3GPP - TSG SA #5 **Tdoc SP-99389**
11-13 October, 1999
Kyongju, Korea

Title: 3G TR 23.923 V 1.0.0:
Combined GSM and Mobile IP Mobility Handling in UMTS IP CN

Date: 1999-10-06

Source: S2

Purpose: For information

Agenda Point: 5.2.3

The attached document contains version 1.0.0 of the 3G TR 23.923: *Combined GSM and Mobile IP Mobility Handling in UMTS IP CN.*

3G TR 23.923 V~~0.9.0~~1.0.0 (1999-~~09-09~~-10-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Combined GSM and MobileIP Mobility Handling in UMTS IP CN (3G TR 23.923 version ~~0.9.0~~1.0.0)

Reference
DTS/TSGS-022923 U

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 Indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the specification;

Introduction

A single generic mobility handling mechanism that allows roaming between all types of access networks would allow users to conveniently move between fixed and mobile networks, between public and private networks as well as between PLMN's with different access technologies. The ongoing work in the IETF Mobile IP working group is targeted towards such a mechanism. To offer Mobile IP(+)[1] also to UMTS and GPRS users, a standard is needed for how to use Mobile IP in overlay to UMTS/GPRS.

Additionally, Mobile IP(+) could be used to handle mobility in the UMTS CN. This would allow transparency to networks external to the UMTS PLMN. Potentially, this would also allow cost savings for operators and a broadening of the market for manufacturers.

This document is the result of two 3GPP-TSG SA-WG2 work items on Mobile IP:

1. "Combined GSM and Mobile IP mobility handling in UMTS IP CN", which main goal is to describe and evaluate an architecture that uses Mobile IP+ for mobility management and tunneling within the CN. With respect to the work in IETF, a time scale for including this architecture in UMTS standards should be proposed.

2. "GPRS Mobile IP interworking", that aims at defining enhancements to the current GPRS standards to allow Mobile IP(+) to be used as an overlay to UMTS/GPRS for release 99.

A summary of the technical results is presented in Chapter 19.

[1] Mobile IP+ is defined in chapter 6.

1 Scope

The present document contains a feasibility study on using Mobile IP+ as a tunneling and mobility management protocol in combination with GSM/UMTS mobility management in the packet domain of UMTS CN. A target architecture will be described and evaluated and the migration path from the current GPRS architecture towards the target architecture will be defined. It shall also describe the driving forces for moving from GTP towards Mobile IP+ as well as the benefits and disadvantages of the target architecture. A time schedule, i.e. UMTS releases, for the standardization of such an architecture shall be proposed. Work on Mobile IP+ in the IETF should be taken into account.

This report will also contain a study on how to offer Mobile IP+ as an overlay to GPRS. This would allow an end user device, which is connected to the Internet (or intranet etc.) via LAN, to be reconnected during an active session via GPRS/UMTS or visa versa, without the need for any re-configuration or re-start of applications. The outcome of this part shall be part of UMTS release 99. Proposed solutions need to be balanced between the requirement to minimize the impact on the current GPRS standards and the requirements generated by further development of using Mobile IP+ within the CN in an efficient way. The output of this study is a description of the system and a set of CR's for those standards handled by 3GPP-TSG SA-WG2.

2 References

This ETS incorporates, by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies. IETF RFC's are available at http://www.ietf.org/rfc/rfcXXXX.txt and internet drafts at http://www.ietf.org/internet-drafts/YYYY.txt .

ETSI TC-SMG UMTS 22-01: "Services Principles"

ETSI TC-SMG GSM 03.02

ETSI TC-SMG GSM 03.60

ETSI TC-SMG GSM 11.14

ETSI TC-SMG GSM 30.01

ETSI TC-SMG GSM 23.01

ETSI TC-SMG UMTS 23.20 "Evolution of the GSM platform towards UMTS"

[RFC 1518] IETF RFC 1518Y, Rekhter, T. Li "An Architecture for IP Address Allocation with CIDR", Sept. 1993

[RFC 1519] IETF RFC1519V, Fuller et Al. "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", September 1993.

[RFC1701] IETF RFC 1701, S.Hanks et. al., "Generic Routing Encapsulation (GRE)", October 1994.

[RFC1702] IETF RFC 1702, S.Hanks et. al., "Generic Routing Encapsulation over IPv4 networks", October 1994.

[RFC1853] IETF RFC 1853, W. Simpson, " IP in IP Tunneling", October 1995.

[RFC2002] IETF RFC 2002, C.E.Perkins, ed. "IPv4 Mobility Support", October 1996.

[RFC2003] IETF RFC 2003, C..Perkins., "IP Encapsulation within IP", October 1996.

[RFC2004] IETF RFC 2004, C.Perkins, "Minimal Encapsulation within IP", October 1996.

[RFC2005] IETF RFC 2005, J.Solomon, "Applicability Statement for IP Mobility Support", October 1996.

[RFC2006] IETF RFC 2006, Ed. D. Cong, M. Hamlen, "The Definitions of Managed Objects for IP Mobility Support using SMIv2" October. 1996.

[RFC2101] IETF RFC2101, B. Carpenter et. Al. " IPv4 Address Behaviour Today"

[RFC2131] IETF RFC 2131, "Dynamic Host Configuration Protocol", March 1997.

[RFC2215] IETF RFC 2215, S. Shenker, J. Wroclawski, "Network Element Service Specification Template", September 1997.

[RFC2344] IETF RFC 2344, Ed. G. Montenegro, "Reverse Tunneling for Mobile IP", May 1998.

[RFC2356] IETF RFC 2356, G. Montenegro,V. Gupta "Sun's SKIP Firewall Traversal for Mobile IP", June 1998

[RFC2267] IETF RFC 2267, P. Ferguson, D. Senie, " Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", January 1998.

[RFC2475] IETF RFC 2475, S. Blake, Editor, An Architecture for Differentiated Services, December 1998.

[RFC2486] IETF RFC 2486, B.Aboba, M.Beadles, "The Network Access Identifier", January 1999.

Work in progress:

[MIPwg] IETF Mobile IP Working Group, http://www.ietf.org/html.charters/mobileip-charter.html

[rsvp-tunnel] A. Terzis, Editor, RSVP Operation Over IP Tunnels, February 1999.
http://www.ietf.org/internet-drafts/draft-ietf-rsvp-tunnel-02.txt

[diffs-frame] S. Blake, Editor, A Framework for Differentiated Services, October 1998.
http://www.ietf.org/internet-drafts/draft-ietf-diffserv-framework-01.txt

[MIP-optrout] Internet draft, "Route Optimization in Mobile IP", November 1997.
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-08.txt

[MIPIPv6] Internet draft, "Mobility Support in IPv6", November 1998.
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-07.txt

[MIPv2] Internet draft, Perkins, C., "IP Mobility Support version 2", November 1997,
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-v2-00.txt

[MIP-DIAM] Internet draft, Calhoun, P. "DIAMETER Mobile IP Extensions", November 1998
http://www.ietf.org/internet-drafts/draft-calhoun-diameter-mobileip-01.txt

[NAI] Internet draft, P.Calhoun, C.Perkins, "Mobile IP Network Address Identifier Extension", February 1999.
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-mn-nai-01.txt

[NAR] Internet draft, G. Montenegro, May 1998,
draft-montenegro-aatn-nar-00.txt

[TEP] Internet draft P.Calhoun et al., "Tunnel Establishment Protocol" March 1998.
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-calhoun-tep-01.txt

[DIAMETER] Internet draft, P. Calhoun, A. Rubens, " DIAMETER Base Protocol", November 1998
http://www.ietf.org/internet-drafts/draft-calhoun-diameter-07.txt

Firewall Support for Mobile IP
http://www.ietf.org/internet-drafts/draft-montenegro-firewall-sup-03.txt

Registration Keys for Route Optimization
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-regkey-00.txt

Special Tunnels for Mobile IP
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-spectun-00.txt

Tunnel Establishment Protocol
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-calhoun-tep-01.txt

Rapid Authentication for Mobile IP
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ra-00.txt

Use of IPSec in Mobile IP
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipsec-use-00.txt

Support for Mobile IP in Roaming
http://www.ietf.org/internet-drafts/draft-ietf-roamops-mobileip-01.txt

Mobile IP Dynamic Home Address Allocation Extensions
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-home-addr-alloc-00.txt

Mobile IP Regionalized Tunnel Management
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-reg-tunnel-00.txt

Mobile IP Challenge/Response Extensions
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-challenge-01.txt

NAI Resolution for Wireless Networks
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-nai-wn-00.txt

Requirements on Mobile IP from a Cellular Perspective
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-cellular-requirements-00.txt

IP Mobility Architecture Framework
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipm-arch-00.txt

Transparent Hierarchical Mobility Agents (THEMA)
http://www.bell-labs.com/~mccap/draft-mccann-thema-00.txt

3G Wireless Data Provider Architecture Using Mobile IP and AAA
http://www.ietf.org/internet-drafts/draft-hiller-3gwireless-00.txt

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

3.1 Definitions

For the purposes of the present document, the terms and definitions apply.

Agent Advertisement [rfc2002] An advertisement message constructed by attaching a special Extension to a router advertisement [4] message.

Care-of Address [rfc2002] The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a “foreign agent care-of address” is an address of a foreign agent with which the mobile node is registered, and a “co-located care-of address” is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

Correspondent Node [rfc2002] A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

DIAMETER [DIAMETER]The DIAMETER base protocol is intended to provide a framework for any services which require AAA/Policy support.

Foreign Network [rfc2002] Any network other than the mobile node’s Home Network.

Home Address [rfc2002] An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home Network [rfc2002] A network, possibly virtual, having a network prefix matching that of a mobile node’s home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node’s Home Address to the mobile node’s Home Network.

Link [rfc2002] A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address [rfc2002]The address used to identify an endpoint of some communication over a physical link. Typically, the Link-Layer address is an interface's Media Access Control (MAC) address.

Mobile Equipment [UMTS 23.01] performs radio transmission and contains applications. The mobile equipment may be further sub-divided into several entities, e.g. the one which performs the radio transmission and related functions, Mobile Termination**,** MT, and the one which contains the end-to-end application or (e.g. laptop connected to a mobile phone), Terminal Equipment.

Mobile IP (MIP) Mobile IP as defined in RFC 2002.

Mobile IP+ (MIP+)Mobile IP and the ongoing work in IETF on Mobile IP. Where applicable this term should be accompanied by specific references. Mobile IP(+) is used to mean either MIP or MIP+.

Mobile Node The part of the mobile equipment that contains the Mobile IP functionality. The term is used in IETF.

Mobile Station [GSM02.60] Equipment intended to access a set of GSM PLMN telecommunication services. Services may be accessed while the equipment capable of surface movement within the GSM system area is in motion or during halts at unspecified points (source: GSM 01.04). The mobile station may include a mobile termination (MT) and terminal equipment (TE). In UMTS, the term mobile equipment (ME) is used instead.

Mobile Termination [GSM02.60] The part of the mobile station which terminates the radio transmission to and from the network and adapts terminal equipment capabilities to those of the radio transmission (source GSM 01.04).
[UMTS 23.01] The part of the mobile equipment which performs the radio transmission and related functions.**Mobility Agent** [rfc2002] Either a home agent or a foreign agent.

Mobility Binding [rfc2002] The association of a home address with a care-of address, along with the remaining lifetime of that association.

Mobility Security Association [rfc2002] A collection of security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them

Node [rfc2002] A host or a router.

Nonce [rfc2002] A randomly chosen value, different from previous choices, inserted in a message to protect against replays.

Security Parameter Index (SPI) [rfc2002] An index identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association. SPI values 0 through 255 are reserved and MUST NOT be used in any Mobility Security Association.

Terminal Equipment: [gsm02.60] Equipment that provides the functions necessary for the operation of the access protocols by the user (source: GSM 01.04). A functional group on the user side of a user-network interface (source: ITU-T I.112). *The part of the mobile station that is not the mobile termination.*
[UMTS 23.01] The part of the mobile equipment that contains the end-to-end application or (e.g. laptop connected to a mobile phone)

Tunnel [rfc2002] The path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Virtual Network [rfc2002] A network with no physical instantiation beyond a router (with a physical network interface on another network. The router (e.g., a home agent) generally advertises reachability to the virtual network using conventional routing protocols.

Visited Network [rfc2002] A network other than a mobile node's Home Network, to which the mobile node is currently connected. **Visitor List** [rfc2002] The list of mobile nodes, visiting a foreign agent.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
AF	Assured Forwarding
AUC	AUthentication Center (GSM)
BG	Border Gateway (GPRS)
BSS	Base SubSystem (GSM access network)
CAMEL	
CH	Correspondent Host (same as correspondent node)
CIO	
CN	Core Network
COA	Care-Of Address
DS	Differentiated Services
ETR	ETSI Technical Report
ETS	ETSI Technical Specification
FA	Foreign Agent
FACOA	Foreign Agent Care-Of Address
FFS	For Further Study
GFA	Gateway Foreign Agent
GGSN	Gateway GPRS Support Node
HA	Home Agent
HLR	Home Location Register
HO	HandOver
IGSN	Internet GPRS Support Node
IPsec	IP security protocols
IWU	InterWorking Unit
LAC	Location Area Code
LLC	Logical Link Control
ME	Mobile Equipment
MIP	Mobile IP

MT	Mobile Termination
NAI	Network Access Identifier
NAS	Network Access Server
N-PDU	Network layer PDU (used in GPRS to identify PDU transported in the GTP payload)
PHB	Per Hop Behaviour
PLMN	Public Land Mobile Network
P-TMSI	Packet TMSI
RADIUS	Remote Access Dialin User Service
RAN	Radio Access Network
RAC	Routing Area Code
RAI	Routing Area Identifier
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RNTI	Radio Network Temporary Identifier
RSVP	Resource ReserVation Protocol
RNC	Radio Network Controller
SGSN	Service GPRS Support Node
SNDCP	Subnetwork Dependent Control Protocol
SRNS	Serving RNS
TE	Terminal Equipment
TIPHON	
TLLI	Temporary Logical Link Identifier
TMSI	Temporary Mobile Subscriber Identifier
UDP	User Datagram Protocol
UE	User Equipment
URAN	UMTS Radio Access Network
USIM	User Services Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
VLR	Visitor Location Register

4 Working Assumptions

1. Foreign Agent, as defined in RFC 2002, should be located in or at the IGSN/GGSN.
2. Foreign Agent care-of address is the standard case in IPv4. Co-located care-of addresses may be considered too.
3. The registration and authentication processes of UMTS and Mobile IP(+) should be independent to facilitate roaming between access networks based on different technologies.
4. When defining standards for how to deploy MIP(+) as an overlay to GPRS (MIP step 1) the full MIP scenario (MIP steps 2 and 3) should be kept in mind to avoid unnecessary future changes.

5 Requirements on UMTS Packet Domain

These are the requirements we believe the UMTS packet domain should satisfy (only those not obviously implied by SMG1 requirements are listed).

- Efficiently support IP transport and access to the Internet.
- Enable support of Virtual Private Networks.
- Enable support of Remote Network Access .
- Roaming procedures based on IETF ROAMOPS WG and AAA WG outcomes, that is support of NAI (Network Access Identifier) based Roaming procedures and IETF standard AAA procedures. This would allow to share an AAA infrastructure that is going to be built in the Internet for AAA and roaming purposes.
- Enable the support of a diversity of protocols in order to provide users with access to private and public networks based on non IP protocols.
- Provide end to end QoS or service differentiation according to IETF standards for IP packet transport.
- Support of Mobile IP+ with Challenge/Response based authentication and NAI extension in order to interoperate with operators, corporations and ISPs offering Mobile IP+ on the core network side.

6 Current Status of Mobile IP, March 1999

Basic Mobile IP (IPv4) is described in [RFC2002], IP Mobility Support. It describes how to route packets to a mobile node that is not in its home network. The transport of packets to and from the mobile node is obtained with different tunnel mechanisms described in [RFC2003][RFC2004] and [RFC2344]. A few key presumptions in RFC 2002 are that a mobile node has a permanent public IP address, which also is used to identify the terminal and that security associations exist between the home network.

For large scale public operation, features like temporary and/or private addresses, identification of the user instead of the terminal, authentication of the user etc. are necessary. The work on these issues has been heavily intensified in the mobileip (IP Routing for Wireless/Mobile Hosts) WG since the end of 1998 and the current result is described in a set of drafts, of which most are planned to become draft standards before the end of 1999 [MIPwg]. Other IETF working groups that are among the most interesting for the launch of MIP+ are the AAA (Authentication, Authorization and Accounting) and ROAMOPS (Roaming Operations) WG's, http://www.ietf.org/html.charters/aaa-charter.html and http://www.ietf.org/html.charters/roamops-charter.html.

This section will, however, only cover the work in the mobileip WG. Except for [MIPv6], all MIP RFC's and MIP+ drafts concern IPv4. However, it is likely that the mechanisms developed for MIP+v4, to a large extent can be used also for MIPv6. The low version numbers of the drafts is not necessarily a sign of instability as many of the ideas has been taken from other drafts which have now expired. Up-to date information is available on http://www.ietf.org/html.charters/mobileip-charter.html.

The following sections lists the RFC's and important drafts with the abstract of each of them.

6.1 Mobile IP RFC's

As of March 2nd, 1999, the following RFC's exist in the Mobile IP working group within IETF:

RFC 2002 - IP Mobility Support

This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

RFC 2003 - IP Encapsulation within IP

This document specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram. Encapsulation is suggested as a means to alter the normal IP routing for datagrams, by delivering them to an intermediate destination that would otherwise not be selected by the (network part of the) IP Destination Address field in the original IP header. Encapsulation may serve a variety of purposes, such as delivery of a datagram to a mobile node using Mobile IP.

RFC 2004 - Minimal Encapsulation within IP

This document specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, with less overhead than "conventional" IP encapsulation that adds a second IP header to each encapsulated datagram. Encapsulation is suggested as a means to alter the normal IP routing for datagrams, by delivering them to an intermediate destination that would otherwise not be selected by the (network part of the) IP Destination Address field i the original IP header. Encapsulation may be serve a variety of purposes, such as delivery of a datagram to a mobile node using Mobile IP.

RFC 2005 - Applicability Statement for IP Mobility Support

As required by [RFC 1264], this report discusses the applicability of Mobile IP to provide host mobility in the Internet. In particular, this document describes the key features of Mobile IP and shows how the requirements for advancement to Proposed Standard RFC have been satisfied.

RFC 2006 - The Definitions of Managed Objects for IP Mobility Support using SMIv2

This memo defines the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it describes managed objects used for managing the Mobile Node, Foreign Agent and Home Agent of the Mobile IP Protocol.

RFC 2344 - Reverse Tunneling for Mobile IP

Mobile IP uses tunneling from the home agent to the mobile node's care-of address, but rarely in the reverse direction. Usually, a mobile node sends its packets through a router on the foreign network, and assumes that routing is independent of source address. When this assumption is not true, it is convenient to establish a topologically correct reverse tunnel from the care-of address to the home agent.

This document proposes backwards-compatible extensions to Mobile IP in order to support topologically correct reverse tunnels. This document does not attempt to solve the problems posed by firewalls located between the home agent and the mobile node's care-of address.

RFC 2356 - Sun's SKIP Firewall Traversal for Mobile IP

The Mobile IP specification establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. Mobility implies higher security risks than static operation, because the traffic may at times take unforeseen network paths with unknown or unpredictable security characteristics. The Mobile IP specification makes no provisions for securing data traffic. The mechanisms described in this document allow a mobile node out on a public sector of the internet to negotiate access past a SKIP firewall, and construct a secure channel into its home network.

In addition to securing traffic, our mechanisms allow a mobile node to roam into regions that (1) impose ingress filtering, and (2) use a different address space.

6.2 Mobile IP+ Drafts

As of March 2nd, 1999, the following internet drafts exists in the Mobile IP working group within IETF:

IP Mobility Support version 2, v02, November 1997, expired in principle but not in practice

Comment: Same content as RFC 2002 with a few changes of some details.

Mobility Support in IPv6 , v07, November 1998

This document specifies the operation of mobile computers using IPv6. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, Mobile IPv6 defines four new IPv6 destination options, including one that MUST be supported in packets received by any node, whether mobile or stationary.

Comment: this draft has been proposed to become a standard in March 1999.

Mobile IP Regionalized Tunnel Management, v 00, November 1998

Comment: RFC2002 assumes that the Foreign Agent and the Home Agent interact directly during the registration process. This assumption creates two problems; first the Mobility Agents can not exist on a private networks and this does not allow for efficient smooth hand-off of the Mobile Node between Foreign Agents. This draft introduces proxy mobility agents which each have one routable address that is accessible from the public network and one address that resides on the private network. In order to reach either the FA or the HA from the public network, the request must be sent through the appropriate Proxy Agent (PA). There is no limit to the levels of hierarchy. The message flows, necessary extensions to the Router Discovery Protocol and new MIP Registration Extensions are defined.

Mobile IP Challenge/Response Extensions, v 01, February 1999

Mobile IP, as originally specified, defined an authentication extension (the Mobile-Foreign Authentication Extension) by which a mobile node could authenticate itself to a foreign agent. Unfortunately, this extension does not provide ironclad replay protection, and worse yet does not conform to existing techniques (such as CHAP) for authenticating transportable computer devices In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow use of such challenge/response mechanisms for allowing a foreign agent to authenticate the mobile node.

Mobile IP Network Address Identifier Extension, v 00, February 1999

AAA servers, such as RADIUS and DIAMETER, are in use within the Internet today to provide authentication and authorization services for dial-up computers. We propose that such services are equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. Such AAA servers typically identify clients by using the Network Access Identifier (NAI). We propose that the NAI be allowed for use with Mobile IP when the mobile node issues a Registration Request.

Comment: This allows identification of the user and not of the terminal as is the case in RFC 2002. NAI is described in [RFC2486].

Requirements on Mobile IP from a Cellular Perspective, v 00, February 1999

The increasing interest in Mobile IP as a potential macro-mobility solution for cellular networks leads to new solutions and extensions to the existing protocol. There is also a need to put together the demands on Mobile IP, from a cellular perspective, in order to harmonize the evolution of Mobile IP and the existing mobility solutions in cellular networks.

This draft lists a first set of requirements on Mobile IP for use in cellular networks, for instance IMT-2000, and relates the requirements to proposed solutions. These requirements consider Mobile IPv4, but the list will be extended for Mobile IPv6 as well.

Comment: The main purpose of this draft is to ensure that general requirements for cellular networks and special UMTS requirements are brought up.

Transparent Hierarchical Mobility Agents (THEMA), v 00, March 1999

For various reasons it may be desirable to separate the functionality of a mobility agent, such as the home and foreign agents in Mobile IP [Perkins96], from their link-layer presence on a given network. This draft outlines mechanisms based on the Tunnel Establishment Protocol [Calhoun98a] for accomplishing this. The tunnels so established will not be visible to a mobile node and therefore provide a transparent way to build hierarchies of mobility agents, which can lessen the frequency of Mobile IP re-registrations.

NAI Resolution for Wireless Networks, v 00, March 1999

RFC 2486 [1] defines the need of a standardized format for identifying ISP subscribers for dial-up roaming operations. It introduced the Network Access Identifier (NAI) to fulfill this need. The NAI is provided by the mobile node to the dialed ISP during PPP authentication.

The ability to resolve an NAI for second and third generation cellular mobile nodes allow traditional cellular service providers to evolve their home cellular networks to provide cellular services, IP packet data services and so on with a single subscription using NAIs. Additionally, this allows cellular provider to evolve their networks to be IP based.

Second and third generation cellular mobile nodes must perform a registration and authentication process with their wireless service provider before the mobile node user may initiate other operations (See [1] for examples). These mobile nodes do not support the programming of an NAI nor does the cellular registration message support the transfer of an NAI to the wireless access network. For example, North American cellular networks (e.g. AMPS, TDMA, CDMA service mobile nodes that register with a Mobile Identification Number (MIN). The MIN is then associated with a cellular subscriber. For the same reasons stated in [1], it would be convenient if an option was available to provide the wireless subscriber identification in the form of an NAI during the wireless registration and authentication process. This draft proposes a solution to resolve NAIs from traditional mobile node identifiers.

IP Mobility Architecture Framework, v 00, March 1999

Today, the wireless network arena is made up of different types of access (TDMA, CDMA, GSM, etc) and core network technologies (IS-41 and MAP over SS7, etc). The heterogeneous nature of today's wireless and wireline packet data networks limits the scope of mobility between these heterogeneous networks. However, as these heterogeneous networks evolve, the mobility management provided by them must evolve to insure seamless roaming between the networks.

