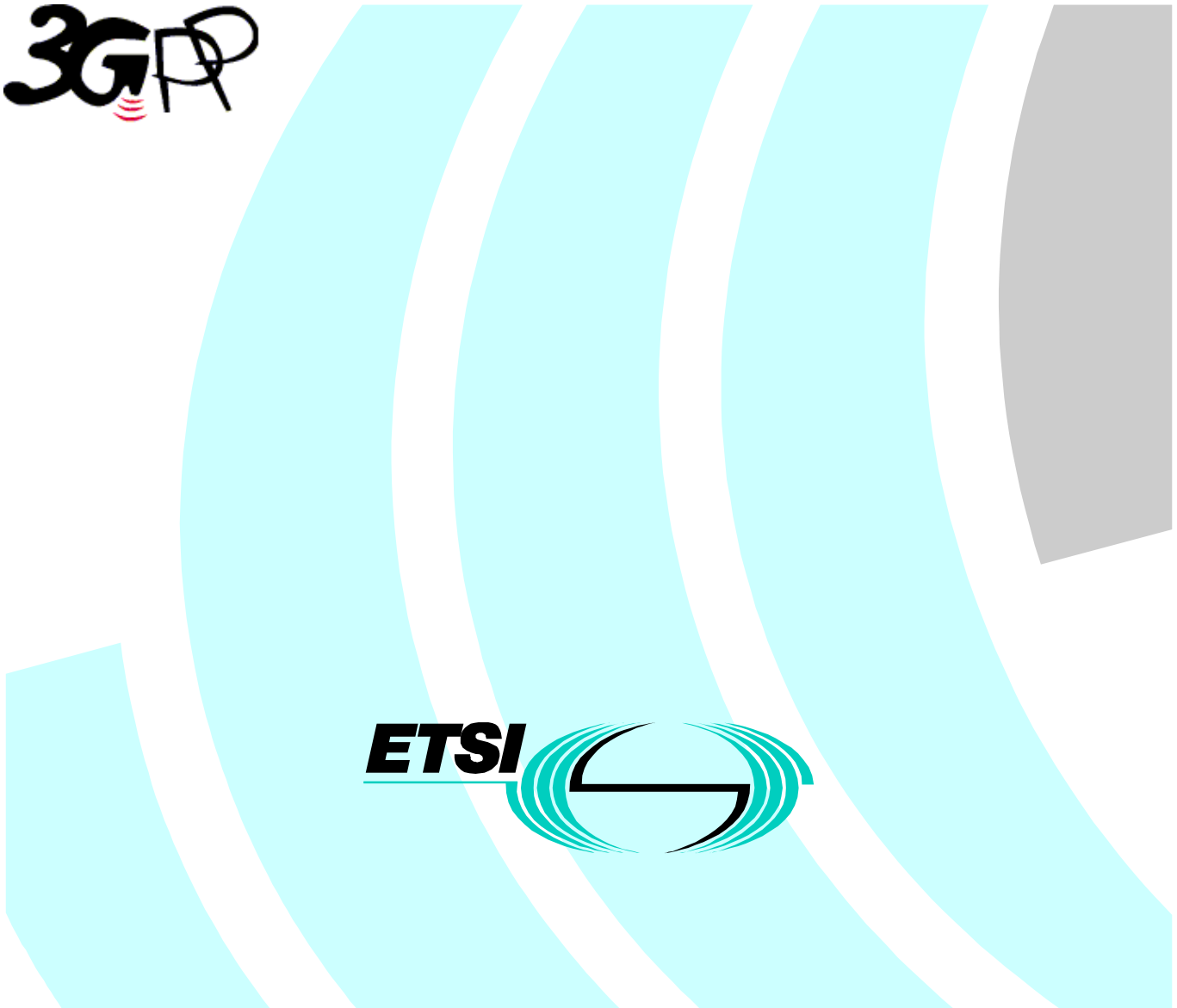
ETSI TR 123 923 V3.0.0 (2001-05)

Technical Report

Universal Mobile Telecommunications System (UMTS);
Combined GSM and Mobile IP mobility handling in UMTS IP CN
(3GPP TR 23.923 version 3.0.0 Release 1999)



Reference
DTR/TSGS-0223923U

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Foreword

This Technical Report (TR) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Report 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 TR, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.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 report;

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 PLMNs 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. Potentially, this would also allow cost savings for operators and a broadening of the market for manufacturers.

The present 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 tunnelling 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.

Conclusions of the technical report is presented in clause 15.

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

1 Scope

The present document contains a feasibility study on using Mobile IP+ as a tunnelling 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 standardisation 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 minimise 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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- For this Release 1999 document, references to documents are for Release 1999 versions.

[1] 3G TS 22.101: "Services Principles".

[2] GSM 03.02: "Digital cellular telecommunications system (Phase 2); Network architecture".

[3] GSM 03.03: "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[4] GSM 02.60: "Digital cellular telecommunications system (Phase 2+);General Packet Radio Service (GPRS); Service description; Stage 1".

[5] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[6] GSM 07.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".

[7] GSM 09.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[8] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM application toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] GSM 12.15: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Charging".

[10] 3G TS 22.115 (V3.3): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Charging and Billing".

[11] GSM 30.01: "Universal Mobile Telecommunications System (UMTS); UMTS baseline document positions on UMTS agreed by SMG".

[12] 3G TS 23.101: "General UMTS Architecture".

[13] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[14] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[15] 3G TS 23.121: "Architectural Requirements for Release 1999".

[16] IETF RFC 1264 (1991): "Internet Engineering Task Force Internet Routing Protocol Standardization Criteria".

[17] IETF RFC 1701 (1994): "Generic Routing Encapsulation (GRE)", S. Hanks.

[18] IETF RFC 1702 (1994): "Generic Routing Encapsulation over IPv4 networks".

[19] IETF RFC 1853 (1995): "IP in IP Tunneling", W. Simpson.

[20] IETF RFC 2002 (1996): "IP Mobility Support", C. Perkins.

[21] IETF RFC 2003 (1996): "IP Encapsulation within IP", C. Perkins.

[22] IETF RFC 2004 (1996): "Minimal Encapsulation within IP", C. Perkins.

[23] IETF RFC 2138 (1997): "Remote Authentication Dial In User Service (RADIUS)", C. Rigney.

[24] IETF RFC 2215 (1997): "General Characterization Parameters for Integrated Service Network Elements", S. Shenker, J. Wroclawski.

[25] IETF RFC 2216 (1997): "Network Element Service Specification Template".

[26] IETF RFC 2344 (1998): "Reverse Tunneling for Mobile IP", G. Montenegro.

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

[28] IETF RFC 2475 (1998): "An Architecture for Differentiated Services", S. Blake.

[29] IETF RFC 2486 (1999): "The Network Access Identifier", B.Aboba, M.Beadles.

[30] ITU-T Recommendation I.112: "Vocabulary of terms for ISDNs".

Work in progress:

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

[32] IETF AAA Working Group, http://www.ietf.org/html.charters/aaa-charter.html

[33] Internet draft, A. Terzis, Editor, RSVP Operation Over IP Tunnels, May 1999. http://www.ietf.org/internet-drafts/draft-ietf-rsvp-tunnel-04.txt

[34] Internet draft, Y. Bernet et al, A Framework for Differentiated Services, February 1999. http://www.ietf.org/internet-drafts/draft-ietf-diffserv-framework-02.txt

[35] Internet draft, Johson and Perkins, "Mobility Support in IPv6", October 1999. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-09.txt

[36] Internet draft, P.Calhoun and C.Perkins, "Mobile IP Network Address Identifier Extension", October 1999. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-mn-nai-05.txt

[37] Internet draft, G. Montenegro, Negotiated Address Reuse (NAR), January 1999, http://search.ietf.org/internet-drafts/draft-montenegro-aatn-nar-01.txt

[38] Internet draft, P.Calhoun, "DIAMETER Base Protocol", October 1999, http://search.ietf.org/internet-drafts/draft-calhoun-diameter-10.txt

[39] Internet draft, C. De Laat et al, "Generic AAA Architecture", http://search.ietf.org/internet-drafts/draft-delaat-aaa-generic-00.txt

[40] Internet draft, S. Glass et al, "Mobile IP Authentication, Authorization, and Accounting Requirements", http://www.ietf.org/internet-drafts/draft-ietf-mobileip-aaa-reqs-00.txt

[41] Internet draft, J. Vollbrecht, "AAA Authorization Application Examples", http://www.ietf.org/internet-drafts/draft-ietf-aaa-authz-samp-00.txt

[42] Internet draft, J. Vollbrecht, "AAA Authorization Framework", http://www.ietf.org/internet-drafts/draft-ietf-aaa-authz-arch-00.txt

[43] Internet draft, Requirements on Mobile IP from a Cellular Perspective, June 1999 (work in progress) http://www.ietf.org/internet-drafts/draft-ietf-mobileip-cellular-requirements-02.txt

[44] ETSI ETR 232 (1995): "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[45] Mobile IP Regionalized Tunnel Management
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-reg-tunnel-01.txt

[46] Mobile IP Challenge/Response Extensions
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-challenge-06.txt
NAI Resolution for Wireless Networks
http://search.ietf.org/internet-drafts/draft-aravamudhan-mobileip-nai-wn-00.txt

[47] Requirements on Mobile IP from a Cellular Perspective
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-cellular-requirements-02.txt

[48] IP Mobility Architecture Framework
http://search.ietf.org/internet-drafts/draft-ietf-mobileip-ipm-arch-00.txt

[49] Transparent Hierarchical Mobility Agents (THEMA)
http://search.ietf.org/internet-drafts/draft-mccann-thema-00.txt

[50] Mobile IP Authentication, Authorization, and Accounting Requirements
http://search.ietf.org/internet-drafts/draft-ietf-aaa-mobile-ip-req-00.txt

[51] Security terms are defined in [ETR232].

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Accounting [43**]:** act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.

Agent Advertisement [20**]:** advertisement message constructed by attaching a special Extension to a router advertisement [5] message.

Authentication [43**]:** act of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication).

Authorisation [43**]:** act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

Care-of Address [20**]:** 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 [20**]:** peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

DIAMETER [37**]:** DIAMETER base protocol is intended to provide a framework for any services which require AAA/Policy support.

Foreign Network [20**]:** any network other than the mobile node's Home Network.

Home Address [20**]:** 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 [20**]:** network, possibly virtual, having a network prefix matching that of a mobile node's home address.

NOTE: Standard IP routing mechanisms will deliver datagrams destined to a mobile node's Home Address to the mobile node's Home Network.

Link [20**]:** facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address [20**]:** 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 [12**]:** 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 [20].

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

Mobile Station [51**]:** 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 [51**]:** 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).
[12] The part of the mobile equipment which performs the radio transmission and related functions.

Mobility Agent [20**]:** "either a home agent or a foreign agent.

Mobility Binding [20**]:** association of a home address with a care-of address, along with the remaining lifetime of that association.

Mobility Security Association [20**]:** collection of security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them.

Node [20**]:** host or a router.

Nonce [20**]:** randomly chosen value, different from previous choices, inserted in a message to protect against replays.

Security Parameter Index (SPI) [20**]:** 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 [51**]:** equipment that provides the functions necessary for the operation of the access protocols by the user (source: GSM 01.04 [14]). A functional group on the user side of a user-network interface (source: ITU-T

Recommendation I.112 [30]). *The part of the mobile station that is not the mobile termination.*
[12] The part of the mobile equipment that contains the end-to-end application or (e.g. laptop connected to a mobile phone).

Tunnel [20**]:** 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 [20**]:** 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 [20**]:** network other than a mobile node's Home Network, to which the mobile node is currently connected.

Visitor List [20**]:** list of mobile nodes, visiting a foreign agent.

3.2 Abbreviations

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

AAA	Authentication, Authorisation and Accounting
AF	Assured Forwarding
APN	Access Point Name
AUC	AUthentication Centre (GSM)
BG	Border Gateway (GPRS)
BSS	Base SubSystem (GSM access network)
CAMEL	Customised Applications for Mobile Enhanced Logic
CDR	Call Detail Record
CGF	Charging Gateway Functionality
CH	Correspondent Host (same as correspondent node)
CN	Core Network
COA	Care-Of Address
DS	Differentiated Services
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
QoS	Quality of Service
RAC	Routing Area Code
RADIUS	Remote Access Dialling User Service
RAI	Routing Area Identifier
RAN	Radio Access Network
RNC	Radio Network Controller

RNS	Radio Network Subsystem
RNTI	Radio Network Temporary Identifier
RSVP	Resource ReserVation Protocol
SGSN	Service GPRS Support Node
SNDCP	Subnetwork Dependent Control Protocol
SRNC	Serving RNC
SRNS	Serving RNS
TE	Terminal Equipment
TIPHON	Telecommunications and Internet Protocol Harmonisation Over Networks
TLLI	Temporary Logical Link Identifier
TMSI	Temporary Mobile Subscriber Identifier
TR	Technical Report
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 [20], 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 RFC 2002 [20], 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 RFC 2003 [21], RFC 2004 [22] and RFC 2344 [26]. A few key presumptions in RFC 2002 [20] 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 [31]. Other IETF working groups that are among the most interesting for the launch of MIP+ are the AAA (Authentication, Authorisation 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 clause will, however, only cover the work in the mobileip WG. Except for [34], 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 first two subclauses list the RFC's and important drafts with the abstract of each of them. In the subsequent subclauses, some basic principles of Mobile IP are explained. A tutorial on Mobile IP is provided in annex A.

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 in 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 [16], 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 Tunnelling for Mobile IP

Mobile IP uses tunnelling 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 [*20*] 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 authorisation 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 [*20*]. NAI is described in RFC 2486 [*29*].*

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 harmonise 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 [29] defines the need of a standardised format for identifying ISP subscribers for dial-up roaming operations. It introduced the Network Access Identifier (NAI) to fulfil this need. The NAI is provided by the mobile node to the dialled 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 RFC 2486 [29] 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 RFC 2486 [29], 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 tunnelling 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 [20] 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 signalling 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 Optimisation in Mobile IP, v08, February 1999

This document defines extensions to the base Mobile IP protocol to allow for optimisation of datagram routing from a correspondent node to a mobile node. Without Route Optimisation, 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 Optimisation;
- Special Tunnels for Mobile IP.

6.3 Basic Principles of Mobile IPv4

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.

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.

6.4 Differences between IPv4 and IPv6

Annex A describes the operation of MIPv4 RFC 2002 [20] and MIPv6 [35]. 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 tunnelling 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. Wider issues must be considered when comparing the deployment of, or migration between IPv4 and IPv6 networks in general. That is a topic FFS.

6.5 Reverse tunnels

Reverse tunnels (that is tunnels from the FA to the HA) are necessary in IPv4, 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 [27].

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).

In Mobile IPv6, reverse tunnels are not needed to avoid problems with ingress filters. However they may still be beneficial when the ME is concerned about location privacy. The MN may use the care-of address as sender address but that is not required.

6.6 Use of Route Optimisation

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.

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 maintaining, for a short period of time, tunnels from the new SGSN to both the old and new GGSN/FA, potential problems with packet loss are minimised. 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.

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

In figure 1-3, 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 PLMNs. The BG is outside the scope of GPRS specifications [5].

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:

- the ME must be able to find a FA, preferably the nearest one. The underlying assumption is that FA's are located at GGSNs and that not all GGSNs 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. The solution is to define an Access Point Name (APN), for example "MOBILEIPv4FA". This APN is 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.

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 utilised. 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 7.1a.

