. 802.11e ska lägga till QoS till 802.11 vilket kan öppna för nya tjänster. HIPERLAN1 kan kanske vara ett alternativ till 802.11e-tekniken.

Säkerheten i 802.11 är undermålig och går inte att lita på. Dels måste en administratör se till att WEP är aktiverat för att någon som helst säkerhet ska finnas på PHY/MAC-nivå och görs det är det ändå inte säkert då en målmedveten angripare lätt kan knäcka WEP. Därmed inte sagt att WEP är värdelöst - genom att aktivera WEP skapas i alla fall upp ett hinder för en eventuell angripare. Säkerheten måste dock garanteras av högre lager tills vidare. T.ex. kan man använda sig av SSL/TSL, IPsec eller någon VPN-lösning. Förhoppningsvis leder 802.11i-arbetet till bättre framtida säkerhet även på MAC/PHY-nivå.

6.5.4. HiperLAN/2

HiperLAN/2 är rent tekniskt en utmärkt standard. Genomströmning och säkerhet är utmärkta, fullt stöd för QoS finns och HiperLAN/2 går utmärkt att koppla mot andra sorters nätverk. Problemet är marknadsförutsättningarna - HiperLAN/2-produkter går inte att köpa idag till skillnad från 802.11a och det är inte alls otroligt att HiperLAN/2-standarden går samma öde till mötes som HiperLAN/1. En möjlighet är också att HiperLAN/2 får en del av marknaden i Europa. Skulle HiperLAN/2 lyckas etablera sig på marknaden så blir tekniken mycket relevant för mobilitet på grund av sina utmärkta tekniska egenskaper.

6.5.5. GSM/GPRS

GSM-tekniken har under 90-talet genomgått en enorm expansion. Från noll till 600 miljoner användare på 10 år talar sitt tydliga språk. Tekniken börjar dock kapacitetsmässigt ställa till problem i tätbefolkade områden. GPRS och EDGE löser dock detta under ytterligare ett antal år, men när UMTS

med sin höga hastighet kommer antågande får GSM se sig passerad av den nya tekniken. GSM kommer dock att leva sida vid sida med UMTS ett bra tag framöver.

Den tekniska lösningen med att reservera en hel kanal mellan två mobilanvändare ersätts med en utrymmeseffektivare lösning där en signal sänds bara när användaren verkligen pratar. Detta gör att betydligt fler kan samsas om samma frekvensområde vilket förbättrar kapaciteten i storstadsregioner.

När det gäller GPRS funktionalitet i praktiken har Erik Lorentzon och Håkan Fransson i smaband med ett examensarbete under hösten 2002 genomfört tester på de tre operatörerna som för tillfället erbjuder GPRS i Umeå. Resultatet av deras undersökning visar att kapaciteten över GPRS varierar högst avsevärt under testperioden och kan inte ses som pålitligt för affärskritisk verksamhet [Lorentzon+ 2002].

Vidare finner de att de mobila enheterna har en stor inverkan på överföringshastigheten vid GPRS. Kapaciteten beror på hur många tidsluckor enheten klarar av att hantera både på upp och nedlänk. Praktiska hastigheter kring 30 Kbit/s med nuvarande mobila enheter är nog vad som kan räknas med när alla parametrar räknats in.

6.5.6. UMTS

UMTS har ett två huvudkonkurrenter på marknaden. Den ena är TD-SCDMA som utvecklats för den kinesiska marknaden av kinesiska operatörer och ett antal operatörer såsom Motorola och Siemens. Den andra är CDMA2000 som har ett försprång på marknaden då övergången från CDMAOne (2G) till 3G endast innebär mindre uppgraderingar och därmed blir billigare då båda bygger på CDMA-teknik. CDMA2000 har redan installerats på ett par platser i världen. UMTS som utvecklas av 3GPP tar däremot längre tid att nå marknaden bland annat för att tekniken kräver mer förändringar på existerande system med GSM till UMTS vilket också gör att kostnaden ökar [3G 2002].

UMTS har dock en fördel då tekniken utvecklas av 3GPP som är ett samarbete mellan en rad ledande leverantörer och organisationer över hela världen. Detta gör att UMTS har en bredare förankring på världsmarknaden då många länder och tillverkare anslutit sig till UMTS. Declan Lonergan från the Yankee Group uppskattar att UMTS kommer få ungefär 80% av världsmarknaden för 3G medan CDMA2000 får övriga 20% [3G 2002].

När det gäller UMTS-utbyggnaden i Europa dras den med förseningar på grund av ett antal anledningar. En anledning är att nya terminaler med stöd för 3G inte lanserats i den utsträckning som det först var tänkt. Utvärderingen och testningen av de nya systemen har också dragit ut på tiden. Operatörer i Europa räknar med att påbörja lanseringen av UMTS i mitten på 2003 [Northstream 2002].

Vår slutsats när det gäller 3G-utvecklingen och UMTS är att den höga målsättningen med ett fungerande svenskt 3G-nät med 99,98% täckning i slutet av 2003 har varit god men lite väl optimistisk. Det fokuserats alldeles för mycket på tekniken och för lite på vilka tjänster som 3G i framtiden kan erbjuda. Enligt en rapport gjord av Northstream på uppdrag av PTS har operatörerna i Europa inte lyckats stimulera utvecklingen av 3G- tjänster i tillräcklig utsträckning. I dag finns det få avancerade mobildatatjänster i Europa. I Korea finns 3G-liknande tjänster, vars användning har stimulerats av avancerade telefoner och kreativ tjänsteutveckling [Northstream 2002].

7. Vetenskaplig fördjupning i Seamless roaming

Slutsatsen av de två första delmomenten, undersökningar av företaget Martinsson och marknadsundersökningen, var att en mobil IP-infrastruktur ligger tydligt i linje med Martinssons teknik och marknadsinriktning. Det är också ett område som i dagsläget ligger i teknikens frontlinje. Därför valdes tekniken Seamless roaming ut för att studeras närmare i den vetenskapliga fördjupningen. Tekniken har undersökts teoretiskt och två produkter, som fortfarande är under utveckling, har testats för att se om de uppfyller Martinsson krav på stabilitet och kundnytta.

7.1. Frågeställningar till den vetenskapliga fördjupningen

Frågeställningarna kan sägas ha tre inriktningar som besvaras på lite olika sätt.

De teknikgenerella frågeställningarna berör tekniken på en högre nivå och inte på applikationerna. Där kommer frågor som kompabilitet, skalbarhet, generalitet och framtidssäkerhet att diskuteras.

- Hur kompatibel är tekniken med övrig teknik?
- Hur väl skalar tekniken?
- Hur generell är tekniken?
- Hur framtidssäker är tekniken?

Prestandafrågorna är beroende av de specifika applikationerna och syftet är att ge en bild av hur bra prestandan är och vilka faktorer som påverkar prestandan.

- Hur fungerar Seamless Roaming?
- Hur ser genomströmning och RTT ut?
- Vilka faktorer påverkar ovanstående resultat?

De sista frågeställningarna är de minst vetenskapliga och berör hur produkterna fungerar och upplevs. Vi gör subjektiva bedömningar om användarvänlighet och stabilitet. Dessa frågor kommer att ha en stor vikt i den slutgiltiga rekommendationen till Martinsson.

- Hur upplevs användarvänligheten?
- Hur stabil känns lösningen?

7.2. Grundtekniska förutsättningar och val av produkter

De två tekniker för Seamless Roaming med VPN som vi undersökt är dels en properitär lösning baserad på splittrade TCP-kopplingar implementerad av företaget Columbitech och dels en implementation av mobile IP från företaget IP Unplugged. Båda företagen är svenska och har i tidningar som t.ex. Ny teknik beskrivits som världsledande inom sina respektive områden [Ryberg 2002].

7.3. Seamless Roaming och VPN

Roaming är en teknisk term som kommer från mobiltelefonbranschen, där det beskriver den tekniska förmågan för en terminal att kunna byta mellan två basstationer utan att uppkopplingen bryts. Seamless Roaming är en vidareutveckling av detta och den betydelse som vi avser är förmågan att kunna växla mellan två olika nätverk utan att uppkopplingen bryts och utan att användaren måste göra det själv. Tekniken ska hela tiden se till att det bästa tillgängliga nätet används och anses allmänt vara en vital komponent i den framtida nätverksmiljö med en mängd heterogena nätverk som ibland kallas för den fjärde generationens mobilnät (4G).

VPN (*Virtual Private Network*) är en teknik för att med hjälp av kryptering och tunnlar etablera en logiskt privat infrastruktur på ett annat nätverk. Tekniken gör att det går att använda sig av en generell infrastruktur, som t.ex. Internet, för den grundläggande uppkopplingen. Sedan kan man ansluta sig till sitt VPN, varvid det ur användarsynpunkt upplevs som om användaren skulle befinna sig på ett eget, privat nätverk. Detta ger möjlighet till en billigare och flexiblare infrastruktur än vad den tidigare motsvarigheten - ett eget fysiskt nät - kan erbjuda.