With the convergence of voice and data, networks of the future will be built on IP packet switched technology, mostly due to inherent advantages offered by the technology.

This document identifies several drivers that provide input for an IP Mobility based network and also describes a high level IP Mobility architecture that extends the current third generation IMT2000 wireless architecture and builds on Mobile IP concepts.

Tunnel Establishment Protocol, v 01, March 1998 - expired

A general tunnel establishment protocol (TEP) is defined to handle multi-protocol tunneling as well as multilevel domains guarded by tunnel agents which may be thought of as security gateways, or alternatively as modified foreign agents defined by with Mobile IP. Mobile IP provides the model for TEP; the registration messages in RFC 2002 establish a tunnel between the home agent and the foreign agent.

Comment: this draft introduces surrogate registrations, which provides a way for handling mobile nodes that do not have Mobile IP signaling implemented in them.

3G Wireless Data Provider Architecture Using Mobile IP and AAA, v00, March 1999

This IETF draft specifies a third generation wireless architecture that is consistent with the requirements set by the International Telecommunications Union (ITU) for International Mobile Telecommunications 2000 (IMT-2000) systems. IMT-2000 systems will provide wireless voice, high speed data, and multimedia services. This draft has been developed by the Telecommunications Industry Association (TIA) Standards Subcommittee TR45.6. As a guiding

principle this draft has leveraged the use of RFCs and Internet drafts wherever possible, including Mobile IP and AAA. A network reference model is provided, along with a set of more detailed requirements. Finally a list of supporting RFCs and Internet Drafts is presented.

Route Optimization in Mobile IP, v08, February 1999

This document defines extensions to the base Mobile IP protocol to allow for optimization of datagram routing from a correspondent node to a mobile node. Without Route Optimization, all datagrams destined to a mobile node are routed through that mobile node's home agent, which then tunnels each datagram to the mobile node's current location. The protocol extensions described here provide a means for correspondent nodes to cache the binding of a mobile node and to then tunnel their own datagrams for the mobile node directly to that location, bypassing the route for each datagram through the mobile node's home agent. Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent based on an out-of-date cached binding, to be forwarded directly to the mobile node's new binding.

Other expired drafts are:

Rapid Authentication for Mobile IP

Use of IPSec in Mobile IP

Support for Mobile IP in Roaming

Firewall Support for Mobile IP

Registration Keys for Route Optimization

Special Tunnels for Mobile IP

7 Stepwise introduction of Mobile IP in the CN

The development of a GPRS network towards a mainstream IP network can be performed in three steps, all backwards compatible with networks and terminals that are not handling MIP(+). Briefly, these steps, which are discussed more in detail further down, are:

1. Step 1 represents a minimum configuration for an operator, who wishes to offer the Mobile IP(+) service. The current GPRS structure is kept and handles the mobility within the PLMN, while MIP(+) allows user to roam between other systems, such as LAN's, and UMTS without loosing an ongoing session, e.g. TCP.

2. In a second step, more efficient routing could be obtained after inter SGSN handovers by changing the GGSN/FA, to which the ME is attached, to a more optimal one. By moving the PDP context and the GTP tunnel from the old to the new GGSN while the ME is not transferring data, potential problems with packet loss are avoided. For ME's, which are transferring data during the inter SGSN handover, the streamlining, i.e. change of GGSN/FA, could be performed after the data transfer has been completed.

3. The third step is combine the SGSN and GGSN into one node, the IGSN and to let MIP+ handle inter IGSN handover , i.e. mobility within the PLMN CN and between networks. It is here assumed that MIP+ can handle inter IGSN handover with the same or better performance than inter SGSN handover in UMTS/GPRS. Thus, handover can occur irrespectively of any ongoing data transfer

An operator may implement step 2 or 3 without first implementing the previous one(s).

In Figure 1-3 below, the filter means any kind of traffic filtering to avoid unwanted traffic from the Internet in the IP network. The Border Gateway (BG) denotes the functionality to avoid unwanted traffic between GPRS PLMN's. The BG is outside the scope of GPRS specifications [GSM03.60].

7.1 Step 1 – Offering Mobile IP(+) service

Mobile IP(+) has the benefit of being access system independent, which allows users to roam from one environment to another, between fixed and mobile, between public and private as well as between different public systems. Assuming a

minimal impact on the GPRS standard and on networks whose operators do not wish to support MIP(+), leads to the following requirements:

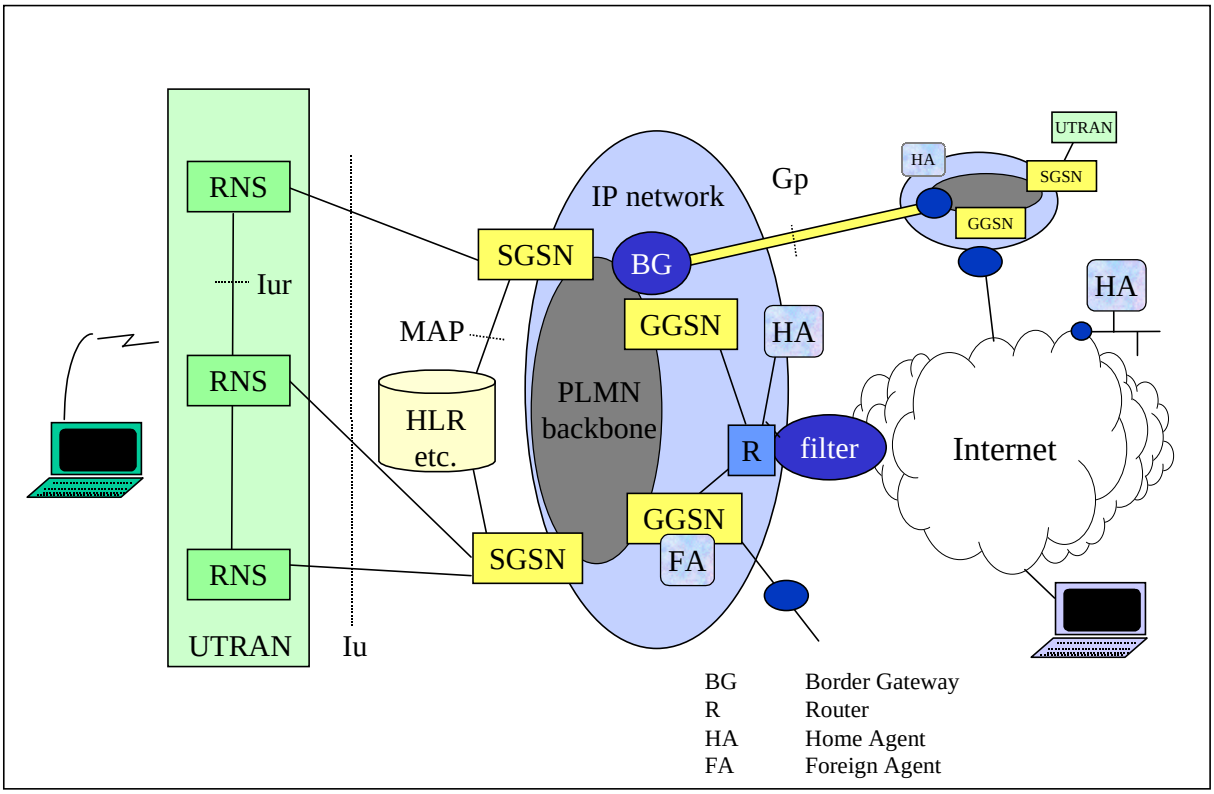

Figure 1. Core network architecture with GPRS MM in and between GPRS PLMN's and Mobile IP MM between different types of systems and optionally between GPRS PLMN's.

- The ME must be able to find a FA, preferably the nearest one. The underlying assumption is that FA's are located at GGSN's and that not all GGSN's may have FA's. One FA in a PLMN is sufficient for offering MIP(+) service, however for capacity and efficiency reasons, more than one may be desired. This means that the ME must request a PDP context to be set up with a GGSN that offers FA functionality. One solution is to define a new PDP type. Another solution is to define an Access Point Name (APN), for example "MOBILEIPv4FA". This APN could be used to connect to the correct GGSN with a FA.

- While setting up the PDP context, the ME must be informed about network parameters of the FA, e.g. care-of address.

- Furthermore, the interaction between the GGSN and the FA needs to be studied more in detail. With the assumption that FA care-of addresses are used, the FA needs to detunnel incoming packets and, together with the GGSN, map the home address of the ME to a PDP context.

Depending on the capabilities of a visited network, two roaming schemes can be identified; GPRS roaming and MIP(+) roaming. With GPRS roaming, we mean roaming via the Gp interface and the use of a GGSN in the home network, which is necessary when the visited network does not offer any FA's. In those cases where the visited network offers a FA, either a GGSN/FA in the visited or in the home UMTS/GPRS network can be utilized. It is assumed that the ME stays with the same GGSN/FA as long as the PDP context is activated. A typical network is shown in Figure 1.

7.2 Step 2 – Intermediate GPRS-MIP(+) system

In step 2, the routing is improved by performing a Mobile IP based streamlining after an inter SGSN handover. A very mobile ME might perform several inter SGSN HO's during a long session which may cause inefficient routing. If the GGSN/FA that is closest to the new SGSN is different from the closest one to the old SGSN, the routing could be improved by changing the GGSN/FA for the mobile during a UMTS/GPRS session. The possibility of optimizing the route is especially desirable in those cases where there are several GGSN/FA's in the PLMN and/or the GGSN/FA's and the SGSN's are co-located.

If the ME is not transferring data, while moving from one SGSN to another, a new PDP context could be setup between the new SGSN and its associated GGSN/FA at the handover. The ME will get a new care-of address with the same procedure as is defined in step 1 for giving the ME a care-of address. If the ME is transferring data, e.g. being involved in a TCP session, the ME would move from the old SGSN to the new one while keeping the PDP Context in the old GGSN as long as it is transferring data. Once the data transfer is terminated, the PDP Context can be changed to the GGSN/FA associated with the new SGSN and a new care-of address can be obtained. Buffers, which already exist in the SGSN's for preventing data loss at inter SGSN HO's, will, with this procedure, be reused as they are. This procedure also has some advantage regarding the handling of firewalls, which are assumed to be attached to the GGSN's. Today, there is no standard for changing firewall e.g during. a TCP session.

As in the previous step, the GPRS interfaces (Gn and Gp) need to be deployed for roaming customers, since there might be networks which not yet support MIP(+). Roaming between PLMN's can be handled either with MIP(+) or with GPRS.

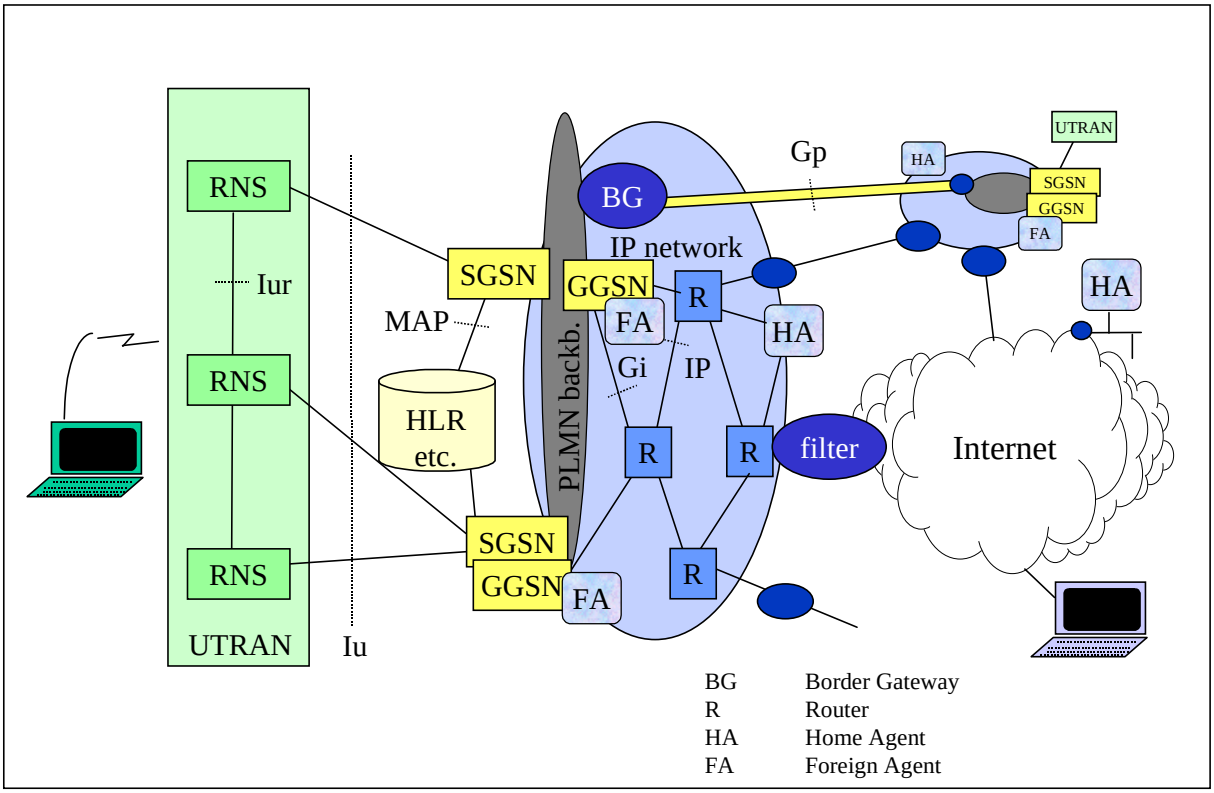

Figure 2. Core network architecture where GPRS MM handles active mobiles and Mobile IP(+) streamlining at inter SGSN handover. The SGSN and GGSN are here co-located.

7.3 Step 3 – Using Mobile IP+ for Intra System Mobility

The third step is to let MIP+ handle intra CN mobility, inter PLMN mobility as well as inter system mobility in the packet domain. The functionality of the SGSN and the GGSN are combined into one node, the Internet GPRS Support Node (IGSN), and functionality is added to utilize Mobile IP for handling inter IGSN mobility. The IGSN/FA will be the node that marks the end of the UMTS specific part of the PLMN.. Figure 3 depicts a logical view of the CN architecture. To allow compatibility with UMTS/GPRS networks which are being upgraded at a slower paste, an option to let the IGSN also act as an SGSN will be necessary during a transition period.

The basic functionality of the IGSN is:

- support of UMTS/GPRS mobility management across the UTRAN/BSS, i.e. what the SGSN does today.
- support of MAP (Mobile Application Part) to communicate with UMTS/GPRS specific nodes, such as HLR, EIR, SMS-C and the functionality needed to handle the information to and from these nodes, such as SIM based authentication and handling of keys for encryption over the radio interface.

- interaction with the HLR, the AAA infrastructure or, most likely, with a combination of the two, for subscriber data handling purposes.
- charging data collection and formatting according to UMTS/GSM specifications, IETF specifications or a combination of the two.
- support of Mobile IP with the necessary functionality to be compliant with Mobile IP deployment in non-UMTS networks around the world. For IPv4, this means to provide FA functionality with commonly deployed extensions (e.g. NAI, challenge response) and functionality to utilize RADIUS, DIAMETER or another AAA infrastructure according to the IETF specifications at hand when a given UMTS specification is finalized.
- support of inter IGSN handovers. In the user plane, the handovers should only be handled by Mobile IP. In the control plane, the PDP context(s) for a ME might need to be transferred from the old to the new IGSN by GTP.

In this scenario, the HA will act as the anchor point for the traffic generated by the ME if reverse tunneling is used, else this traffic will be routed directly to the correspondent node. If Mobile IP route optimization mechanisms will be available and deployed, by their optional use the anchor point will exist mostly for control purposes, whereas the traffic will normally be routed along paths avoiding triangular routing problems. ME's without Mobile IP functionality could be handled by letting the IGSN register the mobile with a HA in a PLMN. Alternatively, SGSN's and GGSN's could be deployed in parallel with the Mobile IP nodes and/or the IGSN could optionally also act as an SGSN.

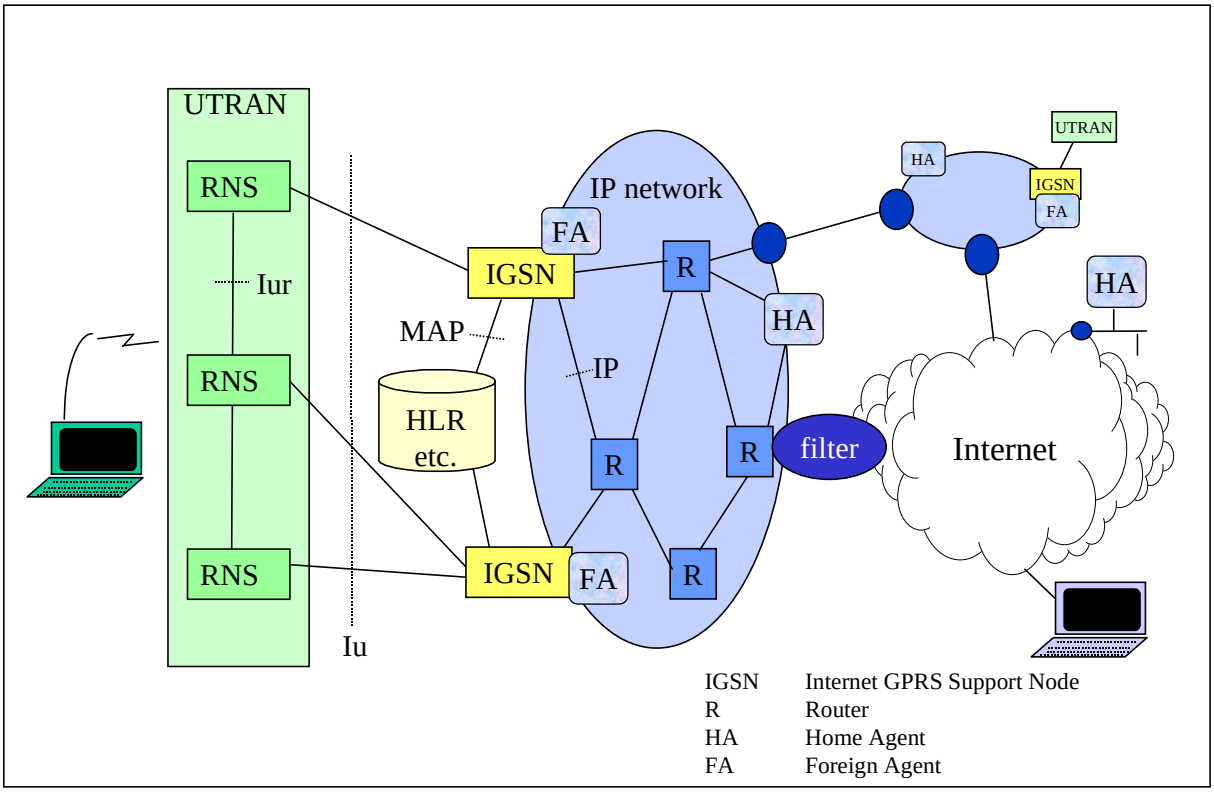

Figure 3. Core network architecture with Mobile IP+ MM within the CN and between different types of systems and between GPRS PLMN's.

8 General Considerations and Explanations

This chapter contains a collection of information, which is valid for all three steps described in this report.

8.1 Saving Radio Resources and IPv4 Addresses with FA Care-of Addresses

Nodes using Mobile IP(+)v4 have two ways of getting a care-of address, which is the temporary address in the visited network to which the home network (HA) forwards incoming packets.

1. A *Foreign Agent care-of address* is shared between several visiting mobile nodes. Packets to the mobile node that arrive in the home network are intercepted by the HA and tunneled to the FA. The FA detunnels the packets and forward them to the mobile node.

2. When using a *co-located care-of address*, the mobile node gets a unique care-of address and the tunnel from the HA is terminated in the mobile node. In this case, it is not required to have a FA in the visited network.

From this the following can be concluded:

1. A UMTS/GPRS ME can use a temporary GPRS IP address, given by the GGSN, as a co-located care-of address and run Mobile IP(+), without any support of the visited network.

2. Co-located care-of addresses require two IP addresses per visited mobile node, one home address and one care-of address. FA care-of addresses can handle many mobile nodes. Thus, FA care-of addresses does not require the visited network to have a large address space on hand. Co-located care-of addresses also facilitate the dimensioning of the available addresses.

3. In case of Foreign Agent care-of address, the tunnel is terminated at the Foreign Agent. When using co-located care-of addresses, the tunnel is terminated in the mobile node, i.e. the tunnel is transported over the radio interface. This means that, in a radio resource perspective, Foreign Agent care-of addresses are more efficient.

As IPv4 addresses and radio resources are scarce, Foreign Agent care-of addresses are preferred for UMTS/GPRS.

8.2 Permanent and Temporary Home Addresses

According to [RFC2002], which defines the basic Mobile IP protocol, each mobile node, i.e. ME, has a permanent IP address belonging to its home network. This is, however, not in line with the use of temporary addresses which are given to nodes, fixed and mobile, while they are connected to the Internet. Therefore, proposals have been made on how to let the mobile node's home network provide a temporary home address. An extension will be added to the MIP Registration Reply message [MIP-NAI]. Those mobiles, which move from another access form into the UMTS/GPRS coverage will already have a temporary home address assigned. As the TE, in that case, is already configured with this home address, it makes no difference to the registration request message whether it is a permanently or temporarily assigned home address.

9 First Step: MIP(+) in overlay to GPRS

9.1 General Design Criteria

The main design criteria are that

- radio resources and IPv4 address should be used with care

- the impact on the current GPRS signaling messages as well as on the MT and (3G)SGSN functionality should be minimized to ensure that this step can be implemented for R99.

The first criterion led to the choice of using Foreign Agent care-of addresses (see section 2.1.1). The second one to the choice of using the APN (Access Point Name) to find the desired GGSN instead of introducing a new PDP type (see section 3.3) and to the choice of transporting all Mobile IP(+) messages in the UMTS/GPRS user plane.

9.2 Assumptions

9.2.1 Signaling

Since the UMTS packet domain is going to be based on the GPRS platform, the description below assumes that GPRS procedures such as “Activate PDP Context Request “ and “Create PDP Context Request” will be reused for UMTS. If, instead, new procedures will be defined for UMTS, the requirements for providing Mobile IP(+) to end users should be taken into account from the beginning.

9.2.2 Terminal Model

The ME (Mobile Equipment) is assumed to consist of the TE (Terminal Equipment), e.g. a laptop, connected to a MT (Mobile Termination), which contains the UMTS/GPRS specific functionality. (Nothing prevents a manufacturer to implement these two devices in one.) The IP stack with Mobile IP(+) is assumed to be located in the TE, which also is the node with the IP address. The signaling to setup and maintain the connection (usually PPP) between the MT and TE is not included in this contribution. In IETF, the term “mobile node” is used instead of TE, i.e. for the node or device that contains the (Mobile) IP stack. Further it assumes that the ME requests PDP type “IP”, however it is likely that PDP type “PPP” also could be used.

9.2.3 GGSN/FA

The GGSN/FA is a GGSN enhanced with FA (Foreign Agent) functionality. The FA functionality is specified by IETF, however, as a UMTS/GPRS release is finalized, the specific IETF standards that should be taken into account may be specified by 3GPP/ETSI for easier interoperability between operators. The interface between the GGSN and FA, including the mapping between the IP address and the local address i.e. the TID (GPRS Tunnel ID), is assumed not be standardized as the GGSN/FA is considered being one integrated node.

9.2.4 Home Network

The home network is the network where the mobile node has its “Mobile IP(+) subscription”. It may be a PLMN, but also a corporate network, an ISP etc. The Home Agent (HA) [RFC2002] that the mobile node uses is located in the home network. There will probably also be an AAA (Authentication, Authorization and Accounting) infrastructure in the home network. However, the use of AAA functionality will not require any changes to GPRS specific standards, as it is external to the UMTS/GPRS networks. It is specified by the IETF.

9.3 Using the APN to Find a GGSN/FA

The SGSN will base the choice of GGSN on the APN (Access Point Name) that is given by the ME. The APN consists of two parts: the Network ID and the Operator ID. The Network ID[2] (e.g. “gateway1.volvo.se”) identifies the external Network to which the user wants to connect. The Operator ID[3] (“operator.country.gprs”) identifies the operator in which network the gateway is located. The user needs only to specify the Network Id, the Operator Id can be added by the SGSN. An APN, which specifies a particular GGSN, is a combination of the two ID’s, e.g. “gateway1.volvo.se.operator.country.gprs”.

