International Telecommunication Union

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(February 2013)

Mobility management in ITU-T: Its current development and next steps heading towards future networks

Forward

This Technical Paper was developed by Mr Oscar Lopez-Torres.

CONTENTS

Page

List of Tables

List of Figures

Page

Technical Paper ITU-T

Mobility management in ITU-T: Its current development and next steps heading towards future networks

1 Introduction

Among one of the key procedures in mobile networks, and with paramount importance in ITU-T next-generation networks (NGN) and future networks, are the mobility management (MM) mechanisms, which provide mobility to their users. MM finds itself at the heart of the world-wide deployed mobile networks, in their 2nd and 3rd generations, and more recent architectures such as long term evolution (LTE). In ITU-T NGN, MM is composed of two mechanism sets, namely location and handover management. In mobile networks, there exist two categories of handovers for user equipment (UE), i.e., intra-system and inter-system handovers. In intra-system handovers, UE moves among different cells, or network nodes of the same system; while in inter-system handovers, UE moves among different access technologies.

ITU-T NGN commenced the development of MM concepts and requirements in its Study Period 2005-2008, with the inclusion of the Question-set established in Study Group 19. Afterwards, in the Study Period 2009-2012, ITU-T took the lead to continue arduous development of MM Recommendations. These efforts include standardization of:

- Requirements on MM for NGN, fixed mobile convergence (FMC), and their respective control scenarios.
- MM solutions on FMC using legacy public switched telephone network (PSTN) and integrated services digital network (ISDN) as the fixed access network for mobile users, on interworking between worldwide interoperability for microwave access (WiMAX) and wireless local area network (WLAN), on mobility supporting architectures for the mobile point-to-point (P2P) service in heterogeneous wireless networks, and interworking between WiMAX and universal mobile telecommunication network (UMTS).
- Generic MM frameworks on location and handover management control, on MM for the service stratum, on communications between users with multiple terminal devices, on MM for Internet protocol (IP) multicast communications, and on mobile virtual private networks (VPNs).

With this in mind, this technical paper not only surveys and presents to the reader the current status quo of MM in ITU-T NGN, based on the set of published Recommendations, but it also pursues to outline recent advances in MM procedures posed in newer services, which may suggest their inclusion after industry requirements, in order to achieve completeness in the ITU-T's MM toolkit. It also makes strides to initiate a MM gap analysis in NGN, in the sense of network element and interfaces definition compared to currently-deployed mobile networks, to offer future completeness and compatibility with presently utilized MM mechanisms in mobile networks.

It is expected that this technical paper will appeal to other groups within ITU-T, inside and outside SG13, to further standardize new MM scenarios and their procedures in the forthcoming emerging/future networks. Such audience should include ITU-T contributors working on MM-related Questions, mobile network researchers, designers, and academia.

2 Scope

This technical paper is intended for researchers and staff of next-generation networks (NGN) and mobile network operators specifically interested in the mobility management (MM) aspects and status quo in NGN and its evolution towards future networks; in other words, those MM mechanisms evolving from the merging of NGN and mobile networks, a topic of major importance in ITU-T's Study Period 2013-2016.

This technical paper describes scenarios and use cases from which operators and users can draw conclusions on the direction of MM procedures and the technological direction in the context of the all-IP mobile network industry.

This technical paper attempts to endure on the current state of NGN MM mechanisms and its maturity, supplementing it with recent technological developments in other mobility management network technologies, i.e., long term evolution (LTE) and the techniques used therein. These technologies include network mobility management reference points and node definitions in standards forums such as 3GPP, IETF, and IEEE. This technical paper thus provides definitions, topic ideas, and techniques drawn from such forums to start strides to convey gaps in the MM network node elements' behaviour, interfaces, and reference points. Consequently, it provides guidance on further steps to achieve a more mature ITU-T mobility management functional architecture in the following recommendation development phase.

3 Abbreviations and acronyms

This technical paper uses the following abbreviations and acronyms. Specific terminology used in other forums is prefixed accordingly for context-referral:

AAA	Authentication, Authorization and Accounting
A-HCF	Access-HCF
AHC-FE	Access HC-FE
A-LMF	Access-LMF
ALM-FE	Access LM-FE
AMBR	Aggregate Maximum Bit Rate
A-MMCF	Access-MMCF
AN	Access Network
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
AP	Application Protocol
APN	Access Point Name
AR	Access Router
ARP	Allocation and Retention Priority
AUC	Authentication Centre
BSC	Base Station Controller
BSS	Base Station System
BTS	Base Transceiver Station
CAMEL	Customized Applications for Mobile network Enhanced Logic
CDMA	Code Division Multiple Access
C-HCF	Central-HCF
CHC-FE	Central HC-FE
CK	Cypher Key
C-LMF	Central-LMF
CLM-FE	Central Location Management Functional Entity
C-MMCF	Central-MMCF
CN	Core Network
CoA	Care-of-Address
CCoA	Co-located Care of Address
CPE	Customer Premises Equipment
CPE-BE	Customer Premises Equipment – Border Element
CS	Circuit Switched
CSCF	Call Session Control Function
CSG	Closed Subscriber Group

CSS	CSG Subscriber Server
CUE	Corresponding UE
DHCP	Dynamic Host Configuration Protocol
DL	DownLink
DM	Data Management
DPI	Deep Packet Inspection
DRX	Discontinuous reception
DSMIPv6	Dual-Stack Mobile IP version 6
ECGI	E-UTRAN Cell Global Identifier
ECM	EPS Connection Management
eKSI	evolved Key Set Identifier
EMM	EPS Mobility Management
eNB	evolved Node B
EPC	Evolved Packet Core
ePDG	evolved Packet Data Gateway
EPS	Evolved Packet System
E-RAB	E-UTRAN Radio Access Bearer
ES	Event Service
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FA	Foreign Agent
FDD	Frequency Division Duplex
FE	Functional Entity
FMC	Fixed Mobile Convergence
FMIP	Fast handover for MIP
GBR	Guaranteed Bit Rate
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio System
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
GUMMEI	Globally Unique MME Identifier
GUP	Generic User Profile
GUTI	Globally Unique Temporary Identity
GW	Gateway

GWCN Gateway Core Network
HA Home Agent
HeNB Home enhanced Node B
HC Handover Control
HCF Handover Control Function
HC-FE Handover Control Functional Entity
HFN Hyper Frame Number
HLR Home Location Register
HMIP Hierarchical Mobile IP
HO Handover
HoA Home Address
HPLMN Home PLMN
HRPD High Rate Packet Data
HS-GWHRPD Serving Gateway
HSS Home Subscriber Server
ICMP Internet Control Message Protocol
ID Identifier
IE Information Element
IK Integrity Key
IKE Internet Key Exchange
IMEISV International Mobile station Equipment Identity and Software Version number
IMS IP Multimedia Subsystem
IMSI International Mobile Subscriber Identifier
IMT-2000 International Mobile Telecommunications-2000
IP Internet Protocol
IP-CAN IP-Connectivity Access Network
IPSec IP Security Protocol
IPTV Internet Protocol Television
IPv4/v6 Internet Protocol version 4/version 6
IS Information Service
ISDN Integrated Services Digital Network
ISP Internet Service Provider
ISR Idle mode Signalling Reduction
KASME key Main key for E-UTRAN key hierarchy based on CK, IK and serving network identity
L2 Layer 2
L3 Layer 3
LA Location Area

LBI	Linked Bearer Identity
LBQ	LID Binding Query
LBU	LID Binding Update
LID	Location Identifier
LIPA	Local IP Access
LM	Location Management
LMA	Localized Mobility Agent
LMF	Location Management Function
LM-FE	Location Management Functional Entity
L-MMCF	Local MMCF
LTE	Long Term Evolution
MAC	Media Access Control
MAG	Mobile Access Gateway
MAP	Mobile Application Part
MBR	Maximum Bit rate
ME	Mobile Equipment
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIMO	Multiple-Input Multiple-Output
MIP	Mobile IP
MM	Mobility Management
MMCF	Mobility Management Control Function
MME	Mobile Management Entity
MP-MP	Multipoint-to-Multipoint
MOBIKE	Mobility and Multihoming Protocol
MR	Multicast Router
MS	Mobile Station
MSISDN	Mobile Station International Subscriber Directory Number
MSC	Mobile-services Switching Centre
MT	Mobile Terminal
MUE	Mobile UE
NAP	Network Attachment Point
NACF	Network Attachment Control Function
NAI	Network Access Identifier
NAS	Non-Access-Stratum
NDC	National Destination Code
NGN	Next-Generation Network

NGN-FRA	Functional Requirements and Architecture for NGN
NNI	Network-to-Network Interface
NSP	Next Study Period
NT	Network Termination
OFDM	Orthogonal Frequency Division Multiplexing
OMA	Open Mobile Alliance
OSA-SCS	Open Service Access-Service Capability Server
OTA	Over-the-Air
P2P	Point-to-Point
PBU	Proxy Binding Update
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCH	Paging Channel
PCRF	Policy and Charging Rule Function
PDA	Personal Digital Assistance
PDCP	Packet Data Convergence Protocol
PD-FE	Policy Decision Functional Entity
PDN	Packet Data Network
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PDU	Packet Data Unit
PE-FE	Policy Enforcement Functional Entity
P-GW	Packet Data Network Gateway
PHY	Physical
PIM	Protocol-Independent Multicast
PLID	Persistent LID (Location Identifier)
PLMN	Public Land Mobile Network
PMIP	Proxy MIP
PMM	Packet Mobility Management
PoA	Point of Attachment
PS	Packet Switched
P-TMSI	Packet TMSI
QCI	QoS Class Identifier
QoS	Quality of Service
RA	Routing Area
RACF	Resource and Admission Control Function
RADIUS	Remote Authentication Dial-In User Services

RAI	Routeing Area Identity
RAN	Radio Access Network
RAT	Radio Access Technology
RAU	Routing Area Update
RF	Radio Frequency
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network System
RP	Reference Point between HSS and application
RRC	Radio Resource Control
S5/S8	Reference Points between 3GPP S-GW and P-GW (PCEF)
SAP	Signalling Access Points
S-CSCF	Serving CSCF
SCF	Session Charging Function
SCTP	Stream Control Transmission Protocol
SDF	(in 3GPP QoS) Service Data Flow
SDO	Standards Development Organization
S-GW	Serving Gateway
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SIPTO	Selected IP Traffic Offload
SIM	Subscriber Identity Module
SP	Service Platform
SPI	Service Platform Interface
SLA	Service Level Agreement
SRNS	Serving RNS
SRVCC	Single Radio Voice Call Continuity
SSID	Service Set ID
SSF	Service Switching Function (IM-SSF)
SUN	Smart Ubiquitous Network
TA	Tracking Area
TA	Terminal Adapter
TAI	Tracking Area Identity
TAU	Tracking Area Update
TCC	Traffic Channel Complete
TCP	Transmission Control Protocol
TDD	Time Division Duplex

TE	Terminal Equipment
TEID	Tunnel Endpoint Identifier
TF	Transport Function
TFT	Traffic Flow Template
TI	Transaccion Identifier
TIN	Temporary Identity used in Next update
TLID	Temporary LID
TMSI	Temporary Mobile Subscriber Identity
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Chip Card
UID	User Identifier
UL	UpLink
ULR	Uniform Resource Locator
UMTS	Universal Mobile Telecommunication System
UNI	User-to-Network Interface
URA	UTRAN Registration Area
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VLR	Visitor Location Register
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VPLMN	Visited PLMN
VPN	Virtual Private Network
W-CDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
xDSL	x Digital Subscriber Line

4 Terminology

A number of terms are used to describe the technology related to mobility management in the context of ITU-T NGN, future networks, and mobile networks in other standard forums in general. The mechanisms target mobility in both the terminal and the network to provide the capability to "follow" the terminals utilizing location management procedures and handovers among the same or different accesses.

Because of the support provided to different radio access technologies, networks, and their corresponding terminals, the terms mobile station (MS), mobile terminal (MT), and user equipment (UE) are used having the same meaning under the NGN framework. The differences are explained between a MS and an UE when referring to specific 3GPP MM procedures. Additionally, in this technical paper, the term UE replaces the term MUE (mobile UE) in NGN, since it is implicit that mobility management mechanisms are intrinsic to the usage of UE.

Mobility management is the term used in the context of ITU-T standardization; this term is also used in other standard forums and, in general, in the industry worldwide.

5 Categorization of mobility management in the framework of NGN

ITU-T initiated the NGN mobility management mechanisms standardization effort by defining requirements under which the mobility management (MM) apparatuses should comply. Additionally, it commenced these activities by classifying the types of mobility management existent for NGN.

Mobility management is an essential requirement for NGN users to maintain communication throughout the length of a voice, data, or a multimedia call. In today's environment, this is realized by using various wireline and wireless access technologies to enable users to communicate over heterogeneous network environments [b-ITU-T Q.1706].

Figure 1, (see [b-ITU-T Q.1706]), depicts the environment in which NGN initially evolved, future networks keep evolving and their intrinsic requirements for mobility among heterogeneous networks. New technologies in MM for 3G and LTE are to be added into these schemes to complement the initial MM requirements.

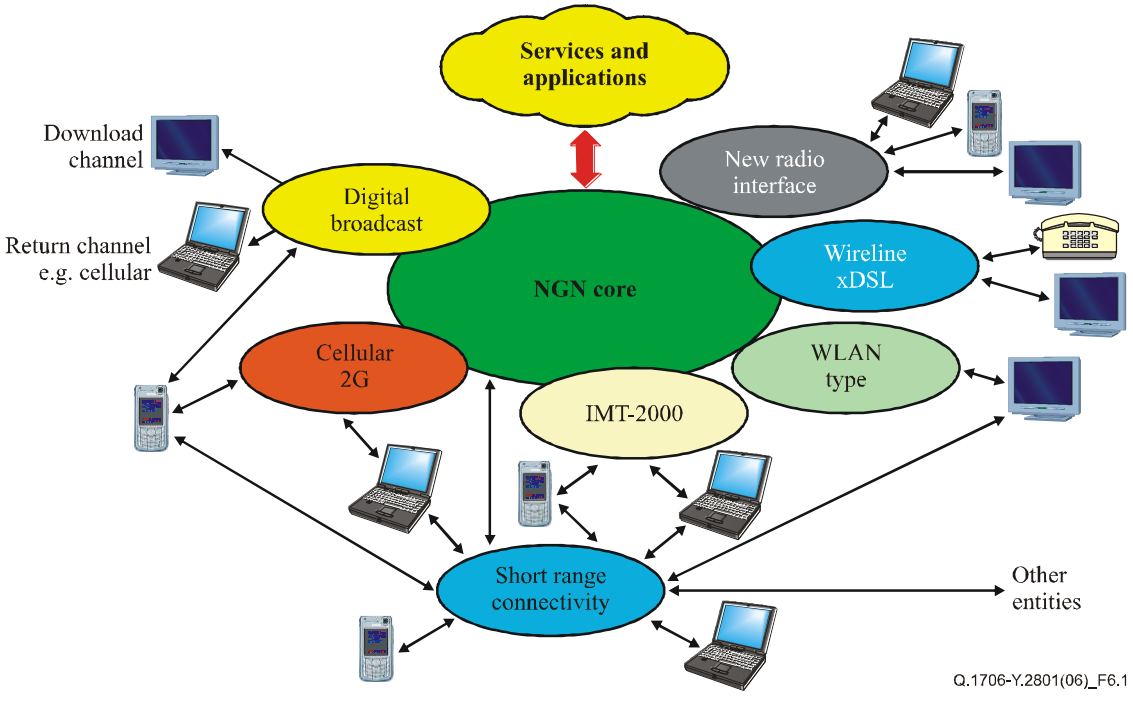


Figure 1 – Envisioned network environment of NGN [b-ITUT Q.1706]

NGN maintains the goal to convergence of fixed and mobile networks and ultimately achieve migration to interoperable and harmonized network architectures. This trend has caused an industry requirement to provide seamless services transparently to the users across different access network (AN) arrangements. Mobility management requirements are thus utilized to support the seamless services in NGN networks [b-ITU-T Q.1706].

Scalability in the number of users and the continuous deployment of heterogeneous networks demands the provision of seamless services to mobile networks, and NGN users reach new dimensions nowadays, presenting new challenges and requirements for new types of MM that could provide seamless services across heterogeneous networks.

A promising solution for the new type of MM in NGN takes into account the long-term trends for future networks, the need for a smooth evolution of the infrastructure, and backward compatibility with existing networks.

It is common that a variety of the existing and new wired/wireless access network technologies be supported, such as wireless local area network (WLAN), x digital subscriber line (xDSL) and 2G/3G mobile networks, etc. Each of the access networks is connected to the NGN core network (CN), to provide the same set of services for users, preferably independently of the access network type [ITU-T Q.1706].

MM may be viewed under different categorizations; some of these categorizations are defined as requirements.

The first categorization contains four types: terminal mobility, network mobility, personal mobility, and service mobility. For more details, see [b-ITU-T Q.1706].

1 Terminal mobility

This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations while in motion and the capability of the network to identify and locate that terminal.

2 Network mobility

The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change as a unit its point of attachment to the corresponding network upon the network's movement itself.

3 Personal mobility

This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

4 Service mobility

This is the mobility applied for a specific service, i.e., the ability of a moving terminal to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose. Note that this service mobility is different from the service level mobility defined in [b-ITU-T Y.2012].

The second categorization is called service quality or service continuity, as shown in Figure 2.

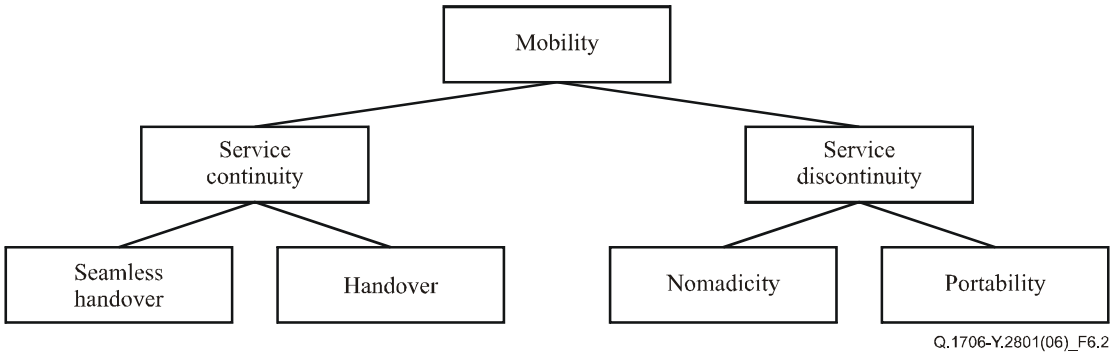


Figure 2 – Mobility classifications according to service quality [b-ITU-T Q.1706]

This categorization is divided into six types: service continuity, service discontinuity, seamless handover, handover, nomadicity, and portability, see [b-ITU-T Q.1706].

1 Service continuity

The ability for a moving object to maintain ongoing service over including current states, such as a user's network environment and session for a service. This category includes seamless handover and handover.

2 Seamless handover

It is a special case of mobility with service continuity since it preserves the ability to provide services without any impact on their service level agreements (SLAs) to a moving object during and after movement.

3 Handover

The ability to provide services with some impact on their service level agreements to a moving object during and after movement.

4 Service discontinuity

The ability to provide services irrespective of environment changes of a moving object without being able to maintain ongoing services. This category includes nomadism and portability.

5 Nomadism

The ability of the users to change their "network access point" while moving. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or handover used. It is assumed that the normal usage pattern is that users shut down their service session before attaching to a different access point.

6 Portability

The ability for a user identifier or address to be allocated to different systems or networkswhen the user moves from one location to another.

The third categorization is a layer concept. It is specified in [b-ITU-R M.1645] and classifies mobility management into two types:

1 Horizontal mobility

Mobility within the same layer. Generally, it is referred to as the mobility within the same access technology.

2 Vertical mobility

Mobility between different layers. Generally, it is referred to as the mobility between different access technologies.

6 User parts

In the NGN requirements, additional consideration is made to “User parts”, see Figure 3 below. The user parts are depicted as user network elements fed by the signalling access points (SAPs) in the service platform and user terminals, also connected to the access network.

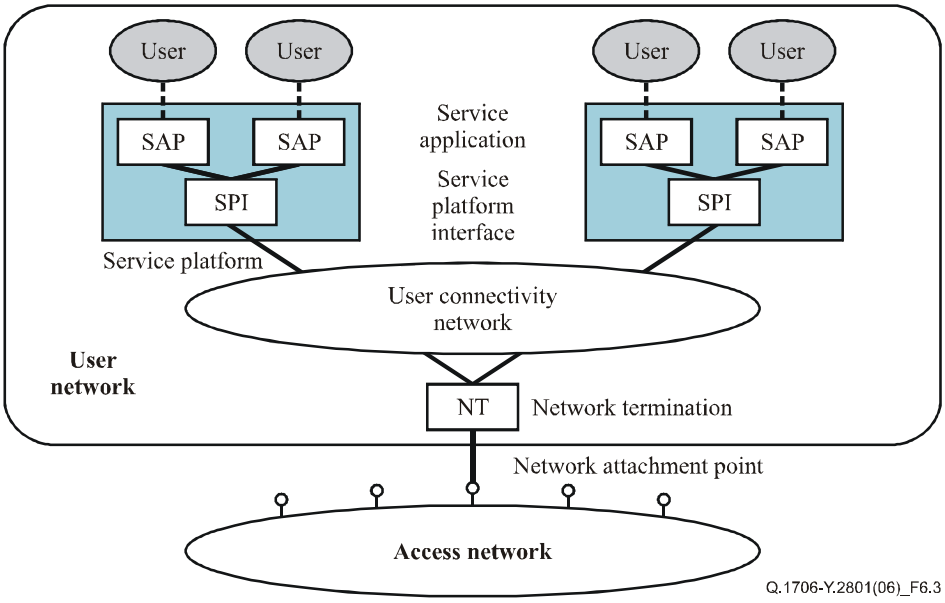


Figure 3 – User network configuration [ITU-T Q.1706]

Figure 3 shows a user network with multiple service platforms. Each service platform may run multiple service applications. In such user networks, multiple users may associate themselves with one or more service applications, by providing one of their user identifiers to the application. For instance, they may be typically represented by a session initiation protocol (SIP) and a uniform resource locator (URL). The service application is bound to a transmission control protocol (TCP)/IP socket in the service platform interface (SPI). SPI binds itself to an access network-specific network termination via the user's connectivity network. Finally, the network termination is bound to the network attachment point (NAP) of the access network.

Only one network termination is shown in the user network, but multi-homing may be considered. See [b-ITU-T Y.2027] for interesting scenarios and an approach on the functional architectural of multi-connection.

In this user network scenario, there is a many-to-one relation between the different types of endpoints. A mobile terminal may represent a limit case where there is a one-to-one relation between the user and the service application, the service application and the service platform interface, and between the service platform interface and the network termination.

ITU-T has also started to handle the development of new services involving a number of UEs allowing users to enjoy multimedia services.

7 3GPP entities and areas active in mobility management mechanisms

This clause provides an overview of location register, the radio area coverage, and zones used in the 3GPP core and radio networks to support the performance of the mobility management mechanisms, see [b-ETSI TS 123 002]. The following definitions, additional radio and core network entities in the architecture may marge as common MM mechanisms, and both may amalgam into a full context of ITU and 3GPP MM mechanisms to support an interoperable MM infrastructure, thus allowing future networks and NGN to enjoy a common vision for mobile operators to take advantage of a common MM architecture. In this context, see [b-ETSI TR 121 905].

7.1 Location register

In order to enable communication to a user equipment (UE) or a mobile station (MS), the network must know where this mobile station is located. This information is stored in a function named location register.

The location register is handled by the following entities:

– The home location register (HLR):

  The home location register (HLR) is the location register to which a mobile subscriber is assigned for record purposes such as subscriber information. For evolved packet system (EPS), the HLR functionality is provided via the home subscriber server (HSS).

– The visitor location register (VLR):

  The visitor location register (VLR) is the location register for circuit switched (CS) services, other than HLR, used by a mobile-services switching centre (MSC) to retrieve information, e.g., handling of calls to or from a roaming UE or MS currently located in its area.

– The serving GPRS support node (SGSN):

  The location register function in SGSN stores subscription information and location information for packet switched (PS) services for each subscriber registered in SGSN.

  SGSN is needed only in a public land mobile network (PLMN) supporting a PS domain with GSM EDGE radio access network (GERAN) or a universal terrestrial radio access network (UTRAN) access.

– The gateway GPRS support node (GGSN):

  The location register function in GGSN stores subscriber information and routeing information, needed to tunnel packet data traffic destined for GPRS UE/MS to SGSN where UE/MS is registered, for each subscriber for which GGSN has at least one PDP context active. GGSN is needed only in PLMN which supports a general packet radio system (GPRS) with GERAN or UTRAN access.

– The mobility management entity (MME):

  The location register function in MME stores subscription information and location information for packet switched (PS) services for each subscriber registered in MME for EPS.

– The packet data network gateway (PDN GW):

  The location register function in PDN GW stores subscriber information and routeing information. This information is needed to tunnel packet data traffic destined for EPS UE to the serving GW, where UE is registered in MME, in SGSN, or in the 3GPP authentication, authorization and accounting (AAA) server in case of non-3GPP access. The information is needed for each subscriber for which PDN GW has at least one PDN connection active.

7.2 Cell

The cell is an area of radio coverage identified by a base station identification as defined in

[b-ETSI TS 123 003].

7.3 Base station controller (BSC) area

The base station controller (BSC) area is an area of radio coverage consisting of one or more cells controlled by one BSC. The boundaries of a BSC area and a location area are independent; a location area may span the boundary between the BSC area and a BSC area may span the boundary between location areas.

7.4 Radio network controller (RNC) area

The radio network controller (RNC) area is an area of radio coverage consisting of one or more cells controlled by one RNC. The boundaries of a RNC area and a location area are independent; a location area may span the boundary between RNC area and a RNC area may span the boundary between location areas.

7.5 Location area (LA)

The location area (LA) is defined as an area in which UE/MS may move freely without updating VLR. A location area includes one or several GERAN/UTRAN cells.

7.6 Routing area (RA)

The routing area (RA) is defined as an area in which UE/MS, in certain operation modes, may move freely without updating SGSN. A routing area includes one or several GERAN/UTRAN cells. RA is always contained within a location area.

7.7 Tracking area (TA)

A tracking area (TA) includes one or several E-UTRAN cells. The network allocates a list with one or more TAs to UE. In certain operation modes, UE may move freely in all TAs of the list without updating the mobility management entity (MME).

7.8 Mobile-services switching centre (MSC) area

The MSC area is the part of the network covered by MSC. An MSC area may consist of one or several location areas. An MSC area may also consist of one or several BSC areas.

7.9 Visitor location register (VLR) area

The VLR area is the part of the network controlled by VLR. A VLR area may consist of one or several MSC areas.

7.10 Serving GPRS support node (SGSN) area

The SGSN area is the part of the network served by SGSN. An SGSN area may consist of one or several routing areas. An SGSN area may also consist of one or several BSC areas. There need not be a one-to-one relationship between the SGSN area and MSC/VLR area.

7.11 Zones for regional subscription

A PLMN operator may define a number of regional subscription areas, each of which is a subset of the service area for an unrestricted mobile subscriber. A regional subscription area may be contained within the service area of a single PLMN, or may lie within the service areas of two or more PLMNs. Each regional subscription area consists of one or more zones; each zone is contained within the service area of PLMN.

The definition of a mobile subscriber's regional subscription area is stored within HLR/HSS per national destination code(s) (NDC) of PLMN and is transferred to VLRs and/or SGSNs/MMEs of that PLMN. VLR and/or SGSN/MME evaluate this information to extract the restricted or accessible MSC and/or SGSN/MME areas and location areas to which the mobile subscriber is allowed to roam. VLR and/or SGSN/MME inform HLR/HSS if an entire MSC and/or SGSN/MME area is restricted.

Zones for regional subscription and their handling are defined in [b-ETSI TS 123 003], [b-ETSI TS 123 008], [b-ETSI TS 129 002], and [b-ETSI TS 129.272] for EPS.

7.12 Service area

The service area is defined as an area in which a mobile subscriber can be reached by another (mobile or fixed) subscriber without the subscriber's knowledge of the actual location of the mobile station within the area. A service area may consist of several PLMNs. One service area may consist of one country, be a part of a country or include several countries. The location registration system associated with each service area must thus contain a list of all the mobile stations located within that service area.

7.13 Group call area

The group call area is a predefined area, composed of one or a number of cells to which a particular voice group calls service (VGCS) or voice broadcast service (VBS) call is distributed. The composition of a group call area is predefined in the network. The group call area may include cells of more than one MSC area and cells of more than one PLMN.

7.14 Mobility management entity (MME) area

The MME area is the part of the network served by MME. The MME area consists of one or several tracking areas. All cells served by eNodeB are included in an MME area. There is no one-to-one relationship between an MME area and an MSC/VLR area. Multiple MMEs may have the same MME area as described in clause 15, "Pool area". MME areas may overlap with each other.

7.15 Pool area

A pool area is an area where an intra-domain connection of radio access network (RAN) nodes to multiple CN nodes is applied. Within a pool area, MS/UE may roam without the need to change the serving core network (CN) node. A pool area is served by one or more CN nodes simultaneously.

7.16 Serving gateway (S-GW) service area

A serving GW service area is the part of the network served by single serving GW. Serving GW service areas consist of one or several complete tracking areas. All cells served by eNodeB are included in a serving GW service area. The serving GW service areas may overlap with each other. There is no one-to-one relationship between an MME area and a serving GW service area.

8 Mobility scenarios according to change of endpoints

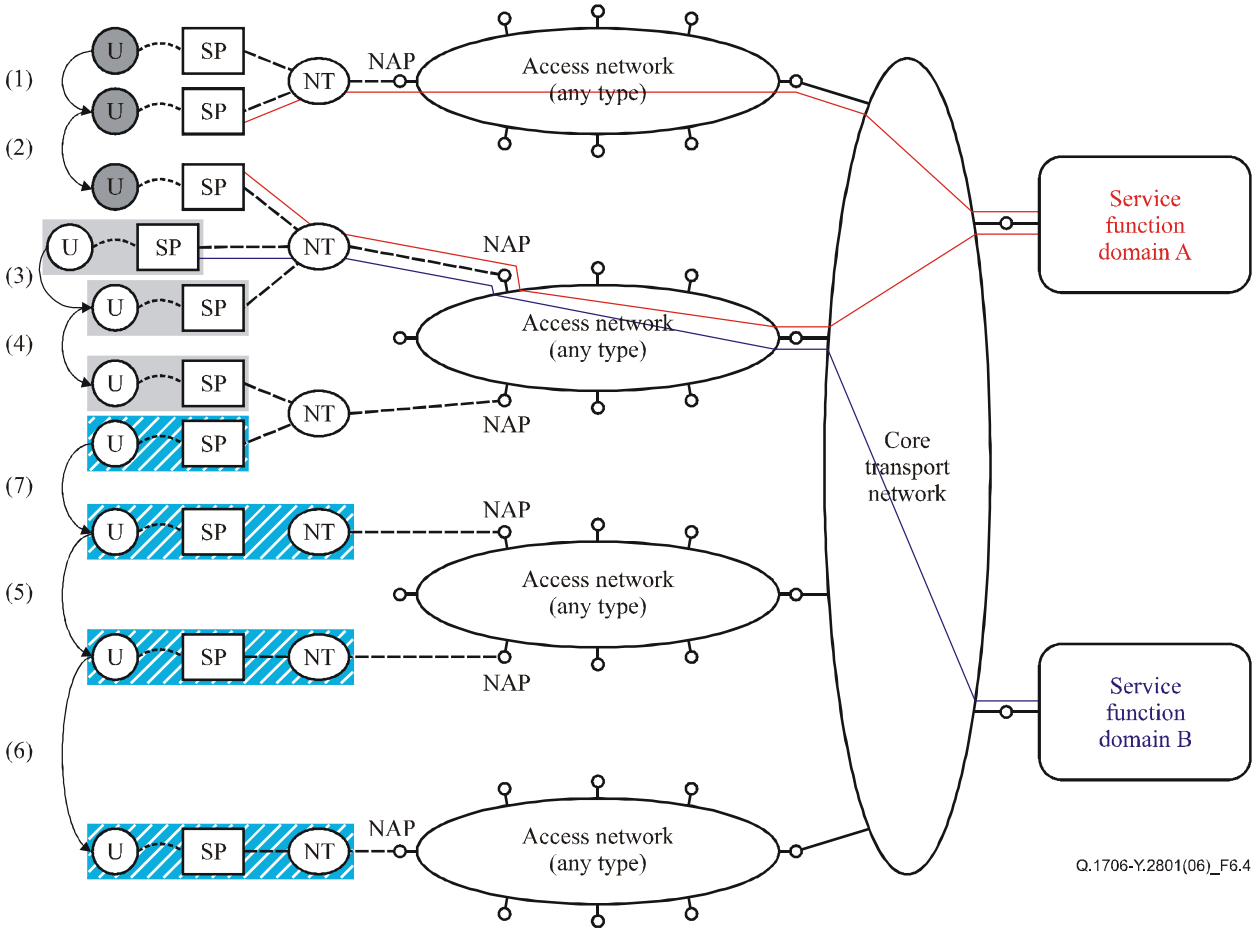


Figure 4 – Mobility scenarios according to the changes of endpoint [b-ITU-T Q.1706]

Figure 4 depicts a number of mobility scenarios including some involving mobility within the end-user equipment area.

The arrows in the left part show different types of mobility. There are seven scenarios shown in Figure 4.

A user may only change the association with a service application when they move from one service platform (SP) to another, either within a user network, scenario (1) or when they move from one user network to another, scenario (2). All other bindings remain fixed in this case.

The user may also move their service platform, thereby changing the binding between the service platform interface and its network termination. Again this may be done within a user network, scenario (3), or when moving from one user network to another, scenario (4). The binding between the network termination and the network attachment point does not change in these two scenarios.

If the network termination supports mobility, the user may change the binding between the network termination and its network attachment point (NAP). The change may be to another NAP on the same access network, scenario (5), or on another access network, scenario (6). The other bindings do not change in these scenarios.

Finally, a more complex scenario is shown in scenario (7), where SPI supports mobility. Such SPI could be used to bind to either NT in a user network or act as NT to bind to NAP.

