



# **VIVIAN subproject**

## Deliverable 2

Project report

Status: intermediate

Authors: Andrei Kotchanov

Sami Merovuo

Ari Valtaoja

Lappeenranta University of Technology

Department of Information Technology

Laboratory of Telecommunications

P.O.Box 20, FIN-53851 Lappeenranta

Lappeenranta, May 2001



## CONTENTS

<b><u>1</u></b>	<b><u>INTRODUCTION</u></b> .....	<b>4</b>
<b><u>2</u></b>	<b><u>THE WIRELESS AND MOBILE ENVIRONMENT</u></b> .....	<b>5</b>
2.1	<u>Mobility Support</u> .....	5
2.2	<u>TCP/IP in the Wireless Environment</u> .....	6
2.2.1	<u>Mobile IP</u> .....	7
<b><u>3</u></b>	<b><u>BLUETOOTH NETWORKING</u></b> .....	<b>8</b>
3.1	<u>Different Network Architectures</u> .....	8
3.1.1	<u>Cable Replacement</u> .....	8
3.1.2	<u>Access Point Based Network</u> .....	9
3.1.3	<u>Ad Hoc Network</u> .....	9
3.2	<u>Special Characteristics of Bluetooth</u> .....	10
3.3	<u>Service Discovery Application Profile</u> .....	11
<b><u>4</u></b>	<b><u>CORBA AND MOBILITY</u></b> .....	<b>12</b>
4.1	<u>Problems Related to CORBA and Mobility</u> .....	12
4.2	<u>Requirements for the CORBA Solution</u> .....	13
<b><u>5</u></b>	<b><u>WIRELESS CORBA</u></b> .....	<b>14</b>
5.1	<u>Architecture</u> .....	15
5.2	<u>Mobile IOR</u> .....	17
5.3	<u>Handoff and Access Recovery</u> .....	19
5.4	<u>Mobile Client</u> .....	20
5.5	<u>Mobile Server</u> .....	21
5.6	<u>Mobile Server and Mobile Client</u> .....	23
<b><u>6</u></b>	<b><u>WIRELESS CORBA AND BLUETOOTH</u></b> .....	<b>25</b>
6.1	<u>Wireless CORBA on Bluetooth Access Point Networks</u> .....	25
6.1.1	<u>Assigning an IP-address to a Bluetooth Device</u> .....	25
6.1.2	<u>Tunneling</u> .....	27
6.1.3	<u>Mapping of GIOP to Bluetooth</u> .....	27



<u>6.2</u>	<u>Wireless CORBA on Bluetooth Ad Hoc Networks</u> .....	28
<u>6.2.1</u>	<u>Advertising</u> .....	28
<u>6.2.2</u>	<u>Using SDP to Locate the Naming Service</u> .....	29
<u>6.2.3</u>	<u>Using SDP Instead of the Naming Service</u> .....	29
<u>7</u>	<u>CONCLUSIONS</u> .....	30
	<u>REFERENCES</u> .....	31



## INTRODUCTION

This document is the deliverable for the second step (D2) of Vivian sub-project. The goal of this step was to provide the mapping of CORBA to Bluetooth including an architecture suggestion. The document should also discuss advantages and limitations of the mappings.

The mappings presented in this document strongly grounded on the specification suggested by Object Management Group (OMG) for the use of CORBA over wireless links [13]. There exist some other solutions too, but this approach turns out to be the best one for the problem of wireless CORBA. The OMG's specification is also on its way to standard, so there is a strong possibility that it will be the widely used approach in the future. However, the specification, like all other solutions too, focuses only on problems and requirements relating to wide-range wireless networks leaving short-range networks, like Bluetooth, untouched. Actually, because of the special characteristics of Bluetooth, it can be significantly different from other wireless networks and should be covered separately anyway. So, this document can be really considered an extension to the OMG's wireless CORBA specification.

The paper is structured as follows. Chapter 2 gives an explanation of wireless networking media; how it differs from framework of fixed network and what kind of issues are concerned with terminal mobility. Chapter 3 is devoted to the description of Bluetooth networks and its special features. Then in chapter 4, general issues of CORBA over wireless links are considered and in chapter 5, the summary of OMG's draft specification of wireless CORBA is presented. Chapter 6 discuss the mapping of CORBA to Bluetooth and how the OMG specification could be extended. Finally, section 7 presents our conclusions.



# 1 THE WIRELESS AND MOBILE ENVIRONMENT

Characteristics of wireless media differ from those of fixed networks. Wireless networks tend to have lower bandwidth and higher error rates and even unexpected connection losses are not rare. Also long round-trip times are typical. Perhaps the biggest differences between traditional wired networks and wireless mobile networks are related to routing. In fixed networks the structure of the network is more or less stable and all devices have their own static addresses so routing is relatively simple once the routing tables have been formed for the first time. But in wireless mobile network the layout changes all the time: devices get connected and disconnected, they move from one access point to another, they can form ad hoc networks, their addresses can change and the load between different parts of the network can vary and change drastically. All in all, the situation is more complex and vulnerable and chance for errors is bigger.

## 1.1 Mobility Support

There are two basic networking scenarios involving wireless terminal mobility. The first one considers wireless access of a device to a fixed network and possibility to move from place to place, changing access points. The other one deals with ad hoc networking, describing the process of forming ad hoc networks and how information is passed from one device to another. An ad hoc network is a collection of mobile devices, which spontaneously form connections with each other to communicate. Ad hoc networks do not have the networking infrastructure and services that are typically provided by wired networks such as DHCP, DNS and Network Management & Other Services.

Several IETF working groups are now studying different issues related to terminal mobility and ad hoc networking. For example, the goal of the Zero Configuration Networking (ZEROCONF) Working Group [1] is to enable networking in the absence of configuration and administration. Zero configuration networking is required for environments where administration is impractical or impossible, such as in the home or



small office, embedded systems 'plugged together' as in an automobile, or to allow impromptu networks as between the devices of strangers on a train. Mobile Ad Hoc Networking (MANET) Working Group [2] is focused on routing protocols of ad hoc networking, which involve intermediate devices that route packets towards the final destination. But problems existing in ad hoc networking are still far from their solution and only some special types of ad hoc networks, such as Bluetooth piconets, can now be used for providing network services to upper layers, including CORBA applications.

The problems caused by terminal mobility can be solved on different levels of the protocol stack, mainly at transport or session layer. Addressing mobility problems at the transport layer hides the mobility from upper layers but requires modifications to used transport protocol. As a result all the devices are required to adopt this modified protocol. IETF's IP Routing for Wireless/Mobile Hosts (Mobile IP) Working Group [3] has developed routing support to permit IP nodes (hosts and routers) using either IPv4 or IPv6 to seamlessly "roam" among IP subnetworks and media types. The Mobile IP method supports transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings.