If no APN is given and PDP type is “IP”, the SGSN chooses a suitable GGSN according to operator’s configuration of the SGSN. Similarly, a Network ID of the format vvv (one label, no dots) can be used to specify any GGSN with a specific service (vvv), e.g. Internet access, gateway for voice over IP, Mobile IP(+) FA. If the SGSN is not configured to identify the requested service it may try with a DNS interrogation for vvv.current-operator.current-country.gprs or, if that is not successful, with vvv.home-operator.home-country.gprs, where the home parameters are taken from the subscription data.

The format of the APN is specified in [GSM03.03]. Using the Network ID to mean a service is not supported today. However, to extend the SGSN’s ability to choose a suitable GGSN depending on the desired service based on the APN

---

[2] The Network Id is typically an Internet Domain Name with the format “xxx.yyy.zzz”, e.g. “gateway1.volvo.se”.

[3] The actual form is MNCzzzz.MCCwwww.GPRS where zzzz are hex coded digits for Mobile Network Code and wwww are hex coded digits for Mobile Country Code.

would increase the flexibility for many operators. Preferably this should be done by using the Network ID as described above.[4] The alternative is to define a new PDP type for each service.

9.4 Detailed Description of Mobile IP(+) Registration in a UMTS/GPRS PLMN

To allow a UMTS or GPRS end user to utilize a Mobile IP(+)v4 service in an efficient way, i.e. with Foreign Agent care-of addresses, the ME needs to be connected with a GGSN, which can provide Mobile IP(+) FA functionality. See section 2.1.1 for a discussion on alternative, but less efficient methods of providing MIP service.

This section describes the complete procedure of PDP Context Activation followed by Mobile IP(+) registration. Note that the Mobile IP(+) service may be offered by a different operator than the home UMTS/GPRS operator.

The signaling scheme in Figure 4 shows how the ME can be connected to a GGSN with FA functionality and to register with its Mobile IP(+) HA with a minimum of enhancements to the existing GPRS attach and PDP context activation messages. Assuming that the ME stays with the same GGSN for the duration of the UMTS/GPRS session, there is no need for procedures, such as GPRS detach or SGSN relocation, to be enhanced for step 1.

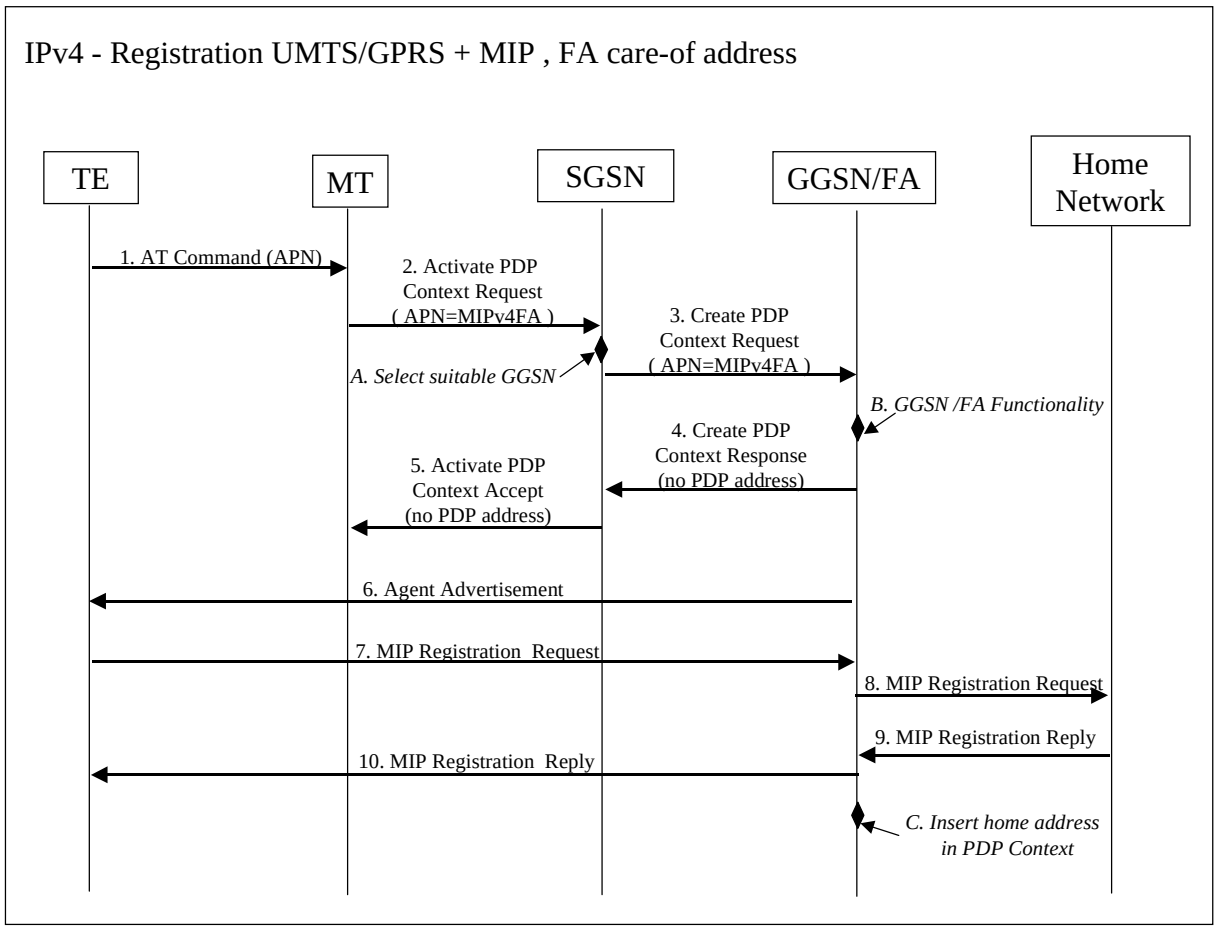

Figure 4, PDP Context activation with Mobile IP(+) registration (the PPP setup and UMTS/GPRS attach procedure not included)

The following messages and functionality have been found to be needed. The setup of the PPP connection and the UMTS/GPRS attach procedure have been omitted for clarity. The arrows denote messages between nodes and the diamonds functionality in a node. These are included for guidance of Figure 4.

1. → AT Command

2. → Activate PDP Context Request

[4] There is a strong interest among members of the GSM Association to include this in the standard.

A. ◆ Select Suitable GGSN

3. → Create PDP Context Request

B. ◆ GGSN/FA Functionality

4. ← Create PDP Context Response

5. ← Activate PDP Context Accept

6. ← (Foreign) Agent Advertisement

7-8. → Mobile IP(+) Registration Request

9-10. ← Mobile IP(+) Registration Reply

C. ◆ Insert PDP address in the GGSN/FA. If the PDP address is needed in the SGSN and the ME PDP Context: Insert home address in PDP Context and trigger an update of the PDP address in the SGSN and MT.

{*Editor's comment: Due to charging and legal interception issues, the SGSN needs to know the PDP address. Hence, the GGSN needs to be able to signal the PDP address to the SGSN after "C" has occurred. How to do this is discussed in S2 as it is related also to other issues than MIP. Once it has been decided how to do this,, the signaling message(s) should be incorporated here.}*

9.4.1 AT Command

Description

The AT command carries parameters that the MT needs to request the PDP Context Activation. The important parameter here, is the APN, as that specifies the GGSN or type of GGSN. The AT command is followed by a setup of the PPP connection between the MT and the TE.

Current Specifications

Several AT commands can carry the APN, e.g. "Define PDP Context", [GSM07.60].

Enhancements

None

9.4.2 Activate PDP Context Request

Description

The MT sends the "Activate PDP Context Request" to the SGSN. The message includes various parameters of which the "APN" and the "Requested PDP Address" are of interest here. The APN, which is discussed in detail in the section 3.3, points at a requested GGSN. The "Requested PDP Address" should be omitted for all ME's using Mobile IP(+). This is done irrespective of if the MT has a permanently assigned Mobile IP(+) address from its Mobile IP(+) home network, a previously assigned dynamic home address from its Mobile IP+ home network or if it wishes the Mobile IP+ home network to allocate a "new" dynamic home address. The reason for this is 1) to treat all Mobile IP(+) registrations in the same way and 2) that the PDP address would have to be entered in the HLR (see below) which makes the situation for the end user inflexible.

Current Specifications

The parameters "APN" and the requested PDP Address are parameters, currently in the standard [GSM04.08]. The PDP Address is allowed be omitted (set to 0.0.0.0).

A permanently assigned PDP address may be included. However, that PDP address must be a UMTS/GPRS IP address, as it is cross-checked in the HLR and mapped to a specific GGSN. If the MT inserts the stationary Mobile IP(+) address, which is related to the mobile node's home network, access is denied by the SGSN.

Enhancements

None.

9.4.3 Select Suitable GGSN

Description

The SGSN will base the choice of GGSN on the APN that is given by the ME. This is described in section 2.1.1. To find the closest GGSN/FA, the Network ID should be used to mean a specific service, in this case MIPv4FA.

Current Specifications

The format of the APN is specified in [GSM03.03]. Using the Network ID to mean a service, is not supported today.

Enhancements

Allow the APN to mean a GGSN with a specific service, not only a physical node. To support this, the operator must have the possibility to configure the SGSN with the choice of GGSN depending on service. A default mechanism is also needed to use a GGSN in the ME's home network if the visited SGSN does not support the requested service. Finally, an agreement between operators is needed on the possible APN's.

9.4.4 Create PDP Context Request

Description

The SGSN requests the selected GGSN to set up a PDP Context for the ME. The PDP address field is the same as in the "Activate PDP Context Request" message, i.e. 0.0.0.0.

Current Specifications

If the ME requests a dynamic PDP address and a dynamic PDP address is allowed, then the PDP address filed in the "End User Address" information element shall be empty. If the ME requests a static PDP address then the PDP address field in the "End User Address" information element shall contain the static PDP address.

Enhancements

In combination with a request for a GGSN with FA functionality, an empty PDP address field in the End User Address information element, means that the GGSN/FA will extract the PDP address, i.e. the mobile node's home address when the Mobile IP Registration Request or, in case of a new temporary home address, Mobile IP(+) Registration Reply messages passes through.

9.4.5 GGSN/FA Functionality

Description

To announce its presence and its parameters, the FA may broadcast Agent Advertisement messages regularly. To avoid unnecessary traffic over the radio interface, the mobile node can request the information when needed by sending an Agent Solicitation Message. However, as the GGSN/FA is aware of that a new ME has entered the network, it could send dedicated Agent Advertisement message directly to the new ME. This would save an Agent Solicitation message over the radio and speed up the registration procedure somewhat.

The Agent Advertisement message should be sent in the user plane to avoid defining new messages in GPRS/UMTS. As the new ME, not yet has an IP address, a limited broadcast address (255.255.255.2555) needs to be used as the destination address in the IP header.

Current Specifications

The functionality of the GGSN is specified in GPRS standards. The FA functionality is/will be specified in IETF standards (RFC's). The mapping between these two is a matter of implementation. The local link address mentioned in the IETF standards corresponds to the TID of GPRS.

Enhancements

The functionality of the GGSN needs to be enhanced with FA functionality, according to IETF specifications. The GGSN/FA needs to send an Agent Advertisement message after sending the Create PDP Context Response. The GGSN should not give the ME a temporary UMTS/GPRS IP (i.e. PDP) address if the Mobile IP(+) FA service has been requested.

9.4.6 Create PDP Context Response

Description

A Create PDP Context Response is sent from the GGSN/FA to the SGSN. If the creation of PDP Context was successful, some parameters will be returned to the SGSN, if not, error code will be returned. For Mobile IP(+) users, the PDP address should be omitted.

Current Specifications

This message is sent by the GGSN/FA to the SGSN. If the ME requests a dynamic PDP address and a dynamic PDP address is allowed, then the End User Information Field information element shall be included. The PDP Address field in the End User Information Field information element shall contain the dynamic PDP Address allocated by the GGSN. Nothing is stated about the case when the ME does not request a dynamic PDP address and has not requested a permanent IP address to be used.

Enhancements

None.

9.4.7 Activate PDP Context Accept

Description

This message is sent by the SGSN to the ME and contains similar information as the Create PDP Context Response message. The PDP address should be omitted.

Current Specifications

Normally, the PDP address is included in this message, however it is not compulsory.

Enhancements

None.

9.4.8 Foreign Agent Advertisement

Description

The Agent Advertisement [RFC2002] is an ICMP (Internet Control Message Protocol) Router Advertisement message with a mobility agent advertisement extension. The latter part contains parameters of the FA that the mobile node needs, among those are one or more care-of addresses that the FA offers. This message should be sent, in the UMTS/GPRS user plane, as an IP local broadcast message, i.e. destination address 255.255.255.255, however only on the TID for the specific ME to avoid broadcast over the radio interface. See also discussion above about GGSN/FA Functionality.

Current Specifications

The Agent Advertisement message is specified in [RFC2002]. Today, the GGSN does not communicate with the ME on the user plane.

Enhancements

The Mobile IP(+) messages that are exchanged between the GGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

9.4.9 Mobile IP(+) Registration Request

Description

The Mobile IP(+) Registration Request is sent from the mobile node to the GGSN/FA across the GPRS/UMTS backbone as user traffic. The GGSN/FA forwards the Request to the Home Network.

The format of the MIP Registration Request is specified in [RFC2002]. There, it is assumed that the mobile node includes its (permanent) home address, which identifies the node. Also the address of the HA is included in the message and the FA forwards the message to the HA. The Mobile-Node-NAI Extension [MIP-NAI] has been proposed in order to handle temporary assignment of home addresses. In that case, the mobile node does not include a home address in the main part of the MIP Registration Request, but instead a Network Access Identifier (NAI) in a Mobile-Node-NAI Extension. The NAI [RFC2486] has the format similar to an email address and uniquely identifies the user and the user's home network. As long as the mobile node does not know its IP address it can use 0.0.0.0, which means "this host on this network", as the source address.
The mobile node sends the request to the FA, which forwards it to the home network of the mobile node, where a Home Agent (HA) processes it.

To map the reply from the home network with the correct ME, the GGSN/FA needs to store the home address of the mobile node or the NAI and the local link address of the ME, i.e. the TID (GPRS Tunnel ID). The GGSN/FA must have an IP address to which the mobile node can send the registration request, however this does not need to be known outside of the PLMN.

Current Specifications

As the Mobile IP(+) messages between the GGSN/FA and the mobile node is sent over the user plane, the GPRS standards are independent of the format of the messages and of future changes to the Mobile IP Registration Request, e.g. extensions to coop with new Mobile IP+ related functionality.

Enhancements

The Mobile IP(+) messages that are exchanged between the GGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

The [MIP-NAI] is planned to become an RFC during the first half of 1999 and interoperability tests are planned for July 1999.

9.4.10 Mobile IP(+) Registration Reply

Description

When the NAI extension is used by the mobile node in the Registration Request, the Registration Reply from the Home Agent must include the Mobile-Node-NAI extension. The Registration Reply must also include a nonzero HA address and the mobile node's home address.

The Registration Reply will be sent from the home network to the FA, which extracts the information it needs (e.g. the home address of the mobile node allocated by the home network) and forwards the message to the mobile node in the UMTS/GPRS user plane. The FA/GGSN knows the TID and the NAI or home address, so it can pass it on to the correct ME. When a home address has been allocated by the home network, the TE does not yet know its IP address. Hence, in analogy with the FA Advertisement, a local broadcast address has to be used as destination address. As the packet is only sent on the TID associated with a specific ME, no broadcast will be sent over the radio interface.

Current Specifications

The functionality of the FA is specified in [RFC2002]. The use of NAI is currently being specified [MIP-NAI] and is stable. The link-address of the mobile node which is used in the IETF specifications corresponds to the TID in GPRS. As there is a point-to-point link between the ME/mobile node and the GGSN/FA, there is no problems for the mobile node to address the FA.

Enhancements

The Mobile IP(+) messages that are exchanged between the GGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

9.4.11 Insert PDP Address in GGSN PDP Context

Description

The PDP address corresponds to the home address of the ME since no address is given by the UMTS/GPRS PLMN.

As the GGSN/FA processes the Mobile IP(+) Registration Request and Mobile IP(+) Registration Reply messages, it extracts the Mobile IP(+) home address of the ME. The GGSN/FA needs to insert it in its PDP Context.

Current Specifications

According to [RFC2002], the FA is requested to be able to map the home address to the local link address, which corresponds to the TID in the case of UMTS/GPRS. The SGSN and MT do not need to know the PDP address. There are no requirements in GPRS specifications, that the MT and the SGSN have to be aware of the PDP address.

Enhancements

The GGSN/FA must extract the home address from Mobile IP(+) messages and insert in the GGSN PDP Context.

9.5 The UMTS/GPRS Detach Procedure

There are two reasons for the mobile node to leave the UMTS/GPRS network. Either it is turned off or it is moving to a different FA/access network. In both cases, this is initiated and executed by the TE. Thereafter, the MT can perform a standard ME-Initiated Detach from the UMTS/GPRS PLMN.

9.6 Summary of Alterations of and Additions to Current GPRS Standards for Step 1

To support Mobile IP(+) as described above, the following alterations and additions to the GPRS specifications are necessary:

1. The functionality of the GGSN needs to be enhanced with FA functionality, according to IETF specifications. For interoperability, a set of RFC's should be recommended. There is no need to standardize an interface between the GGSN and the FA, as it is considered being one integrated node.

2. The GGSN/FA node should send a FA Advertisement message after sending the Create PDP Context Response.

3. The GGSN should not give the ME a temporary UMTS/GPRS IP (PDP) address if the Mobile IP(+) FA service has been requested.

4. The GGSN/FA and the ME shall exchange Mobile IP(+) signaling messages in the UMTS/GPRS user plane.

5. Allow the APN to mean a GGSN with a specific service, not only a physical node. To support this, the operator must have the possibility to configure the SGSN or DNS with the choice of GGSN depending on service. A default mechanisms is also needed to use a GGSN in the ME's home network if the visited SGSN does not support the requested service. Finally, an agreement between operators is needed on the possible APN's.

Note that none of the points above require any change to the current GPRS protocols.

10 Second Step: Intermediate UMTS/GPRS-MIP(+) System

10.1 The GGSN/FA Change

In the Figure 5, an example of a GGSN change is described. The GGSN change is controlled by the SGSN. The GGSN change would naturally be done after SGSN handover, but it could also be used for load balancing between two GGSN/FAs.

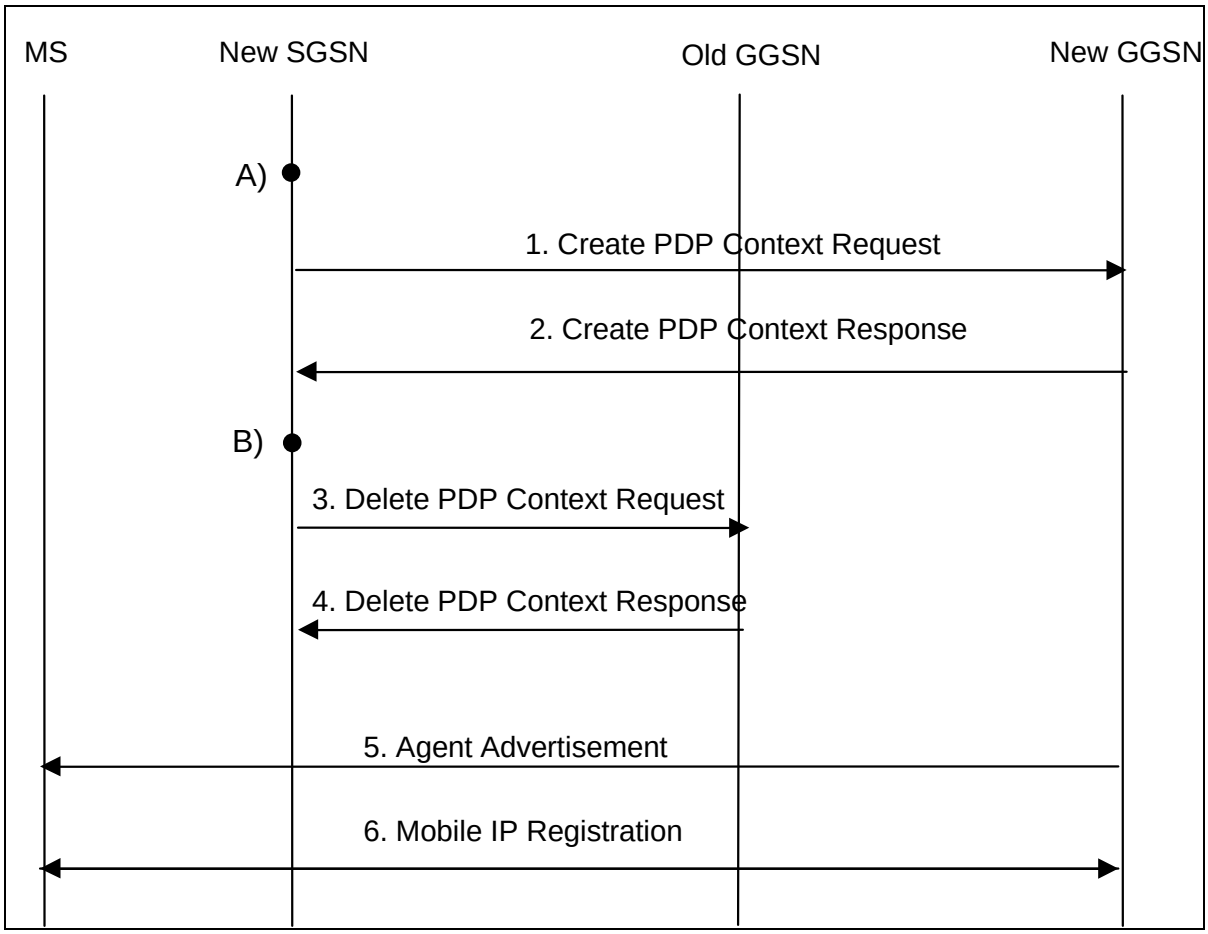

Figure 5 The GGSN/FA handover

The scheme works as following:

A) After a SGSN handover, a Step 2 SGSN has the possibility to change the GGSN/FA. The decision is based on the SGSN's knowledge of the GGSNs that it has. How the SGSN knows about the GGSNs that have a Foreign Agent is not relevant here. If the decision is negative, the PDP Context is kept as normal and the old GGSN is kept. Hence, the Step 2 SGSN functions as a Step 1 SGSN. On the other hand, if the handover is decided to be performed, the GGSN handover is proceeded as following.

1. The new SGSN sends a Create PDP Context Request to the new GGSN with the information that the PDP Context is a Mobile IP PDP Context. The information of the type of the context is put in the APN field as described for Step 1.

2 The new GGSN answers with a Create PDP Context Response and creates the connection between the Foreign Agent and the new PDP Context.

B) After successful creation of the new PDP Context, a timer can be set. The timer counts time until the old PDP Context is deleted. This allows the datagrams that arrive at the old GGSN/FA to be forwarded to the UE.

3. The new SGSN sends a Delete PDP Context Request to the old GGSN.

4. The old GGSN deletes the PDP Context and responses to the request with a Delete PDP Context Response.

5. The Foreign Agent sends the UE an Agent Advertisement as defined in [RFC2002].

6. Agent registration is performed as defined in [RFC2002].

The function of the timer B) is to allow the datagrams to flow to the UE from the old GGSN/FA for a set period of time. The timer can also be set to zero to mark the absence of a timer. Hence, the PDP Context to the old GGSN is deleted immediately after the new PDP Context is created.

10.2 GGSN/FA denial of service

When the GGSN/FA change is performed, the MN registers for the first time to the FA, or a periodical Mobile IP registration is done, the SGSN has no knowledge of the status of the Mobile IP registration. Hence, it is GGSN/FA is the node to react to the registration failure. A registration failure might occur for instance because the new FA does not support a service require by the MN, or because of HA refusal. In case of the FA refusal, the optimisation of the connection by the GGSN/FA change would fail. Thus, a fallback on the old GGSN/FA might be wished. In any case, the PDP Context to the GGSN/FA that refused the registration would be useless. After the registration failure, the FA has the knowledge of the severity of the failure and can take action based on that knowledge.

If the FA decides that the failure is not severe, but the MN can try a new registration, the FA can decide to wait. On the other hand, if the failure is severe the GGSN/FA can delete the PDP Context.

The deletion of the PDP Context is depicted in the Figure 6.

