TSG-SA meeting #3
26 - 28 April 1999
Yokohama

TSGSP#3(99)154

Title: **UMTS ETR XX.yy Mobile IP, version 0.5.0**

Source: **TSG SA WG2**

Purpose: **Information**

Extract from meeting report SMG#28 meeting, February 1999:

"UMTS 30.01, *UMTS Baseline document*, in Tdoc SMG P-99-112 was presented by Antun Samukic to SMG#28. The document shall be updated according to major decisions at SMG#28. The updated document shall be distributed to SMG for approval by 22 February 1999. The UMTS 30.01 shall be transferred to 3GPP. Further use of the UMTS Baseline document for SMG can be studied later."

This version of the UMTS Baseline document reflects the last approved version of the document by SMG and is transferred and given to 3GPPP for further work.

3GPP - TSG SA - WG2 – MIP
9-11 March 1999
Stockholm - Farsta

Tdoc S2 M 99 009

Title: Draft version 0.5.0 of WI/ETR ”Combined GSM and Mobile IP mobility handling in UMTS IP CN”

Date: 1999-02-26

Source: Rapporteur (elisabeth.a.hubbard@telia.se)

Purpose: For approval

Introduction

This document contains the current draft, v0.5.0, of the technical report on “Combined GSM and Mobile IP mobility handling in UMTS IP CN”

Two revised documents from the Heathrow meeting have been included. These are Tdocs C-99-055 and Tdocs C-99-057.

DTR/SMG-YYXXU V.0.5.0 (1999-02-26)

Draft Technical Report

Combined GSM and MobileIP Mobility Handling in UMTS IP CN UMTS YY.XX version 0.5.0

European Telecommunications Standards Institute

Reference
DTR/SMG-0323XXU

Keywords
UMTS, Core Network, IP, MobileIP, Mobility

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex – FRANCE

Office address
650 Route des Lucioles – Sophia Antipolis
Valbonne – 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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
Error! Bookmark not defined..fr
Error! Bookmark not defined..etsi.fr

Contents

1 Intellectual Property Rights

2 Foreword

3 Introduction

4 Scope

This document will contain a feasibility study on using a standard IP backbone for UMTS CN, which would use a combination of GSM mobility management and Mobile IP. Issues related to network architecture, security, evolution from GPRS, services as well as dependencies on IETF will be examined with respect to the current GPRS standard….

5 References

This ETS incorporates, by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies. IETF standards (RFC's) and internet drafts are available at **Error! Bookmark not defined.**.ietf.org/

ETSI TC-SMG UMTS 22-01: "Services Principles"
ETSI TC-SMG GSM 03.02
ETSI TC-SMG GSM 03.60
ETSI TC-SMG GSM 11.14
ETSI TC-SMG GSM 30.01
ETSI TC-SMG GSM 23.01
ETSI TC-SMG UMTS 23.20 "Evolution of the GSM platform towards UMTS"

[RFC 1518] IETF RFC 1518Y, Rekhter, T. Li "An Architecture for IP Address Allocation with CIDR", Sept. 1993
[RFC 1519] IETF RFC1519V, Fuller et Al. "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", September 1993.

[RFC 2002] IETF RFC 2002, C.E.Perkins, ed. "IPv4 Mobility Support", October 1996.
Error! Bookmark not defined..doc.ic.ac.uk/computing/internet/rfc/rfc2002.txt
[RFC2003] IETF RFC 2003, Perkins, C., "IP Encapsulation within IP", October 1996.
Error! Bookmark not defined..doc.ic.ac.uk/computing/internet/rfc/rfc2003.txt
[RFC2004] IETF RFC 2004, Perkins, C., "Minimal Encapsulation within IP", October 1996.
Error! Bookmark not defined..doc.ic.ac.uk/computing/internet/rfc/rfc2004.txt
[RFC2005] IETF RFC 2005, Solomon, J., "Applicability Statement for IP Mobility Support", October 1996
Error! Bookmark not defined..doc.ic.ac.uk/computing/internet/rfc/rfc2005.txt
[IP4ADDR]IETF RFC2101, B. Carpenter et. Al. " IPv4 Address Behaviour Today"

[RFC2131] IETF RFC 2131, "Dynamic Host Configuration Protocol", March 1997.
Error! Bookmark not defined..doc.ic.ac.uk/computing/internet/rfc/rfc2131.txt
[MIP-optrout] Internet draft, "Route Optimization in Mobile IP", November 1997.
Error! Bookmark not defined..ietf.org/internet-drafts/draft-ietf-mobileip-optim-07.txt
[MIPIPv6] Internet draft, "Mobility Support in IPv6", November 1998.
Error! Bookmark not defined..ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-07.txt
[MIPv2] Internet draft, Perkins, C., "IP Mobility Support version 2", November 1997,
Error! Bookmark not defined..ietf.org/internet-drafts/draft-ietf-mobileip-v2-00.txt
[MIP-DIAM] Internet draft, Calhoun, P. "DIAMETER Mobile IP Extensions", November 1998
Error! Bookmark not defined..ietf.org/internet-drafts/draft-calhoun-diameter-mobileip-01.txt,
[NAR] Internet draft, G. Montenegro, May 1998,
draft-montenegro-aatn-nar-00.txt
[TEP] Internet P.Calhoun et al., "Tunnel Establishment Protocol" March 1998
draft **Error! Bookmark not defined.**.ietf.org/internet-drafts/draft-ietf-mobileip-calhoun-tep-01.txt

6 Definitions and abbreviations

6.1 Definitions

The following definitions have been introduced within this document.
[*Editor's comment: with "Mobile IP" is meant more than RFC 2002, i.e. also some of the current drafts and maybe more. The discussion about a definition is going on within the MIP drafting group.*]

6.2 Abbreviations

For the purposes of this ETS the following abbreviations apply.

Note: all chapters will discuss the MobileIP scenario with respect to the current GPRS standard.

7 Working Assumptions

[Editor's comment: this chapter is a place holder for working assumptions until the document is finished and everything properly documented in other chapters]

8 Reqirements on UMTS Packet Domain

[Editor's comment: it is necessary to have the requirements stated to justify the target architecture and to perform a comparison between GPRS and MIP]

9 Current Status of Mobile IP

[Editor's comment: this should include both IETF standardization work and deployment. A clearification is needed on what parts are describe in RFC's and what parts are presented in drafts]

10 Overview of Target Architecture

10.1 Network Architecture

The network architecture is based on and will evolve from the current GPRS backbone elements. A combined SGSN and GGSN, here called IGSN…

[Editor's comment: see Appendix D. Part of that text and figures need to be updated and included here]

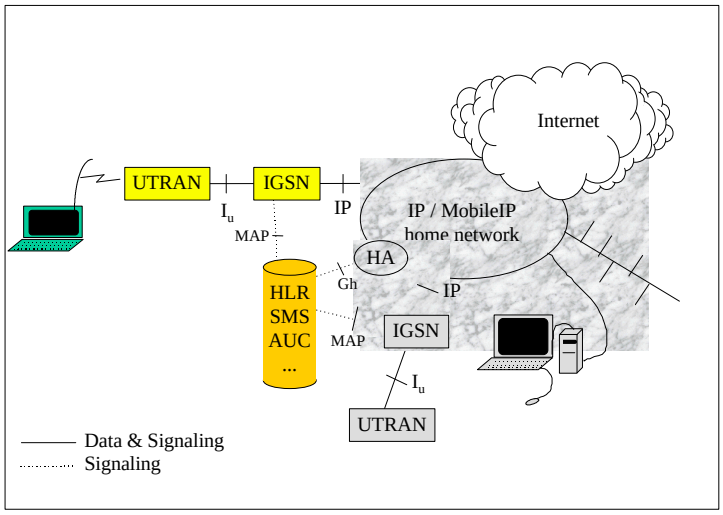


Figure 1. One possible network implementation –figure to be improved

11 Evolution and Intermediate Stages

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

1. Stage 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. The SGSN and GGSN can be co-located without any alterations of the interfaces. However, to obtain more efficient routing, the MS could change GGSN/FA, i.e. PDP context and care-of address after an inter SGSN handover if it is not in active mode. MS's who are in active mode during the inter SGSN handover could perform the streamlining when it goes into standby mode. This is similar to the anchor-MSC concept and the Gn interface is utilized until MIP streamlining, i.e. change of care-of address, can occur.

3. The third stage is to let MIP handle also handover during ongoing data transfer, i.e. while the mobile is in active mode. The Gn interface is here only needed for handling roaming customers without support for MIP.

11.1 Stage 1 – Offering Mobile IP service

Mobile IP has the benefit of being access system independent, which allows users to roam from one environment to another, between fixed and mobile, between public and private as well as between different public systems. Assuming a minimal impact on the GPRS standard and on networks whose operators do not wish to support MIP, leads to the following requirements:

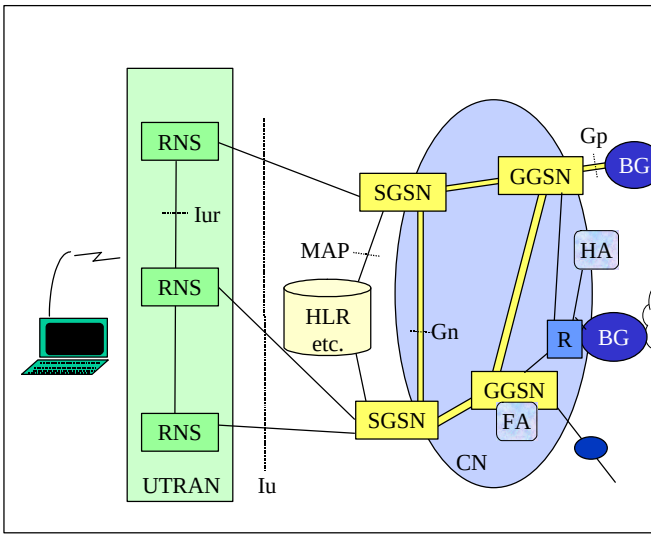


Figure 2. Core network architecture with GPRS MM in and between GPRS PLMN's and Mobile IP MM between different types of systems and optionally between GPRS PLMN's.

