HELSINKI UNIVERSITY OF TECHNOLOGY
Department of Electrical and Communications Engineering
Networking Laboratory

S-38.119 Tietoverkkotekniikan seminaari

Mobiili Internet

Teknillinen Korkeakoulu
Tietoverkkolaboratorio
Espoo 2002

SISÄLLYSLUETTELO

1. GPRS

General Packet Radio Service (GPRS) on uusi julkisen mobiiliverkon palvelu, jonka erona edeltäjiinsä on täysin pakettivälitteinen tiedonsiirto. Pakettivälitteisellä liikenteellä pyritään vastaamaan paremmin verkolle asetettuihin suoritusvaatimuksiin.

Kun verkossa kulkevasta liikenteestä yhä suurempi osa on dataliikennettä, saadaan pakettivälitteisellä tekniikalla hyödynnettyä huomattavasti paremmin verkon resursseja. Dataliikenteelle on tyypillistä purskeisuus, jolloin samalle siirtokaistalle voidaan laittaa lomittain useamman eri käyttäjän lähettämiä paketteja samanaikaisesti. Tällöin käyttäjillä on käytettävissä suhteellisesti enemmän siirtokaistaa kuin siinä tapauksessa että sama kaista annettaisiin kerrallaan vain yhden käyttäjän hallintaan.

GPRS –tekniikka muuttaa julkisten matkaviestinverkko-operaattorien perinteisiä toimintamalleja muuttamalla asiakasyhteyden laskutusperusteita ja mobiiliyhteyksien reitittämistä operaattoreiden välillä. GPRS –verkkojen yhteydessä operaattoreiden on myös mahdollista tuottaa matkaviestinverkkoon entistä monipuolisempia palveluita.

1.1 GPRS –tekniikka yleisellä tasolla

General Packet Radio Service (GPRS) tuo matkaviestinverkkoon uudenlaisen tavan yhteyden pitämiseen verkon ja päätelaitteen välillä. GPRS –tekniikalla toteutetussa yhteydessä varsinaiseen yhteyden muodostamiseen ei enää kulu aikaa, jolloin yhteyden voidaan katsoa olevan aina käytettävissä (always on).

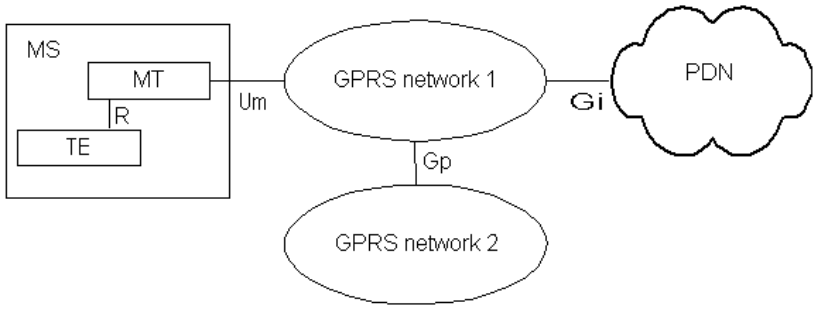
Merkittävin GPRS –tekniikan mukanaan tuoma uudistus on verkon sisäisen liikenteen muuttaminen IP –pohjaiseksi, jolloin perinteisen piirikytkentäisen yhteyden sijaan käytetään verkon resursseja paremmin hyödyntävää pakettikytkentäistä välitystekniikkaa.

Lisäksi GPRS -tekniikan yhteydessä on usein mainittu yhteysnopeuden huomattava nousu verrattuna esimerkiksi GSM –tekniikkaan. Teoreettisesti GPRS –tekniikalla on mahdollista päästä 171,2 kbps yhteysnopeuteen. Käytännössä kuitenkin päätelaitteiden nopeudet ovat luokkaa 14,4 – 33,6 kbps ja verkon kuormituksen kasvaessa yhteysnopeuden pelätään putoavan jopa alle 10 kbps [2].

1.1.1 GPRS –verkon rakenne

Pohjana GPRS –verkon toteutukselle on GSM –verkko, jonka rakenteeseen on tehty muutoksia kun verkon liikenne on muutettu pakettipohjaiseksi. GPRS –verkko on Gateway GPRS Support Node (GGSN) –laitteen avulla yhteydessä julkisiin dataverkkoihin (Public Data Networks) ja tämän yhteyden rajapinta on nimetty Gi–rajapinnaksi. Yhteys kahden eri GPRS -

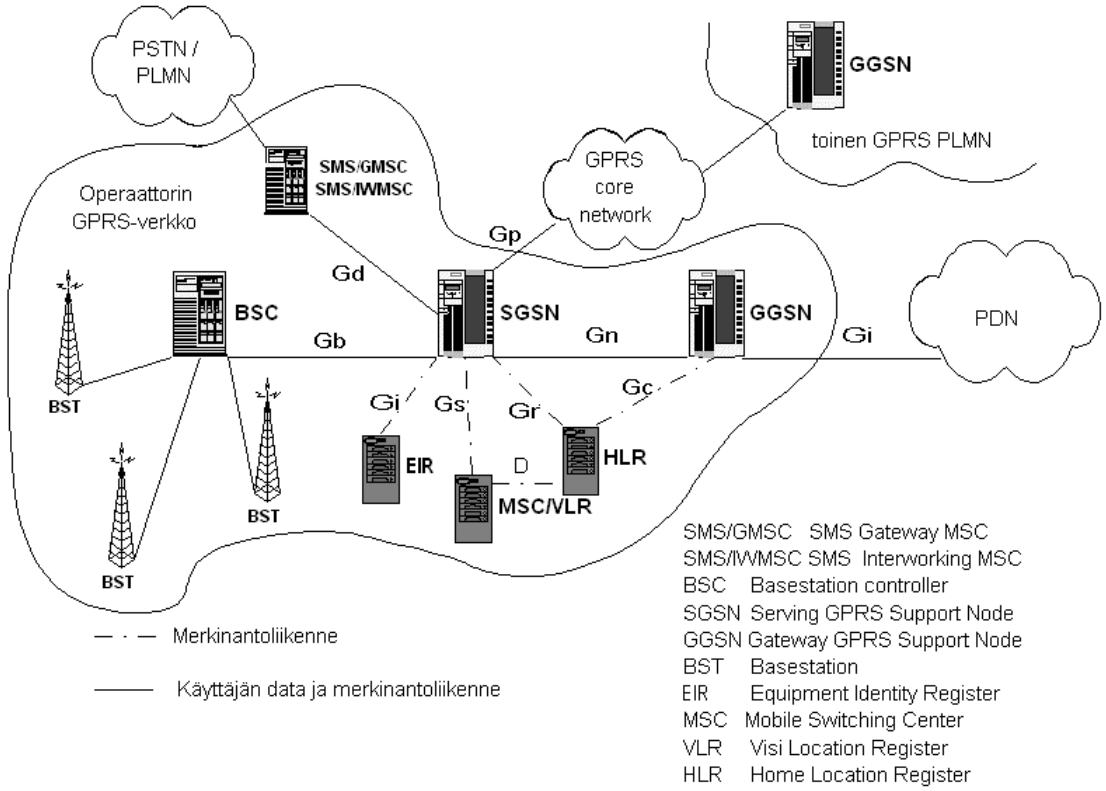
verkon välillä hoidetaan Gp–rajapinnan kautta, Gp:n yli liikennöivät sekä Serving GPRS Support Node (SGSN) että GGSN –laitteet.



Kuva 1 ITU-T GMS 09.60 GPRS –verkon rajapinnat [1}

Kuvassa 2 GPRS –verkkoon kuuluvia laitteita on kuvattu vielä hieman tarkemmin. Kuvan vasemmassa laidassa on esitetty GPRS -verkon radiorajapinta, jossa tukiasemat (BST) ja tukiasemakeskus (BSC) ovat yhteydessä. Verkon keskeisimpänä laitteena on SGSN, jonka tehtävänä on hoitaa verkon keskeisimmät toiminnot eli pakettien reititys, liikkuvuuden hallinta ja käyttäjien tunnistaminen. SGSN hyödyntää toiminnoissaan sen läheisyyteen sijoitettuja rekistereitä Home Location Register (HLR), Visited Location Register (VLR) ja Equipment Identity Register (EIR). Edellä mainituista VLR on sijoitettu kiinteästi varsinaisen kytkennän hoitavan Mobile Switcing Centerin (MSC) yhteyteen. Lisäksi SGSN on yhteydessä SMS -Gateway MSC –laitteen kanssa, jonka avulla hoidetaan GPRS –verkon tekstiviestiliikenne.

GPRS -verkon rajapintana muihin julkisiin dataverkkoihin toimii GGSN, joka muuntaa GPRS -verkon datapaketit ulkopuolisen verkon käyttämään muotoon. Kaksi GPRS –verkkoa voi olla myös suoraan yhteydessä toisiinsa Gp-rajapinnan kautta.



Kuva 2 GPRS -verkon tarkennettu rakenne [3]

1.1.2 GPRS -yhteyspalvelut

GPRS –verkko tarjoaa periaatteessa kahdenlaisia pakettivälitteisiä yhteyspalveluja (bearer services): yhdeltä yhdelle ja yhdeltä monelle. Edellä mainituista jälkimmäinen kuitenkin tullaan toteuttamaan vasta GPRS –verkon toisessa vaiheessa.

Tällä hetkellä GPRS –verkkoon on määritelty kaksi erityyppistä pisteestä pisteeseen muodostettavaa yhteystyyppiä, yhteydellinen ja yhteydetön. GPRS –verkko tukee kaikkia nykyisessä GSM –verkossa olevia palveluita, esimerkiksi tekstiviestiliikenne voidaan siirtää toimimaan GPRS –yhteyden ylitse. Vaikka useat operaattorit vielä tarjoavatkin tekstiviestipalvelun perinteisesti piirikytkentäisen palvelun kautta, on selvää, että ajan myötä tekstiviestit tulevat siirtymään joustavammin toimivan GPRS -yhteyden välityksellä. GPRS –tekniikan avulla operaattorit voivat lisäksi toteuttaa verkkoon uudenlaisia palveluita, jotka hyödyntävät GPRS:n nopeaa yhteydenmuodostusta ja joustavaa toimintaa.

GPRS –tekniikan ympärillä on käyty keskustelua jopa suoran sarjamuotoisen yhteyden (Octet Stream) tarjoamisesta GGSN:n ja päätelaitteen välille. Kyseinen sarjaliikenne mahdollistaisi periaatteessa minkä tahansa yhteysprotokollan toteuttamisen mobiilikäyttäjän ja toisen yhteyspisteen välillä.

1.1.3 GPRS –tekniikan elinkaari

Pakettivälitteisenä laajan peittoalueen omaavana verkkona GPRS tulee varmasti pitämään pintansa vielä pitkään, sillä tulevaisuuden langattomia laajakaistaverkkoja ei varmastikaan kannata toteuttaa GSM / GPRS –verkkoa vastaavilla peittoalueilla.

Tämän hetkisten GSM / GPRS –verkkototeutusten ongelmana on se, että pakettikytkentäinen liikenne aiheuttaa hieman häiriötä piirikytkentäisille yhteyksille. Tästä johtuen pakettikytkentäiset yhteydet on jouduttu eristämään tiettyihin aikaväleihin, mikä rajoittaa radiorajapinnan suorituskykyä huomattavasti [2]. Edellä mainitusta ongelmasta päästään kuitenkin eroon kasvattamalla puhtaasti pakettivälitteisten aikavälien osuutta tai osoittamalla tukiasemia liikenteen kytkentätyypin mukaan niin, että pakettivälitteinen liikenne kulkee oman tukiasemansa kautta ja piirivälitteinen omansa.

GPRS –tekniikan kehittäminen radiorajapinnan käytön tehokkuuden osalta tulee varmasti tapahtumaan jollakin aikavälillä, mutta kokonaisuudessa pakettivälitteinen verkkorakenne pitää varmasti pintansa pitkälle tulevaisuuteen.

1.2 GPRS verkkotasolla

Pakettivälitteisyys tuo etuja varsin monella eri tasolla, kun ajatellaan GSM / GPRS –verkkoja. Liikenteen muuttaminen pakettivälitteiseksi parantaa järjestelmän suoritustasoa sekä radiorajapinnan että runkoverkon osalta. Pakettivälitteinen liikenne on huomattavasti joustavampaa kuin piirikytkentäinen. Erityisesti kuormituksen kasvaessa pakettivälitteinen liikenne mahdollistaa yhteyksien paremman ja luotettavamman toiminnan.

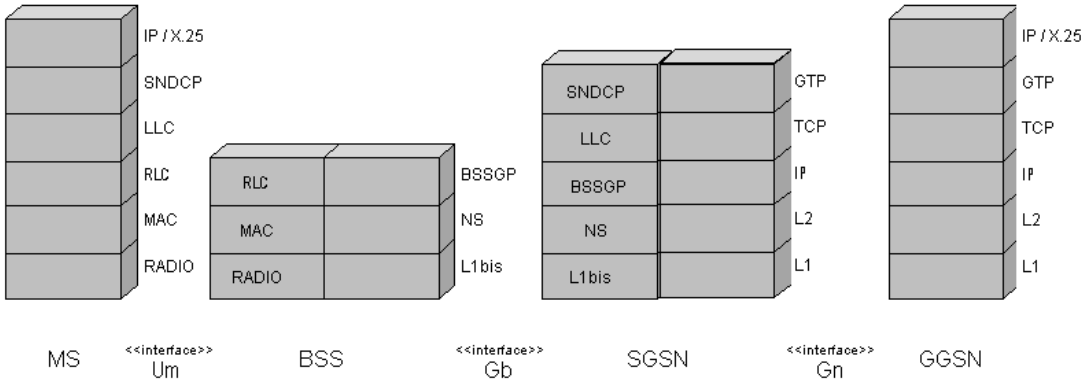
1.2.1 GPRS –tekniikan aiheuttamat muutokset verkon rakenteessa

Pakettivälitteisyys toi mukanaan GPRS –verkkoon kaksi uutta komponenttia, SGSN ja GGSN –laitteet. Nämä kaksi laitetta ovat hyvin monella tavoin yhteydessä toisiinsa, eikä laitteiden väliset yhteydet rajoitu vain tiettyihin laitteisiin, vaan GGSN voi toimia rajapintana usealle eri SGSN –laitteelle ja vastaavasti SGSN voi liikennöidä saman aikaisesti usean eri GGSN –laitteen kautta.

GPRS –tekniikan myötä verkon rakenteesta on tullut entistä joustavampi, operaattorien välinen liikenne ei ole enää sidottu tiettyihin liityntäpisteisiin vaan yhteydet voidaan tarvittaessa reitittää varsin pienin muutoksin vaihtoehtoista reittiä, esimerkiksi laitevian ilmetessä.

1.2.2 GPRS –verkon protokollat

Seuraavassa on kuvattu kokonaisuudessaan GPRS –verkon käyttämät protokollat päätelaitteen ja GGSN –laitteen välillä.



Kuva 3 GPRS -verkon kuljetusprotokollat päätelaitteesta GGSN:ään [5,10]

Edellä kuvatusta protokollarakenteesta voidaan havaita, että esimerkiksi päätelaitteen hakema IP –paketti pakataan GGSN –laitteessa uudelleen IP –paketin sisään, jolloin ”ylimääräisestä” kehysrakenteesta aiheutuu siirtokaistan hukkaa. Jotkut operaattorit yrittävät parantaa GPRS –verkkonsa kokonaisnopeutta kompensoimalla otsikkotiedoista aiheutuvaa kaistanhukkaa pakkaamalla IP –kehykset ennen kuin tunneloivat ne GPRS –verkon lävitse [6].

GPRS –verkossa on käytössä oma sisäinen osoiteavaruus, jota käytetään verkon sisäisessä tiedonsiirrossa. Kun mobiilipäätelaite (MS) on yhteydessä ulkopuoliseen verkkoon, annetaan sille erikseen operaattorin tai erillisen Internet-palvelun tarjoajan (ISP) toimesta julkinen osoite.

GPRS –operaattori voi tarjota asiakkaalle yhteyden tämän omaan lähiverkkoon, reitittämällä yhden GGSN –laitteen rajapinnoista asiakkaan lähiverkkoon. Edellä kuvatussa ratkaisussa asiakkaan datapaketit kulkevat GPRS Tunneling Protocol (GTP) –protokollalla GPRS –verkon lävitse, mutta esimerkiksi asiakkaan näkemä IP –osoite on allokoitu asiakkaan lähiverkon osoiteavaruudesta.

1.2.3 Yhteydet eri operaattorien välillä GPRS –verkossa

Suurimpana erona GSM –verkkojen roaming-järjestelyihin on se, että GPRS –verkossa voidaan tiedon kuljettaminen ja signalointi hoitaa saman verkon kautta, eikä erillisille signalointi- ja tiedonsiirtoverkoille ole enää tarvetta. GPRS –palvelujen reititykseen käytetään GPRS Roaming Exchange (GRX) –verkkoa, joka on keskitetty IP –pohjainen reititysverkko joka hoitaa GPRS –verkkojen yhdistämisen [7].

GPRS –verkkojen yhteistoimintaan liittyvä ”julkinen” GPRS –backbone on verkko-operaattoreille uusi asia ja siihen on luotava uudet toimintamallit. Käytännössä vierailevan päätelaitteen liikenne tunneloidaan GTP:tä käyttäen vierailtavan verkon SGSN:stä päätelaitteen kotiverkkoon, jolloin kaikki kotiverkon palvelut ovat käytettävissä.

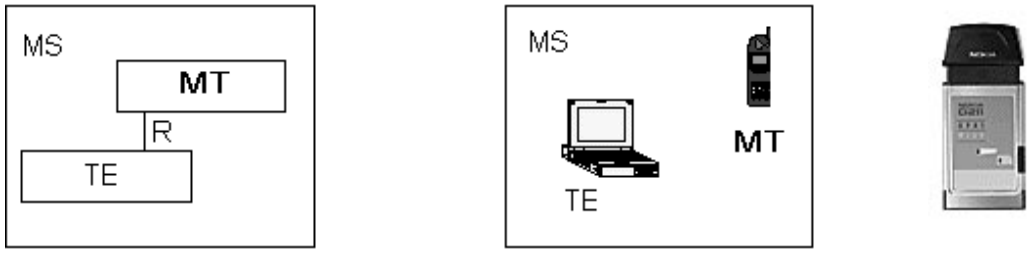
GPRS –verkossa käytettävän GTP -tunneloinnin ansiosta asiakkaalle voidaan tarjota huomattavasti helpommin kotiverkon palveluita käytettäväksi riippumatta siitä missä GPRS –verkossa asiakas on. GSM –tekniikkaan verrattuna selkeä etu on siinä, että asiakasyhteyksien tunnelointi

on kiinteä osa verkkoa, jolloin toiminnallisuus on myös käytettävissä kaikissa GPRS –verkoissa [8].

1.3 GPRS päätelaitteissa

GPRS –tekniikan myötä verkkoon liitetään varmasti entistä useammin päätelaitteita, joissa puhelintoiminto ei ole enää ainoa merkittävä ominaisuus. Keskeistä GPRS –päätelaitteiden kehityksessä on varmasti terminaalien toiminnallisuuksien lisääntyminen, tulevaisuudessa päätelaite osaa hyödyntää verkon tarjoamia palveluita entistä monipuolisemmin.

Päätelaitteiden kehityksestä erottuu varmasti tulevaisuudessa myös entistä selkeämmin toinen kehityssuunta, jossa GPRS –verkkoon yhteyden muodostaa mobiiliterminaali (MT), mutta yhteyttä käyttää varsinaisesti erillinen terminaalilaite (TE) [Kuva 4].



Kuva 4 GPRS -päätelaitteiden käsitteet. Kuvassa oikealla Nokian integroitu GPRS, HSCSD ja WLAN -kortti, joka ei suoraan sisällä mitään TE -ominaisuuksia [4].

1.3.1 Edellytykset GPRS –päätelaitteelta

GPRS –päätelaitteen on pystyttävä käsittelemään vähintään kahta samanaikaista yhteyttä (lähetys ja vastaanotto), maksimissaan GPRS –päätelaitteelle voi tulla viisi yhteyttä, joista vähintään yhden täytyy olla vastakkaiseen suuntaan muihin.

GPRS –päätelaitteelle on vaikea määrittää suoranaisia edellytyksiä, sillä varsinaisen GPRS –yhteyden muodostamiseen tarvittavien resurssien ja yhteyden tehokkaaseen hyödyntämiseen tarvittavien resurssien rajaa on vaikea määrittää.

1.3.2 Päätelaitteiden luokat

GPRS –päätelaitteita on kolmea eri luokkaa A, B ja C. A –luokan laitteet pystyvät käsittelemään samanaikaisesti sekä piiri- että pakettikytkentäistä liikennettä. B –luokan laitteet pystyvät kytkeytymään kumpaakin liikennetyyppiä välittäviin asemiin, mutta voivat aktiivisesti olla yhteydessä vain yhdellä liikennetyypillä kerrallaan. C-luokan laitteet pystyvät kytkeytymään vuorotellen joko piiri- tai pakettikytkentäisiin asemiin, eli liikennetyypin muunnos vaatii uudelleenkytkeytymisen.

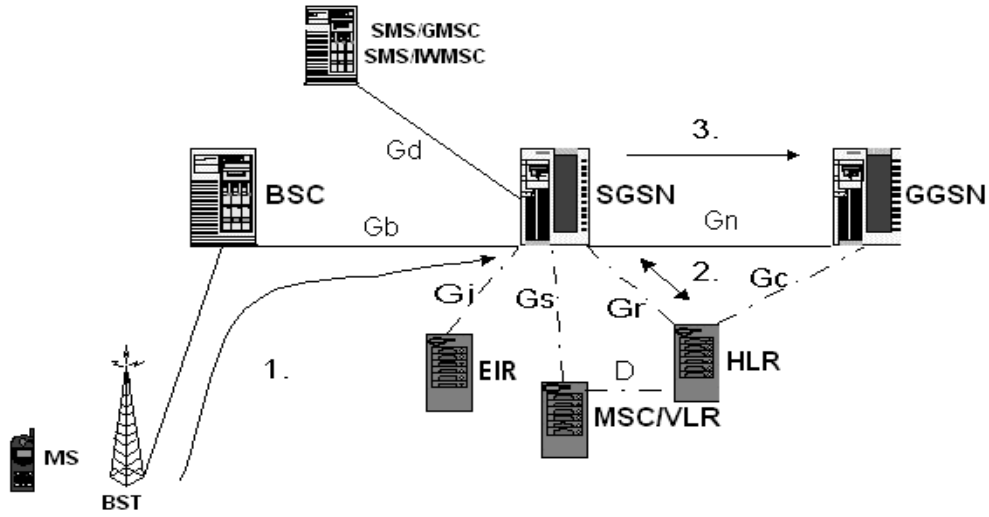
1.4 GPRS -yhteys

GPRS –verkon yhteydet ovat järjestelmän ensimmäisessä vaiheessa pisteestä pisteeseen yhteyksiä. Paketit reititetään verkon lävitse joko yksilöllisesti (yhteydetön), tai muodostamalla tietyille paketeille kiinteitä reitityksiä (yhteydellinen). Tässä työssä ei käsitellä GPRS –verkkoon tulevaisuudessa toteutettavia yhdeltä monelle yhteyksiä.

1.4.1 GPRS -yhteyden muodostamisesta

GPRS –yhteyden muodostaminen päätelaitteesta alkaa siten, että päätelaite (MS) lähettää ”Activate PDP Context Request” –viestin SGSN –laitteelle. SGSN puolestaan tarkistaa käyttäjän tiedot HLR –rekisteristä johon voidaan tarvittaessa määritellä käyttäjäkohtaisesti käytettävä IP –osoite ja esimerkiksi käytettävä Access Point (AP). Seuraavassa vaiheessa SGSN lähettää GGSN –laitteelle ”Create PDP Context Request” –viestin. Tämän jälkeen päätelaitteelle voidaan muodostaan reititys ja varata osoite GPRS –verkosta.

GPRS –tekniikka tuo muutoksia liikkuvuudenhallintaan lisäämällä käsitteen reititysalue liikkuvuuden käsitteistöön. Reititysalueella tarkoitetaan sitä SGSN –laitetta, jonka palveluja päätelaite käyttää.



Kuva 5.GPRS -yhteyden muodostaminen

1.4.2 Laskuttaminen GPRS –verkossa

GPRS –verkon yhteydessä myös puheluiden laskutus on muuttunut perinteisestä aikaperustaisesta kustannuksesta joko kiinteään hinnoitteluun tai siirretyn tietomäärän mukaan laskettavaan korvaukseen.

Varsin monet operaattorit hakevat vielä lopullista toimintamalliaan. Tällä hetkellä Suomen kolmesta suuresta operaattorista yksi tarjoaa palveluaan kiinteällä kuukausikustannuksella ja kaksi muuta operaattoria hinnoittelevat palvelunsa siirretyn tiedon mukaan.

1.5 GPRS –verkko ja mobiili Internet

GPRS –tekniikan voidaan katsoa olevan ensimmäinen joustavan langattoman IP -pohjaisen liikenteen mahdollistava tekniikka. Lähinnä nopean yhteydenmuodostuksen ja purskeiselle liikenteelle soveltuvan verkon takia GPRS on hyvä vaihtoehto mobiiliin Internetiin.

GPRS –tekniikan rajoituksena on kuitenkin vielä suhteellisen pienet yhteysnopeudet ja mahdollisesti käytettäviin päätelaitteisiin liittyvät rajoitteet, eli Internet-palvelujen toteutuksessa on vielä otettava erikseen huomioon GPRS -käyttäjät.

1.5.1 Mobiili Internet GPRS –tekniikan avulla

Useisiin GPRS –puhelimiin on rakennettu Internetiä hyödyntäviä toiminnallisuuksia kuten sähköposti ja WAP –sovelluksia. Usein päätelaitteena toimii kuitenkin jokin muu kuin varsinainen matkapuhelin. Esimerkiksi matkapuhelin voi olla yhdistetty BlueTooth –teknologialla sylimikroon, joka toimii päätelaitteena.

GPRS –verkko vahvistaa suuntautumista entistä enemmän Internet –tyyppiseen liikenteeseen, jossa toiminnot sijaitsevat älykkäissä päätelaitteissa. Tällä hetkellä voidaan selkeästi havaita, että päätelaitteiden toiminnallisuuksia pyritään kasvattamaan. Uusien matkaviestinten ominaisuudet kehittyvät jatkuvasti kohti entistä monipuolisempaa viestintää, puhelimeen integroidaan tai puhelin integroituu moneen käytössämme olevaan laitteeseen.

1.5.2 Palvelujen turvallisuus GPRS –verkossa

GPRS –verkossa tapahtuvissa toiminnoissa voidaan turvallisuuden katsoa olevan melko korkea, mutta luonnollisesti kaikkea on syytä epäillä. Siirryttäessä vuorovaikutukseen ulkopuolisten verkkojen kanssa ei käyttäjän turvallisuutta / tunnistettavuutta voida enää taata vaan se täytyy toteuttaa erillisin ratkaisuin.

GPRS –verkon sisällä käyttäjät voidaan tunnistaa SIM –korttiin perustuneen alkuperäisen tunnistamisen avulla. Näin ollen voidaan sanoa, että operaattorin verkon sisäisissä palveluissa käyttäjät pystytään tunnistamaan varmasti.

Käyttäjän tunnistamiseen ja autentikointiin liittyvät palvelut on sijoitettu GPRS –verkossa SGSN –laitteeseen. SGSN –laitteen avulla on tarvittaessa mahdollista myös suorittaa kyselyjä käyttäjätietoja ja laitetietoja sisältäviin rekistereihin, millä on osaltaan pyritty varmistamaan myös rekisteritietojen käytön kontrollointi.

1.5.3 GPRS -palvelujen laatu

GPRS –verkossa on mahdollista määritellä käyttäjälle profiili, jossa määritellään millaiseen palveluun käyttäjä on oikeutettu. Profiiliin voidaan määrittää parametreja, jotka kuvaavat käyttäjän lähettämän ja

vastaanottaman liikenteen prioriteettia, hukkuvien pakettien suhdetta, viivettä sekä siirtokaistan leveyttä [9].

Tällä hetkellä suurimmat ongelmat esiintyvät GPRS –verkkojen radiorajapinnoissa. Jotkut operaattorit ovat pyrkineet parantamaan asiakkaalle tarjoamaansa palvelun laatua esimerkiksi kompensoimalla radiorajapinnan liikennerajoitteita. Tämä on tehty hieman kyseenalaisesti käsittelemällä käyttäjän siirtämää tietoa poistamalla siitä ”tarpeettomia” otsikkotietoja. Tulevaisuudessa radiorajapinnan käyttöä voidaan parantaa esimerkiksi hyödyntämällä EDGE (Enhanced Data rates for Global Evolution) –teknologiaa.

GPRS -palvelu ei tällä hetkellä tarjoa mitään ylivertaista ratkaisua muihin käytettäviin tekniikoihin verrattuna, mutta GPRS –palvelua hyödyntämällä asiakkaan on mahdollista hyödyntää verkkoa entistä monipuolisemmin ja tehokkaammin. Esimerkiksi jos käyttäjä liittää kannettavaan tietokoneeseensa verkkokortin, jonka avulla hän voi olla yhteydessä sekä WLAN, GPRS että HSCSD –verkkoihin päästään jo lähelle toimintamalleja joita on esitetty 3G –verkkojen yhteydessä.

1.6 GPRS -palvelun tulevaisuus

Tulevaisuudessa GPRS -palvelu tulee olemaan kiinteä osa GSM –verkkoa ja sen suorituskyky tulee varmasti kasvamaan ajan myötä. Erilaisten GSM –verkkoon ja GPRS –palveluun tehtävien parannusten myötä uskon, GPRS -palvelu tulee tarjoamaan varsin pitää kilpailukykyisen olla yhteydessä tietoverkkoihin.

GPRS –palvelu tulee varmasti pysymään käytössä olevien verkkopalvelujen joukossa, sillä se pystyy varmasti vielä pitkään tarjoamaan parhaan pakettivälitteisen yhteyden erittäin laajalla peittoalueella. Lisäksi tällä hetkellä kehitettävän toisen vaiheen GPRS –palvelun uusien yhteysmuotojen myötä voidaan myös mobiiliverkossa tarjota erilaisia multicast –palveluja, jolloin tietoa pystytään entistä tehokkaammin jakamaan suurelle määrälle käyttäjiä.

1.7 Lyhenteet

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HSCSD	High Speed Circuit Swithed Data
MS	Mobile Station
MT	Mobile Terminal
TE	Terminal Equipment
SGSN	Serving GPRS Support Node
GGSN	Gateway GPRS Support Node
BST	Basestation
BSC	Basestation Controller
HLR	Home Location Register
VLR	Visited Location Register
EIR	Equipment Location Register
MSC	Mobile Switcing Center
GRX	GPRS Roaming Exchange Network
GTP	GPRS Tunneling Protocol
AP	Access Point
WLAN	Wireless Local Area Network
EDGE	Enhanced Data rates for Global Evolution

1.8 Lähteet

1. *ETSI ITU-T GSM 09.60 version 7.5.1 Release 1998* http://www.itu.int/home/index.html

2. *DigiToday -verkkolehti (viitattu 18.2.2002) :* http://www.digitoday.fi/digi98fi.nsf/pub/te20020218141357_jvi_38319066

3. *Christian Bettstetter, Hans-Jörg Vögel, and Jörg Eberspächer, TUM: GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface. Copyright 1999 IEEE http://www.comsoc.org/livepubs/surveys/public/3q99issue/pdf/Bettstetter.pdf*

4. *Nokia Oyj verkkosivut* http://www.nokia.com/phones/nokiad211/

5. *TKK – Tietoliikennelaboratorio – Kurssi S-72.423 – Telecommunication Systems* http://www.comlab.hut.fi/opetus/423/lect2001/gsm.pdf

6. *DigiToday -verkkolehti (viitattu 21.2.2002)* http://www.digitoday.fi/digi98fi.nsf/pub/te20020221085404_jvi_99093614

7. *GSM Associationin International Roaming Expert Group (IREG), recomendation IR.34*

8. *Anders Roos, Northstream – GPRS Roaming – Moving towards 3G* http://www.gsmworld.com/technology/gprs/presentations.shtml

9. *ETSI ITU-T GSM 02.60 version 6.3.1 Release 1997* http://www.itu.int/home/index.html

10. *Protocols.com* http://www.protocols.com/pbook/gprs.htm

2. SIP

SIP eli Session Initiation Protocol on pakettivälitteiseen IP-verkkoon kehitetty merkinantoprotokolla, jonka avulla voidaan muodostaa yhteys käyttäjien välille. Merkinantopalveluiden lisäksi SIP tarjoaa myös lisäpalveluita sekä mobiliteettituen.

SIP-protokolla on suunniteltu erittäin mukautuvaksi sekä käytettävän verkon että välitettävän viestin osalta. Protokollan viestien sisältämän tiedon muoto määritellään kyseisen viestin otsikkotiedoissa, joten viestien sisältämä tieto mukautuu hyvin vallitsevaan toimintaympäristöön.

SIP-protokolla rakentuu siten, että protokollaan voidaan määritellä laajennuksia joiden avulla protokollan toiminnallisuuksia saadaan lisättyä. Tulevaisuuden monimuotoisen ja jatkuvasti muuttuvan verkkoympäristön kannalta on erittäin tärkeää, että käytettävissä on mukautuvia, uudistumiskykyisiä ja Internet-protokollien kanssa yhteensopivia protokollia ja näin ollen SIP-protokollan tulevaisuus näyttää lupaavalta.

2.1 Yleistä SIP:stä

SIP (Session Initiation Protocol) on merkinantoprotokolla reaaliaikaisten puheluiden luomiseen IP-verkoissa. SIP perustuu Internet Engineering Task Force (IETF) -standardiin RFC 2543 ja määrittelee multimediasessioiden ja puheluiden muodostamisen, muokkaamisen ja katkaisun. Multimediasessioita voivat olla esimerkiksi puhelin- tai videoneuvottelut, etäopetus ja verkkopelit [1].

SIP:tä käytetään siis kahden päätelaitteen väliseen kommunikaatioon ja se käyttää asiakas-palvelin –mallia. SIP:n peruskäyttötapauksia ovat mm. käyttäjän rekisteröityminen verkkoon, kahden käyttäjän välisen puhelun muodostaminen, käyttäjän osallistuminen puhelinneuvotteluun, puheluun liittyvän tiedon lähetys sekä puhelun lopettaminen. SIP:n avulla käyttäjä voi myös lähettää puheluun liittymätöntä tietoa kuten pikaviestejä (instant message).

SIP on pakettikerroksen siirtotavasta riippumaton protokolla, joka on suunniteltu käytettäväksi useiden erilaisten, sessioiden muodostamista vaativien palvelujen yhteydessä.

2.1.1 SIP -viestit

SIP–protokolla on tekstipohjainen ja viestejä on näin ollen helppo tulkita, mutta ne vievät paljon tilaa. SIP-viesti koostuu otsikko-osasta sekä varsinaisesta viestirungosta, jonka tyyppi voidaan määritellä sähköposteista tutulla MIME –tyypillä (kuva 1).

SIP–viestin otsikkotiedoissa on määritelty mm. viestin lähettäjä ja vastaanottaja. Lisäksi viestin otsikkotiedoissa kerätään tietoa siitä, millaista

reittiä viesti on käyttäjälle saapunut eli pidetään kirjaa viestin kohtaamista palvelimista. Otsikkokenttään lisätään aina välityspalvelimissa ”via”–kenttä, jotta viestin vastaus voidaan välittää samaa reittiä pitkin.

SIP-viestin rungon sisältämä tieto määritellään SIP-otsikkotietojen Content-Type -parametrin avulla. SIP-viestin runko voi siis olla joko tekstipohjainen SDP-sanoma, HTTP-dokumentti tai vaikkapa JPEG-koodattu kuva kutsun lähettäjästä.

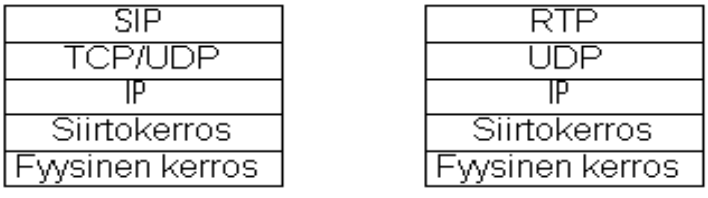
Kuva 1 SIP-viestin rakenne [2]

SIP-viestien sisällä käytetään SDP:tä (Session Description Protocol) multimediayhteyksien ominaisuuksien (esim. puhekoodekkien, porttien) kuvaamiseen Internetissä. Nimestään huolimatta SDP ei kuitenkaan ole protokolla vaan tekstiformaatti [3].

2.1.2 SIP -ohjelmistoympäristö

SIP on sovellustason protokolla joka on riippumaton pakettikerroksen siirtomenetelmästä. Sitä voidaan käyttää UDP:n ja TCP:n päällä. UDP on käytetympi, koska se on yksinkertainen, nopea ja tehokas. Merkinannossa tarvitaan luotettavuutta: jos käytetään UDP:tä, SIP-protokollakerros tarjoaa tarvitun luotettavuuden ja uudelleenlähetyksen. Tulevaisuudessa SCTP (Stream Control Transport Protocol) näyttää sopivalta SIP –liikenteeseen [4].

SIP -protokollaa käytetään session muodostamiseen ja varsinainen tieto siirretään tarkoitukseen paremmin sopivalla protokollalla, esimerkiksi VoIP-puhelussa ääni kuljetetaan RTP:llä. Merkinantoon käytettävä protokollapino eroaa varsinaisen tiedon kuljettamiseen käytettävästä protokollapinosta (Kuva 2).



Kuva 2 Signalointiin ja viestin välittämiseen käytettävät protokollat [3]

Merkinanto eli SIP-protokollalla välitetyt viestit kulkevat useimmiten eri reittiä kuin varsinainen siirrettävä tieto. Reaaliaikaisissa sovelluksissa signalointiin käytetään usein välityspalvelimia, mutta varsinainen tieto välitetään suoraan käyttäjien välillä [4].