7.4. Columbitechs Split TCP-lösning Systemarkitektur

7.4.1. Grundläggande beskrivning

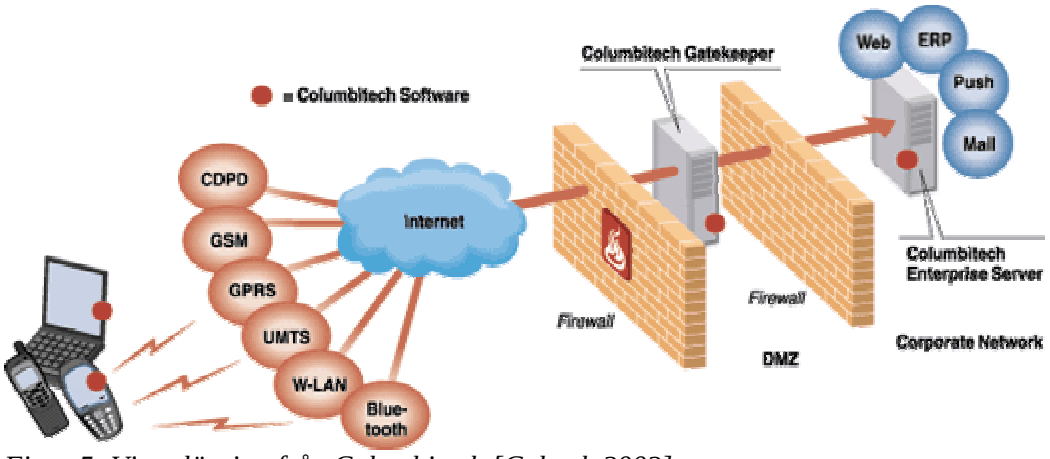
[Coltech 2002] beskriver översiktligt systemarkitekturen för Columbitech WVPN. Figur 5 visar lösningen från Columbitech. Systemet är implementerat på sessionslagernivå och fungerar transparent mot underliggande nätverk. Det enda kravet är att nätverket kan förmedla IP-trafik. Systemet består av två grundläggande delar, klienten WVPN Client och servern CES (*Columbitech Enterprise Server*). Det går även att, om man önskar, använda sig en extra säkerhets- och lastbalanseringsserver, Columbitech Gatekeeper. Lösningen är en ren mjukvaruprodukt och ej heller en rent generell lösning.

7.4.2. Programvarukomponenter

WVPN-klienten installeras i de maskiner som ska kopplas upp mot VPN:et och består av en ett virtuellt nätverkskort med en klientprogramvara som ser till att en TCP-koppling mot CES upprätthålls samt hanterar nätbyten. Applikationerna ser det virtuella nätverkskortet som vilket nätverkskort som helst och all trafik skickas genom detta.

CES är den egentliga VPN-servern och VPN:et termineras vid servern. Applikationer skickar all data som ska till applikationen via CES och CES skickar sedan datat vidare till klienten i krypterad och eventuellt komprimerad form. CES sköter identifiering av användare på VPN-nätet om inte Gatekeepern används. Servern innehåller också en PKI-portal för certifikatdistribution och programvara för certifikathantering.

Columbitech Gatekeeper är en frivillig komponent som kan användas för att öka säkerheten genom att lägga identifieringen av användare i en DMZ, *DeMilitarized Zone*, utanför det interna nätet. På så sätt går det att undvika att släppa in osäker trafik i det egna nätet. VPN-prestandan förbättras genom att möjliggöra lastbalansering mellan många CES på samma nät.



Figur 5: Visar lösning från Columbitech.[Coltech 2002]

7.4.3. Uppkoppling och dataflöde

Klientprogramvaran ser till att hela tiden försöka hålla en TCP-uppkoppling mellan det virtuella nätverkskortet och Columbitech Enterprise Servern. Klienten använder Windows Media Sense för att se om de fysiska gränssnitten har någon uppkoppling och väljer sedan den bästa tillgängliga uppkopplingen. Klienten har minst två IP-adresser. Det virtuella interfacet får en IP-adress från det interna nätet via DHCP som är statiskt under hela sektionen och de fysiska nätverkskort som har en uppkoppling har var sin IP-adress. Dessa adresser är dock aldrig synliga för applikationerna, utan applikationerna känner enbart till det virtuella interfacets IP-adress. Det virtuella NIC:et rapporterar alltid till applikationerna att en uppkoppling finns, så att applikationerna upplever alltid situationen som att en uppkoppling finns även om så inte är fallet.

Det virtuella nätverksinterfacet i klienten tar emot all trafik från applikationerna. Det virtuella interfacet komprimerar och krypterar sedan trafiken innan den skickas ut på något av de fysiska nätverksinterfacen.

CES:en uppträder också transparent mot applikationsservrar. Om en applikationsserver vill skicka data till en klient skickas denna till CES, som försöker skicka den vidare till klienten. Om detta skulle misslyckas, t.ex. beroende på att klienten inte alls är uppkopplad för tillfället, svarar CES applikationsservern med ett lämpligt ICMP-meddelande. Eftersom den normala end-to-end-semantiken bryts använder CES också TCP:s vanliga mekanismer för att hantera paketförluster och flödeskontroll. Om CES tillfälligt tappar uppkopplingen till klienten får applikationsservern en rapport om att klientens mottagarbuffert är full, varvid applikationsservern slutar sända. UDP-trafik fungerar på ett liknande sätt. Alla UDP-paket tunnlas över TCP-kopplingen mellan CES och virtuellt NIC [Coltech 2002].

7.4.4. Säkerhet och PKI

All data skickas krypterad över WTLS (*Wireless TLS*). WTLS är en variant av TLS (*Transport Layer Security*) men är anpassat för trådlöst bruk. TLS är en standard som baserar sig på de-factostandarden SSL (*Secure Socket Layer*) men inte är properitär. WTLS har en speciell resume-funktion som gör att det ska gå snabbt att återskapa förlorade uppkopplingar. WTLS stödjer DES och 3DES för kryptering, RSA för nyckelutbyte och MD5 och SHA för signering och hashning.

Identifieringen mot det egna VPN:et är en viktig del. Identifieringen kan ske endera innanför det egna nätet i CES eller utanför i en DMZ med Gatekeeper-servern. Ett flertal authenticeringsmetoder stöds. Windows Active Directory med användarnamn och lösen, Novell med användarnamn och lösen, Radius, X.509-certifikat, WTLS-certifikat och RSA SecurID. Med hjälp av detta är det möjligt att samköra inloggning på en t.ex. en windowsdomän med VPN-inloggning. En viktig del av säkerhetstänkande i WVPN är att det ska vara enkelt och smidigt för användaren.

Nyckeldistribution är ett centralt problem inom säkerhet. Columbitech hanterar detta genom att ha en certifikathanterare och en PKI-portal. PKI-portalen kan kopplas mot databaser med windows-användare och automatiskt skapa digitala certfikat. Columbitech menar att detta skalar mycket bra och skapar enkel certifikathantering i stora organisationer. Det är även möjligt att lägga ut certifikathanteringen till en extern organisation.

Produkten kan även integreras med en befintlig Active Directory-struktur vilket förenklar hanteringen av stora användargrupper.

7.4.5. Problem som följer av teknikvalet

7.4.5.1. Split TCP bryter end-to-end-semantiken

Då TCP-kopplingen splittras i flera delar bryts den end-to-end-semantik som är grundstenen i Internetdesign. Detta komplicerar den övergripande systemstrukturen. Ett följdproblem som då uppstår är att UDP skickas över en TCP-koppling trots att UDP är ett kopplingslöst protokoll och detta berövar UDP på en del av dess egenskaper.

7.4.5.2. TCP over wireless

TCP-protokollet är i grunden designat för att användas på förbindelser med små paketförluster och därför antar TCP alltid att paketförluster beror på congestion (stockning i näten) och reagerar därför med att halvera datahastigheten när paket förloras. Trådlösa förbindelser har mycket stora paketförluster och därför riskerar TCP att halvera datahastigheten i onödan i väldigt många fall. Under perioder av höga störningar kan TCP i praktiken bli närmast obrukbart över en trådlös uppkoppling.

Columbitechs WVPN döljer sin trådlösa TCP-uppkoppling utåt och har därmed möjlighet att byta protokoll eller omimplementera TCP att det fungerar bättre över trådlösa förbindelser. Något sådant har dock inte gjorts.

7.4.5.3. Properitär lösning

Columbitechs tekniska lösning är egenutvecklad lösning som använder sig av standarder, men lösningen är properitär, vilket innebär vissa affärsrisker. Om produkten ej får genomslag på marknaden blir investeringen mindre värd och utvecklingsmöjligheterna mindre.

7.4.5.4. Egen komprimeringsfunktion

Den komprimeringsfunktion som finns är inbyggd och behöver varken vara bra eller anpassad till användarens krav och önskemål. En öppnare lösning där det gick att välja mellan olika komprimeringsmoduler hade varit fördelaktigare. Det ska dock nämnas att det går att välja bort komprimeringsfunktionen.

7.5. IP Unpluggeds Mobile IP

7.5.1. Grundläggande beskrivning

Mobile IP (www.mobileip.com) är utvecklat av IETF, Internet Engineering Task Force (www.ietf.org), är det forum som arbetar med att utveckla de kommunikationsprotokoll vilket utgör Internet. Mobile IP är en utvidgning av IP-protokollet och innebär kortfattat att en mobil terminal skall kunna förflytta sig från ett nätverk till ett annat utan att tappa sin TCP-förbindelse. Mobilt IP löser frågan gällande att låta en terminal behålla sin IP adress utan att kräva att routrar lär sig nodspecifika rutter. Lösningen ligger i att låta den mobila enheten att ha två IP-adresser samtidigt, en primär och en sekundär adress. Den primära adressen är permanent och utgör adressen till nätverket där terminalen normalt hör hemma (även kallad ”Home network”). Den primära adressen används som destinationsadress för andra datorer som vill kommunicera med den mobila noden (MN). Den sekundära adressen kallas vanligen Care-of-Adress (COA) och växlar beroende på vilket nätverk noden besöker. COA utgör adressen till det nätverk (”Foreign network”) som den mobila terminalen för tillfället befinner sig på.