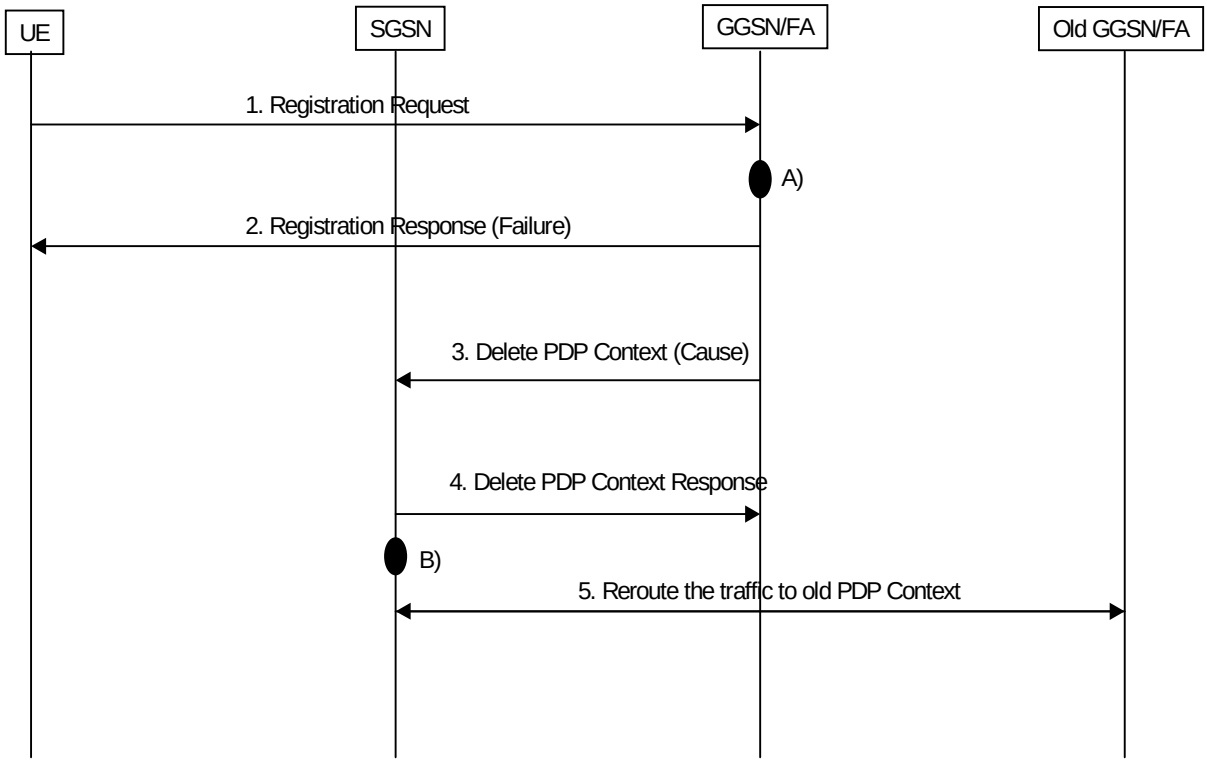

Figure 6 Mobile IP registration failure

It is assumed that the PDP Context activation procedure is done in beforehand.

1. The UE sends an Registration Request to the Foreign Agent

A) The Agent Registration procedure fails and the GGSN determinates that the failure is fatal enough to delete the PDP Context and not to let the MN to try to register again.

2. The Register Response with the failure indication is sent to the UE by the GGSN/FA

3. Delete PDP Context Request is sent by the GGSN/FA to the SGSN with a cause value.

4. The SGSN confirms the deletion by sending a Delete PDP Context Response

B) The SGSN determinates the possibility of re-registration from the cause value given. If the SGSN detects that a fallback is possible, and the PDP Context to the previous GGSN/FA is still open, the PDP Context is reused and the deletion timer is stopped.

1. The traffic is re-routed to the old PDP Context

In the example above, a fallback to the old PDP Context is performed. This situation could occur when the new FA refuses some service that the old FA could provide. Hence, the fallback is possible. In Figure 7, the case where no fallback is possible is described.

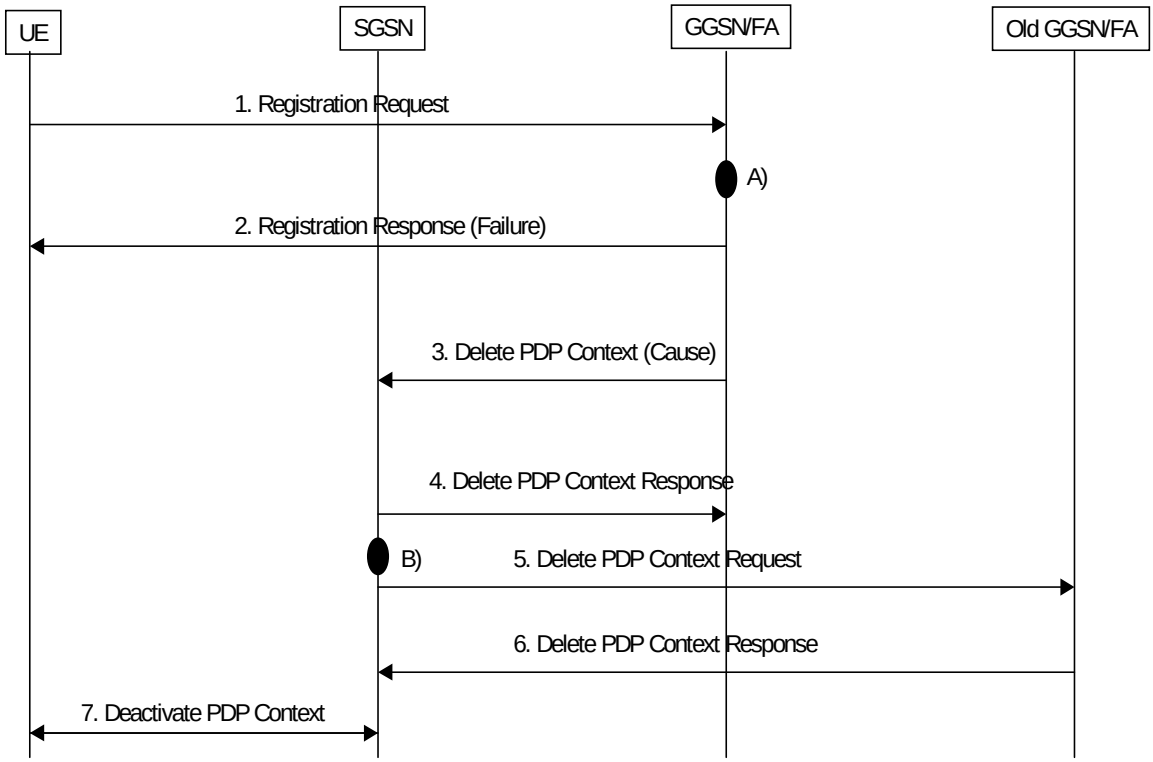

Figure 7 Case when no fall-back is possible

The Signalling goes as following.

1. The UE sends an Registration Request to the Foreign Agent

A) The Agent Registration procedure fails and the GGSN determinates that the failure is fatal.

2. The Register Response with the failure indication is sent to the UE by the GGSN/FA

3. Delete PDP Context Request is sent by the GGSN/FA to the SGSN

4. The SGSN confirms the deletion by sending a Delete PDP Context Response

B) The SGSN determinates the fatality of the failure from the cause value. Since the error is severe enough e.g. HA refusal, the PDP Context is deactivated to the UE. If SGSN has still a PDP Context open to the old GGSN/FA that is deleted.

5. SGSN sends a Delete PDP Context Request to the old GGSN.

6. The old GGSN answers with a Delete PDP Context Response.

7. The PDP Context to the UE is deactivated.

The current specification:

The GTP specification does not have a cause value on the Delete PDP Context Request message. It does have a field called Private Extension defined in the 09.60 (V. X.X.X) in the section 7.9.25.

Extension to the current specification:

The Private Extension field should be defined to carry the cause value.

11 Third Step: Target Architecture

11.1 Network Issues IPv4

[Editor's note: This section will probably be moved to the tutorial appendix and a summary of it should be placed here.]

11.1.1 Basic Principles

IP mobility support, or Mobile IP, as it is more commonly known, allows a mobile node to maintain connectivity to the Internet or to a corporate network using a single and unchanging address (its home address) even when the link layer point of attachment is changing.

When the mobile node moves from the home network to a foreign network it registers with its Home Agent (HA) an IP address that the HA can use to tunnel packets to the mobile node (the Care Of Address (COA)). The HA intercepts packets addressed to the mobile node's home address and tunnels these packets to the COA. No interaction with UMTS location registers is required.

The COA can be a dedicated address each mobile node gets in the visited network (colocated-COA). In this case the mobile node is the tunnel endpoint. Otherwise, the COA is an address advertised (or retrieved in some other way) by a Foreign Agent (FA). In this case it is a FA-COA and the FA is the tunnel endpoint. The FA extracts packets from the tunnel and forwards them to the correct RAN logical link in order to deliver them to the appropriate mobile node. Hence at the FA some interaction with link layer mechanisms/functionality of the access network is in order. This will typically map to the interaction with the UTRAN via the I_u interface.

11.1.2 Mobile IP(+) Manages Macro Mobility Only

Mobility events which do not result in the mobile node entering the domain of a mobility agent different from the current mobility agent domain are transparent to Mobile IP(+). Therefore, only macro mobility events require Mobile IP(+) level handling. A design assumption of Mobile IP is that such macro mobility events do not happen more than once per second and per user. The UTRAN must be designed so that Mobile IP(+) is not affected by mobility events more frequently than that.

11.1.3 Location of the HA and the FA

The FA that a user is currently connected to is necessarily within the UMTS operator's network. However, the HA may be in a different network. The following are examples of HA placements:

If access to a corporate network is provided to a user, then the HA is located in the corporate network.

If the user has subscribed to Internet access with a wireline or wireless provider (in the remainder of the document called "Home Provider") different from the UMTS operator that the user is visiting, then, depending on mutual agreements, the HA may be in the Home Provider network or in the visited UMTS operator's network (in which case outsourcing of the HA functionality is offered by the UMTS operator).

If the user has subscribed to Internet access with the UMTS operator the user is visiting while accessing the Internet, then the HA is in this UMTS operator's network.

11.1.4 Discovery of the FA

Discovery of the FA address in UMTS will be performed either by sending a Mobile IP Agent solicitation as soon as the mobile node attaches to the UMTS network and needs to register with a FA, or the address of the FA could be piggybacked in some UMTS control message the mobile node receives at Routing Area updates. Both of these approaches avoid unnecessary broadcast of FA advertisements and make FA discovery fast.

11.1.5 Compound Tunnels

There is currently a well developed proposal (Tunnel Establishment Protocol – TEP- [TEP]) which would allow a UMTS operator to establish *compound Mobile IP+ tunnels* by introducing the concept of a Gateway Foreign Agent (GFA). The GFA behaves as a HA for a FA and downstream GFA, and as a FA for a HA and upstream GFA. Two benefits of the GFA (i.e., compound tunnels) are:

- Effects of mobility events can be limited to the UMTS operator's domain, by placing a GFA between FAs in the UMTS operator's network and the HA in a remote network. The segment of the tunnel between a GFA and a HA in the remote network is used only to provide remote network access via compulsory tunnelling. Only the segment of the tunnel between the GFA and FAs changes when the mobile node changes FA.

- Trust management is made simpler, since the tunnel between the UMTS operator's network and a remote network is not affected by mobility events, therefore no re-negotiation of session keys is necessary as the mobile changes FA.

11.1.6 Reverse tunnels

Reverse tunnels (that is tunnels from the FA to the HA) are necessary both for **remote network secure access** and to avoid packet drops due to **ingress filtering**. Ingress filtering allows tracking of malicious users attempting denial of service attacks based on topologically inconsistent source address spoofing [RFC2267].

TEP assumes the tunnel is always bi-directional (the tunnel looks therefore as a virtual point to point link).

An end to end bi-directional tunnel may result in **non optimal routing**, but it may be desirable to tunnel packets back to the home network (e.g. for **security enforcement** when a business user accesses the corporate intranet, or for **charging on a per byte fashion** at the HA both transmitted and received traffic, in addition to charging at the FA, in scenarios where it makes sense).

11.1.7 Intra System Handover

{editor's comment:

intra RNC – does not involve CN, except maybe for location update in the VLR, i.e. not of interest for this report

- *inter RNC and intra IGSN – should be handled over Iu, which means that is can be handled the same way for IGSN's as for SGSN's*

- *inter RNC and inter IGSN – means streamlining in the CN in connections with SRNS Relocation – distinguish cases with and without support from Iur interface.*

See also chapter with traffic cases

}

11.1.8 Inter System Handover (ISHO)

If a mobile is equipped with a dual mode radio interface that makes UMTS/GSM intersystem handover feasible, and if the UMTS network uses Mobile IP(+) while the GSM network is based on GPRS, then the only way to provide uninterrupted service as the mobile moves across areas covered by these different radio access technologies is to run Mobile IP(+) in overlay to GPRS. This is accomplished by placing FA functionality at some GGSN. The APN (Access Point Name) enclosed in the "Activate PDP Context Request" could identify a GGSN offering FA functionality. The issue is FFS.

11.2 Network Issues IPv6

Appendix A describes the operation of MIPv4 [RFC2002] and MIPv6[MIPIPv6]. The key differences between these protocols are listed below:

- Mobile IPv4 allows the use of Foreign Agents (FAs) to forward traffic thus requiring one care of address for multiple mobile stations, or the use of co-located care-of addresses (COA). In contrast MIPv6 supports co-located COA's only.
- Route optimisation is an add-on to MIPv4 whereas it is an integral part of the MIPv6 specification.
- MIPv4 route optimisation still requires traffic to be tunnelled between the correspondent host (CH) and the mobile station. In MIPv6 packets can be forwarded with no tunnelling, only the addition of a routing header.
- In MIPv4 the Home Agent (HA) must be involved in the setup of optimised routes. In MIPv6 the mobile station can initiate an optimised route to a CH directly (without involving the HA), and therefore more quickly and efficiently.
- In MIPv4 a COA is obtained from a FA or via DHCPv4. In MIPv6 a COA can be obtained via IPv6 stateless or stateful address auto-configuration mechanisms.
- In MIPv4, separate Mobile IP specific messages are required to communicate with the FA, HA and if employing route optimisation, CHs. In MIPv6, Mobile IP specific information can be piggybacked onto data packets.
- The ability to provide smoother hand-over in MIPv4 is an add-on feature that forms part of the route optimisation protocol. In contrast support for smoother hand-over is an integral part of the MIPv6 specification.
- In MIPv4 reverse tunneling is required to avoid ingress filtering problems (where firewalls drop the mobile's outgoing packets) since packets are sent with the home address as the source. In MIPv6 packets may be sent with the COA as the source address, hence there should not be any problems with ingress filtering.
- MIPv4 provides its own security mechanisms whereas MIPv6 employs the IPsec protocol suite.

To adequately assess the evolution and compatibility issues between MIPv4 and MIPv6 when applied to UMTS networks, each of these differences must be addressed. Section 11.1 describes how MIPv4 can be employed in UMTS networks. Section 11.2 describes the implications if MIPv6 is employed rather than MIPv4. Wider issues must be considered when comparing the deployment of, or migration between IPv4 and IPv6 networks in general. That is a topic FFS.

11.2.1 Care-of Addresses

In MIPv4, FA allocated COA's (FA-COA) are recommended for use in large cellular networks such as UMTS. In contrast, there is no concept of a FA in MIPv6. Furthermore, if MIPv6 is employed in HA mode it is less efficient than MIPv4 over the air interface. In terms of evolution, even though COA's are allocated differently, both MIPv4 and MIPv6 need interaction with other IGSN protocols to forward the IP packets over the correct logical link.

11.2.2 Location of the HA and the FA

The HA can be present in the same locations as for the MIPv4 case.

11.2.3 Discovery of the FA

FA discovery is not required in MIPv6. Instead mechanisms are needed to allow the ME to obtain a co-located COA. This can be achieved via stateless address autoconfiguration or stateful address configuration. Alternatively, like the MIPv4 case, it is possible for an IPv6 COA to be communicated to the ME in a UMTS control message. This has the benefit of avoiding IP level message passing over the air interface to obtain a COA. If the latter approach is followed, the COA could be communicated in the same UMTS control message regardless of whether MIPv4 or MIPv6 is employed.

There could be potential problems with employing stateless or stateful address autoconfiguration to obtain the COA for MIPv6 in UMTS. This is because these protocols require duplicate address detection (DAD). DAD, in its current form,

requires messages to be multicast to all MSs on the same link, and, can significantly lengthen the time to obtain a COA compared to MIPv4. This issue needs to be resolved before UMTS operators can deploy MIPv6.

11.2.4 Use of Route Optimiation

Benefits of route optimisation include a reduction in delays between the CH and ME, and a reduction in the load placed on HAs. Route optimisation in MIPv4 adds to the complexity of the HA and requires security associations between the HA and all CH's. Furthermore it still requires packets to be tunnelled from the CH to the FA-COA. In contrast, route optimisation in MIPv6 removes the need to tunnel packets, instead a routing header is added to each packet. The ME also has more control over deciding when to optimise routes since it creates the optimised route rather than the HA. This also means the HA is simpler in MIPv6. In terms of migrating from MIPv4 to MIPv6, in MIPv4 changes need to be made to CHs to employ route optimisation. In contrast, if MIPv6 is employed, all IPv6 CHs will support route optimisation automatically.

11.2.5 Compound Tunnels

If the UMTS operator employs compound tunnels for MIPv4, it is FFS how they should be evolved to MIPv6.

11.2.6 Reverse Tunnels

Reverse tunnels are not needed to avoid problems with ingress filters in MIPv6. However they may still be beneficial when the ME is concerned about location privacy. {*Editor's comment: the MN can use the care-of address as sender address but that is not required*}

11.2.7 QoS

If traffic is forwarded via the HA, MIPv6 has similar problems with the provision of QoS as MIPv4. In MIPv4 problems interworking with RSVP arise because the RSVP control messages are hidden inside the tunnel between the HA and COA. In MIPv6 this problem doesn't exist with route optimisation because the tunnels disappear. However there is a mismatch in the addressing information in the RSVP control messages and in the IP header which causes routing problems. This can be resolved as long as the RSVP layer at both the CH and ME are aware of the ME's COA.

11.3 Robustness and Scalability

11.4 Need for Broadcasting over Radio

Although Mobile IP(+) utilizes various router and agent advertisement messages, which normally are broadcast over the local network, it is not necessary to broadcast these messages to all ME's over the UMTS radio interface. When the terminal is switched on, it will communicate with the CN, like it does today in GPRS to attach to the network. Thereafter, it is possible for it to communicate on the IP level with the IGSN.

To find out on which IP subnet the ME is located and where the nearest router is located, it sends a router solicitation and gets a unicast ICMP router advertisement in response from the nearest router. A mobility agent, i.e. HA or FA, can be configured to send agent advertisements only in response to agent solicitation messages. The response to such a message is always a unicast router advertisement message. Since the FA is a type of router, it is, however, not necessary to send both Router Solicitation and Foreign Agent Solicitation messages. This method has a few advantages compared to letting the ME wait for router and mobility agent advertisements:

- No broadcast over radio is needed
- Decreases set-up time since the ME does not need to wait for the next advertisement

The latter point is especially important when using this method also at handovers between IGSN's.

To inform the ME that it has changed to a new subnetwork after a handover that requires streamlining in the CN, one dedicated message is needed on the link layer between the ME and the IGSN. Alternatively, the ME may detect the change of SGSN on the basis of other network parameters.

11.5 Traffic Cases

To illustrate how the combined GSM/GPRS/IP System could interwork, some basic traffic cases will be explained in detail below. To give a complete view, also UMTS and GPRS specific procedures have been included. These are assumed to be based on the GSM procedures adapted to UMTS and should be seen as examples, since they are not yet standardized and also not specific to this particular core network scenario.

11.5.1 Registration

This section illustrates how a full UMTS/GPRS and Mobile IP registration procedure could work. It includes registration with the HLR (IMSI attach etc.) and the Home Agent. The Mobile IP registration procedure, which is defined in [RFC2002], is independent of the UMTS/GPRS specific procedures for IMSI attach and setup of PDP Context.

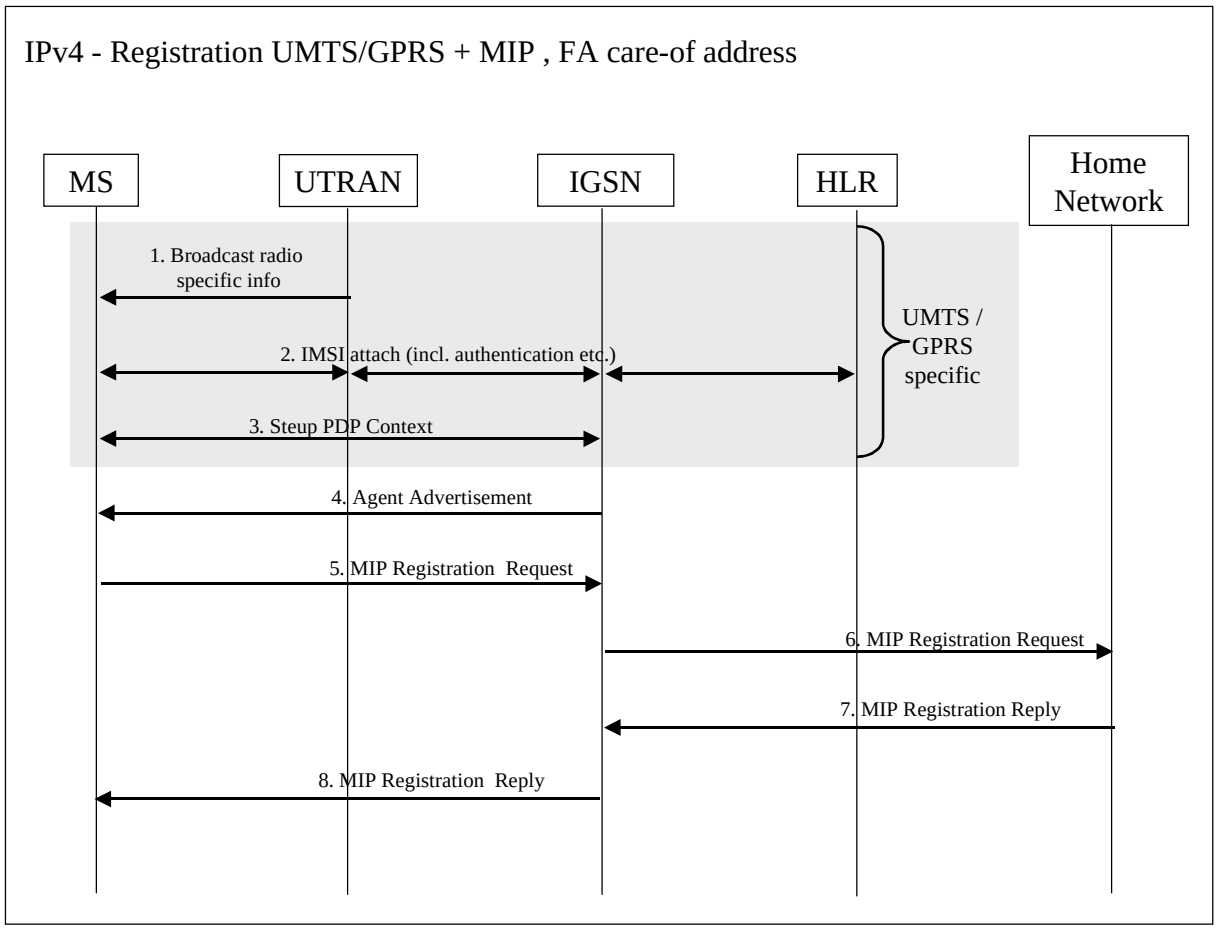

Figure 6. The registration procedure. The details of the UMTS specific part (shadowed) are left out.

11.5.1.1 UMTS/GPRS specific part

The first thing an ME has to do after being turned on in a UMTS or GPRS network is to set up the radio connection and register with the visited network.

1. When the ME arrives at a new UTRAN/BSS, it listens to the radio broadcast messages, which contain radio and UTRAN/BSS parameters, protocol information, network, CN domain and cell identity, etc.[UMTS25.331]/[GSM-TBD]
2. The ME performs an IMSI attach, which includes UMTS/GSM security functions etc. IMSI attach is specified in [UMTS23.121] for UMTS and in [TBD] for GSM. If needed, a location update procedure will be executed.

3. From the ME's point of view, the PDP Context is set up in the same way as proposed for step 1. Although every IGSN is expected to contain FA functionality, the APN can be used to handle e.g. the request for Mobile IPv4 and Mobile IPv6.