SIP on perinyt useita ominaisuuksia HTTP:ltä, esimerkiksi numeeriset vasteet ja samanlaisen otsikkorakenteen. SIP -protokollalla on muutenkin paljon yhteistä HTTP- ja SMTP -protokollien kanssa, mikä osaltaan helpottaa SIP-merkinannon yhdistämistä kyseisiä protokollia hyödyntäviin palveluihin.

2.1.3 SIP:n autentikointi ja turvallisuus

SIP:n käyttäjäagentit pystytään tunnistamaan käyttäen jaettuun salaisuuteen perustuvia vasteita, eli rekisteri lähettää haasteen verkkoonsa pyrkivälle käyttäjälle ja varsinainen tunnistaminen tapahtuu haasteeseen annettavaan vasteen perusteella [3].

Käyttäjien välinen SIP-merkinanto voi olla suojattu käyttäen salaisiin ja julkisiin avaimiin perustuvaa tekniikkaa kuten PGP tai tulevaisuudessa myös S/MIME. SIP-tekniikka voi kuljettaa varsinaisen tietosisällön salaamiseen käytettäviä salausavaimia sisällään SDP:tä hyödyntäen. Välitettäviin SIP-viesteihin voidaan yhdistää myös digitaalinen allekirjoitus.

Käyttäjän kannalta on oleellista, että SIP-viestien otsikkotiedot pystytään salaamaan, sillä otsikkotiedot sisältävät käyttäjän kannalta arkaluontoista materiaalia. SIP-viestin otsikkotietojen salaus on toteutettava väli-väliltä -periaatteella (hop-by-hop), jotta viestin välittäminen verkossa olisi mahdollista [5]. Väli-väliltä –periaatteesta seuraa myös se, että verkossa olevien välitys- ja uudelleenohjauspalvelimien on oltava tietoturvaratkaisuiltaan luotettavia. SIP-viestien väli-väliltä salaus voidaan toteuttaa verkkokerrokseen sijoitetun IPSec:in tai kuljetuskerrokseen sijoitetun TLS –salauksen avulla.

Käyttäjän tunnistamisen lisäksi SIP tarjoaa anonyymipalvelun (Anonymizer), jonka avulla käyttäjän identiteetti voidaan kätkeä muilta käyttäjiltä.

2.2 SIP -osakokonaisuudet

SIP:n neljä osakokonaisuutta ovat käyttäjäagentit (user agents), rekisterinpitäjä (registrar), välityspalvelimet (proxy servers), ja uudelleenohjauspalvelimet (redirect server) [3].

2.2.1 Käyttäjäagentti

Käyttäjäagentti on päätelaiteohjelmisto, joka lähettää istunnon muodostus- ja lopetuspyyntöjä verkolle ja vastaanottaa kuittauksia verkolta. SIP-päätelaitteina voivat toimia SIP-puhelin, PC tai kannettava tietokone, PDA sekä matkapuhelin [2].

SIP-verkon perusarkkitehtuuri on asiakas/palvelin –tyyppinen. Käyttäjäagentit toimivat asiakkaina (UAC) pyyntöjä muodostettaessa ja

palvelimina (UAS) pyyntöihin vastattaessa. Käyttäjäagentit voivat kommunikoida keskenään suoraan tai välipalvelimen kautta. Käyttäjäagenttia, joka palvelee useaa käyttäjää samanaikaisesti kutsutaan sillaksi (Gateway). Käyttäjäagentit pitävät kirjaa puheluiden tiloista.

2.2.2 Rekisterinpitäjä

Rekisterinpitäjä tarkoittaa verkossa sijaitsevaa SIP-palvelinta, joka vastaanottaa ja hyväksyy päätelaitteelta tulevat rekisteröintipyynnöt. Lisäksi palvelinta käytetään SIP-osoitteiston ja fyysisten osoitteiden yhteyksien määrittämiseen. Rekisterinpitäjä sijaitsee tyypillisesti välityspalvelimen yhteydessä.

2.2.3 Välityspalvelin

Välityspalvelin on SIP-palvelimen ohjelmisto joka lähettää päätelaitteen pyynnöt eteenpäin ja vastaukset takaisin päätelaitteelle. Palvelin vastaanottaa käyttäjäagentilta SIP-pyynnön, lisää otsikkotietoja ja muokkaa niitä tarvittaessa sekä välittää pyynnöt seuraavalle palvelimelle tai toiselle käyttäjäagentille. Lisäksi välityspalvelimen tehtäviin kuuluu säilyttää tietoa laskutusta varten. Välityspalvelinta voidaan käyttää myös käyttäjän olinpaikan piilottamiseen (anonyymipalvelu), sillä se mahdollistaa alueen nimen (domain name) käytön tietyn käyttäjän paikallistamiseen mikäli vastaanottajan IP -osoite tai isäntäkoneen nimi ei ole tiedossa [5].

Välityspalvelin voi olla joko tilaton tai tilallinen: tilaton välityspalvelin ei ylläpidä yhteyden tilatietoa eikä lähetä viestejä uudestaan, kun taas tilallinen välityspalvelin tarjoaa viestien uudelleenlähetyksen ja ylläpitää puhelun tai muun liikennetapahtuman tilaa. Tilatietoja tarvitaan laskutukseen.

2.2.4 Uudelleenohjauspalvelin

SIP-uudelleenohjauspalvelin vastaanottaa asiakkaan pyynnön ja vastaa siihen uudelleenohjausvasteella, joka sisältää pyydetyn palvelimen osoitteen. Palvelin ei siis välitä viestejä vaan palauttaa lähettäjälle vastaanottajan olinpaikan.

2.3 SIP:n sanomat

SIP:ssä on kahdenlaisia sanomia, pyyntöjä (request) ja vasteita (response). Pyyntöjä nimitetään myös SIP-metodeiksi (method). Standardissa [6] on määritelty kuusi perusmetodia:

- REGISTER: rekisteröi käyttäjän ja tämän sijainnin verkkoon
- INVITE: käytetään session (puhelun) muodostamiseen
- ACK: kuittaus session muodostumisesta
- BYE: käytetään session päättämiseen
- CANCEL: peruuttaa käynnissä olevan session tai viimeisen pyynnön

- OPTIONS: käytetään toisen käyttäjäagentin kapasiteetin tiedusteluun

SIP-pyyntöön vastataan aina vasteella. Vasteet viestittävät pyynnön onnistumisesta tai epäonnistumisesta. Vasteiden numeerisista koodeista suurin osa on peritty suoraan HTTP:ltä. Yleisimmät vasteet ovat

- 100 Trying: ”INVITE” –metodia käsitellään
- 180 Ringing: tavoitellun henkilön / B-tilaajan päätelaite hälyttää
- 182 Queued: puhelu on jonossa toisessa päässä
- 200 OK: myönteinen vahvistus
- 404 Not Found: tavoiteltua henkilöön ei saada yhteyttä

SIP:n pyynnöillä ja vastauksilla on sähköpostin otsikkotietoja vastaavat otsikkokentät. Pakollisten kenttien To, From, Via, Call-ID ja Cseq lisäksi SIP:ssä on määritelty runsaasti valinnaisia kenttiä kuten Subject ja Date [2].

2.3.1 Laajennukset metodeihin

Perusmetodeiden lisäksi Internetistä löytyvissä hyväksymättömissä dokumenteissa (draft) on määritelty useita laajennuksia metodeihin. Näitä laajennuksia käytetään lisäämään SIP:n tarjoamia palveluja. Laajennusmetodeita ovat esimerkiksi [2]

- INFO: käytetään sessioon liittyvän tiedon siirtoon
- MESSAGE: metodi pikaviestintään (instant messaging), metodi kuljettaa pikaviestiä viestikentässään
- SUBSCRIBE: ilmoitusten tai läsnäolotiedon tilaus
- NOTIFY: käytetään muutoksista tai läsnäolosta tiedottamiseen

2.4 Yhteyden muodostaminen ja purkaminen

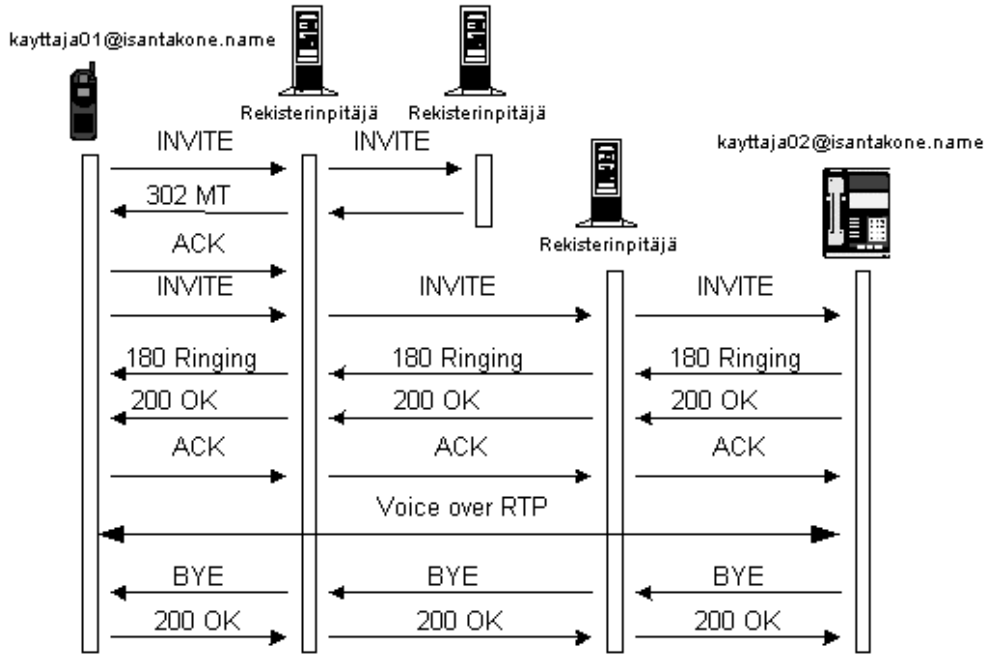
SIP-yhteydenmuodostuksessa käytetään helposti muistettavia SIP-osoitteita, joiden avulla yhteyspyynnöt välitetään tavoitellulle käyttäjälle.

Yhteyttä muodostettaessa tavoiteltavan käyttäjän kotirekisterinpitäjälle lähetetään yhteydenmuodostuspyyntö käyttäjän SIP-osoitteen avulla. Mikäli käyttäjä ei yhteydenmuodostushetkellä sijaitse kotirekisterinsä toimialueella, on kyseisellä palvelimella tieto käyttäjän varsinaisesta sijainnista.

Kuvassa 3 on esitetty SIP-puhelun yhteydenmuodostus:

1. Käyttäjä 1 ottaa yhteyttä käyttäjään 2
2. Käyttäjän 2 ensisijainen rekisterinpitäjä ilmoittaa, että kyseinen käyttäjä on tilapäisesti tavoitettavissa toisen palvelimen kautta ja palauttaa tämän palvelimen osoitteen
3. Käyttäjä 1 kutsuu käyttäjää 2 saamastaan uudesta osoitteesta. Käyttäjän 2 puhelin soi (Ringing-vaste) ja hän vastaa puhelimeen (OK-vaste)

4. Käyttäjä 1 vastaa ACK-metodilla ja yhteys muodostetaan
5. Äänipaketit kulkevat suoraan terminaalien välillä RTP:n välityksellä
6. Käyttäjä 2 lopettaa puhelun BYE-metodilla
7. Käyttäjä 1 vastaa OK-vasteella ja yhteys katkeaa



Kuva 3 Yhteydenmuodostus SIP –protokollan avulla [4], [8]

2.5 SIP mobiilissa IP -verkossa

Tulevaisuudessa käyttäjät voivat liikkua erilaisissa langattomissa verkoissa, joten käytettävältä protokollalta vaaditaan kykyä toimia monissa erilaisissa ympäristöissä. Tähän tarkoitukseen SIP soveltuu erittäin hyvin, sillä sen toteutus on täysin riippumaton käytettävästä verkosta eli sitä voidaan käyttää minkä tahansa protokollan päällä joka mahdollistaa tiedon siirtämisen paikasta toiseen. SIP tuleekin olemaan kolmannen sukupolven verkoissa standardimerkinantoprotokolla [4].

SIP:n joustavuus mahdollistaa sen, että SIP-palvelimet ottavat yhteyden ulkopuolisiin paikkatietopalvelimiin (location server) selvittääkseen osapuolten käyttäjätiedot ja viestien reititysjärjestyksen [9]. Näin ollen SIP ei sido käyttäjää vain yhteen järjestelmään käyttäjiä paikannettaessa.

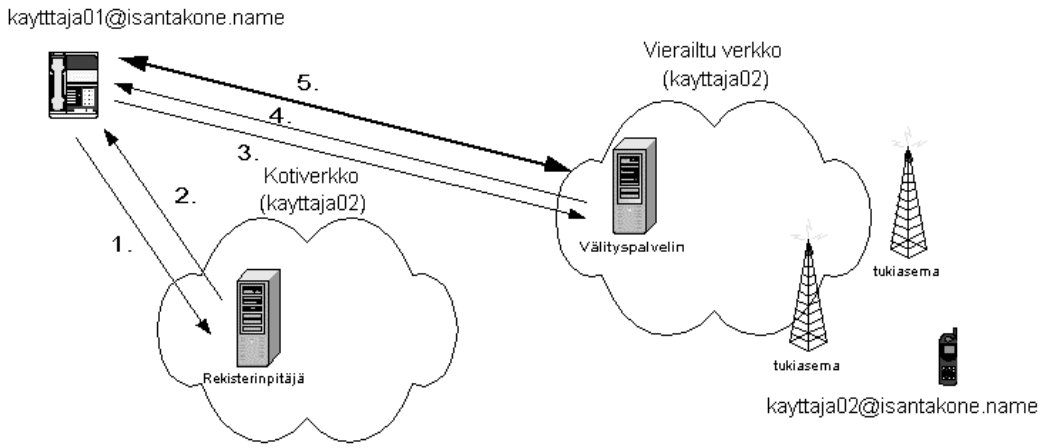
Mobiilissa verkossa rekisterinpitäjää voidaan käyttää paikallistamispalveluissa, joten käyttäjäagentit eivät tarvitse staattisia IP –osoitteita ja näin ollen SIP toteuttaa eräänlaisen sisäänrakennetun mobiliteettituen. SIP siis mahdollistaa henkilökohtaisen liikkuvuuden tarjoamalla mahdollisuuden tavoittaa käyttäjä yhdestä paikasta käyttäjän SIP-osoitteen avulla.

2.5.1 SIP-osoitteet

Käyttäjä on siis tavoitettavissa yhden osoitteen kautta huolimatta siitä, mistä hän kyseisellä hetkellä on verkkoon liittyneenä. Puhelun tai muun session osapuolten SIP-osoitteet (URL:it) ovat sähköpostiosoitteen tyyppisiä, muotoa käyttäjä@isäntäkone, esimerkkinä "sip:kayttäja@palvelin.domain.net". SIP-osoitteena voivat toimia myös E.164 -puhelinnumerot tyyliin ”sip:+358504657698”. Puhelinnumeroiden liittäminen SIP–osoitteisiin tapahtuu joko käyttäjäagentin tai välityspalvelimen toimesta [4].

2.5.2 Liikkuvuuden hallinta

Mobiilissa verkkoympäristössä vierailevan asiakkaan laite (UE) lähettää SIP-sanomansa aina vierailtavan verkon välityspalvelimen kautta (Proxy-Call State Control Function, P-CSCF), joka toimii käytännössä tavallisen SIP -välityspalvelimen tavoin [4]. Serving CSCF eli rekisterinpitäjä on aina sijoitettu käyttäjän kotiverkkoon ja käyttäjään siis otetaan yhteyttä aina kotiverkon kautta eli liikkuvuus hallitaan samaan tapaan kuin esimerkiksi GSM-verkoissa. Kuvassa 4 on esitetty SIP -sanomien toimittaminen toisessa verkossa vierailevalle käyttäjälle.



Kuva 4 Käyttäjän liikkuvuuden hallinta SIP –protokollan osalta

SIP-protokollan reaaliaikainen liikkuvuuden hallinta (handover) on toteutettu siten, että käyttäjän vaihtaessa aliverkkoa (verkko-osoitetta) lähetetään INVITE –metodi sekä rekisterinpitäjälle että käynnissä olevan istunnon vastapuolelle [5]. Lisäksi liikkuvuuden hallinnassa esimerkiksi mobiiliverkkojen osalta auttaa P-CSCF –palvelin, joka tarjoaa liikkuvuuden hallinnan omassa aliverkossaan ja näin mahdollistetaan esimerkiksi tukiasemien vaihdot 3G-verkossa yhteyden katkeamatta.

Mobiiliverkoissa SIP -protokollan on tarpeellista hallita liikkuvuutta vain tietylle välityspalvelintasolle, jonka jälkeen viestin toimittaminen perille on verkon tehtävä. Näin ollen riittää kun rekisterinpitäjä pystyy ohjaamaan 3G-verkossa olevan käyttäjän SIP-viestin kyseisen verkon välityspalvelimelle, jonka tehtävänä on välittää viestit edelleen oikeaan osoitteeseen 3G-verkon sisällä.

2.5.3 Mobiliteetin ongelmat

SIP:n suurimpana ongelmana langattomassa verkkoympäristössä on se, ettei protokolla ole tarpeeksi kompakti [4]. Ilmarajapinnan ylitse tapahtuvassa viestinnässä on erittäin tärkeää, että koko käytössä oleva siirtokaista käytetään mahdollisimman tehokkaasti hyödyksi ja näin ollen väljäotsikkoista SIP-protokollaa on pakattava, jotta viestit pystytään siirtämään tehokkaasti ilmarajapinnan ylitse.

SIP on suunniteltu olemaan yleinen protokolla, joten laajennuksia ja lisämäärittelyjä on jouduttu tekemään runsaasti ja tehdään lisää koko ajan. Lisämäärittelyjä tarvitaan yhteentoimivuuden (interoperability) varmistamiseksi, mutta näiden lisämäärittelyjen avulla voidaan myös parantaa SIP:n käytettävyyttä ja laajentaa palvelutarjontaa mobiiliverkoissa.

2.5.4 Pikaviestintä- ja läsnäolopalvelut

Sessioiden muodostamisen lisäksi SIP-tekniikka tarjoaa myös muun tyyppisiä palveluja. Näistä merkittävimpiä ovat standardin laajennuksessa [7] määritellyt pikaviestintä- ja läsnäolopalvelut (Instant Messaging and Presence) eli IM/P –palvelut. IM/P –palvelut sopivat hyvin SIP-protokollaan, sillä rekisterinpitäjällä on jo suoraan käytettävissään tieto käyttäjän toiminnan tilasta.

Instant Messaging eli pikaviestintä tarkoittaa reaaliaikaista viestintää osapuolten välillä. Message-metodi kuljettaa viestirungossaan viestiä, joka voi olla muodoltaan HTML-tyyppinen, puhdas teksti tai jotakin muuta. Pikaviestipalvelua varten SIP-sanomaan ei tarvita erikseen uutta otsikkokenttää, vaan sanoman viestirungon tyypin avulla voidaan välittää tarvittava tieto viestin sisällöstä. Pikaviesti voidaan lähettää myös ilman SIP:n perusistunnonmuodostusta välittämällä viestit erillisinä SIP-sanomina käyttäjien välillä [4].

Presence- eli läsnäolopalvelu välittää käyttäjän kommunikaatiotilan eli läsnäolon tiedot ja muutokset sekä yhteyden laadun. Tiedot tilataan Subscribe-metodilla ja palvelin lähettää ne Notify-metodilla. Notify-metodia käytetään myös silloin, kun käyttäjä viestittää oman tilansa muutoksista läsnäolopalvelimelle. Läsnäolopalvelun avulla käyttäjä voi viestittää käyttämänsä yhteyden laadusta liikkuessaan erilaisissa mobiiliverkkoympäristöissä, jolloin käyttäjälle suunnattujen viestien lähetys pystytään optimoimaan käyttäjän senhetkisen yhteyden mukaan.

2.6 SIP:n edut

Etuina äänen kuljettamisessa IP:n päällä on pienentyneet kustannukset sekä uudet ja entistä laajemmat palvelut, joista sekä operaattorit että asiakkaat ovat kiinnostuneita. Näin ollen varsinkin IP-verkoissa toimivat tekniikat, joissa pystytään yhdistämään erilaiset kommunikointitavat ja jotka soveltuvat mobiiliin käyttöympäristöön tulevat kasvattamaan suosiotaan.

SIP on avoin standardi ja on näin ollen laajennettavissa uusien tarpeiden mukaiseksi. Laajennuksia on helppo tehdä uusia metodeja määrittelemällä. Laajennettavuutensa ansiosta SIP soveltuu hyvin muuhunkin kuin

perusmerkinantoon: pikaviestintä ja läsnäolopalvelut ovat esimerkkeinä SIP:n tarjoamista uusista palveluista.

SIP tukee liikkuvuuden hallintaa osoitteistonsa sekä modulaarisen verkkorakenteensa avulla. Lisäksi SIP:n etuna on myös sen joustavuus: SIP-protokollalle ei ole kiinteästi määritelty sen vaatimaa kuljetusprotokollaa eikä SIP-viestin sanoman sisältöä ole sidottu mihinkään tiettyyn tyyppiin. Näin ollen SIP on helppo implementoida kompleksisia järjestelmiä rakennettaessa.

2.7 SIP tulevaisuudessa

Tulevaisuudessa kaikki kiinteät ja mobiiliverkot tulevat perustumaan Internet-teknologialle [4]. SIP-protokolla on vahvasti mukana tulevaisuuden verkoissa monestakin syystä, eikä vähäisimpänä niistä ole protokollan saumaton yhteensopivuus muiden Internet-protokollien kanssa tai sen laajennetavuus lukuisiin käyttötarkoituksiin.

Tulevaisuuden mobiilissa verkkoympäristössä SIP-protokollan käytettävyyttä lisää myös se, että SIP-tekniikkaan pystytään liittämään myös riittävät QoS -toiminnot. SIP:n avulla toteuttettavien palvelujen priorisoinnin avulla voidaan taata riittävän tehokas liikennöinti tulevaisuuden verkoissa [2].

Yksi vahva SIP -sovellus tulee olemaan erilaiset multicast-lähetyksiin liittyvät palvelut. Multicastin avulla voidaan järjestää vaikkapa neuvottelupuhelutyyppisiä tapahtumia suurellekin osanottajamäärälle nopeasti kuluttamatta kuitenkaan liikaa verkon resursseja. SIP-protokollan skaalautuvuuden ansiosta näiden sessioiden merkinanto pystytään hoitamaan tehokkaasti.

Ongelmia ja puutteitakin SIP:ssä vielä on. Reaaliaikaisuuskysymys odottaa ratkaisuaan muiden IP-pohjaisten tekniikoiden tavoin myös SIP:ssä eikä ilmarajapinnan käytön tehostamista ole pystytty toteuttamaan. Monia muitakin teknisiä käytäntöjä, kuten laskutusta, tulee vielä kehittää. SIP on kuitenkin perusrakenteeltaan toimiva ja sen monipuolisia ominaisuuksia tullaan varmasti kehittämään sekä hyödyntämään tulevaisuuden verkkoratkaisuissa.

2.8 Lyhenteet

IM/P	Instant Messaging / Presence
IPSec	IP Security
MIME	Multi-Purpose Internet Mail Extensions
P-CSCF	Proxy-Call State Control Function
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
S-CSCF	Serving Call State Control Function
SIP	Session Initiation Protocol

S/MIME	Secure Multi-Purpose Mail Extensions
TCP	Transmission Control Protocol
TLC	Transport Layer Security
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
VoIP	Voice over IP

2.9 Lähteet

[1] Trillium, IP Telephony Solutions, SIP Solutions -esite

[2] Worldcom, SIP Overview -konferenssikalvot

[3] Oja, S., Nokia, Session Initiation Protocol (SIP) -kalvosarja

[4] Nokia, MITA Mobile Internet Architecture, Edita Plc, 2001, 392s.

[5] Kaikkonen, J. Erikoistyö: Session Initiation Protocol [viitattu 27.2.2002] URL: http://keskus.hut.fi/julkaisut/tyot/erikoistyot/VoIP/42890J.pdf

[6] IETF RFC 2543, Session Initiation Protocol URL: ftp://ftp.funet.fi/rfc/rfc2543.txt

[7] IETF Internet Draft, Common Presence and Instant Message URL: http://search.ietf.org/internet-drafts/draft-ietf-impp-cpim-msgfmt-06.txt

[8] Dynamicsoft, White Paper over Session Initiation Protocol

[9] Radvision, Overview Session Initiation Protocol –konferenssipaperi, URL: www.radvision.com

3. PALVELUN LAATU MOBIILISSA INTERNETISSÄ

Internet suunniteltiin organisaatioiden väliseen luotettavaan tiedonsiirtoon. Internet alkoi kuitenkin kehittyä kaupalliseksi verkoksi, jonka käyttäjämäärä on kasvanut paljon suuremmaksi kuin osattiin alun perin odottaa.

Nyt Internet on siirtymässä myös mobiiliverkkoihin. Tämän lisäksi kehityksen suunta on ollut se, että kaikki tieto haluttaisiin siirtää IP:n päällä.

Internetin kehitys ja mobiiliverkkojen rajalliset resurssit ovat luoneet kasvavia paineita tehokkaiden palvelun laatumekanismien kehittämiselle. Sekä protokollia että reititystä on kehitettävä.

Tämän hetken verkoissa toimii ”paras yritys” -palvelun laatu. Tilanne on kuitenkin muuttumassa kolmannen sukupolven matkapuhelinverkkojen myötä.

UMTS-verkko aiotaan kehittää toimimaan kokonaan IP:n päällä release 5:ssä. Palvelun laatuvaatimukset ovat siis todella kovat ja laatu aiotaan saavuttaa mahdollisesti käyttämällä MPLS:ää ja DiffServiä.

3.1 Johdanto

Alun perin Internet kehitettiin datan siirtämiseen. Palvelua kehitettiin siis datasiirrolle sopivaksi. Oleellinen tekijä datasiirron palvelun laadussa oli datan kulkeminen perille täsmälleen oikeana. Eli Internet suunniteltiin siten, että tieto saadaan siirrettyä erilaisten verkkojen yli ja jokainen datagrammi saadaan vastaanotettua muuttumattomana.

Nykyään Internet on toisenlainen kuin alun perin osattiin odottaa. Internetin kaupallinen käyttö on lisääntynyt valtavasti. Käyttäjämäärä on kasvanut suuremmaksi kuin alussa osattiin odottaa.

Dataliikenteen määrä on kasvanut todella nopeasti. Kiinteässä verkossa puheliikenne on jäämässä pienemmäksi kuin dataliikenne. Myös langattomissa puhelinverkoissa dataliikenteen määrän odotetaan kehittyvän samansuuntaisesti kuin kiinteässä verkossa. Liikennemäärien kehitys on luonut paineita kaiken liikenteen siirtämiseen pakettikytkentäisenä.

Alussa IP-verkot olivat ainoastaan datasiirtoa varten, mutta nyt IP.n päällä haluttaisiin kuljettaa kaikenlaista liikennettä. Perinteisen datasiirron vaatimaton best effort -palvelun laatu ei enää riitä uusille sovelluksille, vaan nyt haluttaisiin saada IP-yhteyksiä joilla on taattu minimisiirtokaista, pieni viive ja minimaalinen viiveen vaihtelu. Nykyään haluttaisiin käyttää reaaliaikapalveluja, jotka toimivat IP:n päällä.

Tämä kehitys on ollut selvästi nähtävissä kiinteässä verkossa, jossa voi esimerkiksi jo nyt soittaa edullisia VoIP-tekniikkaa hyödyntäviä

ulkomaanpuheluita. Kiinteässä verkossa tapahtuva kehitys on siirtymässä mobiilin Internetin myötä myös matkapuhelinverkkoihin.

3.2 Mitä tarkoitetaan palvelun laadulla

Palvelun laadusta käytetään usein nimitystä QoS eli quality of service. Tämän lisäksi käytetään myös termiä GoS eli grade of service. Nämä molemmat tarkoittavat palvelun laatua, mutta QoS on näistä laajempi termi.

Grade of service tarkoittaa palvelun laatua käyttäjän näkökulmasta, eli sitä millaisena käyttäjä kokee palvelun laadun. Käyttäjän kokemaan palvelun laatuun kuuluu myös yhteyksillä mahdollisesti esiintyvä esto.

QoS tarkoittaa palvelun laatua jo muodostetulla yhteydellä. QoS:ssä tarkastellaan palvelun laatua käyttäjän, sovelluksen ja verkon näkökulmasta. Käyttäjää kiinnostavia asioita ovat esimerkiksi yhteyden häiriöttömyys, äänen tai kuvan laatu ja yhteyden tasalaatuisuus. Sovelluksen kannalta palvelun laadussa on tärkeää se, että datasiirto on niin sujuvaa ja virheetöntä että sovellus pystyy toimimaan. Verkon kannalta palvelun laatua tarkasteltaessa tärkeitä asioita ovat esimerkiksi pakettien viive, viiveen vaihtelu, pakettihukka ja verkon läpäisy.

3.3 Millaista laatua palveluille halutaan

Eri palveluiden laatuvaatimukset eroavat merkittävästi toisistaan. Esimerkiksi sähköpostissa jokaisen bitin on mentävä oikein perille, ja hukkuneet paketit on lähetettävä uudelleen, mutta toisaalta sähköpostin siirrossa IP-pakettien viiveellä ei ole suurta merkitystä. Reaaliaikaisissa palveluissa puolestaan ei ole kovin kriittistä vaikka joitakin paketteja häviäisi matkalla. [1]

Reaaliaikaisillakin sovelluksilla on erilaisia palvelun laatuvaatimuksia. Laatuvaatimuksiin vaikuttaa eniten se, onko sovelluksessa tarkoituksena molempien osapuolien kommunikoida keskenään vai lähettääkö toinen vain dataa toiselle. Esimerkiksi VoIP-puhelussa viive ja viiveen vaihtelu ovat erittäin kriittisiä tekijöitä, kun taas streaming-palvelussa viive on vähemmän kriittinen tekijä. Streamingissä vastaanottaja voi saada palvelun useidenkin sekuntien viiveellä ilman, että viive haittaa vastaanottajaa. [1]

Reaaliaikapalveluista VoIP-puheluilla ja videoneuvotteluilla on kaikkein tiukimmat palvelun laatuvaatimukset. Kolmannen sukupolven UMTS release 5 -verkoissa on tarkoituksena olla mahdollisuus siirtää kaikki tieto IP:n päällä, siis myös puhelut. Tästä syystä on mielenkiintoista tarkastella hieman tarkemmin VoIP-puheluiden vaatimia palvelun laatuvaatimuksia.

3.3.1 VoIP:n vaatima palvelun laatu

Puhelun laatu jaetaan kahteen osaan, puhelun muodostamisen laatuun ja puhelun laatuun. Puhelun muodostamisen laatu koostuu pääasiassa puhelunmuodostusviiveestä. Puhelun laatu koostuu puheen viiveestä ja viiveen vaihtelusta sekä äänen laadusta. [2]

Puhelun viiveen ollessa alle 150 ms tilaajien välinen kommunikointi on tehokasta, eikä viive haittaa. Viiveen ollessa 200 – 400 ms, tilaajien välinen kommunikointi on hieman heikentynyt, mutta tällainen viive on vielä hyväksyttävä. Kun viive on yli 400 ms, puhelinkeskustelu on hankalaa ja viive häiritsevä. Puhelinliikenteessä viiveen pitäisi pysyä lisäksi mahdollisimman lähellä vakiota. [2]

Tiukkojen viivevaatimusten lisäksi puhelu pitää välittää luotettavasti ja taata puhelulle riittävä siirtokaista. Pakettihukan olisi pysyttävä pienenä, mieluiten muutamassa prosentissa.

Verkko, laitteisto, ohjelmat päätelaitteissa ja puhekoodekit vaikuttavat äänen laatuun ja siihen kuinka suuri pakettihukka on hyväksyttävää. Microsoftin NetMeeting ja Selsius/Cisco IP Phone liitettynä 10 Mbit/s Ethernet-verkkoon ovat testeissä pitäneet äänen laadun kohtuullisena jopa 20 prosentin pakettihukalla [3]. Kuitenkin on otettava huomioon, ettei edes kolmannen sukupolven matkapuhelinverkoissa ole puheluille käytettävissä kovin suuria tiedonsiirtonopeuksia.

Myöskään kutsuesto ei saa ylittää sallittuja arvoja. Tällä hetkellä suurin sallittu kutsuesto määritellään telehallintokeskuksen voimassa olevan määräyksen mukaan seuraavasti [4]:

”Kansallisessa verkossa asiakkaan kokema verkon aiheuttama estyneiden puheluyritysten osuus saa olla enintään 2,5 % vuoden kaikista puheluyrityksistä. Erikoistilanteet, kuten puhelinäänestykset, kilpailut tms. eivät saa häiritä televerkon muuta toimintaa. Kaikissa tilanteissa on turvattava hätäliikenneyhteydet.

Keskusten välisen tai keskusten ja keskittimien välisten väylien nimellisesto saa olla enintään 1 %.

Yleisen valintaisen puhelin/ISDN-verkon yleiseen matkaviestinverkkoon tai yleiseen dataverkkoon yhdistävän väylän nimellisesto saa olla korkeintaan 1 %.”

3.4 Palvelun laatu tämän hetken verkoissa

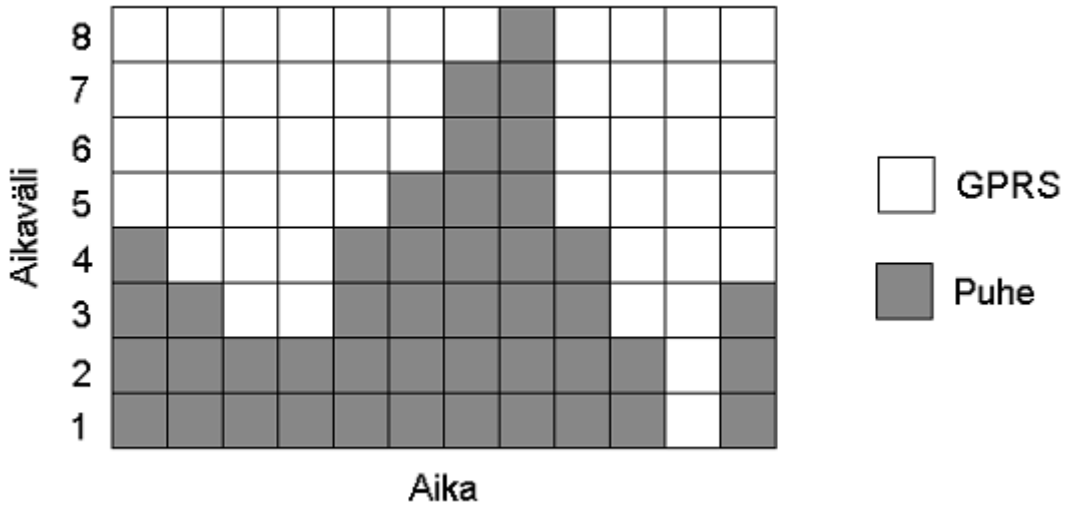
Tällä hetkellä Internet perustuu niin sanottuun ”best effort” eli ”paras yritys” –palvelun laatuun. Tämä tarkoittaa käytännössä sitä, että verkko tekee parhaansa paketin välittämiseksi, mutta ei takaa mitään. Kuitenkin esimerkiksi GPRS-verkoon on määritelty palvelun laatuparametrejä.

GPRS release 1998:ssa ja 1999:ssä on määritelty seuraavat palvelun laatumääreet: Järjestys, viive, luotettavuus, huippunopeus ja keskimääräinen siirtonopeus. Järjestys tarkoittaa pakettien reititysprioriteetteja, joita on kolme. Luotettavuus käsittää todennäköisyydet pakettihukalle, pakettien kahdentumiselle, pakettien järjestyksen muuttumiselle ja pakettien vikaantumiselle. Luotettavuusluokkia on kolme. Viiveluokkia on neljä, joista viimeinen on paras yritys -luokka. Huippunopeus ja keskimääräinen nopeus määrittävät yhteyden nopeutta. [5]

GPRS on suunniteltu välittämään ei reaaliaikaista dataliikennettä. Jos palvelulla on tiukat viivevatimukset ja tasainen siirtokaistan tarve, niin

silloin ei voida käyttää GPRS:n pakettikytkentäistä liikennettä vaan pitää käyttää piirikytkentäistä liikennettä [6].

Käytännössä tämän hetken GPRS-verkossa datasiirto toimii siten, että piirikytkentäinen puheliikenne priorisoidaan ensimmäiseksi ja dataliikenne käyttää jäljellejäävää siirtokaistaa. On mahdollista, että välillä dataliikenteelle ei jää ollenkaan siirtokaistaa, mutta datayhteys säilyy kuitenkin. Seuraava kuva havainnollistaa liikennettä GPRS-verkossa. [7]



Kuva 1. Puheliikenteen kuorman vaihtelu vaikuttaa GPRS:n suorituskykyyn [7]

Tämän hetken matkapuhelinverkoissa mobiilin Internetin palvelun laatu ei ole kovin hyvä. Siirtonopeudet ovat luokkaa parikymmentä kilobittiä sekunnissa. Viiveet ja vasteajat ovat vielä suuria GPRS-verkossa. GPRS tarjoaa kuitenkin mahdollisuuden käyttää toimivaa mobiilia Internettiä.

3.5 Palvelun laatu 3G-verkossa

Kolmannen sukupolven matkapuhelinverkoissa aiotaan tulevaisuudessa kuljettaa kaikki liikenne IP:n päällä. Tämä suunnitelma vaatii taakseen toimivan ja kattavan palvelun laatuarkkitehtuurin. Seuraavassa käsitellään hieman tarkemmin UMTS:n palveluluokkia ja laatuarkkitehtuuria.