- The MS must be able to find a FA, preferably the nearest one. The underlying assumption is that FA's are located at GGSN's and that not all GGSN's may have FA's. One FA in a PLMN is sufficient for offering MIP service, however for capacity and efficiency reasons, more than one may be desired. This means that the MS must request a PDP context to be set up with a GGSN that offers FA functionality. One solution is to define a new PDP type, but this should be handled in the SMG4 MIP WI.

- While setting up the PDP context, the MS must be informed about network parameters of the FA, e.g. care-of address.
- Furthermore, the interaction between the GGSN and the FA needs to be studied more in detail. With the assumption that FA care-of addresses are used, the FA needs to detunnel incoming packets and, together with the GGSN, map the home address of the MS to a PDP context.

Depending on the capabilities of a visited network, two roaming schemes can be identified; GPRS roaming and MIP roaming. With GPRS roaming, we mean roaming via the Gp interface and the use of a GGSN in the home network, which is necessary when the visited network does not offer any FA's. In those cases where the visited network offers a FA, either a GGSN/FA in the visited or in the home network can be utilized.
It is assumed that the MS keeps the same care-of address as long as the PDP context is activated.
A typical network is shown in Figure 2.

11.2 Stage 2 – Intermediate GPRS-MIP system

One way to implement a GPRS backbone is to co-locate the SGSN and GGSN, as depicted in Figure 3 . This might be favorable for operators with a strong interest in utilizing standard IP (IETF) networks as far as possible and does not require any changes in the current GPRS protocol architecture.

In stage 1, the assumption was that the MS stays with the same care-of address, during a session, i.e. as long as a PDP context is activated. A very mobile MS, might perform several inter SGSN HO's during a long session which may cause inefficient routing. As an initial improvement, a streamlining procedure, similar to the anchor-MSC concept in the GSM CN could be introduced:
If the MS is in an inactive state, i.e. no data transfer, while moving from one SGSN to another, a new PDP context could be setup between the new SGSN and its associated GGSN at the handover. The MS will get a new care-of address. The procedure for informing the MS that it has arrived to a new network has to be defined.
If the MS is in an active state, e.g. being involved in a TCP session, the MS would move from the old SGSN to the new one while keeping the PDP Context in the old GGSN as long as it stays in active state. Once the data transfer is terminated and the mobile is about to go into an inactive state, the PDP Context can be changed to the GGSN associated with the new SGSN and a new care-of address can be obtained.
Buffers, which already exists in the SGSN's for preventing data loss at inter SGSN HO's, will, with this procedure, be reused as they are. This procedure also has some advantage regarding the handling of firewalls, which are assumed to be attached to the GGSN's. Today, there is no standard for changing firewall during e.g. a TCP session.

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

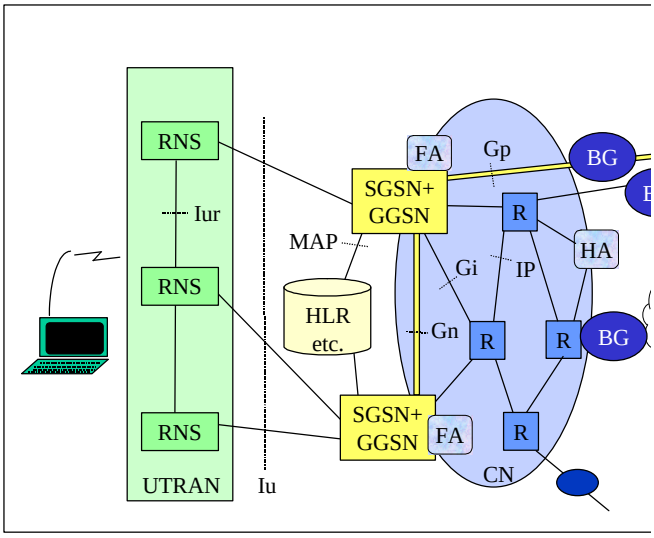


Figure 3. Core network architecture where GPRS MM handles active mobiles and Mobile IP streamlining at inter SGSN handover. The SGSN and GGSN are here co-located.

11.3 Stage 3 – Using Mobile IP for Intra System Mobility

The third and last stage is to let MIP handle all intra system mobility, including all handovers between GGSN's or IGSN's. This is depicted in Figure 4, where the IGSN represents an integrated SGSN/GGSN. The Gn and Gp interfaces may optionally be kept to handle roaming customers, whose terminals do not support MIP and the operator's own customers roaming to networks without MIP functionality. This would also allow operators to support 2G services using 2G equipment (e.g. LAN access via a GGSN). This is the target architecture of this document and hence the requirements on the UMTS part of the network as well as the requirements on MIP are described in other chapters.

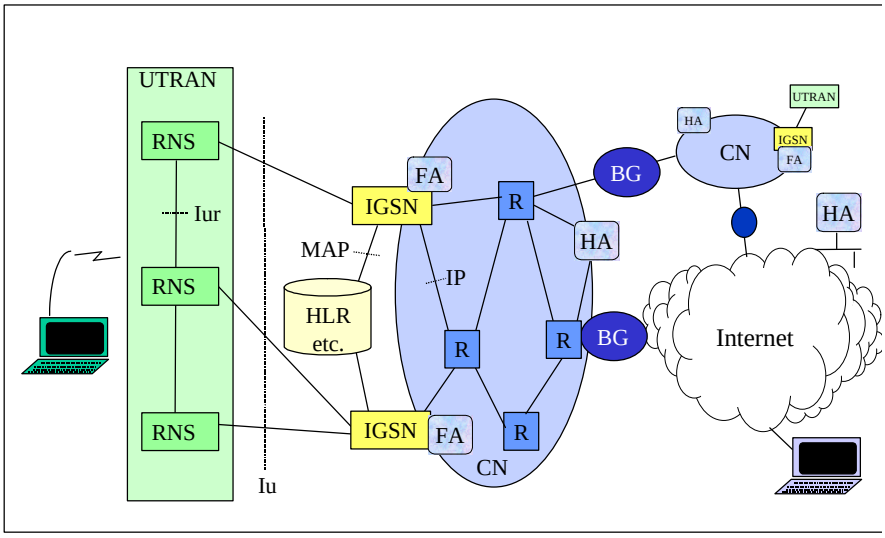


Figure 4. Core network architecture with Mobile IP MM within the CN and between different types of systems and between GPRS PLMN's.

12 Target Architecture

12.1 Network Issues IPv4

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

12.1.1 Basic Principles

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

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

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

12.1.2 Mobile IP Manages Macro Mobility Only

Mobility events which do not result in the mobile node entering the domain of a mobility agent different from the current mobility agent domain are transparent to mobile-IP. Therefore, only macro mobility events require mobile IP level handling. A design assumption of mobile IP is that such macro mobility events do not happen more than **once**

per second. The UTRAN must be designed so that mobile IP is not affected by mobility events more frequently than that.

12.1.3 Care-of Addresses

The result of implementing the colocated-COA solution is that FAs are not required. However, until IPv6 is available and implemented, the following reasons make the FA-COA the preferred choice for UMTS:

- Using an address per mobile node is demanding in terms of address space consumption (e.g. no dedicated IP address from the address space owned by the UMTS operator is necessary for a remote network access).
- Using a colocated COA the number of mobile nodes a particular subnetwork could simultaneously support would be limited by the number of addresses administratively assigned to it, e.g. the users a network entity controlling a subnet can handle would be limited by the number of IP addresses allotted to it (hence a waste of IP addresses or an unnecessary limitation would be the eventual consequences) .
- Using a colocated COA the mobile node would be the tunnel endpoint, hence unnecessary overhead over the radio interface.

Therefore, at least until IPv6 is deployed, UMTS operators will more than likely prefer the FA-COA option of mobile-IP.

12.1.4 Location of the HA and the FA

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

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

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

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

12.1.5 Discovery of the FA

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

12.1.6 Compound Tunnels

There is currently a well developed proposal (Tunnel Establishment Protocol – TEP- [draft-ietf-mobileip-calhoun-tep-01.txt]) which would allow a UMTS operator to establish *compound mobile IP tunnels* by introducing the concept of a Gateway Foreign Agent (GFA). The GFA behaves as a HA for a FA and downstream GFA, and as a FA for a HA and upstream GFA. Two benefits of the GFA (i.e., compound tunnels) are:

- **Effects of mobility events can be limited** to the UMTS operator's domain, by placing a GFA between FAs in the UMTS operator's network and the HA in a remote network. The segment of the tunnel between a GFA and a HA in the remote network is used only to provide remote network access via compulsory tunnelling. Only the segment of the tunnel between the GFA and FAs changes when the MN changes FA.
- **Trust management is made simpler**, since the tunnel between the UMTS operator's network and a remote network is not affected by mobility events, therefore no re-negotiation of session keys is necessary as the mobile changes FA.