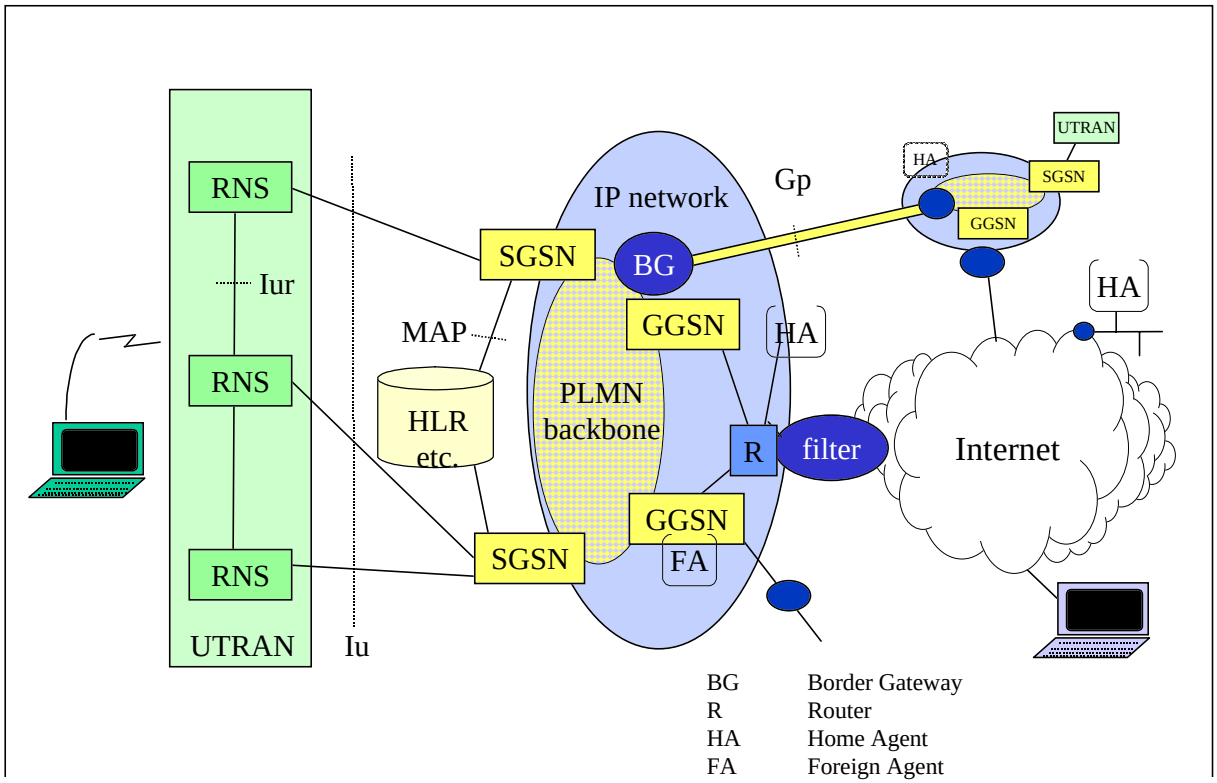


Figure 7.1a: Core network architecture with GPRS MM in and between GPRS PLMNs and Mobile IP MM between different types of systems and optionally between GPRS PLMNs

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. During such a change two tunnels are maintained, for a short period of time, between the new SGSN and the old and the new GGSN/FA. This will minimise problems with packet loss. The possibility of optimising 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 SGSNs are co-located. 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. 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 PLMNs can be handled either with MIP(+) or with GPRS.

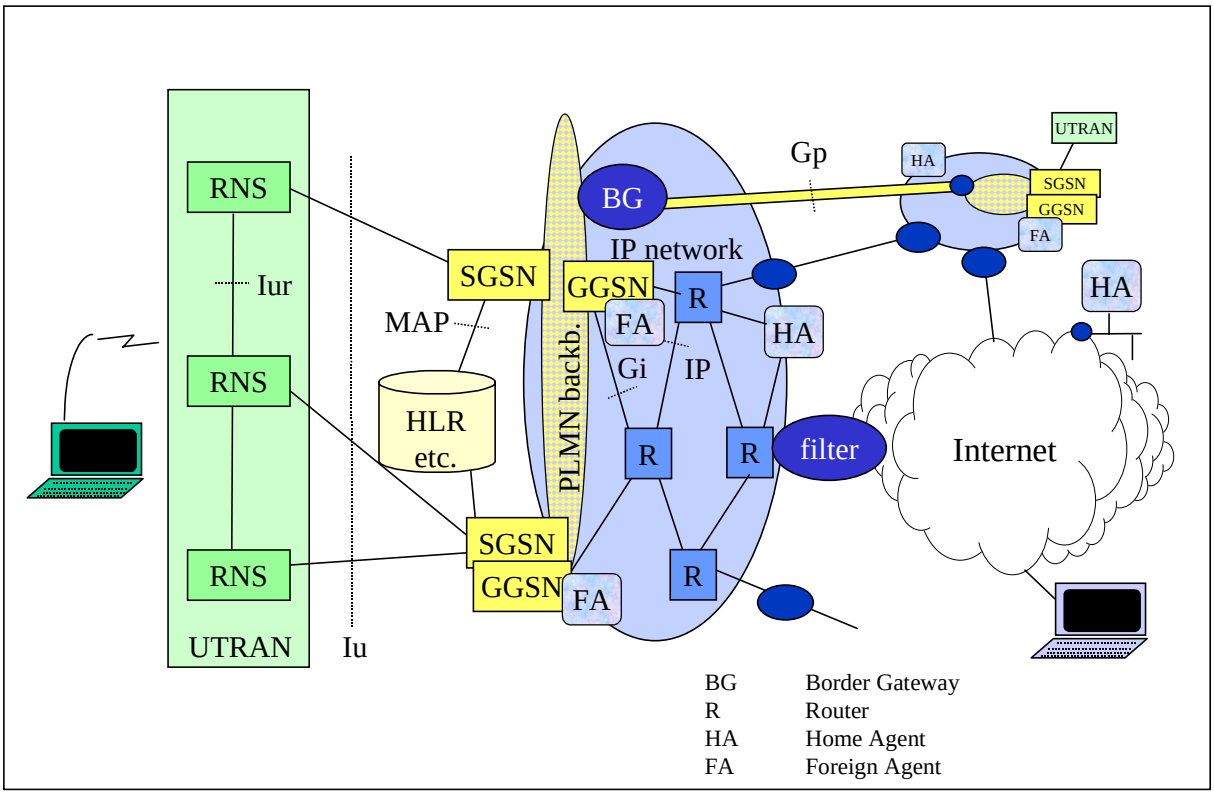


Figure 7.2a Core network architecture where GPRS MM handles active mobiles and Mobile IP(+) streamlining at inter SGSN handover. The SGSN and GGSN are here co-located

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 utilise 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 7.3a 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 or GGSN will be necessary during a transition period.

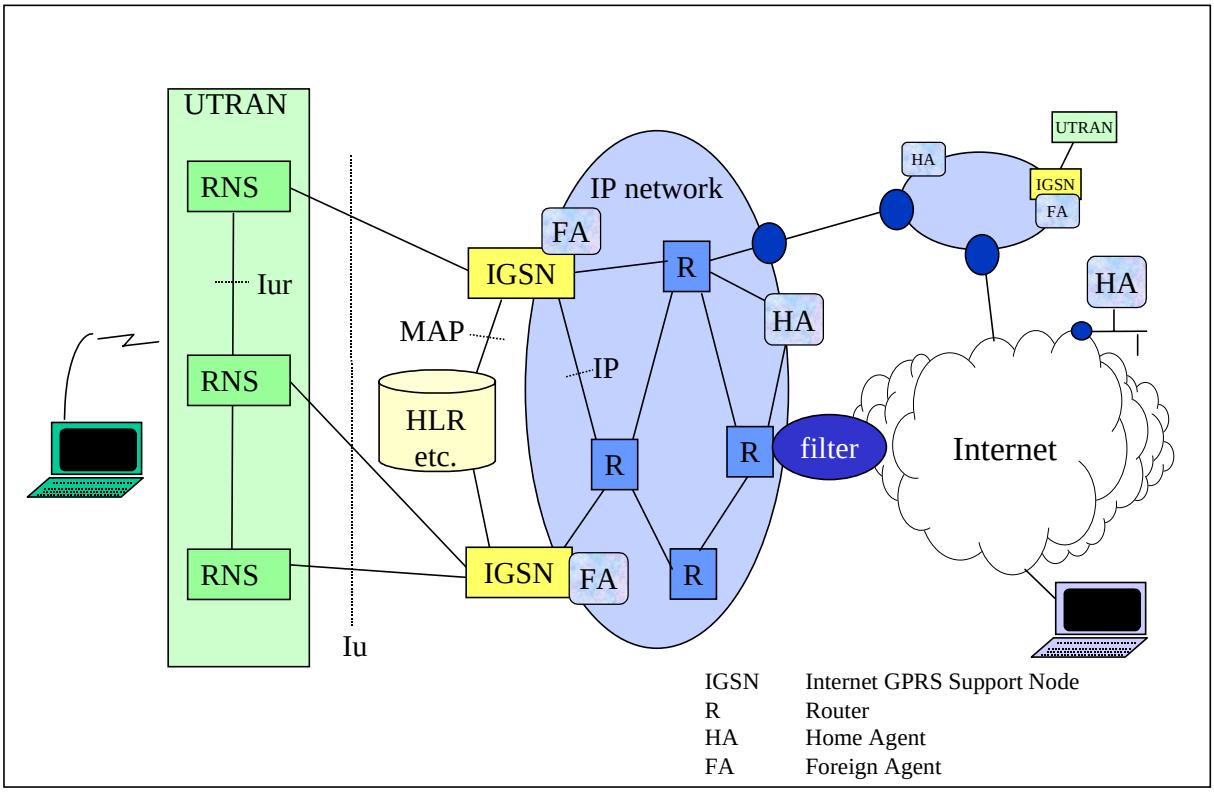
The basic functionality of the IGSN is:

- 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 and via the FA with the AAA infrastructure;
- charging data collection and formatting according to UMTS/GSM specifications. IETF specifications may be used for FA accounting;
- 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 utilise RADIUS or another AAA infrastructure according to the IETF specifications at hand when a given UMTS specification is finalised;
- support of inter IGSN handovers, either by Mobile IP or GTP. 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.

The following table summarises the supported features of an IGSN:

Feature	O/C/M Optional/ Conditional/ Mandatory	Comments
Gb interface	C	In case the IGSN interfaces to GSM BSS
Iu interface	C	In case The IGSN interfaces to UTRAN or HIPERLAN 2 .
Gn, Gp interface, signalling between IGSNs (e.g. for context transfer at inter IGSN RA update)	M	
Gs interface	O	Optional today
Gr interface	M	Mandatory today
Gd interface	O	
Gc interface	O	Optional today
Gi interface	M	The IGSN takes over this interface from GGSN.
Gf interface	M	
FA support	M	
AAA client support	M	Whichever AAA protocol will be used (initially RADIUS) we need this for MIP roaming purposes.
Charging data collection	M	
Ga interface	M	

In this scenario, the HA will act as the anchor point for the traffic generated by the ME if reverse tunnelling is used, else this traffic will be routed directly to the correspondent node. If Mobile IP route optimisation 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, SGSNs and GGSNs could be



deployed in parallel with the Mobile IP nodes and/or the IGSN could optionally also act as an SGSN.

Figure 7.3a: Core network architecture with Mobile IP+ MM within the CN and between different types of systems and between GPRS PLMNs

8 General Considerations and Explanations

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

8.1 The Care-of address

8.1.1 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 tunnelled 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. FA 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.

8.1.2 The Care-of address in IPv6

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.

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 MEs 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.

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.

8.2 The Home Address

8.2.1 Permanent and Temporary Home Addresses

According to [20], 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 [35]. 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.

8.2.2 Private Home Address

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 [36] 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). Private addresses in Mobile IP are not standardised by the IETF. Private addresses are not recommended to be used outside the private network domain.

8.3 Location of the HA and the FA

The FA (IPv4) that a user is currently connected to is necessarily within the UMTS operator's network. In IPv6, only co-located care-of address are used and the FA is not needed.

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.

8.4 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 from the beginning.

8.4.1 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 signalling to setup and maintain the connection (usually PPP) between the MT and TE is not included in this report. 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.

8.5 Need for Broadcasting over Radio

Although Mobile IP(+) utilises 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 IGSNs.

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.

8.6 Security

UMTS security is built into the network layers, out of the control of the end user. Contrary, IP security is implemented in or above the IP layer of the IP stack, easily accessible by the IP user. In step 1 and 2, MIP (+) is run over the UMTS/GPRS network. UMTS/GPRS security is deployed within the PLMN but does not provide end-to-end security when the user is communicating with a node outside the PLMN. IP-security is an end-to-end security solution, which works independently of the UMTS/GPRS security mechanisms. In step 3, UMTS/GPRS security protects the network between the ME and the IGSN. In addition, the users association with their home PLMN (HLR) will be protected by the UMTS authentication procedures. IP security mechanisms can provide security for MIP (+) and end-to-end.

This subclause describes these mechanisms in relation to MIP and UMTS/GPRS.

Since the Internet is an insecure network and GPRS is supposed to be connected to it, it needs a security application that runs over IP to support end-to-end security. Looking at picture 8.6.a, we can see that end to end security cannot be guaranteed since we do not have control over all the intermediate IP networks. The application above IP has to secure the datagrams instead. Below is one, out of many, proposed way of doing this for Mobile IP.

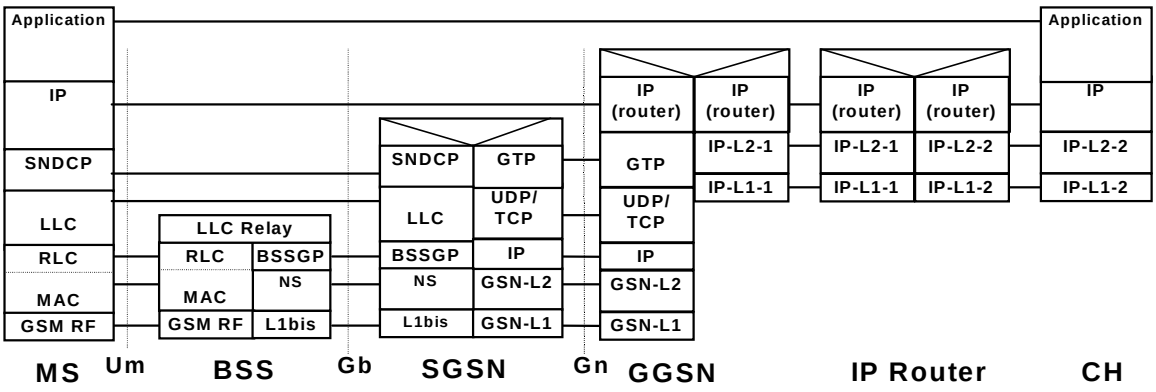


Figure 8.6a: Protocol stack for GPRS including the Internet

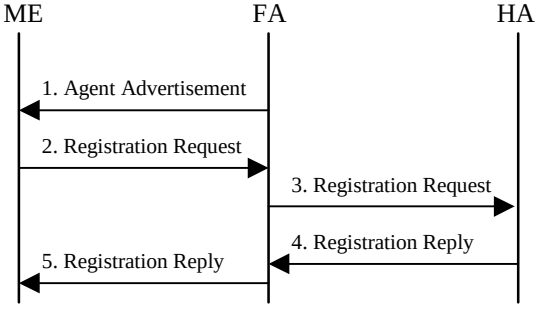


Figure 8.6b: Packet routing in a Mobile IP network in Registration

8.6.1 Mobile IPv4 control messages: security issues

The Mobile IP Standard requires registration datagrams between the HA and the ME to be authenticated and proposes a solution for this. The standard does not require the FA and HA or the FA and ME to be authenticated. The reason for this is that the FA is a standard intermediate router and routers are not authenticated on the Internet. In the particular case of GPRS/UMTS, the IGSN/FA and ME are authenticated at the link layer.

Authorisation is done in the message numbered 2, in figure 8.6b, and it is forwarded to the HA. The HA replies with a negative acknowledgement if the authorisation fails. The authorisation algorithms are made in such ways that replaying is impossible.

Equal authorisation is done in the message numbered 4, in figure 8.6b. it is also forwarded via the FA to the ME. After this procedure the HA and ME knows that they have been registered with each other.

8.6.2 MIPv4 Protocol Security Analysis

The problem with MIP security could be set up into a set of questions:

1. How does the ME know it is talking to an honest FA? Is anyone else sending data from my address?
2. How does the ME know it is receiving data from its HA? Is it the correct data? Can anyone eavesdrop it?
3. How does the ME know that the data is not altered/spoofed on its way to the destination? End to end security.
4. How do I hide my geographical position in a Mobile IP network? Do I want to hide my position?
5. Signalling.
6. Header compression and security.

8.6.2.1 FA-ME Considerations

The ME sends user datagrams (IP-packets) on top of the GPRS link. The information in these packets are filled by the ME which means that any ME connected to any FA can send IP packets with any source address and any destination address. This is not desirable and some kind of filter must be applied in the foreign agent to check the PDP context against the IP packets sent out by the ME. Likewise, the ME must confirm that the packets it receives are sent by the correct FA. This is done in a similar manner.

8.6.2.2 HA-ME Considerations

The HA forwards all the packets received for the ME to the FA. They are sent out over the Internet, which is an insecure network, and forwarded to the FA. On the Internet people with access to intermediate routers can eavesdrop/alter/add new packets. This is normal IP security, but not acceptable to tunnel confidential intranet data. If additional end-to-end security is needed, it must be added in the protocol stack above IP. End-to-end security is out of the scope of this document.

8.6.2.3 ME-CH Considerations

No method for integrity check is present in basic IP. The normal case of IP traffic is to send traffic and hope that no attack is done to your machine. This works pretty well for public web surfing and other equal services, but if additional security is needed, this is not acceptable. Protocol above IP needs to be used, like IPsec, S/MIME or other security protocols. End to end security is a matter for the IETF to provide and out of scope of this document.

8.6.2.4 Geographical position

In a normal IP network, routes can be examined by using the ICMP protocol. This means that any host can at any time see all the intermediate routers towards an IP host. This means, in the Mobile IP case, that any host can look at what FA a ME is connected to. If the FA is named viplounge22.heathrow.london.<operator>.gprs no further detective tasks has to be done to understand where the ME is attached. The reason for this is because the FA must answer some ICMP messages at some points. Work has to be done how to cover this scenario up.

In order for route optimisation to work, I have to send my care-of address (the FA address) to my CR, which directly tells my point of attachment to the network.

Logical network position is not equal to geographical position, but might still reveal information about the current position.

