PUHELINJÄRJESTELMÄN UUDISTAMINEN

VOIP-Puhelut

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan suuntautumisvaihtoehto
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Pekka Savumaa

Lahden ammattikorkeakoulu
Tietoliikennetekniikan koulutusohjelma
SAVUMAA, PEKKA : Puhelinjärjestelmän uudistaminen
VOIP-Puhelut

Tietoliikennetekniikan opinnäytetyö, 67 sivua, 5 liitesivua
Kevät 2006
TIIVISTELMÄ

Tämän työn tarkoituksena on tarkoitus tutkia uutta GSM tekniikka jossa langaton verkko WLAN toimii GSM puhelimessa. Asiasta tutkitaan tietoturvaa ja yleistä tekniikkaa. Tarkoitus on ottaa käyttöön VOIP ratkaisun rinnalle langatonta WLAN- verkkoa hyödyntävää GSM tekniikkaa jonka avulla saadaan yhteys yrityksen VOIP-verkkoon. Aluksi tutkitaan GSM puhelimien tietoturvaa ja yleensä toimintaa. Esitellään GSM järjestelmää ja algoritmeja. Tämän jälkeen tutkitaan WLAN-tekniikan tietoturvaa ja yleistä toimintaa. Tässä osiossa esitellään myös eri käytettävät standardit. Näitä kahta asiaa tutkitaan tulevaisuutta varten. Lopuksi teoreettisessa osiossa tutkitaan VOIP-tekniikkaa. Esitellään siitä tekniikkaa ja tietoturvaa. Protokollapinot esitellään myös tässä osassa. Tätä tutkitaan koska järjestelmä otettiin käyttöön yrityksessämme. Teoreettisen osion jälkeen kerrotaan käytännössä, kuinka yrityksessämme Halton Oy on toteutettu uusittu puhejärjestelmä uudistus. Käyttöönotto VOIP-puheluihin ja samalla esitellään eri vaihtoehtoja laitteista jolla uuden GSM tekniikan avulla saadaan yhteys WLAN-verkkoon ja sitä kautta saadaan käyttöön yrityksessä käytettävät VOIP-puhelut.

Avainsanat: WLAN, VOIP, GSM

Lahti University of Applied Sciences
Faculty of Technology

SAVUMAA, PEKKA: Replacing an old telephone system with VOIP-Call

Bachelor's Thesis in Telecommunications technology, 67 pages, 5 appendices
Spring 2006
ABSTRACT

The aim of this study was to investigate the new GSM system where a WLAN-application is used by a GSM data phone. The study focuses on security and the general technique.

First, a look into the data security and general operation of GSM phones is taken. Then WLAN-data protection and general operations are discussed. This part also introduces the differents standard of WLAN. At the end of the theoretical part the VOIP-system is studied. The inspected items are VOIP- data protection and the general operations of the system.

Finally, it is described how the commissioning company Halton Oy has implemented the system's replacement. At the same time, some of the new GSM techniques to the WLAN are introduced.

Keywords: WLAN, VOIP, GSM

SISÄLLYS

1 JOHDANTO

Puhelinjärjestelmä uudistuksessa toteutettiin VOIP-ratkaisu Halton Oy:n nimiselle yritykselle. Tämä toteutettiin aluksi vain täällä Suomessa. Samalla, kun VOIP-ratkaisu otettiin käyttöön haluttiin tutkia mahdollisuutta ottaa käyttöön uutta tekniikka jota käytetään GSM-puhelimissa. Tämä uusi tekniikka on sitä, että kannettavalla mobiililaitteella päästään uutta tekniikkaa käyttäen WLAN-verkkoon ja sitä kautta päästään yrityksen omassa WLAN-verkossa yhteys VOIP-puhelu järjestelmään. Tätä VOIP-tekniikkaa tullaan aluksi käyttämään vain täällä suomessa, mutta tarkoitus on laajentaa aluksi pohjoismaan konttorit mukaan ja sen jälkeen muut maailmalla olevat konttorit ja tehtaat. VOIP-ratkaisu otetaan käyttöön koska vanha puhelinjärjestelmä olisi pitänyt uusia ja ei katsottu tarpeelliseksi lähteä uusimaan enää puhelinkeskukseen perustuvaa puhelinjärjestelmää. Jotta tätä uutta järjestelmää päästäisi käyttämään kokonaisvaltaisesti, niin samalla tässä työssä tutkittiin tulevaisuutta varten siis langatonta verkkoa ja GSM-tekniikkaa. Uusi mobiililaitteiden tekniikka jolla päästään WLAN verkkoon on nyt koko ajan yleistymässä ja siksi aihe tuntui ajankohtaiselta tätä työtä silmälläpitäen. Haittapuolena on tietenkin se, että informaatiota on vielä vaikea saada uudesta tekniikasta. Tämän vuoksi tutkiminen jäi aika vajavaiseksi tässä vaiheessa. Tarkoitus olisi toteuttaa lisäratkaisut kesän aikana.

2 TIETOTURVA MATKAPUHELIMISSA

2.1 Yleistä GSM –verkon historiaa

GSM (Global System for Mobile Communications) on maailman laajuisesti käytetyin matkaviestintä järjestelmä nykyisin. Käyttäjiä tällä järjestelmällä on jo liki miljardi ja kasvua tapahtuu keskimäärin 15 miljoona kuukaudessa. Suurin kasvualue on tällä hetkellä Aasian - Tyynenmeren alue. GSM oli ensimmäinen digitaalinen matkapuhelinstandardi. Vuonna 1982 muodostettiin GSM (Groupe Special Mobile) -komitea määrittelemään yhtenäistä standardia silloin käytössä olleiden analogisten ei yhteensopivien järjestelmien vastineeksi. Vuonna 1989 kehitystä jatkoi ETSI ja ensimmäiset GSM -spesifikaatiot vahvistettiin vuonna 1990 sekä rakennettiin ensimmäiset kaupalliset palvelut vuonna 1991. Ensimmäiset 36 GSM – verkkoa oli käytössä 1993 yhteensä 22 eri valtiossa. Samaan aikaan otettiin käyttöön suuremmalla taajuudella 1800 MHz oleva ensimmäinen GSM – verkko. Tämän jälkeen GSM on otettu käyttöön laajasti Euroopan ulkopuolellakin. Tilasto käyttäjistä alueittain. (Taulukko 1) (Digitoday 2004)

Aasia ja Eurooppaa hallitsevat gsm-tilastoja

GSMA:n alue	Käyttäjiä 02	Käyttäjiä 03	Kasvu 2003	%:n käyttäjäkunnasta
GSM Africa	23.7	32.9	38.82%	3.40%
GSM Arab World	24.4	33.5	37.30%	3.40%
GSM Asia Pacific	300.4	370.8	23.44%	38.20%
GSM Central Asia	6.7	9.2	37.31%	0.90%
GSM Europe	382.6	425.1	11.11%	43.80%
GSM India	10.5	20.8	98.10%	2.10%
GSM Latin America	7.1	16.5	132.39%	1.70%
GSM North America	18.8	29.2	55.32%	3.00%
GSM Russia	16.3	32.8	101.23%	3.40%
Globaali käyttäjäkunta	790.5	970.8	22.81%	100.00%

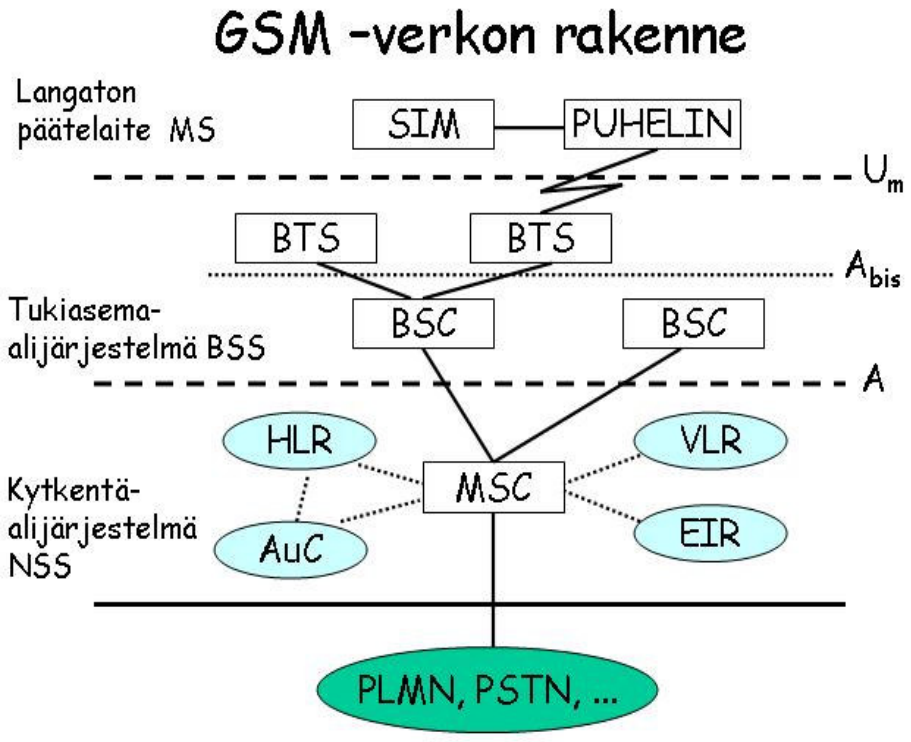
Taulukko 1

EMC Database (www.emc-database.com) ja GSM Association (www.gsmworld.com)

2000-luvulla GSM-verkkoa laajennettiin siten että siitä saatiin GPRS-verkko, jonka avulla saadaan paremmin hyödynnettyä internetpalveluita. GPRS-verkko lanseerattiin vuonna 2000, mutta silloin vielä itse verkosta puuttuivat GPRS-palvelut. Tämän jälkeen verkkoihin on otettu käyttöön EDGE-tekniikkaa (Enhanced Data Rates for GSM Evolution), jonka avulla GPRS-palveluiden nopeutta voidaan moninkertaistaa, ja samalla mahdollistetaan kolmannen sukupolven laajakaistapalvelut jo käytössä olevassa GSM-verkossa. EDGE-teknologia jota hyödynnytetään GSM puhelimissa on niin kutsuttu 2,5 sukupolven puhelin. UMTS:in aika alkoi vuonna 2003. Tällä uudella tekniikalla voidaan puhelimen avulla siirtää liikkuvaa kuvaa ja puhua puhelimessa samanaikaisesti. Tämä toiminto mahdollistuu suuremman siirtoteholtaan suuremman verkon avulla. Tällä uudella mahdollistetaan myös langaton internetyhteys. Kun taas UMTS:n julkaisussa esimerkiksi videoneuvottelupalvelut, olivat jo ehtineet kehittyä käyttäjien saataville ennen UMTS-verkon lanseerausta.
UMTS -tekniikassa käytettävät palvelut toimivat verkkoteknologiasta riippumatta jolloin käyttäjän ei tarvitse miettiä itse tekniikka. UMTS tekniikassa palvelut voidaan toteuttaa päätelaitteisiin eri tekniikoiden avulla(esimerkiksi GPRS, java, xhtml), jolloin itse käyttäjä ei huomaa käytettävän teknologian vaihtumista toiseen. UMTS-verkon tiedonsiirtonopeuten kasvattamiseen on kaksi eri tapaa joko parantamalla nykyisen GSM/GPRS-verkon ominaisuuksia EDGE-tekniikalla, tai sitten rakentamalla UMTS-verkkoa. EDGE-tekniikkan avulla mahdollistetaan käytettävän päätelaitteen tiedonsiirtonopeudeksi jopa 236 kb/s. UMTS-verkon tiedonsiirtokapasiteetti on taas 384 kb/s. Olennaista kolmannen sukupolven palveluissa on, että ne tehdään yhdessä avoimia rajapintoja hyödyntäen. Tässä avainasemassa ovat operaattorit, päätelaitevalmistajat ja sisältöpalveluntuottajat (www.fico.fi Verkkoteknologiaa suomeksi: 3G on täällä tänään)

2.2 GSM -verkon rakenne

GSM –verkkon rakenne voidaan jakaa suurin piirtein kolmeen osaan. Langaton päätelaite MS (Mobile Station,) joka on käyttäjän päätelaite.
Tukiasema-alijärjestelmä BSS (Base Station Subsystem,) on laite jolla vastaa radioyhteydestä langattomaan päätelaitteeseen. Kytkentäalijärjestelmä NSS (Network Switching Subsystem,) joka sisältää matkapuhelinkeskuksen MSC (Mobile services Switching Center), jonka avulla hoidetaan puhelunvälitys mobiili käyttäjien ja mobiili käyttäjän ja kiinteän verkon käyttäjien kesken. MSC hoitaa myös käyttäjien liikkuvuuteen liittyvät operaatiot. Kuviossa 1 on kuvattu verkon rakenne.



Kuvio 1

2.3 Langaton päätelaite MS

Mobiililaite muodostuu kahdesta pääosasta, eli puhelinlaitteesta ja älykortista SIM (Subscriber Identity Module) SIM –korttin avulla suoritetaan käyttäjän tunnistaminen riippumatta siitä missä päätelaitteessa kortti sijaitsee. Mobiili päätelaitteen tunnistamiseen käytetään IMEI (International Mobile Equipment Identity) -koodia, jonka voi katsoa puhelimesta näppäilemällä *#06#. SIM -kortilla on taas erikseen käyttäjän tunniste IMSI (International Mobile Subscriber Identity). PIN (Personal Identification Number)- sekä PUK (Personal Unblocking Key)-koodeja käytetään SIM kortin avaamiskoodeina. PUK – koodia käytetään silloin , kun käyttäjä on erheellisesti asettanut PIN – koodin kolme kertaa väärin ja saanut kortin lukittautumaan tästä huolimatta tämmöisellä puhelimella voi soittaa hätäpuhelut. SIM-kortti on eräänlainen tietokone joka ottaa vastaan ja lähettää tietoa päätelaitteelle. Siirtomuotona käytetään sarjamuotoista vuorosuuntaista väylää.(Vesanen A. 2005).

2.4 Radiotie

GSM:n spesifikaatioissa radiotie on yksi tarkimmin määritellyistä GSM- verkon osista. GSM:lle on spesifikoitu seuraavat taajuusalueet käytettäväksi: MS:stä BSS:ään 890-915 MHz (uplink) ja BSS:stä MS:ään 935-960 MHz (downlink). Radiotien resurssien jakamisessa on käytetty TDMA:tä (Time Division Multiple Access)ja FDMA:tä. FDMA:n (Frequency Division Multipleaccess) avulla koko 25 MHz:in taajuuskaista on jaettu 124 kantoaaltoon, ja näiden välinen ero on 200 Khz. Jokaiseen kantoaaltoon on sovellettu vielä lisäksi TDMA:ta, jonka tuloksena kantoaalto on jaettu ajallisesti kahdeksaan soluun (577 us) ja näin on saatu TDMA-kehys (4.6 ms), joiden jokaista solua voidaan käyttää lähetykseen tai vastaanottoon. TDMA kehyksistä muodostetaan edelleen ylikehyksiä, jotka voivat koostua 26 (120 ms) tai 51 (235 ms) kehyksestä. Edelleen voidaan vielä 26 tai 51

ylikehystä koostaa superkehykseksi. Hyperkehys koostuu puolestaan 2048 kpl:sta superkehyksiä (noin 3.5 tuntia), joten järjestelmä toistaa kanavakonfiguraatioita 3.5 tunnin välein. Jokainen TDMA kehys voi sisältää viittä erilaista informaatiotyyppiä: normaalipurskeen, taajuuskorjauspurskeen, synkronointipurskeen, hajasaantipurskeen ja dummy-purskeen. Yhtä solua voidaan käyttää sanoman vastaanottamiseen tai lähettämiseen. Kuitenkin lähetettävän ja vastaanotettavan solun välillä on erotettava muutamalla solulla, jolloin ei tarvitse vastaanottaa tai lähettää samanaikaisesti, mikä taas yksinkertaistaa laitteistorakennetta huomattavasti. Puhekoodaus (RPE-LTP) tuottaa 20 ms:in välein 260 bitin näytteitä. Puheenkoodauksen avulla syntyneet bitit jaetaan eri luokkiin virheenkorjauksen kannalta eli koodauksen aikana syntyneisiin bitteihin lisätään informaatiobittejä sopivasti. Konvoloimalla taas saadaan hyvä suoja purskettaisia virheitä vastaan. Kanavan ulostulo on 456 bittinen kehys. Tämä 456 bittinen kehys lomitetaan sopivasti, jolloin saadaan varmistettua että alunperin vierekkäiset bitit eivät ole alttiina samalle häiriölle. kokonaisbittinopeudeksi puheenkoodaukselle saadaan 13 kbps ja kanavakoodauksen bittinopeudeksi saadaan 22.8 kbit/s. Radiokanavan bittinopeudeksi puolestaan saadaan 270.833 kbit/s. Puheenkoodauksesta saadaan täyden nopeuden kanava radiotielle lähetettäväksi. Itse radiojärjestelmän kanavat muodostuvat kahdenlaisista kanavista, TCH liikennekanavista (Traffic Channel), joilla voidaan välittää puhetta tai dataa ja CCH ohjauskanavista (Control Channel), joilla voidaan välittää signalointi-informaatiota ja synkronointia. Ohjauskanavat jaetaan edellen useisiin kanavatyyppeihin. BCCH Yleislähetyskanava (Broadcast Control Channel) jatkuvasti lähettää tietoa mm. taajuushyppelysarjasta, tietoa taajuuksien allokoinnista ja tukiaseman identiteetistä. CCCH Yhteiskanava (Common Control Channel) koostuu kolmesta kanavasta: RACH hajasaantikanavasta (Random Access Channel), jonka avulla pyydetään yhteyttä verkkoon, PCH kutsukanavasta (Paging Channel), jonka avulla tiedotetaan MS:lle tulevasta puhelusta ja AGCH, jonka avulla allokoidaan SDCCH (Stand alone Dedicated Control Channel) signalointikanava MS:lle. SDCCH Yhteyskohtaista ohjauskanavaa käytetään mm. sijainnin päivitykseen, autentikoimiseen, registeröimiseen ja puheyhteyden asettamiseen. Muita kanavia on mm. SACC rinnakkainen hidas ohjauskanava (Slow Assosiated Control Channel),SCH synkronointikanava (Synchronisation Channel), FCCH taajuuskorjauskanava (Frequency Correction Channel) ja FACCH rinnak-

kainen nopea ohjauskanava (Fast Associated Control Channel). GSM käyttää modulaatiomenetelmänä GMSK. Sen ominaisuus on suhteellisen kapea spektri riittävällä tehokkuudella. Lisäksi kaistan ulkopuoleinen hajaspektri on matala näinollen vähentäen kanavien välistä häiriötä (Penttinen P. 1999).

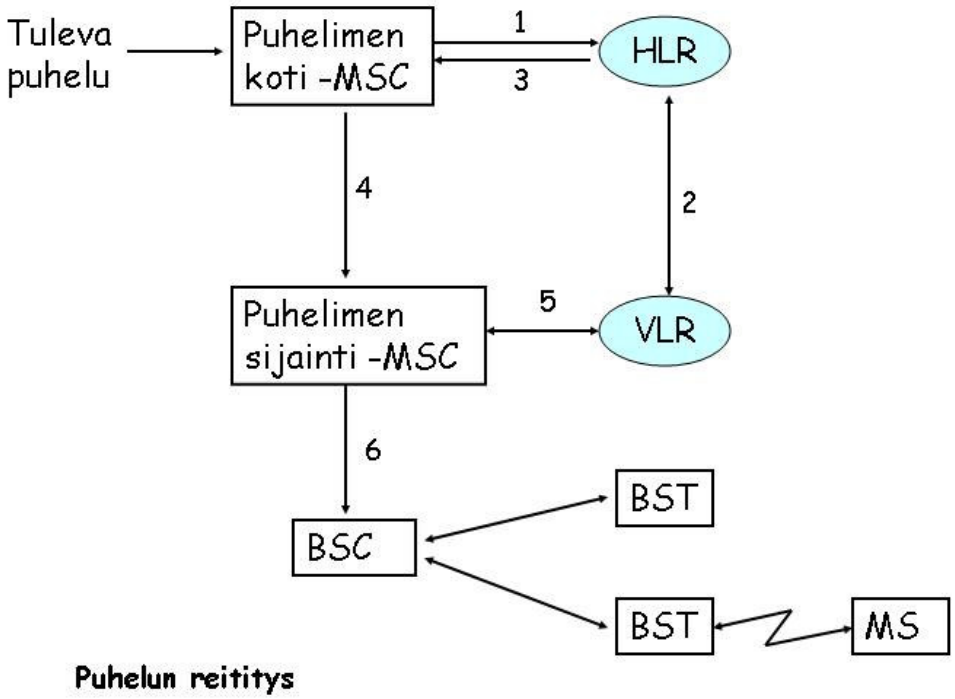
2.5 Tukiasema alijärjestelmä BSS

BSS muodostuu kahdesta osasta, tukiasema BTS (Base Transceiver Station) ja tukiasemakontrolleri BSC (Base Station Controller). Näiden kahden järjestelmän välinen rajapinta on standardisoitu siten, että valmistajasta riippumatta komponentit ovat yhteensopivia. BTS huolehtii puhelimen radioliikenteestä ja BSC taas kontrolloi BTS:iä ja sen toimintoihin kuuluu alustaa radiokanava, taajuushyppely ja käyttäjän siirto eri solujen välissä. BSC huolehtii myös BSS:n ja MSC:n välisestä liikenteestä. (Vesanen A. 2005)

2.5 Kytkentä alijärjestelmä NSS

NSS (The Network and Switching Subsystem) pääkomponetti on MSC. Tämän tarkoituksena on toimia yhteytenä kiinteään verkkoon ja samalla se toimii rekisteröimis- ja autenktitoimispalvelun tarjoajana. Tämän avulla hoidetaan myös liikkuvuuteen liittyvät palvelut joita ovat siis sijainnin määritys ja päivittäminen, siirtyminen tukiasemien välillä. Tässä järjestelmässä on myös tekstiviestikeskus SMSC (Short Message Service Center), jonka toimintona on huolehtia SMS viestien välittäminen. SMSC hakee tarvittavat reititystiedot jotka se saa HLR -rekisterin kautta.. HLR (Home Location Register) kotirekisteri ja VLR (Visitor Location Register)vierailija rekisteri näiden rekistereiden tarkoituksena on huolehtia käyttäjän liikkuvuuden hallinta ja puheluiden reitityket. HLR on rekisteri jossa on tiedot siihen verkkoon rekisteröityneistä käyttäjistä ja näitä on vain 1 kappale verkossa, kun taas VLR sisältää tiedot käyttäjistä verkon alueella. AuC(Authentication Center) on taas käytössä autentikaatio- ja turvaoperaatioihin. Laiterekisteri EIR (Equipment Identitty Register,) on rekis-

teri johon listataan kaikki laitteet IMEI- tunnisteen. Päätelaitteen sijainnin määritykseen käytetään siis MSC:tä käyttäen siellä hyväksi HLR:ää ja VLR:ää. Päätelaitteen vaihtaessa sijaintiaan on sen aina rekisteröidyttävä jotta puhelimen sijainnin päivitys onnistuu. Tämä on näytetty kuviossa 2 tarkemmin kuinka tapahtuma toimii.

