Mobility support for ubiquitous Internet access

Abstract

This document describes an architecture that is providing Internet access to mobile hosts, by allowing them to access this architecture through various access points and using various wireless technologies. In particular, this deliverable focuses on QoS and mobility between various IP subnetworks that are using different wireless technologies, e.g., UMTS (Universal Mobile Telecommunication Services) and Bluetooth.

Contents

1 Introduction

The diversity of the current Internet applications from the most simple ones like e-mailing and web browsing going to high demanding real time applications like the IP telephony and multimedia conferencing, has raised the expectations that both, users and software developers of these applications have from Internet. These demands are driving the development and introduction of QoS in the Internet. Furthermore, the increased user demand on being reachable everywhere and any time introduces high requirements from the future Internet technology to support user mobility.

This requires that the next generation Internet architecture will have to be very flexible and open, capable of supporting all these different types of networks, terminals and applications. In this document we investigate a network architecture that can provide ubiquitous Internet access to mobile hosts, by allowing them to access this architecture through various access points and using various wireless technologies. However, this architecture is at the moment not able of providing a complete solution. Moreover, in this document several open issues related to this topic are identified.

Based on the above given considerations we have created a list of requirements that should be fulfilled by our proposed architecture:

- The IP core network is based on either the Diffserv network architecture or a mix of Diffserv and overprovisioned IP core networks. The second option is only valid if the provider of IP overprovisioned networks guarantees certain QoS bounds.
- Both static and dynamic provisioning of resources in the IP Diffserv core network should be supported.
- The access networks may support any of the existing IP QoS management architectures, like Integrated Services Architecture, Differentiated Services Architecture, QoS capabilities of the access technology, overprovisioning of resources, etc. In the situation that an access network operator configures its network in such a way that it becomes overprovisioned, applications may or may not gain the demanded QoS.
- The access networks may support different access technologies, e.g. Bluetooth, General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Wireless Local Area Network (W-LAN).
- Each mobile host that supports multiple access technologies should be able to select the most efficient and cost-effective technology that supports the application QoS requirements.
- Handoffs between different access networks and technologies should be supported. These handoffs should be seamless to the user. In other words, the user should not experience any disruptions in the quality of the used application.
- Global QoS interoperation of local QoS mechanisms should be possible.

In this document we used as IP subnetwork examples the UMTS (Universal Mobile Telecommunication Services) and Bluetooth technologies. However, the IP QoS and IP mobility scenarios described in this document can also be used in the situation that other technologies are involved. In particular, this deliverable focuses on QoS and mobility between various IP subnetworks that are using different wireless technologies. Additionally, it is considered that a roaming Host has the possibility of being simultaneously connected on different wireless technologies. The main challenge will be to select the wireless technology that satisfies all the user and network provider demands in the most efficient way.

This deliverable is organised as follows. Section 2 describes the network topology. Section 3 gives a brief summary of the framework for IP QoS and mobility presented in [KaRe00]. Furthermore, it as example, it emphasises the QoS architectures used in UMTS and Bluetooth. Section 4 presents various solutions on the QoS and mobility between various IP subnetworks that are using different wireless technologies. The protocols used to support the mobility solutions are the current specified versions of the Mobile IPv4 and Mobile IPv6 protocols. As resource reservation protocol we use the Resource Reservation Protocol (RSVP) that is applied on an end to end basis. However, the IP core networks is using the Differentiated Services concept, that is dynamically managed by the Load Control protocol [WeTu00]. Section 5 presents a possible way of achieving seamless handoff in Mobile IPv4 and Mobile IPv6. Finally, Section 6 concludes and lists the derived open issues.

Note that the ideas proposed in this document by the authors do not imply any kind of Ericsson strategy. Moreover, it is assumed that the reader is familiar with the UMTS, Bluetooth, TCP/IP protocol stack, and Integrated and Differentiated Services frameworks.

2 Network Topology

In this document we investigate a network architecture that can provide ubiquitous Internet access. Furthermore, the IP subnetworks that are mainly used in this study are the UMTS and the Bluetooth technologies. Before presenting the network topology that is investigated in this study, we present on a high abstraction level, the UMTS/GPRS (General Packet Radio Service) and Bluetooth networks.

2.1 UMTS/GPRS network topology

The UMTS/GPRS network topology is defined by the 3GPP (3rd Generation Partnership Project) standardisation body. The main description of the current UMTS/GPRS network specification is given in [3GPP23.060], while the possible evolutionary steps of the GPRS core network towards a mainstream IP network are described in [3GPP23.923]. The UMTS/GPRS description given by us in this section is based on [3GPP23.923].

3GPP mentions that the evolution of the GPRS network towards a mainstream IP network may be accomplished in three steps. The main goal in this evolution is to provide IP mobility using the current and/or future version of Mobile IPv4 [RFC2002] (see also [Kar99]). The abbreviation used in [3GPP23.923] for the future version of Mobile IPv4 is (MIP+). Each of these steps are backwards compatible with terminals and networks that are not supporting Mobile IP.

The first step, named in [3GPP23.923] as “Offering Mobile IP(+) service”, is depicted in Figure 2-1. The description of the entities depicted in Figure 2-1 are described in [3GPP23.060] (see also [Kar00]). The main entities that are participating in this evolutionary steps are the SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node), FA (Foreign Agent) and HA (Home Agent). Furthermore, note that the UTRAN (UMTS Terrestrial Radio Access Network) is the UMTS access network. Two entities are used to protect the GPRS core network from unwanted traffic. One of them, depicted as “filter” in Figure 2-1 is used to avoid unwanted traffic generated by an external IP domain into the internal IP network. The other entity is the “Border Gateway” (BG) that is mainly used to avoid unwanted traffic between GPRS PLMNs (Public Land Mobile Networks).

In this step the current GPRS structure is maintained, being able to handle the mobility within the PLMN. The future version of Mobile IP (MIP+) is used to provide IP mobility between other systems such as LAN’s, Bluetooth and UMTS.

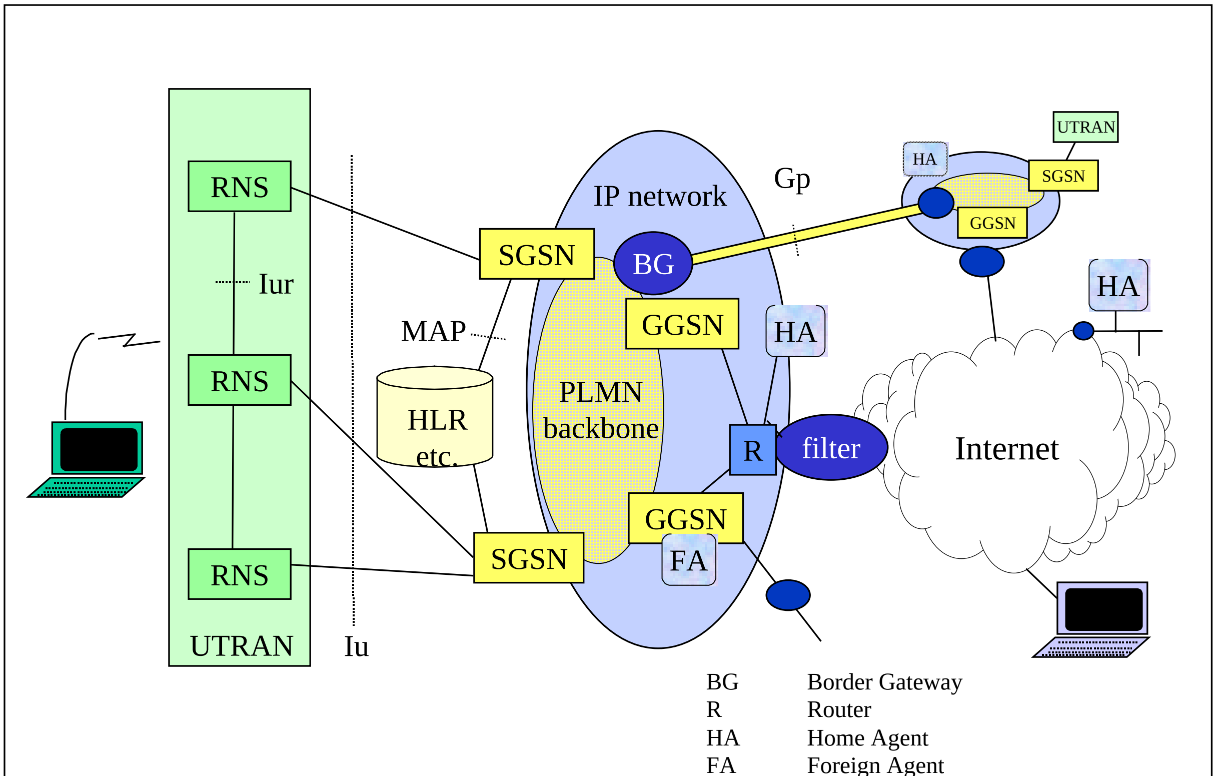


Figure 2-1: IP mobility in GPRS: Step1 (from [3GPP23.923])

The second evolutionary step, named in [3GPP23.923] as “Intermediate GPRS-MIP(+) system”, is depicted in Figure 2-2.

In this step the efficiency in the routing due to mobility, is increased. This is accomplished during the inter SGSN handoff, by changing the GGSN/FA, to which the mobile host is attached to a more optimal one. The packet loss during handoff is minimised by e.g., maintaining for a short time tunnels from the new SGSN to both the new and old GGSN/FA. In the situation that the mobile host transfers data during inter-SGSN handoff, the change of GGSN/FA, from old to new, might be transferred after the data transfer has been completed.

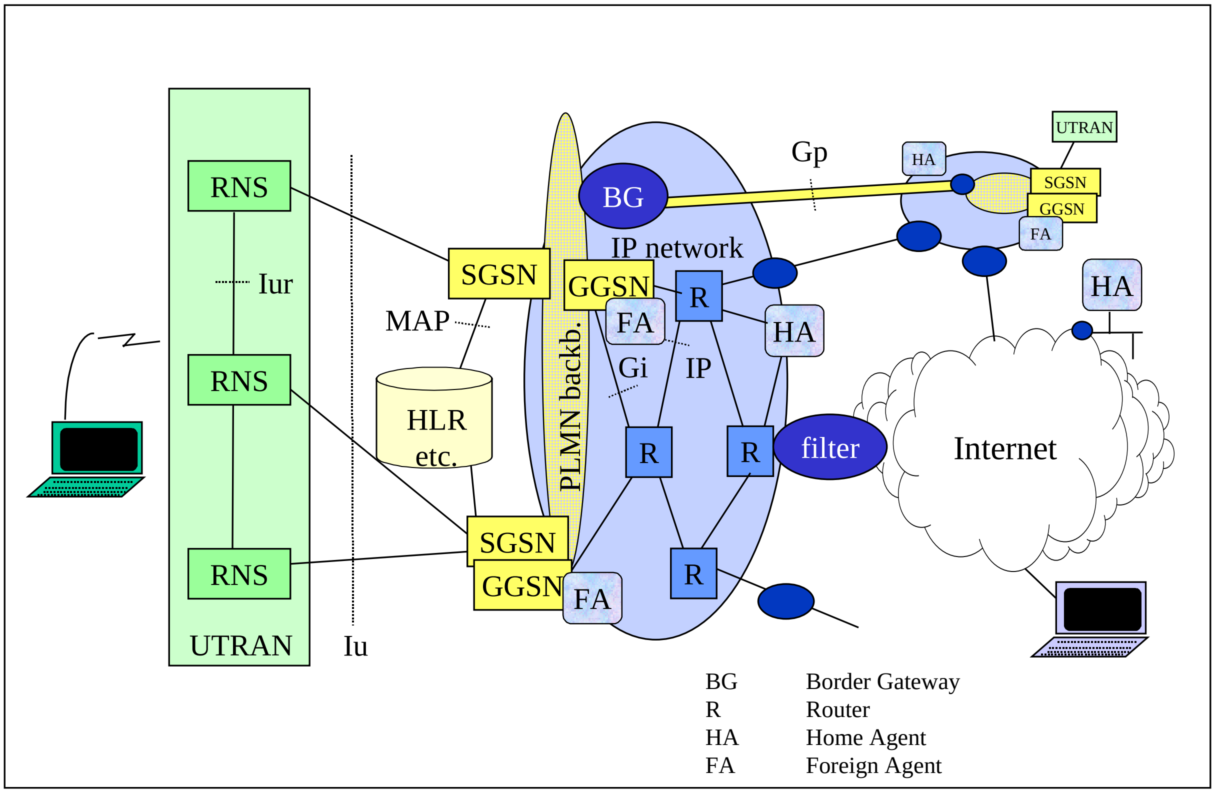


Figure 2-2: IP mobility in GPRS: Step 2 (from [3GPP23.923])

The third evolutionary step, named in [3GPP23.923] as “Using Mobile IP+ for Intra System Mobility”, is depicted in Figure 2-3. In this step the SGSN and GGSN nodes are combined into one node, i.e.,

IGSN (Internet GPRS Support Node). The mobility within the PLMN CN and between networks is now completely handled by (MIP+).

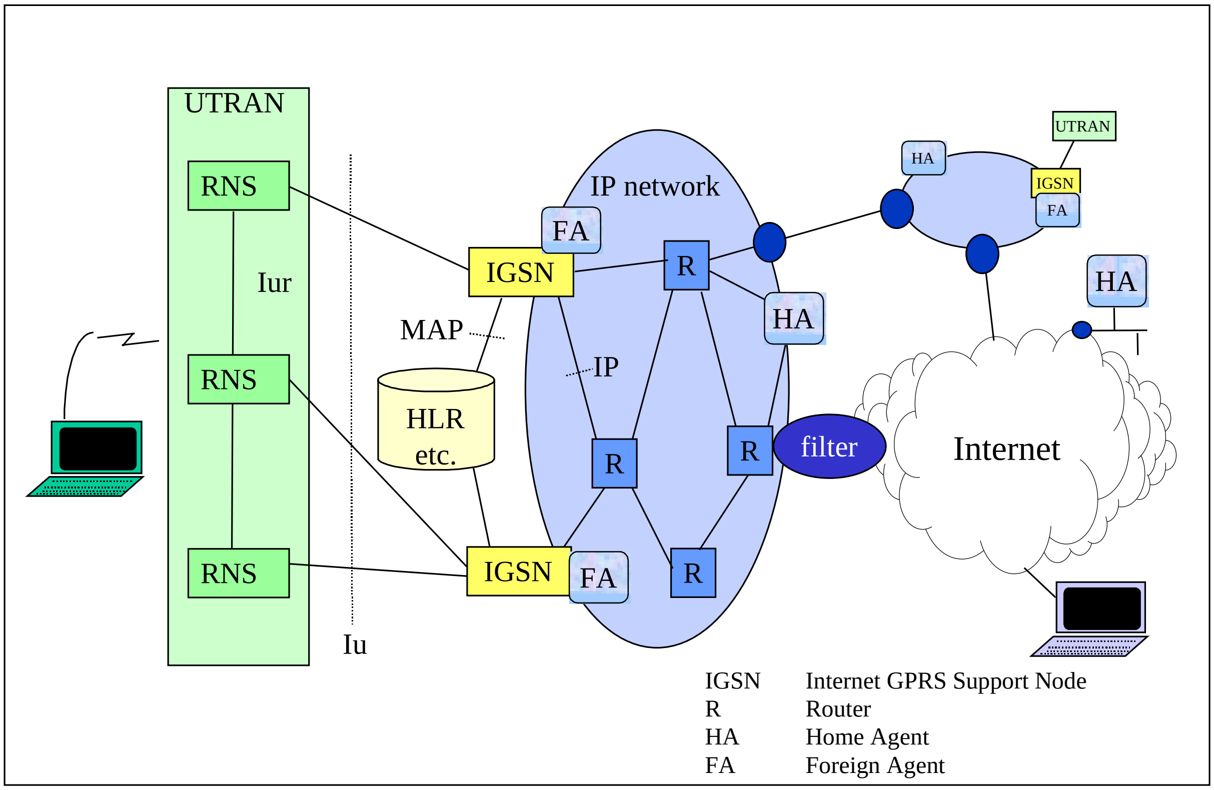


Figure 2-3: IP mobility in GPRS: Step 3 (from [3GPP23.923])

2.2 Bluetooth network topology

The Bluetooth access technology, see e.g., [Haa98], [Zee00], is mainly specified as an ad-hoc technology that enables different electronic devices (see Figure 2-4) to connect and communicate wirelessly to each other in a relatively short range without having to be configured or connected to a backbone network. It is claimed (see [Haa98]) that Bluetooth being a cheap and efficient radio technology, that can be integrated in a small power-efficient radio Integrated Circuit (IC) will be superior compared to the existing infrared technology used for the same purpose.

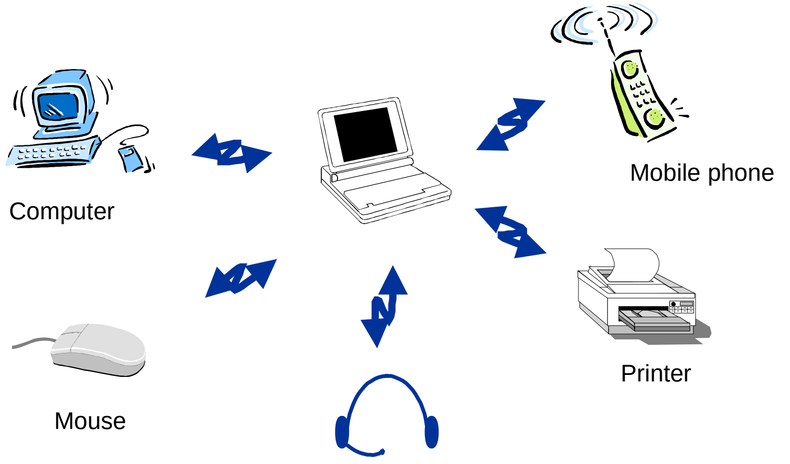


Figure 2-4: Local ad-hoc connectivity (from [Zee00])

The frequency band that is used for Bluetooth is the 2.45 GHz Industrial-Scientific Medical (ISM) band and the medium available bandwidth is 80 MHz.

The Bluetooth devices are able to communicate with each other through radio communication channels. These channels use a frequency-hop/time-division-duplex (FH/TDD) scheme (see e.g., [Haa98], [Zee00]) and are divided into 625 μs time slot intervals, wherein a different hop frequency is applied for each slot. The nominal hop rate is 1600 hops per second. In order to reduce the probability of collisions, the frequency hop per each channel is determined pseudo randomly and is based on a combination of parameters that are used to identify a channel.

Two or more devices that share the same channel form a piconet. In each piconet a device can simultaneously communicate with up to seven other devices. However, during this simultaneous communication between the participants of a piconet there is only one device, called master, that is able to regulate the intercommunication traffic between the piconet participants. The rest of the participants are called slaves.

It is very important to note that the master- slave functionality can be switched**.** In other words, a requesting slave will become a master and the master will become a slave.

This could for example be useful for the situations that due to malfunctioning, the master will probably collapse and therefore, as soon as possible should handle over its master responsibility to a slave.

In order to increase the Bluetooth overlapping area of coverage and the number of users that simultaneously communicate, an additional Bluetooth scheme is specified that is consisting of a group of piconets and is called scatternet.

In [Haa98] is mentioned that in a scatternet the total throughput accumulated over all piconets will increase by increasing the number of piconets. However, when the number of piconets is increased, the collision probability will also increase and therefore the frequency hop system degrades gracefully. By using simulation it has been shown that for a scatternet consisting of 10 piconets (see [Haa98]) the reduction in throughput per piconet is less than 10 % compared to the achieved throughput in a single piconet.

The Bluetooth technology can be used as an ad-hoc technology that enables different electronic devices to connect and communicate wirelessly to each other without using a backbone network. Moreover, recently, the Bluetooth devices are capable of getting access to the Internet (see Figure 2-5) via an entity denoted as the Network Access Point (NAP).

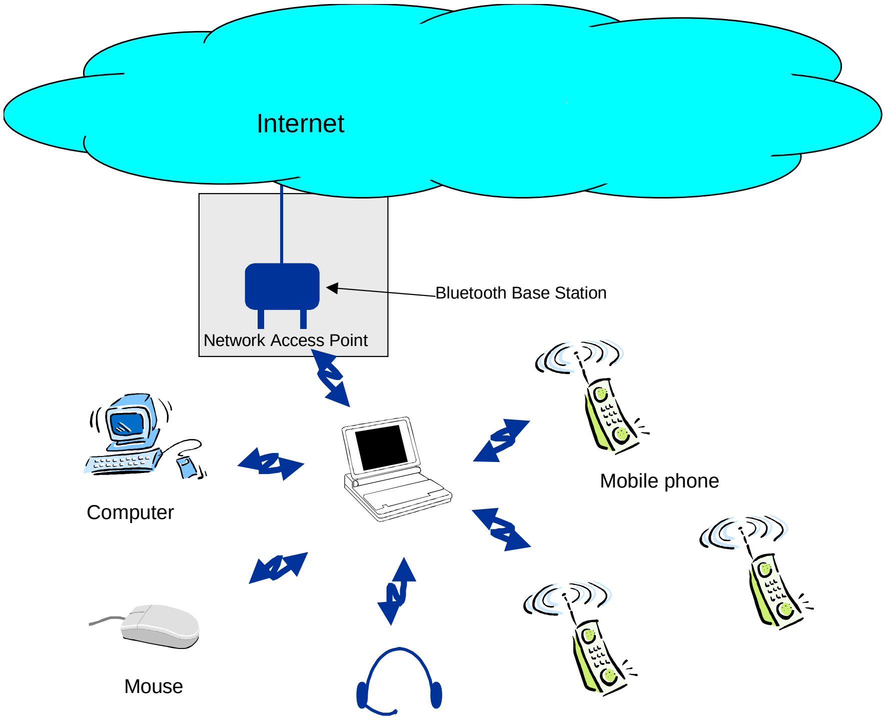


Figure 2-5: Bluetooth Internet access in a piconet

In a piconet up to 8 devices can simultaneously inter-communicate. Assuming that in a piconet, one of the Bluetooth devices is a base station (see Figure 2-5) that has access connectivity to an IP network, there could be at most 7 other active devices that can simultaneously communicate with this base station. This number can be increased by creating a scatternet, wherein the base station might operate as a master in one of the piconets and as a slave in all the other piconets that are composing the scatternet. Note that in a scatternet a device may operate in different piconets that are composing this scatternet, but it can only be master in one of these piconets (see [Haa98]). Moreover, in a piconet a base station may become a slave. In this situation the base station will only be able to communicate with another slave of this piconet via the master. It is expected that this will impose a performance degradation compared to the situation that the base station is by itself a master. This degradation will increase by increasing the number of devices that simultaneously need to have Internet access.

This performance degradation can be eliminated by considering the NAP as the piconet master. Thus even if the created piconet is not initiated by this NAP but by another device, a master-slave switch role between this device and the base station should take place. However, the NAP should be able to function in both modes, i.e., master and slave.

2.3 Investigated Network Architecture

In this document we investigate a network architecture that can provide ubiquitous Internet access. The Network Architecture which is depicted in Figure 2-9 consists of a UMTS subnetwork similar to the one depicted in Figure 2-3 and of a Bluetooth subnetwork similar to the one depicted in Figure 2-5. This network architecture identifies the following components:

- Host X, represents either one entity (see Figure 2-6 and Figure 2-7) or a group of entities (see Figure 2-8) that can inter-communicate with the end user. In this architecture we consider that the Host X is represented by one entity, see Figure 2-6 and Figure 2-7. The scheme wherein the Host X is represented by a group entities is considered as an open issue.

Furthermore, in this architecture it is considered that the Host X is capable of being connected simultaneously to two different wireless technologies, i.e., UMTS and Bluetooth. However, in this architecture we consider that for the same area covered by both wireless technologies, the entities supporting one of these wireless technology are included in a different IP subnetwork than the entities supporting the other wireless technology. Note that we consider the situation where both wireless technologies are covering the same area and are belonging to the same IP subnetwork as an open issue.