The problem gets more severe in step 3 than in step 2 or step 1 due to FA granularity and each move of a ME into a new region, served by a FA, may imply a change of the FA. This change of FA is detectable by communicating partners (using ping, traceroute or other means) and therefore allows parsing the location of the mobile entity with a potentially high precision. Moreover, this may make known network internal design details to the public.

8.6.2.5 Signalling

If we have a security association between the HA and the FA and use IPsec, all the packets, including signalling, between the hosts will be protected and authenticated by IPsec. The use of IPsec has other issues associated with it but these are out of the study of this report. Other ways of protecting the signalling, if needed, can also be applied.

8.6.2.6 Header compression and security

When doing header compression, the compressor must be able to intercept the packets and access/alter the data in one or more layer in the protocol. The purpose of security protocols is to remove the possibility to read, alter or add data in the packets. Therefore, it might often be the case that usage of header compression and security protocols in the same layer is not possible.

8.6.3 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), etc.

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.

8.7 AAA (Authentication, Authorisation and Accounting) and Roaming issues

When a data network access service is provided, there are two independent authentication, authorisation and accounting requirements. One requirement is to look-up the user profile stored in the HLR and to update billing records as currently done in GSM. Another requirement is to use future AAA authentication mechanisms, specified by IETF. The RADIUS protocol was designed to support dial up SLIP and PPP within one administrative domain. It suffers from security and scaling problems and is not suitable for sending information across different administrative domains. Hence, it is not the ideal IETF protocol for use together with Mobile IP.

The Mobile IP technology allows mobile nodes to move to and receive services from a foreign administrative domain different than their home domain. This leads to a need for Authorisation, which in turn leads to Authentication and of course to Accounting. The AAA functions are intimately interdependent.

The availability of an AAA infrastructure is considered important for a large-scale deployment of Mobile IP. Within the IETF AAA working group [31], work is in progress on development of requirements for Authentication, Authorisation and Accounting as applied to network access. Also, the MIP working group [29] is currently looking at requirements on AAA and the functionality the protocols have to support.

The purpose is to create a base protocol applicable to a number of specific network access models. These will include Network Access Server (NAS) AAA, Mobile IP, and roaming. By creating an architecture and base protocol, the amount of work to create specific network access AAA protocols will be reduced. The AAA working group will incorporate requirements provided by the IETF Mobile IP working group.

The long-term goal is to create a generic framework [38] with a generic AAA server, which should support the various needs of applications requiring authentication of users, handling authorisation requests, and collecting accounting data.

Examples of applications considered are [40]: Mobile IP, PPP dial in service, and e-commerce. This can be realised through a network of interconnected AAA servers. But the different applications each have their own needs, which may require application specific protocols. Therefore, an interface is proposed between the generic AAA server and a set of one or more application specific modules.

A basic model, or framework, that seems to be well supported by both the IETF working groups AAA and MIP is depicted in figure 8.7a. The basic conceptual entities in this model are:

1. a user, or client, who wants access to a service or resource;
2. a User Home Domain, or Home Authority (AAAH), that has agreement with the user;
3. a service provider's AAA server, or Local Authority (AAAL), that authorises a service based on an agreement with the AAAL;
4. a service provider's service equipment that provides the service itself, e.g. a NAS in dial service.

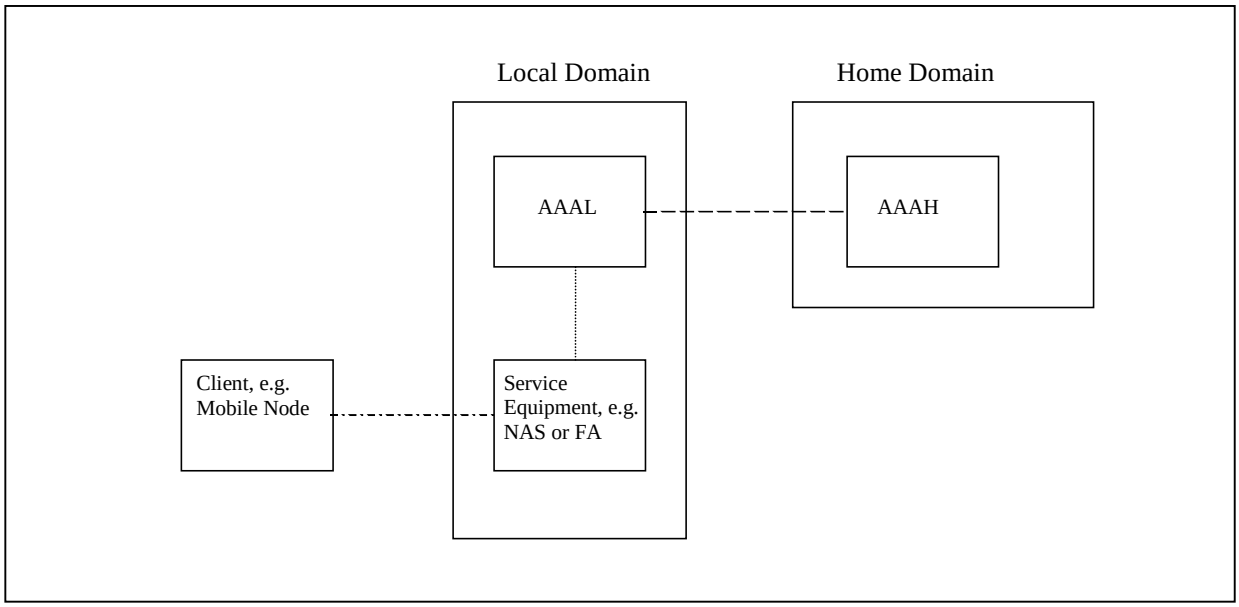


Figure 8.7a: Basic AAA model

For a description of the different message sequences and features of the model as well as requirements placed on the protocols, see [46] and [47]. If seen from a MIP perspective, the mobile node (MN) is considered to be the client in the figure, and the SE to be the foreign agent (FA). The home agent (HA) has a role during initial registration that is subordinate to the role played by the AAAH.

A broker node may exist between the AAAL and AAAH to solve the scalability problems associated with requiring direct relationships between every two administrative domains.

8.7.1 AAA Support of MIP in UMTS

Authorisation based on UMTS identity authentication is not sufficient, since the **data network identity and UMTS identity are unrelated.** For instance, this is the case of a mobile station composed of a TE and a MT, such as a Laptop and a UMTS data card. The data card could be shared by a group of users accessing different networks, or the same network under different identities. Therefore, separate authorisation and accounting for UMTS access services and data network usage are required.

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 a reason why deploying an IETF standard AAA infrastructure may make sense.

Mobile IP+ will natively rely on data network AAA protocols and support 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. In figures 8.7.1a and 8.7.1b, some of the scenarios described are summarised.

Logically the AAA server/FA/HA authentication is independent from the IGSN/HLR authentication. In this report the IGSN and FA are assumed to be co-located. However, the IGSN/FA has independent and separate logical interfaces to the two security systems. The AAA servers may or may not be a part of the UMTS network.

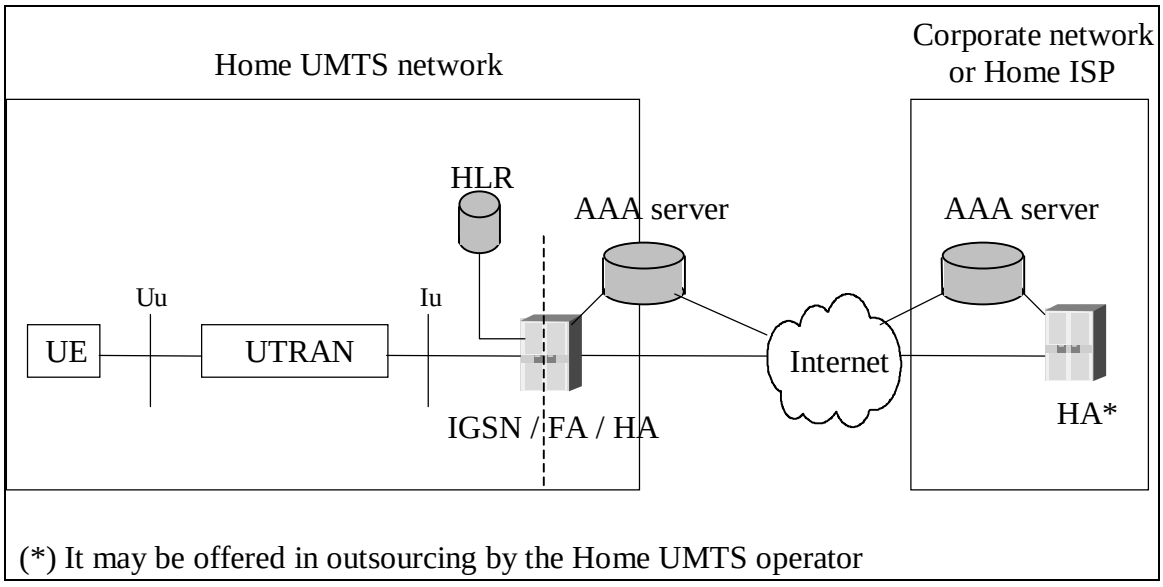


Figure 8.7.1a: UE attached to the Home UMTS operator

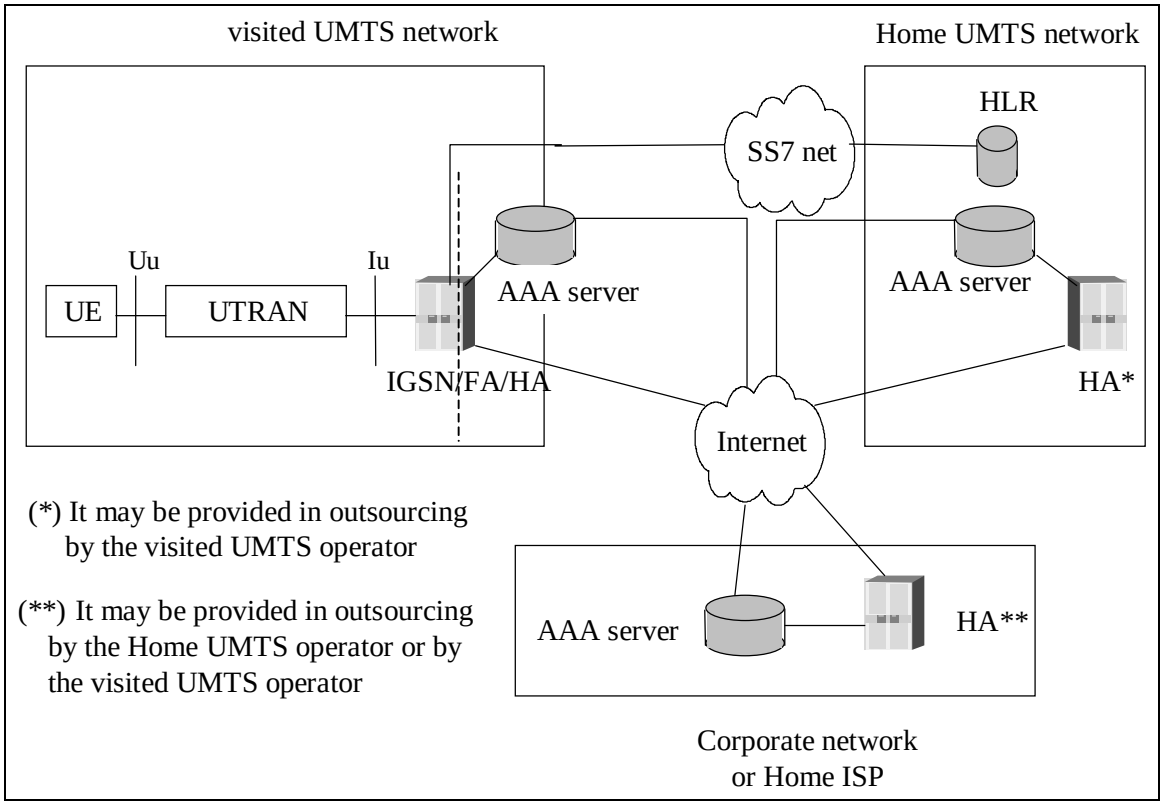


Figure 8.7.1b: UE not attached to the Home UMTS operator

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 are expected to be similar to those used in version 4.

8.8 UMTS/GPRS Charging

In GPRS [9], the Charging Gateway Functionality (CGF) provides a mechanism to transfer charging information to the Billing System. The information is collected from the SGSN and GGSN as Call Detail Records (CDR). The IGSN will collect the same CDRs as in a combined SGSN and GGSN. It is here assumed that the same charging model is used as in GPRS. The main new service aspect requirements for UMTS charging and billing are described in [10]. However, any new entries in the CDRs due to these requirements, will be subject to all types of GSNs and are out of the scope of this report.

The following table describes the data content in the CDRs generated by the SGSN (S-CDR), GGSN (G-CDR) and IGSN (I-CDR) for each PDP context. The tables contain a key indicating whether or not the field is mandatory (M), only available under certain conditions (C), or optional (O). The S-CDR and the G-CDR are taken from [9], the I-CDR is generated by an IGSN. The IGSN address is a new entry. Today, the GSNs involved in a session provides the CGF with charging data independently of each other. The IGSN will also do that. When the IGSN acts as an SGSN, it produces S-CDRs.

As users of step 3 are connected to an IGSN in the visited network, there will be no UMTS level CDR production in the home network for a user connected to a foreign network. This corresponds to the case when a user accesses the Internet through a GGSN in the visited network in today's GPRS architecture.

Charging data in SGSN, GGSN and IGSN

Field	SGSN S-CDR	GGSN G-CDR	IGSN I-CDR	Description	Comment If the IGSN acts as an SGSN, it produces S-CDRs
Record Type	M	M	M	GPRS SGSN/GGSN/IGSN PDP context record.	
Network Initiated PDP Context	C	C	C	Present if this is a network initiated PDP context.	
Anonymous Access Indicator	C	C	C	Set to true to indicate anonymous access (and that the Served IMSI is not supplied)	
Served IMSI	M	M	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).	
Served IMEI	C	-	C	The IMEI of the ME, if available.	
SGSN Address	M	M		SGSN: The IP address of the current SGSN. GGSN: List of SGSN addresses used during this record	
GGSN Address	M	M	-	SGSN: The IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP. GGSN: The IP address of the GGSN used.	
IGSN Address	-	-	C	The IP address of the IGSN used.	This is a new entry, that does not exist in GSM 12.15 [9]
ME Network Capability	O	-	O	The mobile station Network Capability.	
Routing Area	O	-	O	Routing Area at the time of the record creation.	
Local Area Code	O	-	O	Location area code at the time of the record creation.	
Cell Identity	O	-	O	Cell id at the time of the record creation.	
Charging ID	M	M	M	PDP context identifier used to identify this PDP context in different records created by GSNs	
Access Point Name	M	M	M	The logical name of the connected access point to the external packet data network.	The APN will reveal if the MIP service was used, see subclause 9.3.
PDP Type	M	M	M	PDP type, e.g. X.25, IP, PPP, IHOSS:OSP	
Served PDP Address	M	M	M	PDP address of the served IMSI, e.g. an IPv4, IPv6 or X.121.	
Remote PDP Address	-	O	O	List of PDP addresses of the remote host or DTE e.g. an IPv4, IPv6, or X.121 (Included if the PDP type is X.25)	

Dynamic Address Flag	-	C	-	Indicates whether served PDP address is dynamic, that is allocated during PDP Context Activation.	
List of Traffic Data Volumes	M	M	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data values are listed. Data volumes are in Octets above the SNDCP(SGSN and IGSN)/GTP(GGSN) layer and are separated for uplink and downlink traffic.	
Record Opening Time	M	M	M	SGSN, IGSN: Time stamp when PDP context activation is created in this SGSN/IGSN or record opening time on following partial records. GGSN: Time stamp when this record was opened.	
Duration	M	M	M	Duration of this record in the GSN.	
SGSN Change	C	-	C	Present if this is first record after SGSN/IGSN change.	
Cause for Record Closing	M	M	M	The reason for the release of record from this GSN.	
Diagnostics	O	O	O	A more detailed reason for the release of the connection.	
Record Sequence Number	C	C	C	Partial record sequence number in this SGSN. Only present in case of partial records.	
Node ID	O	O	O	Name of the recording entity	
Record Extensions	O	O	O	A set of network/ manufacturer specific extensions to the record.	
Local Record Sequence Number	O	O	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.	

In addition to the I-CDR information described in the table above, the IGSN will also collect the mobility management data (M-CDR) and the SMS data (S-SMO-CDR and S-SMT-CDR) generated in the SGSN according to [9].

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 signalling messages as well as on the MT and (3G)SGSN functionality should be minimised 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 subclause 8.1). 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 subclause 9.3) and to the choice of transporting all Mobile IP(+) messages in the UMTS/GPRS user plane.

9.2 Assumptions

9.2.1 Signalling

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 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 finalised, 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 standardised as the GGSN/FA is considered being one integrated node.

9.2.3 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) [20] that the mobile node uses is located in the home network. There will probably also be an AAA (Authentication, Authorisation 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 [3]. Using the Network ID to mean a service is not supported today. However, to extend the SGSNs ability to choose a suitable GGSN depending on the desired service based on the APN 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 utilise 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 subclause 8.1 for a discussion on alternative, but less efficient methods of providing MIP service.