A minimum impact on the current GSM and UMTS messages has been assumed, which means that the UMTS/GSM subscription information is located in the HLR. If the mobile terminal is not allowed in the current UTRAN/IGSN, the connection will be halted at this point.

11.5.1.2 Mobile IP specific part (FA care-of address)

The ME and the IGSN now starts communicating with each other on the IP layer, i.e. in the user plane. The messages are defined in [RFC2002]. This part is the same as for step 1 and extensively described in section 9.4. The only difference is that the IGSN will handle the Mobile IP FA functionality instead of the GGSN/FA.

4 A successful setup of PDP context triggers the IGSN to send a dedicated Agent Advertisement message, which contains network parameters and at least one Mobile IP care-of-address.

5 The ME sends a Mobile IP Registration Request to the IGSN. A dynamic home address may be requested.

6 The IGSN processes and forwards the registration request to the Home Network.

7 The HA replies with a registration reply that grants or denies the request.

8 The registration reply is sent from the Home Network to the IGSN, which forwards it to the ME.

If the care-of address was accepted by the HA, the ME can now inform other nodes about its current care-of address if route.

11.5.2 Sending Packets

[mobile-to-mobile and mobile-to-fixed]

11.5.3 Receiving Incoming Packets

11.5.3.1 Mobile Terminated Datagrams, IPv4

The following section describes how incoming IP datagrams are handled in the different nodes. It is assumed that the Mobile Node has a FA care-of address, which is registered at the HA and that the MN is in (UMTS) stand-by mode when the incoming datagram arrives. The Mobile IP procedures are according to [RFC2002].

The datagram to the mobile node arrives in the home network via standard IP routing. The HA intercepts the datagram and tunnels it to the care-of address, in this case the FA (IGSN). Before the IGSN can deliver the datagram to the mobile node, paging etc. needs to be performed according to general UMTS/GPRS procedures. If optimized routing is desired and if the correspondent node supports binding cache, the HA sends a binding update message to inform the correspondent node about the current care-of address of the mobile node. From now on, the correspondent node can send datagrams directly to the mobile node by tunneling them to the FA care-of address. This is depicted in Figure 7. If the correspondent node does not support a binding cache, all packets will go through the HA as in Figure 8.

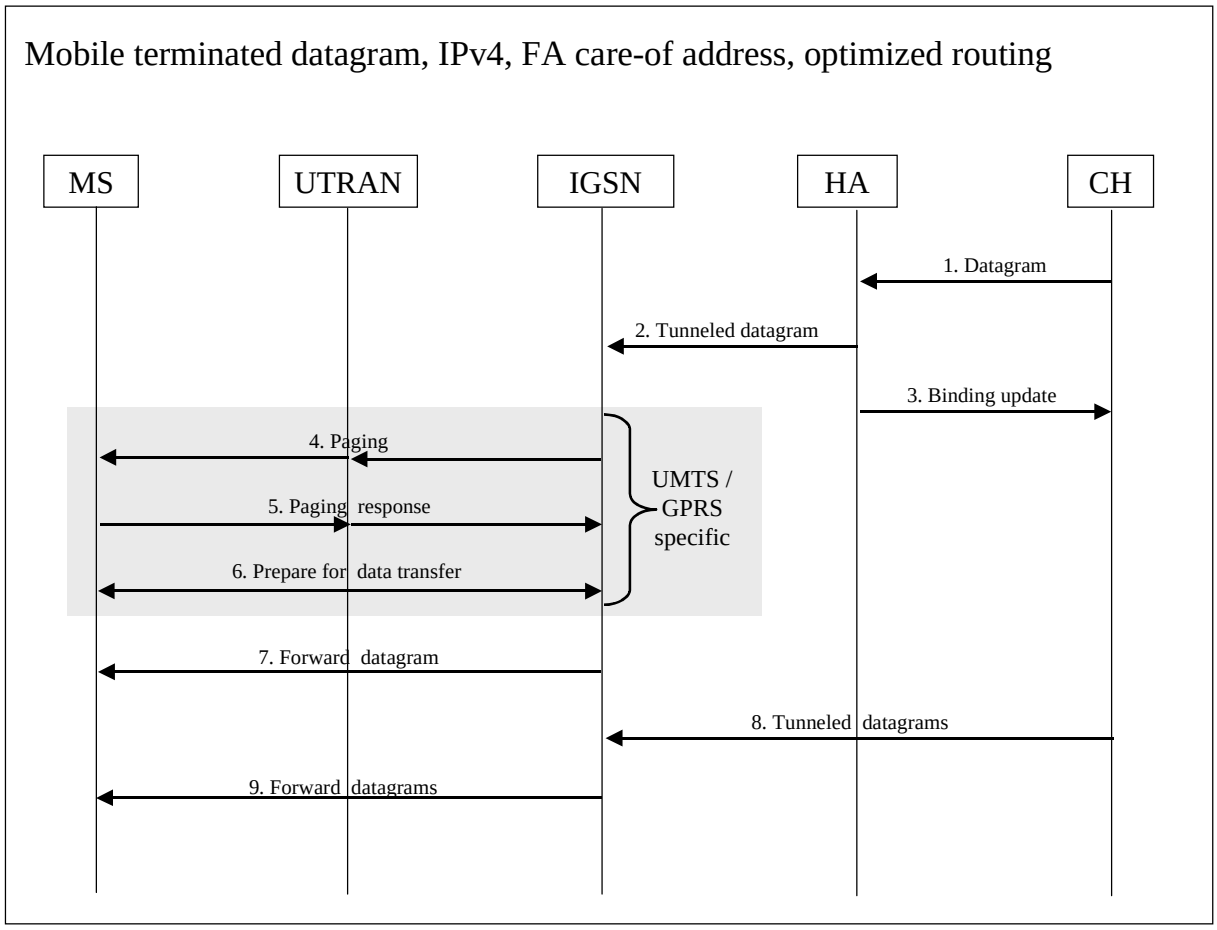

Figure 7. Delivery of mobile terminated datagrams, optimized routing.

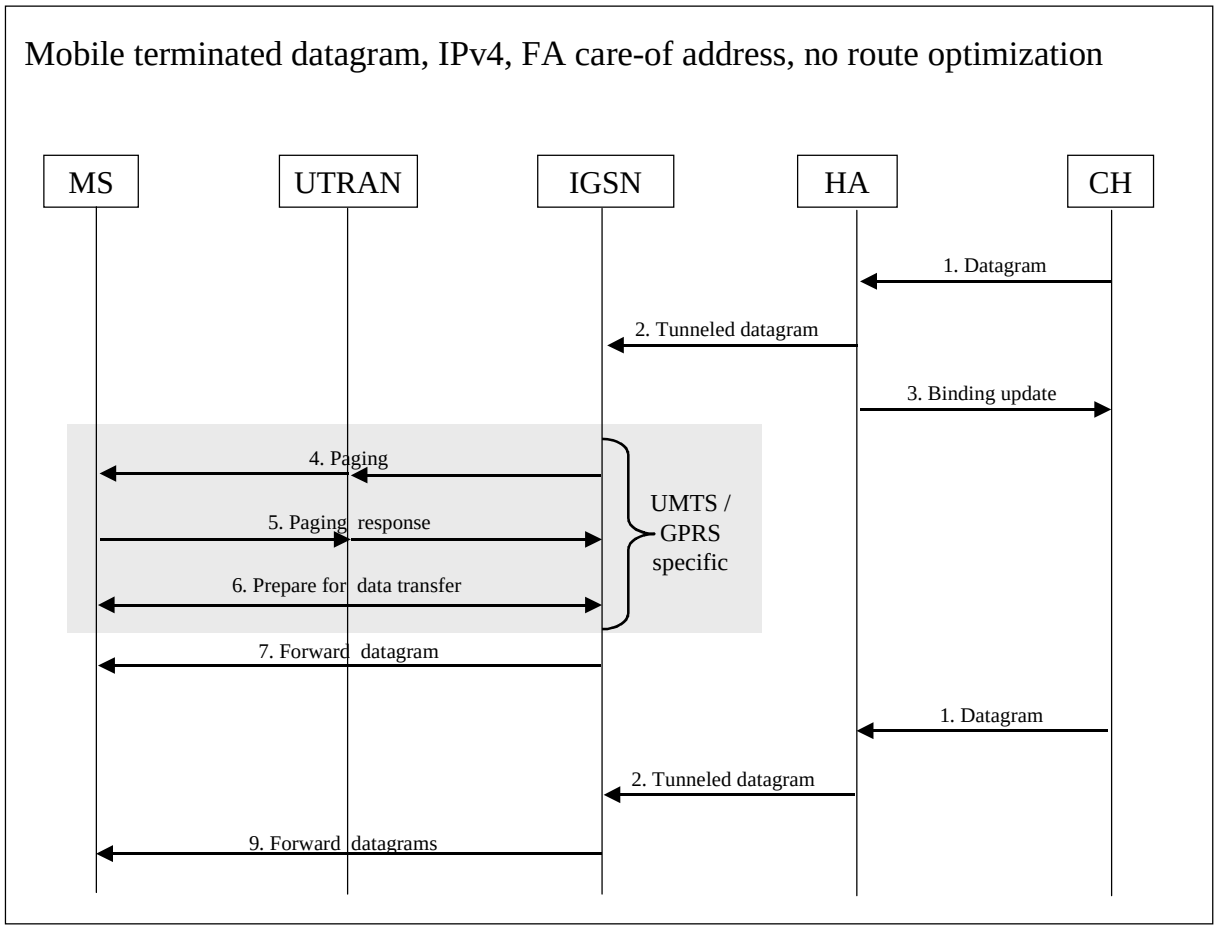

Figure 8. Delivery of mobile terminated datagrams, no route optimization

11.5.4 Roaming

11.5.5 Handover Cases

11.6 Addressing

11.6.1 Addressing Issues in IPv4

The IPv4 address is a 32 bit string. Historically it has played both the roles of identifier and locator [RFC2101]. In fact it has been used both to identify the endpoints of an IPv4 session and to decide where to route packets.

As the Internet has evolved scaling problems have made it impossible to keep the address unrelated to the topology, thus the class based addressing scheme has been replaced by the Classless Inter Domain Routing approach (CIDR) [RFC 1518][RFC 1519].

CIDR allows aggregation of addresses on a finer-grain resolution (aggregation happens on a per bit, instead of on a per octet basis), thus it allows the allotment of addresses to ISPs' customers with more flexibility and in a more efficient way. On the other hand the hierarchical and topology bound nature of CIDR means that an address can't be kept by an organization if the provider changes. An organization would therefore have to renumber. In addition providers and

corporations assign addresses on a temporary basis. Therefore the IP address is no more temporarily unique, hence the role of identifier is no more well suited by the IP address (let alone security reasons).

Also, due to the deployment of Intranets based on private IP addressing schemes, addresses are no longer guaranteed to be unique. As such, an IP address can't be considered as a universal locator, since the Internet also comprises networks configured as independent routing realms. Connectivity across routing realms is possible by means of Application Level Gateways (ALG) or Network Address Translators (NAT), or similar devices.

These new ways of utilising IP addresses, and the possibility to decouple the functionality of Locator and Identifier via the use of logical names, reduce the limitations imposed by the 32 bit address space.

Let's consider what UMTS operators can do to avoid excessive IP address space consumption.

For a UMTS operator, the immediate way to provide Internet access is to dynamically assign public addresses to UEs. An IP address is needed only when a UE enters a data session, that is only when the UE is in active state. Therefore the number of IP addresses needed would be determined by a statistic analysis of the number of concurrently active UEs that an operator needs to support, so that the blocking probability due to lack of public addresses is smaller than a desired (or standardized) quality parameter.

The assignment of IP addresses to inactive UEs would be needed for inactive UEs to be reachable from the Internet. It can be envisioned, however, that over time the deployment of directory services and an E.164 to IP mapping infrastructure, currently being defined by the IETF, will allow the set-up of data sessions with UEs in inactive state that are not assigned an IP address, provided they are identified by a logical name and that they are attached to the mobile network so that they can be paged.

When remote network access is desired using Mobile IPv4 based on FA-COA, no dedicated address from the address space owned by the UMTS operator is required. The same is true for non UMTS operators providing Internet access to their users utilizing the UMTS operator's wireless network.

11.6.2 Addressing issues in IPv6

11.6.3 Private Addresses

Sometimes private addressing schemes are used either by the UMTS operator or by a remote network that a user wants to access. Then, at the boundary of the routing realms stateful and Mobile IP+ aware mechanisms as the one proposed in [NAR] are needed in order to correctly route packets across them. Also, the information stored in such devices must be negotiated by the terminals, so that terminals can consistently insert proper addressing information in Mobile IP+ registration messages. Alternatively, the HA and FA functionality could be located at the boundary of the routing realms (thus a public IP address is assigned to them).

11.7 Terminal aspects

The mobile terminals need to be enhanced with MIP(+) functionality. For compatibility with other systems, it is of great importance that standard IETF Mobile IP(+) and not special UMTS versions is used. Any interaction between the IP layer and the "UMTS layer" needs to be identified and defined. To avoid future updates of the mobile terminal, it should be considered to include the possibly needed UMTS specific functionality of all three steps in the MT at once.

11.8 Security, Roaming and AAA

11.8.1 Mobile IPv4 control messages: security issues

The standard requires mobile nodes to be authenticated when they update the HA about their current point of attachment to the network. The standard does not require that the mobile node is authenticated with the FA and that the FA is authenticated with the HA. There is a simple reason why this makes sense. Let's consider a cellular network operator who owns an IP backbone equipped with FAs and HAs for IP mobility support. HAs and FAs trust each other, only

trusted mobile nodes can deliver packets to the FA (the radio link to the FA is secure and is granted only after UMTS authentication takes place), but even a trusted mobile station could redirect packets bound to another mobile node by spoofing its identity in registration messages, if not properly verified by home agents. This can happen because the data network identity and UMTS identity may be unrelated.

Therefore, for Internet access directly provided by a UMTS operator only a shared secret between MN and HA is required.

When a mobile node requires access to a remote corporate network or its home network, a shared secret between mobility agents (i.e., the HA and the FA) is required [RFC2002]to ensure the secure exchange of Mobile IP control messages since the HA and the FA are in different security domains.

Therefore, for the UMTS operator to provide users roaming in its network access to their home network or their corporate intranet, two shared secrets are required: between the MN and the HA, and between the FA and the HA.

11.8.2 Mobile IPv6 control messages: Security Issues

Security issues differ between MIPv4 and MIPv6 primarily due to the absence of the FA. One significant difference is that IPv4 may require security associations between a FA in the UMTS network and a HA in a corporate intranet, whereas IPv6 requires security associations from the ME to HAs and correspondent nodes.

11.8.3 Screening and Flooding

Network screening and user screening, i.e. to prevent flooding of network nodes by keeping unwanted incoming traffic out of the network, is an important issue both for mobile and fixed networks. Effort is put into obtaining these features in IP networks and the techniques developed for fixed networks will be used also for GPRS. These encompass firewalls (FW), border gateways (BG), …

Static filtering rules at the FA and **compulsory tunnels** from the FAs to security enforcement points of the IP network owned by the UMTS operator can be used to avoid any unwanted and uncontrolled access to critical network resources by mobile users. For data incoming from other networks, normal security enforcement devices and methods are used.

11.8.4 AAA (Authentication, Authorization and Accounting) and Roaming issues

When a data network access service is provided, there are two possible ways to authenticate, authorize and account. One possibility is to look-up the user profile stored in the HLR and to update billing records as currently happens in GSM. Another possibility is reusing AAA protocols used in data networks (e.g. RADIUS or, in the future, DIAMETER). Some considerations follow:

- Authorization based on UMTS identity authentication is not sufficient if **data network identity and UMTS identity are possibly unrelated**. For instance, this is the case of a mobile station composed of a TE and a MT, such as a Laptop and an UMTS data card. The data card could be shared by a group of users in accessing different networks or the same network under different identities. Therefore separate authorization and accounting for UMTS access services and Data Network usage are desirable.

- **Data network roaming procedures** are based on interaction between AAA servers. Support of data network roaming procedures is a fundamental component in the provision of scalable ubiquitous corporate intranet access services and for the support of Internet access service via subscription with a single wireline or wireless provider. This is another reason why deploying a IETF standard AAA infrastructure makes sense.

Mobile IP+ will natively rely on data network AAA protocols and supports IP level roaming procedures via the NAI (Network Access Identifier) extensions. In a Mobile IP(+) based UMTS network **separation of radio access and data network identity** is natively supported. Below, some of the scenarios described are summarized in Figure 9 and Figure 10.

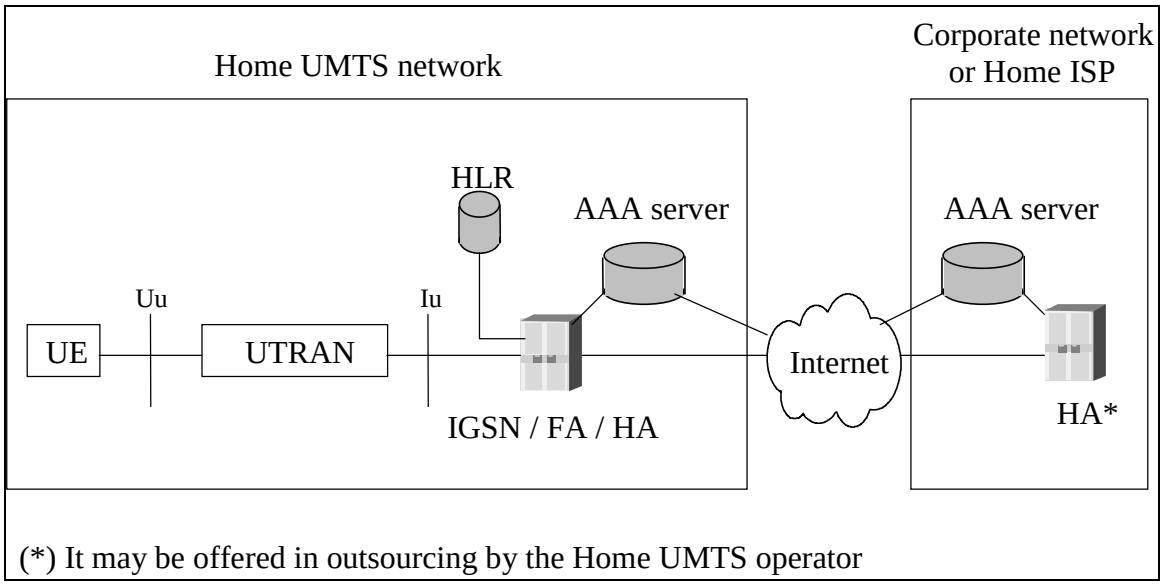

Figure 9 - UE attached to the Home UMTS operator

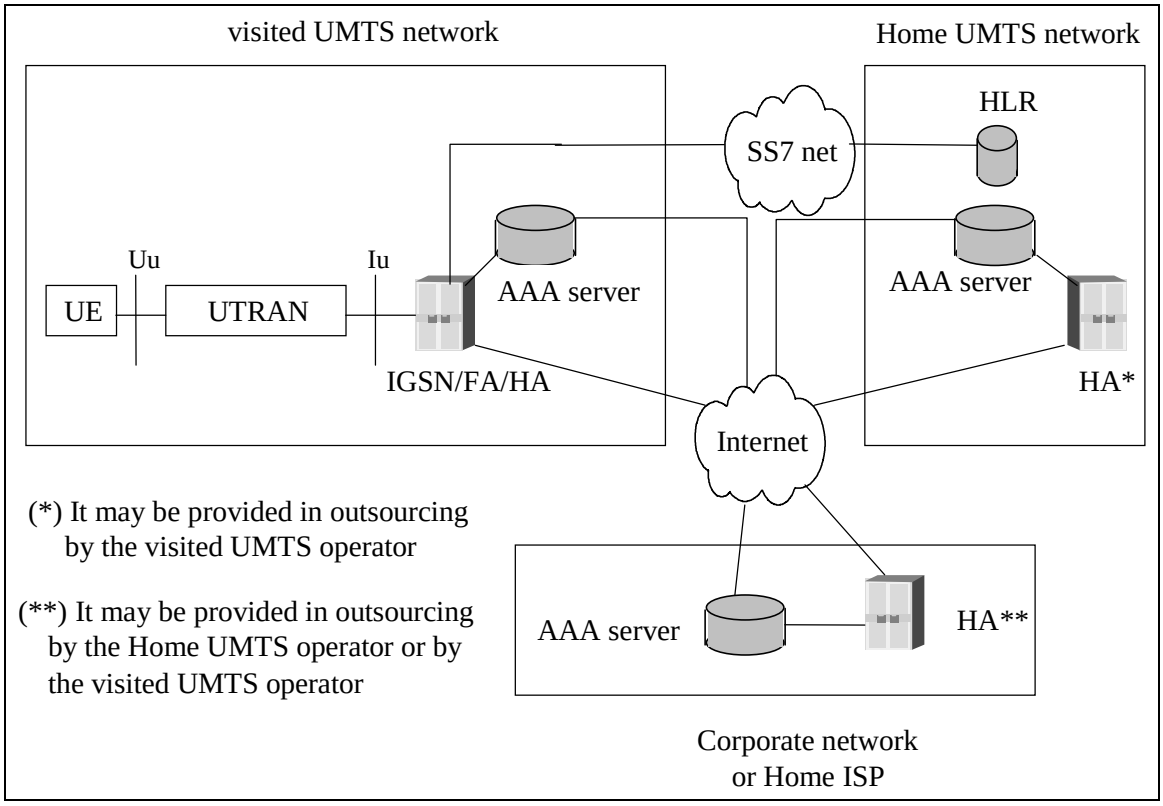

Figure 10 – UE not attached to the Home UMTS operator

As is the case for MIP+v4, separate authorisation and accounting for UMTS access services and data network usage is desirable also for MIP+v6. Procedures for AAA in MIP version 6 have not yet been addressed, but we can expect them to be similar to those used in version 4.

11.8.5 Use of IPsec

Permanent IPsec associations through the IP backbone established and maintained by the IGSN's would allow signaling information to be transmitted in a secure manner. Signaling information is transmitted in transport mode. IGSN's could have a specific IP address solely used for signaling purposes. The IPsec connections, though permanent, should change keys at proper intervals.

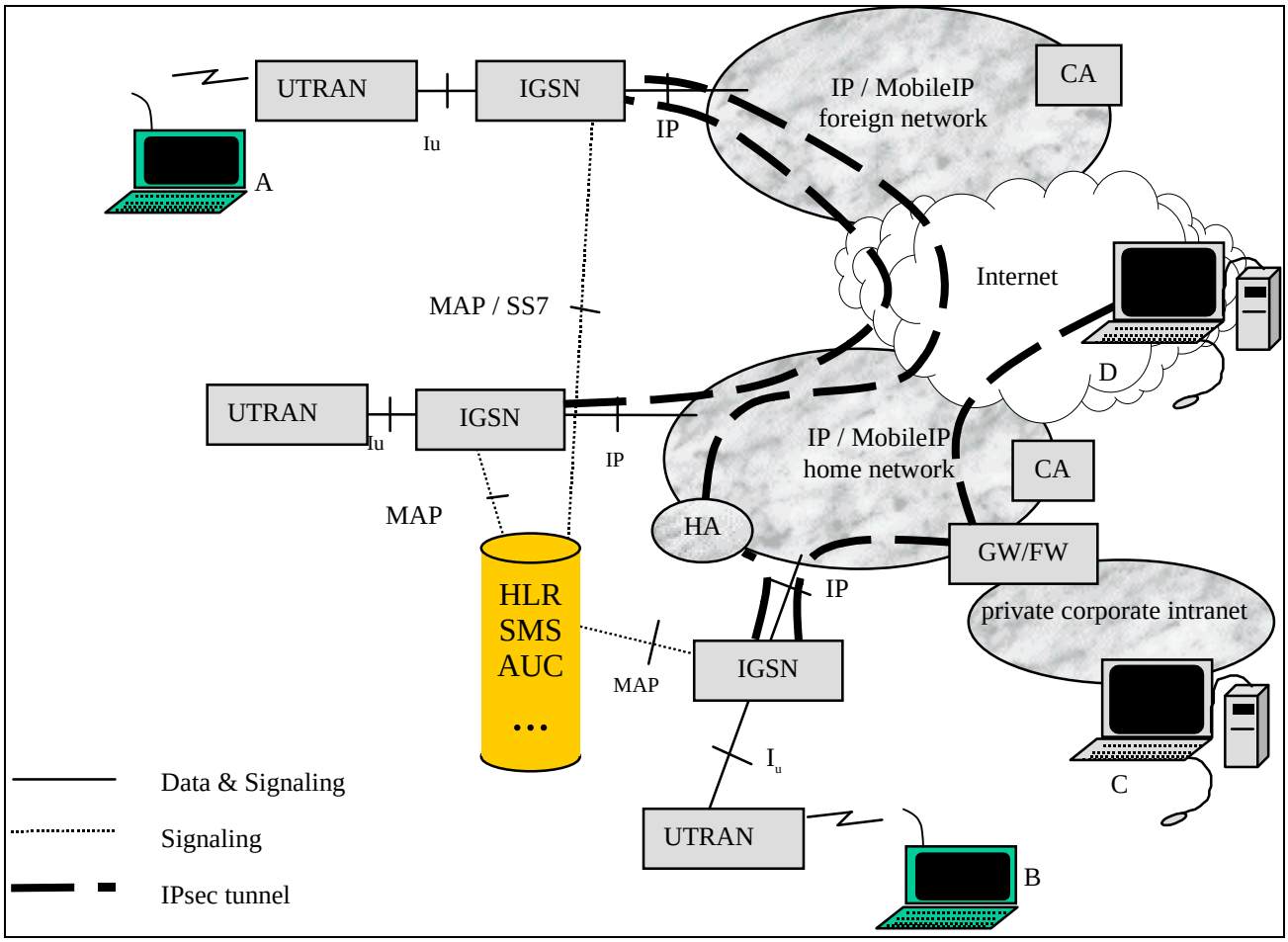

Figure 11. *IPsec for connection to private corporate intranet*

IPsec tunnels may also be used for corporate customers to connect to their intranet in a VPN fashion. A gateway that also acts as a firewall sits between the IP core network and the corporate intranet.