Solving the problem at the session layer leaves the transport protocol intact but forces applications to use the session layer instead of the transport layer. In the case of CORBA however, this solution can be acceptable because it allows to modify ORBs only on those devices which are directly involved in mobility support and do not touch non-mobile, or fixed network ORBs.

## **1.2 TCP/IP in the Wireless Environment**

Although TCP/IP is well suited for fixed networks and offers a reliable way to transfer data it has some serious shortcomings in wireless networks [4]. These shortcomings arise from the error semantics and basic mechanisms of TCP/IP.

If a packet is not acknowledged within a certain time the TCP assumes that congestion exists and reduces the transmission speed. In the wireless networks however, packet



loss is more likely due to packet corruption than congestion. Furthermore handoffs may cause additional packet loss because some packets may not reach their destination during the handoff procedure. In these cases slowing the transmission is not desirable because data loss is not a result of congestion. Instead the transmission should continue at full speed.

Another considerable problem is that both connection establishment and termination are time consuming processes because three-way-handshaking is used in both cases. That combined with long round-trip times of wireless networks leads to increased latency times. As a conclusion TCP/IP is not necessarily the best solution for wireless media and in order to cope with these problems wireless connection should be separated from the wired one.

### **1.2.1 Mobile IP**

Mobile IP [5] is an extension of traditional IP developed to enable the usage of IP based networking in wireless environment. Home network has a component called Home Agent (HA) in order to support mobility for its mobile terminals (Mobile Node, MN). A visited (foreign) network has Foreign Agent (FA) to provide Internet access for visiting mobile devices using their home network addresses. When MN arrives to a foreign network it calls FA that gives it a Care-of Address (COA) i.e. an address in the foreign network. Then HA is informed that all traffic to MN must be redirected to its COA. So when Correspondent Node (CN) sends packets to MN's home network address, HA tunnels those packets to MN's current COA. The tunneling is performed using IP-in-IP encapsulation i.e. a new IP header containing MN's COA as a destination and HA as source address is created and the original packet is carried as a payload. Sending is simpler; the MN just uses FA as gateway (see Figure 2.1).

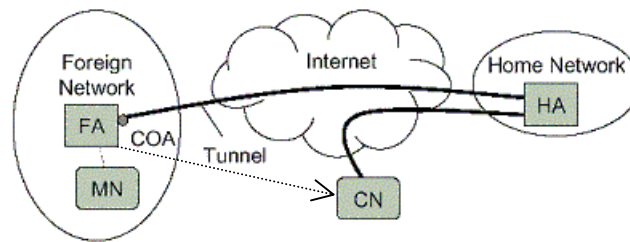


Figure 2.1: Mobile IP

Different optimisations and enhancements to standard Mobile IP are discussed in IETF's Mobile IP Working Group. Internet Draft "Route Optimization in Mobile IP" [6] describes how to avoid the so-called triangular routing of packets (CN-HA-FA-MN and back to the CN) by sending binding updates to the CN to inform it of the MN's current location.

Another enhancement of particular importance to short range wireless networking media like Bluetooth is micro-mobility support, i.e., efficient handling of handoffs between access points within visited administrative domain without contacting the home agent. This can be achieved by introducing a hierarchy of additional infrastructure entities into the foreign network. Several micro-mobility supporting approaches are currently being developed [3].

## 2 BLUETOOTH NETWORKING

### 2.1 Different Network Architectures

Three basic architectures can be defined for networks using Bluetooth. Additionally combinations of these three basic networks can exist.

#### 2.1.1 Cable Replacement

Bluetooth is used as a simple cable replacement just like infrared connection. These applications most likely don't utilize CORBA so this architecture can be bypassed for the time being. And this architecture is just a simple point-to-point connection so

solutions developed for more complex situations can be easily utilized in this architecture if ever needed.

### 2.1.2 Access Point Based Network

Mobile terminals have access to some fixed network via access points (LAN access point, Dial-up networking, etc) and use services provided by some fixed network node (Figure 3.1). One access point can provide access for seven active clients and is itself acting as the master of the piconet.

### 2.1.3 Ad Hoc Network

Network consisting of Bluetooth enabled devices without access to any fixed network (Figure 3.2). The network is standalone Bluetooth network, which can be formed “spontaneously” without pre-planning, when at least two data terminals are in the Bluetooth range of action. There can be seven active slaves and one master in one piconet.