This subclause describes the complete procedure of PDP Context Activation followed by Mobile IP(+) registration.

NOTE: The Mobile IP(+) service may be offered by a different operator than the home UMTS/GPRS operator.

The signalling scheme in figure 9.4a 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.

---

[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.

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

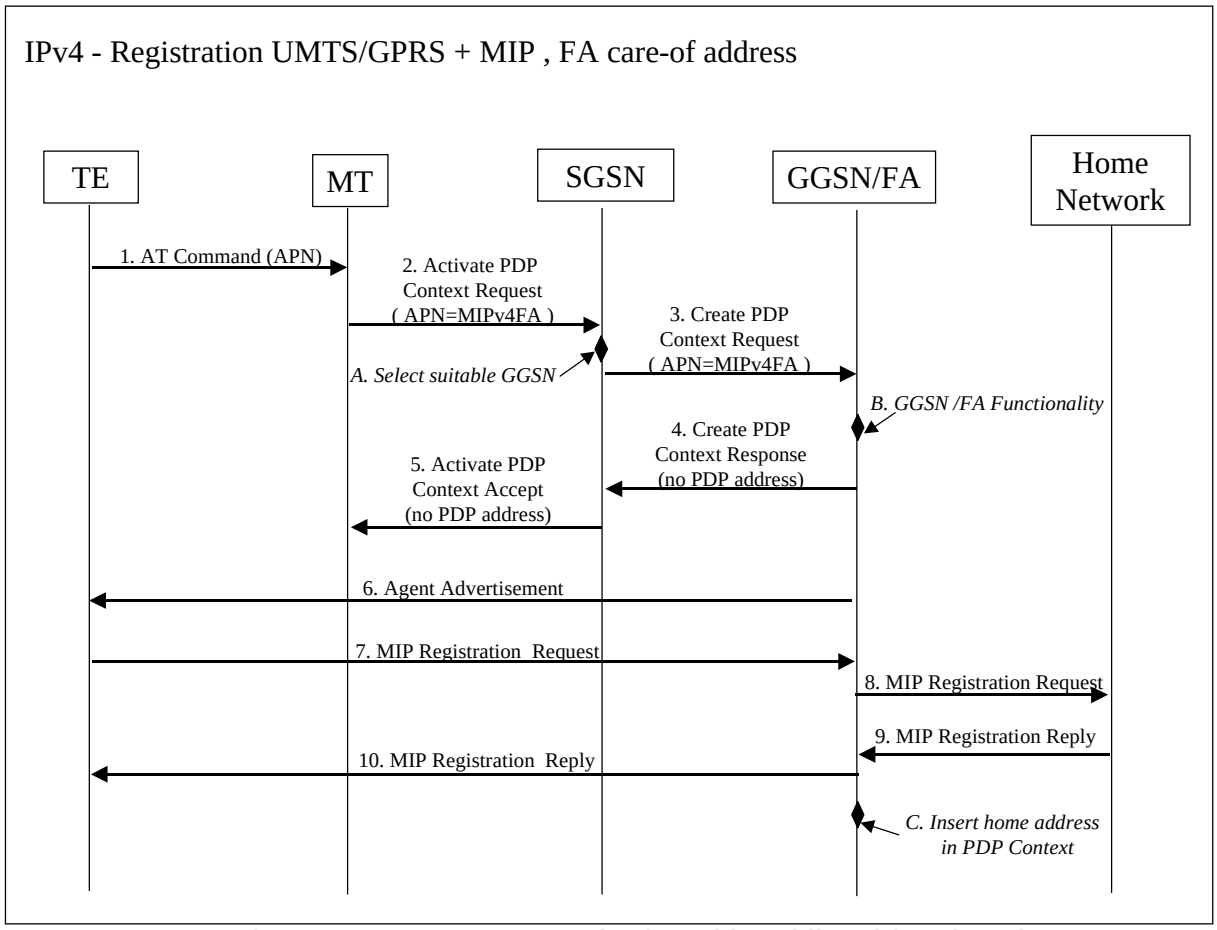


Figure 9.4a, PDP Context activation with Mobile IP(+) registration (the PPP setup and UMTS/GPRS attach procedure not included)

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 9.4a.

1. → AT Command
2. → Activate PDP Context Request

   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.

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", [6].

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 subclause 9.3, 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 GSM 04.08 [13]. 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. To find the closest GGSN/FA, the APN should be used to mean a specific service, in this case MIPv4FA.

Current Specifications

The format of the APN is specified in [3]. 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 APNs.

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 [20] 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 [20]. 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 [20]. 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 [36] 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 [29] 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 [35] 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 [20]. The use of NAI is currently being specified [36] 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 [20], 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 standardise 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(+) signalling 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 APNs.

NOTE: None of the points above require any change to the current GPRS protocols.

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

The Step 2 introduces a further optimisation to the Step 1. The Step 2 comprises the same Core Network as the Step 1 but the GGSN may be changed during a session in order to optimise the route.

The SGSN has the control of the change. It can change the GGSN for instance after an inter-SGSN handover to optimise the route from the new SGSN to a more optimal GGSN. If there is not a more optimal GGSN available the SGSN will not change the GGSN. The SGSN has the information about the GGSNs that are in its domain, thus avoiding the change to a GGSN that has no FA.

10.1 The GGSN/FA Change

In the figure 10.1a, 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.

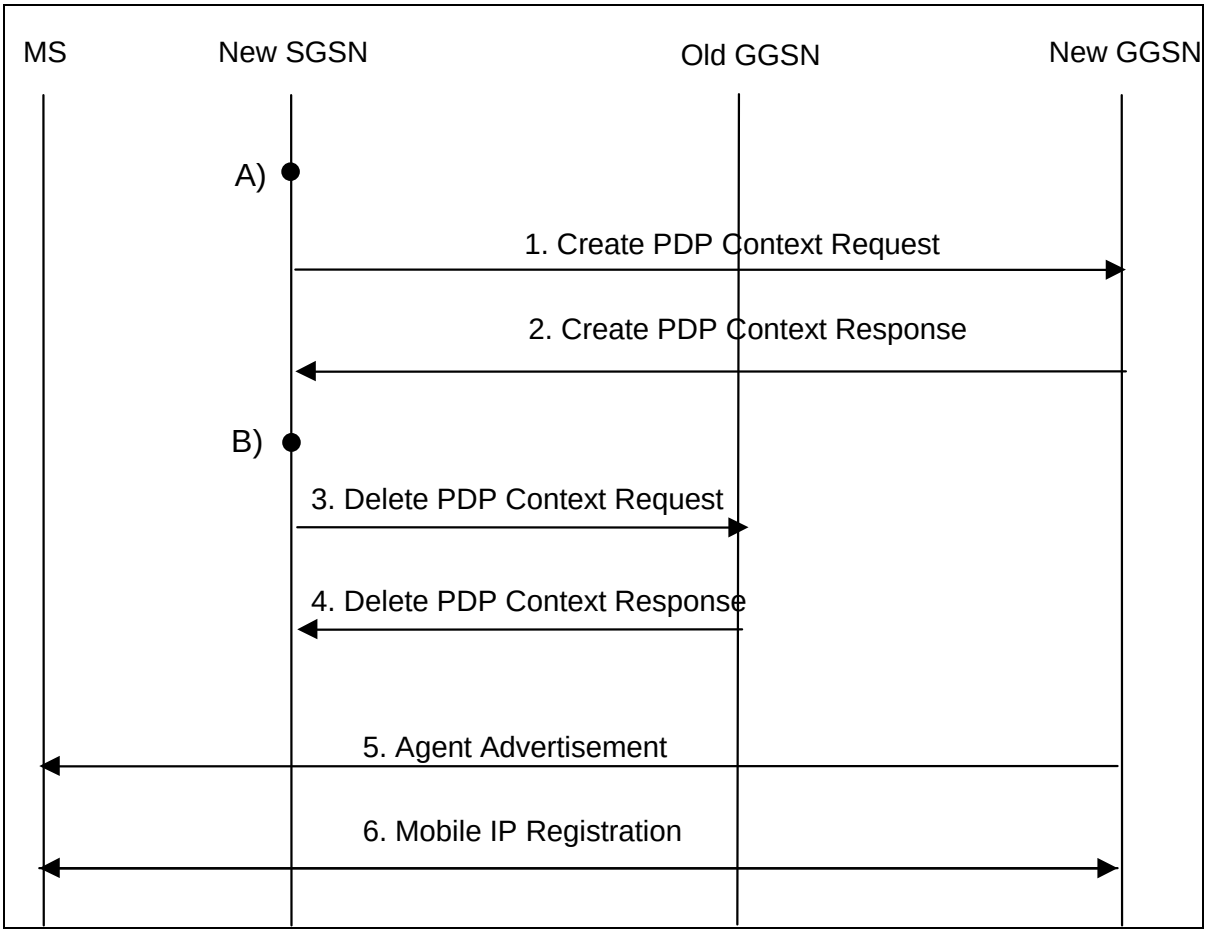


Figure 10.1a: The GGSN/FA handover

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 SGSNs 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 [20].

6. Agent registration is performed as defined in [20].

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 10.2a.

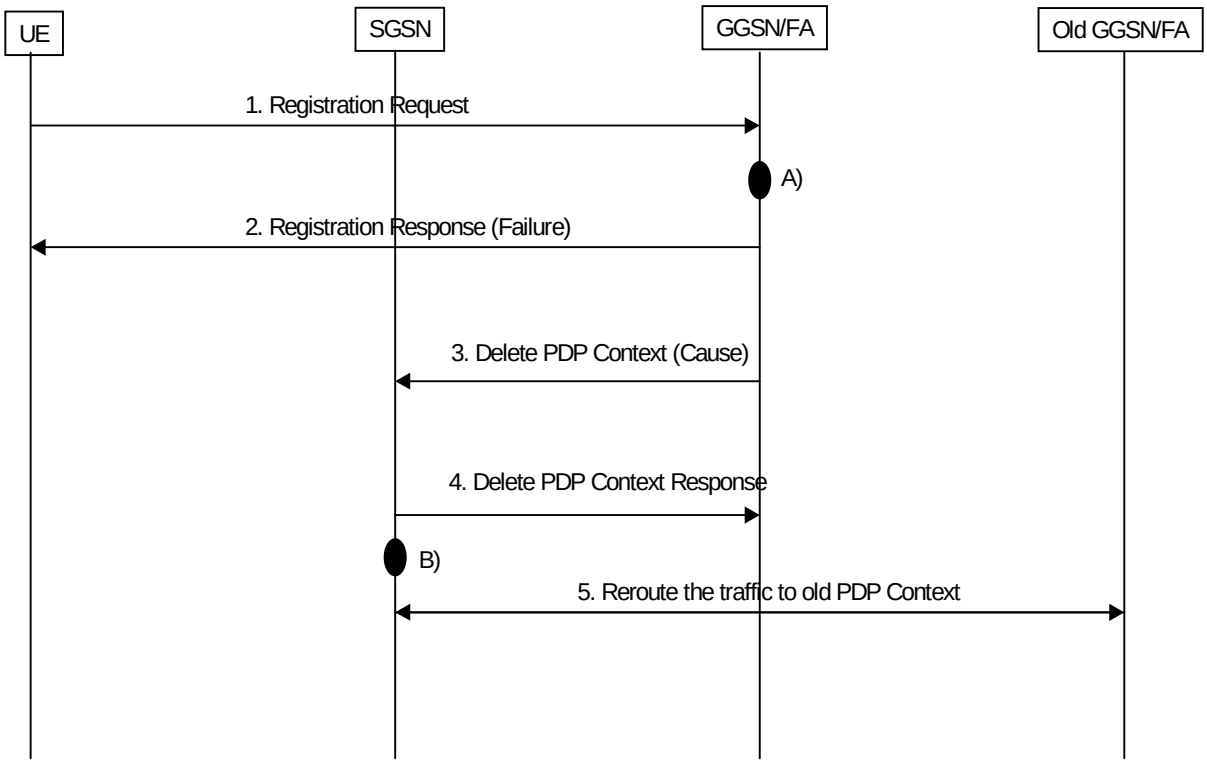


Figure 10.2a: Mobile IP registration failure

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.

4. 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 10.2b, the case where no fallback is possible is described.

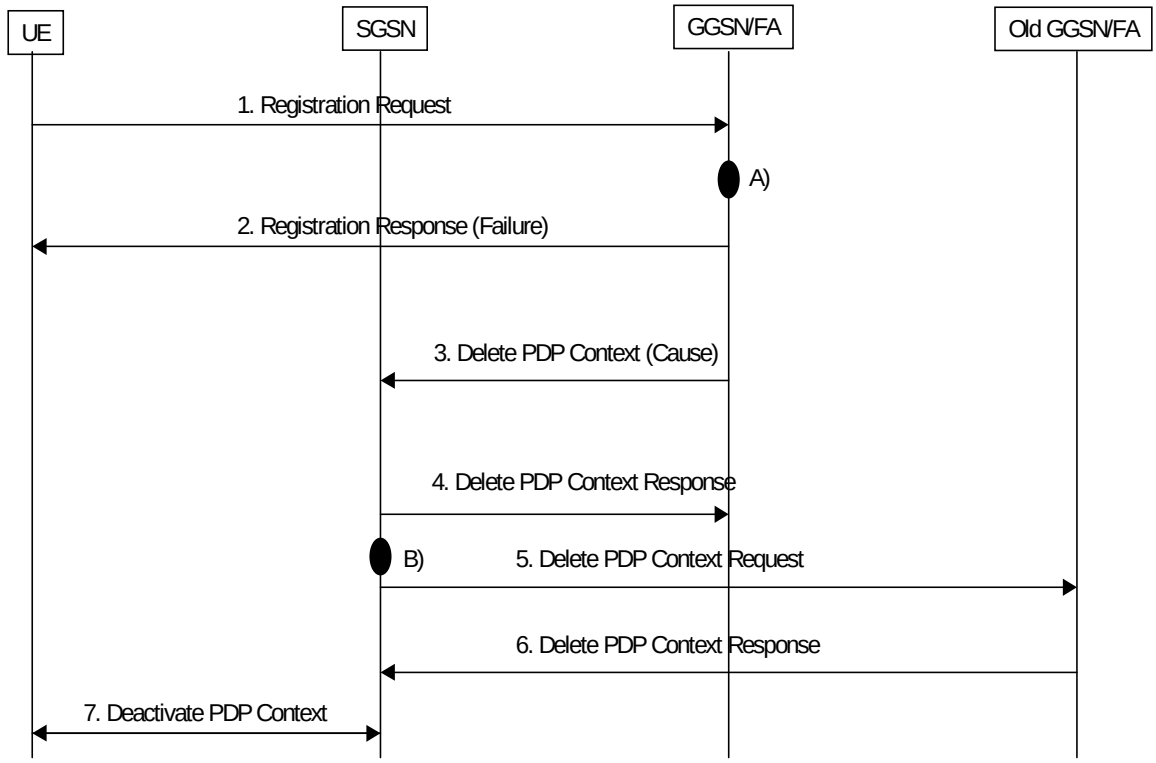


Figure 10.2b: Case when no fall-back is possible

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 GSM 09.60 [7] in the subclause 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

Step 3 differs from step 1 and step 2 in that Mobile IP is used for intra-system mobility for those ME equipped with a Mobile IP(+) client and asking for Mobile IP(+) service.

In step 3 an IGSN (Internet GPRS Support Node) as described in subclause 7.3 is assumed to be used. This scenario may be seen as an extension of GPRS to support Mobile IP in a way that solves PLMN non optimal routing problems without requiring any new messages such as in step 2. Also, if Mobile IP route optimisation will be used in the future, optimal routing will be possible end to end.

The operation of the MIP based mobility support in step 3 may be summarised in this way:

- particular SM and MM messages received at an IGSN are used to trigger a FA so that it sends a MIP advertisement. This document does not describe in which way this is accomplished (it maybe subject of other standardisation efforts or proprietary, if the IGSN and the FA are modules of the same box);
- the MIP advertisement is delivered via the IGSN which was handling those particular SM or MM messages only to the ME that sent those MM or SM messages;
- the Mobile station registers according to Mobile IP standards with the FA issuing the advertisement.

To allow compatibility with UMTS/GPRS networks which are being upgraded at a slower pace, an option to let the IGSN also act as an SGSN will be necessary during a transition period.