3.5.1 UMTS:n palvelun laatuluokat [8]

UMTS:ään on määritelty neljä varsinaista palvelun laatuluokkaa. Nämä luokat ovat conversational, streaming, interactive ja background eli puhe, streaming, vuorovaikutteinen ja taustaluokka.

Puheluokassa on tarkoitus siirtää kaikki puhelut. Tässä luokassa on kaikkein tiukimmat vaatimukset viiveelle ja viiveen vaihtelulle. UMTS:n kuljetuspalvelussa puheluokalle on asetettu viivevaatimus 100 ms:sta ylöspäin. Tavoite viiveelle on 100 ms. Seuraavassa palvelun laatuluokassa eli streamingissä viive on 250 ms:sta ylöspäin.

Streaming-luokassa siirretään esimerkiksi videokuvaa, ääntä tai musiikkia. Siirto tapahtuu yksisuuntaisena streaminginä, joten viivevaatimukset eivät ole kovin tiukkoja tässä luokassa. Lähetyksen laadun takaamiseksi viiveen vaihtelu on streaming-luokassa rajoitettu. Viiveen vaihtelun raja ei kuitenkaan ole aivan yhtä tiukka kuin puheluokassa.

Vuorovaikutteisesta luokkaa käytetään, kun joko ihminen tai kone hakee tietoa toiselta koneelta. Tällaista käyttöä on esimerkiksi Internet-sivujen lataaminen. Vuorovaikutteisen luokan tärkeimmät laatutekijät ovat kiertokulkuviive ja läpinäkyvä tiedonsiirto.

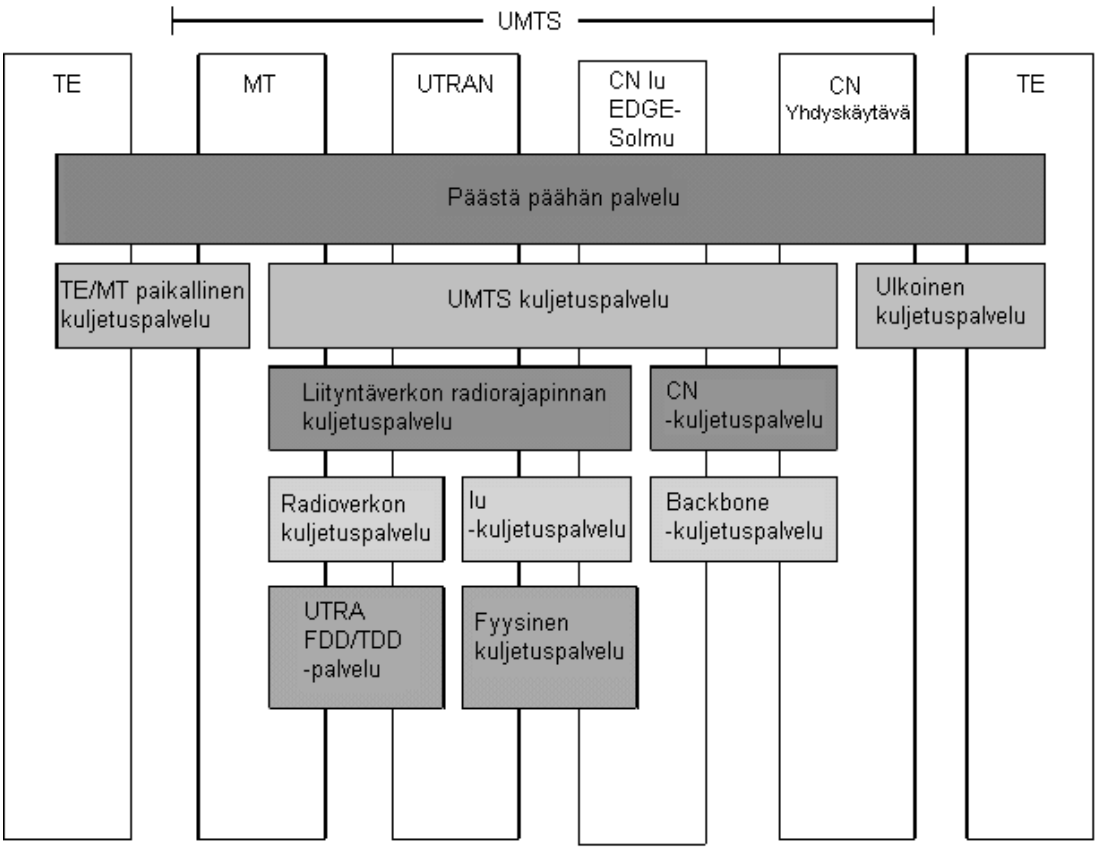
Taustaluokka tarjoaa mahdollisuuden siirtää tietoa taustalla päätelaitteelle. Taustaluokkaa voidaan käyttää esimerkiksi sähköpostien tai tekstiviestien vastaanottoon. Toisin sanoen taustaluokkaa käytetään sellaisiin tarkoituksiin, joissa palvelun ei tarvitse olla lainkaan reaaliaikaista, vaan tärkeätä on mahdollisimman virheetön ja läpinäkyvä tiedonsiirto.

3.5.2 UMTS palvelun laatuarkkitehtuuri [8]

Verkkopalveluille halutaan saada taattu päästä-päähän -palvelun laatu. Palvelun laadun pitää kattaa siis koko järjestelmä päätelaitteita myöden, eli kaikki mitä käyttäjärajapintojen välillä on.

Palvelun laadulle annetaan raja-arvot eri palveluluokkiin. Koska laadun kokeminen on subjektiivista ja yksilöllistä, niin jää käyttäjän päätettäväksi, onko hän tyytyväinen saatuun palvelun laatuun.

Seuraavassa kuvassa on esitetty UMTS-verkon palvelun laatuarkkitehtuuri.



Kuva 2. UMTS-verkon palvelun laatuarkkitehtuuri [8]

Kuten kuvasta nähdään, niin UMTS kuljetuspalvelu on ratkaiseva osa palvelun laadu takaamisessa. Varsinainen UMTS palvelun laatuarkkitehtuuri ei vastaa päätelaitteen sisällä tapahtuvasta toiminnasta eli TE – MT rajapinnasta eikä ulkopuolisiin palveluihin kommunikoinnista. Nämä rajapinnat on määriteltävä erikseen. UMTS:n palvelun laatuarkkitehtuuri käsittää radioverkon ja runkoverkon.

Radioverkon kuljetuspalvelu sisältää mekanismit radiorajapinnan tiedonsiirron palvelun laadulle. Radioverkon kuljetuspalvelu käyttää UTRA FDD/TDD -palvelua.

Iu -kuljetuspalvelu tarjoaa palvelun laatua radioverkon ja runkoverkon (CN) väliseen rajapintaan.

Runkoverkon kuljetuspalvelu koostuu kahdesta osasta CN eli core network ja backbone. CN -kuljetuspalvelu käyttää backbone -kuljetuspalvelua, joka toimii OSI-kerroksilla yksi ja kaksi.

3.6 Tekniikat palvelun laadun takaamiseksi

Nokian näkemyksen mukaan kolmannen sukupolven matkapuhelinverkkojen palvelun laatu voitaisiin rakentaa MPLS:n ja DiffServin eli differentiated services varaan. DiffServ tarjoaisi nimensä mukaisesti tavan eriyttää eri palveluja eli antaa erilaisia prioriteetteja eri paketeille. MPLS:ää voidaan käyttää pakettien tehokkaaseen reititykseen

DiffServin kanssa. Näiden tekniikoiden käytön lisäksi tarvitaan mahdollisesti myös muita liikenteenhallintamenetelmiä parantamaan QoS:n tehokkuutta. [1]

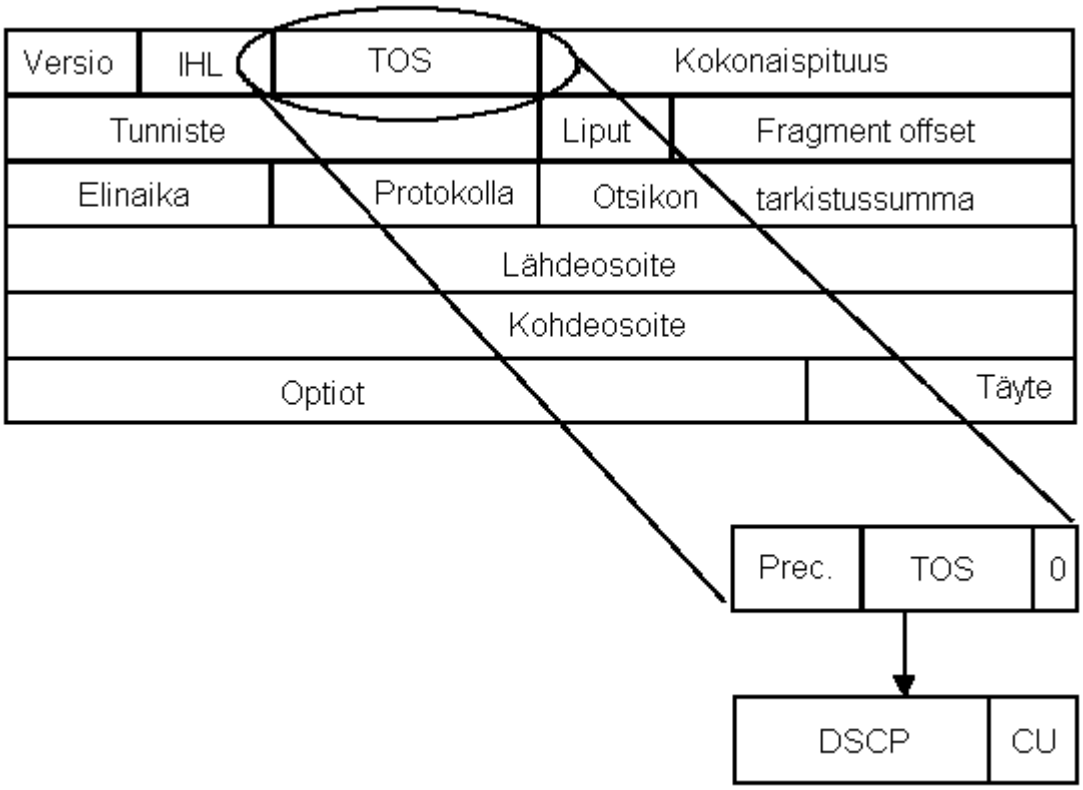
3.6.1 DiffServ

DiffServ eli differentiated services ei varsinaisesti tarjoa palvelun laatua, vaan se tarjoaa mahdollisuuden antaa paketeille erilaisia prioriteetteja. DiffServin avulla paketit voidaan jakaa luokkiin ja antaa luokille erilaisia prioriteetteja.

DiffServ käyttää IPv4 – otsikon TOS eli palvelun tyyppi kenttää, johon se lisää paketin luokkaa koskevan tiedon. DiffServ muuttaa tavallisen palvelun tyyppi –kentän sisällön itselleen sopivampaan muotoon. DiffServin käyttämään TOS-kenttään tulee seuraavat tiedot: DSCP eli differentiated service code point, joka on 6 bittiä ja CU (currently unused) eli ei käytössä [9]. DSCP sisältää siis paketin luokan, joka takaa paketille halutun prioriteetin.

IPv6:ssa DiffServin käyttö on helppoa, koska liikenteen luokkaa käsittelevän oktetin rakennetta ei olla määritelty yhtä tiukasti kuin IPv4:ssä [9]. DiffServ toimii IPv6:n kanssa samaan tapaan kuin IPv4:n kanssa.

Seuraavassa kuvassa on esitetty miten DiffServ käyttää IPv4 otsikkoa.



Kuva 3. DiffServ muokkaa IPv4-otsikon palvelun tyyppi –kenttää [9] [10]

3.6.2 MPLS

Paketin tullessa MPLS:ää käyttävään verkkoon pakettiin lisätään leima. Leimassa voidaan huomioida liikenneluokka, eli leimat tukevat erilaisia palvelun laatuja ja mahdollistavat DiffServin käytön.

MPLS:ää käyttävässä verkossa paketit reititetään leimojen perusteella. Kun pakettiin on lisätty leima, niin IP-osoitteesta ei tarvitse välittää reitityksessä.

Kun paketti saapuu MPLS:ää käyttävän verkon reunalle, niin paketista poistetaan leima. Tämän jälkeen pakettia käsitellään tavallisen IP-paketin tapaan.

MPLS:llä saavutetaan muutamia etuja verrattuna tavalliseen IP-osoitteisiin perustuvaan reititykseen. Leimareitityksen avulla voidaan muodostaa leimapolkuja ja näin saadaan reititettyä liikenneagregaatteja. MPLS tarjoaa myös keinoja liikenteen hallintaan ja mittaamiseen. [1]

Lisäksi MPLS:ää voidaan käyttää ATM:n sijaan. Tämä helpottaa ja yksinkertaistaa pakettien kuljettamista verrattuna ATM:ään, joka kuljetetaan SDH:n päällä, joka kuljetetaan puolestaan WDM:n päällä. Ei siis tarvita raskasta ATM/SDH/WDM-protokollapinoa. [1]

3.7 Yhteenveto

Tällä hetkellä Internetissä palvelun laadun parantaminen perustuu siirtonopeuksien nostamiseen. Tällainen siirtonopeuksien nostaminen ei kuitenkaan ole kovin kestävä ja laadukas ratkaisu tarjota palvelun laatua. Palvelun laadun takaavia järjestelmiä kehitetään jatkuvasti, jotta tämän hetkiseen tilanteeseen saataisiin parannusta.

Monet uudet IP:n päällä kuljetettavat palvelut vaativat tehokkaan järjestelmän, joka takaa palveluille sovitun riittävän laadun. Erityisesti kolmannen sukupolven matkapuhelinverkoissa, joissa aiotaan siirtää kaikki tieto IP:n päällä, tarvitaan nopeasti hyvä QoS-järjestelmä. Matkapuhelinverkossa palvelun laadun takaava järjestelmä on erityisesti tarpeen, koska radioverkon resurssit ovat hyvin rajalliset.

Tämän hetken GPRS-verkosta täysin IP-pohjaiseen UMTS-verkkoon siirryttäessä palvelun laadun täytyy kehittyä todella paljon. Nokian näkemyksen mukaan haluttu palvelun laatu aiotaan saavuttaa käyttämällä MPLS:ää ja DiffServiä sekä mahdollisesti näiden tukena muita liikenteen ja siirtokaistan hallintaa parantavia menetelmiä. Parhaiten nämä järjestelmät toimisivat IPv6:n kanssa.

3.8 Lyhenteet

ATM	Asynchronous Transfer Mode
CN	Core Network
EDGE	Enhanced Data GSM Environment
FDD	Frequency Division Duplex
GoS	Grade of Service

GPRS	General Packet Radio Services
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MPLS	Multiprotocol Label Switching
MT	Mobile Terminal
OSI	Open Systems Interconnection
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
TDD	Time Division Duplex
TE	Terminal Equipment
TOS	Type of service
UMTS	Universal Mobile Telecommunication System
UTRA	UMTS Terrestrial Radio Access
UTRAN	UMTS Terrestrial Radio Access Network
VoIP	Voice over IP
WDM	Wave Division Multiplexing

3.9 Lähdeluettelo

[1] Jyrki Kivimäki (editor). 2001. MITA Mobile Internet Technical Architecture. Suomi. Edita. 391 s. ISBN 951-826-499-6

[2] Anon. 1999. Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS). France. ETSI. ETSI TR 101 329 V2.1.1 (1999-06). 37 pgs.

[3] Raimo Kantola (editor). 2001. IP Telephony protocols, architectures and issues. Espoo. Otamedia Oy. Report 2/2001. 115 pgs. ISBN 951-22-5452-2

[4] THK 29 A/1997 M. 1997. Määräys TELEVERKKOJEN SUORITUSKYVYSTÄ. Telehallintokeskus. 3 s.

[5] QoS in GPRS. http://www.ub.utwente.nl/webdocs/ctit/1/00000039.pdf

[6] 1999. Student Text GPRS System Survey. Stockholm. Ericsson Radio Systems AB. 86 s. EN/LZT 123 5374 R1B.

[7] Mika Saren. 2001. Early performance experiences with GPRS. The Evolution to All-IP Mobile Networks, London, 21. – 23.5.2001. London. IBC Global Conferences Mortimer House.

[8] 3GPP TS 23.107 V5.3.0. 2002. 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; QoS Concept and Architecture (Release 5). 3GPP. 39 s.

[9] RFC 2873. 2000. TCP Processing of the IPv4 Precedence Field. IETF. 7 s.

[10] RFC 791. 1981. INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION. IETF. 44 s.

4. AD HOC -VERKOT

Viime vuosina langaton viestintä on kasvattanut huimasti suosiotaan. Langattomien palvelujen voimakkaasti kasvava kehitys on poikinut muun muassa Mobile IP –protokollan, joka tuo joitain ratkaisuja langattoman viestinnän toteuttamiseen.

Siirtonopeuksien nopea kasvu langattomassa viestinnässä mahdollistaa aivan uudenlaisten palvelujen ja verkkoarkkitehtuurien kehittämisen. Toisaalta on myös olemassa kysyntää uudenlaiselle tekniikalle, joka yhdistäisi olemassa olevat teknologiat siten, että liikkuva käyttäjä voisi siirtyä verkosta toiseen saumattomasti ja joustavasti. Matkapuhelinverkkojen välillähän tällainen liikkuvuuden tuki on jo samaa standardia käyttävissä verkoissa tehokkaasti toteutunut.

Aivan uudenlaista tietoverkkoarkkitehtuuria edustaa rakenteeton ad hoc –verkko, jossa ei ole selkeää verkkoinfrastruktuuria, kuten perinteisessä tietoverkossa.

4.1 Johdanto

Ad hoc –verkkojen perusidea ei ole oikeastaan mitenkään uusi. Jo 70-luvulla kehiteltiin verkkoa, jossa kukin verkon solmu edusti yhtä itsenäistä päätelaitetta. Alun perin tätä tekniikkaa kehitettiin sotilastarkoituksiin, jonka tehtävänä oli mahdollistaa kommunikointi taistelukentällä. [1]. Vielä nykyäänkin sotilaalliset tarkoitukset ovat ad hoc –verkkojen yksi käyttötarkoitus, mutta sille on keksitty myös paljon uusia sovelluskohteita siviilimaailmasta.

Ad hoc –verkkoja voitaisiin hyödyntää tietojen välittämiseen mobiilissa ympäristössä. Sillä voitaisiin myös korvata tai toisaalta laajentaa olemassa olevaa solupohjaista mobiiliverkkoa. Ad hoc –verkot soveltuvat hyvin myös tapauksiin, joissa täytyy nopeasti pystyttää verkko tiedonsiirtoa varten. Tällaisia tilanteita ovat esimerkiksi konferenssitilanteet, jossa konferenssiin osallistujat haluavat siirtää tietoa päätelaitteidensa välillä langattomasti.

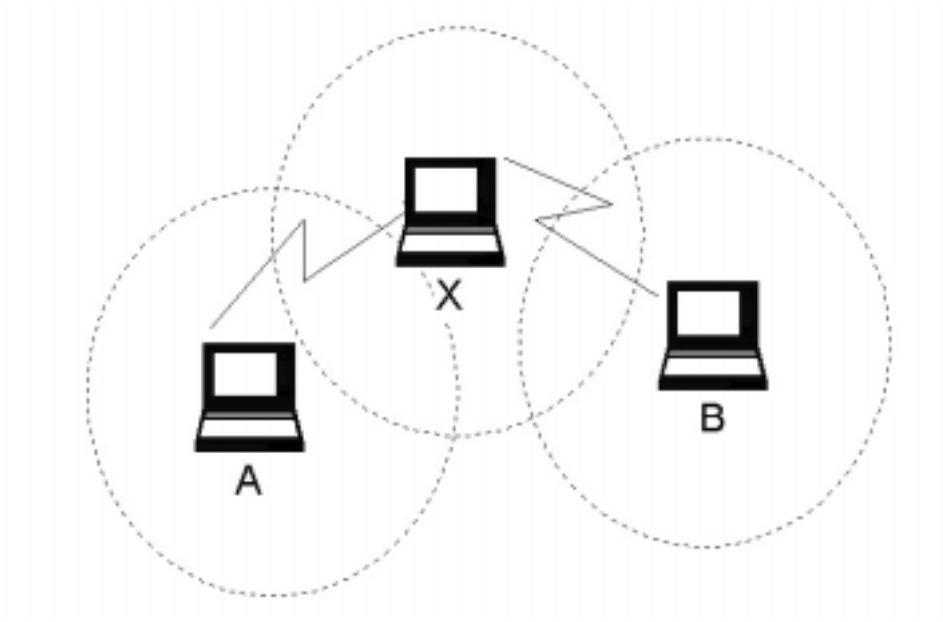
Ad hoc –verkkojen protokollakehityksestä vastaa lähinnä IETF:n MANET–työryhmä (Internet Engineering Task Force Mobile Ad-hoc Networks - workgroup), jonka tehtävänä on evaluoida ja kehittää olemassa olevia ehdotuksia kohti maailmanlaajuista standardia. Protokollakehityksessä tärkeimmässä asemassa on reititysprotokollat ja tästä syystä ad hoc –reititysprotokollia kutsutaan toisinaan MANET- protokolliksi [2].

4.2 Ad hoc –verkon rakenne

Ad hoc –verkko on rakenteeton verkko, joka koostuu langattomista, siirrettävistä päätelaitteista, jotka voivat keskustella keskenään. Rakenteettomuudella tarkoitetaan arkkitehtuuria, jossa kommunikoivia

laitteita syntyy ja katoaa verkossa jatkuvasti. Tällaisessa verkossa ei siis ole mitään kiinteää rakennetta, vaan verkko “elää” koko ajan. Ad hoc –verkoissa ei myöskään ole tukiasemia tai palveluntarjoajia, jotka tarjoavat tiedonsiirtopalvelut. Jokainen laite ad hoc –verkossa toimii tarvittaessa paitsi päätelaitteena niin myös liikenteen reitittäjänä. Reitittimenä päätelaite toimii esimerkiksi silloin kun kaksi laitetta haluaa keskustella keskenään, mutta ovat toistensa kantaman ulkopuolella. Kyseisessä tilanteessa näiden kahden laitteen välissä olevat päätelaitteet reitittävät liikenteen perille. Ad hoc –verkoissa ei siis voi tehdä jakoa päätelaitteisiin ja reitittimiin kuten perinteisessä lankaverkossa. Päätelaite ad hoc –verkossa voi olla esimerkiksi kannettava tietokone, älypuhelin tai PDA-laite. [3]

Kuvassa 1 esitetään tilanne, jossa laite A haluaa kommunikoida laitteen B kanssa, joka on laitteen A kantaman ulkopuolella. Kuvan tapauksessa liikenne reititetään laitteen X kautta. Käytännössä laitteiden A ja B välillä voi olla hyvinkin useita liikennettä reitittäviä laitteita.



Kuva 1. Reititys ad hoc -verkossa

Ad hoc –verkossa toimivien laitteiden tulee itseorganisoitua automaattisesti verkoiksi suurella nopeudella. Ad hoc –verkoissa ei siis ole mitään keskitettyä palvelua, joka hoitaisi laitteiden yhteenliittämisen. Tämä luo ongelmia esimerkiksi luotaessa yhteydenmuodostusalgoritmeja, sillä virrankulutuksen optimointi nousee tärkeäksi tekijäksi. [3]

Vaikka tavoite on kehittää itsenäinen ad hoc –verkko, täytyy se useissa tilanteissa liittää osaksi olemassa olevaa solukkoverkkoa. Tällainen verkko saattaa pohjautua esimerkiksi GPRS –tekniikkaan. Tällöin ongelmaksi tulee valinta milloin päätelaitteen kannattaa kuulua ad hoc –verkkoon ja milloin on parempi hyödyntää solukkoverkon tarjoamia palveluja.

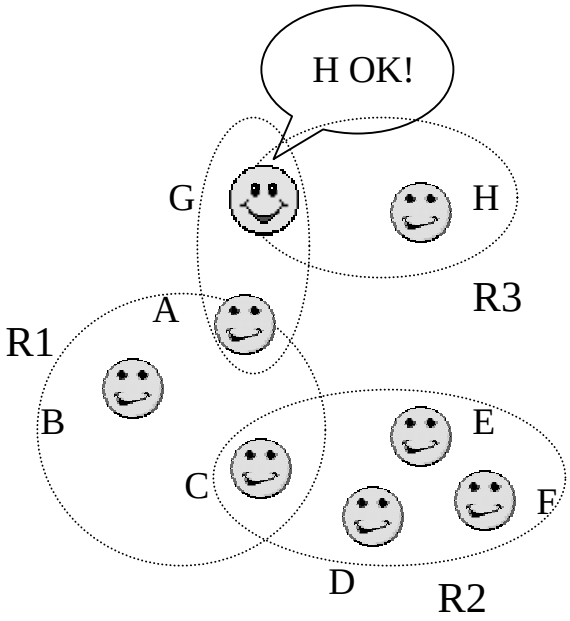
4.3 Tietoturva

Kuten langattomissa tietoverkoissa yleensäkin, on myös ad hoc –verkoissa kiinnitettävä erityistä huomiota tietoturvallisuuteen. Kuinka voidaan olla varmoja, ettei kukaan kuuntele yhteyttä?

Reititysprotokollien tietoturvallisuus perustuu yleensä avaimien levittämiseen ja autentikoimiseen sen avulla. Autentikoiminen tosin aiheuttaa paketinkoon kasvua ja täten hidastuttaa protokollan toimintaa.

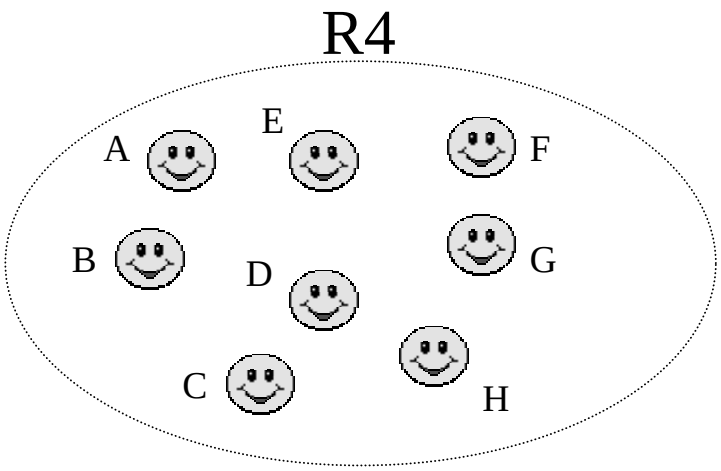
Esimerkiksi Diffie-Hellman avaimensiirtotekniikka auttaa luomaan turvallisen yhteyden kahden päätepisteen välille, mutta on vahingoittuva yhteyden keskeltä tapahtuviin väärinkäytöksiin [5].

Kuvassa 2 on havainnollistettu tilannetta, jossa on kolme eri solmuryhmää R1, R2 ja R3. A toimii tapauksessa palvelinsolmuna, jonka tehtävänä on luottamuksellisten suhteiden delegointi muualle verkkoon. Esimerkiksi kaikki R2:n solmut jakavat epäsuorasti luottamuksellisen suhteen A:han C:n kautta. Solmu A voi kerätä digitaalisesti allekirjoitettuja avaimia esimerkiksi R3:sta solmun G kautta. A viestittää kaikki saamansa allekirjoitetut avaimet muualle verkkoon, jonka seurauksena syntyy ryhmien R1, R2 ja R3 pohjalta uusi luetettujen solmujen ryhmä R4 (Kuva 3) [6].



Kuva 2. Solmu G välittää julkisen avaimen H:lta A:lle

Kunnollisen tietoturvan tuominen ad hoc –verkkoihin on erittäin vaativa tehtävä, ja on täten jopa mahdollista, että ad hoc –verkkojen toimintaa optimoidaan jopa tietoturvallisuuden kustannuksella.



Kuva 3. Solmu A viestittää allekirjoitetut avaimet koko verkkoon, jonka seurauksena syntyy uusi luotettu ryhmä R4

4.4 Palvelut ad hoc -verkossa

Ad hoc –verkossa olisi tarkoitus pystyä siirtämään kaikenlaista pakettipohjaista liikennettä, mitä kolmannen ja neljännen sukupolven tietoverkoissa on tarkoitus siirtää. Tämä käsittää kaikki Internet applikaatiot, mukaan lukien reaaliaikaiset puhe -ja kuvapalvelut.

Jonkinlaisena ad hoc –verkkojen prototyyppitapauksena voisi pitää langatonta konferenssineuvottelua. Tässä tapauksessa tietokoneet kytketään langattomasti toisiinsa kokoustilanteessa, muodostaen pieni ad hoc –verkko, jonka avulla koneet pystyvät kommunikoimaan keskenään.

Toisena ad hoc –verkkojen käyttötarkoituksena voisi ajatella tapausta, jossa alkuperäinen tietoverkko on epäkunnossa tai sellaista ei ole laisinkaan. Tällainen voisi olla tilanne esimerkiksi katastrofitilanteessa, jolloin esimerkiksi luonnonmullistuksen seurauksena alkuperäinen tietoverkko on vahingoittunut käyttökelvottomaan kuntoon. Toisaalta ad hoc –verkot antavat hyvän mahdollisuuden rakentaa verkko paikkaan, johon kaapelointiin perustuvan verkon rakentaminen olisi taloudellisesti kannattamatonta.

Ad hoc –verkkoja voidaan ajatella myös käytettävän esimerkiksi autoissa älykkään tietokonejärjestelmän tietoliikennepalvelujen tarjoajana. Auton oma tietoverkkojärjestelmä voisi tällöin vaikkapa siirtää autossa mukana olevaan kannettavaan tietokoneen tiedon viasta auton jossain järjestelmässä, jonka jälkeen tietokone huolehtisi lähimmän korjaamon etsimisestä.[5]

4.5 Huomioon otettavia tekijöitä ad hoc –verkon suunnittelussa

Ad hoc –verkon solmut käyttävät IP-osoitteita. Mutta koska ad hoc –verkossa ei ole paikallaan pysyvää verkkorakennetta kuten esimerkiksi Internetissä, on IP-osoitteiden jakaminen paljon hankalampaa. Internetissä

voidaan osoitteita jakaa perustuen maantieteelliseen sijaintiin. Samassa verkossa sijaitsevat tietokoneet saavat tälloin saman reititysetuliitteen. Tällöin voidaan reittejä aggregoida esimerkiksi CIDR-protokollan avulla, jolloin reititystaulujen koko ei kasva liian suureksi edes isossakaan verkossa. Ad hoc –verkoissa ei kuitenkaan ole mahdollisuutta aggregoida reittejä ja tämä luo ongelmia suuria verkkoja luotaessa.

4.5.1 Skaalautuvuus

Ad hoc –verkot eivät mahdollista samanlaisia aggregointitekniikoita kuin Internetissä käytetetyt protokollat, joten ad hoc –verkot ovat alttiita skaalautuvuusongelmille. Solmujen määrän kasvaessa verkossa suureksi, voi reititystaulujen koko kasvaa myös kohtuuttomasti. Tämä aiheuttaa ylimääräisen muistikapasiteetin lisäämistä reittien säilyttämiseen. [5]

Ad hoc –verkon solmujen liikkuessa muuttuu myös reititysinformaatio koko ajan. Tällöin täytyy lähettää ohjausviestejä ympäri verkkoa tiedottaen nykyisestä reititystilanteesta. Lisääntynyt ohjausviestien määrä kuormittaa verkkoa ja varsinaisen informaation läpimeno verkossa tällöin heikentyy.

Reititysprotokollia suunniteltaessa pyritäänkin nimenomaan vähentämään ohjausviestien määrää koko liikenteessä. Ohjausliikenteen määrä ei saisi viedä kovinkaan suurta osaa koko olemassa olevasta kaistasta.

4.5.2 Virrankulutus

Ad hoc –verkon laitteet toimivat yleensä akkuenergian avulla. Verkon laitteet saattavat paitsi lähettää tai vastaanottaa, myös reitittää liikennettä. Tämä asettaa kovia vaatimuksia virrankulutukselle, sillä verkon laite on käytännössä tällöin aina aktiivisessa tilassa. Jos laite ei kuitenkaan tee mitään, asetetaan se nukkumistilaan.

Tästä syystä onkin mietitty algoritmeja joiden mukaan esimerkiksi täydellä akulla toimivan laitteen tulisi halukkaammin toimia reitittimenä, kuin laitteen, jonka akku on vähissä.

Korkeampi lähetysteho mahdollistaa suuremman kantaman, mutta toisaalta tällöin kasvaa myös muiden signaalien aiheuttama häiriötaso ja virrankulutus.

Edellä mainituista syistä on välttämätöntä tehdä yhteistyötä elektroniikan tutkijoiden kanssa, jotta virrankulutus päätelaitteissa saataisiin riittävän pienelle tasolle. Toisaalta algoritmien suunnittelussa täytyy miettiä tarkkaan, että ne ovat hyvin optimoituja juuri virrankulutuksen suhteen.[5]

4.5.3 Siirtonopeudet

Siirtonopeus ad hoc –verkoissa tulee jäämään jälkeen langallisista verkoista, kuten yleensäkin langattomista verkoissa on tapana tapahtua. Langattomassa verkossa tapahtuu myös paljon bittivirheitä johtuen siirtotien epäluotettavuudesta kaapelointiin verrattuna. Tästä syystä esimerkiksi TCP-protokollaa ei voida suoraan hyödyntää langattomissa ad hoc –verkoissa. TCP suunniteltiin käsittämään pakettihäviöt merkkinä ruuhkautumisesta. Langattoman verkon tapauksessa ei pakettien hukkuminen välttämättä ole

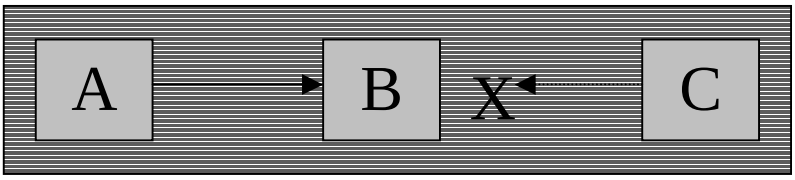
merkki verkon ruuhkautumisesta. Paketteja saattaa hukkua erilaisten ulkoisten häiriöiden johdosta, minkä seurauksena ei ole syytä hidastaa lähetysnopeutta, kuten lankaverkon tapauksessa.

Tällä hetkellä ei kuitenkaan ole standardisoitua korvaajaa TCP:lle ja todennäköisesti ensimmäisissä ad hoc –sovelluksissa tullaan käyttämään juuri TCP-protokollaa [5].

4.5.4 Radiorajapinta

Radio –rajapinta luo monia rajoituksia, jotka täytyy ottaa huomioon langatonta verkkoa luotaessa. Ensinnäkin signaalivoimakkuus laskee vähintäänkin etäisyyden kuutiona. Toisaalta joitain perinteisiä lankalähiverkon protokollia ei voida käyttää. Esimerkiksi Ethernet verkossa olevaa törmäyksen havaitsemisalgoritmia ei voida käyttää, sillä solmu ei pysty yleensä kuuntelemaan samalla kun lähettää.

Myös kaksi päätelaitetta saattaa häiritä kolmatta tietämättään. Tätä sanotaan piilossa olevan päätelaitteen ongelmaksi. Tapaus on havainnollistettu kuvassa 4, jossa A lähettää B:lle, mutta C on A:n kantaman ulkopuolella. Samalla C kuitenkin lähettää B:lle, jolloin tapahtuu törmäys B:ssä. A:n sanotaan tällöin olevan piilossa C:ltä. [1]



Kuva 4. Piilossa olevan päätelaitteen ongelma

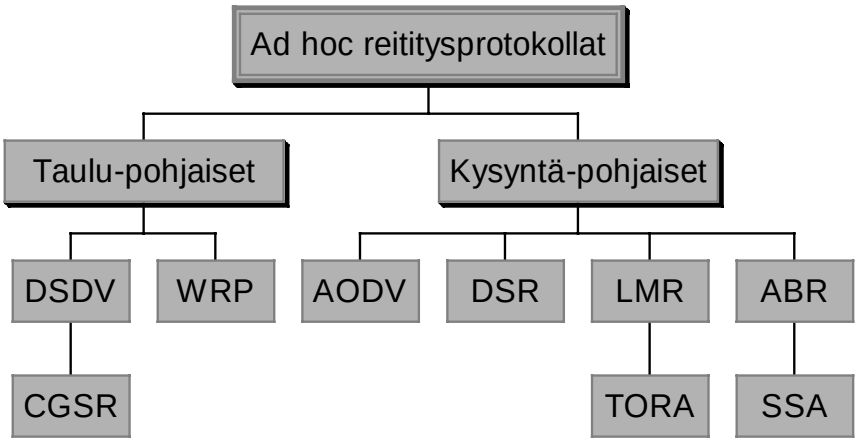
4.5.5 Standardisointi

Jotta ad hoc –verkoista voisi tulla yleisesti käytetty verkkotekniikka, täytyy sitä ennen tapahtua standardisointia, jonka avulla järjestelmän eri osat pystyvät ongelmitta kommunikoimaan keskenään. Ilman riittävää standardisointia käyttäjä voi joutua asentamaan päätelaitteeseensa erinäisiä ohjelmanpätkiä yhteensopivuuden takaamiseksi. Tällainen tilanne ei kuitenkaan ole toivottu ja tapahtuessaan vähentää varmasti loppukäyttäjien määrää.

4.6 Reititys ad hoc -verkossa

Reititys on keskeinen toiminto missä tahansa tietoverkossa. Ad hoc –verkon reititystä suunnitellessa on kaksi ylimääräistä haastetta perinteiseen verkkoon nähden. Perinteisessä verkossa verkkorakenne on jokseenkin muuttumaton. Ad hoc –verkossa verkon rakenne muuttuu koko ajan ja täten myös reititysinformaatio. Toisaalta perinteisessä verkossa tieto reitityksestä voidaan tallentaa erityisiin palveluntarjoajan tarjoamiin solmuihin. Ad hoc –verkoissa ei tällaisia erikoissolmuja ole, jolloin reititystiedon tallentamisesta tulee ongelma.