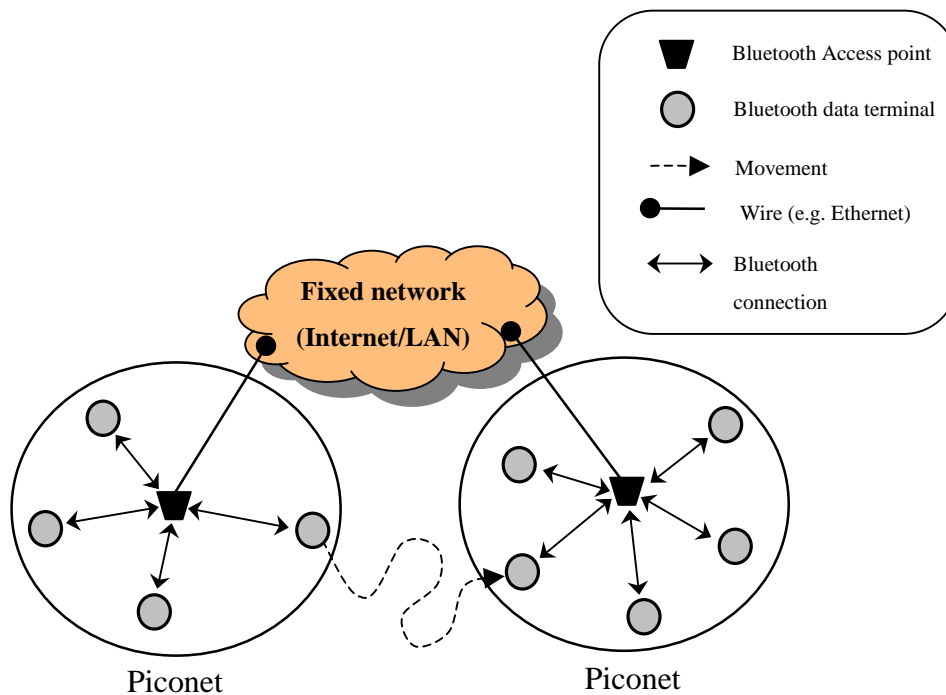


Figure 3.1: Access point based network

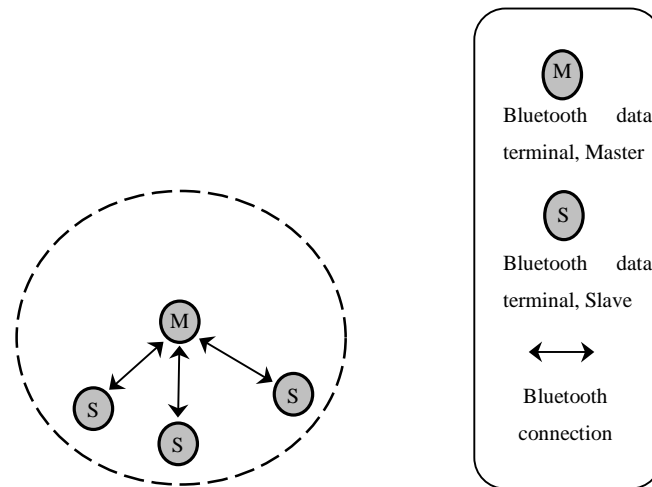


Figure 3.2: Isolated ad hoc network

## 2.2 Special Characteristics of Bluetooth

Bluetooth has some unique characteristics that differ it from other wireless media (GPRS, WLAN etc). These differences need some special attention because of the restrictions they set. Its 10 meters range is very short compared to WLAN and GSM so handoffs will occur frequently if the device is moving. This makes the availability of fast and reliable handoff handling a mandatory requirement.

Other distinctive feature is piconet and its restriction of eight active members, one master and seven clients. In addition more slaves may remain in parking mode where they remain synchronized to the master but are not allowed to communicate. The maximum number of parked slaves per master is 256 [15].

Third feature is scatternet. In this case two or more piconets are connected through one of their members. The members of those two piconets will be able to communicate with each other through these nodes. The connecting nodes can be either master or slave in



their original piconets but it should be noted that one device can not act as a master for more than one piconet. A maximum of ten piconets may constitute a scatternet.

By combining all this it can be easily seen that very complex situations are possible. For example, in theory it could be possible to have a situation where some client has to access a service in fixed network through scatternet.

The problems of Bluetooth networking are now under consideration by Personal Area Networking Working Group (PAN) of the Bluetooth Special Interest Group (SIG) [16]. The Bluetooth networking specification will allow Bluetooth mobile ad-hoc IP networks for data, voice, video and other forms of communications. This ad-hoc network does not require the existence of any special purpose products or infrastructure, but it will inter-operate with such devices if they exist, to (a) facilitate the ad-hoc network or (b) provide LAN access to a separate wired (or wireless) network.

Bluetooth PAN Profile is developing in phases, each phase providing more and more features. Bluetooth PAN Profile Phase I is now nearly finished and:

- Supports Peer to Peer Ad Hoc Networking
- Enable IP in Piconet
- Uses the Bluetooth Networking Encapsulation Protocol (BNEP) over L2CAP
- Enable Slave to Slave communication

Bluetooth PAN Profile Phase II will focus on providing the missing pieces:

- Network formation and topologies
- Handoff among access points
- Inter-piconet routing

### **2.3 Service Discovery Application Profile**

Service discovery application profile uses Service Discovery Protocol (SDP) to locate available services. It defines the protocols and procedures that shall be used to locate objects on other Bluetooth-enabled devices using SDP. Devices can add their own



objects to their SDP databases for other devices to look for and browse remote databases to find services they are interested of. SDP provides direct support for the following service inquiries [17]:

- Search for services by service class
  - Used to find known and specific services (for example the naming service).
- Search for services by service attribute(s)
  - Almost the same as above but instead of answering question “Is service X available?” it is used to make queries like “Is service X with characteristic Y available?”
- Service browsing
  - General service search that can be used to list all available services or all available services of some specific class.

In order to run SDP query on some particular device the device needs to be discovered and linked with. After that the SDP query can be carried out.

### **3 CORBA AND MOBILITY**

The utilization of CORBA middleware technology in wireless mobile environment contains certain obstacles and difficulties. It also sets some new requirements for the CORBA solution that are derived from mobility. These problems and requirements are discussed in the following two chapters.

#### **3.1 Problems Related to CORBA and Mobility**

The mobile environment causes many problems for the usage of CORBA. These problems inherited from traditional CORBA solutions include following:

1. Traditional CORBA solutions assume that DNS names and IP addresses of IIOP servers rarely change. In the mobile environment however, the case is just the



opposite because devices are expected to be on move all the time so addresses will change frequently.

2. The connection is expected to be very reliable. IIOP doesn't have support for resuming a broken connection so if the connection is lost then the state of the connection is irrecoverably lost too. Unfortunately wireless connections tend to break more often than wired connections.
3. IIOP assumes a same transport connection to be used for the lifetime of a connection so network media should stay same all the time. In other words, it isn't possible to change the network interface from Bluetooth to UMTS during the connection but this might be a common situation in the future.
4. IIOP is intended to be easy to use at the cost of bandwidth usage but in mobile networks bandwidth is scarce resource.

### **3.2 Requirements for the CORBA Solution**

Because of the moving nature of mobile devices it can't be assumed that the connection between different ORBs is – or will stay - static so CORBA solution must support mechanisms that hide the mobility and provide both error handling and handoff support when the client moves from one piconet or access node to other. The telecom domain task force of Object Management Group (OMG) recognized the requirements in the mobile environment and released a request for proposals RFP on supporting wireless access and mobility in CORBA [7]. In accordance with it in order to be useful the CORBA solution has to fulfil the following requirements at minimum:

- Maintain message interoperability between traditional (stationary) ORBs and ORBs running on mobile terminals
  - It should be possible to have some traditional ORB running in the fixed network and wireless one running on the mobile device so that these different ORBs could communicate with each other without any modifications or additions to traditional ORB's messaging. To maintain interoperability between different ORBs every stationary ORB of version 2 or higher must support Internet Inter-ORB Protocol (IIOP), which is a TCP/IP mapping of General Inter-ORB Protocol (GIOP) [8]. In other words,



the traditional ORB should be able to send and receive IIOP messages just like when communicating with any other traditional ORB.

- Hide mobility so that traditional ORBs can be used with the mobile one
  - Because a mobile device can move from one domain to another address forwarding should be handled so that traditional ORB doesn't have to care where the mobile device actually is.
- Provide error handling
  - ORB should be able to generate appropriate exceptions and pass those to application if errors occur (connection is lost, transmission fails, data is corrupted or there's no answer, etc). Next action is up to the application: it can decide to shut down, reconnect or carry the invocation again. The point is that ORB should enable controlled actions in the case of failure and programmers should use those in a way that best suits their application.
- Routing issues (handoff support)
  - The connection should stay open during the movement of the mobile device and no data loss is accepted even during the change of access point. Some buffers are needed to ensure that no data is lost during the "blind" moment when the piconet or access point is changing. This question is vital because it determines the usability of the solution by large degree.