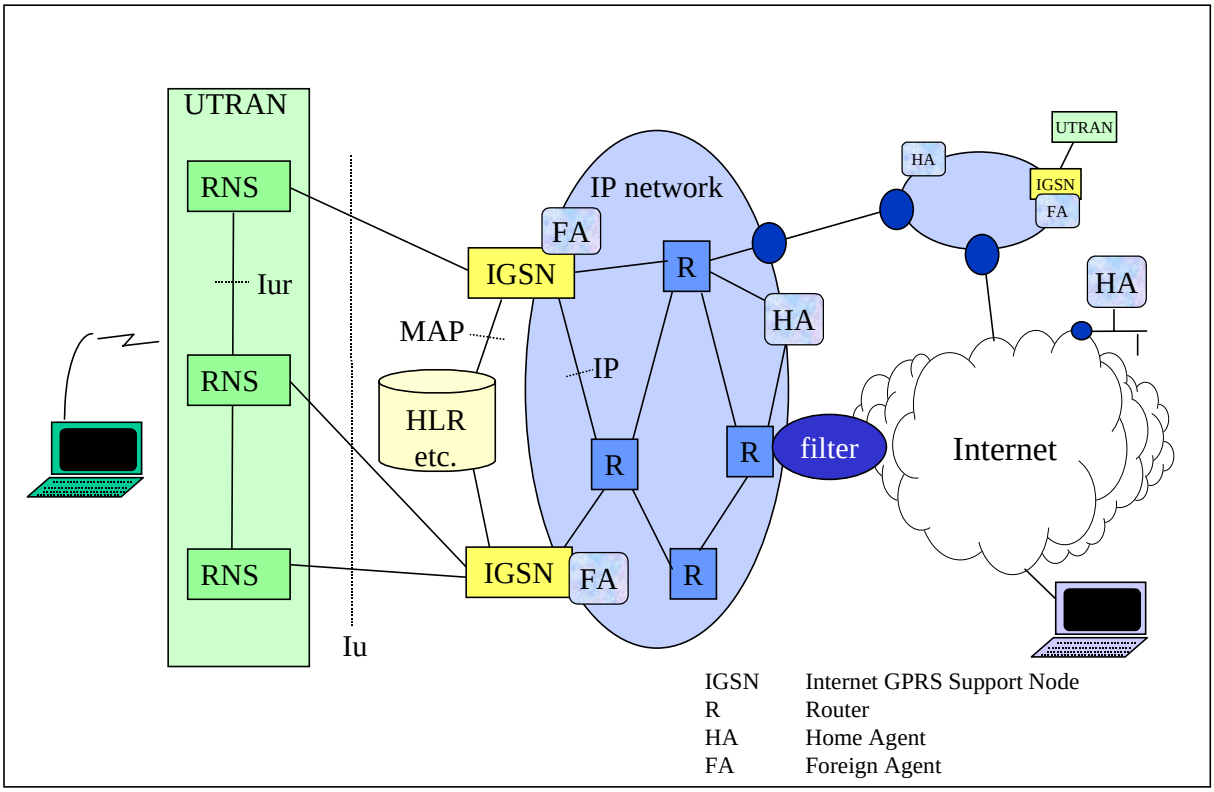


Figure 11a: Step 3 network architecture

11.1 General Design Criteria for step 3

The main design criteria are that:

- radio resources and IPv4 address should be used with care;
- the impact on the current UMTS/GPRS signalling messages between the MT and (2G/3G)SGSN should be avoided or minimised;
- it is required that terminals used in step 1 and 2 networks can be used in step 3 networks.

The first criterion led to the choice of using Foreign Agent care-of addresses (see subclause 8.1).

The second one to the choice of using the APN (Access Point Name) as a service selection mechanism instead of introducing a new PDP type (see subclause 3.3), to the choice not to modify the GPRS and UMTS system control plane and to the choice of transporting all Mobile IP(+) messages in the UMTS/GPRS user plane.

Indeed, this proposal requires only an FA to interact with the SGSN functional part of the IGSN as described below.

11.2 Assumptions

The interface between the IGSN and FA, is assumed not be standardised as the IGSN/FA may be one integrated node.

11.3 Using the APN to select MIP service

The IGSN will provide MIP service based on the APN (Access Point Name) that is given by the ME (see subclause 9.3 for a detailed description of the APN). Also, subscription data may be used to generate the APN, if the ME does not provide one, and thus MIP service selection may be part of subscription information.

The alternative is to define a new PDP type for each service. This is not desirable as the standard must be extended for each new service.

Although it can be assumed that all terminals will support MIP at some point in the future, the APN can be used to distinguish between the request of MIPv4 and MIPv6.

11.4 Session activation for ME requesting MIP(+) service and equipped with a MIP(+) client

The Session activation for ME requesting MIP(+) service and equipped with a MIP(+) client differs from the current GPRS model in that it's locally handled by the IGSN without the need to use a GGSN.

From the ME perspective, the session activation and initial MIP(+) registration is completely identical to the case in which the FA is placed at a GGSN as described in step 1 (see subclause 9.4).

Every IGSN is assumed to be equipped with a FA. After receiving an activate PDP context request from the ME, the IGSN sends a "Activate PDP context accept" to the mobile terminal and triggers a FA to send the advertisement to the mobile station that is requesting the activation of a session, in the same way as in the case when the FA is at the GGSN in step 1 (see subclause 9.4).

For sake of clarity, the complete session activation procedure (PDP Context Activation followed by Mobile IP(+) registration) is now described.

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.

1. → AT Command
2. → Activate PDP Context request

   A. ◆ Select MIP service

B. ◆ IGSN/FA Functionality: trigger MIP agent advertisement

3. ← Activate PDP Context Accept

4. ← (Foreign) Agent Advertisement

5-6. → Mobile IP(+) Registration Request

7-8. ← Mobile IP(+) Registration Reply

C. ◆ IGSN/FA functionality: Insert PDP address used in the home network in the IGSN PDP context.

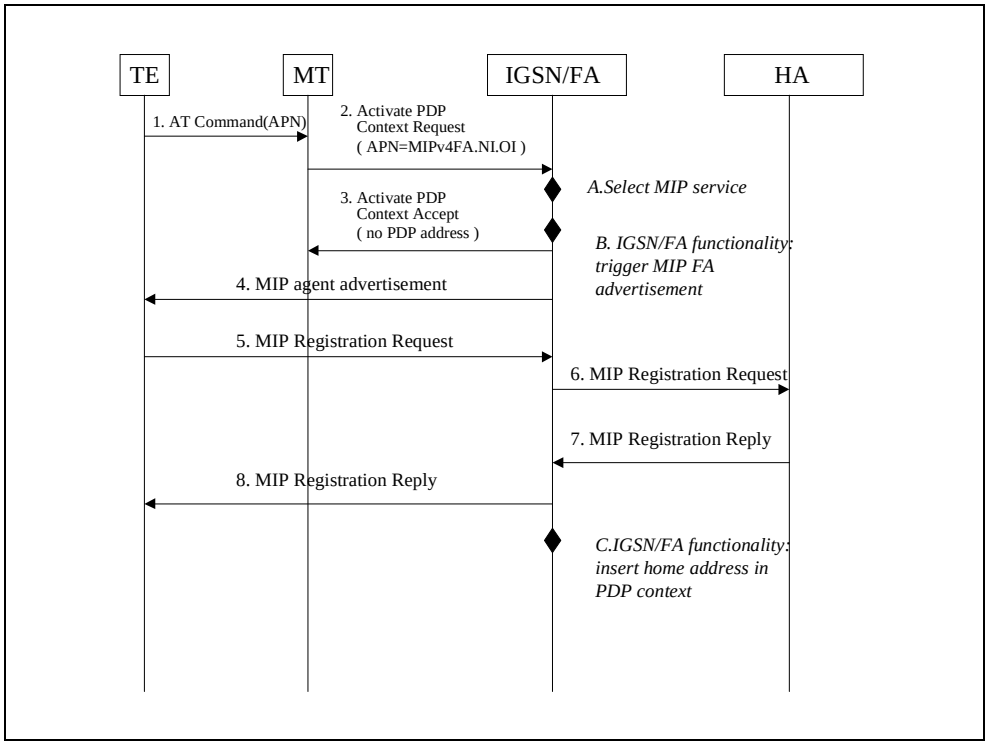


Figure 11.4a: Session activation in a step 3 network

11.4.1 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 selection of MIPv4 service. 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", [6].

Enhancements

None.

11.4.2 Activate PDP Context Request

Description

The MT sends the "Activate PDP Context Request" to the IGSN. The message includes various parameters of which the "APN" and the "Requested PDP Address" are of interest here. The "Requested PDP Address" should be omitted for all ME's using Mobile IP(+).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.

The APN is, in principle, not needed as all ME's are expected to support MIP(+). However, during the transition period, the APN will be necessary to also handle those roaming ME's that still need to connect to a GGSN.

Current Specifications

The parameters "APN" and the requested PDP Address are parameters, currently in the standard GSM 04.08 [13]. 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 static Mobile IP(+) address, which is related to the mobile node's home network, access is denied by the SGSN.

Enhancements

None.

11.4.3 Select MIP service

Description

The IGSN will base the provision of MIP service on the APN that is given by the ME. The Network ID in the APN should be used to mean a specific service, in this case MIPv4FA.. In case MIPv4 is specified in the APN, the IGSN may ignore the other fields of the APN, since no GGSN needs to be selected.

Current Specifications

The format of the APN is specified in [3]. Using the Network ID to mean a service, is not supported today.

Enhancements

Allow the APN to select a specific service, not only a physical node. To support this, the operator must have the possibility to configure the IGSN behaviour depending on service selected. Finally, an agreement between operators is needed on the possible APN service specific syntax.

11.4.4 Activate PDP Context Accept

Description

This message is sent by the IGSN to the ME. The PDP address should be omitted.

Current Specifications

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

Enhancements

None.

11.4.5 Foreign Agent Advertisement

Description

The Agent Advertisement [20] is an ICMP (Internet Control Message Protocol) Router Advertisement message with a mobility agent advertisement extension, which contains parameters of the FA that the mobile node needs. This message should be sent, in the UMTS/GPRS user plane only on the link associated to the specific ME that is activating the session.

Current Specifications

The Agent Advertisement message is specified in [20].

Enhancements

None, except the ability to send advertisements to a single ME, which requires the IGSN and FA to be co-ordinated.

11.4.6 Mobile IP(+) Registration Request

Description

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

The format of the MIP Registration Request is specified in [20]. 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 [36] 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 [29] 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 IGSN/FA needs to store the home address of the mobile node or the NAI and the local link address of the ME. The IGSN/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 IGSN/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 cope with new Mobile IP+ related functionality. The [36] is planned to become a standard track RFC during 1999

Enhancements

None, except the ability to send Mobile IP(+) messages that are exchanged between the IGSN/FA and the ME in the UMTS/GPRS user plane.

11.4.7 Mobile IP(+) Registration Reply

Description

The Registration Reply will be sent from the home network to the IGSN/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. 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 link associated with a specific ME, no broadcast will be sent over the radio interface.

Current Specifications

The functionality of the FA is specified in [20]. The use of NAI is currently being specified [36] and is stable. As there is a point-to-point link between the ME/mobile node and the IGSN/FA, there is no problem for the mobile node to address the FA.

Enhancements

None, except the ability to send Mobile IP(+) messages that are exchanged between the IGSN/FA and the ME in the UMTS/GPRS user plane.

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

Current Specifications

According to [20], the FA is requested to be able to map the home address to the local link address. The IGSN and MT do not need to know the PDP address.

Enhancements

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

Hence, no new GTP messages are required differently from Steps 1 and 2.

11.5 User mobility support for ME requesting MIP(+) service and equipped with a MIP(+) client (GPRS)

Inter-IGSN mobility is handled by Mobile IP for terminals equipped with a Mobile IP client. When a ME moves from the old IGSN/FA coverage to a new IGSN/FA coverage, it will have to perform a Mobile IP registration. During the interval of time necessary to establish a tunnel from the HA to the new IGSN/FA, packets will keep being sent to the old IGSN/FA over the old MIP(+) tunnel. Currently, GTP defines a packet transfer procedure from the old SGSN to the new SGSN when inter-SGSN mobility happens and a new GTP tunnel to the new SGSN is being set-up. Similarly, a transfer of packets from the old IGSN to the new IGSN using GTP may be used in step 3.

In the following subclauses GTP based transfer of packets between IGSNs, although optional, will be shown.

For Mobile IP to handle mobility it must be possible to trigger Mobile IP registrations, that is define a movement detection mechanism. Routing area Update messages seem to be the right trigger for them.

Inter IGSN RA update *must* trigger a Mobile IP registration.

A high level description of RA update procedures is provided below. In the Message Sequence Charts that follow, the arrows denote messages between nodes and the diamonds denote functionality in a node.

Messages Labelled with number 'x' or 'x.y' are dealt with in subclause 'x' of this subclause.

11.5.1 Inter IGSN ROUTING AREA update for terminals requesting MIP(+) service and equipped with a MIP(+) client

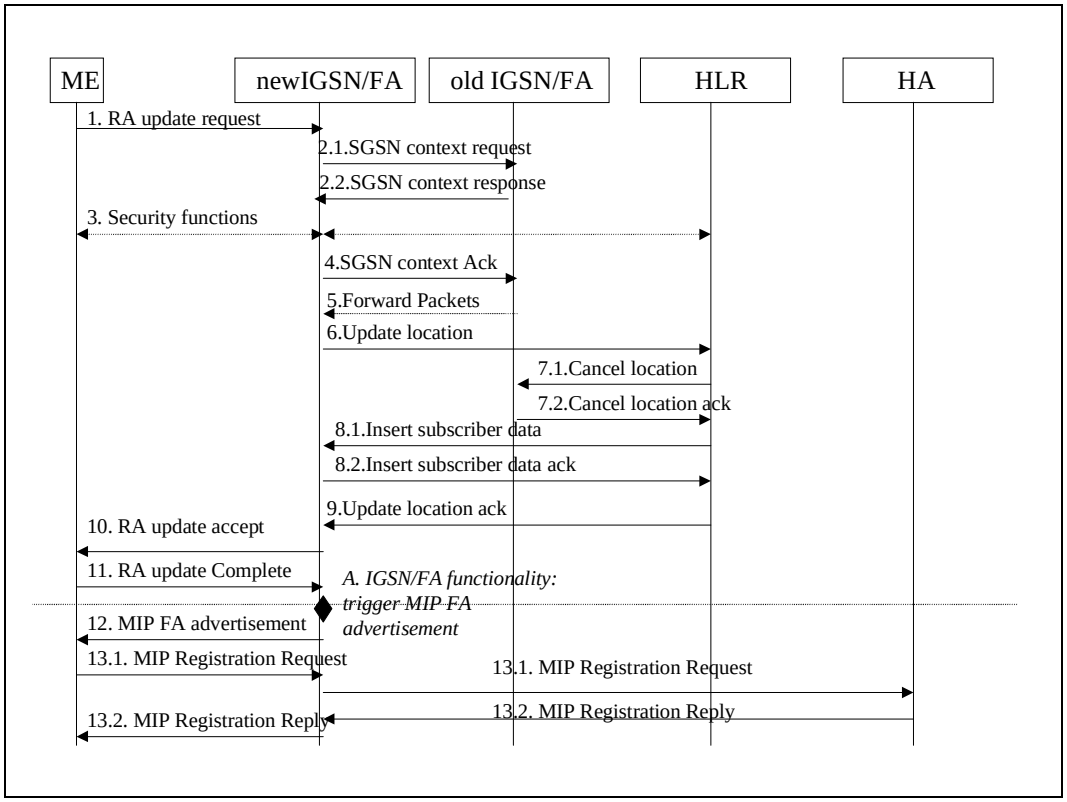


Figure 11.5.1a: Inter IGSN RA update

11.5.1.1 Routing Area update request

The ME sends a Routing Area Update Request to the new IGSN.

Current Specifications

In GPRS the Routing Area Update Request (old RAI, old P-TMSI Signature, Update Type) is sent 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.

Enhancements

None. The only difference is in that IGSNs are in place of SGSNs.

11.5.1.2 SGSN context Request/Response

The new IGSN sends SGSN Context Request to the old IGSN to get the MM and PDP contexts for the ME. The old IGSN responds with SGSN Context Response. The old IGSN stores New IGSN Address sent in the SGSN Context request, to allow the old IGSN to forward data packets to the new IGSN.

The SGSN context Response contains the acknowledgements for each LLC connection used by the ME. The old IGSN starts a timer and stops the transmission of N-PDUs to the ME.

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

The old IGSN needs to interact with a MIP tunnel, instead of GTP tunnel, as it receives over it packets bound to the terminal that has moved to the new IGSN.

11.5.1.3 Security functions

Security functions may be executed.

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.1.4 SGSN Context Acknowledge

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

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]). However, in current specification the GGSN information is also marked as invalidated. This is not needed in step 3, since no GGSN is involved in this procedure.

Enhancements

No invalidation of GGSN information in the old IGSN is required.

11.5.1.5 Forward Packets

The old IGSN duplicates the buffered packets and starts tunnelling them to the new IGSN using GTP. Additional packets received by the old IGSN/FA from the HA before the timer described in subclause 11.5.1.2 expires are also duplicated and tunnelled to the new IGSN. Packets that were already sent to the ME and that are not yet acknowledged by the ME are tunnelled together with the number of the LLC frame that transferred the last segment of the packet. The transfer of the LLC number is necessary so that the LLC layer state is transferred from the old to the new IGSN. No packet shall be forwarded to the new IGSN after expiry of the timer described in subclause 11.5.1.2. Note that this procedure may be limited to the simple transmission of not yet LLC acknowledged packets or skipped altogether depending on whether MIP level mechanisms will be defined to transfer packets between the old and the new FA.