12.1.7 Reverse tunnels

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

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

It's clear that 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).

12.1.8 Surrogate Registrations

The TEP [TEP] specification introduces the concept of surrogate registration. This concept is necessary for the operation of the GFA, but it can turn out to be useful also in order to set-up tunnels without requiring the mobile node to implement a mobile IP stack, since the FA could *surrogate* the mobile node in performing Mobile IP registrations with the Home Agent. The use of surrogate registrations has a potential use in supporting non mobile IP aware terminals using a mobile IP based infrastructure. In particular non IP mobile terminals and dial-up users handling are the areas of applicability which make this concept most attractive. How to actually use it in UMTS is FFS.

12.1.9 Intra System Handover

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

- *inter RNC and intra IGSN – should be handled over Iu, which means that is can be handled the same way for IGSN's as for SGSN's*
- *inter RNC and inter IGSN – means streamlining in the CN in connections with SRNS Relocation – distinguish cases with and without support from Iur interfacE.*

See also chapter with traffic cases]

12.1.10 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

Let's 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 interoperate with the GPRS PLMN B in a single piece of equipment.

In Figure 4 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.

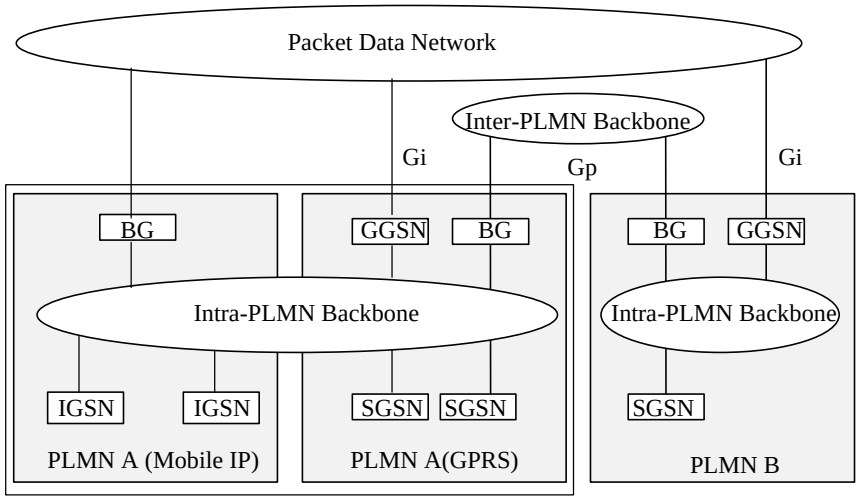


Figure 5 Interoperability with GPRS

12.1.11 Inter System Handover (ISHO)

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

12.2 Network Issues IPv6

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

- Mobile IPv4 allows the use of Foreign Agents (FAs) to forward traffic thus requiring one care of address for multiple mobile stations, or the use of co-located care-of addresses (coa). In contrast MIPv6 supports co-located coa's only.
- Route optimisation is an add-on to MIPv4 whereas it is an integral part of the MIPv6 specification.
- MIPv4 route optimisation still requires traffic to be tunnelled between the correspondent host (CH) and the mobile station. In MIPv6 packets can be forwarded with no tunnelling, only the addition of a routing header.
- In MIPv4 the Home Agent (HA) must be involved in the setup of optimised routes. In MIPv6 the mobile station can initiate an optimised route to a CH directly (without involving the HA), and therefore more quickly and efficiently.
- In MIPv4 a coa is obtained from a FA or via DHCPv4. In MIPv6 a coa can be obtained via IPv6 stateless or stateful address auto-configuration mechanisms.
- In MIPv4, separate Mobile IP specific messages are required to communicate with the FA, HA and if employing route optimisation, CHs. In MIPv6, Mobile IP specific information can be piggybacked onto data packets.
- The ability to provide smoother hand-over in MIPv4 is an add-on feature that forms part of the route optimisation protocol. In contrast support for smoother hand-over is an integral part of the MIPv6 specification.
- In MIPv4 reverse tunneling is required to avoid ingress filtering problems (where firewalls drop the mobile's outgoing packets) since packets are sent with the home address as the source. In MIPv6 packets are sent with the coa as the source address, hence there are no ingress filtering problems.
- 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. Previous subchapter describes how MIPv4 can be employed in UMTS networks. The remainder of this document describes the implications if MIPv6 is employed rather than MIPv4. Wider issues must be considered when comparing the deployment of, or migration between IPv4 and IPv6 networks in general. These are a topic for further study.

12.2.1 Care-of Addresses

In MIPv4, FA allocated COAs (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 COAs are allocated differently, both MIPv4 and MIPv6 need interaction with other IGSN protocols to forward the IP packets over the correct logical link.

12.2.2 Location of the HA and the FA

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

12.2.3 Discovery of the FA

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

There could be potential problems with employing stateless or stateful address autoconfiguration to obtain the COA for MIPv6 in UMTS. This is because these protocols require duplicate address detection (DAD). DAD, in its current form, requires messages to be multicast to all MSs on the same link, and, can significantly lengthen the time to obtain a COA compared to MIPv4. This issue needs to be resolved before UMTS operators can deploy MIPv6.

12.2.4 Use of Route Optimisation

Benefits of route optimisation include a reduction in delays between the CH and MS, 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 CHs. Furthermore it still requires packets to be tunnelled 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 MS 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.

12.2.5 Compound Tunnels

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

12.2.6 Reverse Tunnels

Reverse tunnels are not needed to avoid problems with ingress filters in MIPv6. However they may still be beneficial when the MS is concerned about location privacy.

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

12.2.7 Interworking with GPRS PLMNs and Inter-system Hand-over

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

12.3 Robustness and Scalability

12.4 Need for Broadcasting over Radio

Although mobile IP utilizes various router and agent advertisement messages, which normally are broadcasted over the local network, it is not necessary to broadcast these messages to all MS'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 MS is located and where the nearest router is located, it sends a router solicitation and gets a unicast ICMP router advertisment 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 MS wait for router and mobility agent advertisements:

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

The latter point is especially important when using this method also at handovers between IGSN's.
To inform the MS that it has changed subnetwork after a handover that requires streamlining in the CN, one dedicated message is needed on the link layer between the MS and the IGSN. Alternatively, the MS may detect the change of SGSN on the basis of other network parameters.

12.5 Traffic Cases

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

12.5.1 Attach

This section illustrates how an attach procedure could work. It includes registration with the HLR and the Home Agent. The Mobile IP procedures are according to [RFC 2002].

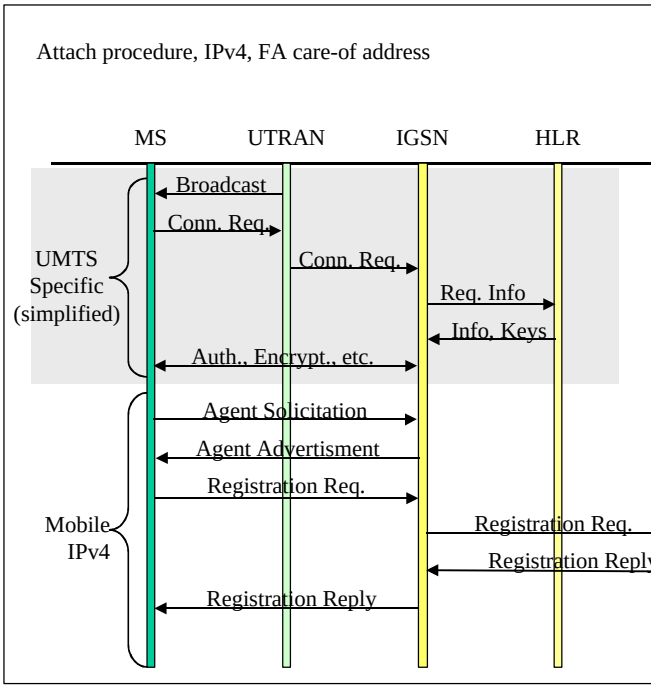


Figure 6. *The attach procedure. The UMTS specific part (shadowed) should be seen as an example.*

12.5.1.1 UMTS specific part

- When the mobile station (MS) arrives at a new UTRAN, it listens to the radio broadcast messages, which contain information about radio parameters, network and cell identity, etc. as well as e.g. information about available core networks, service providers, service capabilities etc.
- The MS sends a registration request including parameters such as identity, desired service provider etc.
- The UTRAN forwards the registration request to the IGSN, which processes it:
- The IGSN contacts the HLR of the mobile terminal to collect data to perform an authentication procedure.
- Once the terminal is authenticated and found to be allowed in the present UTRAN, all information over the radio interface can be encrypted. Encryption keys are obtained from the HLR/AuC.

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

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

The MS now starts communicating with the IGSN on the IP layer:

- The MS sends an agent solicitation message, which is a MoileIP specific version of a router solicitation ICMP message.
- The FA responds with a dedicated agent advertisement message, which contains network parameters and at least one Mobile IP care-of-address.
- The MS contact its home agent (HA) to register its new care-of address:
- The registration request is sent from the MS to the FA, which forwards it to the HA
- The HA replies with a registration reply that grants or denies the request.

- The registration reply is sent from the HA to the FA, which forwards it to the MS

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

12.5.2 Sending Packets

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

12.5.3 Receiving Incoming Packets

12.5.3.1 Mobile Terminated Datagrams, IPv4

The following section describes how incoming IP datagrams are handled in the different nodes. It is assumed that the Mobile Node has a FA care-of address, which is registered at the HA and that the MN is in (UMTS) stand-by mode when the incoming datagram arrives. The Mobile IP procedures are according to [RFC 2002].