11.8.5.1 The importance of IP level authentication

There is no way of knowing who sent the request without some sort of authentication at IP level. The danger of replay attacks has to be addressed. Both these problems are solved natively in Mobile IP.

Consider the following scenarios:

An intruder has registered at an UTRAN in a normal and fully legitimate fashion and has received a C/O-address, but he does not inform the HA. He also has access to the IP core network. Later on a legitimate user registers at the UTRAN and tries to register at the HA with his C/O-address. By intercepting the registration request from the legitimate user and alter the C/O-address the imposter can pose as the legitimate user.

An intruder wishes to launch a denial of service attack and has access to the IP core network. This can be done easily by intercepting registration requests to the HA and return false registration accept messages to the sender. Of course he can accomplish denial of service by simply discarding registration requests, but if he sends a false reply the attacked user won't know of the attack. An attacker could also send false registration denies to the user.

Mobile IPv4In Mobile IPv4 [RFC2002] it is stated that the authentication extension must be used and that all implementations must be able to handle keyed MD5 with 128 bit keys. That is, the HA and ME must have a shared and secret 128 bit key. However, [RFC2002] doesn't exclude the possibility to use other methods.

On the GSM SIM card there is a secret key stored called Ki, which is 128 bits long and used for authentication purposes[UMTS22.00]. However, since it is not known outside the AUC and the SIM it cannot be utilized also for Mobile IP(+). Therefor a completely different set of keys must be used to authenticate Mobile IP(+) messages.

A private/public-key technique could be used. If all users know the public key of their HA and all users public keys e.g. are stored in the HLR, and thus accessible for the HA, an authenticated exchange of MobileIP messages can be

performed. Public keys can be transmitted from HLR to HA over the SS7 Gh interface without any risk of a security breach. An other way to store an distribute public keys is the use of a trusted third party and digital certificates as proposed recently in the IETF Internet draft ”Mobile IP and Public Key Based Authentication” [PubKey] by Stuart Jacobs of GTE Laboratories.

The use of digital certificates and a Certificate Authority (CA) has a few other advantages. An hierarchy of CAs on different IP core networks could be set up by operators with roaming agreements.

1. IPsec uses digital certificates as the most general way of authentication. Two IGSNs on different IP core networks can use digital certificates as a means of authentication without any prior knowledge of each other.

2. Addition of an IGSN only requires an update of the CA.

3. An IP core network operator customer could use the CA when establishing an IPsec connection to his private corporate intranet.

11.8.5.2 Security in Mobile IPv6

In IPv6 the authentication (and encryption) is handled natively by IPsec. So for each Mobile IP+ message that the ME generates, it has to set up a new IPsec connection to the HA or use a pre-existing one if it hasn’t timed out. These IPsec connections could naturally also take advantage of a CA.

11.8.5.3 Encryption of Mobile IP(+) messages

Only authentication is mandatory in Mobile IPv4. Encryption of Mobile IP messages is out of scope in the Mobile IPv4 standard [RFC2002]. Encryption of registration requests is however crucial to protect personal integrity. With unencrypted registration messages, a user could be tracked if an intruder has access to the IP core network. To prevent this, IPsec encryption should be provided by the network operator between IGSN and HA.

In IPv6 both authentication and encryption is handled end-to-end by IPsec.

11.8.5.4 IPsec for protection of user data

Primarily, it is up to the user to protect user data with end-to-end encryption and authentication. However, the bandwidth need will increase somewhat.

11.8.6 IP Authentication Mechanisms – Radius and Diameter

11.8.7 UMTS Charging

[*charging can be performed in the IGSN using more or less the same system as GPRS – what changes need to be introduced?*]

11.8.8 IP Charging mechanisms – Radius and Diameter

[*Using Radius/Diameter for charging is one way to align UMTS with fixed IP networks and ISP needs. How does it work? Does it fulfill the requirements for UMTS?*]

11.9 Service Support

11.9.1 QoS – the Use of Differentiated and Integrated Services

QoS support in UMTS IP CN could be based on either (1) over provisioning of network capacity or (2) IP layer QoS mechanisms. If the IP network, i.e. routers and links, is over provisioned, traffic transported through the network will experience limited packet delays and low packet losses.

In addition, there are currently two IP layer QoS mechanisms under development within IETF, Differentiated Services and Integrated Services.

11.9.1.1 Differentiated Services

The Differentiated Services (DS) architecture [diffs-frame][RFC2475] is based on a model where IP traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single DS codepoint in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior (PHB) associated with the DS codepoint. This architecture achieves scalability, since per- application flow or per-customer forwarding state not need to be maintained within the core of the network.

There are two per-hop behaviors currently being standardized within IETF, Expedited Forwarding (EF) and Assured Forwarding (AF).

The EF PHB can be used to build a low latency, assured bandwidth, end-to-end service through diffserv domains. To support this service, it is required in every transit node, that the aggregate's maximal arrival rate is less than that aggregate's minimal departure rate. This service appears to the endpoints like a point-to-point connection or a "virtual leased line".

The AF PHB provides delivery of IP packets in four independently forwarded classes. Within each class, an IP packet can be assigned one of three different levels of drop precedence.

At each differentiated service customer/provider boundary, the service provided is defined in the form of a SLA (Service Level Agreement). The SLA is a contract, static or dynamic, that specifies the overall features and performance, which can be expected by the customer.

In order to support a Differentiated Services network, the boundary routers of one administrative domain need to handle functions like admission control, policy control and traffic conditioning.

A standard RSVP component is currently proposed by the IETF to be implemented in the boundary router, and that makes it possible for a host to dynamically configure the diff-serv traffic condition components using RSVP signaling.

11.9.1.2 Integrated Services

The Internet Integrated Services framework [RFC2215] [RFC2216] provides the ability for applications to choose among multiple, controlled levels of end-to-end delivery service for their data packets. States per packet flow in every router is required and every router also makes admission control and policy control. The Integrated Services architecture adds complexity to the network compared to the previously described Differentiated Services architecture, but it makes it possible to reserve resources separately for every flow. There are two delivery services currently specified, a Guaranteed service, and a Controlled-load service.

The Guaranteed service provides firm bounds on end-to-end packet queuing delays and makes it possible to provide a service that guarantees both delay and bandwidth.

The Controlled-load service provides the data flow with a quality of service that is close to the quality that the flow would experience in an unloaded network.

RSVP is the protocol, which is used to signal resource reservation messages between hosts and routers for end-to-end flows.

11.9.1.3 Mobile IP and Integrated Services (RSVP)

Tunnels in both directions (From HA to FA and from FA to HA) can follow provisioned paths along which QoS is provided using routers with appropriate buffer management and scheduling mechanisms, as well as policy based routing and classification. Alternatively reservations can be established using RSVP tunnel extensions, but in this case UDP encapsulation of packets transported over RSVP tunnels is required.

When using Mobile IP(+) in an Integrated Services capable environment primarily two things need to be considered:

1. Mobile IP(+) uses IP-in-IP encapsulation to tunnel packets between the mobility agents, and tunnels make end-to-end RSVP messages invisible to the intermediate routers.

2. In case of a Mobile IP(+) handover, new reservations along the new tunnel path need to be setup.

The following section describes how to handle these issues. In addition, the use of multiple simultaneous care-of-addresses per mobile node in combination with RSVP, to possibly support an enhanced handover performance, should be studied in the future.

The IETF document [rsvp-tunnel] describes a mechanism, which allows RSVP to make reservations across, for example, Mobile IP(+) tunnels. The main idea is to have a separate RSVP session between the tunnel end-points. The tunnel entry point serves as the sender for the tunnel RSVP session, and the tunnel exit-point serves as the receiver.

The tunnel RSVP session can exist independently of the end-to-end RSVP messages, or it can be triggered by end-to-end RSVP messages.

Several mobile nodes, using the service from the same mobility agents, could share a RSVP tunnel and minimize the added states in the network. Alternatively, a new RSVP tunnel could be setup separately for every mobile node and/or flow.

When a mobile node moves to a new foreign network, reservations for the new tunnel need to be setup. In order to minimize the service interruption during the handover, the new tunnel between the mobility agents could be pre-configured at some level.

If traffic is forwarded via the HA, MIPv6 has similar problems with the provision of QoS as MIPv4. In MIPv4 problems interworking with RSVP arise because the RSVP control messages are hidden inside the tunnel between the HA and COA. In MIPv6 this problem doesn't exist with route optimisation because the tunnels disappear. However there is a mismatch in the addressing information in the RSVP control messages and in the IP header which causes routing problems. This can be resolved as long as the RSVP layer at both the correspondent nodes and ME are aware of the ME's COA.

11.9.1.4 Mobile IP and Differentiated Services

FFS…

11.9.2 Multi Protocol Support

Multi protocol support over MIP tunnels can be performed using GRE encapsulation [RFC1701][RFC1702]. Note that either surrogate registration or a normal Mobile IP registration can be used. However, the use of normal Mobile IP registration requires the mobile node to support Mobile IP(+) even if it is not an IP terminal. Presently, UMTS and GPRS are required to support IP and X.25 traffic. *{Editor's comment: Is GPRS phase 2 required to support also PPP ?}*

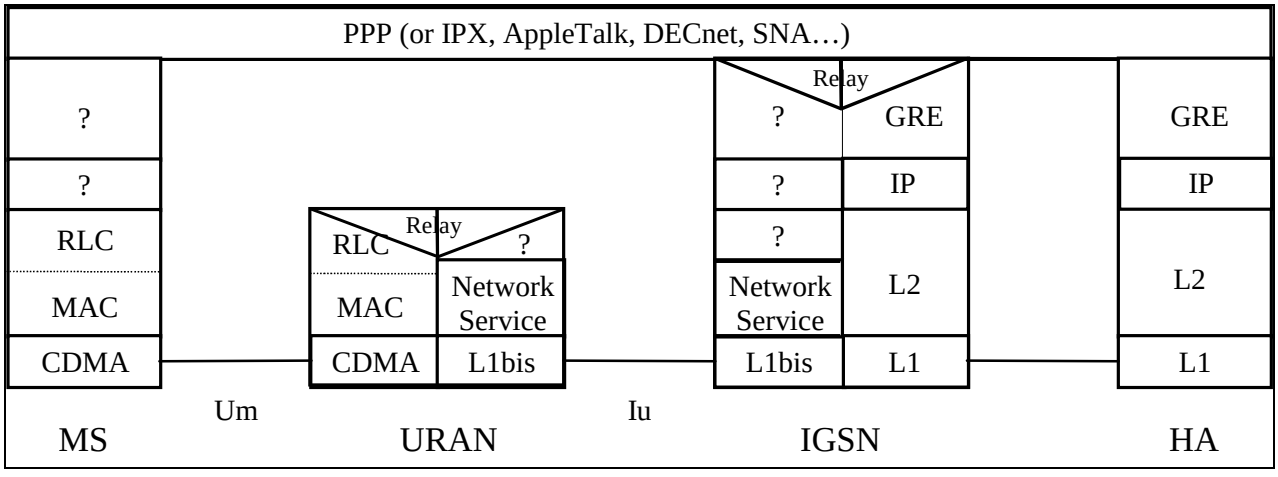

Figure 12 – Multiprotocol support in Mobile IP(+)

11.9.3 Service Control

11.9.4 Support of Multimedia

11.9.5 Support of VHE

One meaning, and probably the most important meaning, of virtual home environment (VHE) is that access to services is independent of the location of the terminal. This means that the same user interface and the same procedure should be used in the home network as well as in visited networks. Through e.g. www interface and java applications, this is easily obtained in IP networks. Address transparency is inherent through DNS (Domain Name Serves) which translate alphanumerical address to routable IP addresses.

Another meaning of VHE is that the user interface will look the same for one user, independent on the terminal. This is already today the case for many terminals attached to LAN's. This technique can probably be used for mobile terminal as well. Especially for business customers, who are expected to use UMTS for mobile LAN access, this is an attractive solution. The possibility of using a previously cached version of the personal terminal profile in the terminal must be supported, to prevent long setup times when the available bandwidth is limited.

[Text on CAMEL for GPRS and how it could be used for this architecture would fit in here]

11.9.6 Personal Mobility

[*voice over IP and other teleservices – call forwarding etc.*]

12 Compatibility Issues

12.1 IPv4 – IPv6

12.1.1 Mixed IPv4 – IPv6 UMTS Networks

If UMTS standards support IPv4 and IPv6, situations will arise where one UMTS operator employs MIP(+)v4 and another MIP(+)v6. Given there are no FAs in MI(+)Pv6 it should be possible to support an MIP(+)v6 ME and HA when the current UMTS network is IPv4 only, via IETF IPv4 to IPv6 transition mechanisms. The general assumption in IETF is that IPv6 nodes will also have an IPv4 stack during the transition time. However, the specific mechanisms and the implications on the UMTS network require further consideration.

12.1.2 Network Elements that need changes if migrating from MIP(+)v4 to MIP(+)v6

During the period when IPv4 and IPv6 nodes will exist in parallel, the nodes are assumed to have double stacks to coop with a dual IP version environment. This period may stretch out over many years. Once all nodes are IPv6 only, the IPv4 functionality will no longer be necessary.

ME

- Must have an IPv6 stack (including MIP(+)v6) in addition to an IPv4 stack

IGSN

- Must provide standard IPv6 router functionality in addition to FA functionality
- May need a DHCP server or another mechanism to provide the COA (not necessary if stateless autoconfiguration is employed).

HA

- Must provide standard IPv6 router functionality in addition to IPv4 router functionality
- Must support MIP(+)v6 HA functions in addition to MIP(+)v4 functions.

Routers

- Must provide standard IPv6 router functionality in addition to IPv4 router functionality

12.2 UMTS/GPRS – Mobile IP(+)

12.2.1 Support of Non-MIP(+) Mobiles in a MIP+ based backbone

One fundamental principle in Mobile IP(+) is that the mobile node is handling the mobility signaling with the home network. GPRS terminals only signal with the visited network and the visited network communicates with the home network. When changing from “GTP-mobility” (present architecture) in a UMTS/GPRS backbone to “Mobile IP+-mobility” (step 3), the terminals need to be enhanced with Mobile IP+ functionality to handle macro mobility. To allow a gradual transition of terminals, a PLMN CN based on Mobile IP+ need to handle terminals without Mobile IP(+) functionality. One solution is “surrogate registrations”, where the IGSN registers the mobile node on behalf of the mobile node. Note that the discussion below only concerns terminals without MIP(+) functionality.

12.2.1.1 Pre Mobile IP(+) situation

A PLMN backbone with the GPRS architecture will have SGSN’s and GGSN’s. The GGSN is a fixed point for the traffic during the GPRS session and the SGSN with change depending on the location of the ME. The change of SGSN is transparent to the IP layer in the ME. There are several alternatives on how to connect the GGSN to external IP networks. Some of these are illustrated in Figure 46-1, where the ME is located in its home network. However, there is no major difference of the ME being in its home network or in a foreign one.

1. A specific GGSN (or logical part thereof) can be requested by the ME to connect to a coorporate LAN. From the GGSN, there is a secure connection to the specified coorporate network. There are different ways to realize the secure connection, e.g.:

I. A leased line

II. An IPsec tunnel across the Internet or other IP networks

III. The GGSN is located in the coorporate domain instead of in the operator’s domain. This is however not likely to be implemented due to security problems.

2. If the ME has a static public IP address, the visited PLMN will always connect the ME to a specific GGSN, from where it can reach the public Internet.
3. If the ME requests a temporary address to connect to the public Internet, the ME will be connected to a GGSN, either in visited or in home network, from where the ME can reach the public Internet.

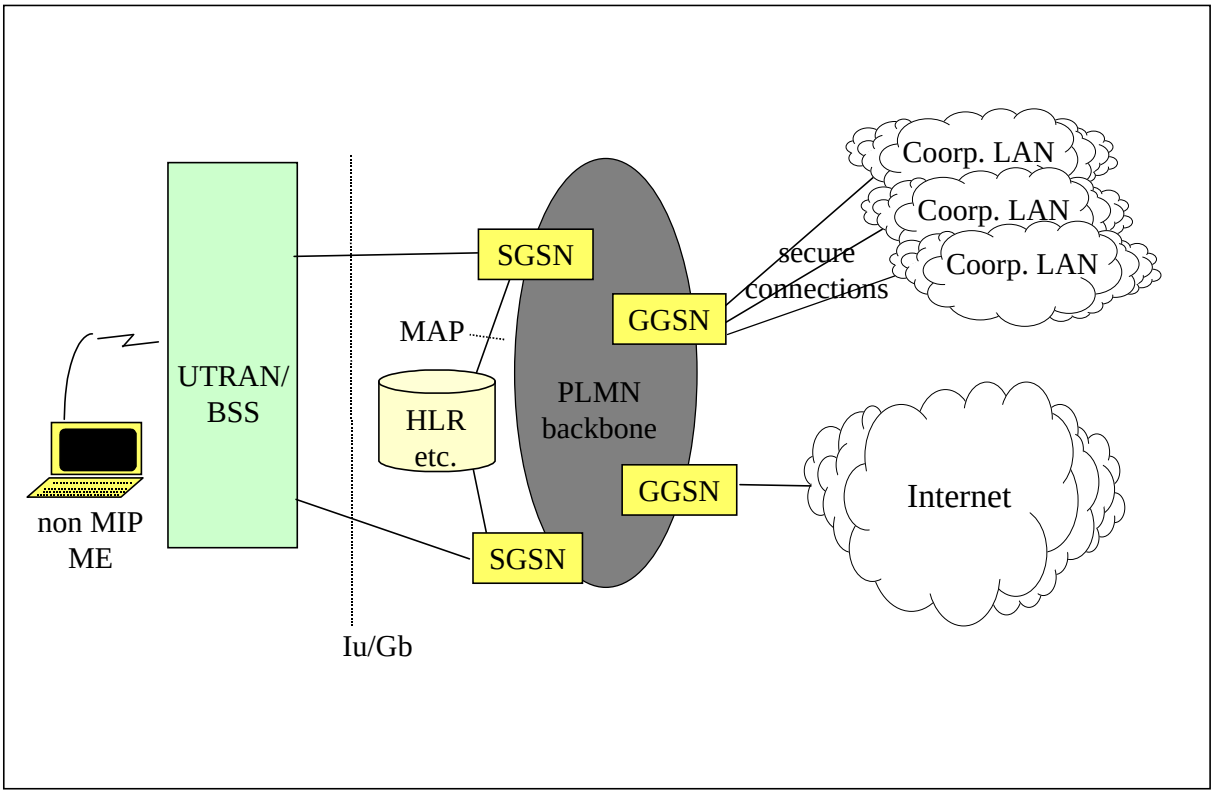

Figure 13. The situation when the PLMN backbone mobility is handled with GTP. The mobile stays with the same GGSN throughout the UMTS/GPRS session.

12.2.1.2 Handling ME's without MIP(+) functionality in a MIP+ based backbone

When migrating from "GTP-mobility" (current GPRS architecture) in a UMTS/GPRS backbone to "Mobile IP+-mobility" (step 3), the ME's need to be enhanced with Mobile IP(+) functionality to handle macro mobility. The upgrade of terminals will not happen overnight and hence a mechanism is needed to handle non-MIP(+) terminals in a MIP+ based backbone.

One solution is "surrogate registrations" (first presented in [TEP]), where the IGSN registers the mobile node on behalf of the mobile node. However, that means that the IGSN needs to know the security parameters that the ME would use for MIP(+) messages if it could handle them. As this security issue is a bit tricky to solve, we should first of all identify which entities and domains that need to be involved in the surrogate registration procedure.

First of all, our problem does not involve any other access than UMTS(packet)/GPRS as it is those systems that need to be backward compatible. The IGSN with its FA is assumed to always be located within the UMTS/GPRS domain.

Second, like the GGSN, the HA can anchor the user traffic throughout the UMTS/GPRS session when reverse tunneling is used [RFC2344].

Further, we assume that if the user does not want to change the ME to handle Mobile IP(+), there is also no interest from the coorporations to change the technology on how to connect their LAN to the PLMN.

Thus, all changes have to occur within the PLMN CN. These are FFS.

12.2.2 Interworking with GPRS PLMNs

It may be the case that a UMTS operator adopting Mobile IP(+) also owns a GPRS network or wants to support subscribers roaming in GPRS networks owned by other operators. In this case the IGSN must support both the G_p and G_n interface.

Suppose that the UMTS operator does not own a GPRS network, but still wants to support roaming of subscribers using GPRS terminals. In this case the UMTS operator can simply own a GGSN offering a G_p interface to operators involved in the roaming agreement.

If the UE uses Mobile IP(+) in an overlay to GPRS, it could use Mobile IP(+) services in the visited GPRS operator, if any. Alternatively, the UMTS operator supporting Mobile IP(+) could choose one of the IGSNs it owns to support the G_p interface, thus integrating Mobile IP(+) functionality and the G_p interface needed to inter operate with the GPRS PLMN B in a single piece of equipment.

In Figure 14 the case of a UMTS operator (PLMN A) who also owns a GPRS network is depicted. The G_p interface is provided by default for subscribers of PLMN A using GPRS only terminals roaming in the GPRS only PLMN B.

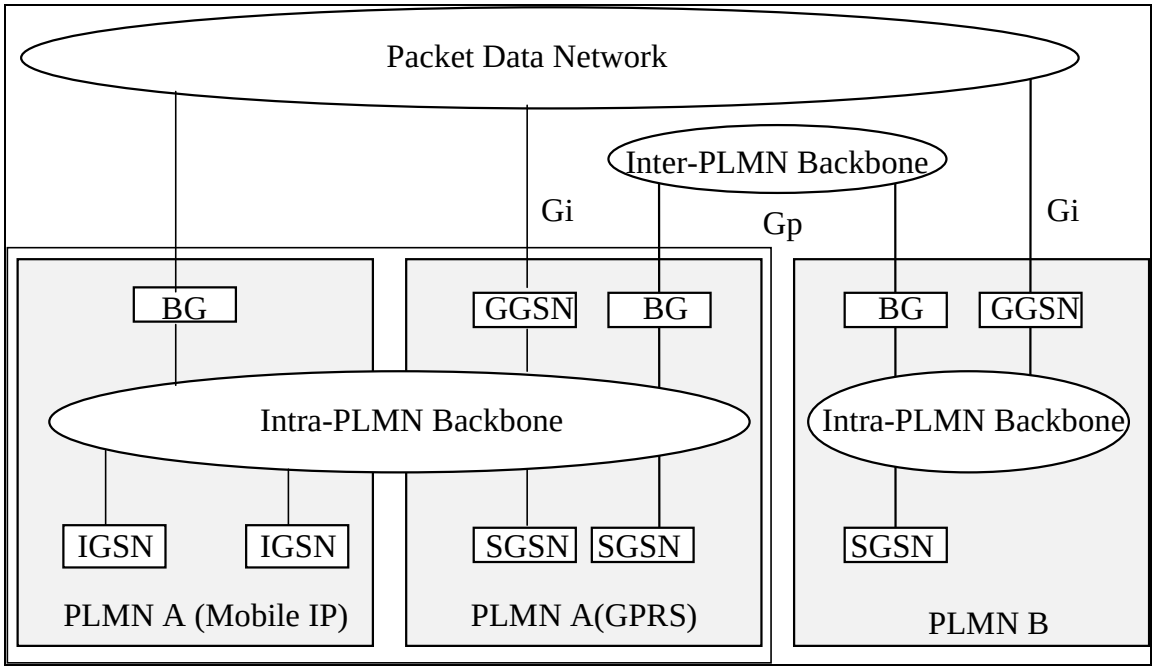

Figure 14 Interoperability with GPRS

12.2.3 Handover GPRS – UMTS – GPRS

12.2.4 Interworking between UMTS/GPRS PLMN's and Mobile IPv6

Like the MIPv4 case, interworking with UMTS and GPRS PLMN's can be provided by running MIPv6 as an overlay in theUMTS/GPRS part of the network.