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]). The only relevant difference is in that packets are received by the old IGSN from the HA, instead of the GGSN.

Enhancements

None. The only relevant difference is in that packets are received by the old IGSN from the HA, instead of a GGSN. If MIP(+) standards will evolve so that packet transfer from the old to the new FA is provided, then packet transfer may happen at the Mobile IP(+) level.

In current GPRS specifications at this point the new SGSN would update the GGSN of being the new serving node. In this case this is not necessary since a GGSN is not used by the new IGSN.

11.5.1.6 Update Location

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

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None. An IGSN number and address is assumed not to be different from what today used for SGSNs

11.5.1.7 Cancel location and Cancel location Ack

The HLR sends Cancel Location (IMSI, Cancellation Type) to the old IGSN with Cancellation Type set to Update Procedure. If the timer described in subclause 11.5.1.2 is not running, then the old IGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old IGSN to complete the forwarding of packets. It also ensures that the MM and PDP contexts are kept in the old IGSN in case the ME initiates another inter IGSN routeing area update before completing the ongoing routeing area update to the new IGSN. The old IGSN acknowledges with Cancel Location Ack (IMSI).

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None. However, if MIP standards will evolve so that packet transfer from the old to the new FA is provided, then the PDP context may be removed immediately, without waiting the timer described in subclause 11.5.1.2 to expire (that timer may not even be used any more).

11.5.1.8 Insert Subscriber Data and Insert Subscriber Data Ack

The HLR sends Insert Subscriber Data (IMSI, GPRS subscription data) to the new IGSN. The new IGSN validates the ME's presence in the (new) RA. If all checks are successful then the IGSN constructs an MM context for the ME and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.1.9 Update Location Ack

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

Current Specifications

This procedure is what is used in current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.1.10 Routeing Area Update Accept

The new IGSN validates the ME's presence in the new RA. If all checks are successful then the new IGSN constructs MM and PDP contexts for the ME. A logical link is established between the new IGSN and the ME. Only from now on packets could possibly be sent to the ME, including MIP advertisements. The new IGSN responds to the ME with Routeing Area Update Accept. This message also includes all the LLC Acks of packets received by the old IGSN at the start of the procedure, so that the ME LLC state is updated.

Current Specifications

This procedure is simply what is used in current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.1.11 Routeing Area Update Complete

The ME acknowledges the new P-TMSI sent to the ME in the RA update accept message with a Routeing Area Update Complete (P-TMSI, LLC Ack). LLC Ack contains the acknowledgements for each LLC connection used by the ME, thereby confirming all mobile-terminated packets successfully transferred before the start of the update procedure.

Current Specifications

This procedure is simply what is specified by current GPRS standards (inter SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.1.12 Mobile IP (+) Agent Advertisement

The new IGSN sends a Mobile IP Agent Advertisement to the ME performing the RA update. It is highly recommended that this advertisement include a subnet prefix extension in order for the subnet movement detection algorithm to work properly.

If the FA sends a NAI uniquely identifying itself in the advertisement, thus providing an effective way to detect movement, this should be the preferred movement detection mechanism.

Current Specifications

Mobile IP currently defines two movement detection algorithms, but does not mandate the use of any of the two. However, it is necessary to use the subnet prefix algorithm since the advertisement lifetime based mechanism would not be good in wireless systems where broadcast of advertisements on the user plane is not used, such as in the GPRS and UMTS systems as so far described. The Mobile IP(+) messages that are exchanged between the IGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

Enhancements

None.

11.5.1.13 MIP registration

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.

Current Specifications

Normal Mobile IP procedures are used.

Enhancements

None.

11.5.2 Intra IGSN ROUTING AREA update for terminals requesting MIP(+) service and equipped with a MIP(+) client

It may be desirable for load distribution or reliability reasons to associate a pool of FAs to a IGSN. It may be desirable, sometimes, to move a user from a FA to another. This may conveniently be done at intra IGSN routing Area update time as follows.

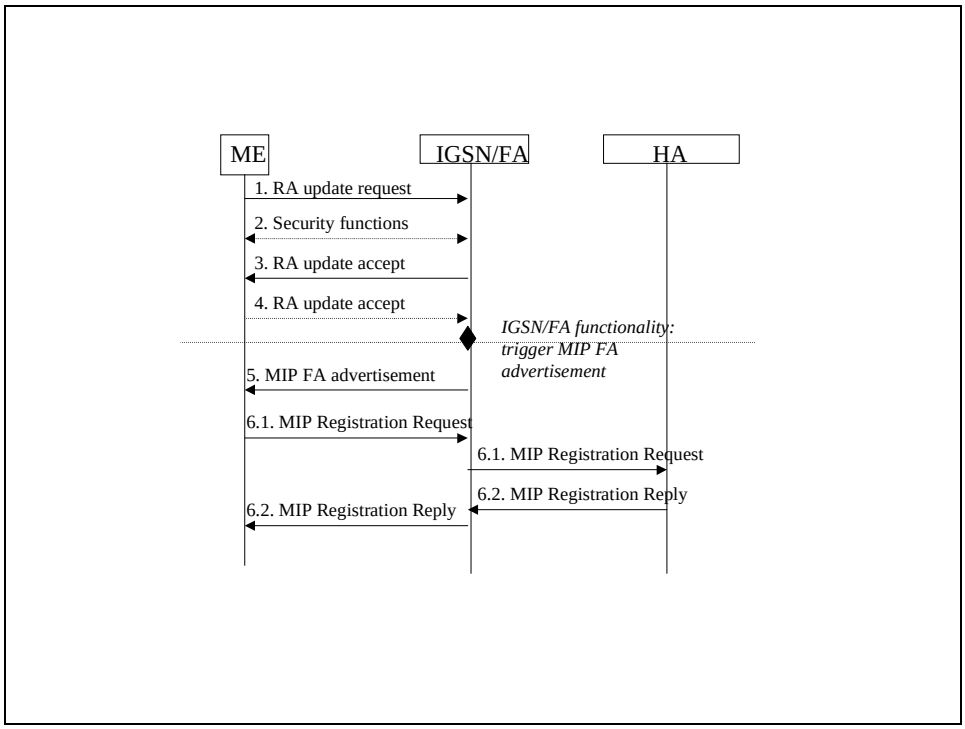


Figure 11.5.2a: Intra IGSN Routing Area Update

11.5.2.1 Routeing Area Update Request

The ME sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the IGSN. Update Type shall indicate RA update.

Current Specifications

This procedure is simply what is specified by current GPRS standards (intra SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.2.2 Security functions

Security functions may be executed.

Current Specifications

This procedure is simply what is specified by current GPRS standards (intra SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.2.3 A Routeing Area Update Accept

The IGSN validates the ME's presence in the new RA. If all checks are successful then the IGSN updates the MM context for the ME. P-TMSI may be reallocated. A Routeing Area Update Accept is returned to the ME.

Current Specifications

This procedure is simply what is specified by current GPRS standards (intra SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.2.4 Routeing Area Update Complete

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

Current Specifications

This procedure is simply what is specified by current GPRS standards (intra SGSN RA update in GSM 03.60 [5]).

Enhancements

None.

11.5.2.5 Mobile IP(+) Agent Advertisement

If a new FA needs to be assigned (e.g. for load sharing reasons) then a Mobile IP(+) Agent Advertisement is sent by the new FA.

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). If the FA sends a NAI uniquely identifying itself in the advertisement, thus providing an effective way to detect movement, this should be the preferred movement detection mechanism.

Current Specifications

This procedure is simply the use of mobile IP standards with the addition of some not described tight coupling between the FAs and the IGSN.

Enhancements

None. Only the ability of the IGSN to trigger MIP advertisement is not part of existing standards. In addition, the FA may send a NAI in the advertisement uniquely identifying itself, thus providing an effective way to detect movement.

11.5.2.6 MIP(+) registration

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. MIP level packet transfer between the old FA and the new FA happens during the registration procedure, if a way to do that will be standardised.

Current Specifications

Normal mobile IP(+) procedures are used.

Enhancements

None. However, if MIP level packet transfer between the old FA and the new FA is desirable, this will happen during the registration procedure.

11.6 User mobility support for ME requesting MIP(+) service and equipped with a MIP(+) client (UMTS)

In this subclause the viability of the use of Mobile IP(+) for UMTS intra-system mobility is demonstrated.

When the ME is in IDLE mode, the procedures defined for GPRS work the same way in UMTS.

In UMTS, SRNS relocation procedures would be used as a trigger when the ME is in UTRAN connected state.

The trigger for Mobile IP advertisements to be sent to the mobile is the completion of the relocation preparation phase and the subsequent successful bearer switch being signalled by the new RNC to the (new)[5] IGSN. Basically, the new RNC signals to the (possibly new) IGSN that the Iu bearer for the ME is in place and that it has been successfully associated to the ME radio resources during the bearer switch phase. This implies that a link from the IGSN to ME has been successfully established and that it's therefore possible to send data from the IGSN to the mobile. An advertisement can therefore be immediately sent to the mobile node.

When a ME requests MIP(+) service and is equipped with a MIP(+) client, the following SRNS relocation procedure takes place (the case that involves change of IGSN is described, but, as in the case of Intra-IGSN RA update, an SRNS relocation that does not require change of IGSN may require changing FA as well).

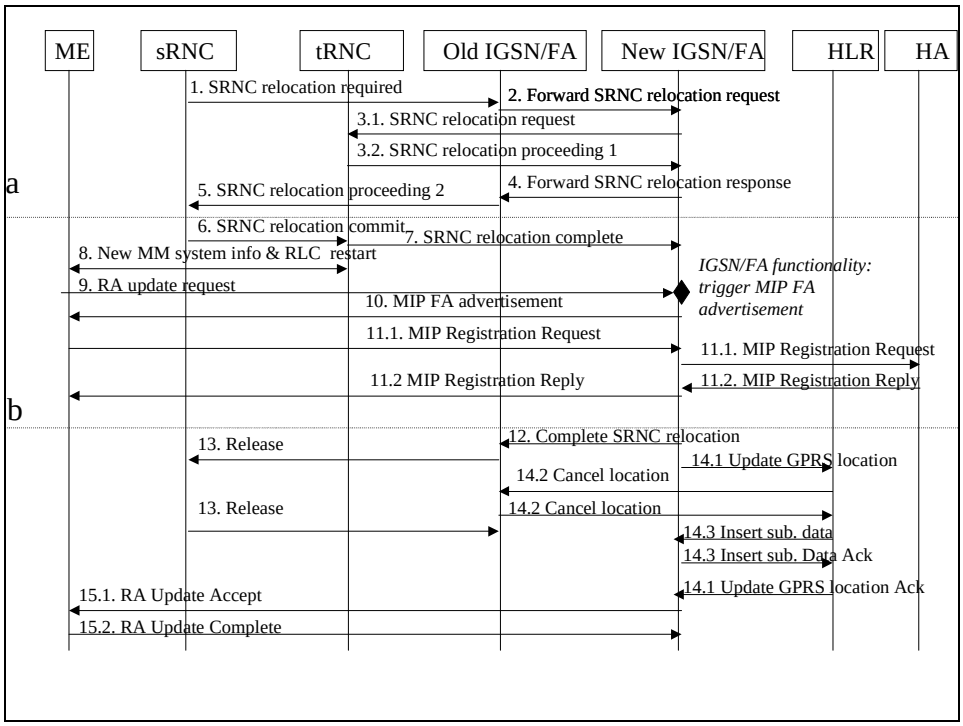


Figure 11.6a: SRNS relocation in a step 3 network

11.6.1 SRNC Relocation required

UTRAN (source RNC) 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 message to the old IGSN. This message includes parameters such as target RNC identifier and information that shall be passed transparently to the target RNC.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

[5] The new RNC may or may not be linked to a new IGSN

Enhancements

None.

11.6.2 Forward SRNC relocation request

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

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None. The PDP context will include the APN with a field informing the new IGSN that the ME is using MIP(+).

11.6.3 SRNC Relocation Request and SRNC Relocation Proceeding 1

The new IGSN 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. ME id., no of connected CN nodes, ME 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 new IGSN.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.4 Forward SRNC Relocation Response

When the traffic resources (Iu bearers) between target RNC and the new IGSN have been allocated and the new IGSN is ready for the SRNC move, then the Forward SRNC Relocation Response is sent from the new IGSN to the old IGSN.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.5 SRNC Relocation Proceeding 2

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

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.6 SRNC Relocation Commit

This message starts the actual Handover of SRNC phase.
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.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.7 SRNC Relocation Detect and SRNC Relocation Complete

Immediately after a successful switch at RNC, target RNC (that now has become the new SRNC) sends SRNC Relocation Detect message to the new IGSN. After sending out the New MM System Information, the target RNC sends SRNC Relocation Complete message to the new IGSN.

Current Specifications

No frozen standard currently exists, and the only Mobile IP(+) specific feature introduced is the trigger of a MIP FA advertisement. In the current standard at this point the GGSN PDP context would be updated with the new SGSN data.

Enhancements

None. The Mobile IP(+) messages that are exchanged between the IGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

11.6.8 New MM system Information and RLC restart

When the target RNC is acting as SRNC, The RLC restart procedures are executed and New MM System Information is sent to the ME indicating e.g. relevant Routing Area and Location Area. A new RAI triggers a routing area update procedure (subclause 11.6.10). Additional RRC information may then also be sent to the ME, e.g. new RNTI identity. This may trigger a LA Update procedure.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.9 Routing Area Update Request

The UE sends a Routing area update request (old RAI; old P-TMSI; old PTMSI signature, Update type) to the IGSN.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None, however this RAU message is the trigger for a subsequent MIP agent advertisement .

11.6.10 Mobile IP (+) Agent advertisement

Upon reception of RAU request , the new IGSN sends a Mobile IP Agent Advertisement to the ME performing the RA update. It is highly recommended that this advertisement include a subnet prefix extension in order for the subnet movement detection algorithm to work properly.

If the FA sends a NAI uniquely identifying itself in the advertisement, thus providing an effective way to detect movement, this should be the preferred movement detection mechanism.

Current Specifications

Mobile IP currently defines two movement detection algorithms, but does not mandate the use of any of the two. However, it is necessary to use the subnet prefix algorithm since the advertisement lifetime based mechanism would not be good in wireless systems where broadcast of advertisements on the user plane is not used, such as in the GPRS and UMTS systems as so far described. The Mobile IP(+) messages that are exchanged between the IGSN/FA and the ME shall be sent in the UMTS/GPRS user plane.

Enhancements

None.

11.6.11 MIP registration

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.

Current Specifications

Normal Mobile IP procedures are used.

Enhancements

None (although the fact no tunnel with a GGSN is in place, and instead a MIP(+) tunnel with a HA is set-up, is a difference with current standards). If MIP level packet transfer between the old FA and the new FA is desirable, this will happen during the registration procedure

11.6.12 Complete SRNC Relocation

Upon reception of RAU request, the new IGSN sends a Complete SRNC Relocation towards the Old IGSN.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.13 Release

At reception of the Complete SRNC Relocation, the old IGSN will send a release indication towards the Source RNC. This will imply release of all UTRAN resources that were related to this ME.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.14 Update GPRS location, Cancel location, Insert subscriber data

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

Current Specifications

No frozen standard currently exists (although these procedures are quite unlikely to be different from this), however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.15 Routing Area Update Accept and Complete

At reception of Insert subscriber data from HLR, the new IGSN will send a Routing Area Update Accept message to the ME. This message will include new RAI, and possibly also new P-TMSI. When the ME has made necessary updates it answers with Routing Area Update Complete.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

Before point a, in figure 11.6a, the connection is established between ME and HA via Source RNC and the old IGSN.

After point b, in figure 11.6a, the connection is established between ME and HA via Target RNC and the new IGSN.

11.7 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/GPRS specific procedures have been included, however, not in detail.

11.7.1 Sending Packets

(a) Sending directly to a corresponding host.

(b) Sending via the HA to a corresponding host (use of reverse tunnelling).

11.7.2 Receiving Packets

The following subclause 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) idle mode when the incoming datagram arrives. The Mobile IP procedures are according to RFC 2002 [20].

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. This is illustrated in figure 11.7.2a.

If optimised 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 tunnelling them to the FA care-of address.

This is depicted in figure 11.7.2b.