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 procedures. If optimized routing is desired and if the correspondent node supports binding cache, the HA sends a binding update message to inform the correspondent node (CN) about the current care-of address of the mobile node. From now on, the correspondent node can send datagrams directly to the mobile node by tunneling them to the FA care-of address. This is depicted in Figure 7. If the correspondent node does not support binding cache, all packets will go through the HA as in

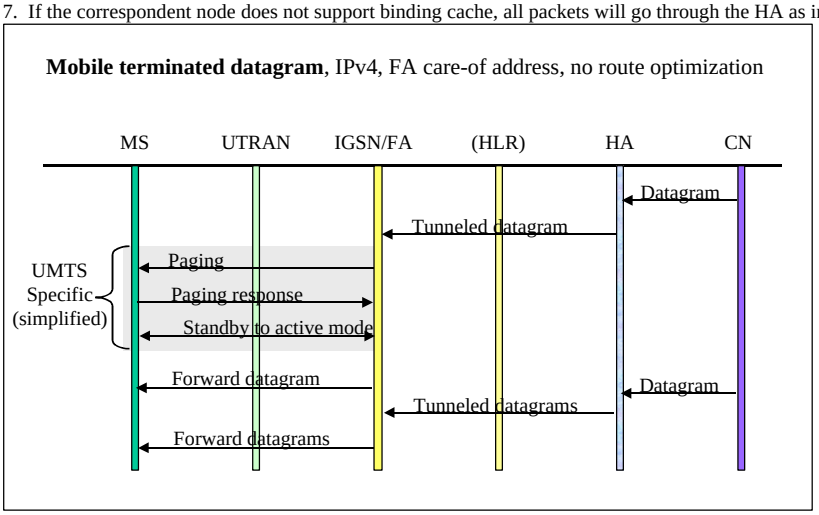


Figure 8.

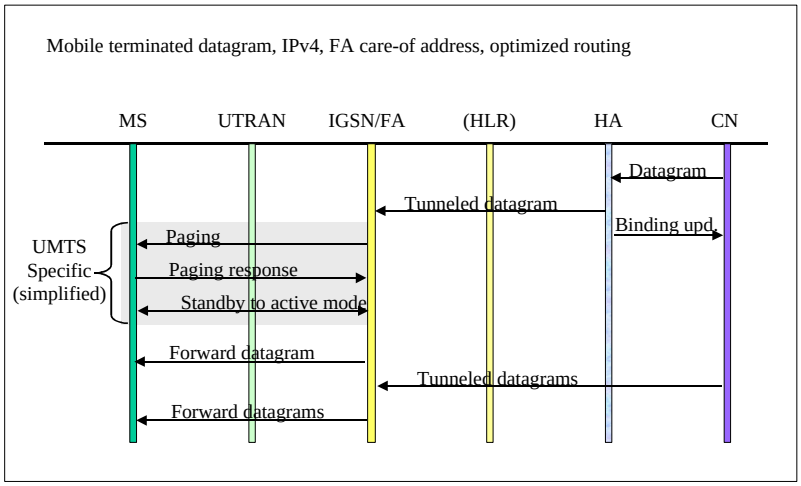


Figure 7. Delivery of mobile terminated datagrams, optimized routing.

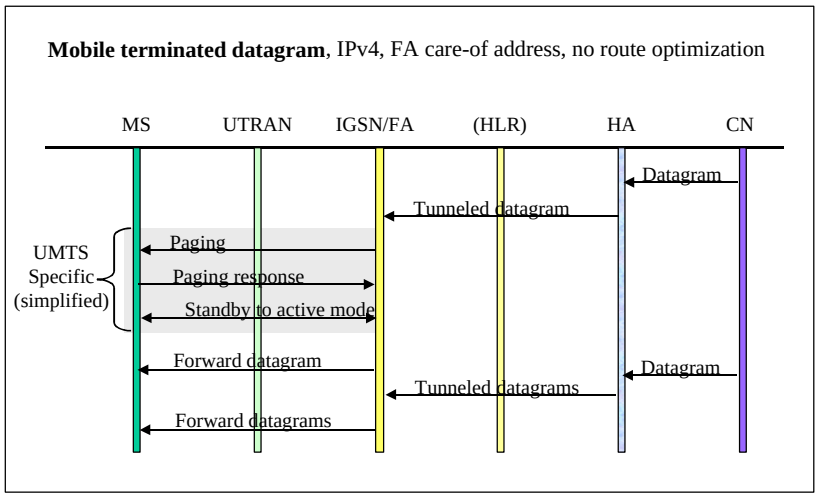


Figure 8. Delivery of mobile terminated datagrams, no route optimization.

12.5.4 Roaming

12.5.5 Handover Cases

12.6 Addressing

12.6.1 Addressing Issues in IPv4

The IPv4 address is a 32 bit string. Historically it has played both the roles of identifier and locator [IP4ADDR]. In fact it has been used both to identify the endpoints of an IPv4 session and to decide where to route packets.

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

CIDR allows aggregation of addresses on a finer grain resolution (aggregation happens on a per bit, instead of on a per octet basis), thus it allows the allotment of addresses to ISPs' customers with more flexibility and in a more efficient way. On the other hand the hierarchical and topology bound nature of CIDR entails that an address can't be kept by an organization if the provider changes. An organization would therefore have to renumber. In addition providers and corporations assign addresses on a temporary basis. Therefore the IP address is no more temporarily unique, hence the role of identifier is no more well suited by the IP address (let alone security reasons).

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

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

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

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

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

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

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

12.6.2 Addressing issues in IPv6

12.6.3 Private Addresses

12.7 Terminal aspects

The mobile terminals need to be enhanced with MIP software, which is rather simple. 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 needed UMTS specific functionality of all three stages in the MS at once.

12.8 Security, Roaming and AAA

12.8.1 Mobile IPv4 control messages: security issues

The standard requires mobile nodes to be authenticated when they update the HA about their current point of attachment to the network. The standard does not require that the mobile node is authenticated with the FA and that the FA is authenticated with the HA. There is a simple reason why this makes sense. Let's consider a cellular network operator who owns an IP backbone equipped with FAs and HAs for IP mobility support. HAs and FAs trust each other, only trusted mobile nodes can deliver packets to the FA (the radio link to the FA is secure and is granted only after UMTS authentication takes place), but even a trusted mobile station could redirect packets bound to another mobile node by spoofing its identity in registration messages, if not properly verified by home agents. This can happen because the data network identity and UMTS identity may be unrelated.

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

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

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

12.8.2 Mobile IPv6 control messages: Security Issues

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

12.8.3 Screening and Flooding

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

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

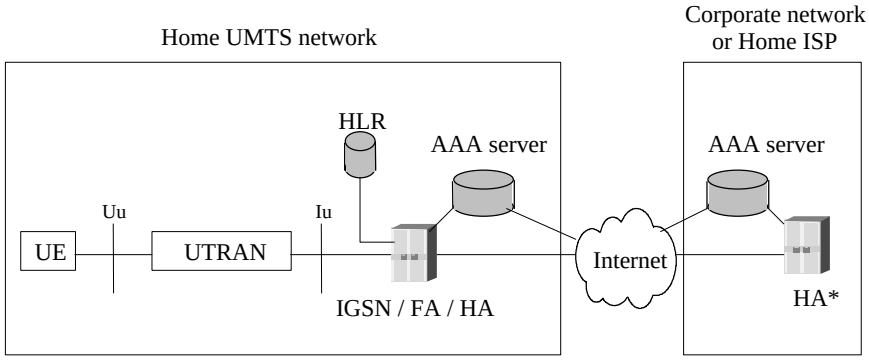
12.8.4 AAA (Authentication, Authorization and Accounting) and Roaming issues

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

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

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

Mobile IP will natively rely on data network AAA protocols and supports IP level roaming procedures via the NAI (Network Access Identifier) extensions. In a mobile IP based UMTS network **separation of radio access and data network identity** is natively supported. Below, some of the scenarios described are summarized in figure 1 and figure 2.



(*) It may be offered in outsourcing by the Home UMTS operator

Figure 9 - UE attached to the Home UMTS operator

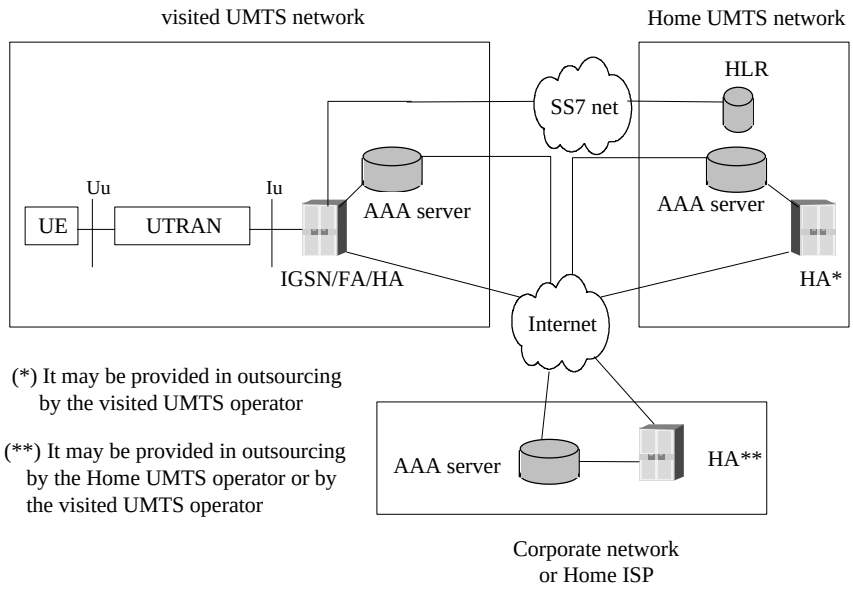


Figure 10 – UE not attached to the Home UMTS operator

As is the case for MIPv4, separate authorisation and accounting for UMTS access services and data network usage is desirable also for MIPv6. Procedures for AAA in MIP version 6 have not yet been addressed, but we can expect them to be similar to those used in version 4.