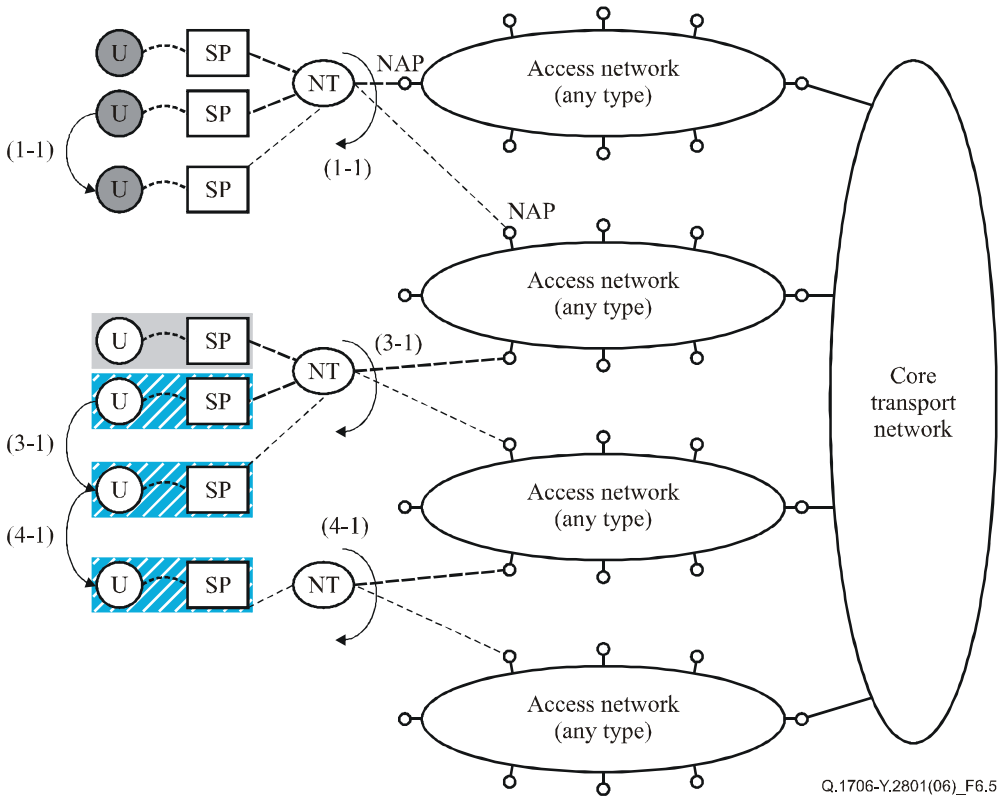


Figure 5 – Single NT with multiple ANs [b-ITU-T Q.1706]

Figure 5 additionally illustrates the option to gain access to different service providers from different service platforms, or different service applications on the same service platform, in the same user network.

Again, the scenarios are shown with arrows in the left part of the figure. These are:scenarios (1-1), (3-1), and (4-1).

A user uses the same service application and the same network termination but changes his network interface card within the same terminal, which has two or more network interface cards of service platform, scenario (1-1). In this case, the user uses the same network termination (NT) but can change its access network, which is matched with the network interface card.

A user can move his service platform, thereby changing the binding between the service platform interface and his network termination. Changing the binding between the service platform interface and his network termination is done within a user network and between two access networks, scenario (3-1), as well as between two user networks and between two access networks, scenario (4-1). These scenarios may be taken as are requirements to improve network performance.

9 Mobility management functionalities

Two MM functionalities are required in NGN: basic mobility-related functionalities and associated functionalities. The basic functionalities are concerned directly with mobility management for mobile users and terminals, whereas the associated functionalities are used for supporting MM or for exchanging related information for overall control and management purposes.

The basic MM functionalities include location and handover management.

9.1 Location management

Location management is performed to identify the current network location of mobile terminal (MT) and to keep track of it as it moves. Location management is used for the control of calls and sessions terminated at MT. Location information is given to the call or session manager for establishing a session. With the support of location management, the corresponding node in the network is able to locate MT and establish a session via the appropriate signalling.

Location management consists of two basic functions:

1 location registration, and

2 call delivery and paging.

Location registration is the procedure to register the current location when MT changes the attachment point within the network.

Call delivery consists in the delivery of packets to the destined MTs, and paging is used to search MTs in dormant mode.

9.2 Handover management

Handover management is used to provide MT with session continuity whenever it moves into different network regions and change their point of attachment within the network during a session. The main objective of seamless handover is to minimize service disruption due to data loss and delay during the handover. Most MM protocols perform handover management together with an appropriate location management scheme.

According to the handover areas concerned, the handover types can be classified into two types:

1 "handover within an AN", where MT moves within a region covered by the same AN in NGN.

2 "handover between different ANs or CNs", where MT changes its access system/network in the ongoing sessions.

10 Mobility management classification – according to network and access

In different NGNs, various types of mobility may exist. Mobility management requirements then vary according to different mobility types. NGN MM considered initially only the classification illustrated in Figure 6 below. Mobility management is classified into:

- Intra-network MM, and
- Inter-network MM.

Intra-network MM is further subdivided into:

- Intra-AN MM, and
- Inter-AN MM.

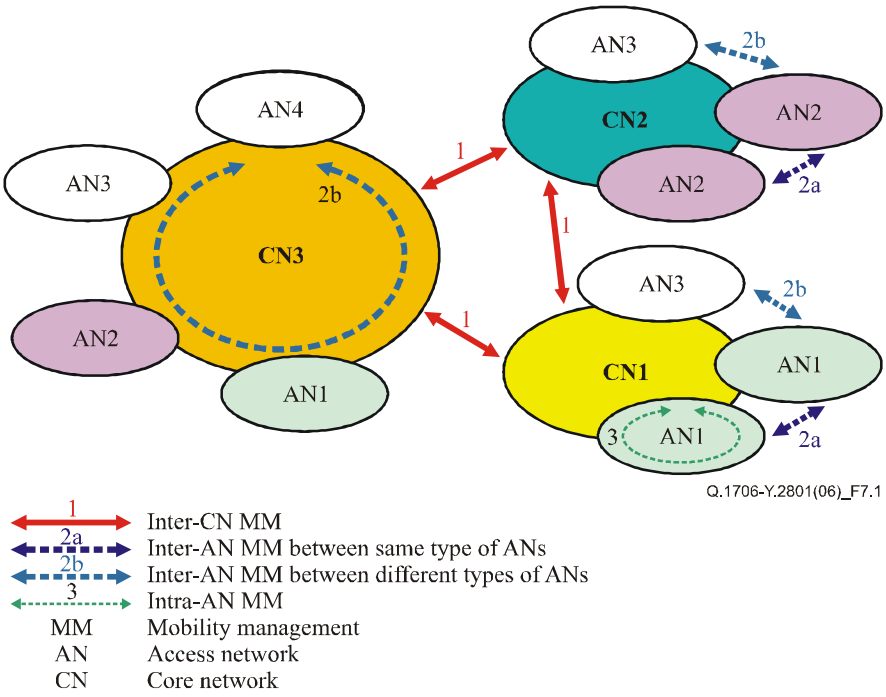


Figure 6 – Classification of MM [b-ITU-T Q.1706]

10.1 Intra-core network mobility management

"Intra-CN" MM addresses MM issues within a network. It can be subdivided into "Intra-AN" MM and "Inter-AN" MM. These mechanisms are defined as follows, as shown in Figure 6:

- *Intra-AN MM*

  "Intra-AN" MM addresses MM issues within an AN. In Figure 6, for example, MM withinAN1 of CN1 can be classified as intra-AN MM, marked as scenario 3 in the figure.

- *Inter-AN MM*

  "Inter-AN" MM addresses MM issues between different ANs within the CN. Inter-AN MM can be further classified into the following two sub-types:

  1 MM between the same type of ANs, e.g., MM between two AN1s within CN1, marked as scenario 2a in Figure 6, and

  2 MM between different types of ANs, e.g., MM between AN1 and AN3 within CN1, marked as scenario 2b in Figure 6.

10.2 Intra-network MM (Inter-CN MM)

"Inter-network" MM addresses MM mechanisms between networks. Inter-network MM mechanisms are used when there is mobility between two ANs, i.e., inter-AN MM.

In addition to those mechanisms, inter-network MM mechanisms handle mobility occurring with MT handovers across different core networks, i.e., network-to-network interface (NNI), such as user authorization and service level agreement (SLA) negotiation. Making reference to Figure 6, MM between CN1 and CN3 is inter-network MM, marked as scenario 1.

11 Classification of mobility based on network topology

Figure 7 shows an example of multiple levels of mobility for certain access network types and mobility technologies, see [b-ITU-T Q.1706]. Other instances for additional access network types and mobility technologies are, of course, possible, see [b-ITU-T Y.2027] for additional examples.

Figure 7 pursues to show that mobility supported at lower levels in the architecture may not be visible at higher levels. It also shows that mobility may be handled at different levels, including that at the application level.

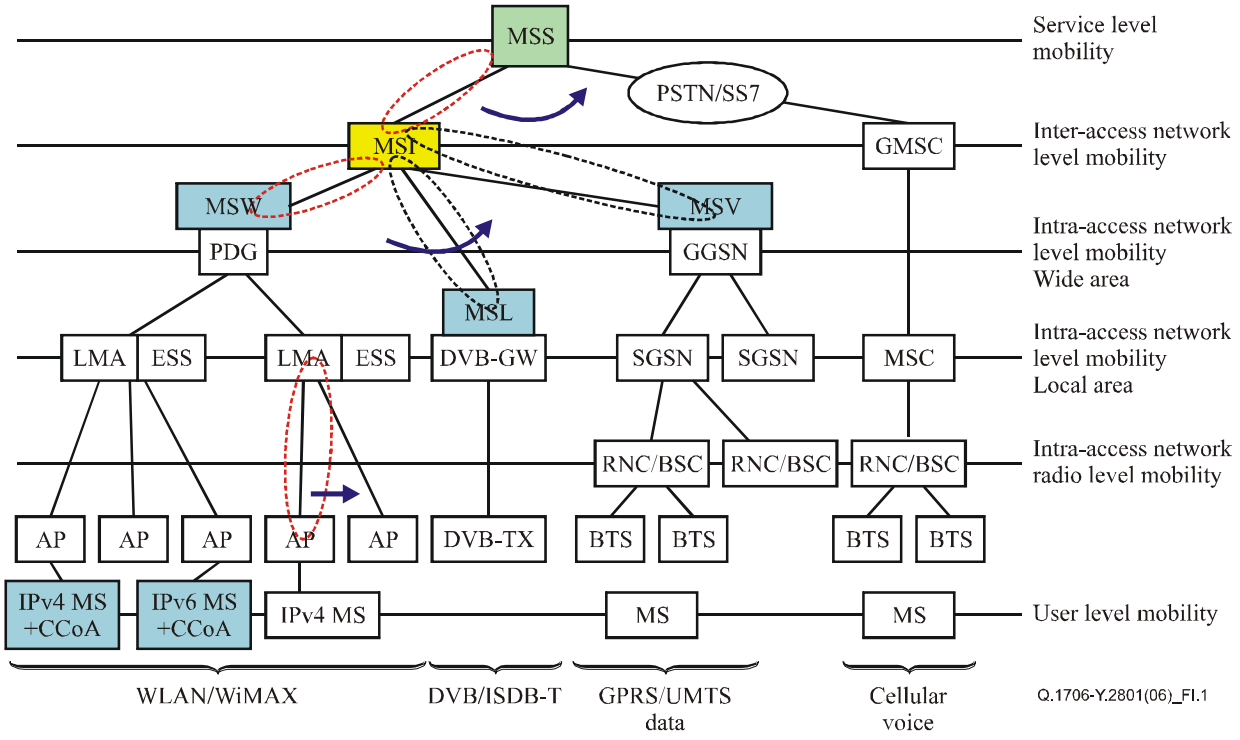


Figure 7 – Example of levels of mobility [b-ITU-T Q.1706]

In the figure, there are different levels of mobility, namely:

- *Mobility at the service level*

  Service level mobility takes place across circuit switched (CS) or packet switched (PS) domains in NGN. This might be within a single NGN or across NGNs. Service level mobility might, for example, exploit the ITU-T E.164 address to session initiation protocol-uniform resource identifier (SIP-URI) resolution capabilities. Using these capabilities, service level mobility can be provided when a user is roaming between different administrative domains, which would necessitate inter-domain mobility at session control level. Service level mobility between different combinations of CS and PS session shall be possible for NGN.

- *Mobility at the inter-access network level*

  Inter-access network mobility allows users to roam across CS or PS domains using various network mobility technologies such as mobile IP or mobile application part (MAP) protocol.

- *Mobility at the intra-access level (wide area)*

  Intra-access level mobility (wide area) refers to either the PS domain or CS domain in NGN. Mobility is provided by the access network technology. For example, mobility at

this level might be provided by GPRS roaming technology for movement between a serving GPRS support node (SGSN) as part of a gateway GPRS support node (GGSN) anchor.

- *Mobility at the intra-access network level (local area)*

  Intra-access network level mobility (local area) refers to mobility within an access that uses a particular technology, generally within a limited geographic area, but handled above the radio resource control layer.

- *Mobility at the intra-access network radio level*

  Intra-access network radio level mobility refers to the mobility at radio level, e.g., radio resource control (RRC) layer in UMTS or cdma2000, and radio resource (RR) layer in GPRS.

- *Mobility at the personal level*

  Personal level mobility refers to the mobility at the user level. For example, a user can perform mobility between terminals, such as an IPv4 MS (mobile station) and an IPv6 MS.

12 Requirements for mobility management

The requirements for MM are provided according to the MM types, covering:

1 Inter-CNs.

2 Inter-ANs.

3 Intra-AN.

The main differences of MM requirements are summarized in Table 1 below:

Table 1 – MM types vs administration and access [b-ITU-T Q.1706]

	Administration	**Access technology**
Inter-CN MM	Different	Same/Different
Inter-AN MM	Same[a)]	Same/Different
Intra-AN MM	Same	Same
[a)] For the case of network sharing, the same physical core network supports two logical CNs.		

A set of minimum requirements are provided in [b-ITU-T Q.1706], it is expected that improved features shall be provided for the different MM mechanisms deployed in NGN. It is also noted that the requirements mainly focus on IP-based new ANs rather than on legacy access networks.

13 General requirements

Regardless of the type of MM mechanism to be used, a set of general requirements for MM in NGN is proposed. The requirements are covered in this clause, see [b-ITU-T Q.1706].

13.1 Harmonization with IP-based networks

In general, NGN offers a number of IP-based services; accordingly, the MM protocols for NGN cover IP-based or, at least, well-harmonized services with IP technology for their efficient and integrated operation in such future networks. It was also recommended to reuse to the extent possible the existing MM techniques/technologies for the design of the MM protocols for NGN, as

discussed in this technical paper through the cooperation with external forums and standards development organizations (SDOs).

13.2 Separation of control and transport functions

The transport plane should be separated from the control plane for efficient mobility management and scalability. Such a separation of control and transport planes provides the architectural flexibility that facilitates the introduction of new technologies and services. Open interfaces between the control plane functions and the transport plane functions are necessary to implement their separation.

13.3 Provision of a location management function

To support the mobility of users and terminals, the location of users and their terminals whenever they move is tracked and maintained by one or more location management functions. In harmony with the overall IP-based structure, location management should be based on an IP-specific approach such as the mobile IP home agent or the SIP registrar.

Location management can be expanded to provide location information to service applications.

13.4 Provision of mechanisms for identification of users/terminals

The MM protocols in NGN must specify how the users and their terminals are to be identified in the networks or systems for mobility management. This identification functionality will be the first step to be taken in the mobility management process and thus used for authentication, authorization and accounting of users and terminals.

13.5 Quality of service (QoS) support

The MM protocols must support QoS which mobile users require. These services include voice over Internet protocol (VoIP), streaming, and other real-time services, as well as Internet best-effort services. The required level of QoS could be different according to the MM types described in Figure 6.

13.6 Interworking with established AAA and security schemes

The MM protocols for NGN must specify how users and terminals are to be authenticated, authorized and accounted, and secured for services using standard authentication, authorization and accounting (AAA) and security mechanisms.

The result of the AAA functionality will be a yes/no decision on the service request made by a user. As a next step, the access network configuration will be adapted to the mobile/nomadic user such that it satisfies the particular quality of service (QoS) level and security association for the requested service. These mechanisms should be based on the user's subscription profile and the technical resource constraints of the respective access networks.

13.7 Location privacy

The location information of particular users should be protected from non-permitted entities. This will entail mutual authentication, security association, and other IP security requirements between the mobile terminal and the location management function.

13.8 Support of network mobility

Network mobility is required in order to cope with NGN, including moving networks as well as moving terminals. Typical example platforms for moving networks could be a bus, a train, a ship, a plane, etc. The MM protocols in NGN need to efficiently support these kinds of moving networks.

13.9 Support of ad hoc networks

The support for ad hoc networks may be considered essential as an important access technology in NGN.

13.10 Resource optimization

The provision of the scheme for resource optimization is required to save power consumption in the terminals and signalling overhead in network side. The resource optimization should be provided to the terminals in the idle mode as well as in the active mode.

The support of resource optimization for idle mode terminals is mainly achieved with a paging procedure. This procedure is usually tightly coupled with location management.

13.11 Support of IPv4/IPv6 and public/private addresses

Currently, IPv4 is still dominant but IPv6 is already being widely deployed, with more instances in the near future. Accordingly, the MM protocols must support IPv6 as well as IPv4. In addition, users and terminals may use their private address rather than their public IP addresses according to the network environment regardless of the IP version. Accordingly, MM should allow for the use of private addresses. In this case, a proxy agent might be needed to support MM-related operations such as location update and paging.

13.12 Provision of personal and service mobility

To realize diverse applications in NGN, personal and service mobility, as well as terminal mobility are required.

13.13 User data accessibility

Services and other network functions require some user data in order to be appropriately customized. These can be either user subscription data or network data; both are required to be supported.

13.14 Support of several types of mobile endpoints

In the NGN environment there are different types of mobile endpoints to be considered. The mobile endpoint can be an application in SIP, an interface in the mobile IP, and existent in a core network, an access network, a user premises network, or a service platform. Each network related to the mobile endpoints should be able to support the mobility of every mobile endpoint.

13.15 Maintenance of binding information

Among the different types of service bindings, the following are important between:

- a user and a service application,
- an application and a network interface card,
- a service platform and a network termination,
- a network termination and a network access point,
- two different access networks.

In NGN, all the above bindings are required to support mobility. Additionally, binding information needs to be maintained in a specific place, i.e., the registers.

13.16 Mobile VPN service and mobility requirements

Additional requirements elaborated and recommended in [ITU-T Y.2811] related to the mobile virtual private network (VPN) service and its mobility connotation include:

- The mobility protocol and related security association mechanisms are required to establish secure mobile VPN tunnels
- The secure mobile VPN tunnels should be released and set up seamlessly as UE moves
- Point-to-point/multipoint-to-multipoint (P2P/MP-MP) VPN tunnel should be created among peers in a community group
- The VPN service control function is required to provide a VPN service by extending the NGN service control function
- Allowing mobile users access to the VPN resources in and out of their networks while supporting seamless mobility
- Resource provisioning and re-provisioning for mobile VPN tunnels in the initial attachment and handover cases should be considered

14 Requirements for inter-core networks mobility management

Inter-core network MM in NGN has the following specific requirements, see [b-ITU-T Q.1706].

14.1 Independence from network access technologies

NGN consists of an IP-based core network with several access networks using different access technologies, as shown in Figure 1. In this architecture, MM should provide mobility between either homogeneous or heterogeneous types of access networks that belong to the same or different operators. Accordingly, it is required that MM be independent of the underlying access network technologies such as 2G, 3G, LTE, WLAN, etc.

14.2 Effective interworking with existing MM protocols

Existing ANs are likely to use their own MM instead of new MM mechanisms. Accordingly, NGN MM must be able to effectively interwork with the existing MM protocols.

15 Requirements for inter-access networks mobility management

Inter-access networks MM mechanisms in NGN have the following specific requirements, see [b-ITU-T Q.1706].

15.1 Independence from network access technologies

As in the inter-core network MM, NGN consists of an IP-based core network with several access networks using different access technologies, as shown in Figure 1. Therefore, MM should provide mobility between either homogeneous or heterogeneous types of access networks that belong to the same or different operators. Accordingly, it is required that MM be independent of the underlying access network technologies such as 2G, 3G, LTE, WLAN, etc.

15.2 Provision of mechanisms for context transfer

It is required that when MT moves across different networks, the context information of the current session, such as QoS level, security method, AAA mechanism, compression type in use, etc., might help to perform the handover of the session from the previous to the new access network, e.g., minimizing the latency involved in handing the session over to new serving entities. The proper use of a context transfer mechanism could substantially reduce the amount of overhead in the servers, individually or in combination, used to support these mechanisms.

15.3 Effective interworking with existing mobility management protocols

Existing access networks are likely to use their own MM mechanisms instead of new ones. Accordingly, the NGN MM mechanisms must be able to effectively interwork with existing MM protocols.

15.4 Provision of a handover management function for seamless services

MM should support handover management to maintain session continuity during movement. Furthermore, those mechanisms should provide fast handovers to cater for seamless non real-time and real-time service requirements, e.g., VoIP and video streaming.

In inter-ANs MM, the handover might be a vertical handover between access networks with different access technologies to different radio access technologies.

15.5 Support of policy-based and dynamic network selection

After detecting the presence of a wireless network, it should be possible for the user to choose to connect to one of the networks to obtain service, based on the following policies driven by the requirements of the service or application to be used, and thus presented to the user.

If the information is presented to a user, the user is not expected to have enough technical knowledge about the parameters listed to take an appropriate decision. Rather, these should be looked after by the service's application software, and the options presented to the user should be only those that can support the needs of the service or application to be executed. These are:

- Quality of service level needed for a particular service, e.g., bandwidth availability, time delay, and packet loss ratio.
- Cost for the particular service in each network, assuming that the network provides cost information as part of its options.
- Security level that the network is able to provide.

Once connected, the terminal should be able to track information of the current network based on the above-mentioned aspects. For example, when a user detects that the QoS level has gone down, it can hand over the service to a new network instantly. From the user's point of view, the network switchover is not visible. For interesting features and possible scenarios using multiple radio access technologies, see [b-ITU-T Y.2027].

16 Requirements for intra-access network mobility management

Intra-access networks MM mechanisms in NGN have the following specific requirements, see [b-ITU-T Q.1706]:

16.1 Provision of mechanisms for context transfer

It is required that when MT moves across different networks, the context information of the current session, such as QoS level, security method, AAA mechanism, compression type in use, etc., might help to perform the handover of the session from the previous to the new access network, e.g., minimizing the latency involved in handing the session over to new serving entities. The proper use of a context transfer mechanism could substantially reduce the amount of overhead in the servers, individually or in combination, used to support these mechanisms.

16.2 Provision of a handover management function for seamless services

Mobility management mechanisms support handover management for maintaining session continuity during movement. Furthermore, those mechanisms should provide fast handovers to cater for seamless non real-time and real-time service requirements, e.g., VoIP and video streaming.

In inter-AN MM, the handover takes place as a horizontal handover within an access network. Accordingly, the handover in intra-AN configurations is expected to provide better performance than for inter-access network configurations.

17 Mobility management design considerations

Initial design considerations conform to the functionality of mobility management mechanisms within NGN. These considerations are screened below to provide an overview of these procedures.

17.1 Network environments

Some of the network environments in NGN are illustrated in Figure 8. The MM framework was designed to support the mobility for NGN users across a wide variety of heterogeneous access networks.

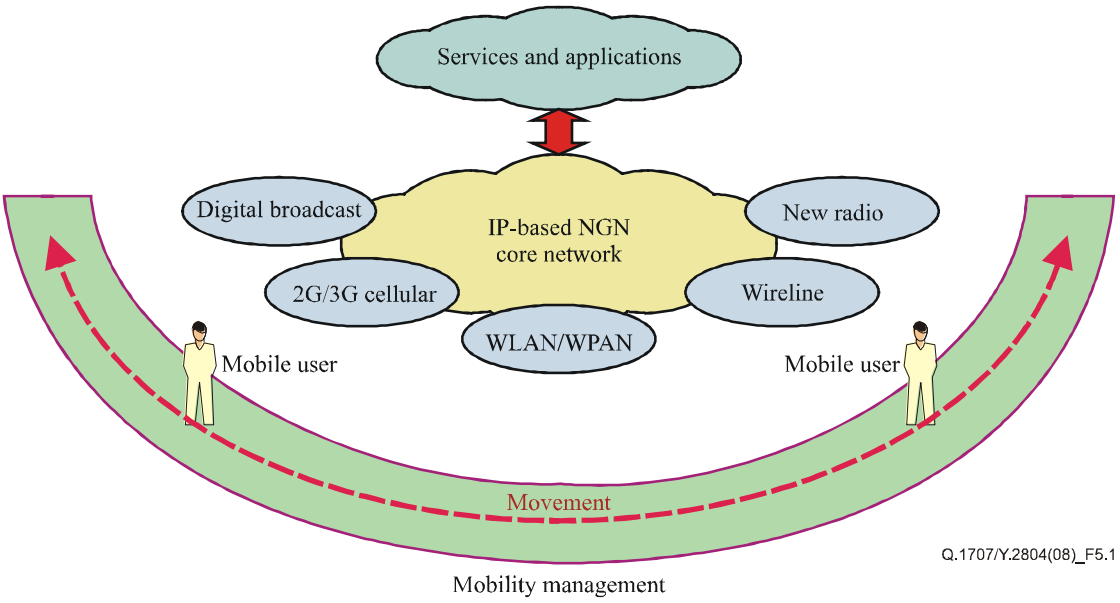


Figure 8 – NGN environments [b-ITU-T Q.1707]

Both signalling and control operations to support the MM mechanisms are set within the context of the NGN architecture. These signalling and control operations are performed among a variety of MM-related functional entities. In NGN, an operator may implement those MM-related functions in the core network (CN) to serve a variety of access networks (ANs). With the help of the appropriate signalling operations for MM, an NGN user benefits by the provision of service continuity in the seamless manner, while it moves around the various access networks in NGN.

17.2 Design principles

The following design principles drive the MM framework specification within the NGN architecture.

17.3 IP-based mobility management framework

One of the major requirements for MM mechanisms in NGN is to operate over the IP-based networks, supporting mobility across a variety of heterogeneous access networks in NGN.

The IP-based framework ensures that the MM functionality be commonly applied to various networks and system infrastructures, independently of the underlying link-layer access technologies.

The IP-based MM framework also facilitates that a variety of the well-defined existing IP-based protocols, such as AAA and dynamic host configuration protocol (DHCP), be reused to support the MM mechanisms.

17.4 Separation of MM control function from transport function

In NGN, the design of the MM functionality is viewed as an independent transport control function, rather than the transport function itself.

The MM control function is designed as a self-contained functionality, not depending on the specific data transport addressed. This feature makes it easier to implement and deploy the MM control function serving a variety of transport networks in NGN.

17.5 Location management and handover control functions

The MM framework is designed to provide location management (LM) functionality. For this purpose, the latest information of the location of a mobile user will be registered and updated each time it continues to move around in the network. The MM framework is also designed to provide handover control (HC) functionality. The HC function supports UE to seamlessly continue data communication during a session, even though the associated IP address changes in the network.

17.6 Separation of user ID and location ID

In the NGN MM framework, the user ID (used as an identifier) is separated from the location ID (used as a locator). An NGN user has its own unique user ID (UID), associated with the user's subscription for his services. The NGN user may have one or more location IDs (LIDs), depending on the specific MM scheme used. A typical example of LID is an IP address. The user ID is statically assigned to an NGN user by the service provider on a per subscription basis. On the other hand, a location ID is dynamically assigned to UE in the network, and it may change.

17.7 Cross-layer interaction for optimized mobility management

To optimize the MM functionality, cross-layer interaction may be required between different protocol layers. The cross-layer optimization enhances mobility management operations such as movement detection, network discovery, network selection, and proactive handover signalling.

In particular, mobility management between heterogeneous access networks may require an open interface for cross-layer interaction. For instance, the open interface can be used for an IP-layer mobility management function to utilize the underlying link-layer services/functions for a wide variety of access technologies.

17.8 Harmonization of different MM protocols

The MM control functionality such as LM and HC shall be realized with a set of MM protocols rather than a single MM protocol. It is then required to effectively harmonize different MM protocols so as to optimize the overall MM functionality.

17.9 Interworking with other protocols

The MM functionality may be realized with additional protocols for authentication, security, call/session establishment, and others. Accordingly, the MM framework is designed to ensure that the MM functions can effectively interwork with all the relevant protocols. For instance, a user should be able to be authenticated via AAA protocols, such as RADIUS or Diameter, without any modification of those protocols. For security purposes, the MM signalling may be protected with the help of protocols such as the IP security protocol (IPSec). For call/session establishment and maintenance, the SIP protocol might be used by MM functions.

17.10 Support of network-based mobility management

The MM framework considers the network-based MM as well as the host-based MM as requirements. A host-based MM may not require any MM functionality in access networks, if the MM control functionality is located in CN.

On the other hand, a network-based MM can minimize the functional overhead of UE, such as the amount of MM signalling. A network-based MM may also support legacy UEs with no MM capability.

17.11 Policy-based mobility management

A policy-based MM shall be considered in order to enhance or optimize the MM functionality. For example, the handover decision might be made as per the pre-configured user/operator policies dictate, which may be contained in the user profile or policy server, see [b-ITU-T Y.2027] for mechanisms used in multi-radio access technologies.

18 Conceptual framework of mobility management

The following clauses present a conceptual framework of the mobility management mechanisms in NGN, see [b-ITU-T Q.1707].

18.1 Mobility management control function

Mobility management may be regarded as control functionality. This functionality is separated from the transport function in NGN; the concept is illustrated in Figure 9.

The MM functionality performs signalling or control operations required by mobility management mechanisms as part of the MM control functions.

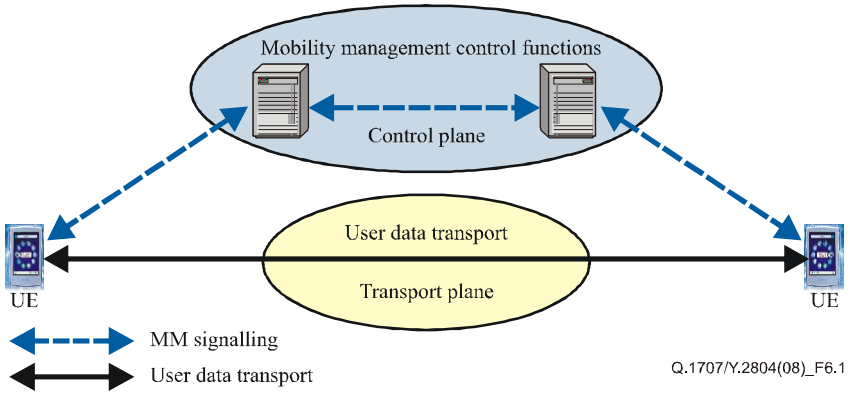


Figure 9 – MM control functionality [b-ITUT Q.1707]

18.2 Types of mobility management in NGN

As described in [b-ITU-T Q.1706], different types of mobility management are applicable in NGN. These may be classified into three types:

1 Inter-core network mobility management between different operators (MM1).

2 Inter-access network mobility management between access networks (MM2).

3 Intra-access network mobility management within the same access network (MM3).

Figure 10 depicts these three types of mobility management.

MM3 considers the MM mechanisms associated with UE moving within an access network. In MM2, UE might change its access network, using its underlying link-layer access technology. MM2 can be further be classified into homogeneous (horizontal) inter-access network MM and heterogeneous (vertical) inter-access network MM.

In MM1, UE may move into the network managed by a different NGN operator.

The MM framework herein described applies to all types of MM.

More detailed issues on each of the three types of MM are addressed in [b-ITU-T Q.1708] and [b-ITU-T Q.1709].

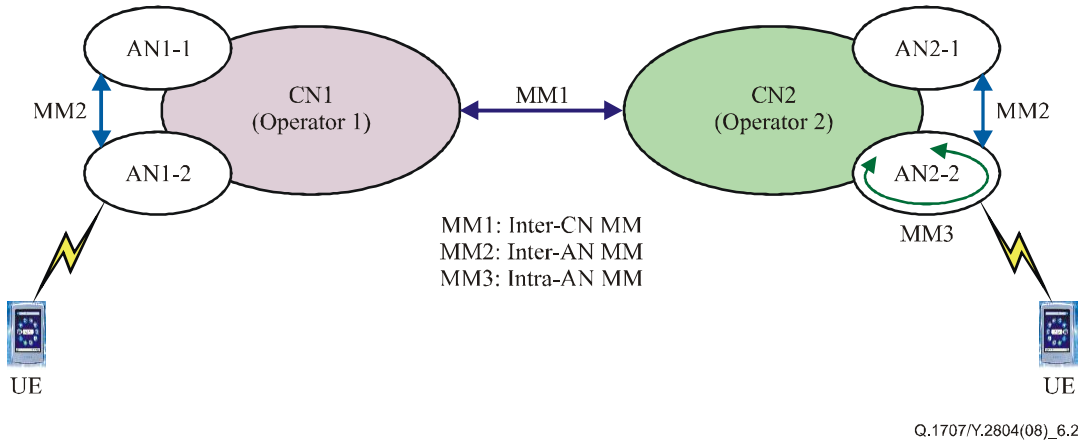


Figure 10 – Types of MM in NGN networks [b-ITU-T Q.1707]

18.3 Mobility management identifiers

This clause describes the main identifiers used for mobility management purposes: user identifier and location identifier.

18.3.1 User identifier

In the MM framework, a user ID (UID) represents an identifier which is defined as a series of digits, characters, symbols or any other form of data which can be used to identify a user, as described in [b-ITU-T Y.2091].

UID shall be able to uniquely identify a specific user in the MM mechanisms. An NGN user may have one or more UIDs, depending on the number of UEs and services associated with the user. Typical examples of UIDs include the international mobile subscriber identity (IMSI), the ITU-T E.164 number (for PSTN services), SIP URI (for IMS-based multimedia services), e-mail address, network access identifier (NAI), and any other identifier of a user or UE.

18.3.2 Location ID

To provide the location management, the MM framework needs to define a location ID (LID) associated with the location of UE. In general, the location information of UE can be classified into two categories:

1 The physical/geographical location ID, e.g., line ID, service set ID (SSID) of access point (AP), or base station ID, and

2 The logical location ID, e.g., routable IP address.

The MM framework will in particular focus on the logical location of UE, i.e., routable IP address, as LID.

Also within the MM NGN scope, an IP address used as LID may have two different features:

1 Temporal, and

2 Persistent.

The temporal IP address may change when UE moves into another network, whereas the persistent IP address may not change.

In the example of mobile IP (MIP), the home address (HoA) can be viewed as a persistent IP address, whereas the care-of-address (CoA) corresponds to a temporal IP address.

In summary, the MM identifiers can be classified into UIDs and LIDs, as shown in Figure 11. UID is used to identify an NGN user, possibly with the associated UE, whereas LID represents the logical or physical location of the user in the network. LIDs are further classified into persistent LIDs and temporal LIDs, depending on whether LID varies with the movement of the user in the network. In particular, an IP address can be used as either a persistent LID or a temporal LID.