13 Dependencies on IETF

[*Editor's comment: this should also discuss the differences in the standardization procedure between ETS and IETF and the consequences for introducing Mobile IP in UMTS.*]

13.1 IPv4

IPsec
DHCP
IETF v4 v6?

13.2 IPv6

MobileIP v6 base protocol– is likely to become proposed standard during 1999

14 Enhancements of Standards

14.1 User Equipment

14.2 PDP Context and GTP

14.3 Functionality of SGSN and GGSN

14.4 HLR

[Editor's comment: in case any enhancements are needed]

14.5 Mobile IP

15 Driving Forces

{Editor's comment: this chapter describes the driving forces for moving from GPRS to Mobile IP}

15.1 Mobile IP+ is standardized by the IETF

Since Mobile IP(+) is standardized by the IETF, it benefits now and into the future from being an integral part of the ongoing development of the Internet. This will result in:

- **Ability to take advantage of the economy of scale that the widespread use of Mobile IP+ in the Internet would represent.**
- **Use of standard routers for the Home Agent functionality**
- **Reuse of large parts of standard Foreign Agent functionality**
- **Standard AAA servers** (e.g. RADIUS or DIAMETER) will be used for Authentication, Authorization and Accounting. This allows administration of data users in a consistent way across wireline and wireless public data networks and corporate intranets. Also, operators already running a data network and corporate CIOs will be able to use the same AAA infrastructure for their wireline and their wireless users.
- **Native support of IP level roaming procedures.** Interprovider IP level roaming agreements are based on the use of an NAI (Network Access Identifier) by the user. An extension to support the transport of the NAI in registration requests has been proposed[NAI]. This will allow the mobile node to dynamically obtain a home agent and a home address even when the mobile is not within the domain of its home provider. A particular instance of a home provider is the corporate network, thus the same mechanism will be used for intranet access as for Internet access.

15.2 Mobile IP(+) is an end-to-end solution

Mobile IP(+) supports data users mobility while providing access to remote networks equipped with Home Agent (HA) functionality.

Other approaches (e.g. GPRS/GTP) to supporting data users mobility will not support access to remote networks unless complemented by other solutions (for GTP to be end-to-end the corporation would have to buy a PLMN specific piece of equipment, namely a GGSN, whereas a HA is not PLMN specific, since wireline users could make use of it).

15.3 Mobile IP(+) can support cellular and non cellular access

Mobile IP(+) is not designed for a particular kind of wireless access technology. This flexibility allows sharing of network resources for the support of a diversity of access technologies, both wireline and wireless.

15.4 Mobile IP(+) does not impact location registers

Data user mobility support stands on its own, meaning that the information required to route packets is managed independently of the information used to locate and authenticate a UMTS user.

16 Potential

17 Pros and Cons

+ optimised routing in the CN between e.g. two mobile terminals

+ mainstream IP equipment can be used to a larger extent

+ mobility handling compatible with fixed networks

+

18 Comparison with GPRS

{*Editor's comment: Issues to consider*

- *Time-to-market for new IP services which are dependent on IP network features (QoS, …)*
- *Cost for deployment, operation and maintenance*
- *Security*
- *Compatibility with the non-UMTS environment*
- *If deploying MobileIP(+) on top of GPRS, both GTP MM and MobileIP(+) have to be handled*

}

This contribution provides a brief comparison between GTP/GPRS and a Mobile IP+ approach to data users mobility support in UMTS.

Comparison of Mobile IP+ with GTP/GPRS

The goal of this section is to perform a comparison between GTP/GPRS and an approach to data users mobility support based on IETF standards ([RFC2002] plus the other drafts currently defining for instance how to extend IP mobility support to interact with AAA and how to provide roaming support).

Comparison item	**GTP/GPRS**	**IETF standards (mobile IP+)**
QoS (intra UMTS operator network)	Based on traffic engineering	Based on traffic engineering
QoS (end to end, that is extending also outside the UMTS PLMN)	Based on IETF QoS Standards	Based on IETF QoS standards

Loss of packets during Hand Over	No loss of packets at inter SGSN HO.	Loss of packets at inter IGSN HO may occur. Use of multiple active registrations could solve the problem, but that would imply sending a duplicate stream of packets to two FA. Route optimization draft introduced a smooth HO procedure. A UMTS level mechanism could be defined. The issue is for further study.
Remote network access	Requires interworking at the Gi interface with a compulsory tunneling mechanism or Mobile IP+ itself. Voluntary tunneling techniques are inefficient over the radio interface, since the tunnel terminates at the mobile node.	Native support for remote network access is provided by IETF Mobile IP+ protocols. The remote network, obviously, must support Mobile IP+ in CPE based scenarios.
AAA (Authentication, Authorization and Accounting)	Use of classic GSM procedures for intra-GPRS-PLMN and inter-GPRS-PLMN operation. Interworking with standard IETF procedures required in order to access non PLMN networks	Wireless access uses it's own specific AAA procedures (e.g. GSM procedures) Mobile IP+ uses standard IETF procedures (e.g. RADIUS or, in the future, DIAMETER).
IP level roaming (e.g. access to a remote Home ISP AAA info in order to keep a single formal customer-vendor relationship with it while roaming across different networks)	Need to use the same IETF protocols as Mobile IP+. The mobile station is therefore required to submit a Network Access Identifier. GSM TS 09.61 should be updated to take this into account.	IETF AAA infrastructure is reused (i.e. Mobile IP+ will not use ad hoc mechanisms). The user identity and the Home provider are conveyed by a Network Access Identifier (NAI) submitted in the Mobile IP+ Registration Request.
Security issues when access to the Internet is provided directly by the UMTS operator	GGSN and SGSN trust each other GTP tunnels avoid access to critical network resources. Protection of the GGSN from denial of service attacks is necessary.	HA and FA trust each other (they are located in the UMTS operators network) The mobile terminal must be authenticated by the HA in order to avoid redirection attacks. Static filtering rules at the termination of the RAN logical link and compulsory tunnels can be used to protect critical network resources Protection of the HA from Denial of service attacks is necessary.
Security issues when access to remote networks is provided	IP level authentication of messages to be exchanged with the remote NAS/HA is necessary. Interaction with data network level AAA necessary. Data confidentiality and integrity with IPSEC	Interdomain operation and security are granted by using AAA extensions to Mobile IP Data confidentiality and integrity with IPSEC
Decoupling of data network identity authentication and UMTS network identity	Provided only in case dial-up access or voluntary tunneling is used.	Built in the model. UMTS bearer level authentication and data network level authentication are separate.

authentication.		
Multiprotocol support	Yes	Yes, with GRE encapsulation used for MIP tunnels.
Optimised for IP in the core transport network	No	Yes (minimal encapsulation in the core network reduces overhead, IP standard AAA mechanisms will be used)
X.25 support (is it a requirement for 3G?)	Yes	No
Overhead over the RAN	Only network layer PDU is transported over the RAN	Only the payload packet of MIP tunnels is transported over the RAN in FA based MIP. Thus no additional overhead if compared to GTP/GPRS.
Likely to be used in intranets	No	Yes
Likely to be used in wireline environments	No	Yes
IETF standards will evolve taking it into account	No	Yes
Available in standard routers	No	Yes
Likely to be deployed Internet-wide, thus economy of scale	No	Yes
Likely to be used in non cellular wireless access	No	Yes
Mobile terminated “data calls”	Only with static address assignment	Currently only if the mobile node has registered with the HA and it can be paged. Directories will enable sophisticated mobile terminated data services, when associated with an E.164 to IP mapping infrastructure currently being defined by the IETF and TIPHON
Intersystem UMTS/GSM handover	Performed by using a common GGSN and possibly the same or different SGSNs	Performed by running MIP+ in overlay to GPRS

19 Summary

20 Open Issues

Additional IETF and ETSI standardization efforts are required. Issues to be addressed include [*Editor’s comment: to be updated as this document progresses*]:

- **Charging** information collection.
- **Evolution from 2G systems to 3G systems** based on mobile IP+.
- **Lossless inter IGSN handover** procedures.
- **How to support incoming data calls** (E.164 to IP address resolution mechanisms are likely to be needed, and is an item of standardization in the IETF and in TIPHON).
- **The AAA mechanism for the Internet** is currently being standardized. At the present time RADIUS is the standard, but an evolution of this standard to DIAMETER is likely.
- **Interdependencies between ETSI and IETF standardization process.** Actions are required in order to clarify how to minimize the time required to use an IETF standards track protocol in ETSI specifications.

21 Conclusions

Annex A (informative): Mobile IP

[editor's comment: contribution from CSELT references needs to be added]

A.1 Basic architecture

The basic assumption underlying the standardization activities of the "mobileip" workgroup is that the mobile terminal must be able to communicate using the same IP address at all times, regardless of its point of access to the Internet. If this were not the case, the active TCP sessions (positively identified by the TCP port number and by the IP source and destination addresses) would be broken off each time the mobile terminal moves from one IP subnet to another, and it would not be possible to guarantee service continuity and ensure that movement is completely transparent to the applications.

Like any conventional non-mobile station, each mobile terminal is thus permanently assigned an IP *home address* belonging its original or home network. The home address remains unchanged as the mobile terminal's location varies, and any packet addressed to it is routed to the home network.

When the mobile station is connected to the *home subnet*, it behaves like any non-mobile station, given that it has a logic interface configured with the *home address* and can be reached through normal IP routing.

When the mobile station leaves its home subnet, on the other hand, it can no longer be reached on the basis of its home address alone, but must be assigned an address belonging to the visited IP subnet, called the *care-of address*. The care-of address positively identifies the instantaneous location of the mobile terminal and may be:

- The address of a router (*foreign agent*) belonging to the visited subnet, which manages traffic forwarding to the mobile terminal.
- An address acquired directly by the mobile terminal through an autoconfiguration mechanism, in which case the term *co-located care-of address* is used.

The mobility management protocol is organized so that the mobile terminal can continue to communicate using its home address even when it is away from its home subnet. To this end, one of the routers connected to the home subnet must be configured to act as a *home agent*.

The mobile terminal is required to register its care-of address with the home agent whenever it moves from one IP subnet to another. Thanks to this mechanism, the home agent can keep the look-up table of home addresses and the corresponding care-of addresses up to date.

Other stations do not know the mobile terminal's location (at least to begin with) and thus can only send packets to its home address. Through normal IP routing, these packets reach the home subnet where they are intercepted by the home agent, which sends them to the mobile terminal by means of a *tunneling* mechanism. The mobile node, on the other hand, can answer the transmitting station directly, using its home address as the source address.

The resulting communication scenario is illustrated in Figure A.1. The only substantial difference between the solutions proposed for IPv4 and for IPv6 consists in the fact that in IPv4 traffic forwarding to the mobile terminal is almost always managed through a foreign agent, whereas in IPv6 the foreign agent no longer exists and it is assumed that the mobile terminal is always able to acquire a co-located care-of address belonging to the visited subnet. The foreign agent, in fact, was conceived expressly to reduce the demand for IP addresses by sharing the same care-of address amongst several mobile terminals. The foreign agent thus made it possible to avoid aggravating the problem of limited IPv4 addressing space, but is no longer needed with IPv6, which has a virtually unlimited addressing space and efficient autoconfiguration mechanisms[5] which the mobile terminal can use to acquire a valid address in the visited subnet.

---

[5] Autoconfiguration of an IPv6 station can be accomplished in two different ways, called respectively "stateful autoconfiguration" and "stateless autoconfiguration". Stateful autoconfiguration takes place under the control of a centralized server and uses the IPv6 version of the DHCP (Dynamic Host Configuration Protocol). Stateless autoconfiguration, on the other hand, simplifies network administration enormously, as it enables the hosts to configure the IPv6 addresses of their interfaces independently starting from the information published by neighboring routers through the Neighbor Discovery (ND) protocol.

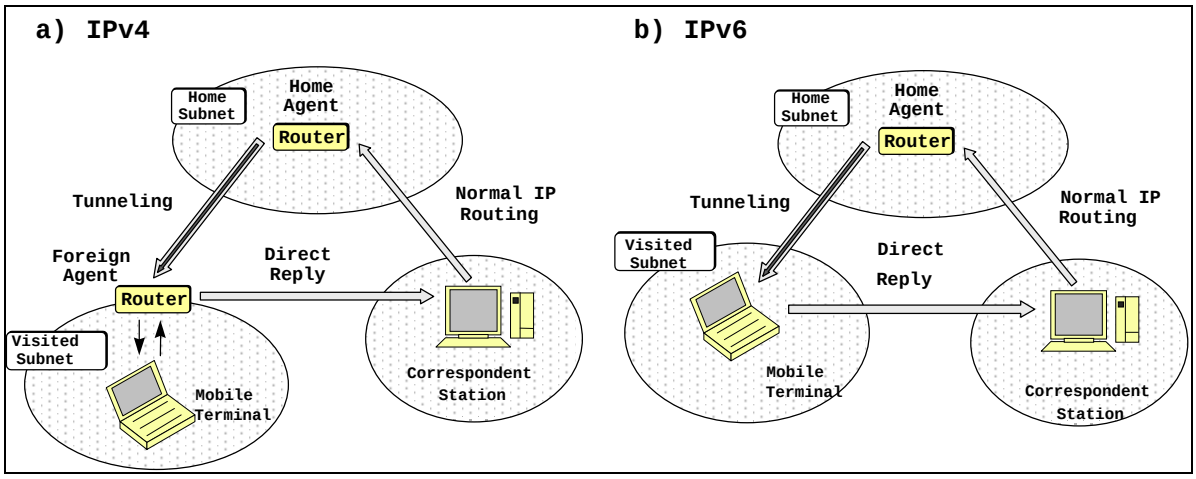

Figure A.1. Basic architecture for supporting IP mobility

A.2 Route optimization

The operating mode illustrated in the preceding paragraph is extremely simple and enables a mobile terminal to continue to communicate using its own home address even when it is away from its home subnet. The drawback of this consists of the fact that all packets addressed to the mobile terminal must necessarily transit through its home subnet before reaching destination, which makes for:

- an additional load in the home subnet; and
- a longer latency time in transferring traffic to destination.

For this reason, the “mobileip” workgroup is analyzing a possible extension (*Route Optimization*) to the terminal mobility support protocol based on the introduction of a mechanism which enables any station with which an IP level data transfer is in progress (the correspondent node), and not just the home agent, to learn the care-of address associated with the mobile terminal and to use it subsequently to reach the mobile terminal without passing through its home network.

The “mobileip” workgroup is specifying a Route Optimization protocol for both IPv4 mobility and IPv6 mobility. By contrast with the basic architecture for supporting IP mobility on the Internet, the solutions proposed for IPv6 in this case feature far from negligible differences with respect to those envisaged for IPv4, as the new capabilities supported by the new-generation IP protocol have permitted several architectural options which are not feasible with the current version of the IP protocol.

A.2.1 The solution proposed for IPv4

In the Route Optimization protocol specified for IPv4, the home agent indicates the mobile terminal’s care-of address to the correspondent node when the terminal is away from its home subnet. After receiving a datagram intended for the mobile terminal, the home agent performs a tunneling operation to the associated care-of address, and also sends an appropriate Binding Update message to the correspondent node. The correspondent node can subsequently send the traffic intended for the mobile terminal directly to its care-of address by means of a tunneling mechanism, and sets up an optimized route which makes it possible to avoid passing through the home agent (Figure A.2).

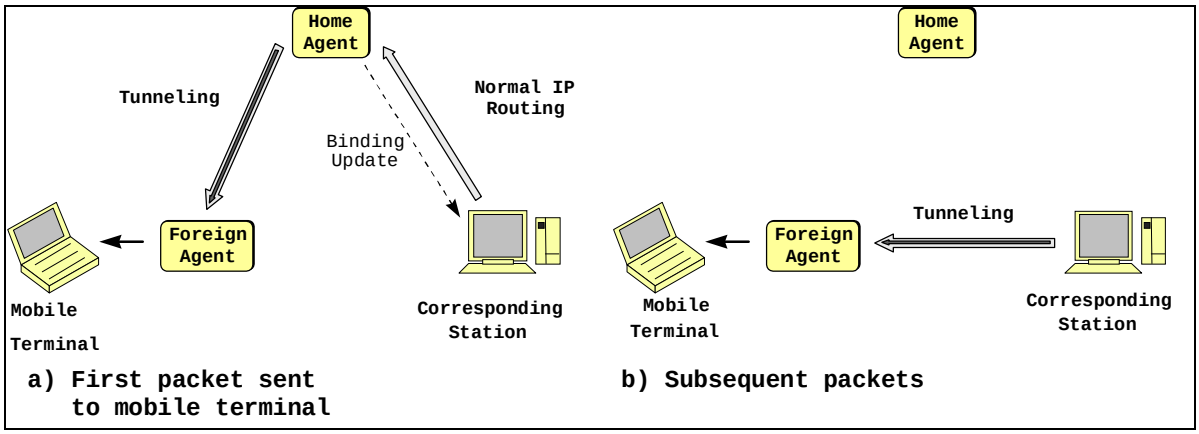

Figure A2. *Route Optimization* in IPv4

On its own, however, this procedure is not sufficient to guarantee permanent optimization of the route to the mobile terminal. A mechanism is also required whereby the correspondent station can learn the mobile terminal's new location every time it moves in the Internet.

Thus, in the IPv4 Route Optimization protocol, the mobile terminal, after moving in a new subnet, can also communicate its new care-of address to its previous foreign agent. In this way, when a correspondent node attempts to reach the mobile terminal using a care-of address which has become obsolete, the foreign agent which receives transmitted traffic can forward it to the mobile terminal's new location using a tunneling mechanism. At the same time, the foreign agent sends the home agent a Binding Warning message, asking that the correspondent station be notified of the mobile terminal's new care-of address by means of an appropriate Binding Update message, thus making it possible to restore an optimized route between source and destination (Figure A.3)

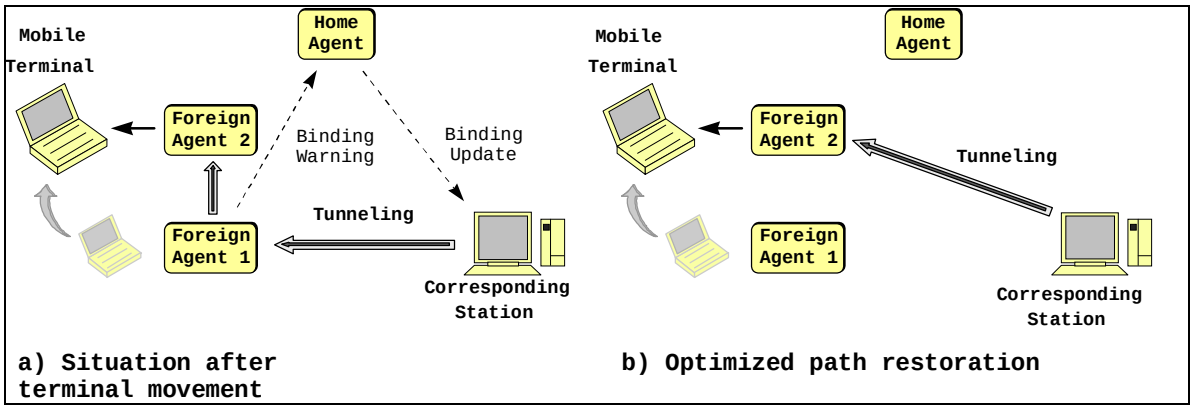

Figure A.3. Mobile terminal movement with notification to the previous foreign agent

If a correspondent node attempts to reach the mobile terminal using an obsolete care-of address and the foreign agent which receives the transmitted traffic does not know the mobile terminal's new location (either because it has not been notified of this location, or because the information has already been removed from its cache), the Route Optimization protocol suggests that each packet addressed to the mobile terminal be re-routed to the corresponding home agent by means of a tunnel. Once it has reached the home agent, this type of traffic is handled in exactly the same way as any other message addressed to the mobile terminal, and is thus sent to the corresponding care-of address through a new tunnel. At the same time, a Binding Update message is transmitted to the correspondent terminal, once again making it possible to restore a direct path between source and destination (Figure A.4).

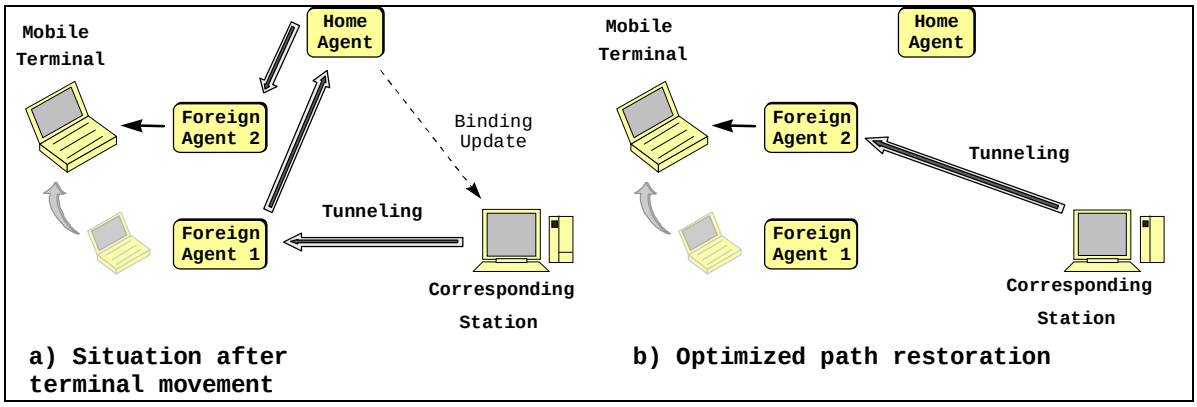

Figure A.3. Mobile terminal movement without notification to the previous foreign agent

The Route Optimization mechanism specified for IPv4 has the advantage of minimizing signaling traffic carried by the portion of the network between the mobile terminal and the foreign agent, as all of the Binding Update messages addressed to the correspondent node are transmitted by the home agent rather than directly by the mobile terminal. This is an extremely important feature, given that the Binding Update messages are coded in UDP packets which are separate from data traffic and thus introduce an overhead that can become unacceptable on a wireless connection such as that between the mobile terminal and the foreign agent.

A.2.2 The solution proposed for IPv6

By contrast with the procedure used in IPv4, the Route Optimization protocol specified for IPv6 requires that the Binding Update messages intended for the correspondent node be transmitted directly by the mobile terminal every time the latter moves in the Internet (Figure A.5). This simplifies the protocol enormously and drastically reduces the latency time before the correspondent node can acquire the mobile terminal's new care-of address.

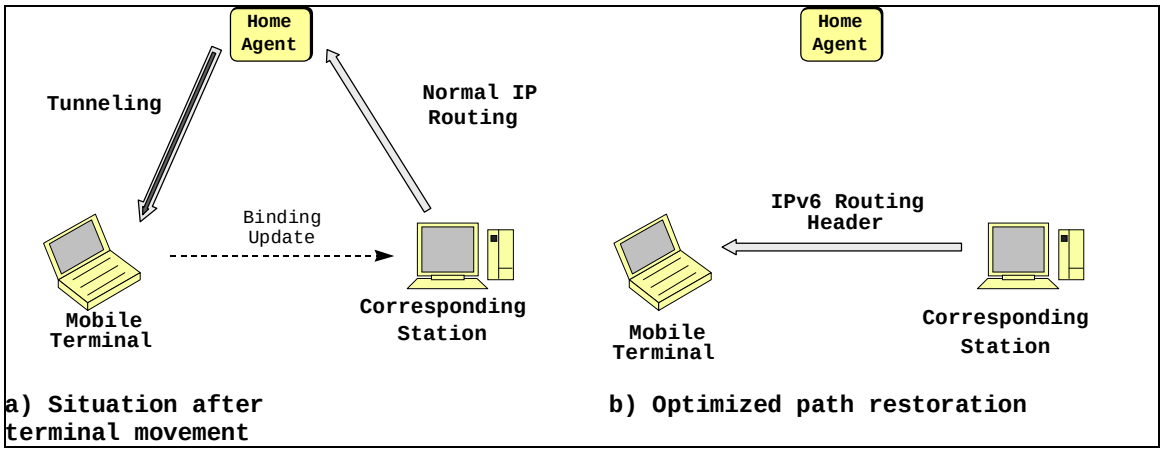

Figure A.4. *Route Optimization* in IPv6

A solution of this type, which was ruled out in IPv4, becomes feasible with the new-generation IP protocol, given that the Binding Update messages are coded in appropriate IPv6 extension headers[6] and can be included in the same packets which carry effective traffic between the mobile terminal and the correspondent or between the mobile terminal and the home agent. This minimizes signaling traffic, making it acceptable to transport it on the network even when the mobile node is connected to the Internet via a wireless interface, which can have a much lower bandwidth than conventional cabled networks and a high error rate.