Reititysprotokollat voidaan jakaa karkeasti kahteen osaan niiden toimintaperiaatteen mukaan. Reititysprotokollien jakautuminen taulu -ja kysyntä-pohjaisiin on esitetty kuvassa 5 [5].



Kuva 5. Reititysprotokollien luokittelu ad hoc -verkossa

4.6.1 Taulu-pohjainen reititys

Taulu-pohjainen reititys on yleisesti käytetty reititysmenetelmä Internetissä. Sen tavoitteena on pitää yllä päivitettyä tietoa reiteistä kaikkien verkon solmujen välillä. Taulupohjaisten reititysprotokollien ongelmana ad hoc –verkossa on sen vaatima suuri signalointiliikenne. Tieto reitityksen muutoksesta täytyy saattaa kaikkiin verkon solmuihin ja tämä aiheuttaa paljon päivitysliikennettä verkossa.

Esimerkkinä taulu-pohjaisesta reititysprotokollasta on WRP (Wireless Routing Protocol). WRP:ssa solmut kommunikoivat toistensa kanssa linkkimuutoksista päivitysviestien avulla. Päivitysviestit lähetetään ainoastaan naapurisoluihin sisältäen listan tarvittavista päivityksistä. Solmut lähettävät myös naapurisolmuilleen “hello” –viestejä tietyn väliajoin, silloin kun solmu ei lähetä muita viestejä. “Hello”-viestien puutosta pidetään merkkinä linkin toimimattomuudesta [6].

4.6.2 Kysyntä-pohjainen reititys

Kysyntä-pohjainen reititys noudattaa aivan toisenlaista strategiaa taulu-pohjaisiin reititysprotokolliin verrattuna. Reititysinformaatio haetaan tällöin vain tarvittaessa. Täydellisiä reititystauluja ei siis ylläpidetä, vaan reitti pyritään etsimään vain siinä vaiheessa kun halutaan lähettää. Solmu lähettää reittipyyntö-viestin verkkoon, jota lähetetään eteenpäin kunnes se saavuttaa kohdesolmun. Kohdesolmu lähettää vastauksen lähettäjälle, jolloin varsinainen tiedonsiirto voidaan aloittaa. [2]

Reitinetsintäalgoritmi aiheuttaa pitkän viiveen ennen kuin varsinaista tietoa voidaan lähettää. Toisaalta muuta prosessointia tai ylimääräistä kommunikointia ei tarvita tämän jälkeen lähettävän ja vastaanottavan solmun välillä.

Esimerkkinä kysyntä-pohjaisesta reititysprotokollasta voidaan mainita AODV (Ad Hoc On-Demand Distance Vector Routing). AODV:n toiminnot voidaan jakaa kolmeen eri osaan: reitin etsintä, reitin ylläpito ja reittitaulun ylläpito. Signalointi hoidetaan AODV:ssa UDP paketteihin pakattuina viesteinä.

Taulukko1. Vertailu kysyntä-pohjaisen ja taulukko-pohjaisen reitityksen välillä [6]

Parametri	Kysyntä-pohjainen	Taulu-pohjainen
Reititysinformaation saatavuus	Saatavilla tarvittaessa	Aina saatavilla riippumatta tarpeesta
Säännöllinen reittien päivitys	Ei tarvita	Tarvitaan
Synnytetyn signalointiliikenteen määrä	Kasvaa aktiivisten solmujen määrän kasvaessa	Enemmän kuin kysyntä-pohjaisessa

4.7 Nykytilanne ja tulevaisuus

Ad hoc –verkkojen parissa käydään tällä hetkellä laajaa tutkimusta. Pääpaino on sopivan reititysprotokollan suunnittelussa, mutta vaaditaan myös monta muutakin innovatiivista oivallusta ennen kuin toimivat, monipuoliset ad hoc –verkot ovat todellisuutta.

Suomessa ad hoc –verkkoihin liittyvää tutkimusta tehdään muun muassa Oulun yliopiston ja VTT:n yhteisessä Winner-projektissa (Wireless Intertechnology Networks with Optimized Data rates), jossa tutkitaan erityisesti Ipv6:n käyttämistä neljännen sukupolven tietoliikenneverkoissa. [3]

IETF:n MANET –työryhmä pyrkii pitämään yllä, että tarvittavat reititysprotokollat sekä radioverkkoteknologiat saadaan kehitettyä ja standardisoitua. Kehitystyö ja standardisoiminen on tosin tunnetusti varsin hidasta puuhaa, joten tuskin ihan lähitulevaisuudessa kannattaa odottaa standardin mukaisia ad hoc –verkkoja.

4.8 Käytetyt lyhenteet

ABR: Associativity-Based Routing

AODV: Ad Hoc On-Demand Distace Vector Routing

CGSR: Clusterhead Gateway Switch Routing

CIDR: Classless Inter-Domain Routing

DSDV: Destination-Sequenced Distance-Vector Routing

DSR: Dynamic Source Routing

GPRS: General Packet Radio Service

IETF: Internet Engineering Task Force

IP: Internet Protocol

LMR: Lightweight Mobile Routing

MANET: Mobile Ad-hoc Networks

PDA: Personal Digital Assistant

SSA: Signal Stability Based Adaptive Routing

TORA: Temporally Ordered Routing Algorithm

UDP: User Datagram Protocol

WRP: Wireless Routing Protocol

4.9 Lähteet

[1] Jean Pierre Hubaux, Thomas Gross, Jean-Yves Le Bourdec, Martin Vetterli. “Towards Self-Organized Mobile Ad Hoc Networks: The Terminodes Project”. IEEE Communications Magazine January 2001.

[2] Ville Typpö, “Micro-Mobility within Wireless Ad Hoc Networks: Towards Hybrid Wirelss Multihop Networks”. Oulun Yliopisto, Sähkötekniikan osasto –diplomityö 2001.

[3] Mika Ylianttila, Anne Lehti, Petri Mähönen ja Matti Latva-aho.“Liikkuvuus IP-verkoissa”. Prosessori Marraskuu 2000.

[4] Magnus Frodigh, Per Johansson ja Peter Larsson. “Wireless ad hoc networking –The art of networking without network”. Ericson Review No. 4, 2000.

[5] Charles E. Perkins (editor). Ad hoc networking. Addison-Wesley 2001. ISBN 0-201-30976-9

[6] Elisabeth M. Royer, Chai-Keong Toh. “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”.

5. BLUETOOTH

Nykyinen ympäristömme on täynnä erilaisia elämää helpottavia, teknisiä apuvälineitä ja niiden lisälaitteita. Eri merkkisten ja ikäisten mallien yhteispeli voi kuitenkin usein olla ongelmallista. Tämän voi huomata jo uutta videonauhuria kytkiessään.

Tällä hetkellä voimakkaasti kasvava langattomien palveluiden kehitys asettaa lisäpaineita laitteiden yhteensopivuudelle. Liikkuvuus lisää tarvetta muodostaa nopeasti väliaikaisia verkkoyhteyksiä moninaisten laitteiden välille.

Bluetooth on standardi, joka tarjoaa tiedonsiirtoa vaativille järjestelmille langattoman yhteyden läpinäkyvällä ja varmalla tavalla mutta silti edullisesti. Sen päätavoite on korvata sovelluskohtaisia johtoja yksinkertaisesti ja vakaasti.

5.1 Johdanto

Kahden laitteen kommunikoidessa täytyy useita asioita olla sovittuna. Laitteiden väliin on useimmiten kytkettävä oikeanlainen johto, jollei kyse sitten ole langattomasta yhteydestä. Digitaalisia tiedonjyviä eli bittejä voidaan siirtää yhtä johtoa pitkin peräkkäin eli sarjassa tai sitten montaa johtoa pitkin samaan aikaan eli rinnan. Lopulta laitteiden tulee olla yhtä mieltä käytettävästä protokollasta, jotta kumpikin ymmärtää samalla tavalla, mitä mikin bitti tarkoittaa. Menemättä edes ohjelmistotasolle pelkästään erilaisten johtojen määrä koneiden välillä voi olla mykistyttävä.

Edellä mainitut ovat peruskysymyksiä, joihin tarvittiin hintaherkkiin, lyhyen kantaman langatonta tiedonsiirtoa edellyttäviin sovelluksiin sopivaa ratkaisua. Vuonna 1998 Ericsson, IBM, Intel, Nokia ja Toshiba perustivat yhteistyöryhmän SIG (Special Interest Group) uuden langattoman standardin luomiseksi. Bluetooth-nimeä kantava standardi julkistettiin heinäkuussa 1999. Standardissa on määritelty vaatimuksia radiorajapinnan toiminnasta lähtien aina OSI-protokollamallin viidenteen eli istuntokerrokseen asti. Se sisältää siten, paitsi määritelmän käytettävästä taajuusalueesta ja –modulaatiosta, myös protokollapinon ja laitevaatimukset. [2]

Bluetooth-järjestelmä voisi yhdistää esimerkiksi sylimikron ja GPRS-matkapuhelimen toisiinsa langattomasti. Muitakin sovelluskohteita on lukemattomia, kuten: erilaiset kuulokkeet ja mikrofonit, peliohjaimet, tietojen päivitys pöytämikrolta kämmentietokoneelle ja jopa rahtikonttien seuranta satama-alueilla. Bluetooth:n käyttökohteiksi onkin määritelty kolme erilaista yleistä tapausta: yhteyspisteen tarjoaminen äänen ja datan siirtoon, henkilökohtaisten ”ad hoc”-verkkojen luominen ja johdon korvaaminen.

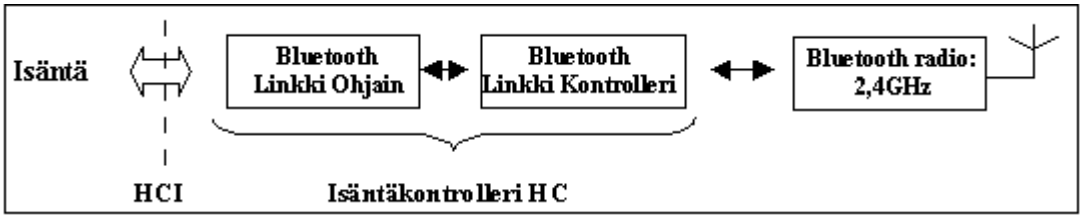
Standardin epätavallinen kutsumanimi Bluetooth tulee pohjoismaalaisesta historiasta. Harald Blåtand oli viikinkihallitsija, joka tunnetaan Tanskan ja Norjan yhdistämisestä 900 luvulla jKr. Blåtand käänsi lisäksi tanskalaiset kristinuskoon. Nimen valinta lienee symbolinen vertauskuva eri tekniikoiden välisten kuilujen kuromisesta umpeen.

5.2 Bluetooth-teknologia

Bluetooth toimii kansainvälisten säännösten mukaisella taajuusalueella, 2,4 GHz:n tuntumassa. Vertailukohdaksi voidaan ottaa esimerkiksi GSM-puhelimien alueet 900 ja 1800 MHz Euroopassa. Maininnan arvoista on myös, että Bluetooth on kehitetty yhteisymmärryksessä Yhdysvaltain imailuviranomaisten FAA:n kanssa ja on näin turvallinen käyttää myös lentokoneissa. [3] Seuraavassa käsitellään tekniikkaa, joka saa Bluetooth:n toimimaan.

5.2.1 Järjestelmän fyysinen osa

Tarkalleen ottaen ei ole määritelty, mitkä osat Bluetooth:ssa pitäisi toteuttaa ohjelmistotasolla ja mitkä laitteistoina. Bluetooth-järjestelmä voidaan kuitenkin jakaa kahteen toiminnalliseen osaan, radiomoduuliin ja linkkimoduuliin eli linkkikontrolleriin. Linkkikontrolleriin liittyy läheisesti ohjelmistopohjainen linkkiohjain, LM (link manager), joten näitä nimitetään usein yhteisellä nimellä isäntäkontrolleri, HC (host controller). Alla on esitetty tavallinen työnjako eri osien välillä; kuten sanottu lopulliset ratkaisut on jätetty valmistajien käsiin. [4]



Kuva 1. Bluetooth-järjestelmän radiomoduuli ja linkkimoduuli

Radiomoduulin vastuulla on luonnollisesti lähetystoiminta, joka tapahtuu kansainvälisesti määritellyllä ISM (Industrial Scientific Medical)-taajuuskaistalla, 2400-2483,5 MHz. Poikkeuksena tähän ovat muutamat maat, tärkeimpinä Ranska (2446,5-2483,5 MHz) ja Espanja (2445-2475 MHz). Kansainvälisellä ISM-alueella lähettäminen tapahtuu välillä 2402 – 2480 MHz, jättämällä siis varmuusmarginaalit kaistan reunoille. Käytetty kaista on jaettu 79:ään (23:een Ranskassa ja Espanjassa) 1 MHz:n levyiseen kanavaan. Bluetooth käyttää hyväkseen niin kutsuttua taajuushyppelyä (frequency hopping), jonka avulla kanavaa vaihdetaan 1600 kertaa sekunnissa. Taajuushyppelyn tarkoitus on muun muassa vähentää ympäristön häiriötekijöitä signaaliin. Taajuushyppelystä ja siihen liittyvistä algoritmeistä kerrotaan lisää hieman tuonnempana.

Bluetooth:n kantama on periaatteessa 10 cm-10 m. Pidempiäkin, jopa 100 metrin etäisyyksiä on koetilanteissa saavutettu, mutta idean kannaltahan olennaisia ovatkin lyhyet matkat. Nimellinen antenniteho Bluetooth:ssa on 0 dBm, jolla saavutetaan noin 10 m kantama. Laitteessa voi olla optio säätää

tehoa, jolloin kantamaa voidaan kasvattaa. Bluetooth käyttää Gaussin taajuusmodulaatiota (GFSK) lähetyksissään. Tällöin ykköset esitetään positiivisina ja nollat vastaavasti negatiivisina taajuuspoikkeamina. Datan lähetys tapahtuu 1 Ms/sekunti symbolinopeudella.

Linkkikontrolleri suorittaa kantataajuussignaalin prosessointia ja fyysisen tason protokollien koodausta. Perustuen linkkikontrollerin tarjoamiin palveluihin ja käyttäen linkkiohjainprotokollaa, LMP (link manager protocol), linkkiohjain vastaa kantataajuusprotokollista ja tietyistä muista alhaisista linkkitason toiminnoista. Näihin kuuluvat datan lähetys ja vastaanotto, yhteyksien luominen, virheiden havaitseminen ja korjaaminen, datan valkaisu (data whitening), tehon säätely ja autentikointi. Isäntäkontrolleri johtaa taajuushyppelyssä käytettävän hyppelyjärjestyksen. LMP:n avulla linkkiohjain on myös yhteydessä muihin verkon linkkiohjaimiin.

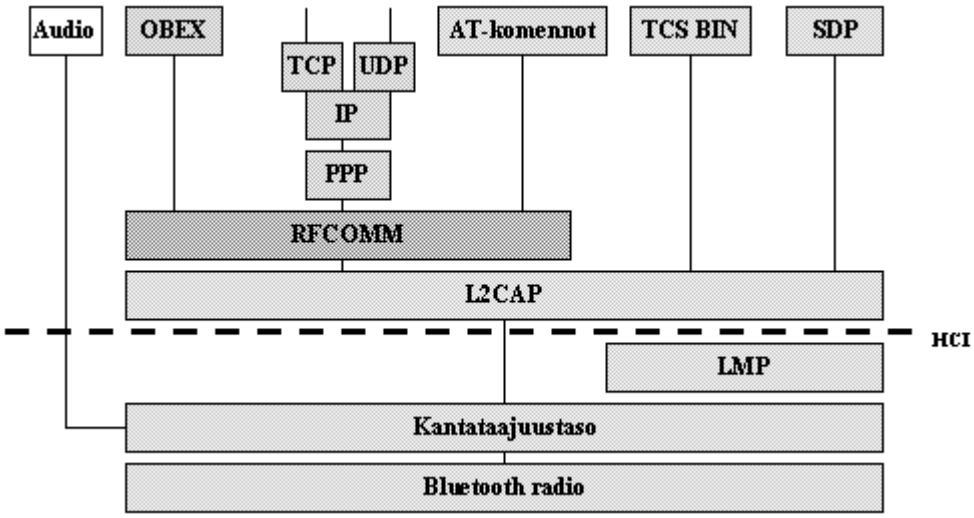
Virheenkorjaus tapahtuu käyttämällä kolmea eri menetelmää: 1/3 FEC:ä ja 2/3 FEC:ä kaikelle liikenteelle sekä ARQ:a dataliikenteelle. Datan valkaisun tavoite on pienentää hyvin samantyyppisen datan aiheuttamaa tasavirtaongelmaa tekemällä siirrettävästä datasta satunnaisempaa. Bluetooth tarjoaa neljää aktiivisuustasoa verkossa oleville laitteille, minkä perusteella myös tehonkulutus vaihtelee. [3], [6] ja [7]

5.2.2 Protokollat

Jotta erilaiset Bluetooth-toteutukset olisivat yhteensopivia, on edellä kuvatun Bluetooth-ytimen ja sen isäntäympäristön, kuten kannettavan tietokoneen välille määritelty isäntäkontrollerirajapinta, HCI (host controller interface) (ks. kuva 1).

Bluetooth-protokollapinossa linkkiohjainprotokollan LMP ja kantataajuuskerroksen päällä on L2CAP-protokolla, jonka tärkeimpänä tehtävänä on peittää alleen alempien kerroksien monimutkaisuudet ja tarjota ylemmille protokollille läpinäkyvä ja luotettava väylä radiorajapintaan asti. Sen muita tehtäviä ovat muun muassa pakettien pilkkominen ja uudelleenkasaaminen sekä multipleksaus. L2CAP:n vastuulla on myös palvelun laatukysymyksiä. L2CAP sijoittuu kutakuinkin OSI-mallin datalinkkikerrokseen.

Seuraavat protokollat kuuluvat välitasolle, OSI-mallin kerroksiin 3-5. Osa niistä on jo aiemmin olemassa olleita, mutta jotkut on varta vasten Bluetooth:ia varten kehitetty.Tärkeimpänä mainittakoon ensimmäiseksi SDP (Service Discovery Protocol). SDP tarjoaa vakioidun tavan selvittää, mitä palveluita verkon muut laitteet tukevat. Tämä on erityisen tärkeää visioiduissa ”ad hoc”-tilanteissa, jolloin laitteita saattaa tulla ja mennä verkossa.



Kuva 2. Bluetooth-protokollapino

RFCOMM on puolestaan tärkeä protokolla, jos ajatellaan jo edellä mainittua johdonkorvauskäyttömallia. Se tarjoaa virtuaalisen sarjaportin, johon olemassa olevien sovellusten on helppo kytkeytyä.

Suoraan RFCOMM:n päällä on OBEX-objektinvaihtoprotokolla, joka perustuu aiemmin kehitettyyn infrapunayhteyksien IrOBEX:iin. Se on laadittu silmälläpitäen arvattavia tilanteita, joissa käyntikortteja tai viestejä halutaan vaihtaa. Neljä erilaista objektia on määritelty vaihdettavaksi Bluetooth-yhteyden yli: vCard (käyntikortit), vCalendar(sähköiset kalenteri- ja aikataulumerkinnät), vNote(lyhyt viesti) ja vMessage(edellistä pidempi viesti tai sähköpostiviesti).

Bluetooth tukee myös audio- ja puhelin sovelluksia. TCS (The Telephony Control System)-spesifikaatio määrittelee, miten audiota siirretään Bluetooth-yhteyden yli. Audiota ei reititetä muiden kerrosten läpi muun datan tavoin, vaan suoraan kantataajuuskerrokseen. Lisäksi spesifikaatio määrittelee AT-pohjaisen puhelinliikenteen kahden laitteen välille. [2] ja [6]

5.2.3 Profiilit

Bluetooth-standardia on kehitetty huomioiden tietyt peruskäyttötapaukset. Näistä käyttötapauksista on johdettu niin kutsutut profiilit, jotka määrittelevät tarkasti, minkälaisia asetuksia ja mitä protokollia tiedonsiirrossa on käytettävä missäkin tilanteessa. Profiilit helpottavat eri valmistajien laitteiden yhteensopivuutta. Profiileja lisätään Bluetooth:n uusien versioiden myötä.

Kolme esimerkkiä käyttötapauksista ovat Internet-silta, Täydellinen kuuloke ja Automaattinen synkronointi. Internet-silta kuvaa tapausta, jossa voidaan langattomasti kytkeytyä lähimpään langalliseen yhteyteen ja sitä kautta ottaa yhteys Internetiin. Täydellinen kuuloke kuvaa esimerkiksi langatonta matkapuhelimen hands-free-kuuloketta tai langattomia korvalappustereoita. Automaattinen synkronointi puolestaan on tilanne, jossa esimerkiksi kämmentietokone päivittyy automaattisesti pöytäkoneesta, kun toimistoon astutaan sisälle.

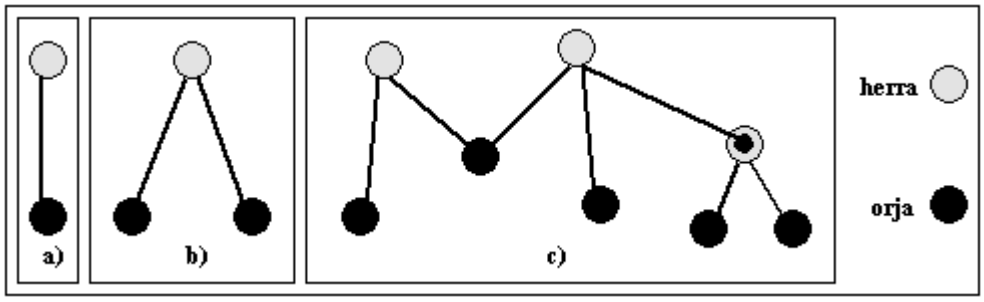
Profiilit jakautuvat hierarkkisesti aliprofiileihin, jolloin aliprofiilin toteuttaminen vaatii myös kaikkien sen yläprofiilien toteuttamista. Tällä hetkellä olemassa olevat 13 profiilia voidaan jakaa neljään pääluokkaan sen mukaan, minkälaisista käyttötapauksista ne on johdettu.

Ensimmäinen on niin sanottujen geneeristen profiilien luokka, joihin kuuluvat General Access Profile (GAP) ja Service Discovery Application Profile (SDAP). GAP on profiilihierarkkian juuri, eli kaikki muut profiilit perustuvat siihen. SDAP toisaalta liittyy edellä mainittuun keskeiseen SDP-protokollaan. Näin ollen kaikkien Bluetooth-laitteiden on toteutettava nämä kaksi profiilia.

Kolme muuta profiililuokkaa ovat Serial Port Profiles, Telephony Profiles ja Networking Profiles. Näihin kuuluvat profiilit määrittelevät luokkiensa nimien mukaisesti johdon korvaus-, puhelinliikenne- ja dataliikennesovelluksiin liittyvät tilanteet. [2], [4] ja [6]

5.2.4 Verkkotopologiat

Bluetooth tukee sekä pisteestä pisteeseen yhteyksiä että pisteestä useaan pisteeseen yhteyksiä. Monipisteyhteydessä laitteet jakavat kanavan. Bluetooth-sanaston mukaisesti, kun kaksi tai enemmän laitteita muodostavat verkon, niin on kyseessä pikoverkko. Verkko muodostuu herra- (master) laitteesta ja maksimissaan seitsemästä orja- (slave) laitteesta. Jokaisella aktiivisella orjalla on kolmen bitin mittainen AMA-osoite (Active Member Address). Niin sanotusti pysäköityjä (parked) orjia sen sijaan verkossa voi olla huomattavasti enemmän. Pysäköidyssä tilassa orja ei pysty toimimaan aktiivisesti kanavalla, mutta se pysyy kuitenkin synkronoituna herralaitteeseen. Pysäköidyssä tilassa orjalla on kahdeksanbittinen pysäköidyn jäsenen osoite PMA (Parked Member Address), mikä tietysti rajoittaa pysäköityjen laitteiden määrän 256:een. Orjien yhteyttä kanavaan säätelee aina herralaite.



Kuva 3. a) Yksi orja, b) Pikoverkko, c) Hajaverkko

Bluetooth-järjestelmä toimii myös, vaikka kaksi pikoverkkoa risteäisivät. Tällaista tilannetta nimitetään hajaverkoksi (scatter network). Kullakin pikoverkolla voi olla ainoastaan yksi herralaite, mutta orjalaitteena voi olla samaan aikaan useammassa verkossa. Lisäksi on mahdollista, että laite on yhdessä verkossa herrana ja toisessa orjana samaan aikaan. Kukin pikoverkko taajuushyppelee oman ominaisen järjestyksensä mukaan, mikä pitää ne poissa toistensa lähetyksistä. Hajaverkon tapauksessa lähettäminen tapahtuu aikajakoisen multipleksoinnin mukaisesti eri aikaväleissä eri verkoihin. [3], [5] ja [7]

5.2.5 Taajuushyppely ja aikavälit

Ensimmäiset varsinaiset taajuushyppelyyn perustuvat sovellukset ovat peräisin 1970-luvulta sotilaskäytöstä. Taajuushyppelyn tarkoituksena oli tehdä vihollisen salakuuntelutoiminta ja taajuuksien häiritseminen vaikeaksi.

ISM-taajuusalueella, jolla Bluetooth:kin toimii, voivat vapaasti lähettää useat erilaiset laitteet ja se onkin jo nykyään laajassa käytössä. Tavallisissa kodeissa ISM-kaistalla toimivia laitteita ovat esimerkiksi kannettavat puhelimet, itkuhälyttimet ja autotallin oven avaajat.

Välttääkseen häiriöitä muista kodinkoneista sekä toisista pikoverkoista myös Bluetooth käyttää hyväkseen taajuushyppelyä. Useimmissa maissa Bluetooth-tajuusalue on jaettu 79:ään 1 MHz:n taajuuskaistaan, joita kukin pikoverkko käy läpi omassa pseudosatunnaisessa järjestyksessään, 1600 kertaa sekunnissa. Hyppelyjakso lasketaan pikoverkon herralaitteen 48-bittisestä Bluetooth-laiteosoitteesta (BD_ADDR). Hyppelyjaksolla on suhteellisesti ottaen huomattavan pitkä pituus, jolloin sen toistuminen ei aiheuta ongelmia.

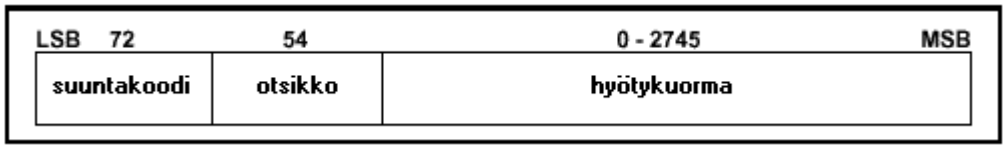
Jokaisella Bluetooth-laitteella on sisäinen kello. Herralaitteen kello näyttää verkon liikennöinnissä käytettävä pääaikaa. Vaihe hyppelyjaksossa määritellään herralaitteen sisäisen kellon mukaan. Orja voi lähettää pikoverkon oikealla taajuudella herran BD_ADDR:n avulla. Oikea vaihe saavutetaan lisäämällä orjan kelloon sen poikkeama herralaitteen kellosta. Oikea poikkeama tarkistetaan joka kerta, kun orja ottaa herralta paketin vastaan.

Koska hyppely tapahtuu noin 1600 kertaa sekunnissa, jää kullakin taajuudella tapahtuvalle liikennöinnille noin 625 μs aikaväli. Herra ja orja lähettävät aikajakoisesti (TDD) eri aikaväleillä. Paketin lähetys alkaa aina aikavälin alusta. Herralaite lähettää parillisissa aikaväleissä ja orjalaite parittomissa aikaväleissä. Tästä seuraa, että jokainen paketti lähetetään omassa aikavälissään, omalla hyppelytaajuudellaan. Lähtökohtaisesti yksi paketti vie aina yhden aikavälin, mutta tarpeen mukaan sille voidaan kohdistaa viisikin aikaväliä. [2], [5] ja [6]

5.2.6 Linkkityypit

Tarpeen mukaan Bluetooth tukee sekä puheliikenteelle soveltuvaa synkronista lähetystä (SCO) että dataliikenteelle sopivaa asynkronista lähetystä (ACL). Synkroninen linkki on yhteydellinen, piirikytkentäinen, jolloin aikaväli varataan aina kiinteästi. SCO-linkkiä käytetään pääasiassa puheliikenteen siirtämiseen pisteestä pisteeseen. Herralaite pystyy tukemaan kolmeakin samanaikaista SCO-linkkiä yhden, kahden tai kolmen orjan kanssa. Aikavälit, joita ei käytetä SCO-liikenteeseen, voidaan käyttää ACL-pakettien kuljettamiseen. SCO-paketteja ei koskaan lähetetä uudelleen.

Asynkroninen linkki on yhteydetön, pakettikytkentäinen. Asynkroninen kanava on pisteestä useaan pisteeseen toimiva linkki. ACL-paketit lähetetään yleensä uudelleen, jos tarvetta esiintyy. ACL toteutetaan käyttäen niin kutsuttua kiertokyselymenetelmää (polling). Kiertokyselyn perusteella herralaite päättää, mille orjalle seuraavaksi annetaan lähetysoikeus. Eri



kiertokyselymenetelmät ovat keskeinen kysymys mietittäessä, miten rajallinen siirtokapasiteetti jaetaan orjien kesken mahdollisimman tehokkaasti ja samalla oikeudenmukaisesti. Näin ollen kiertokyselyn toteutustavalla voidaan tuntuvasti vaikuttaa palvelun laatuun.

Erilaisissa kiertokyselyn lähestymistavoissa voidaan muun muassa lähetysoikeus jakaa tasaisesti kaikkien orjien kesken, mikä kuitenkin tuhlaa resursseja niiden osalta, joilla ei lähetettävää dataa ole. Toisaalta yhden orjan voidaan antaa käyttää kerralla tarpeensa mukainen määrä aikavälejä, jolloin muita orjia voi pahimmassa tapauksessa uhata ”nääntyminen” resurssinpuutteessa. Keskitie edellisten väliltä on pyritty löytämään tiettyjen enteiden perusteella, orjien lähetystarvetta ennustamalla ja jaettuja resursseja seuraamalla.

Alla olevassa taulukossa on esitetty erilaisten liikennetyyppien yhdistelmillä saavutettavat siirtonopeudet.

Taulukko 1. Siirtonopeudet eri konfiguraatioilla

konfiguraatio	**maksimisiirtonopeus ylävirtaan**	**maksimisiirtonopeus alavirtaan**
3 samanaikaista puhekanavaa	64 kbps x 3 kanavaa	64 kbps x 3 kanavaa
symmetrinen data	433,9 kbps	433,9 kbps
asymmetrinen data	723,2 tai 57,6 kbps	57,6 tai 723,2 kbps

Lisäksi on olemassa yhdistetty datapuhe-SCO-paketti, jolla on mahdollista saavuttaa 64kbit/s dataliikenteelle ja 64kbit/s puheliikenteelle molempiin suuntiin. [5], [7] ja [8]

5.2.7 Pakettiformaatti

Bluetooth:n kantataajuuskerrokselle on määritelty 13 erilaista pakettia Ylemmät kerrokset käyttävät näitä pohjana, luodessaan omia datayksiköitään (PDU). Osa paketeista on ainoastaan SCO-linkkien ja osa ACL-linkkien käyttöön. Jokainen paketti sisältää kolme osuutta, kuten kuvasta 4 ilmenee. Kuitenkin, on mahdollista, että pakettiin kuuluu ainoastaan suuntakoodi tai suuntakoodi ja otsikko. Tilanteiden erottamiseksi suuntakoodi on 72 bittiä pitkä, mikäli sitä seuraa otsikko ja vain 68 bittiä, jos se on yksinään. Otsikon pituus on 54 bittiä ja hyötykuorma voi olla 0-2745 bittiä pitkä.

Kuva 4. Paketin formaatti

Suuntakoodia käytetään aikojen synkronointiin, kellojen erotuksien kompensointiin sekä haku- ja tiedustelutoimintoihin, joista kerrotaan lisää kohdassa 1.3. Suuntakoodeja on määritelty kolmea eri tyyppiä: CAC, DAC

ja IAC, joita käytetään pikoverkon tunnistukseen, hakutoimintoon ja tiedustelutoimintoon, vastaavasti.

Otsikko sisältää kuittaus- ja numerointitietoja, joiden avulla paketit saadaan oikeaan järjestykseen. Otsikkoon kuuluvat lisäksi tiedot vuonohjauksesta, orjan osoitteesta ja otsikon omasta virheentarkistuksesta.

Hyötykuorma voi sisältää datakentän, äänikentän tai molemmat. Mahdollisen datakentän mukana tulee erillinen hyötykuormaotsikko. [2]

5.3 Bluetooth-verkon toiminta

Bluetooth-laitteille on määritelty erilaisia tiloja sen mukaan, millaisella aktiivisuustasolla ne parhaillaan toimivat pikoverkoissaan. Osa tiloista kuluttaa tuntuvasti vähemmän energiaa kuin aktiivisimmat tilat, joten niillä on merkitystä laitteiden toiminta-ajan kannalta. Varsinainen yhteyksien muodostaminen riippuu tarkasteltavasta lähtötilanteesta. Se tapahtuu erilailla riippuen siitä, ”tuntevatko” laitteet toisensa jo ennestään.

5.3.1 Bluetooth-tilat

Tärkeimmät tilat, joissa Bluetooth-laite toimii, ovat Odotus ja Yhteys (Standby ja Connection). Ennen kuin mitään yhteyksiä on luotu, laite on matalatehoisessa Odotus-tilassa. Tällöin ainoastaan laitteiden kellot käyvät, eikä tietoa niiden välillä lähetetä. Odotus-tilassa oleva laite kuuntelee kuitenkin 1,28 sekunnin välein 32 eri hyppelytaajuudella mahdollisten kutsujen varalta. Kuunneltavat taajuudet määritellään joko kaikille Bluetooth-laitteille yhteisen niin kutsutun GIAC-suuntakoodin tai laitetyyppikohtaisen DIAC-suuntakoodin avulla.

Yhteyksien luomiseen käytetään tiedustelu- ja hakukutsuja (inquiry ja page), joista lisää seuraavassa kohdassa. Kun yhteydet on luotu ja liikennöinti on tapahtunut, laitteiden on mahdollista pysyä yhteydessä verkkoon mutta laskeutua tehonkulutuksessa alemmalle tasolle. Tällaisia tiloja ovat, osin jo aiemmin mainitut, nuuhkiminen (sniff), pito (hold) ja pysäköity (park).

Nuuhkimistilassa laite säilyttää AMA-osoitteensa ja pysyy synkronoituna verkkoon. Laitteen tehonkulutus laskee kuitenkin, sillä se kuuntelee verkon liikennettä harventuneella tahdilla. Tämä aikaväli on ohjelmoitavissa ja riippuu sovelluksesta. Säästötiloista nuuhkiminen on vähiten tavallisesta kulutuksesta poikkeava.

Pitotilassa laite ei lähetä eikä vastaanota liikennettä, ainoastaan sisäinen ajastin käy. Säädetyn ajan päästä laite herää ja lähetystoiminta jatkuu normaalisti. Pitoa käytetään muun muassa lämpötilasensoreissa, joissa virrankulutus on alhainen. Pidossa olevat laitteet säilyttävät AMA-osoitteensa.

Vähiten kuluttava säästötila on pysäköinti. Pysäköity laite pysyy synkronoituna pikoverkkoon mutta ei lähetä mitään. Pysäköidyt laitteet luopuvat AMA-osoitteistaan. Ne kuuntelevat paikoin verkon liikennettä

tarkistaakseen kelloaan ja vastaanottaakseen broadcast-lähetyksiä. [2], [5] ja [7]

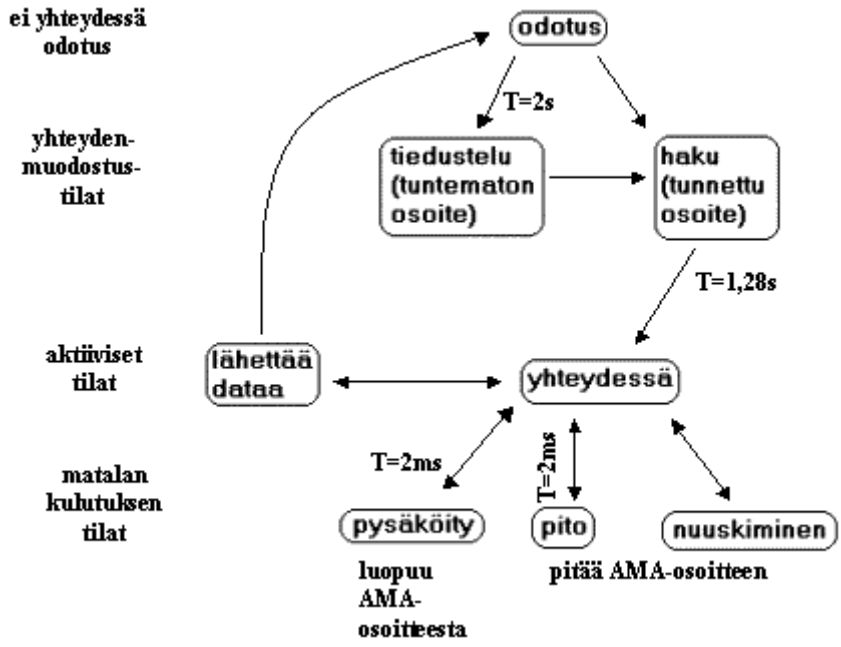
5.3.2 Yhteyksien luominen

Yhteyden muodostuksen voi aloittaa mikä hyvänsä kantamalla oleva laite, josta sitten tulee verkon herralaite. Yhteyden muodostuksen kulku riippuu siitä, mitä ennalta tiedetään toisista laitteista. Mikäli toisen laitteen osoitetta ei tunneta, aloitteen tekevä laite lähettää tiedustelun ja onnistuneen tiedustelun jälkeen haun. Jos osoite tunnetaan ennestään, voidaan tiedustelu ohittaa ja lähettää suoraan haku.