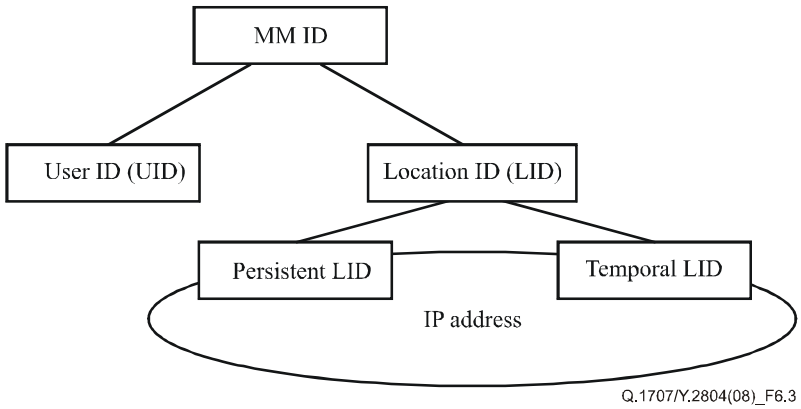


Figure 11 – MM identifiers in NGN [b-ITU-T Q.1707]

18.4 Location management

The location management (LM) function keeps track of the UE movement in the network and locates UE for data delivery.

The LM function also supports the forthcoming 'incoming' session (or call) to the mobile user. The LM functionality includes the following two sub-functions:

1 Location registration and update, and

2 Location query/response (for user data transport) that may be performed with a service control function for call/session establishment.

The location registration and update functions keep track of the current location of UE.

When UE is attached to the network, it will register its current location with the LM location database.

When UE moves into another network, the corresponding LID will be updated.

The location registration and update function manage and update continuously the mapping between UID and LID for a specific UE.

The location query and response functions locate UE. The information on the current location of UE is identified by the suitable location query and response operations.

The location query and response operations may be performed in combination with the relevant service control function.

18.5 Handover control

The handover control (HC) function provides session continuity to the ongoing session while UE moves. To provide the seamless mobility or session continuity, the HC function shall minimize data loss and handover latency during the handover process of UE.

In general, the handover control schemes can be divided into three categories depending on the applicable protocol layer, as follows:

1 handover control in the link layer;

2 handover control in the network layer; and

3 handover control in the transport or application layer.

Each of the handover schemes is performed using the corresponding signalling between the entities associated with the handover.

The handover signalling is based on movement detection in the link layer and/or in the network layer. A different HC protocol or scheme may be employed, depending on the usage of the available information on movement detection and/or on how the handover signalling is delivered.

Different HC schemes may be used, depending on the type of mobility management mechanism, e.g., inter-CN, inter-AN, and intra-AN handover.

19 NGN mobility management functional architecture and 3GPP entities

The following subclauses focus on the functional architecture of mobility management in NGN and its reference points, see [b-ITU-T Q.1707].

The 11 functions and reference points discussed are:

1 mobility management control function (MMCF),

2 central MMCF (C-MMCF),

3 access MMCF (A-MMCF),

4 location management function (LMF) and reference points,

5 central-location management function (C-LMF),

6 access-location management function (A-LMF),

7 reference points within location management function,

8 handover control function (HCF),

9 central-handover control function (C-HCF),

10 access-handover control function (A-HCF),

11 handover control function and reference points.

19.1 Mobility management control Function (MMCF)

Mobility management (MM) in NGN includes mobility management control function (MMCF). MMCF is a set of control functions which provide seamless mobility for NGN users

Figure 12 presents a conceptual model of MMCF in the NGN network. As a control function, MMCF operates independently of the data transport scheme used in the network.

MMCF may further be divided into:

1 location management function (LMF), and

2 handover control function (HCF).

Both serve the location management and handover control, respectively.

[FH – Pls modify the spelling of ‘’signaling’ in Figure 12 to ‘signalling’.]

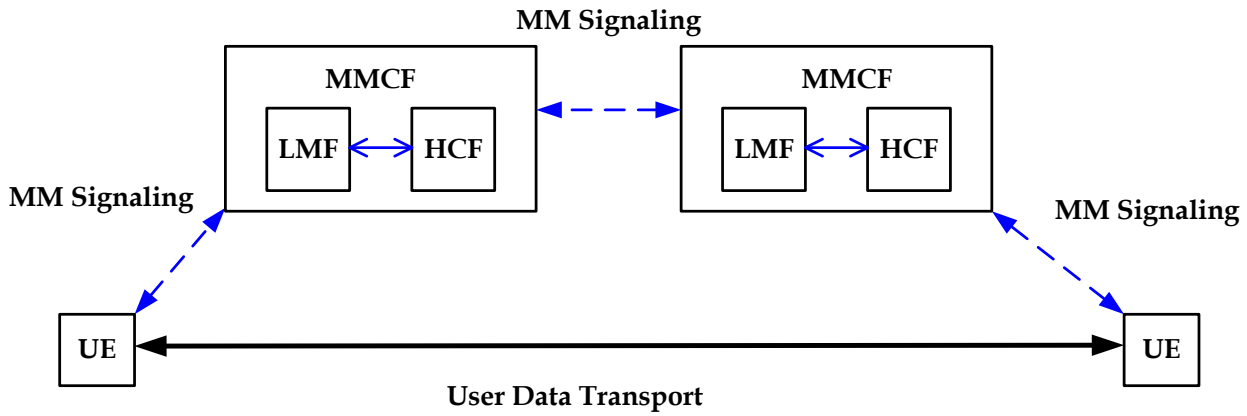


Figure 12 – Mobility management control function (MMCF) model [b-ITU-T Q.1707]

The MM signalling operations are performed between UE and MMCF, and between different MMCFs in the network. In the host-based mobility management mechanisms, the MM control operations include signalling procedures between UE and MMCF, whereas in the network-based MM, the MM control operations may be performed only between MMCFs.

MMCF includes the location management function (LMF) and the handover control function (HCF). Both LMF and HCF represent logical functions, which may be implemented on either a single network component or on different network components.

Therefore, the MM signalling operations may include interworking between LMF and HCF via an internal or external interface. It is required that MMCF be included in the NGN functional architecture.

Figure 13 shows the two-level functional architecture of MMCFs in NGN, with the central MMCF (C-MMCF) and the access MMCF (A-MMCF).

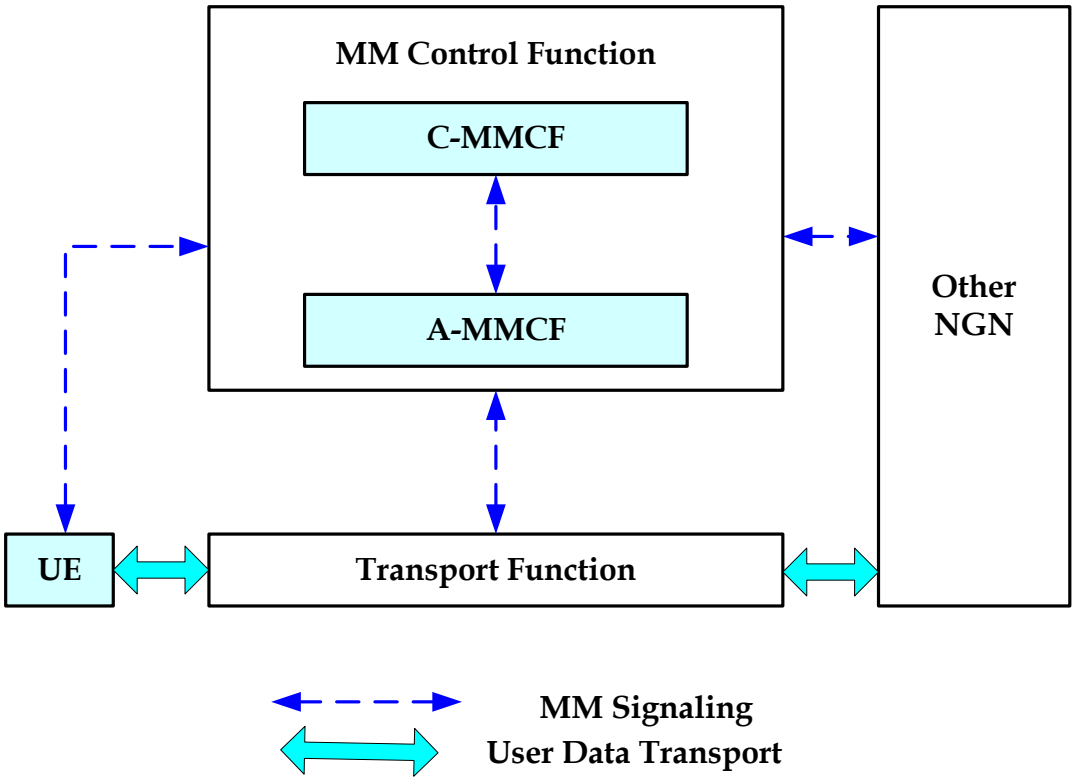


Figure 13 – Functional architecture of mobility management control function (MMCF) in NGN [b-ITU-T Q.1707]

The C-MMCF function manages the user's roaming process between different NGN operators (for MM1, as illustrated in Figure 10).

C-MMCF also manages the mobility within the NGN operator with the help of its downstream A-MMCFs in the network (for MM2 and MM3, as illustrated in Figure 10).

C-MMCF may be located in CN of an NGN operator. C-MMCF consists of central-location management function (C-LMF) and central-handover control function (C-HCF).

The access-mobility management control function (A-MMCF) manages the intra-AN mobility of UE within an access network (for MM3 as illustrated in Figure 10). This function may also support the inter-AN mobility by interaction with C-MMCF (for MM2 as illustrated in Figure 10). A-MMCF may be co-located with the access router (AR) which provides IP connectivity for UE. A-MMCF consists of A-LMF and A-HCF.

Figure 14 depicts MMCFs in NGN. MMCFs can be classified into A-MMCF and C-MMCF; each MMCF may contain LMF and HCF.

MM framework focuses on the functionality and information flows associated with MMCFs which also interact with other NGN functions or functional entities in the MM framework.

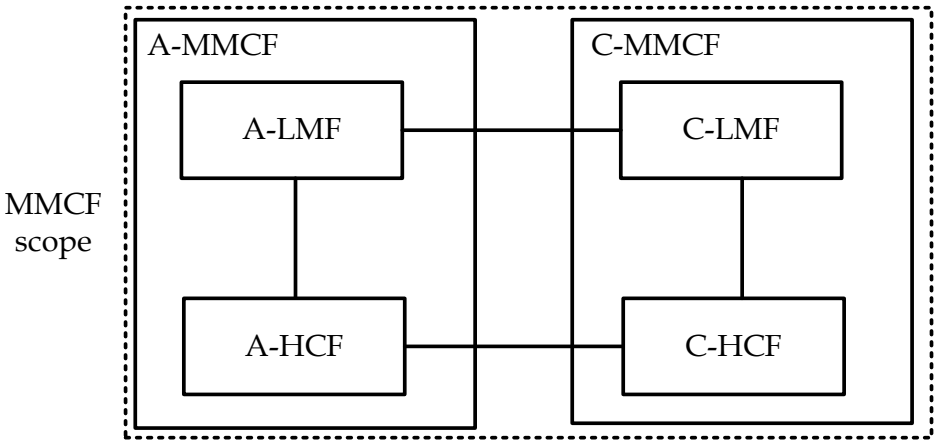


Figure 14 – Structure of mobility management control functions (MMCFs [b-ITU-T Q.1707]

Figure 15 depicts an example of the network configuration of MMCFs in NGN. C-MMCFs and A-MMCFs are logically configured in the NGN network. There may be a variety of other possible configurations of MMCFs in the network. The possible combinations of the MM-related functional entities deployment into one or several network physical nodes is implementation dependent.

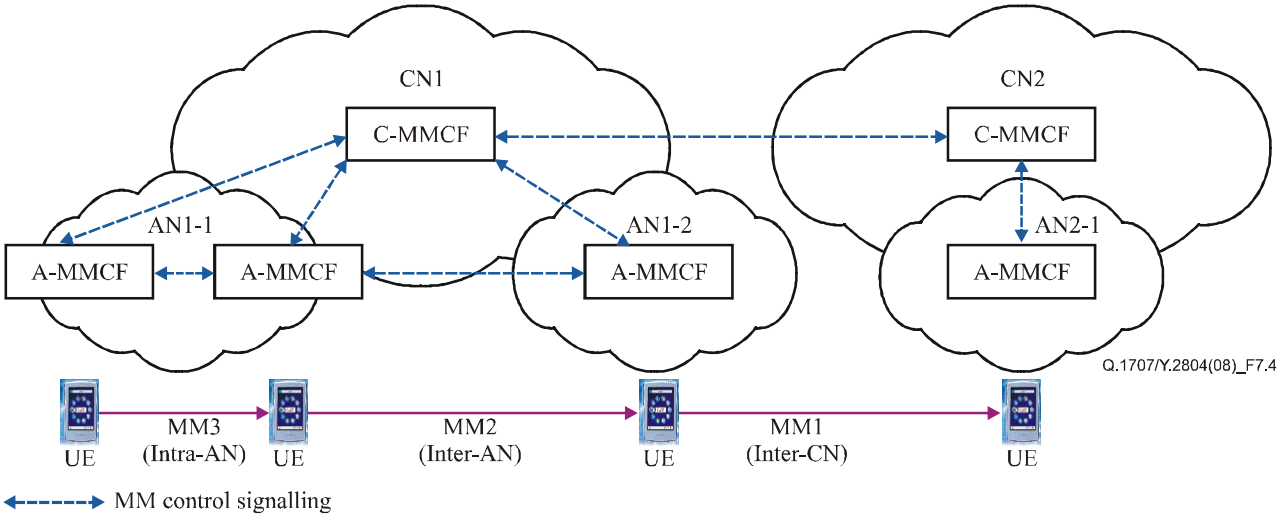


Figure 15 – Example of mobility management control functions (MMCFs) configurations in NGN [b-ITU-T Q.1707]

Alternatively, a hierarchical mobility management functional architecture may be considered in order to enhance scalability of the MM signalling, i.e., to reduce the signalling load and latency as well as to support UE's local mobility within a local network region. This is the objective of IETF hierarchical MIP.

For this purpose, a new MMCF, local MMCF (L-MMCF), may be considered in the MM architecture, resulting in a three-level functional architecture with C-MMCF, L-MMCF, and A-MMCF. In such 3-level architecture, L-MMCF is used to locally manage the mobility of UEs in the network. L-MMCF may be located at the access gateway of the access network. The primary goal of L-MMCF is to support scalability of the MM control operations for a large-scale network and a large number of users in the access network. Such a three-level MMCF architecture is described in [b-ITU-T Q.1708] and [b-ITU-T Q.1709].

19.2 Location management function (LMF)

This clause describes ITU-T approach in which the different elements of NGN LMF were crafted into the basic network infrastructure fabric, including:

- detailed design considerations
- identifiers
- operations
- functional entities
- reference points
- information flows

The location management function (LMF) may be classified into:

1 access-LMF (A-LMF), and

2 central-LMF (C-LMF).

According to its functional role, A-LMF is required to be implemented in the access network. This function cooperates with UE, C-LMF, and the pairing A-LMFs to provide location management functionality.

C-LMF is located in the core network. This function interacts with C-LMFs of another NGN operator, as well as the downstream A-LMFs within the same NGN operator, see [b-ITU-T Q.1707].

19.2.1 Central-Location management function (C-LMF)

The central-LMF (C-LMF) supports the location management of UE moving between different NGNs (MM1), see Figure 10. In this respect, C-LMF is classified into home C-LMF and visited C-LMF. C-LMF has also the functionality to support the location management of UEs within an NGN network (for MM2 and MM3), see Figure 10, by cooperating with its downstream A-LMFs.

19.2.2 Access-Location management function (A-LMF)

Access-LMF (A-LMF) supports the location management of UEs moving within an NGN (for MM2 and MM3), see Figure 10, with the help of C-LMF.

There exist many different LM schemes. For instance, in the host-based MM, the signalling messages for LM can be exchanged between UE and A-LMF. On the other hand, in the network-based MM, an A-LMF may initiate the LM signalling operations instead of UE.

19.2.3 Reference points of location management function

Table 2 shows the reference points in the location management function.

Table 2 – Reference points in location management function

	UE	C-LMF	A-LMF
UE		L_{UC}	L_{UA}
C-LMF	L_{UC}	L_{CC}	L_{AC}
A-LMF	L_{UA}	L_{AC}	L_{AA}

1 The L_{UA} reference point is used to support the location management (LM) signalling between UE and access-LMF (A-LMF). An example of L_{UA} is the MIPv4 protocol used between a foreign agent (FA) and UE.

2 The L_{UC} reference point is used to support the signalling between UE and central-LMF (C-LMF). An example of L_{UC} is the MIPv6 protocol used between the home agent (HA) and UE.

3 The L_{AC} reference point is used to support the signalling between A-LMF and C-LMF. An example of L_{AC} is the MIPv4 protocol used between FA and HA.

4 On the other hand, L_{AA} represents the reference points between two different A-LMFs. For example, in the location update operations, the new A-LMF may request the de-registration of the old information to the old A-LMF; this operation is implementation dependent.

5 L_{CC} represents the reference points between two different C-LMFs, which is used to support the roaming case of UE by using the home LMF and visited LMF.

A detailed treatment and behaviour of these reference points are discussed in [b-ITU-T Q.1708].

19.3 Identifiers revisited

As in indicated in the previous clauses, the identifiers in the context of MM may be classified into user ID (UID) and location ID (LID). The location ID can be further classified into persistent LID (PLID) and temporary LID (TLID), see [b-ITU-T Q.1708].

Table 3 provides an example set of location management identifiers and related used addresses and formats, used in the context of the NGN location management.

Table 3 – Example of ITU-T location management identifiers and related addresses and formats

Format: identifier:	**URI**	**NAI**	**IMSI**	**IP-Address**	**Geographical location**	**HoA**	**CoA**
UID	X	X	X				
Physical location ID					X		
Logical location ID				X			
Persistent LID				X		X	
Temporary LID				X			X

19.3.1 User identifier (UID)

UID represents a user or UE in NGN. UID may be in a variety of formats such as uniform resource identifier (URI), network access identifier (NAI) and international mobile subscriber identifier (IMSI), to name a few. In the MM NGN framework, it is assumed that UID is provided to a user subscribed to the NGN mobility service, see [b-ITU-T Q.1708].

19.3.2 Location identifier (LID)

The location management (LM) functionality is used to keep track of user equipment (UE) in the network. Thus, LM functionality identifies and maintains the location information of UE. The location information or location identifier (LID) is further classified into 'physical' LID and 'logical' LID. The physical LID represents the geographical location of UE. The logical LID includes an IP address to route and/or forward IP packets to UE, see [b-ITU-T Q.1708].

In the current ITU-T MM framework, the physical and geographical LID is normally not considered, but only the logical LID. Furthermore, the IP address is used as LID. In the IP-based LM context, a logical LID or IP address is further classified into persistent LID (PLID) and temporary LID (TLID).

19.3.3 Persistent LID (PLID)

A typical example of PLID is the home address (HoA), defined in mobile IP (MIP). When UE is connected to the network at initial power-on, PLID should be statically or dynamically allocated to UE.

In order to support session continuity for UE, PLID may not be changed, even if UE moves into another IP subnet. In this sense, this LID is called “persistent”. However, in some cases, PLID may be newly configured, e.g., when UE is reconnected to the network after a failure or power-off, or when it enters a new local domain in a localized MM scheme.

19.3.4 Temporary LID (TLID)

A typical example of TLID is the care-of-address (CoA) defined in MIP. If UE moves into another IP subnet, it obtains a new TLID, as in the case of MIPv6 CoA.

In host-based LM procedures, TLID is dynamically allocated to UE, possibly by the dynamic host configuration protocol (DHCP).

In network-based LM procedures, the IP address of the related access router may be used as TLID of UE.

19.4 Location management operations

IP-based Location Management (LM) is used to manage, for each UE, mappings between UID and PLID, and between PLID and TLID. The LM operations consist of:

1 UID binding operation for mapping between UID and PLID, and

2 LID binding operation for mapping between PLID and TLID.

In the following subclauses, the LID binding operations are described in detail.

Although paging management is one of the essential functionalities used in location management procedures in mobile networks, in the current state of ITU-T MM mechanisms the IP-based paging function is for further study, see [b-ITU-T Q.1708].

19.4.1 User identifier (UID) binding operation

The UID binding operation is used to perform and manage mappings between UID (user identifier) and the persistent LID (PLID), for each UE. UID is assigned to an NGN user on a per-subscription basis. As mentioned before, PLID is represented by an IP address.

The UID binding information is registered when UE obtains PLID. Such information is updated if PLID is re-configured by UE, see [b-ITU-T Q.1708].

UID binding operation schemes are quite dependent on the type of UID associated with the user, e.g., in the format usage of URIs, IMSIs, or UE identifiers. Thus, there are a variety of schemes or scenarios for UID binding management.

19.4.2 Location identifier (LID) binding operation

The LID binding operation is used to manage the mapping between persistent LID (PLID) and TLID for each UE. The LID binding update (LBU) operation will be used for LID binding management. This Recommendation focuses on the LID binding operation, rather than on the UID binding operation, see [b-ITU-T Q.1708].

When UE is initially connected to the network, an 'initial' LBU operation is performed. In host-based LM, when UE gets TLID from the network, it should register its TLID with the LM-related functional entity. In network-based LM, in which the IP address of a network agent is used as TLID, the LBU operation will be performed by the corresponding LM-related functional entity in the network. Each time UE moves into a new IP subnet and thus its TLID changes, LBU is performed.

19.4.3 Consideration when using multiple interfaces

UE may have multiple PLIDs (i.e., multiple IP addresses or HoAs) if UE accesses different NGN service providers in order to enjoy different mobile services, see [b-ITU-T Q.1708].

UE may have multiple TLIDs (i.e., multiple IP addresses or CoAs). For instance, one TLID per accessed interface may be allocated to UE, thus allowing UE to use various types of network interfaces and maintain wide area network connectivity.

UE may have one single TLID, even though it may have multiple PLIDs.

UE may also have one single PLID, even though it may have multiple TLIDs.

If multiple PLIDs are allocated to UE, the LID binding update (LBU) operation, for each PLID, may be performed with different central location management functional entities (CLM-FEs). In addition, if multiple TLIDs are allocated to UE, the LID binding operation binds multiple TLIDs to each PLID.

As a typical example, UE with multiple interfaces may have one PLID and multiple TLIDs, one TLID per interface. When UE is initially connected to an access network through one of its interfaces, its PLID is bound to TLID for that interface. Then, if another available interface is selected by UE, UE is also connected to another access network through that interface, and its PLID is also bound to the latter TLID of that interface.

If a new TLID is bound to PLID, the prior TLIDs previously bound to PLID are not overwritten. In addition, there exists a proper mechanism to revoke the binding between PLID and TLID. The detailed functionality and signalling flows for these scenarios are not treated in the initial ITU-T MM procedures, but are considered for further study.

19.4.4 Dynamic assignment of the location management functional entity (LM-FE)

The dynamic assignment mechanism of the LM functional entity (LM-FE) is supported during the location registration according to load balancing, administrative policies, and other requirements.

If a LID binding update (LBU) request (LBU_Request) to LM-FE is responded to with an LBU response (LBU_Response) with failure notification or redirection information, an LBU_Request to the other location management functional entity is attempted, see [b-ITU-T Q.1708].

19.5 Location management for data packet delivery

For data packet delivery or call/session establishment between the corresponding UE (CUE) and UE, the current location information of UE needs to be identified. LM or LM-related functional entity is used to provide the location information of UE for data packet delivery or call/session establishment, see [b-ITU-T Q.1708].

The detailed scheme of data packet delivery or session establishment depends on the associated service control functions or mechanisms used, e.g., with or without session set-up signalling. There exists a variety of operational scenarios to find the location information of UE, e.g., using the persistent LID (PLID) or TLID, via interworking between the LM-related functional entity and the service control function. The current LM mechanisms in NGN do not describe currently the details data packet delivery or session establishment, but focus on the functional architecture and information flows only for the LBU operation within the LM functionality.

19.6 Location management functional reference architecture

This clause covers in more detail the LM reference architecture, see [b-ITU-T Q.1708], in terms of:

1 Functional entities:
   a. Access LM-FE (ALM-FE),
   b. Central LM-FE (CLM-FE).

2 Reference points:
   a. Non-roaming case,
   b. Roaming case.

19.7 Location management functional entities

As described in [b-ITU-T Q.1707], the MM control function (MMCF) consists of the location management function (LMF) and the handover control function (HCF), see [b-ITU-T Q.1708]. LMF includes the following functional entities (FEs):

a. Access LM-FE (ALM-FE), and

b. Central LM-FE (CLM-FE).

Both are logical FEs defined for the location management functionality. These FEs may be located on a single physical entity, or may be implemented into several physical FEs, i.e., they are implementation dependent. Figure 16 shows the architectural model of the LM function with its LM-FEs.

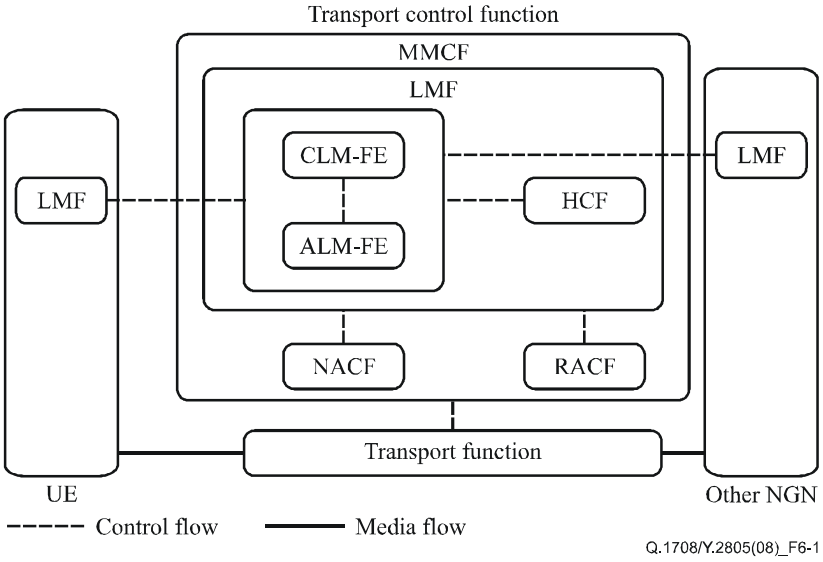


Figure 16 – Functional architecture of location management (LM) [b-ITU-T Q.1708]

UE contains its own LMF function with its counterpart LM-FEs in the host-based LM in the network side. LM-FEs in the network are organized into a two-level hierarchy, ALM-FE and CLM-FE. Each LM-FE performs the LID binding update (LBU) operation.

In terms of MM, LM-FEs can interact with the handover control function (HCF). Each LM-FE has interactions with at least one of the following NGN functions:

1 network attachment control function (NACF),

2 resource and admission control function (RACF), and

3 transport function (TF).

19.7.1 Access location management functional entity (ALM-FE)

ALM-FE is responsible to perform the following LM operations, see [b-ITU-T Q.1708]:

- LBU operation with UE and CLM-FE in host-based LM, and
- LBU operation with CLM-FE in network-based LM.

19.7.2 Central location management functional entity (CLM-FE)

CLM-FE is responsible to perform the following LM operations, see [b-ITU-T Q.1708]:

- LBU operation with UE and ALM-FE in host-based LM, and
- LBU operation with ALM-FE in network-based LM.

19.8 Location management reference points

This clause discusses the reference points and interfaces used to describe the information flows for LM, see [b-ITU-T Q.1708].

19.8.1 Location management reference points for the non-roaming case

For the non-roaming case, the reference points for the LM operations (L_{UA}, L_{AC}, L_{UC}) are shown in Figure 17.

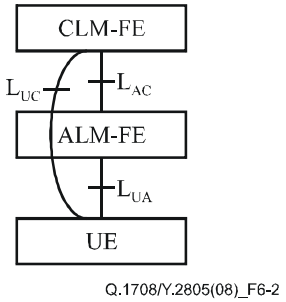


Figure 17 – Reference points for LM for the non-roaming case [b-ITU-T Q.1708]

In the non-roaming case, the LM scenarios are classified as follows:

- Host-based LM with ALM-FE,
- Host-based LM without ALM-FE,
- Network-based LM.

In the case of host-based LM using ALM-FE, two reference points are used:

1 L_{UA} between UE and ALM-FE, and

2 L_{AC} between ALM-FE and CLM-FE.

In the case of host-based LM without ALM-FE, the reference point:

L_{UC} between UE and CLM-FE is used.

In the case of network-based LM, the reference point:

L_{AC} between ALM-FE and CLM-FE is used.

19.8.2 Location management reference points for the roaming case

For the roaming case, the NGN scenarios assume that a roaming agreement is already established between a home NGN provider and a visited NGN provider, and that authentication, accounting and authorization for roaming have also been executed.

The reference points for LM operations in the roaming case (L_{UA}, L_{AC}, L_{UC}) are shown in Figure 18.

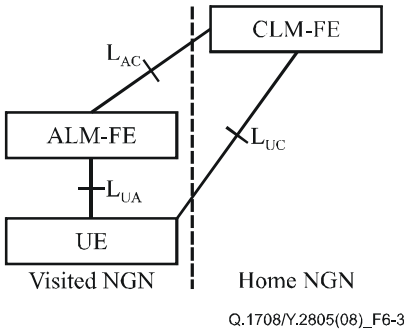


Figure 18 – Reference points for LM for the roaming case [b-ITU-T Q.1708]

For the roaming case, the LM scenarios are classified as follows:

- Host-based LM with the visited ALM-FE,
- Host-based LM without the visited ALM-FE,
- Network-based LM.

In the case of host-based LM using the visited ALM-FE, the two reference points used are:

1 L_{UA} between roaming UE and the visited ALM-FE, and

2 L_{AC} between visited ALM-FE and the home CLM-FE.

In the case of host-based LM, without the visited ALM-FE, the reference point:

L_{UC} between roaming UE and the home CLM-FE is used.

In the case of network-based LM, the reference point:

L_{AC} between the visited ALM-FE and home CLM-FE is used.

19.9 Information flows for non-roaming UE

UE or access LM-FE (ALM-FE) initiates the initial LID binding update (LBU) procedure when it initially attaches to its home network. There are two cases covered in the architecture to describe the procedure:

- Host-based location management where:

  UE initiates the initial LBU procedure by exchanging LID binding update (LBU) messages with the central LM-FE (CLM-FE) directly or via ALM-FE.
- Network-based location management where:

  ALM-FE detecting UE's attachment initiates the initial LBU procedure by exchanging LBU messages with CLM-FE in the home network.

The initial LBU procedure may be omitted, depending on where UE is initially attached with respect to the host-based location management. For instance, when UE's PLID, e.g., HoA in MIP, is topologically correct in respect to its access network, UE does not need the initial LBU procedure. The initial LBU procedure also needs a data path set-up procedure, which may require handover control function (HCF) support. The data path set-up procedure is the same as in the handover case, described in [b-ITU-T Q.1709]. This clause focuses only on the location management procedure.

19.10 Host-based location management

When UE is attached to an access network, UE performs the initial LBU procedure in the host-based location management architecture. As shown in Figure 19, the host-based location management, in the non-roaming case, uses the interaction among UE, ALM-FE and CLM-FE in the home network. After a successful LBU procedure, the relevant LMF entity maintains the mapping between the persistent LID (PLID) and the temporary LID (TLID).

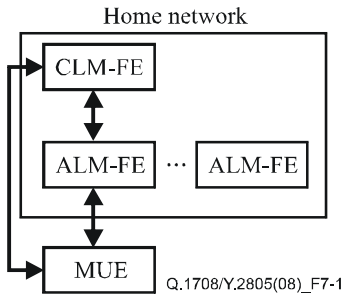


Figure 19 – Host-based LBU architecture for the non-roaming case [b-ITU-T Q.1708]

Figures 20 and 21 show the information flow for the initial host-based LBU procedure in the non-roaming case. UE, attached to its home network initially, starts the initial LBU procedure with CLM-FE by exchanging LBU messages directly or via an ALM-FE. Figures 20 and 21 are the LBU procedures with and without ALM-FE involvement respectively.

If ALM-FE is involved, ALM-FE may act as a proxy for CLM-FE. When CLM-FE receives the initial LBU_Request message, it will respond with an LBU_Response message to UE directly or via ALM-FE. The LBU_Response message may indicate whether the registration is successful or not. A number of reasons for failure of the registration may exist, which may include the overload condition of CLM-FE or administration policies. In case of registration failure, CLM-FE may respond with additional information such as redirection indication and new CLM-FE information for the redirection, which forces UE to re-initiate the LBU procedure with the new CLM-FE. If the LBU_Response message is received with only redirection indication and without new CLM-FE information, UE may try another candidate CLM-FE from the list of candidate CLM-FEs that UE maintains.

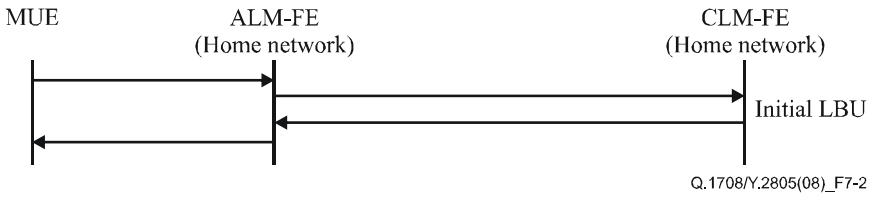


Figure 20 – Host-based initial LBU procedure with ALM-FE in the non-roaming case

[b-ITU-T Q.1708]

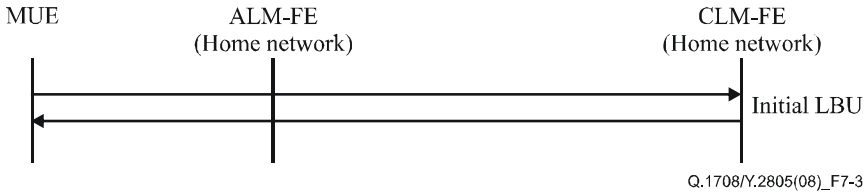


Figure 21 – Host-based initial LBU procedure without ALM-FE in the non-roaming case [b-ITU-T Q.1708]

If UE has multiple interfaces such as wireless fidelity (Wi-Fi), high speed downlink packet access (HSDPA), WiMAX, etc., and multiple TLIDs are allocated to each interface, it may perform multiple LBU procedures with CLM-FE, and so the LID binding operation might bind multiple TLIDs to PLID. In addition, if multiple PLIDs are allocated to UE, it may perform multiple LBU procedures with multiple CLM-FEs for each PLID.

19.11 Network-based location management

When UE is attached to an access network, ALM-FE detecting UE's attachment performs the initial LBU procedure in the network-based location management. As shown in Figure 22, the network-based location management in the non-roaming case is based on the interaction between ALM-FE and CLM-FE. After a successful LBU procedure, the relevant LM-FE maintains the mapping information between the temporary LID (TLID) and the persistent LID (PLID).

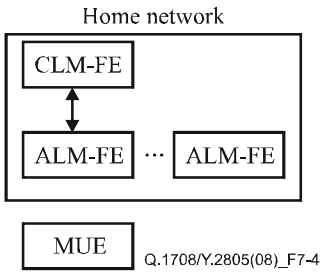


Figure 22 – Network-based LBU architecture in the non-roaming case [b-ITU-T Q.1708]

Figure 23 shows the information flow for the initial network-based LBU procedure in the non-roaming case. ALM-FE detecting an UE's initial attachment starts the initial LBU procedure with CLM-FE by exchanging LBU messages. When CLM-FE receives the initial LBU_Request message from ALM-FE, it responds with an LBU_Response message to ALM-FE. The LBU_Response message indicates whether the registration is successful or not. There are a number of reasons for failure cases; these include overload condition of CLM-FE and administration policies. In case of registration failure, CLM-FE may respond with additional information such as redirection indication and new CLM-FE information for the redirection, forcing ALM-FE to re-initiate the LBU procedure with the new CLM-FE. If the LBU_Response message is received with only redirection indication and without new CLM-FE information, ALM-FE may try another candidate CLM-FE from the list of candidate CLM-FEs that ALM-FE maintains.