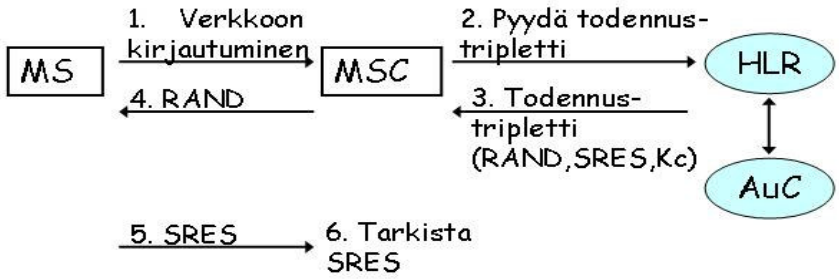


Kuvio 2
(Engdahl T. 2005)

2.3 GSM -Tietoturva

GSM puheluissa käyttäjän tunnistamiseen käytetään tilaajatunnisteen IMSI (International Mobile Subscriber Identity) tilaajatunnistetta apuna käyttäen. IMSI –koodin tarkoitus on tunnistaa varsinainen liittymä verkossa. IMSI tunniste muodostuu kolmesta eri osasta jotka ovat:
MCC (Mobile Country Code) eli maakoodi,
MNC (Mobile Network Code) kotioperaattori
MSIN (Mobile Subscriber Identity Number) liittymä kohtainen tunniste.

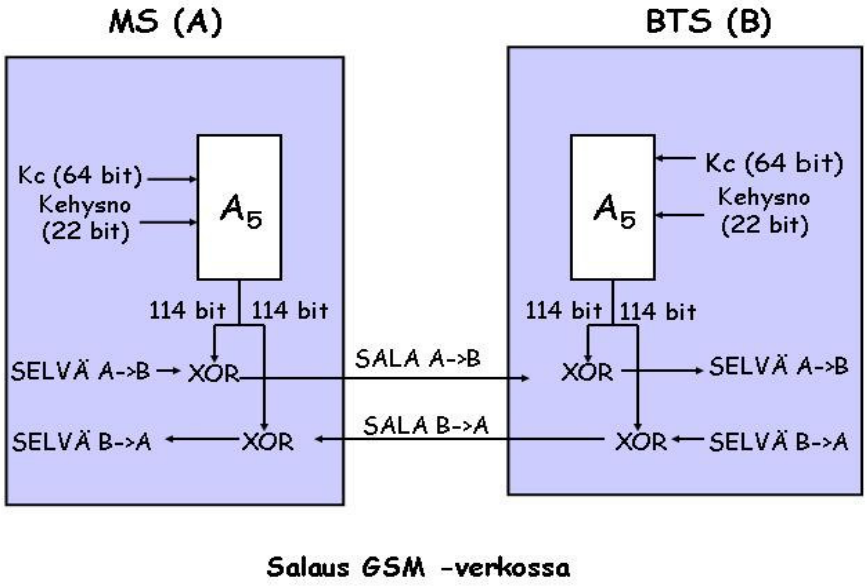
Jotta IMSI-koodia ei lähetetä koskaan salaamattomana radiotielle vaan sen sijasta käytetään väliaikaista tunnistetta TMSI joka luodaan joka kerran, kun käyttäjän sijainti vaihtuu. Tällä menetelmällä pyritään siihen että IMSI tunnistetta ei voida kaappata eikä tietyn liittymän liikennettä voida seurata. Kun käyttäjä aktivoituu käyttäjäksi verkkoon tapahtuu autentikointi. Autentikaation suorittavat osiot ovat SIM -kortti ja autenktitointikeskus (AuC). Itse autentikaatio suoritetaan siis haaste-vastaus -menetelmällä. Autentikointi tapahtuma esitetty kuviossa 3.



Autentikaatio GSM -verkossa

Kuvio 3

(Vesanen A. 2005)



Kuvio 4 Salaus GSM-verkossa

Lähetetystä liikenteestä salataan vain ainoastaan ilmatien liikenne (kuvio 4). Silloin kun lähetetyt sanomat saavuttavat käytettävän tukiaseman, niin ne puretaan selkokieliseksi ja lähetetään eteenpäin runkoverkkoon. Salaus toteutetaan siten, että käyttäjä todentaa itsensä ensin SIM-kortilla laitteelle ja tämän jälkeen laite todentaa itsensä verkolle.Tapahtuma tapahtuu haaste-vastaus periaatteella, siten että ensin MS kirjautuu verkkoon ja tämän jälkeen BTS lähettää kirjautumisen kotioperaattorille joka lähettää BTS:lle RAND() ja SRES()-taulukon. Tämän jälkeen BTS lähettää RAND haasteen MS:lle ja MS vastaa SRES sanomalla. Tämän jälkeen BTS tutkii että kotioperaattorin lähettämä SRES on sama kuin MS:n lähettämä ja jos on niin kirjautuminen onnistuu. Mobiili laitteiden tunnistamiseen käytetään IMEI koodia jotka on EIR – rekisterissä.
EIR – rekisterissä on seuraavanlaisen listan mukaan lajiteltu laitteet.
EIR-rekisteriä ylläpidetään Dublinissa CEIR(Central EIR)-rekisterissä. Näitä ylläpitää suurin osa operaattoreista.

Valkoinen lista
Laitteet on oikean omistajan / käyttäjän hallinnassa.

Harmaa lista
Näitä laitteita tarkkaillaan, mutta saavat toimia verkossa normaalisti.

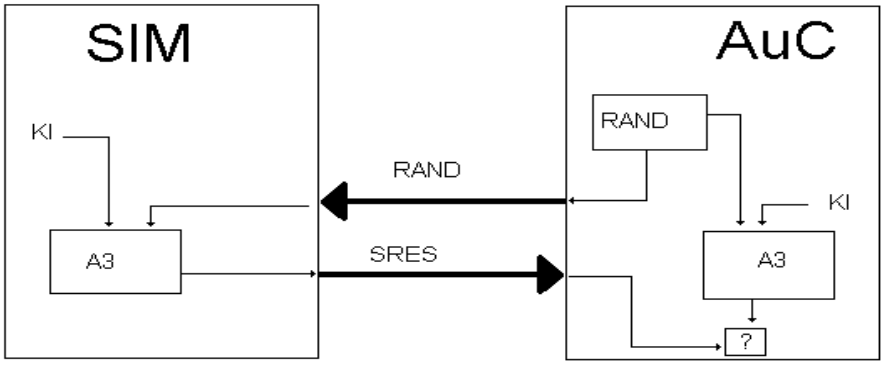
Musta lista
Tällä listalla olevat laitteet on ilmoitettu varastetuiksi / kadonneiksi ja näillä laitteilla ei ole pääsyä verkkoon.
Näistä listoista käytössä on yleisesti vain musta lista.
(Vesanen A. 2005)

2.4 ALGORITMEISTA

2.4.1 A3, Päätelaitteen autentikaatioalgoritmi

Algoritmi on yleisesti ottaen mahdollisimman pitkälle tarkennettu toimenpidesarja, jossa askel askeleelta esitetään yksikäsitteisessä muodossa ne toimenpiteet, joita asetetun ongelman ratkaisuun tarvitaan. Elikkä algoritmi muodostetaan matemaattisilla operaatioilla joiden avulla selkokielinen teksti muodostetaan salatuksi. A3 Autentikointi- eli tunnistusalgoritmi on asennettu puhelimen SIM korttiin ja sen tarkoituksena on estää kortin väärinkäyttö. AuC (Authentication Centre) tutkii on kyseisen käyttäjän puhelimen SIM korttilla oikeus käyttää verkkoa. Näiden oikeuksien tarkistamiseen käytetään parametreja RAND (Random Number), Ki ja SRES (Signed RESponse). AuC arpoo satunnaisluvun RAND, ja tämä luku lähetetään alustusmerkinannossa puhelimen SIM-kortille. Tämän jälkeen SIM-kortti laskee RAND:n , kortilla olevan salausavaimen Ki ja salausalgoritmin A3 avulla arvon SRES (Signed RESponse). AuC:ssa , jolla on tieto käyttäjän salausavaimesta Ki laskee saman SRES arvon. Ki salausavainta ei siirretä puhelun aikana puhelimen ja AuC:n välillä. Vertailu tehdään siis SRES tuloksia vertaamalla ja jos tulokset ei ole toisiinsa sopivia, niin virheenä voi olla silloin käyttäjän Ki-salausavain väärä tai A3- algoritmi väärin. Tästä johtuen ei puhelu onnistu koska verkko katsoo puhelun olevan luvaton. Kuvio 5 näyttää kuinka tunnistuskäytäntö toimii. Kaikilla toimivilla operaattoreilla on siis oma

A3- algoritmi joka pitäisi olla julkinen.



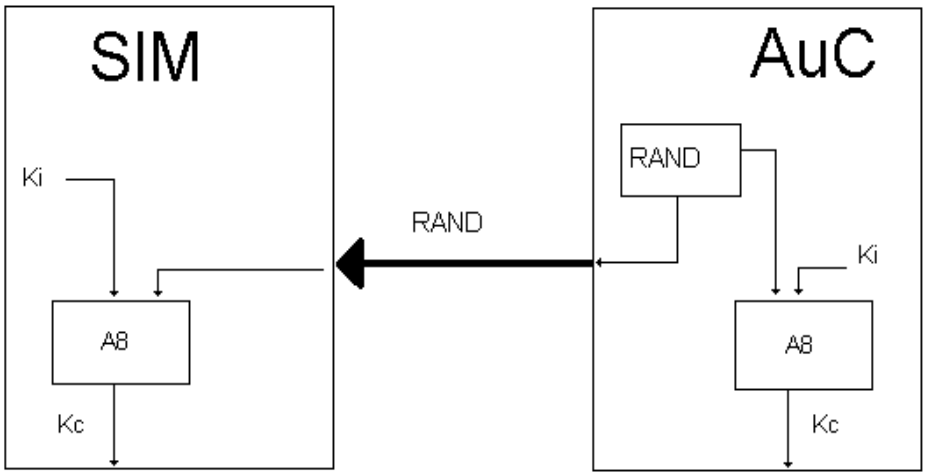
KUVIO 5

(Kiviranta M. ,Paavola M. , Pöyhönen T. , Rastas J.)

2.4.2 A8- eli salausavaimen generointialgoritmi

A8-algoritmi käyttää hyväksi puhelinkeskuksen lähettämää RAND-sanomaa kehittämällä siitä salausavaimen. Tätä saatua avainta käytetään sitten mobiililaitteen ja tukiaseman välillä käyvään liikenteen salaamiseen. Itse radiotiellä tapahtuvan liikenteen salaaminen toteutetaan siten, että ensin muodostetaan uusi salausavain Kc joka lasketaan sekä SIM– kortilla sekä AuC:ssa. Tässä käytetään hyväksi RAND-sanomaa ja algoritmia A8. Kc:n muodostaminen on esitetty kuviossa 6. Toiminto on samankaltainen kuin

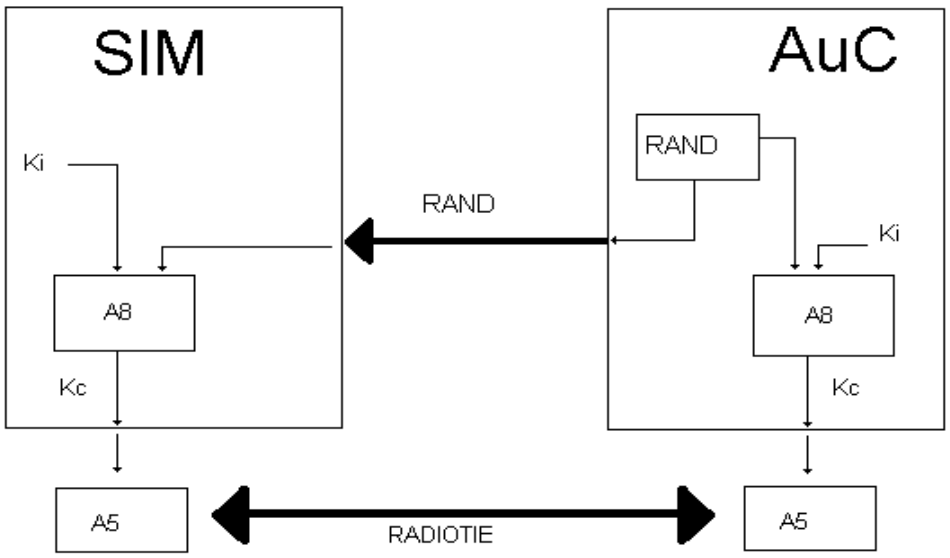
autentikoinnissa käytetyn SRES:n laskeminen. Kc on yhteyskohtainen ja sen muodostamisen jälkeen aloitetaan itse radiotiellä liikkuvan tiedon salaus.



KUVIO 6
(Kiviranta M. ,Paavola M. , Pöyhönen T. , Rastas J.)

2.4.3 A5- eli puheensalausalgoritmi

Algoritmilla A5 on käytössä 3 eri siirtorekisteriä, jotka ovat pituuksiltaan 19, 22 ja 23 bittiä. Jos rekisterien ns. karakteristiset polynomit on valittu oikein, niin bitti-virran jakson pituus on noin 1.84 * 10^19 jolloin A5:n tuottamalla bittivirralla voidaan salataan puhetta 114 bitin lohkoissa ja kunkin 114 bitin lohkon jälkeen salaus alustetaan avaimen ja lohkonumeron perusteella. Lohkonumerot toistuvat 3 tunnin ja 29 minuutin välein. Puheen salaus menee vapaassa ilmatilassa, kun taas datan salaus on salatussa liikenteessä.
KUVIO 7
Myös A5-algoritmista on useita eri versioita:
A5/0 ei sisällä lainkaan salakirjoitusta
A5/1 on alkuperäinen A5-algoritmi
A5/2 on heikennetty algoritmi
A5/3 on vahva salausalgoritmi



Kuvio 7

(Kiviranta M. ,Paavola M. , Pöyhönen T. , Rastas J.)

2.4.4 COMP128

”COMP128 on salaisesti kehitetty algoritmi, mutta se on vuotanut julkisuuteen. Tekijät Marc Briceno, Ian Goldberg ja David Wagner väittävät koodin olevan osittain peräisin vuotaneista GSM -spesifikaatioista ja täydennetty reverse-engineeringillä toimivasta SIM -kortista. Tekijät väittävät myös löytäneensä näin joitakin ristiriitoja spesifikaation ja toteutuksen välillä. Algoritmia voidaan käyttää sekä A3 että A8 -algoritmina, koska COMP128 tuottaa sekä SRESin että Kc:n yhdessä ajossa. Ensimmäiset 32 bittiä muodostavat luvun SRES, minkä jälkeen tulosteesta käytetään 54 alinta bittiä avaimeen ja 10 bittiä täytetään nollilla. Näin toimitaan myös niissä toteutuksissa, joissa ei käytetä COMP128 -algoritmia. Siten ilmatien salausavaimen tehollinen pituus on itse asiassa 54 bittiä”. (Vesanen A. 2005)

3 WLAN

3.1 Yleistä

WLAN (Wireless Local Area Network) eli langatonta lähiverkkoa. Tässä sovelluksessa tietoliikenne kulkee kaapeloinnin sijasta radiotaajuuksia käyttämällä. Langattomalla lähiverkolla on etunsa sekä myös haittansa kun verrataan lankamallilla toteutettuun verkkoon. Suurin langattomuuteen liittyvä hyöty on mahdollisuus liikkua ilman katkoksia lähiverkon alueella. Langattomuus helpottaa myös asennuksia ja kustannuksia, kun kuparikaapelointia ei tarvitse enää toteuttaa uusiin rakennuksiin. Tällä voidaan toteuttaa myös tietoliikenne yhteydet paikkoihin joihin ei ole mahdollista toteuttaa langallista verkkoa. WLAN - verkkoon kuuluvat keskeisesti erilaiset standardit. Yleisin standardi on 802.11b, joka määrittelee käytettävän taajuusalueen (2,4GHz) sekä tiedonsiirtonopeuden (11Mbps). Standartit esitellään erillisenä lukuna tässä osiossa. Päätelaitteessa täytyy olla langaton verkkokortti (WLAN -kortti) sekä käyttöjärjestelmä, joka tukee korttia. IEEE 802.11 WLAN –laitteet täyttävät FCC (Federal Communications Commissions) määräykset 2.4GHz:n ISM -kaistan (Industrial, Scientific ja Medical) käytöstä. Tämän taajuuskaistan käyttöön ei tarvita erikseen lisenssiä. (Seppänen L. 2002)

3.2 Yleistä langattomasta lähiverkosta

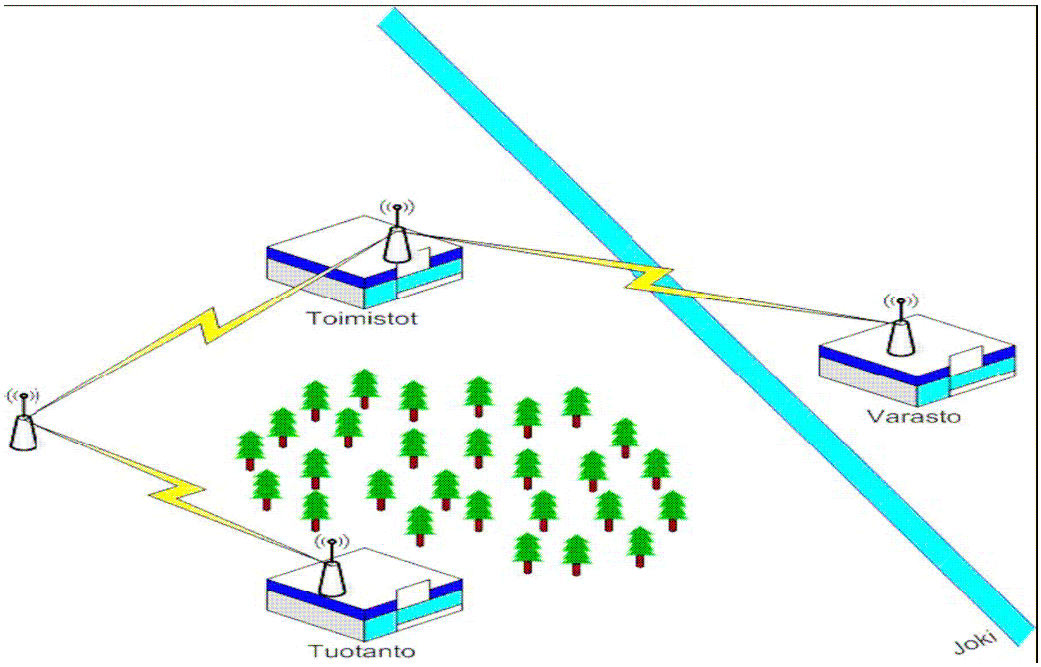
Matkapuhelin on ollut ensimmäisiä langattomuutta käyttävä laitteita joita suurin osa ihmisiä on oppinut käyttämään ja joka nykyisin näkyy jokapäiväisessä elämässä. Matkapuhelimen yleistyessä on tullut ihmisille mielikuva langattomuuden tuomasta vapaudesta ja helppoudesta. Langatonta lähiverkkoa pidetään helppona rakentaa, koska ei tarvitse vetää kaapelointia ja tätä kautta työpisteiden asettelu helpottuu. WLAN - verkossa tietoa lähetetään ja vastaanotetaan langattomasti. Tästä johtuen ajatellaan, että tietoturva ei voi olla kovin hyvä silloin. Langattomuuden johdosta myös verkkoyhteyksien toimivuutta saatetaan epäillä. Langattomien laitteiden tiedonsiirtonopeuksilla joita

valmistaja ilmoittaa ei uskota päästävän yhtä tehokkaisiin nopeuksiin kuin kaapeloidulla verkolla. (Seppänen L. 2002)

3.3 Langattoman verkon edut

WLAN on nyt nykyaikana kasvattanut hyvin suosiotaan nopeutuvalla kasvulla. WLAN kauden alussa saattoi kasvua hidastaa ennakkoluulot verkon tietoturvasta ja laitteistojen saatavuus. Myös tiedonsiirron luotettavuutta ja nopeutta epäiltiin. Langaton ratkaisu tuo eri mahdollisuuksia, mitä lankaverkko ei pysty tarjoamaan. Näistä tärkeimpänä voidaan ehkä pitää liikkuminen verkon kuuluvuus alueella ilman katkoksia ja liittämistä erikseen verkkoon. Uusien tietojen päivitys onnistuu helposti paikoissa mihin ei ole vedetty lankaverkkoa tai tarvitaan liikkuvuutta. Tämmöisiä paikkoja on esim. kaupat jossa hintoja täytyy päivittä, jolloin se onnistuu mainiosti langattomaan verkkoon kytketyllä koneella ja samalla, kun hinta tietoa päivitetään astuu se voimaan samalla kassakoneisiin. (Viestimaa.fi 2006)

Kun toteutetaan uutta tietoliikenneverkkoa on langaton verkko hintavertailussa huomattavasti edullisempi, kuin langallinen verkko. Toteuttamiseen tarvitaan ainoastaan tukiasemat ja päätelaitteisiin WLAN-kortit. Langallisessa verkossa tulee kustannuksiin tietoliikennekaapelit ja niiden laittaminen paikoilleen. Suuria säästöjä saadaan silloin kun toimipisteet sijaitsevat lähekkäin, mutta ei samassa rakennuksessa. Tällöin langattoman verkon toteutus tulee halvemmaksi, kuin vedettäisi kaapelia toimipisteiden välille. Langattomissa vaihtoehdoissa tarvitaan vain tukiasemia riittävä määrä. Mikäli tukiasemien välillä on jokin läpitunkematon este, tarvitaan yksi ylimääräinen tukiasema sen kiertämiseen.(kuvio 8) (Geier 1999: 9,11)



Kuvio 8

3.4 Langattoman verkon haittapuolet

Vaikka WLAN verkko tuo hyviä etuja käyttäjille yrityksessä, niin saattaa se tuoda päänvaivaa ylläpidolle. Tiedonsiirtonopeus saattaa pätkiä ja yhteensopivuus käytössä oleviin laitteistoihin ei ole välttämättä kaikkein paras. Ilman suojausta verkkoon voi kirjautua kuka vaan joka on verkon kantaman sisäpuolella ja käytössä on sopivat laitteet.

