



TAMPEREEN TEKNILLINEN KORKEAKOULU

Tietotekniikan osasto

TERO HAKKARAINEN

**PAIKALLISET WAP-PALVELUT PAN-VERKOSSA**

DIPLOMITYÖ

Aihe hyväksytty osastoneuvoston kokouksessa 14.3.2001.

Tarkastajat: Prof. Ilkka Haikala  
Jari Ahola, tekn. lis.

## **Alkulause**

Olen tehnyt diplomityöni VTT Tietotekniikassa Tampereella. Erityisen tyytyväinen olen siihen, että sain tehdä työni aiheesta, joka on koettu tutkimusryhmässämme tärkeäksi ja jota on jo pitkään kypsytelty mielissämme.

Kiitän työn tarkastajaa, professori Ilkka Haikalaa, sekä työn ohjaajaa, tekn. lis. Jari Aholaa, rakentavista kommentteista ja parannusehdotuksista.

Esitän myös kiitokseni kollegalleni Ali Lattuselle, jonka ideat ja kysymykset selvensivät työtäni usein enemmän kuin lähteistä löytyneet vastaukset.

Piia, sinua kiitän kärsivällisyydestä ja tuesta niinä parina kuukautena, joiden aikana olen hektisesti kirjoittanut tätä työtä.

Tampere, toukokuu 2001

Tero Hakkarainen  
Virtainpolku 13 A 15  
33720 TAMPERE

# Sisällysluettelo

Alkulause.....	i
Sisällysluettelo .....	ii
Tiivistelmä.....	iv
Abstract .....	v
Lyhenteet ja termit .....	vi
1 Johdanto .....	1
2 Wireless Application Protocol (WAP).....	3
2.1 Taustaa .....	3
2.2 Perusteet .....	4
2.2.1 WAP-protokollaan kohdistuvat vaatimukset .....	4
2.2.2 Sovellusten rakenne.....	5
2.2.3 Toiminnallinen malli .....	7
2.2.4 Protokollapino .....	9
2.3 Tulevaisuus.....	12
2.3.1 Kehitysnäkökohtia.....	12
2.3.2 Kilpailijat.....	12
3 Paikalliset WAP-palvelut .....	15
3.1 Paikallisuuden ongelma.....	15
3.2 Ominaispiirteet .....	16
3.3 Käyttökohteet .....	17
3.4 Vaatimukset verkkotekniikalle.....	19
4 PAN-verkot .....	22
4.1 Määritelmä .....	22
4.2 Ominaisuudet .....	22
4.3 Liittymät .....	24
5 PAN ja langattomat verkkotekniikat .....	25
5.1 Bluetooth .....	25
5.1.1 Taustaa .....	25
5.1.2 Tiedonsiirtomenetelmä.....	26
5.1.3 Kommunikaatiomalli.....	28

5.1.4	Protokollapino .....	34
5.1.5	Sopivuus PAN-verkoksi.....	39
5.2	Langaton paikallisverkko .....	39
5.2.1	Taustaa .....	40
5.2.2	Tiedonsiirtomenetelmä.....	41
5.2.3	Rakenne.....	43
5.2.4	Protokollapino .....	47
5.2.5	Toiminta .....	48
5.2.6	Sopivuus PAN-verkoksi.....	49
5.3	Muut järjestelmät.....	50
5.3.1	IrDA .....	50
5.3.2	HomeRF .....	52
5.3.3	HIPERLAN .....	53
5.4	Yhteenveto .....	55
6	Paikallisen WAP-palvelun toteutus Bluetoothilla.....	56
6.1	WAP:n ja Bluetoothin väliset liittymät .....	56
6.2	Laitteisiin kohdistuvat vaatimukset ja rajoitteet.....	58
6.2.1	Asiakaslaite .....	58
6.2.2	Palvelin.....	59
6.3	WAP-istunnon kulku.....	60
6.4	Useiden asiakkaiden palveleminen .....	66
6.5	Toteutusnäkökohtia .....	67
6.5.1	Asiakkaan tunnistaminen .....	67
6.5.2	WAP-sisällön salaus.....	68
6.5.3	Yhteydenmuodostusajan minimointi .....	69
6.5.4	Virhetilanteiden käsittely .....	69
6.6	Esimerkkisovelluksia .....	70
6.6.1	Kehitysvaiheessa olevan WAP-palvelun testaus.....	70
6.6.2	Linja-autoliikenteen asiakasjärjestelmä .....	71
7	Yhteenveto .....	73
	Lähdeluettelo.....	76

# TAMPEREEN TEKNILLINEN KORKEAKOULU

Tietotekniikan osasto

Ohjelmistotekniikka

HAKKARAINEN, TERO: Paikalliset WAP-palvelut PAN-verkossa

Diplomityö, 78 s.

Tarkastaja: prof. Ilkka Haikala

Rahoittaja: VTT Tietotekniikka

Toukokuu 2001

Avainsanat: WAP, PAN, Personal Area Networking, Bluetooth,  
WAP-over-Bluetooth, WLAN

Perinteiset WAP-palvelut eivät pysty tehokkaasti jakamaan paikallista informaatiota, koska asiakkaan paikantaminen vaatii aina ulkoisia verkko- tai laitepalveluita. Paikallinen WAP-palvelu tarjotaan päätelaitteisiin lyhyen kantaman langattoman, ilmaiseksi käytettävän verkon kautta. Palveluun kytkeytyvä asiakas paikannetaan automaattisesti edellä kuvatun nk. PAN-verkon rajatun käyttöalueen avulla. Paikallisen WAP-palvelun avulla päätelaitteisiin voidaan tarjota tarkkaa ja ajankohtaista lähiympäristöön liittyvää informaatiota.

Tässä työssä pohditaan paikallisten WAP-palveluiden periaatteita ja toteutukseen liittyviä ratkaisuja. Saatavilla olevia langattomia verkkotekniikoita vertaillaan, jotta niiden soveltuvuus paikallisen palvelun kantajaksi selviää. Bluetooth-tekniikan todetaan olevan teknisesti vahvin ehdokas paikallisen WAP-palvelun toteuttavaksi langattomaksi menetelmäksi. Työssä esitetään sen vuoksi WAP-over-Bluetooth –konseptin toteuttamiseen liittyviä protokolla-, verkko- ja sovellustason ratkaisuja. Työssä saavutettuja tuloksia tullaan hyödyntämään VTT Tietotekniikan aiheeseen liittyvissä toteutusprojekteissa.

TAMPERE UNIVERSITY OF TECHNOLOGY

Department of Information Technology

Software Systems Laboratory

HAKKARAINEN, TERO: Local WAP Services in Personal Area Networks

Master of Science Thesis, 78 pages.

Examiner: Prof. Ilkka Haikala

Financier: VTT Information Technology

May 2001

Keywords: WAP, PAN, Personal Area Networking, Bluetooth,  
WAP-over-Bluetooth, WLAN

Traditional WAP services adapt poorly to delivering local or location-dependent information, because external locating services or devices are always needed. The approach used in local WAP services is somewhat different: services are delivered in short-range wireless networks that can be used without operator fees. These networks are commonly called *Personal Area Networks (PAN)*. Customers are automatically positioned with adequate accuracy when they enter the range of the local service. The positioning is based on the limited range of the PAN network, so there is no need for additional hardware. Local WAP services offer accurate and current localized information to the customer.

This thesis describes the principles and implementation issues of local WAP services. The currently available wireless short-range networks are studied in respect of PAN network concept. The Bluetooth technology is found to be the most suitable network technology for local WAP services. Implementation issues of *WAP-over-Bluetooth* systems are therefore described including protocol, network and application level aspects. The findings of this thesis will be utilised in local WAP service implementation projects of VTT Information Technology.

## Lyhenteet ja termit

<i>ACL</i>	Asynchronous, Connection-Less
<i>AP</i>	Access Point
<i>ATM</i>	Asynchronous Transfer Mode
<i>BLIP</i>	Bluetooth Local Infotainment Point
<i>bps</i>	bittiä sekunnissa
<i>CAC</i>	Channel Access Control
<i>CGI</i>	Common Gateway Interface
<i>CP</i>	Connection Point
<i>CRC</i>	Cyclic Redundancy Check
<i>CSD</i>	Circuit Switched Data
<i>CSMA/CA</i>	Carrier Sense Multiple Access Collision Avoiding
<i>DECT</i>	Digitally Enhanced Cordless Telephony
<i>DHCP</i>	Dynamic Host Configuration Protocol
<i>DNS</i>	Domain Name System
<i>DS</i>	Distribution System
<i>DSSS</i>	Direct-Sequence Spread Spectrum
<i>EP</i>	Extension Point
<i>ETSI</i>	European Telecommunications Standards Institute
<i>FHSS</i>	Frequency-Hopping Spread Spectrum
<i>GPRS</i>	General Packet Radio System
<i>GPS</i>	Global Positioning System
<i>GSM</i>	Global System for Mobile Communications
<i>HCI</i>	Host Controller Interface
<i>HDML</i>	Handheld Device Markup Language
<i>HIPERLAN</i>	High Performance Radio Local Area Network
<i>HTML</i>	HyperText Markup Language
<i>HTTP</i>	HyperText Transfer Protocol
<i>IANA</i>	Internet Assigned Numbers Authority
<i>IAS</i>	Information Access Service
<i>IEEE</i>	Institute of Electrical and Electronics Engineers

<i>IETF</i>	Internet Engineering Task Force
<i>IP</i>	Internet Protocol
<i>IPX</i>	Internetwork Packet eXchange
<i>IrDA</i>	Infrared Data Association
<i>ISDN</i>	Integrated Services Digital Network
<i>ISM</i>	Industrial, Scientific, Medical. Vapaasti käytettävä taajuusalue.
<i>ITTP</i>	Intelligent Terminal Transfer Protocol
<i>ITU-T</i>	International Telecommunications Union - Telecommunication
<i>LAN</i>	Local Area Network
<i>LAP</i>	LAN Access Profile
<i>LLC</i>	Logical Link Control
<i>LMP</i>	Link Manager Protocol
<i>L2CAP</i>	Logical Link Control And Adaptation Protocol
<i>MAC</i>	Medium Access Control
<i>Mbps</i>	Miljoonaa bittiä sekunnissa
<i>MPEG-4</i>	Moving Picture Experts Group Layer 4
<i>OBEX</i>	OBject EXchange
<i>OSI</i>	Open Systems Interconnection
<i>PAN</i>	Personal Area Networking
<i>PCM</i>	Pulse Code Modulation
<i>PIN</i>	Personal Identification Number
<i>PPP</i>	Point to Point Protocol
<i>SCO</i>	Synchronous, Connection-Oriented
<i>SDP</i>	Service Discovery Protocol
<i>SIG</i>	Special Interest Group
<i>SMS</i>	Short Message Service
<i>SSL</i>	Secure Sockets Layer
<i>SWAP</i>	Shared Wireless Access Protocol
<i>TCP</i>	Transmission Control Protocol
<i>TCP/IP</i>	Internetin perustana oleva protokollamalli
<i>TCS-BIN</i>	Telephony Control Specification, Binary Encoding
<i>TDD</i>	Time Division Duplex
<i>UART</i>	Universal Asynchronous Receiver Transmitter
<i>UDP</i>	User Datagram Protocol



<i>UMTS</i>	Universal Mobile Telecommunications System
<i>URL</i>	Universal Resource Locator
<i>USB</i>	Universal Serial Bus
<i>WAP</i>	Wireless Application Protocol
<i>WDP</i>	Wireless Datagram Protocol
<i>WEP</i>	Wireless Equivalent Privacy
<i>WLAN</i>	Wireless Local Area Network
<i>WML</i>	Wireless Markup Language
<i>WPAN</i>	Wireless Personal Area Network
<i>WTAI</i>	Wireless Telephony Application Interface
<i>WTLS</i>	Wireless Transport Layer Security
<i>WSP</i>	Wireless Session Protocol
<i>WTP</i>	Wireless Transport Protocol
<i>WWW</i>	World Wide Web
<i>XML</i>	eXtensible Markup Language

# 1 Johdanto

WAP on kuulunut jo useiden vuosien ajan matkapuhelinmarkkinoiden iskusanoihin. Alkuaikoina lyhenteellä oli lähinnä imagoarvo, koska puolivalmiit palvelut eivät pystyneet tyydyttämään käyttäjäkunnan vaatimuksia. Tähän päivään mennessä sekä palvelut että päätelaitteet ovat kehittyneet, joten WAP:lla on vihdoinkin mahdollisuus näyttää kyntensä. Ripeää kehitystyötä tarvitaan kuitenkin edelleen, koska maailmalta on tulossa kilpailevia, ominaisuuksiltaan parempia tekniikoita.

Henkilökohtainen verkottuminen on tällä hetkellä tietoliikennealan kuumimpia aiheita. Termi *Personal Area Network (PAN)* on vakiintunut tarkoittamaan langatonta tietoverkkoa, joka muodostuu dynaamisesti käyttäjän päätelaitteen ja ympäristön laitteiden välille. PAN-verkot avaavat sovelluskehittäjille täysin uudenlaisen ympäristön, jossa ei ole kaapeleiden tai infrastruktuuriverkkojen rajoitteita. Koska verkko toimii ja konfiguroituu hyvin itsenäisesti, jää sovelluksille resursseja palvella käyttäjää entistä monipuolisemmilla ja älykkäämmillä tavoilla. PAN-verkkoja voidaan perustellusti pitää avaimena langattomien päätelaitteiden kehittämiseen ja yleistymiseen.

WAP-konseptin ja PAN-verkkojen yhdistäminen on mielenkiintoinen idea, joka tuo esille kummankin tekniikan parhaat puolet. PAN-verkko tarjoaa tehokkaan, dynaamisesti konfiguroituvan paikallisen siirtomedian, joka voidaan muodostaa hyvin erilaisten laitteiden välille. WAP-sovellukset on suunniteltu mukautumaan langattomiin päätelaitteisiin, joiden näyttö- ja syöttölaitteet sekä suorituskyky voivat olla ominaisuuksiltaan rajoitetut. WAP-arkkitehtuuri toimii siis yhdistelmässä käyttöliittymän ja sovelluslogiikan osassa, kun taas PAN-verkko huolehtii yhteyksien muodostamisesta ja ulkoisten palveluiden käytettävyydestä. Yhdistelmäjärjestelmän tarjoamista joustavista, ilmaisista, paikkaan sidotuista palveluista muodostuu käsite nimeltä paikallinen WAP-palvelu. Palvelu on käytettävissä vain sillä alueella, jolla henkilökohtainen verkko toimii. Koska alue on tyypillisesti pieni ympyrä, jonka säde on noin 10 metriä, voidaan käyttäjälle tarjota paikkariippuvaa, ajanmukaista tietoa ilman ulkoisia paikannusmenetelmiä tai -laitteita.

Tässä työssä esitellään paikallisen WAP-palvelun tekniikkaa. Työn luonne on tutkiva ja erilaisia vaihtoehtoja punnitseva, koska työtä tullaan hyödyntämään VTT Tietotekniikan aihetta käsittelevissä toteutusprojekteissa. Paikallisen WAP-palvelun konseptia pohditaan perusteellisesti sekä WAP-palvelun että PAN-verkon kannalta.

Koska henkilökohtaista verkottumista ei ole sidottu mihinkään tiettyyn verkkotekniikkaan, tutkitaan työssä myös olemassaolevien langattomien lähikommunikaatiomenetelmien sopivuutta verkon toteuttamiseen. Paikallisen WAP-palvelun rakentamista käsitellään sekä yleisesti että Bluetooth-tekniikan kannalta, koska koko PAN-ideologia on oikeastaan syntynyt juuri Bluetoothin myötä. Valinta on perusteltu, koska Bluetooth tulee olemaan lähivuosien merkittävin henkilökohtaisten verkkojen tekniikka.

Luvussa 2 esitellään WAP-tekniikan lähtökohdat ja perusratkaisut, koska ne ovat oleellisia myös paikallisen WAP-palvelun olemuksen ymmärtämisessä. Luvussa 3 määritetään, mikä on paikallinen WAP-palvelu. Samalla pohditaan mahdollisia sovelluskohteita ja vaatimuksia käytettävälle verkkotekniikalle. Luvussa 4 kerrotaan yleisellä tasolla henkilökohtaisten PAN-verkkojen ominaisuuksista ja siitä, miten verkko voidaan liittää muihin sovellus- ja protokollajärjestelmiin. Luvussa 5 sovitaan Bluetooth-, WLAN-, IrDA-, HomeRF- ja HIPERLAN-verkkotekniikoita PAN-verkon pohjaksi. Luvussa 6 käsitellään paikallisen WAP-palvelun toteuttamista Bluetooth-tekniikalla. Luvussa esitetään WAP:n protokollapinon ja perusmekanismien sovitusta Bluetooth-verkon päälle ja otetaan kantaa muutamiin esimerkiksi tietoturvallisuuteen liittyviin toteutusnäkökohtiin.

## 2 Wireless Application Protocol (WAP)

Lyhenne WAP muodostuu sanoista *Wireless Application Protocol*, joka voidaan suomentaa vapaasti esimerkiksi “menetelmä langattomille sovelluksille”. Suomentos antaa selviä viitteitä tekniikan käyttötarkoituksesta: interaktiivisen informaation langattomasta siirtämisestä kädessä pidettäviin päätelaitteisiin.

### 2.1 Taustaa

1990-lukua voidaan perustellusti pitää Internetin ja matkapuhelinten vuosikymmenenä. Informaation dynaaminen saatavuus oli teema, joka muutti merkittävästi ja peruuttamattomasti monien palveluiden luonteen. Vuosikymmeniä vanhat traditiot kokivat dramaattisen lopun, kun kaiken tiedon pankkitileistä lottonumeroihin piti yhtäkkiä olla kenen tahansa saatavilla, milloin ja missä tahansa. Puhumattakaan siitä, että päivän trendin mukaan jokaisen piti olla tavoitettavissa vuorokauden ympäri matkapuhelimen välityksellä.

Matkapuhelinten maailma ja Internet olivat aluksi täysin erityyppisiä. Internet liitettiin käsitteenä ei-kannettaviin, tehokkaihin, kiinteässä verkossa oleviin tietokoneisiin, vaatimattomilla resursseilla varustetut kännykät taas soveltuivat ainoastaan kahden ihmisen väliseen kommunikaatioon joko puheen tai tekstin välityksellä. Mobiili- ja Internet-maailma elivät muutamia vuosia omaa, eristettyä elämäänsä. Kumpikin koki voimakkaan kasvusuhdanteen, jossa käyttäjien määrän lisääntymistä kuvattiin eksponentiaalisilla käyrillä. Muutaman vuoden kuluttua alkoi kuitenkin esiintyä merkkejä siitä, että näiden kahden sittemmin jo vakiintuneen tekniikan tiet tulisivat kohtaamaan. Kiihkeään kehitykseen tottunut matkapuhelinkäyttäjäkunta ei enää pysynyt tyytyväisenä pelkillä soittoäänillä tai värikuorilla: matkapuhelimella piti päästä lukemaan sähköpostia ja selaamaan seittisivuja. Motivaationa yhdistämiselle olivat siis paitsi käyttäjien vaatimukset, myös markkinoilla liikkuvat suuret rahat. Ei siis ihme, että 90-luvun puolivälissä lähes kaikki suuret matkapuhelinvalmistajat alkoivat suunnata resurssejaan Internetin ja matkapuhelinten erilaisten maailmojen yhdistämiseen. Tämä johti monien vaiheiden kautta WAP:n syntyyn.

WAP:lle voidaan löytää useita esi-isiä. Ruotsalainen matkapuhelinvalmistaja *Ericsson* alkoi vuonna 1995 kehittää tapaa toteuttaa lisäpalveluja matkapuhelimiin. Työn tuloksena syntyi protokolla nimeltä ITTP (*Intelligent Terminal Transfer*

*Protocol*). Suomalainen matkapuhelinvalmistaja *Nokia* aloitti hieman myöhemmin omalla tahollaan *Smart Messaging* –tekniikan kehittämisen. Tekniikka tarjosi avoimen rajapinnan lyhytviestipohjaisten matkapuhelinsovellusten kehittämiseen. Yhtiö nimeltä *Unwired Planet* (sittemmin *Phone.com*) kehitti HTML-kieleen<sup>1</sup> pohjautuvan, pienille näytöille optimoidun dokumentinkuvauskielen, HDML:n (*Handheld Device Markup Language*). Yhtiöt ymmärsivät kuitenkin melko pian, etteivät eri tahoilla kehitetyt ratkaisut tuottaisi maailmanmarkkinoita tyydyttävää tulosta. Niiden vaikutus saattaisi olla täysin päinvastainen: markkinat pirstoutuisivat yhteensopimattomiin palasiin ja tekniikoiden uskottavuus tuhoutuisi. Ainoaksi järkeväksi ratkaisuksi jäi konsortion, WAP Forum:n, perustaminen kesällä 1997. Sen tehtäväksi muodostui eri tahoilla siihen asti tehdyn tutkimustyön tulosten yhdistäminen, kehitystyön jatkaminen sekä uusien yritysten ja organisaatioiden mukaantuominen. Perustajajäseniä olivat edellä mainitut Ericsson, Nokia ja Unwired Planet sekä yhdysvaltalainen elektroniikkajätti Motorola. WAP Forumin työ on ollut ilmeisen menestyksekkästä, koska tällä hetkellä konsortiossa on yli 500 jäsentä. [Held2001]

WAP-spesifikaation versio 1.0 julkistettiin keväällä 1998, noin vuosi WAP Forum:n perustamisen jälkeen. Siihen perustuvia tuotteita ei kuitenkaan koskaan tuotu markkinoille. Ensimmäiset WAP-matkapuhelimet perustuivat WAP-spesifikaation versioon 1.1, joka julkistettiin kesällä 1999. Viimeisin WAP Forum:n julkaisema spesifikaatio on kesällä 2000 julkaistu versio 1.2.1.

## **2.2 Perusteet**

WAP on langattoman kahdenvälisen tietoliikenteen toteuttava protokollapino, jossa on yhtäläisyyksiä Internetissä käytettävään TCP/IP-protokollapinoon [Tane1996]. Sen käyttöympäristö eroaa kuitenkin huomattavasti tyypillisestä Internet-isäntäkoneesta, mikä näkyy väistämättä protokollien perusratkaisuissa.

### **2.2.1 WAP-protokollaan kohdistuvat vaatimukset**

Kädessä pidettävät, massatuotannossa olevat langattomat päätelaitteet (esimerkiksi matkapuhelimet) ovat tyypillisesti huomattavasti pöytäkoneita vaatimattomammin va-

---

<sup>1</sup> HyperText Markup Language. Seitissä käytettävä dokumentinkuvauskieli [Tane1996].

rusteltuja. Niissä on heikkotehoisempi mikroprosessori, vähemmän muistia, pieni näyttö, rajoitettu tehonsaanti ja yksinkertaiset syötelaitteet. Langattomat tiedonsiirtoverkot puolestaan tarjoavat kiinteitä verkkoja vähemmän kaistanleveyttä, luotettavuutta ja ennustettavia viiveitä. [WAPF1998]

Jotta WAP:sta olisi mahdollista kehittyä maailmanlaajuisesti varteenotettava ratkaisu langattomien päätelaitteiden liittämiseksi Internetiin, on sen arkkitehtuurin oltava harkiten suunniteltu. Olemassaolevia standardeja on voitava hyödyntää mahdollisimman pitkälle, jotta yhteensopivuus Internet-maailman kanssa voidaan turvata. Protokolla-arkkitehtuurin on oltava pinomainen, jotta yksittäisiä protokollia voidaan korvata uusilla versioilla tai jopa toisilla protokollilla silloin, kun WAP:n ympäristöön tulee muutoksia. Tämä vaatimus on erityisen tärkeä juuri langattomien verkkojen ja Internetin kiihkeästi kehittyvässä maailmassa. Lisäksi arkkitehtuurin on oltava skaalautuva ja laajennettava, jotta WAP-protokollaa pystytään hyödyntämään myös tulevaisuuden suorituskykyisissä langattomissa verkoissa.

WAP-arkkitehtuurin tulee olla mahdollisimman verkkoriippumaton, toisin sanoen arkkitehtuurin tulee tukea liittymistä erilaisiin verkkotekniikoihin. Markkinat ovat tällä hetkellä melko homogeeniset, koska suurin osa langattomista päätelaitteista toimii joko GSM-verkon (*Global System for Mobile Communications*) tai infrapuna-kommunikaation avulla. Tilanne tulee kuitenkin lähitulevaisuudessa muuttumaan, kun erilaiset pakettikytkentäiset langattomat verkkoratkaisut yleistyvät. WAP-protokollan on pystyttävä mukautumaan mahdollisimman moneen uuteen järjestelmään, jotta sen asema globaalina langattomien sovellusten kehyksenä voidaan turvata.

Monet niistä sovelluksista, joita WAP-ympäristössä tullaan käyttämään, asettavat tiukkoja vaatimuksia tietoliikenneyhteyden turvallisuudelle. Tällaisia sovelluksia ovat esimerkiksi pankki-, maksu- ja kulkuoikeussovellukset. Tietoturvallisuuteen liittyvät näkökohdat on näin ollen otettava huomioon jo protokolla-arkkitehtuuria suunniteltaessa, jotta yhteysosapuolten tunnistaminen ja yhteyden salaaminen voidaan toteuttaa mahdollisimman aukottomasti ja tehokkaasti.

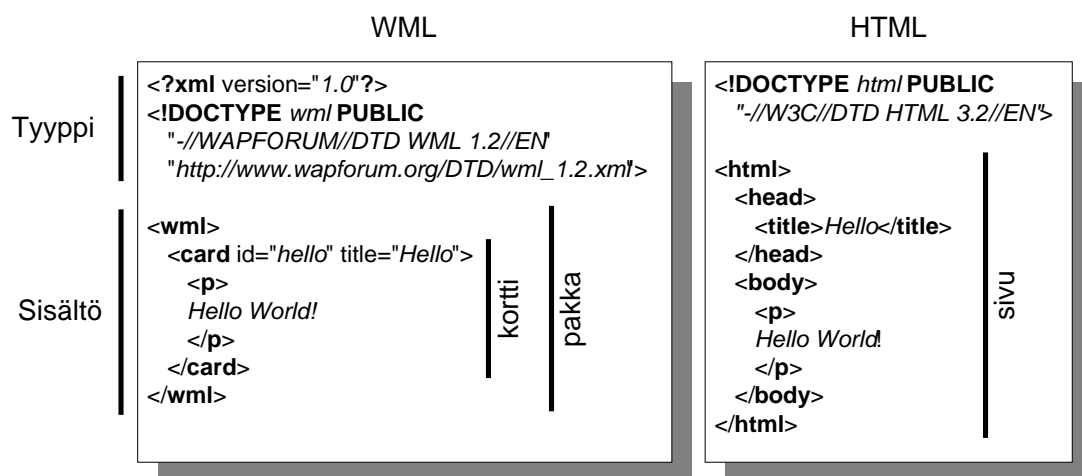
### **2.2.2 Sovellusten rakenne**

WAP-sovellukset eroavat merkittävästi tyypillisistä työasemasovelluksista. Perinteisessä tietojenkäsittelyssä sovellus, siihen liittyvä laskenta ja käyttöliittymän esittäminen suoritetaan samassa tietokoneessa. Tämä paradigma ei kuitenkaan sovi WAP-pää-

telaitteisiin, koska niiden heikko prosessointiteho ja pieni muistikapasiteetti rajoittavat sovellusten toteuttamista. Sovelluksen käsitettä joudutaan siis WAP-ympäristössä muokkaamaan.

WAP-sovellus on periaatteessa hypertekstidokumentti, joka koostuu toisiinsa liittyvistä näkymistä. Näkymät muodostuvat tekstistä, kuvista ja interaktiivisista elementeistä, kuten linkeistä, jotka luovat näkymien välille assosiatiivisuutta. Käyttäjä voi kontrolloida sovelluksen etenemistä aktivoimalla linkkejä. Syötteet annetaan sovelluksen näkymissä sijaitseviin objekteihin, kuten teksti- ja valintakenttiin sekä nappeihin, ja tulosteet näytetään joko uusina tai päivitettyinä näkyminä. WAP-sovellukset muistuttavat siis läheisesti Internetistä tuttuja seittisivuja.

WAP-sovellukset ovat WML (*Wireless Markup Language*) -dokumentteja. WML on XML-standardiin (*eXtensible Markup Language*) perustuva kuvauskieli, jolla on tiettyjä yhtäläisyyksiä HTML:n kanssa. Kuvassa 2.1 on nähtävissä yksinkertainen tervehdyssivu toteutettuna kummallakin kuvauskielellä. Kielten elementit on merkitty kuvaan lihavoidulla, attribuutit normaalilla ja sisältö kursivoidulla tekstityypillä. Voidaan huomata, että sekä dokumenttien rakenteessa että elementeissä on yhtäläisyyksiä ja eroavaisuuksia. Kummassakin dokumentissa määritellään ensin dokumentin tyyppi ja sen jälkeen sisältö. Tyypinmäärittely on pääpiirteissään sama, mutta sisällön kuvaukseen käytetyt elementit ovat lähes täysin erilaisia. Kuvauskielten peruseriaatteet ovat kuitenkin yhtenevät, sillä dokumentit muodostuvat tekstistä, jota erilaiset rakennetta ja assosiatiivisuutta luovat tunnisteet jäsentävät.



Kuva 2.1. Yksinkertainen tervehdys WML- ja HTML-muodossa.

WML-dokumenttia voidaan verrata korttipakkaan, joka koostuu yhdestä tai useammasta kortista. Edellä esitetyssä kuvassa oleva WML-pakka sisältää esimerkiksi vain yhden kortin. Pakkaa voidaan ajatella HTML-sivustona, jolla on osoite ja joka esittää jonkin sisällöllisen kokonaisuuden [Held2001]. Kortti määrittelee yhden näkymän, joka muodostuu yhdestä tai useammasta elementistä. Kuvan 2.1 kortti sisältää vain yhden elementin: tekstilohkon ”*Hello World*”. Kortti sisältää yleisesti ottaen pienen osan koko dokumentista, joten se on helposti sovitettavissa pienikokoiselle näytölle. Tässä mielessä WML:n voidaan ajatella olevan joustavampi kuin HTML, jossa käyttäjälle esitetään kerralla koko dokumentti, vaikka se olisi laaja ja vaikeasti jäseneltävissä. WML-dokumentin lukija sen sijaan navigoi yksittäisten näkymien eli korttien välillä hakien tietoa ja tehden valintoja seuraavien korttien näyttämiseksi.