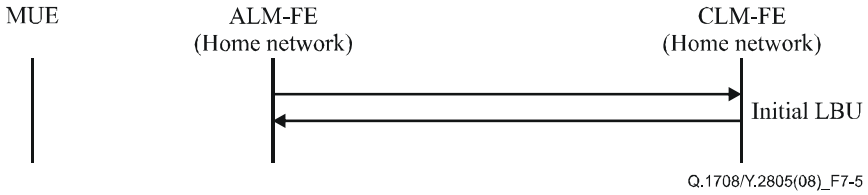


Figure 23 – Network-based initial LBU procedure in the non-roaming case

[b-ITU-T Q.1708]

If UE has multiple interfaces such as Wi-Fi, HSDPA, WiMAX, etc., and each interface is attached to different ALM-FEs, each ALM-FE may perform its own LBU procedure with the same CLM-FE, and so the LID binding operation may bind multiple TLIDs to PLID, see [b-ITU-T Y.2027] for an architecture developed for such cases. On the other hand, if multiple PLIDs are allocated to UE, it may perform multiple LBU procedures with the respective CLM-FEs for each PLID or multiple LBU procedures with the same CLM-FE to create multiple mappings of TLID and PLID in CLM-FE.

19.12 Information flows for roaming UE

When UE roams to a visited network, there are two possible allocation scenarios for the IP address point of view. Firstly, a new IP address may be allocated, regardless of which IP address was allocated to UE in its home network, i.e., a new PLID can be allocated to UE in the visited network. Or, on the other hand, PLID is maintained as the same one, and only a new TLID is allocated to UE.

The ITU-T architecture for location management focused initially only on the second case, where PLID is maintained and a new TLID is allocated, when UE is attached to a visited network.

UE or ALM-FE starts the initial LBU procedure when it attaches to a visited network. As in the non-roaming case, there are two architectures to perform the procedure:

- Host-based location management where:

  UE starts performing the initial LBU procedure by exchanging LBU messages with the home CLM-FE directly or via the visited ALM-FE.
- Network-based location management where:

  The visited ALM-FE detecting an UE's attachment starts performing the initial LBU procedure by exchanging the LBU messages with the home CLM-FE in the UE's home network.

Different however from the non-roaming case, the initial LBU procedure cannot be omitted for host-based location management in the roaming case since UE's PLID is never topologically correct with respect to its access network. The data path set-up procedure is described in detail in [b-ITU-T Q.1709].

19.13 Host-based location management

When UE is attached to an access network in a visited NGN, UE performs the initial LID binding update (LBU) procedure, in the host-based location management architecture. The involved functional entities are shown in Figure 24; the host-based location management uses the interactions among UE, the visited ALM-FE, and the home CLM-FE. After a successful LBU procedure, the relevant LMF entity will maintain the mapping between PLID and TLID.

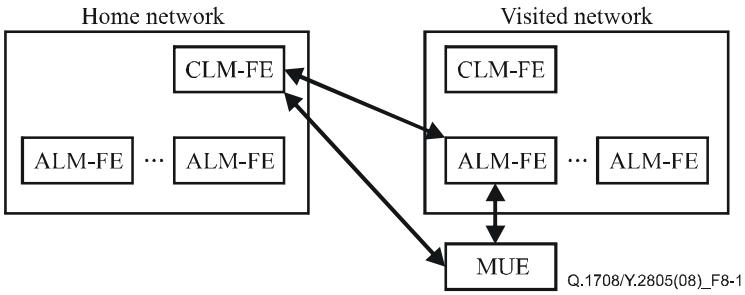


Figure 24 – Host-based LID binding update architecture in roaming case [b-ITU-T Q.1708]

Figures 25 and 26 show the information flows for the initial host-based LID binding update (LBU) procedure in the roaming case.

UE initially attached to a visited network starts the initial LBU procedure with its home CLM-FE by exchanging LBU messages directly or via a visited access LM-FE (ALM-FE). Figures 25 and 26 describe the LBU procedures with and without the visited ALM-FE involvement, respectively.

If a visited ALM-FE is involved, ALM-FE may act as a proxy for the home CLM-FE. When the home CLM-FE receives the initial LBU_Request message, it responds with an LBU_Response message to UE directly, or via a visited ALM-FE. The LBU_Response message may indicate whether the registration is successful or not. A number of failure reasons for the registration may occur; they may range from an overload condition of CLM-FE to administration policies. In case of registration failure, CLM-FE may respond with additional information, such as redirection indication and new CLM-FE information for the redirection, forcing UE to re-initiate the LBU procedure with the new CLM-FE. If the LBU_Response message is received with only redirection indication and without new CLM-FE information, UE may try another candidate CLM-FE from the list of candidate CLM-FEs that UE maintains.

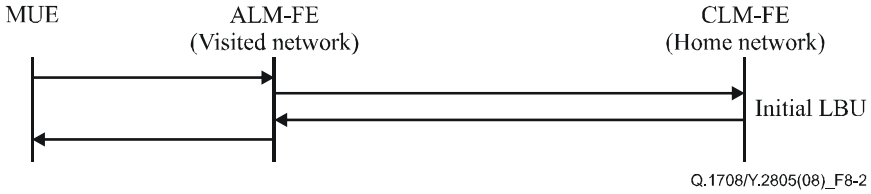


Figure 25 – Host-based LID binding update procedure with visited ALM-FE in roaming case [b-ITU-T Q.1708]

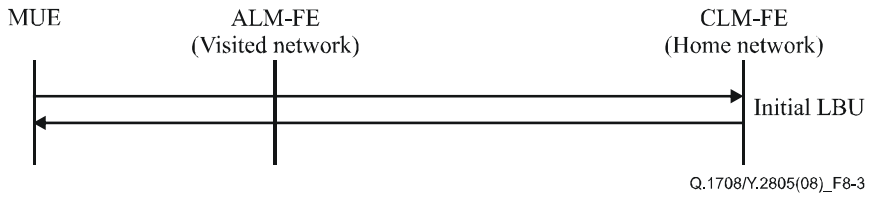


Figure 26 – Host-based LID binding update procedure without visited ALM-FE in the roaming case [b-ITU-T Q.1708]

As in the non-roaming case, the LID binding operation may bind multiple TLIDs to PLID for UEs with multiple interfaces such as Wi-Fi, HSDPA, WiMAX, etc. UE may perform multiple LBU procedures with multiple CLM-FEs for each PLID, or multiple LBU procedures with the same CLM-FE to create multiple bindings of TLID and PLID in CLM-FE.

19.14 Network-based location management

When UE is attached to an access network in a visited NGN, the visited access LM-FE (ALM-FE) detecting UE's attachment performs the initial LBU procedure in the network-based location management architecture.

As shown in Figure 27, the network-based location management is based on the interaction between the visited ALM-FEs and the home CLM-FE. After a successful LBU procedure, the relevant LM-FE maintains the mapping between PLID and TLID.

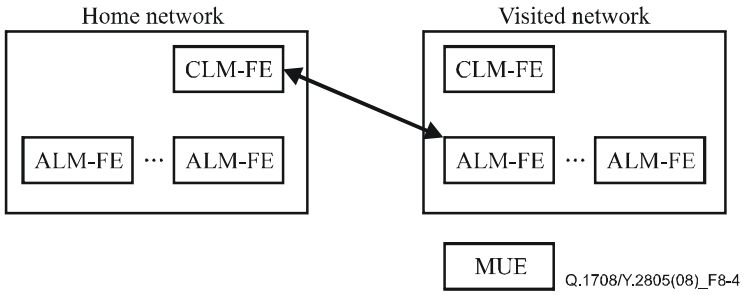


Figure 27 – Network-based LID binding update architecture in the roaming case

Figure 28 shows the information flow for the initial network-based LID binding update (LBU) procedure in the roaming case. A visited ALM-FE detecting an UE's initial attachment starts the initial LBU procedure with the UE's home CLM-FE by exchanging LBU messages. When the home CLM-FE receives the initial LBU_Request message from the visited ALM-FE, it responds with an LBU_Response message to the visited ALM-FE. The LBU_Response message may indicate whether the registration is successful or not. A number of failure reasons may exist in the registration. They may range from an overload condition of CLM-FE to administration policies. In case of registration failure, CLM-FE may respond with additional information such as redirection indication and new CLM-FE information for the redirection, forcing ALM-FE to re-initiate the LBU procedure with the new CLM-FE. If the LBU_Response message is received with only redirection indication and without new CLM-FE information, ALM-FE may try another candidate CLM-FE from the CLM-FE list that ALM-FE maintains.

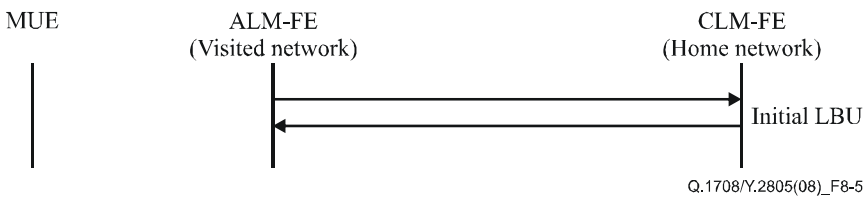


Figure 28 – Network-based initial LID binding update procedure in the roaming case

[b-ITU-T Q.1708]

As in the non-roaming case, the LID binding operation may bind multiple TLIDs to PLID for UEs with multiple interfaces such as Wi-Fi, HSDPA, WiMAX, etc., and ALM-FEs may also perform LBU procedures with multiple CLM-FEs for each PLID or multiple LBU procedures with the same CLM-FE to create multiple mappings of TLID and PLID in CLM-FE.

19.15 Handover control function (HCF)

This clause describes the ITU-T approach in which the different elements of NGN HCF were crafted into the basic network infrastructure fabric, including:

- detailed design considerations
- operations
- functional entities
- reference points
- information flows
- scenarios
- enhanced handover control procedures

The handover control function (HCF) is used to provide the seamless mobility feature to UE when moving around in the NGN network. HCF is further classified into:

1 access HCF (A-HCF) and

2 central HCF (C-HCF),

depending on its functional role and physical location.

A-HCF is the HCF located closest to UE; it is generally located within the access router. It detects handover events and performs the relevant handover control procedures, see [b-ITU-T Q.1709].

C-HCF is generally located in the core network. C-HCF interacts with A-HCF to support the inter-AN handover of UE, see [b-ITU-T Q.1707].

19.15.1 Central-Handover control function (C-HCF)

C-HCF supports the handover of UEs moving around in the NGN operator's network together with the A-HCFs; the specific functional procedure of C-HCF to be applied depends on the handover scheme utilized in the network, see [b-ITU-T Q.1709].

The use of C-HCF for inter-CN (MM1) handover, see Figure 10, was proposed in [b-ITU-T Q.1707] as a case for further study.

19.15.2 Access-Handover control function (A-HCF)

A-HCF controls the handover process of UE moving across or within an access network (MM2 or MM3), see Figure 10. There are a number of different HC schemes, see [b-ITU-T Q.1709].

In host-based MM, UE initiates signalling operations for handover control with the relevant A-HCF, and A-HCF acts relaying the associated information to C-HCFs and/or other relevant A-HCFs.

In network-based MM, A-HCF initiates the handover signalling operations instead of UE.

19.15.318.15.3 Reference points of handover control function

Figure 29 shows the HCF reference points.

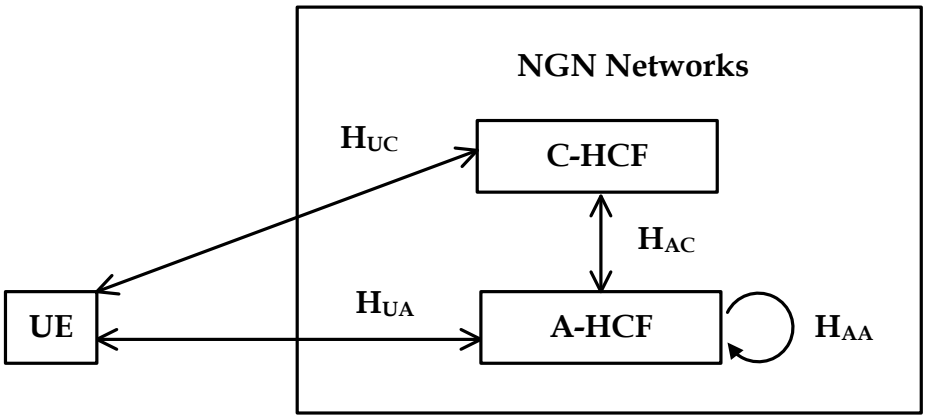


Figure 29 – Handover control function reference points [b-ITU-T Q.1707]

These reference points support the following functionality:

1 The H_{UA} reference point is used to support the signalling between UE and A-HCF. An instance of the H_{UA} reference point in the host-based handover control scheme is the MIPv4 protocol used between the foreign agent (FA) and UE, e.g., in the Internet control message protocol (ICMP) extension for MIPv4. On the other hand, an instance of the H_{UA} reference point in the network-based handover control scheme is the media independent handover (MIH) protocol used between the point of attachment (PoA) and UE, i.e., a handover trigger.

2 The H_{UC} reference point is used to support direct signalling between UE and C-HCF. In terms of the host-based handover control scheme, an instance of H_{UC} is the MIPv6 protocol used between the home agent (HA) and UE, e.g., for MIPv6 route optimization.

3 The H_{AC} reference point is used to support the handover signalling between A-HCF and C-HCF. An instance of H_{AC} for the host-based handover control is the MIPv4 protocol used between FA and HA. Another instance of H_{AC} for the network-based handover control is the proxy MIP (PMIP) protocol used between the mobile access gateway (MAG) and the localized mobility agent (LMA).

4 The H_{AA} is the reference point between the two different A-HCFs. It is used to interact between neighbouring A-HCFs. For instance, the new HCF for UE may request the old HCF to temporally store the data packets destined to UE and to forward the packets after the handover is completed.

The specific usage for these reference points is discussed in [b-ITU-T Q.1709].

19.16 Handover control (HC) framework revisited

This clause revisits the handover control framework for NGN in more detail. The goal of the HC functionality is to provide the mobile user equipment (MUE) seamless services while moving in different NGNs. Seamless handover is supported in ITU-T to provide no service disruption, even if the location ID (LID) is updated, see [b-ITU-T Q.1709].

As described in the previous clauses, the MM identifiers are divided into user ID (UID) and location ID (LID). LID is further classified into persistent LID (PLID) and temporary LID (TLID).

Initially, the NGN MM framework focuses only on the case in which IP addresses are used as LID. The UID binding operation is responsible for mapping UIDs and PLIDs, whereas the LID binding operation is used to map PLID and TLID. The LID binding operation is executed by the LID binding update (LBU) operation.

The LBU operation is performed for location management as well as for handover control. The LBU operation is performed by LM functional entities (LM-FEs) with the support of HC functional entities (HC-FEs).

The following clauses cover the LBU operation as seen by the HC functionality.

By moving into a new IP subnet, also called "Layer 3 (L3) handover", UE changes its TLID. The configuration of TLID is performed differently, depending on whether HC is host based or network based. The LID binding information shall be updated with the new TLID by the LBU operation.

19.16.1 Layer 3 handover and seamless handover

The layer 3 (L3) handover occurs when UE changes its IP address, i.e., its TLID, by moving between different IP subnets. This clause focuses only on IP handover or "L3 handover". The L3 handover is supported by a corresponding layer 2 (L2) handover. The HC operations are further classified into handover and seamless (or fast) handover, as described in clause 6.2.2 of [b-ITU-T Q.1706].

When UE moves into a new IP subnet, a handover operation takes place, and thus a new TLID is updated by the LID binding update (LBU) operation. In the LBU operation, the information related to the mapping between PLID and TLID is updated by the related location management functional entities (LM-FEs), and handover control functional entities (HC-FEs).

The seamless (or fast) handover operation is performed to minimize the service disruption during handover, e.g., packet loss and delay. For this purpose, some optimization schemes may be introduced, see [b-ITU-T Q.1709], such as:

- handover tunnel establishment
- fast access authentication
- pre-emptive HC signalling
- others

19.16.2 Handover operations

The L3 handover tracking UE is typically associated with the operations described in the following clauses, see [b-ITU-T Q.1709]. These are:

1 movement detection or "Handover detection",

2 network selection,

3 TLID configuration,

4 LID binding update.

19.16.2.1 Movement detection

The movement detection, or "handover detection", implies an operation that detects a handover situation or predicts an imminent handover. The movement detection can be further classified into layer 2 (L2) and layer 3 (L3) movement detections. This clause does not discuss the L2 movement detection. However, the notification of L2 movement events needs to be delivered to a HC function (HCF) to trigger the immediate L3 movement detection and to initiate the subsequent HC procedure, see [b-ITU-T Q.1709].

19.16.2.2 Network selection

To control a handover between different access networks, the handover control function (HCF) needs to identify the candidate list of point of attachments (PoAs) currently accessible by UE. Based on this information, UE can choose one of the reachable PoAs to establish a new communication link, see [b-ITU-T Q.1709].

In the network selection operation, the HC function may get some useful information such as signal quality or available resources provided by the candidate PoAs. For this purpose, HCF may interact with the resource and admission control function (RACF) defined in [b-ITU-T Y.2111].

The network selection operation can be also performed with support of the media independent handover (MIH) scheme, see [b-IEEE 802.21].

19.16.2.3 Temporary location identifier (TLID) configuration

When UE moves into a new access network (or IP subnet), its TLID is newly configured. Therefore, UE obtains an IP address as a new TLID from the network, or the IP address of a specific network component may be used as TLID, see [b-ITU-T Q.1709].

19.16.2.4 Location identifier (LID) binding update

To complete the HC procedure, the new TLID should be registered with the suitable location management functional entity (LM-FE) through the location binding update (LBU) operation. This LBU operation shall be performed between UE and LM-FE in the host-based HC scheme. It may also be performed only between LM-FEs in the network-based HC scheme, as described in [b-ITU-T Q.1708].

For handover optimization, the LBU operation needs to be performed as soon as a handover (movement) is detected. For this purpose, HC-FE shall trigger the LBU operation performed by the relevant LM-FE. Communications between HC-FE and LM-FE for the LBU operation are performed by internal reference points (interfaces), which is implementation dependent, see [b-ITU-T Q.1709].

19.16.3 Operations for handover optimization

To provide seamless services for UE during handover, a variety of schemes for handover optimization may be used. Some of those optimization schemes for seamless handover are described below, see [b-ITU-T Q.1709]. They include:

- LBU triggering by the handover control (HC-FE)
- routing path optimization
- handover tunnel establishment
- other schemes for handover optimization

19.16.3.1 LBU triggering by handover control functional entity (HC-FE)

Layer 3 (L3) movement is usually detected by using the “router advertisement” and the “solicitation” messages. This may imply and result in quite long handover latency. To provide seamless handover, the handover control functional entities (HC-FEs) may trigger the location binding update (LBU) operation of the location management functional entities (LM-FEs) as early as possible, see [b-ITU-T Q.1709].

19.16.3.2 Routing path optimization

For efficient data packet delivery or for seamless handover, the routing path between UE_1 and UE_2 needs to be optimized. Specifically, it can be beneficial for UE to send data packets using TLID rather than PLID. For this purpose, the LID binding query (LBQ) operation may be used. The LBQ operation can be classified into the following two categories, see [b-ITU-T Q.1709]:

1 LBQ from UE2 to UE1; and

2 LBQ between handover control functional entities (HC-FEs).

The LBQ operations between UE_2 and UE_1 are shown in the example of the IETF mobile IP (MIP) route optimization scheme between a mobile node and its correspondent node. This operation is performed directly between end UEs without network support. This type of the LBQ operation is for further study and details were out of the scope of the initial MM ITU-T framework.

In LBQ between HC-FEs, HC-FE associated with UE_2 finds TLID of UE_1 by contacting the relevant location management functional entity (LM-FE). Afterwards, data packets to UE_1 are delivered using TLID. ITU-T mobility management Recommendations specify the details of this type of LBQ operation, these mechanisms are described in the following clauses.

19.16.3.3 Handover tunnel establishment

To provide seamless handover, a handover tunnel may be established between two access routers, or two tunnel endpoints controlled by the handover control functional entities (HC-FEs) concerned with the handover of UE. The handover tunnel is used to minimize the data packet loss during handover, see [b-ITU-T Q.1709].

19.16.3.4 Other schemes for handover optimization

In addition, other schemes may be used for handover optimization, including for instance bicasting, pre-emptive LBU, and others. These optimization schemes are for further study in ITU-T, see [b-ITU-T Q.1709].

19.16.4 Host-based and network-based handover control

The handover control (HC) schemes are classified into the following two categories:

1 Host-based scheme in which HC signalling is performed based on (or controlled by) UE.

2 Network-based scheme in which HC signalling is performed (or controlled) by the handover control functional entity (HC-FE).

In the host-based HC, when UE moves into another network region (or IP subnet), it activates the HC operations with the concerned location management functional entities (LM-FEs) and HC-FEs. UE may also perform some handover signalling operations.

In the network-based handover control, HC-FE takes the role of UE. HC-FE may perform most of the handover signalling operations, such as LID binding update (LBU) initiation and handover tunnel establishment, see [b-ITU-T Q.1709].

19.17 Handover control functional reference architecture

This clause describes the functional entities involved in handover control (HC) and their reference points in NGN. See [b-ITU-T Q.1709].

These functional entities include:

1 central LM-FE (CLM-FE),

2 central HC-FE (CHC-FE),

3 access LM-FE (ALM-FE),

4 access HC-FE (AHC-FE), and

5 UE.

The reference points involved in the handover control are shown in Table 4:

1 L_{AC}

2 M_{CC}

3 H_{AC}

4 M_{AA}

5 L_{UA}

6 H_{UA}

Table 4 – Reference points involved in handover control

	CLM-FE	CHC-FE	ALM-FE	AHC-FE	UE
CLM-FE		M_{CC}	L_{AC}		
CHC-FE	M_{CC}			H_{AC}	
ALM-FE	L_{AC}			M_{AA}	L_{UA}
AHC-FE		H_{AC}	M_{AA}	H_{AA}	H_{UA}
UE			L_{UA}	H_{UA}	

19.17.1 Handover control functional entities

As described in [b-ITU-T Q.1707], the mobility management control function (MMCF) consists of the location management function (LMF) and the handover control function (HCF). HCF is composed of the following functional entities (FEs):

- access handover control functional entity (AHC-FE),
- central handover control functional entity (CHC-FE).

It is implementation dependent if these functional entities are located in a single physical entity, or spread into more than one physical entity.

Figure 30 shows the functional architectural model of HCF with the related HC-FEs. It might be interesting to note that the "Functional architecture of handover control" has a strong resemblance to the "Functional architecture of location management (LM)", see [b-ITU-T Q.1708]. Thus, by replacing:

1 LMF by HCF;

2 CLM-FE by CHC-FE;

3 ALM-FE by AHC-FE; and

4 HCF by LMF,

one obtains a similar functional architecture:

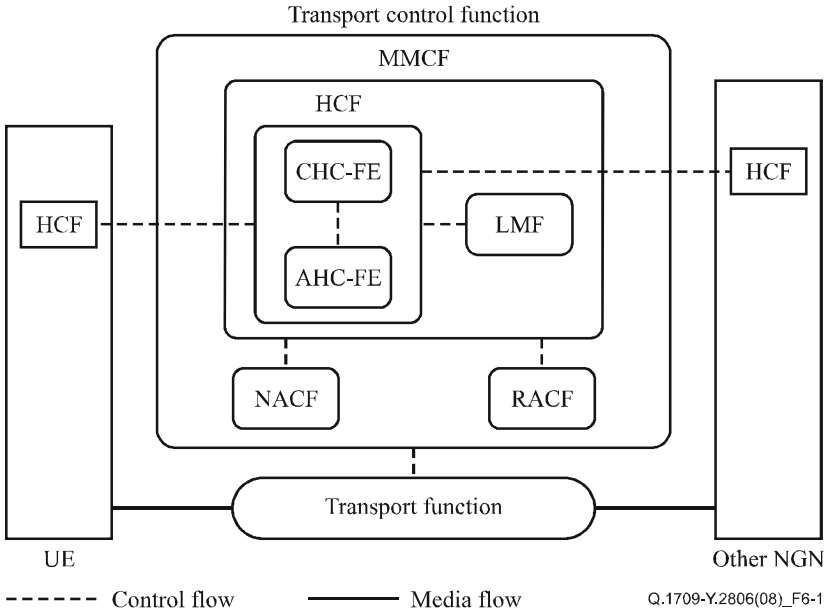


Figure 30 – Functional architecture of handover control (HC) [b-ITU-T Q.1709]

The access HC-FE (AHC-FE) is generally located in the access network. It interacts with the central HC-FE (CHC-FE) and its neighbouring AHC-FEs, the latter is not shown in the figure. CHC-FE is generally located in the core network (CN) and interacts with AHC-FEs in the same NGN and the peering CHC-FE in the other NGN (for inter-CN handover).

Each HC-FE performs HC operations by interworking with UE, LM-FEs, and other HC-FEs. Specific HC operations depend on the host-based HC or network-based HC scheme. In particular, HC-FE shall initiate the LID binding update (LBU) operation with the associated LM-FE in the network-based HC scheme. It is implementation dependent whether LM-FE is located with the corresponding HC-FE in single or different physical platforms.

HC-FE also interacts with other functions in NGN, e.g., NACF, RACF, and transport functions to request/control HC-related operations provided by those NGN functions. For instance, HC-FE may invoke AAA or the IP address allocation function of the network attachment control function (NACF), if it is required to control the handover of UE. RACF may allocate network resources requested by HC-FE to support QoS-guaranteed handovers.

19.17.1.1 Access handover control functional entity (AHC-FE)

In the host-based HC, AHC-FE is responsible to perform:

- Data tunnel establishment with CHC-FE,
- Control of data tunnel path on the UE's handover,
- Establishment of handover tunnel with neighbouring AHC-FEs.

In the network-based HC, AHC-FE is responsible to perform:

- movement detection of UEs,
- LBU initiation with the corresponding ALM-FE,
- data tunnel establishment with CHC-FE or AHC-FE,
- control of data tunnel path on UE's handover,
- establishment of handover tunnel with neighbouring AHC-FEs (optional),
- LID binding query (LBQ) operation with CHC-FE.

19.17.1.2 Central handover control functional entity (CHC-FE)

In the host-based HC and network-based HC, CHC-FE is responsible for:

- supporting network selection of UEs,
- data tunnel establishment with AHC-FEs,
- control of data tunnel paths on UE's handover,
- LID binding query (LBQ) operation with AHC-FEs.

19.17.2 Handover control reference points

This clause identifies the reference points used to describe the information flows for the cases of host-based HC and network-based HC.

Figure 31 shows the reference points in the handover control, also summarized in Table 4.

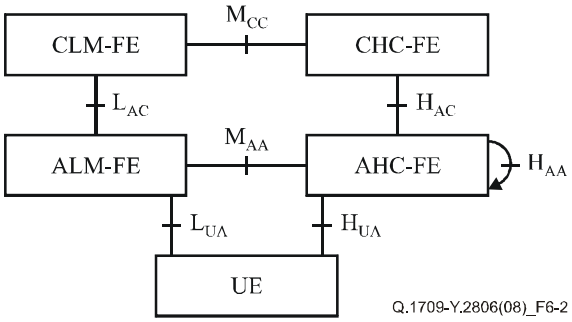


Figure 31 – Reference points in handover control [b-ITU-T Q.1709]

It is noted that HC-FEs are tightly coupled with LM-FEs from the viewpoint of the LBU operation. For the LBU operation, AHC-FE or UE shall request the LBU operation to ALM-FE via the reference point M_{AA} or L_{UA}. The LBU operation is performed between ALM-FE and CLM-FE via L_{AC}, as described in [b-ITU-T Q.1708]. After the completion of the LBU operation, CLM-FE may interact with CHC-FE for handover signalling via M_{CC}. It is implementation dependent if reference points M_{AA} and M_{CC} are implemented via an internal interface, in case HC-FE is located with the corresponding LM-FE in the same device.

In the host-based HC, UE detects the movement and initiates the HC operations. In this case, the reference point H_{UA} between UE and AHC-FE is utilized. For LBU initiation, UE interacts with ALM-FE via L_{UA}. For the establishment of the handover tunnel, AHC-FE may interact with the other AHC-FEs via the reference point H_{AA}.

In the network-based HC, AHC-FE detects the movement of UE and initiates the HC operations. For LBU initiation, AHC-FE interacts with ALM-FE via M_{AA}. For the establishment of the handover tunnel, AHC-FE may interact with the other AHC-FEs via the reference point H_{AA}.

In Figure 31, the reference point H_{AC} between AHC-FE and CHC-FE is used to perform the signalling operations for handover optimization, such as bicasting – which is for further study in ITU-T.

19.18 Information flows for host-based handover control

In the host-based HC scheme, UE initiates the HC operations whenever it moves into another network region (or IP subnet). The associated HC-FE performs the handover signalling procedure by interacting with other HC-FEs and LM-FEs relevant to the handover situation. This clause describes the following two host-based HC cases:

- generic host-based handover control,
- handover control-based on the handover tunnel.

Information flows for host-based HC are conceptually referred to the operations of MIP and fast handover for MIP (FMIP) protocols in IETF.

19.18.1 Generic host-based handover control

In the host-based HC scheme, UE initiates the operations of mobility management control functions (MMCFs) to control a handover. Figure 32 shows the generic architecture of the host-based HC scheme. UE performs the LBU operation with an associated LM-FE as soon as a handover between different AHC-FE's regions is detected. LBU_Request and LBU_Response messages are used for signalling of HC as well as LM among UEs and MMCFs.

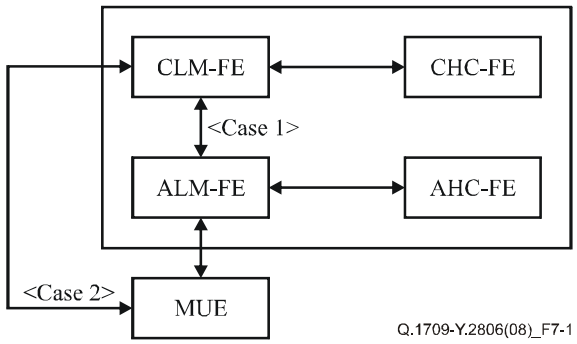


Figure 32 – Generic host-based handover control architecture [b-ITU-T Q.1709]

A data tunnel to deliver packets destined to UE is established along the following two paths:

- between two endpoints controlled by CHC-FE and AHC-FE,
- between UE and an endpoint controlled by CHC-FE.

The signalling interfaces used for those two cases are represented as cases 1 and 2 in Figure 32.

To set up or update a data tunnel for UE, LM-FEs exchange data tunnel control messages with the associated HC-FEs.

Figure 33 illustrates an information flow to handle UE's initial connection establishment to NGN based on the generic host-based HC architecture. Since one of the important roles of HCF is to adjust the data tunnels used by the packets destined to UEs, the tunnel set-up operations in the initial connection step are strongly related to the type of HC scheme. The flow in Figure 33 shows the case in which a data tunnel for UE is established between two endpoints controlled by CHC-FE and AHC-FE (case 1).

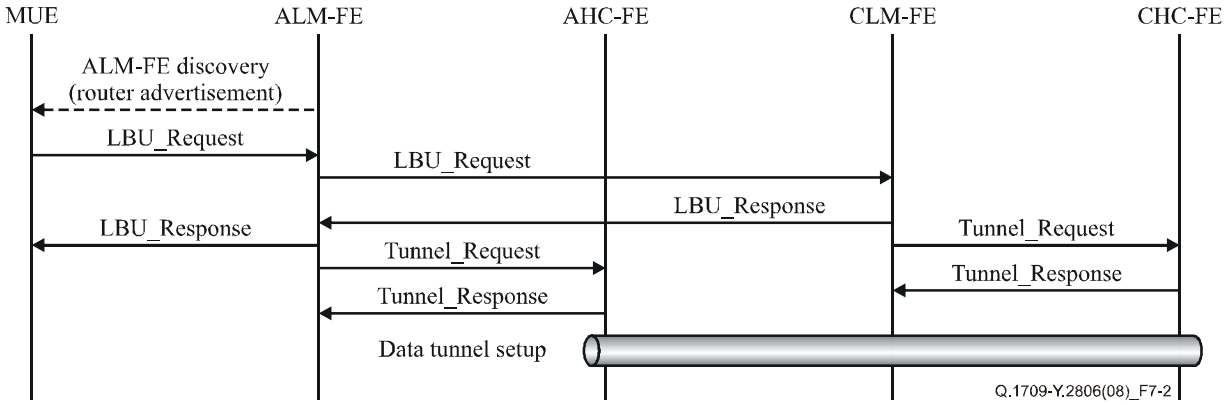


Figure 33 – Initial connection establishment for generic host-based HC (case 1) [b-ITU-T Q.1709]

To simplify the description, the tunnel endpoints are illustrated as HC-FEs in Figure 33. However, most likely the real endpoints of a tunnel are NGN transport functions controlled by those HC-FEs. This simplification is applied to all figures presented in this clause. It is implementation dependent if HC-FE and the relevant transport function are located on a single device.

In Figure 33, when UE is first attached to NGN, it discovers ALM-FE to request its initial LBU procedure. A router advertisement message can be used to inform UE which is the closest ALM-FE responsible for the region. Afterwards, UE initiates the LBU procedure by sending an LBU_Request message to ALM-FE. ALM-FE forwards the LBU_Request message to CLM-FE to request to create the LID binding information of UE.

After an LBU_Response message is transmitted by CLM-FE, CLM-FE and CHC-FE exchange Tunnel_Request and Tunnel_Response messages with each other. This process requests the NGN transport functions to set up an endpoint of a data tunnel with which ALM-FE and UE are bound.

On receiving the LBU_Response message from CLM-FE, ALM-FE and AHC-FE exchange Tunnel_Request and Tunnel_Response messages to set up another endpoint of the data tunnel. Thereafter, data packets are delivered to UE through the data tunnel between CHC-FE and AHC-FE.

Figure 34 shows another information flow to handle UE's initial connection establishment to NGN in the generic host-based HC architecture. This flow illustrates a case in which a data tunnel for UE is established between UE and an endpoint controlled by CHC-FE (case 2).