12.8.5 Use of IPsec

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

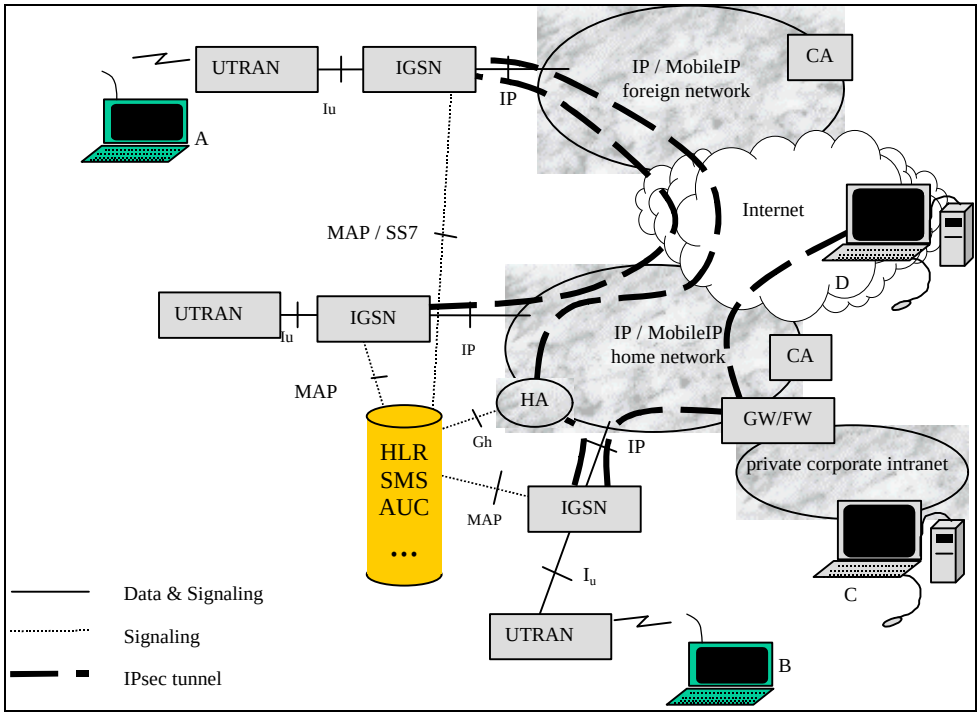


Figure 11. *IPsec for connection to private corporate intranet*

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

12.8.5.1 The importance of IP level authentication

It is shown in the scenarios below that even though the Gh interface allows the HA, when receiving a registration request, to see whether an MS is properly authenticated or not at the UTRAN. There is no way of knowing who sent the request without some sort of other authentication at IP level. The danger of replay attacks has to be addressed. Both these problems are solved natively in mobileIP.

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

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

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

On the GSM SIM card there is a secret key stored called Ki, which is 128 bits long and used for authentication purposes[UMTS22.00]. However, since it is not known outside the AUC and the SIM it cannot be utilized also for Mobile IP. Therefor a completely different set of keys must be used to authenticate Mobile IP messages.
A private/public-key technique could be used. If all users know the public key of their HA and all users public keys e.g. are stored in the HLR, and thus accessible for the HA, an authenticated exchange of MobileIP messages can be performed. Public keys can be transmitted from HLR to HA over the SS7 Gh interface without any risk of a security breach. An other way to store an distribute public keys is the use of a trusted third party and digital certificates as proposed recently in the IETF Internet draft ”Mobile IP and Public Key Based Authentication” [PubKey] by Stuart Jacobs of GTE Laboratories.

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

1. IPsec uses digital certificates as the most general way of authentication. Two IGSNs on different IP core networks can use digital certificates as a means of authentication without any prior knowledge of each other.
2. Addition of an IGSN only requires an update of the CA.
3. An IP core network operator customer could use the CA when establishing an IPsec connection to his private corporate intranet.

12.8.5.2 Security in Mobile IPv6

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

12.8.5.3 Encryption of Mobile IP messages

Only authentication is mandatory in Mobile IPv4. Encryption of Mobile IP messages is out of scope in the Mobile IPv4 standard [RFC2002]. Encryption of registration requests is however crucial to protect personal integrity. With unencrypted registration messages, a user could be tracked if an intruder has access to the IP core network. To prevent this, IPsec encryption should be provided by the network operator between IGSN and HA.
In IPv6 both authentication and encryption is handled end-to-end by IPsec.

12.8.5.4 IPsec for protection of user data

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

12.8.6 IP Authentication Mechanisms – Radius and Diameter

12.8.7 UMTS Charging

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

12.8.8 IP Charging mechanisms – Radius and Diameter

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

12.9 Service Support

12.9.1 QoS – the Use of Differentiated and Integrated Services

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.

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

12.9.2 Multi Protocol Support

Multiprotocol support over MIP tunnels can be performed using **GRE encapsulation**, as envisioned by IP mobility support standard. 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.

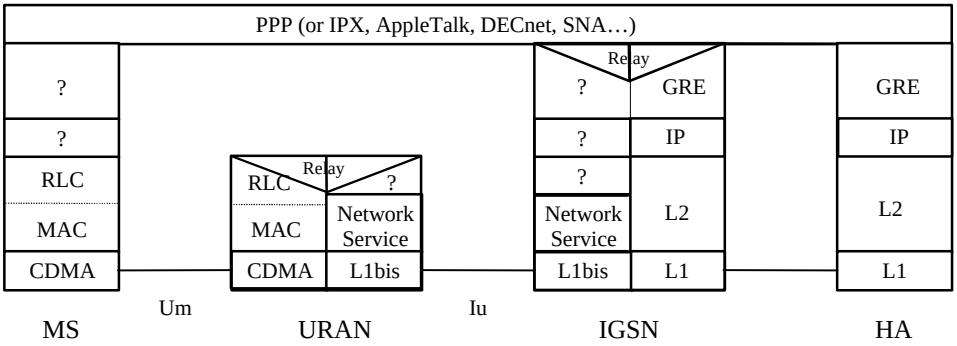


Figure 12 – Multiprotocol support in Mobile IP

12.9.3 Service Control

12.9.4 Support of Multimedia

12.9.5 Support of VHE

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

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

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

12.9.6 Personal Mobility

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

13 First Evolution Stage: MIP in overlay to GPRS

13.1 General Design Requirements

13.2 Proposed Solutions

[Editor's comment: this text is not complete and different options need to be evaluated]

13.2.1 Option 1 for Stage 1

The starting point for the evolution path for use of MIP within the UMTS core network is dependent upon support of MIP in overlay to GPRS. A possible high level schematic for the support of MIP within GPRS is shown in Figure 13. Alternatively, a normal use of MIP control messages on top of GTP tunnels could be envisioned. The additional functionality required is outlined below.

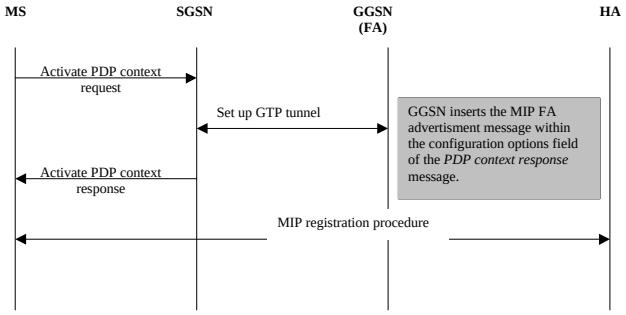


Figure 13 Support of MIP within GPRS

The user shall send an *Activate PDP Context Request* message, identifying a GGSN that provides the FA functionality. If no GGSN address is declared, then the SGSN can derive the GGSN address as currently defined within 03.60. In this case, the user must request a PDP context, which identifies that a GGSN with FA functionality is required. The SGSN shall set up a tunnel towards the GGSN requested with a *Create PDP Context Request* message. At this point the GGSN, which is providing the FA functionality, shall insert a FA advertisement message within the PDP configuration options of the *Create PDP context Response* message. This information is sent transparently through the SGSN to the MS within the *Activate PDP Context Accept* message. The MS now has the information required to register with a HA.
During this mode of operation, the FA shall not change during the lifetime of a PDP context, and movement between SGSNs will be handled by GTP inter-SGSN handover procedures.

13.2.2 Option 2 for Stage 1

[*Editor's note comment: the surrogate registration needs further study*]

As an alternative to or an evolution of step 1, the following method for support of GPRS access procedures using a MIP based data users mobility support may be implemented. This method would probably be better as an evolution from step 1, as it requires significant changes to the core network node (SGSN). Furthermore, the GGSN functionality will no longer be required.[1] An operator whose intention is to base their UMTS systems on a MIP approach may choose to use this scenario. The MS should perceive no differences, and will continue to use the normal GPRS access procedures. The functionality required are outlined below.