Tiedustelun havaitseva laite lähettää vastauksena ”taajuushyppelyn synkronointi”–paketin (FHS), josta ilmenee sen laiteosoite ja kellonaika. Nyt tiedustelun aloittaneesta laitteesta tulee pikoverkon herra ja tiedusteluun vastanneista orjia. Mikäli vastauksissa tiedusteluun sattuu törmäyksiä, laitteet odottavat satunnaisen määrän aikavälejä ja alkuperäinen aloitteentekijä lähettää uuden tiedustelun.

Varsinaisen yhteyden muodostamiseen käytetään hakua. Haku tehdään, kun tavalla tai toisella tunnetaan muiden laitteiden laiteosoitteet ja on kohtuullinen aavistus niiden kelloista. Kelloarvio nopeuttaa yhteydenmuodostusprosessia. Haussa herralaite etsii orjaa lähettämällä hakupaketteja, joihin orja vastaa omalla hakuvastauspaketilla (inquiry reply). Saatuaan tämän kuittauksen herralaite lähettää orjalle vielä FHS-paketin varmistaakseen synkronisaation samalle hyppelytaajuudelle. [2], [5] ja [7]

Kuvassa 5 on yhteenveto tässä kappaleessa esitetyistä tiloista ja niiden



yhteyksistä toisiinsa.

Kuva 5. Bluetooth-tilat. Ajat T ovat tyypillisiä tilanvaihtoon kuluvia aikoja. Mukailtu lähteestä [3]

5.4 Tietoturvanäkökohdat

Bluetooth:ssa käytetty tekniikka ja sen tavalliset käyttöolosuhteet jo sinänsä edistävät tietoturvallisuutta. Taajuushyppely vaikeuttaa salakuuntelua ja yhteyksien häiritsemistä. Toisaalta Bluetooth:n lyhyt kantama auttaa myös asiaa pitämällä liikennöinnin suppean, hyvin hallittavissa olevan alueen sisäpuolella. Tietoturvallisuutta on lisäksi edistetty teknisin ratkaisuin.

Bluetooth:n perustavimassa profiilissa, GAP:ssa, on määritelty kolme tietoturvan tasoa: 1. ei suojausta, 2. palvelutasolla tapahtuva suojaus ja 3. linkkitasolla tapahtuva suojaus. Pääasiallinen ero toisen ja kolmannen tason välillä on, että toisen tason suojauksessa toimenpiteisiin ryhdytään yhteydenmuodostuksen jälkeen kun taas kolmannella tasolla jo ennen muodostusta. Näin ollen toisen tason toimenpiteet tapahtuvat protokollapinon ylemmissä kerroksissa ja kolmannen tason toimenpiteet alemmissa kerroksissa.

Linkkitason turvallisuuteen vaikuttavat olennaisesti neljä parametria. Ensimmäinen näistä on jokaiselle Bluetooth-laitteelle allokoitu uniikki 48-bittinen laiteosoite (BD_ADDR). Toinen ja tärkein kaikista parametreistä on 128-bittinen linkkiavain (link key), jota käytetään kahden Bluetooth-laitteen välillä niiden autentikoituessa toisilleen. Linkkiavaimesta on johdettavissa 8-128-bittinen salausavain (encryption key), jolla salataan pakettien sisältöä, ja joka luodaan uudelleen jokaista uutta lähetystä varten. Salausavain on erotettu linkkiavaimesta, jotta voidaan käyttää lyhyempää avainta heikentämättä autenkoimisprosessin turvallisuutta. Neljäntenä on Bluetooth-laitteen sisällä generoitava satunnaisluku. Lisäksi on olemassa käyttäjän asettama PIN-koodi, joka niin ikään auttaa laitteita tunnistamaan toisensa ja nostaa turvallisuuden tasoa.

Palvelu/sovellustasolla tietoturvasta vastaavat ylemmän tason protokollat, eli protokollat L2CAP:sta ylöspäin. Verkossa toimivat laitteet voidaan jakaa kahteen ryhmään: luotettaviin ja epäluotettaviin. Luotettavilla on tällöin oikeus kaikkiin tarjottuihin palveluihin. Epäluotettavat laitteet voidaan edelleen ryhmitellä sen mukaan, miten korkeatasoista tunnistusta niiltä vaaditaan. Palveluille voidaan tarpeen mukaan määrittää erilaisia autentikointiin ja tiedon salaukseen liittyviä vaatimuksia.

Raportoituja ongelmia Bluetooth:n tietoturvassa on jonkin verran. Psykologisessa mielessä esimerkiksi PIN-koodit ovat epäluotettava menetelmä, sillä laiskuuttaan käyttäjä voi helposti asettaa ne vaikkapa nolliksi. Toinen esiintynyt ongelma on, että yhden laitteen linkkiavain voi jäädä toisen laitteen muistiin vaikka liikenne on jo loppunut. Kun lisäksi edellisen laitteen BD_ADDR on tunnettu, jälkimmäiselle tarjoutuu mahdollisuus salakuunnella edellisen laitteen myöhempiä liikennöintejä verkossa. BD_ADDR:n tunteminen voi johtaa myös yksityisyyden suojan rikkomuksiin, sillä koska se on uniikki, voidaan käyttäjän toimia seurata.

DoS-hyökkäykset saavat langattomassa ”ad hoc”-ympäristössä aivan uuden merkityksen, jos hyökkääjä onnistuu estämään laitteita menemästä virransäästötiloihin. Seurauksena voi olla, että laitteiden paristot loppuvat ennen aikojaan ja verkon toiminta rampautuu tätä kautta.

Bluetooth:n tietoturvallisuutta on kritisoitu, mutta se lienee kuitenkin kohtuullisella tasolla, jos otetaan huomioon liikenteen laatu ja tavalliset kantamat. Toisin kuin Internetissä yleensä, Bluetooth-hakkerin täytyisi istua melkein samassa huoneessa, mikä rajoittanee näiden joukon vain kylmäpäisimpiin. Siirrettävän datan laatu ei yleisesti myöskään edellytä suuria turvatoimenpiteitä vaan pysyy yksinkertaisten sovellusten tasolla. Kritiikki onkin saanut ehkä alkunsa ajatuksista, joissa Bluetooth on tulkittu WLAN:ien haastajaksi. [9]

5.5 Bluetooth suhteessa muihin teknologioihin

Bluetooth ei ole ensimmäinen standardi, joka on kehitetty korvaamaan johtoja ja luomaan lyhyen kantaman verkkoja. Monien tekniikkojen sovellusalueet menevät Bluetooth:n kanssa päällekkäin. Seuraavassa tarkastellaan kahta laajalle levittäytynyttä tekniikkaa, joita kumpaakin on osin luonnehdittu Bluetooth:n kilpailijoiksi.

5.5.1 IrDA

IrDa eli Infrared Data Associationin spesifioima infrapunayhteys on laajalti levinnyt lisäväline maailmalla. Sitä on asennettu 150 miljoonaa kappaletta maailmanlaajuisesti ja sen kasvu on 40%:n tietämillä vuositasolla. Infrapunalinkkiä käytetään muun muassa tietokoneissa, matkapuhelimissa ja kämmenmikroissa lyhyen kantaman tiedonsiirtoon. Infrapunasäteet muodostavat noin 30:n asteen kulmassa olevan kartion, joka yhdistää kaksi pistettä, enimmillään metrin etäisyydellä toisistaan. Tiedonsiirtonopeudet liikkuvat 9600 bps:n ja 16 Mbps välillä.

Varsinaisesti infrapuna ja Bluetooth eivät ole kilpailevia tekniikoita vaikka ne toteuttavatkin samantapaisia toimintoja. Käytännössä on niin, että missä ominaisuuksissa toinen näistä kahdesta on huono niin toinen on parhaimmillaan ja päinvastoin. Tästä seuraa, että molemmat ovat elinvoimaisia tekniikoita omissa sovelluksissaan. Ir:n ja Bluetooth:n sovellukset menevät kuitenkin suurelta osin päällekkäin, joten on tärkeää katsoa, mitkä niiden väliset erot ovat.

Ir:n ollessa täsmällinen pisteestä pisteeseen linkki, sillä on hankala luoda verkkoja. Se vaatii myöskin näköyhteyden, eikä saa siis yhteyttä esimerkiksi seinien läpi. Bluetooth:lle nämä kysymykset ovat helppoja, sillä radioaallot eivät esteistä välitä ja niillä on luotavissa monipisteinen verkko.

Vastaavasti Ir:n vahvuus tietyissä tilanteissa on, että lähetyksen vastaanottaja on tarkasti määritelty; ensiksikin manuaalisen suuntaamisen avulla ja sitten lyhyen kantaman ja kapean suuntakartion myötä. Tämä on eduksi esimerkiksi ruuhkaisessa kokoushuoneessa, jossa useat parit yrittävät vaihtaa sähköisiä käyntikortteja. Bluetooth:ssa ei tähtääminen ole mahdollista ja sillä kuluukin aikaa miettiessä, mikä on oikea vastapuoli.

Lopulta, hintavertailu kallistuu toistaiseksi kypsemmän infrapunatekniikan eduksi. Täydellinen Ir-asennussarja maksaa noin $1, kun taas Bluetooth:n tavoitehinta on noin $5. Todellisuudessa nuoren Bluetooth:n hinta on pyörinyt $10-20 tuntumassa. Viime vuoden lopulla Motorola tosin teki

kauan odotetun ilmoituksen, että se alkaa toimittaa vuoden 2002 ensimmäisellä neljänneksellä Bluetooth-siruja noin $6:n hintaan. [10] ja [11]

5.5.2 IEEE 802.11b ja WLAN

WLAN eli Wireless Local Area Network on standardin 802.11b mukainen langaton yhteys, jolla voidaan käytännössä luoda perinteinen LAN ilman johtoja. Sen tarjoama siirtonopeus on jopa 10Mbps. 802.11b on kasvattanut suosiotaan huimasti toimistoissa, kodeissa ja niin kutsutuissa ”hot spot”-paikoissa, kuten esimerkiksi lentokentät ja vaikkapa Otaniemi. 802.11b:n maksimikantama parhaimmassa tapauksessa on 300 metriä.

Monet tahot ovat maalailleet Bluetooth:sta haastajaa ja kilpailijaa 802.11b:lle WLAN-saralla. Vaikkakin nämäkin teknologiat on kehitetty periaatteessa samaa ajatusta, eli johtojen korvaamista, silmälläpitäen, niillä on eri käyttökohteet. Bluetooth soveltuu käytettäväksi pienten laitteiden langattomiin henkilökohtaisiin lähiverkkoihin (WPAN) vankan ja suhteellisen yksinkertaisen rakenteensa johdosta sekä erityisesti alhaisen energiankulutuksen puolesta. Myös sen alhainen hinta on ratkaiseva tekijä. 802.11b tarjoaa huomattavasti korkeamman siirtonopeuden, mutta se kuluttaa tehoa niin paljon, että käytännössä sylimikroa pienemmän laitteen akut eivät sitä kestä.

Vastaavasti Bluetooth:n edellä mainitut edut tekevät siitä 802.11b:tä huonommin sopivan massiiviseen tiedonsiirtoon. Pieni kantama, alhainen siirtonopeus ja pieni protokollapino tekevät siitä hitaan ja kömpelön WLAN-teknologiaksi. Viimeaikoina yritykset ovat kuitenkin alkaneet ymmärtää, että kyse ei ole kilpailevista, vaihtoehtoisista teknologioista vaan toisiaan täydentävistä ratkaisuista [12].

Niin tai näin, viimeaikaisten tutkimusten mukaan Bluetooth-markkinoiden kasvunopeus on suurempi kuin 802.11b:n. [13]

5.6 Nykytilanne ja tulevaisuuden näkymät

Monien arvioiden mukaan Bluetooth:n oli määrä räjähtävästi lisääntyä jo aiemmin, mutta osoittautui, että aika ei ollut vielä kypsä. Telekommunikaatioalan maailmanlaajuinen taantuma saattoi omalta osaltaan hidastaa kehitystä. Bluetooth:iin ladattiin alusta asti valtavasti odotuksia; jopa liikaa, sillä siitä povattiin joka paikan ratkaisua WPAN:eista WLAN:eihin. Markkinoilla vaikutti kuitenkin hitausmomentti, joka antoi odottaa sekä kunnollisia laitteita että käyttökelpoisia sovelluksia. Hintataso esti lisäksi lisäämästä Bluetooth-sirua moniin pikkulaitteisiin, joihin se oikeastaan parhaiten soveltuu.

Nyt näyttää kuitenkin siltä, että kaivattu kasvu on löytynyt. Useat valmistajat ovat jo tuoneet tai ainakin luvanneet tuoda markkinoille tuotteita, jotka tukevat Bluetooth:a. Tietokonevalmistajat kuten Compaq, IBM, Palm, ja Toshiba ovat tuomassa markkinoille yhteensopivia tuotteita. samoin matkapuhelinvalmistajat Ericsson, Nokia ja Motorola. Jälkimmäisissä Bluetooth on yleensä liitetty 2,5G- ja 3G-tyyppisiin

palveluihin. Sonylta tuli markkinoille Bluetooth-sirun sisältävä digitaalikamera, josta digikuvan voi esimerkiksi lähettää sähköpostilla langattomasti GPRS-puhelimen kautta.

Arvostettu Gartner Consulting arvioi Bluetooth-sirujen hinnan laskevan alle $5:iin vuoden 2002 loppuun mennessä. Näin ollen vaikuttaa, että hinnankin muodostama este on poistumassa.

Vahvan kasvun ja leviämisen myötä Bluetooth vakiinnuttanee paikkansa WPAN:ien toteutustapana.

5.7 Käytetyt lyhenteet

2,5/3G: 2,5:n ja 3.:n sukupolven matkapuhelintekniikka

ACL: Asyncronous Connection-Less

AMA: Active Member Address

ARQ: Automatic Retransmission Request

BD_ADDR: Bluetooth Device Address

bps: bittiä per sekunti

CAC: Channel Access Code

DAC: Device Access Code

DIAC: Dedicated Inquiry Access Code

DoS: Denial of Service

FAA: The Federal Aviation Administration

FEC: Forward Error Correction

FHS: Frequency Hopping Synchronization

GFSK: Gaussian Frequency Shift Keying

GIAC: General Inquiry Access Code

GPRS: General Packet Radio Services

GSM: Global System for Mobile communication

GAP: Generic Access Profile

HC: Host Controller

HCI: Host Controller Interface

IAC Inquiry Access Code

IBM International Business Machines

IrDA: Infrared Data Association

IrOBEX: Infrared Object Exchange Protocol

ISM: Industrial Scientific Medical

L2CAP: Logical Link Control and Adaptation Protocol

LAN: Local Area Network

LM: Link Manager

LMP: Link Manager Protocol

LSB: Least Significant Bit

MSB: Most Significant Bit

OBEX: Object Exchange Protocol

OSI: Open Systems Interconnection

PDU: Protocol Data Unit

PMA: Parked Member Address

RFCOMM: Serial Cable Emulation Protocol

SCO: Synchronous Connection Oriented link

SDAP: Service Discovery Application Protocol

SDP: Service Discovery Protocol

SIG: Special Interest Group

TCS: Telephone Control protocol Specification

TDD: Time Division Duplex

WLAN: Wireless Local Area Network

WPAN: Wireless Personal Area Network

5.8 Lähteet

[1] Virallinen Bluetooth-www-sivu: www.bluetooth.com

[2] Palowireless Bluetooth Resource Center: www.palowireless.com

[3] James Kardach, Intel; Bluetooth Architecture Overview; (maaliskuu 1999); http://www.palowireless.com/infotooth/download.asp

[4] LM Ericsson; http://www.ericsson.com/bluetooth/

[5] Cathal McDaid; University of Limerick, Ireland; Routing Connections In Bluetooth; (huhtikuu 2000)

[6] Nokia Corporation; Mobile Internet Technical Architecture MITA; Edita Plc; (2001)

[7] Wireless Development Network; An Introduction To Bluetooth; http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html

[8] The Internet Next Generation Project; Polling Best Effort Traffic In Bluetooth; http://ing.ctit.utwente.nl/WU4/Documents/aityaiz_wpmc01_full.pdf

[9] Cathal McDaid, Cathal's Corner, Palowireless Bluetooth Resource Center; Bluetooth Security Part 1-3 (helmikuu 2001) http://www.palowireless.com/bluearticles/cc1_security1.asp;

[10] Dave Suvak, Extended Systems Inc.; IrDA and Bluetooth: A Complementary Comparison; (2000); http://www.extendedsystems.com/ESI/Products/Wireless+Connectivity+Products/Bluetooth+Embedded+Protocols/Product+Detail/BT_vs_IR.htm

[11] Motorola, Media Center; http://www.motorola.com/mediacenter/news/detail/0,1958,823_574_23,00.html

[12] Cathal McDaid, Cathal's Corner, Palowireless Bluetooth Resource Center; Bluetooth & 802.11b; (tammikuu 2002); http://www.palowireless.com/bluearticles/cc4_bluetooth802.11b_part2.asp

[13] Devin Pike, Senior Editor AnywhereYouGo.com; Study: Bluetooth Development Outpacing 802.11; (elokuu 2001); http://ayg.com/wireless/Article.po?type=Article_Archives&page=491317

[14] Robin Simpson, ZDNet/Gartner; Bluetooth to arrive amidst concerns; (maaliskuu 2002); http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2854261,00.html

6. SYMBIAN-KÄYTTÖJÄRJESTELMÄ

Symbian-käyttöjärjestelmä on kehitetty vakaaksi alustaksi puhelimiin, tietureihin ja kommunikaattoreihin. Sen suunnittelussa on alusta asti otettu huomioon kannettavien laitteiden pienemmät resurssit ja muut erityisvaatimukset, kuten pienempi muistin ja rajallinen sähköenergian määrä sekä kommunikaatiosovellusten tarve.

Symbian tarjoaa avoimen kehitysympäristön laite- ja ohjelmistotoimittajille. Avoimessa kehitysympäristössä kuka tahansa voi ryhtyä kehittämään sovellusohjelmia. Symbian on siis tarkoitettu käyttöjärjestelmäksi, jonka koko telekommunikaatioteollisuus voi ottaa käyttöön tuotteissaan.

Yrityksenä Symbian on Ericssonin, Matsuhitan (Panasonic), Motorolan, Nokian, Sony Ericssonin ja Psionin omistama yhtiö. Sen tarkoituksena on kehittää ja ylläpitää Symbian-käyttöjärjestelmää.

6.1 Symbian yhteistyön historia

Vuoden 1998 alussa Ericsson, Motorola ja Nokia aloittivat neuvottelut tulevan yhteisen käyttöjärjestelmän kehittämiseksi. Kesäkuussa 1998 neuvottelut kantoivat hedelmää. Neuvottelujen pohjalta perustettiin itsenäinen yritys vastaamaan käyttöjärjestelmän kehittämisestä. Käyttöjärjestelmän pohjaksi tuli Psion Softwaren valmistama EPOC-käyttöjärjestelmä. Sekä käyttöjärjestelmän että yhtiön nimeksi tuli Symbian. [1]

Hieman myöhemmin vuonna 1999 omistajien joukkoon tuli Matsuhita (Panasonic). Syksyllä 2001 Sony ja Ericsson yhdistivät matkapuhelin tuotantonsa ja perustivat Sony Ericssonin [2]. Se liittyi heti vuoden 2002 alussa Symbiania omistavien yritysten joukkoon.

Symbian-käyttöjärjestelmän ovat lisensoineet muun muassa Siemens, Sony, Sanyo, Kenwood ja Fujitsu.

6.1.1 Yhteistyön tavoitteet

Tavoitteena on kehittää ja ylläpitää alustaa seuraavien sukupolvien mobiililaitteille. Yhteisestä käyttöjärjestelmän kehityksestä on tarkoitus olla hyötyä jokaiselle osallistuvalle osapuolelle.

Yhteistyön avulla osallistuvien yritysten kehityskustannukset pienenevät. Lisäksi yritysten riskit pienenevät, kun jokainen ei kehitä omaa, toisten kanssa kilpailevaa, järjestelmää.

Syntyvä standardikäyttöjärjestelmä muodostuu houkuttelevaksi alustaksi kehittää ohjelmistoja ja muita tuotteita. Jokaista mahdollista valmistajaa kohden ei tarvitse tehdä omia versioita, jolloin ohjelmistotuotteiden markkinat tulevat kerralla laajemmiksi.

Symbian-käyttöjärjestelmän voi lisensoida mikä tahansa yritys. Symbiania käyttäviä tuotteita valmistavalle yritykselle Symbianista tulee kuluja ainoastaan kiinteä maksu jokaisesta myydystä Symbian-käyttöjärjestelmää käyttävästä laitteesta.

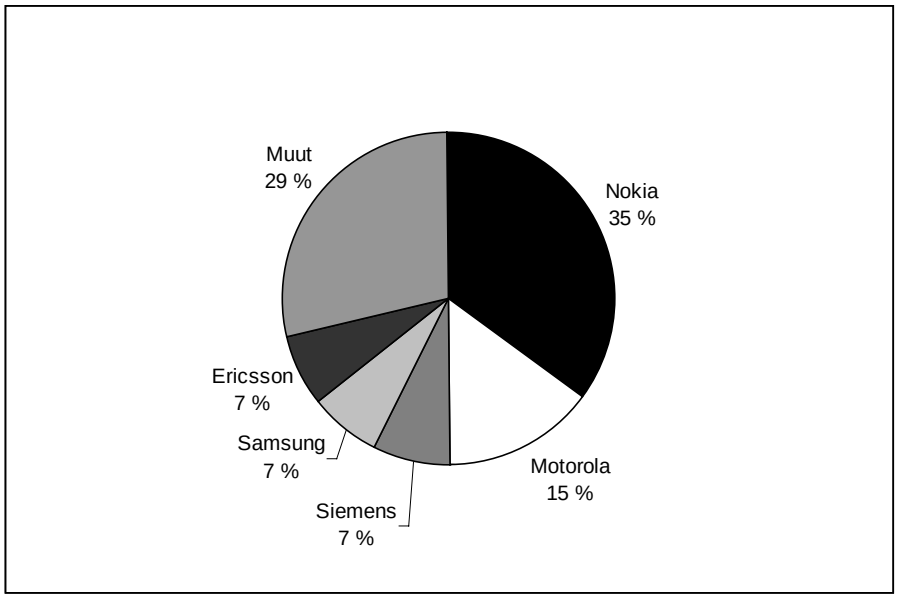
Yleinen ja tunnettu käyttöjärjestelmä muodostuu myös asiakkaille kiinnostavaksi. Mitä laajemmalle käyttöjärjestelmä leviää, sitä enemmän sille löytyy ohjelmia. Laajasti käytössä olevalle järjestelmälle tulee myös olemaan paremmin tarjolla tukea muiden ohjelmien ja laitteiden taholta.

6.1.2 Muut tavoitteet

Tärkeänä tavoitteena on myös suojata Symbianiin osallistuvien valmistajien markkinoita. Puhelinvalmistajilla oli pelkona, että niille tulisi käymään kuin PC-valmistajille. PC-maailmassa PC-tietokoneiden valmistamisen katteet ovat hyvin pieniä ja koko ala on hyvin riippuvainen Microsoftin käyttöjärjestelmistä, jotka ovat käytössä suurimmassa osassa PC-tietokoneita. Tiedossa on myös, miten voimakas Microsoft vaikeuttaa Javan käyttöä Windows ympäristössä.

6.1.3 Symbian omistajien osuus matkapuhelin markkinoista

Kuva 1. Matkapuhelin valmistajien markkinaosuudet 2001 [7]



Symbianin omistajilla ja lisensoijilla on huomattava osuus vuoden 2001 matkapuhelinmarkkinoista. Toisaalta monet lisensoijista ovat yhteistyössä myös muiden käyttöjärjestelmävalmistajien kanssa. Esimerkiksi Samsung on lisensoinut jo Palm-, Microsoft- ja Symbian-käyttöjärjestelmät. Samsung aikookin olla valmistajana sille järjestelmälle, joka voittaa käyttöjärjestelmäkilpailun [6].

6.2 Symbian-käyttöjärjestelmän tekniikka

Symbian-käyttöjärjestelmä on kehitetty vaativaan käyttöympäristöönsä. Se ei ole pienennetty versio mistään PC-käyttöjärjestelmästä, vaan suunnittelussa on alusta asti huomioitu kannettavien laitteiden pienemmät resurssit. Näin käyttöjärjestelmä osaa tehokkaasti ottaa huomioon käyttöympäristön rajoitteet ja vaatimukset.

Symbian-käyttöjärjestelmä on suunniteltu laajoille kuluttajamarkkinoille. Se on siis pyritty tekemään helpoksi käyttää. Graafinen käyttöliittymä on suunniteltu yksinkertaiseksi ja toimivaksi. [1]

6.2.1 Mobiilin ympäristön rajoitteet

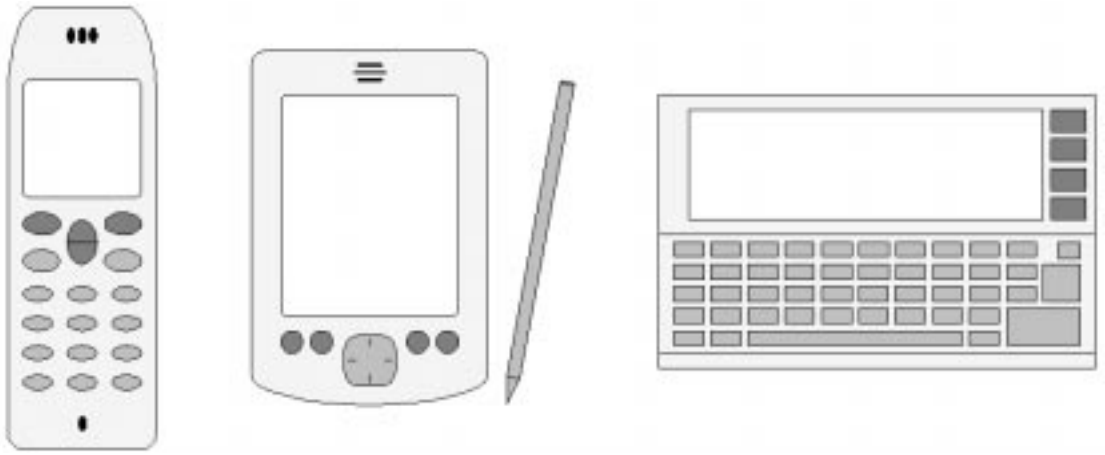
Käyttöjärjestelmän ensimmäinen ja tärkein vaatimus on, että sen pitää olla vakaa. Järjestelmä ei saa mennä lukkoon ja sen pitää pystyä toimimaan jatkuvasti ilman uudelleenkäynnistämistä. Käyttäjän pitää voida luottaa laitteen toimintaan tilanteessa kuin tilanteessa. Järjestelmä ei saa hukata tietoa, eikä puhelintoiminnoissa saa tapahtua virheitä. Symbianin mukaan: ”Vaikka se normaaleille PC-tietokoneita käyttäville ihmisille saattaa tulla yllätyksenä, on vakaan ja kaatumattoman käyttöjärjestelmän rakentaminen aivan mahdollista”. [1]

Kannettavissa laitteissa on myös hyvin rajoittavia tekijöitä. Käyttöjärjestelmän pitää olla riittävän pieni, sillä se sijaitsee ROM muistissa. PC-tietokoneista tuttuja kiintolevyjä mobiililaitteilla ei ole. Laitteessa on myös rajallinen määrä käyttömuistia ja prosessoritehoa. Järjestelmän ajamien prosessien pitää olla myös näiden suhteen säästeliäitä. [1]

Lisäksi rajoittavana tekijänä on energian määrä, koska laitteen vaatima sähköenergia on varastoitava akkuihin. Akkujen koko ei saa kasvaa liian suureksi, sillä ne lisäävät laitteen kokoa ja painoa. Energiavarat ovat siis hyvin rajalliset, joten käyttöjärjestelmä ei saa kuluttaa paljoa energiaa.

Laitteet voivat olla myös kokooonpanoltaa hyvin erilaisia. Eroja voi olla prosessoreissa, muisteissa, näytöissä jne. Käyttöjärjestelmän pitää sopia siis erilaisiin kokoonpanoihin, puhelimista tietureihin ja kommunikaattoreihin. Näissä jokaisessa on eri tyyliset ja muotoiset näytöt ja hallintalaiteet.[4]

6.2.2 Viitetoteutukset



Kuva 2 Symbian-käyttöjärjestelmällä on viitetoteutukset erilaisia laitteita varten. Vasemmalla älypuhelin, keskellä tieturi kynäohjaimella ja oikealla kommunikaattori.

Symbian-käyttöjärjestelmästä on olemassa kolme erilaista viitetoteutusta erilaisia laitetyyppejä varten; älypuhelimiin Pearl, näppäimistöohjattuihin kommunikaattoreihin Chrystal ja kynäohjattuihin tietureihin Quartz. Perusta on sama, mutta käyttöliittymä ja sovellusohjelmisto on näissä erilainen. Viitetoteutukset ovat siis lähtökohta suuniteltaessa käyttöjärjestelmän kokoonpanoja erilaisiin käyttökohteisiin.[3]

Älypuhelimissa näyttö on pieni ja laitteen hallinta tapahtuu puhelimen näppäimistöllä. Älypuhelimien laitevaatimukset ovat pienimmät ja käyttöjärjestelmässä ei ole niin paljoa sovellusohjelmia.

Tietureissa on isompi kosketusnäyttö. Hallintavälineenä toimii osoitinkynä, jolla voidaan kirjoittaa näytölle tai tehdä näytöllä valintoja. Lisäksi tietureissa on usein muutamia erikoisnäppäimiä.

Kommunikaattoreissa on täydellinen näppäimistö. Lisäksi voi olla erikoisnäppäimiä, kuten osoittimen (pointer) ohjausnäppäin. Näyttö on yleensä leveämpi, mutta tarkempi koko ja muoto riippuvat mallista.

6.2.3 Käyttöjärjestelmän rakenne

Symbian-käyttöjärjestelmä on oliosuuntautunut ja perusajatukseltaan tapahtumapohjainen. Verrattuna säiepohjaiseen rakenteeseen tapahtumapohjainen rakenne tarjoaa etua mm. pienempinä yleiskuluina (overhead). Säiepohjaisessa rakenteessa jokainen säie aiheuttaa yleiskuluja.[4]

Taulukko 1. Symbian-käyttöjärjestelmän rakenne kerroksittain [9]

Ohjelmataso	
Java	Yhteydet
Selain	Viestintä
Kommunikointi	
Runko	
Perusta	

Perusta on käyttöjärjestelmän ydin (kernel). Siellä ovat mm. ajonhallinta (run-time), alimman tason turvallisuus, tiedostojärjestelmä ja muistinhallinta. Lisäksi perusta-tasolla valvotaan energian kulutusta.

Runko sisältää ytimen ulkopuoliset, mutta käyttöjärjestelmään oleellisesti liittyvät toiminnot, kuten ohjelmointirajapinnat (API) datan hallintaan, leikepöytään, grafiikkaan, tekstinkäsittelyyn, graafiseen käyttöliittymään yms. käyttöjärjestelmän peruskomponentteihin.

Kommunikointi-tasolla hoidetaan käyttöjärjestelmän yhteyksien luonti, sekä protokollien ja menetelmien hallinta. Kommunikoinnin pohjalla on kolme erityyppistä rakennetta: COMM-palvelu, joka tarjoaa mm. sarjaportin, IrDA:n ja Bluetooth rajapinnat, socket-palvelu jonka päällä ovat WAP, TCP/IP, tekstiviestit ja modeemi sekä viimeisenä puhelinpalvelut, jonka päällä toimivat mm. GSM , GPRS ja Fax. Tämän kerroksen palvelut ovat hyvinkin laitekohtaisia.

Selain-taso sisältää WWW- ja WAP-selaimet.

Viestintä-tasolla huolehditaan viestintäprotokollien, kuten sähköpostin, tekstiviestien ja faksin tarjoamisesta käyttäjälle.

Java-taso tarjoaa J2ME-rajapinnan (Java2 Micro Edition). Tähän kuuluvat mm. PersonalJava- ja JavaPhone-toteutukset (implementation). Java-ohjelmat toimivat tämän kerroksen tarjoamien kirjastojen ja rajapintojen päällä.

Yhteydet-taso toimii välittäjänä vieraiden dataformaattienkuten Microsoft Wordin yhteydessä, sekä rajapinnan PC:n kanssa kommunikointiin.

Päällimmäisenä on **ohjelmataso**, jossa toimivat käyttöjärjestelmän päällä olevat ohjelmat kuten kalenteri, laskin, muistio. Nämä palvelut vaihtelevat viitetoteutusten välillä, sekä tietenkin tuotteittain.

6.3 Symbian-käyttöjärjestelmän ominaisuudet

Symbian pyrkii aina mahdollisimman nopeasti siirtämään uudet langattomaan ympäristöön soveltuvat tekniikat, kuten GPRS ja Bluetooth, käyttöjärjestelmään liitettäväksi. Symbian sisältää käyttöjärjestelmän lisäksi mobiilin laitteen perusohjelmiston, kuten kalenterin, puhelinmuistion, www-selaimen jne.

Käyttöjärjestelmien ominaisuudet eroavat jonkin verran eri versiossa. Psionin alkuperäiseen EPOC-käyttöjärjestelmä, johon Symbian perustuu,

ehti versioon 5. EPOC tuki vain yhtä viitetoteutusta, jolloin laitteessa oli sekä kynäohjain että täydellinen näppäimistö.

Ensimmäinen avoin versio oli 6.0. Sen mukana EPOC-käyttöjärjestelmän nimi muuttui Symbian-käyttöjärjestelmäksi. Tässä Symbian tuki jo kahta viitetoteutusta, kynäohjattavaa tieturia ja kommunikaattoria. Kommunikointiominaisuudet myös paranivat. Lisäksi järjestelmä tuki puhelinominaisuuksia. Käyttöjärjestelmään integroitiin WAP ja Bluetooth. Myös turvallisuusominaisuudet paranivat ja tuettuina olivat mm. SSL, HTTPS ja WTLS. Lisäksi tuli useita muita parannuksia käytettävyyteen, kuten kyky tunnistaa useampia tiedostotyyppejä, PersonalJava- sekä JavaPhone-tuki ja parannettu graafinen käyttöliittymä.[1]

Versiossa 6.1 mukaan tuli myös tuki GPRS:lle ja WAP 1.2. [1]

Keväällä 2002 Symbian-käyttöjärjestelmä on tullut jo versioon 7.0. Versio 7.0 tukee jo kaikkia viitetoteutuksia ja vuoden 2002 aikana markkinoille tulee tuote jokaisesta viitetoteutuksesta, esimerkiksi Nokia 7650 älypuhelin, Sony Ericsson P800 tieturi ja Nokian 9210i kommunikaattori. Uuden version merkittäviä parannuksia ovat muun muassa multimediaviestit, parantuneet WAP- ja WWW-selaimet sekä tuki IPv6:lle. Lisäksi tarjolla on GPRS- ja EDGE-tuki sekä SynchML. [1]

Laitteiden ominaisuudet eroavat myös tuotteittain. Kaikissa tuotteissa ei ole esimerkiksi uusimpia Bluetooth- tai GPRS-ominaisuuksia. Eroja on myös prosessoreissa ja muisteissa. Käyttöjärjestelmä on noin 80 % sama kaikissa samaa käyttöjärjestelmä versiota käyttävissä laitteissa. Noin 20 % on sitten laitekohtaisia ominaisuuksia ja sovelluksia, joita kyseisessä laitteessa tarjotaan.

6.4 Ohjelmistosuunnittelu Symbian ympäristöön

Symbian-käyttöjärjestelmä on C++-pohjainen, eli sille luonnollinen ohjelmointi kieli on C++. Sillä saavuttaa myös kaikkein suurimman tehokkuuden.

Symbianiin on alusta asti voinut tehdä ohjelmia myös Javalla. Java-toteutukset kuluttavat hieman enemmän laitteen resursseja, kuin C++-ohjelmat. Java ohjelmien etuna on helppo ajettavuus ja siirrettävyys eri ympäristöihin; ’Write once run everywhere’.

Ohjelmisto, jolla voi tehdä Symbianiin ohjelmia Visual Basicillä, on kokeiluvaiheen testauksessa. Tästä työkalusta on (keväällä 2002) saatavilla ensimmäiset versiot, joilla ohjelmia voi tehdä vasta Nokia 9200-sarjan puhelimiin. Nokian ilmoituksen mukaan on tarkoitus, että tämä tulee mahdolliseksi muihinkin Symbian-laitteisiin. [1] [8]

Laitteissa toimivien ohjelmistojen lisäksi Symbian-tuotteisiin voi tehdä myös palvelinpohjaisia sovelluksia. Tällöin Symbian-laite toimii asiakkaan ominaisuudessa. Palvelinohjelmistoja voi toteuttaa esimerkiksi joko WAP-protokollalla tai käyttäen HTML-kielisiä sovelluksia. [4]

6.4.1 Ohjelmistojen sovittaminen Symbianille

Ohjelmat, jotka tehdään Symbianille, voivat aina vaatia pienen sovittelun, jotta ne toimivat ja näyttävät hyvältä kunkin laitteen käyttöliittymässä. Laitteissa voi olla hyvinkin erikokoiset näytöt ja vaihtelevat hallintalaitteet.

C++- ja Java-ohjelmille sovittaminen tarkoittaa parhaimmillaan vain graafisen käyttöliittymän sovittamista kullekin laitemallille. Tällöin ohjelma kannattaa suunnitella niin, että ohjelman runko on erillään ohjelman käyttöliittymästä. Vaadittava sovittaminen ei ole iso tehtävä oikein suunnitellulla käyttöliittymällä.