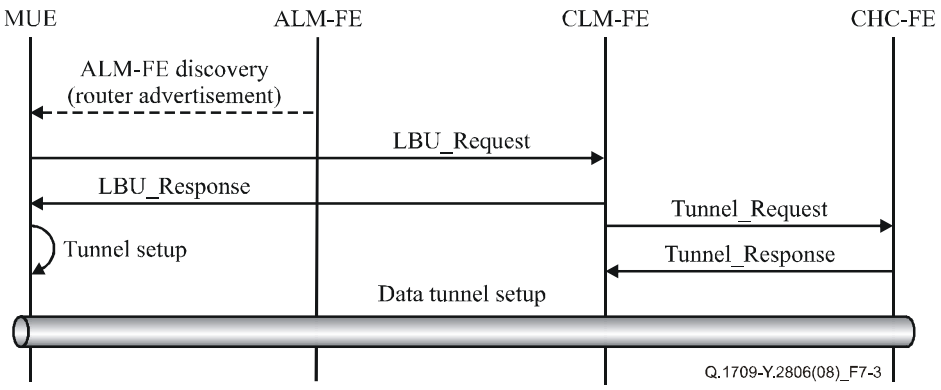


Figure 34 – Initial connection establishment for generic host-based HC (case 2)

[b-ITU-T Q.1709]

In the case of Figure 34, UE initiates the initial LBU procedure by sending an LBU_Request message directly to CLM-FE. This is performed by using a control message for the ALM-FE discovery, which contains the information of CLM-FE. An endpoint of a data tunnel is configured on UE itself after receiving an LBU_Response message. UE should be equipped with the IP-in-IP tunnel endpoint functionalities including encapsulation and de-capsulation of the data packets. The other operations in the flow are equivalent to those for case 1.

Figure 35 illustrates an information flow to control UE's handover between two A-MMCFs' regions based on the generic host-based HC architecture. It describes a case in which a data tunnel for UE is established between two endpoints controlled by CHC-FE and AHC-FE (case 1).

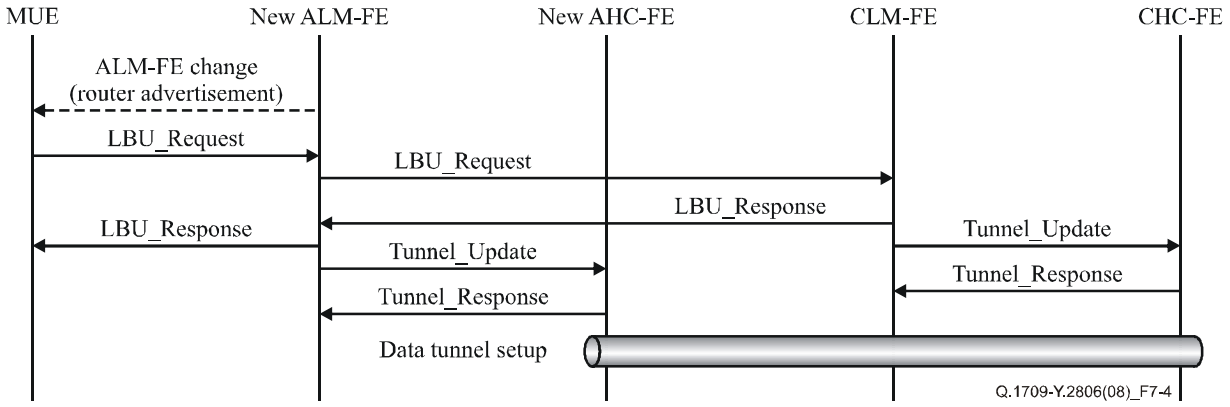


Figure 35 – Generic host-based HC procedure (case 1) [b-ITU-T Q.1709]

The flow in Figure 35 is similar to that of the initial connection procedure, but the Tunnel_Request message is replaced with a Tunnel_Update message. A Tunnel_Update message contains the information to enable AHC-FE and CHC-FE to distinguish the handover situation of UE from the initial connection situation.

When an LBU_Request message is delivered from the new ALM-FE, CLM-FE updates the LID binding information of UE using a newly assigned TLID and replies with an LBU_Response message. A Tunnel_Update message delivered from CLM-FE requests CHC-FE to search and

update the data tunnel binding information of UE so that a new data tunnel, towards the new AHC-FE, is bound by UE. The operations for a Tunnel_Update message at AHC-FE are equivalent to those for the initial connection establishment procedure. Subsequently, data packets for UE are delivered through the tunnel between CHC-FE and the new AHC-FE.

Figure 36 shows another information flow based on the generic host-based HC architecture. It represents a case in which a data tunnel for UE is established between UE and an endpoint controlled by CHC-FE.

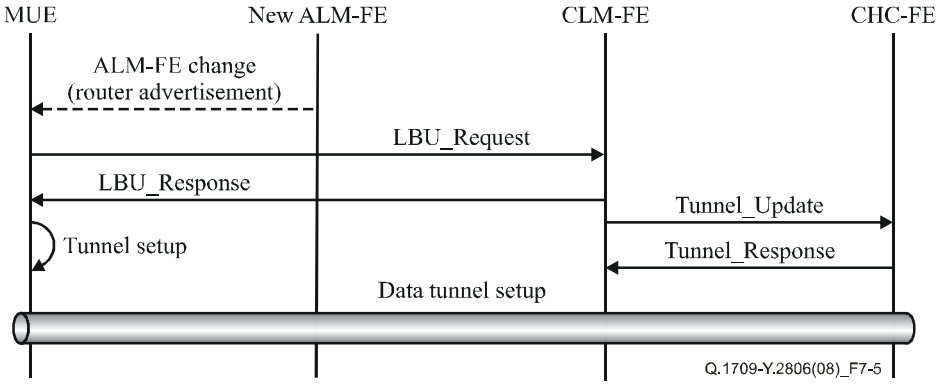


Figure 36 – Generic host-based HC procedure (case 2) [b-ITU-T Q.1709]

As shown in Figure 36, the Tunnel_Request message in the initial connection establishment procedure is also replaced with a Tunnel_Update message to distinguish the handover situation. The LBU_Request and LBU_Response messages are exchanged directly between UE and CLM-FE. The operations to handle those LBU_Request and Tunnel_Update messages are equivalent to those of case 1; the only difference is that UE sets up a data tunnel endpoint instead of AHC-FE.

To reduce the overhead of having all the packets delivered to UE tunnelled under the control of the CHC-FE, CHC-FE may notify to the two corresponding UEs, i.e., those involved in the session, or AHC-FEs of the necessity for a data path optimization processing. This may result in the creation of a new data tunnel established directly between those two corresponding UEs or AHC-FEs. Thereafter, the existing data tunnel controlled by CHC-FE may be replaced with the optimized one, directly established between the two involved UEs. It is implementation dependent whether the data path optimization process is initiated by UE or CHC-FE. Details on the data path optimization are for further study.

19.18.2 Handover control-based on handover tunnel

The HC procedure may be performed using a handover tunnel to minimize data packet loss during the handover. A handover tunnel is established between two endpoints controlled by the old and new AHC-FEs concerned in the handover. Figure 37 shows the host-based HC architecture using the handover tunnel.

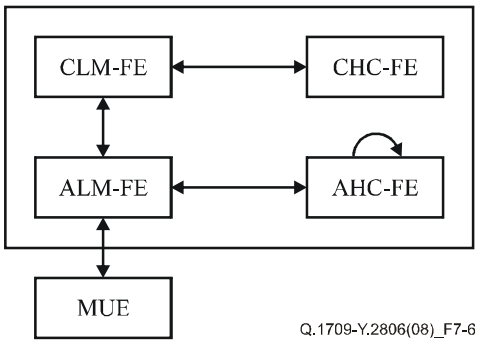


Figure 37 – Host-based HC architecture using a handover tunnel [b-ITU-T Q.1709]

To establish a handover tunnel between two endpoints controlled by AHC-FEs, UE performs the LBU procedure by interacting with the relevant ALM-FEs, i.e., it cannot directly interact with CLM-FE. Two neighbouring AHC-FEs exchange control messages to set up or update handover tunnel for UE.

The initial connection establishment procedure of UE follows the generic information flow presented in Figure 33. However, the signalling operation to establish a handover tunnel is performed between two neighbouring AHC-FEs. Figure 38 depicts an information flow to handle UE's handover between two AHC-FEs' regions using a handover tunnel. It is assumed that UE was originally located in the AHC-FE1's region and then moves into the AHC-FE2's region.

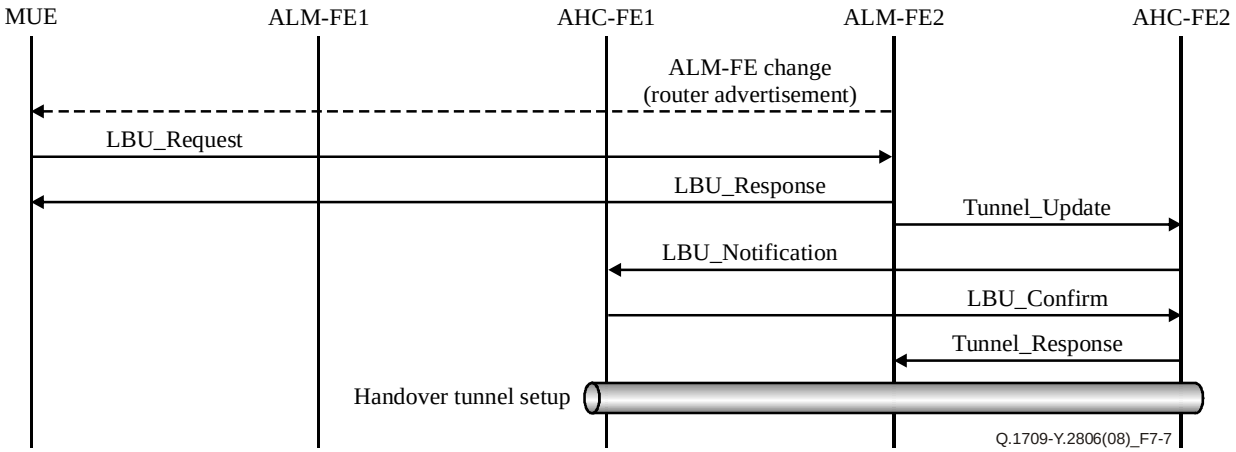


Figure 38 – Handover tunnel establishment procedure [b-ITU-T Q.1709]

UE initiates the LBU procedure by sending an LBU_Request message to ALM-FE2. This LBU_Request message should contain the information to inform ALM-FE2 that UE has moved from the region of AHC-FE1. After replying to the LBU_Request message, ALM-FE2 sends a Tunnel_Update message to AHC-FE2 to establish a handover tunnel.

On receiving the Tunnel_Update message, AHC-FE2 requests the NGN transport functions to set up an endpoint of the handover tunnel and sends an LBU_Notification message to AHC-FE1. Afterwards, AHC-FE1 also requests the transport functions to set up the other endpoint of the handover tunnel. Thereafter, data packets delivered to AHC-FE1 are forwarded to AHC-FE2 through the handover tunnel. Subsequently, AHC-FE2 forwards the packets to UE.

Optionally, the LBU_Request message from UE can be forwarded to CLM-FE by ALM-FE2, thus enabling a new data tunnel between CHC-FE and AHC-FE2 to replace the existing data tunnel extended by the HC procedure, not shown in Figure 38.

19.19 Information flows for network-based handover control

In the network-based HC scheme, AHC-FE initiates the HC operations whenever UE moves into another network region (or IP subnet). HC-FE performs the handover signalling procedure by interacting with other HC-FEs and LM-FEs handling the handover. The following two HC cases are described in this clause:

1 Handover control based on the LID binding update (LBU) operation.

2 Handover control based on the LID binding update (LBU) notification.

19.19.1 Handover control based on LID binding update (LBU) operation

The HC procedure is performed in a tightly coupled manner with the LBU operation between LM-FEs. In this case, only LBU_Request and LBU_Response messages are used for the signalling of HC as well as for LM between A-MMCF and C-MMCF. CHC-FE and AHC-FE control two endpoints of a tunnel to deliver data packets destined to UE, respectively. Figure 39 shows the network-based HC architecture based on the LBU operation.

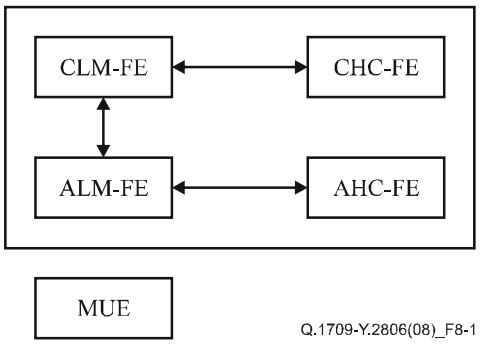


Figure 39 – Network-based HC architecture based on the LBU operation [b-ITU-T Q.1709]

As shown in the figure, UE is not involved in the HC architecture since the mobility management control functions (MMCFs) in the network are fully responsible for the required HC operations in the network-based scheme.
An LBU_Request message from ALM-FE informs CLM-FE of UE's handover situation. CHC-FE and AHC-FE do not interact directly with each other. Each HC-FE has only a message interface between itself and a corresponding LM-FE.

Figure 40 illustrates the information flow for handling UE's initial connection establishment to NGN in the network-based HC scheme based on LBU operation. When UE is first attached to NGN, a Link_Up event trigger is generated from the link layer and delivered to the AHC-FE responsible for the attachment. Using this trigger, AHC-FE should know UE's L2 ID which is unique in NGN, e.g., the international mobile station identity (IMSI) number is an example of UE's unique L2 ID.

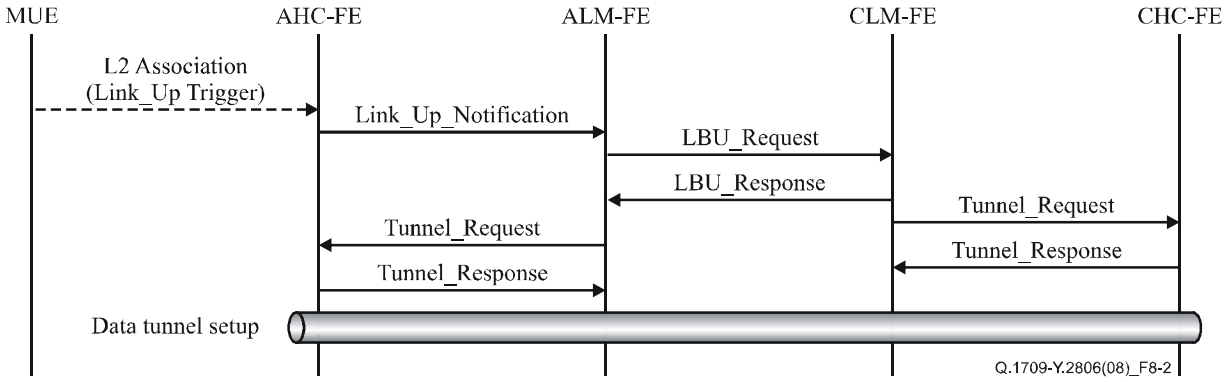


Figure 40 – Initial connection establishment for network-based HC based on LBU operation [b-ITU-T Q.1709]

On receiving a Link_Up trigger, AHC-FE sends a Link_Up_Notification message to the ALM-FE which is included in the same A-MMCF. Then ALM-FE initiates the LBU procedure by sending an LBU_Request message to CLM-FE. The Link_Up_Notification and LBU_Request messages contain UE's unique L2 ID used to identify UE and to search for an associated PLID.

In this case, a data tunnel to deliver packets to UE is established between two endpoints controlled by CHC-FE and AHC-FE, respectively. This tunnel is built when UE is first attached to AHC-FE, or when HC-FEs are deployed in NGN. CLM-FE and CHC-FE exchange Tunnel_Request and Tunnel_Response messages with each other after an LBU_Response message is received from CLM-FE. This process leads the NGN transport functions to set up an endpoint of a data tunnel with which UE is bound. If the data tunnel already exists, only binding information of UE and the associated data tunnel is created.

To simplify the description, the tunnel endpoints are illustrated as HC-FEs in Figure 40. However, it is worth noting that the real endpoints of the tunnels are NGN transport functions controlled by those HC-FEs. This simplification is applied to all the figures presented in this clause.

After ALM-FE receives an LBU_Response message from CLM-FE, ALM-FE and AHC-FE exchange Tunnel_Request and Tunnel_Response messages to set up or update another endpoint of the data tunnel. Thereafter, data packets are delivered to UE through the tunnel between CHC-FE and AHC-FE.

Figure 41 depicts the information flow for handling UE's handover between two A-MMCFs' regions in the network-based HC scheme based on LBU operation. It is similar to that of the initial connection establishment, but the Tunnel_Request message is replaced with a Tunnel_Update message. The Tunnel_Update message contains the information to enable HC-FEs to distinguish the initial connection establishment and handover situations of UE.

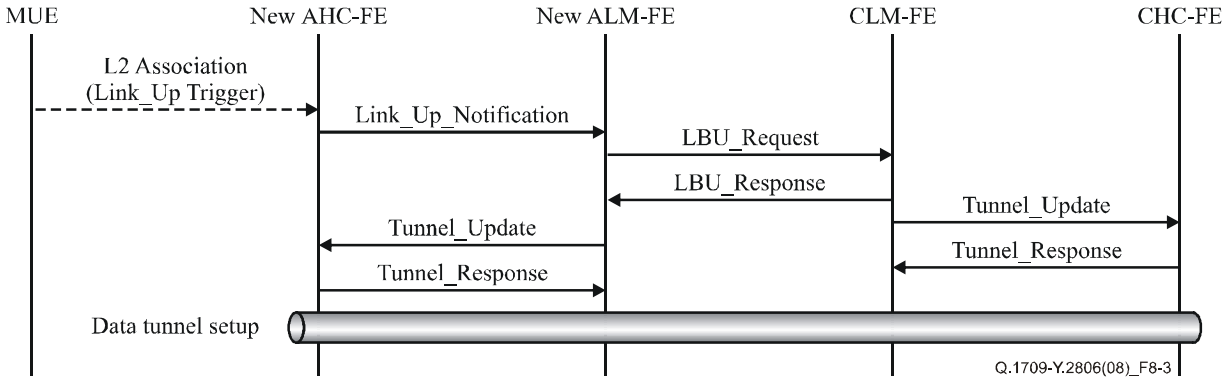


Figure 41 – Network-based HC procedure based on LBU operation [b-ITU-T Q.1709]

When an LBU_Request message from the new ALM-FE is received, CLM-FE updates the LID binding information of UE with a newly assigned TLID. Then CLM-FE replies to the previous LBU_Request message by sending an LBU_Response message. Subsequently, CLM-FE sends a Tunnel_Update message to CHC-FE. On receiving the Tunnel_Update message, CHC-FE searches and updates the data tunnel binding information of UE, so that a new data tunnel, towards the new AHC-FE, is bound by UE. The operation to handle a Tunnel_Update message at AHC-FE is equivalent to that of the initial connection establishment procedure. Finally, data packets are delivered to UE through the tunnel between CHC-FE and new AHC-FE.

In the network-based HC scheme based on the LBU operation, a data tunnel having an endpoint controlled by CHC-FE may be optimized to reduce the overhead of having all the packets delivered to UEs tunnelled under the control of CHC-FE. The optimized data tunnel is established between two endpoints controlled by two corresponding AHC-FEs instead of CHC-FE.

19.19.2 Handover control based on LID binding update (LBU) notification

To avoid bottlenecks at a single point, i.e., a data tunnel endpoint controlled by CHC-FE, a data tunnel may be directly established between the endpoints controlled by AHC-FEs associating two UEs. Thus, the HC procedure may be performed using additional control messages such as LID binding query (LBQ) and LBU_Notification message, as well as LBU_Request and LBU_Response messages.

Figure 42 shows the network-based HC architecture based on LBU notification. Since this case provides the network-based HC operations, UE is not involved in the architecture. CHC-FE and AHC-FE have an interface to interact directly with each other. When establishing a data tunnel for UE, AHC-FE sends an LBQ_Request message to CHC-FE to find out the other endpoint of the tunnel, i.e., UE's TLID. An LBQ_Notification message may also be delivered through this message interface to create the other endpoint of the tunnel. During the HC procedure, CHC-FE sends LBU_Notification messages to the relevant AHC-FEs to create or update the data tunnel endpoints according to the handover (case 1). Otherwise, these LBU_Notification messages may be delivered between two corresponding AHC-FEs (case 2).

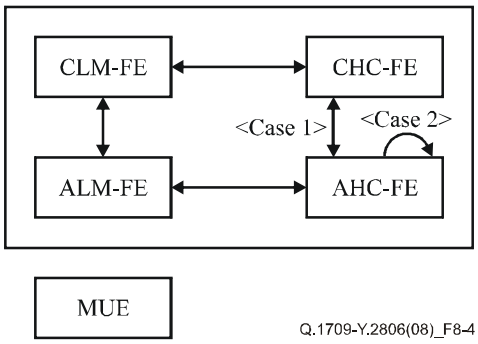


Figure 42 – Network-based HC architecture based on LBU notification [b-ITU-T Q.1709]

Figure 43 shows the information flow for handling UE's initial connection establishment to NGN in the network-based HC scheme based on LBU notification. Since a data tunnel is established on demand when data packets are first delivered from UE_1 to UE_2, the messages to establish a data tunnel are omitted in Figure 43.

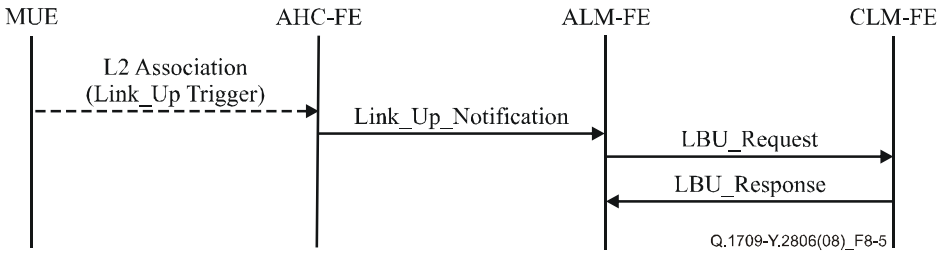


Figure 43 – Initial connection establishment for network-based HC based on LBU notification [b-ITU-T Q.1709]

The Link_Up_Notification message contains UE's unique L2 ID and triggers AHC-FE to initiate the LBU procedure. By exchanging LBU_Request and LBU_Response messages, LM-FEs perform the initial LBU operation for UE which is firstly attached to NGN.

Figure 44 illustrates the information flow for establishing a data tunnel between two corresponding AHC-FEs to deliver packets from UE_1 to UE_2. In the figure, It is assumed that UE_1 (MUE in the figure) is located in the AHC-FE1's region and UE_2 (CUE in the figure) is located in the AHC-FE3's region, respectively.

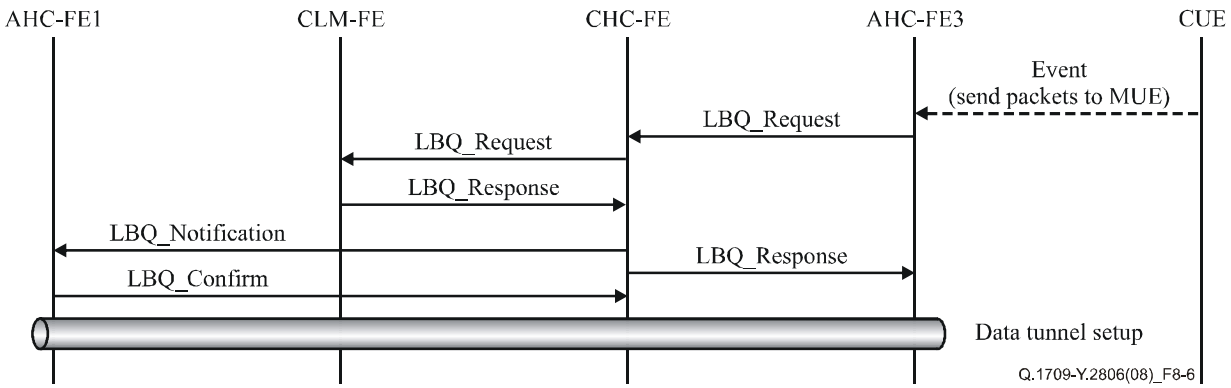


Figure 44 – Data tunnel set-up for network-based HC based on LBU notification

When data packets destined to the PLID of UE_1 (MUE in the figure) are first transferred by UE_2 (CUE in the figure), AHC-FE3 sends an LBQ_Request message to CLM-FE via CHC-FE to find out TLID of UE_1, i.e., a data tunnel endpoint controlled by AHC-FE1. CLM-FE replies to the LBQ_Request message with an LBQ_Response message. Afterwards, AHC-FE3 sets up a data tunnel endpoint using TLID of UE_1 contained in the LBQ_Response message.

On the other hand, upon receiving an LBQ_Response message from CLM-FE, CHC-FE sends an LBQ_Notification message to AHC-FE1 to set up the other endpoint of the data tunnel. This LBQ_Notification message contains TLID of UE_2, i.e., a data tunnel endpoint controlled by AHC-FE3. By completing the set-up of endpoints controlled by AHC-FE1 and AHC-FE3, a bidirectional data tunnel is established to encapsulate and de-capsulate data packets between UE_1 and UE_2. Finally, AHC-FE1 sends an LBQ_Confirm message to CHC-FE as a reply to the previous LBQ_Notification message.

Figure 45 illustrates the information flow for UE_1 (MUE in the figure) handover between two AHC-FE's regions in the network-based HC scheme based on the LBU notification. The flow in the figure describes the case in which UE_1 is handed over from the AHC-FE1's region to the AHC-FE2's region. It is assumed that AHC-FE3 currently controls a data tunnel endpoint associated to UE_2 (CUE in the figure).

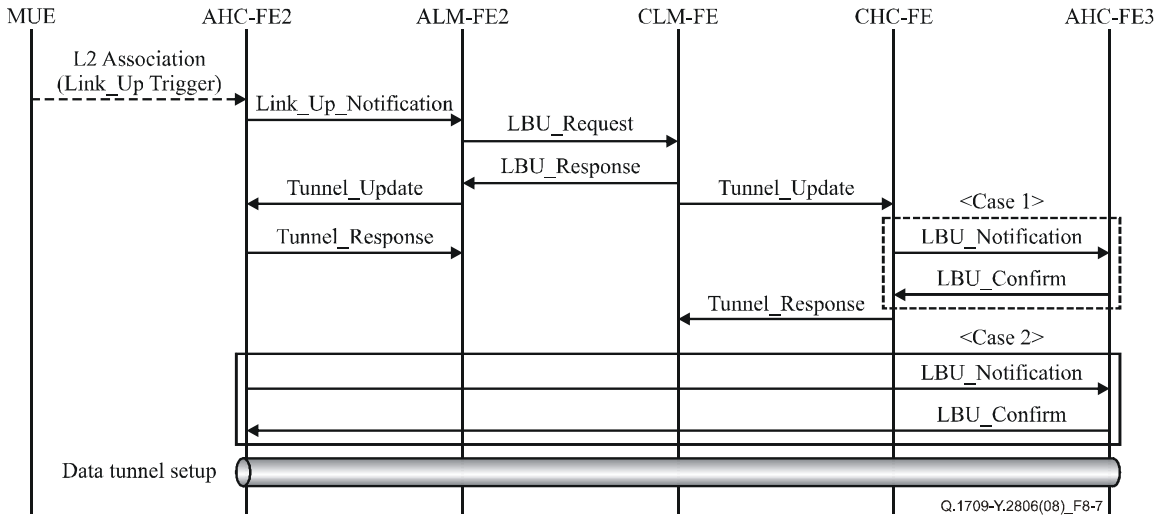


Figure 45 – Network-based HC procedure based on LBU notification [b-ITU-T Q.1709]

Before CLM-FE receives an LBU_Request message from ALM-FE2, the operations performed by the HC procedure are equivalent to those of the initial connection establishment procedure.

CLM-FE knows whether the LBU_Request message handles a handover situation or the initial connection establishment of UE. In the handover case, CLM-FE updates the LID binding information of UE with a newly assigned TLID and then replies to the previous LBU_Request message by sending an LBU_Response message to ALM-FE2. On receiving the LBU_Response message, ALM-FE2 and AHC-FE2 exchange Tunnel_Update and Tunnel_Response messages to set up an endpoint of the data tunnel for UE.

As shown in Figure 45, the data tunnel update operations for AHC-FE3 may be performed in one of the following forms:

1 In case 1, it is assumed that CHC-FE is able to know TLID of EU2 (CUE in the figure). CHC-FE sends an LBU_Notification message to AHC-FE3 to notify the change of the other endpoint of data tunnel. An LBU_Confirm message is used for the reply message.

2 In case 2, it is assumed that AHC-FE2 is able to receive TLID of UE2 from the old AHC-FE, i.e., AHC-FE1. AHC-FE2 sends an LBU_Notification message to AHC-FE3 to notify the change of the other endpoint of data tunnel. An LBU_Confirm message is used for the reply message.

19.20 Home subscriber server (HSS)

Likewise, in the mobile architecture, see [b-ETSI TS 123 002], the location registration and update functions keep track of the current location of UE.

HSS acts as the master database for a given user, containing the subscription-related information to support the network entities handling the calls and sessions.

A home network may contain one or several HSSs, depending on the number of mobile subscribers, on the capacity of the equipment and on the organization of the network.

HSS provides support to the call control servers in order to complete routing and roaming procedures, by providing the data necessary to resolve authentication, authorization, naming and addressing resolution, location dependencies, and others.

HSS is responsible for holding the following user-related information:

1 User identification, numbering and addressing information.

2 User security information: Network access control information for authentication and authorization.

3 User location information at inter-system level: HSS supports user registration, and stores inter-system location information, etc.

4 User profile information.

HSS also generates user security information for mutual authentication, communication integrity check and ciphering.

Based on this information, HSS also is responsible to support the call control and session management entities of the different domains and subsystems of the operator, as shown in Figure 46.

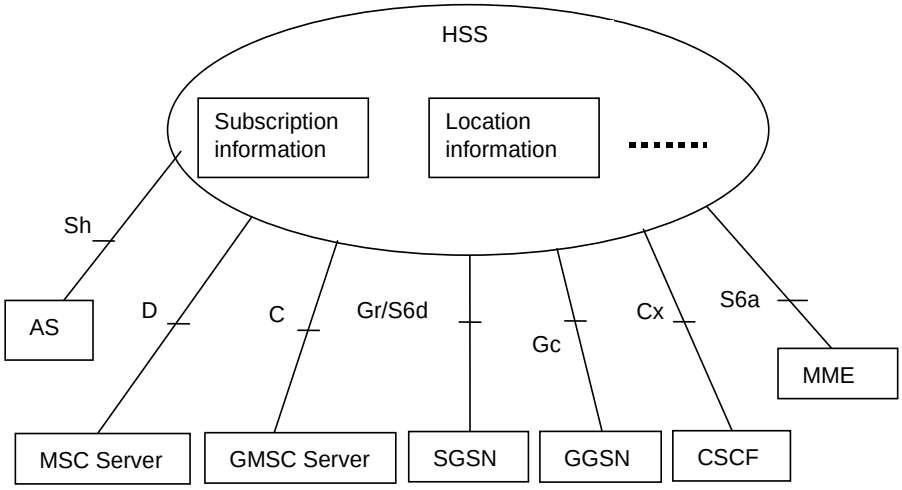


Figure 46 – Generic HSS structure and basic interfaces [ETSI TS 123 002]

HSS may integrate heterogeneous information, and enable enhanced features in the core network to be offered to the application and services domain, while at the same time hiding the heterogeneity.

HSS consists of the following functionalities:

1 IP multimedia functionality providing support to control functions of the IP multimedia subsystem (IMS) such as the call session control function (CSCF). It is needed to enable subscriber usage of services offered by IMS. The IP multimedia functionality is independent of the access network used to access IMS. In connotation not only with subscription information storage, but also to services on top of the transport stratum related to MM, specifically IMS, see [b-ITU-T Y.2809], in which a detailed description of the framework of mobility management in the service stratum is provided. [b-ITU-T Y.2809] addresses issues on terminal mobility based on the IP multimedia subsystem (IMS), by means of identifying the functional architecture of MM in the NGN service stratum, and specifying procedures for location management and handover control.

2 The subset of the home location register (HLR)/authentication centre (AUC) functionality required by the packet switched (PS) domain, i.e., GPRS and evolved packet core (EPC).

3 The subset of the HLR/AUC functionality required by the CS domain, if it is desired to enable subscriber access to the CS domain or to support roaming to legacy GSM/UMTS circuit switched (CS) domain networks.

For more details in the organization of subscriber data, see [b-ETSI TS 123 008]. Additionally, for more details on the numbering system, addresses and identifiers stored in HSS, see [b-ETSI TS 123 003].

19.21 Home subscriber server (HSS) logical functions

In 3GPP EPC, HSS supports mobility management among other functionalities. The following provides a high level but not an exhaustive description of HSS functionality, see [b-ETSI TS 123 002].

The functionality supports the PS domain, the CS domain, and IMS. It includes:

1 Mobility management

This function supports user mobility through the PS domain, IMS, and the CS domain.

2 Call and session establishment support.

3 For terminating traffic, HSS supports the call and/or session establishment procedures by providing information on which call or session control entity currently hosts the user.

4 User security information generation.

5 User security support. HSS generates user authentication, integrity, and ciphering:

HSS supports the authentication procedures by storing the generated data for authentication, integrity and ciphering and by providing these data to the appropriate entity in the core network (CN), e.g., SGSN, MME, 3GPP AAA server or CSCF, and MSC/VLR.

6 User identification handling:

It provides the appropriate relations among all the identifiers uniquely determining the user in the system, e.g., IMSI, MSISDNs, and IP addresses for the PS domain; IMSI and MSISDNs for the CS domain; and private identity and public identities for IMS.

7 Access authorization:

It authorizes the user to have mobile access when requested by SGSN, MME, 3GPP AAA server, CSCF, and MSC/VLR by checking that the user is allowed to roam to that visited network.

8 Service authorization support:

It provides basic authorization for mobile terminating (MT) call/session establishment and service invocation. It also updates the appropriate serving entities, i.e., SGSN, MME, 3GPP AAA server, CSCF, and MSC/VLR with the relevant information used by the services to be provided to the user.

9 Service provisioning support.

10 It provides access to the service profile data, including application services and customized applications for mobile network enhanced logic (CAMEL) services support for GERAN and UTRAN access:

HSS communicates with the SIP application server and the OSA-SCS to support the application services in IMS. It communicates with the service switching function (IM-SSF) to support CAMEL-related services provided by IMS. It communicates with the service capability feature (gsmSCF) to support CAMEL services in GPRS, the PS domain, and the CS domain for GERAN and UTRAN access.

11 Generic user profile (GUP) data repository:

It supports the storage of IMS user-related data and provides access to such data through the Rp reference point.

Figure 47 shows the logical MM functionality embedded in HSS.