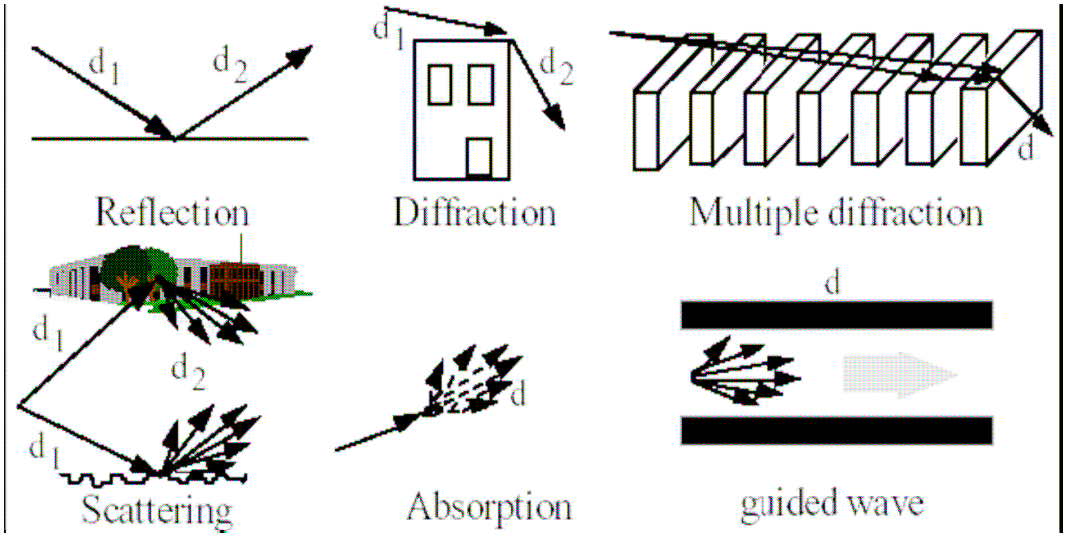
3.4.1 Rakenteelliset esteet

Tila jossa ei ole väliseiniä tai muita rakennettuja esteitä toimii WLAN verkko hyvin ja on helppo toteuttaa. Kun taas yleensä teollisuusrakennuksissa on väliseiniä ja kerroksia useita, niin silloin signaalin kantama ja voimakkuus yleensä heikkenee riippuen fyysisistä esteistä. Näitä ongelmia onneksi voidaan kartoittaa jo toteuttamisvaiheessa mittaamalla signaalin laatua ja voimakkuutta. Näiden mittaus-

ten perusteella on sitten helppo päättää kannattaako WLAN verkkoa toteuttaa. (Seppänen L. 2002)

3.4.2 Signaalinen eteneminen

Signaalit käyttäytyvät erilaisissa ympäristöissä eri tavalla esim. sisätiloissa signaalin etenemiseen vaikuttavat rakennuksessa käytetyt materiaalit, hissikuilut, porraskäytävät, huoneiden korkeus, ikkunoiden lukumäärä ja huoneiston kalusteet. Kun taas ulkotiloissa epävarmuustekijöitä on enemmän: kuiva/kostea ilma, vuodenaika, kasvillisuus, lumipeite, kaupunki maaseutuympäristö, jne. Etenemistä voidaan ennakoida etenemismalleilla. Näitä etenemismalleja ovat vapaan tilan eteneminen, monitie-eteneminen, heijastuminen, taittuminen, taipuminen, …(kuvio9)



KUVIO 9 Etenemismallit

3.4.3 Radiosignaalin aiheuttamat haitat

WLAN verkossa käytetään tiedon lähettämiseen ja vastaanottamiseen radioaaltoja. Tästä johtuen verkosta tulee haavoittuvainen ulkopuolisille

häiriötekijöille. Yleisempiä häiriötekijöitä on samalla taajuuksilla toimivat laitteet, kuten esimerkiksi mikroaaltouuni jolla on sama taajuus 2,4 GHz mitä myös langatonverkko käyttää. Tämmöisistä häiriöistä saattaa syntyä viivettä tai virheellistä lähetystä pahimmissa tapauksissa. Vaikka laitteita jotka häiritsevät langatonta verkkoa niin ei se ole este verkon rakentamiselle. Häiriö jota laitteet aiheuttavat käyttävät kapeaa kaistaa kun vertaa sitä WLAN -verkon käyttämään kaistaan. (Geier 1999: 21)

3.5 Käytettävät standardit

IEEE (Institute of Electrical And Electronics Engineers) on tietoliikennealan standardointijärjestö , joka vastaa monien muiden standardien ohella myös langattomissa lähiverkoissa toimivasta 802.11-standardeista.
IEEE 802.11 -suosituksen tehtävänä on määritellä toiminta sellaisessa langattomassa lähiverkossa, jossa kanavavaraukseton päätöksenteko on yksittäisillä työasemilla tai keskitetysti tukiasemalla. IEEE 802.11 -suosituksen ensimmäinen versio hyväksyttiin vuonna 1997. Alkuperäinen siirtonopeus oli yksi ja kaksi megabittiä sekunnissa. Standardi sisälsi verkoille monia vaihtoehtoisia toteutuksia eikä taannut keskinäistä yhteensopivuutta, mikä vähensi niin laitevalmistajien kuin kuluttajienkin suosiota. Paranneltu versio julkaistiin vuonna 1999, ja se toi mukanaan kaksi laajennusta: IEEE 802.11a, joka tukee 54Mbps siirtonopeuksia 5GHz ISM-alueella ja IEEE 802.11b, joka tukee 11Mbps siirtonopeuksia 2,4 GHz:n ISM -alueella. (Granlund 2001: 230)

Standardoinnin avulla saadaan selvät pelisäännöt jotta ei syntyisi ristiriitoja eri tekniikoiden välille, kuten bluetooth jolla on sama taajuus käytössä kuin WLAN verkolla. Näin standardoinnin avulla saadaan poistettua uhkia että nämä sotkisivat toisiaan. (Seppänen L. 2002)

3.6 Standardit

Standardeista perusstandardeja ovat 802.11a, 802.11b ja 802.11g lisäksi lisästandardeja ovat 802.11h,802.11d, 802.11i, 802.11e,802.11f ja 802.11s Näistä yritykseemme tulemme valitsemaan 802.11b. Tämä standarti on laajimmalle levinnyt ja eniten käytetty tällä hetkellä, joten sen käyttöön ottaminen on siksi turvallinen ratkaisu. Harkinnassa on myös 802.11g jolloin saataisi nopeampi yhteys. Tämähän on parannettu versio 802.11b:stä

3.6.1 Standardi 802.11b

Alussa 802.11-standardin nopeus 1 ja 2 Mbps ei ollut riittävä vastaamaan kaapeliverkon nopeuksia. IEEE määritteli suuremman siirtonopeuden multimediapalveluja silmällä pitäen. Vuonna 1999 IEEE 802.11 ”High rate” -lisäys hyväksyttiin. Siinä määriteltiin tiedonsiirtonopeudet 5,5 ja 11 Mbps sekä parempi yhteyden laatu. Suurempaa tiedonsiirtonopeutta varten valittiin suorasekvenssi. 802.11b-järjestelmät toimivat 1 ja 2 Mbps 802.11 DSSS-järjestelmien (Direct Sequence Spread Spectrum) kanssa. Koodaustekniikka CKK (Complementary Code Avaining) kehitettiin 802.11-standardin nopeuden lisäämiseksi.(Wikipedia 2006)

802.11b on tällä hetkellä suosituin käytettävistä olevista standardeista. Liikennöinti tapahtuu ISM -taajuusalueella 2,4-2,4835 GHz Samalla taajuudella toimii myös bluetooth – laitteet. Koska taajuusalue on vapaa alue, niin tämän ansiosta voidaan WLAN verkko pystyttää mihin tahansa ilman radiolupaa. 802.11b teoreettinen nopeus on 11Mbps:n. Käytännössä nopeus on kuitenkin yleensä vain 5 – 7 Mbps koska kaikki häiriötekijät tiputtavat liikennöintinopeutta. Näitä haittatekijöitä on samaa taajuutta käyttävät laitteet ja fyysiset esteet. (Wikipedia 2006)

3.6.2 Standardi 802.11a

Tämä standardi julkaistiin yhtä aikaa kuin versio 802.11b. Mutta tässä nopeudessa päästään teoriassa nopeuteen 54 Mbps:n. Tämän vuoksi valitaan tämä standardi käyttöön jos tarvitaan suurempaa kaistaa vaikkapa videon välittämiseen. Tämä standardi määritteli tiedonsiirtoa varten ODFM -tekniikan (otrhogonal division frequency modulation), joka perustuu signaalin jakamiseen pienempiin alasignaaleihin. Jaetut signaalit siirretään yhtäjaksoisesti eri taajuuksilla. Tämän avulla saatiin taajuusalue jolla standardi 802.11a toimii on vähän yli viiden gigahertsiä. Euroopassa käytetään taajuuksia 5,15 - 5,35 ja 5,470 - 5,725 GHz. Usa:ssa käytettävät taajuudet 5,15 - 5,35 ja 5,725 - 5,825 GHz ja Japanissa 5,15 - 5,25 GHz. Näistä taajuuksista alemmat taajuudet on tarkoitettu käytettäviksi sisätilaratkaisuihin ja lähetysteho on rajattu 200 milliwattiin. Ylemmät taajuudet on taas luokiteltu käytettäviksi ulkotilaratkaisuihin ja näillä taajuuksilla lähetys teho saa olla 1 watti. (Kuokka 2002: 10-12)

3.6.3 Standardit 802.11h ja 802.11d

Standardissa 802.11a:ssa on tiettyjä puutteita, joten kehittelyn alla oleva standardi 802.11h, lisäisi versiosta 802.11a puuttuneita ominaisuuksia kuten dynaamisen kanavan vaihdon sekä myös automaattisen tehonsäädön. 802.11d taas liittyy kehitteillä olevaan h-standardiin kiinteästi. Tämän standardin avulla saadaan mahdollisuus sopia käytettävät taajuuskaistat sopiviksi joka maalle erikseen. Tämä merkitsisi sitä siis että WLAN – kortti osaisi virittäytyä automaattisesti jokaisen maan tarjoamille taajuuksille lukemalla tiedot suoraan tukiasemalta johon on yhteydessä. (Kuokka 2002: 13)

3.6.4 Standardi 802.11g

Tämän standardin mukaiset laitteet toimivat standardin 802.11a tapaan 54Mbps:n nopeudella, mutta taajuudella 2,4GHz. Tämä standardi kehitettiin koska versio 802.11a ei ollut yhteensopiva version 802.11b kanssa. Versio 802.11g on siis yhteensopiva version 802.11b kanssa jota versio 802.11a ei ollut ja tätä versiota käytetään yleisesti paikoissa jossa vaaditaan suurta kaistaa kuten messu tapahtumat tai isot auditoriot. (Kuokka 2002: 13)

3.5.5 Standardi 802.11i

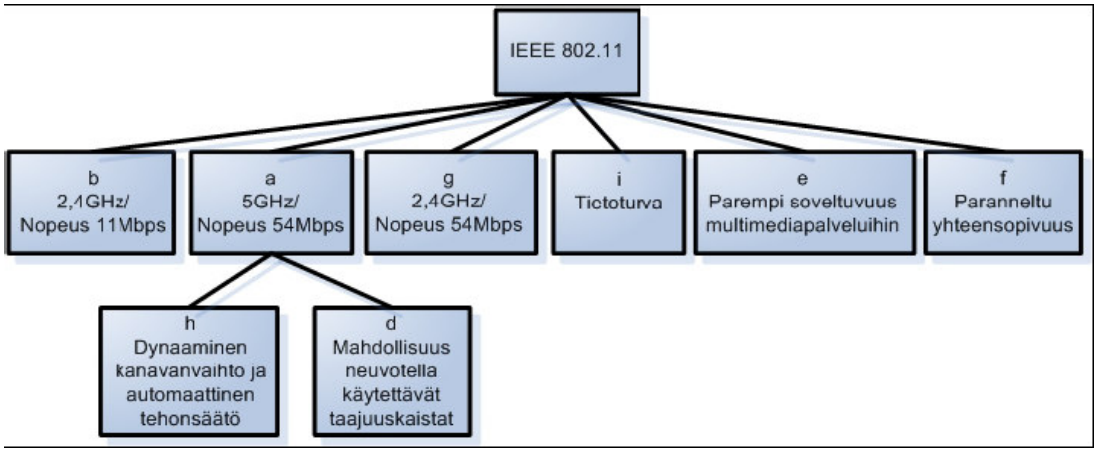
Uusin langattomien lähiverkkojen standardi, 802.11i on saanut standardijärjestö Wi-Fi Alliancen lopullisen hyväksynnän. Uusi standardi tuo 802.11:een tietoturvaa parantavan AES -tekniikan (Advanced Encryption Standard).
AES on vahvempi suojaus kuin nykyinen WPA. AES on myös Yhdysvaltojen julkishallinnon langattomien verkkojen tietoturvastandardi.
(Kuokka 2002: 13; The wireless lan association 2002)

3.6.6 Standardit 802.11e ja 802.11f

E ja f-versiot parantavat laitteiden uusia ominaisuuksia. 802.11e pyrkii parantamaan WLAN -verkon soveltuvuutta multimediapalveluihin. F-version pyrkimyksenä on parantaa eri valmistajien välistä yhteensopivuutta.
Standardit (Kuvio 10)

3.6.7 Standardi 802.11s

Tämän tulevan standardin tarkoituksena on mahdollistaa WLAN -tukiasemien liittäminen suureksi silmukkaverkoksi. Standardia käytettäneen kaupunki WLAN -verkkojen rakentamisessa. (Wikipedia 2006)

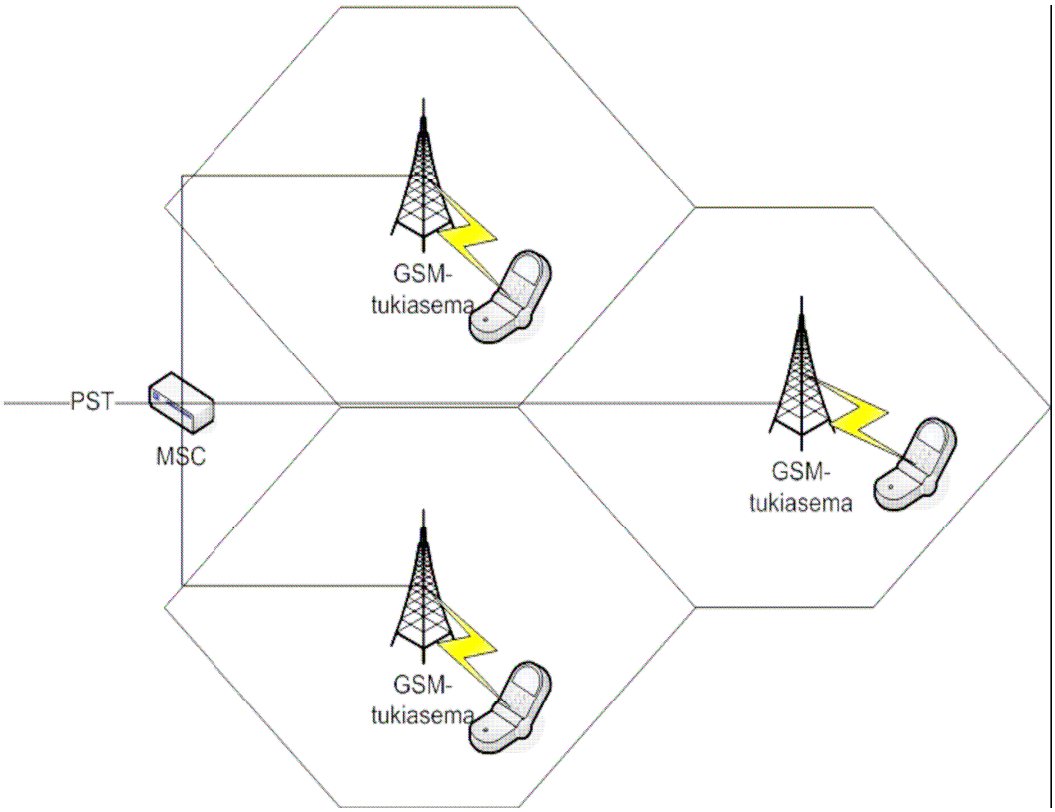


Kuvio 10

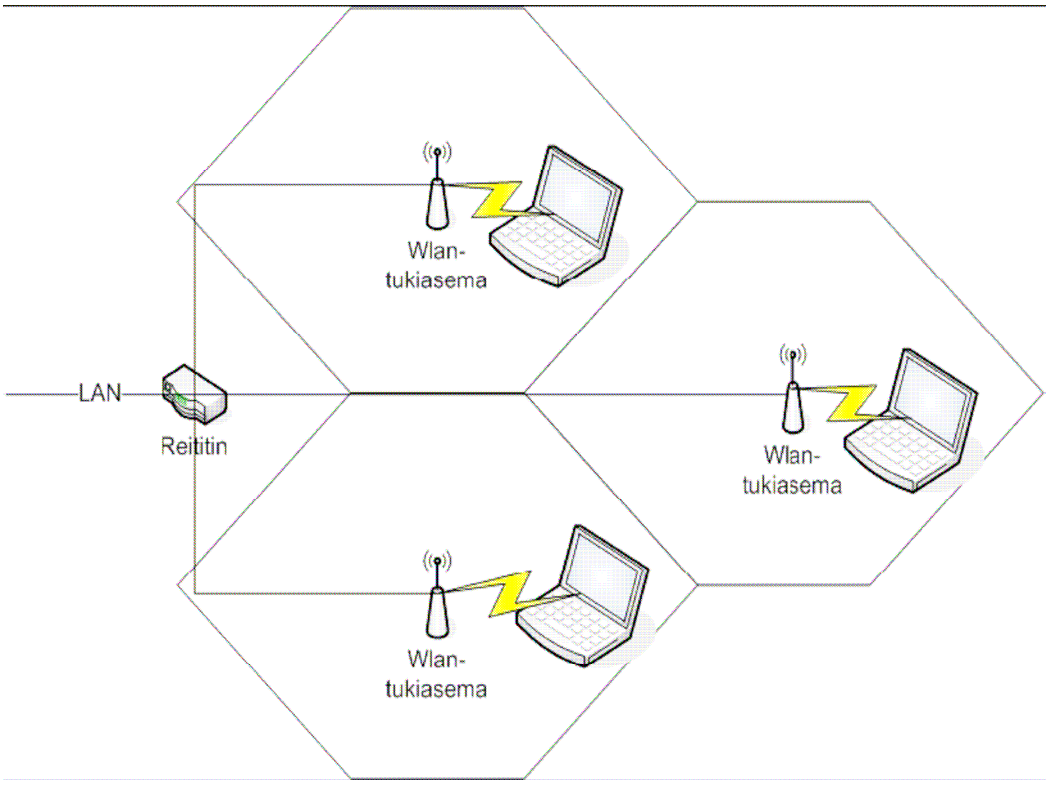
4. WLAN – VERKKON RAKENNE

4.1 WLAN - verkko

WLAN - verkko arkkitehtuuri muistuttaa GSM-verkosta tuttua solurakennetta. (Kuvio 11, kuvio 12) Jokaisella solulla on siis oma taajuusalueensa, jolloin yhteydenpito tapahtuu solun vaikutusalueen sisällä. Jotta toimivuus voidaan taata, niin vierekkäiset solut eivät saa käyttää samaa taajuutta. Tukiasemat hoitavat solun sisällä WLAN liikennettä. Tukiasemat ovat keskenään yhteydessä toisiinsa runkoverkon välityksellä. Yhteys tukiasemiin hoidetaan WLAN-kortista radiorajapinnan välityksellä. Alla olevissa kuvioissa on havainnoitu verkkojen samankaltaisuutta. (Seppänen 2002)



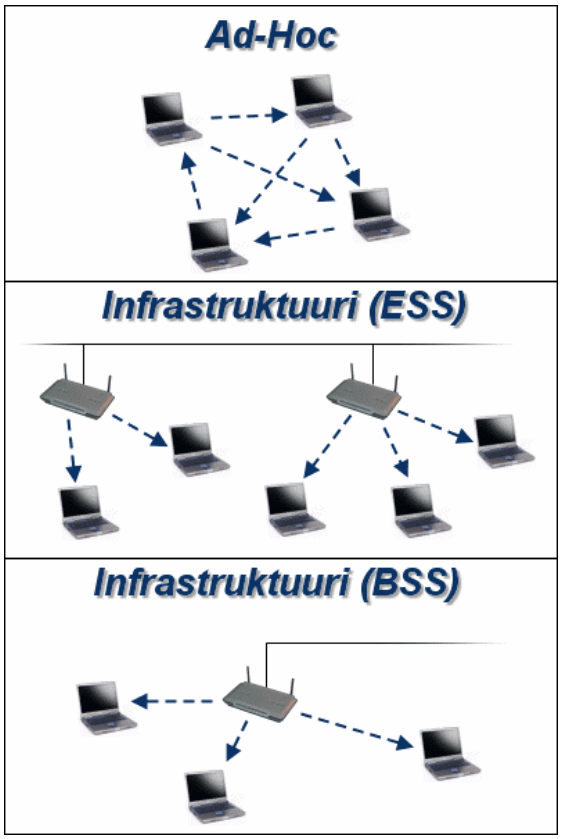
Kuvio 11 GSM-verkko Seppänen S. 2002.