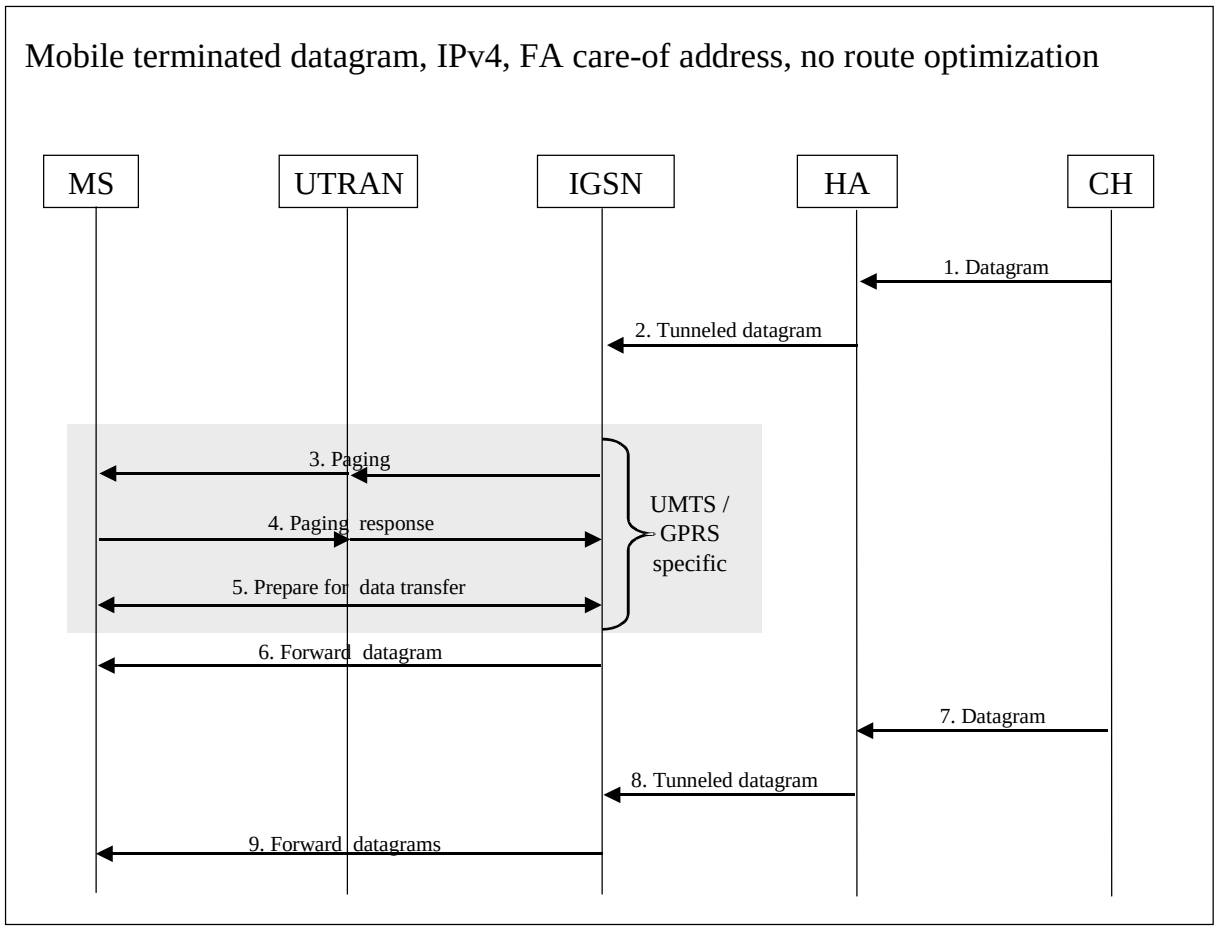


Figure 11.7.2a: Delivery of mobile terminated datagrams, no route optimisation

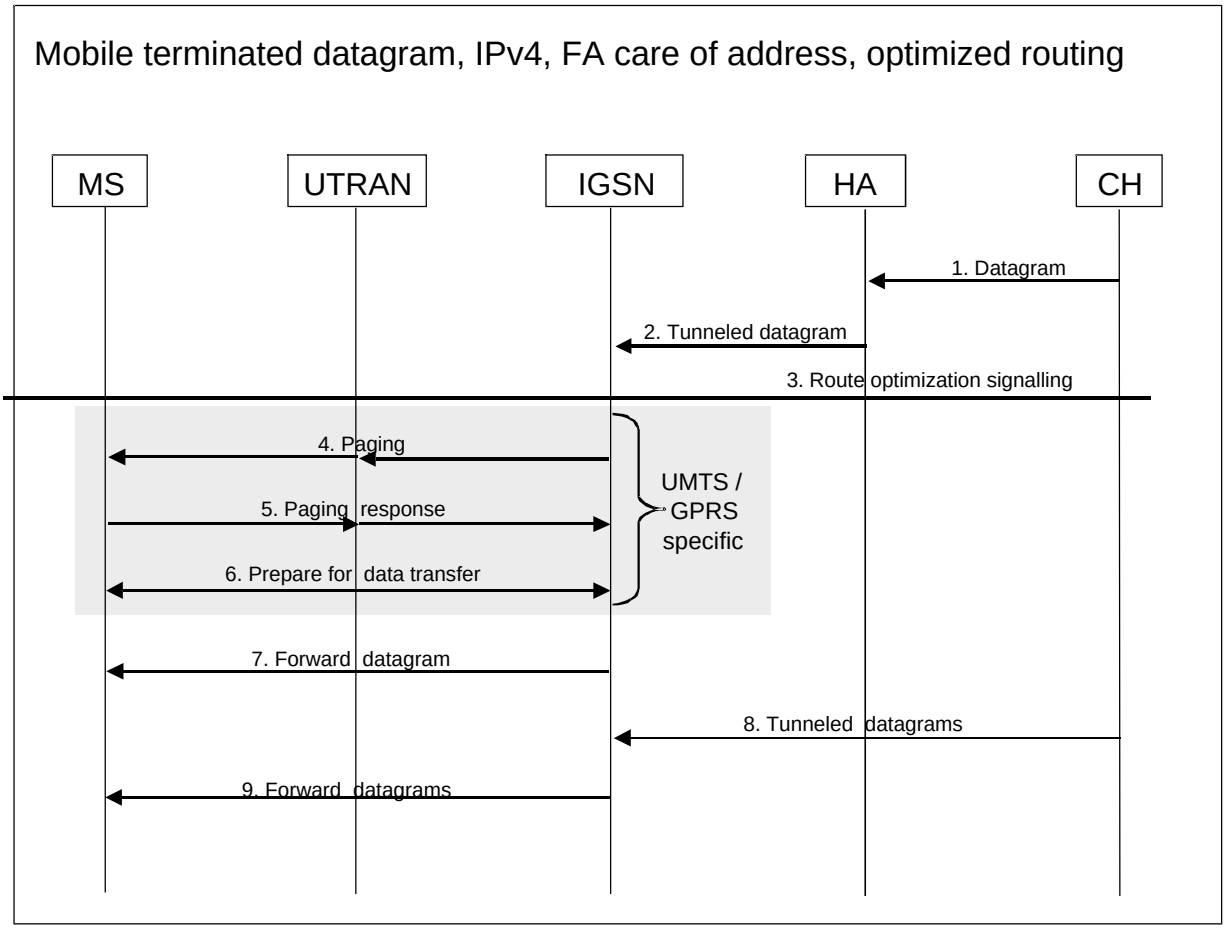


Figure 11.7.2b: Delivery of mobile terminated datagrams, optimised routing

11.8 Service Support

11.8.1 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.

11.8.1.1 Differentiated Services

The Differentiated Services (DS) architecture [34], [28] 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 behaviour aggregates. Each behaviour aggregate is identified by a single DS code point in the IP header. Within the core of the network, packets are forwarded according to the per-hop behaviour (PHB) associated with the DS code point. 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 behaviours currently being standardised 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 diffserv traffic condition components using RSVP signalling.

11.8.1.2 Integrated Services

The Internet Integrated Services framework RFC 2215 [24] and RFC 2216 [25] 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.

11.8.1.3 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 subclause 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 [32] 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 minimise 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 minimise 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.

11.8.2 Multi Protocol Support

Multi protocol support over MIP tunnels can be performed using GRE encapsulation RFC 1701 [17] and RFC 1702 [18]. 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.

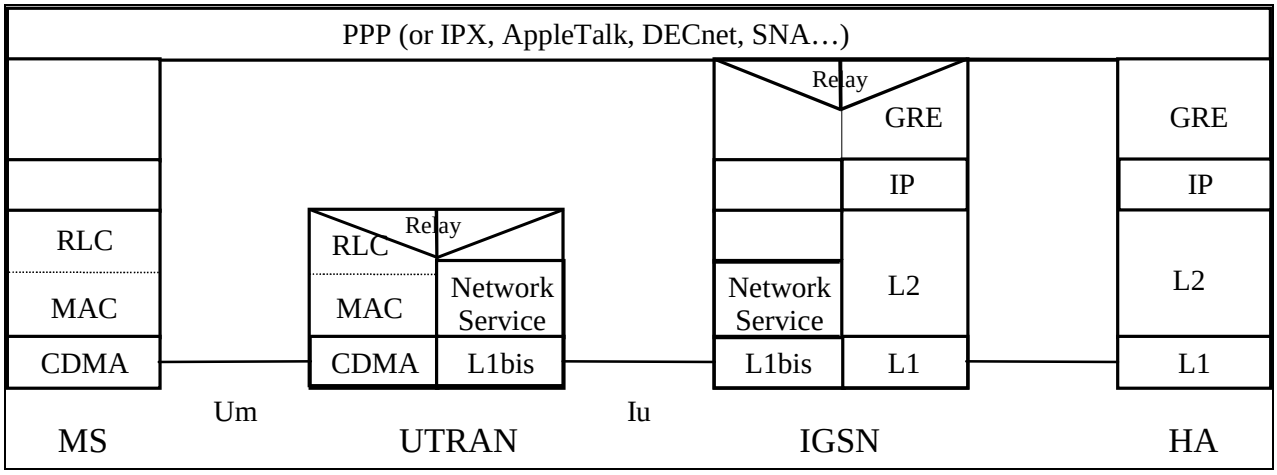


Figure 11.8.2a: Multiprotocol support in Mobile IP(+)

11.8.3 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.

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(+)

Since operators will upgrade their networks independently of each other, it is necessary to ensure that a step 3 Mobile IP network can operate properly with UMTS/GPRS networks not supporting Mobile IP during a transition period. There is also a need to support legacy terminals, i.e. without MIP support, in a step 3 MIP network.

The table below considers all possible cases of roaming and handover between legacy networks and step 3 MIP networks. It also takes into account whether or not the home network supports MIP (any step). The purpose is to define for which cases the Gn and Gp interfaces are mandatory. Note that the user planes and signalling planes are handled separately.

The signalling plane for the Gn and Gp interface is mandatory. In order to support legacy terminals, an operator can continue the operation of the full set of Gn and Gp interfaces between IGSNs, between IGSNs and SGSNs and between IGSNs and GGSNs. If Mobile IP Surrogate Registrations mechanisms will be viable to support the mobility of non-Mobile IP enabled terminals (see subclause 12.2.1), their use may lessen the requirement to support the Gn and Gp for the same purpose. This is for further study.

Packet forwarding between IGSNs at handover time can be performed with the Gn and Gp if no smooth handover Mobile IP mechanisms are available to do that.

It is envisaged that the use of the Gp interface between IGSNs and a GGSN in different PLMN not supporting Mobile IP, is necessary in order to support handover of terminals roaming from that PLMN. An operator needs to support this interface as long as it supports roaming agreements with non-MIP operators. The Gp interface also needs to be used between IGSN and SGSN if handover shall be supported from native GPRS/UMTS networks.

If an operator supports roaming agreements only with other PLMNs supporting mobile IP, then the interprovider interface is provided by Mobile IP itself and possibly by a Gp interface between IGSNs for packet forwarding at handover time (if no mobile IP mechanism for smooth handover is available).

The following table summarises the cases when Gn and Gp interfaces are mandatory or not. The interfaces have been divided in four groups. That is because these two interfaces shall support messages between an SGSN and a GGSN and this should be done in both signalling plane and user plane, i.e. four groups. Handover and roaming occur between first and second visited network. The numbers 1-10 correspond to the comments at the end of the table.

Does terminal support Mobile IP?	Does home network support Mobile IP?	Does first visited network support Mobile IP?	Does second visited network support Mobile IP?	Gn and Gp, SGSN-SGSN signalling	Gn and Gp, SGSN-SGSN transport	Gn and Gp, SGSN-GGSN signalling	Gn and Gp, SGSN-GGSN transport
Yes	Yes	Yes	Yes	M	4	X, 5	X, 5
			No	M	4, 6	X, 5	X, 5
		No	Yes	M	M	M, 7	FFS
			No	M	X, 3	X, 3	X, 3
	No	Yes	Yes	FFS, 10			
			No, 1	X			
		No	Yes	FFS, 10			
			No, 1	X			
No	Yes	Yes	Yes, 2	M	FFS	FFS	FFS
			No	M	M	3	3
		No	Yes	M	M, 3	M, 3	M, 3
			No, 8	X			
	No, 9	Yes	Yes	M	M, 3	M, 3	M, 3
			No	M	M, 3	M, 3	M, 3
		No	Yes	M	M, 3	M, 3	M, 3
			No, 8	X			

1. Co-located Care of Address.
2. Surrogate registration, FFS.
3. Standard UMTS case.
4. Needed if there is no Mobile IP smooth handover mechanism
5. Probably not needed, FFS.
6. A GGSN/FA is needed in home network.
7. Inform the home network IGSN
8. No IGSNs at all
9. Home agent in a different PLMN than one's home PLMN used for surrogate registration, FFS.
10. ME could maybe use Mobile IP even without a home PLMN supporting Mobile IP, FFS.

M – Mandatory
X – Not applicable
FFS - For further study

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 signalling 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 SGSNs and GGSNs. 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 12.2.1.1a, 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 corporate LAN. From the GGSN, there is a secure connection to the specified corporate network. There are different ways to realise 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 corporate 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.

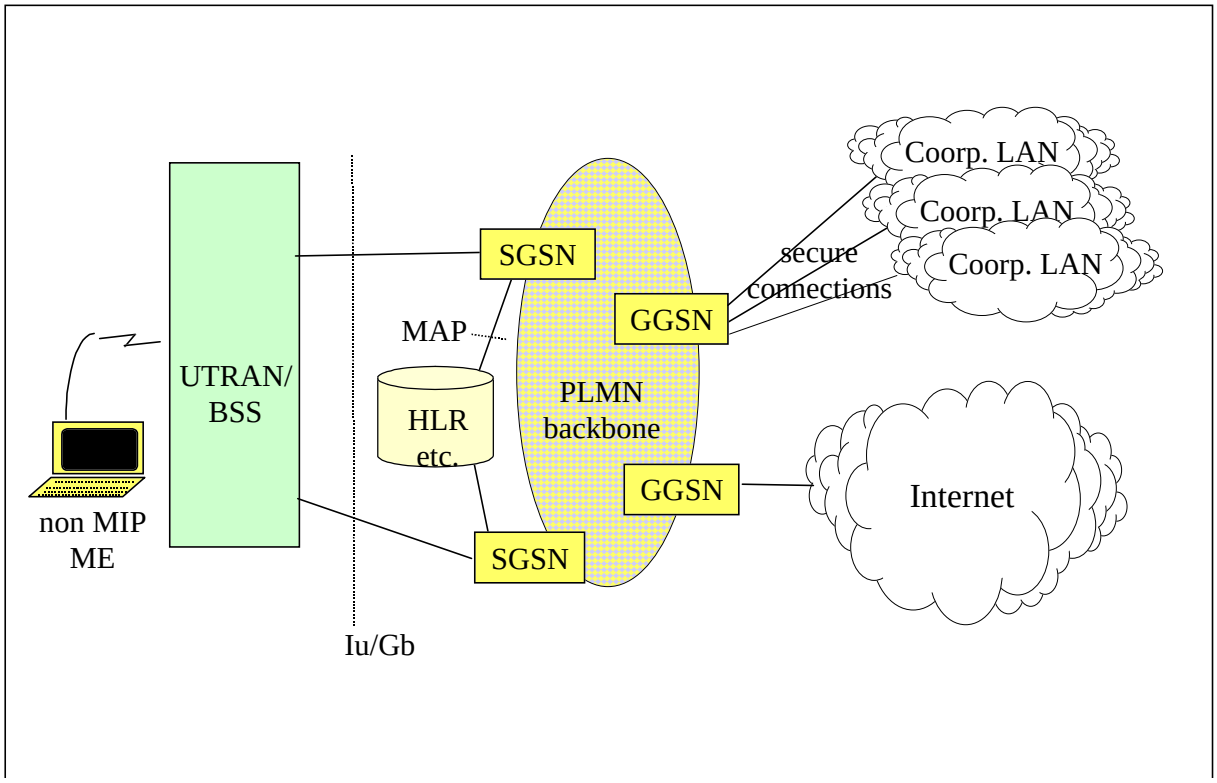


Figure 12.2.1.1a: The situation when the PLMN backbone mobility is handled with GTP. The mobile stays with the same GGSN throughout the UMTS/GPRS session

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 tunnelling is used RFC 2344 [26].

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 corporations 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 12.2.2a 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.