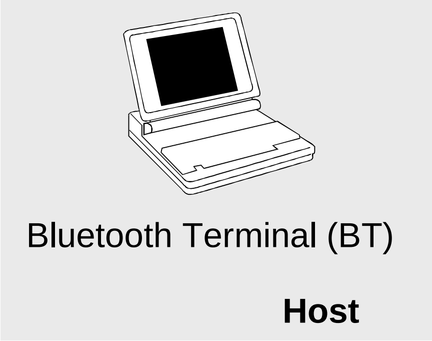


Figure 2-6: Host represented by one entity

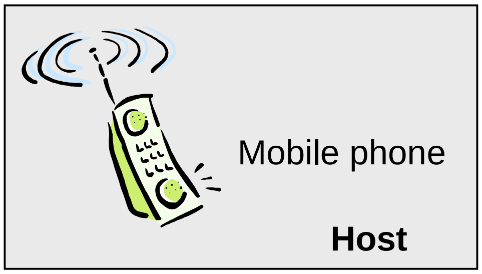


Figure 2-7: Host represented by one entity

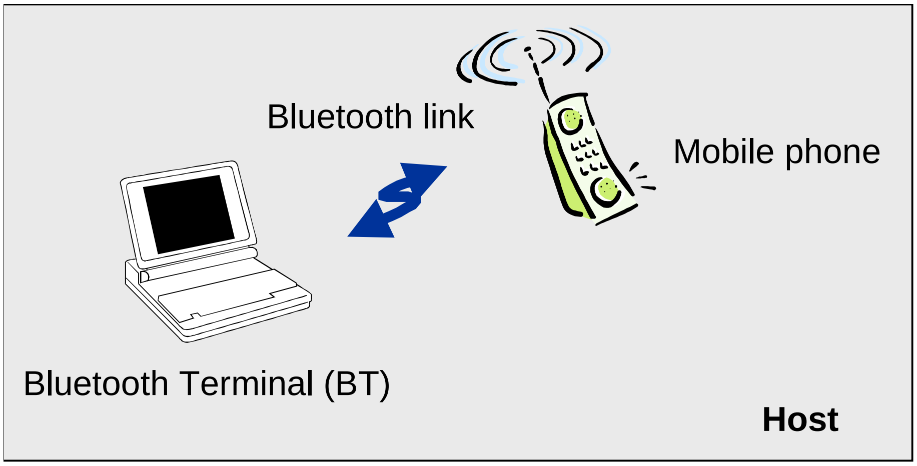
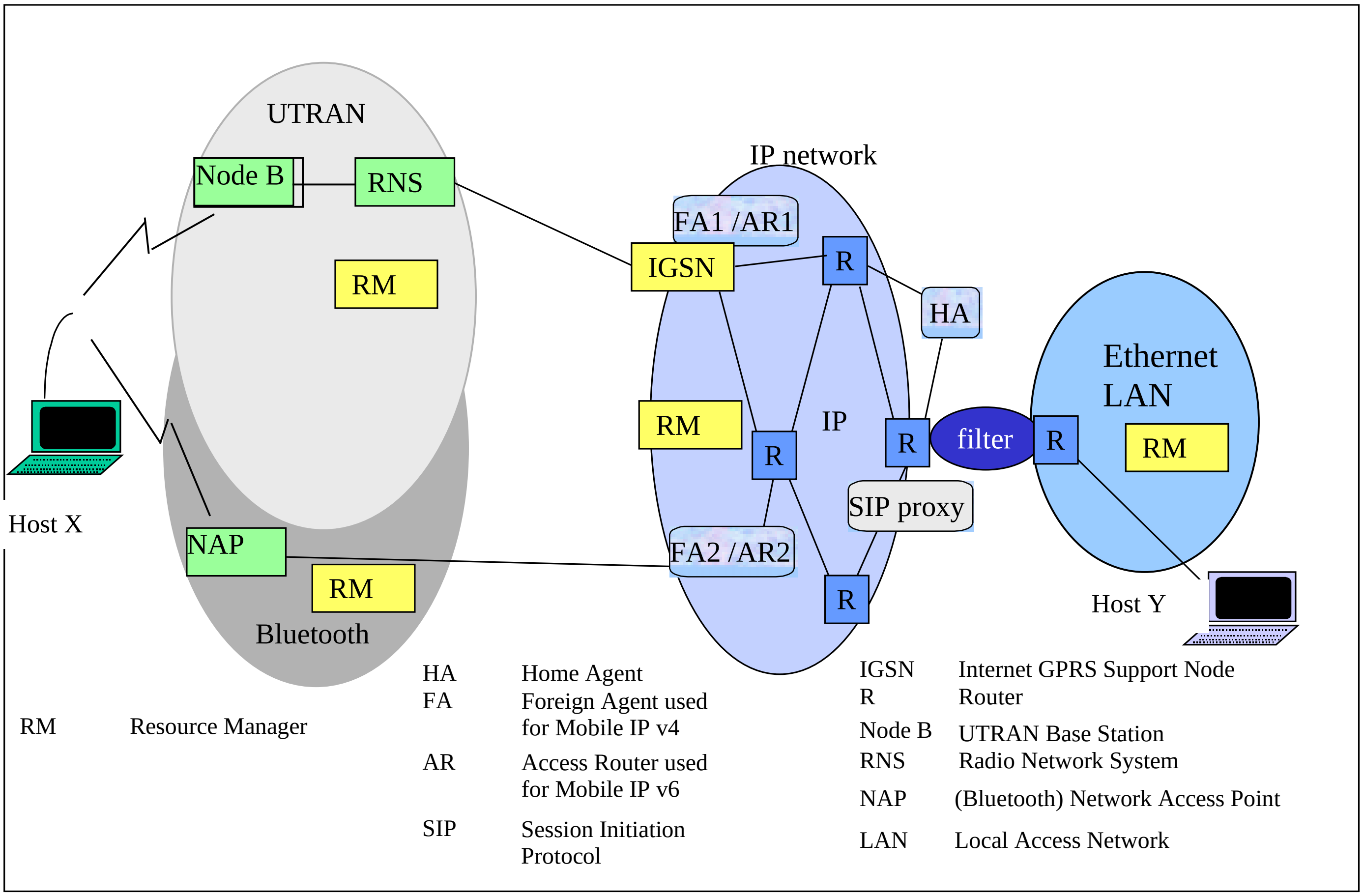


Figure 2-8: Host represented by a group of entities

✓ BT (Bluetooth Terminal) represents the mobile Bluetooth device, e.g. laptop, PDA;

✓ Mobile phone represents the UMTS mobile device;

- Host Y, represents a fixed end terminal that is using the Ethernet technology and it is capable of inter-communicating with the end user.
- NAP: (Network Access Point) represents a base station that serves one or more piconets (depending on the number of radio interfaces) and is considered as a public access point for BT's. This entity is also interconnecting the Bluetooth access network to a public network, e.g. internet.
- Node B: represents an UTRAN (UMTS Terestrial Radio Access Network) base station;
- RNS: (Radio Network Subsystem): is controlling a number of base stations by managing the radio channels on the air interface including soft handoffs in the UTRAN. It includes soft handoff devices to implement macrodiversity of air frames between cells. Furthermore, the RNS is responsible for the reservation in the UTRAN of the transport resources.
- IGSN (Internet GPRS Support Node): it combines the SGSN and GGSN functionalities and is able to handle the Mobile IP protocol. The SGSN (Serving GPRS Support Node) physical entity: is in general responsible for the communication between the UMTS/GPRS network and all the UMTS users located within its service area. It supports the mobility management (among others storing the Visitors Location Register (VLR), the visitors user profile (International Mobile Subscriber Identity) and the Packet Data Protocol (PDP) context), security management (i.e., authentication and ciphering), charging information and logical link management for each Mobile Station (MS) that is roaming in its service area. A PDP is representing the network protocol used by an external Packet Data Network (PDN) that is interfacing to GPRS. The PDP context represents the relation between a PDP (e.g., IP) address, PDP type (i.e., static or dynamic address), the address of a GGSN that serves as an access point to an external PDN, and a Quality of Service (QoS) profile. The PDP context is stored in the MS, SGSN and GGSN. The GGSN (Gateway GPRS Support Node): is the gateway towards external networks, such as GPRS networks operated by different network operators, e.g., IP networks. It can translate data formats, signalling protocols and address information to allow communication among different networks. Furthermore, the GGSN can provide dynamic allocation of network (e.g., IP) addresses.
- FA (Foreign Agent): it is used in Mobile IPv4 and it represents a router on a Mobile Host's visited network which co-operates with the Home Agent to complete the delivery of IP packets to the Mobile Node while it is away from home. FA1 is used in the UMTS IP subnetwork, while FA2 is used in the Bluetooth IP subnetwork.
- AR (Access Router): it is used in Mobile IPv6 and it represents the first hop router that a Mobile Host is connected to. AR1 is used in the UMTS IP subnetwork, while AR2 is used in the Bluetooth IP subnetwork.
- HA (Home Agent): it is used in Mobile IPv4 and Mobile IPv6 and it represents a router on a Mobile Host's home link with which the Mobile Host has registered its current care-of address. While the Mobile Host is away from home, the Home Agent intercepts packets on the home link destined to the Mobile Host's address, encapsulates them, and tunnels them to the Mobile Host's registered care-of address.
- SIP (Session Initiation Protocol) proxy: it is a SIP node that is used to locate the destination party of an invitation to a session and it remains in the signalling path for the duration of the session setup
- RM (Resource Manager): It manages the resource reservation and resource allocation procedures within one IP subnetwork



RM	Resource Manager
HA	Home Agent
FA	Foreign Agent used for Mobile IP v4
AR	Access Router used for Mobile IP v6
SIP	Session Initiation Protocol
IGSN	Internet GPRS Support Node
R	Router
Node B	UTRAN Base Station
RNS	Radio Network System
NAP	(Bluetooth) Network Access Point
LAN	Local Access Network

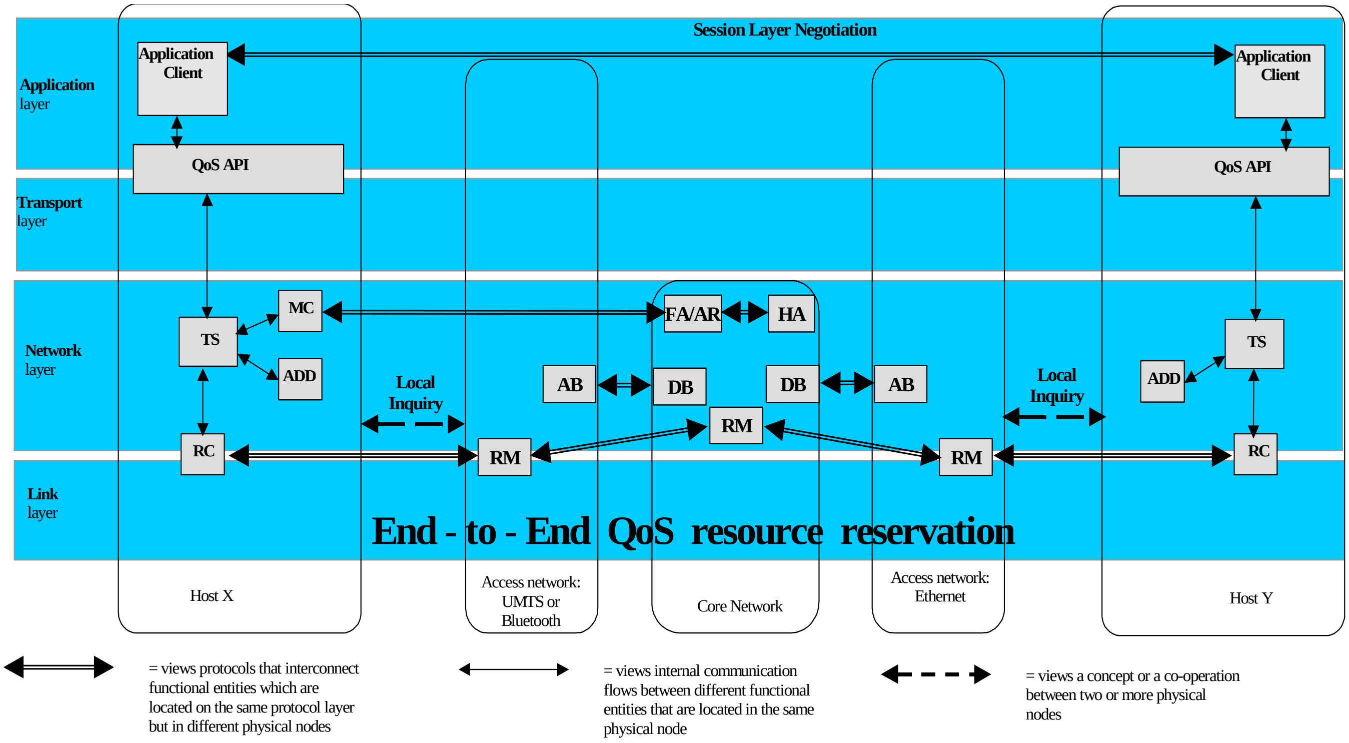
Figure 2-9: The investigated Network Architecture

3 Background information

This section describes the IP QoS and mobility background used in this investigation. First of all, the IP QoS and mobility framework used in this investigation is presented. Furthermore, this section presents the IP QoS schemes used in the UMTS and Bluetooth technologies. Moreover, the IP mobility scheme based on Mobile IP is briefly presented.

3.1 Framework for IP QoS and mobility

The framework for IP QoS and mobility used in this investigation is based on the framework presented in [KaRe00]. Applying this framework to the network architecture depicted in Figure 2-9 a QoS functional decomposition, see Figure 3-1, is obtained. The architecture depicted in Figure 3-1 consists of three major building blocks: Hosts, local Access Networks, and a Diffserv Core Network. Hosts represents the calling and called hosts, i.e. Host X and Host Y, respectively. The local Access Network represents either the UMTS or the Bluetooth wireless access technologies and it includes local QoS mechanisms. The Core Network represents one Diffserv domain, but it may consist of more than one Diffserv domains. Each block includes the main active functional entities that have to be used in the QoS and mobility framework. Furthermore, Figure 3-1 depicts the allocation of these functional entities into an TCP/IP protocol suite.


Session Layer Negotiation
Application layer
Transport layer
Network layer
Link layer
Application Client
QoS API
TS
MC
ADD
RC
Local Inquiry
RM
AB
DB
FA/AR
HA
RM
DB
AB
RM
Local Inquiry
ADD
TS
RC
QoS API
Application Client
End - to - End QoS resource reservation
Host X
Access network: UMTS or Bluetooth
Core Network
Access network: Ethernet
Host Y
= views protocols that interconnect functional entities which are located on the same protocol layer but in different physical nodes
= views internal communication flows between different functional entities that are located in the same physical node
= views a concept or a co-operation between two or more physical nodes

AB	Access Boundary (it is located in a router (R))	HA	Home Agent
ADD	functional entity that could be added in the future	RC	Resource Client
DB	Diffserv Boundary (it is located in a router (R))	RM	Resource Manager
MC	Mobility Client	TS	Technology Selector
FA	Foreign Agent (used in Mobile IPv4)	QoS API	Quality of Service Application Program Interface
AR	Access Router (used in Mobile IPv6)		

Figure 3-1: QoS & Mobility Framework building blocks and protocols

3.1.1 Protocols

The following examples of protocols may be used to interconnect the various functional entities in the QoS and Mobility framework.

Session Layer Negotiation protocol is any protocol that the Application entities will use for initiating a session between hosts. It might be SIP (Session Initiation Protocol) or H.323, or it might be an entirely new protocol, as long as it fits within the architecture requirements listed in Section 1. In this investigation we assume that this protocol is the SIP protocol [RFC2543].

End-to-End QoS Resource Reservation protocol is a protocol that will be used for resource reservation in the end-to-end path. It might be RSVP [RFC2205], RSVP aggregation [BaIt00], tunnelled RSVP, or a combination of the former protocols. In this investigation we assume that this protocol is the RSVP protocol.

The Local Inquiry views the information exchange between the host and the access network. It is mainly used for local resource inquiry (see Figure 2-9), i.e. communicating with the access network resource manager. This information exchange can be implemented using various protocols e.g., resource reservation protocols such as RSVP, network management protocols such as SNMP [RFC1905] or COPS [RFC2748], or mobility management protocols such as Mobile IP.

The mobility management protocol is any protocol that can provide the network mobility management, e.g., location management and handoff between different IP sub-networks. In this investigation we assume that this protocol is the Mobile IP protocol [RFC2002], [JoPe00].

3.1.2 Functional entities

The functional entities that are required for the QoS and mobility framework in the Hosts are:

- Application Client is realised by the Application layer and it is an abstraction of a QoS aware application. It is also required that the application client support the session layer protocols. When e.g., the application is SIP then the application client will be a SIP client.

- QoS API is the abstraction of mechanisms that based on application attributes (e.g. audio, video) and QoS requirements, determine the application's service profile. This functional entity is realised by the co-operation of the Application and Transport layers. However, the QoS API should be able to send and receive information to and from the Network and Link layers.

- The host Resource Client (RC) is the abstraction of the entity that is in fact a QoS decision point for the end host. It will provide the mechanism for resource control within the end host based on request and responses it receives from the QoS API, the Technology Selector (TS) and the Local Inquiry protocol messages. This functional entity is realised either entirely by the Network layer or by the co-operation of the Network and Link layers.

- The Mobility Client (MC) is a functional entity that in combination with the Mobility Agent located at the access networks is providing IP mobility management. The Mobility Client is realised either by the Network layer, e.g., Mobile IP, or by the Application layer, e.g., SIP mobility. In this investigation the Mobility Client is a Mobile IP client and it is realised by the Network Layer

- Technology Selector (TS) is the entity, which will be part of any mobile host that wishes to select a certain underlying radio technology and/or underlying wired technology supported by an access network. The TS is able to provide this selection by using certain criteria, based on e.g. application's service profile, mobility scenario, available resources, authentication and accounting scenarios. The TS functional entity is realised by the Network layer. In this investigation it is considered that the Technology Selector is able to select between two wireless technologies, e.g., UMTS and Bluetooth.

  We consider the development of the Technology Selector as an open issue.

- ADD (see Figure 3-1) represents any other functional entity associated with the Technology Selector that could be added to the framework and that should be located into the Host. Such functional entities could be the authentication and accounting management functional entities.

Figure 3-2 depicts the situation that the host is able and is willing to perform the technology selection. In this situation the host is capable of selecting one of the underlying radio technologies, e.g. Bluetooth and UMTS. The main operation is as follows.

The Host needs to start a real time application, e.g. VoIP. The QoS API will perform the mapping of the application requests to parameters that are understood by the TS. If the TS entity has the required profile information to perform the technology selection it will do so and it will inform the application entity (i.e. session client) about it. Otherwise, the TS will send one request, i.e. TS_Inquiry REQUEST to the Bluetooth access technology and another request to the other access technology, e.g. GPRS. Note that the TS_Inquiry Request may be sent in either one or more than one messages. These requests will include query information regarding for example: (1) the requested QoS parameters, (2) the authentication restrictions, (3) accounting restrictions, (4) the financial and complexity cost of a connection to the core network, etc. This query information will have to be distributed to all functional entities, e.g. RM, in the access technologies that will be able to answer them. The replies of each queried functional entity will be either sent individually in one TS_Inquiry RESPONSE or they will all be combined in one TS_Inquiry RESPONSE and sent to the Host TS. The TS by applying the predefined criteria will choose one of the access technologies and it will inform the application entity (i.e. session client) about it.

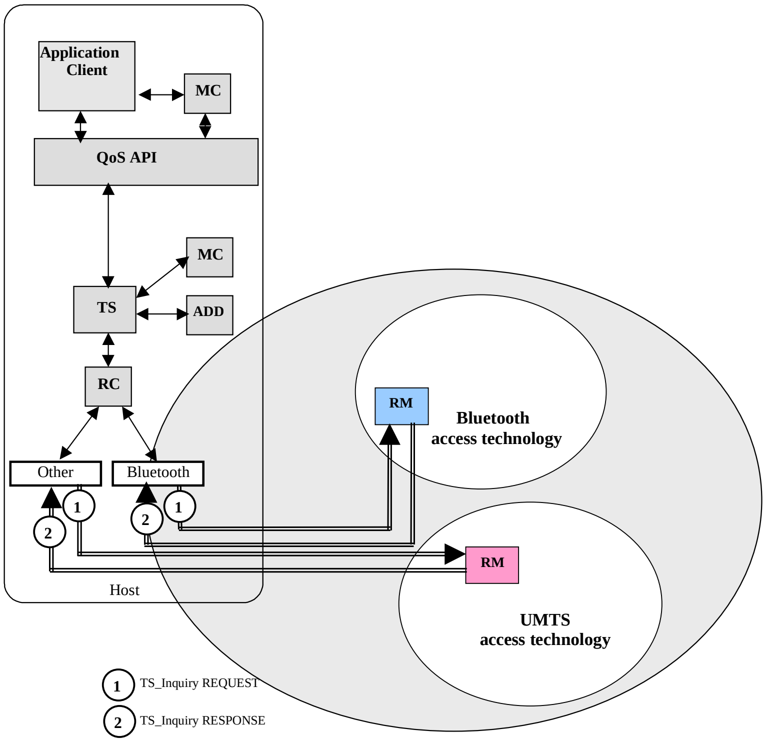


Figure 3-2: Example of technology selection accomplished by the host

The functional entities that are located in the core network and are used in the QoS and mobile framework should be in full compliance with the Diffserv network architecture definitions. The functional entities that are located in the Diffserv core network region are:

- The Resource Manager (RM) performs the resource allocation and admission control for the core network either statically or dynamically. We assume that it can be centralised (e.g. Bandwidth Brokers, [RFC2638] or [TeCh99]) or distributed within the core network (e.g. see [RFC2475]). This functional entity is realised by the Network layer.
- The Diffserv Boundary (DB) represents the functionality that is available in standard Diffserv border (R) routers (see e.g., [RFC2475]) and that is managing traffic aggregates from the adjacent domains in compliance with the SLS agreement. In some particular cases it might also perform other tasks for interoperation with other, non-Diffserv domains. This functional entity is realised by the Network layer.

The functional entities that are located in a Local Access Network and are necessary for the QoS and mobility framework are the following:

- The Resource Manager (RM) functional entity is applied in the access network and similarly to the Diffserv core network Resource Manager is responsible for resource allocation and admission control. Its specific realisation depends on the IP QoS architecture that will be used at the access network and it is realised either entirely by the Network layer or by the co-operation of the Network and Link layers.

- Access Boundary (AB) represents the functionality that is available in any edge device, e.g., Edge Router, residing at the periphery or boundary of an administrative domain. Its functionality depends on specific IP QoS architecture used at the access network and the architecture of the ingress routers of the Diffserv domain. This functional entity is realised by the Network layer.
- The functionality provided by the Foreign Agent, Home Agent and Access Router is already discussed in Section 2.3.

3.2 QoS in the UMTS/GPRS core network

The UMTS technology is capable of supporting application with different QoS requirements. Therefore, in UMTS different types of QoS classes are defined to efficiently satisfy these various types of applications.

3.2.1 UMTS QoS classes and attributes

The UMTS QoS classes (see [3GPP23.107]) are specified depending on delay sensitivity of the user data traffic used by certain applications. These are:

- Conversational class: this class represents conversational streaming applications, e.g., telephony speech that is very delay sensitive. Furthermore, they preserve time relation between the information entities of the stream;
- Streaming class: this class represents real time streaming applications that are not conversational. This could for example be the situation that the UMTS user wants to listen to real time speech or real time video.
- Interactive class: it represents all the non real time applications, such as Web browsing, server access. The main characteristics are the use of request reply pattern and preserve payload content.
- Background class: This class represents all the applications that are the most delay insensitive. In other words the data that is sent by such an application can be processed in the background. Such applications are e.g., e-mail, SMS (Short Message Service).

The list of QoS attributes that are used in characterising the above listed QoS classes are:

- *Maximum bit-rate (kbs):* defined as the maximum number of bits delivered that are delivered by UMTS at a Service Access point (SAP) within a period of time divided by the duration of the period;
- *Guaranteed bitrate (kbps):* defined as the guaranteed number of bits that are delivered by UMTS at a SAP during a period of time, divided by the duration of time;
- *Delivery order (y/n):* indicates if UMTS bearer provides in sequence delivery of SDU (Service Data Units) or not;
- *Maximum SDU (octets):* maximum allowed Sdu size;
- *SDU format information (bits):* list of possible exact sizes of SDU's;
- *Residual bit error ratio*: indicates the number of undetected bit error ratio in the delivered SDUs. It is eaual to the bit error ratio in the SDU's when no error detection is requested.
- *Delivery of erroneous SDU (y/n*): indicates whether the detected erroneous SDU's will be delivered or not.

- *Transfer delay (ms):* maximum delay for 95th percentile of the distribution of the delay of all delivered SDU during the lifetime of a bearer session. Delay is defined as the duration of time from the moment that a SAP requests to transfer a SDU up to the moment of time that the packet is delivered to another SAP.
- *Traffic handling priority:* relative importance of handling SDUs belonging to one UMTS bearer compared to the SDU's of other bearers.
- *Allocation/Retention priority:* specifies the relative importance of one UMTS bearer compared to other UMTS bearers for allocation and retention of the UMTS bearers.

Table 3-1 shows the UMTS bearer attributes and their relevancy for each bearer class, while

Table 3-2 shows the value ranges of the UMTS bearer attributes for each bearer class.

Table 3-1UMTS bearer attributes defined for each bearer class (from [3GPP23.107])

Traffic class	**Conversational class**	**Streaming class**	**Interactive class**	**Background class**
Maximum bitrate	X	X	X	X
Delivery order	X	X	X	X
Maximum SDU size	X	X	X	X
SDU format information	X	X		
SDU error ratio	X	X	X	X
Residual bit error ratio	X	X	X	X
Delivery of erroneous SDUs	X	X	X	X
Transfer delay	X	X		
Guaranteed bit rate	X	X		
Traffic handling priority			X	
Allocation/Retention priority	X	X	X	X

Table 3-2: Value ranges for UMTS Bearer Service Attributes (from [3GPP23.107])

Traffic class	**Conversational class**	**Streaming class**	**Interactive class**	**Background class**
Maximum bitrate (kbps)	< 2 048	< 2 048	< 2 048 - overhead	< 2 048 - overhead
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502
SDU format information				
Delivery of erroneous SDUs	Yes/No	Yes/No	Yes/No	Yes/No
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$
SDU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100 – maximum value	250 – maximum value		
Guaranteed bit rate (kbps)	< 2 048	< 2 048		
Traffic handling priority			1,2,3	
Allocation/Retention priority	1,2,3	1,2,3	1,2,3	1,2,3

3.2.2 UMTS QoS management

The QoS profiles and classes can be negotiated and managed using the mechanisms of PDP (Packet Data Protocol) context management [3GPP23.060].

The PDP represents any protocol, e.g., IP, which transmits data packets. Moreover, the PDP contexts applied in UMTS, are information sets held in MS, SGSN and GGSN (or IGSN) and are used to specify the tight connection between one subscriber that identifies an application, a PDP type and one QoS profile. More PDP contexts with different QoS parameters can share the same PDP address. In order to activate PDP contexts two types of procedures can be used (see Figure 3-3). The first procedure, called Activate PDP Context includes subscription checking, APN (Access Point Name) selection, and host configuration. The second procedure, called Secondary Activate PDP Context procedure may be used to activate a PDP context while reusing the PDP address and other PDP Context information from an already existing PDP Context, but with a different QoS Profile. The latter procedure can be repeated. Note that at least one PDP context shall be activated for a PDP address before a Secondary PDP Context Activation procedure may be initiated.

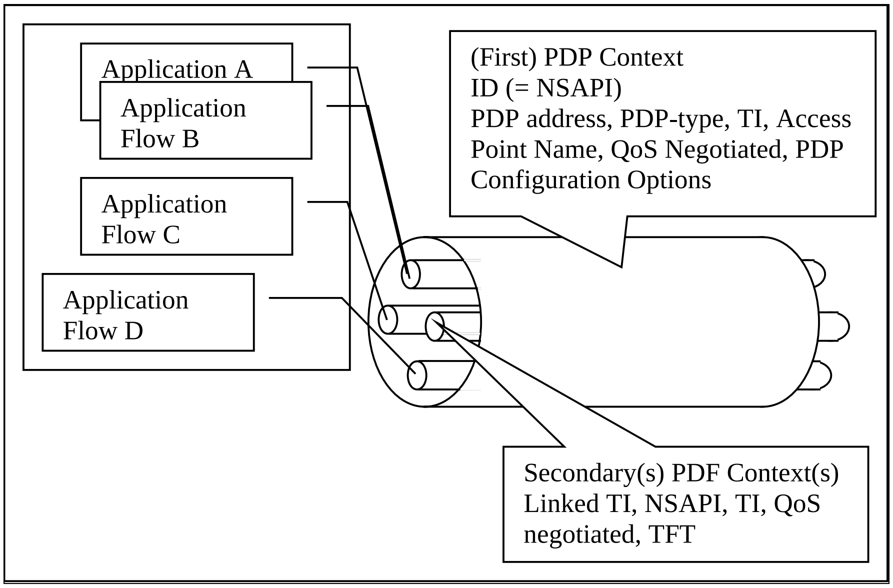

Application A
Application Flow B
Application Flow C
Application Flow D
(First) PDP Context
ID (= NSAPI)
PDP address, PDP-type, TI, Access Point Name, QoS Negotiated, PDP Configuration Options
Secondary(s) PDF Context(s)
Linked TI, NSAPI, TI, QoS negotiated, TFT

Figure 3-3: “first” and Secondaries PDP contexts

A detailed description of the QoS management procedures used in the GPRS core network are given in [Kar00]. Furthermore, [Kar00] describes several interworking procedures between:

- the Integrated Services architecture and the UMTS/GPRS QoS architecture;
- the Differentiated Services and the UMTS/GPRS architecture.

In this investigation we focus on the interworking between the Integrated Services architecture and the UMTS/GPRS QoS architecture . However, the UMTS/GPRS system may consist of isolated IP clouds, e.g., in the UTRAN. In this situation, and due to scalability concerns the Differentiated Services architecture will be used in these IP clouds. The dynamic management of the resources available in these Differentiated Services architectures can be accomplished by using the Load Control Protocol [WeTu00], (see also [KaRe00]).

3.2.3 QoS mangement functions

The QoS management functions used to control the UMTS bearer service are depicted in Figure 3-4. These control functions are used by the UMTS technology to manage the establishment and the modification of UMTS bearer services.