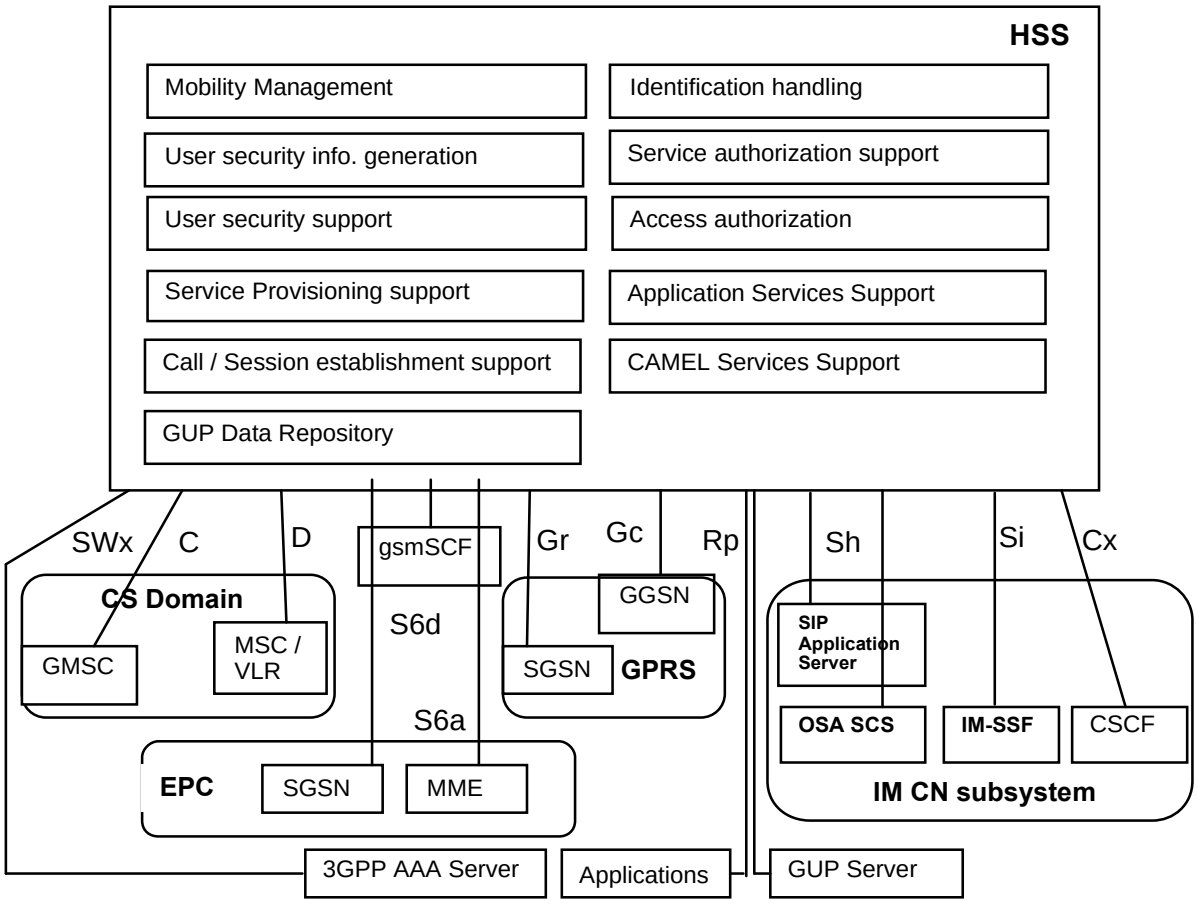


Figure 47 – Home subscriber server logical functions [b-ETSI TS 123 002]

19.22 Policy and charging rule function (PCRF)

PCRF interacts between IMS and EPC creating a bearer with the corresponding QoS characteristics. This functionality is needed since the introduction of a service layer, i.e., IMS, separated the SIP signalling to negotiate the session bearer capabilities from the actual bearer establishment procedure in EPC. The interaction in PCRF is also required to bond signalling and bearer for billing purposes.

19.23 Mobile management entity (MME)

Mobile management entity (MME) is responsible for managing and storing UE contexts, generating temporary identities for UE, control of the idle state mobility, distributing paging messages to the evolved Nodes B (eNBs), security control, and control of the EPS bearers.

More specifically, see [b-ETSI TS 123 002]; MME is the control plane entity within the evolved packet system (EPS) supporting the functions listed below. For the detailed functionality of MME, see [b-ETSI TS 123 401], [b-ETSI TS 123 402], and [b-ETSI TS 123 216].

For mobility management related purposes, MME is responsible for:

- non-access-stratum (NAS) signalling and security,
- inter-CN node signalling for mobility between 3GPP access networks,
- tracking area list management,
- packet data network (PDN) gateway (GW) and serving GW selection,
- serving GPRS support node selection for handovers between 2G or 3G 3GPP access networks,
- roaming,
- authentication,
- bearer management functions including dedicated bearer establishment,
- lawful interception of signalling traffic.

In order to support 3GPP2 access, MME supports:

- high rate packet data (HRPD), access node selection and maintenance for handovers to HRPD,
- transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access.

The procedures for information transfer between SGSN, MME and HSS are defined in [b-ETSI TS 123 401] and [b-ETSI TS 123 060].

When MME supports the interworking to 3GPP CS, MME supports the following functions, as specified in [b-ETSI TS 123 216]:

- performing the PS bearer splitting function by separating the voice PS bearer from the non-voice PS bearers,
- handling the non-voice PS bearers handover with the target cell according to inter-RAT (radio access technology) handover procedure as defined in [b-ETSI TS 123 401],
- initiating the single radio voice call continuity (SRVCC) handover procedure for handover of the voice component to the target cell,
- coordinating PS handover and SRVCC handover procedures when both procedures are performed,
- supporting interworking and SRVCC-related functions for 1xRTT code division multiple access (CDMA) access.

19.23.1 Load balancing between mobility management entities (MMEs)

The MME load balancing functionality permits UEs that are entering into an MME pool area to be directed to an appropriate MME in a manner that achieves load balancing between MMEs, see [b-ETSI TS 123 401]. The procedure sets a weight factor for each MME, such that the probability of the eNodeB selecting MME is proportional to its weight factor. The weight factor is typically set according to the capacity of an MME node relative to other MME nodes. The weight factor is sent

from MME to the eNodeB via S1-AP messages, see [b-ETSI TS 136 413]. If HeNB GW is deployed, the weight factor is sent from MME to HeNB GW.

NOTE 1 – An operator may decide to change the weight factor after the establishment of S1-MME connectivity as a result of changes in the MME capacities, e.g., a newly installed MME may be given a very much higher weight factor for an initial period of time making it faster to increase its load.

NOTE 2 – It is intended (according to [b-ETSI TS 123 401]) that the weight factor is NOT changed frequently, e.g., in a mature network, changes on a monthly basis could be anticipated, e.g., due to the addition of RAN or CN nodes.

19.24 Gateways

In 3GPP, see [b-ETSI TS 123 002], two gateways mainly support the MM mechanisms, introduction to the entities defined already in NGN are suggested to achieve compatibility. These gateways are the:

1 serving GW, and

2 the packet data network (PDN) GW.

These are described in the following subclauses.

19.24.1 Serving GW (S-GW)

The serving GW terminates the interface towards the evolved universal terrestrial radio access network (E-UTRAN). It anchors the user plane for inter-eNBs handovers and inter-3GPP mobility. In this respect, S-GW is similar to SGSN in UMTS, but without the mobility and session functionality, and obly minimal data bearer functions. The packet date convergence protocol (PDCP) and ciphering functions of SGSN reside in eNB in LTE. S-GW supports also lawful interception.

For each UE associated with EPS, at a given point of time, there is a single serving GW. For detailed S-GW functions, see [b-ETSI TS 123 401] and [b-ETSI TS 123 402]. Connectivity to GGSN is not supported.

Some of the functions of the serving GW include:

- local mobility anchor point for inter-eNodeB handover
- mobility anchoring for inter-3GPP mobility
- ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
- lawful interception
- packet routeing and forwarding
- transport level packet marking in the uplink and the downlink
- accounting on user and QoS class identifier (QCI) granularity for inter-operator charging
- local non-3GPP anchor for the case of roaming when the non-3GPP IP accesses connected to the visited PLMN (VPLMN)
- event reporting (change of RAT, etc.) to PCRF
- uplink and downlink bearer binding towards 3GPP accesses as defined in [b-ETSI TS 123 003]
- uplink bearer binding verification with packet dropping of "misbehaving UL traffic"
- mobile access gateway (MAG) functions if proxy MIP (PMIP)-based S5 or S8 is used (3GPP reference points between 3GPP S-GW and PDN gateway (P-GW))

- the support of the necessary functions in order to enable GPRS tunneling protocol (GTP)/PMIP chaining functions

19.24.2 Packet data network (PDN) GW (P-GW)

PDN GW terminates the SGi interface towards PDN. It anchors the user plane for mobility between 3GPP and non-3GPP accesses. It behaves like a home agent (HA) in mobile IP (MIP) providing support for charging, lawful interception, and policy enforcement. UE may be associated with a number of P-GWs.

If UE is accessing multiple PDNs, there may be more than one PDN GW supporting UE; however, a mix of S5/S8 (between 3GPP S-GW and P-GW) interface connectivity and Gn/Gp connectivity might not be supported for UE simultaneously.

PDN GW provides PDN connectivity to both GERAN/UTRAN-only UEs and E-UTRAN capable UEs using any of E-UTRAN, GERAN or UTRAN. PDN GW provides PDN connectivity to E-UTRAN-capable UEs using E-UTRAN only over the S5/S8 interface. PDN GW may also provide PDN connectivity to UEs using non-3GPP access networks with the procedures defined in [b-ETSI TS 123 402].

For detailed PDN GW functions, see [b-ETSI TS 123 401] and [b-ETSI TS 123 402].

P-GW functions include:

- per-user based packet filtering, using for instance deep packet inspection (DPI)
- lawful interception
- UE IP address allocation
- transport level packet marking in the uplink and downlink, e.g., setting the DiffServ code point, based on the QoS class identifier (QCI) of the associated EPS bearer
- uplink (UL) and downlink (DL) service level charging, gating control, rate enforcement as defined in [b-ETSI TS 123 203]
- UL and DL rate enforcement based on APN-aggregate maximum bit rate (AMBR)
- DL rate enforcement based on the accumulated maximum bit rates (MBRs) of the aggregate of service data flows (SDFs) with the same GBR QCI, e.g., by rate policing/shaping
- DHCPv4 (server and client) and DHCPv6 (client and server) functions Additionally, PDN GW includes the following functions for the GPRS tunneling protocol (GTP)-based S5/S8/S2a/S2b:
- UL and DL bearer binding as defined in [b-ETSI TS 123 203]
- UL bearer binding verification PDN GW functions also include user plane anchor for mobility between 3GPP access and non-3GPP access. They support:

- LMA function for dual-stack mobile IPv6 (PMIPv6), if PMIP-based S5 or S8, or if PMIP based S2a or PMIP based S2b is used
- A dual-stack mobile IPv6 (DSMIPv6) home agent, if S2c is used
- Allocation of generic routing encapsulation (GRE) key, which is used to encapsulate uplink traffic to PDN GW on the PMIP-based S5/S8, or PMIP based S2a or PMIP based S2b interface
- A MIPv4 home agent, if S2a with MIPv4 FA care-of-address (CoA) mode is used
- GPRS tunnelling protocol for the control plane and the user plane to provide PDN connectivity to UEs using non-3GPP accesses, if GTP based S2a or GTP based S2b is used

19.25 Serving GPRS support node (SGSN)

In 3GPP, see [ETSI TS 123 002], in addition to the functions described for GPRS, for EPC SGSN, SGSN functions include:

- Inter-EPC node signalling for mobility between 2G/3G and E-UTRAN 3GPP access networks;
- PDN and serving GW selection. The selection of S-GW/PDN GW bye SGSN is similar to MME;
- MME selection for handovers to E-UTRAN 3GPP access network.

For details, see [b-ETSI 123.401] and [ETSI 123 060].

19.26 Evolved packet data gateway (ePDG)

As detailed in [ETSI TS 123 002], in 3GPP the functionality of ePDG includes:

- functionality defined for PDG in [ETSI 123.234] for the allocation of a remote IP address as an IP address local to ePDG which is used as care-of-address (CoA) when S2c is used;
- functionality for transportation of a remote IP address as an IP address specific to PDN when S2b is used;
- routing of packets from/to PDN GW (and from/to serving GW if it is used as local anchor in VPLMN) to/from UE; if GTP based S2b is used, this includes routing of uplink packets based on the uplink packet filters in TFTs assigned to the S2b bearers of the PDN connection;
- routing of downlink packets towards the SWu instance associated to the PDN connection;
- decapsulation/encapsulation of packets for IPSec and, if network based mobility (S2b) is used, for GTP or PMIP tunnels;
- mobile access gateway (MAG) for PMIPv6 if PMIP based S2b is used;
- tunnel authentication and authorization:

  Termination of IKEv2 signalling and relay via AAA messages;
- local mobility anchor within untrusted non-3GPP access networks using MOBIKE, if needed;
- transport level packet marking in the uplink;
- enforcement of QoS policies based on information received via AAA infrastructure;
- lawful interception.

For details, see [ETSI 123.402].

19.27 3GPP AAA server

As specified in [ETSI TS 123 002], the 3GPP AAA server is located at the home PLMN (HPLMN), and it:

1 Provides support for non-3GPP access users supporting services like authentication, authorization, and location management services in order to get access to EPS.

2 Contains necessary user-related information in order to grant access to non-3GPP access.

3 Coordinates the information needed to support mobility between 3GPP and non-3GPP accesses such as coordination of PDN GW information.

4 Interacts with HSS to maintain consistent information for users supporting mobility and service continuity between 3GPP and non-3GPP access.

For more details, refer to [ETSI 123.402].

19.28 3GPP AAA proxy

In 3GPP, see [ETSI TS 123 002], the AAA proxy provides support for roaming non-3GPP access users in VPLMN which is necessary for the authentication, authorization and location management services in order to get access to EPS.

It may also provide roaming-related information for the support of chaining scenarios as described in [ETSI 123.402].

If an S-GW is needed for non-3GPP access in the visited network, the 3GPP AAA proxy selects S-GW for UE during the initial attach or handover attach.

19.29 Access network discovery and selection function (ANDSF)

In 3GPP, see [ETSI TS 123 002],ANDSF, which is an optional element in the architecture, contains data management and control functionality necessary to provide network discovery and selection assistance data as per the operators' policies. ANDSF is able to initiate data transfer to UE, based on network triggers, and respond to requests from UE. It provides functions such as inter-system mobility policy, and access network discovery information.

ANDSF in the subscriber's home operator network may interact with other databases such as the HSS user profile information residing in the subscriber's home operator network. For details on ANDSF, see [ETSI 123.402].

19.30 3GPP access network (AN) entities

Three different types of access network are used by the 3GPP core network, in 3GPP, see [ETSI TS 123 002]:

1 GERAN, also called the base station system (BSS),

2 UTRAN, also called the radio network system (RNS), and

3 E-UTRAN.

MSC and SGSN are able to connect to one of the following access network types, or to both of them:

1 BSS, and

2 RNS.

MME connects to E-UTRAN.

For access technologies offered by BSS, see the 3GPP 45-series Specifications.

The access technologies offered by RNS (FDD, TDD) are described in the 3GPP 25-series Specifications.

The access technologies offered by E-UTRAN (FDD, TDD) are described in the 3GPP 36-series Specifications.

19.30.1 Base station system (BSS)

The base station system (BSS) is the system of base station equipment, including transceivers, controllers, etc. which MSC perceives through a single A and/or Iu-CS interface as being the entity responsible for communicating with mobile stations in a certain area, see [ETSI TS 123 002].

Similarly, in PLMNs supporting GPRS, BSS is viewed by SGSN through a single Gb or Iu-PS interface.

When the intra-domain connection of RAN nodes to multiple CN nodes is applied, BSS may connect to several MSCs by several A and/or Iu-CS interfaces, and BSS may connect to several SGSNs by several Gb and/or Iu-PS interfaces.

The functionality for the A interface is described in [ETSI 148.002] and for the Gb interface in [ETSI 123 060]. The functionality for the Iu-CS interface is described in [ETSI 125.410] and for the Iu-PS interface in [ETSI 123 060].

The radio equipment of BSS may support one or more cells. BSS may consist of one or more base stations. Where an Abis-interface is implemented, BSS consists of one base station controller (BSC) and one or more base transceiver station (BTS). The split of functions between BSS and CN for an Iu interface is described in the 25-series of UMTS Technical Specifications.

The split of functions between BSS and CN for a A/Gb interface is described in the 48-series of GSM Technical Specifications. The split of functions between BSS and CN for an Iu interface is described in the 25-series of UMTS Technical Specifications.
The mobile station shall operate using only the following modes:

a) **A/G_b mode**: for 3GPP pre-Release 4 terminals, or for Release 4 terminals when connected to BSS with no Iu interface towards the core network.

b) **Iu mode**: i.e., Iu-CS and Iu-PS, for Release 4 terminals when connected to BSS with Iu interfaces towards the core network.

No other modes, e.g., A/Iu-PS or Iu-CS/Gb, are allowed. See also [b-3GPP TS 43.051].

19.30.1.1 Base station controller (BSC)

A base station controller (BSC) is a network component in PLMN the function of which is to control one or more base transceiver stations (BTSs), see [ETSI TS 123 002].

19.30.1.2 Base transceiver station (BTS)

A base transceiver station (BTS) is a network component serving one cell, see [ETSI TS 123 002].

19.30.2 Radio network system (RNS)

The radio network system (RNS) is the system of base station equipment, i.e., transceivers, controllers, etc. which is viewed by MSC through a single Iu-interface as being the entity responsible for communicating with mobile stations in a certain area, see [ETSI TS 123 002].

Similarly, in PLMNs supporting GPRS, RNS is viewed by SGSN through a single Iu-PS interface.

When intra-domain connection of RAN nodes to multiple CN nodes is applied, RNS may connect to several MSCs by several Iu-CS interfaces, and RNS may connect to several SGSNs by several Iu-PS interfaces.

The functionality for the Iu-CS interface is described in [ETSI 125.410] and for the Iu-PS interface in [ETSI 123 060].

The radio equipment of RNS may support one or more cells. RNS may consist of one or more base stations. RNS consists of one radio network controller (RNC) and one or more node Bs.

The split of functions between RNS and CN is described in the 25-series of UMTS Technical Specifications.

19.30.2.1 Radio network controller (RNC)

A radio network controller (RNC) is a network component in PLMN which controls one or more node Bs, see [ETSI TS 123 002].

19.30.2.2 Node B

A node B is a logical network component serving one or more UTRAN cells. See [ETSI TS 123 002].

19.30.3 Access network elements for E-UTRAN

The following two subclauses explain the relationship between E-UTRAN node B and the evolved UTRAN, for details in their specification see [ETSI TS 123 002].

19.30.3.1 E-UTRAN node B (eNB)

An eNB is a logical network component serving one or more E-UTRAN cells.

19.30.3.2 Evolved UTRAN

Evolved UTRAN (E-UTRAN) consists of eNBs, providing the E-UTRA user plane (PDCP/RLC/MAC/PHY) and control plane (RRC) protocol terminations towards UE.

eNBs can be interconnected with each other by means of the X2 interface. eNBs are connected by means of the S1 interface to the evolved packet core (EPC), more specifically to the mobility management entity (MME) by means of S1-MME and to the serving gateway (S-GW) by means of the S1-U interface. The S1 interface supports a many-to-many relation between MMEs/serving gateways and eNBs.

The split of functions between eNB and EPC is described in [b-ETSI 123.401], [ETSI 136.300], and [ETSI 136.401].

E-UTRAN consists of a set of eNBs connected to EPC through the S1 interface.

An eNB can support FDD mode, TDD mode, or dual mode operation.

19.31 Mobile station (MS)

The mobile station consists of the physical equipment used by a PLMN subscriber; it comprises the mobile equipment (ME) and the subscriber identity module (SIM), called UMTS subscriber identity module (USIM) from Release 99 and onwards, see [ETSI TS 123 002].

ME comprises the mobile terminal (MT) which, depending on the application and services, may support various combinations of terminal adapter (TA) and terminal equipment (TE) functional groups. These functional groups are described in [b-ETSI 124.002].

19.32 User equipment (UE)

The user equipment allows a user access to the network services, see [ETSI TS 123 002]. For purpose of 3GPP Specifications, the interface between UE and the network is the radio interface. User equipment can be subdivided into a number of domains, the domains being separated by reference points. Currently the user equipment is subdivided into the UICC domain and the ME domain. The ME domain can be further subdivided into one or more mobile terminal (MT) and terminal equipment (TE) components showing the connectivity between multiple functional groups.

20 3GPP and MM related reference points and procedures – Enhancing the compatibility of NGN mobility management framework towards future networks

Based on the functionality of the previously defined 3GPP entities, a closer look into their entities, based on their interfaces, is given in this clause. It is thus hoped that this clause provides guidance to initiate a gap analysis for the activities in the Study Period 2013-2016 encompassing mobility management (MM), therefore making both NGN and 3GPP entities interoperable, specifically LTE, and their interfaces towards a future network development.

After showing the main 3GPP all-IP LTE MM reference points detailed functionality, control plane stacks, flow diagrams, procedures, information fields, and identities are provided to compare and advance the initiation of a gap analysis to fulfil the future network agenda on MM mechanisms and compatibility to existing deployed commercial mobile networks.

In general, when data forwarding is used as part of mobility procedures, different user plane routes may be used based on the network configuration, e.g., for direct or indirect data forwarding. These routes may be between, see [b-ETSI 123.401]:

- eNodeB and RNC
- eNodeB and SGSN
- RNC and S-GW
- S-GW and SGSN

Explicit reference points are not defined for these routes. These user plane forwarding routes may cross inter-operator boundaries, e.g., in case of inter-operator handovers.

The protocol assumptions for the following reference points are such that the:

1 S1-U is based on GTP-U protocol.

2 S3 is based on GTP protocol.

3 S4 is based on GTP protocol.

4 S5 is based on GTP protocol. PMIP variant of S5 is described in [ETSI 123.402].

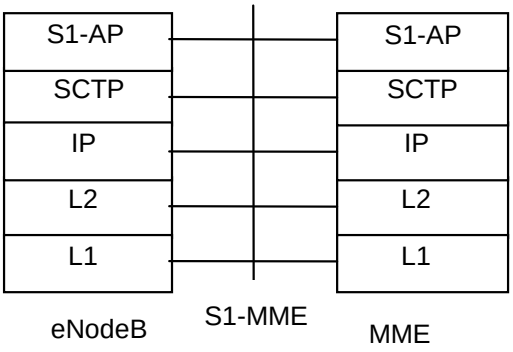
5 S8 is based on GTP protocol. PMIP variant of S8 is described in [ETSI 123.402].

6 S3, S4, S5, S8, S10 and S11 interfaces are designed to manage the evolved packet system (EPS) bearers.

The relevant MM reference points are explained in detail in the following clauses.

20.1 Reference point for the control plane protocol between E-UTRAN and the mobility management entity (MME) (S1-MME)

Reference point S1-MME manages the control plane protocol between E-UTRAN and the mobility management entity (MME). The control plane for this interface is depicted in Figure 48, for details see [b-ETSI 123.401].



- S1 application protocol (S1-AP): Application layer protocol between eNodeB and MME.
- Stream control transmission protocol (SCTP): This protocol guarantees delivery of signalling messages between MME and eNodeB (S1). SCTP is defined in [b-IETF RFC 4960].

Figure 48 – Control plane for S1-MME interface [b-ETSI 123.401]

For further details, see [ETSI 136.300] for the corresponding control plane for the HeNB subsystem – MME.

A number of identities are used in this reference point, two of which are:

1 eNodeB S1-AP UE identity (eNodeB S1-AP UE ID), which is the temporary identity used to identify UE on the S1-MME reference point within eNodeB. It is unique within eNodeB.

2 MME S1-AP UE identity (MME S1-AP UE ID), which is the temporary identity used to identify UE on the S1-MME reference point within MME. It is unique within MME.

20.2 Reference point between E-UTRAN and serving GW (S1-U)

The reference point between S1-U is defined between E-UTRAN and the serving GW (S-GW) on a per bearer user plane tunnelling and inter eNodeB path switching during handover, see [b-ETSI 123.401].

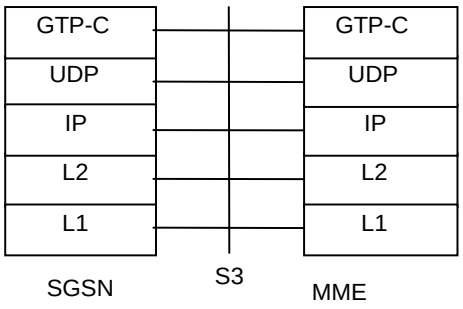
When inter-operator boundaries are crossed, S1-U may be based on the GTP-U protocol.

20.3 Reference point between serving GPRS support node (SGSN) and mobility management entity (MME) (S3)

Reference point S3 enables user and bearer information exchange for inter-3GPP access network mobility in the idle and/or the active state. This reference point may be used in intra-operator or inter-operator scenarios, e.g., in the case of inter-operator handover, see [b-ETSI 123.401].

When inter-operator boundaries are crossed, S3 is assumed to be based on the GTP protocol.

The MME function includes inter core network node signalling, for mobility between 3GPP access networks, i.e., terminating S3 reference point. The control plane for this interface is depicted in Figure 49.



- GPRS tunneling protocol for the control plane (GTP-C): This protocol tunnels signalling messages between SGSN and MME (S3).
- User datagram protocol (UDP): This protocol transfers signalling messages. UDP is defined in [b-IETF RFC 768].

Figure 49 – Control plane for the S3 interface [b-ETSI 123.401]

In regards to routing, for all the messages used in the exchange of RAN information:

The source RAN node sends a message to its MME or SGSN including the source and destination addresses. SGSN/MME uses the destination address to route the message encapsulated in a GPRS tunneling protocol (GTP) message to the correct MME/SGSN via the S3 or Gn interface.

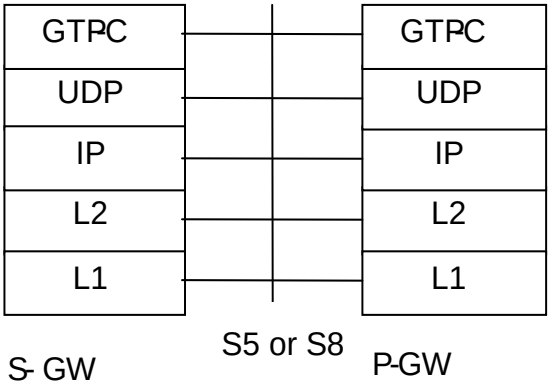
MME/SGSN connected to the destination RAN node decides which RAN node to send the message to, based on the destination address.

20.4 Reference point between serving GW and PDN GW (S5)

Reference point S5 provides user plane tunnelling and tunnel management between serving GW and PDN GW. It is used for serving GW relocation due to UE mobility and also if the serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity, see [b-ETSI TS 123 401].

The S5 reference point is based on GTP protocol. For a PMIP variant of S5, refer to [b-ETSI TS 123 402].

The control plane for this interface is depicted in Figure 50.

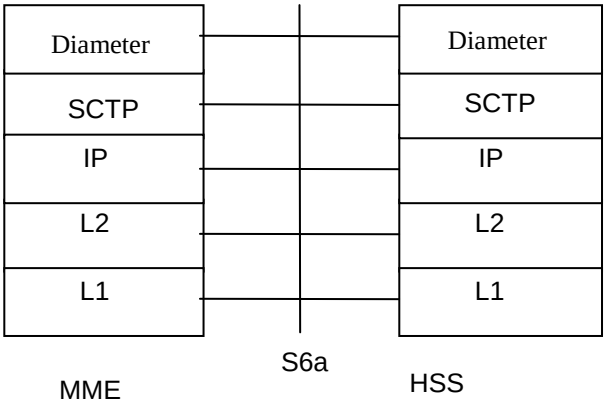


- GPRS tunneling protocol for the control plane (GTP-C): This protocol tunnels signalling messages between S-GW and P-GW (S5 or S8).
- User datagram protocol (UDP): This protocol transfers signalling messages between S-GW and P-GW. UDP is defined in [b-IETF RFC 768].

Figure 50 – Control plane for S5 and S8 interfaces [b-ETSI TS 123 401]

20.5 Reference point between mobility management entity (MME) and home subscriber server (HSS) (S6a)

Reference point S6a enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS, see [b-ETSI TS 123 401]. The control plane for this interface is depicted in Figure 51.



- Diameter: This protocol supports transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system between MME and HSS (S6a); the Diameter protocol is defined in [b-IETF RFC 3588].
- Stream control transmission protocol (SCTP): This protocol transfers signalling messages. SCTP is defined in [b-IETF RFC 4960].

Figure 51 – Control plane for the S6a interface [b-ETSI TS 123 401]

20.6 Reference point between SGSN and HLR/HSS (S6d)

Interface S6d is the interface between the SGSN and HLR/HSS, which is Diameter based, see [b-ETSI TS 123 060].

HLR/HSS contains GPRS and EPS subscription data and routeing information. HLR/HSS is accessible from the Gn/Gp SGSN via the Gr interface, from the S4-SGSN via the S6d interface and from GGSN via the Gc interface. For roaming UEs, HLR/HSS may be in a different PLMN than the current SGSN.

This interface is usually required for roaming subscribers from MME towards the home HSS.

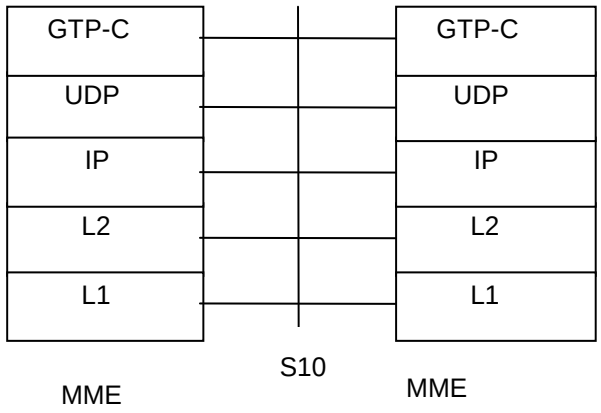
20.7 Reference point between serving GW in VPLMN and PDN GW in HPLMN – (S8)

The S8 reference point between the serving GW in VPLMN and PDN GW in HPLMN provides an inter-PLMN reference point for user and control plane. S8 is the inter PLMN variant of S5, see [b-ETSI TS 123 401]. Similar to reference point S5, the S8 reference point is based on the GTP protocol, refer to [b-ETSI TS 123 402] for a PMIP variant of S8.

For the reference point control plane for this interface, see the S5 control plane above.

20.8 Reference point between mobility management entities (MMEs) (S10)

The reference point S10 between MMEs is utilized for MME relocation and MME to MME information transfer. This reference point can be used for intra-operator or inter-operator, e.g., in case of inter-operator handovers, see [b-ETSI 123.401]. Figure 52 depicts the control plane for the S10 reference point.



- GPRS tunnelling protocol for the control plane (GTP-C): This protocol tunnels signalling messages between MMEs (S10).
- User datagram protocol (UDP): This protocol transfers signalling messages between MMEs. UDP is defined in [b-IETF RFC 768].

Figure 52 – Control plane for S10 interface [b-ETSI 123.401]

Regarding routing, for all configuration transfer messages used for the exchange of the E-UTRAN transparent container:

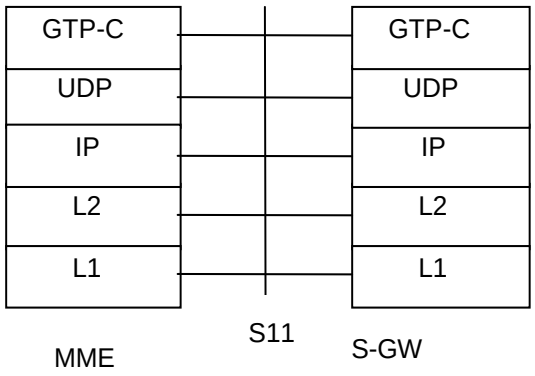
The source RAN node sends a message to its MME including the source and destination addresses. MME uses the destination address to route the message encapsulated in a GTPv2 message to the correct MME via the S10 interface, see [ETSI 129.274].

MME connected to the destination RAN node decides which RAN node to send the message to, based on the destination address.

20.9 Reference point between mobility management entity (MME) and serving GW (S11)

The reference point S11 between MME and the serving GW (S-GW) is designed as other reference points to manage the 3GPP evolved packet system (EPS) bearers, see [b-ETSI 123.401].

Figure 53 shows the control plane for the S11 reference point.



- GPRS tunneling protocol for the control plane (GTP-C): This protocol tunnels signalling messages between MME and S-GW (S11).
- User datagram protocol (UDP): This protocol transfers signalling messages. UDP is defined in [b-IETF RFC 768].

Figure 53 – Control plane for the S11 interface [b-ETSI 123.401]

20.10 Reference point between eNBs (X2)

The X2 reference point is used to hand over UE from a source eNodeB to a target eNodeB. The X2 reference point between the source and target eNodeB relies on the presence of S1-MME reference point between MME and the source eNodeB as well as between MME and the target eNodeB, see [b-ETSI 123.401].

20.11 3GPP LTE MM-related procedures

This clause lists the mobility management procedures, involving the mobility management entity (MME) in which the previous 3GPP LTE reference points are involved. The procedures include the exchange of MM identities, control information, and corresponding actions taken by different entities while attaching, performing area updates and handovers, etc.

There are four procedures described in detail in this technical paper, these are:

1 Tracking area update procedure with serving GW change, showing the behaviour of the tracking area updates under specific triggers,

2 X2-based handover with serving GW relocation, used when handing over UE from a source eNodeB to a target eNodeB using X2 when MME is unchanged and MME decides that the serving GW is to be relocated,

3 S1-based handover, showing when the X2-based handover cannot be used. The source eNodeB initiating a handover by sending a Handover Required message over the S1-MME reference point, and the

4 E-UTRAN to high rate packet data (HRPD) handover on the S101 reference point, showing the call flow for optimized E-UTRAN to HRPD handover procedures.