[1] Operators may choose to keep existing GGSN equipment for providing non-MIP based access. Furthermore, existing subscribers may continue to be supported using the GGSN, with new subscribers using the MIP based solution, or ALL subscribers may be migrated

The subscriber would require special parameters stored within the HLR relating to MIP registration parameters. It is possible that a new PDP type would be introduced in order to support this. An *Activate PDP Context Request* message is sent by the MS requesting a PDP context activation relating to the particular PDP context subscription records which the MIP parameters are stored against. The SGSN would then carry out a surrogate registration with the HA, using the information from the HLR subscription record to construct the MIP registration request. Note that a separate subscription record needs to be stored for every HA which the user may wish to register with. Once the registration with the HA is completed, the SGSN shall send an *Activate PDP Context Response* message to the MS. At this stage, the MS can send data towards the SGSN, which shall encapsulate the data towards the HA. Data arriving at the SGSN shall be decapsulated and sent to the MS. (Standard FA functionality)

Handover between SGSNs shall continue to be supported by the use of the GTP inter-SGSN handover procedures, however these must be modified in order to support the surrogate re-registration of the MS with the new FA address. This should not be too much of an impact, as the new SGSN already has to update the GGSN.

13.3 The User Equipment

13.4 PDP Context and GTP

13.5 SGSN and GGSN

14 Compatibility Issues

14.1 IPv4 – IPv6

14.1.1 Mixed IPv4 – IPv6 UMTS Networks

If UMTS standards support IPv4 and IPv6, situations will arise where one UMTS operator employs MIPv4 and another MIPv6. Given there are no FAs in MIPv6 it should be possible to support an MIPv6 MS and HA when the current UMTS network is IPv4 only, via IETF IPv4 to IPv6 transition mechanisms. However, the specific mechanisms and the implications on the UMTS network require further consideration.

14.1.2 Network Elements that need changes if migrating from MIPv4 to MIPv6

MS
- Must have an IPv6 stack (including MIPv6) rather than an IPv4 stack

IGSN
- Must provide standard IPv6 router functionality rather than 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 rather than IPv4 router functionality
- Must support MIPv6 HA functions rather than MIPv4 functions.

Routers
- Must provide standard IPv6 router functionality rather than IPv4 router functionality

14.2 GPRS – Mobile IP

14.2.1 Handover GSM – UMTS – GSM

There will be the requirement to handle intersystem HO for a dual mode MS (i.e. one that can access both the GSM access network and the UTRAN). Let's assume that MIP is deployed in the UMTS core network.

Two possible approaches may be adopted. It is assumed within both approaches the MS could be informed via a layer 3 message (e.g. Routing Area Update message) that a change of FA has occurred. This message may also include the FA advertisement message. (The exact message which will be sent in case of inter-system handover is FFS.)
Approach 1 requires no implementation of any GPRS interfaces within the UMTS core network node, but may involve significant loss of data. Approach 2 requires implementation of the Gn interface (GTP protocol), but *should* not involve any loss of data.
Note that what is being proposed here is relevant only to how the MIP part of the handover will be done. Consideration for intersystem handover with regards to authentication, ciphering, key management etc. are not addressed.

Approach 1:
Assuming that the MS is registered with a HA in either of the networks (UMTS or GPRS), the MS shall carry out the new MIP registration by using the relevant procedure for the system roamed into. Specific information (QoS) relating to the sessions (PDP contexts) active at the time of the handover would have to be re-activated using the session (PDP) activation procedures native to the system roamed into. Note that the MS is required to hold this information, and hence this is a feasible though not very "air interface friendly" proposition.
If the MS has an ongoing data session (PDP context) then there would appear to have been a link layer connectivity loss with the link being restored once the HA starts to forward packets to the correct FA.

Approach 2:
Again, assuming that the MS is registered with a HA in either of the networks, then dependent on the direction of the handover, one of two actions will be taken.

UMTS → GPRS
Here the IGSN shall be required to fully support the Gn interface, and act as both SGSN and GGSN towards the roamed to GPRS system. The GTP inter-SGSN handover will be utilised to pass state information towards the new SGSN. The new SGSN shall then create a GTP tunnel towards the IGSN. (Note that here the IGSN is carrying out GGSN functionality). The IGSN shall continue to receive packets from the HA, decapsulate them, and send them along a GTP tunnel towards the SGSN within the GPRS network. This two levels of tunneling shall be carried out whilst data transmission is pending. Once the MS detects low levels of data activity (eg by going into standby mode), it shall initiate the MIP registration procedure for the new FA. Once this has happened, the IGSN will release the tunnels and contexts for the MS.

GPRS → UMTS
Here the GGSN shall be acting as the FA. The IGSN shall utilise the GTP inter-SGSN handover to receive state information from the old SGSN. The IGSN shall then create a tunnel towards the serving GGSN. The GGSN shall continue to receive packets from the HA, decapsulate them, and send them along a GTP tunnel towards the IGSN within the UMTS network. This two levels of tunneling shall be carried out whilst data transmission is pending. Once the MS detects low levels of data activity (eg by going into standby mode), it shall initiate the MIP registration procedure for the new FA.

15 Dependencies on IETF

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

15.1 IPv4

IPsec
DHCP
IETF Internet draft "Mobile IP and Public Key Based Authentication" [PubKey] by Stuart Jacobs of GTE Laboratories. v4 v6?

15.2 IPv6

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

16 Enhancements of Standards

16.1 User Equipment

16.2 PDP Context and GTP

16.3 Functionality of SGSN and GGSN

16.4 HLR

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

16.5 Gh (HLR-HA) Interface

[Editor's comment: in case the Gh interface is needed]

16.6 VLR – Mobile IP interaction

[Editor's comment: in case any interaction is needed]

16.7 Mobile IP

17 Driving Forces

17.1 Mobile IP is standardized by the IETF

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

- **Ability to take advantage of the economy of scale that the widespread use of Mobile IP in the Internet would represent.**
- **Use of standard routers for the Foreign Agent and the Home Agent functionality**
- **Standard AAA servers** (e.g. RADIUS or DIAMETER) will be used for Authentication, Authorization and Accounting. This allows administration of data users in a consistent way across wireline and wireless public data networks and corporate intranets. Also, operators already running a data network and corporate CIOs will be able to use the same AAA infrastructure for their wireline and their wireless users.
- **Native support of IP level roaming procedures.** Interprovider IP level roaming agreements are based on the submission of an NAI (Network Access Identifier) by the user. An extension to support the transport of the NAI in registration requests has been proposed for inclusion in the revision of RFC2002. 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.

17.2 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).

17.3 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.

17.4 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.

18 Potential

19 Pros and Cons

+ optimised routing in the CN between e.g. two mobile terminals
+ mainstream IP equipment can be used to a larger extent
+ mobility handling compatible with fixed networks
+
- difficult to handle private addresses (?)
-

20 Comparison with GPRS

Issues to consider

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

[*Editor's note: A revised version of Tdoc C-99-055 is to go here*]

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

Comparison OF mobile IP with GTP/GPRS

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

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

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

21 Summary

22 Open Issues

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

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

23 Conclusions

24 Appendix A – Mobile IP

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

24.1 Basic architecture

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

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

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

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

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

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

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

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

The resulting communication scenario is illustrated in Figure 2.1. 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[2] which the mobile terminal can use to acquire a valid address in the visited subnet.

---

[2] 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.

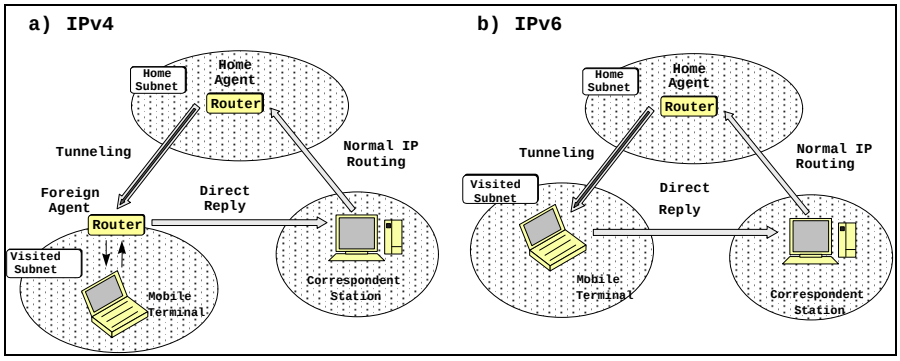


Figure 14. Basic architecture for supporting IP mobility

24.2 Route optimization

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

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

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

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

24.2.1

24.2.2 The solution proposed for IPv4

In the Route Optimization protocol specified for IPv4, the home agent indicates the mobile terminal’s care-of address to the correspondent node when the terminal is away from its home subnet. After receiving a datagram intended for the mobile terminal, the home agent performs a tunneling operation to the associated care-of address, and also sends an appropriate Binding Update message to the correspondent node. The correspondent node can subsequently send the traffic intended for the mobile terminal directly to its care-of address by means of a tunneling mechanism, and sets up an optimized route which makes it possible to avoid passing through the home agent (Figure 2.2).