7.5.2. Uppkoppling och dataflöde

För att en mobil terminal som befinner sig i ett foreign network ska kunna skicka och ta emot paket behöver dess home network en Home Agent (HA). Se figur 6. Denna HA utgörs oftast av en router som håller reda på samtliga MN. Alla inkommande paket som har den primära adressen som destinationsadress tunnlas (IP-in-IP inkapsling). Inkommande paket får en extra header innehållandes

COA till det foreign network där den MN befinner sig. I mobile IP finns två möjligheter i foreign network. Dels kan det i foreign network finnas en Foreign Agent (FA) som har COA som adress dit samtliga paket skickas, packas upp och vidarebefordras till MN. I det andra fallet finns ingen FA vilket medför att MN har COA som sin adress och sköter själv uppackning av paket samt kommunicerar med sin HA då den byter Foreign Network.

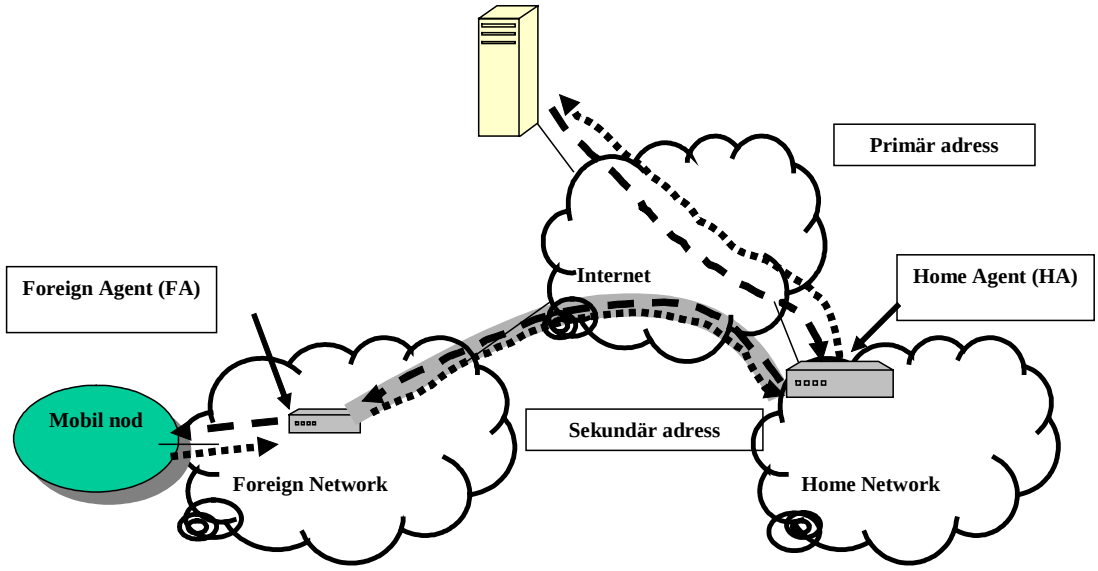
För att en MN ska veta vilket nätverk den befinner sig på skickar FA kontinuerligt ut ett ”Agent Advertisement” paket. Detta paket broadcastas ut på det foreign network som FA tillhör. Det är också med hjälp av dessa paket som den upptäcker ifall den befinner sig på ett nytt nätverk. Detta gör den ifall den får ett Agent Advertisement från någon ny FA. Skulle MN inte erhålla något agent advertisment kan den själv skicka ut en förfrågan efter en FA. Får MN då inget svar erhåller den en COA från t.ex. en DHCP-server och kontaktar själv sin HA [Schiller 2000].

7.5.3. Programvarukomponenter

IP Unpluggeds lösning för Seamless Roaming består av en Romaing Gateway (RG), Roaming Server (RS) och en Roaming Client (RC). Roaming Gateway är en router och utgör HA. Alla inkommande samtal som ska till en mobil nod passerar genom denna router. Inkommande paket tunnlas till den mobila nodens foreign agent i de fall där en sådan existerar. Utgående paket skickas från den mobila noden till RG med den mobila nodens Care-of-Adress som avsändare där den sedan ersätts med den primära adressen. På samma sätt byts de inkommande paketens destinationsadress ut mot den mobila nodens Care-of-Adress i Roaming Gateway innan den skickas vidare. En Roaming Gateway kan agera både HA och FA samtidigt vilket gör att andra mobila noder kan kommunicera med den HA som finns på dess hemmanätverk via denna. I IP Unpluggeds lösning har RG även funktioner och stöd för DHCP-server, brandvägg, NAT/NATP (*Network Adress Translation Protocol*) och AAA (*Authentication, Authorization and Accounting*).

Roaming Server är en administrationsserver som används till att konfigurera systemet. Systemets administration kan delas in i organisationer t.ex. företag, där företaget sedan har möjlighet att i sin tur dela in sig i underorganisationer. RS gör det möjligt att skapa användare till respektive organisation som sedan kopplas till de resurser och policys som man vill att dessa användare ska få tillgång till. Denna server kan delas av flera olika organisationer med egna administratörer för att sköta sin organisations användare och resurser. Via RS går det också att göra de inställningar som ska gälla för en eller flera Roaming Gateways. Servern har stöd för AAA där RADIUS-protokollet (*Remote Access Dailer In USe*) används för autentisering men inom kort väntas ett nytt protokoll kallat Diameter ersätta Radius. RS har ett web-baserat GUI, MySQL som databas och behöver SUSE Linux 7.1 (www.suse.com) som operativsystem.

Programvaran för den mobila klienten kallas Roaming Client och sköter kontakten med FA samt väljer den bärarteknik som för tillfället finns tillgängligt. I de fall en FA inte finns på nätverket kopplar den själv upp sig mot sin HA och registrerar sin COA. På så sätt fungerar produkten även på nätverk som inte har stöd för Mobile IP. Roaming Client är idag kompatibelt med Windows 2000 och XP och under första kvartalet 2003 väntas även en version för Pocket PC släppas. Vid installation laddas programvaran ner från Roaming Server och efter installation hämtas den mobila nodens egna konfigurationsfil med nödvändig information och inställningar.



Figur 6: Principskiss för Mobile IP. Egen modell.

7.6. Säkerhet

IP Unplugged använder sig av IPsec vid överföring av data mellan HA och FA. I de fall där den mobila noden befinner sig på sitt hemmanät används ingen kryptering då hemmanätet anses vara säkert som standard. För kryptering används DES och 3DES samt HMAC-MD5 och HMAC-SHA *(Hashing for Message Authentication)* för signering och hashning. För att upprätta tunneln mellan HA och FA används IKE *(Internet Key Exchange)* som förhandlar fram vilken algoritm som ska användas mellan noderna samt skapar de rätta nycklarna för ändamålet.

7.7. Testsystem

7.7.1. Målsättning med testsystem

Målsättningen med testsystemet är att undersöka frågeställningarna som ej är främst teknikgenerella. De båda produkternas prestanda ska undersökas och vilka faktorer som påverkar prestandan ska undersökas. Utifrån observationer och mätdata skall frågeställningarna besvaras. De generella frågeställningarna som berör användarvänlighet och stabilitet både ur slutanvändar- och administratörsperspektiv skall också besvaras.

7.7.2. Teknisk implementationsplan

7.7.2.1. Tekniska krav

Målet med testnätet är att simulera ett system där en mobil terminal kan komma åt ett internt nät via ett VPN. Man ska därför kunna koppla upp sig på sitt VPN var som helst på internet och på i princip vilket accessmedium som helst. Grundläggande säkerhet ska finnas.

7.7.2.2. Nätkomponenter

7.7.2.2.1. WLAN-nät

Två WLAN-nät byggs för att undersöka roaming mellan näten. För att göra detta har näten givits olika nätnamn, rent fysiskt befinner de sig på samma nät och även på samma subnet. WLAN-näten betraktas som osäkra pga. deras inbyggda säkerhetsproblem, men eftersom syftet med testsystemet inte är att bygga en fullständig säkehetslösning väljer vi att enbart använda WEP-kryptering som säkehetsåtgärd. Andra möjliga tekniker är att begränsa vilka datorer som får ansluta med hjälp av MAC-adresserna, men dessa implementeras ej.

Varje nät består av en accesspunkt. Näten ligger bakom en brandvägg (PIX 501) och förses med dynamisk PAT (*Port Address Translation*) så att resten av internet blir åtkomligt. Noderna på de trådlösa näten kommer alltså kunna komma åt internet inifrån men de kommer inte att vara direkt åtkomliga utifrån. Brandväggen agerar PAT-server.

7.7.2.2.2. Internt testnät

En lokal server simulerar ett internt system. Detta förenklar testsystemet och eliminerar en möjlig felkälla i prestandatesterna. I prestandatesterna agerar webbservern även som FTP-server eftersom överföringshastigheterna är enklare att testa med en FTP-klient.

7.7.2.2.3. Internt LAN

Parallellt med WLAN-nätet sätts ett internt LAN upp för att prestandajämförelser mellan WLAN och LAN ska kunna göras. Liksom i WLAN-nätet används brandväggen som DHCP-server. Rent tekniskt består nätet av en vanlig TP-kabel som kopplas till brandväggen.

7.7.2.2.4. Externt LAN

För att testa hopp på ett LAN med längre RTT och lägre prestanda använde vi Martinssons LAN som går via Stockholm och genom minst en brandvägg. Adresserna delas ut via DHCP och Internet kommer man åt via NAT. Nätet lämpar sig väl för test i en verklig miljö då trafiken på nätet och därmed den tillgängliga kapaciteten, är väldigt varierande.