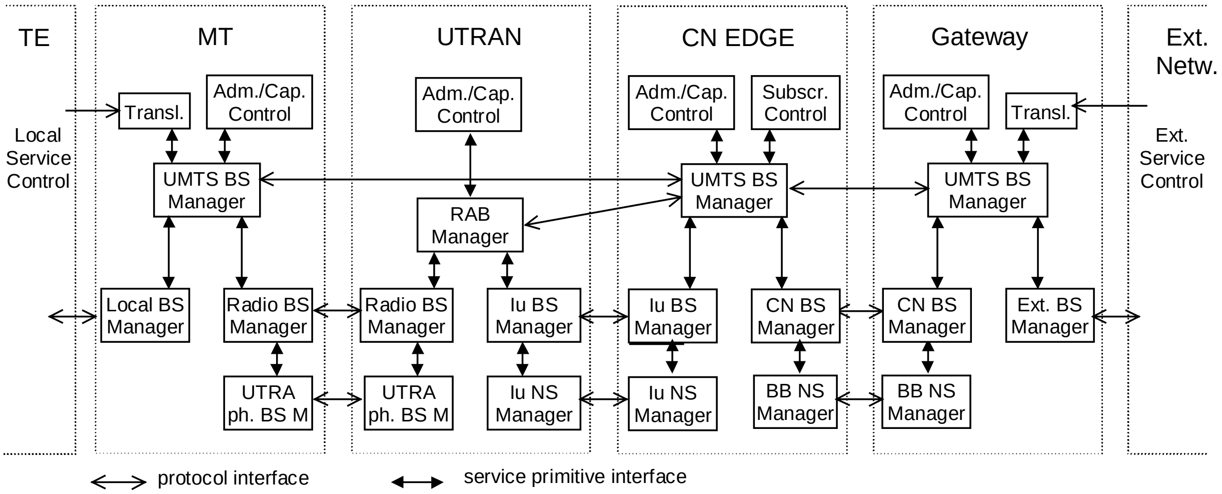


Figure 3-4: QoS management functions for UMTS bearer service in the control plane (from [3GPP23.107])

The QoS management control functions are:

- translation functions (Trans.) is used in the MT and Gateway to translate external signaling to internal signalling;
- admission/capability (Adm/Cap) is used in the MT, UTRAN, CN Edge and Gateway to either admit or reject an UMTS bearer service request.
- UMTS BS (Bearer Service) manager is used in the MT, CN EDGE and the Gateway interoperates with any external instances to establish or modify a UMTS bearer service. Furthermore, each of the UMTS BS managers is inquiring the admission/capability control to find out whether the network entity supports the specific requested service and whether the required resources are available.
- RAB (Radio Access Bearer) manager is inquiring the admission/capability control to find out whether the UTRAN supports the specific requested service and whether the required resources are available.

The QoS management functions used for the UMTS bearer service in the user plane are depicted in Figure 3-5. These functions are used by the UMTS technology to maintain the data traffic characteristics according to the reservations made by the BS managers.

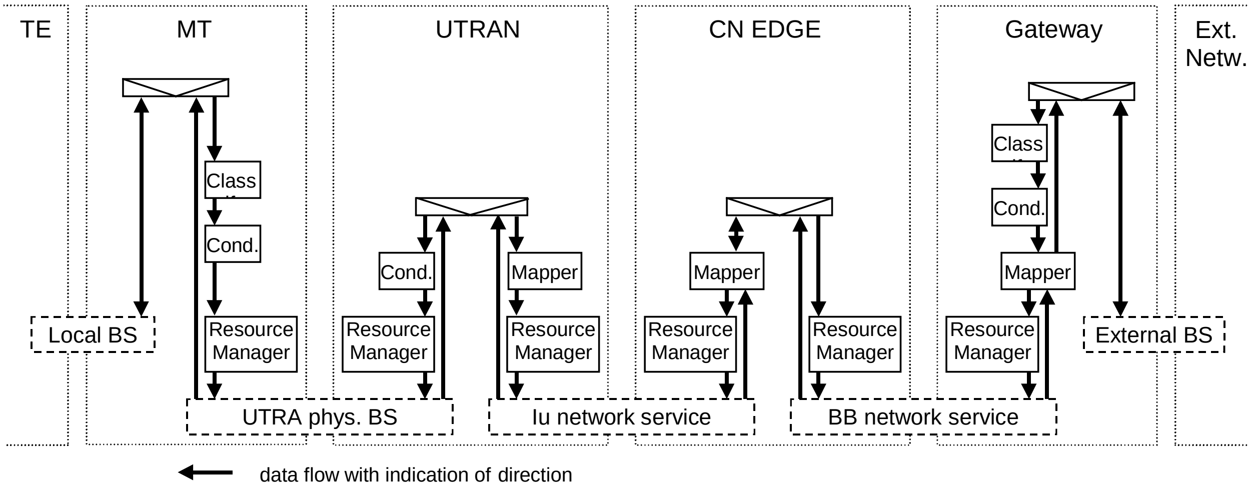


Figure 3-5: QoS management functions for the UMTS bearer service in the user plane (from [3GPP23.107])

The QoS management functions for the UMTS bearer service in the user plane are:

- classification function (Class.) used in the Gateway and in the MT it classifies received external user data units to the appropriate UMTS bearer service according to the QoS requirements of each user data unit;
- traffic conditioner (Cond.) used in the MT provides policing and conformance of the uplink user data traffic with the QoS attributes of the relevant UMTS bearer service. Moreover, in the Gateway a traffic conditioner may provide policing and conformance of the downlink user data traffic with the QoS attributes of the relevant UMTS bearer service.
- Mapper function it marks each data unit related to a specific bearer service with a specific QoS indication.
- resource manager of a network entity is responsible for a specific resource. The resource manager is distributing its resources between all bearer services requesting transfer of data units on these resources.

3.3 QoS in the Bluetooth network

In Bluetooth [BLUESPEC] two link layer types are specified. One of them is the Synchronous Connection Oriented (SCO) that provides a circuit switched type of service and the Asynchronous Connectionless Link (ACL) that it is mainly providing a packet switched type of network. This section is based on [Ze00] and it is briefly presenting the main QoS features used in the Bluetooth QoS framework.

3.3.1 QoS classes and attributes

The current Bluetooth specification can support QoS demanding applications such as voice or video by either using the SCO link or the Guaranteed class in the ACL link.

In [Ze00] an enhanced Bluetooth QoS framework has been presented that gives the possibility on the Bluetooth technology to support an additional number of QoS classes on top of the packet-switched ACL link. These additional QoS classes are the: Priority, Isochronous and Low Bitrate Low Delay (LBLD). For more details on these classes we refer to [Zee00].

The QoS parameters that can be supported by the Bluetooth technologies are:

- Bandwidth: an application is often able to run satisfactory only if a certain bandwidth is available on the Bluetooth link;
- Delay and delay variation: interactive real-time and streaming audio/video applications may have strict requirements on delay and delay variation;
- Reliability: some applications such as audio and video applications may tolerate some packet loss, other ones such as typical data applications do not tolerate packet losses;
- Ordering: some applications do not tolerate packet re-ordering. The Bluetooth technology does preserve the ordering of the packets, while the Internet does not do that.

3.3.2 Bluetooth QoS management

The basic functions and procedures used in the Bluetooth QoS framework (Figure 3-6, Figure 3-7) are the following:

- Resource Allocation: this function provides control over the usage of resources. These resources can be either air-interface resources, i.e., amount of bandwidth on the air interface that required by an application, or local and remote resources, i.e., amount of buffer space available for the QoS packets belonging to the same application to travel up and down the Bluetooth stack;
- Classification: this function identifies the data traffic that is associated to QoS application. Without this classification, the resource allocation can not be applied.
- Resource reservation: this function is enabling the reservation of the air-interface, local and remote resources that are associated to one QoS demanding application.
- Resource Manager (RM) located in the master of the Piconet. Further the Resource Requester (RR) entity cancels the reservation with the Resource Manager and deletes the configuration of the local RA when the QoS flow is terminated. The RM provides also admission control functionality, applied to guarantee that the requested QoS is maintained during the lifetime of the QoS demanding application.

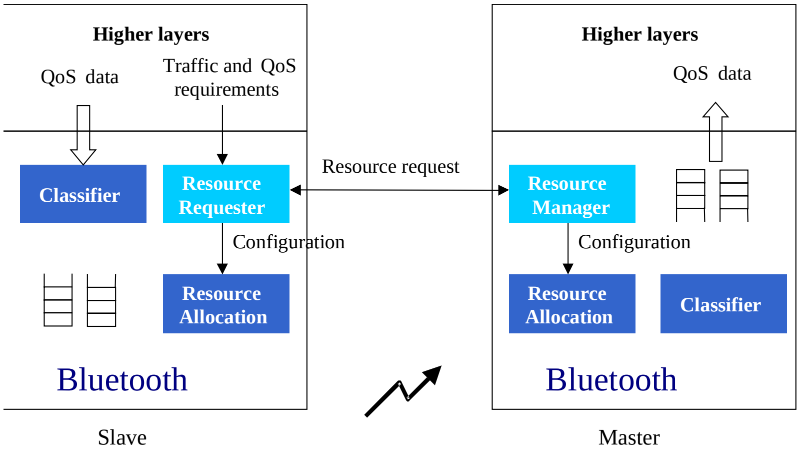


Figure 3-6*:* QoS functions for Slave-to-Master QoS flow (from [Zee00])

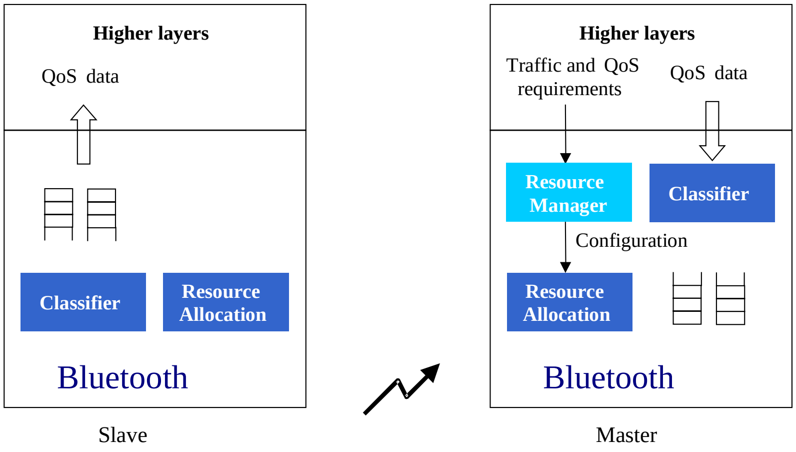


Figure 3-7: QoS functions for Master-to-Slave QoS flow (from [Zee00])

In case of resource reservation and assuming that the NAP operates as a master, the resource reservation request is sent by an MS to the NAP over the air interface. This procedure is depicted in Figure 3-8. The ResR (Resource Requester) function after receiving the traffic and QoS requirements from the higher layers the MS is configuring the parameters used by the RA (Resource Allocation) function. If these requirements are accepted, i.e., message “3. Accept” then the ResR is requesting the QoS and Traffic requirements from the NAP, i.e., message “4”. The RM (Resource Manager) that is a function that manages the resources in a Piconet, after receiving the reservation request is configuring the parameters used in the RA. If the allocation of the requested resources is accepted then a notification is sent to the RM. This notification is sent in a response message, i.e., “7. Response” to the ResR.

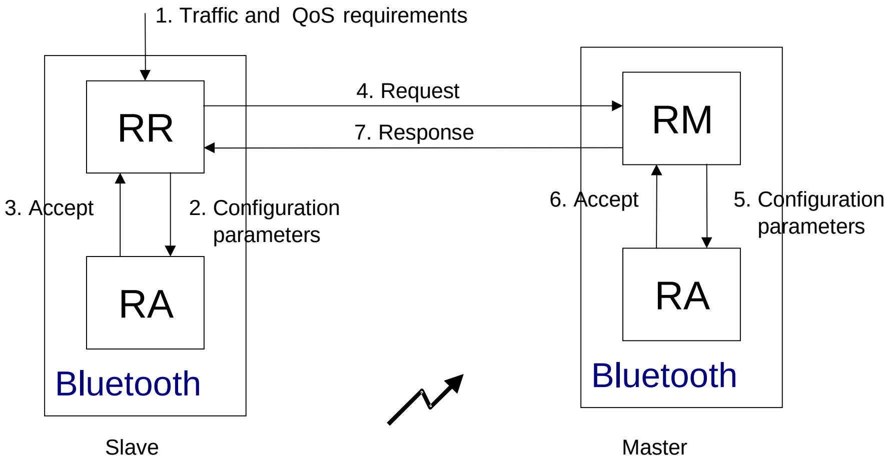

1. Traffic and QoS requirements
RR
4. Request
7. Response
RM
3. Accept
2. Configuration parameters
6. Accept
5. Configuration parameters
RA
RA
Bluetooth
Bluetooth
Slave
Master

Figure 3-8: Resource reservation for Slave-to-Master scheme (from [Zee00])

In [Zee00] two different options to implement the Resource Reservation mechanism are presented. One of them is the L2CAP (Logical Link Control and Adaptation Protocol) QoS option. The other option is the LMP (Link Manager Protocol) QoS.

3.4 IP mobility

Due to roaming, a mobile device may change its network attachment each time it moves to a new IP sub-network.

This might cause a disruption for the Internet data packets that have to reach the mobile host. Mobile IP [RFC2002] is a protocol, developed by the Mobile IP Internet Engineering Task Force (IETF) working group, that is able to inform the network about this change in network attachment such that the Internet data packets will be delivered in a seamless way to the new point of attachment.

When this change in network attachment is accomplished during an ongoing (application) session then the procedure that is responsible for delivering the IP data packets to the new point of attachment is called macro-mobility handoff.

3.4.1 Mobile IPv4

The key feature of the Mobile IPv4 (see e.g., [Per98], [Kar99]) design is that all required functionalities for processing and managing mobility information are embedded in well-defined entities, the Home Agent (HA), Foreign Agent (FA), and Mobile Node (MN). The current Mobile IPv4 protocol is completely transparent to the transport and higher layers and does not require any changes to currently used Internet hosts and routers.

The Mobile IP protocol allows the MNs to retain their IP address regardless of their point of attachment to the network. This can be fulfilled by allowing the MN to use two IP addresses. The first one, called home address, is static and is mainly used to identify higher layer connections, e.g., TCP. The second IP address that can be used by a MN is the Care-of Address. While the mobile is roaming among different networks, the Care-of Address changes. The reason of this is that the Care-of Address has to identify the mobile's new point of attachment with respect to the network topology. In Mobile IPv4 the Care-of Address management is typically achieved by an entity called Foreign Agent.

The Mobile Node, using its home address is appearing to be able to receive data on its home network, through a Home Agent. In the situation that the mobile roams into a foreign region, it will need to obtain a new Care-of Address via the Foreign Agent. Note that, in this situation the Mobile Node can also obtain a new Care-of Address by contacting the Dynamic Host Configuration Protocol (DHCP) [RFC1541] or Point-to-Point Protocol (PPP) [RFC1661]. This new Care-of Address will be registered with its Home Agent. At the moment that the Home Agent (see Figure 3-9) receives a packet that has to be send to the mobile, it delivers it from the home network to the mobile's Care-of Address. The delivery can take place only if the packet is redirected or tunnelled, such that the Care-of Address appears as the destination IP address. The Home Agent tunnels the packet to the Foreign Agent. After receiving the packet, the Foreign Agent will have to apply the reverse transformation to decapsulate it, such that the packet will appear to have the mobile's home address as the destination IP address. After decapsulation, the packet is sent to the Mobile Node. Due to the fact that the packet arrives at the Mobile Node, being addressed to its home address, it will be processed properly by the upper protocol layers, e.g., TCP. The IP packets sent by the Mobile Node, are delivered by standard IP routing procedures, each to its destination (see step 4 in Figure 3-9 (i.e., home address)). When the Mobile IP packet flow, follows a route similar to the one viewed in Figure 3-9, then the routing situation is typically called triangle routing. The packets sent by the host, called correspondent host (CH), follow the path 1,2 and 3, while the packets sent by the Mobile Node follow routes 3 and 4.

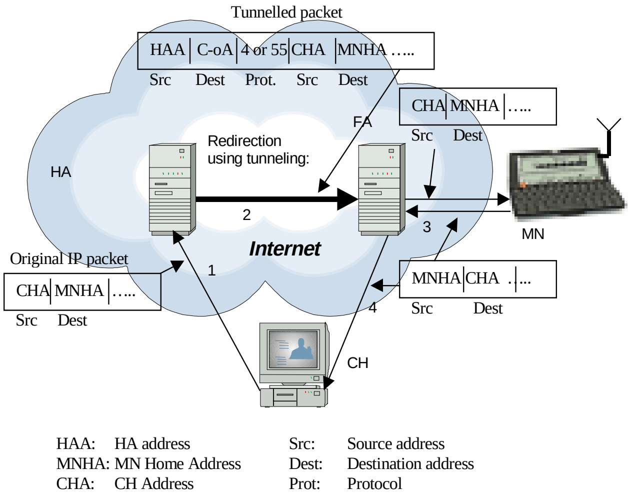


Figure 3-9: Mobile IP packet flow

The briefly explained Mobile IPv4 functionality can be realised by using three mechanisms (for a detailed description of these mechanisms see [Per98] and [Per97]):

- Discovering the Care-of Address: The Care-of address discovery procedure used in Mobile IP is based on the ICMP (Internet Control Message Protocol) Router Advertisement standard protocol, specified in RFC 1256 [RFC1256]. In Mobile IPv4, the router advertisements are extended to also contain the required Care-of Address. These extended router advertisements are known as agent advertisements. Home Agents and Foreign Agents typically broadcast at regular intervals (e.g., once a second, or once every few seconds) and in a random fashion, agent advertisements.
- Registering the Care-of Address: After the Mobile Node gets the Care-of Address it will have to inform the Home Agent about it. In Mobile IP this can be accomplished by using the registration procedure (see Figure 3-10). The Mobile Node sends a registration request (using the User Datagram Protocol (UDP)) with the Care-of Address information. This information is received by the Home Agent and normally, if the request is approved it adds the necessary information to its routing table and sends a registration reply back to the Mobile Node.

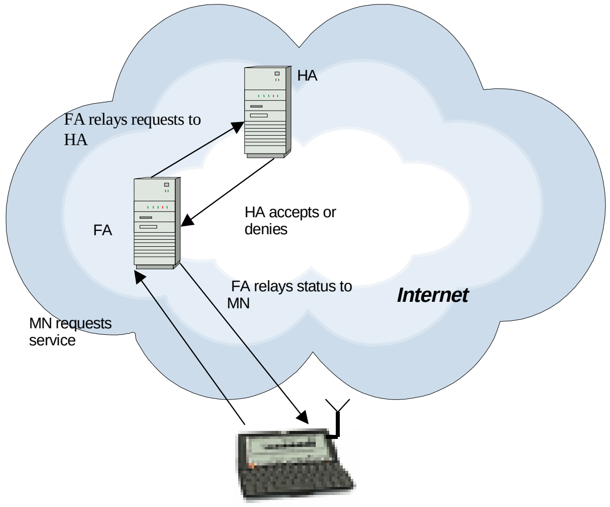


Figure 3-10: Registration in Mobile IP

- Tunnelling to the Care-of Address: is accomplished by using encapsulation mechanisms. All mobility agents, i.e., Home Agents and Foreign Agents, using Mobile IPv4 must be able to use a default encapsulation mechanism included in the IP within IP protocol [RFC2003]. By using this protocol, the source of the tunnel, i.e., Home Agent, inserts an IP tunnel header, in front of the header of any original IP packet addressed to the Mobile Node’s home address. The destination of this tunnel is the Mobile Node’s Care-of Address. In IP within IP [RFC2003] there is a way to indicate that the next protocol header is again an IP header. This is accomplished by indicating in the tunnel header that the higher level protocol number is ‘4’. The entire original IP header is preserved as the first part of the payload of the packet. By eliminating the tunnel header the original packet can be recovered.

3.4.2 Triangle routing and route optimisation

In [PeJo00] (see e.g., [Per97] and [Per98]), the operation of the base Mobile IPv4 protocol is extended to allow for more efficient routing procedures, such that IP packets can be routed from a correspondent host to a Mobile Node without going to the Home Agent first.

These extensions are referred to as route optimisation, wherein new methods for IP nodes, e.g., correspondent hosts, are provided. The correspondent host receives a *binding update* message from the mobile’s node Home Agent that contains the Mobile Node’s Care-of Address. The binding specifies the association of the home address of a Mobile Node with a care-of address for that Mobile Node, along with the remaining lifetime of that association. This binding is then stored by the correspondent host in a binding cache and is used to tunnel its own IP packets directly to the care-of address, bypassing the Mobile Node's Home Agent. In this way, the triangular routing situation, explained in Section 3.4.1 is eliminated. However, in the initiation phase, the IP packets sent by the correspondent host still use the triangle routing until the moment that the *binding update* message sent by the Mobile Node’s Home Agent, is received by the correspondent host.

In addition to the *binding update* message, the route optimisation procedure is using the following messages:

- A *binding warning* control message is usually sent by a node (e.g., Mobile Node or Correspondent Host), to the Home Agent (i.e., recipient), indicating that a Correspondent Host (i.e., target) seems unaware of the Mobile Node’s new Care-of Address;
- A *binding request* message is sent by a Correspondent Host to the Home Agent at the moment it determines that its binding should be initiated or refreshed. Note that if the home agent for a certain reason, e.g., the Mobile Node is in its home domain, can not find or does not want to inform the correspondent host about the MN’s Care_of Address, then the Home Agent will also send a *binding update* message to the CH. However, this message will include a Care_of Address that is set equal to the MN’s home address and the association lifetime is set to zero. The CH will then have to delete the binding cache entry for that particular MN.
- A *binding acknowledgement* message can be requested by a Mobile Node from a Correspondent Host that has had received the *binding update* message.

3.4.3 Mobile IPv6

The Mobile IPv6 uses the experiences gained from the design and development of Mobile IPv4 ([RFC2003], [RFC2002], [RFC2004]) together with the new IPv6 protocol features (see [JoPe00]). Mobile IPv6 shares many features with Mobile IPv4, but the protocol is now fully integrated into IPv6 and provides many improvements over Mobile IPv4. The major differences between Mobile IPv4 and Mobile IPv6 that are:

- Support for "Route Optimisation" [PeJo00]. This feature is now built in as a fundamental part of the Mobile IPv6 protocol. In Mobile IPv4 the route optimisation feature is being added on as an optional set of extensions that may not be supported by all IP nodes. However, this does not mean that always the route optimisation option will be applied in Mobile IPv6. A MN may decide to use or not use this option.
- In Mobile IPv6 the functionality of the Foreign Agents can be accomplished by IPv6 enhanced features, such as Neighbour Discovery [RFC1970] and Address Autoconfiguration [RFC1971]. Therefore, there is no need to deploy Foreign Agents in Mobile IPv6.
- Mobile IPv6 and IPv6 use the source routing feature. This feature makes it possible for a Correspondent Host to send packets to a Mobile Node while it is away from its home network using an IPv6 Routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets. However, in Mobile IPv6 the Home Agents are allowed to use encapsulation for tunnelling. This is required, during the initiation phase of the binding update procedure.
- In Mobile IPv6 the packets which arrive at the home network and are destined for a Mobile Node that is away from home, are intercepted by the Mobile Node’s Home Agent using IPv6 Neighbour Discovery [RFC1970] rather than ARP [RFC826] as it is used in Mobile IPv4.
- In IPv6 a new routing procedure is defined called anycast. This feature is used in Mobile IPv6 for the dynamic Home Agent address discovery mechanism. This mechanism returns one single reply to the Mobile Node, rather than the corresponding Mobile IPv4 mechanism that used IPv4 directed broadcast and returned a separate reply from each Home Agent on the Mobile Node's home subnetwork. The Mobile IPv6 mechanism is more efficient and more reliable. This is due to the fact that only one packet need to be replied to the Mobile Node.
- All Mobile IPv6 control traffic can be piggybacked on any existing IPv6 packets. This can be accomplished by using the IPv6 destination options. In contrary, for Mobile IPv4 and its Route Optimisation extensions, separate UDP packets were required for each control message.

4 End to end IP QoS support during Mobile IP handoff

This section describes various solutions on the QoS and mobility between various IP subnetworks that are using different wireless technologies. Two wireless technologies are used as examples, i.e., UMTS and Bluetooth. Figure 2-9 depicts the investigated Network topology. As example, we considered that the dynamic end to end QoS management in the investigated Network topology is achieved by the RSVP [RFC2205] protocol. Moreover, it is considered that the IP core network and the (possible) isolated IP clouds in the UTRAN are using the Differentiated Services concept. The dynamic QoS management of these Differentiated Services domains are accomplished using the Load Control protocol [WeTu00]. The protocols used to support the mobility solutions are the current specified versions of the Mobile IPv4 [RFC2002] and Mobile IPv6 [JoPe00] protocols. Furthermore, the route optimisation feature described in Section 3.4.2, is neither used in the Mobile IPv4 nor in the Mobile IPv6 scenarios applied in this Section.

4.1 IP QoS and mobility support

This section describes the operation of the IP QoS and mobility support mechanisms applied in the network topology viewed in Figure 2-9. Furthermore, as mentioned in Section 3.1 in this investigation we apply the framework architecture presented in [KaRe00]. The operation of the IP QoS and mobility framework architecture uses certain procedures. These procedures are:

- “Network attachment”: a mobile host attaches to a certain network, using a specific access technology. In Mobile IP v4 this can be realised by using three mechanisms (see section 3.4.1):
  - ✓ Discovering the Care-of Address;
  - ✓ Registering the Care-of Address;
  - ✓ Tunnelling to the Care-of Address

  After successful network attachment the SIP protocol has to be triggered in order to start the “QoS session setup”. We consider the development of such a triggering algorithm as an open issue.
- “QoS session setup”: a session is initiated between the end hosts that are willing to start an application.
- “QoS resource reservation”: reservation of the required resources in the access and / or core network.
- “IP user data transfer”: the flow of IP user data traffic.
- “QoS resource release”: the reserved resources are released.
- “QoS session termination”: the session is terminated.
- “Network detachment”: a mobile host detaches from a network

The processing sequence of these procedures can be specified by e.g., a predefined user profile that is assigned by the user. In our proposal we consider that the processing sequence of these procedures is sequential (see Figure 4-1). Another possible processing sequence could be partially simultaneous (see Figure 4-1).

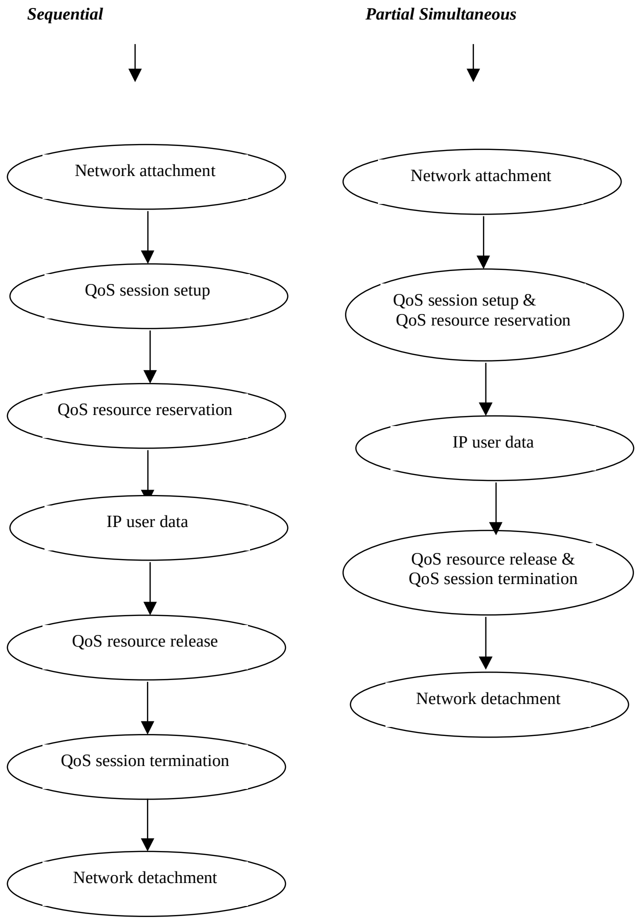


Figure 4-1: Processing order of operational phases viewed using a state diagram; each state represents one or more operational phases; if a state represents more than one operational phases then these phases are activated simultaneously.

Note that detailed flow diagrams used to describe the functionality of several protocols applied in this Section are presented in [KaRe00].

Depending on the IP mobility situation, i.e., the user, e.g., Host X, is roaming within an access technology or is roaming among different access technologies, the framework will have to support different operation scenarios. Two such operation scenarios are identified:

- **Intra access technology roaming**: the user, e.g., Host X, in Figure 2-9, is roaming within one access technology, e.g., UTRAN. In this situation it is considered that the mobility management will be provided by the underlying access technology, i.e., UTRAN. Therefore, the IP mobility management procedures, e.g., Mobile IP procedures, will not be activated. In case of Bluetooth the IP mobility procedures will not be activated assuming that the wireless access technology covers only one IP subnetwork.
- **Inter access technology roaming**: the user, e.g., Host X, in Figure 2-9, is roaming among two different access technologies, i.e., from UMTS into Bluetooth. In this situation the mobility management can not be solved by the underlying access technologies but it will be accomplished by the IP mobility management procedures. i.e., Mobile IP procedures.