Several research projects have addressed these problems; most notable are ALICE [9], Proxy Platform P<sup>2</sup> [10,11], and Wireless CORBA [12], based on the earlier EU ACTS project DOLMEN [13]. All projects introduce some kind of indirection based on gateways, proxies, or bridges that handle the problems in the wireless domain. The results of Wireless CORBA and DOLMEN projects constituted the basement of OMG's Draft Adopted Specification "Wireless Access and Terminal Mobility in CORBA" [14].

## 4 WIRELESS CORBA

As mentioned in section 4.2, it sets some special requirements to the ORB to allow applications on mobile terminals while in motion to exploit and to provide CORBA

objects. This section describes how these restrictions are fulfilled in a wireless CORBA solution “*Wireless Access and Terminal Mobility in CORBA*”, which is a specification by the telecom domain task force of Object Management Group (OMG) [14]. The specification is in a draft phase at the moment, but on its way to a standard. Hereafter, the term **wireless CORBA** is used to mean Wireless Access and Terminal Mobility specification.

## 4.1 Architecture

Wireless CORBA defines architecture and interfaces to support wireless access and terminal mobility in CORBA. The overall architecture of wireless CORBA is presented in the Figure 5.1. As the figure shows, the architecture consists of different domains, some bridges, and a GIOP tunnel between bridges.

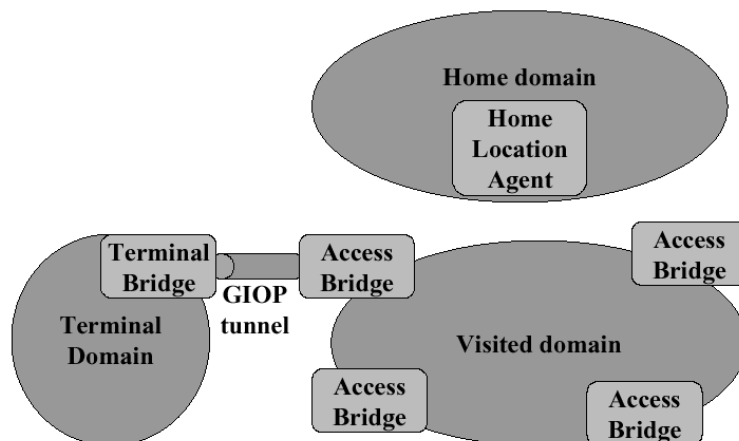


Figure 5.1: Architecture for Terminal Mobility in CORBA [14]

Wireless CORBA identifies three different domains: home domain, visited domain and terminal domain. Home domain is the home network of wireless terminal (for example, if IP addresses are used, this could be the domain where the device’s IP address belongs to). Visited domain is the foreign network where wireless terminal might visit when it moves. Terminal domain is the own domain of the terminal, which actually consist only the data terminal and the terminal side ORB.



In home domain lies so-called Home Location Agent (HLA) that keeps track of the current location of the terminal. Access Bridge and Terminal Bridge are wireless CORBA components located in Visited domain and Terminal domain. The Access Bridges have many responsibilities but in briefly, it is the link between the mobile terminal and the fixed network. In other words, Access Bridge is the one who is providing ORB access to mobile terminals. Terminal Bridge is the terminal side of this link, taking care of that the terminal can communicate with object in other networks. Both of these bridges are also taking care of handoff support (covered in section 4.3). Access Bridge has also important role to inform Home Location Agent about terminals' movements. Whenever a terminal establishes a connection to some Access Bridge, terminal's location is updated to the Home Location Agent so that it always knows in which Access Bridge the data terminal is connected.

Access Bridge and Terminal Bridge also forms together the GIOP tunnel, which is used to deliver General Interoperability Protocol (GIOP) and some control messages between them. As it is known, GIOP messages are the messages that CORBA uses for communication between inter-operating ORBs. Anyway, GIOP is just an abstract protocol and for example in ordinary CORBA, concrete Internet Inter-ORB Protocol (IIOP) is used to specify how GIOP messages are exchanged over a TCP/IP network. Now, when sending GIOP messages over wireless links, tunneling is needed because the wireless network medium might not have the same transport protocol than corresponding fixed network. For example, in fixed network, ORBs use TCP/IP stack as a transport layer for IIOP messages but if there is no TCP/IP protocol implemented on wireless link this cannot be done. In this case, IIOP messages should be tunneled through existing transport protocol (section 6.2).

Wireless CORBA defines a special protocol, which is used to take care of GIOP tunneling between Access Bridge and Terminal Bridge. This protocol is called GIOP Tunneling Protocol (GTP). Actually, GTP is also an abstract protocol just like GIOP itself, and it should be mapped onto some concrete protocol in order to use it. At the moment, the wireless CORBA specification defines three mappings for GTP: TCP Tunneling, UDP Tunneling, and WAP Tunneling.

The main architecture of GIOP Tunneling Protocol is presented in the Figure 5.2 below. As it can be seen from the figure, GIOP messages that are coming from the peer to the Access Bridge are actually IIOP messages (this is because GIOP is just an abstract protocol). Now, when the Access Bridge receives these IIOP messages, it should tunnel them into GTP messages that are mapped to some concrete protocol (e.g. TCP/IP) before sending them to the data terminal over wireless link. Onwards, on terminal side the GTP should be implemented so that it can strip GTP messages back to IIOP messages and deliver them to the terminal's ORB.

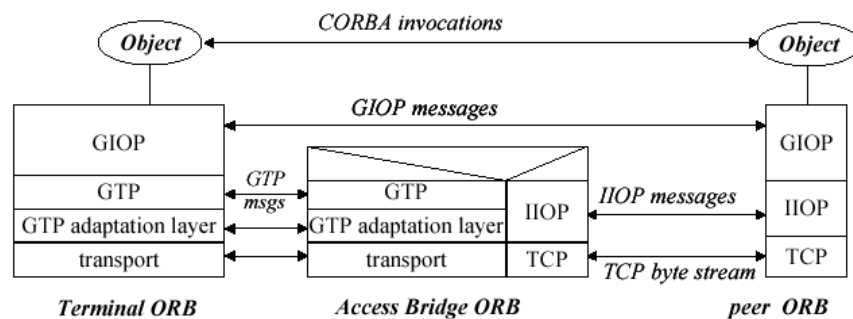


Figure 5.2: GIOP Tunneling Protocol Architecture

## 4.2 Mobile IOR

GIOP defines also methods how clients can manipulate objects, regardless where the objects are located and which ORBs are used. In order to send a message to an object, a client must hold an object reference to the object. The object reference acts as a handle that uniquely identifies the target object and encapsulates all the information required by the ORB to send the message to the correct destination. Since CORBA 2.0, standardized object reference format, Interoperable Object Reference (IOR) has been used define object reference. Standardization maintains the interoperability, and all ORBs which implements CORBA 2.0 can interoperate among each other.