Including those exhibited detailed procedures, the following is a list of the MM LTE procedures. The extensive technical detail involved in them is the reason why they are not all shown herein. For more specific details on the MM procedures, see [b-ETSI 123.401] and [ETSI 123.402]:

1 Attach procedure,

2 Tracking area update procedure with serving GW change,

3 E-UTRAN tracking area update without S-GW change,

4 Routing area update with MME interaction and without S-GW change,

5 Routing area update with MME interaction and with S-GW change,

6 UE triggered service request procedure,

7 Network triggered service request procedure,

8 S1 release procedure,

9 Globally unique temporary identity (GUTI) reallocation procedure,

10 UE-initiated detach procedure – UE camping on E-UTRAN,

11 UE-initiated detach procedure – UE camping on GERAN/UTRAN, idle mode signalling reduction (ISR) Activated,

12 MME-initiated detach procedure,

13 SGSN-initiated detach procedure with ISR Activated,

14 Home subscriber server (HSS)-Initiated detach procedure,

15 Insert subscriber data procedure,

16 MME purge procedure,

17 Non-access-stratum (NAS) security mode command procedure,

18 Identity check procedure,

19 UE reachability notification request procedure,

20 UE activity procedure,

21 Update closed subscriber group (CSG) location procedure,

22 Insert CSG subscriber data procedure,

23 UE radio capability match request,

24 Dedicated bearer activation procedure,
25 Bearer modification procedure with bearer QoS update,
26 HSS-initiated subscribed QoS modification,
27 Bearer modification procedure without bearer QoS update,
28 PDN GW initiated bearer deactivation,
29 MME initiated dedicated bearer deactivation,
30 UE requested bearer resource modification,
31 X2-based handover without serving GW relocation,
32 X2-based handover with serving GW relocation,
33 S1-based handover,
34 S1-based handover reject,
35 E-UTRAN to UTRAN Iu mode inter RAT HO, preparation phase,
36 E-UTRAN to UTRAN Iu mode inter RAT HO, execution phase,
37 E-UTRAN to UTRAN Iu mode inter RAT HO reject,
38 UTRAN Iu mode to E-UTRAN inter RAT HO, preparation phase,
39 UTRAN Iu mode to E-UTRAN inter RAT HO, execution phase,
40 UTRAN Iu mode to E-UTRAN inter RAT HO reject,
41 E-UTRAN to GERAN A/Gb inter RAT HO, preparation phase,
42 E-UTRAN to GERAN A/Gb mode inter RAT HO, execution phase,
43 E-UTRAN to GERAN A/Gb inter RAT HO reject,
44 GERAN A/Gb mode to E-UTRAN inter RAT HO, preparation phase,
45 GERAN A/Gb mode to E-UTRAN inter RAT HO, execution phase,
46 GERAN A/Gb mode to E-UTRAN inter RAT HO reject,
47 Inter RAT handover cancel,
48 Location reporting procedure,
49 Notification of the E-UTRAN cell global identifier (ECGI) and/or user closed subscriber group (CSG) information changes,
50 UE requested PDN connectivity,
51 UE or MME requested PDN disconnection,
52 MME to 3G SGSN combined hard handover and SRNS relocation procedure,
53 3G Gn/Gp SGSN to MME combined hard handover and SRNS relocation procedure,
54 Routing area update procedure,
55 Gn/Gp SGSN to MME tracking area update procedure,
56 E-UTRAN to GERAN A/Gb inter RAT HO, preparation phase,
57 E-UTRAN to GERAN A/Gb mode inter RAT HO, execution phase,
58 GERAN A/Gb mode to E-UTRAN inter RAT HO, preparation phase,
59 GERAN A/Gb mode to E-UTRAN inter RAT HO, execution phase,
60 Dedicated bearer activation in combination with the default bearer activation at attach or UE requested PDN connectivity,
61 ISR activation,
62 Downlink data transfer with ISR active.

20.11.1 Tracking area update procedure with serving GW change

There exist certain triggers for tracking area updates, see [b-ETSI 123.401]. A stand-alone tracking area update (with or without S-GW change) occurs when a GPRS-attached or E-UTRAN-attached UE experiences any of the following conditions:

1 UE detects it has entered a new TA that is not in the list of tracking area identities (TAIs) that UE registered with the network (except for the case of UE configured to perform Attach with IMSI when entering TA in a new non-equivalent PLMN in RRC-IDLE mode);

2 The periodic TA update timer has expired;

3 UE was in UTRAN PMM_Connected state, e.g. URA_PCH, when it reselects to E-UTRAN;

4 UE was in GPRS READY state when it reselects to E-UTRAN;

5 TIN indicates "P-TMSI" (packet temporary mobile subscriber identity) when UE reselects to E-UTRAN, e.g., due to bearer configuration modifications performed on GERAN/UTRAN);

6 The radio resource control (RRC) connection was released with release cause "load re-balancing Tracking Area Update (TAU) required";

7 The RRC layer in UE informs the UE's non-access-stratum (NAS) layer that an RRC connection failure (either in E-UTRAN or in UTRAN) has occurred;

8 A change of the UE network capability and/or MS network capability and/or UE specific DRX parameters and/or [ETSI 124.008] MS radio access capability, e.g., due to GERAN radio capability change or CDMA2000 radio access technology capability change, information of UE;

9 For UE supporting CS fallback, or configured to support IMS voice, or both, a change of the UE's usage setting or voice domain preference for E-UTRAN;

10 For a SRVCC capable UE, a change of MS Classmark 2 and/or MS Classmark 3 and/or supported codecs;

11 UE manually selects a closed subscriber group (CSG) cell whose CSG ID and associated PLMN is absent from both the UE's allowed CSG list and the UE's operator CSG list;

12 UE receives a paging request from MME while the mobility management back-off timer is running and UE's TIN indicates "P-TMSI".

NOTE 1 – The complete list of tracking area update (TAU) triggers is specified in [ETSI 124.301].

The procedure is initiated by UE in either ECM-IDLE state or ECM-CONNECTED state. The decision to perform S-GW change during the tracking area update procedure is made by MME independently from the triggers above.

If selected IP traffic offload (SIPTO) is allowed for APN associated with a PDN connection, MME should re-evaluate whether the PGW location is still acceptable. If MME determines that PGW relocation is needed, MME may initiate PDN deactivation with reactivation requested according to clause 5.10.3 of [b-ETSI 123.401] at the end of the tracking area/routing area update procedure.

NOTE 2 – It depends on the operator's configuration in MME whether to use the deactivation with reactivation request or allow the continued usage of the already connected GW.

If local IP access (LIPA) is active for a PDN connection of UE, the source MME (or S4-SGSN) shall not include LIPA bearer(s) in the EPS bearer context during the tracking area update procedure and shall release the core network resources of this LIPA PDN connection by performing the MME requested PDN disconnection procedure according to steps 2 to 6 in clause 5.10.3 of [b-ETSI 123.401] before it responds with the Context Response message in the case of inter-MME/SGSN mobility or after it receives Tracking Area Update Request in the case of intra-MME mobility.

NOTE 3 – The source MME may not be able to release the LIPA PDN connection after the Context Response is sent as there is no S-GW relocation, S-GW will assign the S11 control tunnel of UE to the new MME after the new MME updates the context information.

During the tracking area update procedure, if MME supports SRVCC and if the UE SRVCC capability has changed, MME informs HSS with the UE SRVCC capability, e.g., for further IMS registration. The cell selection for UTRAN is described in [b-ETSI 125.304] and [ETSI 125.331].

The tracking area update procedure with serving GW change is shown in Figure 54.

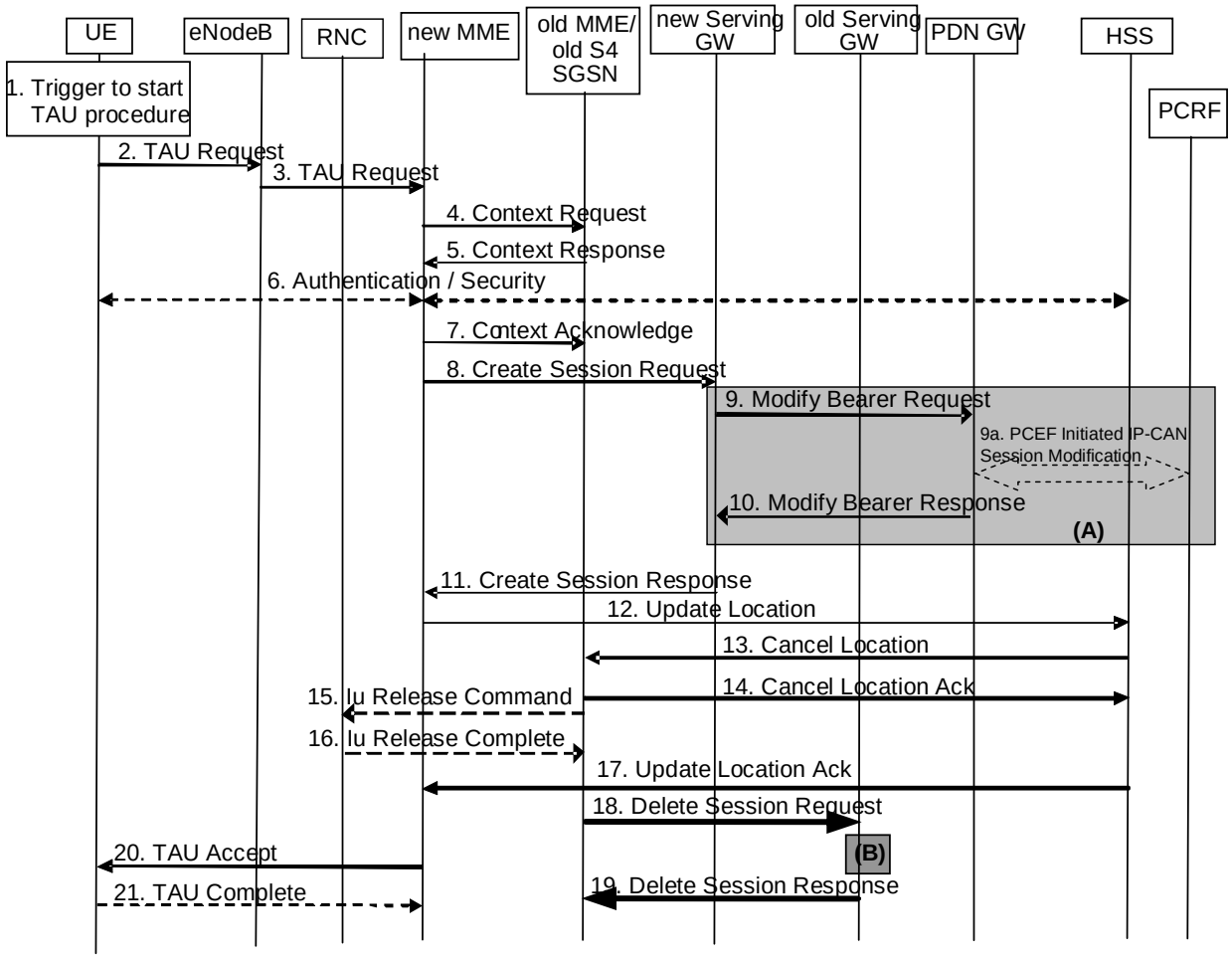


Figure 54 – Tracking area update procedure with serving GW change [b-ETSI 123.401]

NOTE 1 – For a PMIP-based S5/S8, procedure steps (A) and (B) are defined in [ETSI 123.402]. Steps 9 and 10 concern GTP-based S5/S8.

NOTE 2 – In case of tracking area update without MME change, the signalling in steps 4, 5, 7 and steps 12-17 are skipped.

In the signalling above:

1 One of the triggers described above for starting the tracking area update (TAU) procedure occurs.

2. UE initiates the TAU procedure by sending, to eNodeB, a TAU Request (UE core network capability, MS network capability, old globally unique temporary identity (GUTI), old GUTI type, last visited TAI, active flag, EPS bearer status, packet-temporary mobile subscriber

identity (P-TMSI) signature, additional GUTI, evolved key set identifier (eKSI), non-access-stratum (NAS) sequence number, NAS-MAC, KSI, voice domain preference and UE's usage setting) message together with radio resource control (RRC) parameters indicating the selected network and the old globally unique MME identifier (GUMMEI). An exception is that if TAU was triggered for load re-balancing purposes (see clause 4.3.7.3 of [b-ETSI 123.401]), the old GUMMEI is not included in the RRC parameters. UE shall set the old GUTI type to indicate whether the old GUTI is a native GUTI or is mapped from P-TMSI and routeing area identity (RAI).

If UE's TIN indicates "GUTI" or "RAT-related TMSI" and UE holds a valid GUTI, then the old GUTI indicates this valid GUTI. If UE's TIN indicates "P-TMSI" and UE holds a valid P-TMSI and a related routeing area identity (RAI), then these two elements are indicated as the old GUTI. Mapping P-TMSI and RAI to GUTI is specified in Annex H. When UE is in connected mode, e.g. in URA_PCH, when it reselects to E-UTRAN, UE shall set its TIN to "P-TMSI".

If UE holds a valid GUTI and the old GUTI indicates GUTI mapped from P-TMSI and RAI, then UE indicates GUTI as an additional GUTI. If the old GUTI indicates a GUTI mapped from P-TMSI and RAI, and UE has a valid P-TMSI signature, the P-TMSI signature shall be included.

The additional GUTI in the Tracking Area Update Request message allows the new MME to find any already existing UE context stored in the new MME when the old GUTI indicates a value mapped from a P-TMSI and RAI.

The RRC parameter "old GUMMEI" takes its value from the identifier that is signalled as the old GUTI according to the rules above. For a combined MME/SGSN, eNodeB is configured to route the MME-code(s) of this combined node to the same combined node. This eNodeB is also configured to route MME-code(s) of GUTIs that are generated by UE's mapping of P-TMSIs allocated by the combined node. Such an eNodeB configuration may also be used for separate nodes to avoid changing nodes in the pool caused by inter RAT mobility.

The last visited TAI shall be included in order to help MME produce a good list of TAIs for any subsequent TAU Accept message. The selected network indicates the network that is selected. Active flag is a request by UE to activate the radio and S1 bearers for all the active EPS bearers by the TAU procedure when UE is in ECM-IDLE state. The EPS bearer status indicates each EPS bearer that is active in UE. The TAU Request message shall be integrity protected by NAS-MAC as described in [ETSI 133.401]. eKSI, NAS sequence number and NAS-MAC are included if UE has valid EPS security parameters. The NAS sequence number indicates the sequential number of the NAS message. KSI is included if UE indicates GUTI mapped from P-TMSI in the information element "old GUTI".

UE sets the voice domain preference and UE's usage setting according to its configuration, as described in clause 4.3.5.9 of [b-ETSI 123.401].

3. eNodeB derives MME from the RRC parameters carrying the old GUMMEI and the indicated selected network. If that MME is not associated with that eNodeB or if GUMMEI is not available or UE indicates that the TAU procedure was triggered by load re-balancing, eNodeB selects MME as described in clause 4.3.8.3 of [b-ETSI 123.401] on "MME Selection Function".

   eNodeB forwards the TAU Request message together with the closed subscriber group (CSG) access mode, CSG ID, TAI + E-UTRAN cell global identifier (ECGI) of the cell from where it received the message and with the selected network to the new MME. CSG ID is provided by RAN if UE sends the TAU Request message via a CSG cell or a hybrid cell. CSG access mode is provided if UE sends the TAU Request message via a hybrid cell. If the

CSG access mode is not provided but CSG ID is provided, MME shall consider the cell as a CSG cell.

4. The new MME differentiates the type of the old node, i.e., MME or SGSN, as specified in clause 4.3.19 of [b-ETSI 123.401], uses the globally unique temporary identity (GUTI) received from UE to derive the old MME/S4 SGSN address, and sends a Context Request (old GUTI, complete TAU Request message, P-TMSI signature, MME address, UE validated) message to the old MME/old S4 SGSN to retrieve user information. UE Validated indicates that the new MME has validated the integrity protection of the TAU message, e.g., based on native EPS security context for UE. To validate the Context Request, the old MME uses the complete TAU Request message and the old S4 SGSN uses the P-TMSI signature and responds with an appropriate error if the integrity check fails in the old MME/S4 SGSN. This shall initiate the security functions in the new MME. If the security functions authenticate UE correctly, the new MME shall send a Context Request (IMSI, complete TAU Request message, MME address, UE Validated) message to the old MME/S4 SGSN with the UE Validated set. If the new MME indicates that it has authenticated UE or if the old MME/old S4 SGSN correctly validates UE, then the old MME/old S4 SGSN starts a timer.

   If UE with emergency bearers is not authenticated in the old MME/old S4 SGSN (in a network supporting unauthenticated UEs), the old MME/old S4 SGSN continues the procedure by sending a Context Response and starting also the timer when it cannot validate the Context Request.

5. If the Context Request is sent to an old MME, the old MME responds with a Context Response (IMSI, ME identity, international mobile station equipment identity and software version number (IMEISV), MM context, EPS bearer context(s), serving GW signalling address and tunnel endpoint identifier (TEID)(s), ISR supported, MS info change reporting action (if available), CSG information reporting action (if available), UE time zone, UE core network capability, UE specific DRX parameters) message.

   If the Context Request is sent to an old S4 SGSN, the old S4 SGSN responds with a Context Response (MM context, EPS bearer context(s), serving GW signalling address and TEID(s), ISR supported, MS info change reporting action (if available), CSG information reporting action (if available), UE time zone, UE core network capability, UE specific DRX parameters).

   The MM context contains security-related information as well as other parameters (including IMSI and ME identity (if available)) as described in clause 5.7.2 of [b-ETSI 123.401], Information Storage for MME. The unused authentication quintets in the MM context are also maintained in SGSN. [ETSI 133.401] provides further details on the transfer of security-related information.

   If the MM context received with the Context Response message did not include international mobile station equipment identity and software version number (IMEISV) and MME does not already store IMEISV of UE, MME shall retrieve the ME identity (IMEISV) from UE.

   The PDN GW address and TEID(s) (for GTP-based S5/S8) or GRE keys (PMIP-based S5/S8 at the PDN GW(s) for uplink traffic) and TI(s), is part of the EPS bearer context. If UE is not known in the old MME/old S4 SGSN or if the integrity check for the TAU Request message fails, the old MME/old S4 SGSN responds with an appropriate error cause. ISR supported is indicated if the old MME/old S4 SGSN and associated serving GW are capable to activate ISR for UE.

   If UE receives emergency services from the old MME/old S4 SGSN and UE is UICCless, IMSI cannot be included in the Context Response. For emergency attached UEs, if IMSI cannot be authenticated, then IMSI shall be marked as unauthenticated. Furthermore, in this case, security parameters are included only if available.

6. If the integrity check of the TAU Request message (sent in step 2) failed, then authentication is mandatory. The authentication functions are defined in clause 5.3.10 of [b-ETSI 123.401] on "Security Function". Ciphering procedures are described in clause 5.3.10 of [b-ETSI 123.401] on "Security Function". If GUTI allocation is going to be done and the network supports ciphering, the NAS messages shall be ciphered.

   If this TAU request is received for UE which is already in ECM_CONNECTED state and the PLMN-ID of the TAI sent by the eNodeB in step 3 is different from that of the GUTI, included in the TAU Request message, MME shall delay authenticating UE until after step 21 (TAU Complete message).

NOTE 4 – MME delays the authentication such that the UE first updates its registered PLMN-ID to the new PLMN-ID selected by the RAN during handover. The new PLMN-ID is provided by MME to UE as part of GUTI in the TAU Accept message in step 20. Doing this ensures that the same PLMN-ID is used in the derivation of the main key for E-UTRAN key hierarchy based on CK, IK and serving network identity (KASME key) by both the network and UE.

   If the new MME is configured to allow emergency services for unauthenticated UE, the new MME behaves as follows:

- where UE has only emergency bearer services, MME either skips the authentication and security procedure or accepts that the authentication may fail and continues the tracking area update procedure; or
- where UE has both emergency and non-emergency bearer services and authentication fails, MME continues the tracking area update procedure and deactivates all the non-emergency PDN connections as specified in clause 5.10.3 of [b-ETSI 123.401].

7. MME (if MME has changed then it is the new MME) determines to relocate the serving GW. The serving GW is relocated when the old serving GW cannot continue to serve UE. MME (if MME has changed then it is the new MME) may also decide to relocate the serving GW if a new serving GW is expected to serve UE longer and/or with a more optimal UE to PDN GW path, or if a new serving GW can be co-located with PDN GW. Selection of a new serving GW is performed according to clause 4.3.8.2 of [b-ETSI 123.401] on "Serving GW selection function".

   If MME has changed, the new MME sends a Context Acknowledge (serving GW change indication) message to the old MME/old S4 SGSN. Serving GW change indication indicates that a new serving GW has been selected. The old MME/old S4 SGSN marks in its UE context that the information in GWs is invalid, and if the old node is MME, the old MME marks in its UE context that the information in HSS is invalid. This ensures that the old MME/old S4 SGSN updates GWs, and the old MME updates HSS, if UE initiates a TAU or RAU procedure back to the old MME/old S4 SGSN before completing the ongoing TAU procedure. If the security functions do not authenticate UE correctly, then TAU shall be rejected, and the new MME shall send a reject indication to the old MME/old S4 SGSN. The old MME/old S4 SGSN shall continue as if the identification and Context Request were never received.

   ISR is not indicated in the Context Acknowledge as ISR is not activated due to the S-GW change.

8. If MME has changed, the new MME verifies the EPS bearer status received from UE with the bearer contexts received from the old MME/old S4 SGSN. If MME has not changed, MME verifies the EPS bearer status from UE with the bearer contexts available in the MM context. MME releases any network resources related to EPS bearers that are not active in UE. If there is no bearer context at all, MME rejects the TAU Request.

   If MME selects a new serving GW, it sends a Create Session Request (IMSI, bearer contexts, MME address and TEID, type, the protocol type over S5/S8, RAT type, serving network, UE time zone) message per PDN connection to the selected new serving GW. The PDN GW

address and TFT (for PMIP-based S5/S8) are indicated in the bearer contexts. Type indicates to the serving GW to send the Modify Bearer Request to PDN GW. The protocol type over S5/S8 is provided to serving GW which protocol should be used over S5/S8 interface. RAT type indicates a change in radio access. If PDN GW requested UE's location and/or user CSG information, MME also includes the user location information IE and/or user CSG information IE in this message.

NOTE 5 – The user CSG information IE is only sent in step 8 if the "Active flag" is set in the TAU Request message.

9. The serving GW informs PDN GW(s) about the change of, for example, the RAT type that can be used momentarily for charging, by sending the message Modify Bearer Request (serving GW address and TEID, RAT type, serving network) per PDN connection to the PDN GW(s) concerned. User location information IE and/or UE time zone IE and/or user CSG information IE are also included if they are present in step 8.

   9a. If dynamic policy and charging control (PCC) is deployed, and RAT type information needs to be conveyed from PDN GW to PCRF, then PDN GW shall send RAT type information to PCRF by means of an IP-CAN session modification procedure as defined in [ETSI 123 203].

NOTE 6 – PDN GW does not need to wait for the PCRF response, but continues in the next step. If the PCRF response leads to EPS bearer modification, PDN GW should initiate a bearer update procedure.

10. PDN GW updates its bearer contexts and returns a Modify Bearer Response (MSISDN, charging Id) message. MSISDN is included if PDN GW has it stored in its UE context.

11. The serving GW updates its bearer context. This allows the serving GW to route bearer PDUs to PDN GW when received from eNodeB.

    The serving GW returns a Create Session Response (serving GW address and TEID for user plane and control plane and PDN GW TEIDs (for GTP-based S5/S8) or GRE keys (for PMIP-based S5/S8) for uplink traffic and control plane) message to the new MME.

12. The new MME verifies whether it holds subscription data for the UE identified by GUTI, the additional GUTI or by IMSI received with the context data from the old CN node.

    If there are no subscription data in the new MME for this UE, or for some network sharing scenario, e.g., GWCN, if PLMN-ID of TAI supplied by eNodeB is different from that of GUTI in the UE's context, then the new MME sends an Update Location Request (MME identity, IMSI, ULR-flags, MME capabilities, homogeneous support of IMS voice over PS sessions, UE SRVCC capability, equivalent PLMN list, ME identity (IMEISV)) message to HSS. ULR-flags indicate that update location is sent from MME and the MME registration shall be updated in HSS. HSS does not cancel any SGSN registration. The MME capabilities indicate MME's support for regional access restrictions functionality. The inclusion of the equivalent PLMN list indicates that MME supports the inter-PLMN handover to a CSG cell in an equivalent PLMN using the subscription information of the target PLMN. The "Homogenous Support of IMS Voice over PS Sessions" indication, see clause 4.3.5.8A of [b-ETSI 123.401], shall not be included unless MME has completed its evaluation of the support of "IMS Voice over PS Session" as specified in clause 4.3.5.8 of [b-ETSI 123.401]. The ME identity is included if step 5 caused MME to retrieve IMEISV from UE.

NOTE 7 – In this step, MME may not have all the information needed to determine the setting of the IMS voice over PS session supported indication for this UE, see clause 4.3.5.8 of [b-ETSI 123.401]. Hence MME can send the "Homogenous Support of IMS Voice over PS Sessions" later on in this procedure.

If UE initiates the TAU procedure in a VPLMN supporting autonomous CSG roaming, and HPLMN has enabled autonomous CSG roaming in VPLMN (via the service level agreement) and MME needs to retrieve the CSG subscription information of UE from CSS, MME

initiates the update CSG location procedure with CSS as described in clause 5.3.12 of [b-ETSI 123.401].

If MME determines that only the UE SRVCC capability has changed, MME sends a Notify Request to HSS to inform about the changed UE SRVCC capability.

If all the EPS bearers of UE have emergency ARP value, the new MME may skip the update location procedure or proceed even if the update location fails.

13. HSS sends a Cancel Location message (IMSI, cancellation type) to the old MME with cancellation type set to update procedure.

14. If the timer started in step 4 is not running, the old MME removes the MM context. Otherwise, the contexts are removed when the timer expires. It also ensures that the MM context is kept in the old MME for the case whenUE initiates another TAU procedure before completing the ongoing TAU procedure to the new MME. The old MME acknowledges with a Cancel Location Ack message (IMSI).

15. When the old S4 SGSN receives the Context Acknowledge message and if UE is in Iu Connected, the old S4 SGSN sends an Iu Release Command message to RNC after the timer started in step 4 has expired.

16. RNC responds with an Iu Release Complete message.

17. HSS acknowledges the Update Location Request message by sending an Update Location Ack (IMSI, subscription data) message to the new MME. If the Update Location is rejected by HSS, the new MME rejects the TAU Request from UE with an appropriate cause. The subscription data may contain the CSG subscription data for the registered PLMN and for the equivalent PLMN list requested by MME in step 12.

    If UE initiates the TAU procedure at a CSG cell, the new MME shall check whether the CSG ID and associated PLMN is contained in the CSG subscription and is not expired. If CSG ID and associated PLMN are not present or expired, MME shall send a Tracking Area Update reject message to UE with an appropriate cause value. UE shall remove CSG ID and associated PLMN from its Allowed CSG list if present. If UE has ongoing emergency bearer services, no CSG access control shall be performed.

    If all checks are successful, then the new MME constructs a context for UE.

18. If MME has changed, when the timer started in step 4 expires, the old MME/old S4 SGSN releases any local MME or SGSN bearer resources and additionally the old MME/old S4 SGSN deletes the EPS bearer resources by sending the Delete Session Request (cause, operation indication) messages to the old serving GW if it received the serving GW change indication in the Context Acknowledge message in step 7. When the operation indication flag is not set, this indicates to the old serving GW that the old serving GW shall not initiate a delete procedure towards PDN GW. If ISR is activated, the cause indicates to the old S-GW that the old S-GW shall delete the bearer resources on the other old CN node by sending Delete Bearer Request message(s) to that CN node.

    If MME has not changed, step 11 triggers the release of the EPS bearer resources at the old serving GW.

19. The serving GW acknowledges with Delete Session Response (cause) message. The serving GW discards any packets buffered for UE.

20. If due to regional subscription restrictions or access restrictions, e.g., CSG restrictions, UE is not allowed to access TA:

- MME rejects the Tracking Area Update Request with an appropriate cause to UE.
- For UEs with emergency EPS bearers, i.e., at least one EPS bearer has an ARP value reserved for emergency services, the new MME accepts the Tracking Area Update Request and deactivates all non-emergency PDN connections as specified in clause 5.10.3 of [b-ETSI

123.401]. If the Tracking Area Update procedure is initiated in ECM-IDLE state, all non-emergency EPS bearers are deactivated by the Tracking Area Update procedure without bearer deactivation signalling between UE and MME.

MME sends a TAU Accept (GUTI, TAI list, EPS bearer status, NAS sequence number, NAS-MAC, IMS voice over PS session supported, emergency service support indicator, LCS support indication) message to UE. If the active flag is set, MME may provide eNodeB with handover restriction list. GUTI is included if MME allocates a new GUTI. If the "active flag" is set in the TAU Request message, the user plane set-up procedure can be activated in conjunction with the TAU Accept message. The procedure is described in detail in [ETSI 136.300]. The message sequence should be the same as for the UE triggered Service Request procedure specified in clause 5.3.4.1 of [b-ETSI 123.401] from the step when MME establishes the bearer(s). MME indicates the EPS bearer status IE to UE. UE removes any internal resources related to bearers that are not marked active in the received EPS bearer status. The handover restriction list is described in clause 4.3.5.7 of [b-ETSI 123.401] "Mobility Restrictions". MME sets the IMS voice over PS session supported as described in clause 4.3.5.8 of [b-ETSI 123.401].

If MME did not receive the voice support match indicator in the MM context, then MME may send a UE Radio Capability Match Request to the eNB as described in clause 5.3.14 of [b-ETSI 123.401]. If MME has not received voice support match indicator from the eNB then, based on implementation, MME may set IMS voice over PS session supported indication and update it at a later stage. After step 12, and in parallel to any of the preceding steps, MME shall send a Notify Request (homogeneous support of IMS voice over PS sessions) message to HSS:

- If MME has evaluated the support of IMS voice over PS sessions, see clause 4.3.5.8 of [b-ETSI 123.401], and
- If MME determines that it needs to update the homogeneous support of IMS voice over PS sessions, see clause 4.3.5.8A of [b-ETSI 123.401].

The emergency service support indicator informs UE that the emergency bearer services are supported. LCS support indication indicates whether the network supports the EPC-MO-LR and/or CS-MO-LR as described in [ETSI 123.271]].

When receiving the TAU Accept message and there is no ISR Activated indication, UE shall set its TIN to "GUTI".

For a S-GW change, ISR Activated is never indicated by MME as it needs RAU with the same S-GW first to activate ISR. For MME change, ISR is not activated by the new MME to avoid context transfer procedures with two old CN nodes.

If the TAU procedure is initiated by manual CSG selection and occurs via a CSG cell, UE upon receiving the TAU Accept message shall add the CSG ID and associated PLMN to its Allowed CSG list if it is not already present. Manual CSG selection is not supported if UE has emergency bearers established.

If the user plane set-up is performed in conjunction with the TAU Accept message and the TAU is performed via a hybrid cell, then MME shall send an indication whether UE is a CSG member to RAN along with the S1-MME control message. Based on this information, RAN may perform a differentiated treatment for CSG and non-CSG members.

NOTE 8 – If UE receives a TAU Accept message via a hybrid cell, UE does not add the corresponding CSG ID and associated PLMN to its Allowed CSG list. Adding a CSG ID and associated PLMN to the UE's local Allowed CSG list for a hybrid cell is performed only by OTA or OMA DM procedures.

21. If GUTI was included in the TAU Accept, UE acknowledges the received message by returning a TAU Complete message to MME.

When the "Active flag" is not set in the TAU Request message and the tracking area update was not initiated in ECM-CONNECTED state, the new MME releases the signalling connection with UE, according to clause 5.3.5 of [b-ETSI 123.401].

NOTE 9 – The new MME may initiate E-RAB establishment, see [b-ETSI 136.413], after the execution of the security functions, or wait until the completion of the TA update procedure. For UE, E-RAB establishment may occur any time after the TA update request is sent.

In the case of a rejected tracking area update operation, due to regional subscription, roaming restrictions or access restrictions, see [ETSI 123.221] and [ETSI 123 008], the new MME should not construct an MM context for UE. In the case of receiving the subscriber data from HSS, the new MME may construct an MM context and store the subscriber data for UE to optimize signalling between MME and HSS. A reject shall be returned to UE with an appropriate cause and the S1 connection shall be released. Upon return to idle, UE shall act according to [ETSI 123 122].

The new MME shall determine the maximum APN restriction based on the received APN restriction of each bearer context in the Context Response message and then store the new maximum APN restriction value.

The bearer contexts shall be prioritized by the new MME. If the new MME is unable to support the same number of active bearer contexts as received from the old MME/SGSN, the prioritization is used to decide which bearer contexts to maintain active and which ones to delete. In any case, the new MME shall first update all contexts in one or more P-GWs and then deactivate the bearer context(s) that it cannot maintain as described in clause "MME Initiated Dedicated Bearer Deactivation Procedure". This shall not cause MME to reject the tracking area update.

The new MME shall not deactivate emergency service-related EPS bearers, i.e., EPS bearers with ARP value reserved for emergency services.

NOTE 10 – If MS (UE) was in PMM-CONNECTED state, the bearer contexts are sent already in the Forward Relocation Request message as described in the clause "Serving RNS relocation procedures" of [ETSI 123 060].

If the tracking area update procedure fails a maximum allowable number of times, or if MME returns a Tracking Area Update Reject (cause) message, UE shall enter the EMM DEREGISTERED state.

20.11.2 X2-based handover with serving GW relocation

This procedure is used to hand over UE from a source eNodeB to a target eNodeB using X2 when MME is unchanged and MME decides that the serving GW is to be relocated. The presence of IP connectivity between the source serving GW and the source eNodeB, between the source serving GW and the target eNodeB, and between the target serving GW and the target eNodeB is assumed.

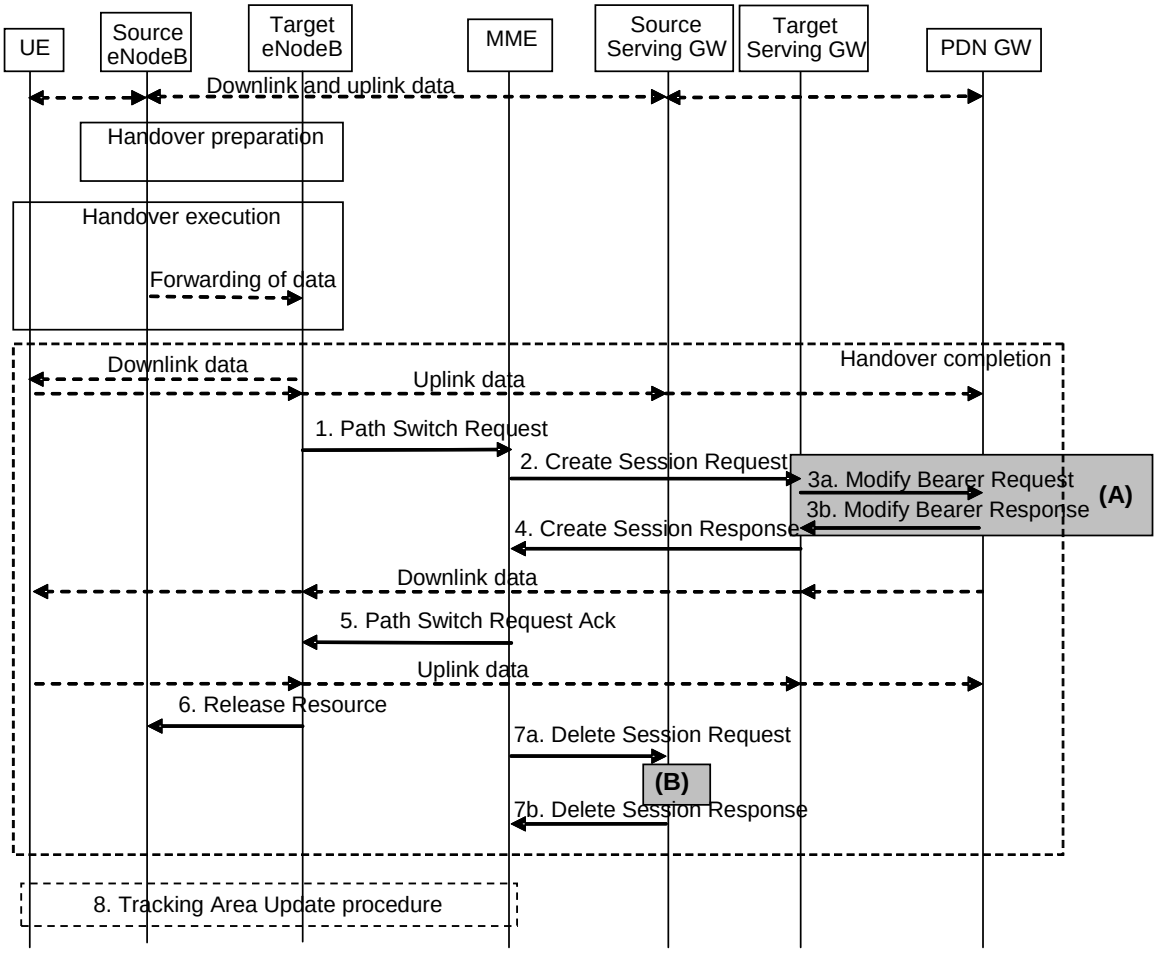


Figure 55 – X2-based handover with serving GW relocation [b-ETSI 123.401]

NOTE – For a PMIP-based S5/S8, procedure steps (A) and (B) are defined in [ETSI 123.402].