Kuvio 12 WLAN-verkko Seppänen 2002.

4.2 Topologiat

WLAN-verkko voidaan rakentaa joko WLAN-tukiasemalla tai ilman. Jos verkko rakennetaan ilman tukiasemaa, sitä kutsutaan AD-HOC verkoksi ja jos taas verkossa on tukiasema, sitä kutsutaan infastruktuuriverkoksi. Tämä AD-HOC ratkaisu on halvempi tapa koska siinä ei ole WLAN-tukiasemaa. Mutta on siinä omat haittapuolensakin, sillä tietokoneiden kantavuus ei veny kovin pitkäksi, koska kaikkien tietokoneiden jotka ovat verkossa pitää olla yhteydessä toisiinsa, kun taas tukiasemallinen verkon kantavuus saadaan jopa kaksinkertaiseksi. AD-HOC on hyödyllinen pienissä tiloissa, koska verkko saadaan tietokoneiden välille rakennettua nopeasti ja vaivattomasti ja tieto kulkee suoraan osoitetulle tietokoneelle ei siis kaikille AD-HOC verkon tietokoneille, joten turhaa verkkoa ei rasiteta. Infastruktuuriverkko voidaan jaotella kahteen eri topologiaan: BSS:ään (Basic Service Set) ja ESS:ään (Extended Service Set), näistä BBS on ehkä yleisempi ja se soveltuu hyvin koteihin ja toimistoihin. Tässä verkossa on ainoastaan yksi tukiasema, jonka kautta tietokoneet kommunikoivat toistensa kanssa. EES-verkossa on useampi tukiasema. Yleensä tukiasema on yhteydessä langalliseen verkkoon, mutta on myös mahdollista yhdistää useampi tukiasema langattomasti toisiinsa, ja tällöin tukiasemien kantavuus voidaan kasvattaa ja tietokoneet voivat olla yhteydessä toisiinsa entistä pidempien matkojen päästä. Esimerkiksi otan matkapuhelinverkon, joissa käytettävät tukiasemat minivoivat taajuusalueen ulkopuolelle jäävät katvealueet rakentamalla tukiasemat lähelle toisiansa, jolloin matkapuhelimien käyttö on mahdollista melkeinpä missä vain.(Kuvio 13)
(Granlund 2001: 231-232)



Kuvio 13 Topologiat

5. TIETOTURVA WLAN

5.1 Yleistä

”Vain harvat yritykset tiedostavat langattoman lähiverkkonsa heikkoudet ja ymmärtävät, mitä datan ja kommunikaation turvaamiseen vaaditaan. Langattomat lähiverkot eivät ole tietoturvan kannalta sen erikoisempia kuin langalliset verkotkaan, mutta WLANit ovat helpommin vakoiltavissa, koska niiden signaalit kulkevat julkisessa ilmatilassa”. (Marek 2001)
WLAN-verkon ei salattua liikennettä on siis helppo kuunnella koko verkon kuuluvuusalueella. Useasti verkon kuuluvuusalue ulottuu laajemmalle kuin verkkoa suunniteltaessa on osattu ottaa huomioon. Yrityksen WLAN-verkko saattaa siis olla vapaasti käytettävissä ja kuunneltavissa yrityksen toimitilojen ulkopuolelta. Ilman riittävää tietoturvaa ja tunnistautumista WLAN-verkot ovat vapaasti kaikkien verkon kuuluvuusalueella olevien käytettävissä. Tällöin ulkopuolinen taho voi käyttää WLAN-verkkoa erilaisiin väärinkäytöksiin, kuten roskasähköpostin levittämiseen ja saattaa päästä tätä kautta yrityksen langalliseen verkkoon käsiksi.
(www.ficora.fi)

5.2 Keskeiset turva-aukot ja suojautuminen

Yrityksen tietoliikennettä voidaan salakuunnella. Voidaan siis tutkia yrityksestä lähtevää ja saapuvaa tietoliikennettä. Salakuuntelun estäminen on hankalaa ja vaikeasti estettävissä ja mahdotonta havaita.Tukiasema on välinen jonka tunkeutuja kautta pääsee sisään verkkoon. Jos WLAN on kytketty yrityksen langalliseen lähiverkkoon, niin WLANiin tunkeutuja pääsee käsiksi silloin yrityksen koko verkkoon. Tunkeutuja halutessaan katkaista yhteydet ja haitata tätä kautta yrityksen tietoliikennettä. Koska WLAN toimii vapaalla radiotaajuusalueella, voidaan kuormittaa taajuusaluetta niin, että verkossa liikennöinti hidastuu tai loppuu kokonaan. Yksi tapa vahingoittaa yrityksen tietoliikennettä on ylikuormittaa verkkoa jatkuvilla tarpeettomilla palvelupyynnöillä. Koska kuka tahansa voi

pystyttää tukiaseman. Tunkeutujan on verkkoon tunkeutumisen jälkeen helppoa pystyttää oma tukiasemansa ja tukiasemassa voidaan käyttää yrityksen Internet-osoitetta, jonka takia silloin yrityksen asiakkaat tulevat sisään verkkoon tämän vale tukiaseman kautta.
(Vesanen A. 2005)

Langattomien lähiverkkojen suurin turvallisuusriski on niiden omistajissa. Lähes joka kolmas WLANin omistajista, lähinnä kotona tai kotitoimistoissa, ei ole asettanut verkkoonsa minkäänlaisia turva-asetuksia päälle ja on käynnistänyt sen tehdasasetuksilla. Kolme neljästä ei käytä salausta lainkaan. (Poropudas 2002)

5.2.1 WEP avain

Yksi hyvä tapa on käyttää WEP (Wired Equivalent Privacy) avainta sekä tarkista, että käytettävät kortit ja tukiasemat ovat asetettu käyttävät vahvempaa salausta, sekä vaihdetaan oletusavaimet ja muuttamalla WEP sovelluksessa käytetään RC4 (Ron's Code 4, Rivest Cipher 4) suojausalgoritmia, joka on sama, jota käytetään turvaamaan online-kaupankäynti. RC4 on langattomasta tuotteesta riippuen 64 tai 128 bittiä pitkä. Teoriassa on mahdollista käyttää avaimia yhdestä bitistä 2048 asti. Vaihdetaan tukiaseman langattomaan verkkoon lähettämä nimi, (SSID,Service SETID) Jos tukiasemalla on käytössä "Broadcast SSID" ominaisuutta, otetaan se pois käytöstä Jos mahdollista käytetään yhteyskohtaisia avaimia (PKI, Public Key Infrastructure) Jos tuote tukee MAC (Media Access Control) osoitteeseen perustuvaa suodatusta, käytä tukiasemissa sitä.(Liite 1) Avaimia on hyvä vaihtaa aina silloin tällöin. Useissa tuotteissa on mahdollisuus tallentaa jopa neljä avainta ja valita niistä yksi käyttöön. Tämän ansiosta säännöllisesti vaihdettava avain on suhteellisen helppo toteuttaa. WEPin staattinen avain –arkkitehtuuri ei ole hyvä ratkaisu verkolle, jolla on yli sata käyttäjää. Suuressa verkossa WEP -avaimien hallinnasta aiheutuu yrityksen IT -osastolle kohtuuttomasti vaivaa.
(Garcia 2002; Molta 2002)

5.2.2 EAP

Tietoturva paranee olennaisesti, jos WLAN -liikenteeseen lisätään sellainen palvelu, että kaikille käyttäjillä tulee henkilökohtaiset salasanat, jotka vaihtuvat säännöllisesti. Tapa jolla tämmöinen voidaan toteuttaa ottamalla käyttöön seuraavat protokollat EAP (Extensible Authentication Protocol) ja RADIUS (Remote Authentication Dial In User Service). EAP on siirtoyhteyskerroksen tunnistamisprotokolla, joka tukee useita eri tunnistamismekanismeja. EAP että RADIUS on kehitetty modeemia käytettävien yhteyksien käyttäjä hallintaan. Käyttäjien tunnistamiseen sovellettiin EAP -protokollaa ja käyttäjien tunnus/salasanaparien hallintaan käytettiin RADIUS -palvelinta. Tällä mahdollistettiin keskitetty hallinta käyttäjätiedoista. Kun WLAN -ympäristöön rakennetaan EAP / RADIUS –yhdistelmä, käyttäjätietojen hallinta voidaan keskittää yhdelle palvelimelle. RADIUS –palvelimen avulla voidaan luoda vaihtuvat ja satunnaisesti generoitavat salasanat jokaiselle käyttäjälle. (Flint 2000; Langattomien lähiverkkojen tietoturva 2002)

5.2.3 PEAP

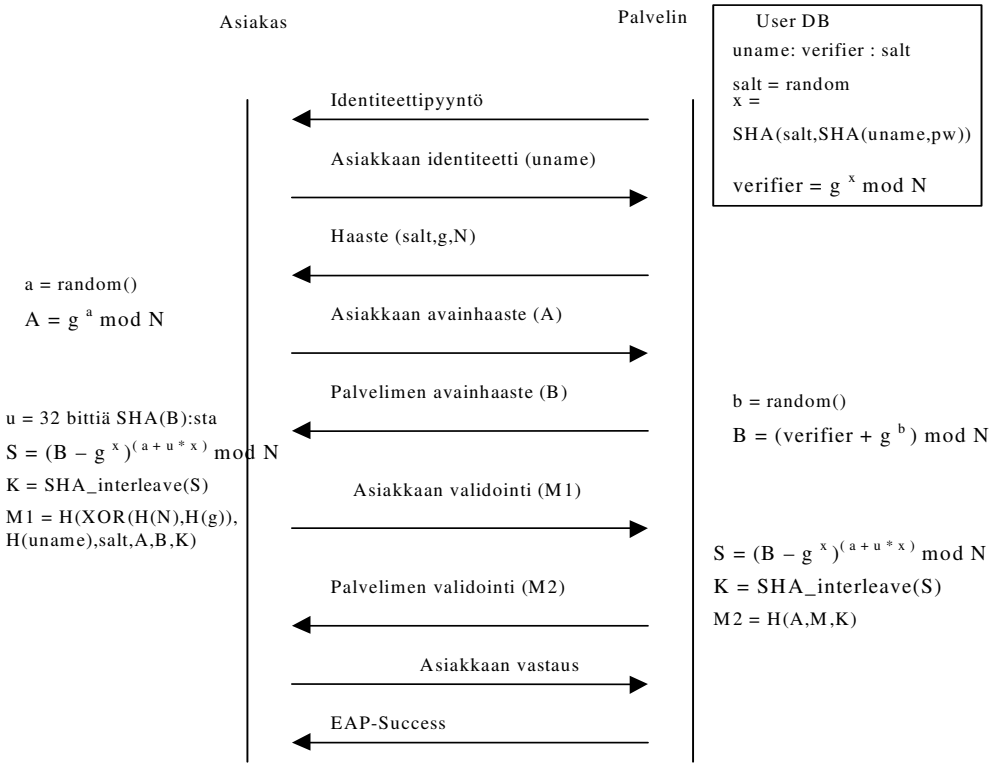
PEAP:n (Protected EAP) tarkoituksena on tarjota kaksivaiheinen autentikointimenettely, jossa ensin luodaan turvallinen TLS (Transport Layer Security)-kanava käyttäjän ja palvelimen välille. Seuraavassa vaiheessa turvallisen kanavan muodostamisen jälkeen on tarkoitus suorittaa varsinainen autentikointi käyttäen jotain muuta EAP-menetelmää. PEAP:ssa protokolla alkaa normaalin EAP:n tapaan identiteetin kyselyllä ja siihen vastaamisella. Käyttäjän ei kuitenkaan ole tarpeen tässä vaiheessa ilmaista oikeaa identiteettiään, vaan vastaukseksi riittää tunniste, jonka perusteella pyyntö osataan ohjata oikealle autentikointipalvelimelle. Tämä sen vuoksi, että salakuuntelija ei pystyisi selvittämään asiakkaan henkilöllisyyttä. TLS-kanavan muodostamisen jälkeen voidaan kuitenkin suorittaa uusi turvallinen TLS-neuvottelu, jonka yhteydessä asiakasvarmenne esitetään.PEAP:n toisessa vaiheessa osapuolten viestien vaihto suoritetaan

suojatussa kanavassa, jolloin EAP:n päällä kuljetetaan kryptografisesti käsiteltyjä TLS-tietueita. Nämä tietueet puolestaan sisältävät hyötykuormanaan varsinaisen käytetyn EAP-autentikointiprotokollan. PEAP tarjoaa myös mahdollisuuden käyttää TLS-neuvottelun aikana muodostettua yhteistä salaisuutta linkkitason avainten muodostamiseen. Määrittely ei kuitenkaan ota tarkemmin kantaa siihen, kuinka linkkitason turvallisuusalgoritmit neuvotellaan asiakkaan ja tukiaseman välille tai kuinka linkkitason avaimet saadaan toimitettua autentikointipalvelimelta tukiasemaan. (NetworkWorld 2002)

5.2.4 EAP-SRP

EAP-SRP (Secure Remote Password) perustuu SRP-määrittelyyn, joka on salasanapohjainen autentikointiprotokolla. Tässä ei lähetä salasanaa koskaan selväkielisenä ja tämä on vastustuskykyinen sanakirjahyökkäyksiä vastaan, eikä etukäteen lasketuista vasteista ole hyötyä hyökkääjälle. Lisäksi sen avulla on mahdollista generoida avainmateriaalia salausfunktioihin. Protokollassa käyttäjän pitää ensin kommunikoida identiteettinsä palvelimelle, jonka jälkeen palvelin osaa hakea oikeat kryptografiset parametrit ko. käyttäjää varten. Palvelin lähettää käyttäjälle nämä käytettävät parametrit, joiden perusteella käyttäjä osaa vastata omalla avainhaasteellaan. Tämän jälkeen palvelin lähettää vielä oman avainhaasteensa, jonka jälkeen molemmilla osapuolilla on tarpeeksi tietoa yhteisen salaisuuden laskemiseksi. Protokollassa vaihdetaan vielä yhdet viestiparit, joissa osapuolet suorittavat varsinaisen autentikoinnin todistamalla, että tietävät lasketun yhteisen

salaisuuden. Viestien vaihto on esitetty kuviossa 14.



Kuvio 14 Viestienvaihto

(Haverinen M.2003)

5.2.5 WPA – Wi-Fi Protected Access

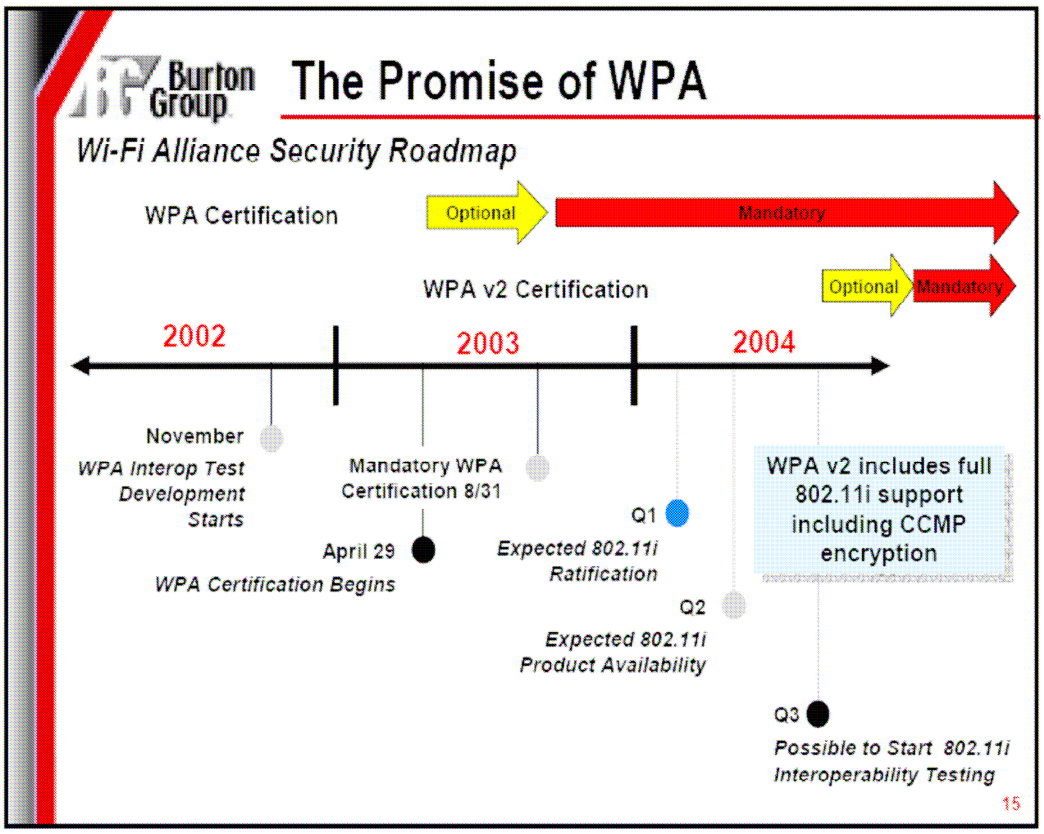
Wi-Fi Allianssi (Wireless-Fidelity) on ei-kaupallinen yhteisö, joka perustettiin vuonna 1999 edistämään IEEE 802.11 -standardiin perustuvien langattomien lähiverkkojen yhteensopivuutta. Allianssin tavoitteena on reagoida standardointielimiä nopeammin markkinoiden ja laitteistojen tarpeisiin tuottamalla standardinomaisia suosituksia teknologioiden nopean käyttöönoton ja yhteensopivuuden mahdollistamiseksi. Wi-Fi-sertifikaatti laitteessa varmistaa, että laite täyttää tietyt yhteensopivuusehdot ja toimii muiden Wi-Fi-sertifioitujen laitteiden kanssa samassa verkossa. Wi-Fi -allianssin kehitti WPAn korjaamaan WEB salauksessa olevia aukkoja. WPA - WiFi Protected Access™ WPA-salaus on yleinen standardi joten se on kaikkien valmistajien käytössä. WPA korjasi WEP -

salauksen heikkoudet ja on nykyisen tiedon mukaan vielä murtamaton. Siitä on olemassa kolme eri versiota:

WPA - PSK (Pre - Shared Key) Helppo ja optimaalinen ratkaisu kotiin tai pien-yritykseen. Tukiasemaan kirjaudutaan määriteltyä salasanaa käyttämällä, jonka jälkeen yhteys tukiaseman ja käyttäjän välillä on suojattu.

802.1X
Vanhaa WEP -salausta käyttävä järjestelmä, jossa käyttäjän tunnistus tapahtuu erillistä RADIUS -palvelinta sekä WEP -salausavainta käyttämällä. Ratkaisua käytetään lähinnä suurissa yrityksissä joissa kaikki laitteet eivät vielä tue WPA -salausta.