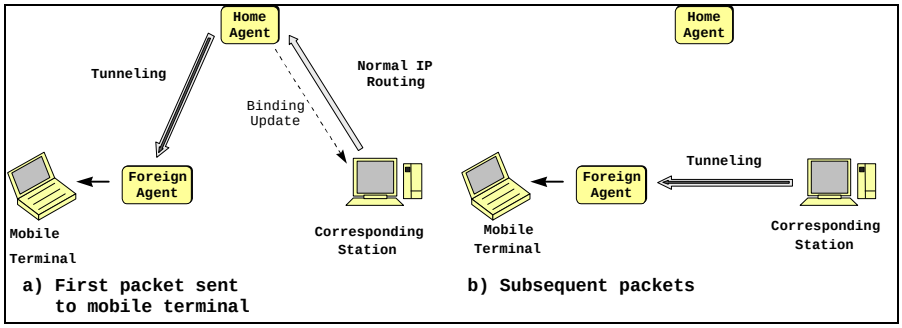


Figure 15. ***Route Optimization*** **in IPv4**

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

Thus, in the IPv4 Route Optimization protocol, the mobile terminal, after moving in a new subnet, can also communicate its new care-of address to its previous foreign agent. In this way, when a correspondent node attempts to reach the mobile terminal using a care-of address which has become obsolete, the foreign agent which receives transmitted traffic can forward it to the mobile terminal's new location using a tunneling mechanism. At the same time, the foreign agent sends the home agent a Binding Warning message, asking that the correspondent station be notified of the mobile terminal's new care-of address by means of an appropriate Binding Update message, thus making it possible to restore an optimized route between source and destination (Figure 2.3)

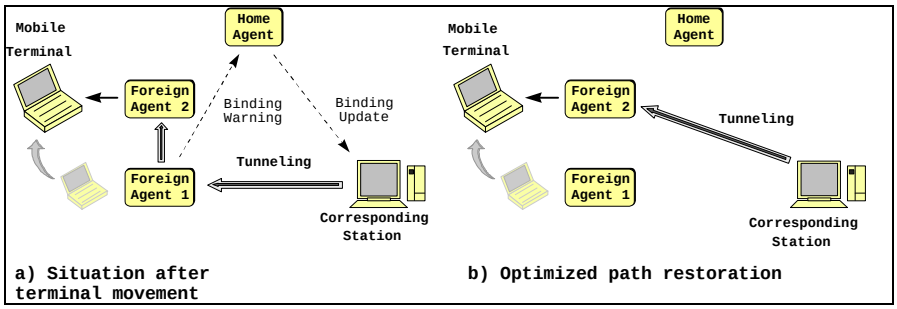


Figure 16. Mobile terminal movement with notification to the previous foreign agent

If a correspondent node attempts to reach the mobile terminal using an obsolete care-of address and the foreign agent which receives the transmitted traffic does not know the mobile terminal's new location (either because it has not been notified of this location, or because the information has already been removed from its cache), the Route Optimization protocol requires 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 2.4).

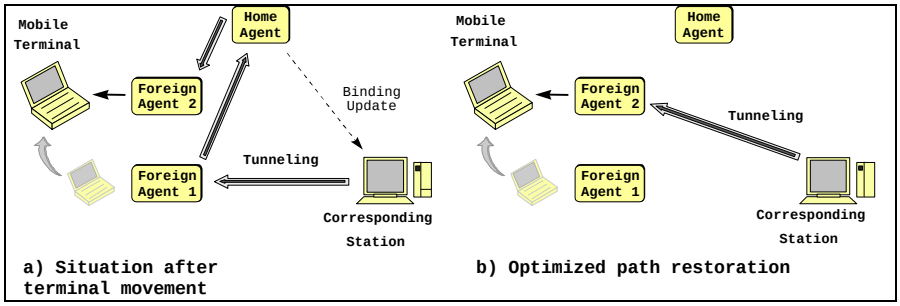


Figure 17 Mobile terminal movement without notification to the previous foreign agent

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

24.2.3 The solution proposed for IPv6

By contrast with the procedure used in IPv4, the Route Optimization protocol specified for IPv6 requires that the Binding Update messages intended for the correspondent node be transmitted directly by the mobile terminal every time the latter moves in the Internet (Figure 2.5). 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.

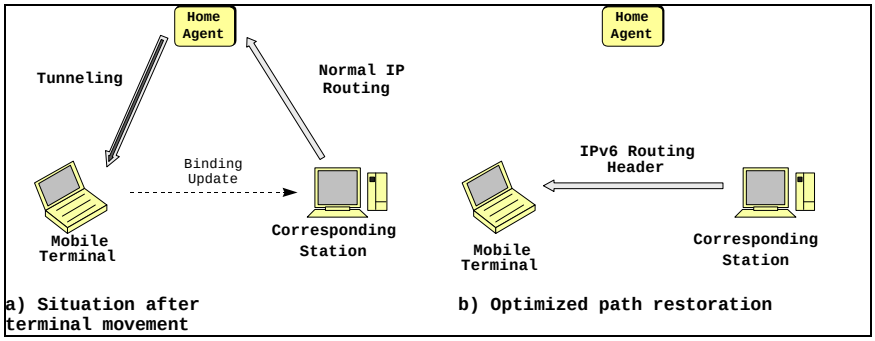


Figure 18. *Route Optimization* in IPv6

A solution of this type, which was ruled out in IPv4, becomes feasible with the new-generation IP protocol, given that the Binding Update messages are coded in appropriate IPv6 extension headers[3] and can be included in the same packets which carry effective traffic between the mobile terminal and the correspondent or between the mobile

---

3 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.

terminal and the home agent. This minimizes signaling traffic, making it acceptable to transport it on the network even when the mobile node is connected to the Internet via a wireless interface, which can have a much lower bandwidth than conventional cabled networks and a high error rate.

In addition, while in IPv4 the traffic transmitted by the correspondent node to the mobile terminal is sent directly to its care-of address by means of a tunneling mechanism, with IPv6 the same result is achieved using a *Routing Header*, i.e. a special extension header that forces the datagram to follow a predetermined route. The advantage of this consists of the fact that the Routing Header introduces a smaller overhead in each packet than would "IPv6 in IPv6" tunneling, which makes it necessary to introduce a new IPv6 header in each packet transmitted to the mobile terminal.

24.3 Security aspects

The most critical factor associated with actually applying IP mobility support protocols in the Internet concerns security aspects.

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

25 Appendix B – IPv4 versus IPv6

[general issues, not specific to MobileIP]

26 Appendix C – IPsec and Digital Certificates

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

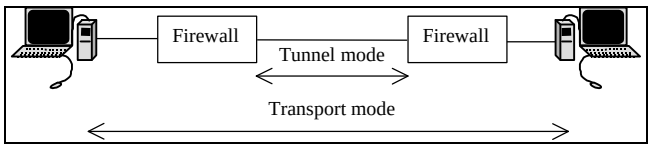


Figure 19 IPsec Tunnel mode and Transport mode

]IPsec Authentication

There are four different ways of user authentication in IPsec:

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

Digital certificates

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

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

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

27 Appendix D – Mobile IP scenario of 23.20

(copied from 23.20, v 0.7.0, August 1998)

3G GSN for IP CN – the IGSN (Internet GPRS Support Node)

The GPRS network must evolve to efficiently support present and future IP services within UMTS. Operators who offer IP services to UMTS users, which also includes fixed users, will benefit from being able to coordinate network resources as well as equipment for mobile and fixed IP based networks, i.e. minimizing the number of different types of networks. By combining the SGSN and GGSN into one node, the Internet GPRS Support Node (IGSN), and adapting it to utilize MobileIP for handling inter IGSN mobility, a standard IP network can operate as a UMTS CN. In such a scenario, most of the functions, presently standardized to be handled by the SGSN and its associated databases VLR, HLR, AuC, etc will be crucial for complementing MobileIP. These functions include authorization of users/terminals, handling of subscriber data, handling and distribution of encryption keys, creation of charging detailed records (CDR) etc.

The example below will clarify the cooperation between GSM/GPRS and Mobile IP. This example assumes IPv6, but the cooperation principles are the same for IPv4.

First, the case where the terminal stays within its home IP network will be described. This is illustrated in figure 27.

- The mobile terminal arrives at a new UTRAN and listens to the radio broadcast messages, which contain information about radio parameters, network and cell identity, etc. as well as information about available core networks, service providers, service capabilities etc.
- The mobile terminal sends a registration request including parameters such as identity, desired service provider etc.
- The UTRAN forwards the registration request to the IGSN, which processes it:
    - The IGSN contacts the HLR of the mobile terminal to collect data to perform an authentication procedure.
    - Once the terminal is authenticated and found to be allowed in the present UTRAN, all information over the radio interface can be encrypted. Encryption keys are obtained from the HLR.
- Now, the terminal can start communicating over the IP layer. The terminal listens to router advertisement messages and solicits the nearest DHCP (Dynamic Host Configuration Protocol) server to obtain configuration parameters and a Mobile IP care-of-address. The HLR records should be enhanced to include the current care-of address of the mobile terminal.
- The mobile terminal will then contact its home agent (HA) to register its new care-of address according to standard MobileIP.
- The HA has to accept or reject the registration of a care-of address. Before making a decision, the home agent could contact the HLR (via a new interface, Gh) to obtain information that this terminal is properly registered. In addition, the keys needed for using the IPsec authentication header and/or the encapsulation security payload between the terminal and the HA could be obtained from the HLR. The mobile terminal can derive its keys from information on its USIM in the same way as in the GSM system.
- While the terminal is connected and transmits data, charging detailed records are produced by the IGSN. Systems for billing and customer handling, already in operation for GSM and GPRS, may be used also for UMTS.