Seittisivuille on mahdollista lisätä osia, jotka tuovat sisältöön ohjelmoitavuutta. Tällaisia laajentavia osia ovat muun muassa *JavaScript*- ja *CGI<sup>2</sup>*-komentojonot sekä Java-appletit. Niiden avulla voidaan luoda dynaamisesti sisältöä, lisätä sivuihin interaktiivisuutta ja suorittaa monimutkaisia graafisia operaatioita. Myös WAP-sovelluksissa on mahdollista käyttää edellä mainitun kaltaisia komentosarjoja; tekniikka on tässä ympäristössä nimeltään *WMLScript* [Held2001]. *WMLScript*-tekniikka pohjautuu Javascriptin tavoin malliin, jossa komentosarja tai ohjelma suoritetaan virtuaalisessa tietokoneessa, jota ajetaan todellisen käyttöjärjestelmän päällä. Nämä ns. *virtuaalikoneet* ovat kuitenkin keskenään yhteensopimattomia. Tekniikoissa on näin sekä yhtäläisyyksiä että fundamentaalisia eroavaisuuksia.

### 2.2.3 Toiminnallinen malli

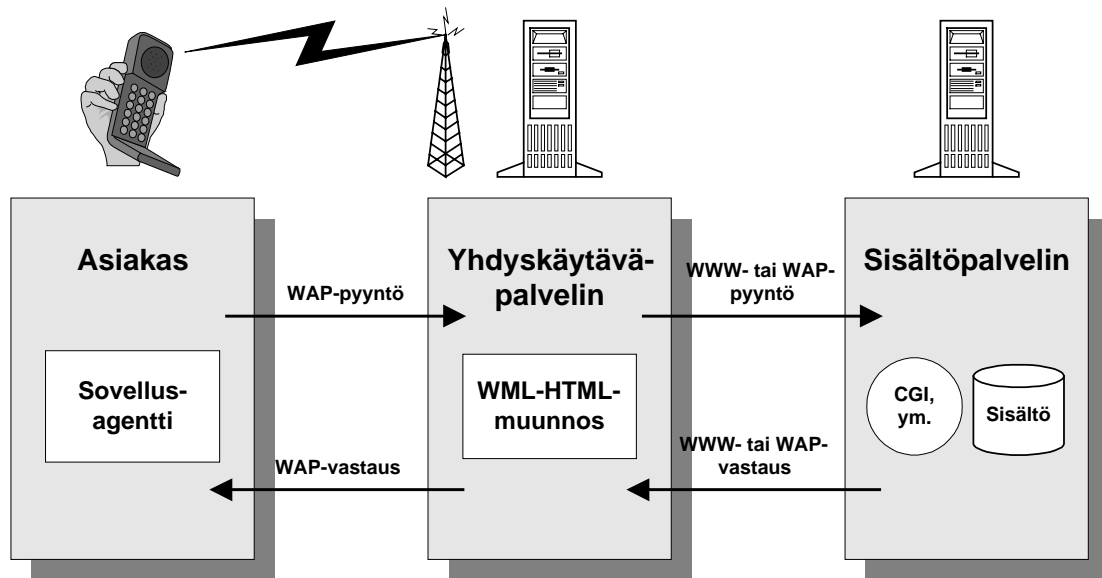
Yhteys Internet-maailmaan näkyy selkeästi WAP:n toiminnallisessa mallissa. Malli perustuu seitissä käytettävään asiakas-palvelin-malliin, jossa palvelin vastaa asiakkaan lähettämiin pyyntöihin. WAP-mallin yhteneväisyys seittimalliin tuo useita etuja, kuten tutun ohjelmointiympäristön, hyväksi havaitun arkkitehtuurin ja mahdollisuuden hyödyntää olemassaolevia työkaluja [WAPF1998].

WAP:n toiminnallisessa mallissa, jota on havainnollistettu kuvassa 2.2, on yksi merkittävä eroavaisuus seitin malliin nähden: WAP:ssa käytetään yhdyskäytäväpal-

---

<sup>2</sup> Common Gateway Interface. Laajasti käytetty ohjelmointirajapinta seittipalvelimille.





Kuva 2.2. WAP:n toiminnallinen malli.

velinta (*Gateway*), joka toimii sovittimena langattoman verkon ja Internetin välissä [WAPF1998]. Yhdyskäytäväpalvelimesta käytetään myös nimeä välityspalvelin (*WAP Proxy*). Sisältöpalvelin on joko WAP- tai seittipalvelin. Kumpikin sisältää hyperdokumenteja, jotka ovat kuitenkin keskenään erimuotoisia. Palvelimet toimivat osana kiinteää Internetiä. Yhdyskäytäväpalvelin toimii siis asiakkaan edustajana kiinteässä verkossa. Käytännön yhdyskäytäväpalvelimet toteuttavat usein myös WAP-palvelimen toiminnallisuuden, jolloin niillä on tarjota päätelaitteille paitsi omaa sisältöä, myös mitä tahansa Internetissä olevaa sisältöä.

Kun WAP-päätelaitteeseen halutaan hakea sisältösivu, muodostaa päätelaite langattoman verkon yli yhteyden yhdyskäytäväpalvelimelle ja lähettää sille pyynnön sivusta. Palvelin tutkii pyyntöä ja selvittää, onko haettu sisältö WAP- vai WWW-muotoista. Mikäli asiakas pyytää WML-sivua, voidaan pyyntö lähettää sellaisenaan kohteena olevalle WAP-sisältöpalvelimelle. Palvelimelta tuleva vastaus palautetaan asiakkaalle. Jos asiakas on pyytänyt WWW-sivua, muuntaa yhdyskäytäväpalvelin pyynnön seittipalvelinten ymmärtämään HTML-muotoon. Kohteena olevan seittipalvelimen osoite selvitetään Internetin nimipalvelun avulla. HTML-pyyntö lähetetään saatuun osoitteeseen ja seittipalvelin palauttaa vastauksessaan halutun sisältökokonaisuuden. Yhdyskäytäväpalvelin muuntaa vastauksen takaisin WML-muotoon ja lähet-

tää sen edelleen WAP-päätelaitteeseen. Sama mekanismi toimii myös silloin, kun haun kohteena on esimerkiksi CGI-skripti.

Päätelaitteessa informaation ottaa vastaan sovellusagentti, joka on mikä tahansa tiettyä sisältötyyppiä tulkitseva ja näyttävä olio. Tyypillisessä WAP-laitteessa on ainakin WML- ja WMLScript-agentit, mahdollisia ovat myös esimerkiksi ääniselain- ja hakukoneagentit. Kuvassa 2.2 sovellusagentin tyyppiä ei ole määritelty, koska pyyntö-vastaus-pari eli transaktio etenee kaikkien sisältötyyppien kannalta samalla tavalla. [WAPF1999a]

Edellä kuvatuissa transaktioissa tapahtuvaa tietoliikennettä on mahdollista tehostaa. Langattomat verkot ovat viimeaikaisesta kehityksestä huolimatta hitaampia ja virhealttiimpia kuin kiinteät verkot, minkä vuoksi verkossa kulkevan informaation määrä tulisi minimoida. Tämä voidaan saavuttaa pakkaamalla päätelaitteen ja yhdyskäytäväpalvelimen välinen liikenne. Näin sekä informaation siirtoon kuluva aika että korruptoitumisen todennäköisyys minimoituvat. Toinen tehokeino on lisätä yhdyskäytäväpalvelimeen sivujen tallennuskapasiteettia (*caching*), jolloin usein pyydettyjä sivustoja ei tarvitse joka kerta erikseen hakea seittipalvelimilta. Näin säästyy sekä aikaa että verkon kapasiteettia.

WAP:n yhteensopivuus seittisivujen kanssa voidaan nostaa erittäin korkeaksi, koska on oikeastaan vain yhdyskäytäväpalvelimen toteutuksesta kiinni, miten hyvin seitistä saatava sisältö pystytään muuntamaan WAP-päätelaitteen ymmärtämään muotoon. Lähiaikojen suurimpiin haasteisiin kuuluu erityisesti multimediasisällön siirtäminen matkapuhelinten ulottuville.

#### **2.2.4 Protokollapino**

WAP-arkkitehtuuriin kohdistuvat vaatimukset ovat kovat. Yhteensovitettavuus olemassaolevien ja tulevien protokollien sekä verkkotekniikoiden kanssa lienee vaatimuksista kaikkein hankalin, sillä langattoman tietoliikenteen kehityssuuntia on vaikeata ennustaa. WAP-spesifikaatio yrittää ratkaista sille asetetut tavoitteet kuusikerroksisen protokollapinon avulla. Pino, joka voidaan nähdä kuvassa 2.3, pohjautuu TCP/IP-referenssimalliin, koska näin on helpompi saavuttaa yhteensopivuus Internetin kanssa [WAPF1998].



Kuva 2.3. WAP-protokollapino.

**Sovellusprotokolla (WAE).** Sovellusprotokolla sisältää WML-kuvauskielen ja WMLScript-komentosarjojen vaatiman toiminnallisuuden. Langattomia puhelinsovelluksia tuetaan WTAI-rajapinnalla<sup>3</sup>, joka tarjoaa pääsyn puhelu- ja verkkopalveluihin sekä sisältää muun muassa kuvien, tapahtumakäsittelyn ja kontakti- sekä kalenteritietojen esittämismuodot. Sovellusprotokollan lähin vastine TCP/IP-referenssimallissa on HTML lisättynä JavaScript:llä. [Held2001]

**Istuntoprotokolla (WSP).** Istuntoprotokolla huolehtii tehokkaasta informaation siirrosta asiakkaan ja palvelimen välillä. Yksi istunto muodostuu tyypillisesti useasta pyyntö-vastaus-parista. Protokolla tukee sekä yhteydellistä palvelua WTP-protokollan että yhteydetöntä palvelua WDP-protokollan kautta. Yhteydellisessä palvelussa yhteyden toiselta päältä odotetaan kuittauksia lähetettyyn informaatioon, kun taas yhteydetön palvelu tyytyy vain lähettämään informaation eteenpäin. TCP/IP-referenssimallissa istuntoprotokollaa vastaa HTTP<sup>4</sup>. [Held2001]

<sup>3</sup> Wireless Telephony Application Interface.

<sup>4</sup> HyperText Transfer Protocol. Seitissä käytettävä istuntoprotokolla [Tane1996].

**Transaktioprotokolla (WTP).** Transaktioprotokolla tarjoaa tarvittaessa ylemmille kerroksille luotettavan siirtopalvelun. Se sisältää transaktioiden numeroinnin, kuittaukset, pakettien kopioiden poiston ja uudelleenlähetykset. Transaktioprotokollaa voidaan käyttää joko WDP:n tai UDP<sup>5</sup>:n päällä. TCP/IP-referenssimallissa transaktioprotokollaa vastaa TCP<sup>6</sup>. [WAPF1999d]

**Turvallisuusprotokolla (WTLS).** Turvallisuusprotokollan käyttö on WAP-soveluksissa valinnaista. Tavallisessa seitin selailussa sitä ei yleensä hyödynnetä, mutta arvokkaampaa informaatiota käsitteleville sovelluksille sen käyttö on suositeltavaa. Protokolla tarjoaa salatun tekstin lähetyks- ja vastaanottopalvelun neljällä kryptograafisella operaatiolla, joita ovat digitaalinen allekirjoitus, tekstin ja tekstilohkon salaus sekä julkisen avaimen salaus. WTLS on siis varsin monipuolinen ja erilaisiin käyttötarkoituksiin sopiva tietoturvaprotokolla. TCP/IP-referenssimallissa protokollaa vastaa lähinnä SSL<sup>7</sup>. [Held2001]

**Kuljetusprotokolla (WDP).** Kuljetusprotokolla on WAP:n yhteensopivuuden kannalta eräs tärkeimmistä protokollista, koska sen tehtävä on suorittaa sovitus allaolevaan siirtomediaan. Protokolla jaetaan usein käsitteellisellä tasolla kahteen osaan: ytimeen ja joukkoon sovitusprotokollia. Ydinosa sisältää kaikille siirtomedioille yhteiset ominaisuudet, kun taas sovitusprotokollat ovat erilaisille siirtomedioille räätälöityjä. Kuljetusprotokollaa voidaan näin ollen pitää joukkona protokollia. WAP:ia tukevia siirtomedioita ovat esimerkiksi GSM-verkossa SMS:t (*Short Message Service*) eli tekstiviestit ja CSD:t (*Circuit Switched Data*) eli datapuhelut [WAPF1999b].

Kuljetusprotokolla käyttää porttinumeroita, kuten TCP, identifioimaan ylemmän tason palveluita ja sovelluksia. WAP Forum on rekisteröinyt tärkeimpiä porttinumeroita Internetin varattujen numeroiden joukkoon, joita hallinnoi IANA (*Internet Assigned Numbers Authority*) [Held2001].

---

<sup>5</sup> User Datagram Protocol. TCP/IP-referenssimallin yhteydetön siirtoprotokolla [Tane1996].

<sup>6</sup> Transmission Control Protocol. TCP/IP-referenssimallin yhteydellinen siirtoprotokolla [Tane1996].

<sup>7</sup> Secure Sockets Layer. Seitissä käytettävä salausprotokolla.

## 2.3 Tulevaisuus

WAP-tekniikka alkaa tänä päivänä olla vakiintunut ja hyväksihavaittu osa mobiili-maailmaa. Langattomien pakettiverkkojen yleistymisen myötä sen asema voisi vielä entisestäänkin parantua. Kilpailevat tekniikat ovat kuitenkin nouseva uhka WAP-protokollalle.

### 2.3.1 Kehitysnäkökohtia

Vaikka WAP on kypsynyt tekniikkana, se ei koskaan tule olemaan valmis. Protokolla yhdistää langattoman maailman Internetiin ja sen on siksi pysyteltävä mukana kummankin verkkoympäristön kehityksessä. Ympäristöjen kehityssuunnat eivät aina ole samanlaisia, joten WAP:n tehtävä ei tule olemaan helppo.

WAP-spesifikaation versio 1.2 esitteli mielenkiintoisen uuden toiminnallisuuden, sisällön työntämisen (*push*) palvelimelta päätelaitteelle. Työntäminen mahdollistaa täysin uudenlaisia käyttöskenaarioita, sillä päätelaitteen ei enää tarvitse olla transaktion aloitteentekijä. Toiminnallisuutta voidaan hyödyntää palvelimissa esimerkiksi saapuneesta sähköpostista tiedottamisen, uutispalveluiden ja mainonnan muodossa. Spesifikaatioversiota 1.2 hyödyntävät päätelaitteet ovat tulossa lähiaikoina markkinoille, joten jäämme mielenkiinnolla odottamaan niille räätälöityjä palveluita.

Internetissä saatavilla oleva sisältö tulee kaiken aikaa monipuolisemmaksi. Vaikka seitti oli alunperin puhtaasti hypermediaa välittävä kanava, tarjoaa se nykyään lisäksi muun muassa videokuvaa, musiikkia ja keskustelukanavia. WAP-päätelaitteissa tuettujen sisältömuotojen lisääminen on yksi tulevaisuuden kehitysnäkökohdistista. WAP Forumin työryhmät kehittelevätkin paraikaa spesifikaatioon multimediatukea. Apuna käytetään W3C:n (*World Wide Web Consortium*) multimedian hallintaan kehittämää SMIL-kuvauskieltä (*Synchronized Multimedia Integration Language*), joka yhdenmukaistaa sekä virtaavan että staattisen ääni-, video- ja animaatiosisällön käsittelemisen.

### 2.3.2 Kilpailijat

WAP-protokollan pahimpia kilpailijoita näyttävät tällä hetkellä olevan operaattorivoitot Internet-matkapuhelintekniikat veturinaan japanilaisyhtiö *NTT DoCoMo*:n lanseeraama *i-mode*. Ilmiö on voimakkaimmillaan juuri Japanissa, missä langatonta In-

ternet-palvelua tarjoaa kolme matkapuhelinoperaattoria. Palveluilla on yhteensä yli 20 miljoonaa käyttäjää, määrä kasvaa noin puolella miljoonalla joka viikko [Juho2000]. Järjestelmien laitteet kiinnittyvät Internetiin pakettikytkentäisen verkon kautta, joka on ollut Japanissa käytettävissä jo neljä vuotta. Päätelaitteet ovat tyypillisesti eurooppalaisia WAP-puhelimia sirompia ja värinäytöllä varustettuja. Joihinkin malleihin on integroitu jopa digitaalikamera ja MP3<sup>8</sup>-soitin. Suosituimpia palveluita ovat sähköposti, seitin selaus, pelit, soittoäänet, logot sekä uutis- ja pankkipalvelut. Lähitulevaisuudessa matkapuhelimella voi katsella myös televisiota, kun MPEG-4<sup>9</sup> -tekniikkaan perustuvaa videokuvaa ryhdytään jakamaan pakettiverkon kautta. NTT DoCoMo tulee avaamaan kesäkuussa 2001 i-moden seuraajan, FOMA-järjestelmän (*Freedom Of Mobile multimedia Access*). Järjestelmä perustuu kolmannen sukupolven matkapuhelinverkkoon ja se on yhteensopiva edeltäjänsä kanssa. Verkossa voidaan tarjota muun muassa 64 kbps videokuvaa sekä yhtäaikaista data- ja puheluyhteyttä.

Operaattoreilla on valmiuksia hankkia laadukkaita sisällöntuottajia tuotemerkkiensä taakse. Esimerkiksi NTT DoCoMo:lla on yli 600 virallista sisällöntuottajaa, joukossa amerikkalainen uutisyhtiö CNN. Epävirallisia sivuja on liitetty järjestelmään yli 23000, minkä lisäksi useimmat Internet-sivut ovat selailtavissa. [Juho2000]

Operaattorivetoiset matkapuhelintekniikat iskivät WAP:n arkaan paikkaan: kehityksenalaisten standardien pitkään kypsymisaikaan. Japani oli ilmiön syntymiselle erityisen otollinen paikka, koska pakettikytkentäinen, langaton verkko oli siellä jo käytössä. Euroopassa sen sijaan odotellaan edelleen tekniikaltaan vastaavien GPRS<sup>10</sup>-järjestelmien yleistymistä. WAP-palveluiden käyttö on nykyisellään esimerkiksi i-mode -palveluihin verrattuna varsin hidasta. Ero huomataan selvästi, jos vertailukohdaksi otetaan yhteydenmuodostus: WAP-palveluun kiinnittyminen kestää vähintään 10 sekuntia, kun taas i-mode -palvelu on käytettävissä parissa sekunnissa. I-mode:n nopeus selittyy sillä, että päätelaite on jatkuvasti yhteydessä pakettiverkkoon, jolloin palveluihin voidaan kirjautua erittäin nopeasti.

Yritysten kehittämien tekniikoiden skaalautuvuus maailmanlaajuiseen käyttöön jää nähtäväksi. NTT DoCoMo on lähiaikoina lanseeraamassa i-mode -tekniikkaansa sekä Eurooppaan että Yhdysvaltoihin, koska alueiden markkinoilla on selvä

---

<sup>8</sup> Digitaalinen, virtaava ääniformaatti. Perustuu MPEG-3 -standardiin, vrt. alla.

<sup>9</sup> Moving Picture Experts Group Layer 4. Videokuvan ja äänen pakkaukseen kehitetty standardi.

<sup>10</sup> General Packet Radio System. Pakettikytkentäinen, langaton tiedonsiirtoverkko.

rako yrityksen tuotteille. WAP on lähtökohtaisesti suunniteltu globaalisti yhteentoimivaksi, joten sitä voitaisiin pitää tässä suhteessa kilpailijoitaan parempana. Pakettikytkentäisten, langattomien verkkojen yleistyminen olisi kuitenkin välttämätöntä WAP:n kehittymiselle, koska piirikytkentäiset yhteydet eivät tarjoa yhtä joustavaa ja suorituskykyistä rajapintaa palveluiden toteuttajille. WAP-palveluiden kirjo on sinällään nykyisin jo varsin kattava, joskaan ei esimerkiksi i-moden veroinen. Laitevalmistajien tulisi panostaa myös päätelaitteiden kehitystyöhön, koska niiden käytettävyys on tätä nykyä valitettavan heikko.

WAP on teknisesti melkoisesti jäljessä yksityisellä sektorilla ideoituja kilpailijoitaan. Mikäli etumatkaa ei pystytä kuromaank pikaisesti umpeen, on vaarana pitkällisen kehitystyön joutuminen markkinavoimien painostuksessa romukoppaan.

### 3 Paikalliset WAP-palvelut

Paikalliset WAP-palvelut ovat pienelle alueelle, esimerkiksi huoneeseen tai kadunkulmaan, rajattuja WAP-palveluja. Niiden varaan voidaan kehittää täysin uudenlaisia palveluja, joissa käyttäjälle tarjotaan paikkasidonnaista, monimuotoista informaatiota ilmaiseksi.

#### 3.1 Paikallisuuden ongelma

Perinteiset WAP-palvelut on suunniteltu laajalle käyttäjäkunnalle hyödyllisen tiedon jakamiseen maailmanlaajuisesti. Niitä voivat käyttää kaikki palvelua tarjoavan matkapuhelinoperaattorin WAP-asiakkaat operaattorin hallinnoiman verkon alueella. Verkko voi olla käytettävissä yhdessä tai useammassa maassa. Palveluita käytetään siis hyvin erityyppisillä alueilla: kaupungeissa, maaseudulla, merellä, erämaassa ja niin edelleen. Käyttäjien informaatiotarpeet ovat myös täysin erilaisia: lähimmän pizzerian kertova WAP-palvelu voi olla kaupunkilaisnuorelle varsin hyödyllinen, kun taas Utsjoella asuvalle poroisännälle pelkkä kuriositeetti.

Paikallisen tiedon jakaminen on osoittautunut hankalaksi perinteisen WAP-palvelun kautta. Tämä on selkeä ongelma, koska käyttäjälle hyödyllinen informaatio on varsin usein luonteeltaan paikallista. Jotta tietoa lähiympäristöstä voitaisiin tarjota, täytyy käyttäjän sijainti olla tiedossa. Tarvitaan siis jokin mekanismi paikkatiedon välittämiseen.

Ensimmäinen vaihtoehto mekanismiksi on se, että käyttäjä kertoo itse olinpaikkansa palvelulle. Sen toimintaperiaate on kuitenkin myös sen ongelma: miten menetellä, jos käyttäjä on eksynyt, eikä tiedä sijaintiaan? Lisäksi käyttäjiä voi ärsyttää se, että joka kerta palvelua käyttäessään joutuu syöttämään olinpaikkansa esimerkiksi kaupunginosan tarkkuudella. Tämä vähentää merkittävästi palvelun käytettävyyttä.

Toinen vaihtoehto on jokin tekninen apuväline: maailmanlaajuiseen satelliittiverkkoon perustuva *GPS*<sup>11</sup>-paikannuslaite tai päätelaitteen käyttämän langattoman verkon oheistoimintona tarjottava paikannuspalvelu. GPS-laitteet antavat erittäin tarkkaa paikkatietoa, mutta ovat ainakin toistaiseksi suurimmaksi osin erillisiä, joten käyttäjien pitäisi kantaa niitä mukanaan varsinaisen päätelaitteen lisäksi. Tilanne

---

<sup>11</sup> Global Positioning System. Yhdysvaltain armeijan kehittämä paikannusjärjestelmä.



saattaa muuttua tulevaisuudessa, sillä päätelaitteisiin integroidut GPS-paikantimet ovat tulossa markkinoille. Langattoman verkon tarjoamat paikannuspalvelut ovat saatavissa ilman lisälaitteita, mutta ne ovat nykymuodossaan varsin epätarkkoja. Paikannustekniikoiden kehittämiseen käytetään kuitenkin paljon resursseja, joten tulevaisuudessa niiden voidaan olettaa parantuvan.

Vaikka paikannusongelma saataisiin ratkaistua, törmättäisiin välittömästi seuraavaan ongelmaan. Jotta operaattorin asiakkaita voitaisiin palvella tasapuolisesti, pitäisi kullakin asiakkaalla olla saatavillaan yhtäläinen paikallisinformaatio. Näin ollen pizzeria-palvelun tulisi osata kertoa sekä Helsingin että Utsjoen pizzeriat. Tämä taas johtaisi palvelun sisältämän informaatiomäärän räjähtävään kasvuun, koska järjestelmän tulisi taltioda kaikki informaatio tietystä aihepiiristä koko verkon alueelta. Informaatiota tulisi lisäksi voida hakea, päivittää ja hallinnoida tehokkaasti.

Paikallisen WAP-palvelun toteuttaminen perinteisen WAP-palvelun välineillä on siis melko hankalaa. Koska nykyisessä palvelukentässä on tilausta paikalliselle informaatiolle ja sitä jakavalle medialle, täytyy paikallisen WAP-palvelun problematiikkaa lähestyä toisesta suunnasta.

### **3.2 Ominaispiirteet**

Paikallinen WAP-palvelu ei ole tavallisen WAP-palvelun erikoistapaus, vaan arvokas lisä protokollamalliin. Paikallinen palvelu perustuu täsmälleen samaan arkkitehtuuriin kuin kantaisänsä, joten myös palvelun toteutus noudattaa samoja suuntaviivoja. Laskeuduttaessa kohti päätelaitteen ja yhdyskäytäväpalvelimen välistä fyysistä yhteyttä huomataan kuitenkin poikkeavia piirteitä, jotka muuttavat itse asiassa koko palvelun luonteen.

Paikallinen WAP-palvelu on paikallista informaatiota lyhyen kantaman langattomassa verkossa jakava, WAP-arkkitehtuuriin perustuva media. Palvelu on käytävissä rajoitetulla alueella, jonka koko on tyypillisesti muutamien kymmenien metrien luokkaa. Kantama ei kuitenkaan ole ongelma, sillä informaatio, jota palvelu tarjoaa, on luonteeltaan sellaista, että sillä on käyttöarvoa vain alueen sisäpuolella. Paikallisuuden ongelma, johon perinteinen WAP-palvelu ei nykyisellään pysty vastaamaan, ratkeaa nimenomaan rajoitetun käyttöalueen avulla: käyttäjä on potentiaalinen informaation hyödyntäjä, mikäli hän on alueen sisällä ja kykenee kytkeytymään palveluun.

Rajatun alueen ulkopuoliset käyttäjät eivät hyödy palvelun tarjoamasta paikallisesta informaatiosta, eivätkä pysty kytkeytymään palveluun.

Paikallinen palvelu on käytännössä tietokone, johon on asennettu sekä yhdyskäytävä- ja WAP-palvelinohjelmistot että tietoliikennelaitteet. Palvelu voi olla kiinteästi sijoitettu tai siirrettävä. Käytännössä tämä heijastuu vain laitteistoon, jolla palvelu tuotetaan: kannettavaan tietokoneeseen sijoitettu palvelu tehostaa siirrettävyyttä. Muut toteutusnäkökohdat pysyvät samoina. Kiinteästi sijoitettu palvelu sopii kohteeseen, jonka sijainti on kohtuullisen vakio. Siirrettävä palvelu taas on omiaan ympäristöön, jossa palvelun sisältö tai kohderyhmä muuttuvat usein. Tällöin myös palvelun päivitettävyys on tärkeä asia.

Paikallisen WAP-palvelun tulisi olla käytettävissä ilmaiseksi. Käyttäjien mielenkiinto tekniikkaa kohtaan voitaisiin maksimoida, jos kokeiluluontoiset palveluihin kiinnittymiset eivät aiheuttaisi kuluja. Mikäli palvelu haluttaisiin kuitenkin tarjota maksullisena, tulisi esittelysivun kertoa selkeästi käyttäjälle se, että käytön jatkaminen tullaan veloittamaan. Palveluun pitäisi näin ollen aina voida kiinnittyä ilmaiseksi, jotta käyttäjä voisi arvioida, haluaako hän maksaa sen käytöstä. Tärkeintä on nykyisin valitsevan WAP-laskutuksen välttäminen, koska se on tehnyt WAP:n käyttämisestä pienen ydinjoukon huvia.

WAP-spesifikaation versiosta 1.2 lähtien palvelimen on ollut mahdollista työntää sisältöä asiakkaalle ilman asiakkaan aloitetta. Tämä toiminnallisuus mahdollistaa sen, että paikallinen WAP-palvelu voi ilmoittaa olemassaolostaan asiakkaalle lähettämällä esimerkiksi lyhyen kuvauksen itsestään. Mainonta auttaa asiakkaita löytämään palvelut ympäristöstään, mutta sillä on myös varjopuoli: liiallinen mainosten käyttö saa aikaan asiakkaissa kielteisiä reaktioita. Asiakkaan pitää näin ollen pystyä kieltäytymään mainoksista jo etukäteen esimerkiksi asettamalla päätelaitteensa tiettyyn tilaan.

### **3.3 Käyttökohteet**

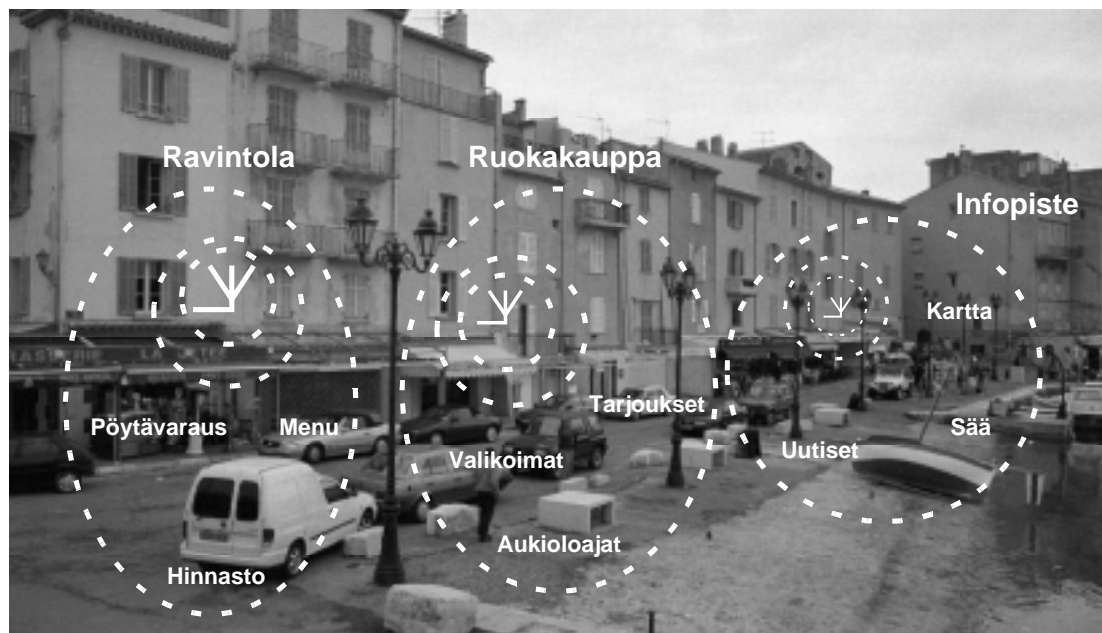
Paikallisille WAP-palveluille voidaan helposti löytää hyödyllisiä sovelluksia. Useimmat yritykset ja organisaatiot voisivat jollakin tasolla hyötyä paikallisista palveluista, joten sovellusten kirjo on oikeastaan riippuvainen vain kehittäjien mielikuvituksesta. Seuraavassa käydään läpi muutamia kuvitteellisia sovellusesimerkkejä, joiden perusteella paikallisissa WAP-palveluissa piilevät mahdollisuudet toivottavasti selviävät.