4.1.1 Intra access technology roaming scenario:

In this scenario it is assumed that the user is roaming within one access technology, e.g., UTRAN. This means that the mobility management will be provided by the underlying access technology, i.e., UTRAN.

The operation steps followed by the IP QoS and mobility framework architecture are listed below.

Note that due to the Mobile IP operation, in all steps listed below, a tunnelling procedure (see Section 3.4.1) have to be applied in the downstream direction between the Home Agent and Foreign Agent. Furthermore, note that for both Mobile IP versions, i.e., Mobile IPv4 and Mobile IPv6, the routing optimisation feature described in Section 3.4.2 is not used.

- ***Step_1*** (***UMTS Network attachment)***: When the Host X (see Figure 2-9) is not attached to the UMTS network it is not able to use any UMTS services. This situation can be changed by performing an UMTS attach procedure, see [3GPP23.060]. During this procedure, the Host X provides its UMTS identity and indicates which type of attach needs to be executed. The UMTS network, i.e, IGSN, will register the user profile of Host X. After this point the Host X user is authorised to use the UMTS services. However, this can only be accomplished when the Host X gets an IP address from the UMTS network. Furthermore, either one new PDP Context (see Section 3.2.2) has to be created or an existing PDP context has to be modified to include the information provided by Host X. This PDP Context is stored into the UMTS network, i.e., IGSN and Host X.
  The PDP Context is created/modified using the Activate/Modify PDP Context procedure, see Figure 4-2 and Figure 4-3. After the creation of the PDP context the MC entity of Host X will initiate the Mobile IP procedures explained in either Section 3.4.1 or Section 3.4.3. Depending on the used Mobile IP version different Message Sequence Charts have to be used. Figure 4-2 views the UMTS Network Attachment procedure when the Mobile IPv4 version is applied, while Figure 4-3 views the UMTS Network Attachment procedure when the Mobile IPv6 version is applied.

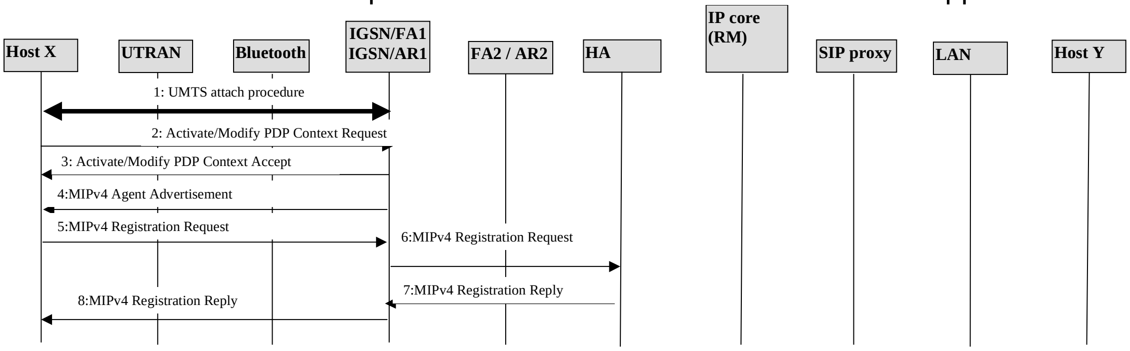

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1: UMTS attach procedure
2: Activate/Modify PDP Context Request
3: Activate/Modify PDP Context Accept
4:MIPv4 Agent Advertisement
5:MIPv4 Registration Request
6:MIPv4 Registration Request
7:MIPv4 Registration Reply
8:MIPv4 Registration Reply

Figure 4-2: UMTS Network Attach using Mobile IPv4

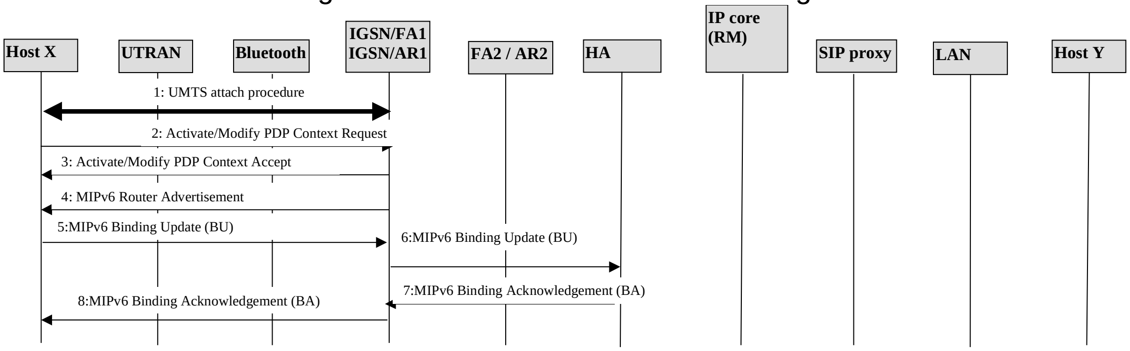

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1: UMTS attach procedure
2: Activate/Modify PDP Context Request
3: Activate/Modify PDP Context Accept
4: MIPv6 Router Advertisement
5:MIPv6 Binding Update (BU)
6:MIPv6 Binding Update (BU)
7:MIPv6 Binding Acknowledgement (BA)
8:MIPv6 Binding Acknowledgement (BA)

Figure 4-3: UMTS Network Attach using Mobile IPv6

A calling user, e.g., application entity in Host X (see Figure 2-9), wishes to use a real time application, e.g., Voice over IP [VoIP], and communicates with another user, i.e., called user – application entity in Host Y. At Host X, the application requirements, e.g., network QoS requirements, authentication and accounting requirements will be translated by the QoS API to QoS parameters, authentication and accounting parameters that can be understood by the underlying access technologies (see Section 3.2.1). The TS depending on a predefined user profile will decide if the technology selection should take place without querying its access technologies. In this roaming scenario it is considered that the coverage area is only supported by UMTS (see Section 3.1.2). Subsequently, the application entity will be notified about the identity of the selected access technology, i.e., UMTS.

- ***Step_2 (UMTS QoS session setup)***: The application entity of Host X will start the QoS "Session setup" phase by using the Session Layer Negotiation (e.g., SIP and Session Description Protocol (SDP)) and requiring from the called user, i.e., application entity of Host Y to start a Voice over IP session (see Figure 4-4). The information contained in the Session Layer Negotiation (e.g., SDP) elements will be the session name, purpose, media and timing information and additional information regarding the bandwidth to be used by the Voice over IP application.

The same procedures that were accomplished earlier in the Host X will also be accomplished at Host Y. In other words, the application requirements, e.g., network QoS requirements, authentication and accounting requirements will be translated by the QoS API to QoS parameters, authentication and accounting parameters that can be understood by the underlying access technologies, i.e., Ethernet (see [ZeAi00]). The called user, i.e., application entity in Host Y, via the Session Layer Negotiation protocol (e.g., SIP and SDP) it will inform the calling user, i.e., application entity in Host X, that the "QoS session setup" phase is satisfactory completed. The functionality of the QoS API is not defined in this document. We consider the development of the QoS API as an open issue.

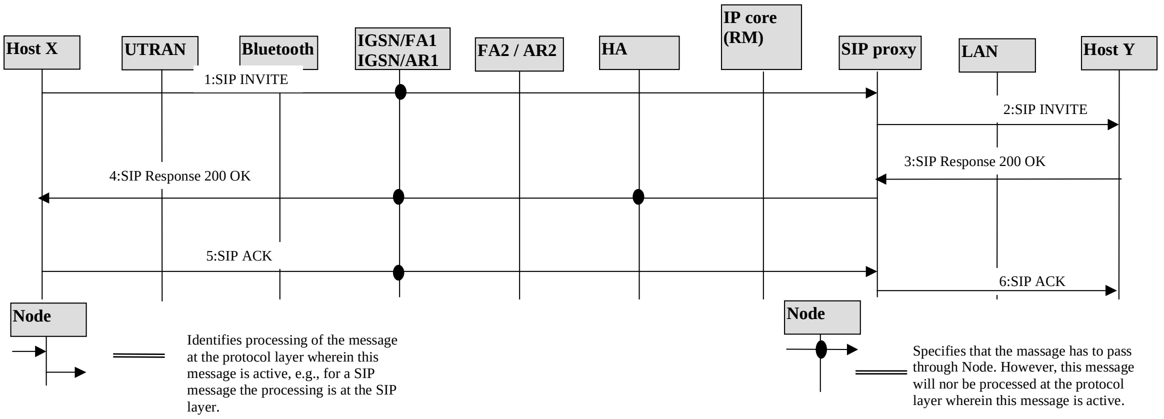

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1:SIP INVITE
2:SIP INVITE
3:SIP Response 200 OK
4:SIP Response 200 OK
5:SIP ACK
6:SIP ACK
Node
Identifies processing of the message at the protocol layer wherein this message is active, e.g., for a SIP message the processing is at the SIP layer.
Node
Specifies that the massage has to pass through Node. However, this message will nor be processed at the protocol layer wherein this message is active.

Figure 4-4: "QoS session setup" phase

- ***Step_3 (UMTS QoS resource reservation):*** It is considered that the investigated scenario supports the "End to end QoS resource reservation" procedure via the RSVP protocol. The "QoS resource reservation" phase (see Figure 4-5) is started by the calling user, i.e., RC (Reservation Client) in Host X. The "QoS resource reservation" phase will be accomplished in the access network of Host X, the Diffserv core network and the access network of Host Y (see Figure 4-5 and Figure 4-6). Considering that the dynamic QoS management in the Diffserv domain in the core network is accomplished by the Load Control protocol (see [KaRe00]), an interoperation between RSVP and this Load Control protocol should be provided. During this phase, the RM entities located in all these network regions and the RCs located in the Host X and Host Y will have to intercommunicate and reserve the negotiated resources. The UMTS PDP activation/modification procedures are used in the access network of host X to reserve the requested resources in the UMTS domain.

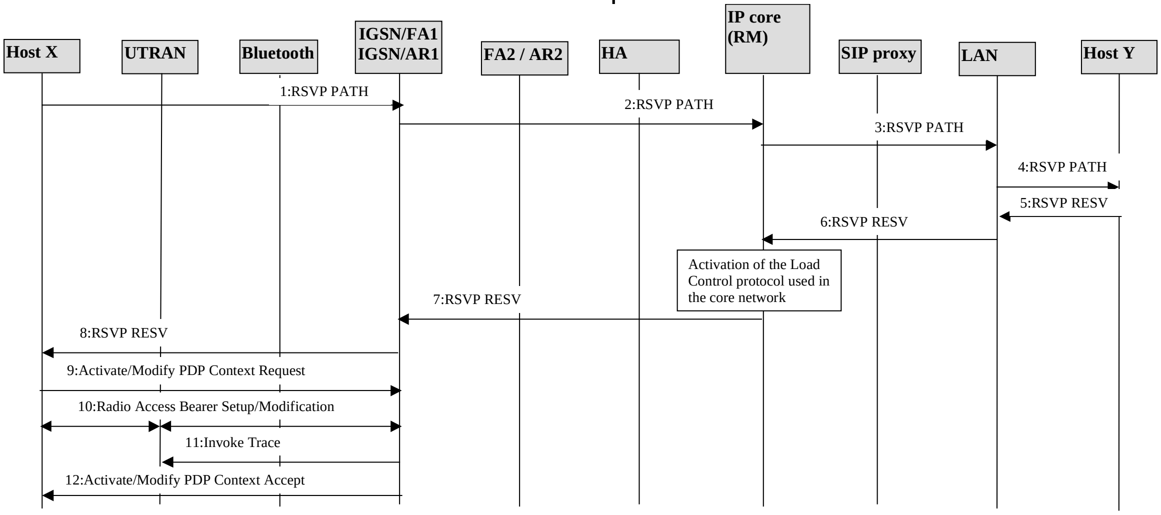

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1:RSVP PATH
2:RSVP PATH
3:RSVP PATH
4:RSVP PATH
5:RSVP RESV
6:RSVP RESV
Activation of the Load Control protocol used in the core network
7:RSVP RESV
8:RSVP RESV
9:Activate/Modify PDP Context Request
10:Radio Access Bearer Setup/Modification
11:Invoke Trace
12:Activate/Modify PDP Context Accept

Figure 4-5: "Upstream QoS resource reservation" phase

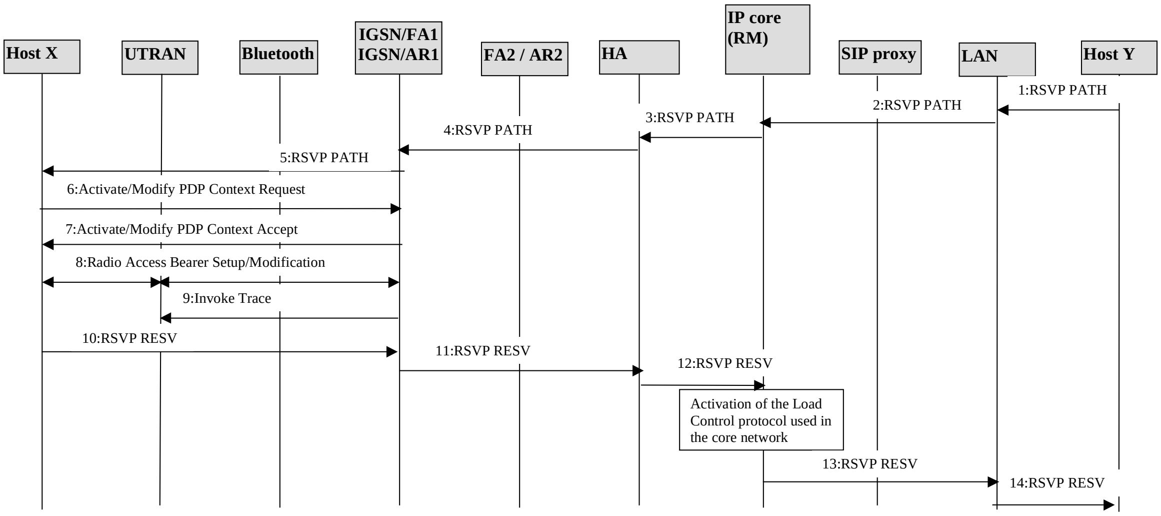


Figure 4-6: "Downstream QoS resource reservation" phase

- ***Step_4 (IP user data traffic)***: After this point, the calling user, i.e, application entity in Host X, and called user, i.e., application entity of Host Y, may start sending IP user data traffic, i.e., Voice over IP speech data (see Figure 4-7).

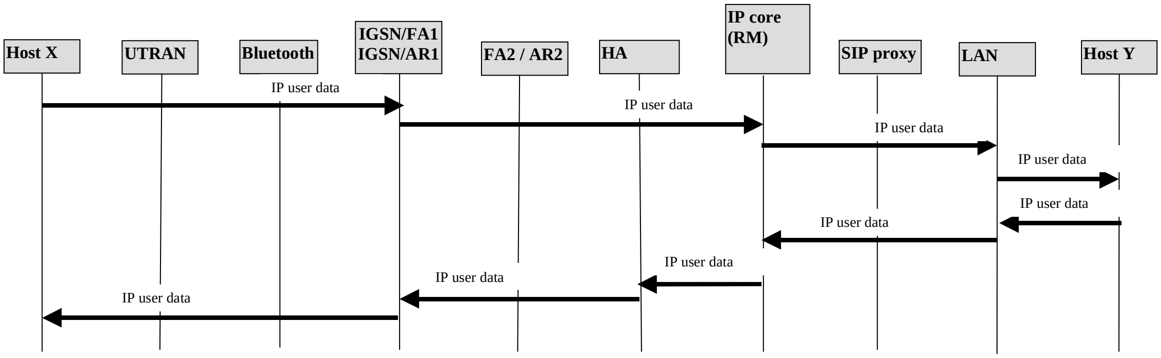


Figure 4-7: “IP user data traffic” phase

- ***Step_5 (UMTS QoS resource release)***: If one of the users, i.e., application entity in Host X, or application entity in Host Y, wishes to end the VoIP application then the “QoS resource release” phase will be initiated by the RC entities located in Host X, and/or Host Y (see Figure 4-8 and Figure 4-9). All the RM and RC entities that were involved during the “QoS resource reservation” phase will have to intercommunicate and release all the reserved resources. Note that the RSVP protocol supports release procedures that are based on the soft state principle, i.e., if a state is not refreshed regularly, will be released. In contrary, UMTS does not support the soft state principle. Therefore, an algorithm has to be developed to interoperate between the RSVP soft state release and the UMTS release. We consider the development of such an algorithm, an open issue.

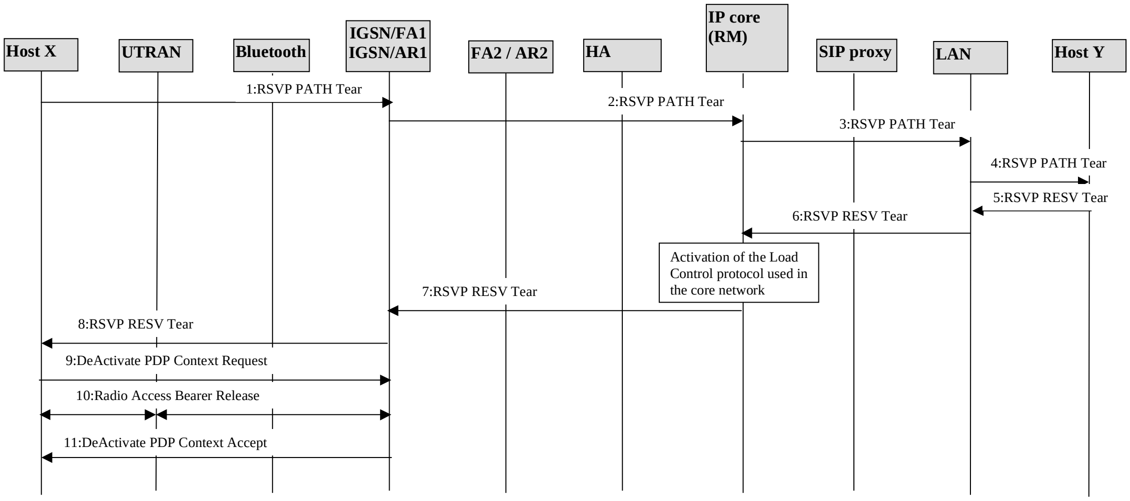


Figure 4-8: “Upstream QoS resource release” phase

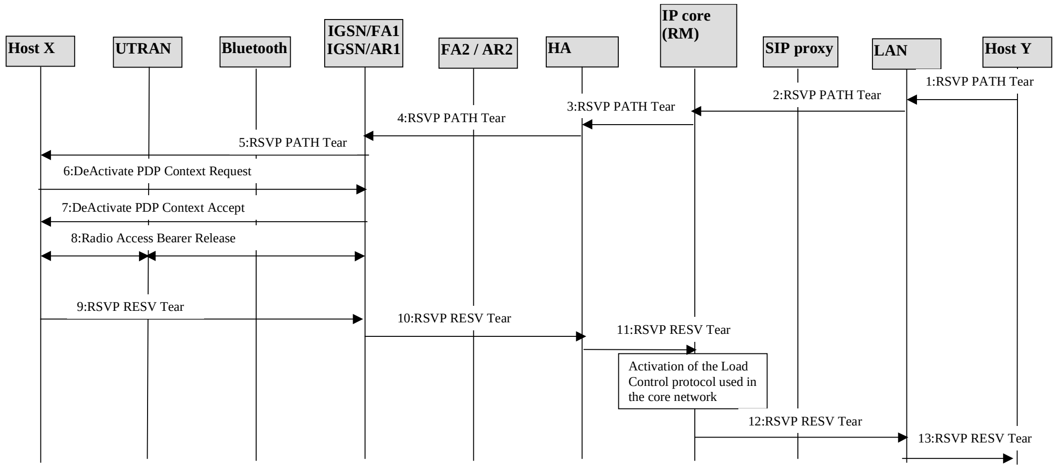
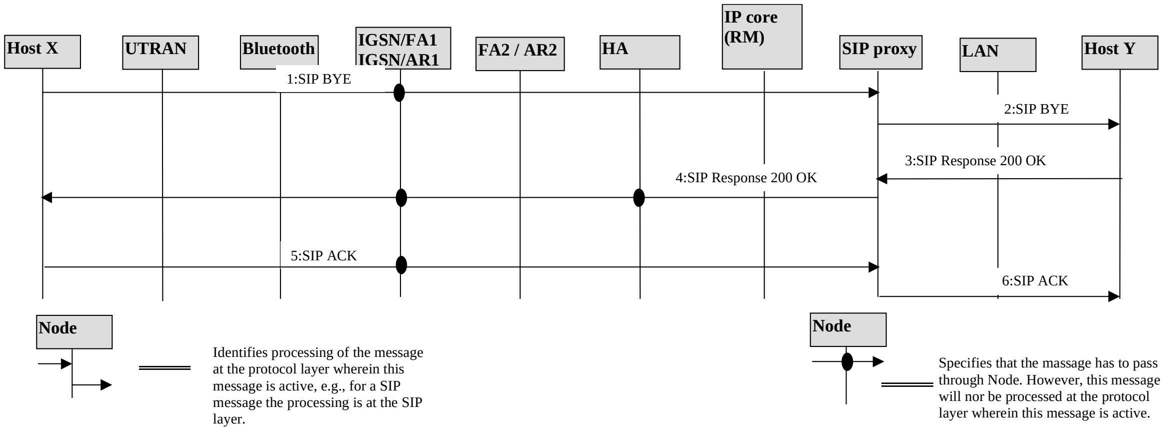


Figure 4-9: “Downstream QoS resource release” phase

- ***Step_6 (UMTS QoS session termination)***: After that the “QoS resource release” phase is completed, the “QoS session termination” phase is initiated by the application entity in Host X (see Figure 4-10). Using the Session Layer Negotiation the application entity in Host X informs the application entity in Host Y that the session should be terminated. If the application entity in Host Y agrees then a confirmation is sent back to the application entity of Host X. After the completion of the “session termination” phase the VoIP application is terminated by the application entities in Host X and Host Y.



Identifies processing of the message at the protocol layer wherein this message is active, e.g., for a SIP message the processing is at the SIP layer.

Specifies that the massage has to pass through Node. However, this message will nor be processed at the protocol layer wherein this message is active.

Figure 4-10: “QoS session termination” phase

- ***Step_7 (UMTS Network detachment)***:If the user, i.e, Host X does not need to access the UMTS network anymore, then it can perform an UMTS Detach procedure. This procedure can be explicit, where the Host X has to invoke the UMTS Detach procedure (see Figure 4-11). The UMTS detachment can also be achieved implicitly by using a predefined timer. If Host X is inactive for a certain amount of time that is bigger than the predefined timer, then the Host X is automatically detached.

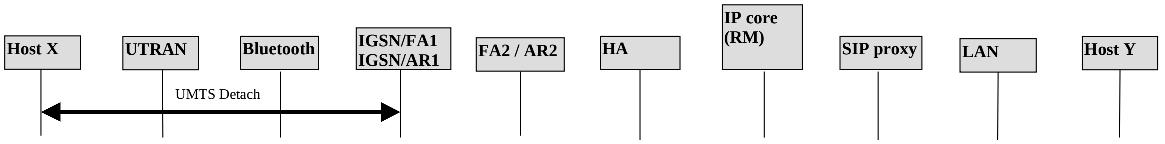


Figure 4-11: “Network detachment” phase

4.1.2 Inter access technology roaming scenario:

In this scenario it is assumed that the user is roaming among two different access technologies, e.g., from UMTS into Bluetooth. In this situation the mobility management can not be solved by the underlying access technologies but it will be accomplished by the IP mobility management procedures. i.e., Mobile IP procedures.

The operation steps followed by the IP QoS and mobility framework architecture, in this situation are similar to the operation steps explained in Section 4.1.1 for the situation that the user, i.e., Host X in Figure 2-9, is roaming within one access technology, i.e., UMTS. At the moment that the user will roam into another access technology, i.e., Bluetooth, then different procedures will be initiated. This section describes these different procedures.

The main point of this roaming scenario is that a roaming Host has the possibility to be simultaneously connected on both wireless technologies. The main challenge will be to always select the wireless technology that satisfies all the user and network provider demands in the most efficient way.

Two different states can be identified. In the first state, that we call “***session_off***” the user, e.g., Host X in Figure 2-9 before roaming from one access technology into another, e.g., from UMTS to Bluetooth, is not running any session. In the second state, that we call “***session_on***” the Host X, is running a session that has been established by using the steps ***Step_2*** to ***Step_4*** described in Section 4.1.1.

In this investigation we consider that:

- the framework architecture operation is in the “***session_on***” state;
- the Host X is running a real time VoIP application, as the one described in Section 4.1.1.
- the processing sequence of the operation steps is done sequentially (see Figure 4-1).
- the roaming Host has the possibility to be simultaneously connected for a certain period of time on both wireless technologies, i.e., UMTS and Bluetooth;
- Host X before handoff is using the UMTS wireless access.

Note that due to the Mobile IP operation, in all steps listed below, a tunnelling procedure (see Section 3.4.1) have to be applied in the downstream direction between the Home Agent and Foreign Agent. Furthermore, note that for both Mobile IP versions, i.e., Mobile IPv4 and Mobile IPv6, the routing optimisation feature described in Section 3.4.2 is not used.

The following steps need to be accomplished:

- ***Step_1 (Bluetooth Network attachment):***The MC entity (see Section 3.1) of the Host X will initiate the Network attachment procedure. In particular, first a Bluetooth link connection is established, see [BLUESPEC], [Zee00]. During the Bluetooth link connection establishment the Host X or the NAP will perform several procedures:
  - ✓ ***Inquiry:*** Host X uses this procedure to find access points, i.e., NAP, in range;
  - ✓ ***Paging***: used by Host X to synchronise with NAP;
  - ✓ ***Link establishment***: the ACL link is established;
  - ✓ ***SDP service request***: details of access service are retrieved through SDP;
  - ✓ ***Master-slave switch***: if required the roles between the slave and master will be switched;
  - ✓ ***Security functions***: the security associated functions are performed;

  An algorithm must be developed to identify when these Bluetooth Network Attachment procedures must be started and by which entity will they be initiated, e.g., the Host or the Bluetooth NAP. We consider the development of such an algorithm an open issue.

  After the Bluetooth link connection is established, Host X, will try to find out what is its new identity, i.e., IP address. The MC entity of Host X will initiate the Mobile IP procedures explained in either Section 3.4.1 or Section 3.4.3. Depending on the used Mobile IP version different Message Sequence Charts have to be used. Figure 4-12 views the Bluetooth Network Attachment procedure when the Mobile IPv4 version is applied, while Figure 4-13 views the Bluetooth Network Attachment procedure when the Mobile IPv6 version is applied.