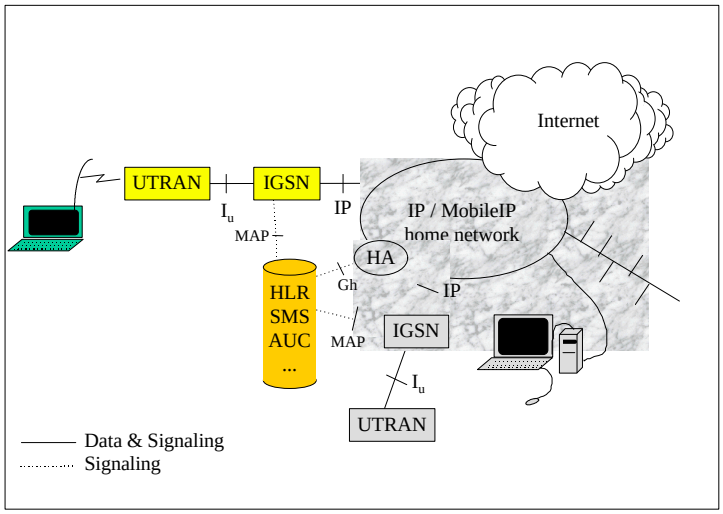


Figure 20 Scenario with IGSN (the combined SGSN and GGSN), and Mobile IP support for inter IGSN mobility. Gh is a new interface between the HA and the HLR

.

The case where the mobile terminal roams into a foreign network is similar, the only difference being that the visited IGSN contacts the HLR in the terminal's home network, either via the international SS7 network or by tunneling the MAP protocol messages through the Internet or an inter PLMN IP network. The mobile terminal registers with its home agent as in the case above.

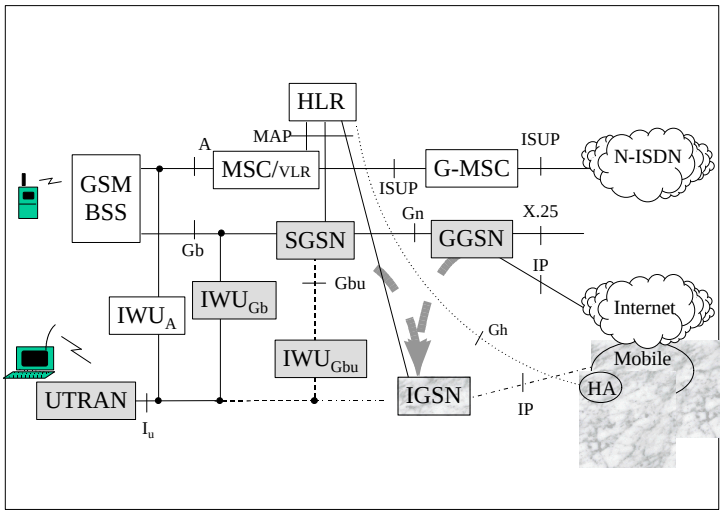


Figure 21 Evolution scenario for UMTS. The SGSN and GGSN are combined into one node, the IGSN

.

The evolution scenario is depicted in Figure 41, where the SGSN and GGSN are combined into one node, the IGSN. Depending on how far the adaptation of the SGSN to the Iu interface has progressed at the time of introduction of the described architecture, the IWU_{Gb} or IWU_{Gbu} (taken from an earlier scenario) may be needed between the IGSN and the UTRAN.

28

29 Annex – GPRS Interconnect to IP Networks and Mobile IP as Inter-System Macro Mobility Support

This annex describes how GPRS phase 1 can be connected to external IP networks. It then goes on to show how mobile IP can be interworked to GPRS phase 1 to provide inter-system macro mobility.

X.1 GPRS Phase 1 Interconnect to IP Networks

This section describes how GPRS phase 1 can be interconnected to external IP networks. The following figure provides an overview.

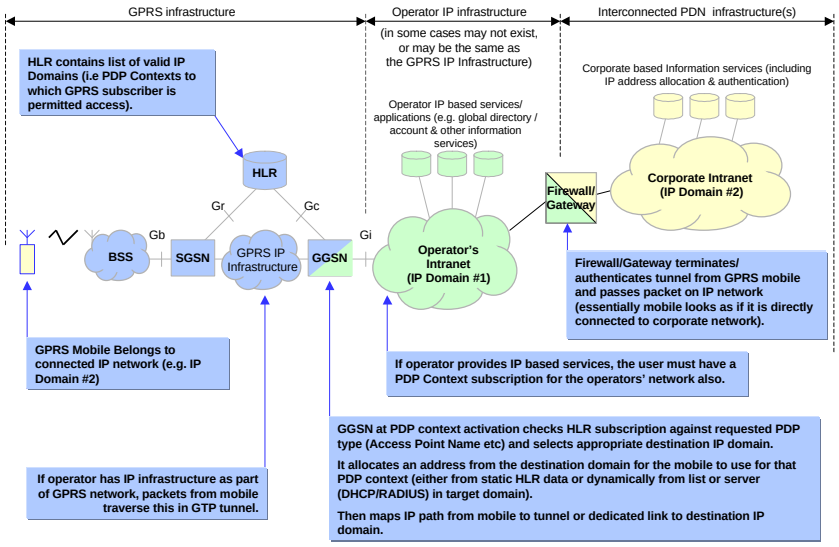


Figure 22

When a GPRS user sets up a PDP context this is directed to a "target" IP domain outside the GPRS environment. In the above slide the target network could be IP domain#1 or IP domain #2.

The above figure shows the "normal" case of GPRS interworking with a target IP domain. The target domain is directly connected to the GGSN (like IP Domain #1) or has a static bi-directional tunnel to the GGSN (like IP Domain #2). From the point of view of routers and clients in the target domains the GPRS mobiles appear to be directly connected. This means that support for GPRS access places minimal requirements on the target domain – eg it is not require to support MIP. This is one of the objectives of GPRS.

Dynamic addressing will be used so that the MS will be temporarily assigned a topologically correct IP address in its target IP domain space.

One disadvantage of this approach occurs if subscribers are allowed to perform international roaming while accessing a nationally-limited target IP domain. In this case the GPRS option to use a GGSN in the home network would have to be used and therefore the international traffic would be carried on the inter-PLMN GPRS backbone network. However, this option may not always be efficient or desirable.

X.2 Mobile IP as Inter-System Macro Mobility Support

This section shows how GPRS phase 1 can be interworked to mobile IP to enable mobile IP to provide inter-system macro mobility support.

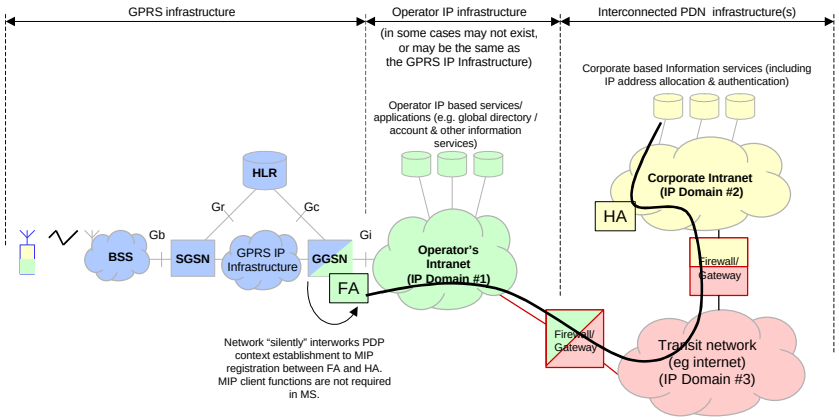


Figure 23

In this case the IP domain being accessed (domain#2) has no direct connection to the GGSN from which the mobile is being served. For example, the mobile has roamed internationally and the system has been configured to use the local GGSN rather than the home GGSN.

In this case MIP may help the subscriber reach his desired network. From a GPRS point of view the target domain would be set to a domain that is directly connected to the GGSN (in this example domain #1). MIP could then be used to tunnel between the domain accessed through GPRS and the finally desired domain. If the FA is associated with the GGSN then PDP context activation could be interworked to MIP registration. When PDP context activation occurs the GGSN would map this on to an MIP registration at a target home agent. This would provide a level of transparency to the user – eg no MIP client is required in the MS. The MIP tunnel is terminated at the GGSN/FA and mapped in to the GPRS data stream.

Some notes on this example:
1) The FA used is at the GPRS anchor point (GGSN). Handover is performed by GPRS without impacting on the FA or MIP. This protects the GPRS environment from the external world. This means the MIP can be used at its current level of development without invention of new procedures.

2) From the service point of view the trade-offs between this approach and the option of using a GGSN in the home PLMN are complicated and need study.

3) Other options would be to include a normal MIP client (and possibly an FA) in the MS. Again the relative merits of this approach should be looked at.

X.3 Summary

The key points in the appendix can be summarised as follows:

GPRS currently provides an access services for IP networks which isolates access-level mobility from the rest of the network. This seems desirable as:

- it reduces dependencies on the external networks and
- it allows the GPRS operator to protect their own billing, grade of service and quality of service issues
- it provides a secure environment for the GPRS network nodes.

GPRS phase 1 can connect to external IP networks without use of mobile-IP or GPRS-specific changes to the external network. This is the normal case of GPRS use.

In some cases interworking GPRS to MIP may be useful for macro-level inter-network mobility. An option to do this is presented which:

- retains the benefits of GPRS

- can be achieved with current MIP standards
- avoids excessive tunneling

History

Document history		
Date	**Status**	**Comment**
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