**Informaatiokioski.** Informaatiokioski on kaupunkimiljööseen sijoitettu informaatiopiste, joka tarjoaa tekstiä, karttoja, kuvia, ääniä ja videota lähialueiden palveluista ja nähtävyyksistä. Asiakkaan on myös mahdollista päästä selaamaan Internet-sivuja kioskin kautta. [BSIG1999]

**Elokuvateatterin esittelypiste.** Elokuvateatterin edustalla kulkeville ihmisille tarjotaan tietoa teatterissa sillä hetkellä esitettävistä elokuvista, aikatauluista ja hinnoista. Päätelaitteen ruudulle on mahdollista saada elokuvien esittelypätkiä. Asiakkaille voidaan myös tarjota erikoistarjouksia pikapuolin alkaviin näytäntöihin.

**Messupalvelu.** Yritys esittelee messuilla toimintaansa esittelypisteen ympärillä käytettävän paikallisen WAP-palvelun välityksellä. Kun toimitusjohtaja lähtee pitämään luentoa messuilla järjestettävään konferenssiin, hän ottaa paikallisen WAP-palvelimen sisältävän kannettavan tietokoneen mukaansa. Palvelu on luennon ajan kuulijoiden käytettävissä ja sen kautta voidaan esimerkiksi jakaa luentomateriaali.

Kuvassa 3.1 on hahmotelma siitä, miten paikalliset WAP-palvelut voisivat sijoittua katukuvaan. Kunkin palvelun yhteydessä on listattu informaatiotyyppettä, joita palvelu voisi tarjota.



*Kuva 3.1. Paikallisia WAP-palveluita katukuvassa.*

### 3.4 Vaatimukset verkkotekniikalle

WAP-spesifikaatio ei ota kantaa käytettävään verkkotekniikkaan, vaan määrittelee yhteensopivuuden joukolle langattomia kommunikaatiomenetelmiä. Yhteensopivuus uusien langattomien verkkotekniikoiden kanssa toteutetaan tavallisesti standardin aseman saavuttaneen TCP/IP-referenssimallin avulla. Verkkotekniikka toteuttaa protokollat fyysiseltä tasolta IP-protokollaan ja niiden päälle sijoitetaan WAP-pino. Langaton verkkotekniikka sopii siis WAP-sisällön kuljettamiseen, mikäli se mahdollistaa sovellusten kiinnittymisen IP-protokollaan.

Langattoman päätelaitteen toiminta on jatkuvaa tapahtumiin reagoimista: informaatiota saapuu ja lähtee, siirtoverkko katoaa ja tulee taas käytettäväksi, laitteen akun teho loppuu ja niin edelleen. Käytettävän verkkotekniikan on välitettävä WAP-pinolle informaatiota päätelaitteen ja sen ympäristön tapahtumista, jotta käyttäjää voidaan tiedottaa niistä sovellustasolla. Käyttäjän informoimisella on usein paljon suurempi kuin pelkkä kohteliaisuusmerkitys: käyttäjä voi helpottaa päätelaitetta kohdantunutta ongelmatilannetta. Jos laitteen ruudulla esimerkiksi ilmoitetaan verkon huonosta kattavuudesta, voi käyttäjä siirtää laitteen verkon kuuluvuuden kannalta parempaan paikkaan.

Laitteiden liikkuvuus kuuluu paikallisen WAP-palveluun luonteeseen. Allaolevalta verkkotekniikalta tarvitaan palvelu, joka osaa tarvittaessa kertoa muiden lähitöllä olevien WAP-laitteiden osoitteet ja tyypit. Palvelimelle ominaisuus on tärkeä työntöominaisuuden kannalta, koska vastaanottavan asiakaslaitteen osoite on oltava tiedossa. Asiakaslaite ei voi tarjota käyttäjälle dynaamisesti päivittyvää listaa käytettävistä WAP-palvelimista, ellei se saa jotenkin selville palvelimien osoitteita ja tekstuaalisia nimiä.

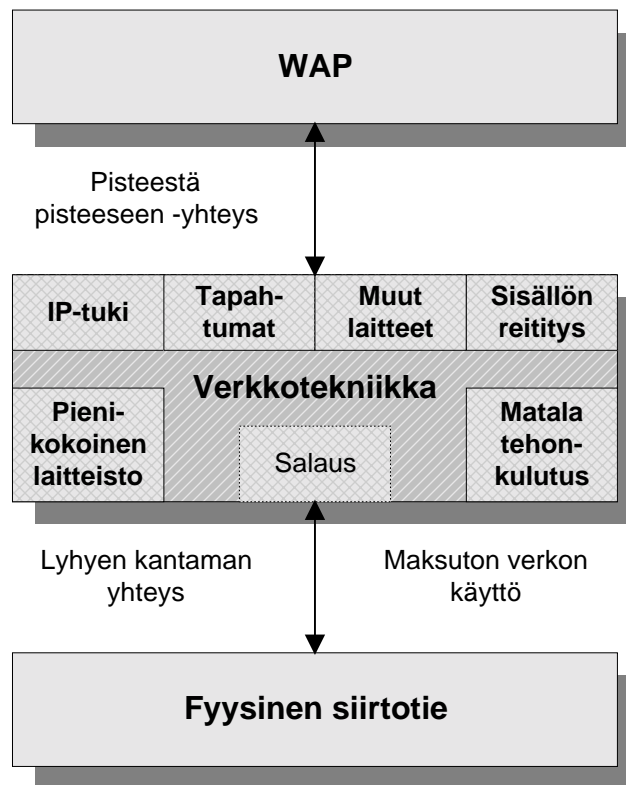
Jotta informaatiota voitaisiin siirtää WAP-päätelaitteiden välillä, tulee verkkotekniikan osata reitittää verkosta saapuva WAP-sisältö WAP-protokollien käsiteltäväksi. Informaatio siirtyy paikallisen palvelun siirtoverkossa tavallisesti IP-protokollan sisällä, joten verkkotekniikan on pystyttävä tutkimaan pakettiliikennettä oikean kohteen selvittämiseksi. Tämä ominaisuus on verkon päätelaitteelle erittäin tärkeä, sillä laitteeseen saapuu jatkuvasti myös sellaista informaatiota, joka ei kuulu WAP-järjestelmän piiriin.

Käytetyn verkkotekniikan tulisi mahdollistaa lyhyen kantaman yhteydet, jotta paikallisen WAP-palvelun määritelmä voidaan toteuttaa. Kantomatkan tulisi olla tyy-

pillisesti muutamia kymmeniä metrejä ja maksimissaan noin sata metriä. Mikäli yhteyksiä pystytään muodostamaan tätä kauemmas, syntyy ongelmia palvelun paikallisen luonteen säilyttämisessä. Liian lyhyt kantama aiheuttaa päinvastaisen ongelman, koska asiakkaiden kiinnittyminen palveluun hankaloituu.

Eräs tärkeimmistä verkkotekniikalle kohdistettavista vaatimuksista on riippumattomuus kolmansista osapuolista eli operaattoreista. Paikallisen palvelun luonteen kuuluu, ettei jokaisesta palvelun käyttökerrasta saa siirtyä rahaa operaattorin tilille. Seitin kaltaista avointa verkkokulttuuria ei voi syntyä mobiilimaailmaan, jos operaattoriosapuolet pääsevät hyötymään jokaisesta tehdystä transaktiosta. Kerran kuukaudessa perittävä vähäinen käyttömaksu on sen sijaan hyväksyttävä ratkaisu, mikäli käyttäjä todella tarvitsee palvelua useita kertoja päivässä. Edellä mainitun kaltainen järjestelmä on käytössä muun muassa i-mode -palveluissa.

Paikallista WAP-palvelua varten muodostettavat yhteydet ovat luonteeltaan pisteestä pisteeseen -yhteyksiä (*point-to-point*), joita verkkotekniikan tulee tukea. Asiakkaan ja palvelimen välillä on siis avoinna yksi tietoliikennekanava, jota osapuo-



Kuva 3.2. Verkkotekniikkaan kohdistuvat vaatimukset.

let käyttävät WAP-spesifikaatiossa määritellyllä tavalla. Yhteys voidaan tarvittaessa suojata, jolloin voidaan varmistua sekä yhteysosapuolten identiteeteistä että informaation yksityisyyden säilymisestä. Koska WAP-protokolla tarjoaa varsin monipuoliset salaustoiminnot, niitä ei vaadita verkkotekniikalta. Jos verkkotekniikka kuitenkin mahdollistaa riittävän tehokkaan salauksen, kannattaa sitä hyödyntää. Tällöin salaus voidaan suorittaa alempana protokollapinossa, mahdollisesti jopa laitteistotasolla, jolloin siitä aiheutuva viive minimoituu.

WAP-päätelaite on tyypillisesti pienikokoinen, kädessäpidettävä ja akkukäyttöinen. Käytetyn verkkotekniikan tulee olla edellä mainittuun päätelaitteeseen soveltuva: verkkoisännän tulee toimia vähän tehoa kuluttaen ja mahdollisten ulkoisten antennien tulee olla pienikokoisia. Vaikka laitteissa käytettävät akut ovat jatkuvasti kehittyneet, eivät niiden suorituskyky ja kestävyys ole silti sähköverkon veroisia. Ulkoiset antennit puolestaan vaikuttavat laitteen ulkonäköön ja käytettävyyteen, eivätkä käyttäjät ole valmiita vaihtamaan nykyisiä kämmentä pienempiä laitteitaan suurempiin ja kömpelömpiin vain uuden tekniikan vuoksi.

Verkkotekniikkaan kohdistuvat vaatimukset on koottu kuvaan 3.2. Kuvasta selviävät sekä WAP-protokollan verkkotekniikalta vaatimat palvelut että verkkotekniikan tarjoamat fyysisen siirtotien ominaisuudet. WAP:n vaatimat ominaisuudet on kerätty keskimmäiseen laatikkoon, WAP-yhteydelle asetettavat vaatimukset kahden ylimmän laatikon välille ja fyysiseen yhteyteen liittyvät asiat alimpien laatikoiden väliin. Salaustoiminnallisuutta ei verkkotekniikalta vaadita, minkä vuoksi ko. laatikko on rajattu katkoviivalla.

## 4 PAN-verkot

Lyhenteet LAN<sup>12</sup> ja WAN<sup>13</sup> lienevät kaikille tietoliikenteen perusteisiin perehtyneille tuttuja. PAN sen sijaan on alan nuorimpia tulokkaita, eikä sen merkitys ole läheskään kaikille selvä.

### 4.1 Määritelmä

PAN (*Personal Area Networking*) –verkot ovat henkilökohtaisia tiedonsiirtotarpeita varten mukautuvia tietoliikenneverkkoja. Henkilökohtaisilla tarpeilla tarkoitetaan sellaisten päätelaitteiden käyttöä, joilla siirretään ja muunnetaan käyttäjälle tärkeää informaatiota. Henkilökohtaiset verkot muodostuvat automaattisesti tällaisten laitteiden välille ja purkautuvat, kun tiedonsiirto on suoritettu.

PAN-verkot liittyvät käsitteenä langattomiin verkkoihin, koska yhteyksien automaattisesta avautumisesta ei ole mielekästä puhua kaapeloiduissa järjestelmissä. Tällöin yhteyksien spontaaniin muodostumiseen tarvitaan käyttäjän apua kaapeleiden asentamisen muodossa. PAN-verkkojen tyypillisiä käyttöskenaarioita ovat esimerkiksi tiedostojen siirto laitteiden välillä, tulostaminen, kahden eri laitteen sisältämän informaation synkronointi, ääni- tai videovirran siirtäminen laitteelta toiselle sekä tiedostojen ryhmässä tapahtuva muokkaus [Comp2000].

### 4.2 Ominaisuudet

PAN-verkkoja ei ole tarkoitettu kilpailemaan muiden verkkojen kanssa suorituskyvyssä tai laajuudessa. Ne on sen sijaan suunniteltu palvelemaan käyttäjää mahdollisimman huomaamattomasti jokapäiväisissä tehtävissä, joihin ei liity suurten tietomassojen siirtoa. Verkkojen käytettävyyden kannalta on tärkeää, että mahdollisimman monet laitteet tukevat PAN-tekniikkaa. Näin on mahdollista luoda kehittyneitä sovelluksia, jotka hyödyntävät kaikkien saatavilla olevien laitteiden tarjoamia resursseja. Tässä mielessä järjestelmä sisältää läsnä-älyllisiä (*ubiquitous computing*) piirteitä, koska

---

<sup>12</sup> Local Area Network. Paikallisverkko [Tane1996].

<sup>13</sup> Wide Area Network. Laajan alueen verkko, joka yhdistää paikallisverkkoja [Tane1996].

osa järjestelmän operaatioista tapahtuu täysin käyttäjän tietämättä, ikäänkuin läsnäolevan tekoälyn toimesta.

PAN-verkon toiminta kulminoituu liikkuvien laitteiden ja palveluiden ympärille. Päätelaitte vastaanottaa jatkuvasti ympäriltään kuuluvaa tietoliikennettä ja yrittää päätellä, onko muita, vastaavia laitteita saapunut lähistölle. Laite lähettää aika-ajoin oman identiteettinsä verkkoon siltä varalta, että jokin toinen laite pystyisi sen kuulemaan. Kun toinen päätelaite saapuu ensimmäisen läheisyyteen, tunnistavat laitteet lyhyen ajan kuluessa toisensa identiteettiviestien perusteella. Laitteet avaavat välilleen yhteyden ja kertovat toisilleen ominaisuutensa, kuten laitetyypin, tunnisteiden ja selväkielisen nimen. Tämän jälkeen yhteys suljetaan ja päätelaitteet alkavat jälleen seurata verkossa kuuluvaa tietoliikennettä. Ne pysyttelevät jatkuvasti tietoisena siitä, mitä muita laitteita on niiden lähellä ja siten käytettävissä, mikäli tarvetta ilmenee.

Verkon muodostamista vaativat tehtävät syntyvät tavallisesti käyttäjän aloitteesta. Kun sovellustasolta saapuu pyyntö yhteyden muodostamisesta tietyn tyyppiseen palveluun, alkaa PAN-verkon rakennustyö. Laitteet neuvottelevat keskenään ja mikäli tarvittavat resurssit ovat kantaman sisällä olemassa, muodostuu laitteiden välille verkko. Tehtävää aletaan suorittaa ja sitä jatketaan niin pitkälle kuin mahdollista. Mikäli jokin resurssi kuitenkin katoaa kesken suorituksen, jää tehtävä odottamaan keskenräisenä sellaista verkkokonfiguraatiota, jolla tehtävä voidaan viedä loppuun. Oletetaan esimerkkitilanne, jossa käyttäjä haluaa lähettää sähköpostia kannettavalla tietokoneella ja matkapuhelimella. Laitteet muodostavat välilleen PAN-verkon. Alueella ei kuitenkaan satu olemaan matkapuhelinverkon peittoa, joten matkapuhelin ilmoittaa tietokoneelle kyvyttömyydestä suorittaa tiedonsiirto. Pyyntö sähköpostin lähettämisestä jää siis odottamaan ja PAN-verkko puretaan. Tehtävän suorittaminen jatkuu, kun matkapuhelin seuraavan kerran löytää signaalipeiton. Se ilmoittaa kannettavalle tietokoneelle muuttuneista olosuhteista ja saa aikaan PAN-verkon muodostumisen. Sähköpostit lähetetään kannettavalta tietokoneelta matkapuhelimelle ja sieltä edelleen Internetiin. PAN-verkko purkautuu tehtävän suorituksen jälkeen.

PAN-verkko sopii hyvin paikallisen WAP-palvelun verkkotekniikaksi. Päätelaitteiden liikkuvuutta ja verkon dynaamista konfiguroituvuutta tuetaan PAN-konseptissa monipuolisesti, joten paikallisen palvelun toteuttaminen on täysin mahdollista. PAN-verkon kantama on henkilökohtaiseen tiedonsiirtoon sopiva eli luokkaa kymmenen metriä. Tämä kantama sopii erinomaisesti paikallisen informaation jakamiseen, koska asiakkaan ja palvelimen välinen etäisyys on todella fyysisestikin lyhyt. Monet



paikallisen WAP-tekniikan asettamista vaatimuksista ovat kuitenkin hyvin toteutus-spesifisiä, joten tarkempaa soveltuvuusanalyysiä varten on valittava jokin PAN-ideo-logian toteuttava verkkotekniikka.

### 4.3 Liittymät

PAN-verkoissa suoritettavat tehtävät ovat luonteeltaan hyvin erilaisia. Ne vaihtelevat yksinkertaisista tiedostonsiirroista virtaavan datan välittämiseen. Verkon on pystyttävä tukemaan protokollatasolla kaikkia operaatioita, sekä nykyisiä että kehitteillä olevia. Yksittäisten sovellusprotokollien suora tukeminen ei näin ollen ole järkevä ratkaisu, koska sovellusmaailman kiihkeän etenemisen seuraaminen veisi resurssit kaikelta muulta kehitystyöltä. On sen sijaan parempi ratkaisu tarjota sovelluksille yhteinen kiinnittymisrajapinta verkkoon.

IP-protokollaa käytetään PAN-verkoissa sovelluksien yhteisenä protokollarajapintana, minkä vuoksi usein käytetään termiä “yleisluontoinen IP-verkottuminen” (*general IP networking*) [Comp2000]. Protokolla on tähän tarkoitukseen erinomainen, koska se on laajasti käytetty, standardoitu ja suorituskykyinen. Nykyisissä verkoissa toimivat sovellukset hyödyntävät protokollaa tavallisesti oletuksena, joten niitä ei tarvitse tältä osin muokata. IP-protokollan käytön kautta myös liittytäraajapinta Internetiin syntyy luonnollisesti, koska maailmanverkko kommunikoi protokollan avulla. IP-verkottumisessa on kuitenkin vielä PAN-verkkojen erityispiirteisiin liittyviä ongelmia, kuten reititys, nimipalvelun toteutus ja osoitteistus [MiBi2001].

WAP-sisällön kuljettaminen onnistuu PAN-verkossa IP-protokollatuen avulla. WAP-pinolle on lisäksi toimitettava informaatiota verkkoympäristön tilasta, jotta sovellukset voivat mukautua muiden asiakas- ja palvelinlaitteiden liikkumiseen. PAN-verkon WAP-yhteensopivuuden voidaan ajatella olevan kaksiosainen: PAN-verkko toimii joko siltana päätelaitteen ja langattoman siirtoverkon välillä tai varsinaisena siirtomediana. Ensimmäisessä vaihtoehdossa päätelaitteella voidaan käyttää kaikkia langattoman siirtoverkon WAP-palveluja. PAN-verkko on vain näkymätön osa siirto-kehittäjää, jonka avulla WAP-sisältö kuljetetaan yhteyden viimeisten metrien yli. Palveluita voidaan siis tarjota myös sellaisiin laitteisiin, jotka eivät luontaisesti tue WAP-protokollaa kuljettavia tekniikoita. Jälkimmäisessä vaihtoehdossa syntyy paikallinen WAP-palvelu. Tällöin vain ne palvelut, jotka ovat tarjolla PAN-verkon päälle rakennettavassa WAP-ympäristössä, ovat käytettävissä.

## 5 PAN ja langattomat verkkotekniikat

Langattomia lähikommunikaatiotekniikoita on kehitetty parinkymmenen vuoden ajan. PAN-konsepti on sen sijaan esitelty vasta hiljattain, joten ei ole lainkaan selvää, soveltuvatko markkinoilla olevat verkkotekniikat konseptin toteuttamiseen.

### 5.1 Bluetooth

Bluetooth on ollut viime aikoina ajankohtainen aihe tietotekniikkapiireissä. Tämä lyhyen kantaman radiotaajuustekniikka on viety spesifointivaiheen läpi ennätysvauhtia. Ensimmäiset tekniikkaa hyödyntävät laitteet ovat tulossa markkinoille kuluvan vuoden aikana.

#### 5.1.1 Taustaa

Ruotsalainen matkapuhelinvalmistaja *Ericsson* aloitti vuonna 1994 projektin, jossa tutkittiin heikkoa lähetystehoja käyttävän, toteutukseltaan edullisen radiotaajuustekniikan hyödyntämistä kaapeleiden korvaajana matkapuhelinten ja niiden lisälaitteiden välillä. Projektin edetessä Ericssonilla alettiin ymmärtää vaatimattomista tavoitteista syntyneessä ideassa piilevä potentiaali. Asiaa ajamaan perustettiin toukokuussa 1998 teollisuuden edustajista koottu ryhmä, Bluetooth SIG (*Special Interest Group*), johon lähtivät mukaan Ericssonin lisäksi *Intel*, *IBM*, *Nokia* ja *Toshiba*. Perustajajäseniä alettiin kutsua edistäjiksi (*promoters*). Kuten jo WAP-protokollaa esiteltäessä todettiin, yksittäisten yhtiöiden kehittämät ratkaisut saavuttavat vain harvoin maailmanlaajuisesti merkittävän aseman. Keskitetyn, avoimen keskustelufoorumin menestymismahdollisuudet ovat sen sijaan paljon paremmat. SIG:n jäsenmäärä jätettiin tietoisesti pieneksi, jotta ryhmän työskentelytehokkuus ja dynamiikka olisivat mahdollimman hyviä. SIG halusi välttää esimerkiksi WAP-tekniikkaa kohdanneen tilanteen, jossa lupaava, innovatiivinen idea menettää kiinnostavuuttaan kehitysprosessin pitkittyessä. [MiBi2001]

Bluetooth-nimi herätti alusta alkaen paljon kysymyksiä, koska se ei noudattanut tietoliikennetekniikassa vallalla olevaa, kolmikirjaimisia lyhenteitä ihannoivaa nimeämiskäytäntöä. Bluetooth nimettiin poikkeuksellisesti 900-luvulla eläneen tanskalaiskuninkaan, *Harald Blåtandin*, mukaan. Historiankirjat kertovat kuninkaan yhdistä-

neen Tanskan ja Norjan sekä tuoneen kristinuskon Skandinaviaan. Tekniikan kehittäjille näitä faktoja tärkeämpi tekijä lienee kuitenkin ollut se, että nimi viittaa selkeästi skandinaavisiin juuriin.

SIG:in pyrkivien yhtiöiden ja organisaatioiden määrä kasvoi voimakkaasti Bluetooth-spesifikaation edistyessä ja tekniikan tullessa tunnetummaksi. SIG:n alaisuuteen perustettiin pyrkijöitä varten erityinen ryhmä: käyttöönottajat (*adopters*). Ydinryhmä haluttiin pitää ennallaan, jottei spesifikaation kehitystyö vaarantuisi, mutta ulkopuolisia ei myöskään haluttu torjua. Tällä hetkellä käyttöönottajia on yli 2100 [BSIG2001]. Joulukuussa 1999 tapahtui muutoksia myös edistäjäryhmässä, kun suur-yhtiöt *3Com*, *Lucent*, *Microsoft* ja *Motorola* liittyivät mukaan [MiBi2001].

Bluetooth-spesifikaation ensimmäinen versio 1.0a julkaistiin heinäkuussa 1999, vain noin puolentoista vuoden kehittelyn jälkeen. Yli 1500 sivua pitkä spesifikaatio jakaantui kahteen osaan: tekniikan ydinosaan ja soveltaviin profiileihin. Laajennettu versio 1.0b valmistui joulukuussa 1999. Helmikuussa 2001 julkaistiin spesifikaation uusi alaversio 1.1. Version 2.0 odotetaan valmistuvan vuoden 2001 loppuun mennessä.

Bluetoothin kehittäminen on jaettu eri osa-alueisiin keskittyvien työryhmien vastuulle. Työryhmien vastuualueita ovat esimerkiksi ilmarajapinnan kehittäminen, protokollapinon spesifiointi, yhteentoimivuuden edistäminen, testausten suorittaminen, lakiasioiden hoito ja tekniikan markkinointi. Eräät edellä mainituista työryhmistä, esimerkiksi protokollapinon kehittäjät, on jaettu edelleen pienempiin osiin. Bluetooth-kehitystyötä valvoo ja koordinoi kokonaisuudessaan komissio, johon kuuluu jäseniä kustakin edistäjäyhtiöstä.

### **5.1.2 Tiedonsiirtomenetelmä**

Bluetooth on lyhyen kantaman langaton kommunikaatiotekniikka. Sekä langattomuus että lyhyt kantama juontavat juurensa tekniikan alkuperäisestä tehtävästä: kaapeleiden korvaamisesta. Tarkoituksena oli helpottaa modernia tietotekniikkaa käyttävien ihmisten elämää korvaamalla yksittäisiä käyttökohteita varten räätälöidyt kaapelit yleiskäyttöisellä langattomalla ratkaisulla. Vaikkei kaikkia Bluetooth-sovelluksia välttämättä pystytä pakottamaan kaapelinkorvaajan muottiin, on periaate kuitenkin nähtävissä hyvin fundamentaalisenä tekniikan spesifikaatiossa.

Langattomuus saavutetaan käyttämällä tiedon siirtämiseen radioaaltoja. Radiotekniikka on tieteenalana melko vanha, sillä *Marconin lennättimen* keksimisestä on kulunut jo yli 100 vuotta. Vaikka radioaaltoja on hyödynnetty jo vuosikymmeniä analogisten, sekä valtakunnallisten että paikallisten radio- ja televisio-ohjelmien jakeluun, lyhyen kantaman digitaaliseen kommunikaatioon niitä on sovellettu vasta muutamia vuosia. Tekniikoiden taustalla ovat kuitenkin täsmälleen samat fysikaaliset ilmiöt.

Valtiolliset elimet kontrolloivat kaikkialla maailmassa radioaaltojen käyttöä. Radiotaajuudet on jaettu alueisiin, joita käytetään eri tarkoituksiin: radio- ja televisio-ohjelmien jakamiseen, matka- ja satelliittipuhelinjärjestelmiin, kaapelitelevisioon ja niin edelleen [Held2001]. Useimmat valtiot ovat hyväksyneet sopimuksen, jossa radiotaajuusalue 2400-2483,5 MHz vapautetaan yleiseen käyttöön. Tätä lisenssivapaata taajuusaluetta eli kaistaa kutsutaan nimellä ISM (*Industrial, Scientific, Medical*) alueen pääasiallisten käyttökohteiden mukaan. Bluetooth-tekniikka hyödyntää kyseistä kaistaa, mutta yksinoikeutta sillä ei valitettavasti ole: eräät toiset langattomat lähikommunikaatiomenetelmät, kuten WLAN, sekä mikroaaltouunit toimivat samalla taajuusalueella. Häiriönsietokyky muodostuuakin erittäin tärkeäksi asiaksi Bluetooth-laitteissa. Käytettävissä oleva kaista, leveydeltään 83,5 MHz, jaetaan yhden megahertsin kokosiin kanaviin, joita on tyypillisesti 79 kappaletta. Eräissä maissa, kuten Espanjassa ja Ranskassa, ISM-taajuusalue ei ole kokonaan käytössä, joten kanaviakin on vain 23.

Bluetooth-laitteiden häiriönsietokykyä yritetään tehostaa käyttämällä hajasppektritekniikkaa (*spread spectrum*). Tekniikalla tarkoitetaan lähetyksen menetelmää, jossa informaatio hajautetaan koko käytettävän radiokaistan alueelle taajuuden, ajan, koodausalgoritmin tai jonkin muun menetelmän perusteella. Kapeakaistaiseen lähe-tykseen verrattuna hajasppektritekniikka tuhlaa taajuuskaistaa, mutta parantaa luotetta- vuutta, informaation eheyttä ja turvallisuutta. Bluetoothissa käytettävä hajasppektritek- niikka hajauttaa lähetettävät informaatiopaketit taajuuden perusteella, eli jokainen pa- ketti lähetetään eri kanavalla. Kanavaa vaihdetaan 1600 kertaa sekunnissa. Sekä pake- tin lähettäjän että vastaanottajan tulee olla selvillä käytetystä taajuussekvenssistä, jon- ka mukaan kommunikaatio suoritetaan. Koska tekniikka edellyttää jatkuvaa lähetyk- ja vastaanottotaajuuden vaihtamista, kutsutaan sitä taajuushyppely-hajasppektritekni- kaksi (*Frequency Hopping Spread Spectrum, FHSS*). [MiBi2001]

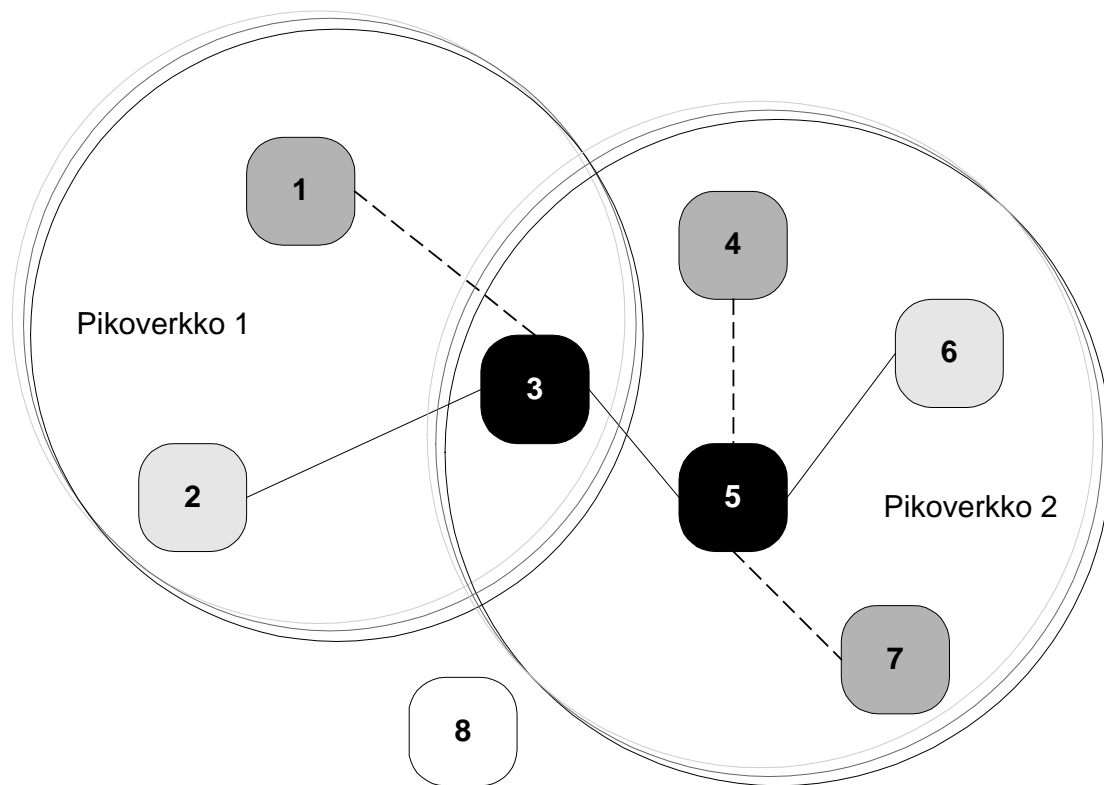
Taajuushyppelytekniikka parantaa häiriönsietoa ja tietyissä olosuhteissa myös tietoturvallisuutta. Mikäli jossakin osassa Bluetoothin käyttämää taajuuspektriä on

muuta radioliikennettä, esimerkiksi langattomasta kotipuhelimesta, voi osa lähetettävästä informaatiosta tärveltyä. Pilalle menneiden pakettien määrä on kuitenkin vähäinen verrattuna pakettien kokonaismäärään, koska informaatio lähetetään toisistaan etäällä olevilla taajuuksilla. Tärveltyneet paketit lähetetään uudelleen toisilla taajuuksilla, joihin häiriöt eivät todennäköisesti ulotu. Taajuuskaistalla olevasta liikenne-ruuhkasta voi olla myös hyötyä. Taajuushyppely on nimittäin melko tehokas salausmekanismi ruuhkaisessa kanavassa [MiBi2001]. Jotta salakuuntelija saisi kaapattua lähetetyn informaation, tulee hänen olla perillä käytetystä hyppysekvenssistä. Sekvenssiä eli yksittäisen yhteyden taajuuspiikkejä on kuitenkin lähes mahdotonta selvittää taajuuskaistasta, jota monet erilliset radiolähteet käyttävät. Mikäli taajuuskaistalla on sen sijaan vain vähän muuta liikennettä, on sekvenssi periaatteessa mahdollista selvittää. Tietoliikenteen salausta ei siis voida perustaa pelkän taajuushyppelytekniikan varaan, mutta sopivissa olosuhteissa siitä on apua.