Now, in Wireless CORBA, when a client wants to invoke operations on target objects located on a mobile terminal, the client's IOR request should be routed to the appropriate terminal. But this cannot be done like in ordinary CORBA, because the

terminal might change its place every once in a while. Well, this is why every terminal has the Home Location Agent who knows the terminal current location; the address of the Access Bridge that the terminal was last known to be associated. So, when the client makes an IOR request to a mobile server, the request goes first to the Home Location Agent. The Home Location Agent then replies with `LOCATION_FORWARD` status and IOR request including the address of appropriate Access Bridge, the terminal identifier and the terminal object key. Now the client knows where the appropriate Access Bridge is and can send the IOR to it. The Access Bridge can then deliver the request further to the appropriate terminal server.

To be able to do all this, wireless CORBA defines special Mobile IOR, which is used to hide the mobility of terminal CORBA server from clients invoking operations from it. The Mobile IOR is like normal IOR, but it consists of at least two protocol profiles. This is possible because the CORBA standard supports the use of several profiles parallel in one IOR; each ORB makes the decision which one will be used. The Mobile Profile consists of the normal IIOP profile required in a standard IOR, but also of a *Mobile Terminal Profile*. The main structure of Mobile IOR is presented in the figure 5.3 below.

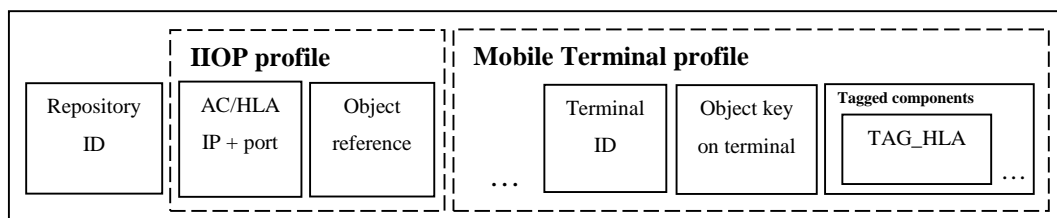


Figure 5.3: Mobile IOR

In Mobile IOR, instead of indicating the address of the target object, the host and port information in an IIOP Profile indicate the address of either the target object's terminal's Home Location Agent or the Access Bridge that the terminal was last associated with. The Mobile Terminal profile consists, among the other things, of the following fields:

1. *Terminal identifier*. A unique worldwide identifier of the terminal. Not strictly defined in the specification and the solutions are left to the implementers.



Specification just gives one possible scheme, where Terminal identifier consists of *IP version*, *IPv4/IPv6 address* and *local identifier*. IP address can be any IP address owned by the organization that is generating the Terminal identifier, and the local identifier is a unique identifier within that organization.

2. *Terminal object key*. A reference to the object that will be invoked from the terminal server.
3. *Tagged components*. Optional fields, but one tag (TAG\_HOME\_LOCATION\_INFO) is required if the terminal has the Home Location Agent. This tag simply identifies the Home Location Agent.

### 4.3 Handoff and Access Recovery

Support for handoff is needed when the mobile terminal moves from one Access Bridge to another and the connection should not be lost during the movement. Actually, Wireless CORBA specification defines two different cases of handoff: *the backward handoff* and *the forward handoff*. The first one is the case where the mobile terminal moves from Access Point to new Access point and keeps up the connection whereas the second one is performed in order to re-establish connectivity after a sudden loss. In the following, the term **handoff** is used to mean backward handoff and the term **access recovery** to mean the forward handoff.

The handoff process establishes a connection to a new Access Bridge, and release the connection to the old Access Bridge. After connection establishment the new Access Bridge invokes the location update process in the Home Location Agent in order to tell that the location of the terminal has changed. After the handoff is completed, the old Access Point informs other Access Points that are interested about the movement of the device (previous Access Bridges where device have been) so that they can forward incoming packets to the new Access Bridge.

In the case where the Terminal Bridge detects that the connectivity to the Access Bridge is lost, The Terminal Bridge starts so called access recovery process. There are two possible successful outcomes of the access recovery process: 1) The access is re-

established to the same Access Bridge as before, or 2) The access is established to a new Access Bridge. After connection lost, the Terminal Bridge establishes connectivity to an Access Bridge and sends a recovery message to it. The message consist of *terminal identifier, reference to the Home Location Agent and information about Access Bridge last accessed*. From this message, the Access Bridge knows is the establishment an access recovery to old Access Bridge or to new Access Bridge and which is the last GTP message that the Terminal Bridge has received. The Access Bridge replies to Terminal Bridge with message which informs it that the Access Bridge is the same as before or new one, and which is the last GTP message that the Access Bridge has received. After that, lost GTP messages can be retransmitted between bridges.

#### 4.4 Mobile Client

This paragraph gives an explanation how wireless CORBA works in practise when the CORBA server is located in fixed network and the client on wireless device. The overall architecture and transactions are presented in the figure 5.4 below.

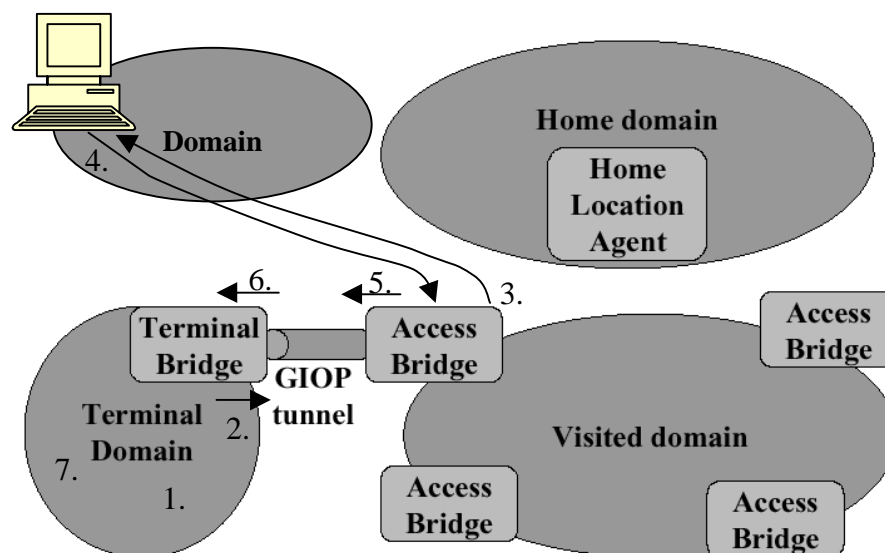


Figure 5.4. Mobile client



The message process contains following steps:

1. A mobile terminal sends an object invocation (IIOP IIOR) targeted to an object located in some other domain.
2. The Terminal Bridge gets the message, encapsulates it and sends it to the GIOP tunnel.
3. The Access Bridge gets the message from the GIOP tunnel, decapsulates it and sends it to the appropriate node.
4. The server receives the message, operates it and sends a response message back to the client.
5. The Access Bridge gets the message targeted to its wireless terminal, encapsulates it and sends it to the GIOP tunnel.
6. The Terminal Bridge gets the message and decapsulates it.
7. Wireless terminal receives the response.