Palvelinpohjaisissa WAP- tai HTML-kielisissä sovelluksissa palvelu pitää sovittaa Symbian laitteen ja selaimen ominaisuuksien mukaan. Esimerkiksi framien käyttö pienellä näytöllä ei ole kovinkaan suotavaa.[1] [4]

6.4.2 Selainversioiden mukaan sovittaminen

Versiossa 6.0 tuetaan WAP-versiota 1.1 ja HTML-versiota 3.2. WEB-selain ei vielä tässä versiossa tue Scriptejä.

Versiossa 7.0 tuetaan WAP-versiota 1.2.1 ja HTML-versiota 4.1. Lisäksi Symbian 7.0 tukee CSS-tyylitiedostoja, XML:ää ja XHTML:ää. WEB-selain tukee myös rajoitetussa määrin JavaScript-kieltä.[1]

Molemmissa sekä version 6 että version 7 selaimissa on tuettuna SSL ja HTTPS.

6.4.3 Emulaattorit

Symbian tarjoaa kaikille viitetoteutuksille emulaattoreita. Emulaattoreilla voi kokeilla ja testata Symbian-ympäristöön tehtyjä ohjelmia ja tuotteita. Myös monet Symbian-käyttöjärjestelmillä toimivia laitteita tarjoavat yritykset tarjoavat emulaattoreita, joilla ympäristöön tehtyjä tuotteita voi kokeilla.

Tarjolla olevat emulaattorit tukevat sekä Java että C++-ympäristössä toimivia ohjelmia.

Emulaattoreilla on myös mahdollista testata WAP- ja HTML-pohjaisia palveluita. Emulaattorin konfiguroiminen näitä varten on kuitenkin kohtuullisen vaikeaa, vaikka aiheesta löytyykin dokumentteja.

Nokialla Symbian tuotekehityksen tuki ja emulaattorit löytyvät http://www.forum.nokia.com sivustoilta. Symbianin viitetoteutusten mukaiset emulaattorit ovat saatavilla http://www.symbian.com sivustoilta.

Sekä Symbianilta että Nokialta löytyy myös hyvä dokumenttikirjasto ja tukea ohjelmistosuunnittelijoille. Niiden avulla on helppo päästä alkuun ohjelmistojen ja tuotteiden kehittämisessä.

6.5 Symbian tuotteet

Ensimmäiset EPOC-käyttöjärjestelmää käyttäneet tuotteet olivat PSIONin taskutietokonetuotteet ja Ericssonin MC 218-taskutietokone. Niissä ei ollut

omia puhelinominaisuuksia, vaan ne vaativat esimerkiksi IrDA-yhteyden modeemiin. [3]

Vuonna 2000 julkaistiin ensimmäinen Symbian-puhelin. Se oli Ericssonin WAP-puhelin R380. Ericsson R380-mallin käyttöjärjestelmä ei ollut vielä avoimen Symbian-standardin mukainen. [1]

Nokia 9210 oli ensimmäinen avointa Symbian-standardia käyttänyt puhelin. Nokian 9210-mallit käyttivät Symbian-käyttöjärjestelmän versiota 6.0. Nokian 9210-mallin mukana Nokia tarjosi jo laajaa kehitystyökaluohjelmistoa ja emulaattoreita. [1][4]

6.5.1 Tulevat tuotteet

Syksyllä 2001 Nokia julkisti seuraavan Symbian-käyttöjärjestelmää käyttävän puhelimensa. Se oli kuvaviestintään kykenevä älypuhelin 7650, jonka pitäisi tulla myyntiin vuoden 2002 toisella neljänneksellä. Puhelin tarjoaa jo huomattavia uusia ominaisuuksia kuten GPRS, multimediaviestit ja Bluetooth. Puhelimen näyttö on suhteellisen, pieni 176x208 pistettä. Puhelimen muisti on 4 MB, joten kovinkaan isoja ohjelmia siihen ei voi tehdä, mutta ominaisuuksiltaan ja jo mukavasti toimivalla kalenterilla varustettuna se alkaa olla jo lähempänä tieturia, kuin tavallista puhelinta. 7650 on ensimmäinen 2.5G puhelin. [4][5]

Kevään 2002 julkistuksia on Nokia 9210i, jossa Nokian kommunikaattoria on hieman uudistettu, muistia lisätty ja Symbian-käyttöjärjestelmä on jo versiota 7.0.

Keväällä 2002 julkistettiin myös Sony Ericsson P800 tieturi, joka Nokian 7650 puhelimen tavoin tukee kuvaviestejä. P800 käyttää Symbian 7.0 versiota. Siinä on jo isompi 208x320 pisteen näyttö. P800 tukee lisäksi i-mode palveluita.[2]

6.6 Symbian Markkinat

Symbian-käyttöjärjestelmän kolme viitetoteutusta [kuva 1] kilpailevat periaatteessa kahdella markkinasegmentillä, jotka kylläkin alkavat koko ajan lähestyvät toisiaan. Puhelimiin tulee jatkuvasti lisää ominaisuuksia ja niiden käytettävyys paranee. Tieturit ja kommunikaattorit kilpailevat keskenään samoilla apajilla hieman erilaisin toteutuksin. [4]

6.6.1 Puhelinmarkkinat

Puhelimissa kilpailu on pääasiassa valmistajakohtaisia käyttöjärjestelmäratkaisuja vastaan. Lisäksi juuri on julkaistu Microsoftin pocket PC Phone Edition eli puhelin ominaisuuksilla varustettu versio Microsoftin tieturista.

Koska puhelinmarkkinoilla Symbianin omistajilla on hallussaan tällä hetkellä noin 70 % (HS 16.3.2002), on Symbianilla sillä saralla kohtuullisen hyvä asema.

6.6.2 Tieturimarkkinat

Tietureissa tilanne on hieman toinen. Siellä Symbianin kanssa kilpailevia isoja käyttöjärjestelmiä on kaksi. Tietureissa ja kommunikaattoreissa kilpailevia ratkaisuja ovat tarjonneet Palm ja Microsoft. Lisäksi on joitain tuotteita, joissa toimii mm. Linux-pohjainen käyttöjärjestelmä.

Näissä tuotteissa Palm on ollut markkinoiden hallitsija, mutta se on nyttemmin jäänyt kehityksessä. Tieturimarkkinoilla tämän hetken kuumin tekijä on Microsoft. Pocket PC tuotteillaan se on nopeasti lisännyt markkinaosuuttaan.

Juuri Microsoftin Pocket PC Phone Edition, eli puhelin ominaisuuksilla varustettu Pocket PC, on Symbianille mahdollisesti kovin haastaja. Näiden Microsoftin käyttöjärjestelmien selain yms. ominaisuuksia on kehuttu, mutta koska käyttöjärjestelmä on alunperin kehitetty tietokoneisiin, se ei ole parhaimmillaan puhelinkäytössä. Pocket PC laitteet vaativat myös enemmän muistia ja nopeamman prosessorin toimiakseen, kuin Symbian laitteet.

Nopeasti etenevillä markkinoilla tuotteiden myyntiosuudet vaihtelevat aina uusien mallien ja ominaisuuksien tullessa markkinoille. Symbianin menestys on kuitenkin eniten riippuvainen alan yleisestä menestyksestä. Mikäli kolmannen sukupolven verkot lähtevät kohtuullisella nopeudella liikkeelle, on Symbian-käyttöjärjestelmällä tulevaisuudessa kysyntää.

6.7 Symbian liiketoimintamallit

Symbian arkkitehtuuri tarjoaa markkinoita kaikille osapuolille.

- Laitevalmistajille (lisensoijille)
- Operaattoreille
- Ohjelmistotuottajille
- Sisällön tuottajille

Avoimelle standardille on helppo kehittää tuotteita ja palveluita, kun jokaista tuotetta ja palvelua ei tarvitse räätälöidä eri laitteille. Edut tulevat siis kaikille helpompana tuotekehitysprosessina ja laajempana asiakaskuntana.

Toisaalta uusi monipuolisempi käyttöjärjestelmä voi tarjota yllätyksiäkin. Nokian 7650 mallille on esimerkiksi kehitetty Javalla toimiva GPRS-paketteina viestejä lähettävä ohjelmisto. Sillä käyttäjät voivat lähettää viestejä tekstiviestijärjestelmän (SMS) ohi, jolloin operaattori ei voi laskuttaa tekstiviestipalvelusta vaan pelkästään GPRS-pakettien välittämisestä.

Mahdollisia liiketoimintamalleja Symbian arkkitehtuurille ovat:

- Teksti- ja multimediaviestit
- Sähköposti
- WWW ja WAP selailu
- Personointi (soittoäänet, kuvat yms.)

- Maksu per lataaminen tai maksu per ohjelman käyttö
- Alueriippuvaiset latauspalvelut (kartat, ravintolaoppaat yms.)
- Yritysverkkojen laajentaminen langattomalle alueelle
- Pelit

Lisäksi Symbian tarjoaa pohjan keksiä ja kehittää aivan uudenlaisia palveluita ja liiketoimintamalleja. [10]

6.8 Symbianin tulevaisuus

Symbian on houkutellut monia yhteistyökumppaneita ja se on lisensoitu hyvin monien yritysten taholta. Markkinoita sille siis pitäisi olla.

Kehityksessä on silti ollut jonkin verran kankeutta. Nokia on reagoinut hitaaseen kehitykseen lisensoimalla omaa Symbianiin pohjautuvaa Series 60-käyttöjärjestelmää. Series 60 on käytössä Nokian 7650 mallissa.

Symbianin tuleva kehitys on kuitenkin vielä avoin. Microsoft tarjoaa Pocket PC tuotteillaan kovan vastuksen. Mikäli jokin iso puhelinvalmistaja menee Microsoftin mukaan, voi se tietää vaikeuksia Symbianin kehitykselle. Lisäksi Symbianin eri omistajien halu vetää kehitystä omiin tarkoitusperiin sopivaksi vaikeuttaa ja hidastaa kehitystä. Menestys onkin pitkälle kiinni yritysten välisestä 'politiikasta'. Lisäksi Symbian kaipaa isojen menestystuotteiden syntymistä.

6.9 Sanasto

6.9.1 Suomennokset

Ajonhallinta – Run-time

Käyttöjärjestelmän ydin – Kernel

Kommunikaattori – Communicator (Chrystal)

Käyttöjärjestelmä – Operating System

Perusta – Base

Runko – Framework

Selain – Browser

Säie – Thread

Tieturi – PDA (Personal Digital Assistant), (Quartz)

Viitetoteutus – DFRD Device Family Reference Designs

Yleiskulut – Overhead (Prosessien vaatimat suorituksen aikaiset resurssit)

Älypuhelin – Smartphone (Pearl)

6.9.2 Lyhenteet

API – Application Program interface

EDGE – Enhanced Data Rates for Global Evolution

GPRS – General Packet Radio Service

HTTP – HyperText Transfer Protocol [11]

HTTPS – HyperText Transmission Protocol, Secure [11]

IrDA – Infrared Data Association

J2ME – Java 2 Micro Edition

SSL – Secret Socket Layer

TCP/IP – Transmission Control Protocol over Internet Protocol

WAP – Wireless Application Protocol

WTLS – Wireless Transport Layer Security

6.10 Lähteet

[1] http://www.symbian.com

[2] http://www.sonyericsson.com

[3] http://www.ericsson.com

[4] http://forum.nokia.com

[5] http://www.nokia.com

[6] http://www.tietokone.fi

[7] http://www4.gartner.com/5_about/press_releases/2002_03/pr20020311a.jsp

[8] http://www.symbian.com/news/2002/appforge-feat.html

[9] Generic Tecnology overview, Nokia 9210 SDK

[10] http://download/forum.nokia.com

[11] http://burks.bton.ac.uk/burks/foldoc

7. WAP

Nykyisin Internet on useille ihmisille välttämätön apuväline. Laitteet ja tekniikat kehittyvät huimaa vauhtia ja markkinoilla on paljon erilaisia selaimia, joiden avulla Internetiä voi käyttää hyväksi. Varsinkin puhelimien ja kämmentietokoneiden lisääntyminen on luonut uudenlaisia haasteita palveluiden kehittämiseen. Reaaliaikapalveluiden kysyntä kasvaa ja liikkuvat ihmiset tarvitsevat tietoa ajasta ja paikasta riippumatta.

Jotta vaatimuksiin voidaan vastata, tarvitaan tekniikka, jolla langaton tiedonsiirto on tarpeeksi tehokasta. Rajoituksensa asettavat myös laitteiden koko ja ominaisuudet sekä palveluiden raskaus.

Käyttäjille tärkeimpiä asioita ovat palvelun saatavuus, helppo ja nopea käytettävyys sekä alhaiset kustannukset. Palvelun tarjoajan näkökulmasta huomionarvoisia asioita ovat palveluihin käytettävät resurssit ja vaadittavat tukitoimet.

7.1 Johdanto WAP:iin

WAP on ympäristö ja joukko protokollia, jotka mahdollistavat langattomien laitteiden pääsyn Internetiin ja muihin kehittyneisiin puhelinyhteyspalveluihin. WAP:in pääasiallinen tarkoitus on luoda ympäristö, joka on täysin riippumaton laitevalmistajista, laitteista ja käytetyistä teknologioista. Käytännössä tämä tarkoittaa sitä, että palveluja voidaan käyttää kaikilla laitteilla riippumatta niiden valmistajasta ja mallista.

WAP on maailmanlaajuinen standardi, jota ei valvo mikään yksittäinen yritys. Suuret yritykset, kuten Ericsson, Nokia, Motorola ja Unwired Planet perustivat WAP-foorumin vuonna 1997 tarkoituksenaan luoda ja kehittää laaja-alainen spesifikaatio erilaisille palveluille langattomassa ympäristössä.

WAP määrittelee joukon protokollia, yhteyden, tiedonsiirron, turvallisuuden ja siirtokerroksen, jotka mahdollistavat eri valmistajien ja operaattoreiden luoda palveluja ja laitteita, jotka ovat keskenään yhteensopivia langattomassa maailmassa. Nykyisin tähän foorumiin kuuluu satoja eri kategorioiden edustajia, mukaan lukien operaattoreita, palvelun tarjoajia, ohjelmistotaloja ja laitevalmistajia.

Edellä mainittujen asioiden lisäksi WAP määrittelee langattoman sovellusympäristön, WAE:n (Wireless Application Environment), jonka tarkoituksena on mahdollistaa kehittyneitä lisäpalveluja, kuten sähköposti, WWW:n ja matkapuhelimen välinen viestintä ja matkapuhelin–telefax yhteydet.

Tällä hetkellä WAP:lla on oikeastaan vain yksi vaihtoehtoinen kilpaileva tekniikka. Tämä on LEAP (Lightweight Extensible Agent Platform).

Muiden mahdollisuuksien puuttuminen johtuu suurelta osin siitä, että tekniikoiden kehittäminen ja standardointi on erittäin vaikeaa ja aikaa vievää toimintaa.

7.2 WAP:in edut

WAP tuo verkko-operaattoreille mahdollisuuden pienentää kustannuksia vähentämällä fyysisiä linjoja, ja käyttäjille lisää erilaisia ja parempia mobiilipalveluja, kuten esimerkikisi voice-mail. WAP:in siirtomekanismi on optimoitu langattoman verkon eri osille. Asiat tekee käteväksi se, että uusien palveluiden ja ohjelmistojen käyttöönotto on helppoa ja nopeaa, eikä niitä varten tarvitse tehdä muutoksia infrastrukstuuriin tai käytettäviin päätelaitteisiin.

Käyttäjille WAP luo mahdollisuuden ajasta ja paikasta riippumatta päästä helposti ja vaivattomasti kiinni Internetin tärkeisiin palveluihin, kuten pankkipalveluihin, viestintään ja erilaisiin viihdesovelluksiin. Lisäksi, koska WAP on avoin standardi ja useat valmistajat tukevat järjestelmää, on päätelaitteiden valinta vapaata. WAP ei siis ole riippuivainen eri valmistajista.

Myös verkkostandardien osalta WAP on riippumaton. Tämä tarkoittaa pääasiassa sitä, että WAP tukee erilaisia verkkoratkaisuja, jolloin järjestelmän käyttö ei rajoitu runkoverkkojen tukemattomuuteen.

7.3 WAP sovellukset ja laitteet

WAP sovellukset luodaan vielä tällä hetkellä WML- merkkikielellä (Wap Markup Language), joka on samankaltainen kuin XML (eXtensible Markup Language). Tulevaisuudessa WML korvautuu suurelta osin XHTML:llä (tästä tarkemmin kappaleessa 2) ja samalla palvelut muuttuvat XML-pohjaisiksi. WML on optimoitu puhelimien mikroselaimille. Sovelluksia voidaan ohjelmoida kokonaan WML:n avulla, tai konvertoida suoraan HTML:stä.

WAP-sovellukset ovat samantyyppisiä kuin on totuttu näkemään normaalin Internetin tapauksessa, kuitenkin sillä erotuksella, että ne on suunnattu erilaisille päätelaitteille. Tämä tarkoittaa sitä, että sovelluksissa joudutaan tarkastelemaan niiden vaatimia resursseja, koska WAP-päätelaitteet ovat usein pieniä ja suhteellisen tehottomia verrattuna kiinteän yhteyden laitteisiin. Vielä tämän hetken mobiililaitteet eivät tehoiltaan riitä tulkitsemaan palveluita, jotka ovat raskaita ja paljon grafiikkaa tai liikkuvaa kuvaa sisältäviä.

Kuva1: Nokia 6250 WAP-puhelin

WAP käyttää hyväkseen Internet- standardeja, kuten UDP (User Datagram Protocol), IP (Internet Protocol) ja XML (eXtensible Markup Language). Monet WAP:in käyttämät protokollat, esim. HTML ja TLS (Transport Security Layer), perustuvat myös Internetissä käytettyihin, mutta ne on optimoitu langattomaan käyttöön tuloksena pieni kaistanleveys ja korkea latenssi. Normaalit Internet-standardit ovat langattomassa verkossa tehottomia, koska ne vaativat suuria määriä dataa siirrettäväksi. Esimerkiksi normaalia HTML-sisältöä ei voi tehokkaasti selata pienillä päätelaitteilla, kuten puhelimilla.

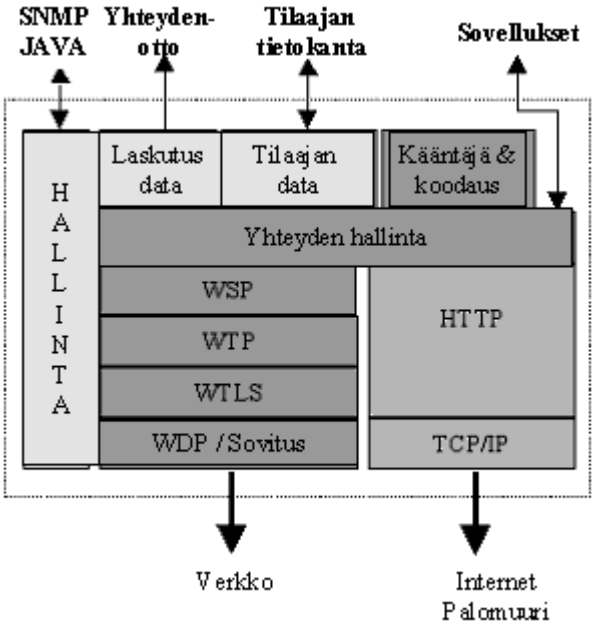
WML ja WMLScript ovat merkkikieliä, joilla luodaan WAP-sovellusten käyttöliittymä ja sisällön esitystapa. Niiden avulla sovellukset optimoidaan käyttämään pieniä näyttöruutuja ja palveluiden käyttäminen eli navigointi luodaan siten, että sen voi suorittaa vaivattomasti yhdellä kädellä. WAP-sisältö skaalautuu kahden rivin tekstipohjaisista näytöistä aina täysgraafisiin älypuhelimiin ja kommunikaattoreihin.

WAP:in protokollapino on suunniteltu minimoimaan tarvittava kaistanleveys ja maksimoimaan langattomien verkkotyyppien määrä, jotka voivat lähettää WAP-sisältöä. Näitä verkkoja ovat mm. GSM-verkot (900, 1800, 1900 MHz), Digital European cordless communication (DECT), time-division multiple access (TDMA) ja Code Division Multiple Access (CDMA). Tämän lisäksi myös kaikki verkkotekniikat ovat tuettuna mukaan lukien Short Message Service (SMS) ja General Packet Radio Service (GPRS).

7.4 WAP arkkitehtuuri

WAP perustuu kerrokselliseen arkkitehtuuriin, jossa jokainen kerros voi kehittyä riippumatta toisista. Tämän vuoksi on mahdollista ottaa käyttöön uusia protokollia tarvitsematta tehdä suuria muutoksia muihin kerroksiin.

Arkkitehtuuri toimii siten, että kun mobiililaite tuottaa kyselyn sivusta tai palvelusta, tämä lähetetään url-osoitteena läpi operaattorin verkon WAP-yhdyskäytävään. Kyseinen yhdyskäytävä on rajapinta operaattorin ja Internetin välillä.



Kuva 2. WAP arkkitehtuuria

WDP eli WAP Datagram Protocol on siirtokerros, joka lähettää ja vastaanottaa viestejä minkä tahansa saatavilla olevan verkon kautta.

WTLS eli Wireless Transport Layer Security on valinnainen turvallisuuskerros. Sen ominaisuutena on salausmekanismi, jonka avulla voidaan turvata suojattu palveluiden siirtäminen.

WTP eli Wap Transaction Protocol on eräänlainen tukikerros, joka tukee varsinaista siirtokerrosta lisäämällä siihen mm. siirron luotettavuutta.

WSP eli Wap Session Protocol on kerros, joka mahdollistaa tehokkaan tiedonsiirron sovellusten välillä.

HTTP rajapinta on tarkoitettu palvelemaan kyselyjä, joita mobiililaitteet tekevät Internetissä.

7.5 WAP:in tulevaisuus

Koska langattomien laitteiden ja järjestelmien lukumäärä kasvaa koko ajan, on odotettavissa, että niitä varten luotavia standardeja ja ideoita kehitetään jatkuvasti. Tällä hetkellä ainoa syy todellisen läpimurron puuttumiseen WAP:in kohdalla lienee se tosiasia, että tämän hetken tekniikalla ei pystytä tuottamaan vastaavanlaisia palveluja, kuten normaalissa Internetissä. Tässä mentiin pahasti harhaan muutama vuosi sitten, kun yleisesti mainostettiin WAP:ia lupaamalla täydellinen Internet taskuun. Koska tämä ei pitänyt paikkaansa, monien kiinnostus lopahti asiaa kohtaan ja syntyi tietynlainen lama, koska käyttäjille mahdollistettiin ainoastaan joitakin Internetistä tuttuja peruspalveluja.

Tulevaisuudessa kuitenkin laitteet kehittyvät ja vaatimukset kasvavat entisestään. Etenkin GPRS:n myötä on WAP:in suosion ennustettu kasvavan suuresti. WAP:in kehittyessä odotetaan eri laitevalmistajien tekevän suuriakin muutoksia tuotteisiinsa. Pääasiallisesti muutokset koskevat laitteiden kokoa ja tehoa sekä näyttöjen kokoa. Nämä asiat tekevät erilaisten kehittyneempien palvelujen tarjoamisen mahdolliseksi WAP:in avulla.

WAP-palveluja pyritään jatkuvasti viemään samaan suuntaan kuin Internet-palvelujakin. WAP:in tapauksessa ideana on saada mahdollisuus käyttää palveluja sekä puhumalla, eli äänirajapinnan kautta, sekä ”normaalimmin” data-rajapintaa hyväksi käyttäen. Palvelujen selaamista kehitetään yhä helpompaan ja nopeampaan suuntaan, jolloin käyttöönottokynnys madaltuu.

Varsinainen valttikortti WAP:lle lienee kuitenkin reaaliaikapalveluiden yleistyminen. Uutiset, pörssikurssit, sää, yms. ovat asioita, joita hyvin monet ihmiset haluavat saada tietoonsa paikasta ja ajasta riippumatta. Tällaisiin palveluihin WAP on erityisen soveltuva, koska jo olemassa olevat kiinteän linjan palvelut pystytään muuntamaan mobiiliin maailmaan soveltuviksi.

Tällä hetkellä noin 75 prosenttia maailman matkapuhelinyhtiöistä tukee WAP:ia. Tämä asia, yhdessä WAP:in valtavan kehityspotentiaalin kanssa, saa WAP:in tulevaisuuden näyttämään erittäin valoisalta. Onkin arvioitu, että vuoteen 2004 mennessä WAP-käyttäjien määrä kasvaa pelkästään Länsi-Euroopassa yli 200 miljoonaan (lähde: Cahners, In-Stat Group).

8. XHTML

Koska edellisessä osiossa mainitut mobiililaitteet ovat toimivuudeltaan ja ominaisuuksiltaan rajallisia, eivät ne pysty tehonsa puolesta tulkkaamaan huonoa tai virheellistä merkintäkieltä. On hyvin yleistä, että WWW-sivustot sisältävät virheellistä tai epämääräistä HTML:ää. Tämän vuoksi on kehitelty merkintäkieli, jossa on edeltäjiensä parhaat puolet ja vahvuudet. Tätä kieltä kutsutaan XHTML:ksi.

Normaalisti mikrotietokoneissa pyörivät selaimet pystyvät tulkitsemaan sivuja, jotka on määritelty epätarkasti tai niissä on muita virheitä. Kuitenkaan mobiilimaailmassa ei olla vielä niin pitkällä, että päätelaitteiden tehokkuus ja resurssit yltäisivät kilpailemaan vastaavien tietokoneiden tai selaimien kanssa. Tosin sanoen mobiililaitteet eivät ”jaksa” tulkata huonolaatuista kieltä. XHTML:llä luotujen sovellusten ja sivujen avulla pienetkin laitteet pystyvät omilla vahvuuksillaan toimimaan mahdollisimman hyödyllisesti.

8.1 Johdanto XHTML:ään

XHTML on web-standardi ja sen versiosta 1.0 tuli W3C-suositus tammikuussa vuonna 2000 (WWW Consortium). W3C suositus voidaan antaa tuotteelle, joka täyttää kolme ehtoa. Spesifikaation on oltava stabiili, W3C jäsenet ovat arvostelleet ja katselmoineet sen ja sen on oltava web-standardi.

XHTML on uuden sukupolven HTML, tiedon merkintäkieli, jonka tarkoitus on korvata vanha HTML. HTML suunniteltiin pääasiassa PC-laitteita varten, jolloin ei otettu huomioon muuttuvia alustoja, joita webissä ja puhelimissa on. Kaikessa yksinkertaisuudessaan XHTML:ää voidaan kutsua HTML:n ja XML:n yhdistelmäksi. Kieli sisältää HTML:n kaikki ominaisuudet, johon on lisätty XML:stä tuttua syntaksia. Voidaan sanoa, että XML on merkintäkeino, jolla on tarkoitus kuvata tietoa ja tiedon rakennetta, kun taas HTML on kehitetty saman tiedon esittämiseen ja näyttämiseen.

8.2 XHTML vs. HTML

XHTML:n ja HTML:n syntaksi on samankaltaista ja ulkoisesti yhtenevää. Suurimmat erot ovat siinä, että XHTML on erittäin tarkka rakenteen oikeellisuudesta ja että kaikkien tagien on oltava pienillä kirjaimilla. Tästä johtuen XHTML:n avulla luodut dokumentit ovat niin sanotusti ”hyvin muodostuneita” (engl. well-formed).

Voidaan sanoa, että XHTML on HTML, joka on määriteltu XML sovellukseksi. Kaikki XML:ää tukevat laitteet pystyvät tulkitsemaan XHTML:ää.

XHTML:n tapauksessa on tärkeää, että käytetyt elementit ovat oikeassa järjestyksessä niiden esiintymisen mukaan.

```
<b><i>Teksti on paksua ja italic-tyyppistä</b></i>       -> HTML
<b><i>Teksti on paksua ja italic-tyyppistä</i></b>       -> XHTML
```

Ylemmässä esimerkissä ei olla erityisen tarkkoja tagien loppujärjestyksestä. Tämä on tyypillistä epätarkkaa html:ää. Alemmassa merkintöjen sisennys ja ilmestymisjärjestys määrää lopputagien käytön. Tämä on xhtml:n mukaista.

Myös muotoseikat ovat tärkeitä. Kaikkien kirjoitettujen tagien (esim.) täytyy olla pienillä kirjaimilla. Tämän lisäksi kaikki elementit pitää sulkea lopetusmerkillä (esim.), eli avoimia rivejä ei sallita.

HTML-sivu toimii vaikka siinä olisi virheitä, mutta XHTML-tyyliä käyttäen ei virheitä voi olla. Virheiksi käyvät vaikkapa normaalit kirjoitusvirheet.

8.3 XHTML:n rakenne

XHTML-dokumentti sisältää kolme eri pääosaa. Dokumentin tyyppi (Doctype) määrittelee dokumentissä käytettävän tyyppiluokituksen. Otsikko (Head) kertoo dokumentin aiheen ja varsinainen runko (Body) käsittää dokumentin todellisen sisällön.

Dokumentin tyyppi sisältää käytettävän kielen versiotiedon sekä kieliopin tarkkuuden. Loppuosa dokumentista, eli otsikko ja runko näyttävät normaalilta HTML-kieleltä.

Esimerkki dokumentin tyyppimäärittelystä:

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

Alussa määritellään, että dokumentti on html-kieltä. Tämän jälkeen määritellään käytettävän xhtml-kielen versio ja sen kieliopin tarkkuus ja se, missä määritelty kielioppi sijaitsee.

Kuten XML:ssä, myös XHTML:ssä on aina määriteltävä DTD (Document Type Definition), eräänlainen kielioppi, jota käytetään dokumenttien pohjana. Tämä kielioppi määrittelee täsmällisesti käytettävän rakenteen ja sallitun syntaksin sekä sisällön muodon SGML:n (Standard Generalized Markup Language) avulla.

XHTML:n standardi määrittelee kolme erilaista DTD:tä. Ne ovat Ehdottoman tarkka (Strict), Vaihteleva (Transitional) sekä Kehysjoukko (Frameset). Yleisin näistä on DTD Transitional.

Strict:

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

Tällaista kielioppia käytetään silloin, kun halutaan erittäin puhdasta merkintää, joka ei sisällä minkäänlaista epäjärjestystä. Tällöin säännöt kielen suhteen ovat tiukimmat.

Transitional:

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Tätä käytetään silloin, kun halutaan hyödyntää HTML:n esitysominaisuuksia. Toisin sanoen silloin säännöt eivät ole tiukimmat mahdolliset, jolloin joitakin HTML:n ”vikoja” voidaan katsoa läpi sormien.

Frameset:

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd">
```

Tätä käytetään, kun halutaan käyttää HTML-kehyksiä jakamaan selain useampiin erillisiin kehyksiin.

8.4 XHTML:n käyttökohteet

XHTML:n käyttökohteina ovat Internet-sivustot, joita on tarkoitus selata suhteellisen tehottomalla ja pienellä päätelaitteella. Koska nämä laitteet eivät pysty kontrolloimaan sivustojen kielten oikeellisuutta, on tarvetta merkintäkielelle, joka on niin tarkka oikeellisuudesta, että virheitä ei synny. Normaalit mikrotietokoneiden selaimet pystyvät tulkitsemaan XHTML:ää. Muilta laitteilta tarvitaan periaatteessa jonkinlainen XML-tuki. Uusimmissa laitteissa, esimerkiksi puhelimissa on jo nykyisin XHTML-mikroselain, joka on täysin yhteensopiva nykyisen WAP-sisällön kanssa ja tukee lisäksi XHTML-standardia.

Sovellusten kehittäjät, jotka tarvitsevat erityistä rakennetta ja kuvaamisen helppoutta valitsevat tällä hetkellä XHTML:n kuvauskielekseen. Mutta erityisesti myös uudet mobiililaitteet, jotka tukevat tätä standardia, hyötyvät siitä. Tietyllä tavalla voidaan sanoa, että XHTML on hyödyllisimmillään juuri nyt, koska mobiililaitteiden ominaisuudet eivät ole vielä tasolla, jolla niitä tarvittaisiin. XHTML-standardi on suureksi osaksi apuväline, jolla

voidaan välttää turha tehokkuuden tarve tarjoamalla silti palveluja, jotka ovat tuttuja myös kiinteällä kalustolla.

8.5 XHTML:n tulevaisuus

XHTML:n käytettävyys perustuu kolmeen pääasiaan. Ensinnäkin sitä on helppoa muokata ja sen rakenne on yksinkertaista toteuttaa. Normaaleilla XML-työkaluilla pystytään tuottamaan kyseisiä dokumentteja tehokkaasti. Toiseksi se on koko ajan yleistyvä, kehittyvä ja tulevaisuudessa todennäköisesti erittäin käytetty kieli. Ja kolmanneksi sen säännöt vähentävät turhaa kuormitusta päätelaitteilta.

Tulevaisuudessa laitteet ja palvelut kehittyvät jatkuvasti rinnakkain. Laitteiden tehot kasvavat, mutta samalla myös palveluiden vaativat resurssit kasvavat. Optimoimalla käytettyjä palveluja ja välttämällä turhan kuormituksen kasvua, pystytään tinkimään tehon- ja resurssien kulutusta. Tämä suuntaus tuskin tulevaisuudessakaan häviää. On jopa odotettavissa, että käytetyt mentelmät leviävät yhä enemmän ja samansuuntaisiin asioihin kiinnitetään kasvavassa määrin huomiota.

XHTML:n kehittyessä ja yleistyessä, sen käytön edut varmasti painavat vaakakupissa entistä enemmän. Nokia, Motorola, Siemens ja Ericsson sekä useat muut mobiilitekniikkayritykset ja operaattorit ovat ilmoittaneet tukevansa XHTML:ää mobiilipalvelujen esitysmuotona. Koska se on WAP:in luonnollinen kehityssuunta ja se tuo luontevasti WAP- ja kiinteän Internetin yhteen, on XHTML tulevaisuudessa erittäin käyttökelpoinen väline web-maailmassa.

8.6 Lyhenteet

XHTML	= eXtensible Hyper Text Markup Language
XML	= eXtensible Markup Language
DTD	= Document Type Definition
WAP	= Wireless Application Protocol
WML	= WAP Markup Language
WAE	= Wireless Application Environment
UDP	= User Datagram Protocol
IP	= Internet Protocol
TLS	= Transport Layer Security
DECT	= Digital European Cordless Communication
TDMA	= Time-Division Multiple Access
CDMA	= Code Division Multiple Access
SMS	= Short Message Service
GPRS	= General Packet Radio Service
W3C	= World Wide Web Consortium
SGML	= Standard Generalized Markup Language
LEAP	= Lightweight Extensible Agent Platform
SNMP	= Simple Network Management Protocol

8.7 Lähdeluettelo

[1] http://www.xhtml.org (XHTML)

[2] http://www.w3schools.com (XHTML)

[3] http://www.iec.org/ (WAP)

[4] http://www.nokia.fi (WAP)

[5] http://www.webreference.com

[6] http://www.w3.org

9. I-MODE

i-mode on Japanin suurimman matkapuhelinoperaattorin NTT DoCoMon tarjoama palvelukonsepti, joka mahdollistaa pakettikytkentäisen yhteyden sekä Internetiin että virallisiin i-moden sisällöntuottajiin. i-moden perustaksi valittiin cHTML-kieli, joka perustuu tavanomaiseen HTML-kieleen. Lisäksi uusimmat päätelaitteet mahdollistavat Java-sovelluksien käytön.

i-mode –palvelut koostuvat epävirallisista ja virallisista palveluista. Viralliset i-mode –sivut ovat NTT DoCoMon hyväksymiä sivuja, joihin pääsee i-moden päävalikon kautta. NTT DoCoMon hyväksymien virallisten i-moden sisällöntuottajien palvelimet on yhdistetty suoraan NTT DoCoMon palvelimiin, tietoa ei siis siirretä Internetin yli. Epävirallisille sivuille päästään ainoastaan Internetin välityksellä.

NTT DoCoMo on ottanut käyttöön kolmannen sukupolven teknologiat Tokion alueella vuoden 2001 lopussa. Tämän ansiosta i-moden käyttönopeus on kasvanut moninkertaiseksi. Uusi teknologia mahdollistaa monenlaisia uusia palveluja ja samalla se myös parantaa vanhojen palveluiden laatua.

9.1 Johdanto

Mobiili Internet on ollut jo pitkään päivän muotisana maailmalla. Kuitenkaan esimerkiksi Euroopassa WAP-teknologialla toteutettu mobiili Internet ei ole vastannut kuluttajien odotuksia. Japanissa asia on kuitenkin toisin. NTT DoCoMon, Japanin suurimman matkapuhelinoperaattorin, i-mode eli Internet-Mode –palvelukonsepti on saanut osakseen suuren suosion. i-mode julkaistiin 22. helmikuuta 1999, jonka jälkeen sen käyttäjämäärä on kasvanut eksponentiaalisesti.

9.1.1 i-moden synty

i-mode syntyi ratkaisuna NTT DoCoMon ongelmaan, joka liittyi nopeasti kasvavaan matkapuhelinten käyttöön. Vuoteen 1997 mennessä NTT DoCoMo huomasi verkkojensa kapasiteetin riittämättömyyden, jonka takia monet puhelut estyivät ja puhelujen laatu heikkeni huomattavasti. Täten yhtiössä pääteltiin, että jos käyttäjät saataisiin käyttämään enemmän datapalveluja puhepalveluiden sijasta olemassa olevassa verkossa, voitaisiin kokonaan uuden infrastruktuurin rakentamista siirtää myöhemmäksi. Lisäksi tavalliset verkkoyhteydet olivat erittäin kalliita monille käyttäjille ja PC:iden penetraatio oli suhteellisen alhainen, mikä edelleen auttoi i-moden suosion kasvua. Asiaa auttoi myös se, että japanilaiset ovat innokkaita vaihtamaan puhelimiaan uudempiin versioihin. Tämä mahdollisti nopean puhelinkannan uusiutumisen datansiirtoon soveltuviin päätelaitteisiin. Lisäksi, koska NTT DoCoMo hallitsee päätelaitteiden kehitystä ja

valmistusta, oli sen helppo tuoda markkinoille uusi teknologia ja palvelukonsepti, i-mode. [1]

9.2 i-modessa käytetty teknologia

i-mode julkaistiin jo ennen kuin WAP-teknologia oli käytössä, ja siksi NTT DoCoMon oli kehitettävä omat teknologiat ja protokollapinot mobiilin Internetin toteuttamista varten. i-moden perustaksi valittiin cHTML (compact HTML) eli tiivistetty HTML-kieli.

9.2.1 PDC-P –mobiiliverkko

i-mode toimii NTT DoCoMon ylläpitämässä pakettikytkentäisessä PDC-P –mobiiliverkossa (Personal Digital Cellular – Packet network), joka toimii 800 MHz:n alueella. PDC-P –verkko on Japanissa käytetyn PDC-standardin laajennus, ja se pystyy jopa 28,8 kbit/s:n nopeuksiin. Käytännössä i-moden päätelaitteet käyttävät kuitenkin vain 9,6 kbit/s:n nopeutta. [1]

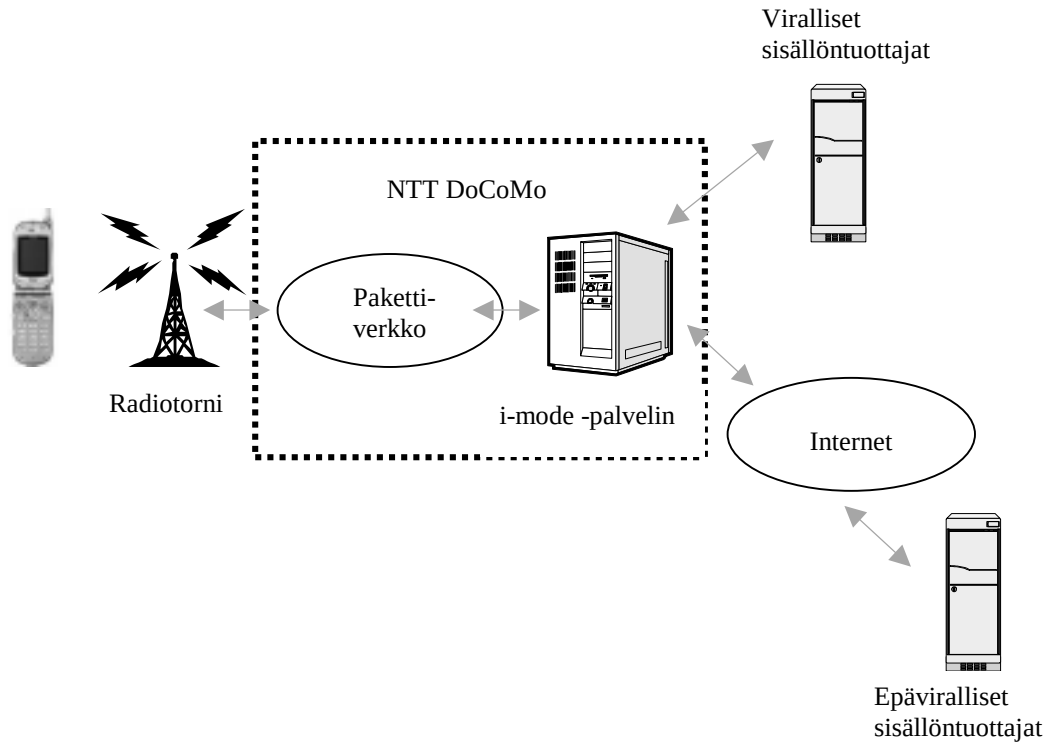
PDC-P –verkko yhdistetään muihin verkkoihin pakettiyhdysporttien (Packet Gateway) kautta. Pakettien reititys asiakkaan päätelaitteeseen tapahtuu pakettien prosessointikeskuksessa (Packet Subscriber Processing Center) ja tukiasemassa. [2]

Pakettikytkentäisyys mahdollistaa sen, että yhteys on aina käytettävissä, “always on”. Tämä tarkoittaa sitä, että i-mode –palveluihin päästään lähes välittömästi sen jälkeen, kun käyttäjä painaa puhelimen i-mode –näppäintä. Yhteydenmuodostusajan arvioidaan olevan vain noin 1-4 sekuntia. [3]

9.2.2 i-moden arkkitehtuuri

i-moden toiminta perustuu NTT DoCoMon ylläpitämään i-mode –keskukseen, jonka kautta kulkevat kaikki yhteydet i-mode –palveluiden ja käyttäjien välillä. i-modessa surffailu on hyvin samankaltaista kuin webissäkin. Päätelaite lähettää aluksi pyynnön, joka kulkee yhdysporttia (gateway) pitkin pääjärjestelmään. Tämän jälkeen pyyntö prosessoidaan ja vastaus lähetetään takaisin päätelaitteelle. Yhdysportti sijaitsee NTT DoCoMon tiloissa, eikä sitä voi siis mikään muu osapuoli käyttää. Yhdysportti sisältää tiedot asiakkaista sekä näiden laskutustiedoista.

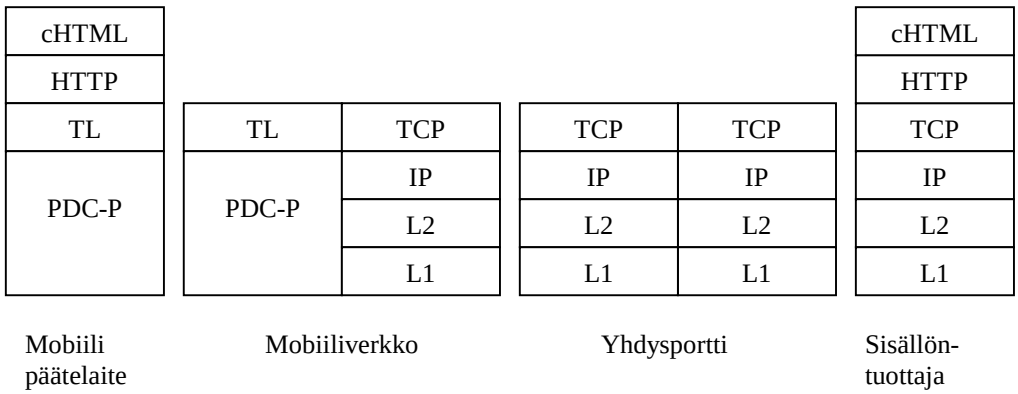
Yhdysporttipalvelimesta on yhteys sekä i-moden virallisiin sisällöntuottajiin että Internetiin. Tämä ei kuitenkaan tarkoita sitä, että kaikki Internetin sivut olisivat i-moden päätelaitteiden käytössä. Muun muassa sivujen koko ja sisältö asettavat rajoituksia. NTT DoCoMo onkin suositellut, että i-mode –sivut eivät saisi olla kooltaan suurempia kuin kaksi kilotavua.



Kuva 1: i-moden arkkitehtuuri [1]

9.2.3 i-modessa käytetyt protokollat

Seuraavassa kuvassa on esitelty i-modessa käytetyt protokollat.



Kuva 2: i-modessa käytetyt protokollat [4]

i-mode toimii GSM-verkon kaltaisessa PDC-standardin laajennetussa versiossa, PDC-P:ssä, joka siis mahdollistaa pakettikytkentäisen tiedonsiirron. TCP-protokollan sijasta NTT DoCoMo on kehittänyt uuden kuljetuskerroksen eli TL:n (Transport Layer), joka käyttää tavanomaisen

TCP:n muokattua versiota. Kyseinen TCP:n muokattu versio soveltuu paremmin langattomaan tiedonsiirtoon, ja NTT DoCoMo onkin nimennyt sen kuvaavasti “wireless-profiled TCP”:ksi. Mobiiliverkosta eteenpäin kuljetusprotokollana käytetään kuitenkin TCP/IP –protokollaa yhdessä HTTP-protokollan kanssa. Kuvauskielenä i-modessa käytetään NTT DoCoMon kehittämää cHTML-kieltä, joka perustuu HTML-standardiin.

9.2.4 cHTML

Päätelaitteiden pieni näyttö sekä rajallinen muisti ja matalatehoinen keskusyksikkö asettavat rajoituksia sisällön esitystavalle. Tätä varten NTT DoCoMo kehitti i-moden sisältöä varten cHTML-kielen, joka perustuu HTML 2.0:n, HTML 3.2:n ja HTML 4.0:n spesifikaatioihin, joita se on laajentanut. cHTML on määritelty W3C-spesifikaatioissa tiivistettynä HTML-kielenä, joka soveltuu pienille datalaitteille. cHTML:stä puuttuu kuitenkin joitain tavallisen HTML:n osia. Näitä ovat:

- JPEG-muotoiset kuvat
- taulukko (Table)
- kuvakartta (Image map)
- erilaiset fontit ja tyylit (Multiple character fonts and styles)
- taustaväri ja kuva (Background colour and image)
- kehys (frame)
- tyylisivu (style sheet)

Eräät i-moden päätelaitteet tukevat osaa yllämainituista ominaisuuksista, mutta koska ne eivät kuulu cHTML-standardiin, ei niitä suositella käytettäväksi.

cHTML sisältää myös joitain lisäominaisuuksia, joita ei ole tavanomaisessa HTML:ssä määritetty. cHTML:ssä on muun muassa joitakin sellaisia erikoismerkkejä eli tageja, joista hyvänä esimerkkinä on “tel:”-tagi. Tähän tagiin on yhdistetty puhelinnumero, ja linkkiä painamalla käyttäjä voi aloittaa puhelun kyseiseen puhelinnumeroon.

Yleisesti oletetaan, että kuljetusprotokollana cHTML:lle käytetään HTTP:tä TCP/IP:n päällä. Tämä tarkoittaa sitä, että olemassa olevia Internet-palvelimia voidaan käyttää suoraan ilman erillistä muunnosta.

cHTML:n kanssa käytettäville URL-osoitteille on kuitenkin seuraavia rajoituksia:

- URL-osoite saa olla enintään 200 tavua
- URL:n pituus, joka voidaan antaa tai laittaa kirjanmerkiksi (bookmark) saa olla enintään 100 tavua
- cHTML on määritelty niin, että kaikki perusoperaatiot sekä sivuilla navigointi tapahtuu käyttämällä vain neljää näppäintä: eteenpäin (Forward), taaksepäin (Backward), valitse (Select) ja takaisin/keskeytys (Back/Stop)

- kaikkien kuvien, joihin viitataan, täytyy olla GIF-muodossa

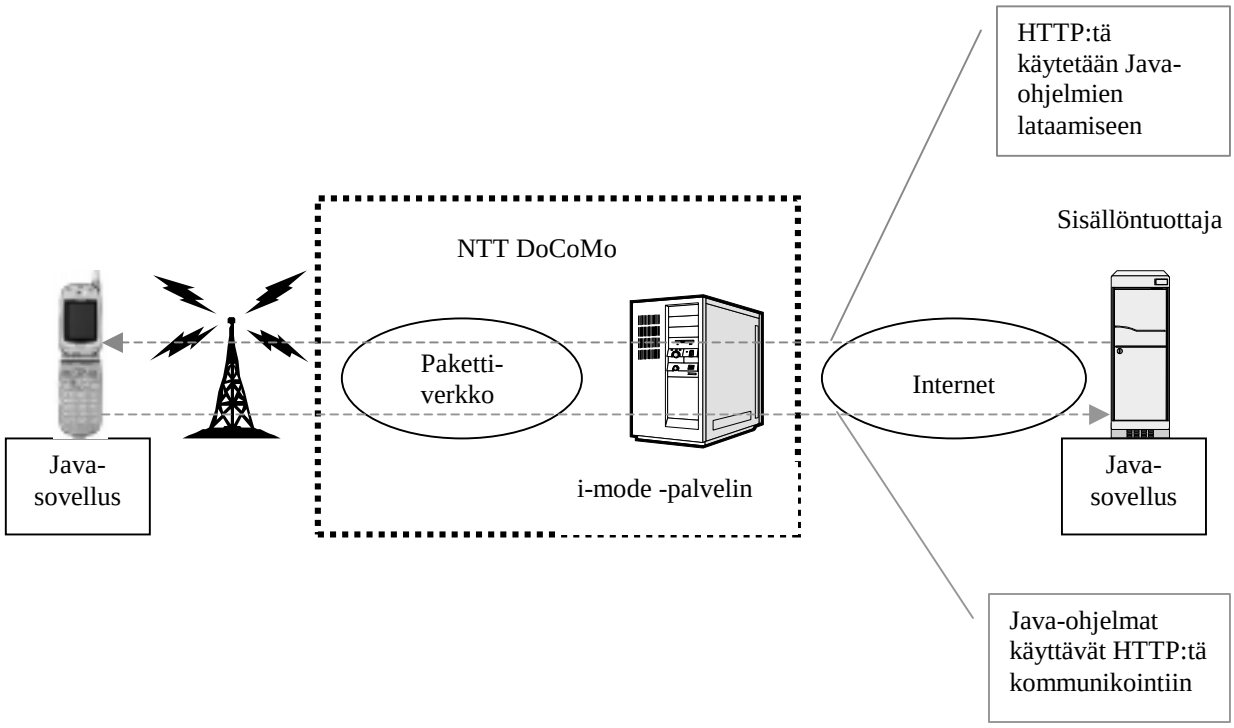
[5]

9.2.5 Java-sovellukset

Uusimmat i-moden päätelaitteet tukevat myös Java-kieltä. NTT DoCoMon iAppli-palvelu perustuu Javan “Java2 Micro Edition Connection Limited Device Configuration (J2ME)”-versioon, johon on lisätty lisäominaisuuksia [1]. Kyseinen Java-versio soveltuu hyvin järjestelmiin, joissa on verraten vähän prosessointitehoa [6].

iAppli-sovellukset ovat dynaamisempia ja graafisesti rikkaampia kuin tavalliset HTML-pohjaiset sovellukset. iAppli on tarkoitettu erillisille, itsenäisille sovelluksille kuten peleille, joissa voidaan tallentaa tietty tila ja käyttää sovellusta ilman yhteyttä. Lisäksi iAppli soveltuu esimerkiksi agenttityyppisille palveluille, jotka yhdistävät tiettyyn palvelimeen ja hakevat päivityksiä, kuten sääkarttoja ja uusimpia osakekurssitietoja. Kaikki ohjelmat ladataan HTTP-verkon yli. [6]

i-moden arkkitehtuuri pysyy lähes samana iApplista huolimatta. iApplin käyttäjät voivat ladata Java-sovelluksia samalla tavalla kuin HTML-dokumenttejakin tavallisilta HTTP-sivuilta. Myös i-mode –päätelaitteiden Java-ohjelmat käyttävät tavallista HTTP-formaattia tiedonvälityksessä ja kommunikoinnissa. [6]



Kuva 3: Java-sovellukset i-modessa [1], [6]

iApplin tietoturvaominaisuudet ovat parempia kuin tavallisessa Java-versiossa. Se tukee Secure Sockets Layer –tietoturvaprotokollaa (SSL), joka takaa korkean turvallisuustason web-selaimen ja –serverin välisessä tietoliikenteessä. Lisäksi iApplissa on monia muita tietoturvaominaisuuksia, jotka esimerkiksi estävät ulkopuolisten tunkeutumisen käyttäjän osoitekirjaan tai muihin henkilökohtaisiin tiedostoihin. Lisäksi iAppli estää Java-sovelluksia käynnistämästä muita Java-sovelluksia ja muokkaamasta niiden sisältöä. Korkean turvallisuutensa ansiosta iAppli on käytännöllinen työkalu etenkin yrityksille, jotka tarvitsevat turvallisen tiedonsiirtoyhteyden. [6]

9.2.6 i-moden päätelaitteet

Japanissa puhelinoperaattori määrittelee, minkälaisia puhelimia sen asiakkaat voivat käyttää. Täten asiakas ei osta esimerkiksi Nokian, Panasonicin, Fujitsun tai NECin puhelinta, vaan hän ostaa NTT DoCoMo-, KDDI- tai J-Phone –merkkisen puhelimen, jonka on valmistanut Nokia, Panasonic, Fujitsu tai NEC. Puhelimissa ei siis ole valmistajan nimeä, vaan se voi esimerkiksi olla NTT DoCoMon N503i- tai F503i-merkkinen puhelin, jossa ensimmäinen kirjain edustaa valmistajan nimeä (N=NEC, F=Fujitsu). [1]

Uusimpien päätelaitteiden näytöt pystyvät näyttämään 256 väriä, jotkut 4096 väriä ja Sonyn uusin puhelinmalli jopa 65 536 väriä. Värien lisäksi i-mode –päätelaitteet soivat moniäänisesti. Olennaisena osana päätelaitetta on i-mode –pikanäppäin, jota painamalla päästään suoraan i-moden päävalikkoon. Tämä helpottaa navigointia. [6]

Kolmannen sukupolven i-mode –puhelimissa, jotka ilmestyivät markkinoille vuoden 2001 lokakuussa, on jopa sisäänrakennettu videokamera (Panasonicin FOMA P2101V-versio). [6]

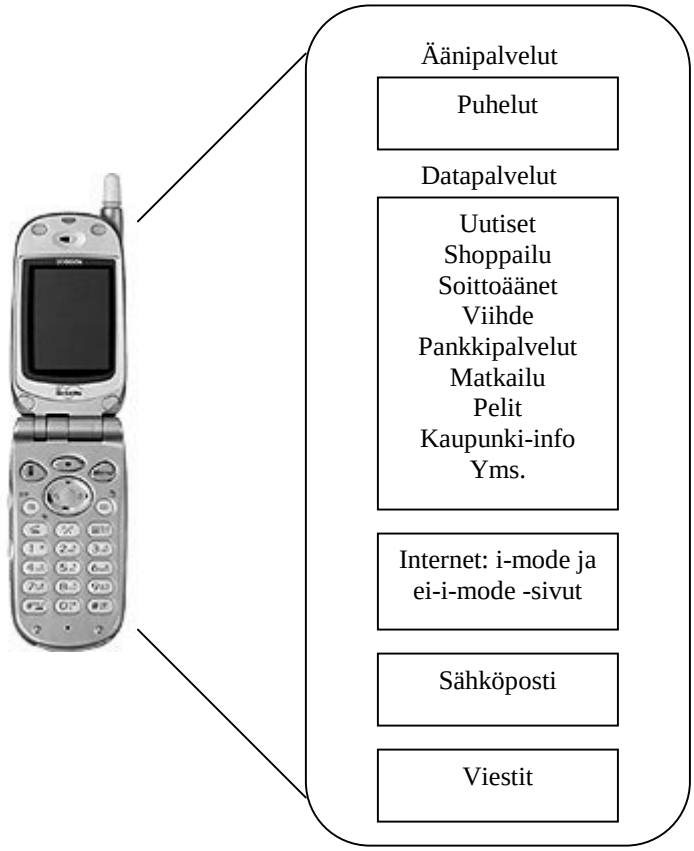
9.3 i-moden palvelut

i-mode –sivuja on kahdenlaisia: virallisia ja epävirallisia. Viralliset i-mode –sivut ovat NTT DoCoMon hyväksymiä sivuja, joihin pääsee i-moden päävalikon kautta. NTT DoCoMon hyväksymien virallisten i-moden sisällöntuottajien palvelimet on yhdistetty suoraan NTT DoCoMon palvelimiin, tietoa ei siis siirretä Internetin yli. Epävirallisille sivuille päästään ainoastaan Internetin välityksellä.

Virallisia i-moden sisällöntuottajia arvioidaan olevan yli 2000 kun taas epävirallisia jopa 51 000. 50 % kaikesta i-moden liikenteestä arvioidaan menevän epävirallisille sivuille. [1]

9.3.1 i-mode –palveluiden kategoriat

i-mode –palvelukonsepti pitää sisällään sekä äänipuhelut, sähköpostin että surffailun virallisilla ja epävirallisilla i-moden ja ei-i-moden sivuilla. Seuraava kuva havainnollistaa asiaa:



Kuva 4: i-mode –palveluiden kategoriat [1]

i-moden kaikkein suosituin palvelu on ehdottomasti sähköposti. Arvellaankin, että keskimääräinen i-moden käyttäjä käyttää jopa 42 % i-moden käyttöajastaan sähköpostin lähetykseen ja vastaanottamiseen, kun ainoastaan noin kolmasosan ajasta hän puhuu ja 24 % menee Internetissä surffailuun. [1]

9.3.2 Viralliset i-moden palvelut

Viralliset i-moden sivut on listattu NTT DoCoMon i-mode –portaaliin, ja niihin päästään helposti neljän tai viiden painalluksen kautta. Näitä palveluja saavat käyttää ainoastaan NTT DoCoMon i-mode –asiakkaat. Niihin ei siis pääse käsiksi kilpailijoiden mobiiliverkoista tai webin kautta. Virallisten palveluiden tuottajilla on myös oikeus veloittaa NTT DoCoMon asiakkaita palveluidensa käytöstä. Veloituksen hoitaa kuitenkin NTT DoCoMo.

NTT DoCoMolla on hyvin tiukkoja ohjeita siitä, minkälaisia viralliset i-mode –palvelut saavat olla. Näitä ovat muun muassa seuraavat:

- Sivuilla ei saa olla sellaisia palveluita, joilla ihmiset voivat ottaa yhteyttä toisiinsa. Tämä tarkoittaa siis ilmoitustauluja, chattejä tai treffipalveluja.

- Yleisesti ottaen sivuilla ei saa olla linkkejä toisille sivuille. Poikkeustapauksissa sallitaan linkit muille virallisille i-mode –sivuille.

[1]

9.3.3 Epäviralliset i-mode -sivut

Epävirallisille sivuille, jotka siis eivät ole NTT DoCoMon hyväksymiä sivuja, päästään suoraan kirjoittamalla sivun URL-osoite. Operaattori ei ota vastuuta näiden sivujen toiminnasta tai sisällöstä, eikä näillä sivuilla ole myöskään yhteistä laskutustoimintoa NTT DoCoMon kanssa.

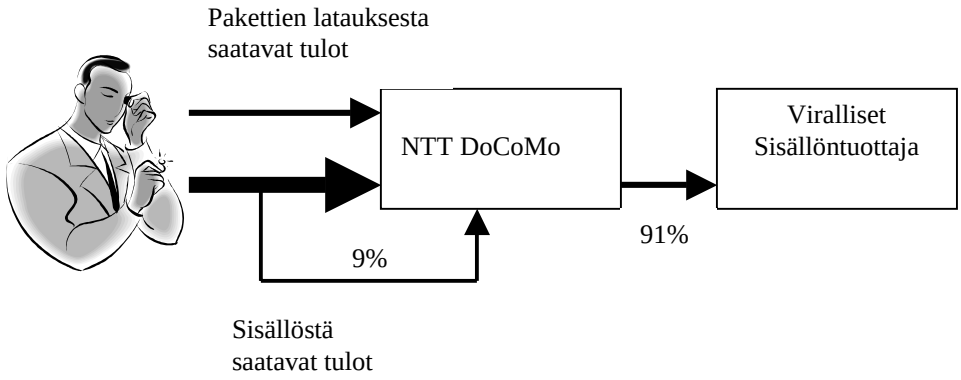
NTT DoCoMolla olisi mahdollisuus rajoittaa ulkopuolisilla sivuilla surffailua, koska kaikki käyttäjät pääsevät Internetiin ainoastaan operaattorin palvelimien kautta. Teoriassa NTT DoCoMo voisi asettaa suodattimia palvelimilleen tai estää jonkun URL-osoitteen läpipääsyn kokonaan, mutta näitä toimia NTT DoCoMo ei kuitenkaan vielä tähän mennessä ole käyttänyt. [1]

9.3.4 Laskutus

i-moden kuukausihinta, käytti sitä tai ei, on 300 jeniä (valuuttakurssi 29.3.2002: 1€ = 115,26¥) eli noin 2,60€ kuukaudessa. NTT DoCoMon tiedonsiirron laskutus perustuu siirrettyjen pakettien määrään. Yhden paketin, jonka koko on 128 bittiä, lataamisesta laskutetaan 0,3 jeniä (0,0026€). i-modella lähetetty sähköposti, jossa on 20 japanilaista merkkiä tai 40 länsimaista aakkosta, maksaa yhden jenin (0,0087€). Muista palveluista, kuten kuvien tai osakekurssien lataamisesta, NTT DoCoMo veloittaa 7 jenistä (0,06€) 60 jeniin (0,52€). [6]

Lisäksi käyttäjä joutuu maksamaan erillisen hinnan, jos hän kirjautuu käyttämään jotain tiettyä i-moden virallista palvelua. Yleensä näiden virallisten palvelujen hinnat vaihtelevat 100 jenistä (0,87€) 300 jeniin (2,60€) kuukaudessa. [6]

NTT DoCoMon liiketoimintamalli poikkeaa huomattavasti suomalaisten operaattorien liiketoimintamalleista. Ensinnäkin i-moden virallisista palveluista laskutetaan kuukausihinta, ei siis kertamaksua. Tämän lisäksi NTT DoCoMo soveltaa toiminnassaan tulonjakomallia (revenue-share model). Sisällöntuottajat saavat laskuttaa NTT DoCoMon asiakkailta aina 300 jeniin asti kuukaudessa, josta NTT DoCoMo ottaa 9 % itselleen. Loput 91 % tuloista menevät sisällöntuottajan taskuun. Lisäksi NTT DoCoMo saa tuloja syntyvästä tietoliikenteestä. [6]



Kuva 5: Tulonjakomalli NTT DoCoMon ja virallisten sisällöntuottajien välillä [6]

Kyseinen tulonjakomalli on osoittanut erityisen hyväksi. Se kannustaa sisällöntuottajia kehittämään yhä parempia palveluja, sillä palvelujen saaminen NTT DoCoMon i-mode –portaaliin on hyvin vaikeaa kilpailun ansiosta. Joinain kuukausina vain alle prosentti kaikista ehdolla olevista palveluista hyväksytään i-moden viralliseksi palveluksi.

Liiketoimintamallin muita hyviä puolia on mm. se, ettei sisällöntuottajien tarvitse kehittää erityistä laskutusjärjestelmää. Myös käyttäjän kannalta järjestelmä on yksinkertainen ja turvallinen, sillä näin hän voi maksaa käyttämistään palveluista yhdellä laskulla eikä hänen tarvitse antaa luottokorttinumeroaan tuntemattomille palveluntuottajille.

9.4 Kilpailijat

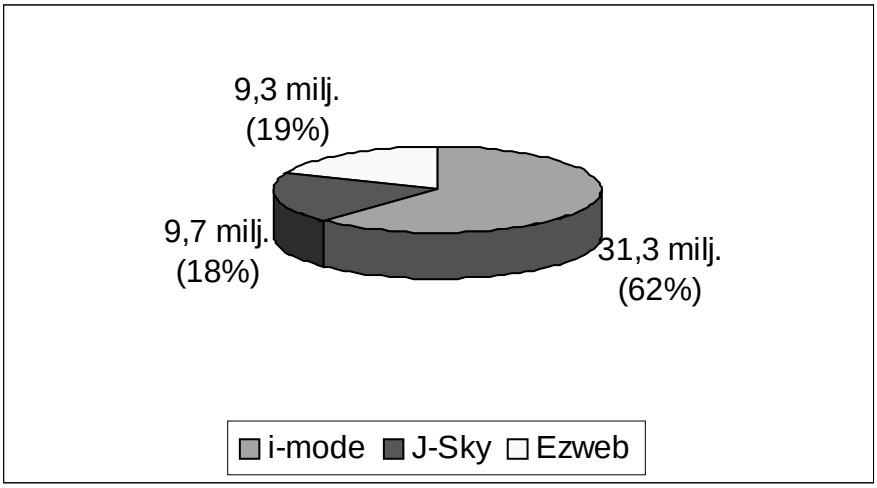
Tässä kappaleessa vertaillaan sekä NTT DoCoMon kilpailijoita operaattorialalla että i-mode –palvelukonseptia WAP-konseptiin. Periaatteessa i-modea ja WAPia ei voida vertailla suoraan toisiinsa, sillä WAP on ainoastaan mobiilin Internetin protokolla, kun taas i-mode käsittää koko mobiilin Internetin palvelukonseptin. Tässä kuitenkin pyritään tarkastelemaan näiden kahden teknologian eroja ja samankaltaisuuksia.

9.4.1 Kilpailutilanne Japanissa

Japanissa on kolme kilpailevaa matkapuhelinoperaattoria, jotka kaikki tarjoavat mobiilin Internetin asiakkaidensa käyttöön. Kaikki operaattorit ovat kuitenkin toteuttaneet mobiilin Internetin eri teknologioilla. NTT DoCoMo hallitsee Japanin markkinoita 60 %:n markkinaosuudellaan. Kilpailevilla operaattoreilla, J-Phonella ja KDDI:llä on kummallakin noin 20 %:n markkinaosuudet, ja myös nämä kaksi operaattoria ovat menestyneitä ja erittäin kannattavia. [2]

J-Phonen mobiili Internet –palvelu J-Sky toimii piirikytkentäisessä PDC-verkossa, ja sen sovellukset on toteutettu MML-kielellä (Mobile Markup Language). MML-kieli on joiltakin osin samankaltainen kuin HTML-kieli. Nopeutta J-Sky –palvelulla on 9,6 kbit/s. [1]

KDDI:n Ezweb-palvelu toimii sekä piirikytkentäisen PDC:n että pakettikytkentäisen cdmaOne-verkon päällä. Ezwebin sovelluksissa käytetty HDML-kieli perustuu WAPin edeltäjään, ja siksi Ezwebiä kutsutaankin joskus WAP-ratkaisuksi. PDC-verkon päällä toteutettu Ezweb toimii 9,6 kbit/s:n nopeudella kun taas pakettikytkentäisen verkon nopeus yltää jopa 64 kbit/s:n nopeuteen. [1]



Kuva 6: i-moden ja sen kilpailijoiden käyttäjämäärät [2]

9.4.2 i-moden ja WAPin vertailua

Lehdistön keskuudessa on ollut paljon vertailua i-moden ja WAPin välillä, vaikka käytännössä nämä ovat kaksi eri asiaa. On sanottu, että i-moden ja WAPin vertaileminen keskenään on sama asia kuin vertailisi “Rolls-Roycen suihkumoottoreita United Airlinesiin tai Air Franceen” [7]. Vertailussa onkin enemmän kyse WAPin ja cHTML:n tai WAPin ja i-moden implementoinnin välisestä vertailusta.

Tällä hetkellä kummatkin teknologiat toimivat 9,6 kbit/s:n nopeudella, ja WAP kykenee jopa hieman suurempiin nopeuksiin HSCSD:n (High Speed Circuit Switched Data) avulla. Tiedonsiirtotavassa on kuitenkin eroa, sillä i-mode on alusta asti toiminut pakettikytkentäisessä PDC-P –verkossa, joka soveltuu paremmin purskeisen datan siirtoon, kun taas WAP on tähän asti toiminut ainoastaan piirikytkentäisen GSM-verkon päällä. GPRS tekee WAPista kuitenkin samankaltaisemman tämän hetkisten i-moden palveluiden kanssa.

Suurin ero WAPin ja i-moden välillä on niiden toteutuskieli. WAP on toteutettu WML-kielellä, kun taas i-mode HTML-kielen johdannaisella eli cHTML:llä. Tilanne on helpompi i-moden sisällöntuottajilla, sillä periaatteessa he voivat julkaista saman sisällön sekä i-modelle että webbiin cHTML-kielellä. Lisäksi i-mode –päätelaitteella pystyy selaamaan tavallisia web-sivuja tietyin rajoituksin (ne eivät saa olla liian suuria, eikä niissä saa olla esim. JPEG-kuvia). WML ei ole suoraan yhteensopiva HTML-kielen kanssa, joten väliin tarvitaan erityisiä WML-HTML –suodattimia.

Arkkitehtuuriltaan nämä kaksi teknologiaa muistuttavat toisiaan, sillä kummatkin tarvitsevat yhdysportin yhteyksien muodostamiseen sisällöntuottajien palvelimien kanssa. Ainoana erona on kuitenkin se, että i-moden yhdysportit ovat kaikki NTT DoCoMon omistamia, kun taas WAPin yhdysportit voivat olla kenen tahansa omistuksessa.

WAPin ja i-moden päätelaitteissa on suuriakin eroja. NTT DoCoMo hallitsee käytännössä päätelaitteidensa valmistusta määräämällä tekniset spesifikaatiot kaikille valmistajille, jotka valmistavat i-mode –puhelimia. Täten ne ovat myös yhdenmukaisempia kuin WAP-puhelimet, joiden valmistusta ei standardisoida operaattorien toimesta. i-moden päätelaitteet ovat myös hieman käyttäjäystävällisempiä siinä mielessä, että i-modea päästään käyttämään vain yhdellä napin painalluksella, kun taas WAPin käyttöönotto vaatii ensin useiden asetusten säätämistä.

9.5 i-moden menestystekijät

i-moden menestykseen on vaikuttanut monta tekijää, ja osa niistä on varmasti kulttuurisidonnaisia. Tässä kappaleessa esitellään suurimpia syitä, jotka ovat aikaansaaneet i-moden huikean menestystarinan.

Ehkä suurin edesauttaja i-moden menestykselle oli se, että i-moden markkinoilletulon aikoihin Japanissa PC-penetraatio oli suhteellisen alhaisella tasolla ja toisaalta matkapuhelin-penetraatio oli hyvin korkea. Lisäksi nettiyhteydet kotikoneilta ovat hyvin kalliita, eikä täten tavallisilla kaduntallaajilla ollut innostusta lähteä edes hankkimaan kotikonetta ja –yhteyttä. Kun NTT DoCoMo esitteli pakettikytkentäisen, suhteellisen nopean ja edullisen tavan käyttää sähköpostia ja saada ajan tasalla olevaa tietoa esimerkiksi juna-aikatauluista, säätiedoista tai ladata puhelimeen soittoääniä ja kuvia, oli menestys lähes taattu.

Käyttäjämäärien huima kasvu houkutteli sisällöntuottajia kehittämään yhä laadukkaampia palveluja, ja toisaalta palveluiden kasvava määrä ja laatu houkutteli yhä enemmän asiakkaita. i-moden datapalveluiden käyttöä edisti myös se, että i-moden julkaisun aikoina Japanissa kiellettiin matkapuhelimessa puhuminen julkisilla paikoilla ja kulkuvälineissä.

Yksi tekijä, missä i-moden kohdalla onnistuttiin ja WAPin kohdalla epäonnistuttiin, on markkinointi. Kun WAPin kohdalla markkinoitiin, että “WAP tuo Internetin kännykkääsi”, kohosivat ihmisten odotukset korkealle, ja kun WAP ei onnistunut täyttämään näitä odotuksia, tuotti se suuren pettymyksen. i-moden markkinoinnissa yritettiin välttää teknologiasanoja, kuten “mobiili Internet” ja “pakettikytkentäinen”, vaan sitä markkinoitiin helppokäyttöisenä palveluna, joka tarjoaa mm. halvan sähköpostin lähetyksen.

9.6 Tulevaisuudennäkymät

Mobiilialalla on hyvin vaikea ennustaa tai edes lähteä arvailemaan, miltä tulevaisuus tulee näyttämään. Teknologia kehittyy vauhdilla ja uusia sovelluksia ja keksintöjä tulee markkinoille yhä nopeammalla vauhdilla.

Kuka olisi esimerkiksi osannut ennustaa kolme vuotta sitten, että i-modesta tulisi näin menestynyt palvelukonsepti?

i-mode on jo astunut askeleen eteenpäin kehityksessään, sillä NTT DoCoMo otti testikäyttöön kolmannen sukupolven teknologiat ensimmäisenä maailmassa keväällä 2001. NTT DoCoMon kolmannen sukupolven laajakaistateknologia on nimeltään FOMA eli Freedom of Multimedia Access ja se perustuu W-CDMA –teknologiaan. [6]

FOMA tarjoaa käyttäjälleen teoriassa 384 kbit/s:n vastaanottonopeuden ja 64 kbit/s:n lähetysnopeuden. FOMA-teknologia tarjoaa korkealaatuiset video- ja audio-ominaisuudet sekä mahdollisuuden puhua puhelimeen samaan aikaan kun i-modella ladataan tietoa. FOMA:n avulla voidaan siirtää videokuvaa, musiikkia, pelejä sekä muita suurta kapasiteettia vaativia sovelluksia mobiiliverkon yli. [6]