### 5.1.3 Kommunikaatiomalli

Bluetooth-kommunikaation keskeisin elementti on pikoverkko (*piconet*). Pikoverkko muodostuu vähintään kahdesta päätelaitteesta, joista yksi on isäntä (*master*), muut renkejä (*slave*). Verkon isäntä on tavallisesti se päätelaite, joka tekee aloitteen verkossa tapahtuvasta kommunikoinnista. Renkien määrä on rajoittamaton, mutta vain seitsemän voi olla yhtäaikaan aktiivisena eli osallisena verkossa tapahtuvaan tietoliikenteeseen. Yhteydet muodostuvat pikoverkossa aina isännän ja rengin, eivät kahden rengin välille. Useimmat Bluetooth-päätelaitteet ovat kykeneviä toimimaan sekä isäntänä että renkinä.

Mikäli kahden tai useamman pikoverkon kantoalueet menevät limittäin, voi yhden pikoverkon jäsen kuulua myös toisiin pikoverkkoihin. Bluetooth-verkon käsite laajenee siis kattamaan myös pikoverkoista muodostuvan verkon, hajaverkon (*scatternet*). On kuitenkin ymmärrettävä, ettei hajaverkottumista voida käyttää pikoverkosta toiseen tapahtuvaan kommunikaatioon, koska verkkojen välillä ei tapahdu minkäänlaista reititystä. Kyse on pohjimmillaan siitä, että pikoverkon jäsen, isäntä tai renki, voi keskustella toisten pikoverkkojen isäntien kanssa. Rajoitteena hajaverkkojen rakenteelle on se, että päätelaite voi toimia kerrallaan vain yhden pikoverkon isäntänä. Yhden pikoverkon isäntä, samoin kuin renki, voi sen sijaan olla renkinä toisissa



*Kuva 5.1. Esimerkki kahden pikoverkon muodostamasta hajaverkosta.*

pikoverkoissa. Kuvassa 5.1 nähdään esimerkki hajaverkosta, joka muodostuu kahdesta pikoverkosta. Pikoverkkojen isännät on merkitty mustalla, aktiiviset renkit vaaleanharmaalla, passiiviset renkit tummanharmaalla ja hajaverkkoon kuulumattomat laitteet valkoisella värillä. Aktiiviset yhteydet on piirretty yhtenäisellä ja synkronointiyhteydet katkoviivalla. Laite 5 on pikoverkon 2 isäntä. Laitteet 2 ja 6 ovat aktiivisia renkejä ja niillä on aktiiviset yhteydet pikoverkkojen isäntiin, laitteisiin 3 ja 5. Laitteet 1, 4 ja 7 ovat passiivisia renkejä ja ne pysyvät synkronoituna pikoverkkojen isäntien kanssa. Laite 8 on valmiustilassa, koska se ei kuulu kumpaankaan verkkoon, vaikka se on verkon kantaman sisäpuolella. Laite 3 yhdistää pikoverkot hajaverkoksi: se on pikoverkon 1 isäntä ja pikoverkon 2 aktiivinen renki.

Isännän rooli on merkittävä vain tasolla, jolla hallinnoidaan yhteyksiä. Ylempien kerrosten kannalta on tavallisesti yhdentekevää, mikä on päätelaitteen rooli pikoverkossa. Poikkeuksiakin löytyy, joten roolia voidaan tarvittaessa tiedustella ja vaihtaa. Isäntä ohjaa pikoverkon toimintaa kolmessa suhteessa: se määrää käytetyn hyppeilysekvenssin ja hyppyjen tapahtumishetken sekä ohjaa renkien kommunikointia. Hyp-

pelysekvenssi määritetään tietyn algoritmin perusteella isäntälaitteen Bluetooth-osoitteesta, joka on jokaiselle Bluetooth-laitteelle annettu uniikki 48-bittinen luku. Algoritmi on suunniteltu niin, että saman hyppelysekvenssin syntyminen kahdelle eri isännälle olisi äärimmäisen epätodennäköistä. Kaikki pikoverkon rengit synkronoituvat isäntälaitteen kelloon, jotta ne pystyvät vaihtamaan taajuuksia samaan tahtiin. Isäntä ohjaa renkien kommunikointia antamalla kullekin rengille vuorollaan oikeuden lähettää informaatiota. Menetelmä perustuu kaksisuuntaiseen aikajakoperiaatteeseen (*Time Division Duplex, TDD*). Isäntänä toimivaa päätelaitetta voidaan myös vaihtaa verkon toimiessa, kuten aiemmin mainittiin. Tällöin jokin verkossa aktiivisena oleva renki ottaa hoitaakseen isännän roolin ja entisestä isännästä tulee renki.

Yhteyksien muodostamisen mekanismi luo leimansa koko Bluetooth-spesifikaation luonteelle. Konseptia suunniteltaessa yhtenä tärkeimmistä päämääristä oli yhteyksien muodostumisen *ad hoc* –luonne eli se, että laitteet muodostavat tarpeen vaatiessa itsenäisesti verkkoja. Kyseisen operaation suorittaminen radiorajapinnan yli on erittäin monimutkainen tehtävä, mutta huolellisella suunnittelulla järjestelmästä on saatu toimiva ja joustava. Laitteiden ja palveluiden löytäminen on olennaisin osa yhteydenmuodostusta. Bluetooth-päätelaite lähettää säännöllisesti ympärilleen hakuviestejä, joihin ympärillä olevat päätelaitteet vastaavat. Ne kertovat muun muassa oman Bluetooth-osoitteensa, nimensä ja tyyppinsä. Saadun informaation perusteella voidaan avata yhteys laitteen sisältämien palveluiden löytämistä varten. Kun palveluiden yksityiskohtaiset ominaisuudet ovat selvillä, voidaan varsinainen palvelua käyttävä tiedonsiirtoyhteys avata. Käyttäjän ei siis tarvitse tietää mitään erityistä informaatiota laitteesta, johon halutaan avata yhteys. Riittää, että hän pystyy identifioimaan kohdepalvelun omalle päätelaitteelleen esimerkiksi selväkielisen kuvauksen perusteella (esimerkiksi "*Teron työhuoneen tulostin*").

Bluetooth-järjestelmässä on periaatteessa mahdollista avata yhteyksiä minkä tahansa kahden laitteen välille. Rajoittamaton yhdistettävyyden ei kuitenkaan ole toivottavaa, koska käyttäjä saattaa olla haluton jakamaan laitteen resursseja kenelle tahansa. Näin saattaa olla esimerkiksi silloin, kun käyttäjän päätelaite sisältää salaista tai yksityistä materiaalia. Tarvitaan siis mekanismi, jolla käyttäjä voi kontrolloida Bluetooth-järjestelmän yhteydenmuodostus- ja turvaominaisuuksia. Päätelaitteelle määritetään löydettävyyden-, yhdistettävyyden-, parituvuuden-, sitoutuvuuden- ja turvallisuusominaisuudet, joiden perusteella voidaan kontrolloida tarkasti laitteen toimintaa toisten laitteiden lä-

hettyvillä. Taulukossa 5.1 esitellään tarkemmin ominaisuudet ja niille määritetyt arvot.

Taulukko 5.1. Päätelaitteen pääsyominaisuudet.

Ominaisuus	Kuvaus	Arvot	Kuvaus
Löydettävyys (discoverability)	Pystyvätkö muut laitteet löytämään tämän laitteen?	Yleisesti Rajoitetusti Ei	Kaikki laitteet pystyvät löytämään tämän laitteen. Erityisasemassa olevat laitteet pystyvät löytämään tämän laitteen. Mitkään laitteet eivät pysty löytämään tätä laitetta.
Yhdistettävyys (connectability)	Pystyvätkö muut laitteet avaamaan yhteyden tähän laitteeseen?	Kyllä Ei	Muut laitteet pystyvät avaamaan yhteyden tähän laitteeseen. Muut laitteet eivät pysty avaamaan yhteyttä tähän laitteeseen.
Pariutuvuus (pairing)	Pystyvätkö muut laitteet autentikoitumaan tämän laitteen kanssa?	Kyllä Ei	Muut laitteet pystyvät autentikoitumaan tämän laitteen kanssa. Muut laitteet eivät pysty autentikoitumaan tämän laitteen kanssa.
Sitoutuvuus (bonding)	Sallitaanko yhteysavaimen luominen ja tallentaminen pariutuneiden laitteiden välille?	Yleinen Erityinen	Voidaan muodostaa sovellustason yhteysavain. Voidaan muodostaa yhteystason yhteysavain.
Turvallisuus (security)	Millainen turvamuuri on käytössä laitteiden välillä?	1 2 3	Ei turvamuuria. Sovellustason turvamuuri. Yhteystason turvamuuri.

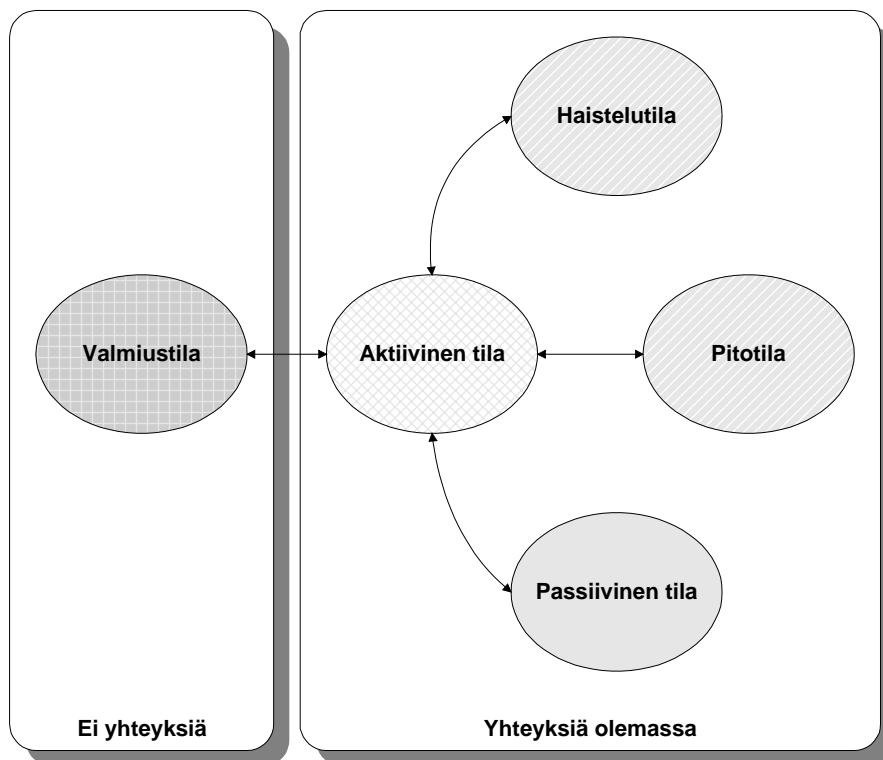
Pikoverkon luonne on varsin dynaaminen, koska renkien määrä ja tilat voivat muuttua verkon toimiessa. Kuten aiemmin mainittiin, pikoverkon renkien määrä on rajoittamaton, mutta aktiivisena voi olla kerrallaan vain seitsemän renkiä. Yli jäävät renkit ovat passiivisessa tilassa (*parked mode*), jolloin ne eivät osallistu verkossa tapahtuvaan kommunikaatioon. Passiivisille rengeille on varattu 255 kiinteää tunnustetta. Renkejä voidaan kutsua myös suoraan niiden omalla Bluetooth-osoitteella, joten tunnisteiden määrä ei rajoita passiivisessa tilassa olevien renkien määrää. Pito- (*hold mode*) ja haistelutilat (*sniff mode*) sijoittuvat aktiivisen ja passiivisen tilan väliin. Viimeksi mainituissa tiloissa olevat renkit luetaan kuitenkin pikoverkon aktiivisiin jäseniin. Erityisen tärkeää on huomata, että sekä aktiiviset että ei-aktiiviset tilat liittyvät aina yhteyteen isännän ja renkin välillä. Mikäli päätelaite ei ole yhteydessä mihinkään toiseen laitteeseen, se on valmiustilassa (*standby*). Ei-aktiivisten tilojen tarkoitus on verkon koon ja toiminnan mukauttamisen lisäksi virransäästö. Päätelaitte



keskustelee näissä tiloissa verkon kanssa huomattavasti aktiivista tilaa vähemmän, joten lähetin-vastaanotin voidaan pitää osan ajasta suljettuna. Siirtyminen aktiivisesta tilasta ei-aktiiviseen tilaan tai päinvastoin voi tapahtua joko päätelaitteen itsensä pyynnöstä tai isännän käskystä. Isäntä ei voi koskaan olla ei-aktiivisessa tilassa. Kuvassa 5.2 on esitetty yksinkertaistettu malli edellä mainittujen tilojen välisistä siirtymistä.

Passiivisessa tilassa oleva renki ei kommunikoi isännän kanssa. Renki pysyy kuitenkin synkronoituna isännän kanssa kuuntelemalla isännän lähettämää ns. majakkasignaalia (*beacon*). Signaalin tarkoituksena on helpottaa siirtymistä takaisin aktiiviseen tilaan, koska siirtymään liittyy keskustelua isännän kanssa. Passiivisessa tilassa oleva renki on kaikkein hitaimmin reagoiva, sillä aktiiviseen tilaan palaamiseen kuluu runsaasti aikaa. Toisaalta tilassa säästyy eniten energiaa, koska renki vastaanottaa vain majakkasignaalia, eikä lähetä mitään. [MiBi2001]

Pitotilassa oleva renki on sopinut isännän kanssa määrätyn ajan mittaisesta radiohiljaisuudesta. Rengin ei tarvitse tänä aikana odottaa isännältä viestejä, vaan se voi keskittyä johonkin toiseen tehtävään, esimerkiksi yhteyden muodostamiseen toisen



Kuva 5.2. Bluetooth-päätelaitteen yksinkertaistettu tilamalli.

isännän kanssa. Yhteys palaa normaalitilaan ajan kuluttua umpeen ja renki alkaa taas kuunnella viestejä isännältä. Pitotilassa päätelaitteen reagoivuus on alentunut, koska laite ei vastaa sille osoitettuihin viesteihin ennenkuin pitoaika on kulunut loppuun. Se, säästääkö pitotilassa oleminen päätelaitteen energiaa, riippuu siitä, mitä laite tekee pidossa ollessaan. [MiBi2001]

Haistelutila on yksi virransäästötekniikoista. Kun renki siirtyy haistelutilaan, se sopii isännän kanssa, että sille lähetetään informaatiota vain määritellyin väliajoin. Renki herää sovittuna määräaikana kuuntelemaan, onko isännällä sille viestejä ja ellei ole, vajoaa takaisin uneen. Jos isännällä sen sijaan on rengille tarkoitettuja viestejä, renki jatkaa kuuntelemista. Haistelutilassa säästyy energiaa, koska lähetin-vastaanotinta pidetään päällä vain osan ajasta. Säästetyn energian määrä riippuu olennaisesti aktiivisen ja passiivisen ajan suhteesta. [MiBi2001]

Isännän ja rengin välillä on mahdollista käyttää kahta erityyppistä yhteyttä. Synkroninen, yhteydellinen yhteys (*Synchronous Connection-Oriented link, SCO*) varaa yhteysvälille kiinteän kapasiteetin eli sitä voidaan verrata piirikytkentäiseen yhteyteen. SCO-yhteydet ovat erittäin tärkeitä esimerkiksi puhelinsovellusten kannalta, koska niitä käyttämällä vältetään reaaliaikaisen datan välittämiseen pakettiverkoissa liittyvät ongelmat. Asynkroninen, yhteydetön yhteys (*Asynchronous Connection-Less link, ACL*) on pakettikytkentäinen palvelu, jolle jaetaan SCO-yhteyksiltä ylijäävää kapasiteettia. ACL-yhteydet voivat olla myös isokronisia (*isochronous*), jolloin lähetettävän informaation on oltava perillä ennen säädettyä ajankohtaa. Isokroninen yhteys on oikeastaan ACL- ja SCO-yhteyksien välimuoto, koska sillä saadaan kuljetettavalle informaatiolle kiinteä läpäisykyky.

Pikoverkon isäntä pystyy muodostamaan yhteen tai useampaan renkiin yhteen kolme SCO-yhteyttä. Mikäli rengille tulevat yhteydet ovat eri isänniltä, niitä voi olla yhtäaikaisesti vain kaksi. Isännän ja rengin välille voidaan muodostaa yksi ACL-yhteys. SCO-yhteyksiä voidaan avata standardia puheenvälitystä varten, jolloin niiden kapasiteetti on 64 kbps<sup>14</sup>. ACL-yhteydet voidaan konfiguroida joko symmetrisiksi tai asymmetrisiksi; SCO-yhteydet ovat aina symmetrisiä. Symmetrinen yhteys tarjoaa saman kapasiteetin kumpaankin suuntaan, asymmetrinen ei. Symmetrisen yhteyden kapasiteetti on 433,9 kbps, asymmetrisen yhteyden 723,2 kbps ylöspäin (lähettäjältä vastaanottajalle) ja 57,6 kbps alaspäin (vastaanottajalta lähettäjälle). [BSIG1999]

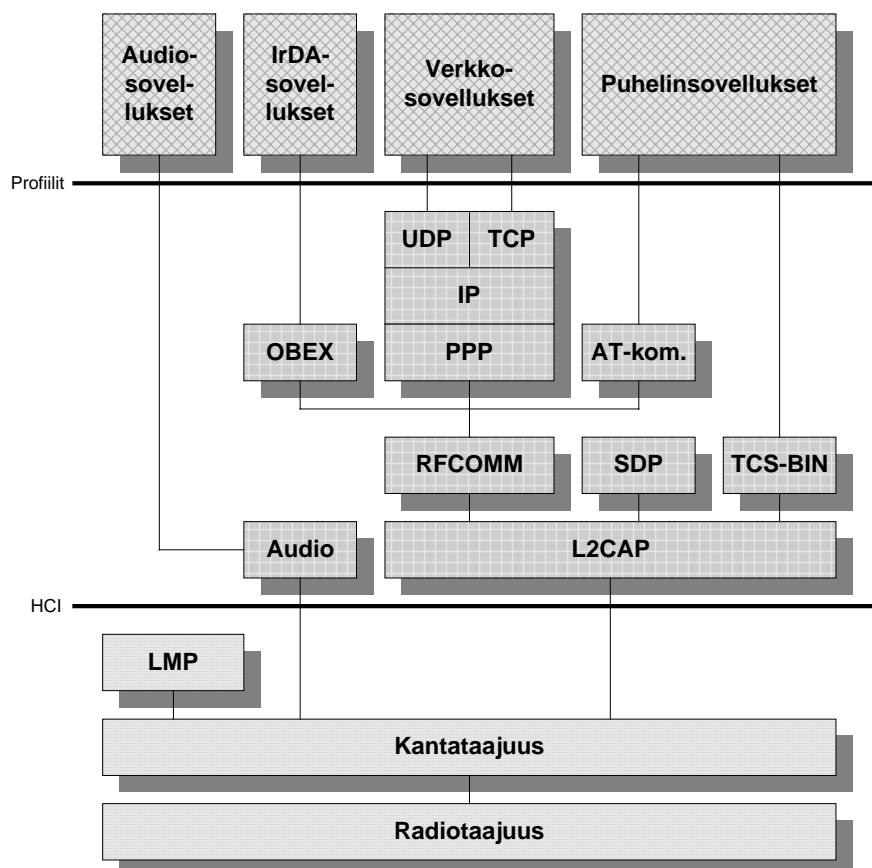
---

<sup>14</sup> kilo bits per second. Suom. tuhatta bittiä sekunnissa.

### 5.1.4 Protokollapino

Bluetoothin protokollapino, joka on esitetty kuvassa 5.3, ei muistuta klassisia protokollamalleja. Se johtuu tekniikan laajasta tuesta erilaisille sovellus- ja yhteystyypeille, mikä monimutkaistaa väistämättä toteutusta. Pinon olemuksen ymmärtäminen vaatii jonkinlaista tietämystä radiotekniikasta, standardiprotokollista ja tuetuista sovelluksista. Alakohta perustuu pääosin lähteeseen [MiBi2001].

Protokollapinosta on löydettävissä kolme erillistä protokollaryhmää: kuljetusprotokolla-, väliprotokolla- ja sovellusryhmät. Ryhmillä on omat loogiset tehtävänsä ja siksi ne erotetaan usein toisistaan toteutustasolla. Huomautettakoon, ettei kuljetusprotokollaryhmällä tarkoiteta samaa kuin OSI-mallin [Tane1996] kuljetuskerroksella. Ryhmä on pikemminkin informaatioputki, joka alkaa yhdestä Bluetooth-päätelaitteesta ja loppuu toiseen. Parempi vertailukohta on siis OSI-mallin siirtokerros.



Kuva 5.3. Bluetooth-protokollapino.

Kuljetusprotokollaryhmä koostuu protokollista, joiden tehtävänä on suorittaa ääni- ja dataliikenteen siirto kahden Bluetooth-laitteen välillä. Kaikki ryhmän protokollat on kehitetty Bluetooth SIG:n toimesta ja ne ovat siis spesifikaatioon räätälöityjä. Ryhmään kuuluvat radio- ja kantataajuuskerrokset sekä protokollat fyysisten yhteyksien hallintaan (*Link Manager Protocol, LMP*) ja loogisten yhteyksien hallintaan (*Logical Link Control And Adaptation Protocol, L2CAP*).

Kuljetusprotokollaryhmään liittyy läheisesti rajapinta isäntälaitteen ja Bluetooth-ohjaimen välillä (*Host Controller Interface, HCI*), joka on määritelty eri valmistajien tekemien Bluetooth-laitteiden yhteensopivuuden takaamiseksi. Rajapinnan taakse piilotetaan kanta- ja radiotaajuuskerrokset sekä LMP-protokolla, joita sovellukset pääsevät käyttämään rajapinnan tarjoamien palveluiden kautta. HCI-rajapinta on kiinnitetty ja siihen tukeutuvat sovellukset toimivat minkä tahansa valmistajan tekemän Bluetooth-lähetinvastaanottimen kanssa. Rajapinnan alle jäävien kerrosten laitteistototeutukset pakataan usein yhteen ja samaan laitteeseen, Bluetooth-ohjaimen, joka yhdistetään isäntälaitteeseen fyysisellä väylällä. Bluetooth-spesifikaatiossa tuetaan tällä hetkellä USB- (*Universal Serial Bus*), PC card- ja UART-väyliä (*Universal Asynchronous Receiver Transmitter*) [BSIG1999].

Seuraavassa käydään läpi kuljetusprotokollaryhmään kuuluvat protokollat ja kerrokset.

**L2CAP.** Protokolla käsittelee sovellusten lähettämää informaatiota. Se myös piilottaa pinon alemmat kerrokset ja fyysisen toteutuksen. Sovellusten ei näin ollen tarvitse huolehtia lähetystaajuuksista tai radiopakettien muodosta. L2CAP tarjoaa multiplexointipalvelun, jonka avulla useiden sovellusprotokollien informaatiota voidaan pakata samalle radiotielle. Protokolla osaa lohkoa ylemmiltä kerroksilta tulevat suuret paketit pienempiin paloihin, jotka sopivat paremmin kantataajuuskerroksen siirrettäväksi. Vastaanottopäässä palat kootaan takaisin alkuperäisiksi paketeiksi. Sovellus voi pyytää L2CAP:n välityksellä yhteydelle haluttua palvelunlaatua.

**LMP.** Protokolla on tarkoitettu radiorajapinnan ja fyysisten yhteyksien hallintaan. Sen avulla voidaan avata ja sulkea yhteyksiä, neuvotella L2CAP-protokollalla pyydettyjä palvelulaatuparametreja, hallita autentikointia ja yhteyden salausta, vaihtaa päätelaitteen tilaa yhteyden aikana sekä säätää kommunikoinnissa käytettävää lähetystehoja.

**Kantataajuuskerros.** Kerros määrittelee Bluetooth-ilmarajapinnan: miten laitteita ja palveluita haetaan kantaman sisäpuolelta ja miten niihin avataan yhteyksiä. Kerroksella määrätään isäntä-renki-roolit, taajuushyppelysekvenssi ja se, miten asynkroniset ja synkroniset yhteydet pakataan samalle radiotielle. Muita toimintoja ovat virheenhavainnointi ja –korjaus, signaalin salausta sekä pakettien lähetys ja uudelleenlähetys.

**Radiotaajuuskerros.** Kerros sisältää toimintoja, jotka liittyvät radiolähettimen ja –vastaanottimen ohjaukseen siten, että käytettävissä oleva radiokapasiteetti voidaan hyödyntää mahdollisimman optimaalisesti. Kerroksen vastuulle kuuluvat muun muassa modulointitekniikat sekä numeerisen informaation siirto radiotielle.

Väliprotokollaryhmän jäsenet hyödyntävät kuljetusprotokollaryhmää ja tarjoavat ylemmille kerroksille standardirajapintoja. Protokollat nostavat Bluetooth-tietoliikenteen abstraktiotasoa, jottei sovellusohjelmoijan tarvitse kiinnittää sovellustaan suoraan kuljetusprotokollaryhmään. Ryhmä koostuu Bluetoothia varten kehitetyistä protokollista (*RFCOMM, SDP, TCS-BIN, Audio*) sekä Bluetoothiin mukautetuista standardiprotokollista (*OBEX, PPP, IP, TCP, UDP, AT-komennot*). Seuraavassa on lyhyt katsaus ryhmän protokoliin ja osiin.

**RFCOMM.** RFCOMM on sarjaportin kautta käytävää kommunikointia emuloiva protokolla. Sarjaportti on sovelluksissa erittäin suosittu liityntätapa ulkomaailmaan, joten sen tukeminen Bluetoothissa on välttämätöntä. Protokollan toteutus perustuu ETSI:n (*European Telecommunications Standards Institute*) standardiin TS 07.10, joten olemassaolevien sovellusten pitäisi olla helposti siirrettävissä Bluetooth-ympäristöön. Protokolla määrittelee 60 multipleksoitua, virtuaalista sarjaporttiyhteyttä, joita sovellus voi käyttää täsmälleen samalla tavoin kuin todellisessa, kaapeloidussa ympäristössä.

**SDP (Service Discovery Protocol).** Kiinteän verkon palveluihin liittyy tavallisesti staattisesti määriteltyjä parametreja, esimerkiksi oletusreitittimen IP-osoite. Bluetooth-järjestelmässä ideana on tarjota palveluita dynaamisesti, joten staattiset konfiguraatiot eivät tuota riittäviä ratkaisuja. SDP-protokolla tarjoaa mekanismin, jolla päätelaitteet voivat kertoa tarjoamista palveluista ja niiden ominaisuuksista. Kus-

sakin päätelaitteessa on sekä SDP-palvelin, joka sisältää tietokannan laitteen omista ja ulkopuolelta saatavista palveluista, että SDP-asiakas, joka keskustelee muiden laitteiden palvelinten kanssa.

**TCS-BIN (Telephony Control Specification, Binary Encoding).** Protokolla on tarkoitettu puhelusovellusten tueksi. Sen toimintoja ovat muun muassa puheluparametrien asettaminen sekä puheluiden ja ryhmäpuheluiden hallinta. Protokolla on yhteensopiva ITU-T:n (*International Telecommunications Union - Telecommunication*) Q.931-spesifikaation kanssa, jota käytetään myös esimerkiksi ISDN (*Integrated Services Digital Network*) –järjestelmässä [Uoti1998].

**Audio.** Audiolla eli ääni-informaatiolla on erityisasema Bluetooth-järjestelmässä. Sitä ei voida varsinaisesti pitää omana protokollanaan, vaan pikemminkin erityisenä informaatioformaattina. Audiota kuljettava tietoliikenne on isokronista. Audio reititetään ajan säästämiseksi suoraan kantataajuuskerrokselle L2CAP:n ohi. Järjestelmässä tuetaan PCM<sup>15</sup>-, A-laki- ja  $\mu$ -laki-audiokoodausta.

**OBEX (Object EXchange).** OBEX on *Infrared Data Associationin (IrDA)* määrittelemä kahdenväliseen kommunikointiin sopiva istuntoprotokolla. Se on tarkoitettu objektien (esimerkiksi kalenteritietojen, käyntikorttien ja tiedostojen) siirtoon infrapuna-yhteyden yli. OBEX-protokollan tarkoitus Bluetooth-pinossa on saada aikaan IrDA-yhteensopivuus.