7.7.2.2.5. GPRS-nät

Telias GPRS-nät används. Nätet använder sig av DHCP och NAT eller PAT.

7.7.2.3. Tester som ska göras

Testerna avser TCP-protokollet och bägge utrustningar. Prestandatesterna ska göras även utan VPN-program inkopplade.

- Prestandatest mellan internt nät och mobil terminal i WLAN (svarstid/RTT, genomströmning).
- Prestandatest mellan internt nät och mobil terminal i GRPS (svarstid/RTT, genomströmning).
- Prestandatest mellan internt nät och mobil terminal i LAN (svarstid/RTT, genomströmning).
- Undersökning av nättapp vid roaming mellan alla olika nätverk utom WLAN till GPRS, eftersom det är omöjligt av tekniska skäl. Båda PCMCIA-korten går nämligen inte att stoppa in i datorn samtidigt.

Relevanta observationer, utöver rena prestandadata, ska givetvis alltid göras.

7.7.2.4. Material som använts

- 2 st WLAN accesspunkter av typ Cisco Aironet 1100. (802.11b)
- 2 st WLAN-kort av typ Cisco Aironet 350 (802.11b)
- 1 st webserverdator (P 90 Mhz, 128 mb ram, Windows NT4).
- 1 st Columbitech Enterprise Server Serverdator (P2 266 Mhz, 450 Mb ram, Windows 2000 Server).
- 1 st IP Unplugged Roaming Server Serverdator (P 166 Mhz, 128 Mb ram, Suse Linux 7.1)
- 1 st bärbar dator för IP Unplugged Roaming Client (P3 700, 320 Mb ram, Windows XP).
- 1 st bärbar dator för Columbitech WVPN Client (P2 700Mhz, 196 Mb ram, Windows 2000).
- 1 st GPRS-kort (Nokia D211 GRPS / WLAN, manuell switch).
- Alternativt GPRS-kort
- Kablage, 5 st IP-adresser (212.217.149.244 - 212.217.149.248).
- Cisco PIX 501 Brandvägg
- 1 st switch Compaq Netintelligent 5226 100/10 mbit
- Testprogramvaror och utrusning från Columbitech och IP Unplugged.
- För test av genomströmning används en FTP-server och en FTP-klient.
- För test av RTT används vanliga ping
- För undersökning av roamingkaraktäristik används programmet IP Detail Information v 4.2 (http://www.softdepia.com/utilities_drivers/network/ip_detail_information.html)

7.7.3. Genomförande

Eftersom de publika IP-adresserna vi hade till vårt förfogande inte var tillräckligt för att testa båda utrustningarna samtidigt valde vi att först bygga upp testnätet för att testa Columbitechs WVPN och därefter koppla ur Columbitech Enterprise Server och koppla in IP Unpluggeds Roaming Server på samma IP-adress. Testerna som utfördes var identiska, givetvis med hänsyn tagen till de olika systemens olikheter.

7.7.3.1. Prestanda

Genomströmningstesterna kunde utföras på identiskt sätt, med undantag för testet som kördes över Martinssons nät där den normala belastningen påverkade testresultaten. Testet gick till så att en fil, överfördes från FTP-servern till klientdatorn med FTP-klienten SmartFTP *(*www.smartftp.com*)*. Varje fil fördes över fem gånger för att stabila värden skulle uppnås.

Filens storlek valdes med hänsyn till vilket nät som testades eftersom vi dels vill låta hastigheten stabiliseras och dels ville vi inte att testerna skulle dra ut på tiden eller bli väldigt dyra då dataöverföring över GPRS är relativt dyrt. För att Columbitechs komprimering skulle få genomslag i testerna valde vi dessutom filer som var möjliga att komprimera. Filerna skapades genom att ett flertal slumpvis valda filer packades ihop till ett zip-arkiv, dock utan att någon komprimering användes. Sedan packades samma filer ihop i ett nytt zip-arkiv, men denna gång komprimerades filerna. Skillnaden i storlek mellan filerna ger en indikation om hur mycket datat kan komprimeras.

Stor fil	21.169.250 bytes	okomprimerad
Liten fil	1.233.183 bytes	okomprimerad

På det interna LAN:et testades Columbitechs utrustning både med och utan komprimering. Anledningen till detta är att processen att både komprimera och kryptera trafik är beräkningsintesiv, vilket gör att överföringshastigheten kan bli lägre med komprimering än utan om serverns

beräkningskapacitet är lägre än nätverkets kapacitet. Försöket upprepades 5 ggr för varje nät och applikation.

7.7.3.2. RTT

Testerna av Round Trip Time gjordes med helt vanlig ping. Ping fick köras tills tiderna blev stabila varefter tiden registrerades. Försöket upprepades 5 ggr i varje testfall.

7.7.3.3. Roamingkaraktäristik

Ett flertal tester av roamingkarakäristiken gjordes. Först konfigurerades programmen för att i första hand använda fast LAN, i andra hand WLAN och i tredje hand GPRS. Sedan framtvingades ett byte av nät. Under tiden för nätbytet lät vi applikationen IP Detail Information sända ut pingar med ett intervall på 100 ms. Antalet förlorade paket visar på ett tydligt sätt hur länge som uppkopplingen tappas.

Följande tester gjordes:

Från	**Till**

Typ 1

Närliggande LAN	WLAN
Internet / LAN	WLAN
Närliggande LAN	GPRS
Internet / LAN	GPRS

Typ 2

WLAN	WLAN	Hård övergång
WLAN	WLAN	Mjuk övergång

Typ 3

WLAN	Närliggande LAN
WLAN	Internet/LAN
GPRS	Närliggande LAN
GPRS	Internet / LAN

Den första gruppen av tester, typ 1, gick i princip ut på att etablera två tillgängliga nätverk: ett fast LAN och ett trådlöst. Utrustningen väljer då automatiskt det fasta nätet. Sedan kopplas helt enkelt den fasta kabeln bort varvid utrustningen byter nät.

Typ 2 är två olika tester. Den mjuka övergången går ut på att WLAN-mjukvaran beordras att byta WLAN-nät. Det är tveksamt om detta förfaringssätt har någon "naturlig" motsvarighet vid normal användning. Det kan dock tänkas att en användare själv vill byta nät och då är denna manöver relevant. Det är dock inget som i dagsläget kan genomföras av vare sig Columbitechs eller IP Unpluggeds klienter. Den hårda övergången går ut på att testa vad som händer när en användare går mellan områden som täcks av olika WLAN-nät. Eftersom ytförutsättningarna för detta inte funnits i testmiljön har detta simulerats genom att strömmen till en accesspunkt brutits. Eftersom klientprogrammen bara kan detektera tillstånden *uppkopplad* respektive *inte uppkopplad* borde detta vara en adekvat simulering.

Typ 3 går ut på att hoppa från ett sämre till ett bättre nät. Bägge näten kommer att vara tillgängliga samtidigt och bytet sker så fort klienten detekterat det bättre nätet. Rent praktiskt stoppar vi helt enkelt in LAN-kabeln i datorn.

7.7.3.4. Upplevelse

De mer subjektiva upplevelsetesterna grundar sig helt på hur systemen upplevts, både ur en ren användarsynpunkt när applikationerna testats och ur en administratörssynvinkel när systemen installerats.

7.7.4. Resultat

7.7.4.1. Prestanda

Under genomströmningstesterna på det närliggande LAN:et visade det sig FTP-servern utan något som helst VPN klarade att mata ut 7,8 Mbit/s över FTP-protokollet. Detta värde är inte på något sätt optimerat utan är ett resultat av standardinställningar på TCP. Nätverkets datahastighet är 10 Mbit/s som lägst mellan FTP-servern och klientdatorn. Dock kan man inte räkna med att uppnå den hastigheten eftersom det som har mätts inte är nätverkets grundläggande datahastighet utan den praktiska överföringshastigheten för användardata. När denna ska överföras över nätverket tillkommer overhead.

		Inget VPN	IP Unplug.	Columb.
Nät	**Test**	**Värde**	**Värde**	**Värde**
Närliggande LAN	Througput	7875 kbit/s	2913 kbit/s	4264* kbit/s
Närliggande LAN	RTT	1 ms	3,4 ms	20 ms
Närliggande WLAN	Througput	5594 kbit/s	2144 kbit/s	4115 kbit/s
Närliggande WLAN	RTT	2 ms	4 ms	22 ms
Internet / LAN	Througput	960 kbit/s	1074 kbit/s	2707 kbit/s
Internet / LAN	RTT	66 ms	66 ms	71 ms
GPRS	Througput	31 kbit/s	30 kbit/s	51 kbit/s
GPRS	RTT	790 ms	840 ms	805 ms
* Hastigheten blev 5078 kbit/s utan komprimering				

Tabell 1. Resultat av prestandatester

Referenshastigheten på WLAN är, helt naturligt, något lägre än på fast LAN. Även om datahastigheten på WLAN är 11 Mbit/s mot 10 Mbit/s för fast LAN är fast LAN snabbare i praktiken, vilket både beror på effektivare protokoll och lägre felfrekvens.

Internet/LAN har en högst varierande kapacitet eftersom det är tester som körts över Internet och Martinssons LAN och de kapaciteter som varit tillgängliga har varierat i hög grad. Resultaten på detta nät ska inte ses som mer än vägledande.