In addition, while in IPv4 the traffic transmitted by the correspondent node to the mobile terminal is sent directly to its care-of address by means of a tunneling mechanism, with IPv6 the same result is achieved using a *Routing Header*, i.e. a

---

6 In IPv6, the "options" are no longer an integral part of the IP header, as each is memorized in a separate header (called the extension header) located between the IPv6 header and the header of the overlying transport layer (e.g. TCP or UDP). In particular, the options which must be analyzed only by the final destination are specified in a special extension header called the destination options header, which is also used to transport Binding Update messages for IPv6 mobility management.

special extension header that forces the datagram to follow a predetermined route. The advantage of this consists of the fact that the Routing Header introduces a smaller overhead in each packet than would “IPv6 in IPv6” tunneling, which makes it necessary to introduce a new IPv6 header in each packet transmitted to the mobile terminal.

A.3 Security aspects

Applying IP mobility support protocols in the Internet dependes critically on security management.

First of all, the home agent must be able to authenticate messages it receives from the mobile terminal in order to ensure that a false registration cannot cause all of the traffic intended for the mobile terminal to be re-directed to an IP subnet other than that effectively visited.

Moreover, further complications emerge when the Route Optimization mechanism is used, given that in this case each correspondent node must be able to authenticate the Binding Update messages received from the mobile terminal (IPv6) or from its home agent (IPv4) respectively. In fact, while we can readily accept that the mobile terminal and its home agent, which are normally stations belonging to the same organization, can be configured manually with a shared secret key used for the authentication algorithms, it is much harder to imagine a similar scenario between the mobile terminal and the correspondent, or between the home agent and the correspondent node, given that the latter may be any Internet station. For this purpose, a mechanism with an appropriate level of security must be developed which enables two stations to agree dynamically on the secret key to be used. A mechanism of this kind has not yet been fully specified by the IETF, though the attention given to this problem by the “ipsec” workgroup is considerable.

Annex B (informative): IPv4 versus IPv6

{*Editor's comment: general issues, not specific to MobileIP*}

Annex C (informative): IPsec and Digital Certificates

IPsec is an IETF standard protocol suite that enables authentication and encryption at the network (IP) layer. It also has functions for automatic key management. IPsec has two modes, tunnel mode and transport mode. In transport mode the receiving node is also the end node unlike in tunnel mode where the receiving node forwards the IPsec packet to the end node after lifting it out of the tunnel.

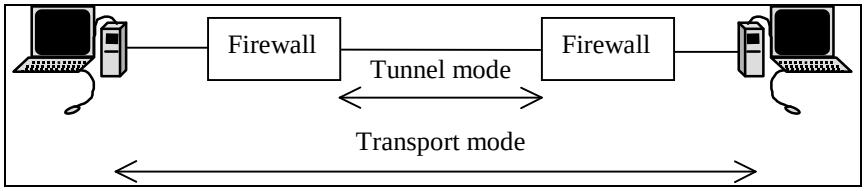

Figure C.1. IPsec Tunnel mode and Transport mode

C.1 IPsec Authentication

There are four different ways of user authentication in IPsec:

- Authentication with digital certificates. The two corresponding nodes exchange digital certificates to authenticate themselves. This is the most general method of authentication since it does not require the two nodes to know anything about each other prior to communication establishment.
- Authentication with public keys. A nonce and the initiator's identity encrypted with the receiver's public key are transmitted to the receiver. If the receiver can respond with a correct hash of the nonce, he is authenticated. This method requires that the two corresponding nodes know each other's public keys and are sure that these are the proper ones.
- Variant on authentication with public keys. Same as above with the exception that the initiator's identity is encrypted in a symmetric fashion using a key derived from the nonce. The nonce is still encrypted with the receiver's public key.
- Authentication with a shared secret. The two corresponding nodes have a shared secret, a key, which they use for authentication. This method must be supported by all IPsec implementations but is only recommended for test and demonstration use.

C.2 Digital certificates

Anyone who wishes to send an encrypted message, applies for a digital certificate from a *Certificate Authority* (CA). The CA issues an encrypted digital certificate, which contains the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message. He should also verify that the certificate really is issued by the actual CA. Thereafter, the receiver obtains the sender's public key and identification information held within the certificate.

The most widely used standard for digital certificates is X.509. Unfortunately, the X.509 standard is not really a standard, but merely an ITU recommendation. This means that different software manufactures may have different X.509 implementation. An example of that is Netscape and Microsoft, who both uses X.509 certificates for their SSL implementations in web servers and browsers. However, an X.509 certificate generated by Microsoft may not be readable by a Netscape product, and vice versa.

Annex D (informative): Detailed Step 3 Procedures

{*Editor's comment: These procedures will be explained in a more readable format in the main body of the report.It is not yet decided to which extent the user plane of the GTP protocol is needed.* }

A detailed description of RA update procedures and UMTS SRNS relocation is provided below. Note that in the next sections, wherever the word 'SGSN' is used, it must be considered as a SGSN functionality. We do not imply or suggest the IGSN be an SGSN only.

D.1 Inter IGSN ROUTING AREA update for terminals using mobile IP SERVICE.

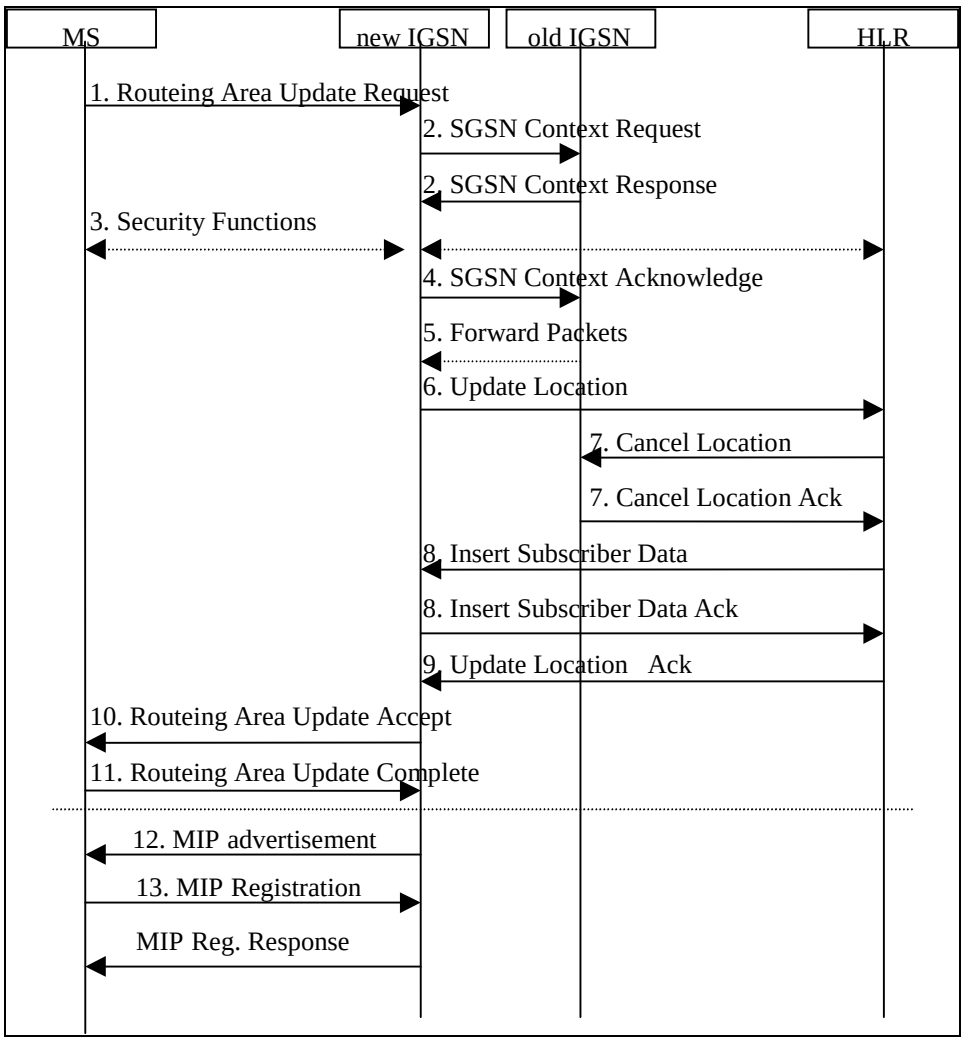

Figure D1

1) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the new SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell form where the message was received before passing the message to the SGSN.

2) The new SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old SGSN to get the MM and PDP contexts for the MS. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN responds with SGSN Context Response (MM Context, PDP Contexts, LLC Ack). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN stores New SGSN Address, to allow the old SGSN to forward data packets to the new SGSN. LLC Ack contains the acknowledgements for each LLC connection used by the MS. Each PDP Context includes the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled via mobile IP tunnel to the HA. The old SGSN starts a timer and stops the transmission of N-PDUs to the MS.

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.

4) The new SGSN sends an SGSN Context Acknowledge message to the old SGSN. This informs the old SGSN that the new SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the HLR are invalid. This triggers the MSC/VLRand the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure. If the security functions do not authenticate the MS correctly, then the routing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.

5) The old SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new SGSN. Additional N-PDUs received before the timer described in step 2 expires are also duplicated and tunnelled to the new SGSN. N-PDUs that were already sent to the MS and that are not yet acknowledged by the MS are tunnelled together with the number of the LLC frame that transferred the last segment of the N-PDU. No N-PDUs shall be forwarded to the new SGSN after expiry of the timer described in step 2.

6) The new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.

7) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, then the old SGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old SGSN to complete the forwarding of N-PDUs. It also ensures that the MM and PDP contexts are kept in the old SGSN in case the MS initiates another inter SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).

8) The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription the MS is rejected, the SGSN rejects the Routeing Area Update Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted Due To Regional Subscription) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

9) The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.

10) The new SGSN validates the MS's presence in the new RA. If due to regional, national or international restrictions the MS is not allowed to attach in the RA or subscription checking fails, then the new SGSN rejects the routeing area update with an appropriate cause. If all checks are successful then the new SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new SGSN and the MS. The new SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, LLC Ack, P-TMSI Signature). LLC Ack contains the acknowledgements for each LLC connection used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.

11) The MS acknowledges the new P-TMSI with a Routeing Area Update Complete (P-TMSI, LLC Ack). LLC Ack contains the acknowledgements for each LLC connection used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If LLC Ack confirms reception of N-PDUs that were forwarded from the old SGSN, then these N-PDUs shall be discarded by the new SGSN. LLC and SNDCP in the MS are reset locally.

12) Over the newly setup link to the mobile, a Mobile IPAgent Advertisement is sent. This is triggered in some way not specified here.
It is sent only to the mobile performing the RA update. This is sent in such a way that subnet prefix based movement detection algorithm the Mobile IP spec [RFC2002] suggests triggers an immediate mobile IP registration (i.e. by making sure no two FA in the PLMN send advertisements with identical subnet prefixes).

13) The normal MIP registration is performed. This will be periodically repeated according to timers negotiated in the registration, in order to keep the MIP session alive.

In the case of a rejected routeing area update operation, due to Routeing Area restrictions, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

If the timer described in step 2 expires and no Cancel Location (IMSI) was received from the HLR, then the old SGSN shall stop forwarding N-PDUs to the new SGSN.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

D.2 Intra IGSN RA update for terminals using mobile IP Service.

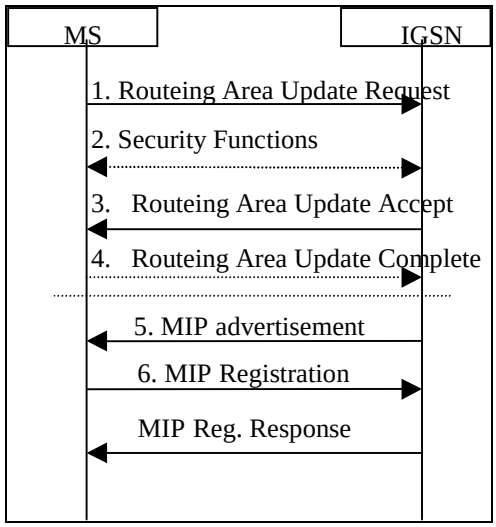

Figure D2.

1) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the SGSN. Update Type shall indicate RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN, see GSM 08.18.

2) Security functions may be executed. These procedures are defined in subclause "Security Function".

3) The SGSN validates the MS's presence in the new RA. If due to regional, national or international restrictions the MS is not allowed to attach in the RA or subscription checking fails, then the SGSN rejects the routeing area update with an appropriate cause. If all checks are successful then the SGSN updates the MM context for the MS. A new P-TMSI may be allocated. A Routeing Area Update Accept (P-TMSI, P-TMSI Signature) is returned to the MS.

4) If P-TMSI was reallocated, the MS acknowledges the new P-TMSI with Routeing Area Update Complete (P-TMSI).

5) If the New routing area is under the domain of a new FA (e.g. for load sharing reasons) then a Mobile IPAgent Advertisement is sent. This is triggered in some way not specified here.
It is sent only to the mobile performing the RA update. This is sent in such a way that subnet prefix based movement detection algorithm the Mobile IP spec [RFC2002] suggests trigger an immediate mobile IP registration (i.e. by making sure no two FA in the PLMN send advertisements with identical subnet prefixes).

6) The regular MIP registration is performed. This will be periodically repeated according to timers negotiated in the registration, in order to keep the MIP session alive.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

D.3 The UMTS case

When the mobile is in idle mode, the procedures defined for GPRS works the same way in UMTS.

When the mobile is in connected state, the following SRNS relocation procedure takes place (the case that involves change of SGSN is described).

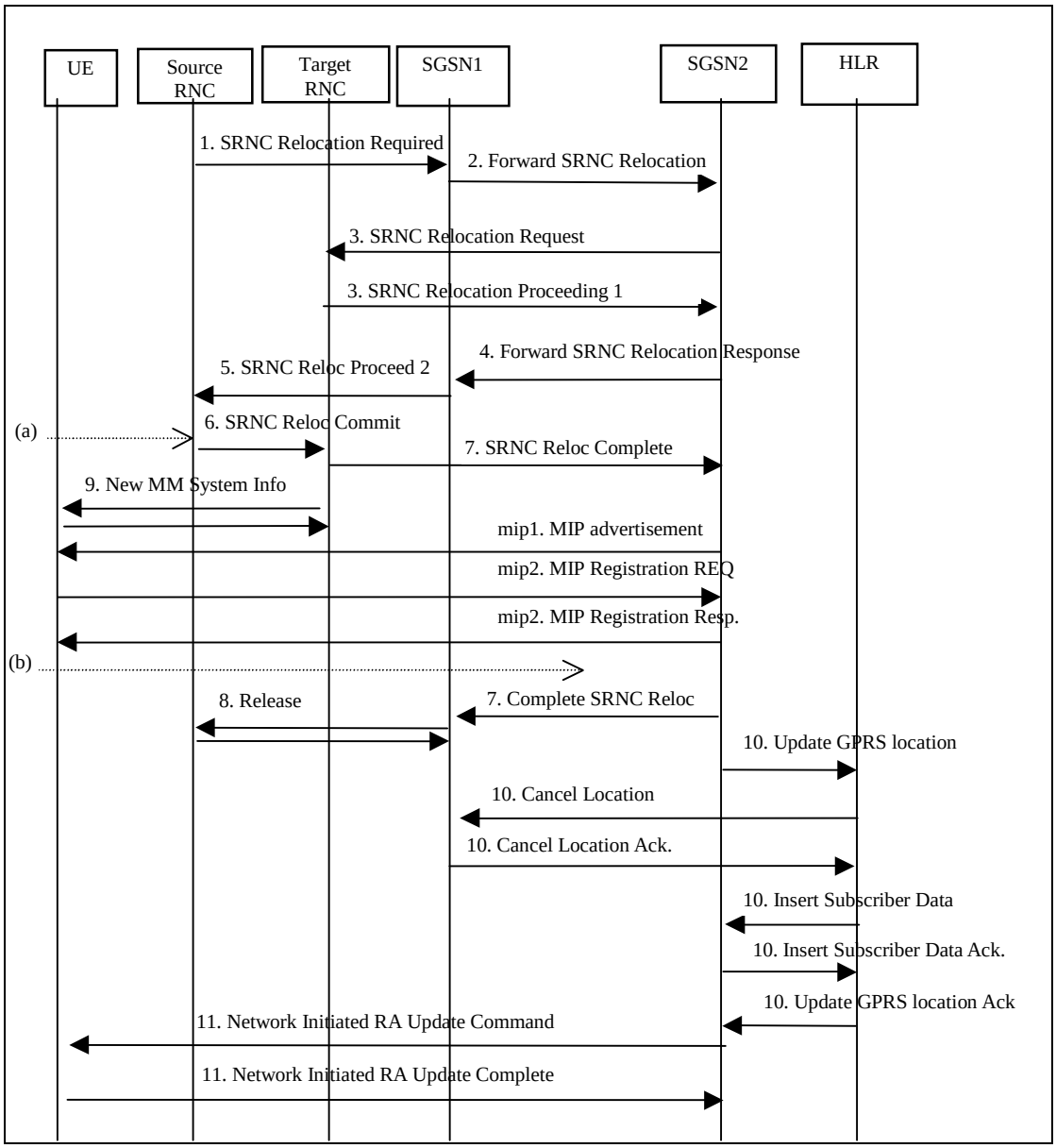

Figure D3.

1) UTRAN makes the decision to perform the Serving RNC relocation procedure. This includes decision on into which RNC (Target RNC) the Serving RNC functionality is to be relocated. The source SRNC sends SRNC Relocation required messages to the SGSN1. This message includes parameters such as target RNC identifier and an information field that shall be passed transparently to the target RNC.

2) Upon reception of SRNC Relocation required message the SGSN1 determines from the received information that the SRNC relocation will (in this case) result in change of SGSN.
The SGSN will then send a Forward SRNC relocation request to the applicable SGSN, SGSN2, including the information received from the Source RNC and necessary information for the change of SGSN (e.g. MM context, PDP context).

3) The SGSN2 will send a SRNC Relocation Request message to the target RNC. This message includes information for building up the SRNC context, transparently sent from Source RNC (e.g. UE id., no of connected CN nodes, UE capability information), and directives for setting up Iu user plane transport bearers.
When the Iu user plane transport bearers have been established, and target RNC completed its preparation phase, SRNC Relocation Proceeding 1 message is sent to the SGSN2.

4) When the traffic resources between target RNC and SGSN2 has been allocated and the SGSN2 is ready for the SRNC move, then the Forward SRNC Relocation Response is sent from SGSN2 to SGSN1. This message indicates that necessary resources have been allocated for the SRNC relocation.

5) When the Forward SRNC Relocation Response has been received in the SGSN1, the SGSN1 indicates the completion of preparation phase at the CN side for the SRNC relocation by sending the SRNC Relocation Proceeding 2 message to the Source RNC.

6) When the source RNC has received the SRNC Relocation Proceeding 2 message, the source RNC sends a SRNC Relocation Commit message to the target RNC. The target RNC executes switch for all bearers at the earliest suitable time instance.

7) Immediately after a successful switch at RNC, target RNC (=SRNC) sends SRNC Relocation Complete message to the SGSN2. The SGSN will also send a Complete SRNC Relocation towards the SGSN1.

8) At reception of the Complete SRNC Relocation, SGSN1 will send a release indication towards the Source RNC. This will imply release of all UTRAN resources that were related to this UE.

Mip 1) Over the newly setup link to the mobile (the target RNS is now acting as SRNS) a Mobile IP Agent Advertisement is sent. This is triggered in some way not specified here .
It is sent only to the mobile performing the SRNS relocation. This is sent in such a way that subnet prefix based movement detection algorithm the Mobile IP spec [RFC2002] suggests triggers an immediate mobile IP registration (i.e. by making sure no two FA in the PLMN send advertisements with identical subnet prefixes).

Mip 2) The normal MIP registration is performed. This will be periodically repeated according to timers negotiated in the registration, in order to keep the MIP session alive.

9) When the target RNC is acting as SRNC, it will send New MM System Information to the UE indicating e.g. relevant Routing Area and Location Area. Additional RRC information may then also be sent to the UE, e.g. new RNTI identity.

10) The SGSN2 informs the HLR of the change of SGSN by sending Update GPRS location (IMSI, new SGSN address etc.) to the HLR. The HLR cancels the context in the old SGSN, SGSN1, by sending Cancel Location (IMSI). The SGSN1 removes the context and acknowledges with Cancel Location Ack. The HLR sends Insert subscriber data (IMSI, subscription data) to the SGSN2. The SGSN2 acknowledges with Insert Subscriber Data Ack. The HLR acknowledges the Update GPRS location by sending Update GPRS Location Ack to the SGSN2.

11) At reception of Insert subscriber data from HLR, the SGSN2 will initiate the update of MM information stored in the UE. This is done by sending Network Initiated Routing Area Update Command to the UE. This message will include new RAI, and possible also new P-TMSI. When the UE has made necessary updates it answers with Network Initiated Routing Area Update Complete.

Before point (a), in Figure 19, the connection is established between UE and HA via Source RNC and SGSN1.

After point (b), in Figure 19, the connection is established between UE and HA via Target RNC and SGSN2.

History

Document history		
14 September '98	Version 0.0.1	ToC
22 October 1998	Version 0.0.2	ToC and some text, electronically distributed and discussed in Montreux
05 November 1998	Version 0.1.0	ToC updated according to Montreux discussion (ToC, one traffic case and tutorial on MIP) [editors notes in brackets]
10 December 1998	Version 0.2.0	Annex added (Tdoc1076v2) and contribution, a tutorial, on digital certificates (Tdoc 1046)
14 January 1999	Version 0.3.0	Contributions from Heathrow meeting added Tdocs C-99-090, 056 Revised Contributions: Tdocs C-99- 008, 053, 054, 058, 089
26 February 1999	Version 0.4.0	Document rearranged to include solutions on how to run MIP in overlay to GPRS. Chapter headings added. Text has been moved around but not changed
26 February 1999	Version 0.5.0	Revised versions of Tdocs C-99-055 and Tdocs C-99-057 have been included
12 May 1999	Version 0.6.0	-The following Tdocs have been included S2 M 99 – 004, 013, 014, 017, 018, 019, 020, 022, 026 -Mobile IP changed to Mobile IP+ or Mobile IP(+) where applicable (except appendices). -"Stage" changed to "step"
30 June 1999	Version 0.6.1	Change due to 3GPP template
13 July 1999	Version 0.7.0	• Editorial changes as agreed at the Helsinki meeting • Inclusion of Tdoc S2M99036(step1), 041(step2) • New text and figure section 7.2 as agreed on the S2 mailing list (rev marks for deleted figure not visible) • Inclusion of figure 2 and 4 (tdoc s2m99035) in chapter 7, rev marks for deleted figures not visible) • ME (Mob. Equipm.) is the UMTS term and MS (Mob. Station) the GPRS term for the same thing. Now the entire document uses ME • Tdoc s2m99038v1 inserted in an annex. • Figures and text on traffic cases updated • The following figures are new – either replacing old ones or completely new (revision marks did not always work): figure 1, 2, 3, 4, 5, 6, 7 and 8 • Some smaller editorial changes where applicable • List of abbreviations improved
22 July 1999	Version 0.8.0	• Included Tdocs s2m99053, parts of 046, 047 and parts of 049. • Added a few achronyms
9 September 1999	Version 0.9.0	• Included Tdocs s2m99066 (new text in section 7.3) and s2m99068 (new section 10.2)
6 October 1999	Version 1.0.0	• No changes compared to previous version