**PPP (Point to Point Protocol).** PPP on *Internet Engineering Task Forcen (IETF)* kehittämä siirtoprotokolla, jota käytetään sekä modeemien että kiinteiden linjojen kanssa. Protokolla toimii sekä synkronisilla että asynkronisilla yhteyksillä ja tukee virheenhavainnointia ja autentikointia. PPP on suunniteltu tukemaan erilaisia verkkoprotokollia, joista tärkein on IP. [Tane1996]

**AT-komennot.** AT-komennot on joukko komentoja, jota käytetään modeemien ohjaukseen. Modeemivalmistaja *Hayes* kehitti ne vuonna 1981 ilmestyneeseen tuotteeseensa. Myös muut valmistajat ottivat komennot käyttöönsä, jotta voisivat mainos-

---

<sup>15</sup> Pulse Code Modulation.

taa tuotteitaan Hayes-yhteensopiviksi. Nykyään komennot ovat saavuttaneet teollisuusstandardin aseman. Vaikka AT-komennot ovat melko primitiivinen tapa ohjata päätelaitetta, niitä on käytetty laajasti menetelmän yksinkertaisuuden vuoksi. Komentojoukko kehitettiin alkeellisia modeemeja varten, joten sitä on jouduttu laajentamaan modeemien nopeutuessa ja matkapuhelinten tultua mukaan modeemivalikoimaan.

**IP (Internet Protocol).** IP on Internetissä käytettävä verkkoprotokolla. Sen tärkein tehtävä on pakettien reititys oikeaan kohteeseen ja ruuhkautumisen välttäminen. IP on Internetin kulmakivi, joka takaa yhteensopivuuden erityyppisten verkkojen kesken. [Tane1996]

**TCP (Transmission Control Protocol).** TCP on luotettava ja yhteydellinen protokolla, joka mahdollistaa tavuvirran siirtämisen virheettömästi päätelaitteelta toiselle. [Tane1996]

**UDP (User Datagram Protocol).** UDP on epäluotettava ja yhteydetön kuljetusprotokolla. UDP ei sisällä TCP:n vuonohjaus- ja numerointipalveluja. Protokollaa käytetään reaaliaikaisten tietovirtojen siirtämiseen. [Tane1996]

Sovellusryhmä muodostuu erilaisista tietoliikennesovelluksista, jotka hyödyntävät jollakin tavalla Bluetoothia. Alempien kerrosten protokollat tarjoavat kattavan tuen synkronisille ja asynkronisille yhteyksille, joten sovellusten toteuttaminen Bluetooth-arkkitehtuuriin noudattaa perinteisiä kaavoja. Sovellukset eivät kuitenkaan normaalisti kiinnity suoraan väliprotokollaryhmän protokoliin, vaan käyttävät profiilirajapinnan palveluita. Rajapinta koostuu alati kasvavasta joukosta profiilitoteutuksia.

Profiili on tiettyä käyttötarkoitusta varten suunniteltu ohjelmointirajapinta, jonka Bluetooth SIG on spesifioinut osaksi koko Bluetooth-järjestelmää. Rajapinta tarjoaa joukon palveluja, joilla voidaan suorittaa profiilille määrätty käyttötehtävä. Profiileilla on yhteisiä ominaisuuksia, minkä vuoksi niiden välillä voidaan ajatella olevan periytymissuhteita. Kaikkien profiilien kantaisä on yleinen pääsiprofiili (*General Access Profile*), joka tarjoaa palvelut muun muassa laitteiden etsintään, yhteydenmuodostukseen ja pääsyparametrien hallintaan. Profiilit palveluiden hakemiseen, sarjaportin emuloimiseen ja puhelujen hallintaan periytyvät suoraan kantaisästä. Kahdella viimeksi mainitulla profiililla on laaja ja alati kasvava joukko perillisiä,

jotka tarjoavat erikoistuneita tiedonsiirtopalveluita: tiedostonsiirto, synkronointi, faksi- ja kuuloketoiminta sekä paikallisverkkoon pääsy. Profiileja kehitetään tällä hetkellä irrallaan muusta spesifikaatiosta, joten niiden julkaiseminen ei ole sidottu uusien järjestelmäversioiden ilmestymiseen.

### **5.1.5 Sopivuus PAN-verkoksi**

On oikeastaan hieman epäreilua pohdiskella Bluetoothin soveltuvuutta PAN-verkoksi, koska koko ideologiasta on alettu puhua vasta Bluetooth-konseptin pohjalta. Ei liene näin ollen yllättävää, että Bluetooth täyttää periaatteellisella tasolla kaikki ne vaatimukset, joita PAN-verkon toteutukselle asetetaan.

Bluetoothin tärkein PAN-verkkoja tukeva ominaisuus on päätelaitteiden kyky muodostaa itsenäisesti verkkoja. Prosessissa ei tarvita ulkopuolisia laitteita eikä palveluita, vaan päätelaitteilla itsellään on kaikki tarvittavat resurssit. Laitteiden välille muodostuneiden verkkojen käyttäminen on myös ilmaista.

Laitteiden löytäminen ja palveluiden hakeminen mahdollistavat PAN-päätelaitteille luontaisen liikkuvuuden. Niiden avulla Bluetooth-laitteet voivat itsenäisesti etsiä lähiympäristöstään tarvitsemiaan palveluita. Laajapohjainen tuki erilaisille sovelluksille ja informaatiovirroille on myös tärkeä asia, koska esimerkiksi puhetta välittävien järjestelmien toteuttaminen on siten yksinkertaista. Bluetooth-profiilit eivät sen sijaan ole vielä kaikenkattavia. Täydellistä PAN-verkon toiminnallisuutta ei sen vuoksi pystytä tällä hetkellä toteuttamaan.

Bluetooth-päätelaitteet mukautuvat hyvin PAN-verkkoihin. Niistä voidaan tehdä pieniä ja kevyitä, koska tehonkulutusta on optimoitu voimakkaasti. Tekniikka sisältää lähellä laitteistotasoa toteutettuja virransäästöominaisuuksia, joiden avulla voidaan säilyttää kohtuullinen reagointinopeus. Radioaaltojen lyhyt kantama ei ole PAN-verkkojen tapauksessa ongelma, koska siten voidaan säästää energiaa menettämättä mitään toiminnallisesti oleellista.

## **5.2 Langaton paikallisverkko**

Langaton paikallisverkko (*Wireless LAN, WLAN*) on vakiinnuttanut asemansa tehokkaana langattomana työasemien välisenä kommunikaatiomenetelmänä. Se on yksi



vahvimmista ehdokkaista yleiskäyttöisen, laajakaistaisen langattoman tiedonsiirron toteuttamiseen.

### 5.2.1 Taustaa

Paikallisverkkojen historia ulottuu 1980-luvun puoliväliin saakka. Standardointiorganisaatio IEEE (*Institute of Electrical and Electronics Engineers*) julkaisi vuonna 1985 joukon verkkostandardeja, joilla voitiin yhdistää pienen alueen työasemia loogisiksi kokonaisuuksiksi. Tekniikoilla muodostettuja verkkoja alettiin kutsua paikallisverkoiksi (*Local Area Network, LAN*). Myös termiä *lähiverkko* käytetään usein. [Tane1996]

Paikallisverkot ovat yksittäisten organisaatioiden, yritysten tai yhteisöjen omistamia ja hallinnoimia tietoverkkoja. Ne sijaitsevat kooltaan rajatulla alueella, esimerkiksi rakennuksessa, yrityksen toimitilojen välillä tai yliopiston kampusalueella. Verkot ovat omistajiensa yksityisessä käytössä, liittymä julkiseen verkkoon on selkeästi rajattu ja hyvin turvattu. Koska omistavat yhteisöt tekevät tavallisesti laitehankintansa keskitetysti, ovat paikallisverkkoon kiinnitetyt laitteet ja palvelut hyvin homogeenisia.

Paikallisverkkoja käytetään resurssien ja informaation jakamiseen. Tulostuksen siirtäminen paikallisverkon palveluksi on klassinen esimerkki resurssien jakamisesta. Tällöin tulostinta voidaan käyttää miltä tahansa verkossa olevalta asemalta, ei pelkästään siltä koneelta, johon tulostin on fyysisesti yhdistetty. Informaation jakamisella voidaan tehostaa organisaation toimintaa. Projektiin kuuluvat tiedostot voidaan esimerkiksi tallettaa keskitetysti halutulle työasemalle tai palvelimelle, johon kaikille asianomaisille myönnetään pääsy. Muutokset voidaan tehdä suoraan verkossa olevaan tiedostoon, jolloin vältetään ristiriitaisten versioiden ongelmalta. Paikallisverkot ovat synnyttäneet kulttuurin, jossa informaation siirtämistä levykkeillä tietokoneelta toiselle pidetään vanhanaikaisena, hitaana ja virhealttiina.

IEEE:n julkaisemat paikallisverkkospesifikaatiot ovat saavuttaneet dominoivan aseman. Spesifikaatio 802.3, joka tunnetaan paremmin nimellä *Ethernet*, on tänä päivänä ehdottomasti suosituin paikallisverkkotekniikka [Tane1996]. Se kuvaa väylämäistä, työasemia yhdistävää verkkoa, jossa kaikki asemat ovat tasa-arvoisia. Ethernet-pohjaisia verkkoja käytetään nopeuksilla 10 Mbps ja 100 Mbps. Myös gigabittiluokan nopeuksiin ylittäviä ratkaisuja on kehitteillä, mutta niiden yleistymisen vie vielä

vuosia. Toinen IEEE:n standardoima paikallisverkkotekniikka on nimeltään 802.5 eli *Token Ring* [Tane1996]. Se kuvaa rengasverkkoa, jossa kommunikointivuoro siirtyy asemalta toiselle isäntäkoneen johdolla. Tekniikka ei ole koskaan saavuttanut samanaista suosiota kuin Ethernet. Myös muutamat yritykset (esimerkiksi *Novell*) ovat kehittäneet omia ratkaisujaan, mutta kuten valmistajakohtaiset ratkaisut yleensäkin, nekin eivät ole saavuttaneet laajaa suosiota.

Paikallisverkkoja kehitettiin muutamia vuosia kaapeloituihin ympäristöihin: toimistoihin, teollisuuteen ja koteihin. Tekniikat kehittyivät voimakkaasti ja niistä tuli työasemien vakiovarusteita. Kun langattomat verkkotekniikat alkoivat nostaa päätään 80-luvun lopulla, kiinnostui myös IEEE aiheesta. Se organisoi vuonna 1990 tutkimusprojektin, jonka tavoitteena oli kehittää maailmanlaajuisesti käytettävän langattoman paikallisverkon standardi [Held2001]. Standardin tuli toteuttaa verkko, jolla voitaisiin laajentaa tai korvata olemassaolevia, kiinteitä paikallisverkkoja. Verkon tuli kuitenkin olla ylempien protokollakerrosten osalta yhteensopiva olemassaolevien paikallisverkkojen kanssa. Näin voitiin turvata vanhojen sovellusten toimivuus uudessa ympäristössä. Projektin tuloksena syntyi standardi 802.11a eli *Wireless LAN*, langaton paikallisverkko. Kehitystyötä jatkettiin ja sen tuloksena ilmestyi myöhemmin toinen standardi, 802.11b.

IEEE:llä on tällä hetkellä käynnissä henkilökohtaisiin verkkoihin liittyvä standardointihanke. Kehitettävää standardia kutsutaan nimellä 802.15 eli WPAN (*Wireless Personal Area Networks*) [IEEE2001]. Standardointityö koostuu viidestä tehtävästä, joista tärkein on uuden, Bluetooth- ja 802.11-järjestelmiä yhteensovittavan verkkotekniikan kehittäminen. Tekniikka perustuu Bluetooth-arkkitehtuuriin, mutta on WLAN-yhteensopiva. Lisäksi standardointiin kuuluu suuri- ja matalanopeuksisten henkilökohtaisten verkkojen kehitys. Suurinopeuksisilla WPAN-verkoilla tarkoitetaan yli 20 Mbps langattomia verkkoja, jotka tulevat olemaan Bluetooth-yhteensopivia. Matalanopeuksisilla verkoilla tähdätään 10-200 kbps siirtonopeuksiin erittäin pienellä tehonkulutuksella. Laitteiden toiminta-aikaa voitaisiin siten nostaa jopa muutama vuosiin.

### 5.2.2 Tiedonsiirtomenetelmä

WLAN-kehittäjien tehtävänä oli suunnitella langaton paikallisverkkotekniikka maailmanlaajuiseen käyttöön. Langatonta kommunikaatiota ohjaavat lait ja säädökset vaih-

televat jonkin verran maittain, minkä vuoksi WLAN-tekniikka tukee kolmea eri tiedonsiirtomenetelmää. Standardin ensimmäinen versio, 802.11a, määritteli tuen kahdelle radiotaajuus- ja yhdelle infrapunamenetelmälle. Toinen versio, 802.11b, keskittyi toisen radiotaajuusmenetelmän jatkokehitykseen. Teollisuuden suurimmat odotukset kohdistuvat tällä hetkellä juuri viimeksi mainittuun versioon, koska sen tiedonsiirtokapasiteetti on suurin.

Radiotaajuusmenetelmät käyttävät samaa ISM-taajuusaluetta kuin Bluetooth. Kommunikaatio tapahtuu hajaspektritekniikkaa hyödyntäen. Toinen radiotaajuusmenetelmä perustuu aiemmin esiteltyyn taajuushyppelytekniikkaan, toinen ns. suorajakso-tekniikkaan (*Direct-Sequence Spread Spectrum, DSSS*). Taajuushyppelytekniikalle spesifioitiin lähetysnopeudet 1 Mbps ja 2 Mbps, joista jälkimmäinen on toteuttajalle valinnainen. Suorajakso-tekniikassa lähetyspään kantoaaltoa moduloidaan digitaalisella koodilla, jota kutsutaan palaksi (*chip*). Vastaanottajalla tulee olla tiedossaan modulaatioon käytetty pala, jotta informaatio voidaan paljastaa kantoaallostaa. Modulointi lisää viestiin redundanssia ja kasvattaa käytettävää taajuuskaistaa. Redundanssin avulla vastaanottaja voi paitsi havainnoida, myös korjata joitakin tiedonsiirrossa tapahtuneita virheitä. Moduloitu kantoaalto on laajakaistainen ja heikkotehoinen signaali, joka muistuttaa kohinaa. Salakuuntelijan on tällöin vaikeata havaita, milloin ilmassa liikkuu todellista informaatiota. Suorajakso-tekniikkaa käytetään sen vuoksi sotilaallisiin sovelluksiin. Sitä tullaan hyödyntämään myös kolmannen sukupolven matkapuhelinverkoissa. Ensimmäisessä WLAN-standardissa (802.11a) suorajakso-tekniikalle spesifioitiin 1 Mbps ja 2 Mbps lähetysnopeudet. Toiseen versioon nopeuksia pystyttiin nostamaan: uudet arvot ovat 5,5 Mbps ja 11 Mbps. [Held2001]

Infrapunamenetelmässä käytetään hyväksi erittäin korkeataajuuksista sähkömagneettista säteilyä, jonka taajuus on hieman näkyvää valoa pienempi [Held2001]. Järjestelmän toimintaa voidaan verrata tilanteeseen, jossa kaksi kaverusta haluaa viestiä toisilleen pimeässä, pitkän matkan takaa. Toinen ystävästä välkyttää taskulampun valoa ja toinen yrittää selvittää viestin sisällön saamastaan informaatiosta. Järjestelmässä piilee kuitenkin kiusallinen ongelma: mitä tapahtuu, jos lähettäjän ja vastaanottajan välissä on valoaläpäisemätön este? Kommunikaatio on tällöin estetty niin kauan kuin este on olemassa tai osapuolia siirretään näköyhteyden aikaansaamiseksi uudelleen. Ongelma on yritetty ratkaista kehittämällä tekniikoita, joita käyttämällä suoran näköyhteyden tarve osapuolten välillä poistuu. Tekniikat perustuvat infrapunavalon heijastusten tulkitsemiseen ja niillä on onnistuttu luomaan yhteyksiä tavallisen huo-

neen kokoisessa tilassa. Monen osapuolen välinen kommunikaatio on hankalaa, joskaan ei mahdotonta, toteuttaa infrapunatekniikalla. Standardissa pitäydytään sen vuoksi kahdenvälisessä kommunikaatiossa. Infrapunavastaanotinten heikko toimintakyky ulkotiloissa on myös ongelma. Auringosta tuleva voimakas infrapunasäteily sekoittaa vastaanotinten toiminnan, minkä vuoksi tehokasta suorituskykyä voidaan odottaa vain sisätiloissa. Infrapunatekniikkaa sovellettaessa on hyväksyttävä sen rajoitteet. Muutamat langattomien paikallisverkkolaitteiden valmistajat ovat tuoneet markkinoille tekniikkaan perustuvia tuotteitaan, mutta infrapunamenetelmä on kokonaisuutena jäämässä radiotaajuusmenetelmien varjoon. Infrapunatekniikalle on spesioitu lähetyksenopeudet 1 Mbps ja 2 Mbps, joista jälkimmäinen on toteuttajalle valinnainen.

### 5.2.3 Rakenne

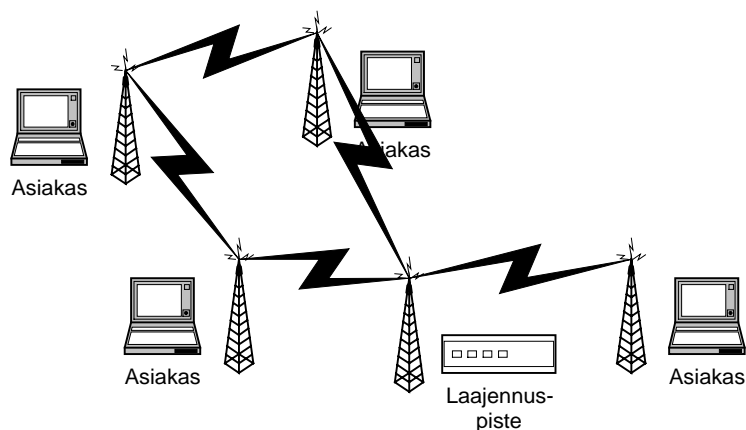
Langaton paikallisverkko voi perustua kahteen eri arkkitehtuuriin: itsenäiseen ja infrastruktuuriarkkitehtuuriin. Vaihtoehdot ovat kuitenkin hyvin erilaisia, minkä vuoksi todellista valintatilannetta ei yleensä synny. Verkon käyttötarkoitus ja konfiguraation pysyvyys sanelevat käytännössä valittavan arkkitehtuurin. Huolimatta arkkitehtuurien välisistä eroista on huomattava, että sovelluksille näkyvä verkkokonfiguraatio on aina sama.

Jokaisessa verkon päätelaitteessa on langattoman paikallisverkon sovitin, joka koostuu karkeasti ottaen radiolähettimestä ja –vastaanottimesta, ohjauslogiikasta sekä liittynästä isäntälaitteeseen. Sovitin liitetään tavallisesti tietokoneeseen lisäkortin (esimerkiksi PC card) avulla, mutta se voidaan myös integroida osaksi päätelaitetta.

Itsenäinen arkkitehtuuri (*independent configuration*) on verkkokonfiguraatio, jossa joukko päätelaitteita muodostaa paikallisverkon. Kuvassa 5.4 on nähtävissä esimerkki tällaisesta verkosta. Verkko on täysin riippumaton ulkopuolisista laitteista ja palveluista, eikä näin ollen sisällä liittymiä kiinteästi asennettuihin verkkoihin. Arkkitehtuuri ei vaadi staattista konfigurointia: asiakkaat voivat liittyä ja poistua verkosta dynaamisesti. Laitteet on sijoitettu niin, että ne ovat toistensa verkkosovittimien kantaman sisäpuolella. Kantamaa voidaan kasvattaa kytkemällä verkkoon laajennuspiste (*Extension Point, EP*). Laajennuspiste toimii kuten kiinteän verkon toistin, se vastaanottaa viestejä ja lähettää ne sellaisenaan eteenpäin oman kantamansa sisällä. Laajen-

nuspiste on muutoin täysin passiivinen eli se ei osallistu verkossa käytävään kommunikaatioon.

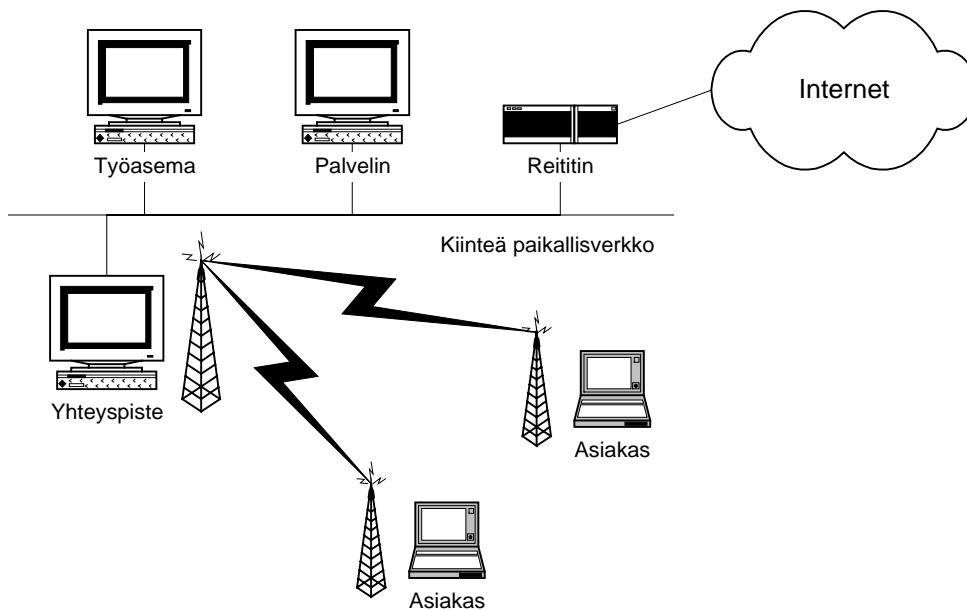
Itsenäistä arkkitehtuuria käytetään muodostamaan verkkoja, joiden rakenne on muuttuva. Sopivia käyttötilanteita ovat esimerkiksi kokoukset, joissa tarvitaan osallistujien kesken jaettua tiedonsiirtokapasiteettia. Arkkitehtuurin heikkous on ulkoisten liittymien puuttuminen, minkä vuoksi se ei yleensä sovellu pitkäaikaiseen ja kiinteämpään käyttöön.



Kuva 5.4. Itsenäisen arkkitehtuurin mukainen verkko.

Infrastruktuuriarkkitehtuurissa (*infrastructure configuration*) langaton paikallisverkko liittyy jollakin tasolla kiinteään verkkoon. Liityntä voi olla kiinteään paikallisverkkoon, Internetiin tai molempiin. Arkkitehtuuria noudattava verkko rakennetaan erityisasemassa olevien päätelaitteiden, yhteyspisteiden (*Access Point, AP*) varaan. Yhteyspisteeseen on asennettu normaali langattoman paikallisverkon sovitin, mutta sen toiminta on erilainen kuin verkon asiakkaalla. Yhteyspisteen ympärille muodostuu alue, jonka sisällä asiakkaat voivat kommunikoida yhteyspisteen kanssa. Tätä aluetta kutsutaan *soluksi*. Solu on tyypillisesti ympyränmuotoinen ja säteeltään 30-60 metriä. Yhteyspiste kykenee käsittelemään 10-20 asiakkaan tietoliikenteen, mutta määrää voidaan kasvattaa rajoittamalla asiakkaiden kommunikointioikeuksia.

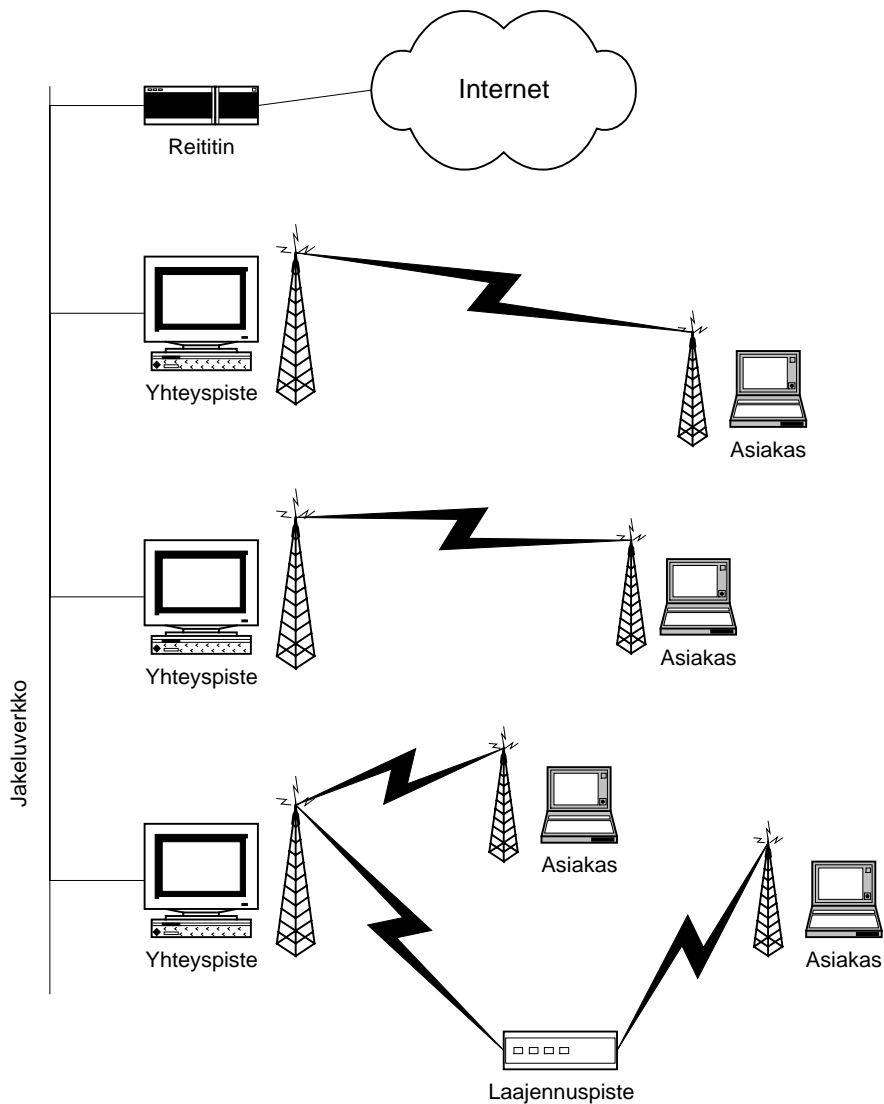
Itsenäisessä arkkitehtuurissa verkon asiakkailla on keskinäisiä yhteyksiä, kun taas infrastruktuuriarkkitehtuurissa asiakkaat kommunikoivat vain yhteyspisteiden



Kuva 5.5. Langattoman verkon liittyminen kiinteään paikallisverkkoon.

kanssa. Tämä ei kuitenkaan rajoita verkossa käytävää keskustelua, koska yhteyspiste toimii *reitittimenä* eli laitteena, joka ohjaa asiakkailta tulevat viestit oikeaan osoitteeseen. Asiakas voi kohdistaa viestinsä mille tahansa verkon laitteelle ja lähettää sen yhteyspisteelle, joka laittaa viestin eteenpäin kohti oikeaa määränpäättä.

Kuvassa 5.5 on esitetty verkkokonfiguraatio, jossa kiinteää paikallisverkkoa laajennetaan langattomalla paikallisverkolla. Yhteyspiste toimii tässä tapauksessa välittäjänä kiinteän ja langattoman verkon välissä. Langattomat asiakkaat saavat yhteyspisteen kautta pääsyn kiinteän paikallisverkon asemiin ja päinvastoin. Koska kiinteä verkko on yhdistetty Internetiin, voidaan myös langattomille päätteille suoda pääsy sinne. Yhteyspisteiden määrää voidaan lisätä mielivaltaisesti, mikäli verkkoon tarvitaan kapasiteettia uusille asiakkaille. Infrastruktuuriverkko voidaan rakentaa myös ilman kiinteää paikallisverkkoa. Tällöin rakennetaan erityinen jakeluverkko (*Distribution System, DS*) yhdistämään yhteyspisteitä. Jakeluverkko, josta voidaan nähdä esimerkki kuvassa 5.6, voidaan toteuttaa joko kiinteänä tai langattomana. Langattomat asiakkaat liittyvät verkkoon yhteyspisteiden luomien solujen välityksellä siten, että asiakas on aina täsmälleen yhden solun jäsen. Eri soluihin kiinnittyneet asiakkaat voivat keskustella toistensa kanssa omien yhteyspisteidensä ja jakeluverkon välityksellä. Yhteyspiste tuntee solunsa alueella olevat asiakkaat ja mikäli viestin kohde



Kuva 5.6. Kolmen yhteyspisteiden langaton paikallisverkko liitynnällä Internetiin.

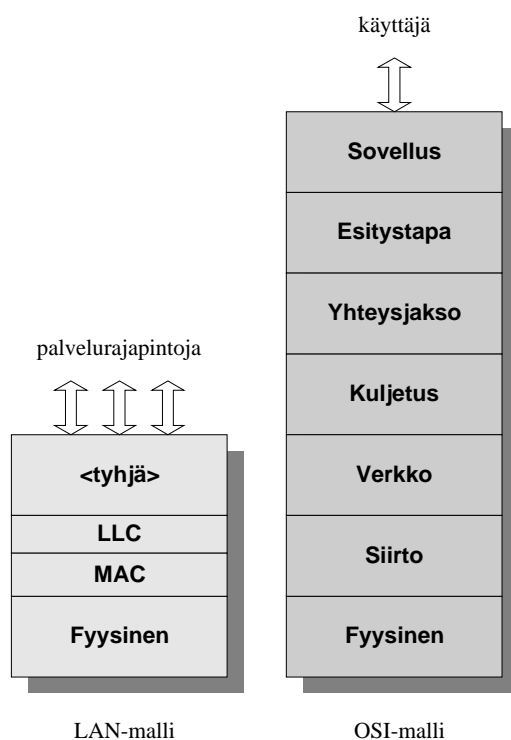
on solun ulkopuolella, se löytyy jakeluverkon kautta. Jakeluverkko reitittää viestin oikealle yhteyspisteelle, joka puolestaan toimittaa viestin perille. Yksittäisten solujen kantamaa voidaan kasvattaa laajennuspisteiden avulla.