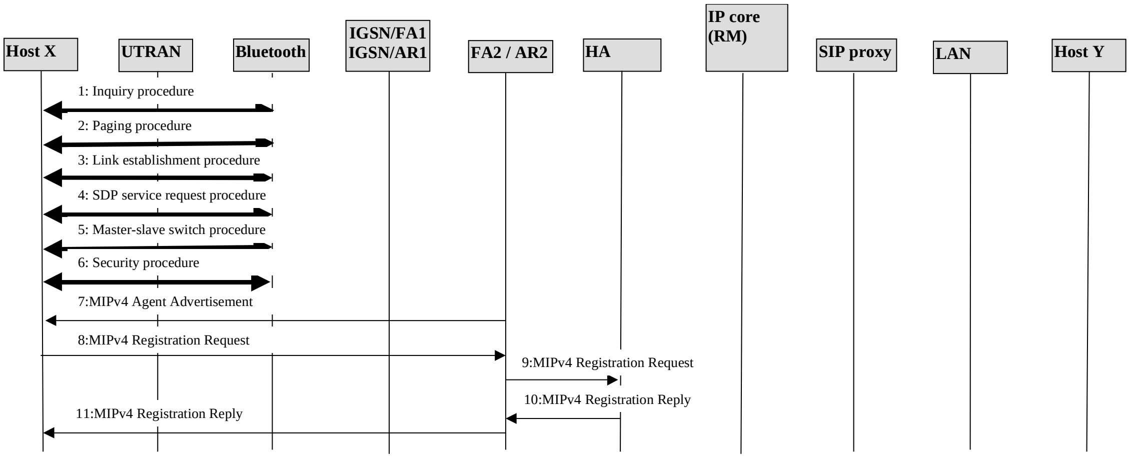

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1: Inquiry procedure
2: Paging procedure
3: Link establishment procedure
4: SDP service request procedure
5: Master-slave switch procedure
6: Security procedure
7:MIPv4 Agent Advertisement
8:MIPv4 Registration Request
9:MIPv4 Registration Request
10:MIPv4 Registration Reply
11:MIPv4 Registration Reply

Figure 4-12: Bluetooth Network Attach using Mobile IPv4

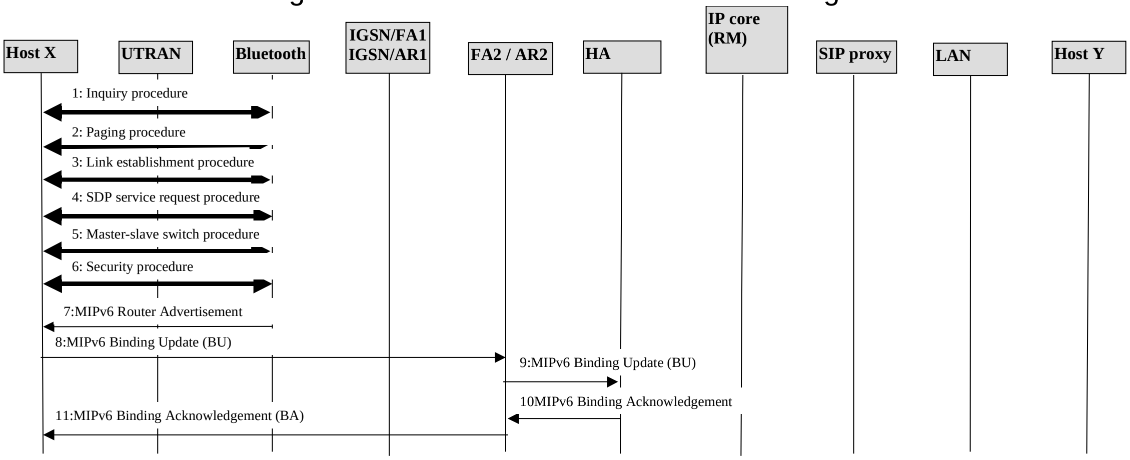

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1: Inquiry procedure
2: Paging procedure
3: Link establishment procedure
4: SDP service request procedure
5: Master-slave switch procedure
6: Security procedure
7:MIPv6 Router Advertisement
8:MIPv6 Binding Update (BU)
9:MIPv6 Binding Update (BU)
10MIPv6 Binding Acknowledgement
11:MIPv6 Binding Acknowledgement (BA)

Figure 4-13: Bluetooth Network Attach using Mobile IPv6

Host X will be connected simultaneously on both wireless technologies, i.e., UMTS and Bluetooth. The application entity of Host X, will use the same application requirements of the session that had been established on the old communication path, i.e., using the UMTS access. By using these requirements and via the QoS API it will request from the TS to select the technology that satisfies them the best, see Section 3.1.2. The Technology Selector after applying the selection procedure it can observe the following:

- *QoS application requirements can not be satisfied on both wireless technologies*: this implies that the application entity of Host X will terminate the old session by accomplishing the "UMTS QoS resource release", "UMTS QoS session terminate" and "UMTS Network detachment" procedures described in Section 4.1.1 as ***Step_5, Step_6 and Step_7,*** respectively.
- *QoS application requirements can not be satisfied by the new wireless technology, i.e., Bluetooth, but they can still be satisfied by the old wireless technology, i.e., UMTS:* In this situation Host X will maintain the reservations and the access to the old wireless technology, i.e., UMTS.
- *QoS application requirements can be satisfied by both wireless technology, but the new wireless technology i.e., Bluetooth is more efficient, e.g., cost efficient:* In this situation, Host X will

terminate the old session by accomplishing the “UMTS QoS resource release” and “UMTS Network detachment” procedures described in Section 4.1.1 as ***Step_5 and Step_7,*** respectively. Furthermore, Host X will start the “Bluetooth QoS resource reservation” procedure, see below. Moreover, there are situations that the access to the old wireless technology deteriorates very quickly. In this situation the involved user in this handoff procedure will experience long delays and data losses. A challenge is to perform the wireless technology handoff as soon as possible. Such a Mobile IP handoff scenario is explained in Section 5.

- ***Step_2 (Bluetooth QoS resource reservation):*** It is considered that the investigated scenario supports the “End to end QoS resource reservation” procedure via the RSVP protocol. The “QoS resource reservation” phase (see Figure 4-14 and Figure 4-15) is accomplished in a similar way as the one described in Section 4.1.1 as ***Step_3***. The main difference is that in place of the UMTS PDP Context activation procedures Bluetooth specific resource reservation procedures are used, see Section 3.3.2. In the situation that the Bluetooth NAP is RSVP aware, then a selection has to be made regarding which entity, i.e., Host or NAP, will initiate the Bluetooth QoS resource reservation procedure. We consider the development of such an algorithm as an open issue.

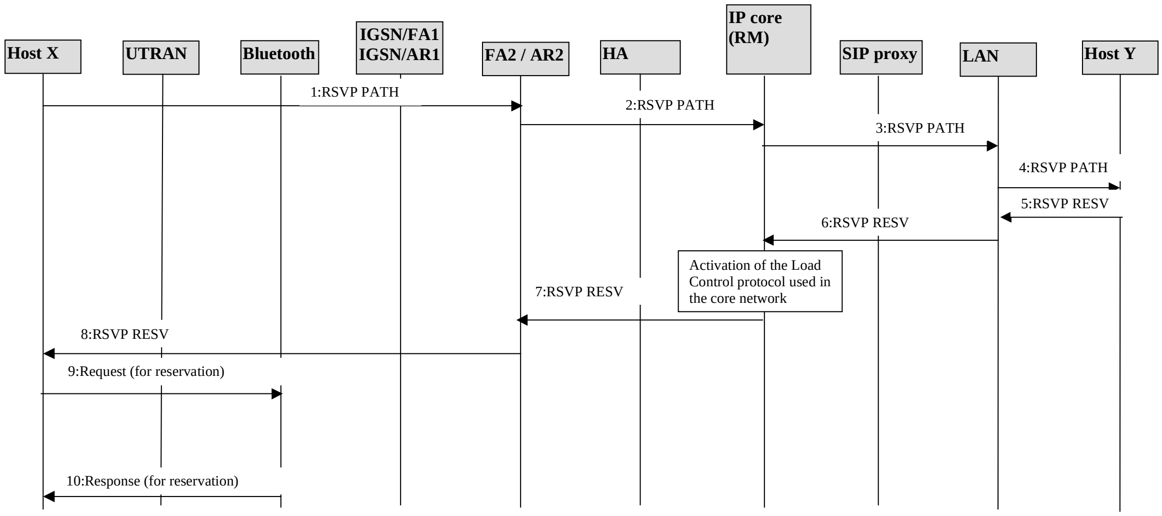


Figure 4-14: “Upstream QoS resource reservation” phase

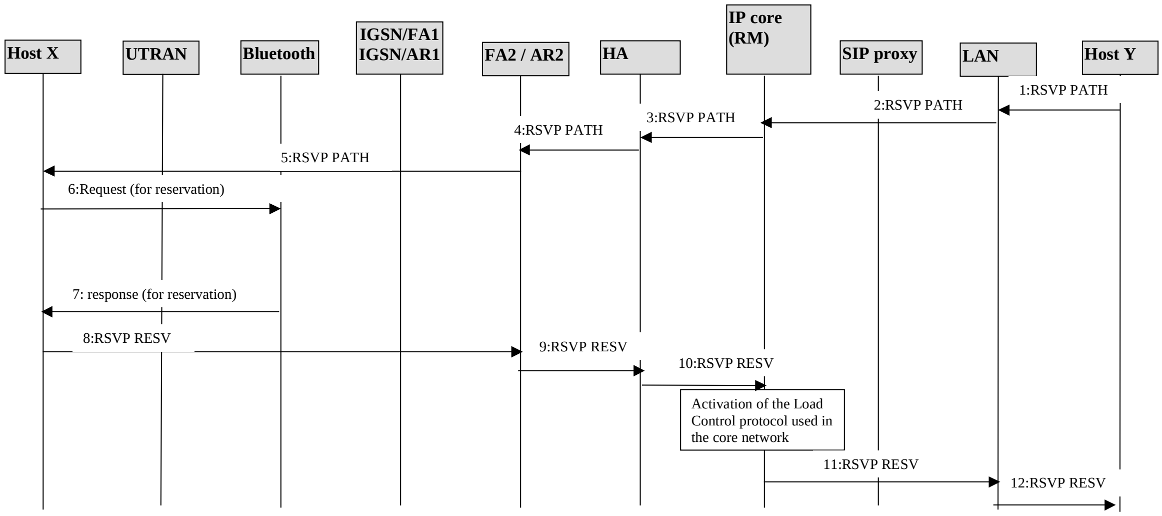


Figure 4-15: “Downstream QoS resource reservation” phase

- ***Step_3 (IP user data traffic)***: After this point, the calling user, i.e, application entity in Host X, and called user, i.e., application entity of Host Y, may start sending IP user data traffic, i.e., Voice over IP speech data (see Figure 4-16).

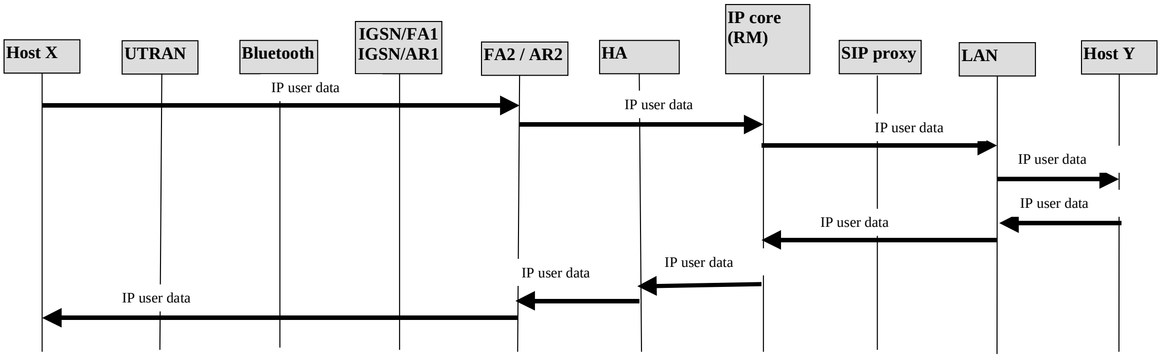


Figure 4-16: "IP user data traffic" phase

- ***Step_4 (Bluetooth QoS resource release)***: If one of the users, i.e., application entity in Host X, or application entity in Host Y, wishes to end the VoIP application then the "QoS resource release" phase will be initiated by the RC entities located in Host X, and Host Y (see Figure 4-17 and Figure 4-18). All the RM and RC entities that were involved during the "QoS resource reservation" phase will have to intercommunicate and release all the reserved resources. Furthermore, note that the RSVP protocol supports release procedures that are based on the soft state principle, i.e., if a state is not refreshed regularly, will be released. In contrary, Bluetooth does not support the soft state principle. Therefore, an algorithm has to be developed to interoperate between the RSVP soft state release and the Bluetooth QoS release procedures. We consider the development of such an algorithm, as an open issue.

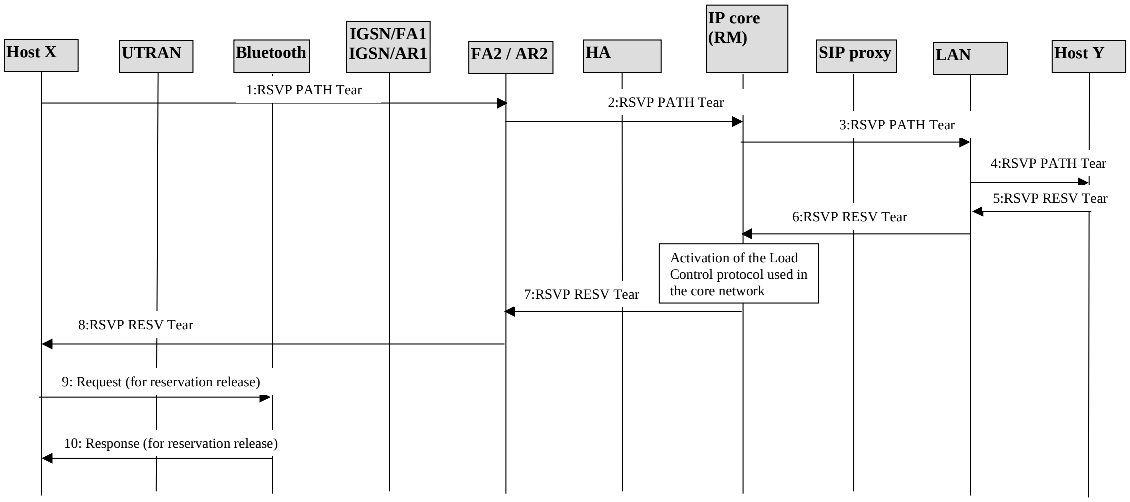


Figure 4-17: "Upstream QoS resource release" phase

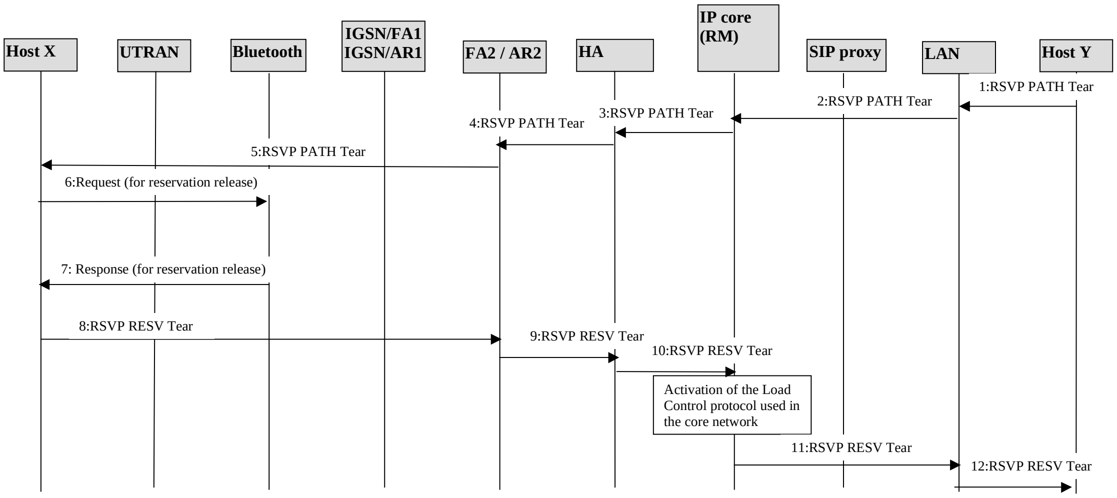


Figure 4-18: "Downstream QoS resource release" phase

- ***Step_5 (Bluetooth QoS session termination)***: After that the "QoS resource release" phase is completed, the "QoS session termination" phase is initiated by the application entity in Host X (see Figure 4-19). Using the Session Layer Negotiation the application entity in Host X informs the application entity in Host Y that the session should be terminated. If the application entity in Host Y agrees then a confirmation is sent back to the application entity of Host X. After the completion of the "session termination" phase the VoIP application is terminated by the application entities in Host X and Host Y.

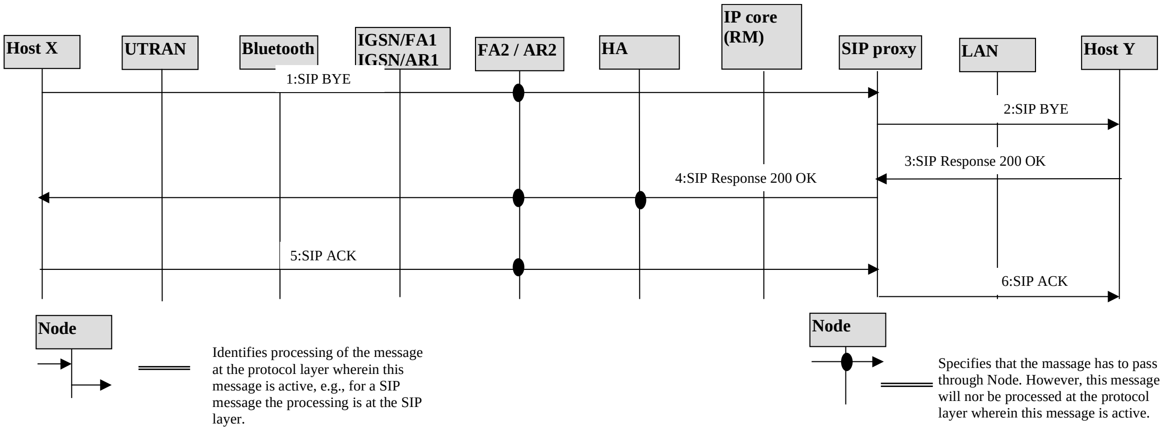

Host X
UTRAN
Bluetooth
IGSN/FA1
IGSN/AR1
FA2 / AR2
HA
IP core
(RM)
SIP proxy
LAN
Host Y
1:SIP BYE
2:SIP BYE
3:SIP Response 200 OK
4:SIP Response 200 OK
5:SIP ACK
6:SIP ACK
Node
Identifies processing of the message at the protocol layer wherein this message is active, e.g., for a SIP message the processing is at the SIP layer.
Node
Specifies that the massage has to pass through Node. However, this message will nor be processed at the protocol layer wherein this message is active.

Figure 4-19: "QoS session termination" phase

- ***Step_6 (Network detachment)***: If the user, i.e, Host X does not need to access the Bluetooth network anymore, then it can perform a Bluetooth Detach procedure (see Figure 4-20).

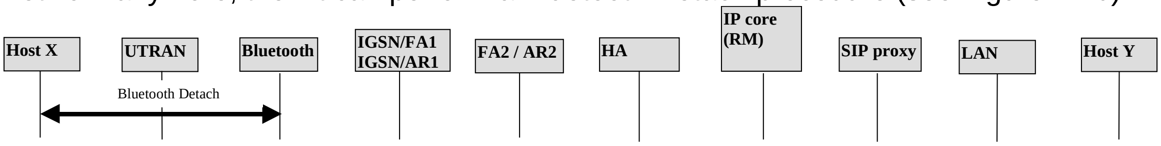


Figure 4-20: "Network detachment" phase

5 Seamless and fast handoff for Mobile IPv4 and Mobile IPv6

In Section 4, is considered that the protocols used to support the IP mobility are the current specified versions of the Mobile IPv4 and Mobile IPv6 protocols. In the situation that a wireless technology handoff has to take place, e.g., handoff from UMTS to Bluetooth, a main drawback on the current specified versions of the Mobile IPv4 and Mobile IPv6 protocols is observed. This drawback is related to the fact that the involved user in this handoff procedure will experience long delays and data losses. This implies that the seamless handoff requirement listed in Section 1 is not satisfied. In this section we present a solution on this drawback. In particular, we propose a scheme where the Mobile IPv4 and Mobile IPv6 handoffs are optimised to be seamless, i.e., the users during a handoff will not notify any disruption in the applications that they are running during handoff.

5.1 Motivation for Mobile IP handoff enhancements

During the macro-mobility handoff (i.e., IP level handoff), procedure a Host X that is active in an ongoing session, will change its network attachment by moving from an IP sub-network, that we call old IP sub-network, to another IP sub-network, that we call new IP sub-network.

Note that all the scenarios, depicted in this document and are used to describe the macro-mobility handoff management operation, are not viewing all the, in reality, used IP nodes. The main reason for this is that these IP nodes are not directly affecting the macro mobility handoff management operation.

One main issue that provide an obstacle on the efficient operation of the Mobile IP macro-mobility handoff is identified as the seamless handoff issue. A brief description of this issue is given below:

- ***seamless handoff***: In the situation that a Host X moved from the old wireless sub-network to the new wireless sub-network, a certain number of IP data packets that were in their way to be delivered to the Host X via the old IP sub-network, will not be able to reach it. The user that is involved in this handoff procedure will notice it. Therefore this type of handoff is not seamless. The handoff is specified as **seamless** when all the Host X's that are involved in the handoff process do not notice any disruption in the quality of the received application data stream. This means that the Mobile IP handoff duration and the IP packet loss during handoff should be minimised. Note that some applications, e.g., voice, tolerate a higher percentage of IP packet losses than other applications, e.g., file transfer.

5.1.1 Macro-mobility handoff in Mobile IPv4

The Mobile IPv4 protocol, described in [RFC2002], is supporting the macro-mobility handoff (see Phase 2 in Figure 5-1).

Note that Figure 5-1 is not viewing all the, in reality, used IP nodes. The main reason for this is that these IP nodes are not directly affecting the macro mobility handoff management operation.

As can be seen in Figure 5-1 this type of macro-mobility handoff is not able to solve the ***seamless handoff*** issue described in Section 5.1. In other words, during the handoff process several IP packets that are destined to the Host X are lost.

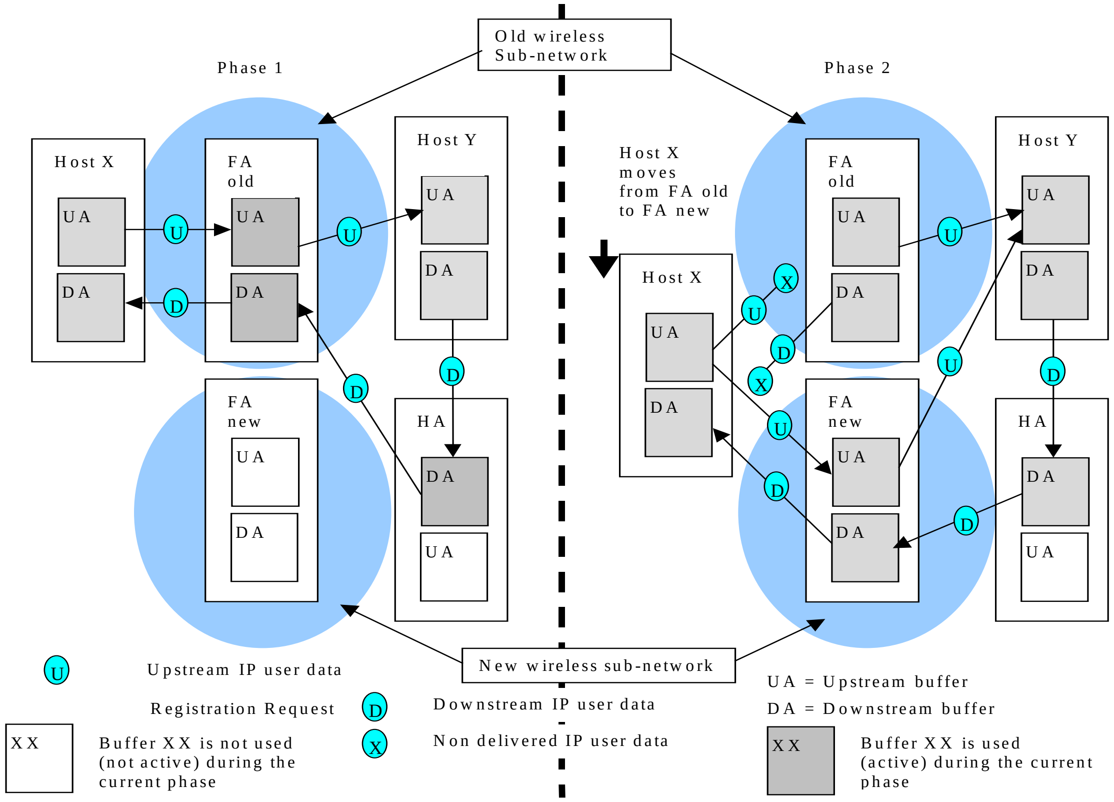


Figure 5-1: IP user data transfer during Mobile IPv4 handoff

5.1.2 Macro-mobility handoff in Mobile IPv6

The macro-mobility handoff is also supported by the Mobile IPv6 protocol, described in [JoPe00]. Note that a main difference between the Mobile IPv4 and Mobile IPv6 is that Mobile IPv6 does not use FA’s (see Figure 5-2, Figure 5-3).

In Mobile IPv6 each Host Y must be capable of supporting the route optimisation option. However, this does not mean that always the route optimisation option will be applied. A Host X may decide to use or not use this option. Therefore, the macro-mobility handoff can be accomplished either using the route optimisation option (see Figure 5-2) or not using this option (see Figure 5-3).

This handoff mechanism, compared to Mobile IPv4, is enhanced to possibly prevent the situation that a certain number of IP data packets that were in their way to be delivered to the Host X via the old IP sub-network, will not be able to reach it. In other words this enhancement should solve the ***seamless handoff*** issue described in Section 5.1. This could be accomplished by identifying, selecting and registering (using a binding update procedure) with a temporary home agent in the old wireless network that will be used to forward the packets that were destined to the previous Host X's care-of address to the new Host X's care-of address. The temporary home agent (see [JoPe00]) can be identified and selected by using two different methods. In the first method the Host X stores the information obtained from the Router Advertisements that were sent by the routers that can be used as home agents and are located in the old wireless network. This information is stored in a "Home Agent list". However, it is possible that the Host X could not identify a home agent in its old wireless sub-network. In this situation another method is used. This method is fulfilled by using the Dynamic Home Agent Discovery procedure. The Host X after moving to the new wireless sub-network and after obtaining its new Care-of Address is sending an ICMP Home Agent Address Discovery Request to the old wireless sub-network. The first Home Agent in the old wireless sub-network that receives the ICMP Home Agent Address Discovery Request message, sends its IP address to the Host X by using a ICMP Home Agent Address Discovery Reply message. This method is much slower than the first method. The success of this solution is very much depending on the speed of the procedure of identifying, selecting and registering with the temporary home agent in the old wireless sub-network. If the speed of these procedures is slow the IP packets that will be lost could became quite significant.