Tällä hetkellä FOMA-verkko on toiminnassa ainoastaan 30 kilometrin säteellä Tokion keskustasta, mutta laajennusta koko Japanin kattavaksi ollaan tekemässä parhaillaan. FOMA-päätelaitteet maksavat noin kaksi tai kolme kertaa niin paljon kuin Javaa tukevat i-mode –päätelaitteet, mutta myös näiden odotetaan laskevan heti, kun niiden kysyntä kasvaa. [1]

Jo lähitulevaisuudessa yrityksen työntekijä voi vastaanottaa ja lähettää i-mode –puhelimellaan suurikokoisia asiakas- ja myyntitiedostoja vaikkapa junassa istuessaan. Kotimatkallaan hän voi ennakoiden laittaa esimerkiksi ilmastoinnin ja valot päälle tai valvoa kotiaan puhelimesta, johon kodin turvakamera on yhdistetty. FOMA-teknologia tarjoaa siis monenlaisia uusia palveluja ja samalla se myös parantaa vanhojen palveluiden laatua.

9.7 Käytetyt lyhenteet

cdmaOne	=	code division multiple access One
cHTML	=	compact Hypertext Markup Language
FOMA	=	Freedom Of Multimedia Access
HDML	=	Handheld Device Markup Language
HSCSD	=	High Speed Circuit Switched Data
HTML	=	Hypertext Markup Language
HTTP	=	Hypertext Transfer Protocol
i-mode	=	Internet-mode
MML	=	Mobile Markup Language
PDC	=	Personal Digital Cellular
PDC-P	=	Personal Digital Cellular – Packet Network
SSL	=	Secure Sockets Layer
TCP/IP	=	Transmission Control Protocol/Internet Protocol
TL	=	Transport Layer
URL	=	Uniform Resource Locator

W3C	=	World Wide Web Consortium
W-CDMA	=	Wideband Code Division Multiple Access
WAP	=	Wireless Application Protocol
WML	=	Wireless Markup Language

9.8 Lähteet

1. Megler, V. 2002. From bandwidth problem to Internet phenomenon. (viitattu 16.3.2002)

   http://www.106.ibm.com/developerworks/library/wi-imode/index.html?dwzone=wireless

2. Mobile Media Japan. (viitattu 3.4.2002)

   http://www.mobilemediajapan.com

3. van Blokland, A. 2001. Message: i-mode is NOT always on. (viitattu 3.4.2002)

   http://www.appelsiini.net/keitai-l/archives/2001-01/0156.html

4. Hata, M. 2000. DoCoMo's i-mode. Toward mobile multimedia in 3G. (viitattu 3.4.2002)

   http://www.ipv6forum.com/navbar/events/xiwt00/presentations/html/hata/sld011.htm

5. Compact HTML for Small Information Appliances, W3C NOTE 09-FeB-1998. (viitattu 3.4.2002)

   http://www.w3.org/TR/1998/NOTE-compactHTML-19980209/

6. NTT DoCoMo (viitattu 3.4.2002)

   http://www.nttdocomo.com/

7. The unofficial i-mode-FAQ (viitattu 3.4.2002)

   http://www.eurotechnology.com

10. MOBILE IPV6

Tähän asti IP:tä käyttävät päätelaitteet ovat pysyneet suhteellisen paikoillaan. Uusien teknologioiden myötä on kuitenkin hyvin todennäköistä, että liikuvuus IP-verkoissa kasvaa. Vaikka liikkuvuuden hallintaan pyritäänkin usein käyttämään kerroksen 2 keinoja, täydellisen saumattomuuden saavuttamiseksi varsinkin eri verkkojen välillä joudutaan turvautumaan myös mobile IP –ratkaisuun. [3]

Mobile IP on IETF:n standardoima menetelmä, jolla liikkuvuus IP-verkossa voidaan toteuttaa. Alunperin mobile IP kehitettiin IPv4:n lisäominaisuudeksi, mutta IPv6:ssa mobile IP on sisällytetty jo kuuluvaksi kiinteänä osana protokollaan. IPv6 tarjoaa myös monia etuja liikkuvuuden toteuttamiseen IPv4:ään verrattuna.

Mobile IP:n kantava ajatus on, että jokainen laite tavoitetaan aina saman osoitteen kautta riippumatta siitä, missäpäin laite on fyysisesti kytkeytyneenä verkkoon. Tämä on mahdollista lähettämällä liikenne ensin kotiverkkoon, josta se sitten tunneloidaan eteenpäin vieraassa verkossa olevalle laitteelle.

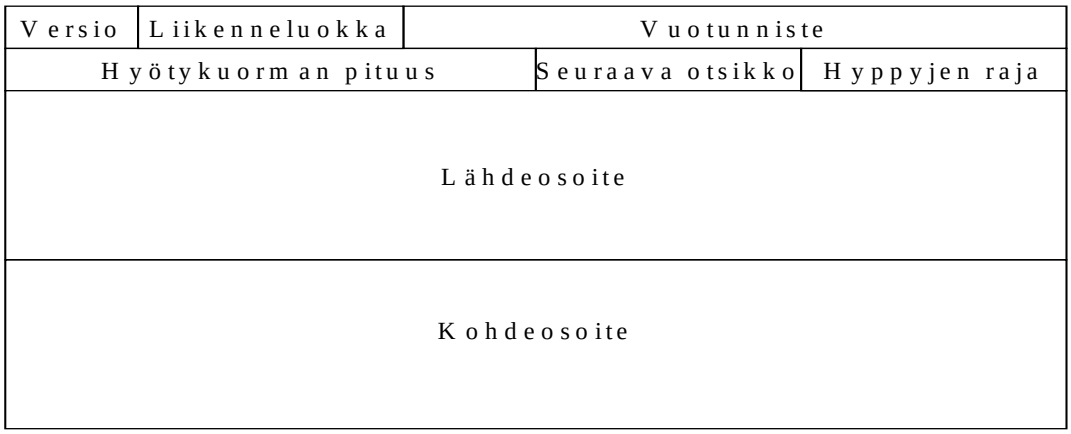
10.1 IPv6

Internetin valtavan suosion myötä huomattiin viime vuosituhannen loppulla, että käytössä olevan IPv4:n vapaa osoiteavaruus alkaa käydä vähiin. Osoitteiden loppumisen uhkaan vaikuttaa paitsi kasvanut osoitteiden tarvitsijamäärä niin myös osoitteiden tehoton luokittelu ja allokointi. IETF alkoikin kehitellä uutta IP-protokollaversiota. Versio viisi jäi kokeelliselle tasolle, mutta IPv6:sta syntyi sitten seuraavan sukupolven IP-protokolla. [1]

IPv6:ssa pyritään paikkaamaan IPv4:ssä havaittuja puutteita. Varsinkin juuri osoiteavaruutta on kasvatettu huikeasti. Kun IPv4:ssä on käytössä 32 bittiä pitkät osoitteet, niin IPv6:n osoitteen pituus on 128 bittiä. Osuvasti on todettu, että näin suuri osoitemäärä riittää vaikka siihen, että jokaiselle mailman hiekanmuruselle annetaan oma IP-osoite. [4]

Toinen suuri parannus IPv6:ssa on otsikon yksinkertaistuminen. IPv4:ssä käytössä olleet turhat tai käyttämättömät kentät on poistettu. Käyttöön on otettu myös lisäotsikot. Lisäotsikoilla toteutetaan protokollan laajennuksia. Varsinaisessa otsikossa on seuraava otsikko –kenttä, joka ilmaisee, mikä lisäotsikko varsinaista otsikkoa seuraa. Lisäotsikoita voi olla seuraava otsikko –kentän avulla linkitettynä useita peräkkäin. Jos lisäotsikoita ei ole, seuraava otsikko –kenttä ilmaisee huötykuorman alkavan. Myös viimeisessä

lisäotsikossa seuraava otsikko –kenttä kertoo alkavasta hyötykuormasta. Lisäotsikoiden käyttö pienentää varsinaista otsikkoa ja näin nopeuttaa prosessointia. [1] [4]



Kuva1 IPv6:n otsikko on tehty mahdollisimman yksinkertaiseksi – kaikki turha ja ylimääräinen on jätetty pois.

Lisäotsikoita on tällä hetkellä kuusi erilaista. Määränpää optiot –lisäotsikko kuljettaa tietoa, jota ei tutkita erikseen joka solmussa reitinvarrella. Määränpää optioiden vastakohta on hypyltä hypylle optiot –lisäotsikko, joka nimensä mukaisesti tutkitaan joka solmussa. Lisäksi esimerkiksi IP Securityn käyttöön on määritelty kaksi lisäotsikkoa. [1]

IPv6:ssa on otettu unicast– ja multicast–osoitteiden lisäksi käyttöön anycast–osoite. Anycast osoitteella lähetetty paketti toimitetaan anycast–osoitteen määrittelemän ryhmän lähimmälle solmulle. [6]

Tulevaisuuteen IPv6:ssa on varauduttu ottamalla Mobile IP alusta asti kiinteäksi osaksi protokollaa. Myös turvallisuuteen on IPv6:ssa panostettu sisällyttämällä protokollaan pakollisena IP Security. Sekä Mobile IP että IP Security ovat IPv4:ssä lisätoiminteita. [3]

10.2 Mobile IPv6

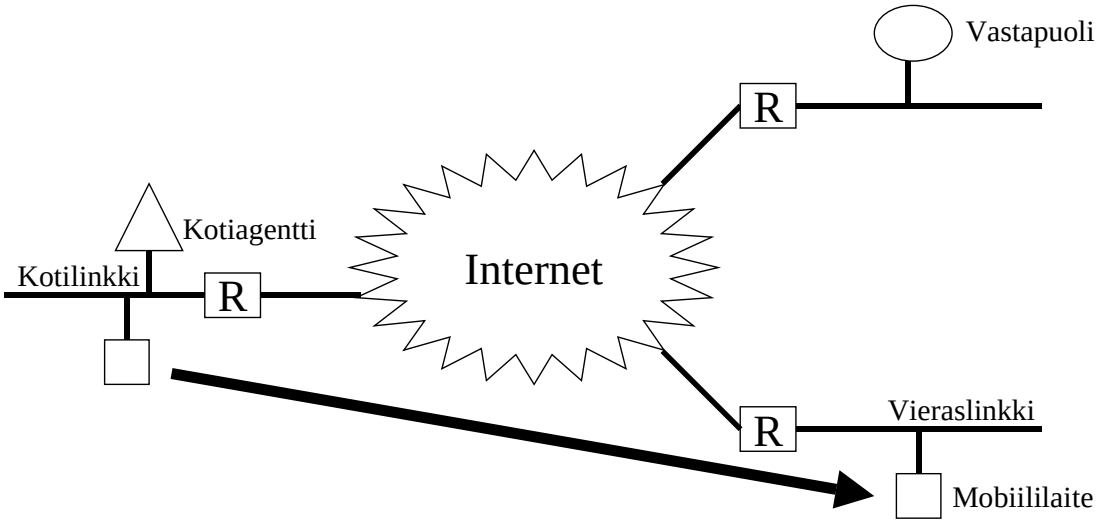
Mobile IP:n tarkoituksena on mahdollistaa päätelaitteiden liikkuvuus eri IP-verkoissa. Hyödyntämällä mobile IP:n mahdollisuuksia päätelaite voi siis siirtyä pois omasta kotiverkostaan ja silti ylläpitää olemassa olevat yhteytensä. Siirtyessään päätelaite myös säilyttää edelleen tavoitettavuutensa.

IP-osoitteisiin perustuvassa reitityksessä IP-osoitteen alkuosa identifioi verkon, johon liikenne on menossa, ja loppuosa itse laitteen tässä verkossa. Jos reititys halutaan tehdä johonkin toiseen verkkoon, on ainakin osoitteen alkuosa vaihdettava. Tällainen reititys toimii hyvin, kun päätelaitteet pysyvät paikallaan. Ongelma muodostuu kuitenkin silloin, kun päätelaitteet

lähtevät liikkeelle. Verkon vaihtuessa päätelaitteiden osoite muuttuu jatkuvasti, mikä johtaa huonoon tunnistettavuuteen: kukaan ei enää hetken päästä tiedä, mistä osoitteesta mikin laite milläkin ajan hetkellä löytyy. Liikkuvasta päätelaitteesta käytetään nimitystä mobiililaite.

Mobile IPv6 ratkaisee osoitteen vaihtumisesta aiheutuvan ongelman ottamalla käyttöön kaksi osoitetta: kotiosoitteen ja tlapäisen osoitteen. Kotiosoite on staattinen ja pysyy siis samana riippumatta mobiililaitteen kytkeytymispisteestä verkkoon. Näin verkon muut käyttäjät tavoittavat aina mobiililaiteen sen kotiosoitteen kautta. Tilapäinen osoite puolestaan on dynaaminen ja vaihtuu mobiililaitteen siirtyessä verkosta toiseen. [2] [3]

Kahden osoitteen hallitsemiseksi kunkin mobiililaitteen kotiverkossa pitää olla reititin, jota kutsutaan kotiagentiksi. Kotiagentti edustaa mobiililaitetta sen omassa kotiverkossa sillä aikaa, kun mobiililaite itse on kytkeytyneenä johonkin toiseen verkkoon. Kun mobiililaite liikkuu, se päivittää tilapäistä osoitettaan jatkuvasti kotiagentilleen. Näin kotiagenttilla on aina mobiililaitteen tarkka sijaintitieto. Kun omasta kotiverkostaan poissaolevan mobiililaitteen kotiosoitteeseen lähetetään liikennettä, kotiagentti kaappaa tämän liikenteen itselleen ja tunneloi paketit sitten mobiililaitteen kulloinkin voimassa olevaan tilapäiseen osoitteeseen. [2] [3]



Kuva2 Mobiililaite on siirtynyt kotilinkiltä vieraslinkille

Tällainen järjestely on täysin läpinäkyvä verkon muille käyttäjille; toiset käyttäjät eivät tiedä, missä päätelilaite kulloinkin liikkuu, sille se on aina tavoitettavissa kotiosoitteensa kautta. Myöskin IP:n yläpuolisille protokolla tasoille kuten TCP:lle ja UDP:lle sekä tietenkin myös sovelluksille tämä järjestely on täysin läpinäkyvä. [2]

10.3 Mobile IPv6:n toiminta

10.3.1 Paikallistaminen

IPv6 reitittimet lähettävät periodisesti reititinmainoksia, joiden avulla ne tiedottavat omasta olemassaolostaan. Reititinmainokset ovat ICMPv6-sanomia. Kotiagentit ovat siis reitittimiä ja lähettävät myös jatkuvasti näitä reititinmainoksia. Mainoksissa kotiagentit kertovat mobiililaitteile halukkuudestaan toimia kyseisen linkin kotiagenttina. Mobiililaitteet joutuvat näin tarkkailemaan jatkuvasti omille linkelleen tulevia mainoksia. Kotiagenttitiedon lisäksi mobiililaitteet päättelevät mainoksista mainosten lähettäjien – reitittimien – osoitteiden verkkoprefiksien avulla, ovatko ne kiinni koti- vai vieraslinkillä. [3]

Jos mobiililaitteella ei ole aikaa odottaa seuraavaa periodista mainosta, se voi lähettää reititinpyynnön, johon linkin reitittimet välittömästi vastaavat reititinmainoksella. Myös reititinpyyntö on ICMPv6-sanoma. [2] [3]

10.3.2 Tilapäisen osoitteen hankkiminen

Kun mobiililaite huomaa olevansa vieraslinkillä, tarvitsee se itselleen tilapäisen osoitteen. Tilapäisen osoitteen hankkimiseen on kaksi vaihtoehtoa: tilallinen tai tilaton osoitteen automaattinen konfigurointi. [1]

Tilallisessa osoitteen automaattisessa konfiguroinnissa mobiililaite saa IPv6 osoitteen esimerkiksi DHCPv6-palvelimelta. [1]

Tilattomassa vaihtoehdossa mobiililaite puolestaan muodostaa itse tilapäisen osoitteensa. Lupa generoida itse tilapäinen osoite ei ole itsestään selvyys, vaan reititinmainokset sisältävät tiedon, sallitaanko kyseisellä linkillä tilaton osoitteen automaattinen konfigurointi. Itsemuodostettavan osoitteen alkuosaksi valitaan linkin, jolla mobiililaite sillä hetkellä sijaitsee, verkkoprefiksi, joka saadaan siis reititinmainoksesta. Osoitteen viimeisiksi 64 bitiksi valitaan uniikki, laitekohtainen osoite. Uniikin osan muodostamisessa voidaan käyttää esimerkiksi laitteen MAC-osoitetta, jolloin uniikkisuus on melko varmasti taattu. Joka tapauksessa osoitteenvalinnan jälkeen linkin muilta käyttäjiltä varmistetaan kuitenkin, etteivät ne jo käytä tätä samaa laitekohtaista osoitetta. Tästä varmistusprosessista käytetään termiä DAD ja se aiheuttaa hitautta verkkoon kirjautumisessa. [1]

10.3.3 Liityntäkohdan päivitys

Mobiililaitteen saatua tilapäinen osoite pitää sen ilmoittaa tämä uusi osoite kotilinkkinsä kotiagentille. Osoitteen ilmoittamiseen käytetään liityntäkohdan päivitys –sanomaa. Kotiagentti talettaa uuden tiedon omaan liityntäkohtamuistiinsa tai päivittää muistissa jo ollutta tietoa. Siinä tapauksessa, että mobiililaite lähettää liityntäkohdan päivitys –sanoman, että

se on palannut takaisin kotilinkilleen, kotiagentti poistaa kyseisen mobiililaitteen tiedot liityntäkohtamuististaan. [2]

Kaikissa tapauksissa kotiagentti lähettää liityntäkohta hyväksytty –sanoman takaisin päivitys tiedon lähettäneelle mobiililaitteelle. Jos mobiililaite ei saa liityntäkohta hyväksytty –sanomaa kotiagentilta, uudelleenlähettää se päivitystietoa periodisesti, kunnes se saa haluamansa kuittauksen. [2]

Tilapäinen osoite on voimassa aina vain tietyn ajan. Liityntäkohdan päivitys –sanoma sisältää tiedon tilapäisen osoitteen elinajasta. Jos halutaan, että osoite on käytössä pidempään kuin sen alkuperäinen elinaika osoittaa, pitää osoitetta päivittää. Elinajan päivitys tapahtuu yksinkertaisesti lähettämällä kotiagentille liityntäkohdan päivitys –sanoma, joka sisälttää uuden elinajan. [2]

Sekä liityntäkohdan päivitys –sanoma että liityntäkohta hyväksytty –sanoma lähetetään käyttäen IPv6-protokollan määränpää optiot –lisäotsikkoa. Nämä molemmat sanomat on lisäksi lähetettävä käyttäen IP Securityn ominaisuuksia. Autentikointi –lisäotsikko on pakollinen ja lisäksi lähetyksessä voidaan käyttää ESP –lisäotsikkoa. [3]

Kun kotiagentti on saanut liityntäkohdan päivitys –sanoman mobiililaitteelta, joka ilmoittaa olevansa vieraslinkillä, ja kuitattuaan päivityksen liityntäkohta hyväksytty –sanomalla, kotiagentti alkaa poimia kyseisen mobiililaitteen kotiosoitteeseen saapuvaa liikennettä. Tämän liikenteen kotiagentti sitten tunneloi mobiililaitteen tilapäiseen osoitteeseen käyttäen IPv6 kotelointia. Mobiililaitteen kotilinkille kotiagentti lähettää ICMPv6-sanoman naapurimainos. Tällä mainoksella kotiagentti ilmoittaa linkin laiteille, että niiden tulee lähettää poislähteneelle mobiililaitteelle suunnattu liikenne kotiagentin linkkitason osoitteeseen. Kotiagentti valvoo myös DAD-prosessia, jotta mikään linkille saapuva uusi laite ei ota käyttöönsä poislähteneiden mobiililaitteiden uniikkeja osoitteita. [1]

Liityntäkohdan päivitys saattaa aiheuttaa pienen katkoksen IP-kerroksen tavoitettavuudessa. Alempien kerrosten toteutuksen ja verkossa sovittavien yleisten toimintatapojen avulla tällaiset katkokset ovat kuitenkin vältettävissä. [3]

10.3.4 Kotiagentin etsintä

Tilanteessa, jossa vieraslinkillä olevan mobiililaiteen käyttämä kotiagentti jostakin syystä menisi epäkuntoon, jäisi kyseinen mobiililaite melkoisen tyhjänpäälle: mobiililaite itse voisi lähettää, mutta kaikki sille osoitetut viestit jäisivät saapumatta perille. Joissakin tilanteissa voisi olla myös mahdollista, että vieraslinkille ajautunut mobiililaite ei yksinkertaisesti

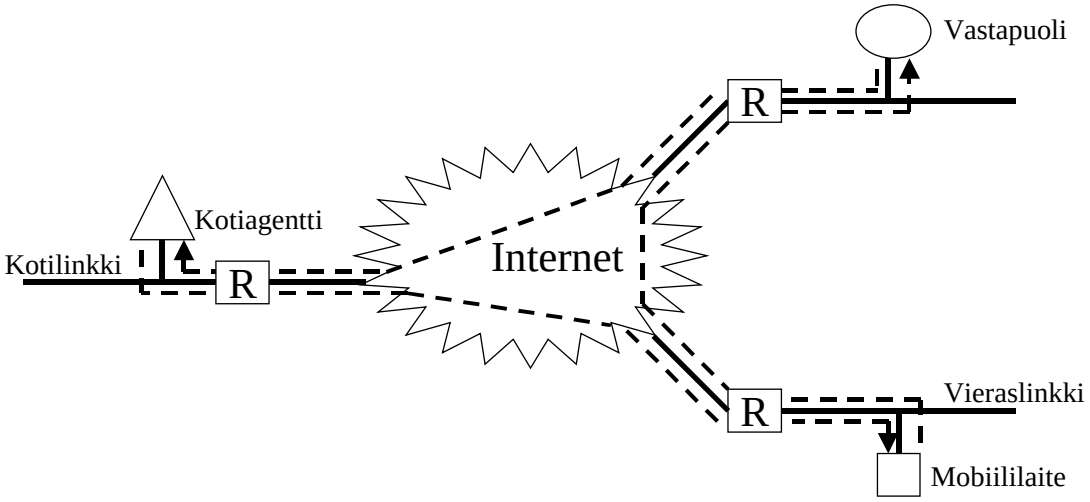
tietäisi oman kotiagenttinsa IP–osoitetta, jolloin tietenkään liityntäkohdan päivitys –sanoman lähettäminen ei olisi mahdollista. [2]

Tällaisia tilanteita varten on kehitetty kotiagentinetsintämekanismi. Mobiililaite voi lähettää ICMPv6-sanoman kotiagentinosoitteenetsintäpyyntö kaikille kotiagenteille menevään anycast-osoitteeseen, jossa verkkoprefiksinä on kotilinkin verkkoprefiksi. Tähän pyyntöön vastaa jokin kotilinkin kotiagenteista ICMPv6-sanomalla kotiagentinosoitteenetsintävastaus. Kotiagentinosoitteenetsintävastaus sisältää mobiililaitteen kotilinkillä olevien kotiagenttien tiedot listattuna sopivuusjärjestykseen, jossa ensimmäisenä ilmoitetaan mobiililaitteen kotiagentiksi parhaiten sopiva kotiagentti. Mikätahansa kotiagentti pystyy lähettämään kaikkien saman linkin kotiagenttien tiedot, koska kotiagentit saavat reititinmainosten avulla tiedon toisistaan ja toistensa sopivuusarvot kotiagentiksi. [2] [3]

Saatuaan kotiagentinetsintävastauksen mobiililaite lähettää liityntäkohdan päivitys –sanoman vastauksen mukaan sopivimmalle kotiagentille. Jos liityntäkohta hyväksytty –sanomaa ei kuulu tai kotiagentti lähettää torjuvan vastauksen, niin mobiililaite voi yrittää lähettää liityntäkohdan päivitys –sanoman listan mukaan seuraavaksi sopivimmalle kotiagentille. [2]

10.3.5 Reitin optimointi

Edellä kuvattu toiminta johtaa kolmioreititykseen, jossa mobiilisolmun vastapuoli lähettää liikennettä kotiagentille, kotiagentti mobiililaitteelle ja mobiililaite vastapuolelle. Tällainen reititys tuhlaa verkon resursseja, koska sanomien välitykseen osallistuu yksi ylimääräinen taho. Ylimääräinen solmu lisää myös virheiden ja pakettien katoamisen mahdollisuutta sekä tuo hitautta kasvattamalla päästä päähän viivettä. Skaalautuvuus suuriin verkkoihin ei tällaisella reitityksellä ole kovinkaan hyvä. Jos yksi kotiagentti joutuu välittämään liikennettä monelle mobiililaitteelle, tulee kotiagentista helposti ruuhkapiste verkkoon – varsinkin lähetettäessä reaaliaikaista tai streaming-tyyppistä dataa. [1]



Kuva3 Kolmioreitityksessä mobiililaite lähettää liikennettä vastapuolelle, vastapuoli kotiagentille ja kotiagentti mobiililaitteelle.

Kolmioreitityksen välttämiseksi Mobile IPv6:ssa mobiililaitteen on mahdollista lähettää liityntäkohdan päivitys –sanoma kotiagentin lisäksi myös vastapuolelle. Näin vastapuoli voi alkaa lähettää liikennettä suoraan mobiililaitteelle ilman kotiagentin avustusta. [1] [3]

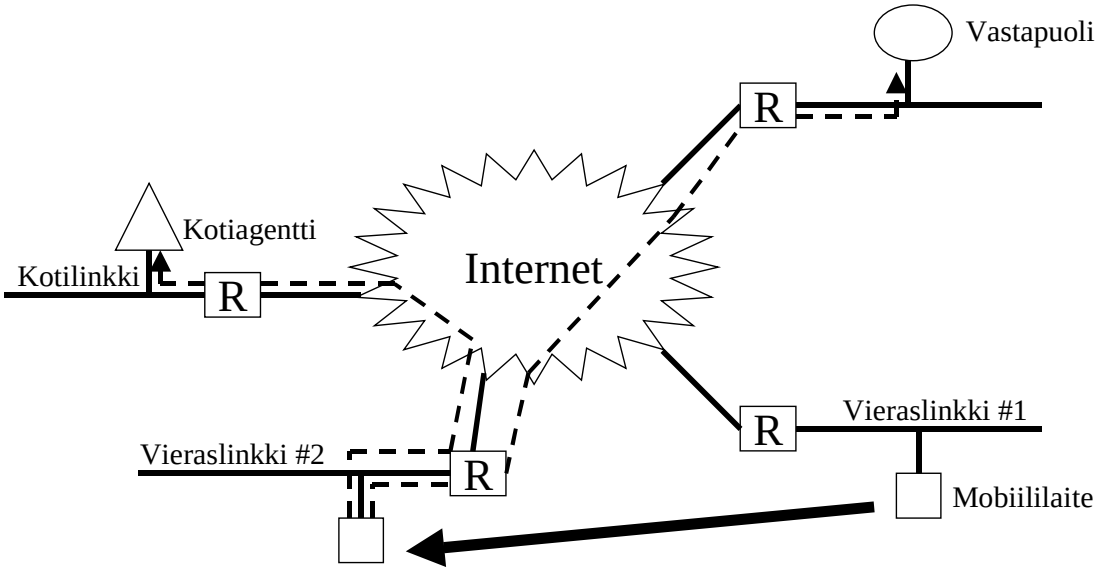
Kun mobiililaite alkaa saada liikennettä vastapuolelta, kulkee tämä liikenne aluksi siis kotiagentin kautta. Tämän jälkeen mobiililaite voi halutessaan lähettää liityntäkohdan päivitys –sanoman vastapuolelle. Kuten kotiagentille lähetettävä päivitys niin myöskin tämä päivityssanoma sisältää aina aikaleiman, joka ilmaiseen, kuinka kauan tilapäinen osoite on voimassa. Erona kotiagentille lähetettävään päivityssanomaan on, että mobiililaite voi itse päättää, haluaako se kuittauksen vastapuolelle lähetettävään liityntäkohdan päivitykseen. Kotiagentille lähetettävä sanoma on aina kuitattava liityntäkohta hyväksytty –sanomalla. [2]

Saatuaan mobiililitteen tilapäisen osoitteen liityntäkohdan –päivitys sanomassa vastapuoli tallettaa tämän osoitteen aikaleimoineen omaan muistiinsa ja lähettää mobiililaitteelle kuittauksen, jos sitä pyydetään. Lähettäessään vastapuoli sitten tarkastaa ensin muististaan, onko sillä kohteen, jolle se on lähettämässä, tilapäinen osoite tiedossa. Jos tilapäinen osoite on saatavilla, vastapuoli käyttää sitä, mutta muuten se joutuu lähettämään liikenteen mobiililaitteen kotiagentin kautta. [2]

Tilanteessa, jossa mobiililaitteen tilapäisen osoitteen elinikä alkaa loppua tai mobiililaite ei jostain syystä ole laisinkaan lähettänyt tilapäistä osoitettaan, voi vastapuoli pyytää mobiililaitetta päivittämään eliniän tai lähettämään tilapäisen osoitteen. Pyyntö tapahtuu liityntäkohdan pyyntö –sanomalla, joka lähetetään liityntäkohdan päivitys ja liityntäkohta hyväksytty –sanomien tapaan käyttäen IPv6-protokollan määränpää optiot –lisäotsikkoa. Liityntäkohdan pyyntöön mobiililaite vastaa liityntäkohdan päivitys –

sanomalla. Mikään pakko mobiililaitteen ei kuitenkaan ole vastata tähän pyyntöön. [2] [3]

Kukin mobiililaite pitää listaa vastapuolille lähettämistään liityntäkohdan päivitys –sanomista. Tähän listaan on myös tallennettu kunkin lähetetyn osoitteen elinaika. Joka kerta, kun mobiililaite saa uuden tilapäisen osoitteen, se lähettää kotiagentin lisäksi liityntäkohdan päivitys –sanoman myös vastapuolille, jotka ovat tässä sen ylläpitämässä listassa. Listasta mobiililaite näkee myös tilapäisen osoitteen päivitystarpeet eri vastapuolille ja pystyy näin halutessaan päivittämään tilapäisen osoitteen elinajan ajoissa. [2]



Kuva4 Mobiililaitteen siirtyessä vieraslinkiltä toiselle se lähettää liityntäkohdan päivitys –sanoman sekä kotiagentille että kaikille vastapuolille, joiden tiedot ovat sen muistissa.

10.3.6 Pääsynsuodatus

Tietoturvan takaamiseksi internetissä on monissa paikoin käytössä pääsynsuodatus. Pääsynsuodatuksella pyritään estämään käyttäjiä esittämästä jotakin toista kuin mitä he oikeasti ovat. Tämä onnistuu tarkkailemalla lähetettävien pakettien lähdeosoitetta.

Pääsynsuodatusalueen rajalla reitittimet tutkivat jokaisen paketin lähdeosoitteen ennen kuin päästävät pakettia eteenpäin julkiseen verkkoon. Rajareitittimet päästävät ohitseen vain sellaiset paketit, joiden lähdeosoite on jokin alueen sisällä oleva mahdollinen osoite. Näin estetään alueen sisältä ulospäin kohdistuvat huijausyritykset. Pääsynsuodatus ei kuitenkaan puutu pakettien lähettämiseen pääsynsuodatusalueen sisällä, jossa siis huijaaminen on edelleen mahdollista. [1]

Mobile IP:lle pääsynsuodatus on ongelma. Mobiililaite käyttää staattista kotiosoitettaan lähdeosoitteena lähettäessään liikennettä, koska yleensä sovellukset tunnistavat mobiililaitteen juuri lähdeosoitteen perusteella. Näin mobiililaite pystytään tunnistamaan myös silloin, kun sen tilapäinen osoite muuttuu kesken olemassaolevan yhteyden. Pääsynsuodatus iskee kuitenkin tällä tavalla lähetettyihin paketteihin, koska kotiosoite lähdeosoitteena ei täytä pääsynsuodatuksen vaatimusta alueen sisäisestä osoitteesta. [1] [3]

Mobile IPv6:ssa pääsynsuodatuksen käyttö on otettu huomioon. Suodatus estetään siten, että kotiosoitetta ei laitetakkaan varsinaisen otsikon lähdeosoitteeksi, vaan se lähetetään käyttämällä määränpää optiot –lisäotsikkoa nimeltä kotiosoite. Varsinaisen otsikon lähdeosoitteeksi voidaan näin laittaa sitten mobiililaitteen tilapäinen osoite. Tällainen järjestely läpäisee pääsynsuodatuksen kriteerit. [1] [3]

Kotiosoitteen lähettäminen määränpää optiot –lisäotsikossa on oltava IPv6–standardin mukaan mahdollista kaikkialla. On tärkeää, että solmupisteet osaavat toimittaa lisäotsikossa lähetetyn kotiosoitteen ylemmille protokollatasoille varsinaisen otsikon lähdeosoitekentässä olevan tilapäisen osoitteen sijaan. Lisäotsikon käyttö kotiosoitteen toimittamiseen aiheuttaa myös muutoksia IP Securityn tarkistuksiin. [1]

10.4 Mobile IPv4 vs Mobile IPv6

Mobile IP –toiminne suunniteltiin alunperin pohjautuvaksi IPv4:ään. IPv4:ssä Mobile IP on kuitenkin lisätoiminne eikä suurin osa IPv4–verkon solmuista tue tätä ominaisuutta. IPv6:n suunnittelussa mobiilisuuden tuki on alusta asti kuulunut vaadittaviin toimintoihin. Näin jokainen IPv6–verkon solmu tulee tukemaan Mobile IP:tä. [3]

Mobile IP:ssä jokaiseen mobiililaitteeseen pitää liittää IP–osoite jokaisella linkillä, johon mobiililaite kytkeytyy. IPv4:ssä osoitteet ovat vähissä jo liikkumattomienkin päätelaitteiden kanssa. Mobiilisuuden myötä jokaisessa verkossa pitäisi siis vielä olla varastossa ylimääräisiä osoitteita, jotta mobiilisuus ylipäänsä pystyttäisiin toteuttamaan. Kun otetaan myös huomioon internetin kasvu ja että kolmannen sukupolven matkapuhelimet tulevat käyttämään IP-osoitteita, loppuvat IPv4–osoitteet auttamattomasti kesken. IPv6:ssa osoitteita on käytössä riittävä määrä. [4]

Turvallisuus on otettu IPv6:ssa alusta alkaen huomioon. Mobile IPv6 hyödyntää IPv6:een integroituja IP Security –ominaisuuksia. Mobile IPv4 joutuu puolestaan käyttämään erillistä UDP–pohjaista protokollaa hoitaakseen turvallisuusasiat kuntoon. [3] [4]

IPv6:ssa osoitteita riittää tarpeeksi ja niinpä Mobile IPv6:ssa tilapäinen osoite on mahdollista muodostaa osoitteen tilattomalla automaattisella konfiguroinnilla. Tällöin tilapäinen osoite saadaan siis yksinkertaisesti yhdistämällä verkkotunnus ja laitetunnus. Tällainen mobiililaitteen itsensä suorittama osoitteenmuodostus ei ole mobile IPv4:ssä mahdollista. [3] [5]

IPv4:n pieni osoiteavaruus on aiheuttanut myös sen, että Mobile IPv4:ssä on jouduttu ottamaan käyttöön vierasagentti. Vierasagentti on jokaisella vieraslinkillä sijaitseva reititin, joka tarjoaa reitityspalveluja mobiililaitteelle. Osoitteita säästyy, koska kaikille vierasagentin takana olevan vieraslinkin mobiililaitteille tuleva liikenne lähetetään tunneloituna vierasagentin IP-osoitteeseen. Vierasagentti sitten poistaa tunneloinnin ja välittää liikenteen eteenpäin mobiililaitteille. Näin jokaiselle mobiililaitteelle ei tarvitse allokoida globaalisti uniikkia IP-osoitetta. Lähettäessään liikennettä vierasagentin takana olevat mobiililaitteet käyttävät vierasagenttia oletusreitittimenä. Mobile IPv4 mahdollistaa kuitenkin myös toiminnan ilman vierasagenttia, jolloin jokaisen vieraslinkin mobiililaitteen täytyy saada oma IP-osoite esimerkiksi DHCP-protokollan avulla. Vierasagenttia ei ole määritelty mobile IPv6:ssa, koska sen käyttöön ei ole tarvetta. [5]

IPv6 tukee anycast-lähetystä, jolloin vieraslinkillä olevan mobiililaitteen on helppo kysyä omalta kotilinkiltään sopivan kotiagentin osoitetta. IPv4:stä anycast-mahdollisuus puuttuu ja ainoa keino kotiagentin kyselyyn on käyttää multicastia. [2] [6]

Verkon tehokkaan käytön aikaansaamiseksi Mobile IPv6 käyttää reitin optimointia, jolloin kolmioreitityksestä päästään eroon. Reitin optimointi on myös implementoitu Mobile IPv4:ään, mutta lisätoiminteena. [1] [3]

Mobile IPv6:ssa voidaan käyttää määränpää optiot –lisäotsikkoa kotioisoitteen lähetykseen, jolloin tilapäisestä osoitteesta lähetettyjen IP–pakettien varsinaisen otsikon lähdeosoitteeksi voidaan laittaa tämä tilapäinen osoite. Näin pääsynsuodatus hyväksyy lähetetyn liikenteen. Mobile IPv4:ssä ei ole mitään mekanismia, jolla pääsynsuodatus voitaisiin kiertää. Tällöin pääsynsuodatuksen ollessa käytössä tilapäisestä osoitteesta lähetetyt paketit menetetään. [1]

10.5 Sanasto

10.5.1 Suomi - Englanti

Autentikointi-lisäotsikko – Authentication header

Hypyltä hypylle optiot – Hop-by-Hop options

Lisäotsikko – Extension Header

Kotelointi – Encapsulation

Kotiagentinetsintämekanismi – Home Agent Discovery Mechanism

Kotiagentinosoitteenetsintäpyyntö – Home Agent Address Discovery Request

Kotiagentinosoitteenetsintävastaus – Home Agent Address Discovery Reply

Kotiagentti – Home Agent

Kotilinkki – Home Link

Kotiosoite – Home Address

Liityntäkohdan pyyntö – Binding Request

Liityntäkohdan päivitys – Binding Update

Liityntäkohta hyväksytty – Binding Acknowledged

Liityntäkohtamuisti – Binding Cache

Mobiililaite – Mobile Node

Määränpää optiot – Destination Options

Naapurimainos – Neighbor Advertisement

Pääsynsuodatus – Ingress Filtering

Reititinmainos – Router Advertisement

Reititinpyyntö – Router Solicitation

Tilallinen osoitteen automaattinen konfigurointi – Stateful Address Autoconfiguration

Tilapäinen osoite – Care-of-Address

Tilaton osoitteen automaattinen konfigurointi – Stateless Address Autoconfiguration

Vastapuoli – Correspondent Node

Vierasagentti – Foreign Agent

Vieraslinkki – Foreign Link

10.5.2 Lyhenteet

DAD – Duplicate Address Detection

DHCP – Dynamic Host Configuration Protocol

ESP – Encapsulating Security Payload

ICMP – Internet Control Message Protocol

IETF – Internet Engineering Task Force

IP – Internet Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

10.6 Lähdeluettelo

[1] MITA - Mobile Internet Technical Architecture, IT Press, 2001

[2] Mobile IPv6 – Mobility Support for the Next Generation Internet, IABG, 2000

[3] Introducing Mobile IPv6 in 2G and 3G Mobile Networks, Nokia, 2001

[4] IPv6 – Enabling the Mobile Internet, Nokia, 2000

[5] RFC 2002

[6] RFC 2373

Internet–osoitteita:

www.ipv6forum.com

www.ietf.org

www.nokia.com/ipv6