Jakeluverkko voi sisältää liityntöjä ulkoisiin verkkoihin. Tyypillisin ratkaisu on se, että verkkoon kytketään Internet-yhteyden tarjoava reititin. Jakeluverkko voi olla kiinnittynyt myös kiinteään paikallisverkkoon, jolloin syntyy itsenäisen ja infrastruktuuriarkkitehtuurin yhdistelmä.

## 5.2.4 Protokollapino

Ethernet-protokollapino on suunniteltu aikana, jolloin Internet-mullistuksesta oli vasta aavistuksia. Käytössä oli sen sijaan useita keskenään yhteensopimattomia verkkosovelluksille näkyviä rajapintoja, kuten Microsoftin *NetBios* ja Novellin *IPX (Internetwork Packet eXchange)*. Ethernet-standardin suunnittelussa keskityttiin tukemaan näitä rajapintoja, minkä vuoksi protokollapinosta tuli varsin erikoinen ja OSI-referenssimalliin mukautumaton, kuten kuvasta 5.7 on nähtävissä [GrMi1998].

Langattoman lähiverkon protokollapino periytyy Ethernetin protokollapinosta. WLAN-pino on LLC<sup>16</sup>-protokollasta lähtien yhtenevä kantaisänsä kanssa. MAC<sup>17</sup>-protokolla ja fyysinen kerros ovat sen sijaan langattomaan ympäristöön räätälöityjä. Koska sovitus langattomaan ympäristöön toteutetaan pinon alimmissa kerroksissa, näkyvät sovellus- ja palvelutasolle perinteisen Ethernetin ja suoraan sen päälle sijoitetun



Kuva 5.7. OSI- ja LAN-mallin eroavaisuus.

<sup>16</sup> Logical Link Control [Tane1996].

<sup>17</sup> Medium Access Control [Tane1996].



TCP/IP-mallin protokollat. Yhteensopivuus olemassaolevien järjestelmien kanssa on ollut tärkeä osa langattoman paikallisverkon konseptia, koska Ethernet-verkot ovat hyvin yleisiä.

Ethernet-mallissa verkossa olevia laitteita yhdistää yksi ja sama siirtomedia. Langattoman paikallisverkon tapauksessa yhteinen media on radiorajapinta, johon mikä tahansa laite voi lähettää informaatiota valitsemallaan ajanhetkellä. Kyseessä on siis kilpavarausperiaatteella toimiva kommunikaatioväylä, jonka ohjaamiseen tarvitaan jokin menetelmä. MAC-protokolla tarjoaa keinon kontrolloida asemien lähetyksiä käyttäen CSMA/CA<sup>18</sup>-menettelyä. Lisäksi se toimii sovituserroksena kolmeen edellä esiteltyyn fyysiseen kerrokseen. MAC-protokollassa voi olla toteutuksesta riippuen myös uudelleenlähetyksen, kuittausten, virransäästön, synkronoinnin ja salauksen toiminnallisuudet. [Held2001]

Langattoman paikallisverkon salaustoiminnallisuutta kutsutaan nimellä WEP (*Wireless Equivalent Privacy*) [Held2001]. Se sisältää informaation salauksen ja autentikoinnin 40-bittisen salaisen avaimen avulla. Avain generoidaan uudelleen jokaisesta kehystä varten. WEP-salausta ei voida kuitenkaan pitää riittävänä, koska salausvahvuus on liian heikko. 128-bittistä salausta pidetään nykyään turvallisen tietoliikenteen perusvaatimuksena.

Kullekin tiedonsiirtomenetelmälle toteutetaan erilliset fyysisen kerroksen protokollat. Niissä esiintyy toisistaan eroavia kehysrakenteita, mutta peruseriaatteet ovat kuitenkin samat. Kaikissa toteutuksissa on esimerkiksi kenttä, joka määrää käytettävän tiedonsiirtonopeuden. Radiotaajuustoteutusten kehyksissä on myös 16-bittinen CRC-tarkistussumma (*Cyclic Redundancy Check*), jonka avulla vastaanottopäässä voidaan varmistua kehyksen oikeellisuudesta.

### 5.2.5 Toiminta

Langattoman lähiverkon toiminta muistuttaa hyvin paljon kiinteän lähiverkon toimintaa. Tekniikoiden väliset eroavaisuudet näkyvät kuitenkin ainoastaan lähellä fyysistä tasoa. Langattomissa verkoissa yhteyspisteet toimivat kaapeleiden korvaajina, mutta niitä ei voida pitää jaettuina medioina. Radiorajapinta on ainoa todellinen jaettu media, mutta sen jakavat vain yhteen soluun kiinnittyneet päätelaitteet. Kiinteissä paikall-

---

<sup>18</sup> Carrier Sense Multiple Access / Collision Avoiding [Held2001].

lisverkoissa ryhmä asemia taas jakaa yhden segmentin eli verkossa toimivan väylän. Tekniikoissa on siis nähtävissä erilaisia ratkaisuja samaan ongelmaan.

Langattomaan paikallisverkkoon liittyminen on monivaiheinen operaatio. Päätelaitteen tulee ensin saada selville yhteyspisteen lähetyksen vaihe. Tämä ns. synkronoituminen voidaan hoitaa joko aktiivisesti tai passiivisesti. Aktiivinen menetelmä tarkoittaa, että päätelaite lähettää suoraan yhteyspisteeseen kyselyn, johon se saa vastauksena synkronoitumiseen tarvittavat tiedot. Passiivisessa menetelmässä päätelaite odottaa yhteyspisteen ajoittain lähettämiä majakkaviestejä (*beacon*), jotka sisältävät synkronointitietoja. Kun päätelaite on synkronoitunut yhteyspisteen kanssa, tapahtuu autentikointi. Jos laitteelle myönnetään pääsy verkkoon, yhteyspisteelle annetaan vastuu laitteen viestien välittämisestä. Päätelaitte on kirjautunut verkkoon ja voi sekä lähettää että vastaanottaa viestejä.

Päätelaitteet voivat liikkua langattomassa paikallisverkossa, mikä on tärkeä langattomuuteen kuuluva ominaisuus. Verkkospesifikaatio tukee liikkumista kuitenkin vain kävelynopeudella eli muutamia kilometrejä tunnissa. Esimerkiksi ajoneuvoihin sijoitetut laitteet eivät näin ollen pysty olemaan aktiivisia liikkuessaan. Päätelaitte seuraa jatkuvasti yhteyspisteeltä tulevan signaalin voimakkuutta. Solun sisällä tapahtuva liikkuminen ei tavallisesti aiheuta haittaa tietoliikenteelle, koska signaali on riittävän vahva. Mikäli signaali heikentyy kriittiselle tasolle, tietää laite joutuneensa solun reuna-alueille. Laite alkaa lähettää kartoitusviestejä, joihin lähistöllä olevat yhteyspisteet vastaavat. Laite valitsee niistä yhden ja lähettää sille liittymispyynnön, jonka jälkeen seuraa edellä kuvattu liittymisproseduuri. Jos liittyminen ei onnistu, kokeilee laite seuraavaa yhteyspistettä ja niin edelleen. Mikäli yhteyspisteitä ei ole käytettävissä tai niihin kiinnittyminen ei onnistu, sovellustasolle välittyy viesti verkon katoamisesta.

### **5.2.6 Sopivuus PAN-verkoksi**

Itsenäisellä arkkitehtuurilla toteutettu langaton paikallisverkko on melko lähellä PAN-verkkojen olemusta. Päätelaitteet voivat liittyä ja poistua verkosta vapaasti, eikä staattista konfigurointia tarvita. Verkko tarjoaa riittävästi kapasiteettia erilaisten sovellusten käyttämiseen. Synkronisia yhteyksiä ei kuitenkaan tueta tekniikan tasolla, mikä hankaloittaa esimerkiksi puheen välittämistä. Pienikokoisessa verkossa, jossa ei ole kovin monia laitteita jakamassa kapasiteettia, ongelmia ei kuitenkaan pitäisi syntyä.

WLAN-tekniikkaan ei ole spesifioitu toimintoja laitteiden tai palvelujen löytämiseen. Laitteita voitaisiin toki hakea esimerkiksi IP-osoitteen perusteella, mutta mistä saada ensin selville IP-osoite? Bluetooth-spesifikaatiossa mukana oleva etsintäproseduuri voitaisiin ehkä toteuttaa uutena sovelluksena tai ylemmän tason protokollana. Sen lisääminen valmiiseen verkkokonseptiin ei kuitenkaan ole kovin suoraviivainen tehtävä.

PAN-verkon päätelaitteiden tulisi olla kädessäpidettäviä tai kannettavia. Langattoman paikallisverkon käyttäminen tällaisessa laitteessa on kuitenkin nykyisellään hankalaa, koska tekniikan tehonkulutus on erittäin suuri. Tärkein syy tähän on se, ettei langatonta paikallisverkkoa ole optimoitu pieniin päätelaitteisiin. Tilanne on itse asiassa täysin päinvastainen, sillä tekniikka on alunperin suunniteltu tietokoneisiin, jotka pystyvät kiinnittymään sähköverkkoon ja toimimaan muutamia tunteja akkujen varassa. WLAN:n kantama on esimerkiksi Bluetoothia suurempi, mikä vielä osaltaan kasvattaa tehonkulutusta. Lisäksi protokollapinossa ei juurikaan tueta virransäästötoimintoja, joten laitteen lähetin-vastaanotin on päällä aina, kun laite on verkossa.

WLAN-tekniikkaa ei voida nykymuodossaan hyödyntää PAN-verkon toteuttamiseen. Mikäli päätelaitteiden löytämiseen ja tekniikan tehonkulutukseen löydetään toimivia ratkaisuja, voi langattomasta lähiverkosta kuitenkin kehittyä merkittävä tekijä myös henkilökohtaisten verkkojen puolella. WLAN-tekniikkaan kohdistunut pitkäaikainen kehitystyö tuo tiettyjä etuja, joita uudemmilla järjestelmillä, kuten Bluetoothilla, ei vielä ole. Laajamittainen yhteentoimivuuteen ja kenttätestaukseen liittyvä kokemus ei ole niistä vähäisin.

## **5.3 Muut järjestelmät**

Markkinoilla on tänä päivänä useita erilaisia langattoman kommunikaation järjestelmiä. Joillakin on keskenään paljon yhteistä, toiset ovat taas ratkaisuiltaan erikoisempia. WLAN:in perustuvia järjestelmiä lienee eniten, koska pohjalla oleva tekniikka on kypsyyntä ja hyväksihavaittua.

### **5.3.1 IrDA**

Infrapunavaloa on käytetty tiedonsiirrossa jo kauan: kodinelektronikassa langattomat kaukosäätimet ovat olleet arkipäivää jo parikymmentä vuotta. Ajatus infrapunon käyt-

töstä tietokoneiden väliseen kommunikointiin heräsi 90-luvun alkuvuosina. Touko-kuussa 1993 perustettiin organisaatio, *The Infrared Data Association* (IrDA), edistämään tekniikan kehitystä. Mukaan lähti silloin noin 50 yritystä, nykyään jäsenmäärä on yli 150. Vuoden kuluttua julkaistiin ensimmäinen spesifikaatio, jota kutsutaan nimellä *IrDA-D*. Sitä on jatkokehitetty ja laajennettu tähän päivään asti. Infrapunatekniikkaa on totuttu nimittämään sitä kehittävä organisaation nimellä, samaa käytäntöä tullaan noudattamaan myös tässä tarkastelussa. [IrDA2001]

IrDA-tekniikan tavoitteena on olla laajasti tuettu, edullinen, matalatehoinen, konfiguraatioltaan dynaaminen, kahdenväliseen kommunikointiin sopiva menetelmä. Infrapunavalon voidaan ajatella korvaavan johtoja laitteiden välillä, minkä vuoksi tekniikan lähin vertailukohta on sarjaliitynnän käyttö. Yhteyden kantama on käytännössä noin kaksi metriä, koska sitä pidemmillä matkoilla heijastusten aiheuttamat häiriöt alkavat muodostua liian suuriksi. Tiedonsiirtonopeus noudattaa sarjaportteille spesifioituja päätenopeuksia: 115200 kbps on perusnopeus. Suurin spesifioitu nopeus on tällä hetkellä 4 Mbps, 16 Mbps:n nopeus on kehitteillä. Infrapunatekniikan tyypillisiin käyttötapauksiin kuuluu sarjaliitännän lisäksi pienehkön informaatiomäärän siirto tarvetta varten synnytettyssä verkossa. Siirrettävää informaatiota ovat esimerkiksi kalenteritiedot, tiedostot ja sähköpostit. Verkko muodostetaan kahden päätelaitteen välille juuri ennen tiedonsiirto-operaatiota. Verkon yhteydet ovat yhdensuuntaisia (*half-duplex*) eli kun toinen yhteyden osapuoli lähettää, toisen on tyydyttävä kuuntelemaan. Kahdensuuntainen (*full-duplex*) yhteys voidaan emuloida, mikäli kyseessä ei ole aika-kriittinen sovellus. IrDA-protokollapino ei tue luontaisesti IP-protokollaa, mutta sitä voidaan kuljettaa sovellustasolla sarjaliityntäprotokollan päällä.

Jotta verkko voidaan rakentaa dynaamisesti, tarvitaan jokin mekanismi, jolla päätelaitteet voivat löytää toisensa. IrDA:ssa sen nimi on *Information Access Service* (IAS). Jokaiseen päätelaitteeseen on toteutettu sekä IAS-asiakkaan että -palvelimen toiminnallisuus. Palvelin vastaa toisissa laitteissa olevilta asiakkailta tuleviin palvelupyyntöihin, asiakas taas kommunikoi muiden laitteiden palvelimien kanssa. IAS-asiakas lähettää infrapunalinkin yli pyynnön tietyn tyyppisestä palvelusta. Pynnön vastaanottava palvelin palauttaa tiedon siitä, onko sen hallinnoimassa laitteessa pyydetty palvelu. Samalla tarkistetaan myös laitteiden välinen yhteensopivuus. IAS mahdollistaa sen, ettei laitteen käyttäjän tarvitse tietää mitään teknisiä yksityiskohtia toisesta infrapuna-aktiivisesta laitteesta. Riittää, että hän kohdistaa oman laitteensa infrapunasäteen toista laitetta kohti. IAS-palvelua voidaan pitää onnistuneena, koska

Bluetooth-spesifikaation SDP-protokolla on toteutettu melko pitkälle samalla tavoin. [MeSK1998]

IrDA-D -spesifikaatio on ollut perustana monille jatkohankkeille. Saatavilla on esimerkiksi kahdenväliset full-duplex -yhteydet mahdollistava *IrDA-C* ja monenväliset yhteydet mahdollistava *AIR*. Alkuperäisen tekniikan rajoitteita on siis pystytty osittain poistamaan.

Infrapunakommunikaatiolla on mahdollista toteuttaa PAN-verkko. IrDA-tekniikan nopeus ja sisäänrakennettu IAS-palvelu ovat eduksi, tehonkulutus on myös riittävän pieni kädessäpidettävään laitteeseen. Tekniikan heikkouksia ovat muutaman metrin pituinen kantama, heikko toiminta ulkotiloissa ja synkronisten yhteyksien puuttuminen. Lyhyt kantama ja rajoittuminen sisäkäyttöön eivät ole ongelmia useimmille sovelluksille, mutta esimerkiksi paikallisen WAP-palvelun toimintaa ne rajoittavat tarpeettoman paljon. Infrapunatekniikkaa ei näin ollen voida pitää riittävänä ratkaisuna yleisluontoiseen PAN-verkottumiseen.

### 5.3.2 HomeRF

HomeRF on koteihin ja toimistoihin suunnattu langaton kommunikaatiomenetelmä. Sitä kehittää samalla nimellä toimiva teollisuuskonsortio, johon kuuluvat muun muassa *Philips, Compaq, IBM, Intel, Motorola* ja *Siemens* [Held2001]. Järjestelmä tarjoaa jaetun langattoman median, jossa voidaan kuljettaa sekä asynkronista että isokronista informaatiota. HomeRF tukee kuutta yhtäaikaista, kaksisuuntaista puheyhteyttä ja yhtä yhteydetöntä datakanavaa. Mediaa hallitsee avoimesti spesifioitu SWAP-protokolla (*Shared Wireless Access Protocol*), joka perustuu IEEE:n WLAN-standardiin 802.11 ja eurooppalaiseen digitaalisten, langattomien puhelinten DECT-standardiin (*Digitally Enhanced Cordless Telephony*) [Home1998]. Kommunikaatio tapahtuu 2,4 gigahertsin ISM-kaistalla taajuushyppelytekniikkaa käyttäen. HomeRF-spesifikaation versiossa 1.0 määritetään verkon siirtonopeuksiksi 0,8 Mbps ja 1,6 Mbps. Kantamaa luvataan noin 50 metriä, minkä pitäisi riittää tyypilliseen koti- ja toimistoympäristöön.

HomeRF-verkko voi noudattaa kahta eri topologiaa. *Ad hoc* -topologiassa verkkoon liittyneet päätelaitteet ovat tasa-arvoisia ja hallitsevat yhdessä hajautetusti verkkoa. Vain asynkroniset yhteydet ovat mahdollisia. Hallinnoidussa verkossa verkon isäntänä toimii yhteyspiste (*Connection Point, CP*), johon päätelaitteet kiinnittyvät. Yhteyspiste tarjoaa pääsyn yleiseen puhelinverkkoon, joten esimerkiksi kodin pu-

helimet voidaan liittää HomeRF-verkkoon. Kummassakin topologiassa verkkoon voidaan liittää maksimissaan 127 laitetta. Yhteydet ulkopuolisiin dataverkkoihin joudutaan järjestämään puhelinverkkoon liitettyjen modeemien avulla, mikä rajoittaa verkotekniikan sovellettavuutta melkoisesti. Spesifikaatiossa ei myöskään määritellä tapaa, jolla päätelaitteet voisivat vaihtaa yhteyspistettä menettämättä verkkoyhteyttä. Verkossa käytetään 56-bitin salaustekniikkaa, jota pidetään nykyään turvalliseen tietoliikenteeseen riittämättömänä. HomeRF:n protokollapino muistuttaa langattoman paikallisverkon pinoa. Kummassakin määritellään omat MAC- ja fyysisen tason protokollat. Yhteensopivuus WLAN:n kanssa taataan kuitenkin vain TCP/IP-tasolla. [Held2001]

HomeRF-tekniikka on etenemässä versioon 2.0, jossa esitellään lukuisia parannuksia vanhaan konseptiin nähden. Uudessa versiossa verkon siirtonopeus on 10 Mbps. Ulkoisiin tietoverkkoihin on mahdollista saada suora liityntä ilman puhelinverkkoa, mikä mahdollistaa nopeat yhteydet. Salaukseen käytetään vahvaa 128-bittistä tekniikkaa. Päätelaitteiden on mahdollista liikkua yhteyspisteiden muodostamien solujen välillä. [Home2000]

HomeRF-tekniikka mahdollistaa PAN-verkkojen *ad hoc* -toiminnallisuuden, jossa kaksi päätelaitetta voi itsenäisesti muodostaa langattoman verkon. Verkon liikenne muodostuu tällöin kuitenkin vain asynkronisista yhteyksistä. Synkronisia yhteyksiä ei ole mahdollista käyttää suoraan, vaan niitä pitää emuloida asynkronisen yhteyden päällä. Koska HomeRF perustuu osittain WLAN-konseptiin, ei siinä ole sisäänrakennettua toiminnallisuutta uusien laitteiden tai palveluiden etsimiseen. Tekniikalla voidaan siis toteuttaa vain osajoukko PAN-verkon toiminnallisuudesta.

### 5.3.3 HIPERLAN

HIPERLAN (*High Performance European Radio Local Area Network*) on ETSI:n kehittämä standardiperhe suorituskykyisille radioverkoille. Perheeseen kuuluu neljä verkkotyyppiä, joista käytetään nimiä HIPERLAN/1, HIPERLAN/2, HIPERACCESS ja HIPERLINK [ETSI2001]. Tyyppien käyttöön on varattu taajuuksia alueilta 5,15-5,25 GHz ja 17,1-17,3 GHz.

HIPERLAN/1 on standardiperheen esikoinen: se valmistui vuonna 1996. Se toimii 5,2 gigahertsin taajuusalueella, tiedonsiirtokapasiteettia on 20 Mbps ja kantamaa noin 50 metriä. Kyseessä on langaton paikallisverkkotekniikka, joka ei tarvitse

kiinteää infrastruktuuria. Radiotien jakamisesta verkon laitteiden kesken huolehtii erityinen CAC-protokolla (*Channel Access Control*), joka sijoittuu fyysisen ja MAC-kerroksen väliin. CAC tarjoaa priorisoidun siirtomedian, minkä ansiosta verkossa voidaan kuljettaa myös synkronista informaatiota. Päätelaitteet muodostavat verkkoja ilman keskitettyä verkonhallintaa. Verkon kantamaa voidaan kasvattaa käyttämällä päätelaitteita viestien toistajina, jolloin myös toistensa kantamattomissa olevat laitteet voivat keskustella keskenään. HIPERLAN/1-verkko on siis suorituskykyinen ja kooltaan joustava.

HIPERLAN/2 on verkkotekniikka, joka on suunniteltu toimimaan kiinteän infrastruktuurin kanssa. Tekniikka hyödyntää 5,2 gigahertsin taajuusaluetta ja sen tiedonsiirtonopeus on maksimissaan 54 Mbps. Sitä käytetään langattomana pääsyverkkona kiinteisiin, kuten IP-, ATM<sup>19</sup>- ja UMTS<sup>20</sup>-verkkoihin. Verkon rakenne on pääpiirteissään samanlainen kuin kuvassa 5.5 esitetyllä langattomalla paikallisverkkolla. Verkossa voidaan käyttää sekä kahden- että monenvälisiä yhteyksiä.

HIPERACCESS on HIPERLAN/2:n variaatio, joka tarjoaa ulkotiloissa viiden kilometrin kantaman 25 Mbps:n siirtonopeudella. Tekniikka toimii siis pitkän kantaman langattomana pääsyverkkona. HIPERACCESS käyttää 5,2 gigahertsin taajuusaluetta.

HIPERLINK on suurinopeuksisia informaatiolähteitä, esimerkiksi muita HIPERLAN-verkkoja, yhdistävä 17 gigahertsin alueella toimiva tekniikka. Sen tiedonsiirtonopeus on 155 Mbps, joka on ATM:n perusnopeus. Kantama on maksimissaan 150 metriä.

Edellä esitellyistä standardeista HIPERLAN/1 soveltuu periaatteellisella tasolla parhaiten PAN-verkkoon. Tekniikka mahdollistaa tarvetta varten muodostettavat verkot, vieläpä huomattavalla tiedonsiirtokapasiteetilla. Puhesovellukset ovat myös toteutettavissa, koska synkronisia yhteyksiä tuetaan protokollatasolla. Päätelaitteiden toteuttamisen kannalta arvokkaita ovat myös tekniikan virransäästöominaisuudet, joita käyttämällä lähetin-vastaanottimen päälläoloaika voidaan minimoida. Ongelmaksi muodostuu kuitenkin se, että HIPERLAN-standardit spesifioivat vain kaksi OSI-mallin alinta kerrosta. Valmistajat, jotka eivät todennäköisesti ryhdy laajamittaiseen yhteistyöhön, saavat toteuttaa kaiken verkkokerroksesta ylöspäin oman harkintansa mu-

---

<sup>19</sup> Asynchronous Transfer Mode. Tekniikka laajakaistaisille monipalveluverkoille [GrMi1998].

<sup>20</sup> Universal Mobile Telecommunications System. 3. sukupolven matkapuhelinverkko.

kaan. Standardeissa ei myöskään oteta kantaa siihen, voivatko HIPERLAN-laitteet löytää toisensa automaattisesti ilman käyttäjän apua. Koska standardin toteuttavista tuotteista ei vielä ole laajaa valikoimaa, on mahdotonta arvioida, kuinka erilaisia eri valmistajien ratkaisut ovat. On kuitenkin todennäköistä, että kaikki valmistajat toteuttavat tuotteisiinsa IP-protokollan. Tämä raottaa ovea myös PAN-verkkojen suuntaan.

## 5.4 Yhteenveto

Tässä luvussa on esitelty langattomia lyhyen kantaman verkkotekniikoita ja pohdittu niiden sopivuutta PAN-verkon toteuttamiseen. Tekniikat ovat lähtökohdiltaan hyvin erilaisia: Bluetooth on suunniteltu PAN-verkkomaiseen kommunikaatioon, WLAN korvaamaan kiinteitä paikallisverkkoja ja IrDA kahdenväliseen tiedonsiirtoon. Tekniikoiden ominaisuudet ovat tästä huolimatta melko samankaltaiset, suurimmat erot ovat nähtävissä laitteiden etsimisen mahdollistavan palvelun ja synkronisten yhteyksien tukemisessa. Verkkotekniikoiden PAN-konseptiin liittyvät ominaisuudet on kerätty taulukkoon 5.2. Taulukosta voidaan nähdä, että Bluetooth soveltuu vertailluista tekniikoista parhaiten PAN-verkoksi. Sen ominaisuudet ovat kaikin puolin riittävät henkilökohtaiseen verkottumiseen, vaikkei tiedonsiirtonopeus olekaan useimpien kilpailijoiden veroinen.

Taulukko 5.2. Yhteenveto langattomista verkkotekniikoista.

Tekniikka	Bluetooth	WLAN	IrDA-D	HomeRF	HIPERLAN/1
<i>Menetelmä</i>	Radiotaajuus	Radiotaajuus	Infrapuna	Radiotaajuus	Radiotaajuus
<i>Nopeus (Mbps)</i>	0,7	11	4	1,6	20
<i>Kantama (m)</i>	10	50	2	50	50
<i>Laitteiden etsim.</i>	X		X		
<i>Ad hoc -toiminta</i>	X	X	X	X	X
<i>Yhteydet</i>					
<i>synkroninen</i>	X			X	X
<i>asynkroninen</i>	X	X	X	X	X
<i>kahdenväl.</i>	X	X	X	X	X
<i>monenväl.</i>	X	X		X	X
<i>IP-tuki</i>	X	X	X <sup>1</sup>	X	*
<i>Salaus (bittinä)</i>	128	40	0	56	*

\* Laittevalmistajan määriteltävissä.

<sup>1</sup> Ei suoraa protokollatukea.



## 6 Paikallisen WAP-palvelun toteutus Bluetoothilla

Kuten luvussa 5 todettiin, soveltuu Bluetooth arvioiduista verkkotekniikoista parhaiten PAN-verkon toteutukseen. Tekniikka täyttää asetetut periaatteelliset vaatimukset, mutta siinä on myös sovellusten rakentamista hankaloittavia piirteitä. Tässä luvussa pohditaan, miten paikallinen WAP-palvelu voidaan toteuttaa Bluetooth-tekniikan avulla.

### 6.1 WAP:n ja Bluetoothin väliset liittymät

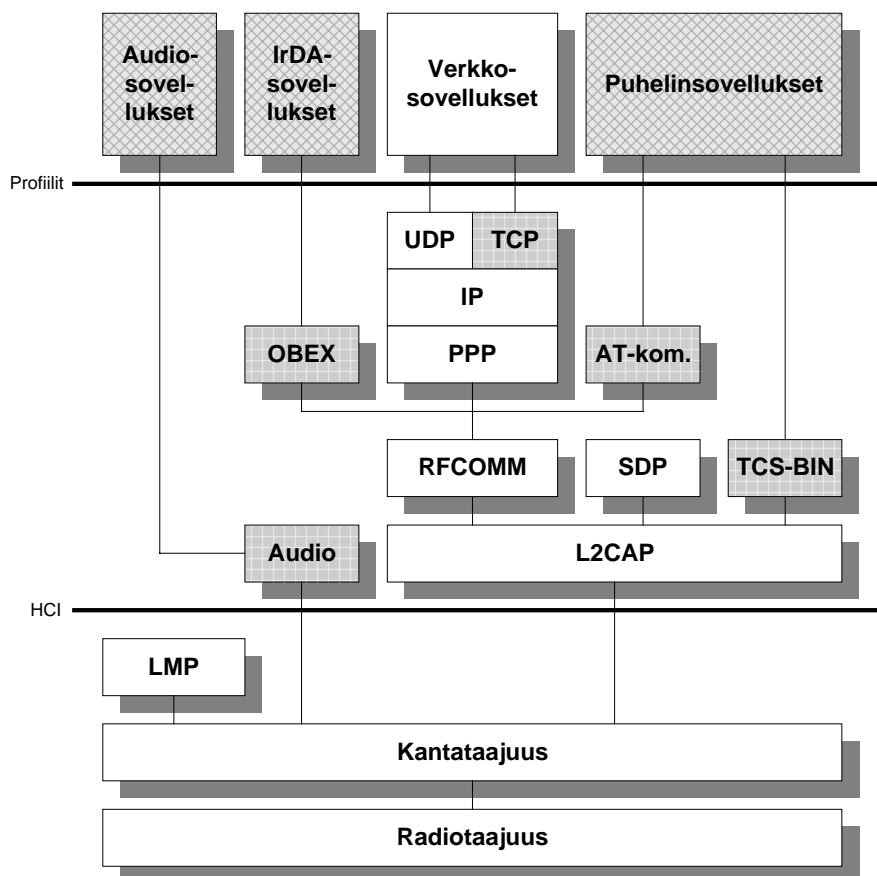
WAP-sovellukset liittyvät Bluetooth-järjestelmään profiilien välityksellä. Jokainen profiili tarjoaa tietyt perusominaisuudet, jotka periytyvät yhteisestä kantaisästä, yleisestä pääsyprofiilista. SDP-palvelut, yhteyksien muodostamisen mekanismit sekä pääsyparametrien hallinta ovat näin yhtäläisesti ja automaattisesti kaikkien sovellusten käytettävissä. Jotta sovelluksen ja Bluetoothin liittynästä tulisi mahdollisimman saumaton, on käytettävän profiilin lisäksi tuettava sovellukselle ominaisia tietoliikenne-eratkaisuja ja -rajapintoja. Vaikka olemassaolevilla profiileilla voidaan toteuttaa suurin osa erilaisista sovellustyypeistä, on valikoimassa kuitenkin vielä aukkoja, joita tulevat Bluetooth-versiot toivottavasti korjaavat.

WAP-protokollapino kiinnittyy allaolevan verkkotekniikan kuljetusprotokollaan. Bluetooth tarjoaa tuen yleisesti Internetissä käytetyille TCP- ja UDP-protokollille. WAP:ssa näistä kahdesta voidaan hyödyntää vain UDP:ta, koska WTP-protokolla tarjoaa TCP:tä vastaavan yhteydellisen, luotettavan tiedonsiirtopalvelun. UDP:n ja WTP:n välinen rajapinta on siis Bluetooth- ja WAP-järjestelmien rajapyykki, jota hallinnoi käytetty profiili. UDP-protokolla reitittää lävitseen kulkevan informaation porttinumeroiden perusteella. Kullekin sovellusprotokollalle on määriteltä kiinteä numero, jota käyttämällä identifioidaan sille kuuluva liikenne. Myös WAP-sovelluksille on varattu omat numeronsa, joiden perusteella Bluetooth-pinon läpi kulkeva informaatio löytää vastaavan WAP-sovellusagentin. UDP:n hyviin puoliin kuuluu myös toteutuksen keveys, mikä on heikkotehoisessa päätelaitteessa merkittävä etu.