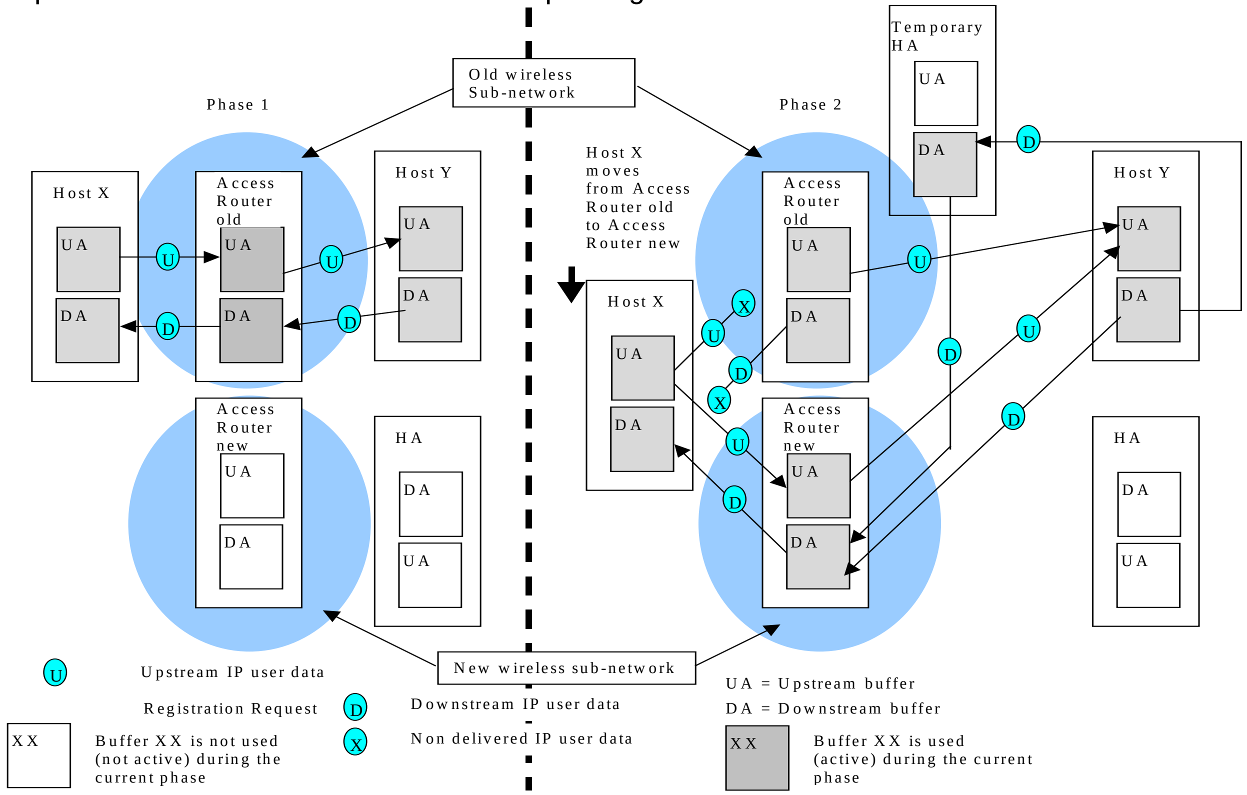


Figure 5-2: IP user data transfer during Mobile IPv6 handoff (with route optimisation)

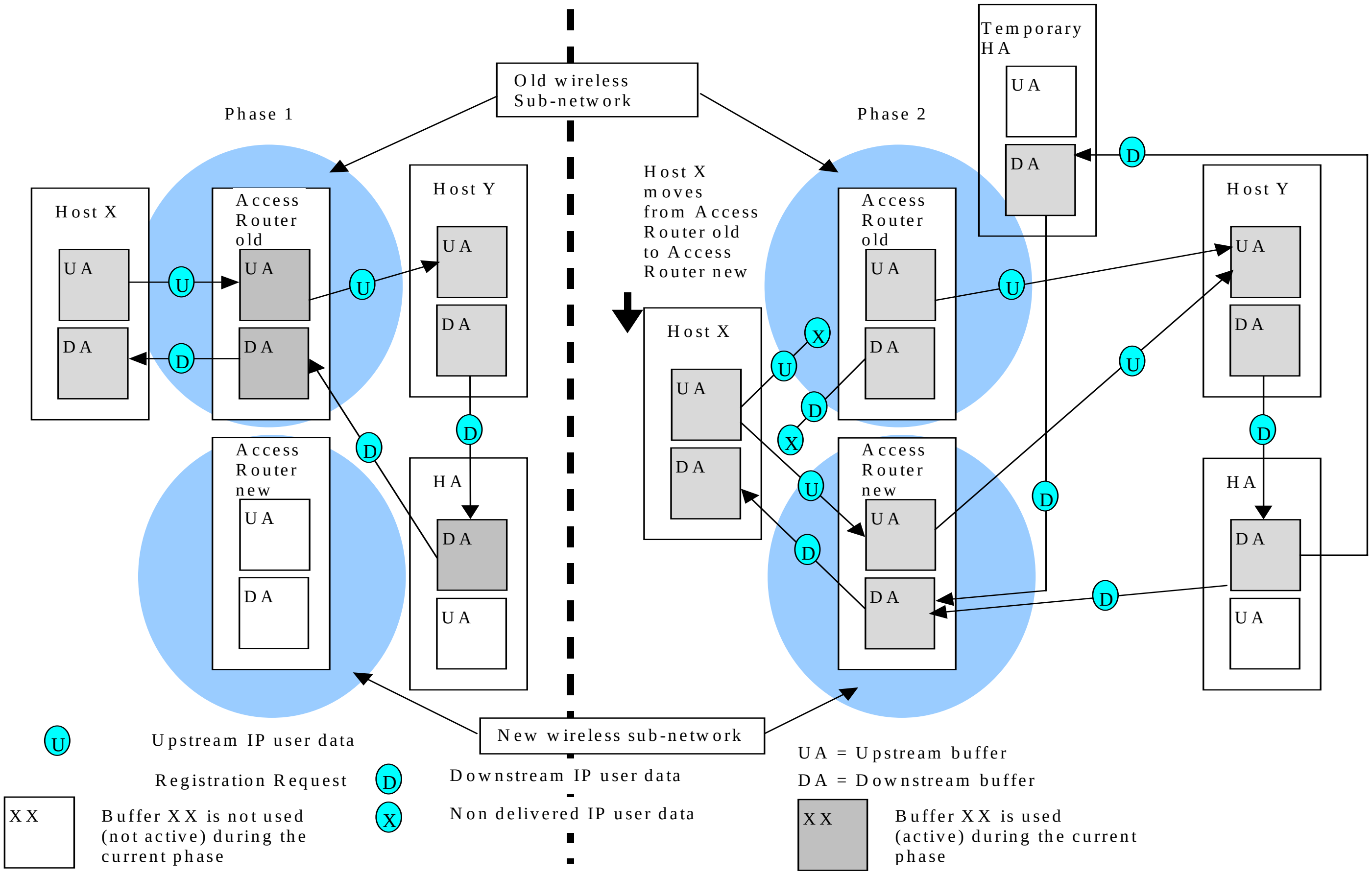


Figure 5-3: IP user data transfer during Mobile IPv6 handoff (no route optimisation is applied)

5.2 KNOWN SOLUTIONS

Several solutions have been presented to solve the Mobile IP ***seamless handoff*** issue described in Section 5.1. All these solutions are based either on the smooth handoff concept or on the multicasting (bicasting) concept.

5.2.1 Smooth handoff concept

This concept is used in combination with the Mobile IPv4 route optimisation algorithm specified in [PeJo00] and described in Section 3.4.2.

The smooth handoff concept is similar to the concept described in Section 5.1.2 that is applied in Mobile IPv6 for the situation that the Host X is willing to use the route optimisation option (see Figure 5-2). The main difference between the solution used in Mobile IPv6 (see Figure 5-2) and this solution (see Figure 5-4) is that in place of the temporary home agent, the old FA is used to forward the IP packets destined to the old care of address to the new care of address. If the speed of registering with the foreign agent in the old wireless sub-network is slow then the number of IP packets that will be lost could become quite significant.

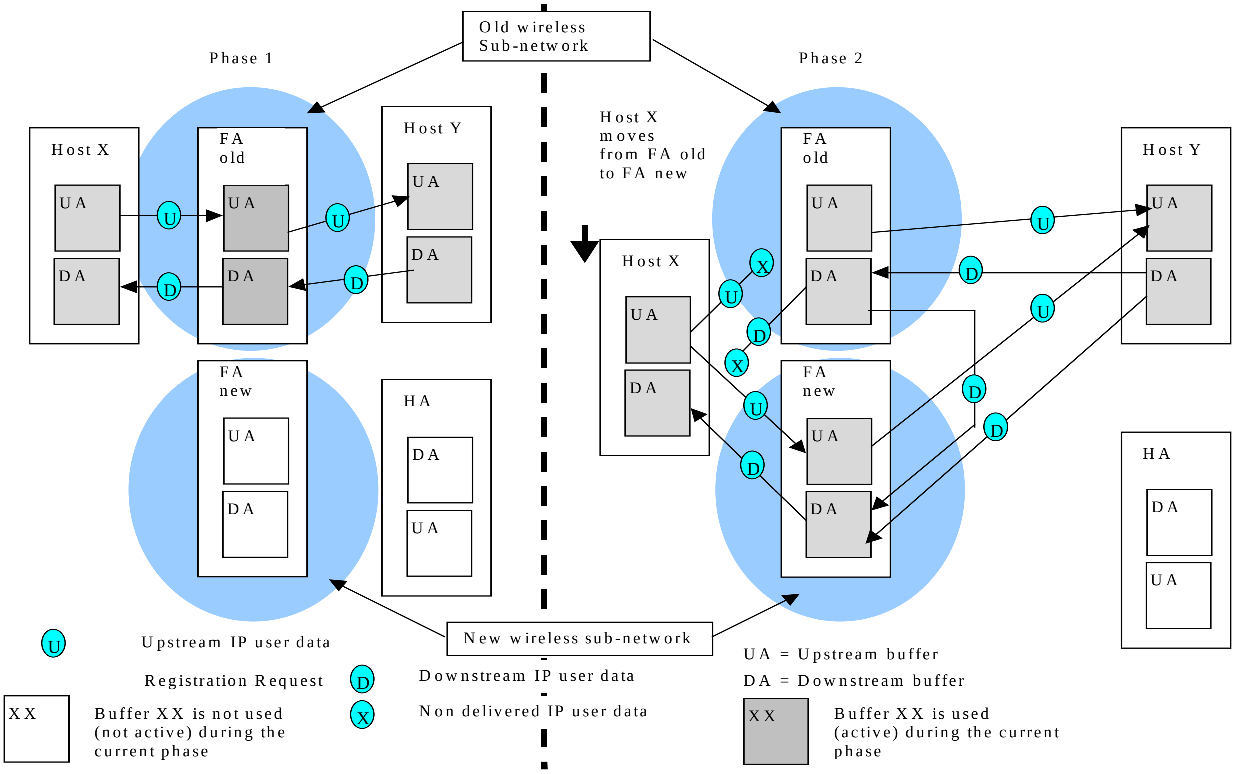


Figure 5-4: IP user data transfer during Mobile IPv4 handoff (with route optimisation smooth handoff)

5.2.2 Multicasting (bicasting) concept

This concept is mainly used in combination with the standard Mobile IPv4 protocol [RFC2002].

During macro-mobility handoff the IP data packets are multicasted (bicasted) to the old and new wireless sub-networks (see Figure 5-5). The IP data packets are multicasted by the home agent. This procedure is initiated by the Host X when it recognises that it moved (or it has to move) to the new wireless sub-network. At that moment in time the Host X is registering with the home agent by using the simultaneous binding option, where the previous binding with the home agent is kept while a new one is created. In this way the home agent copies each IP packet that is destined for the Host X and sends each copy of the IP packet to the old and new wireless sub-network. In [MaSo00] the fast handoff concept has been introduced in the hierarchical Mobile IPv4 and Mobile IPv6.

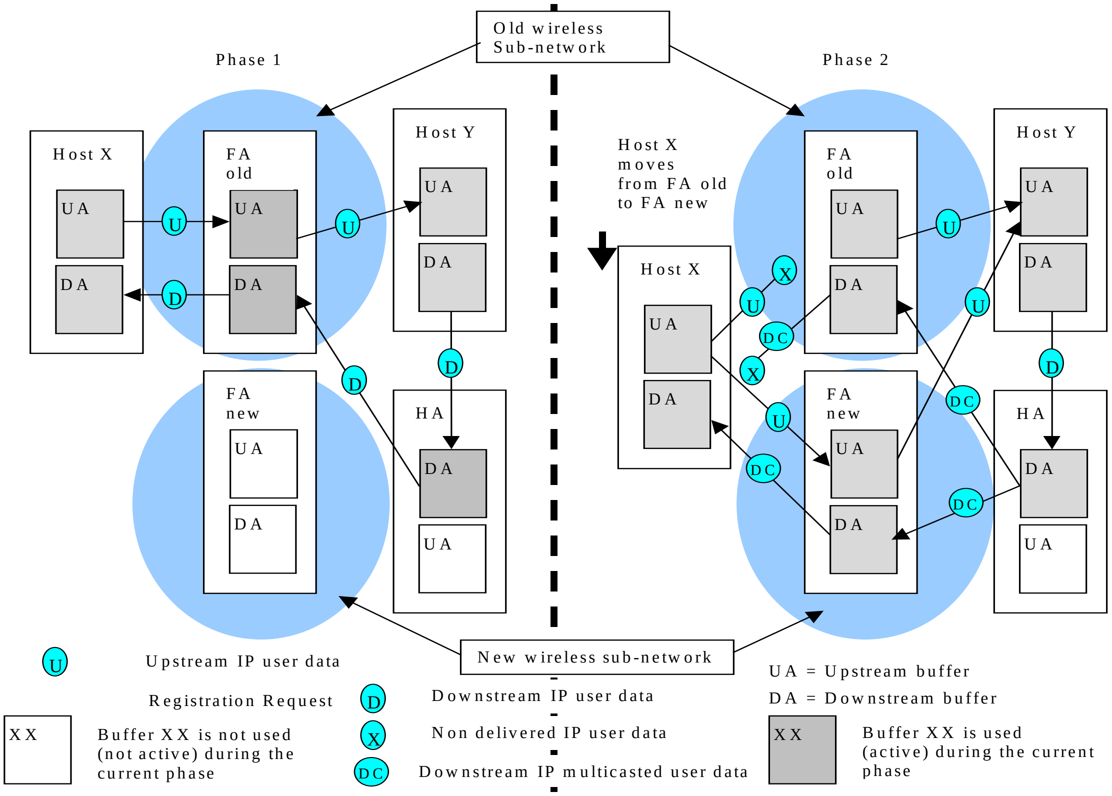


Figure 5-5: Multicasting used during Mobile IPv4 fast handoff

The hierarchical Mobile IPv4 protocol (see [GuJo00]) introduces a new network node called the Gateway Foreign Agent (GFA). This network entity is used to manage the Host X registrations in a certain region. This region may include more then one FA's. Furthermore, it gives the possibility to Host X's to register locally, i.e., perform regional registrations, in a visited (new wireless) network. The Host X when it arrives in a new wireless sub-network, that is able to support regional registrations, it registers the Care-of Address of the GFA located in this wireless sub-network with the HA. The GFA will then have a binding of the Host X's Care-of Address and Host X's home address. This information is kept in its visitor's list.

If the Host X afterwards moves to another FA that is also located in the region that is managed by the GFA, the binding with the Host X's HA will not have to change since the Care-of Address registered at the HA is the GFA address. Therefore, the HA does not need to be informed of any Host X movements beneath the GFA. This will decrease the signalling delay and it may improve the handoff performance.

The fast handoff used in the Hierarchical Mobile IPv4 protocol is described in [MaSo00]. The main operation of this handoff can be explained by using Figure 5-6. This operation is similar to the one viewed in Figure 5-5. The difference is that the entity that performs the multicasting of the IP data packets in the downstream direction is not anymore the HA but the GFA.

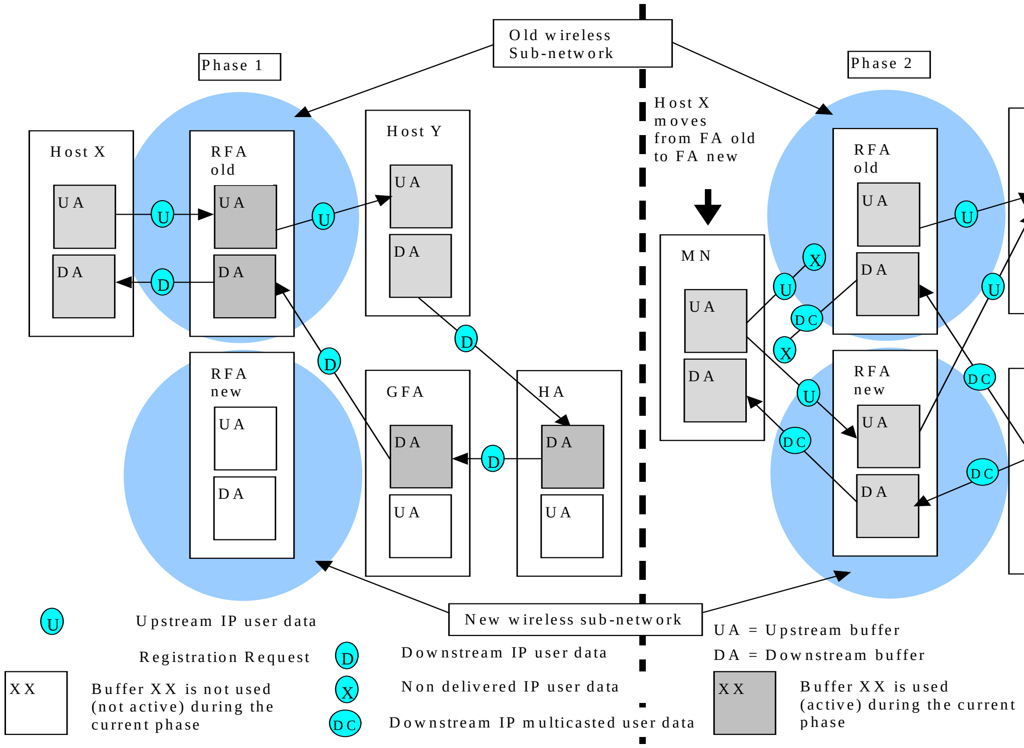


Figure 5-6: Fast handoff in Hierarchical Mobile IPv4

The hierarchical Mobile IPv6 protocol (see [MaSo00]) introduces a new network node called the Mobility Anchor Point (MAP). The goal of using this network entity is similar to the goal of using the GFA entity in the Hierarchical Mobile IPv4. MAP is used to manage the Host X registrations in a certain IPv6 region. This region may include more then one IPv6 Access Routers. Furthermore, it gives the possibility to Host X's to register locally, i.e., perform regional registrations, in a visited (new wireless) network. These regional registrations are accomplished by using the binding update procedure. For more details we refer to [MaSo00].

The fast handoff used in the Hierarchical Mobile IPv6 protocol is described in [MaSo00]. The main operation of this fast handoff can be explained by using Figure 5-7 for the situation that the Mobile IPv6 does not use the route optimisation option and by using the Figure 5-8 for the situation that the Mobile IPv6 does use the route optimisation option. The multicasting of the IP data packets in the downstream direction is accomplished by the MAP.

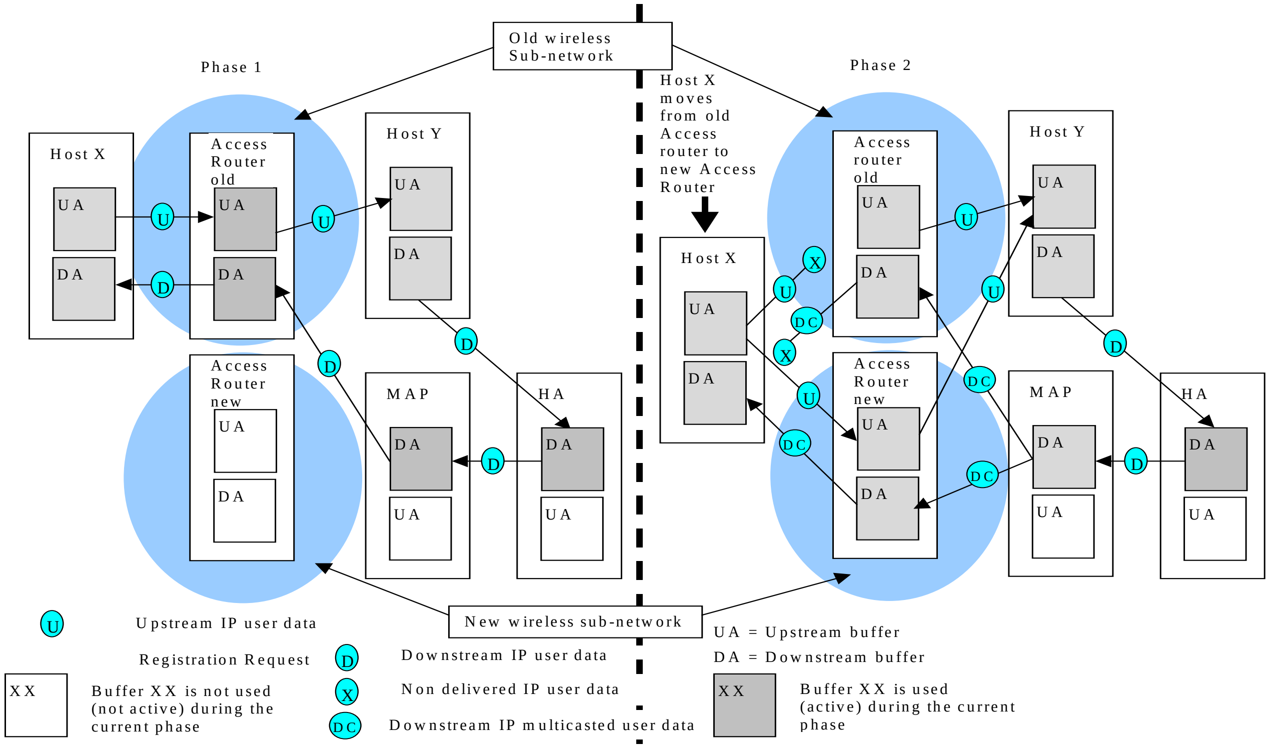


Figure 5-7: Fast handoff in Hierarchical Mobile IPv6 (without route optimisation)

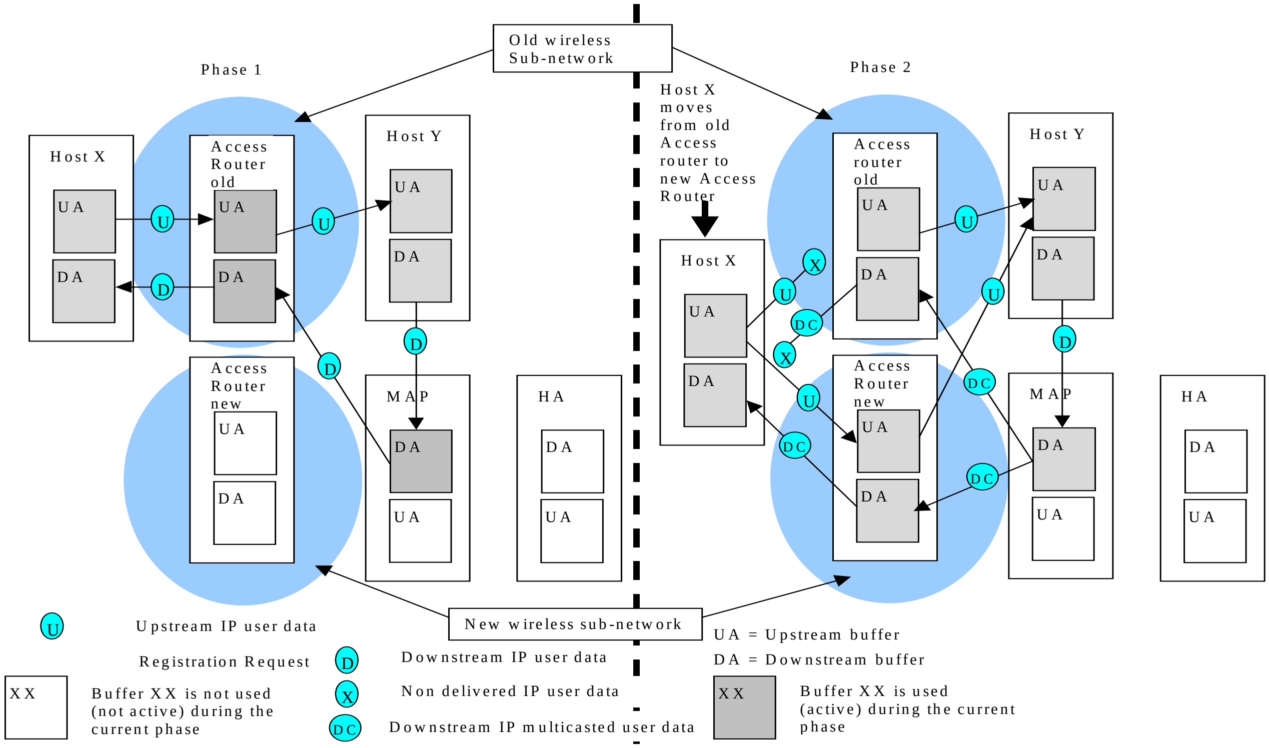


Figure 5-8: Fast handoff in Hierarchical Mobile IPv6 (with route optimisation)

5.3 PROBLEMS WITH KNOWN SOLUTIONS

The current smooth handoff concept is not able to efficiently solve the ***seamless handoff*** issue described in Section 5.1, for both Mobile IPv4 and Mobile IPv6 protocols.

The success of the smooth handoff concept for Mobile IPv4 on providing seamless handoff is very much depending on the speed of the procedure of registering with the Foreign Agent in the old wireless sub-network. If the speed of this procedure is slow then the disruption duration, that is the duration between the time that the old wireless access network becomes unreachable (due to quality deterioration of the wireless link) and the time that a new forwarding binding cache is created on the old Foreign Agent, could be high enough such that a significant number of IP packets will be lost. Note that this problem occurs only on the downstream direction, i.e., from the core network towards the Host X. In the opposite direction, i.e., upstream, all the packets that are already sent by the Host X towards the core network via the old wireless access network will be routed towards their destination by using standard IP routing procedures.

Similarly, the success of the smooth handoff concept for Mobile IPv6 on providing seamless handoff is very much depending on the speed of the procedure of identifying, selecting and registering with the temporary home agent in the old wireless sub-network. If the speed of these procedures is slow then the disruption duration, that is the duration between the time that the old wireless access network becomes unreachable (due to quality deterioration of the wireless link) and the time that a new forwarding binding cache is created on the old Access Router, could be high enough such that a significant number of IP packets will be lost.

A solution on this issue is provided by our proposal by efficiently buffering the IP packets that otherwise would have been lost during the disruption duration. An important issue that have to be solved is to estimate the size (length) of the required buffer that is used to buffer the packets sent by Host Y to the old Care-of Address of Host X. We consider this issue as an open issue.

Similarly, the current multicasting (bicasting) handoff concept is able to solve the ***seamless handoff*** issue, described in Section 5.1, for both Mobile IPv4 and Mobile IPv6 protocols, only if the following requirements are fulfilled:

- ✓ For both Mobile IPv4 and Mobile IPv6, the starting handoff time should be made known as soon as possible to the algorithm.
- ✓ Furthermore, for Mobile IPv6 the new entity specified in [MaSo00], called MAP should be used.
- ✓ A disadvantage of this concept is that during whole period of the handoff process and also for a period of time measured after the handoff completion, each IP packet that is destined to the Host X will have to be copied by the HA (in Mobile IPv4) or the GFA (in Hierarchical Mobile IPv4) or the MAP (in Hierarchical Mobile IPv6) and bicasted to the old (previous) and new Host X's Care-of Addresses.
- ✓ During whole the handoff process and also for a period of time measured after the handoff completion, a higher communication bandwidth from the communication network that is supporting the handoff process it will be required.

Our proposal during the handoff process does not require any higher communication bandwidth and does not use any bicasting.

5.4 DESCRIPTION

This section describes the requirements and the operation of this proposal.

The main advantages of this proposed seamless handoff concept compared to the smooth handoff concept described in Section 5.2.1, is that the handoff can be performed faster and that it can minimise or eliminate the number of packets that will otherwise be lost during the disruption duration (see Section 5.3). Moreover, the main advantage of this proposed seamless handoff concept compared to the existing bicasting concept described in Section 5.2.2 is that it is more efficient since it does not require any additional network bandwidth during the disruption duration. Furthermore, this concept does not require the establishment and maintenance of simultaneous bindings.

Moreover, depending on how capable the Host X is to be attached to wireless access networks we can identify two scenarios. One of these scenarios, that we call, “simultaneous wireless access”, represents the scenario that a Host X is connected simultaneously to two wireless access networks. This occurs when the radio technology allows such attachments or the handoff takes place between two different access technologies. The other scenario, that we call “single wireless access”, represents the scenario that the Host X is capable of being connected to one wireless access network at a time. In this document we only present the “simultaneous wireless access” scenario.