WPA
Suurissa ratkaisuissa käytettävä salaus, jossa erillistä RADIUS-palvelinta hyväksikäyttämällä saavutetaan erittäin korkea tietoturvan taso sekä keskitetty hallinta käyttäjäntunnistukselle. Tulevaisuus WPA (kuvio 15)
(WiFi Alliance 2006)
WPA –tekniikan salaus perustuu TKIP(Temporal Key Integrity Protocol) -protokollaan, tämä lisäys tuli standardissa 502.11i ja tamä pitää sisällään muun muassa viestin integriteetin tarkastuksen ja laajennetun aloitusvektorin. Käyttäjätodennuksesta huolehtii autentikointipalvelin, joka tunnistaa käyttäjät ennen verkkoon liittymistä. 2003 (Huhtanen 2002).
WPAn heikkoutena on järjestelmän alttius palvelunestohyökkäyksille. Tämä heikkous johtuu WPAn tavasta selvitä verkkohyökkäyksistä: WPA hyökkäyksen sattuessa sulkee koko verkon minuutiksi, jolloin myös verkon lailliset käyttäjät jäävät katkon aikana ilman palvelua. Tämä WPAn DoS -alttius on kuitenkin suhteellisen vakava ongelma, sillä hyökkäyksen toteuttamiseen ei vaadita kuin muutaman paketin lähettämisen muutaman minuutin välein. Hyökkäyksen jäljittäminen on siten paljon hankalampaa kuin perinteisissä radiotientukkimisissa. (Kuivalainen 2002.)



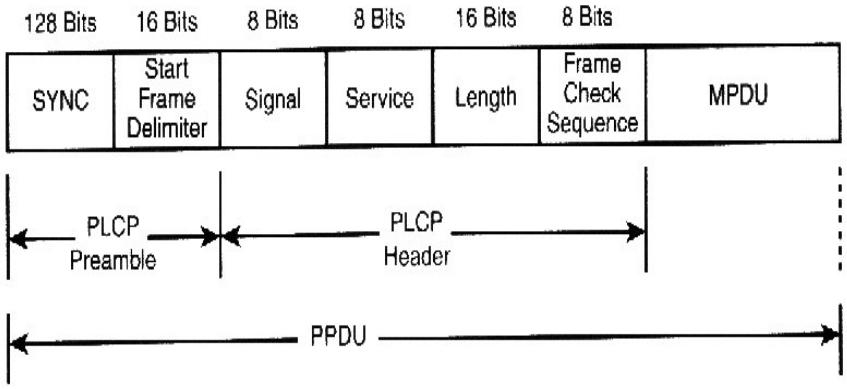
Kuvio 15

5.2.6 WLAN toiminta

WLAN käyttää lähetys toimintaansa tekniikoina seuraavia.

DSSS (Direct Sequence spread spectrum) (Kuvio 16) suorasekvenssihajaspektri-menetelmä
; 2.4-2.4835GHz: Data nopeus 1, 2 ja 11 Mbps korkeampi kuin Frequency Hopping tekniikassa ja nopeampi vasteaika kuin FHSS- tekniikassa. Käytetään määritellyn taajuusalueen kaikkia alitaajuuksia rinnakkain. Lähetettävään tietoon lisätään bittejä, jotta lähetettävä RF-signaali saadaan levitettyä koko käytössä olevalle taajuusalueelle. Yhden tietobitin siirtämiseksi muodostetaan lähetettävään RF-signaaliin 11 alibittiä, joilla kuvataan yhtä siirrettävää tietobittiä. Siirrettävä datasignaali moduloidaan tekokohinaan ja lopputulokseksi saadaan yksitoista kertaa alkuperäistä leveämpi signaali, joka ei juuri erotu normaalista taustakohinasta. RF-

signaali lähetetään samanaikaisesti 11 alitaajuutta pitkin, jolloin yksittäisillä alitaajuuksilla esiintyvät häiriöt eivät estä tiedonsiirtoa ja minimoivat virheitä.



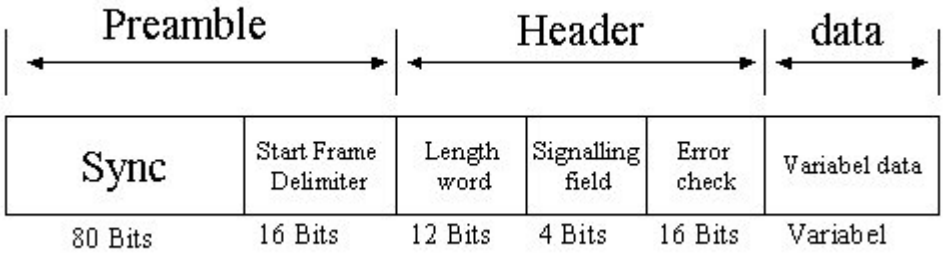
KUVIO 16 DSSS- kehys

FHSS (Frequency Hopping spread spectrum)(Kuvio 17) ; 2.4-2.4835GHz
Käyttää yhtä taajuutta taajuushyppelyyn kaikilla taajuusalueilla.
Data nopeus 1-2 Mbps ja pidemmät vasteajat kuin DSSS- tekniikassa
Lähetystä mahdoton havaita taustakohinasta mittalaitteilla. Nopeampi kahdesta tekniikasta, koska sekä lähetin että vastaanotin ovat jatkuvasti samalla taajuudella. Paketti jaetaan tietyllä avaimella kaikille alikanaville ja lähetetään amanaikaisesti. Vastaanottaja kokoaa paketin jälleen alkuperäiseen muotoonsa. Nykyiset laitteistot käyttävät suorasekvenssitekniikkaa. Etuina helpompi toteutus ja parempi läpäisykyky RF-signaali levitetään radiotaajuudelle satunnaiseksi sarjaksi. RF-signaalia vastaanotettaessa on vastaanottimen vaihdettava taajuutta samaan tahtiin, jotta lähetetty signaali saadaan vastaanotettua. Sivullisten vaikea vastaanottaa ja tulkita signaalin sisältämää tietoa (Opinnäytetyö WLAN Seppänen L.).

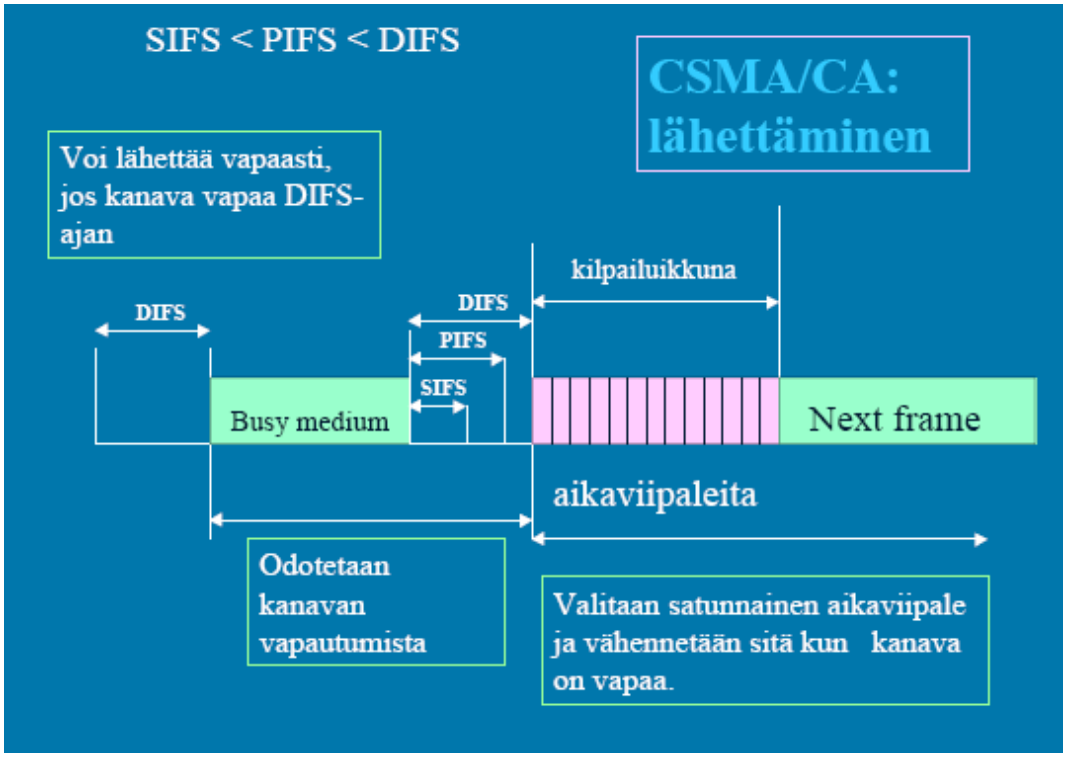
Datan lähettäminen taas tapahtuu siten, että lähettäjä lähettää RTS-kehyksen (Request To Send), jossa on kehyksessä datalähetyksen pituus. Vastaanottaja lähettää takaisin CTS- kehyksen(Clear To Send), jossa on data lähetyksen pituus. Itse lähetyksen koordinointi taas tapahtuu IFS (Interframe space) avulla.
- DIFS (Distributed IFS) määrää kuinka pitkään aseman on kuunneltava ennenkuin se voi valmistautua lähettämään tavallista dataa
- SIFS (short IFS) määrää kuinka pitkään on kuunneltava ennen kuittauksen lähettämistä

- PIFS odotusaika ei -kilpaileville lähetyksille(Kuvio 18).

(Marttinen 2003)



KUVIO 17 FHSS- kehys



KUVIO 18 Lähetys

5.2.7 VPN – Virtual Private Network

VPN on tehokas, valmistajariippumaton WLAN -verkkojen tietoturvan lisäys. Perinteisesti VPN:llä on rakennettu julkisen siirtoyhteyden (esimerkiksi Internetin) välityksellä oma turvallinen ja suojattu verkko, joka näkyy ulospäin kuten normaali verkko. Tarkoituksena on luoda eristetty tunneli julkisen siirtotien sisään yhdistämään lähiverkkoja toisiinsa. VPN:llä voidaan toteuttaa esimerkiksi etätyöntekijän yhteydet organisaation palvelimelle julkista verkkoa, kuten Internetiä, hyväksikäyttäen. Tällöin VPN on Point-to-Point-yhteys käyttäjän tietokoneen (VPN Client) ja organisaation palvelimen (VPN Server) välillä. WLAN:ssä käytetään vastaavanlaista toteutusta suojattaessa langattoman työaseman yhteys lähiverkkoon. VPN-Gateway sijoitetaan lähiverkon ja WLAN-tukiasemien välille siten, että kaikki liikenne tukiasemalta lähiverkkoon kulkee Gatewayn kautta. WLAN-työasemille asennetaan VPN Client-ohjelma, joka salaa liikenteen työasemalta Gatewaylle asti. VPN:n käyttöönottoa harkitseville suosittelemme käyttöympäristön perusteellista selvittämistä ja huolellista suunnittelua.
(Tietoturva WLANissa 2001)

5.2.8 SSN ja TKIP

SSN (Simple Secure Network) vaihtaa salausavainta säännöllisin väliajoin. Verrattuna IEEEn 802.11iprotokollaan, jonka on määrä tukkia WEPin tietoturva-aukot, SSN ei vaadi niin paljoa tehoa koneilta. (Nobel 2002.)
TKIP (Temporal Key Integrity Protocol) on kehitetty paikkaamaan WEPin tietoturvaa ilman että tarvitsee tehdä kalliita laite vaihtoja. TKIP vaihtaa salausavaimia useasti ja sen käyttämä mekanismia on nimeltä

fast-packet rekeying. TKIPistä puhuttaessa useimmat kuitenkin ymmärtävät, että kysymyksessä on pikemminkin hetkellinen apu kuin strateginen parannus. (Garcia 2002; Molta 2002; Phifer 2002)

5.2.9 Tukiaseman ja verkonvalvonta

Tukiasema tulisi sijoittaa mieluummin rakennuksen keskelle kuin ikkunoiden lähelle. Tietohallinnon tulisi säännöllisesti käyttää ohjelmia kuten NetStumbler tai vastaava huomatakseen epäluotettavat tukiasemat. Esimerkiksi NetStumbler-ohjelmalla ja ulkoisella antennilla varustetulla kannettavalla tietokoneella on helppo selvittää minkälaista tietoliikennettä välittyy rakennuksen ulkopuolelle. Tietoturvasta kiinteässä verkossa saadaan huomattavasti parempi, jos WLAN -verkko rakennetaan palomuurin ulkopuolelle ja suojataan verkko palomuurilla. (Tolonen K. 2004)

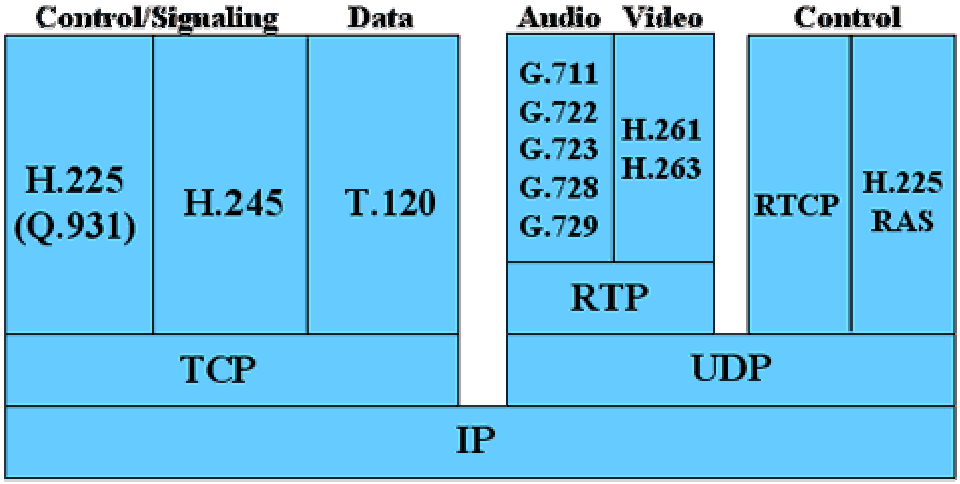
5.2.10 Johtopäätöksiä

Vaikka koko ajan tehdään työtä WLANin turvallisuuden lisäämiseksi, vielä täysin varmaa ratkaisua ei ole pystytty luomaan. Täydelliseen tietoturvaan tuskin koskaan päästäänkään, mutta yrityksillä on kuitenkin jo nykyisinkin käytettävissään useita vaihtoehtoja parantamaan verkkojensa turvaa ja uusia ratkaisuja tulee markkinoille jatkuvasti. (Tolonen K. 2004) WLAN verkko helpottaisi huomattavasti omassa yrityksessämme liikkuvuutta ja koneiden käytettävyyttä esim. neuvottelutilanteissa. Neuvotteluhuoneissa on rajattu määrä verkkopistokkeita joten verkkoon ei pääse kirjautumaan kuin muuta kerrallaan, tässä tapauksessa langaton verkko ratkaisisi ongelman.

6. VOIP

6.1 Yleistä

VoIP (Voice over IP) on tekniikka jolla ääntä siirretään IP (Internet protokolla) (Kuvio 19) hyväksi käyttäen. VoIP on periaatteessa suurin verrattavissa perinteiseen langallinen puhelimeen, mutta sen protokollana käytetään internet protokollaa ja tavallisten puhelinnumeroiden sijasta käytössä on IP -numerot. Yleisesti sanottuna VoIP on äänen siirtämistä digitaali- ja pakettimuotoisena verkon yli. Verrattuna perinteiseen IP:hen VoIP käyttää RTP (real -time protokollaa), jolla varmistetaan, että paketit tulevat perille juuri oikea-aikaisesti.
Oikea-aikaisuus ja pakettien perille tulo oikeassa järjestyksessä on todella tärkeää, jotta puhe olisi ymmärrettävää Tiedonsiirron nopeuden on oltava tarpeeksi suuri, jotta keskustelu osapuolten välillä on mahdollista.
(VoIP- a searchNetworking.com Definitions, 1.4.2003)



KUVIO 19 Protokollapino

6.2 Käytettävä tekniikka

VoIP -tekniikassa analoginen ääni muunnetaan digitaaliseksi käyttäen hyväksi A/D-(Analog to Digital Converter) muunninta. Tämän jälkeen muunnetut paketit pakataan datapaketteihin käyttäen hyväksi RTP -protokollaa ja tämä pakattu

digitaalinen data lähetetään verkon yli IP -paketeissa. Tässä tekniikassa siis ei ole koko ajan pysyvä yhteys päällä kuten se on analogisella tekniikalla. Vastaanotettaessa saapuva digitaalinen signaali puretaan paketeista ja muunnetaan äänisignaaliksi D/A-muuntimella. Käytettäessä RTP -protokollaa signaalin välityksessä mahdollistetaan lähetettävien pakettien järjestämisen vastaanottopäässä sekä saadaan aikaan se, ettei mahdollisia puuttuvia paketteja jouduta odottamaan liian kauan. Miksi VoIP -tekniikan käytössä ilmenee ongelmia, yleensä johtuu suurimmaksi osaksi käytettävän verkon hitaudesta sekä matkan varrella olevista reitittimistä. VoIP -tekniikassa äänipaketit leimataan tavallisesti ”hyvin tärkeiksi” suurelle prioriteetille, jotta niitä siirretään matkan varrella mahdollisimman nopeasti. Reitittimillä on kuitenkin usein paljon palveltavia asiakkaita, jolloin aina ei voida taata juuri tietyn puhelun pakettien kulkemista tietyllä nopeudella. (Haapakangas U-M. 1999)

6.3 VoIP:n hyödyt

VOIP tekniikassa ei siirretä pelkästään ääntä vaan sillä voidaan siirtää myös kuvia, liikkuvakuvaa ja muuta dataa. VoIP -tekniikkan avulla saadaan aikaan myös ryhmäneuvottelu puhelut helposti aikaiseksi. Koska VoIP tekniikassa tieto siirretään digitaalisessa muodossa, niin sen siirto on helpompaa ja varmempaa. Siirrossa tulevia mahdollisia virheitä voidaan yrittää korjata. Lähetettävää digitaalista signaalia pystytään myös pakkaamaan, jolloin saadaan aikaan suurempia nopeuksia tiedonsiirrossa. Siirrettävä digitaalinen signaali ei ole myöskään yhtä häiriöille altista kuin perinteinen analoginen signaali tekniikkaa Tätä tekniikkaa varten on signaaliin siirtoon valmiit reitit, sillä tekniikkahan käyttää IP –protokollaa ja tällainen verkkohan on jo käytössä ympäri maailman. VoIP -tekniikkalla saadaan siirrettyä noin kymmenkertaisesti enemmän puheluja yhtä aikaan verrattuna vanhaan järjestelmään. Tämän on mahdollista koska itse puhelua varten ei tarvitse muodostaa omaa yhteyttä vaan puheliikenne kulkee samaa kaistaa muun IP –liikenteen kanssa IP –paketteina VoIP ei myöskään sido käyttäjää päätelaiteriippuvuuteen, sillä näitä puheluita voidaan hoitaa pöytä PC:llä, kannettavalla tietokoneella, IP -puhelimella, WLAN puhelimella,

kämmenkoneella tai perinteisellä analogisella puhelimella käyttäen
ATA -sovitinta.
(Hiironniemi O. 1999)

6.4 VoIP puhelun heikkoudet

Jotta pystytään toteuttamaan internet-puheluja on hankittava laitteet jotka mahdollistavat tarvittavan tarpeeksi nopea tiedonsiirron, jotta keskustelu olisi mahdollista. VoIP –siirtoa varten laitevaatimuksia on esimerkiksi että käytettävä tietokone on riittävän nopea sekä kaksisuuntaiseen liikenteeseen sopiva ja sisältää siirtoa nopeuttavan äänikortin. Koska data lähetetään paketeissa, nopean siirron lisäksi pakettien saapuminen perille täytyy tapahtua oikeassa järjestyksessä tai sitten olla järjestettävissä. Jotta VOIP puhelu olisi ymmärrettävää, niin lähetyksestä ei saa hukkua lähetettyjä paketteja matkalla Tämä osa-alue ei aina ole kaikissa tapauksissa kunnossa, johtuen juuri verkon suuresta kuormituksesta, jolloin lähetettyjä paketteja saattaa tippua pois. Koska puhelun pitää olla reaaliaikainen, niin pakettien uudelleen lähetys ei ole tarkoituksenmukaista. Tästä saattaa muodostua ongelma VOIP puheluissa, koska IP –verkoissa tiedon siirto perustuu suurelta osin pakettien uudelleen lähetykseen. (Heinonen M. 2000)

6.5 TEKNIIKAT JA STANDARDIT

Tämän kappaleen tarkoitus on tarkastella VOIP tekniikkaan liittyvää tekniikkaa ja standardeja

6.5.1 Merkinanto

Merkinanto tekniikka jolla puhelu saadaan muodostettua, hallittua ja purettua. Päätepisteillä joiden välillä yhteyttä pidetään täytyy olla osoitteet joihin voidaan muodostaa yhteys. Aluksi käsitellään kiinteän puhelinverkon merkinantoa ja tämän jälkeen vastaavaa VOIP puheluiden puolella. Tämän jälkeen vielä vertaillaan H.323 ja SIP tekniikoita keskenään.(Liikenne- ja viestintäministeriö 2005)