Sisältöä kuljettavan verkkotekniikan eli Bluetoothin on informoitava WAP-sovellusta päätelaitteen ja sen ympäristön tilassa tapahtuneista muutoksista. Käytännössä muutokset liittyvät toisten WAP-laitteiden lähestymiseen ja loitontumiseen sekä palvelinten työntämän informaation vastaanottamiseen. Kaikki nämä ilmoitukset ovat

saatavilla käytettävän profiilin kautta. Sovellus voi pysytellä tietoisena muiden WAP-laitteiden olemassaolosta suorittamalla ajoittain yleisen pääsyprofiilin etsintäoperaation. Palvelimelta tuleva sisällön työntö taas näkyy sovellukselle yhteyspyyntönä. Päätelaitteen WAP-arkkitehtuurin toteuttavan ohjelmiston on siis tukeuduttava profiilien palveluihin hallinnoidessaan transaktioiden kulkua ja käytettävissä olevista laitteista informointia.

Paikallisverkkoprofiili (*LAN Access Profile, LAP*) on tällä hetkellä ainoa spesifioitu profiili, joka soveltuu edellä kuvatun kaltaiseen WAP:n ja Bluetoothin yhdistämiseen. Se tarjoaa IP- ja samalla siis myös UDP-protokollatuen. IP-paketteja kuljettaa PPP-protokolla, joka on tähän tarkoitukseen luonteva valinta. Profiilin spesifioinnin aikoihin kahdenvälisen, langattoman *ad-hoc* -yhteyden toteuttamiseen liittyi mo-



Kuva 6.1. Paikallisverkkoprofiilin käyttämät protokollat ja palvelut.

nia ratkaisemattomia ongelmia, kuten *DNS*<sup>21</sup>- ja *DHCP*<sup>22</sup>-palveluiden tarjoaminen. PPP on sen sijaan laajasti Internetissä käytetty liityntäprotokolla, jonka päällä voidaan tehdä normaaliin IP-liikenteeseen kuuluvia konfigurointioperaatioita. Bluetooth-järjestelmässä PPP on toteutettu sarjaliityntäprotokolla RFCOMM:n päälle, kuten kaikki muutkin tiedonsiirtoa tarjoavat palvelut. Kuvassa 6.1 voidaan nähdä profiilissa käytetyt protokollat ja palvelut valkoisella pohjalla. Samalla huomataan profiileihin yleisesti pätevä ominaisuus: profiili lohkaisee protokollapinosta pystysuoran leikkauksen. [MiBi2001]

Myöhemmissä Bluetooth-spesifikaatioissa tulee olemaan mukana yleisen ad hoc -verkottumisen tarjoava profiili, joka kulkee työnimellä *Personal Area Networking (PAN)*. Sitä kehittää työryhmä, jota johtavat Microsoft ja Intel. Profiilissa tarjotaan IP-protokollaan perustuva sovellusrajapinta, jossa edellä esitellyt konfigurointiongelmat on ratkaistu. Keinotekoisia ratkaisuja, kuten PPP:n käyttöä, ei näin ollen tarvita. Profiili tulee tukemaan muun muassa täydellistä PAN-toiminnallisuutta ja WAP-protokollaa, mutta se tullaan näkemään vasta spesifikaatioversiossa 2.0, jota odotetaan julkaistavaksi vuoden 2001 loppupuolella. Monille WAP-kehittäjille tämä aikataulu ei riitä, joten heidän on yritettävä pärjätä olemassaolevalla profiilivalikoimalla. PAN-profiilia ei käsitellä tässä luvussa tarkemmin, koska keskeneräisiä spesifikaatioita ei ole julkisesti saatavilla.

## 6.2 Laitteisiin kohdistuvat vaatimukset ja rajoitteet

Paikallisten WAP-palveluiden tarjoamiseen ja käyttämiseen tarvittavat laitteet eivät juurikaan eroa tavallisten WAP-palveluiden vastaavista. Ainoa käytännössä merkitsevä eroavaisuus laitteiden välillä on verkkosovitin käytettävään lyhyen kantaman kommunikaatiomenetelmään eli tässä tapauksessa Bluetoothiin.

### 6.2.1 Asiakaslaite

Paikallisten WAP-palveluiden asiakaslaite on tyypillisen WAP-päätelaitteen kaltainen. Laite on kädessäpidettävä ja kevyt. Siinä on kämmentä pienempi mustavalko- tai

---

<sup>21</sup> Domain Name System. Mekanismi IP-osoitteiden muuntamiseen [Tane1996].

<sup>22</sup> Dynamic Host Configuration Protocol. Protokolla IP-osoitteen dynaamiseen hankintaan.

värinäyttö, joka on taustavalaistu, jotta laitetta voidaan käyttää myös hämärässä. Syöttölaitteena toimii näppäimistö, kynä, kosketusnäyttö tai puhe. Laitteen energiansaannista huolehtivat akut tai paristot, jolloin ei tarvita virtajohtoja. Käyttäjälle on varattu pieni määrä muistia, johon voi tallettaa esimerkiksi kontaktitietoja ja suosikkisivuja. Käyttöjärjestelmä on tyypillisesti laitteeseen räätälöity ja reaaliaikainen.

Asiakaslaite tarvitsee WAP-asiakasohjelmiston: protokollapinototeutuksen ja tyypilliset sovellusagentit kuten WML-selaimen. Jos laitteen halutaan tukevan palvelimelta tulevaa työntöä, on ohjelmiston oltava yhteensopiva WAP-version 1.2 kanssa. Jotta yhteys WAP-palvelimeen voitaisiin avata, tarvitaan Bluetooth-moduuli. Moduuli on integroitu piiri, joka sisältää kaiken kommunikaatioon tarvittavan laitteiston: lähetin-vastaanottimen, antennin, ohjauslogiikan ja liittymän isäntälaitteeseen. Moduulin ohella laitteessa on oltava HCI-rajapinnan, välikerrosprotokollien ja WAP-liikenteeseen käytettävän profiilin ohjelmistototeutukset.

WAP-protokolla pystyy tehokkaasti lieventämään päätelaitteiden rajoitteita. Paikallista palvelua ei näin ollen tarvitse erityisesti räätälöidä päätelaitteille, koska esimerkiksi näytön ja syöttölaitteiden rajoitteet on huomioitu jo sovellusarkkitehtuurissa. Paikallista WAP-palvelua voi siis mainiosti käyttää normaalin WAP-puhelimen kaltaisella laitteella, kunhan siinä on Bluetooth-sovitin.

### **6.2.2 Palvelin**

Paikalliseksi WAP-palvelimeksi riittää tehokas työasema, koska palveltavia asiakkaita ei tavallisesti ole muutamaa kymmentä enempää. Aseman varustukseen kuuluu runsaasti käyttö- ja massamuistia, jotta palvelu saadaan mahdollisimman nopeaksi, stabiiliksi ja laajaksi. Mikäli puhutaan ns. siirrettävästä palvelimesta, on laitteisto syytä sijoittaa tehokkaaseen kannettavaan tietokoneeseen. Palvelimen käyttöjärjestelmän on oltava moniajava, yleisesti tuettu ja erittäin vakaa, jotta palvelu voi toimia katkoksitta. Kiinteää yhteyttä Internetiin ei välttämättä tarvita, ellei jokin tarjottava palvelu sitä edellytä.

Paikallinen palvelin sisältää tyypillisesti sekä yhdyskäytävä- että WAP-palvelimen. Kummallekin palvelimelle on oma ohjelmistonsa, jotka käyttävät keskinäiseen keskusteluun ulkoisen verkkoyhteyden sijaan palvelimen muistia. Mikäli palveluissa halutaan käyttää työntöominaisuutta, on ohjelmistojen oltava yhteensopivia WAP-ver-

sion 1.2 kanssa. Palvelinohjelmistojen on oltava sekä stabiileja että helposti ylläpidettäviä ja päivitettäviä.

Palvelin tarvitsee vähintään yhden Bluetooth-sovittimen. Sovittimien tarkka määrä riippuu palveltavien asiakkaiden määrästä, yksi sovitin pystyy käsittelemään muutaman kymmenen asiakkaan WAP-selaukseen tarvittavan tietoliikenteen. Sovitin käyttää asiakkaiden kanssa kommunikointiin kahdenvälisiä yhteyksiä, joita voi olla yhtäaikaaisesti muutamia. Yhteydet kestävät tavallisesti yhden WML-pakan siirtämiseen kuluvan ajan eli yhteydenmuodostuksineen muutaman sekunnin. Myös palvelin tarvitsee HCI-rajapinnan sekä välikerrosprotokollien ja WAP:n kuljettamiseen käytettävän profiilin ohjelmistototeutukset.

Paikallinen palvelin toimii loogisesti kuten yhdyskäytävä- ja WAP-palvelimen yhdistelmä. Toimintaa rajoittavaksi tekijäksi voi muodostua Bluetooth-sovitinten kautta avautuva radorajapinta silloin, kun asiakkaita on kapasiteettiin nähden liikaa. Ruuhkautumista ja tukkeutumista voi esiintyä, ellei asiakkaiden määrää rajoiteta sellaiselle tasolle, jolla keskinäiset häiriöt pysyvät kohtuullisella tasolla. Sovittimien laadulla ja HCI-rajapinnan toteutusyksityiskohdilla on myös vaikutusta tähän asiaan.

Paikallisen palvelimen ei ole pakko muistuttaa työasemaa. Maaliskuussa 2001 Ericsson julkisti BLIP-laiteperheen (*Bluetooth Local Infotainment Point*), jonka jäsenet ovat Bluetooth-valmiudella varustettuja paikallisen WAP- ja seittipalvelimen yhdistelmiä. BLIP-laitteet ovat kämmenenkokoisia keskittimiä, joissa ajetaan *Linux*-käyttöjärjestelmää ja jotka voivat kiinnittyä paikallisverkkoon. Laitteisiin voidaan asentaa kolmansien osapuolien tekemiä ohjelmistoja ja sivuja, joita asiakkaat voivat käyttää Bluetooth-yhteyden välityksellä. BLIP:stä saattaa tulla ensimmäinen merkittävä paikallisia WAP-palveluita hyödyntävä tuote.

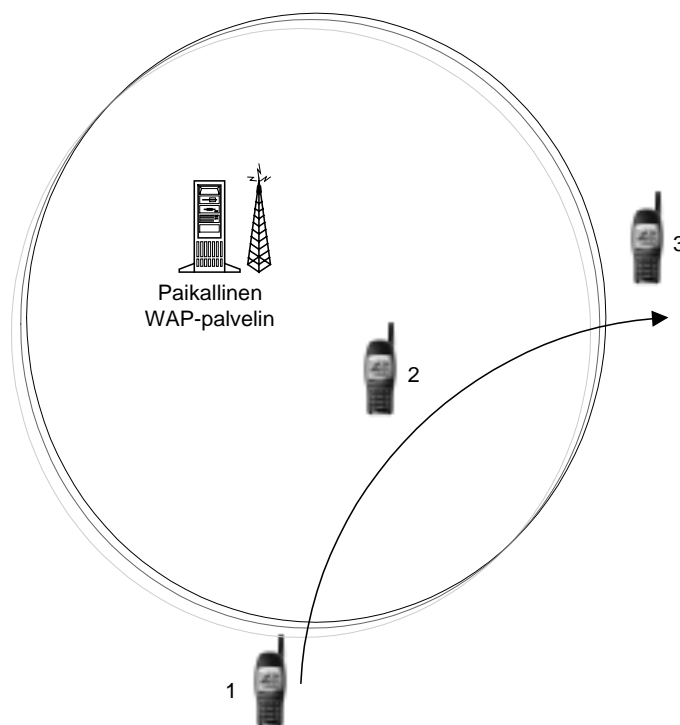
Tulevaisuuden visioissa paikallinen WAP-palvelin kutistuu huomattavan pieneksi, esimerkiksi napin kokoiseksi, itsenäiseksi, paristolla toimivaksi kokonaisuudeksi, johon on integroitu laitteisto, ohjelmisto ja kiinteä WAP-sisältö. Yksikään valmistaja ei ole vielä julkistanut tällaista sulautettua palvelinta, vaikka tekniset valmiudet sen tekemiseen alkavat jo olla olemassa.

### **6.3 WAP-istunnon kulku**

Paikallisen WAP-palvelun istunto ei ole loogisesti samanlainen kuin tavallisen WAP-palvelun istunto. Asiakas voi kiinnittyä tavalliseen palveluun missä tahansa operaatto-

rin verkon alueella. Paikalliseen palveluun ei sen sijaan voi kiinnittyä, ellei ole palvelun kantaman eli palvelimen Bluetooth-sovittimen kantoalueen sisällä. Istunnon kulku noudattaa kuvassa 6.2 esitettyä mallia, jonka ensimmäinen vaihe on päätelaitteen saapuminen palvelun kantaman sisälle, toinen vaihe palvelun varsinainen käyttäminen ja kolmas vaihe poistuminen palvelun alueelta.

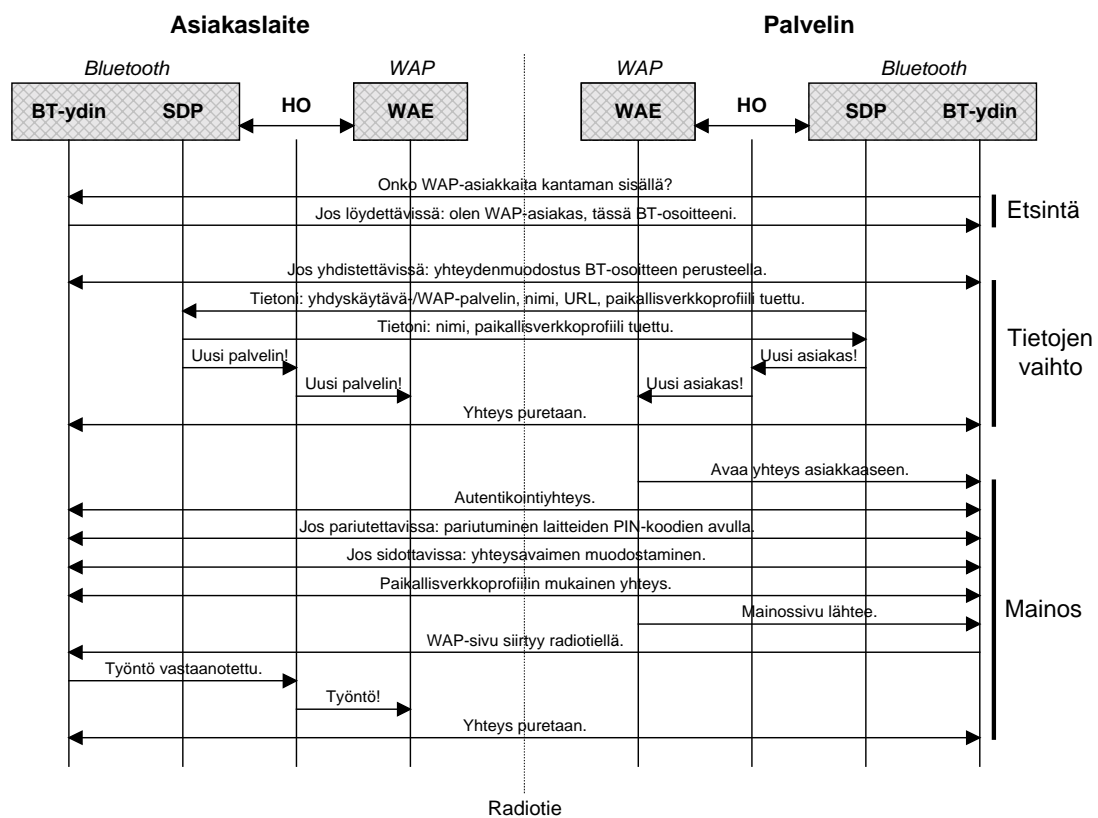
Istunnon kulussa ei ole WAP-protokollien kannalta mitään epänormaalia: ensimmäisessä vaiheessa laite saapuu verkon peittoalueelle ja kolmannessa vaiheessa verkko ei ole enää käytettävissä. Protokollat on suunniteltu toimimaan vastaavissa tilanteissa esimerkiksi GSM-verkon kanssa. WAP-spesifikaatioissa määritellään WDP-hallintaolio (*WDP Management Entity*), joka informoi WAP-pinoa kuljettavan verkkotekniikan tilassa tapahtuneista muutoksista [WAPF1999b]. Koska WAP-over-Bluetooth -järjestelmässä ei käytetä WDP-protokollaa, kutsutaan asynkronisia notifiikaatioita välittävää oliota yksinkertaisesti hallintaolioksi. Sen tehtävä on täysin sama kuin WDP-hallintaolion. Oliota voidaan käyttää myös parametrien, esimerkiksi laitteen osoitteen, asettamiseen WAP-tasolta verkkotasolle. Olio räätälöidään kutakin verkkotekniikkaa varten.



*Kuva 6.2. Paikallisen WAP-istunnon kulku.*

Seuraavassa käydään läpi kuvassa 6.2 esitetyn istunnon vaiheet. Tarkastelussa oletetaan, että paikallinen WAP-palvelu on kaiken aikaa toimintakuntoinen ja vapaa palvelemaan päätelaitteita. Kaavioissa esiintyvällä lyhenteellä HO tarkoitetaan hallintaoliota.

**Saapuminen paikallisen WAP-palvelimen kantaman sisälle (1).** Ensimmäistä vaihetta kuvaava tapahtumasekvenssikaavio on esitetty kuvassa 6.3. Palvelin suorittaa säännöllisesti Bluetoothin kantataajuusosan etsintäoperaation (*inquiry*), jolla se yrittää löytää kantamansa sisällä olevat WAP-asiakaslaitteet. Operaatio on käytettävissä yleisessä pääsyprofiilissa. Jos asiakas on kantoalueella ja pääsyparametrit sallivat laitteen löytämisen, huomaa palvelin asiakkaan. Palvelin etsii nimenomaan WAP-asiakkaita, jotta muut Bluetooth-laitteet eivät vastaisi kyselyyn ja aiheuttaisi tarpeetonta tietoliikennettä. Palvelin saa tietoonsa etsintäprosessin aikana asiakkaan Bluetooth-osoitteen ja synkronointiin tarvittavan informaation.



Kuva 6.3. Päätelaitteen saapuminen palvelun kantaman sisälle.

Saatuun asiakkaan osoitteen palvelin yrittää avata yhteyden. Jos asiakkaan pääsparametrit eivät tätä estä, muodostuu yhteys, jota laitteiden SDP-protokollaoliot hyödyntävät tietojen vaihtamiseen. Palvelin kertoo olevansa palvelutyypiltään yhdyskäytävä-/WAP-palvelin sekä antaa tekstuaalisen nimensä ja WAP-osoitteensa (*URL*<sup>23</sup>). Asiakas luokittelee itsensä WAP-asiakkaaksi ja palauttaa tekstuaalisen nimensä. Laitteet sopivat myös käytettävästä profiilista, joka on siis paikallisverkkoprofiili, ja tarkistavat profiilitoteutustensa versionumerot. Hallintaoliot informoivat osapuolten WAP-pinoja löydetystä päätelaitteesta. Kun tarvittava keskustelu on käyty, purkautuu yhteys laitteiden väliltä.

Hallintaoliolta tuleva ilmoitus voidaan käsitellä asiakaslaitteessa monin eri tavoin. Laitteen näytöllä voidaan esimerkiksi esittää viesti paikallisen WAP-palvelimen ilmestymisestä, palvelimen tekstuaalista tunnistetta voidaan käyttää identifioivana tekijänä (esimerkiksi *“Uusi paikallinen WAP-palvelu löydetty: Hämeenkadun infopiste”*). Ilmoitus voidaan käsitellä myös hiljaisesti, jolloin käyttäjää ei informoida tapahtumasta. Tieto palvelusta kuitenkin talletetaan siltä varalta, että käyttäjä haluaa myöhemmin listan käytettävissä olevista palveluista.

Saatuun asiakkaan tiedot palvelin voi mainostaa palveluitaan. Se voi lähettää WAP:n työntöominaisuutta käyttäen asiakaslaitteeseen esimerkiksi etusivunsa. Palvelin pyytää yhteyden muodostamista, jolloin yhteyspyyntö laskeutuu Bluetooth-pinon kantataajuusosaan, jossa alkaa asiakaslaitteen haku. Asiakas vastaa hakuun ja yhteysosapuolet rakentavat pikoverkon. Palvelimesta tulee verkon isäntä ja asiakkaasta renki. Palvelimen LMP-protokolla pyytää autentikointikanavan avaamista asiakkaalle, jota seuraa laitteiden autentikoinnin suorittava pariutumisosprosessi (*pairing*). Autentikointi tapahtuu laitteisiin talletettujen PIN-koodien (*Personal Identification Number*) avulla [MiBi2001]. Koodien perusteella generoidaan alustusavain, jolla varsinainen autentikointiproseduuri suoritetaan. PIN-koodeja ei näin ollen lähetetä lainkaan toiselle laitteelle. Kun autentikointi on läpäisty menestyksellisesti, ehdottaa palvelin laitteiden sitomista (*bonding*). Sitominen nopeuttaa jatkossa laitteiden välistä yhteydenmuodostusta, koska normaalia pariutumisosprosessia ja avainten generointia ei tarvita. Kumpaankin sitoutuneeseen laitteeseen talletetaan yhteysavain (*link key*), jolla osapuolet voivat myöhemmin tunnistaa toisensa. Asiakaslaite voi kuitenkin kieltäytyä sitoutumisesta, mikäli sen pääsparametrit eivät ole sopivat. Kun asiasta on saavutettu

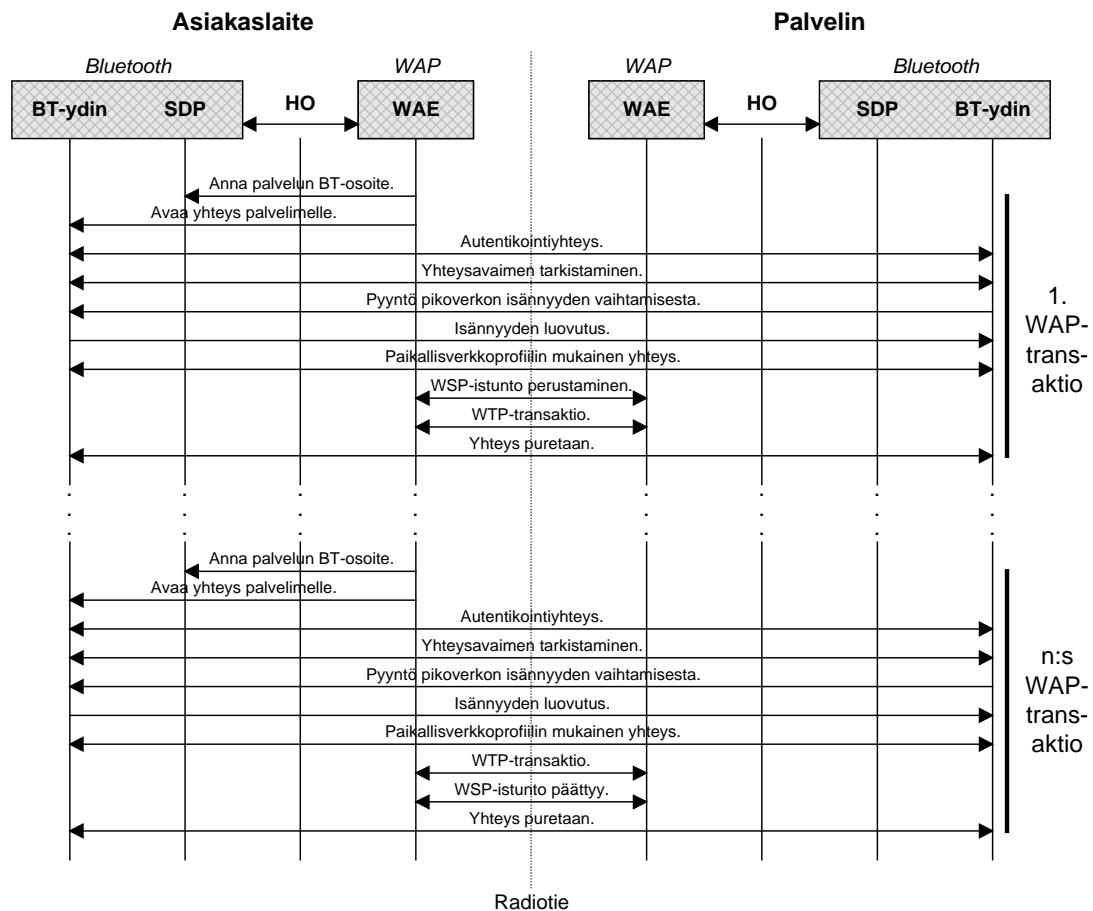
---

<sup>23</sup> Universal Resource Locator. Internetissä käytettävä tiedostojen tunniste.



yksimielisyys, avataan laitteiden välille ACL-yhteys, jonka päällä lähetetään paikallisverkkoprofiilin mukaista protokollainformaatiota. Palvelin palauttaa oletusistuntoa käyttäen haluamansa WAP-sivun. Oletusistunto on aina olemassa, joten sitä ei tarvitse erikseen avata. Se on sopiva mainostosoperaatioon, koska operaatiossa tapahtuu tavallisesti vain yksi transaktio. WAP-protokollat saavat tiedon saapuneesta sivusta hallintaolion toimesta. Sivun välitetään WML-sovellusagentille, joka esittää sen laitteen näytöllä käyttäjälle, ja tämän jälkeen yhteys puretaan.

**Kytkeytyminen paikalliseen WAP-palvelimeen (2).** Kun asiakaslaite on paikallisen palvelun kantaman sisällä, voidaan uusi WAP-istunto aloittaa käyttäjän pyynnöstä. Palvelun käytön tapahtumasekvenssikaavio on esitetty kuvassa 6.4. Palvelimen tiedot on talletettu SDP-tietokantaan ensimmäisen vaiheen aikana. Palvelinta haetaan



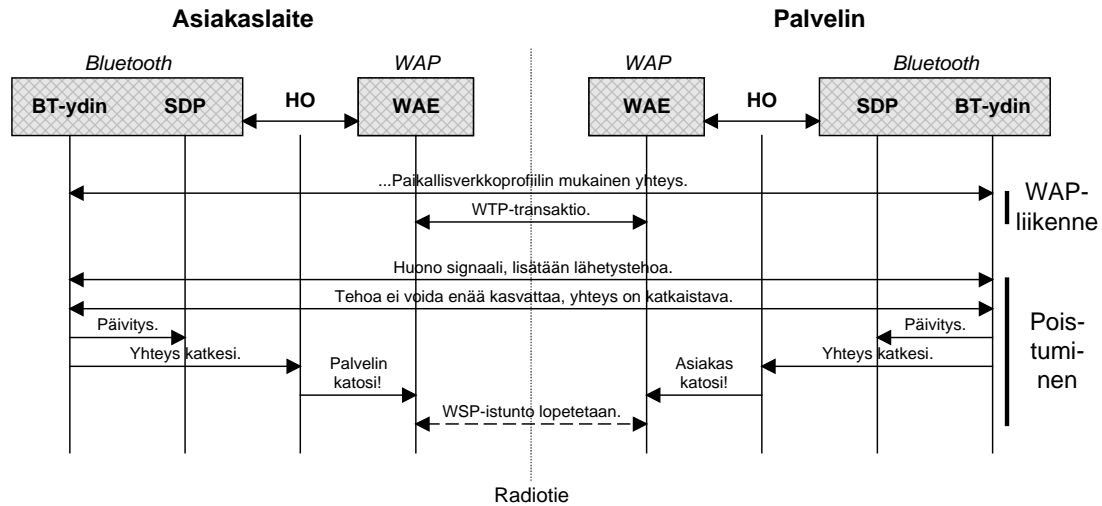
Kuva 6.4. Palvelun käyttäminen.

sen Bluetooth-osoitteella, minkä jälkeen seuraa autentikointiproseduuri. Mikäli laitteet sitoutuivat ensimmäisessä vaiheessa, voidaan autentikointi hoitaa yhteysavaimen tarkistamiseen liittyvällä haastetehtävällä (*challenge*). Jos yhteysavainta ei ole, voivat laitteet pariuutua edellä kuvatulla tavalla. Asiakaslaitteesta tulee muodostuneen piko-verkon isäntä, koska se aloitti kommunikaation. Palvelimen kannalta tämä on huono ratkaisu, koska palvelukseen useita asiakkaita sen on pystyttävä hallinnoimaan piko-verkkoa. Palvelin pyytää näin ollen asiakaslaitetta luovuttamaan verkon isännöyden sille. Asiakaslaitteella ei ole yleensä perusteita kieltäytyä pyynnöstä. Kun käytetyn profiilin mukainen yhteys on muodostettu, syntyy asiakkaan ja palvelimen välille WSP-istunto [WAPF1999c]. Asiakaslaitteella pyytää palvelimelta joko aloitussivua tai käyttäjän määrittämää sivua. Sivu siirretään palvelimelta radiotien kautta asiakaslaitteelle, jossa se näytetään käyttäjälle WML-sovellusagentin toimesta. Kun pyyntö on käsitelty, katkaistaan laitteiden välinen yhteys; istunto sen sijaan jää päälle.

Yhteyden katkaisemista transaktioiden välillä voidaan perustella sekä virran-että verkon kapasiteetin säästöllä. Koska käyttäjän pyynnöt saapuvat laitteen kannalta harvoin, esimerkiksi 10 sekunnin välein, ei yhteyttä kannata jättää tyhjäkäynnille. Yhteydenmuodostusviive ei muodostu häiritseväksi, koska laitteet ovat sitoutuneet toisiinsa ja pystyvät palauttamaan yhteyden nopeasti. Istunto lopetetaan joko käyttäjän tai palvelimen pyynnöstä. Kun viimeinen transaktio on suoritettu, lopettavat osapuolten WSP-protokollaoliot yhteistyön ja laitteiden välinen yhteys purkautuu.