Requirements

The “seamless handoff in Mobile IP” proposal can be applied either in Mobile IPv4 or Mobile IPv6 only if a predefined set of the requirements given in this Section are fulfilled. Note that each Mobile IP handoff scenario may use a different set of requirements. In the following sections we will specify in detail which set of requirements, each Mobile IP handoff scenario needs in its operation.

- Requirement_1: The handoff starting time should be notified by the lower layers. Furthermore, if the Host X movement can be predicted before the handoff initiation moment, then this information should be used by this synchronised handoff algorithm to speed up the handoff process. This requirement is applied for Mobile IPv4 and Mobile IPv6. Moreover, this issue is not specified in this document and it is considered as an open issue.

  For Mobile IPv4 the initiation of the Mobile IP handoffs can be accomplished in the same way as described in [MaSo00], via the previous (or old) FA. Two methods of accomplishing this are described in [MASo00].

  ✓ The first method is based on Inter FA solicitation where it is assumed that the “current” FA with which the Host X is currently registered is aware of the IP address of the “new” FA which the Host X is moving to. The “current” FA will have to be informed by the lower protocol layers that the Host X will need to handoff. Subsequently the “current” FA will send to the “new” FA an Agent Solicitation message. The “new” FA will then send via the “current” FA an Agent Advertisement to the Host X. The Host X will subsequently send a registration request to the “new” FA through the “old” wireless access point served by the “current” FA.

  ✓ The second method is based on piggy-backing Advertisements on layer 2 protocol messages. In order to accomplish this, it is required that the layer 2 protocol should be able to interwork with Mobile IP. Once a layer 2 protocol handoff occurs, such that the Layer 2 of the “old” wireless access network is communicating with the Layer 2 of the “new” wireless access network, it is possible for the Layer 2 of the “new” wireless access network to solicit an Agent Advertisement from the “new” FA and transfer it to the “old” FA via the Layer 2 of the “old” wireless access network. The Host X after receiving the Agent Advertisment message, can perform a Registration Request that will be directed to the “new” FA .

For Mobile IPv6 the initiation of the Mobile IP handoffs can be accomplished in a similar way as described in [SoMa00]. In particular, it is required that the layer 2 protocol should be able to interwork with Mobile IPv6. Furthermore, once a layer 2 protocol handoff occurs, such that the Layer 2 of the "old" wireless access network is communicating with the Layer 2 of the "new" wireless access network, the following actions occur. The Host X is notified by the Layer 2 to send a Binding Update message to the Home Agent using the communication path set on the Layer 2 protocol between the "old" wireless access network and the "new" wireless access network.

- Requirement_2: The Host X must be notified by the layer 2 protocol that the connection between the Host X and the "old" wireless access network will be discarded in a very short time. This notification procedure can be applied for both "simultaneous wireless access" and "single wireless access" scenarios.
- Requirement_3: This requirement applies to the Mobile IPv4 and the Hierarchical Mobile IPv4 protocols that are not using the route optimisation feature. The HA or the GFA that receive a Registration Request message from the Host X, and requires the creation of a "new" binding with a "new" Care-of Address, must create this new binding and send two Registration Reply messages to the Host X. One of them should be sent to the new Care-of Address via the "new" FA that will notify the Host X that the binding has been created. The other Registration Reply is actually a DeRegistration Reply message that will be send to the old Care-of Address via the "old" FA and will notify the Host X that the binding with the "old" Care-of Address has been removed. Note that the DeRegistration Request message is a Registration Request message that has a lifetime header field equal to zero. Furthermore, the DeRegistration Reply message is a Registration Reply message that has a lifetime header field equal to zero. The lifetime header field equal to zero means that the binding with the Care-of Address specified in these registration messages will be deleted.
- Requirement_4: This requirement applies to the Mobile IPv4 and the Hierarchical Mobile IPv4 protocols that are not using the route optimisation feature. The FA that receives a DeRegistration Reply message from either the HA or GFA must send it to the Host X that initiated the DeRegistration Request message which caused the creation of this DeRegistration Reply message.
- Requirement_5: This requirement applies to the Mobile IPv4 protocol that is using the route optimisation feature, the Hierarchical Mobile IPv6 and the Mobile IPv6 protocols. The Host X that sends a deregistration BU (Binding Update) to a Host Y, to a HA or to a MAP via either the "old" FA or the "old" Access router, should activate the header flag "A". In this way the nodes that received the deregistration BU message will send a BA (Binding Acknowledgement) message back to the Host X via either the "old" FA or the "old" Access Router. Note that as deregistration BU we call the BU message that has a lifetime header field equal to zero.
- Requirement_6: All the Access Routers that are involved in a Mobile IPv6 and Hierarchical Mobile IPv6 handoff should be capable of becoming temporary Home Agents (see [JoPe00]). This temporary home agent will be used by a Host X that moves from an "old" Care-of Address to a "new" Care-of Address to identify the packets that were stored in the temporary home agent and were sent to the "old" Care-of Address and forward them to the "new" Care-of address via the "new" Access Router. This temporary home agent will create a "new" binding cache, after it receives a BU from the Host X. Note that in [JoPe00] it is not mentioned that also the packets that were stored before the creation of this "new" binding have to be forwarded. In our algorithm this is required (must be forwarded). This BU is constructed utilising the following steps (see [JoPe00]):
  - ✓ The packet that is carrying the BU must set the Home Address field in the Home Address option to the "old" (or "previous") Care-of Address for which packet forwarding is established.

  - ✓ The new binding's Care-of Address must be set to the new Care-of address to which packets destined to the "old" Care-of Address are to be forwarded.
  - ✓ In order to let the node that receives the BU to become a temporary home agent, the Home Registration (H) flag MUST also be set in this BU.

- Requirement_7: All Host X, FA's and HA's should be capable of supporting a modified version of the smooth handoff feature described in [PeJo00]. The modification is concerning two points:
  - ✓ The Host X must be capable of sending a BU directly to the "old" (or "previous") FA to create a "new" binding cache that binds its "old" Care-of Address with its "new" Care-of Address. In this way the "old" (or "previous") FA will not send the stored user data packets to the "old" Care of Address but it will tunnel all the packets that were stored and/or arriving at the "old" Care-of Address of the Host X to the "new" Care-of Address, i.e., to the "new" FA. Furthermore, the "old" FA must notify the creation of the "new" binding cache to the Host X by sending a BA via the "new" FA to the Host X. Note that in the standard smooth handoff procedure [PeJo00] it is mentioned that the BU that initiates the creation of this new binding cache (by the "old" or "previous" FA) is mainly sent by the "new" FA. However, it is also mentioned that the BU can also be sent by the Host X in the situations that the Host X does not receive the BA on time.
  - ✓ The "old" FA creates the "new" binding cache that binds the Host X's "old" Care-of Address with the Host X's "new" Care-of Address in the following way. Once the "old" FA receives the BU from the Host X that requests from this FA to create this new binding cache, it will not send the stored user data packets to the "old" Care-of Address but it will create a binding cache entry for the Host X to serve as a forwarding pointer (see [PeJo00]) to its new location. Any tunnelled messages to the "old" Care-of Address of the Host X that are stored in the "old" FA and/or that are arriving at this FA after the forwarding pointer has been created must be re-tunnelled to the Host X's new Care-of Address. Note that in the standard smooth handoff procedure [PeJo00] it is mentioned that after the creation of the new binding cache, any tunnelled packets for the Host X that arrive at its "old" FA after the forwarding pointer has been created can be re-tunnelled to the Host X's new Care-of Address. Thus, in the standard smooth handoff procedure [PeJo00] it is not mentioned that the already stored packets that arrived at the FA before the forwarding pointer has been created must be sent to new Care-of Address. In our proposed concept this is a requirement.
- Requirement_8: This requirement applies to the Mobile IPv4 and the Hierarchical Mobile IPv4 protocols. The security associations between the Mobile IP nodes is fulfilled using security procedures described in [RFC2002], [GuJo00], [PeCa00], [MaSo00] and [PeJo00].
- Requirement_9: This requirement applies to the Mobile IPv6 and the Hierarchical Mobile IPv6 protocols. The security associations between the Mobile IP nodes is fulfilled using security procedures described in [JoPe00], [PeCa00], [MaSo00] and [SoMa00].
- Requirement_10: This requirement applies to the Mobile IPv4 and the Hierarchical Mobile IPv4 protocols that do not use the route optimisation option. The Deregistration Reply (DRR) messages are stored and processed in the same way, i.e., identical scheduling mechanism, as the user data packets that are belonging to the same binding;
- Requirement_11: This requirement applies to the Mobile IPv4 protocols that are using the route optimisation feature, the Mobile IPv6 and the Hierarchical Mobile IPv6 protocols. The DBA messages that are used to confirm a de-registration BU message are stored and processed in the same way, i.e., identical scheduling mechanism, as the user data packets that are belonging to the same binding;

<u>Operation</u>

This section describes the operation of the proposed algorithm on various Mobile IP handoff scenarios. Note that all the figures that are used to describe this proposed algorithm use different IP nodes, i.e., Host X, Host Y, Access Routers, FA, GFA, MAP and HA. In these figures each of these nodes contain two buffers. One that is used for the upstream flows, called UA, and another one that is used for the downstream flows called DA. In some situations these buffers have a grey colour, meaning that they are used at that moment. In other situations these buffers are transparent, meaning that these buffers are not used at that moment.

5.4.1 Synchronised handoff in Mobile IPv4 with "simultaneous wireless access" and without route optimisation features

This handoff scenario can be realised only if the following requirements are fulfilled:

Requirement_1, Requirement_2, Requirement_3, Requirement_4, Requirement_7, Requirement_8 and Requirement_10.

This synchronised handoff type is applied for the situation that the Host X is capable of simultaneously being connected to two wireless access networks. In this document we consider that these wireless access networks are the UMTS and Bluetooth. Moreover, this handoff type is used for Mobile IPv4 scenarios that do not support the route optimisation feature. Depending on if the Host X receives on time the DeRegistration Reply (DRR) message from the FA (see Requirement_4) two scenarios can be distinguished:

- DRR received by the Host X via the "old" FA;
- DRR is not received by the Host X via the "old" FA.

5.4.1.1 DRR received by the Host X via the "old" FA

This situation occurs when the Host X receives the DRR, for a certain binding, before the "old" wireless access is deteriorating very badly, i.e., before the Host X is notified by the layer 2 protocol that the connection between the Host X and the "old" wireless access network will be discarded in a very short time (see Requirement_2). Considering that the DRR message is stored and processed by all the IP nodes in the same manner as the user data packets that are belonging to the same binding (see Requirement_10), it is realistic to consider that once the Host X receives the DRR message it can deduce that all packets that belong to the same binding as the DRR and were sent by the HA downstream to the Host X are received by this Host X. In this way the ***seamless handoff*** issue described in Section 5.1 is solved, since the packets sent between Host Y and Host X are not lost.

The operation of this synchronised scenario is viewed in Figure 5-9, Figure 5-10 and Figure 5-11.

The operation of this handoff type is accomplished in 5 subsequent phases.

- Phase 1: This operational phase is defined in [RFC2002]. During the first phase (see Figure 5-9) the Host X is communicating with the Host Y via the old wireless sub-network, "old" FA and HA.
- Phase 2: The second phase (see Figure 5-9) is activated at the moment that the Host X is willing to send the Registration Request (RQ) message to the HA. The HA is still sending downstream IP packets to the Host X via the old wireless sub-network. The Host Y is still receiving upstream packets from the "old" FA. During the second phase the following subsequent steps have to be fulfilled:

  - ✓ Step_1: This operational step is defined in [MaSo00]. The Host X using the algorithm described in Requirement_1 (see [MaSo00]) it will discover the “new” Care-of Address of the “new” FA via either the “old” FA or via the Layer 2 protocol of the “old” and “new” wireless access networks.
  - ✓ Step_2: This operational step is defined in [MaSo00]. Once the Host X knows the “new” Care-of Address of the “new” FA, it will send a Registration Request (RQ) message to the “new” FA via either the “old” FA or via the Layer 2 protocol of the “old” and “new” wireless access networks. This RQ message is sent to the HA. Note that this RQ message should not require the creation of a simultaneous binding.

- Phase 3: This operational phase is a new proposal. The third phase (see Figure 5-10) is activated at the moment that the HA is willing to send the Registration Reply (RR) message to the Host X. The Host Y is still receiving upstream packets from the “old” FA. During the third phase the following subsequent steps have to be fulfilled:
  - ✓ Step_1: the HA is using the algorithm described in Requirement_3. Once the HA received the RQ message from the Host X then the HA must create the new binding and send two Registration Reply (RR) messages to the Host X. One of them should be sent to the new Care-of Address via the “new” FA that will notify the Host X that the new binding has been created. The other RR is actually a DeRegistration Reply (DRR) message that will be send to the old Care-of Address via the “old” FA and will notify the Host X that the binding with the “old” Care-of Address has been removed.
  - ✓ Step_2: the HA sends downstream user data packets to the “new” FA.
  - ✓ Step_3: the “new” FA sends the RR to the Host X. The Host X will then know that the new binding has been successfully created. Moreover, the Host X will send upstream user data packets to the “new” FA and the “new” FA will send downstream user data packets to the Host X.
- Phase 4: This operational phase is a new proposal. The fourth phase (see Figure 5-10) is activated at the moment that the Host X receives the DRR packet via the “old” FA. This means that all packets that belong to the same binding as the DRR and were sent by the HA downstream to the Host X are received by this Host X. Thus the seamless handoff issue described in Section 5.1 is solved, since the packets sent between Host Y and Host X are not lost. Furthermore, the Host Y may still receive upstream packets via the “old” FA. The Host Y will also receive upstream packets via the “new” FA. The HA sends downstream user data packets to the “new” FA.
- Phase 5: This operational phase is defined in [RFC2002]. During phase 5 (see Figure 5-11) the Host X is communicating with the Host Y via the new wireless sub-network, “new” FA and HA.

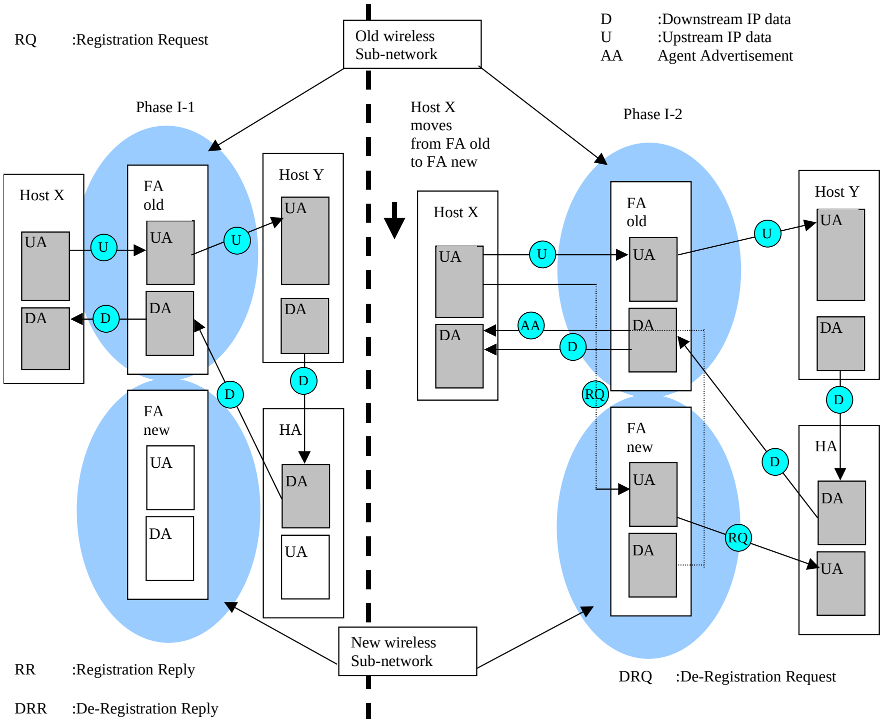


Figure 5-9: Mobile IPv4 without route optimisation with “simultaneous wireless access”; phase I-1 and phase I-2

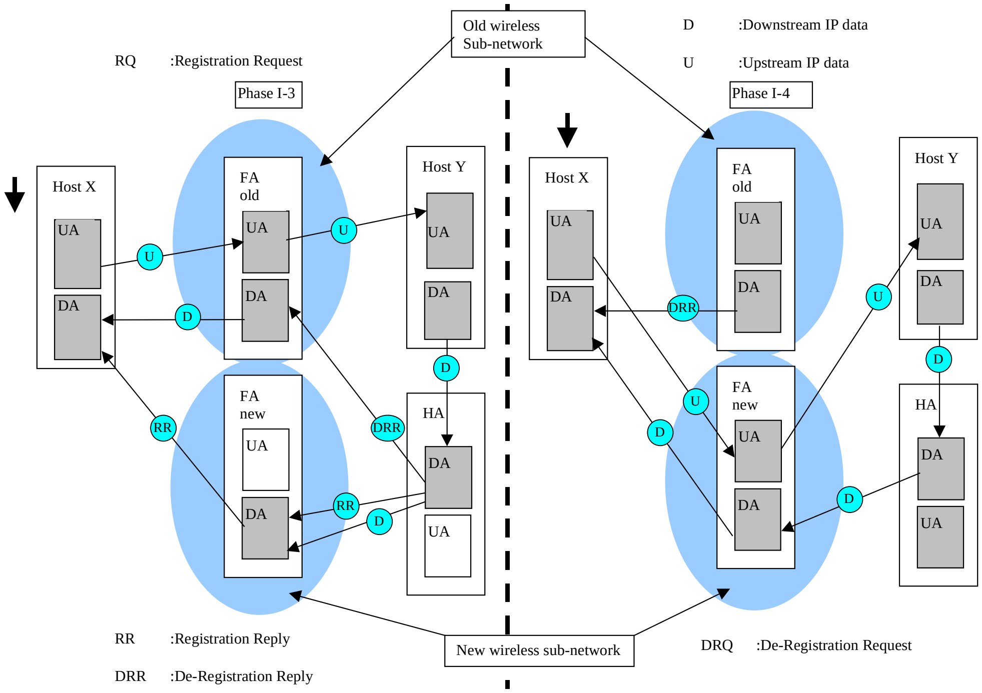


Figure 5-10: Mobile IPv4 without route optimisation with “simultaneous wireless access”; phase I-3 and phase I-4

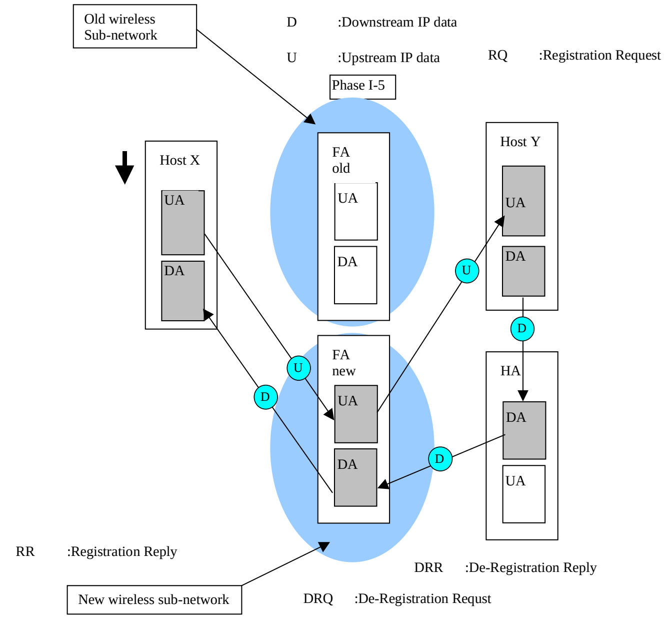


Figure 5-11: Mobile IPv4 without route optimisation with "simultaneous wireless access"; phase I-5

5.4.1.2 DRR is not received by the Host X via the "old" FA

This situation occurs when the Host X does not receive the DRR, for a certain binding. If the Host X will be notified by the layer 2 protocol about a bad deterioration of the "old" wireless access network (see Requirement_2), and if the Host X did not receive the DRR message it will then send a BU (see Requirement_7) directly to the "old" (or "previous") FA to create a "new" binding cache for its "old" Care-of Address with its "new" Care-of Address. In this way the "old" (or "previous") FA will stop sending the stored user data packets to the "old" FA, and it will be able to tunnel all the packets that were stored and/or arriving at the "old" Care-of Address of the Host X to the "new" Care-of Address, i.e., to the "new" FA. In this way the Host X will receive all the user data packets that were stored and sent to the "old" Care-of Address, thus solving the ***seamless handoff*** issue explained in Section 5.1, since the packets sent between Host Y and Host X are not lost.

The operation of this handoff type is accomplished in 6 subsequent phases. The operational phases Phase 1, Phase 2 and Phase 3 are identical to phases Phase 1, Phase 2 and Phase 3, respectively, described in Section 5.4.1.1.

- Phase 4: The fourth phase (see Figure 5-17) is activated at the moment that the Host X is notified by the layer 2 protocol (see Requirement_2) that the connection between the Host X and the "old" wireless access network will be discarded in a very short time. The Host Y may still receive upstream packets sent via the "old" FA. Moreover the Host Y will receive upstream packets sent via the "new" FA. The HA sends downstream user data packets to the "new" FA. During the fourth phase the following subsequent steps have to be fulfilled:
  - ✓ Step_1 This operational step is a new proposal. The Host X is notified by the layer 2 protocol that the connection between the Host X and the "old" wireless access network will be discarded in a very short time.

- ✓ Step_2: This operational step is a new proposal. The Host X sends a BU directly to the “old” (or “previous”) FA to create a “new” binding cache for its “old” Care-of Address with its “new” Care-of Address. In this way the “old” (or “previous”) FA will not send the stored user data packets to the “old” Care of Address but it will tunnel all the packets that were stored and/or arriving at the “old” Care-of Address of the Host X to the “new” Care-of Address, i.e., to the “new” FA.

- ✓ Step_3: This operational step is described in [PeJo00]. The “old” FA after accepting this BU request (see also [PeJo00]) it will create this “new” binding cache for the Host X’s “old” Care-of Address with the Host X’s “new” Care-of Address and it will notify this to the Host X by sending him one BA message via the “new” FA.

- Phase 5: This operational phase is defined in [PeJo00]. Phase 5 (see Figure 5-18) is activated at the moment that the “old” FA starts forwarding the user data packets that were sent to the Host X’s “old“ Care-of Address (see Requirement_7) to the “new” FA. These packets are sent by the “new” FA to the Host X. Furthermore, during phase 5, the Host X is communicating with the Host Y via the “new” FA and the HA.

- Phase 6: This operational phase is defined in [RFC2002]. Phase 6 (see Figure 5-18) is activated when all the user data packets that were send to the Host X’s “old” Care-of Address are sent to the Host X via the “new” FA. During this phase the Host X is communicating with the Host Y via the “new” FA and the HA.

5.4.2 Synchronised handoff in Mobile IPv6 with “simultaneous wireless access” and without route optimisation features

This handoff scenario can be realised only if the following requirements are fulfilled:

Requirement_1, Requirement_2; Requirement_5; Requirement_6; Requirement_9 and Requirement_11.

This synchronised handoff type is applied for the situation that the Host X is capable of simultaneously being connected to two wireless access networks. In this document we consider that these wireless access networks are the UMTS and Bluetooth. Moreover, this handoff type is used for Mobile IPv6 scenarios that do not support the route optimisation feature. Depending on if the Host X receives on time the deregistration Binding Update (DBA) message from the “old” Access Router (see Requirement_5) two scenarios can be distinguished:

- DBA received by the Host X via the “old” Access Router;

- DBA not received by the Host X via the “old” Access Router.

5.4.2.1 DBA received by the Host X via the “old” Access Router

This situation occurs when the Host X receives the DBA, for a certain binding, before the “old” wireless access is deteriorating very badly, i.e., before the Host X is notified by the layer 2 protocol that the connection between the Host X and the “old” wireless access network will be discarded in a very short time (see Requirement_2). Considering that the DBA message is stored and processed by all the IP nodes in the same manner as the user data packets that are belonging to the same binding (see Requirement_11), it is realistic to consider that once the Host X receives the DBA message it can deduce that all packets that belong to the same binding as the DBA and were sent by the HA downstream to the Host X are received by this Host X. In this way the ***seamless handoff*** issue described in Section 5.1 is solved, since the packets sent between Host Y and Host X are not lost.

The operation of this synchronised scenario is viewed in Figure 5-12, Figure 5-13 and Figure 5-14.

The operation of this handoff type is accomplished in 5 subsequent phases.

- Phase 1: This operational phase is defined in [JoPe00]. During the first phase (see Figure 5-12) the Host X is communicating with the Host Y via the old wireless sub-network, “old” Access Router and HA.
- Phase 2: The second phase (see Figure 5-12) is activated at the moment that the Host X is willing to send the BU message to the HA. The HA is still sending downstream IP packets to the Host X via the old wireless sub-network. The Host Y is still receiving upstream packets from the “old” Access Router. During the second phase the following subsequent steps have to be fulfilled:
    - ✓ Step_1: This operational step is defined in [MaSo00], [SoMa00]. The Host X using the algorithm described in Requirement_1 (see [MaSo00]) it will discover the “new” Care-of Address of the “new” Access Router via either the “old” Access Router or via the Layer 2 protocol of the “old” and “new” wireless access networks.
    - ✓ Step_2a: This operational step is defined in [MaSo00], [SoMa00]. Once the Host X knows the “new” Care-of Address of the “new” Access Router, it will send a BU message to the “new” Access Router via either the “old” Access Router or via the Layer 2 protocol of the “old” and “new” wireless access networks. This BU message is sent to the HA.
    - ✓ Step_2b: This operational step is a new proposal. Furthermore, the Host X will send a deregistration BU (DBU) to the HA via the “old” Access Router. The reason of this is to delete the “old” binding from the HA. The flag “A” of both BU messages is set to active. In this way the HA is requested to send BA’s to the Host X.
- Phase 3: This operational phase is a new proposal. The third phase (see Figure 5-13) is activated at the moment that the HA is willing to send the BA message to the Host X. The Host Y is still receiving upstream packets from the “old” Access Router. During the third phase the following subsequent steps have to be fulfilled:
    - ✓ Step_1: Once the HA received the BU message from the Host X then the HA must create the new binding and send a BA message to the Host X. This will be sent to the “new” Care-of Address via the “new” Access Router that will notify the Host X that the new binding has been created. When the HA receives the DBU message it will delete the “old” binding that the HA had stored for the Host X’s “old” Care-of Address and it will send a DBA to the Host X via the “old” Access Router.
    - ✓ Step_2: the HA sends downstream user data packets to the “new” Access Router.
    - ✓ Step_3: the “new” Access Router sends the BA to the Host X. The Host X will then know that the new binding has been successfully created. Moreover, the Host X will send upstream user data packets to the “new” Access Router and the “new” Access Router will send downstream user data packets to the Host X.
- Phase 4: This operational phase is a new proposal. The fourth phase (see Figure 5-13) is activated at the moment that the Host X receives the DBA packet via the “old” Access Router. This means that all packets that belong to the same binding as the DBA and were sent by the HA downstream to the Host X are received by this Host X. Thus the seamless handoff issue described in Section 5.1 is solved, since the packets sent between Host Y and Host X are not lost. Furthermore, the Host Y may still receive upstream packets via the “old” Access Router. Moreover the Host Y will receive upstream packets via the “new” Access Router. The HA sends downstream user data packets to the “new” Access Router.

- Phase 5: This operational phase is described in [JoPe00]. During phase 5 (see Figure 5-14) the Host X is communicating with the Host Y via the new wireless sub-network, “new” Access Router and HA.