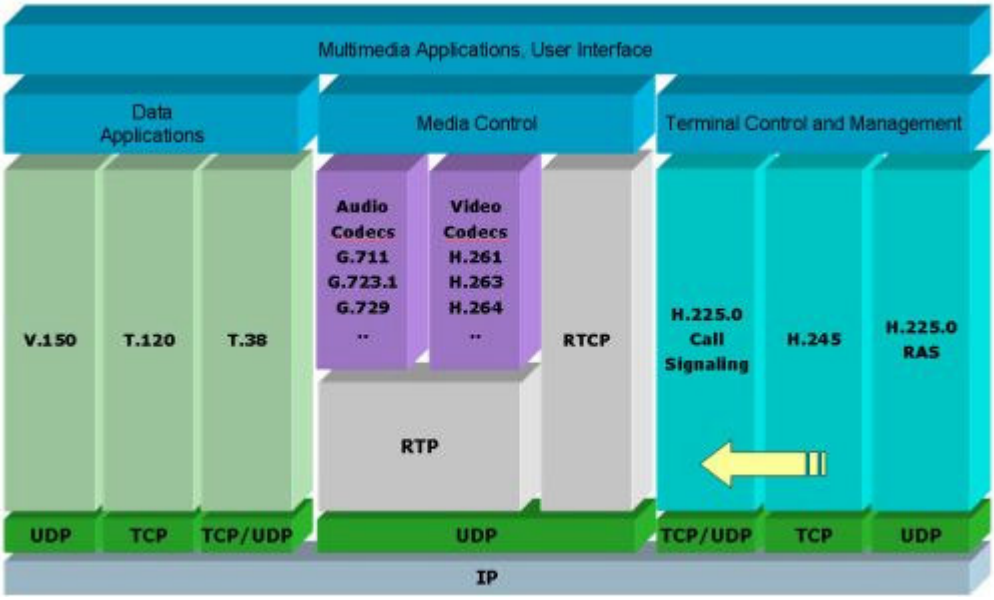
6.5.2 Merkinanto kiinteässä puhelinverkossa

Kiinteä puhelinverkko toimii siten, että kun käyttäjä nostaa puhelimen luurin asettuu puhelin samalla suuri -impedanssiseen tilaan. Tällöin puhelinkeskus huomaa käyttäjän ja samalla varaa käyttäjäliittymälle merkinantolaitteen joka lähettää käyttäjälle valintaääntä. Tämän jälkeen käyttäjä valitsee numeron joka lähtee numero kerrallaan pääkeskukselle. Jotta pääkeskus voisi kommunikoida muiden keskusten kanssa käytetään yleiskanavamerkinantoa. Puhelinverkko reitittää puhelut annetun numeron perusteella kutsuttavan liittymän päätekeskukselle ja samalla varaa koko reitin puhelulle piirikytkentäisestä puhekanavasta. Vastaanottava päätekeskus lähettää tämän jälkeen soittajan puhelinjohtoon korkeajännitteisen soittosignaalin jonka taajuus vaihtelee eri maiden kesken 15 – 68 Hz ja jännite 40 – 150 V välillä, tämän avulla siis vastaanottajan puhelinlaite alkaa soimaan. Vastaanotto päässä kuulokkeen nostaminen muuttaa puhelimen suuri -impedanssi tilaa, jolloin pääkeskus huomaa, että puheluun on vastattu. Puhelun lopetuksen keskus taas huomaa, kun puhelin luuri asetetaan takasin paikalleen ja puhelin siirtyy pieni -impedanssi tilaan
samalla keskus vapauttaa varatut resurssit yleiseen käyttöön. Kuten tässä esitetty pelkistetty kuvaus kiinteän puhelinverkon signaloinnista näyttää sen, että yksinkertaisenkin puhelun soittaminen on kohtalaisen monimutkainen kokonaisuus, jossa kuitenkin itse käyttöliittymä on toteutettu melko yksinkertaisesti. Maailmanlaajuinen automaattivalintainen puhelinverkko hallinta- ja laskutusjärjestelmineen on merkittävä saavutus, joka perustuu pääasiassa ITU-T:ssä ja sen edeltä-

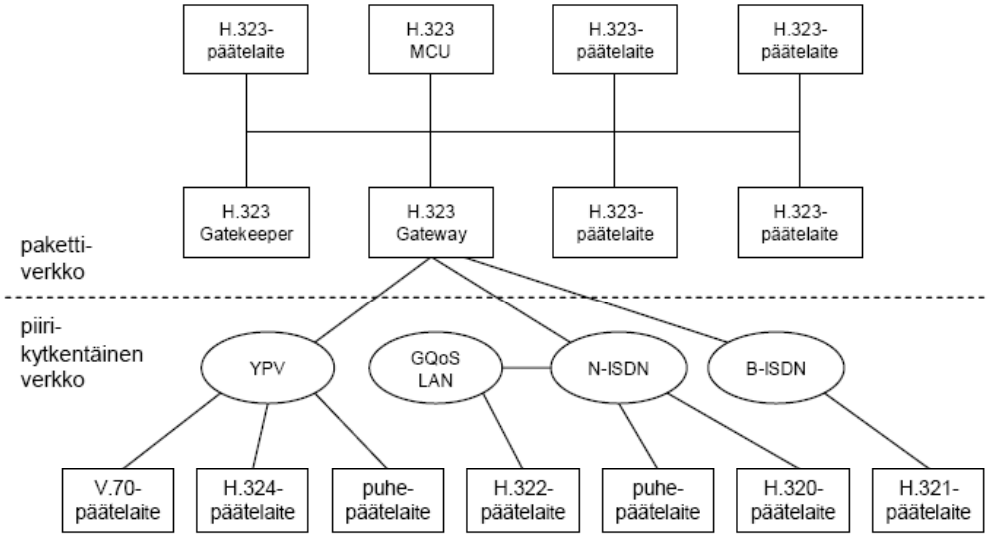
jässä CCITT:ssä suoritetulle pitkäaikaiselle kansainväliselle standardoinnille. Internet-puheluita varten tarvitaan vastaava järjestelmä, joka toimii internetissä.(Liikenne- ja viestintäministeriö 2005)

6.5.3 H.323

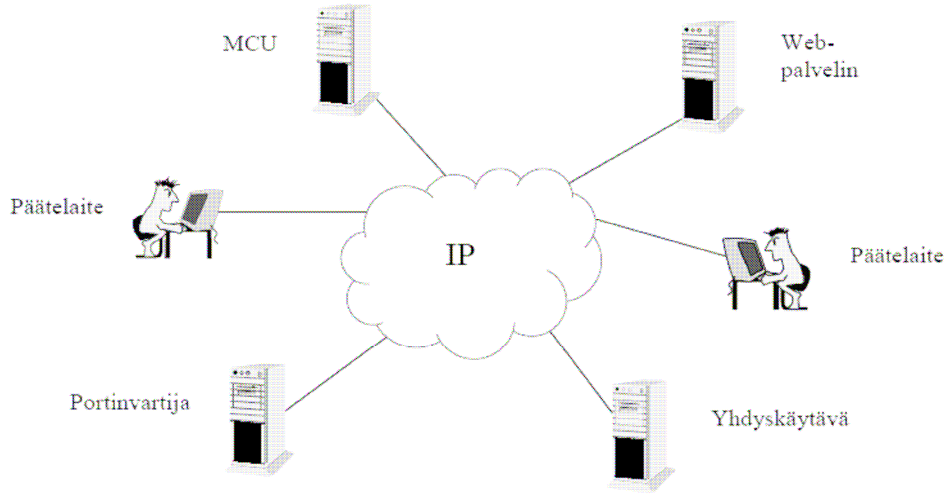
Aluksi VOIP -puheluissa oli käytössä ITU -T:n määrittelemää H.323 – merkinantoprotokollaa (kuvio 20). Joka ITU:ssa aluksi määriteltiin vain piirikytkentäisiä videoneuvotteluja varten joko yrityksen sisällä lähiverkossa tai internetissä H.320 -merkinantoprotokolla, josta kehitettiin erikseen pakettiverkkoja varten H.323-protokolla. H.323 on perinteinen ITU-T:n tuote, jonka avulla pyritään standardoimaan kokonaiset palvelut kaikkineen osineen. H.323 noudattaa yleisen puhelinverkon lähtökohtia ja määrittelee teleoperaattorityyppiset valinnat VOIP -merkinantoon. H.323 on protokolla, jolla määritetään järjestelmäarkkitehtuuri, toteutuksen suuntaviivat, puhelunmuodostus ja hallinta, siirtotie jne. H.323-protokolliin kuuluu kymmenkunta ITU-T:n suositusta. Oheinen kuvio 21 havainnollistaa H.323-järjestelmäarkkitehtuuria. Samalla siitä huomataan H.323:n ongelmia. Koska arkkitehtuuri on suunniteltu piirikytkentäisissä verkoissa toimivaan liikenteeseen ja kehitys kuitenkin on mennyt niin että liikenne siirtyy pakettipohjaiseksi. H.323 on myös protokollana raskas ja monimutkainen ja siksipä se muistuttaa enemmän perinteistä televerkkoa kuin internetiä. Kuviossa 22 esitetty VOIP verkko.



KUVIO 20 H.323 Protokollapino



KUVIO 21 H.323 Järjestelmä arkkitehtuuri



KUVIO 22 H.323-standardin mukainen VOIP verkko

IP Päätelaite

Päätelaite (Terminal) on verkon päätepiste, joka tarjoaa reaaliaikaisen, kaksisuuntaisen liikennöinnin toiseen päätelaitteeseen, yhdyskäytävään tai MCU:n. Päätelaitteen tulee tukea äänen välitystä, tarvittaessa myös kuvan ja datan välitystä.

Yhdyskäytävä

Yhdyskäytävä (Gateway) on valinnainen H.323-verkon elementti. Yhdyskäytävän tarjoama tärkein palvelu on olla rajapintana H.323-päätelaitteiden ja muiden päätelaitetyyppien välillä. Lisäksi yhdyskäytävä voi muuntaa eri audio- ja video-koodekkeja sekä muodostaa yhteyden IP-verkon ja kytkentäisen verkon välille.

Portinvartija

Portinvartija (Gatekeeper) on tärkein H.323 verkon elementti. Se ohjaa verkon puheluita sekä huolehtii rekisteröityjen päätelaitteiden hallinnasta. Portinvartija on eräänlainen verkon virtuaalinen kytkin.

MCU

MCU (Multipoint Control Unit) tukee konferenssiyhteyksiä kolmen tai useamman päätelaitteen välillä.

Web-palvelin

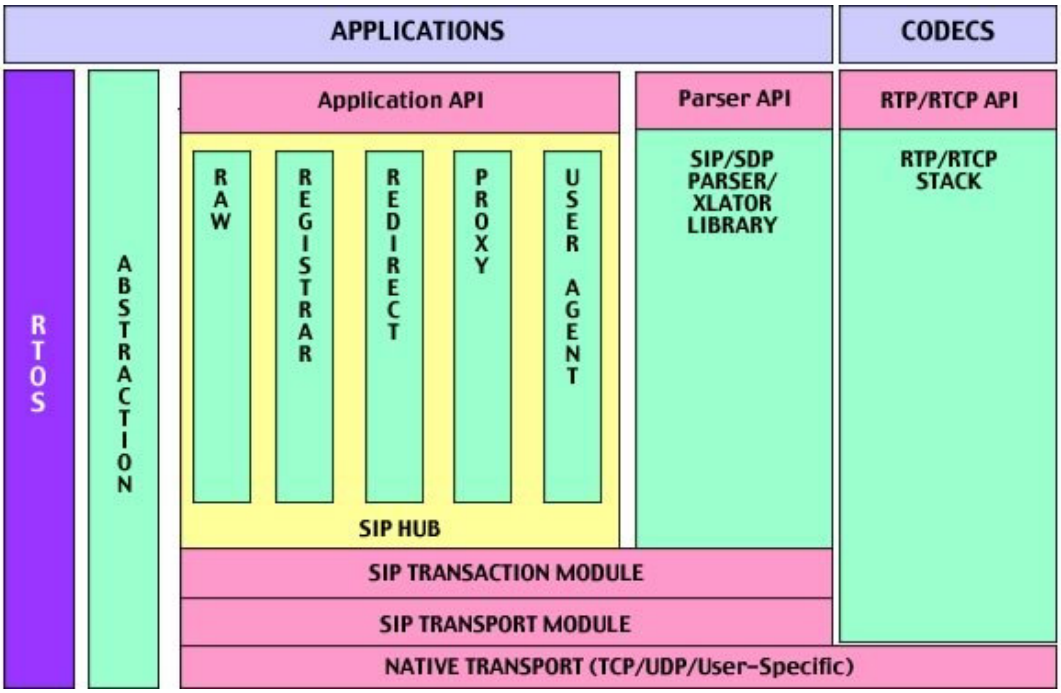
Web-palvelinta ei vaadita standardin mukaisessa kokoonpanossa. Tätä kannattaa kuitenkin ylläpitää informatiivisiin tarkoituksiin. (Väänänen K. 1999)

6.5.4 SIP

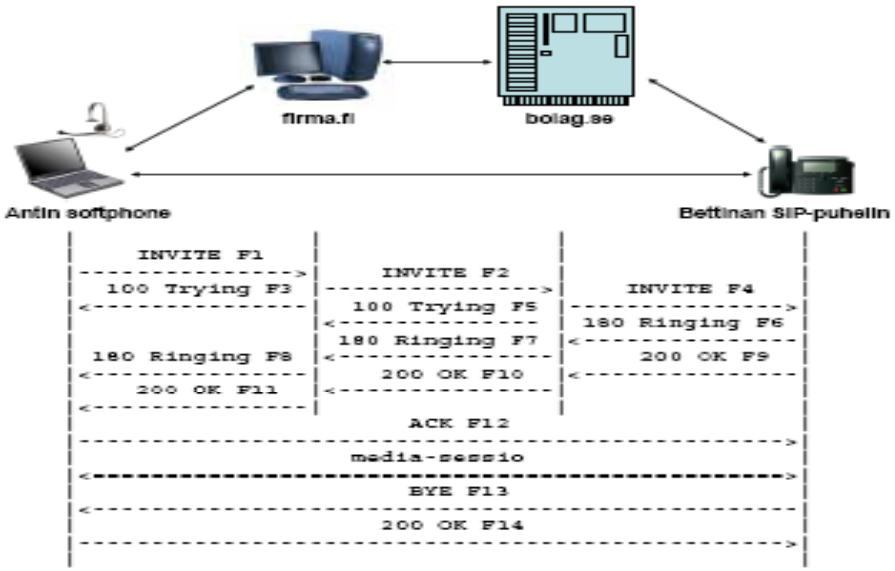
SIP (Session Initiation Protocol)(kuvio 23) on IETF:n kehittämä merkinantoprotokolla, joka kehitettiin muutama vuosi H.323 protokollan jälkeen. SIP:n kehitys on alkanut 1990-luvulla MBONEssa (Multicast Backbone) toteutettujen videoneuvottelukokeilujen yhteydessä. SIP on VoIP:n ydintekniikka, minkä vuoksi kerrotaan hieman tarkemmin siitä. SIP merkinantoprotokollaa, alettiin kehittä siksi, että se mahdollistaisi istuntojen muodostamisen, hallinnan ja purkamisen perustuen yksinkertaisiin tekstipohjaisiin sanomiin.
H.323, ja SIP protokollat kehitettiin aluksi videoneuvotteluja varten mutta sitä alettiin pian soveltaa myös IP-puheluihin. SIP-työryhmä perustettiin IETF:ään vuonna 1999, jolloin H.323 oli kerinnyt muodostua hallitsevaksi standardiksi ensimmäisissä VoIP -ratkaisuissa. SIP levisi nopealla vauhdilla koska se muistuttu hyvin paljon perusteeltaan internet arkkitehtuuria. SIP -sanomat ovat tekstimuotoisia ja käyttävät ISO UTF-8 (ASCII Unicode) -merkistöä. Syntaksiltaan SIP muistuttaa hyvin paljon internetiä varten kehitettyä HTTP:tä.SIP toimii sovelluskerroksessa, jota käytetään multimediaistuntojen muodostamiseen, hallintaan ja purkuun IP-verkoissa. SIP:n protokollalla muodostetaan joko kahden tai sitten monenkeskisiä video/puhelu neuvotteluistuntoja ottamatta kantaa millainen istunto on kyseessä. Kesken istunnon voidaan muokata istuntoa siten, että siihen voidaan liittää tai poistaa käyttäjiä, ääntä tai videota. Käyttäjiä voidaan SIP protokollassa tavoittaa SIP osoitteen kautta riippumatta siitä missä heidän sijaintinsa on.
SIP protokolla tukee viittä eri multimediaviestinnän näkökohtaa:
Käyttäjän sijainti ja kommunikaatioon kulloinkin käytettävän laitteen (käyttäjäagentti, user agent) löytäminen verkosta.Käyttäjän tila, käyttäjän mahdollisuus tai halu ottaa vastaan puheluita tms. Käyttäjän vaatimukset – mitä medioita, parametreja yms. käyttäjän tämänhetkinen päätelaite ja verkkoliitäntä mahdollistavat.

Istunnon luominen – sekä istunnossa käytettävien parametrien sopiminen osapuolten välillä. Istunnon hallinta – istunnon siirto, purku ja modifiointi. SIP protokollaan on lisätty myös mahdollisuus lyhyitten sanomien välittämiseen eri käyttäjien välillä merkinantoprotokollan sisällä ilman erillistä mediaa. Internetissä verkossa liikenne siirtyy IP-paketteina ja multimediajärjestelmät perustuvat yleensä yhteydettömään UDP (User Datagram Protocol*)* -protokollaan. Lisäksi SIP:n kanssa käytetään VoIP-palvelun toteuttamiseen mm. seuraavia protokollia:
RTP on UDP:n päällä toimiva protokolla reaaliaikaisen tiedonsiirron ja palvelutason seurantaan. RTP lisää UDPsanomiin järjestysnumerot ja aikaleimat.
SDP (Session Description Protocol) on protokolla, jolla voidaan kuvata Internetin multimediaesityksiä tai -istuntoja, kuten Internet-puheluja, elokuvien suoratoistoa tai puhelinneuvotteluja. SDP suunniteltiin alun perin MBONEssa välitettävien reaaliaikaisten multimediaesitysten kuvaamiseen. SDP-kuvauksessa luetellaan esityksen ajankohta, esitykseen kuuluvat mediat ja niiden tarvitsemat parametrit (koodekit, siirtoprotokollat, porttinumerot). SDP-kuvauksia voidaan välittää HTTP:n, SAPin, RTSP:n tai SIPin avulla. SIPpiä varten on määritelty lisäksi neuvotteluprotokolla (Offer/Answer Model with SDP), jolla voidaan muodostaa uusia multimediaistuntoja tai muokata olemassa olevia.
MEGACO (Media Gateway Control Protocol) on protokolla joka on luotu ohjaamaan yhdyskäytävät yleiseen puhelinverkkoon. SIP:n toiminta perustuu käyttäjäagentteihin sekä valtakirja-agentteihin (”SIP proxy”), jotka edustavat käyttäjiä internet verkossa. Käyttäjällä saattaa käytettävä VOIP päätelaite vaihtua, tai sijainti saattaa olla palomuurin takana, sekä välillä on poissa päältä tai irti verkosta. SIP proxy on siis palvelin, johon käyttäjän laite rekisteröityy ja jonka kautta on myös tavoitettavissa. Tässä mielessä SIP proxy palvelin muistuttaa sähköpostipalvelinta, joka on tavoitettavissa internetistä on aina päällä sekä jonka kautta käyttäjän sähköpostiagentti käy noutamassa / lähettämässä postin. Puhelu tapahtuu SIP protokollassa siten, että käyttäjän soittaessa käyttäjäagentti lähettää SIP:n ”INVITE”-sanoman käyttäjän omalle SIP-proxylle, tämä palvelin välittää viestin edelleen vastaanottajan SIP-proxylle. Vastaanottajan SIP-proxy tutkii mistä IP-osoitteesta ja UDP-portista vastaanottaja on rekisteröitynyt ja välittää sanoman edelleen sinne. Puhelun aloittajalle tulee takaisin niin kutsuttu ”OK” –sanoma takaisin SIP –proxyn kautta ja tätä kautta soittaja saa IP –osoitteen ja portti numeron jota kautta

yhteys toimii. Tämän jälkeen voidaan lähettää ”ACK”-sanoman suoraan soiton vastaanottajalle eikä varsinaisen puhelun tai sen päättämiseen liittyvän signaloinnin tarvitse kulkea proxy -palvelimien kautta. Pitää kuitenkin huomioida, vaikka SIP on merkkipohjainen protokolla, jota ihminen pystyy melko helposti lukemaan, niin silti käyttäjät eivät näe SIP -sanomia vaan pelkästään laitteensa tai ohjelmistonsa käyttöliittymän. Kuvio 24 yksityiskohtien ymmärtäminen ei ole tavalliselle käyttäjälle tarpeellista. Tärkeintä kuitenkin kuviossa on, että VoIP -puhelun muodostus tapahtuu kummankin osapuolen SIP –proxy palvelimien kautta kun taas varsinainen puheliikenne ja myös puhelun lopettaminen, voi tapahtua suoraan osapuolten kesken.



KUVIO 23 SIP-protokollapino



Kuva 7: Esimerkki SIP-puhelun muodostuksesta, käytöstä ja purusta sekä Antin lähettämä "INVITE"-sanoma (RFC 3261:tä mukaellen).