**Poistuminen paikallisen WAP-palvelimen kantaman sisältä (3).** Kun asiakaslaitteen ja palvelimen välinen etäisyys kasvaa riittävän suureksi, ei palvelun käyttäminen ole enää mahdollista. Vaihetta kuvaava tapahtumasekvenssikaavio on esitetty kuvassa 6.5. LMP-protokolla tarkkailee palvelimen ja asiakkaan välisen yhteyden laatua transaktio aikana. Mikäli signaali heikkenee, voidaan lähetystehoa nostaa tiettyyn rajaan asti yhteisellä sopimuksella. Kun tehoa ei enää voida nostaa, on yhteys pakko katkaista. Osapuolten SDP-tietokannat päivitetään ja viittaukset kadonneeseen laitteeseen poistetaan. WAP-protokollat saavat tiedon asiasta hallintaolion kautta ja WSP-istunto lopetetaan. Käyttäjää tiedotetaan tilanteesta. Laitteiden sitomisessa syntynyt yhteysavain säilytetään siltä varalta, että asiakas palaa myöhemmin käyttämään samaa palvelua.

Mikäli palvelimen ja asiakkaan välillä ei ole aktiivista istuntoa, ei asiakaslaitteen katoamista voida huomata yhtä nopeasti. Palvelimen tekemä säännöllinen etsintä-



Kuva 6.5. Poistuminen palvelun alueelta.

operaatio paljastaa kuitenkin puuttuvat asiakkaat ennen pitkää. Kun asiakaslaite ei enää ilmoittaudu käytettäväksi, on se liikkunut kantaman ulkopuolelle ja sen tiedot voidaan poistaa SDP-tietokannasta.

## 6.4 Useiden asiakkaiden palveleminen

Paikallinen WAP-palvelin ei tavallisesti voi rajoittua palvelemaan vain yhtä asiakasta kerrallaan. Ruuhkatilanteessa palveluun voi olla kiinnittyneinä useita kymmeniä asiakkaita. Pikoverkon konfiguraatio ja palvelimen suorituskyky joutuvat silloin koe- tukselle.

Palvelin muodostaa yhden ACL-tyyppisen yhteyden kuhunkin asiakaslaittee- seen. Asiakkaat toimivat pikoverkossa renkeinä, palvelin itse isäntänä. Pienikokoisel- le palvelulle riittää yksi Bluetooth-sovitin, joka tarjoaa pääsyn maksimissaan seitse- mälle yhtäaikaiselle asiakkaalle. Asiakkaiden todellinen maksimimäärä on kuitenkin paljon suurempi, koska yksittäiseltä asiakkaalta saapuu pyyntöjä melko verkkaiseen tahtiin. Käyttäjät eivät myöskään närkästy sekunnin tai kahden viipeestä palveluun kiinnittymisessä. Yhden sovittimen kapasiteetin voidaan näin ollen arvioida olevan noin 20-30 asiakasta.

Mikäli asiakkaita on enemmän, on Bluetooth-sovittimien määrää väistämättä nostettava. Jokainen sovitin muodostaa oman pikoverkkonsa ja on sen isäntä. Verkot

menevät osittain päällekkäin, joten palvelu muodostaa kokonaisuutena hajaverkon. Tällöin palvelimen on mahdollista joutua tilanteeseen, jossa asiakas on kiinnittyneenä useampaan kuin yhteen sovittimeen. Jos WAP-päätelaite tukee useita yhtäaikaista yhteyksiä, on yhteyksien ehdottomasti kuuluttava eri istuntojen hallintaan, jotta eri yhteyksille kuuluvat paketit eivät menisi sekaisin. Yleisesti ottaen sekä palvelinohjelmiston että –laitteiston toteutus monimutkaistuu, mikäli on tuettava useita Bluetooth-sovittimia. Sovittimien hallitseminen ja niiden läpi kulkevan informaatiovirran käsittely on hankalaa ja vaatii erilaisia ratkaisuja. Periaatteellisena tavoitteena täytyy pitää myös sitä, että palvelun tulisi useista sovittimista huolimatta näkyä asiakaslaitteessa edelleen yhtenä palveluna, eikä palvelujoukkona.

## **6.5 Toteutusnäkökohtia**

WAP-over-Bluetoothiin toteuttamiseen liittyy suuri määrä pieniä pulmia, jotka täytyy ratkaista, ennenkuin järjestelmä on toimintakuntoinen. Seuraavissa alakohdissa käydään läpi muutamia ongelmia ja esitetään niihin ratkaisuja.

### **6.5.1 Asiakkaan tunnistaminen**

Yleisluontoisten, informaatiota jakavien paikallisten WAP-palvelujen ei ole tarkoituksenmukaista vaatia asiakkaan tarkkaa identifiointia, koska ideana on suoda tietoa kenelle tahansa. Yksityisiä tietoja tai rahaa käsittelevän palvelun on sen sijaan pystyttävä yksiselitteisesti tunnistamaan palvelua käyttävä henkilö.

Tunnistaminen voidaan yksinkertaisimmillaan toteuttaa päätelaitteen Bluetooth-osoitteen ja salasanan avulla. Järjestelmä vaatii käyttäjien rekisteröitymistä ennakolta, jotta käyttäjän henkilöllisyys voidaan todentaa ja laitteen osoite tallentaa. Kun päätelaite yrittää kytkeytyä paikalliseen WAP-palveluun, palvelin vastaanottaa päätelaitteen Bluetooth-osoitteen, joka on siis laitteille yksilöllinen tunniste. Palvelimen tietokannasta haetaan tunnistetta vastaava salasana, jota kysytään WML-pakan välityksellä käyttäjältä. Salasanan kysyminen on käyttäjän kannalta hieman kaksitahtoinen asia: toisia se voi ärsyttää, mutta käyttäjä saa konkreettisen, näkyvän varmistuksen tunnistusprosessista. Järjestelmä muistuttaa pankkiautomaateissa käytettävää tunnistusmekanismia ja sen avulla pystytään estämään varastetun päätelaitteen luvaton käyttö.

Mikäli palveluun kytkeydyttäessä pelkän päätelaitteen tunnistaminen riittää, on toteutusmahdollisuuksia monia. Kuten edellä mainittiin, laitteen Bluetooth-osoite takaa yksiselitteisen tunnistuksen. WTLS-protokolla tarjoaa lisäksi autentikoinnin sertifikaattien avulla. Sertifikaatti tallennetaan sekä asiakaslaitteeseen että palvelimeen ja laite voidaan tunnistaa sen avulla. Menetelmien ongelma on kuitenkin se, etteivät ne takaa, että päätelaitteen käyttäjä olisi laitteen laillinen omistaja.

Palvelun luonne määrää pitkälti tunnistamisen tarkkuuden. Anonyymeinä käytettävissä palveluissa tunnistamista ei tarvita lainkaan. Yleisluontoisissa palveluissa, joissa on esimerkiksi mahdollista tallettaa henkilökohtaisia asetuksia, riittää tavallisesti päätelaitteen tunnistus. Yksityistä sisältöä tai rahaa käsittelevissä palveluissa tunnistukseen on kiinnitettävä väärinkäytösten estämiseksi paljon huomiota.

### **6.5.2 WAP-sisällön salaus**

Palveluissa, joissa asiakkaan tunnistaminen on kriittinen tekijä, myös kuljetettavan informaation salaus on tarpeen. WAP-over-Bluetooth -järjestelmässä salaaminen voidaan suorittaa kahdella eri tasolla: Bluetoothin LMP- tai WAP:n WTLS-protokollan toimesta.

LMP-protokolla tarjoaa tehokkaan, yhteyskohtaisen salauksen, jonka parametrit neuvotellaan osapuolten autentikoinnin jälkeen. Salauksessa käytettävä avain määritetään pariutumisesä muodostetun yhteysavaimen perusteella. Salauksen vahvuus voidaan neuvotella sovelluksen tarpeita vastaavaksi; maksimivahvuus on 128 bittiä, jota pidetään yleisesti riittävän turvallisena kaikille sovelluksille.

WTLS-protokolla tarjoaa, kuten luvussa 2 todettiin, monipuoliset salausominaisuudet. Protokolla sisältää salatun tekstin lähetys- ja vastaanottopalvelun neljällä eri kryptograafisella operaatiolla, joita ovat digitaalinen allekirjoitus, tekstin ja tekstilohkon salaus sekä julkisen avaimen salaus.

Kumpikin protokolla tarjoaa riittävän tehokkaan salauksen WAP-sisällölle. LMP-protokollalla tehty salaus on kuitenkin suorituskyvyltään parempi, koska protokolla toteutetaan lähellä laitteistotasoa. LMP-salaus ei myöskään vaadi ylimääräisen protokollan lisäämistä järjestelmään, kuten WTLS tekee. Tämä on vartenotettava etu, kun otetaan huomioon WAP-over-Bluetooth -järjestelmän toteuttamiseen tarvittavien protokollien määrä.

### 6.5.3 Yhteydenmuodostusajan minimointi

Nykyisissä Bluetooth-järjestelmissä laitteiden välisen yhteydenmuodostuksen suurin yksittäinen viipeenaiheuttaja on etsintäoperaatio. Se muodostuu ongelmaksi varsinkin silloin, kun kahden laitteen välille halutaan yhteys heti, kun ne ovat saapuneet toistensa kantoalueille. Jos laitteet ovat olleet toistensa läheisyydessä riittävän kauan, ovat ne ehtineet huomata toistensa säännöllisesti tapahtuvien laite-etsintöjen avulla jo ennen varsinaista yhteyspyyntöä.

Etsintäoperaation pitkä kesto selittyy käytetyllä proseduurilla. Sekä etsivä että etsittävä laite käyvät läpi ns. etsintähypellysekvenssiä (*inquiry-hopping sequence*), joka on kiinteä 32 taajuuden sarja. Etsivä laite lähettää kullekin sekvenssin taajuudelle viestin ja odottaa hetken vastauksia. Vastauksia pitää tulla riittävä määrä, jotta etsivä laite voi varmistua toisten laitteiden läsnäolosta. Elleivät vastaukset tyydyttäneet etsijää, aloitetaan prosessi alusta. Yksi etsintäkierros vie aikaa maksimissaan noin 2,5 sekuntia.

Olemassaolevien Bluetooth-toteutusten etsintäoperaatiossa on siis vielä paljon kehittämisen varaa. Etsintä vie käytännössä pahimmillaan jopa kymmenen sekuntia, joten etsintäprosessia joudutaan selvästi toistamaan liian monta kertaa. Koska ongelma liittyy matalan tason Bluetooth-protokolliin, ei sovellusten kehittäjä voi juurikaan vaikuttaa yhteydenmuodostusaikaan. Tulevissa Bluetooth-spesifikaatioversioissa asiaan tullaan kiinnittämään huomiota. Tavoitteena on, että etsintä veisi pisimmilläänkin vain pari sekuntia.

### 6.5.4 Virhetilanteiden käsittely

Laadukkaan tietoliikenneprotokollan tulee pystyä hallitsemaan lukuisia virhetilanteita: pakettien puuttumista tai kopioitumista, paketeissa olevia virheitä, yhteyden katoamista ja ruuhkautumista. WAP-over-Bluetooth -järjestelmän pinossa edellä mainittuja palveluita tarjoavat LMP-, L2CAP- ja WTP-protokollat. Sovellukselle tuleva informaatio on näin ollen erittäin todennäköisesti oikeaa.

Rahaa käsittelevissä palveluissa on syytä seurata jollakin tavalla transaktioiden oikeellisuutta. Bluetooth-verkossa tapahtuvat transaktioiden kahdentumiset tai katoamiset ovat erittäin epätodennäköisiä, mutteivat mahdollisia. Suurin yksittäinen virhelähde on silti sovellus itse, koska sovelluslogiikan puutteet voivat generoida virheitä kertaluokkia suuremmalla todennäköisyydellä kuin siirtoverkko. Huolellinen tes-

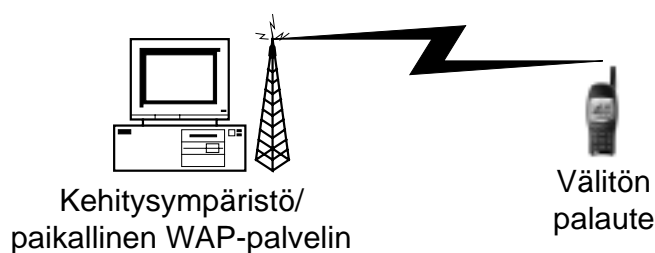
taus ja sovellukseen lisätyt tarkistukset auttavat rakentamaan stabiileja, asiakkaille oikeudenmukaisia järjestelmiä.

## 6.6 Esimerkkisovelluksia

Paikallisiin WAP-palveluihin perustuvia sovelluksia voidaan ideoida mielivaltaisen paljon. Konsepti on kuitenkin verrattain uusi, joten kaikkia sen tarjoamia mahdollisuuksia ei vielä osata hyödyntää täysimittaisesti. Seuraavassa esitellään lyhyesti kaksi sovellusta, joiden toteuttamiseen voidaan luontevasti ja monipuolisesti käyttää Bluetooth-järjestelmän päälle rakennettua paikallista WAP-palvelua.

### 6.6.1 Kehitysvaiheessa olevan WAP-palvelun testaus

WAP-palveluiden kehittäjillä on ollut tähän asti kaksi keinoa testata keskeneräisiä palveluitaan: testaus kehitysympäristöön integroidulla päätelaite-emulaattorilla ja varsinainen kenttätestaus operaattorin ylläpitämässä verkossa. Ensiksi mainittu tapa on nopea ja helppo käyttää, muttei anna välttämättä oikeaa käyttökokemusta. Jälkimmäinen testaustapa antaa autenttisen kokemuksen, mutta on kohtuuttoman hidas viedä läpi. Varsinkin operaattoreiden ulkopuoliset kehittäjät voivat kohdata vaikeuksia yrittäessään testata keskeneräisiä palveluitaan julkisessa WAP-verkossa.



*Kuva 6.6. WAP-palvelun testaus päätelaitteessa.*

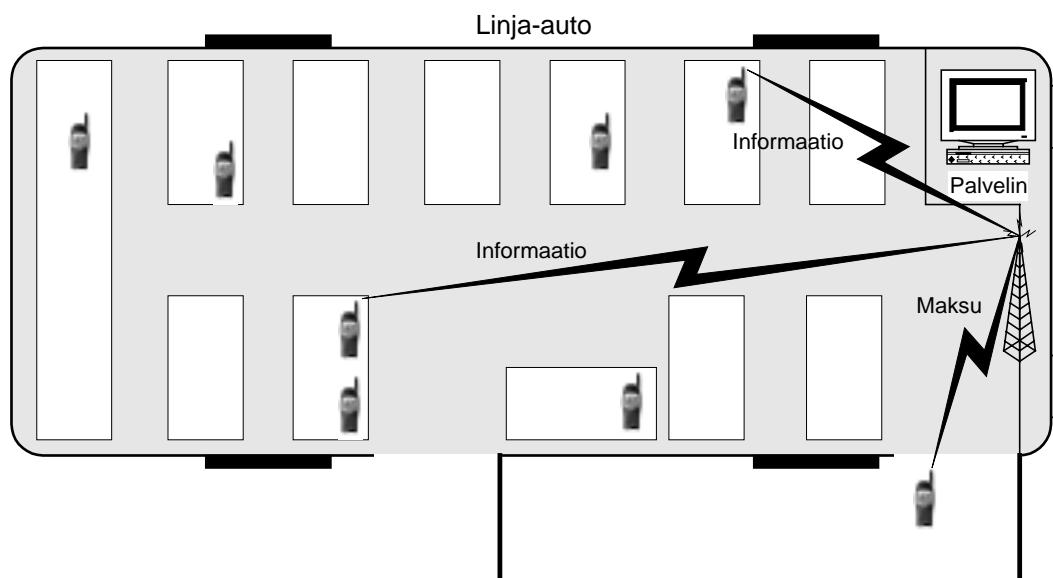
Kehitysvaiheessa olevaa WAP-palvelua voidaan testata oikeassa päätelaitteessa Bluetooth-yhteyden avulla, kuten kuvasta 6.6 voidaan nähdä. WAP-sivusto rakennetaan kehitysympäristössä ja testataan alkuvaiheessa työasemassa ajettavassa päätte-

laite-emulaattorissa. Kun sivut ovat kypsyneet riittävästi, ne siirretään työaseman paikalliselle WAP-palvelimelle ja siitä langattomasti päätelaitteeseen, jossa niitä voidaan tarkastella ja kokeilla. Prosessi on nopea, maksuton ja automatisoitavissa. Virheiden löytäminen helpottuu järjestelmää käyttämällä, koska kehittäjän ei tarvitse luottaa emulointiohjelmistoihin. Testauksesta saadaan välitöntä palautetta, jota voidaan hyödyntää palvelun jatkokehityksessä. Jokaisella iterointikierröksellä palvelusta tulee valmiimpi ja miellyttävämpi käyttäjälle.

### 6.6.2 Linja-autoliikenteen asiakasjärjestelmä

Linja-autoyhtiöt ovat olleet innokkaita uuden tekniikan käyttöönottajia. Asiakkaille on kehitetty muun muassa WAP-palvelu, joka arvioi seuraavan linja-autovuoron saapumisaikaa. WAP-over-Bluetooth –konseptin avulla voitaisiin kuitenkin kehittää paljon aiempia älykkäämpiä järjestelmiä.

Linja-autoliikenteen asiakasjärjestelmän avulla asiakkaille voidaan tarjota maksu- ja informaatiopalveluja. Järjestelmän linja-autoon on asennettu paikallinen WAP-palvelin Bluetooth-sovittimella. Asiakkailla on Bluetooth-valmiudella varustettu WAP-päätelaite, jossa on elektronista rahaa sirukortille ladattuna. Astuttuaan linja-autoon asiakas avaa päätelaitteellaan WAP-yhteyden palvelimelle ja saa maksupalve-



Kuva 6.7. Linja-autoliikenteen asiakasjärjestelmän toiminta.



lun WML-sivun. Seuraa transaktio, jossa asiakas hyväksyy PIN-koodillaan sirukortilta tapahtuvan matkan veloituksen. Elektroninen raha siirtyy palvelimen tietokantaan ja asiakas voi etsiä itselleen paikan linja-autosta. Matkan aikana paikallisen WAP-palvelimen informaatiopalvelu on asiakkaan käytettävissä, josta voi esimerkiksi tarkastaa paluuseen käytettävän linja-autovuoron, lukea paikallisuutisia tai katsella mainoksia. Linja-autoyhtiöllä on valta päättää asiakkaille tarjottavasta sisällöstä. Jos järjestelmässä oleva linja-auto liitetään langattomasti Internetiin, myös tavallinen seittiselailu tulee mahdolliseksi. Kuvasta 6.7 voidaan nähdä järjestelmän perustoiminta.

Järjestelmän toiminnan kriittisin vaihe on uusien asiakkaiden saapuminen linja-autoon. Jotta järjestelmän käyttöönotto olisi ylipäättänsä järkevää, tulisi maksutapahtuma pystyä suorittamaan vähintään yhtä nopeasti kuin älykortilla tai käteisellä rahalla. Tämänhetkisen Bluetooth-spesifikaation mukainen päätelaite ei kuitenkaan pysty muodostamaan yhteyttä toiseen laitteeseen hetkessä, vaan prosessi voi viedä pahimmillaan jopa kymmenen sekuntia. Linja-autoliikenteen asiakasjärjestelmän toteuttaminen saattaa siis olla mahdollista vasta sitten, kun Bluetooth-järjestelmän yhteydenmuodostusta on optimoitu spesifikaatiotasolla.

## 7 Yhteenveto

Paikallisen WAP-palvelun mekanismi on hämmästyttävän yksinkertainen. Palvelun rakenne on WAP-protokollien kannalta täysin yhtenevä tavanomaisen, operaattorin verkossa jaettavan palvelun kanssa. Esimerkiksi sovellusympäristö ja tietoturvatekniikat periytyvät suoraan spesifioiduista ratkaisuista. Palvelun paikkatietoisuus syntyy henkilökohtaisen PAN-verkon avulla. Verkon kantama on rajoitettu, minkä vuoksi vain fyysisesti toistensa lähellä olevat päätelaitteet voivat verkottua keskenään. Palvelinlaitteeseen voidaan tallentaa sijoituspaikkaan liittyvää informaatiota, jota asiakaslaite voi hakea PAN-verkon kautta. Päätelaitteiden paikantamiseen ei siis käytetä ulkoisten laitteiden tai verkkojen palveluita, vaan verkkoon kytkeytymistä. Jos laite kykenee hakemaan paikallisen palvelun sisältämää informaatiota, on se riittävän lähellä palvelinta. Mikäli verkon kantama olisi liian suuri, menetettäisiin paikallisen palvelun luonne, koska myös kauempana olevista laitteista voisi tulla asiakkaita. Tällöin palvelussa jaettava informaatio ei kuitenkaan olisi pitkän välimatkan takia hyödyllistä asiakkaalle, vaan koko paikallisuuden konsepti romahtaisi.

Vain muutama nykyään tarjolla olevista verkkotekniikoista soveltuu PAN-verkoksi. Koska kaikilla tekniikoilla saavutetaan riittävä suorituskyky, ei vertailua voida suorittaa sen perusteella. Asynkronisia, pakettimuotoisia yhteyksiä tuetaan samoin kaikissa järjestelmissä, mutta synkronisia, piirikytkentäisiä yhteyksiä ei. Synkroniset yhteydet ovat sopivia virtaavan informaation välittämiseen PAN-verkossa, joka on tärkeä sovelluskohde tulevaisuudessa. Tekniikoiden välillä olevat erot tulevat parhaiten esille, kun pohditaan toisten laitteiden ja palveluiden löytämisen mahdollistavaa toiminnallisuutta. Se on olennainen osa PAN-verkkojen dynaamista luonnetta, jota ei voida saavuttaa staattisilla asetuksilla. Bluetooth on vertailluista tekniikoista ehdottomasti paras, koska sen perusratkaisut ja –mekanismit on räätälöity dynaamiseen, henkilökohtaiseen verkkoon. Se tukee kaikkia edellä mainittuja, tärkeäksi arvioituja toimintoja. IrDA yltää lähes samaan, sitä rasittavat vain synkronisten yhteyksien puute, liian lyhyt kantama ja heikko toimintakyky ulkotiloissa. WLAN:n, HomeRF:n ja HIPERLAN:n sinänsä tehokkaiden arkkitehtuurien yhteinen ongelma on järjestelmään rakennetun laitehaun puuttuminen.

Suoran WAP-tuen puuttuminen Bluetoothista ei nykyisellään ole ongelma. WAP-palvelimen ja –asiakaslaitteen välille voidaan paikallisverkkoprofiilia käyttäen

muodostaa kahdenvälinen PPP-yhteys, joka riittää WAP-transaktioiden suorittamiseen. Paikallisella WAP-palvelimella on kutakin asiakasta kohti yksi PPP-yhteys. Koska yksi Bluetooth-laite voi käsitellä vain rajallisen määrän yhteyksiä, saatetaan palvelimeen joutua asentamaan lisää laitteistokapasiteettia asiakkaiden määrän kasvaessa. Paikallisverkkoprofiililla ei voida toteuttaa täydellistä PAN-toiminnallisuutta, koska monenvälisiä yhteyksiä ei tueta. Kehittyneempi *Personal Area Networking* – profiili on tulossa myöhempisiin Bluetooth-spesifikaatioihin.

Bluetoothiin päälle toteutettu WAP-arkkitehtuuri, josta käytetään usein nimeä *WAP-over-Bluetooth*, noudattaa istuntomallia, joka perustuu lyhyen kantaman radiotekniikan rajoitteisiin. Istunto voidaan aloittaa, kun päätelaitteet ovat ensin havainneet toisensa. Mikäli päätelaitteiden välinen etäisyys kasvaa liian suureksi, joudutaan istunto lopettamaan kesken. WAP-spesifikaatiossa määritelty työntötoiminnallisuus mahdollistaa paikallisiin WAP-palveluihin mielenkiintoisia lisätoimintoja, esimerkiksi palvelun mainostaminen. Liiallista sisällön työntämistä asiakaslaitteisiin on kuitenkin syytä välttää, jottei toiminnasta syntyisi negatiivisia reaktioita.

Asiakkaan tai päätelaitteen tunnistaminen on monissa paikallisen WAP-palvelun sovelluskohteissa välttämätöntä. Jos päätelaitteen tunnistaminen riittää, tunnistus voidaan suorittaa päätelaitteen uniikin Bluetooth-osoitteen perusteella. Mikäli on varmistuttava myös asiakkaan henkilöllisyydestä, on päätelaitteen tunnistuksen ja salasavarmistuksen yhdistelmä tehokas menetelmä. WAP-over-Bluetoothissa tuetaan tehokasta sisällön salausta kahdella eri protokollatasolla, joten tietoturvallisten palveluiden kehittäminen on mahdollista.

Työssä tehtiin laajapohjainen tarkastelu paikallisten WAP-palveluiden problematiikasta. Asioita pohdittiin sekä teoreettiselta että käytännölliseltä kannalta. Teoreettinen pohdiskelu oli välttämätöntä mietittäessä käytännön toteutusta, koska aiheeseen liittyvää materiaalia on saatavilla erittäin niukasti. Tulevan PAN-profiilin tutkiminen ja soveltuuden arviointi olisi ollut työhön mielenkiintoinen lisä, mutta kehitysvaiheessa olevia spesifikaatioita ei valitettavasti pystytty hankkimaan. Toisen verkkotekniikan, esimerkiksi IrDA:n, mukaanottaminen toteutusarviointiin olisi myös ollut hyödyllistä, koska toteutusmallista oltaisiin siten saatu yleisemmin käytettävä.

Työn tuloksia tullaan hyödyntämään VTT Tietotekniikan paikallisiin WAP-palveluihin liittyvissä projekteissa. Tuloksia käytetään lähtötietoina valittaessa toteutusmekanismeja palveluille, joiden sovelluskohde, käyttäjäryhmä, sisältö ja laajuus eroavat toisistaan. Samalla nyt esitettävien tulosten ja ennusteiden toteutumaa voidaan

tarkastella uudelleen, kenties muuttuneessa markkinatilanteessa. Jatkokehitystyö tulee näin ollen suuntautumaan käytännöllisempään suuntaan.

## Lähdeluettelo

- [BSIG1999] Specification of the Bluetooth System: Core v1.0b. Bluetooth SIG, 1.12.1999. 1082 s.
- [BSIG2001] The Official Bluetooth Website ([www.bluetooth.com](http://www.bluetooth.com)). Bluetooth SIG, 27.2.2001.
- [Comp2000] White Paper: Bluetooth Technology Overview. Compaq, 11/2000. 21 s. Saatavilla osoitteesta [www5.compaq.com/products/wireless/wpan/files/WhitePaper\\_BluetoothTechnologyOverview-QA.pdf](http://www5.compaq.com/products/wireless/wpan/files/WhitePaper_BluetoothTechnologyOverview-QA.pdf).
- [ETSI2001] ETSI – Telecom Standards ([www.etsi.org](http://www.etsi.org)). European Telecommunications Standards Institute, 8.3.2001.
- [GrMi1998] Grundström, M., Mickos, R. ATM-tekniikka ja monipalveluverkot. Suomen Atk-kustannus, 1998. 396 s.
- [Held2001] Held, G. Data Over Wireless Networks (Bluetooth, WAP & Wireless LANs). McGraw-Hill, 2001. 344 s.
- [Home1998] Technical Summary of the SWAP Specification. HomeRF, 3/1998. 1 s. Saatavilla osoitteesta [www.homerf.org/data/tech/hrfwgtec.pdf](http://www.homerf.org/data/tech/hrfwgtec.pdf).
- [Home2000] HomeRF: Introduction to the HomeRF Technical Specification. HomeRF, 18.12.2000. 17 s. Saatavilla osoitteesta [www.homerf.org/data/tech/techpres.pdf](http://www.homerf.org/data/tech/techpres.pdf).

- [IEEE2001] IEEE 802.15 Working Group for WPANs  
([www.ieee802.org/15/](http://www.ieee802.org/15/)). Institute of Electrical and Electronics Engineers, 26.3.2001.
- [IrDA2001] IrDA Website: About IrDA ([www.irda.org/about/index.asp](http://www.irda.org/about/index.asp)).  
Infrared Data Association, 7.3.2001.
- [Juho2000] Juhola, H. Matkaraportti Japanista: Langattomien internetpalvelujen käyttäjämäärä kasvaa nyt puolella miljoonalla viikossa. GT-lehti, 8/2000. s. 4-9.
- [MeSK1998] Megowan, P., Suvak, D., Knutson, C. IrDA Infrared Communications: An Overview. Counterpoint Systems Foundry, Inc., 6.11.1998. 21 s. Saatavilla osoitteesta [www.irda.org/use/pubs/Overview.pdf](http://www.irda.org/use/pubs/Overview.pdf).
- [MiBi2001] Miller, B., Bisdikian, C. Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications. Prentice Hall, 2001. 303 s.
- [Tane1996] Tanenbaum, A. Computer Networks, 3<sup>rd</sup> Edition. Prentice Hall, 1996. 813 s.
- [Uoti1998] Uotila, P. Tietoliikenteen tekniikka, verkot ja protokollat, 2. painos. Suomen Atk-kustannus, 1998. 238 s.
- [WAPF1998] Wireless Application Protocol Architecture Specification. WAP Forum, 30.4.1998. 20 s. Saatavilla osoitteesta [www1.wapforum.org/tech/documents/SPEC-WAPArch-19980430.pdf](http://www1.wapforum.org/tech/documents/SPEC-WAPArch-19980430.pdf).

- [WAPF1999a] Wireless Application Protocol Wireless Application Environment Overview. WAP Forum, 4.11.1999. 26 s. Saatavilla osoitteesta [www1.wapforum.org/tech/documents/SPEC-WAEO-19991104.pdf](http://www1.wapforum.org/tech/documents/SPEC-WAEO-19991104.pdf).
- [WAPF1999b] Wireless Application Protocol Wireless Datagram Protocol Specification. WAP Forum, 5.11.1999. 78 s. Saatavilla osoitteesta [www1.wapforum.org/tech/documents/SPEC-WDP-19991105.pdf](http://www1.wapforum.org/tech/documents/SPEC-WDP-19991105.pdf).
- [WAPF1999c] Wireless Application Protocol Wireless Session Protocol Specification. WAP Forum, 5.11.1999. 114 s. Saatavilla osoitteesta [www1.wapforum.org/tech/documents/SPEC-WSP-19991105.pdf](http://www1.wapforum.org/tech/documents/SPEC-WSP-19991105.pdf).
- [WAPF1999d] Wireless Application Protocol Wireless Transaction Protocol Specification. WAP Forum, 11.6.1999. 67 s. Saatavilla osoitteesta [www1.wapforum.org/tech/documents/SPEC-WTP-19990611.pdf](http://www1.wapforum.org/tech/documents/SPEC-WTP-19990611.pdf).