#### **4.5 Mobile Server**

This paragraph gives an explanation how wireless CORBA works in practise when the CORBA server is located in wireless terminal and the client on fixed network. The overall architecture and transactions are presented in the figure 5.5 below.

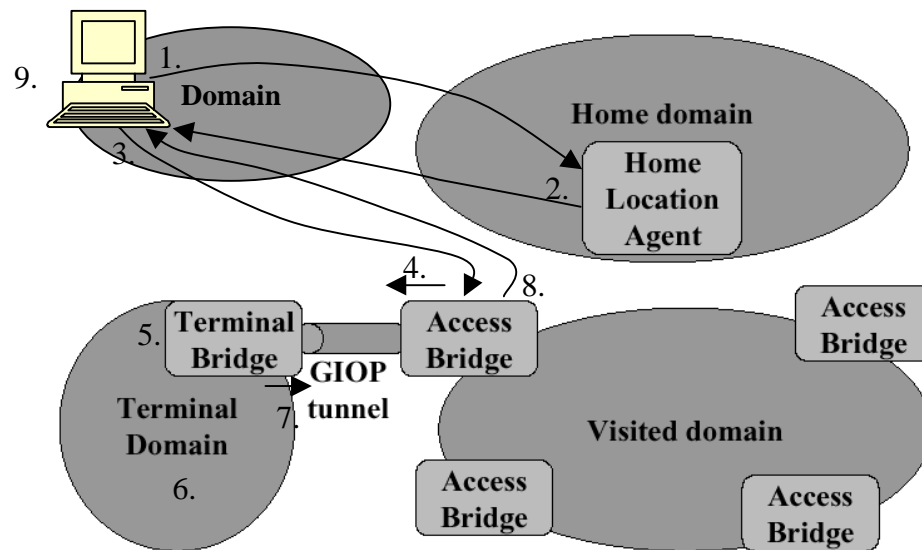


Figure 5.5. Mobile server

The message process contains following steps:

1. A client sends an object invocation (IIOP IOR) targeted to object located in mobile terminal server.
2. Home Location Agent (HLA) receives the message. If HLA has an Access Bridge associated with that terminal, it replies with the LOCATION\_FORWARD status and returns the Mobile IOR identifying the current Access Bridge. Otherwise OBJECT\_NOT\_EXISTS or UNKNOWN\_OBJECT status is replied.
3. Client receives the Mobile IOR and sends a new object invocation to the identified Access Bridge.
4. The Access Bridge gets the message targeted to its wireless terminal, encapsulates it and sends it to the GIOP tunnel.
5. The Terminal Bridge gets the message and decapsulates it.
6. Wireless terminal operates the message sends a response to the client.
7. The Terminal Bridge gets the response, encapsulates it and sends it to the GIOP tunnel.
8. The Access Bridge gets the message targeted to some node, decapsulates it and sends it to the client.
9. The client receives the response

### 4.6 Mobile Server and Mobile Client

This paragraph gives an explanation how wireless CORBA works in practise when both, CORBA server and CORBA client are located on wireless terminals. The overall architecture and transactions are presented in the Figure 5.6 below.

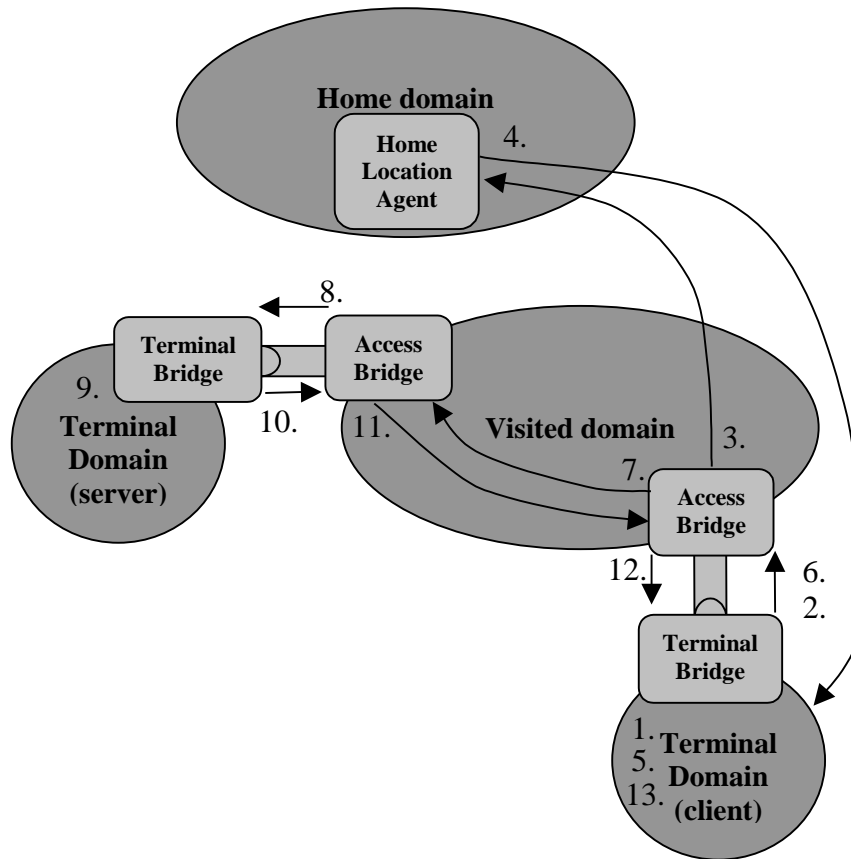


Figure 5.6. Server and client mobility

The messaging process contains following steps:

1. Mobile terminal client sends an object invocation (IIOP IOR) targeted to object located in mobile terminal server.
2. Client's Terminal Bridge gets the message, decapsulates it and sends the message to the GIOP tunnel.
3. Client's Access Bridge receives the message, encapsulates it and sends it to the Home Location Agent of the mobile server.