KUVIO 24
(Liikenne- ja viestintävirasto 2005)

6.5.5 SIP vs. H.323

Koska H.323 että SIP protokollia voidaan kumpaakin käyttää sekä videoneuvotteluissa sekä myös IP –puheluissa johtuen osoitteen ollessa suhteellisen samanmuotoinen kuin sähköpostissa. Aikaisemmin julkaistulla H.323:lla on edelleen oma käyttäjäkuntansa johtuen siitä, että sitä pidetään telepiireissä muistuttavan enemmän perinteistä televerkko ajattelua kuin SIP. Viime vuosien aikoina SIP on yleistynyt nopeasti ja se syrjäyttää vähitellen kokonaan H.323:n. SIP tarjoaa helpon yhdentymisen IP-puheen ja muiden internetin sovellusten välillä SIP protokolla on syrjäyttämässä H.323:n mutta H.323 tullee kuitenkin säilymään vielä pitkään joidenkin operaattoreiden sekä varhaisten VoIPkäyttäjien järjestelmissä. Useat tuotteet tukevat molempia standardeja joten

näiden kahden protokollan välille on helposti järjestettävissä yhdyskäytävät. Uudet VoIP-palvelut kannattaa joka tapauksessa kehittää SIP:n varaan
(Liikenne- ja viestintävirasto 2005)

7. KÄYTÄNNÖN TOTEUTUS

7.1 Johdanto

Puhelinjärjestelmä uudistuksessa toteutettiin VOIP ratkaisu Halton Oy:n nimiselle yritykselle. Samalla, kun VOIP ratkaisu otettiin käyttöön haluttiin samalla tutkia mahdollisuutta ottaa käyttöön uutta tekniikka jota käytetään GSM tekniikassa. Tämä uusi tekniikka on sitä, että kannettavalla mobiili laitteella päästään uutta tekniikkaa käyttäen WLAN verkkoon ja sitä kautta voisi päästä yrityksen omassa WLAN verkossa yhteys VOIP puhelu järjestelmään. Käytännön toteutuksena siis toteutettiin nyt vain VOIP ratkaisu, mutta kyseistä uutta tekniikkaa tullaan ottamaan käyttöön, kun laitteet yleistyvät ja toimintavarmuus paranee.

7.2 Yleistä

Halton Oy käytti tähän saakka normaalia puhelinkeskus ratkaisua jossa joka toimipisteellä oli oma puhelin keskus johon oli määritelty kyseisen toimipisteen puhelinnumerot. Aina kun tarvittiin puhelimen siirtoa tai uutta numero oli kutsuttava paikalle puhelinlaitoksen henkilö joka suoritte kyseisen operaation. Tämä oli hyvin hidasta ja kallista toimenpidettä. Nyt kun siirryttiin VOIP puhelin järjestelmään nämä kyseiset ongelmat on nyt saatu pois. Tätä VOIP tekniikkaa tullaan aluksi käyttämään vain täällä suomessa, mutta tarkoitus on laajentaa aluksi pohjoismaan konttorit mukaan ja sen jälkeen muut maailmalla olevat konttorit ja tehtaat.

8.0 Toteutus

Tätä VOIP ratkaisua aloitettiin toteuttamaan syksyllä 2005 ja toteutus saatiin valmiiksi 16.2.2006 Liite 2. Toteutuksessa oli mukana vahvasti Telia Sonera ja Cygate Oy. Cisco CallManagerin konfiguraatiot hoiti Cygate ja opastuksen Halton Oy:n adminstration tunnuksille omaaville. Administraation tunnuksen omaavat pääsevät nyt käyttöönoton jälkeen sitten lisäämään ja poistamaan / muuttamaan tietoja Callmanageriin. Puhelinvaihde toiminta siirtyi Soneran hallintaan ja tätä varten laadittiin kaikista puhelimen käyttäjistä Merex taulukkoa (Liite 3) ja puhelu ohjauksia varten CID taulukko (Liite 4) . Merex taulukon täyttäminen tapahtui tammikuun aikana ja siihen tuli tietoja puhelimen käyttäjästä, uudesta numerosta, vanha numero joka ohjataan 3 kuukauden ajan uuteen numeroon, työnimike, paikkakunta, jne. Tätä taulukkoa käyttävät vaihteenhoitopalvelu hyväksi puhelun yhdistämisessä Halton oy:n käyttöön varattiin numerot 020 792 xxxx numeroavaruudesta. Käyttäjiä VOIP järjestelmässä luokiteltiin seuraavasti :

Käyttäjäluokka 1.
Nämä käyttäjät ovat sellaisia joilla on käytössä vain Ciscon pöytäpuhelin ja heidän puhelut yhdistetään siihen.

Käyttäjäluokka 2
Nämä käyttäjät ovat sellaisia jotka käyttävät vain mobiili puhelinta.

Käyttäjäluokka 3
Nämä käyttäjät ovat sellaisia jotka käyttävät sekä mobiililaiteetta sekä pöytäpuhelinta.

Käyttäjäluokka 4
Nämä käyttäjät ovat sellaisia joilla on käytössä Cisco IP Communicator.
CID taulukolla joka täytettiin, niin suoritettiin puheluiden ohjaus siten että käyttäjäluokka 1 puhelut yhdistyvät suoraan pöytäpuhelimeen ja jos ei vastata tietyssä ajassa kääntyy puhelu keskukseen jossa nähdään tiedoista onko henkilö

paikalla. Käyttäjäluokan 2 puhelut yhdistyvät soitettaessa 020 792 xxxx siten, että tämän numeron taakse on määritelty mobiililaitteen numero johon puhelu sitten reitittyy. Käyttäjäluokka 3 puhelut yhdistyvät siten että ensin soi pöytäpuhelin ja sen jälkeen puhelu siirtyy mobiililaitteeseen jos puheluun ei ole vastattu. Ohjaus näissä tapauksissa tehtiin siten, että yritysnumeron taakse linkitettiin mobiili puhelimen numero ja siirto siihen 20 sekunnin kuluttua jos pöytäpuhelimeen ei vastata. Käyttäjäluokka 4 puhelut on järjestetty taas siten, että henkilöt joilla on sekä IP Communicator sekä mobiililaite soi puhelun tullessa molemmat yhtä aikaa ja käyttäjä voi valita kumpaan vastaa.

8.1 Toteutuspaikat

Tällä kertaa paikoiksi jotka tulivat nyt aluksi mukaan tähän VOIP ratkaisuun valittiin Halton Oy:n toimipisteistä Kausala johon sijoitettiin CallManager josta ohjataan puhelut muihin toimipisteisiin. Kausalan toimipisteeseen tuli pöytäpuhelimia 12 kappaletta, mobiilikäyttäjiä on 41 kappaletta ja IP Communicattoreita 18 kappaletta ja ATA sovittimia 7 kappaletta. Seuraava toimipiste oli Lahti johon sijoitettiin pöytäpuhelimia 15 kappaletta, mobiilikäyttäjiä 30 kappaletta ja IP Communicattoreita 7 kappaletta sekä ATA sovittimia 6 kappaletta. Vantaan myyntikonttori johon pöytäpuhelimia sijoitettiin 4 kappaletta sekä mobiilikäyttäjiä 15 kappaletta ja IP Communicaattoreita 4 kapaletta sekä ATA sovittimia 5 kappaletta. Viimeinen toimipiste Suomessa oli Oulu johon sijoitettiin 1 pöytäpuhelinmalli ja 1 ATA -sovitin. Näiden toimipisteiden lisäksi asennettiin kaksi kappaletta IP Communicator versioita henkilöille jotka ovat Halton Oy Marine Lahti palveluksessa, mutta tällä hetkellä ulkomailla töissä. Toinen näistä on käytössä Ranskassa ja toinen Kiinassa. Kuvio VOIP verkosta (Liite 2). Kaiken tämän jälkeen, kun VOIP verkko oli saatu toimivaksi tehtiin käyttäjiä varten käyttöönottoa varten koulutusmateriaali ja opastus järjestettiin kahdessa osiossa siten että pöytäpuhelin käyttäjille oma koulutus ja IP –communicator käyttäjille oma.

8.2 Käytettäviä laitteitta

Laitteet jotka otettiin käyttöön VOIP ratkaisua toteutettaessa ovat Ciscon laitteita. Valitut laitteet olivat seuraavanlaisia :
Cisco Callmanager 4.1(3)
Pöytäpuhelimet 7912G
Cisco IP Communicator
ATA sovittimet

8.3 Laitteiden tietoja

Tässä osassa esitellään toteutuksessa käytettyjä laitteita.

8.3.1 Cisco Callmanager 4.1(3)

Cisco IP Communications -viestintäratkaisu on kattava järjestelmä, joka sisältää suorituskykyiset yritystason ratkaisut IP-puhelinliikenteeseen, yhdistettyyn viestintään, IP-pohjaisiin video/puhelinneuvotteluihin ja asiakasyhteyksien hoitamiseen. Niiden avulla organisaatio voi tehostaa toimintaansa, parantaa tuottavuuttaan ja lisätä asiakastyytyväisyyttä saavuttaen näin selviä etuja toiminnalleen. Cisco CallManager on olennainen osa Cisco IP Communications -viestintäjärjestelmää. Se on Ciscon yrityskäyttöön kehitetyn IP-puhelinratkaisun puhelujen prosessoinnista vastaava ohjelmistokokonaisuus ja perustuu Ciscon AVVID-arkkitehtuuriin (Architecture for Voice, Videoand Data).
Cisco CallManager -ohjelmisto laajentaa yritysten puhelinjärjestelmien ominaisuudet pakettimuotoisen puhelinliikenteen verkkolaitteisiin kuten IP-puhelimiin, mediaprosessointilaitteisiin, VoIP-yhdyskäytäviin ja multimedia-sovelluksiin. Data-, puhe- ja videosovellukset kuten yhdistetty viestintä (unified

messaging), multimedianeuvottelut, ohjelmistojen yhteiskäyttöä hyödyntävät yhteyskeskukset ja vuorovaikutteiset multimediapohjaiset vastauspalvelujärjestelmät toimivat yhdessä IP-puhelinratkaisun kanssa Cisco CallManagerin avointen puhelinsovellusliittymien (TAPI) kautta. Cisco CallManager asennetaan Cisco Media Convergence Server -palvelimiin ja valikoituihin kolmansien osapuolten palvelimiin. Cisco CallManager -ohjelmistotoimitus sisältää useita integroituja puhesovelluksia ja apuohjelmia, kuten ohjelmistopohjaiset Cisco CallManager Attendant Console ja Bulk Administration Tool (BAT), CDR Analysis and Reporting (CAR), Admin Serviceability Tool (AST), puhelunvälittäjän perusominaisuudet tarjoava Cisco CallManager AutoAttendant (CM-AA), Tool for Auto-Registered Phones Support (TAPS)ja IP Manager Assistant (IPMA) -sovellusohjelmisto.

8.3.2 Keskeiset ominaisuudet ja edut

Cisco CallManager versio 4.1 on skaalautuva, hajautettava ja korkean käytettävyyden tarjoava, yrityskäyttöön kehitetty IP-pohjainen puhelujen prosessointiratkaisu. CallManager -palvelimet muodostavat yhtenä kokonaisuutena hallittavan klusterin. Ciscon AVVID tarjoaa markkinoiden ainoana arkkitehtuurina useiden puhelujen prosessointipalvelinten kokoamisen klusteriksi. Cisco CallManager -klusteri skaalautuu tukemaan yhdestä aina 30 000 IP-puhelinta ja tarjoaa kuormantasauksen ja puhelujen prosessointipalvelujen vikasietoisuuden. Järjestelmän kapasiteetti voidaan klustereita yhdistämällä kasvattaa miljoonaan käyttäjään yli sadassa pisteessä. Klusteri kokoaa yhteen useiden hajautettujen Cisco CallManagerien suorituskyvyn ja skaalautuu palvelemaan laajasti koko järjestelmän puhelimia, yhdyskäytäviä ja sovelluksia ja niiden tavoitettavuutta. Puhelujen prosessointipalvelinten kolminkertaistettu vikasietoisuus parantaa järjestelmän kokonaiskäytettävyyttä. Hajautetun arkkitehtuurin etuina ovat järjestelmän parempi käytettävyys, kuormantasaus ja skaalautuvuus. Call Admission Control (CAC) -puhelunhallinta takaa, että puheen palvelunlaatu (QoS) säilyy kapasiteetiltaan rajoitetuissa IP-verkkoyhteyksissä ja ohjaa puhelut automaattisesti vaihtoehtoisille yleisen puhelinverkon reiteille silloin, kun IP-

verkon kaistanleveys ei ole käytettävissä. Selainpohjaisen tietokantakäyttöliittymän avulla järjestelmä ja laitteet voidaan konfiguroida etäyhteyden kautta. Käyttäjiä ja järjestelmänvalvojia varten ohjelmistossa on HTML-pohjainen opastustoiminto. Version 4.1 parannettuihin ominaisuuksiin kuuluvat entistä parempi turvallisuus, yhteentoimivuus, skaalautuvuus, toiminnallisuus, hallittavuus ja tuottavuus sekä parannetut videopuheluominaisuudet. Cisco CallManager 4.1 sisältää monia turvaominaisuuksia jotka mahdollistavat Cisco CallManagerin palvelimien ja IP-puhelimien identifioinnin sekä liikenteen salauksen. Laitteet, jotka voivat osallistua salattuun liikennöintiin ovat Cisco IP 7940G IP-puhelin, Cisco IP 7960G IP-puhelin, Cisco IP 7970G IP-puhelin ja MGCP (Media Gateway Control Protocol) -yhdyskäytävät. Cisco CallManager 4.1 hallintaan käytetään tietoturvallista HTTPS (HTTP over SSL) -protokollaa. Parannukset Cisco CallManager 4.1 Q.SIG -signaloinnissa laajentavat ominaisuuksia yhdistettäessä Cisco CallManager Q.SIG -signalointia tukevien ratkaisujen kanssa. Laajennukset Cisco CallManager API -rajapintoihin (AXL, JTAPI, TSP) tarjoavat asiakkaille ja kolmannen osapuolen toimittajille paremmat mahdollisuudet kehittää parempia sovelluksia.

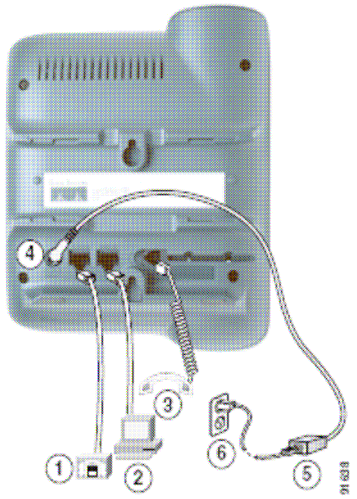
8.3.3 Pöytäpuhelimet Cisco IP Phone 7912G

Cisco IP Phone 7912G IP-puhelimessa (kuvio 25) on monipuoliset ominaisuudet. 2 kappaletta 10/100Base-T Ethernet-kytkinportti Iso nestekidenäyttö Kaiutin Mitat 20,3x17,67x15. Tämä puhelin malli valittiin , koska sen kytkimellä varustettua ja siihen saadaan liitettyä 2 ethernet kaapeli (kuvio 26). Tämän ominaisuuden avulla saadaan kytkentä liitettyä tietokoneen kautta ja ylimääräisiä ATK pistokkeita ei tarvitse laittaa paikkoihin joissa on vain yksi paikka. Tämä laitteisto tukee äänen siirtoa dataverkossa. Helppokäyttöinen selkeä näyttö. Käyttäjä voi tehdä puhelinkohtaisia muutoksia käyttäjälle annettavalla https://10.1.1.7/ccmuser/logon.asp (kuvio 27) osoitteella. Käyttäjille jaetaan käyttäjätunnukset ja tarvittava salasana. Täällä annetussa osoitteessa käyttäjä pääsee valikoimaan soittoääniä, käytätettävän kielen, pikavalintoja ja soitonsiirtoja.

Painikkeet ja laitteisto

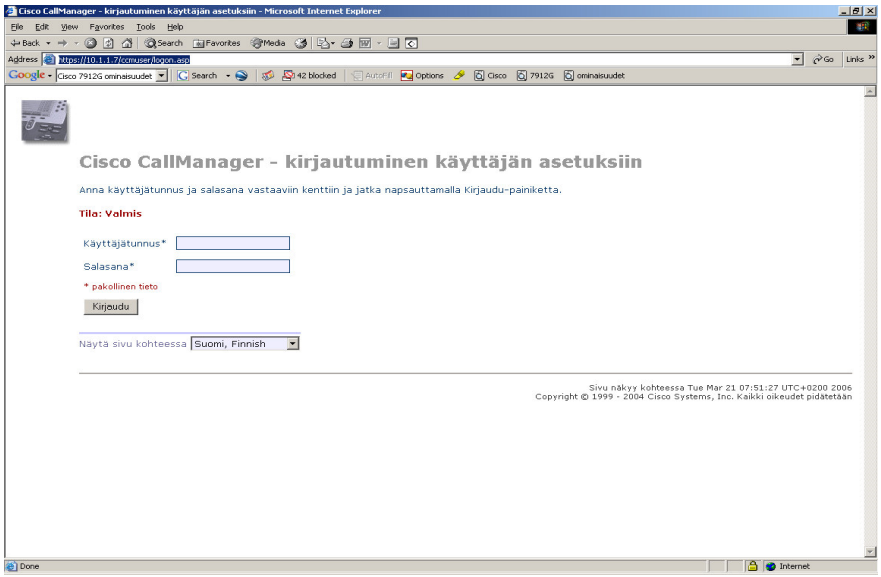
1	Nestekidenäyttö	Näyttää esimerkiksi kellonajan, päivämäärän, käyttäjän puhelinnumeron, soittajan tunnuksen, puhelutilan ja toimintopainikkeiden välilehdet.
2	Cisco IP -puhelinsarja	Osoittaa Cisco IP -puhelimen mallin numeron.

KUVIO 25



1	Verkkoportti (10/100 SW)	2	Yhteysportti (10/100 PC)
3	Kuulokkeen portti	4	Tasavirtasovittimen portti (DC48V)
5	Ciscon toimittama virtalähde (valinnainen)	6	Virtajohto

KUVIO 26



KUVIO 27

8.3.4 Cisco IP Communicator

Tämä sovellus on PC pohjainen puhelinsovellus (kuvio 28) . Tämä on käyttökelpoinen sovellus kaikille kannettavan tietokoneenkäyttäjille. Näitä sovelluksia asennettiin Halton Oy työntekijöille jotka joutuvat työnsä ohessa matkustamaan paljon ja yhteyttä yrityksen verkkoon he ottavat VPN tunnelin kautta. Yksi sovellus näistä asennettiin Halton Marine Lahden työntekijälle joka on työkomennuksella Ranskan tehtaalla. Yhtä sovellusta käyttää Kiinan tehtaan johtaja joka on yhteydessä Suomeen päin usein. IP Communicatorin käyttäjille hommattiin tämän lisäksi Plantronics Headset systeemit joilla hoidetaan puhuminen ja kuuntelu.

KUVIO 28 Cisco IP Communicator

8.3.5 ATA186-I2-A sovitin

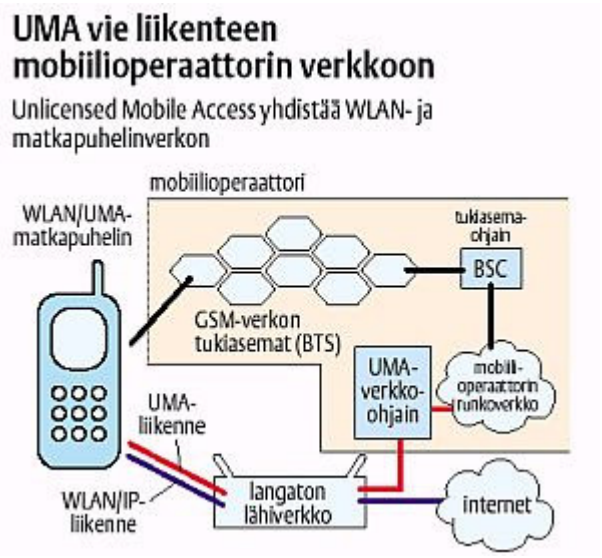
ATA (Analog Telephone Adapter)- sovittimia (Kuvio29) asennettiin kaikkiin paikkoihin joihin tarvittiin analogisen yhteyden muuttamista VOIP yhteen sopivaksi. Tämmöiset kohteet olivat kaikki FAX liittymät, Mondel rahastuskoneet ja valvonta yhteydet.

KUVIO 29 ATA-sovitin

8.4 Tulevaisuus

Tulevaisuudessa on tarkoitus liittää nyt ainakin aluksi VOIP ratkaisuun kaikki pohjoismaissa olevat yrityksen toimipisteet, eli Ruotsi, Norja ja Tanska.
Ennen kuin tähän ryhdytään kokonaisuudessa, niin kesän alussa ensin sijoitetaan jokaiseen toimipisteeseen mukaan lukien myös Ranska ja Puola niin kutsutut kuumanlinjan puhelimet, eli 1 pöytäpuhelin joka toimipisteeseen josta keskitetysti voidaan hoitaa puhelu yrityksen toimipisteiden välillä ja tätä kautta saadaan puhelukustannuksissa säästöjä. Kotimaasta mukaan liitetään vielä Orimattilan toimipiste kesän–syksyn 2006 aikana. Tämän VOIP ratkaisun ohella oli minulla tutkittavana GSM laitteita jotka voisi liittää yrityksen WLAN verkon kautta. Tämä UMA(Unlicenced mobile access) tekniikka on se jolla GSM puhelin saadaan liitettyä WLAN-verkkoon(kuvio 30) ja sitä kautta VOIP puhelujärjestelmään. UMA tekniikka on 3GPP:n standardi. Operaattorit ja laitevalmistajat aloittivat UMAN:n standardoinnin vuonna 2004.Standardin avulla GSM- ja GPRS -palvelujen liityntäverkossa voidaan käyttää lisensoimattomia taajuuksia 802.11 eli WLAN -standardien lisäksi UMA toimii myös bluetooth –yhteydellä. UMA -standardi kuvaa UMA -verkko-ohjaimen (uma network controller) ja GSM/GPRS -liikenteen ja -signaloinnin siirron IP –liikenteenä. Nokian ja Motorolan lisäksi UMA -kännyköitä on tulossa muun muassa LG:lta, BenQ:lta ja Samsugilta. Verkkolaitevalmistajista standardoinnissa mukana ovat olleet mm.