IP Unplugged utrusning ger på det närliggande nätet en överföringshastighet på knappt 3 Mbit/s, vilket kan tyckas väldigt lågt. Detta beror inte på stort overhead, utan på väldigt höga systemkrav på klientsidan. En enkel prestandaobservation på klientdatorn visar att processorutnyttjandet konstant ligger på 100%. IPU Roaming Gateway ska klara att mata ut 20 Mbit/s [John Rehnberg, IPU] och [John Rehnberg, IPU] hävdar att IPsec också har höga systemkrav. Uppenbarligen är det detta som är flaskhalsen i detta fall.

På WLAN blir genomströmningen något lägre för IPU, vilket delvis kan bero på att omsändningarna av förlorade paket hanteras av TCP-protokollet vilket gör att en större del paket måste dekrypteras. En mer tänkbar förklaring är att paketförluster i kombination med ökad RTT sänker överföringshastigheten.

Över Internet/LAN var genomströmningen högre för IPU än referensvärdet utan, vilket beror på stora variationer i nätets kapacitet. Resultatet indikerar dock att IPU inte har någon stor overhead. Denna indikation stärks också av GPRS-resultatet som endast skiljer med ca 3% till IPU:s nackdel.

Columbitech WVPN på närliggande nät ger en genomströmning på knappt 4,3 Mbit/s med komprimering på, medan hastigheten blir 5,1 Mbit/s med komprimering deaktiverad. En kontroll av processorbelastningen på CES-servern visar att processorn belastas till 100%. Uppenbarligen är det komprimeringen och krypteringen som utförs i servern som är flaskhalsen. David Ranner på Columbitech hävdar också att komprimering kan vara till nackdel då man har en svag server eller svag klient i kombination med en bredbandig nätverksanslutning och att man då gör en prestandavinst på att stänga av komprimeringen. Med tanke på att vår CES-server är en 266 Mhz PII IBM PC-server och klientdatorn en 700 Mhz PIII talar allt för att det är servern som är flaskhals.

Resultatet över WLAN talar för att komprimeringen är användbar, men det är särskilt över Internet/LAN och GPRS som komprimeringens fördelar blir uppenbara. Även om dessa värden bör tas tolkas försiktigt med tanke på att nätens kapacitet fluktuerar oregelbundet är mönstret tydligt. Genomströmningen med Columbitech WVPN är mycket hög, betydligt bättre än referensfallet utan VPN. Uppenbarligen är det över smala länkar som komprimeringen är en fördel.

RTT-testerna ger ett ganska enkelt resultat. Columbitechs utrustning ger ett något högre tillägg till RTT än vad IP Unpluggeds utrustning gör.

7.7.4.2. Roamingkaraktäristik

		IPU	Col
Från	**Till**	**Tid**	**Tid**
Närliggande LAN	Närliggande WLAN	1,7 s	8,5 s
Internet / LAN	Närliggande WLAN	2,0 s	9,4 s
Närliggande LAN	GPRS	4,6 s	12,7 s
Internet / LAN	GPRS	4,2 s	11,4 s
Närliggande WLAN	Närliggande WLAN	13,9 s**	fung. ej.**
Närliggande WLAN	Närliggande WLAN	2,3 s*	4,0 s*
Närliggande WLAN	Närliggande LAN	0 s	0 s
Närliggande WLAN	Internet / LAN	0 s	0 s
GPRS	Närliggande LAN	0 s	0 s
GPRS	Internet / LAN	1,5 s	3,2 s
* Mjukvarubeordrad övergång			
** Hård övergång (Dra strömmen till accesspunkt)			

Tabell 2. Testresultat för roamingkaratäristik.

Testerna visar ett tydligt mönster. De nätbyten som tillhör typ ett (från LAN till WLAN) fungerar smidigt med IP Unpluggeds utrustning medan det fungerar sämre med Columbitechs utrustning. Störningen varierar kraftigt och 8,5 respektive 9,4 sekunder är just medelvärden. Man ser också ett tänkbart samband mellan RTT:n hos det nät man byter till och tiden man förlorar uppkoppling.

Hoppen till GPRS visar ett omvänt mönster där uppkopplingstappet är längre då man byter från Närliggande LAN till GPRS än då man växlar från Internet/LAN till GPRS. Skillnaderna är dock relativt små. Intressant är dock att detta avviker från mönstret som noterades tidigare. Det bör också

noteras att GPRS-uppkopplingen gjorts manuellt innan LAN-kabeln kopplades ut. Det fungerar också att låta utrustningen koppla upp mot mobilnätet (GPRS) när behovet finns men då kommer växlingstiden dels att bli mycket lång och så kommer tiden inte att bero på roamingsystemet i första hand utan mer på hur lång tid själva uppkopplingen tar, vilket i sin tur beror på utrustning, mobilnät och aktuell nätbelastning.

Hopp mellan två WLAN-nät fungerar utmärkt med IP Unpluggeds utrustning. Då man gör en mjuk övergång (manuellt beordrar mjukvaran att byta nät) så går det mycket smidigt och uppkopplingsförlusten är kort. Att göra en hård övergång ger lite försämrad prestanda. Columbitechs utrustning fungerar betydligt sämre i dessa test. Den mjuka övergången går att genomföra men den hårda övergången, som är den mest relevanta, fick vi inte alls att fungera.

Det som fungerar mest smärtfritt är byte från ett trådlöst nät till ett trådbundet (typ 3). Allra bäst fungerar det när nätet man byter till har en kort RTT. Eftersom två nät blir tillgängliga samtidigt behöver systemet bara byta nät när väl det bästa nätet detekteras. Hur lång tid själva detekteringen tar spelar ingen roll eftersom det alltid finns ett tillgängligt nätverk. Det är bara när RTT-tiderna är stora som ett sådant nätbyte ger upphov till förlust av uppkopplingen.

7.7.4.3. Upplevelse

IP Unpluggeds system upplevdes ur ett administratörsperspektiv som bra. Tröskeln för att komma igång är högre än för Columbitech WVPN men när väl den inledande installationen gjorts fungerar det bra. Systemet torde kunna tilltala vana installatörer av nätverksutrustning eftersom Roaming Gateways dels kan styras via en seriekabel i ett teminalfönster med ett textinteface, dels via ett webbgränssnitt i en roaming server.

Tröskeln består främst i att installera och konfigurera en Roaming Server på en linux-dator. SuSE Linux som Roaming Server körs på är inte svårt att installera, men betydligt svårare än t.ex. Windows 2000. Serverapplikationen är också något mer komplicerad att installera än en vanlig Windowsapplikation. När väl Roaming Server fungerar är dock resten av installationen mycket enkel eftersom alla Roaming Gateways kan fjärrstyras från en Roaming Server. Detta gör all fortsatt installation och konfigurering mycket enkel och allt kan fjärrstyras fullständigt.

Användarna i IP Unpluggeds system läggs upp genom webbgränssnittet på Roaming Servern och användaren får sedan ett e-mail som instruerar om hur klientprogrammet ska laddas ned och installeras. Progammet laddas ned direkt från Roaming Servern och en användare som har installerat ett program förut borde kunna klara det utan direkta problem. Att använda själva klienten är inte heller komplicerat.

Ur stabilitetssynpunkt upplever vi IP Unpluggeds system som mycket stabilt och alla tester har fungerat utan problem.

Columbitechs system uppvisar ett lite annat mönster. Serverapplikationen CES (*Columitech Enterprise Server*) är mycket enkel att installera, svårighetsgraden ligger ungefär i klass med att installera Microsoft Word. CES körs på Windows NT eller 2000/XP, som också är enkelt att installera. CES innehåller även en certifikathanteringsapplikation som ger möjlighet att skapa användarcertifikat och en PKI-portal som ska underlätta cerfikathanteringen vid installation av klientprogramvaran.

Columbitechs WVPN-klient är, precis som IP Unpluggeds klientapplikation, mycket enkel att använda. Installationen är dock inte lika automatisk.

Upplevelsen av Columbitechs mjukvara har varit att det fortfarande är en programvara under utveckling. Programvaran har varit instabil och funktionaliteten har varierat. Ibland fungerar seamless roaming, ibland inte. Stödet från Columbitech har varit bra och vi ha under testningen fått tillgång till nya versioner som har löst tidigare problem. Dock är programvaran inte stabil. Det bör noteras att

Columbitech hävdar att deras testkunder inte har upplevt några problem och att våra tester är de enda som inte har fungerat bra.

8. Marknadsbedömningar

Vi har hämtat in marknadsbedömningar från analysfirman Gartner (http://www.gartner.com/), Columbitech och IP Unplugged. De åsikter och tankar som presenteras här är sammanställningar av deras bedömningar.

8.1.1. IP Unplugged

IP Unpluggeds John Rehnberg hänvisar bland annat till rapporten *Mobile Intranets Towards the Wireless Enterprise* [Ovum 2001] från Ovum som säger att marknaden 2006 kommer att vara 2 miljarder USD, men att det är svårt att veta hur stor den svenska delen av marknaden är. Samma rapport pekar på att det initialt kommer att finnas proprietära lösningar på marknad men att det över tiden kommer att fasas ut och att marknaden kommer att domineras av standardiserade lösningar. Man menar också att de flera kundnyttor finns med lösningen:

- VPN mellan användare, företag och site-to-site.
- Säkra WLAN med kryptering och brandvägg i RG.
- Goodwill genom möjligheten att ge ut gästkonton.
- Enkel administration av systemet.