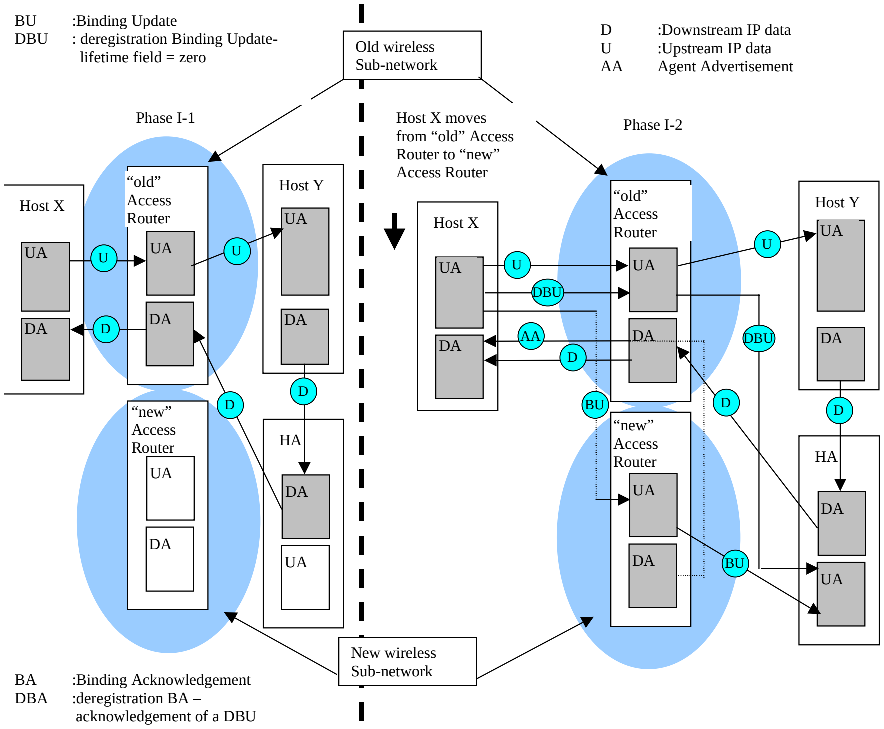


Figure 5-12: Mobile IPv6 without route optimisation with “simultaneous wireless access”; phase I-1 and phase I-2

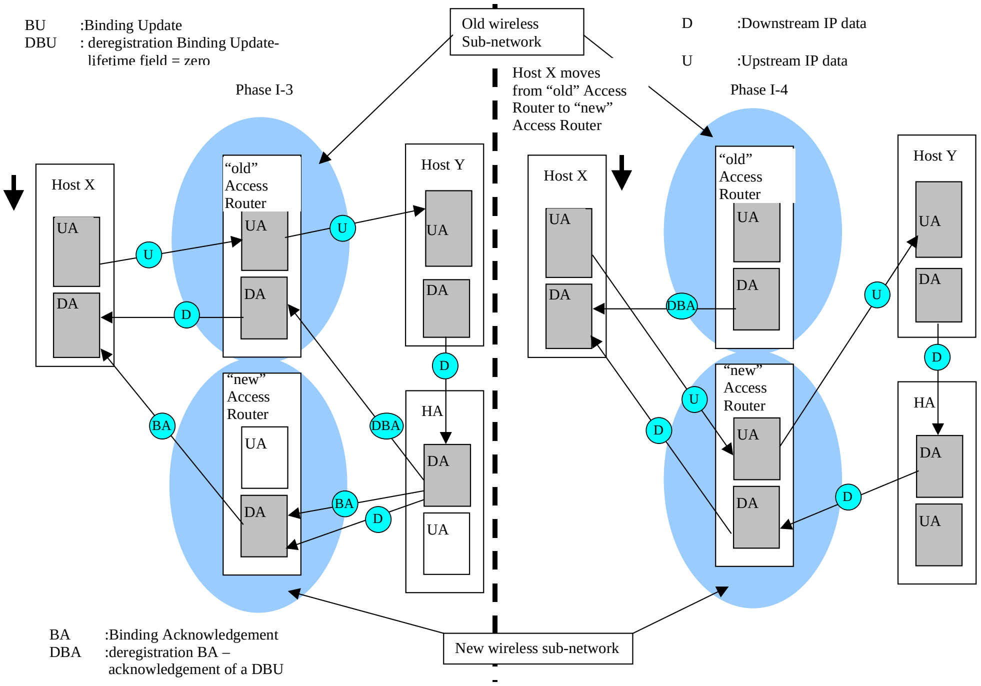


Figure 5-13: Mobile IPv6 without route optimisation with “simultaneous wireless access”; phase I-3 and phase I-4

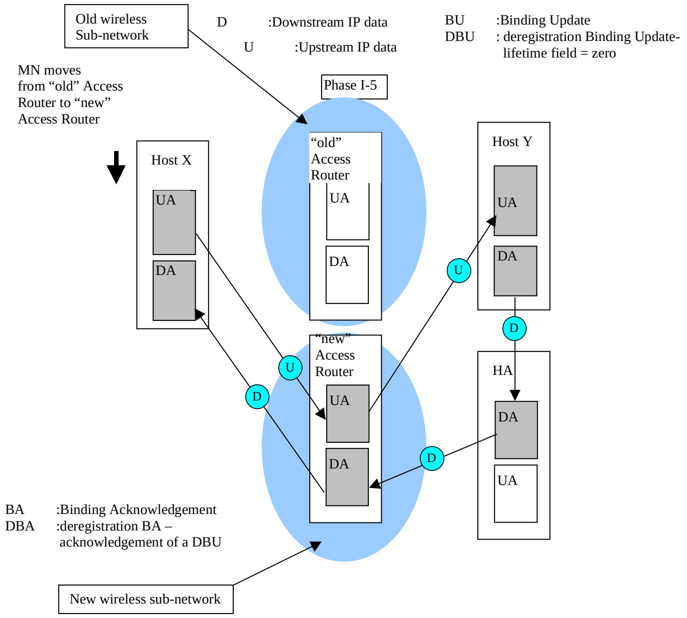


Figure 5-14: Mobile IPv6 without route optimisation with “simultaneous wireless access”; phase I-5

5.4.2.2 DBA is not received by the Host X via the “old” Access Router

This situation occurs when the Host X does not receive the DBA, for a certain binding.

If the Host X will be notified by the layer 2 protocol about a bad deterioration of the “old” wireless access network (see Requirement_2), and if the Host X did not receive the DBA message it will then send a BU (see Requirement_6) directly to the “old” (or “previous”) Access Router to create a “new” binding cache for its “old” Care-of Address with its “new” Care-of Address. This “old” Access Router will then become a temporary home agent (see Requirement_6). In this way the “old” (or “previous”) Access Router will stop sending the stored user data packets to the “old” Access Router, and it will be able to tunnel all the packets that were stored and/or arriving at the “old” Care-of Address of the Host X to the “new” Care-of Address, i.e., to the “new” FA. In this way the Host X will receive all the user data packets that were stored and sent to the “old” Care-of Address, thus solving the ***seamless handoff*** issue explained in Section 5.1, since the packets sent between Host Y and Host X are not lost.

The operation of this handoff type is accomplished in 6 subsequent phases. The operational phases Phase 1, Phase 2 and Phase 3 are identical to phases Phase 1, Phase 2 and Phase 3, respectively, described in Section 5.4.2.1.

- Phase 4: The fourth phase (see Figure 5-15) is activated at the moment that the Host X is notified by the layer 2 protocol (see Requirement_2) that the connection between the Host X and the “old” wireless access network will be discarded in a very short time. The Host Y may still receive upstream packets sent via the “old” Access Router. Moreover the Host Y will receive upstream packets sent via the “new” Access Router. The HA sends downstream user data packets to the “new” Access Router. During the fourth phase the following subsequent steps have to be fulfilled:
  - ✓ Step_1: This operational step is a new proposal. The Host X is notified by the layer 2 protocol that the connection between the Host X and the “old” wireless access network will be discarded in a very short time.

- ✓ Step_2: This operational step is a new proposal. The Host X sends a BU directly to the “old” (or “previous”) Access Router (see Requirement_6) to create a “new” binding cache for its “old” Care-of Address with its “new” Care-of Address. In this way the “old” (or “previous”) Access Router will not send the stored user data packets to the “old” Care of Address but it will tunnel all the packets that were stored and/or arriving at the “old” Care-of Address of the Host X to the “new” Care-of Address, i.e., to the “new” Access Router. This “old” Access Router will then become a temporary home agent (see Requirement_6) for this Host X.

- ✓ Step_3: This operational step is defined in [JoPe00]. The “old” Access Router after accepting this BU request (see also [JoPe00]) it will create this “new” binding cache that binds the Host X’s “old” Care-of Address with the Host X’s “new” Care-of Address and it will notify this to the Host X by sending him one BA message via the “new” Access Router.

- Phase 5: This operational phase is defined in [JoPe00]. Phase 5 (see Figure 5-16) is activated at the moment that the “old” Access Router starts forwarding the user data packets that were sent to the Host X’s “old“ Care-of Address (see Requirement_6) to the “new” Access Router. These packets are sent by the “new” Access Router to the Host X. Furthermore, during phase 5, the Host X is communicating with the Host Y via the “new” Access Router and the HA.

- Phase 6: This operational phase is defined in [JoPe00]. Phase 6 (see Figure 5-16) is activated when all the user data packets that were send to the Host X’s “old” Care-of Address are sent to the Host X via the “new” Access Router. During this phase the Host X is communicating with the Host Y via the “new” Access Router and the HA.

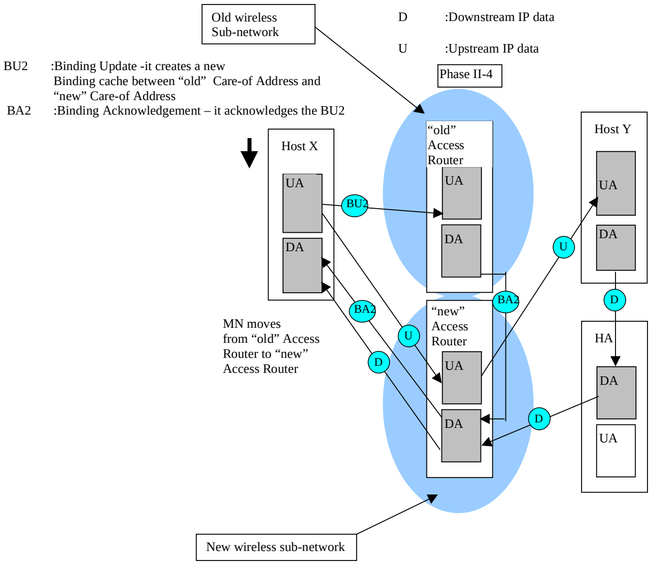


Figure 5-15: Mobile IPv6 without route optimisation with “simultaneous wireless access”; phase II-4

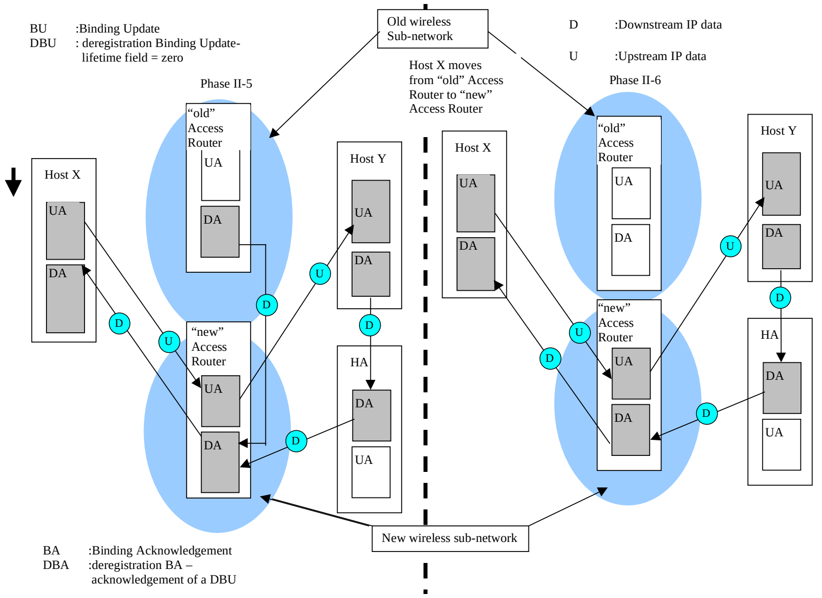

BU :Binding Update
DBU : deregistration Binding Update- lifetime field = zero
Old wireless Sub-network
D :Downstream IP data
U :Upstream IP data
Host X moves from "old" Access Router to "new" Access Router
Phase II-5
Phase II-6
"old" Access Router
UA
DA
Host X
Host Y
HA
"new" Access Router
D
U
New wireless sub-network
BA :Binding Acknowledgement
DBA :deregistration BA – acknowledgement of a DBU

Figure 5-16: Mobile IPv6 without route optimisation with "simultaneous wireless access"; phase II-5 and phase II-6

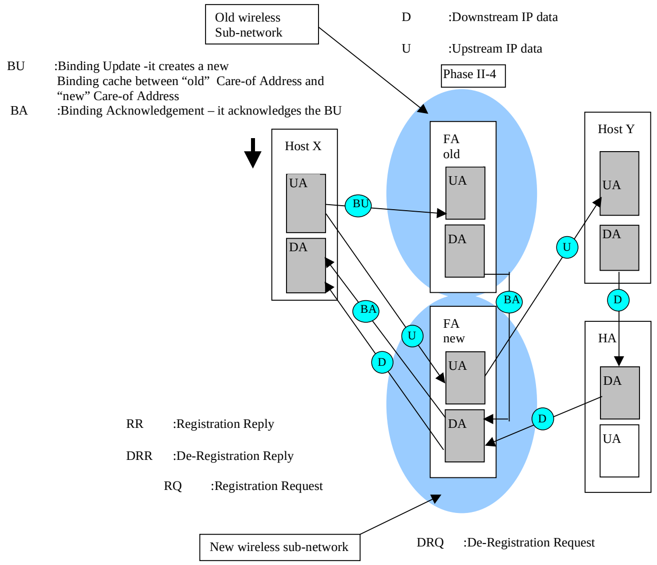

Old wireless Sub-network
D :Downstream IP data
U :Upstream IP data
BU :Binding Update -it creates a new Binding cache between "old" Care-of Address and "new" Care-of Address
BA :Binding Acknowledgement – it acknowledges the BU
Phase II-4
Host X
FA old
FA new
Host Y
HA
UA
DA
BU
BA
U
D
RR :Registration Reply
DRR :De-Registration Reply
RQ :Registration Request
New wireless sub-network
DRQ :De-Registration Request

Figure 5-17: Mobile IPv4 without route optimisation with "simultaneous wireless access"; phase II-4

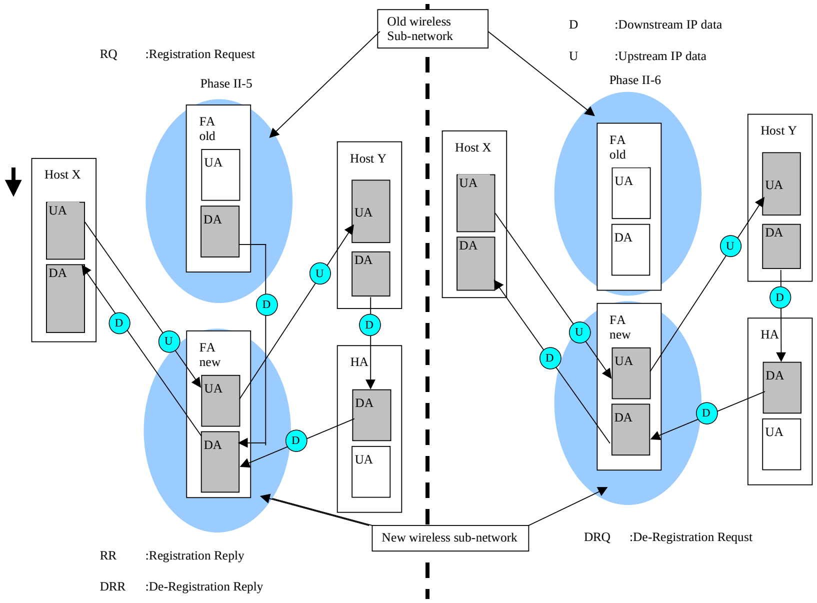


Figure 5-18: Mobile IPv4 without route optimisation with “simultaneous wireless access”; phase II-5 and phase II-6

6 Conclusions

Real time applications, like IP telephony and multimedia conferencing, that will be supported by mobile environments demand the development and introduction of QoS and mobility solutions in the Internet.

In this document an architecture is described that can provide Internet access to mobile hosts by allowing them to access this architecture through various access points and using various wireless technologies.

In this architecture the roaming host has the possibility of being simultaneously connected to different technologies. As example, we considered that the roaming host can be simultaneously connected to two technologies, i.e., UMTS and Bluetooth.

In this document a method is presented of selecting the wireless technology that satisfies all the user and network demands in the most efficient way. RSVP is used as the dynamic QoS management protocol applied to establish and maintain end to end QoS sessions among IP subnetworks that may use different types of QoS management architectures. However, the same principles may be applied when other QoS management protocol, e.g., RSVP aggregation [BaIt00] is used instead RSVP.

The IP mobility protocols used in this architecture are the current specified versions of Mobile IPv4 and Mobile IPv6. However, using these Mobile IP versions it could happen that during handoff the user will experience high delays and packet losses. This document presents a solution to this drawback, by providing seamless mobility. In this way the proposed architecture is capable of satisfying all the requirements listed in Section 1.

Furthermore, this document identified and listed a number of open issues, see Section 6.1, that are related to the topic presented in this document and have to be solved in the future.

6.1 Open issues

The proposed network architecture used to provide ubiquitous Internet access to mobile hosts contains several open issues that need to be solved in the future. These are:

- the architecture should support the possibility of having a host that is represented by a group entities similar to Figure 2-8;
- the architecture should support the situation where both wireless technologies are covering the same area and are belonging to the same IP subnetwork;
- the architecture should support a Technology Selector unit (see Figure 3-2). We consider the development of the Technology Selector as an open issue;
- after successful network attachment (see Section 4.1) the SIP protocol has to be triggered in order to start the “QoS session setup”. We consider the development of such a triggering algorithm as an open issue.
- the RSVP protocol supports release procedures that are based on the soft state principle, i.e., if a state is not refreshed regularly, will be released. In contrary, UMTS does not support the soft state principle. Therefore, an algorithm has to be developed to interoperate between the RSVP soft state release and the UMTS QoS release (see Section 4.1.1). We consider the development of such an algorithm, as an open issue.
- an algorithm must be developed to identify when the Bluetooth Network Attachment procedures (see Section 4.1.2) must be started and by which entity, e.g., the Host or the Bluetooth NAP, will they be initiated. We consider the development of such an algorithm an open issue.

- In the situation that the Bluetooth NAP is RSVP aware (see Section 4.1.2), then a selection has to be made regarding which entity, i.e., Host or NAP, will initiate the Bluetooth QoS resource reservation procedure. We consider the development of such an algorithm an open issue.
- the RSVP protocol supports release procedures that are based on the soft state principle, i.e., if a state is not refreshed regularly, will be released. In contrary, Bluetooth does not support the soft state principle. Therefore, an algorithm has to be developed to interoperate between the RSVP soft state release and the Bluetooth QoS release (see Section 4.1.2). We consider the development of such an algorithm, as an open issue.
- the functionality of the QoS API (see Section 4.1.1) is not defined in this document. We consider the development of the QoS API as an open issue.
- using performance evaluation, the size (length) of the required buffer used to store the packets sent by Host Y to the old Care-of Address of Host X could be estimated. We consider this issue as an open issue.
- a mechanism must be developed to provide the interoperation between the Layer 2 and the Mobile IP algorithms. In particular, it must be capable of notifying the Mobile IP algorithms when a Layer 2 handoff starts and when it ends. This issue is not specified in this document and it is considered as an open issue.

7 References

[3GPP23.060] 3GPP Deliverable, “General Packet Radio Service (Release 1999); Service Description stage 2”, Deliverable 3G TS 23.060, January 2000.

[3GPP23.107] 3GPP technical Specification Group Services and System Aspects, “QoS Concept and Architecture, Release 1999, version 3.3.0, 2000.

[3GPP23.923] 3GPP Deliverable, “Combined GSM and Mobile IP Handling in UMTS IP CN”, Deliverable 3G TS 23.923, May 2000.

[BaIt00] Baker, F., Iturralde, C. Le Faucher, F., Davie, B., “Aggregation of RSVP for Ipv4 and Ipv6 Reservations”, draft-ietf-issl-rsvp-aggr-03.txt, 2000 (work in progress).

[BLUESPEC] Bluetooth SIG report, “Specification of the Bluetooth System; Core”, Version 1.0 B, December 1st 1999.

[GuJo00] Gustafsson E., Jonsson A., Perkins C., “Mobile IP Regional Registration”, Internet draft, draft-ietf-mobileip-reg-tunnel-02.txt, Work in progress, March 2000.

[Haa98] Haartsen J. “BLUETOOTH – the universal radio interface for ad hoc, wireless connectivity”, Ericsson review No. 3, 1998.

[JoPe00] Johnson, D., B., Perkins, C., “Mobility Support in IPv6”, Internet draft, draft-ietf-mobileip-ipv6-13.txt, Work in progress, November 2000.

[KaRe00] Karagiannis, G., Rexhepi, V., “A Framework for QoS & Mobility in the Internet Next Generation”, Internet Next Generation report, 2000, located at: http://ing.ctit.utwente.nl/WU4/Documents/frame_a.pdf

[Kar99] Karagiannis, G., “Mobile IP: State of the Art”, Internet Next Generation report, 1999, located at: http://ing.ctit.utwente.nl/WU4/Documents.

[Kar00] Karagiannis, G., “QoS in GPRS”, Internet Next Generation report, 2000, located at: http://ing.ctit.utwente.nl/WU4/Documents.

[MaSo00] El Malki K., Soliman H., “Hierarchical Mobile IPv4/v6 and Fast Handoffs”, Internet draft, draft-elmalki-soliman-hmipv4v6-00.txt, Work in progress, March 2000.

[PeCa00] Perkins, C., E., Calhoun, P., R., “Mobile IP Challenge/Response Extensions”, IETF draft draft-ietf-mobileip-challenge-12.txt, Work in progress, June 2000.

[PeJo00] Perkins, C., Johnson, B., J., “Route Optimisation in Mobile IP”, Internet draft, draft-ietf-mobileip-optim-10.txt, Work in progress, November 2000.

[Per97] Perkins, C., E., “Mobile IP”, IEEE Communications Magazine, May 1997.

[Per98] Perkins, C., E., “Mobile networking through mobile IP”, IEEE Internet Computing, 1998.

[RFC826]. Plummer, D., C., “An Ethernet address resolution protocol: Or converting network protocol addresses to 48.bit Ethernet addresses for transmission on Ethernet hardware”, RFC 826, November 1982.

[RFC1256] Deering, S., (ed.), “ICMP Router Discovery Messages”, RFC 1256, August 1989.

[RFC1541] Droms, R., “Dynamic Host Configuration Protocol”, RFC 1541, October 1993.

[RFC1633] Braden, R., Clark, D., Shenker, S., “Integrated Services in the Internet Architecture: An Overview”, IETF RFC 1633, 1994.

[RFC1661] Simpson, W., (editor), “The Point-to-Point protocol (PPP)”, RFC1661, July 1994.

[RFC1905] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, 1996.

[RFC1970] Narten, T., Nordmark, E., Simpson, W., A., “Neighbour Discovery for IP version 6 (IPv6)”, RFC 1970, August 1996.

[RFC1971] Thomson, S., Narten, T., “Ipv6 stateless address autoconfiguration”, RFC1971, August 1996.

[RFC2002] Perkins, C., E., “(ed.) “IP Mobility Support”, RFC2002, proposed standard. IETF Mobile IP Working Group, Oct., 1996.

[RFC2003] Perkins, C., “IP encapsulation within IP”, RFC2003, October 1996.

[RFC2004] Perkins, C., “Minimal encapsulation within IP”, RFC2004, October 1996.

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S., “ Resource Reservation Protocol (RSVP) Version 1 Functional Specification”, IETF RFC 2205, 1997.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Zh., Weiss, W., “An architecture for Differentiated Services”, IETF RFC 2475, 1998.

[RFC2543] Handley, M., Schulzrinne, H., Schooler, E., Rosenberg, J., “ SIP: Session Initiation Protocol”, IETF RFC 2543, 1999.

[RFC2597] Heinanen, J., Baker, F., Weiss, W., Wroclawski, J., “Assured Forwarding PHB group”, IETF RFC 2597, 1999.

[RFC2748] Durham, D., Boyle, J., Cohen, R., Herzog, S., Raja, R., Sastry, A., “The COPS (Common Open Policy Service) Protocol ”, IETF RFC, January 2000.

[RFC2638] Nichols, K., Jacobson, V., Zhang, L., “ A two-bit Differentiated Services Architecture for the Internet”, IETF RFC 2638, 1999.

[TeCh99] Teitelbaum, B., Chimento, P. “Qbone Bandwidth Broker Architecture” at “http://qbone.ctit.utwente.nl/deliverables/1999/d2/bboutline2.html” (work in progress)

[SoMa00] Soliman H., El Malki K., “Hierarchical Mobile IPv6 and Fast Handoffs”, Internet draft, draft-soliman-mobileip-hmipv6-00.txt, Work in progress, June 2000.

[VoIP] U. Black, “Voice OVER IP”, Prentice Hall Series in Advance Technologies, 2000.

[WeTu00] Westberg, L., Turanyi, Z. R.,.Partain, D., “Load Control of Real-Time Traffic”, IETF draft, draft-westberg-loadcntr-03.txt, Work in progress, April 2000.

[Zee00] van der Zee, “Quality of Service in Bluetooth networking”, Internet Next generation report, 2000, located at: http://ing.ctit.utwente.nl/WU4/Documents/

[ZeAi99] van der Zee, M., Ait Yaiz, R., “Quality of Service over Specific Link Layers”, QWING State of the Art Report, 1999, located at: http://ing.ctit.utwente.nl/WU4/Documents/

8 Abbreviations

3GPP	3^{rd} Generation Partnership Project
AB	Access Boundary
ACL	Asynchronous Connectionless Link
API	Application Programming Interface
APN	Access Point Name
AR	Access Router
BB	Bandwidth Broker
BG	Border Gateway
BS	Bearer Service
BT	Bluetooth Terminal
BU	Binding Update
CH	Correspondent Host
CN	Correspondent Node
CRM	Core Resource Manager
DB	Diffserv Boundary
DBA	Deregistration Binding Update
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiated Services
DRR	DeRegistration Reply
FA	Foreign Agent
FH	Frequency-hop
GFA	Gateway Foreign Agent
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HA	Home Agent
HLR	Home Location Register
IC	Integrated Circuit
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGSN	Internet GPRS Support Node.
IP	Internet Protocol
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6

ISM	Industrial-Scientific Medical
L2CAP	Logical Link Control and Adaptation Protocol
LMP	Link Manager Protocol
MAP	Mobility Anchor Point
MC	Mobility Client
MIP+	Mobile IPv4 future version
MS	Mobile Station
MT	Mobile Terminal
NAP	Network Access Point
NS	Network Service
NSAPI	Network Layer Service Access Point Identifier
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMNs	Public Land Mobile Networks
PPP	Point-to-Point Protocol
QoS	Quality of Service
RA	Resource Allocation
RAB	Radio Access Bearer
RC	Resource Client
RM	Resource Manager
RNS	Radio Network Subsystem
RQ	Registration Request
ResR	Resource Requester
RR	Registration Reply
RSVP	Resource ReserVation Protocol
SAP	Service Access Point
SCO	Synchronous Connection Oriented
SDP	Session Description Protocol
SDU	Service Data Units
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SMS	Short Message Service

TCP	Transmission Control Protocol
TDD	time-division-duplex
TE	Terminal Equipment
TFT	Traffic Flow Template
TI	Transaction Identifier
TS	Technology Selector
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication Services
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitors Location Register
VoIP	Voice over IP
W-LAN	Wireless Local Area Network