4. If HLA has an Access Bridge associated with the mobile server asked, it replies with the LOCATION\_FORWARD status and returns the Mobile IOR identifying the Access Bridge where the server is located. Otherwise OBJECT\_NOT\_EXISTS or UNKNOWN\_OBJECT status is replied.
5. When the client receives the response of HLA it sends the new object invocation (Mobile IOR) targeted to the Access Bridge where the server is located.
6. Client's Terminal Bridge encapsulates the message using a GIOP tunnelling Protocol (GTP) and sends it to the GIOP tunnel.
7. Client's Access Bridge receives the message, decapsulates it and sends it to the server's Access Bridge.
8. Server's Access Bridge gets the message and encapsulates it using a GIOP tunnelling Protocol (GTP) and sends it to the GIOP tunnel.
9. Server's Terminal Bridge gets the message and decapsulates it using a GIOP tunnelling Protocol (GTP). Wireless terminal operates the message and sends a response to the client.
10. Server's Terminal Bridge gets the response message, decapsulates the message and sends it to the GIOP tunnel.
11. Server's Access Bridge gets the message and encapsulates it using a GIOP tunnelling Protocol (GTP) and sends it to the GIOP tunnel
12. Client's Access Bridge receives the message, encapsulates it and sends it to the GIOP tunnel.
13. Client's Terminal Bridge decapsulates the message. The client receives the response.



## **5 WIRELESS CORBA AND BLUETOOTH**

Wireless CORBA, described in the previous chapter, was developed to meet the requirements of long and medium distance wireless media, such as GSM, GPRS, UMTS or WLAN. It can be mapped to cover Bluetooth with some small extensions and modifications depending on usage scenario.

### **5.1 Wireless CORBA on Bluetooth Access Point Networks**

First immediate problem is that neither current Bluetooth specification nor even PAN Profile supports IP in scale that would be adequate to utilize wireless CORBA i.e., GIOP tunneling over TCP. The problem is that a mobile Bluetooth device should keep the same IP address during CORBA session while moving between different access points, especially when a CORBA server runs on the mobile terminal. This leaves us with two main possibilities: to greatly extend Bluetooth's IP support or to map CORBA subsets, mainly GIOP onto some Bluetooth layer, e.g. L2CAP. Mapping of GIOP to Bluetooth can be further divided into two separate solutions. This includes scenarios where GIOP is either mapped to a Bluetooth layer or messages are tunnelled over it. All approaches have their advantages and disadvantages that are discussed detailier in the following sections.

#### **5.1.1 Assigning an IP-address to a Bluetooth Device**

Currently the Bluetooth specification supports TCP/IP only over Point-to-Point protocol (PPP) connections that are not very useful especially in the case of ad hoc networks. More than that PPP is not very efficient protocol and considering the limited and varying bandwidth of radio frequencies all extra headers and traffic should be avoided as much as possible. And as described detailier in chapter 2.2 TCP/IP is not necessarily the best available solution for wireless media. Even more problems arise from the restrictions of different operating systems because IP addresses should be assigned dynamically on the fly. This approach will face problems especially in the case of ad hoc networks where some of the participants, most likely the master, should handle all

the tasks involved (assign IP addresses, inform all clients about the others, keep track of the usage of IP addresses and their correspondence to Bluetooth hardware addresses).

There is some work going on to extend the use of IP on Bluetooth networks. These include e.g. the proposals of Personal Area Networking Working Group [16] and BLUEPAC [18]. These proposals handle most of the issues including routing issues and handoff support but none of them is finished yet and they are not part of Bluetooth specification 1.1.

A method to assign a local IP address to Bluetooth devices is presented in BLUEPAC [18]. This solution relies on DHCP to assign unique IP address to all devices in the BLUEPAC network area. The BLUEPAC area has a central DHCP server that is responsible for assigning IP addresses (Figure 6.1). The idea is that base stations act as DHCP relays and relay DHCP messages between mobile devices and the centralized DHCP server by using the Bootstrap Protocol (BOOTP). IP addresses obtained from the server have limited lifetime and a device has to renew its address before it times out in order to retain it. BLUEPAC also offers a solution for handoff support on transport layer.

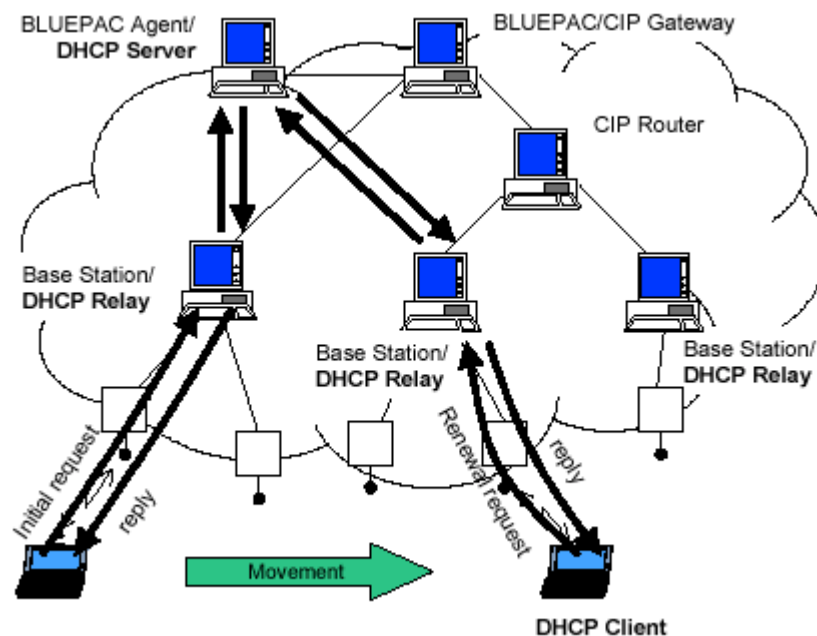


Figure 6.1: DHCP in BLUEPAC



### 5.1.2 Tunneling

The third solution consists of using IIOP while in the fixed network and tunneling messages over the Bluetooth part of the network. This idea is described more detail in chapter 5 and in OMG's document Wireless Access and Terminal Mobility [14]. This solution has some advantages:

- Compatibility with traditional ORBs
  - CORBA solution using the tunneling method is possible to implement such a way that interoperability with traditional ORBs is maintained. This can be considered as a huge advantage because it doesn't force service providers who offer services in fixed networks to change their existent CORBA providers and solutions.
- Low processing requirements
  - The process of tunneling itself is quite simple and straightforward so it is suitable for low processing power mobile devices.
- Possible future usage
  - Because this solution relays heavily to OMG's proposal it might have long lifetime with slight modifications if Wireless access and terminal mobility proposal will be widely accepted.
- Compatibility with Bluetooth specification
  - Because no modifications are needed to Bluetooth itself manufacturers don't need to implement any extra, non-standard functionality in their drivers.
- Fixed network doesn't have to provide functionality for dynamic IP address assignment for Bluetooth devices (i.e. DHCP or other that kind of solutions).