Angående konkurrensen från Cisco hävdar IPU att Cisco saknar en heltäckande lösning för mobila-VPN med seamless roaming. Cisco behöver använda teknik från fyra produkter för att uppnå samma funktionalitet som IPU. Ciscos routrar har mobile-IP implementerat men klarar inte av att både agera foreign och home agent samtidigt vilket då kräver två routrar. Cisco behöver även deras Broadband Building Service Manager (BBSM) för att hantera Internet access kontroll för WLAN samt PIX-produkter för att upprätta ett VPN. Ett sådant system är inte motiverat ur ett kostnadsperspektiv. Ciscos saknar en mobile IP-implementation till deras VPN-system vilket gör att det bland annat saknas möjlighet till en central profilhantering, snabbt nätbyte och nyckeldistribution.

8.1.2. Columbitech

Informationen från Columbitech baserar sig på en intervju med Ola Jonsson. När han får frågan om hur Columbitech ser på marknadsförutsättningarna för seamless roaming produkter på några års sikt har han kan han inte bedöma storleken på marknaden, men menar att seamless roaming är ett krav om man ska kunna ha ett system där användaren kommunicerar över många olika nät. Seamless roaming kommer att betraktas som en självklarhet i den nya nätverkmiljön. För att den nya nätverksmiljön ska bli verklighet krävs det att många bitar faller på plats. T.ex. krävs terminaler, nätverk och abonnemang och detta sker nu. Det är ett tecken på marknadsmognad. Detta kommer att leda till en omfattande integration av system och applikationer. Exempel på folk som kommer att ha nytta av det är folk som rör sig i arbetet, t.ex. lagerarbetare och butiksanställda.

Ola anser vidare att de tydligaste försäljningsargumenten och kundnyttorna med deras produkt är säkerhet, enkelhet och prestanda:

Säkerhet är grundläggande. Att affärsverksamhet ska vara säker är helt enkelt ett krav. En lösning som inte kan erbjuda säkerhet kommer inte att finnas kvar länge på marknaden. Det är också viktigt att en man använder standardlösningar, eftersom egenutvecklade hemliga säkerhetsfunktioner oftast inte alls är säkra. Säkerheten ska vara anpassningsbar till annan säkerhet och den säkerhetsnivå som krävs. Om en användare vill använda certifikat ska man kunna göra det och även andra säkerhetslösningar ska kunna användas. Om man vill ha extra stark authenticering med t.ex. koddosa eller engångsnycklar så ska det gå att göra.

Enkelhet: Säkerheten ska också vara enkel. Användaren ska inte behöva uppleva säkerheten som ett besvär utan det ska finnas med i bakgrunden. Användarens ska heller ej behöva bry sig om att hon jobbar på ett VPN. Seamless roaming är också ett steg mot det säkerhetstänkanden. Användarens ska helt enkelt bara behöva logga in en gång och sen ska det vara säkert och uppkopplat hela tiden. Man ska inte behöva bry sig om hur man är uppkopplad.

Prestanda är viktigt över trådlösa uppkopplingar med låg genomströmning. Därför använder man komprimering. Komprimering inte bara ökar genomströmningen, utan sänker också kostnaden för att överföra data över en kanal där man betalar per överförd datamängd. WTLS är också att föredra framför IPsec ur prestandasynpunkt, då WTLS har en resumefunktion som gör att en handskakning ska gå på ca 2 sekunder. Med IPsec tar en fullständig handskakning teoretiskt 8 sekunder. IPsec ger också overhead. WTLS är att föredra framför SSL och TSL, eftersom WTLS är anpassat för trådlöst bruk.

Det är svårt att räkna hem en investering för kunden enbart på seamless roaming - det är ju egentligen värdelöst i sig. Fördelen är den ökade effektivitet som kan uppnås. Man skulle kunna jämföra det med ett VPN, fast enklare för användaren och bättre integrerat med applikationen. På några års sikt är det tänkt att nya typer av klienter och servrar ska tillkomma. Optimeringar ska ske på verktyg och IT-sidan samt administrationen ska bli bättre [Ola Jonsson 2003, personlig kommunikation].

Det finns inga planer på att införa stöd för avkänning av WLAN-signalstyrka för att göra smidigare nätbyten. Dels finns det i praktiken ingen efterfrågan för detta eftersom roaming mellan WLAN och gprs inte kommer att ske särskilt ofta. Det är också svårt att genomföra eftersom det inte finns någon standard för hur olika hårdvaror och drivrutiner rapporterar signalstyrkan till applikationer och man då skulle behöva göra drivrutinsspecifika modifieringar för att kunna uppnå detta och det skulle inte fungera med alla kort. Det skulle därmed vara svårt att marknadsföra. Det största kundkravet från Symbol (som gör handdatorer) är att man ska kunna dölja VPN:et [Ola Jonsson 2003, personlig kommunikation].

När det gäller konkurrensen från andra aktörer har Cisco och Checkpoint (www.checkpoint.com) vpn-produkter, samt stöd för Mobile IP i sina produkter. Företaget Birdstep (www.birdstep.com) är också med och jobbar med IPsec. Detta gör att det kommer att krävas en klient för mobile ip-vpn och en för ipsec vilket är osmidigt för användaren. Seamless roaming krävs också, men hur det fungerar vet Comumbitech inte. Cisco har också inget API för applikationsutvecklare, vilket Columbitech har och det är en av de viktigaste styrkorna. Man menar att IPsec inte är tillräckligt, utan ett API för applikationsutvecklare måste finnas. Applikationsutvecklarna ska inte behöva bygga applikationsspecifika lösningar på generella problem som VPN. Ciscos och Checkpoint konkurrerar främst med säkerhet, standard och det faktum att Cisco är marknadsledande på nätverksutrustning. Columbitech konkurrerar med standarden WTLS, säkerhet, enkelhet och prestanda, men det absolut viktigaste är API:et för utvecklare [Ola Jonsson 2003, personlig kommunikation].

En konkurrent som man ser är amerikanska Netmotion (www.netmotion.com) som gör ungefär samma produkt, men använder en egen säkerhetslösning istället för WTLS. De är rätt stora på den amerikanska marknaden. Man ser även företag som bygger in liknande funktionalitet i applikationer som konkurrenter. Ett exempel på detta är Infowave (www.infowave.com) [Ola Jonsson 2003, personlig kommunikation].

8.1.3. Gartner

Vi har tagit del av några rapporter från analysfirman Gartner och har sammanfattat det som är relevant för denna undersökning ur dessa rapporter.

I [Redman+ 01] säger man att år 2010 kommer, med 70% sannolikhet, 15% av alla mobila användare att använda IP över integrerat LAN/WAN i en 3G-miljö. Man hävdar också att 4G är en mer integrerad variant av 3G och andra paketförmedlande nät, såsom t.ex. WLAN, med förbättrade prestanda.

I [Chapman 2002] uppskattar Gartner att det ska finnas mer än 23,000,000 användare av WLAN-hotspots år 2007 i Europa. Man menar också att mobiloperatörerna har en vision om att erbjuda flera former av luftgränssnitt (WLAN och 3G) till samma nät, men detta ligger långt fram i tiden. Man noterar dock att Telenor erbjuder roaming mellan WLAN- och GSM-/GPRS-nät. Slutsatsen i rapporten är att WLAN kommer att bli en del av operatörernas utbud och fler operatörer kommer att börja erbjuda det under 2002 och 2003. Priserna för hotspot-access kommer också att falla under hela 2003.

[Stuart+ 2002]menar att användarna fortfarande inte helt litar på VPN och undviker VPN till affärskritiska applikationer, men att trenden går mot ett allt högre användande av VPN för viktiga applikationer. Det är bara en tidsfråga innan VPN ersätter traditionella alternativ som uppringda förbindelser, leasad lina eller dedikerade nätverk. Marknaden har mognat mycket de senaste 12 månaderna.

De tekniska problemen är i första hand integrationssvårigheter eftersom standarder saknas. Dels är tekniken relativt komplex och det krävs kunskap om säkerhet. IPsec är den vanligaste krypteringstypen och har nästan eliminerat säkerhetsproblemen.

Fördelarna med VPN är skalbarhet, säkerhet, QoS, extranets (externa nät), remote access, integration, prestandakontroll, flexibilitet och lägre kostnader i och med att man slipper leasade linor.

9. Slutsatser. Avslutning

De viktigaste slutsatserna från undersökningen av Martinsson är att allt bedrivs strikt affärsmässigt och allt vad teknikpreferenser och prestanda kommer i andra hand. Fokuset ligger på att erbjuda standardlösningar som ger en stabil IT-miljö. Att man bygger infrastruktur innebär att man sätter upp servrar och kommunikationslänkar i första hand. Detta gör att man är ovillig att ta risker och använda icke-etablerad teknik. Samtidigt försöker man att anpassa fokusområdesstrukturer så att den teknik som är nyare ligger i fokusområdena, medan den äldre tekniken hamnar bland bastjänsterna. Det gör att det, säkerheten till trots, finns ett intresse på ny teknik. Att det som är modernt för tillfället ingår i fokusområdena har affärsmässiga fördelar.

Man eftersträvar också enkelhet för användarna. De ska inte behöva bry sig om IT-systemet. Det ska helt enkelt fungera.

Omvärldsundersökningsfokus var bärarteknikerna för mobila lösningar och från dem kan ett flertal intressanta slutsatser dras.

GPRS är en omogen teknik. Det märks av den skiftande kvaliteten och funktionaliteten både hos GPRS-nät och konsumentutrustningen. Kapaciteten är heller inte pålitlig. Den praktiska funktionaliteten ligger heller inte i linje med den teoretiska. Slutsatsen är att GPRS inte är användbart till affärskritiska applikationer, men väl till andra applikationer där kraven på funktionalitet inte är lika stora.