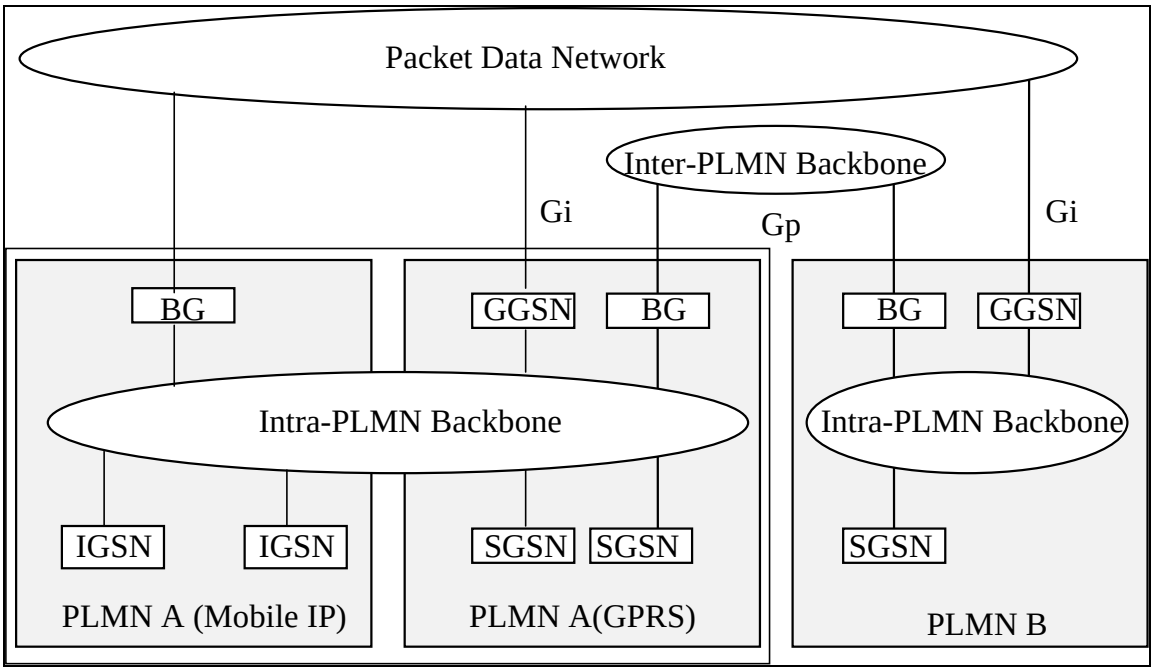


Figure 12.2.2a: Interoperability with GPRS

12.2.3 Interworking between UMTS/GPRS PLMNs and Mobile IPv6

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

13 Driving Forces

13.1 Mobile IP+ is standardised by the IETF

Since Mobile IP(+) is standardised 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) will be used for Authentication, Authorisation 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.

13.2 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).

13.3 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.

13.4 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.

14 Open Issues

The following open issues are identified and may be placed in the following categories: A. Those which identify further studies and specification required in the 3GPP; B. Those where study is underway elsewhere, which the 3GPP is requested to co-operate with; and C. Those where no specific solution or required study is identified or proposed.

1. A number of interoperability issues have been identified for inter-working between Step 3 and pre-Step 3 networks for a number of cases of roaming with Mobile IP enabled terminals, see the table in subclause 12.2. The study of these issues is critical to the migration to and the deployment of Mobile IP in network scenario step 3.

2. A number of issues have been identified for the backward compatibility of non-Mobile IP enabled mobiles, in step 3 networks where Mobile IP is used to support inter-IGSN handover and roaming, see chapter 12. The study of these issues is critical to the compatibility of terminals and UMTS networks.

3. The use of and migration to IPv6 requires further study for all of the identified three steps. The general aspects of these issues are a major study of the IETF.

4. Security encompasses a set of issues which are considered in this report as critical requirements. These issues include: Lawful interception, Location Confidentiality, Data Privacy, Non-repudiation, Key distribution and Core Network security. These issues are considered to be outside the scope of this study and the expertise of the people involved in drafting this report. The IETF, ETSI TC Security and 3GPP SA3 are expert groups who should co-operate to further these issues and find solutions for the identified requirements.

5. AAA and the related protocols are in themselves not a security issue, however these protocols are expected to provide solutions to the roaming, security and management requirements. These protocols require securing in

terms of data integrity, data confidentiality and protection against replay attacks. AAA specifically addresses Authorisation, Authentication and Accounting and the transfer of the related data. This work is critical because it is still in progress in the IETF.

6. Support for other protocols besides IP, currently supported over UMTS GPRS at the application layer (e.g. PPP, X.25, OSP) needs to be considered further.

7. Support for QoS, especially for real-time traffic, is the subject of a continuing study. This has not been adequately pursued in this report. It is recognised as a critical issue for support in Mobile IP enabled networks, this is identified in subclause 11.8. Specifically the issues: QoS re-negotiation at the Foreign Agent for Steps 2 and 3; avoidance of triangle routing and performance during inter- and intra-domain handovers, require further study. Domain in step 2 is a UMTS PLMN, in Step 3 is an IP managed area determined by the Operator.

15 Conclusions

This Technical Report is a feasibility study of Mobile IP, based on IPv4 as described in [RFC2002], in combination with GPRS/UMTS. In this TR, MIP(+) is introduced in three steps.

The first step 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 LANs, and UMTS without loosing an ongoing session, e.g. TCP. Step 1 has already been agreed to be incorporated in GPRS/UMTS R99.

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 maintaining, for a short period of time, tunnels from the new SGSN to both the old and new GGSN/FA, potential problems with packet loss are minimised. 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. This step could possibly be introduced in R00. Changes to current specifications need to be done in order to make it possible to support the hand over between two GGSN/FAs.

The third step is to combine the SGSN and GGSN into one node, the IGSN, and to enable MIP+ handle inter IGSN handover , i.e. mobility within the PLMN CN and between networks. The signalling plane for the Gn and Gp interfaces is mandatory. The transport plane for the Gn and Gp interfaces will probably be needed for a transient period when not all GPRS/UMTS networks are MIP enabled. Route optimisation or something similar could be used to improve the support of inter IGSN routing area update. An alternative is to use GTP at inter IGSN routing area update. AAA protocols need to be developed to support a large-scale deployment of step 3. The relation of step 3 and GPRS/UMTS releases is FFS.

Annex A:
Mobile IP

A.1 Basic architecture

The basic assumption underlying the standardisation 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 organised 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 *tunnelling* 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[6] which the mobile terminal can use to acquire a valid address in the visited subnet.

[6] 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.

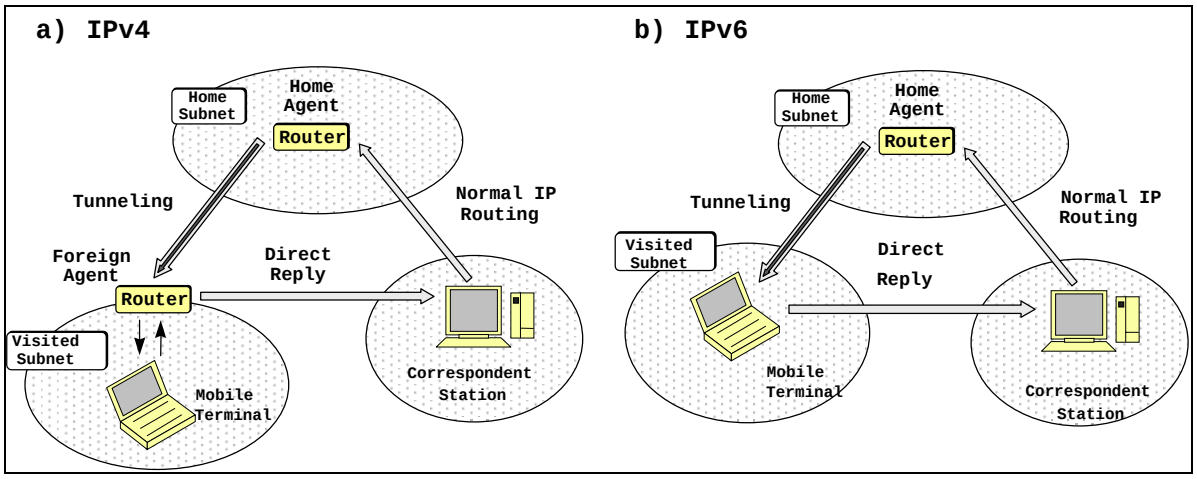


Figure A.1: Basic architecture for supporting IP mobility

A.2 Route optimisation

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 analysing a possible extension (*Route Optimisation*) 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 Optimisation 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 Optimisation 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 tunnelling 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 tunnelling mechanism, and sets up an optimised route which makes it possible to avoid passing through the home agent (figure A.2).

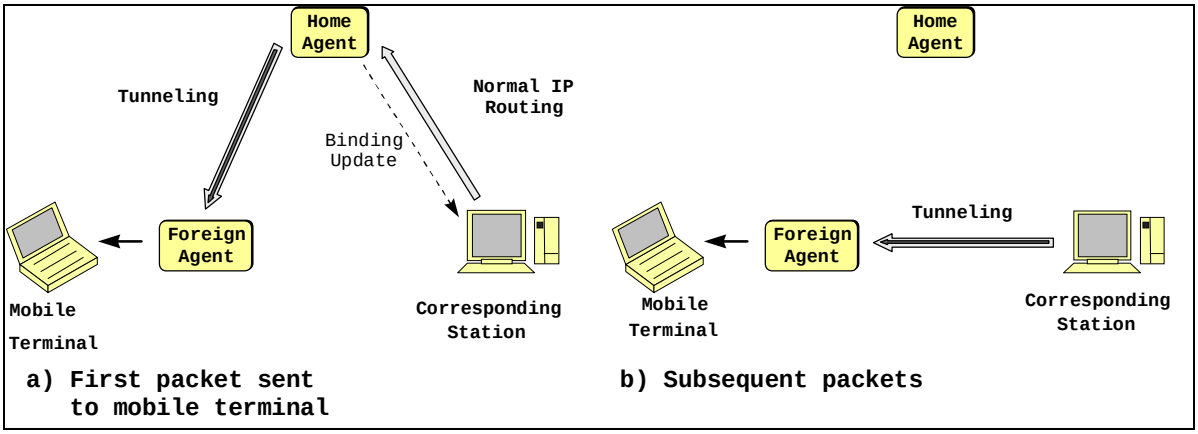


Figure A.2: *Route Optimisation* in IPv4

On its own, however, this procedure is not sufficient to guarantee permanent optimisation 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 Optimisation 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 tunnelling 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 optimised route between source and destination (figure A.3).

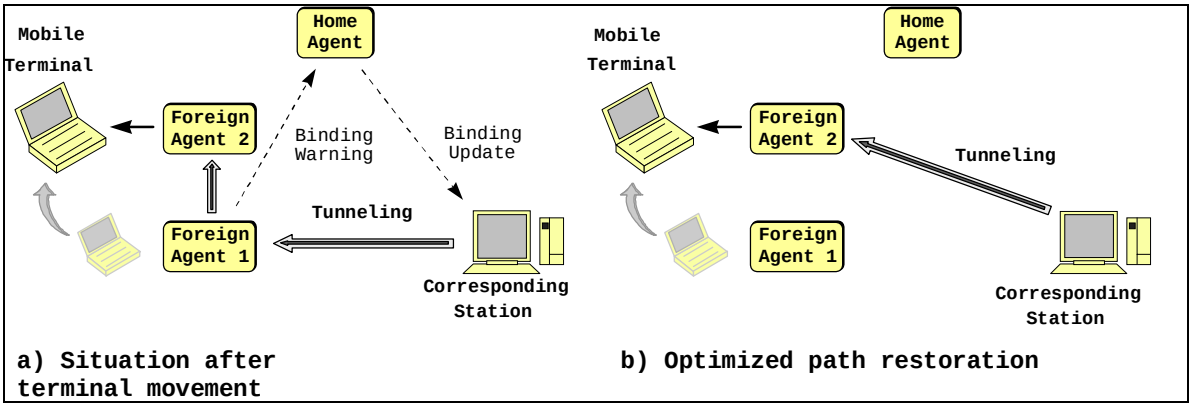


Figure A.3: Mobile terminal movement with notification to the previous foreign agent

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 Optimisation 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).

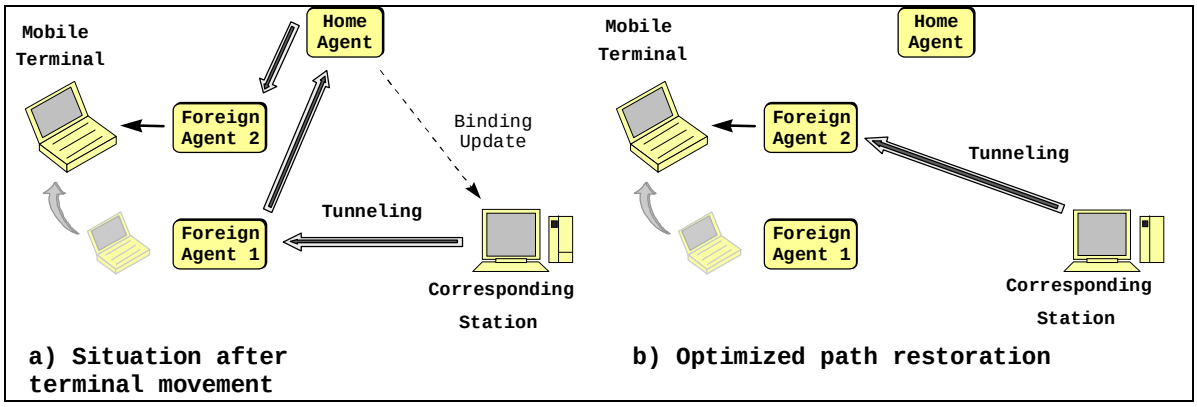


Figure A.4: Mobile terminal movement without notification to the previous foreign agent

The Route Optimisation mechanism specified for IPv4 has the advantage of minimising signalling 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 Optimisation 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.

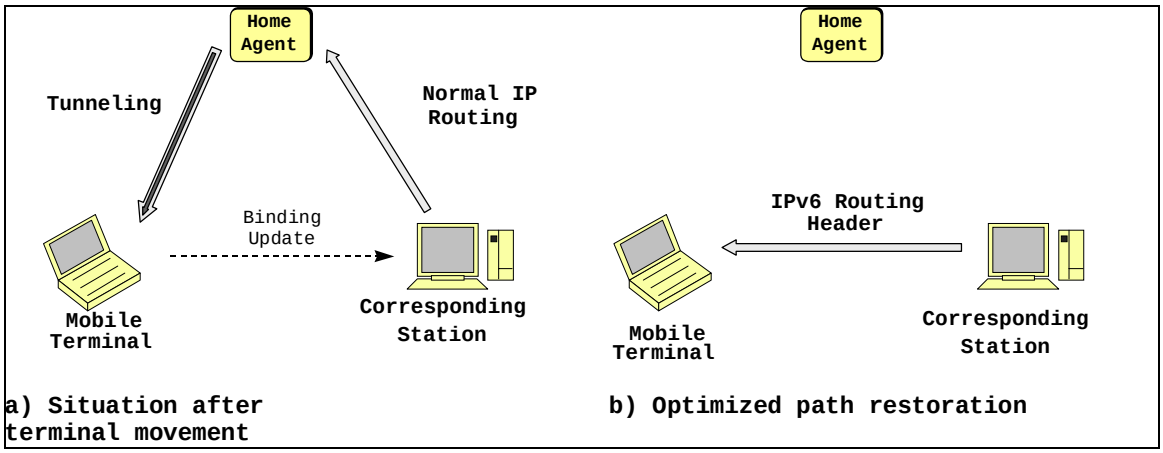


Figure A.5: *Route Optimisation* in IPv6

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[7] 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 minimises signalling 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.

---

7 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.

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 tunnelling mechanism, with IPv6 the same result is achieved using a *Routing Header*, i.e. a 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" tunnelling, 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 depends 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 Optimisation 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 organisation, 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:
Document change history

Date	Version	Information about changes
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 subclause 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 subclause 7.3) and s2m99068 (new subclause 10.2)
6 October 1999	Version 1.0.0	• No changes compared to previous version
22 October 1999	Version 1.1.0	• Included Tdoc s2m99084 (on step 3 procedures) and • Tdoc s2m99085 on UMGS/GPRS Charging

18 November 1999	Version 1.2.0	• Reordering as in Tdoc s2m99095 • Included Tdoc s2m99106 (Text on AAA) • Included Tdoc s2m99108 (Text on Step 2 introduction) • Included Tdoc s2m99109 (Text on IGSN description) • Included Tdoc s2m99110 (Text on security) • Included Tdoc s2m99114 (Text on Open Issues) • Included Tdoc s2m99115 (Text on Conclusions) • Included Tdoc s2m99116 (Text on AAA) • ME (Mob. Equipm.) is the UMTS term and MS (Mob. Station) is the GPRS term for the same thing. Now the entire document uses ME. • Editor's comments removed • Renumbering of all subclauses, including compression and reference update. • Renumbering of all figures. New nomenclature of figures to support scaling. • Definitions (ch.3.1) updated. • Abbreviations (ch. 3.3) corrected. • References (ch.2) updated. • Obvious misspelling of words and extra/to few linefeeds, spaces etc. was corrected. • Chapters 13, 14, 16, 17, 18 and 19 have been deleted. • Annexes B, C and D have been deleted. • Apart from above mentioned changes minor changes to the text have been made, mostly deletions.
13 December 1999	Version 2.0.0	• Raised to v.2.0.0 for approval by TSG SA #6. Technical content identical to the one of v.1.2.0.
May 2000	Version 3.0.0	• Raised to v.3.0.0 after lot of efforts to put the document in a correct shape

History

Document history		
V3.0.0	May 2001	Publication