### 5.1.3 Mapping of GIOP to Bluetooth

As stated earlier CORBA definition allows mapping of GIOP to virtually any network protocol. Basing on this GIOP can be mapped onto some Bluetooth layer as well. However this approach might be laborious and time consuming because some heavy



testing is needed in order to ensure interoperability with other ORBs. This kind of mapping has on the other hand some advantages too. Most importantly it minimizes bandwidth usage because no additional information (i.e. IIOP and TCP/IP headers) is transferred. In addition it doesn't require any extra processing, which is important on mobile devices because of their limited processing capabilities. And if a network consists of only Bluetooth-enabled devices the solution is simple because all devices involved use same network media and protocol. If access to fixed network is needed then the mobile device and the last TPC/IP capable node before the Bluetooth network have to use gateways that translate IIOP messages to Bluetooth mapped GIOP messages and vice versa. This of course lengthens latency times because of the time required to process messages in the gateway.

## **5.2 Wireless CORBA on Bluetooth Ad Hoc Networks**

Because networking support in general case of scatternet is a matter of future, we can now consider only mapping of CORBA on Bluetooth piconets. On a separate piconet consisting of devices that support PAN Profile even traditional CORBA could be used. There is no fixed network, there are no different access points, and hence there is no need for message redirections to support mobility. And only wireless character of Bluetooth connection and necessity of mobility support in the case when the piconet gets access to a fixed network could force us to use wireless CORBA. Usage of wireless CORBA is inevitable if we use GIOP mapping or tunneling over Bluetooth. Access Bridge then resides on the piconet master node alongside with the CORBA Naming Service and redirects messages from one slave to another.

### **5.2.1 Advertising**

In order to find, use and register CORBA objects some mechanism that makes clients aware of different objects is needed. The native CORBA method for this task is the naming service. In the case of access point architecture this hardly causes problems because the naming service can be run on some fixed network node that all clients are aware of. Just like in the static, non-mobile environment clients should know the



location of the naming service. Things turn to quite different in ad hoc networks. Because addresses are not static i.e. it can't be assumed that client knows the address of some service beforehand there has to be some way to find out where the naming service is running or where the CORBA objects are located. For this purpose Bluetooth's native method, Service Discovery Application Profile can be used. This leaves us two different approaches: Service Discovery Application Profile can be used to specify either the location of the naming service or CORBA objects.

### **5.2.2 Using SDP to Locate the Naming Service**

A device can add the naming service to its SDP database and other devices can find it using SDP query and then use the naming service to obtain or register object references. The naming service can be installed either one specified location (most likely master of the piconet) or any device can be allowed to set up a naming service of its own. Running the naming service only at the master is simpler solution because all devices can then assume beforehand where the naming service is running. It removes the need to do multiple SDP and naming service queries in order to find a suitable service. It also follows the principle to have only limited number of naming services that all clients are aware of.

### **5.2.3 Using SDP Instead of the Naming Service**

In order to minimize processor usage on mobile devices SDP can be utilized to replace the naming service totally. It also adds some flexibility because all devices can advert their services more easily. All to do is to add the service to local SDP database. It has some restrictions however because a client trying to find some service has to possibly browse many devices' SDP database in order to find what it is looking for instead of doing just one call to the naming service (this assumes that the location of the naming service is known beforehand). Additionally it means that direct binding has to be used to invoke CORBA objects. This isn't recommended by OMG because direct binding is meant to be used only to locate services like the naming service and the trading service. Preferred method to locate objects is the naming service.



## 6 CONCLUSIONS

In this deliverable we studied the mapping of CORBA to Bluetooth. We found that

- Wireless CORBA approach can be used on Bluetooth networks both for access to fixed networks and on standalone piconets
- GIOP tunneling over TCP requires cumbersome infrastructure of fixed network to support IP addressing of Bluetooth devices
- GIOP tunneling over one of Bluetooth protocols (e.g., L2CAP) allows to minimize modifications while using all the advantages of wireless CORBA
- Bluetooth SDAP can be used to advertise CORBA services on mobile devices



## REFERENCES

- [1] <http://www.ietf.org/html.charters/zeroconf-charter.html>.
- [2] <http://www.ietf.org/html.charters/manet-charter.html>.
- [3] <http://www.ietf.org/html.charters/mobileip-charter.html>.
- [4] H. Balakrishnan, S. Seshan, and R. Katz. Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks. *Wireless Networks*, 1(4): 469-481, Feb 1995.
- [5] C. Perkins. IP Mobility Support, Oct 1996. RFC 2002.
- [6] C. Perkins and D. B. Johnson. Route Optimization for Mobile IP, Nov. 2000. Internet Draft, draft-ietf-mobileip-optim-10.txt (work in progress).
- [7] Wireless Access and Terminal Mobility, Request For Proposal, OMG telecom/99-05-05.
- [8] Object Management Group. The Common Object Request Broker: Architecture and Specification, V2.4.2. Object Management Group, February 2001.
- [9] M. Haar, R. Cunningham and V. Cahill. Supporting CORBA Applications in a Mobile Environment. *MobiCom '99: 5th International Conference on Mobile Computing and Networking*. Seattle, August 1999.
- [10] R. Ruggaber, J. Seitz and M. Knapp. P<sup>2</sup>: a Generic Proxy Platform for Wireless Access and Mobility in CORBA. 19th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC), Portland, USA, July 2000.
- [11] F. Pählke, R. Ruggaber and J. Schiller. Providing Nomadic CORBA Servers by Integrating P<sup>2</sup> and FATIMA. *European Wireless 2000*, Dresden, September 2000.
- [12] <http://www.cs.helsinki.fi/u/kraatika/wCORBA.html>.
- [13] Service Machine Development for an Open Long-term Mobile and Fixed Network Environment. Editor Kimmo Raatikainen. Response to OMG Telecom RFI on Wireless Access and Mobility. OMG telecom/98-08-08.
- [14] Wireless Access and Terminal Mobility, Draft Adopted Specification, OMG dtc/2001-05-01.
- [15] Specification of the Bluetooth system: Core, v1.1 Feb 22, 2001.



- [16] Kris Fleming. [http://internet.motlabs.com/Bluetooth BOF at 50th IETF PAN Talk\\_files/frame.htm](http://internet.motlabs.com/Bluetooth%20BOF%20at%2050th%20IETF%20PAN%20Talk_files/frame.htm).
- [17] Specification of the Bluetooth system: Profiles, v1.1 Feb 22, 2001.
- [18] M. Albrecht, M. Frank, P. Martini, M. Schetelig, A. Vilavaara and A. Wenzel. IP Services over Bluetooth: Leading the Way to a New Mobility. Proceedings of the 24th Conference on Local Computer Networks, Lowell, MA, October 1999, pp. 2-11.