UMTS eller 3G är en utveckling av GSM, men den finns inte tillgänglig ännu. När tekniken blir accepterad kan den vara användbar men det återstår att se.

HiperLAN/1 och HiperLAN/2 är två standarder för trådlöst nätverk som inte fått fäste på marknaden. HiperLAN/1 är en teknik som inte kommer att användas, medan HiperLAN/2 har en oviss framtid. I dagsläget är det inga teknologier som Martinsson behöver bekymra sig om. Om de börjar användas borde dessa kunna fasas in i samma område som vanligt WLAN.

WLAN (802.11b och 802.11a) är den enda trådlösa bärarteknik som är fullständigt användbar för affärskritiska tillämpningar idag och tekniken är mycket mogen och prisläget är bra. Dock lider tekniken av flera problem, dels är kapaciteten jämfört med trådbundna nät dålig men framförallt är säkerheten långt ifrån tillfredställande. Den inbyggda WEP-standarden är feldesignad och näten är långt mycket mer osäkra än trådbundna nät. För att ett WLAN ska kunna betraktas som säkert krävs det ytterligare säkerhetsfunktioner, som t.ex. ett VPN.

Ur undersökningarna av Martinsson och bärarteknikerna kan man dra några slutsatser: Om Martinsson ska ha ett fokusområde inom mobilitet bör det ligga i linje med Martinsson filosofi, dvs. infrastruktur baserad på etablerad teknik, men ändå på något sätt i närheten av teknikfronten. Kundnyttan ska vara säkra, stabila system som fungerar med ett minimum av användarinteraktion. De bärartekniker som är användbara för Martinsson i dagslägen och en nära framtid för mobil infrastruktur är i första hand WLAN och i andra hand GSM/GPRS. Det är också sådan infrastruktur som byggs av teleoperatörer och som därför kommer att finnas tillgänglig. Därav valet att inrikta djupstudien på seamless roaming.

Djupstudierna av seamless roaming visar på några saker. Den måste ses som en förenkling och en möjliggörare, eftersom det de testade produkterna gör är att erbjuda en säker, mobil infrastruktur. Användaren ska vara uppkopplad utan att behöva bry sig om hur och systemet ska automatiskt välja den bästa uppkopplingen. Båda produkterna som vi testat uppfyller dessa krav ur ett grundläggande perspektiv. Dock finns några problem med produkterna.

- Columbitechs utrustning ger bra prestanda, men är instabil.
- IP Unpluggeds system har dåliga prestanda och höga systemkrav.
- Hopp från WLAN då täckningen försvagas bör fungera dåligt då systemen inte känner av signalstyrkan. IPUnplugged ska årgärda detta, Columbitech hävdar att kunderna inte efterfrågar det.
- Detektion av tillgängliga nät litar i första hand på Windows Media Sense. Det innebär att utrustningens förmåga att känna av nätverk blir viktig och detta varierar mellan olika utrustningar.
- Ingen av produkterna är etablerade på marknaden

Ur ett marknadsperspektiv verkar det utan tvivel vara så att Seamless roaming kommer att ha betydelse. Det är en nödvändig komponent i fjärde generationens mobilsystem. Mobila system blir allt viktigare och säkerheten kan garanteras med VPN-lösningar.

Den slutgiltiga rekommendationen till Martinsson är att mobilitet definitivt är något att satsa på och mobil infrastruktur går att erbjuda kunderna redan idag. Tyvärr är dock systemen unga och det visar sig tydligt i form av problem med prestanda, instabilitet, brister i funktionalitet och marknadsosäkerhet. Columbitechs WVPN är intressant, men i dagsläget för instabilt för att erbjudas Martinssons kunder. IP Unpluggeds system har högre systemkrav, men är ändå tillräckligt stabilt för att snart erbjudas till några få testkunder som är medvetna om begränsningarna. Storskalig försäljning ligger dock i framtiden.

Området kan med fördel följas upp i framtiden. Båda företagens acceptans på marknaden bör följas, möjligheten finns att något av systemen blir en de-facto-standard. Risken finns också att något, eller båda, systemen helt misslyckas på marknaden. Hur marknaden kring mobilitet utvecklas återstår att se.

Källförteckning

[3G 2002] Okänd författare - *3G by any other name*, 2002-01-10 <http://www.economist.com/business/displayStory.cfm?Story_ID=930233>, 2002-10-14

[3G 2001] 3G Today - *The 3G Choice is CDMA* <http://www.3gtoday.com/standard.html>, 2002-10-08

[Bergljung 2002] Christian Bergljung - *Wireless-LAN: a Complement to 3G for Wireless Access*, 2002-04-15 <http://www.nordunet2002.dk/powerpoint/a__christian_bergljung.pdf>, 2002-11-30

[BGW 2001] Nikita Borisov, Ian Goldberg, David Wagner - *(In)security of the WEP algorithm*, University of California at Berkley, 2001-01 <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>, 2002-10-02

[Boyle 2001] Padraic Boyle - *The War of the Directory Services*, 2001-06-01 <http://www.extremetech.com/print_article/0,3998,a=1559,00.asp>, 2002-09-19

[CDG 2002] CDG - Introduction to CDMA <http://www.cdg.org/tech/a_ross/Intro.asp>, 2002-10-08

[CS 2002] Jon Johnsson - *Pengar att tjäna på sms*, 2002-03-14 <http://www.idg.se/ArticlePages/200203/14/20020314010000900_CS2/20020314010000900_CS2.dbp.asp>, 2002-09-30

[Champness] Angela Champness - *IEEE 802.11 DSSS: The Path To High Speed Wireless Data Networking* <http://www.wirelessethernet.org/downloads/weca80211boverview.pdf>, 2002-09-27

[Chapman 2002] J. Chapman - *European Operators Aim to Integrate Wireless LAN Services* [Gartner Research, Note Number: COM-17-7697, 8 October 2002]

[Citrixwp 2002] Citrix - *Citrix Whitepaper: Citrix workforce mobility*, 2002 <http://download2.citrix.com/ctxlibrary/products/pdf/WirelessBusiness_whitepaper.PDF>, 2002-09-17

[Citrix 2002-09-17] Citrix - *Citrix Webbplats/Unplugged* <http://12.8.192.113/solutions/wireless.asp>, 2002-09-17

[Coltech 2002] Columbitech - *Columbitech wireless VPN technical description* [Columbitech 2002]

[EMS 2001] Ericsson mobile communications AB - *Enhanced Message Service Whitepaper*, 2001-03 <http://www.mobileems.com/EMSwp.pdf>, 2002-10-03

[Ericsson 2002] Ericsson mobile communications AB – EDGE Introduction of high-speed data in GSM/GPRS networks, 2002 <http://www.ericsson.com/products/white_papers_pdf/edge_wp_technical.pdf>, 2003-02-25

[ETSI h1] ETSI - HiperLAN 1 standard overview <http://www.etsi.org/frameset/home.htm?/technicalactiv/HiperLAN/HiperLAN1.htm>, 2002-10-10

[ETSI 2002] ETSI Pressrelease - *ETSI approves HIPERACCESS core standards for Broadband Fixed Wireless Access*, 2002-05-17 <http://www.etsi.org/frameset/home.htm?/pressroom/Previous/2002/ETSI-HYPERACCESS.htm>, 2002-10-10

[Geier 2002] Jim Geier - *Sizing up your Wlan,* 2002-03-14 <http://www.80211planet.com/tutorials/article/0,4000,10724_992011,00.html> , 2002-10-01

[GHAR 2002] James W. Green, Steve Henrichon, Magdi Ahmed-Said, Steve Roberts - *802.11a or HiperLAN2: Which Technology Will Emerge as the 5 GHz WLAN Standard?,* 2002-05-09 <http://198.11.21.25/capstoneTest/Students/Papers/docs/5GHz_WLANs311234.pdf>, 2002-10-10

[GSM 2003] Awards 2003 – *Best infrastructure or network solution product* <http://www.gsmworld.com/awards/nominees.html>, 2003-01-30

[GSM 1995] John Scourias - *Overview of the GSM Cellular System Extended Abstract*, 1997-08-03 <http://www.shoshin.uwaterloo.ca/~jscouria/GSM/trio.html>, 2002-09-25

[GSM 2002] Kerala - *GSM Security and Encryption* <http://www.keralaconnect.com/gsm_security_encryption.htm>, 2002-09-30

[GSM 2003] GSM Association – *Membership& market statistics*,2003-01-14 <http://www.gsmworld.com/news/statistics/14jan03_stats.pdf>, 2003-02-19

[Hayes 2000] Vic Hayes - *Response to the UK-RA Strawman proposal for the use of RLANs in the 5 GHz band Draft 2* , 2000-05 <http://grouper.ieee.org/groups/802/15/pub/2000/May00/00146r0P802-15_WG-Draft38R-Presentation-for-UK-RA.ppt>, 2002-10-09

[IDG 2002] Bo Nordlin - *Trådlös säkerhet fortfarande eftersatt*, 2002-01-19 <http://nyheter.idg.se/display.asp?ID=020119-CSD1,2003-02-18>

[IEEE 802.11 1999] IEEE - *Part 11: Wireless LAN Medium Access* Control (MAC) and Physical Layer (PHY) Specifications,1999

[IEEE 802.11a 1999] IEEE - *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, 1999

[IEEE 802.11b 1999] IEEE - *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band* [IEEE Standard 1999]

[IEEE 802.11d 2001] IEEE - *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) speci.cations Amendment 3: Speci.cation for operation in additionalregulatory domains,* 2001

[IEEE 802 2001] IEEE - *802® IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture* [IEEE Standard 2001]