Kinoto Wireless, Ericsson, Nokia, Nortel Networks. Asiaa tutkiessani huomasin, että tästä on vielä huomattavan vähän tietoa jaossa, mutta löysin kuitenkin laitevalmistajia joilta löytyy nyt jo tuotteita palvelun toteutukseen. Seuraavana luettelo puhelimista joita nyt olevilla markkinoilla olevat toimittajat tarjoavat käyttöön laitteita joilla saadaan VOIP puheluita aikaiseksi.



KUVIO 30 UMA

8.4.1 Sony Ericsson P990i

Tämä on malli jolla käytöön saadaan on kaikkialla Internet, push-sähköposti, jonka avulla saadaan sähköpostit suoraan puhelimeen sekä videopuheluominaisuus ja viestitoiminnot tehokasta viestintää varten. Saadaan hyödynnettyä nopeita WLAN verkkoja. Puhelin käyttää Symbian OS 9.1 joka on käytetyimmän avoimen älypuhelinkäyttöjärjestelmän uusin versio, jota käytetään P990i:ssä. Lisää puhelimeesi innovatiivisia sovelluksia ja tekee puhelimestasi tehokas liiketoiminnan työkalu (Kuvio 31).

KUVIO 31 Sony Ericsson P990i

8.4.2 Nokia 6136

Nokia 6136 -puhelin mahdollistaa saumattoman siirtymisen langattomien lähiverkkojen ja matkapuhelinverkon välillä. Tämä puhelin hyödyntää UMA-teknologiaa jolla voidaan yhdistää kaksi laajalti käytettyä langatonta teknologiaa. Tämä tekee mahdolliseksi puheen ja datan saumattoman siirtymisen GSM-matkapuhelinverkkojen ja langattomien lähiverkkojen (WLAN) välillä. UMA (Unlicensed Mobile Access)-teknologian avulla eri operaattorit pystyvät tarjoamaan puhe- ja datapalveluja asiakkailleen WLAN -verkkojen kautta, millä saadaan lisättyä huomattavasti mobiilipalvelujen saatavuutta ja vähentää verkkojen laajentamiseen liittyviä kustannuksia. Käyttäjille UMA -teknologia mahdollistaa puhelut vaivattomasti internetin kautta WLAN -yhteyden välityksellä. (KUVIO 32)

KUVIO 32 Nokia 6136

8.4.3 HP iPAQ h6340 Pocket PC (FA203A)

Tämä on laite jolla saadaan myös GSM/GPRS ominaisuudet. Tähän on rakennettu sisäinen WLAN 802.11b, sisäinen langaton Bluetooth®-tekniikka; IrDA (SID-tuki). Tämä on kämmentietokone johon edellä mainitut ominaisuudet on lisätty. Käyttöjärjestelmänä tässä laitteessa on Microsoft Windows Mobile 2003 Software. (KUVIO 33)

KUVIO 33 HP iPAQ h6340 Pocket PC (FA203A)

8.4.4 Intelin Universal Communicator

Intel demosi jo vuonna 2003 puhelimen joka hyödyntää WLAN-verkkojen ja GSM-verkkojen yhteistoimintaa ja roaming -toimintoa. Yritys on kehittänyt Universal Communicator -kännykän, joka toimii sekä langattomassa 801.11b-lähiverkossa että GSM/GPRS -matkapuhelinverkossa(KUVIO 34).

KUVIO 34 Intelin Universal Communicator

6. YHTEENVETO

Johtopäätökset tästä projektista ovat seuraavanlaisia. Ratkaisun toteutus aloitettiin syksyllä 2005 ja toteutettiin Suomessa olevien toimipisteiden osalta käyttöön helmikuu 2006 loppuun mennessä. Työnä tämän toteutus oli suhteellisen helppo, sillä toimipisteisiin uusittiin tietoliikenne verkot vuoden 2004 aikana, joten kapasiteetti sillä osin oli kunnossa ja riittävä. Eri taulukkojen täyttäminen oli haastava ja aikaa vievä osuus työssä, sillä näiden annettujen tietojen perusteella lähdettiin liikkeelle aloituspäivänä. Jos ja kun kaikki näistä tiedoista ei ollut kuitenkaan aivan kunnossa oli aloituspäivänä puhelut vielä hieman hukassa ja näiden ohjauksien korjaamiseen kului ylimääräistä aikaa. Kaikki erheelliset tiedot jotka oli päässyt tietoihin jotka syötettiin järjestelmään saatiin korjattua hyvin nopeasti ja VOIP-puhelut toimivat nyt erinomaisesti. Mobiilaitteita jotka hyödyntävät WLAN verkkoa ei otettu vielä käyttöön, koska niiden käyttökokemukset ja luotettavuus ei ole viellä tarpeeksi tiedossa. WLAN verkkoa kokeiltiin muutamalla tukiasemalla Kausalan tehtaalla tehtaan nurkkauksessa johon ei ole vedetty tietoliikenne kaapelia, mutta kokeilussa ilmeni lähellä olevasta maalaamolinjasta häiriöitä ja ei saatu ainakaan siellä tarpeeksi luotettavaa yhteyttä toimimaan. On tutkittu Lahdessa WLAN verkon toteuttamista konttori ja neuvotteluhuone tiloihin, jolloin liikkuvuus paranisi ja kannettavien tietokoneiden käytettävyys paranisi. Jos käyttöön otetaan uudet WLAN tekniikkaa käytettävät GSM puhelimet, niin niiden valinnassa tullaan päättymään Nokian malleihin. Suojaus ulkopuolisia vastaan tulisi tehdä WLAN asetuksissa. Asetuksissa asetettaisiin suodatukset päälle ja vain tietyt MAC ositteet päästetään lävitse WLAN verkkoon ja sitä kautta yrityksen käyttämään järjestelmään käsiksi.

LÄHTEET:

Digitoday 2004 [verkkodokumentti] [viitattu 26.02.2006].
Saatavissa: http://www.digitoday.fi/showPage.php?page_id=12&news_id=27728

EMC Database [verkkodokumentti] [viitattu 23.02.2006].
Saatavissa: www.emc-database.com

GSM Association [verkkodokumentti] [viitattu 04.02.2006].
Saatavissa: www.gsmworld.com

Vesanen A. 2005 [verkkodokumentti] [viitattu 04.01.2006].
Saatavissa:
http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/puhelin/GSM.html

Engdahl T. 2005 [verkkodokumentti] [viitattu 25.01.2006].
Saatavissa: http://users.tkk.fi/~then/matkapuhelin/gsm.html

Kiviranta M. ,Paavola M. , Pöyhönen T. , Rastas J. [verkkodokumentti] [viitattu 16.01.2006].
Saatavissa: http://www.cc.jyu.fi/~mtkivira/jtl/yhteydensalaus.html

Seppänen 2002 [verkkodokumentti] [viitattu 16.01.2006].
Saatavissa: http://trade.hamk.fi/%7Elseppane/courses/wlan/doc/Materiaali.pdf

Viestimaa.fi 2006 [verkkodokumentti] [viitattu 20.2.2006].
Saatavissa: http://www.viestimaa.fi/index.php?30

Geier 1999 [verkkodokumentti] [viitattu 12.01.2006].
Saatavissa: http://www.nwfusion.com/research/2003/0331wpa.html

Granlund 2001: 230
Granlund Kaj 2001. Langaton tiedonsiirto. 1.painos. Porvoo. Docendo Finland Oy.

Granlund 2001: 231-232
Granlund Kaj 2001. Langaton tiedonsiirto. 1.painos. Porvoo. Docendo Finland Oy.

Wikipedia 2006 [verkkodokumentti] [viitattu 15.03.2006].
Saatavissa: http://fi.wikipedia.org/wiki/802.11

Kuokka 2002: 10-12
Kuokka, Henri 2002. WLAN vyöryy verkkoihin. Mobiili-IT 10B/2002 s.10-19. Forssa: Sanoma Magazines Finland Oy.

Wikipedia 2006 [verkkodokumentti] [viitattu 20.02.2006].
Saatavissa: http://fi.wikipedia.org/wiki/802.11

Marek 2001 [Kirjoitelma] [viitattu 20.02.2006].
Marek, Sue (2001) Wireless' weakest link. *Wireless Week*, Vol. 7, Issue 43, 26–27.

Poropudas, Timo (2002) Bongarit kartoittivat 25 000 verkkoa: Kolme neljästä WLANista on suojaton. [verkkodokumentti] [viitattu 6.12.2005].
Saatavissa:
http://www.digitoday.fi/digi98fi.nsf/pub/te20021106101638_kni_70859693

Flint 2000; Langattomien lähiverkkojen tietoturva 2002 [Kirjoitelma] [viitattu 20.01.2006].
Authenticating VPNs with RADIUS. *Network Computing*,

WiFi Alliance 2006 [verkkodokumentti] [viitattu 15.02.2006].
http://www.wi-fi.org/opensection/protected_access_devbackup.asp

WiFi Alliance 2003 [verkkodokumentti] [viitattu 18.03.2006].
Saatavissa: http://www.wi-fi.org/membersonly/getfile.asp?f=Wi-Fi_ProtectedAccessWebcast_2003.pdf

Tietoturva WLANissa (2001) [verkkodokumentti] [viitattu 29.12.2005].
Saatavissa: http://www.cs.uta.fi/~csjupa/opetus/TiTu/LAMK/PDF/WLAN.pdf

Garcia 2002; [Kirjoitelma] [viitattu 24.01.2006].
Garcia, Andrew (2002) Making the insecure secure. *PC Magazine*, Vol. 21, Issue 10,107–109.

Tolonen K. 2004 [verkkodokumentti] [viitattu 05.03.2006].
Saatavissa: http://www.oulu.fi/atkk/tiedotus/sessio/sess220/langaton_verkko.htm

Haapakangas U-M. 1999 [verkkodokumentti] [viitattu 10.02.2006].
Saatavissa: http://www.netlab.hut.fi/opetus/s38118/s99/htyo/33/ippuhelu.shtml

Hiironniemi O. 1999 [verkkodokumentti] [viitattu 10.02.2006].
Saatavissa: http://keskus.hut.fi/opetus/s38118/s99/htyo/44/eka.shtml

Heinonen M. 2000[verkkodokumentti] [viitattu 12.02.2006].
Saatavissa: http://keskus.hut.fi/opetus/s38118/s00/tyot/17/voip.shtml

Liikenne- ja viestintäministeriö 2005[verkkodokumentti] [viitattu 12.02.2006].
Saatavissa: http://www.mintc.fi/oliver/upl402-Julkaisuja%2016_2005.pdf

Väänänen K. 1999
http://www.netlab.tkk.fi/julkaisut/tyot/erikoistyot/VoIP/44380T.pdf 28.01.2006

Beijar N. 1998[verkkodokumentti] [viitattu 26.02.2006].
Saatavissa: http://www.netlab.tkk.fi/tutkimus/ipana/paperit/sip.pdf

VoIP- a searchNetworking.com Definitions 11.1.2006 [verkkodokumentti] [viitattu 02.01.2006].
Saatavissa:
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214148,00.html

Verkkoteknologiaa suomeksi: 3G on täällä tänään [verkkodokumentti] [viitattu 12.04.2006]. Saatavissa:
http://www.ficom.fi/fi/a_uutisaread.html?Id=1101819408.html

Langattomien lähiverkkojen (WLAN) turvallisuus 2006[verkkodokumentti] [viitattu 12.04.2006].
Saatavissa: http://www.ficora.fi/suomi/tietoturva/ohjeet/ohje-2002-07.htm

Opinnäytetyö WLAN Seppänen L. [verkkodokumentti] [viitattu 24.04.2006].
Saatavissa: http://trade.hamk.fi/~lseppane/courses/wlan/doc/WLANmat.doc

Haverinen M.2003 [verkkodokumentti] [viitattu 24.04.2006]
Saatavissa: http://www.potaroo.net/ietf/all-ids/draft-haverinen-pppext-eap-sim-16.txt

NetworkWorld 2002 [Verkkodokumentti] [viitattu 14.04.2006]
Saatavissa: http://www.networkworld.com/details/795.html5.2.4 EAP-SRP

Penttinen P. 1999 [Verkkodokumentti] [Viitattu 24.04.2006]
Saatavissa: http://www.it.lut.fi/kurssit/98-99/1591/seminars/Penttinen/Penttinen.html

Marttinen L. 2003 [verkkodokumentti] [Viitattu 24.04.2006]
Saatavissa: http://www.cs.helsinki.fi/u/marttine/tili/IIs01/luennot/L10c1.pdf

LIITTEET:

Liite 1 Tukiaseman salasanan vaihto

1. Vaihdetaan tukiaseman hallintaliittymän salasana omaksesi.

2. Vaihdetaan tukiaseman langattomaan verkkoon lähettämä nimi (SSID, Service Set ID) omaksesi, koska oletusnimi on liian helposti arvattavissa.

Vaihdetaan SSID:nä olevan MyWLAN-nimen tilalle oma keksitty nimi!

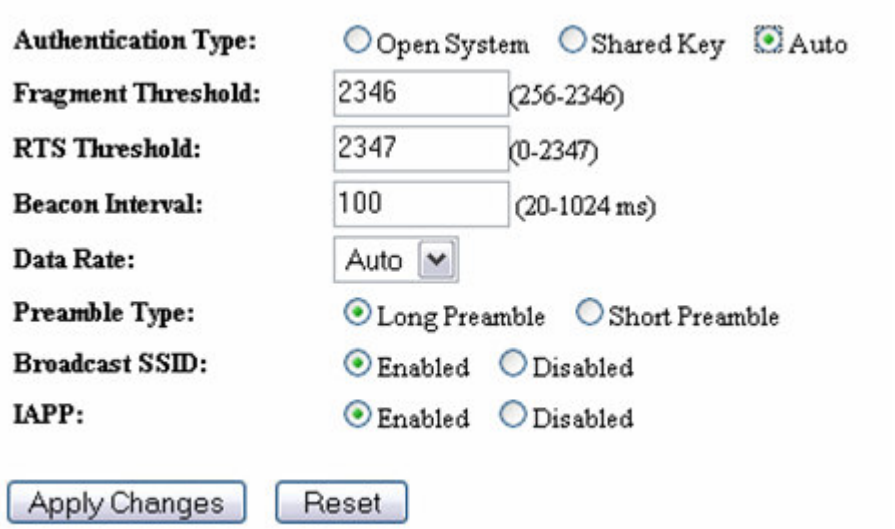
3. Otetaan käyttöön 128-bittinen WEP -salaus ,jossa todellinen salausavain on 104 bittiä, ja määritä oma, vaikeasti arvattava, salausavain. Avaimen voi antaa joko heksadesimaalilukuna tai helpommin muistettavana vakiomittaisena tekstinä.

Salausasetuksissa voidaan vaihtaa sekä 64 että 128 bittinen WEP -salaus, joka tulee ottaa käyttöön.
Tosin tässä tukiasemassa voitaisiin käyttää myös WPA:n mukaisia salausteknii-koita.

4. Verkkokorttien MAC-osoite (Media Access Control) on yksilöllinen tunniste käytettävälle kortille. Tämän takia tukiasemaan tulee määrittää niiden korttien MAC-osoitteet, joilta sallitaan yhteydet tukiasemaan.

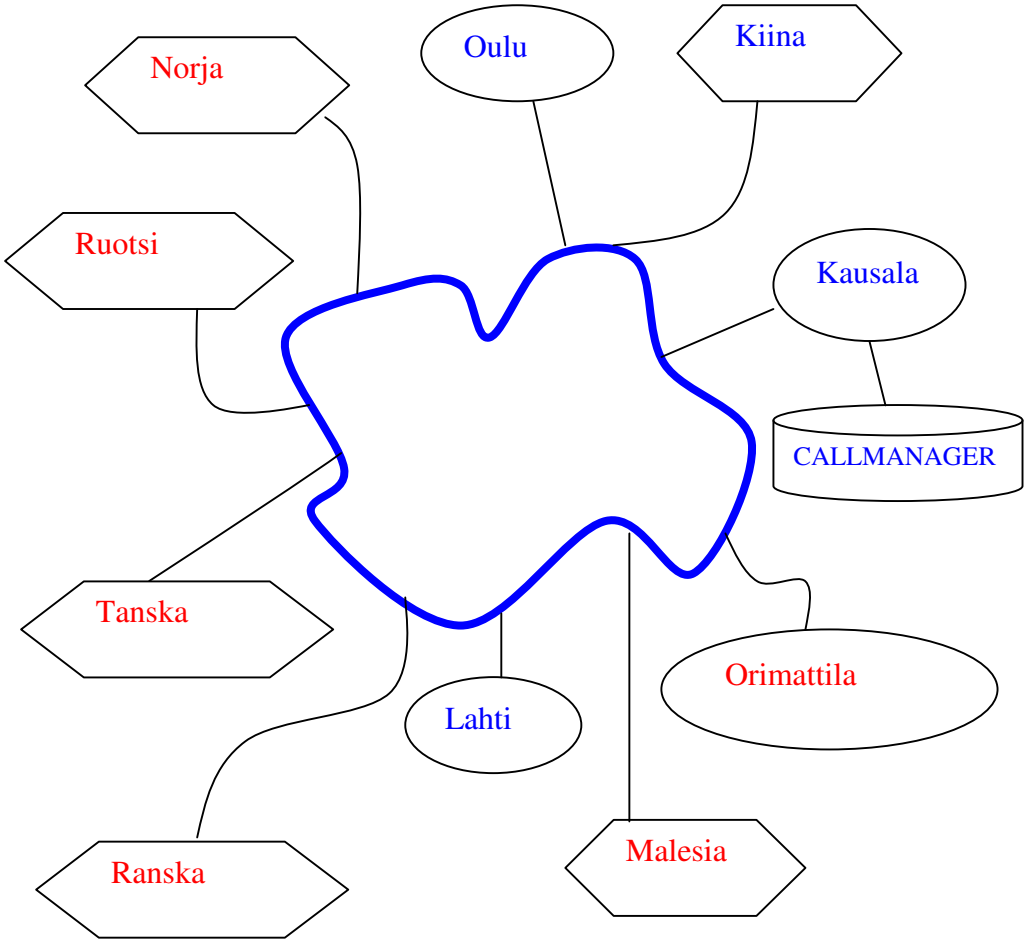
MAC -osoitteiden määritys tapahtuu syöttämällä osoitteet,
joko käsin kuten tässä mallilaitteessa tai joissain malleissa suoraan sallimalla tukiaseman peittoalueella olevista asiakaskoneista haluamansa. MAC -osoitteen näkee kortin ominaisuuksista, jossa osoitteesta käytetään nimeä fyysinen osoite (Physical Address), tai Windows koneissa komento-kehotteessa komennolla ipconfig/all.

5. Viimeisenä toimenpiteenä tulee poistaa käytöstä ”broadcast SSID” ominaisuus eli tukiaseman nimen ilmoittelu WLAN -verkkoon aika ajoin. Tämä oleellinen toimenpide kannattaa tehdä siksi viimeisenä, että verkon suojaaminen ja toimivak-si testaaminen on helpompaa.



Broadcast SSID valinta on yleensä SSID-nimen yhteydessä,
mutta mallilaitteessa ko. asetus oli eri valikossa. Ominaisuus tulee estää (disabled).

Liite 2 VOIP Verkko Halton Oy



Liite 3 Merex - taulukko

Halton

MEREX

TIETOJENKORJAUSLOMAKE

Henkilön nimitiedot:			
Sukunimi ja etunimi	Meikäläinen Matti		(30)
Nickname 1	(30)	**Nickname 2**	(30)
Henkilön tehtävänimikkeet:			
Nimike 1	(30)	**Nimike 3**	(30)
Nimike 2	(30)	**Henkilönumero**	(20)
Henkilön puhelinnumerot:			
Alanumero	2567 (30)		
Matkapuhelinnumero	(30)	**Sijaisen numero**	(30)
Privatel numero	(30)	**Sihteerin numero**	(30)
Vara numero	(30)	**Esimiehen numero**	
Henkilön osastotiedot:			
Yhtiö	**Muutos** (30)	**Kustannuspaikka**	(30)
Osasto	**Muutos** (30)	**Fax numero**	(30)
Ryhmä	**Muutos** (30)	**Sijainti**	(30)
Henkilön osoitetiedot:			
Käyntiosoite	**Muutos**		(30)
Postiosoite	**Muutos**		(30)
Huone			(30)
Muita tietoja:			
Kulunvalvontakortin numero	(10)	**Sähköpostiosoite**	(50)
Määräaikaisuus/osa-aikaisuus			(30)
Henkilön sihteerien, sijaisten & esimiehen nimet:			
Sijainen 1	Laakso Marjo **Muutos** Niemi Niina (30)	**Sijainen 2**	(30)
Sihteeri 1	(30)	**Sihteeri 2**	(30)
Esimies	(30)		
Henkilön työtehtävät, asiat, palvelut, kielitaito yms.(max.14 kpl / 30 merkkiä per tehtävä):			
Poistettavat tiedot		**Lisättävät tiedot**	
englanti	tuotannonkehitys	espanja	laskutus

Liite 4 CID taulukko

Toimipaikka	Cid - numeron alkuosa	Ala-numero	Kopio	Maa-koodi
Lahti	020792	2439		