[IEEE 1997] IEEE - *Standard Status Report for Wireless,* 2002-09-30 <*http://standards.ieee.org/cgi-bin/status?wireless*>,2002-09-30

[ITU 2002] ITU Overview - *History*, 2002-02-13 <http://www.itu.int/aboutitu/overview/history.html>, 2002-10-08

[Johnsson 1999] Martin Johnsson - *HiperLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band, HiperLAN2/2 Global Forum 1999* <http://www.HiperLAN2.com/presdocs/site/whitepaper.pdf>, 2002-10-08

[Judge 2001] Peter Judge - HiperLAN *collapse opens European door to 802.11a*, ZDNet-artikel 2001-12-18 <http://news.zdnet.co.uk/story/0,,t269-s2101101,00.html>, 2002-10-09

[Keene 2002] Ian Keene - *What to expect from 802.11 wireless LAN standards and when* ,2002-03-14 <http://www.zdnet.com/filters/printerfriendly/0,6061,2857227-92,00.html>, 2002-10-01

[Kiepels 2001] Caroline Kiepels -*Företagens IT-säkerhet läcker som ett såll*,2001-01-25 <http://www.nyteknik.se/pub/ditArkiv.asp?art_id=1008521>, 2002-09-10

[Lorentzon+ 2002] Erik Lorentzon, Håkan Fransson – *Applikationsutveckling och mobilitet*, 2002-12 < http://www.cs.umu.se/~c98ppn/rapport_v5.pdf>, 2002-12-30

[Malmqvist 2002] Mattias Malmqvist - *Mannen som spårar framtiden*,2002-06-20 <http://www.idg.se/ArticlePages/200206/20/20020620111342_IDG.se_CS91/20020620111342_IDG.se_CS91.dbp.asp>, 2002-09-11

[Martinsson 2003] Martinssons hemsida – *Martinssons affärsidé* <http://www.martinsson.se/default.asp?meny1=9&sida=22>,2003-03-17

[MIS 2002] Martinsson - *Översiktlig beskrivning av fokusområdet Storage & Dataprotection.* <http://www.martinsson.se/default.asp?meny1=3&meny2=5&sida=10>, 2002-09-16

[MIS2 2002] Martinsson - *Översiktlig beskrivning av fokusområdet Server Based Computing* <http://www.martinsson.se/default.asp?meny1=3&meny2=4&sida=9>, 2002-09-17

[Molta 2001] Dave Molta - *Proxim 802.11a Line Brings Harmony to Wireless LANs* Network Computing Technology Resource Center, 2001-12-10

<http://www.networkcomputing.com/shared/printArticle.jhtml?article=/1225/1225sp1.html&pub=nwc>, 2002-10-02

[Nfuse 2002] Nfuse - *Nfuse Elite FAQ*
<http://12.8.192.113/nfuse_elite/faq.asp>, 2002-09-17

[Northstream 2002] Northstream – *3G rollout status*, 2002-10-04
<http://www.pts.se/dokument/getFile.asp?FileID=3221>,
2002-12-01

[Ryberg 2002] Ny teknik - *Sex svenskar i europeiska tekniktoppen*, 2002-05-29
<http://www.nyteknik.se/pub/ipsart.asp?art_id=21298>, 2003-02-26

[Ovum 2001] Graham Titterington, Jean Leston, Jessica Figueras, Keshinee Shah, Neil Ward-Dutton, Nigel Smith - *Mobile Intranets Towards the Wireless Enterprise*, 2001

[Parks 2001] Gregory Parks - *802.11e makes wireless universal*
Network World Fusion, 2001-12-03
<http://www.nwfusion.com/news/tech/2001/0312tech.html>, 2002-10-02

[Protect 2001] Protect Data - *PD konsult avslöjade säkerhetsbrister hos trådlösa nätverk*
<http://www.protectdata.com/common/upl/files/file45520.pdf>, 2002-09-12

[PTS 2002:11] Svensk telemarknad - *RAPPORT PTS-ER-2002:11*
<http://www.pts.se/dokument/getFile.asp?FileID=3021>, 2002-09-26

[PTS 2002-08] PTS - *Konsumentmarknaden för mobila innehållstjänster*, 2002-08-29
<http://www.pts.se/dokument/getFile.asp?FileID=3166>, 2002-10-01

[PTS] PTS - *Radiolan i 5 GHz-bandet: Regler avseende undantag från tillståndsplikt*
<http://www.pts.se/dokument/getFile.asp?FileID=2589>, 2002-09-30

[PTS 2002-06] PTS - Radiolan i 5 GHz-bandet: Regler avseende undantag från tillståndsplikt
<http://www.pts.se/dokument/getFile.asp?FileID=3211>, 2002-10-09

[Redman+ 2001] Phillip Redman, Jean-Claude Delcroix, Kathy Harris, Rich Mogull, John Monroe - *A Brave Mobile World: Emerging Technologies for Mobility* [Gartner Research, Note Number: T-14-0297, 1 October 2001]

[Salami 2002] Doctor Salami - *GSM in the USA*
<http://www.mywirelesspalm.com/article5.htm>, 2002-10-09

[Schiller 2000] Jochen Schiller - *Mobile Communications*
[Addison-Wesley 2000]
ISBN 0 201 39836 2

[Sony 2001] Sony - *Networking & Docks products*
<http://www.sonystyle.com/home/scat.jsp?hierc=9683x9714x9732&scatid=9732>, 2002-10-01

[Stuart+ 2002] Donald Stuart, Joe Tuset - *Global Virtual Private Network (VPN)* [Gartner Research, Note Number: DPRO-90307, 29 May 2002]

[TD-SCDMA 2002] TD-SCDMA-forum - *3G and TD-SCDMA* <http://www.tdscdma-forum.org/nenglish/tdscdma/tdtech.html>, 2002-10-14

[Tivoli 2001] IBM - *Tivoli Software*, 2001-10-24 <http://www.tivoli.com/news/events/presentations/toronto/tivoli_tuesdays_2001.ppt>, 2002-09-18

[UMTS 2002] Okänd författare - *Quality of Service* <http://www.umtsworld.com/technology/qos.htm>, 2002-10-14

[UMTS 2003] Okänd författare - *UMTS security* <http://www.umtsworld.com/technology/security.htm>, 2002-10-14

[UMTS W] UMTS World - *CDMA Overview* <http://www.umtsworld.com/technology/cdmabasics.htm>, 2002-10-10

[Walker 2001] Jesse Walker - Overview *of 802.11 security Intel Corp / IEEE document*, 2001-03 <http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt>, 2002-10-02

[WECA 2002] WECA Homepage - *Wi-Fi Oveeview* Wireless Compability Alliance <http://www.weca.net/OpenSection/why_Wi-Fi.asp?TID=2#Wi-Fi_CERTIFIED=Confidence>, 2002-10-03

Intern information Martinsson

[Andersson 2002-02] Håkan Andersson - *Presentation av Server Based Computing*, 2002-02-01. Internt dokument Martinsson, 2002-09-16

[Andersson 2002-06] Håkan Andersson -*Tjänstebeskrivning TryIT*, 2002-06-07 Internt dokument Martinsson, 2002-09-17

[Andersson 2002-08] Håkan Andersson - *programförklaring SBC*, 2002-08-05 Internt dokument Martinsson, 2002-09-16

[Arvidsson 2002] Personlig kommunikation, Fredric Arvidsson, Martinsson 2002-10-10

[Boström 2002-05] Jonas Boström – *Presentation av katalogtjänster*, 2002-02-13. Internt dokument Martinsson, 2002-09-18

[Boström 2002-08] Jonas Boström – *Programförklaring katalogtjänster*, 2002-08-28. Internt dokument Martinsson,2002-09-19

[Emilsson 2002] Jonas Emilsson -*Programförklaring SysMgmt*, 2002-06-12 Internt dokument Martinsson, 2002-09-18

[Emilsson 2002-10] Personlig kommunikation, Jonas Emilsson, Martinsson, 2002-10-10

[Henriksson 2002] Roland Henriksson - *IPC Rekommendationer Brandväggar/VPN lösningar*, 2002-08-26. Internt dokument Martinsson, 2002-09-11

[Henriksson2 2002] Roland Henriksson – *Rekommenderade tele/data operatörer*,2002-08-26 Internt dokument Martinsson, 2002-09-11

[Henriksson 2002-06] Roland Henriksson –*Programförklaring IP Communications*,2002-06-03 Internt dokument Martinsson, 2002-09-12

[Kramberger 2002-06] Fredrik Kramberger – *Programförklaring Databasse & Messaging*, 2002-06-05. Internt dokument Martinsson, 2002-09-18

[Kramberger 2002-08] Fredrik Kramberger – *Teknisk utförandebeskrivning*, 2002-08-15 Internt dokument Martinsson, 2002-09-18

[Ola Jonsson 2003] Intervju, Ola Jonsson, Columbitech, 2002-12-15

[Pyykkö 2002] Kosta Pyykkö – *Tjänstebeskrivning återläsningstest*, 2002-02-25 Internt dokument Martinsson, 2002-09-13

[Pyykkö2 2002] Kosta Pyykkö – *Tjänstebeskrivning backup-översyn*, 2002-02-25 Internt dokument Martinsson, 2002-09-13

[Pyykkö3 2002] Kosta Pyykkö – *Tjänstebeskrivning workshop-san*, 2002-02-25 Internt dokument Martinsson, 2002-09-13

[Wahlström 2002] Lena Wahlström - *Företagspresentation av MIS*, 2002-09-10 Internt dokument Martinsson, 2002-09-10