1. The target eNodeB sends a Path Switch Request message to MME to inform that UE has changed cell, including the E-UTRAN cell global identifier (ECGI) of the target cell and the list of EPS bearers to be switched. If the target cell is a closed subscriber group (CSG) cell, the target eNodeB includes CSG ID of the target cell in the Path Switch Request message. If the target cell is in hybrid mode, it includes the CSG ID of the target cell and CSG access mode set to "hybrid" in the Path Switch Request message. MME determines the CSG membership based on CSG ID and CSG access mode received from the target eNodeB. MME updates the user CSG information based on CSG ID and CSG access mode received from the target eNodeB and CSG membership if one of the parameters has changed.

NOTE 1 – X2 handover between HeNBs is possible when the handover is between closed/hybrid access HeNBs having the same CSG ID or when the target HeNB is an open access HeNB.

MME determines that the serving GW is relocated and selects a new serving GW, see clause 4.3.8.2 of [b-ETSI 123.401] on "Serving GW Selection Function".

NOTE 2 – MME knows the S-GW service area with a tracking area (TA) granularity.

2. MME sends a Create Session Request (bearer context(s) with PDN GW addresses and TEIDs (for GTP-based S5/S8) or GRE keys (for PMIP-based S5/S8) at PDN GW(s) for uplink traffic, eNodeB address(es) and tunnel endpoint identifiers (TEIDs) for downlink user plane for the accepted EPS bearers, the protocol type over S5/S8, serving network, UE time zone) message per PDN connection to the target serving GW for each PDN connection where the default bearer has been accepted by the target eNodeB. The target serving GW allocates the S-GW addresses and TEIDs for the uplink traffic on S1-U reference point (one TEID per

bearer). The protocol type over S5/S8 is provided to the serving GW which protocol should be used over S5/S8 interface. If PDN GW requests UE's location info, MME also includes the user location information IE in this message. If PDN GW requests UE's user CSG information (determined from the UE context), MME includes the user CSG information IE in this message if the user CSG information has changed.

MME uses the list of EPS bearers to be switched, received in step 1, to determine whether any dedicated EPS bearers in the UE context have not been accepted by the target eNodeB. MME releases the non-accepted dedicated bearers by triggering the bearer release procedure as specified in clause 5.4.4.2 of [b-ETSI 123.401] via the target serving GW. If the serving GW receives a DL packet for a non-accepted bearer, the serving GW drops the DL packet and does not send a downlink data notification to MME.

If the default bearer of a PDN connection has not been accepted by the target eNodeB and there are multiple PDN connections active, MME shall consider all bearers of that PDN connection as failed and release a PDN connection by triggering the MME requested PDN disconnection procedure specified in clause 5.10.3 of [b-ETSI 123.401] via the source serving GW.

If none of the default EPS bearers have been accepted by the target eNodeB, or if there is a local IP access (LIPA) PDN connection that has not been released, MME acts as specified in step 5.

3. The target serving GW assigns addresses and TEIDs (one per bearer) for downlink traffic from PDN GW. The serving GW allocates DL TEIDs on S5/S8, see [b-ETSI 123.401], even for non-accepted bearers. It sends a Modify Bearer Request (serving GW addresses for user plane and TEID(s), serving network) message per PDN connection to PDN GW(s). S-GW also includes user location information IE and/or UE time zone IE and/or user CSG information IE if it is present in step 2. PDN GW updates its context field and returns a Modify Bearer Response (charging Id, MSISDN, etc.) message to serving GW. MSISDN is included if PDN GW has it stored in its UE context. PDN GW starts sending downlink packets to the target serving GW using the newly received address and TEIDs. These downlink packets will use the new downlink path via the target serving GW to the target eNodeB. The serving GW shall allocate TEIDs for the failed bearers and inform MME.
4. The target serving GW sends a Create Session Response (serving GW addresses and uplink TEID(s) for user plane) message back to the target MME. MME starts a timer, to be used in step 7.
5. MME confirms the Path Switch Request message with the Path Switch Request Ack (serving GW addresses and uplink TEID(s) for user plane) message. If the UE- APN-aggregate maximum bit rate (AMBR) is changed, e.g., all the EPS bearers which are associated to the same APN are rejected in the target eNodeB, and MME shall provide the updated value of UE-AMBR to the target eNodeB in the Path Switch Request Ack message. The target eNodeB starts using the new serving GW address (es) and TEID(s) for forwarding subsequent uplink packets.

   If some EPS bearers have not been switched successfully in the core network, MME shall indicate in the Path Switch Request Ack message which bearers failed to be established, see more details in [ETSI 136.413], and for dedicated bearers to initiate the bearer release procedure, as specified in clause 5.4.4.2 of [b-ETSI 123.401], to release the core network resources of the failed dedicated EPS bearers. The target eNodeB shall delete the corresponding bearer contexts when it is informed that bearers have not been established in the core network.

   If none of the default EPS bearers have been switched successfully in the core network or if they have not been accepted by the target eNodeB or the LIPA PDN connection has not been released, MME shall send a Path Switch Request Failure message, see more details in [ETSI

136.413], to the target eNodeB. MME performs an explicit detach of UE as described in the MME initiated detach procedure in clause 5.3.8.3 of [b-ETSI 123.401].

6. By sending a Release Resource message, the target eNodeB informs the success of the handover to the source eNodeB and triggers the release of resources. This step is specified in [ETSI 136.300].

7. When the timer has expired after step 4, the source MME releases the bearer(s) in the source serving GW by sending a Delete Session Request message (cause, operation indication). The operation indication flag is not set, which indicates to the source serving GW that the source serving GW shall not initiate a delete procedure towards PDN GW. The source serving GW acknowledges with a Delete Session Response message. If idle mode signalling reduction (ISR) has been activated before this procedure, the cause indicates to the source S-GW that the source S-GW shall delete the bearer resources on the other old CN node by sending Delete Bearer Request message(s) to that CN node.

8. UE initiates a tracking area update procedure when one of the conditions listed in clause "Triggers for tracking area update" applies.

NOTE 3 – It is only a subset of the TA update procedure that is performed by MME, since UE is in ECM-CONNECTED state. UE is informed about the ISR status in the tracking area update procedure.

20.11.3 S1-based handover

The S1-based handover procedure is used when the X2-based handover cannot be used. The source eNodeB initiates a handover by sending a Handover Required message over the S1-MME reference point. This procedure may relocate MME and/or the serving GW. The source MME selects the target MME. MME should not be relocated during the inter-eNodeB handover unless UE leaves the MME pool area where UE is served. MME (target MME for MME relocation) determines if the serving GW needs to be relocated. If the serving GW needs to be relocated, MME selects the target serving GW, as specified in clause 4.3.8.2 of [b-ETSI 123.401] on “Serving GW selection function”.

The source eNodeB decides which of the EPS bearers are subject for forwarding of downlink and, optionally, also uplink data packets from the source eNodeB to the target eNodeB. EPC does not change the decisions taken by the RAN node. Packet forwarding can take place either directly from the source eNodeB to the target eNodeB, or indirectly from the source eNodeB to the target eNodeB via the source and target serving GWs (or if the serving GW is not relocated, only the single serving GW).

The availability of a direct forwarding path is determined in the source eNodeB and indicated to the source MME. If X2 connectivity is available between the source and target eNodeBs, a direct forwarding path is available.

If a direct forwarding path is not available, indirect forwarding may be used. The source MME uses the indication from the source eNodeB to determine whether to apply indirect forwarding. The source MME indicates to the target MME whether indirect forwarding should apply. Based on this indication, the target MME determines whether it applies indirect forwarding.

If MME receives a rejection to an S1 interface procedure, e.g., a dedicated bearer establishment/modification/release, location reporting control, NAS message transfer, etc., from the eNodeB with an indication that an S1 handover is in progress, see [ETSI 136.300], MME shall reattempt the same S1 interface procedure when either the handover is complete or is deemed to have failed if MME is still the serving MME, except in the case of serving GW relocation.

In order to minimize the number of procedures rejected by eNodeB, MME should pause non-handover related S1 interface procedures, e.g. downlink NAS message transfer, E-RAB Setup/Modify/Release, etc., while a handover is ongoing, i.e., from the time that a Handover Required message has been received until either the handover procedure has succeeded (Handover Notify) or failed (Handover Failure), and continue them once the handover procedure has completed if MME is still the serving MME, except in the case of serving GW relocation.

If during the handover procedure MME detects that the serving GW or/and MME needs be relocated, MME shall reject any PDN GW initiated EPS bearer(s) request received since the handover procedure started and shall include an indication that the request has been temporarily rejected due to handover procedure in progress. The rejection is forwarded by the serving GW to PDN GW, with the same indication.

Upon reception of a rejection for an EPS bearer(s) PDN GW initiated procedure with an indication that the request has been temporarily rejected due to handover procedure in progress, PDN GW starts a locally configured guard timer. PDN GW shall reattempt, up to a pre-configured number of times, when either it detects that the handover is completed or has failed using message reception or at expiry of the guard timer.

If emergency bearer services are ongoing for UE, handover to the target eNodeB is performed independently of the handover restriction list. MME checks, as part of the tracking area update in the execution phase, if the handover is to a restricted area and, if so, MME releases the non-emergency bearers as specified in clause 5.10.3 of [b-ETSI 123.401].

If the emergency bearer services are ongoing for UE, handover to the target CSG cell is performed independently of the UE's CSG subscription. If the handover is to a CSG cell that UE is not subscribed to, the target eNodeB only accepts the emergency bearers and the target MME releases the non-emergency PDN connections that were not accepted by the target eNodeB as specified in clause 5.10.3 of [b-ETSI 123.401].

If MME receives a rejection to a UE Context Modification Request message with a CS fallback indication from the eNodeB with an indication that an S1 handover is in progress, MME shall resend a UE Context Modification Request message with CS fallback indicator to the target eNodeB when, either the handover is complete, or to the source eNodeB, when the handover is deemed to have failed if MME is still the serving MME.

For inter-PLMN handover to a CSG cell, if the source MME has the CSG-ID list of the target PLMN, the source MME shall use it to validate the CSG membership of UE in the target CSG cell. Otherwise, based on the operator's configuration, the source MME may allow the handover by validating the CSG membership of UE in the target CSG cell using the CSG-ID list of the registered PLMN-ID. If neither the CSG-ID list of the target PLMN nor the operator's configuration permits the handover, the source MME shall reject the handover due to lack of CSG membership information of the target PLMN-ID.

NOTE – Inter-PLMN handover to a CSG cell in a PLMN which is not an equivalent PLMN for UE is not supported.

This procedure describes the S1-based handover in the normal case; clause 5.5.1.2.3 of [b-ETSI 123.401] describes it if the procedure is rejected by the target eNodeB or the target MME, and clause 5.5.1.2.4 of [b-ETSI 123.401] describes it when the procedure is cancelled by the source eNodeB.

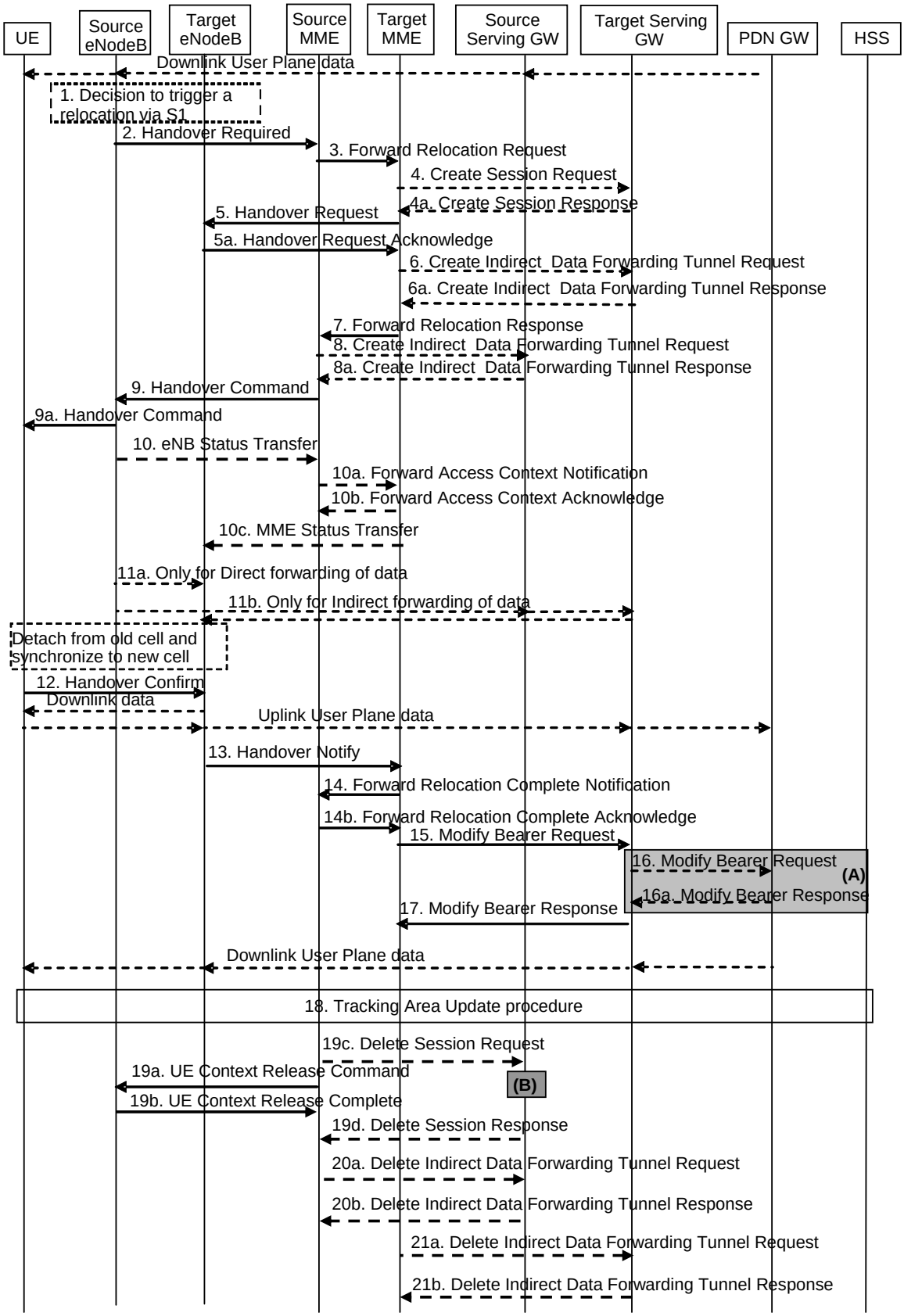


Figure 56 – S1-based handover [b-ETSI 123.401]

NOTE – For a PMIP-based S5/S8, procedure steps (A) and (B) are defined in [b-ETSI 123.401]. Steps 16 and 16a concern GTP-based S5/S8.In the above flow diagram:

1 The source eNodeB decides to initiate an S1-based handover to the target eNodeB. This can be triggered, for example, by an X2 connectivity to the target eNodeB, or by an error indication from the target eNodeB after an unsuccessful X2-based handover, or by dynamic information learnt by the source eNodeB.

2 The source eNodeB sends Handover Required (direct forwarding path availability, source to target transparent container, target eNodeB identity, CSG ID, CSG access mode, target TAI, S1AP cause) to the source MME. The source eNodeB indicates which bearers are subject to data forwarding. Direct forwarding path availability indicates whether direct forwarding is available from the source eNodeB to the target eNodeB. This indication from the source eNodeB can be based on, for example, the presence of X2. The target tracking area identity (TAI) is sent to MME to facilitate the selection of a suitable target MME. When the target cell is a CSG cell or a hybrid cell, the source eNodeB shall include CSG ID of the target cell. If the target cell is a hybrid cell, the CSG access mode shall be indicated.

3 The source MME selects the target MME, as described in clause 4.3.8.3 of [b-ETSI 123.401] on "MME Selection Function", and if it has determined to relocate MME, it sends a Forward Relocation Request (MME UE context, source to target transparent container, RAN cause, target eNodeB identity, CSG ID, CSG membership indication, target TAI, MS info change reporting action (if available), CSG information reporting action (if available), UE time zone, direct forwarding flag, serving network) message to the target MME. The target TAI is sent to the target MME to help it determine whether S-GW relocation is needed (and, if needed, help in S-GW selection). The old serving network is sent to target MME to support the target MME to resolve if serving network has changed. In network sharing scenarios, the serving network denotes the serving core network. The source MME shall perform access control by checking the UE's CSG subscription when CSG ID is provided by the source eNodeB. If there is no subscription data for this CSG ID or the CSG subscription is expired, and the target cell is a CSG cell, the source MME shall reject the handover with an appropriate cause unless UE has emergency bearer services. The MME UE context includes the international mobile subscriber identifier (IMSI), ME identity, UE security context, UE network capability, AMBR, selected CN operator ID, APN restriction, serving GW address and tunnel endpoint identifier (TEID) for control signalling, and EPS bearer context(s). An EPS bearer context includes the PDN GW addresses and TEIDs (for GTP-based S5/S8) or GRE keys (for PMIP-based S5/S8) at PDN GW(s) for uplink traffic, APN, serving GW addresses and TEIDs for uplink traffic, and TI. RAN cause indicates the S1AP cause as received from the source eNodeB. The source MME includes the CSG ID in the Forward Relocation Request when the target cell is a CSG or hybrid cell. When the target cell is a hybrid cell, or if there are one or several emergency bearers and the target cell is a CSG cell, the CSG membership indication indicating whether UE is a CSG member shall be included in the Forward Relocation Request message. The direct forwarding flag indicates if direct forwarding is applied, or if indirect forwarding is going to be set up by the source side. The target MME shall determine the maximum APN restriction based on the APN restriction of each bearer context in the Forward Relocation Request, and shall subsequently store the new maximum APN restriction value. If UE receives only emergency services and UE is UICCless, IMSI cannot be included in the MME UE context in the Forward Relocation Request message. For emergency attached UEs, if IMSI cannot be authenticated, then IMSI shall be marked as unauthenticated. In addition, in this case, security parameters are included only if available.

4 If MME has been relocated, the target MME verifies whether the source serving GW can continue to serve UE. If not, it selects a new serving GW, as described in clause 4.3.8.2 of [b-ETSI 123.401] on "Serving GW Selection Function". If MME has not been relocated, the source MME decides on this serving GW re-selection. If the source serving GW continues to serve UE, no message is sent in this step. In this case, the target serving GW is identical to the source serving GW. If a new serving GW is selected, the target MME sends a Create

Session Request (bearer context(s) with PDN GW addresses and TEIDs (for GTP-based S5/S8) or GRE keys (for PMIP-based S5/S8) at PDN GW(s) for uplink traffic, serving network, and UE time zone) message per PDN connection to the target serving GW. The target serving GW allocates the S-GW addresses and TEIDs for the uplink traffic on S1-U reference point (one TEID per bearer). The target serving GW sends a Create Session Response (serving GW addresses and uplink TEID(s) for user plane) message back to the target MME.

5 The target MME sends a Handover Request (EPS bearers to setup, AMBR, S1AP cause, source to target transparent container, CSG ID, CSG membership indication, handover restriction list) message to the target eNodeB. This message creates the UE context in the target eNodeB, including information about the bearers, and the security context. For each EPS bearer, the bearers to setup include the serving GW address and uplink TEID for user plane, and EPS bearer QoS. If the direct forwarding flag indicates unavailability of direct forwarding and the target MME knows that there is no indirect data forwarding connectivity between the source and the target, the Bearers to Setup shall include "Data forwarding not possible" indication for each EPS bearer. The handover restriction list is sent if available in the target MME; it is described in clause 4.3.5.7 of [b-ETSI 123.401] on "Mobility Restrictions". S1AP cause indicates the RAN cause as received from the source MME. The target MME shall include CSG ID and CSG membership indication when provided by the source MME in the Forward Relocation Request message. The target eNodeB sends a Handover Request Acknowledge (EPS Bearer Setup list, EPS bearers failed to set up list target to source transparent container) message to the target MME. The EPS Bearer Setup list includes a list of addresses and TEIDs allocated at the target eNodeB for downlink traffic on S1-U reference point (one TEID per bearer) and addresses and TEIDs for receiving forwarded data if necessary. If UE-AMBR is changed, e.g., all the EPS bearers which are associated to the same APN are rejected in the target eNodeB, MME shall recalculate the new UE-AMBR and signal the modified UE-AMBR value to the target eNodeB. If none of the default EPS bearers have been accepted by the target eNodeB, the target MME shall reject the handover as specified in clause 5.5.1.2.3 of [b-ETSI 123.401]. If the target cell is a CSG cell, the target eNodeB shall verify CSG ID provided by the target MME, and reject the handover with an appropriate cause if it does not match CSG ID for the target cell. If the target eNodeB is in hybrid mode, it may use the CSG membership indication to perform a differentiated treatment for CSG and non-CSG members. If the target cell is a CSG cell, and if the CSG membership indication is "non-member", the target eNodeB only accepts the emergency bearers.

6 If indirect forwarding applies and the serving GW is relocated, the target MME sets up forwarding parameters by sending a Create Indirect Data Forwarding Tunnel Request (target eNodeB addresses and TEIDs for forwarding) message to the serving GW. The serving GW sends a Create Indirect Data Forwarding Tunnel Response (target serving GW addresses and TEIDs for forwarding) message to the target MME. If the serving GW is not relocated, indirect forwarding may be set up in step 8 below. Indirect forwarding may be performed via a serving GW which is different from the serving GW used as the anchor point for UE.

7 If MME has been relocated, the target MME sends a Forward Relocation Response (cause, target to source transparent container, serving GW change indication, EPS Bearer Setup List, addresses and TEIDs) message to the source MME. For indirect forwarding, this message includes the serving GW address and TEIDs for indirect forwarding (source or target). The serving GW change indication indicates a new serving GW has been selected.

8 If indirect forwarding applies, the source MME sends a Create Indirect Data Forwarding Tunnel Request (addresses and TEIDs for forwarding) message to the serving GW. If the serving GW is relocated, it includes the tunnel identifier to the target serving GW. The serving GW responds with a Create Indirect Data Forwarding Tunnel Response (serving GW

addresses and TEIDs for forwarding) message to the source MME. Indirect forwarding may be performed via a serving GW which is different from the serving GW used as the anchor point for UE.

9 The source MME sends a Handover Command (target to source transparent container, bearers subject to forwarding, Bearers to Release) message to the source eNodeB. The bearers subject to forwarding includes a list of addresses and TEIDs allocated for forwarding. The Bearers to Release includes the list of bearers to be released.

9a. The Handover Command is constructed using the Target to Source transparent container and is sent to UE. Upon reception of this message, UE will remove any EPS bearers for which it did not receive the corresponding EPS radio bearers in the target cell.

10 The source eNodeB sends the eNodeB Status Transfer message to the target eNodeB viaMME(s) to convey the packet data convergence protocol (PDCP) and hyper frame number (HFN) status of the E-RABs for which PDCP status preservation applies, as specified in [ETSI 136.300]. The source eNodeB may omit sending this message if none of the E-RABs of UE shall be treated with PDCP status preservation. If there is MME relocation, the source MME sends this information to the target MME via the Forward Access Context Notification message which the target MME acknowledges. The source MME or, if the MME is relocated, the target MME sends the information to the target eNodeB via the MME Status Transfer message.

11 The source eNodeB should start forwarding of downlink data from the source eNodeB towards the target eNodeB for bearers subject to data forwarding. This may be either direct (step 11a) or indirect forwarding (step 11b).

12 After UE has successfully synchronized to the target cell, it sends a Handover Confirm message to the target eNodeB. Downlink packets forwarded from the source eNodeB can be sent to UE. Also, uplink packets can be sent from UE, which are forwarded to the target serving GW and on to PDN GW.

13 The target eNodeB sends a Handover Notify (TAI+ECGI) message to the target MME.

14 If MME has been relocated, the target MME sends a Forward Relocation Complete Notification message to the source MME. The source MME in response sends a Forward Relocation Complete Acknowledge message to the target MME. Regardless if MME has been relocated or not, a timer in the source MME is started to supervise when resources in the source eNodeB, and if the serving GW is relocated, and also resources in the source serving GW shall be released. Upon receipt of the Forward Relocation Complete Acknowledge message, the target MME starts a timer if the target MME allocated the S-GW resources for indirect forwarding.

15 The target MME sends a Modify Bearer Request (eNodeB address and TEID allocated at the target eNodeB for downlink traffic on S1-U for the accepted EPS bearers, ISR Activated) message to the target serving GW for each PDN connection, including the PDN connections that need to be released. If PDN GW requested UE's location and/or user CSG information (determined from the UE context), MME also includes the user location information IE and/or user CSG information IE in this message. If the UE time zone has changed, MME includes the UE time zone IE in this message. If the serving GW is not relocated but the serving network has changed, or if MME has not received any old serving network information from the old MME, MME includes the serving network IE in this message. In the case when neither MME nor S-GW has changed, and if ISR was activated before this procedure, MME should maintain ISR. UE is informed about the ISR status in the tracking area update procedure. If the serving GW supports Modify Access Bearers Request procedure

and if there is no need for the S-GW to send the signalling to P-GW, MME may send Modify Access Bearers Request (eNodeB address and TEID allocated at the target eNodeB for downlink traffic on S1-U for the accepted EPS bearers, ISR Activated) per UE to the serving GW to optimize the signalling. MME releases the non-accepted dedicated bearers by triggering the bearer release procedure as specified in clause 5.4.4.2 of [b-ETSI 123.401]. If the serving GW receives a DL packet for a non-accepted bearer, the serving GW drops the DL packet and does not send a Downlink Data Notification to MME. If the default bearer of a PDN connection has not been accepted by the target eNodeB and there are other PDN connections that are active, MME shall handle it in the same way as if all bearers of a PDN connection have not been accepted. MME releases these PDN connections by triggering the MME requested PDN disconnection procedure specified in clause 5.10.3 of [b-ETSI 123.401]. When the Modify Bearer Request does not indicate ISR Activated, the serving GW deletes any ISR resources by sending a Delete Bearer Request to the other CN nodes that have bearer resources on the serving GW reserved.

16 If the serving GW is relocated, the target serving GW assigns addresses and TEIDs (one per bearer) for downlink traffic from PDN GW. It sends a Modify Bearer Request (serving GW addresses for user plane and TEID(s), serving network) message per PDN connection to PDN GW(s). S-GW also includes user location information IE and/or UE time zone IE and/or user CSG information IE if they are present in step 15. The serving GW also includes serving network IE if it is present in step 4 or step 15. The serving GW allocates DL TEIDs on S5/S8 even for non-accepted bearers. PDN GW updates its context field and returns a Modify Bearer Response (charging Id, MSISDN) message to the target serving GW. MSISDN is included if PDN GW has it stored in its UE context. PDN GW starts sending downlink packets to the target serving GW using the newly received address and TEIDs. These downlink packets will use the new downlink path via the target serving GW to the target eNodeB. If the serving GW is not relocated but has received the user location information IE and/or UE time zone IE and/or user CSG information IE and/or serving network IE from MME in step 15, the serving GW shall inform PDN GW(s) about this information that, for example, can be used for charging, by sending the message Modify Bearer Request (user location information IE, UE time zone IE, user CSG information IE, serving network IE) to the PDN GW(s) concerned. A Modify Bearer Response message is sent back to the target serving GW. If the serving GW is not relocated and it has not received user location information IE or UE time zone IE, or user CSG information IE or serving network IE from MME in step 15, no message is sent in this step and downlink packets from the serving-GW are immediately sent on to the target eNodeB.

17 The serving GW shall return a Modify Bearer Response (serving GW address and TEID for uplink traffic) message to MME as a response to a Modify Bearer Request message, or a Modify Access Bearers Response (serving GW address and TEID for uplink traffic) as a response to a Modify Access Bearers Request message. If the serving GW cannot serve the MME Request in the Modify Access Bearers Request message without S5/S8 signalling or without the corresponding Gxc signalling when PMIP is used over the S5/S8 interface, it shall respond to MME by indicating that the modifications are not limited to S1-U bearers, and MME shall repeat its request using the Modify Bearer Request message per PDN connection. If the serving GW does not change, the serving GW shall send one or more "end marker" packets on the old path immediately after switching the path in order to assist the reordering function in the target eNodeB.

18 UE initiates a tracking area update procedure when one of the conditions listed in clause "Triggers for tracking area update" applies. The target MME knows that it is a handover procedure that has been performed for this UE as it received the bearer context(s) by handover messages, and therefore the target MME performs only a subset of the TA update procedure,

specifically it excludes the context transfer procedures between the source MME and the target MME.

19 When the timer started in step 14 expires, the source MME sends a UE Context Release Command message to the source eNodeB. The source eNodeB releases its resources related to UE and responds with a UE Context Release Complete message. When the timer started in step 14 expires and if the source MME received the serving GW change indication in the Forward Relocation Response message, it deletes the EPS bearer resources by sending Delete Session Request (cause, LBI, operation indication) messages to the source serving GW. The operation indication flag is not set, which indicates to the source serving GW that the source serving GW shall not initiate a delete procedure towards PDN GW. The source serving GW acknowledges with Delete Session Response messages. If ISR has been activated before this procedure, the cause indicates to the source S-GW that the source S-GW shall delete the bearer resources on the other old CN node by sending Delete Bearer Request message(s) to that CN node.

20 If indirect forwarding was used, then the expiry of the timer at source MME started in step 14 triggers the source MME to send a Delete Indirect Data Forwarding Tunnel Request message to S-GW to release the temporary resources used for indirect forwarding that were allocated in step 8.

21 If indirect forwarding was used and the serving GW is relocated, then the expiry of the timer at target MME started in step 14 triggers the target MME to send a Delete Indirect Data Forwarding Tunnel Request message to the target S-GW to release temporary resources used for indirect forwarding that were allocated in step 6.

20.11.4 Reference point and handover between E-UTRAN and HRPD networks (S101)

The S101 reference point supports procedures for pre-registration, session maintenance and active handovers between E-UTRAN and high rate packet data (HRPD) networks. The procedures are performed by tunnelling over S101 signalling for one technology, while UE camps in another technology, see [ETSI 123.402]. The HRPD air interface messages tunnelled over S101 in E-UTRAN to HRPD mobility are defined in 3GPP2.

The S101 reference point shall support the following requirements:

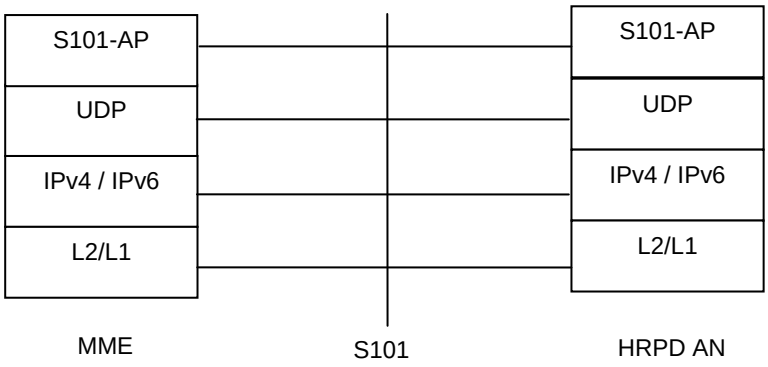
– HRPD and E-UTRAN/EPS messages shall be transported as opaque containers without modifications by MME or HRPD AN;

– Messages may carry separate information IEs to indicate status, message types, e.g. handover command, forwarding addresses, etc., as required by signalling procedures;

– Provide identifiers, i.e., S101 session ID, to distinguish messages belonging to different UEs in order to allow responses originating from the target system to UE to be appropriately forwarded to UE by the source system;

– Reliable transport for S101 messages should be provided at the application layer and will not require transport layer reliability mechanism.

Figure 57 shows the protocol stack for the S101 interface.



- S101 application protocol (S101-AP): It is the application layer protocol between MME and HRPD AN.
- User datagram protocol (UDP): This protocol transfers messages. UDP is defined in [b-IETF RFC 768]
- S101 application protocol (S101-AP) provides application layer reliability for its messages, if required.

Figure 57 – Protocol stack for the S101 reference point [ETSI 123.402]

All S101 messages contain a S101 session identifier (session ID) which serves to identify the UE context at MME and HRPD AN. The S101 session ID uniquely and globally identifies UE.

In particular, for HRPD networks accesses, MM and the corresponding handover procedures in general, a main objective is to minimize the total service interruption time experienced at UE, by allowing UE to attach and perform service activation (in the case of E-UTRAN) or to perform a session configuration or traffic allocation request (in the case of HRPD) in the target access system before leaving the source access system.

In the case where UE is connected to E-UTRAN and conditions are such that a handover to HRPD may be required, the source system provides UE with sufficient information to perform pre-registration with the target HRPD access and core network, over the S101 tunnelling interface. If conditions subsequently guarantee that a handover should occur, the handover signalling is also performed over the S101 tunnelling interface. Once UE is ready to connect to the target system, it switches HRPD access on. Alternatively, E-UTRAN may redirect UE to HRPD using the radio resource control (RRC) connection release with redirection information set. If pre-registration has not been performed successfully, upon receiving the redirection message, UE acquires the HRPD channel and performs the non-optimized handover. If pre-registration is successful, upon receiving the redirection message, UE follows the RRC connection release with redirection procedure to reselect the HRPD cell and then perform the idle-mode optimized handover procedure.

In the case where UE is connected to HRPD and conditions are such that a handover to E-UTRAN may be required, the source system provides UE with sufficient information to perform pre-registration with the target EPS. The pre-registration may be performed over the S101 tunnelling interface. If conditions subsequently guarantee that a handover should occur, the handover signalling may also be performed over the S101 tunnelling interface. Once UE is ready to connect to the target system, it switches to the E-UTRAN access.

Figure 58 illustrates a high-level call flow for the optimized E-UTRAN to HRPD handover procedure, the handover phase. The prerequisite of the handover phase is the successfully performed pre-registration phase, for more details see [ETSI 123.402].

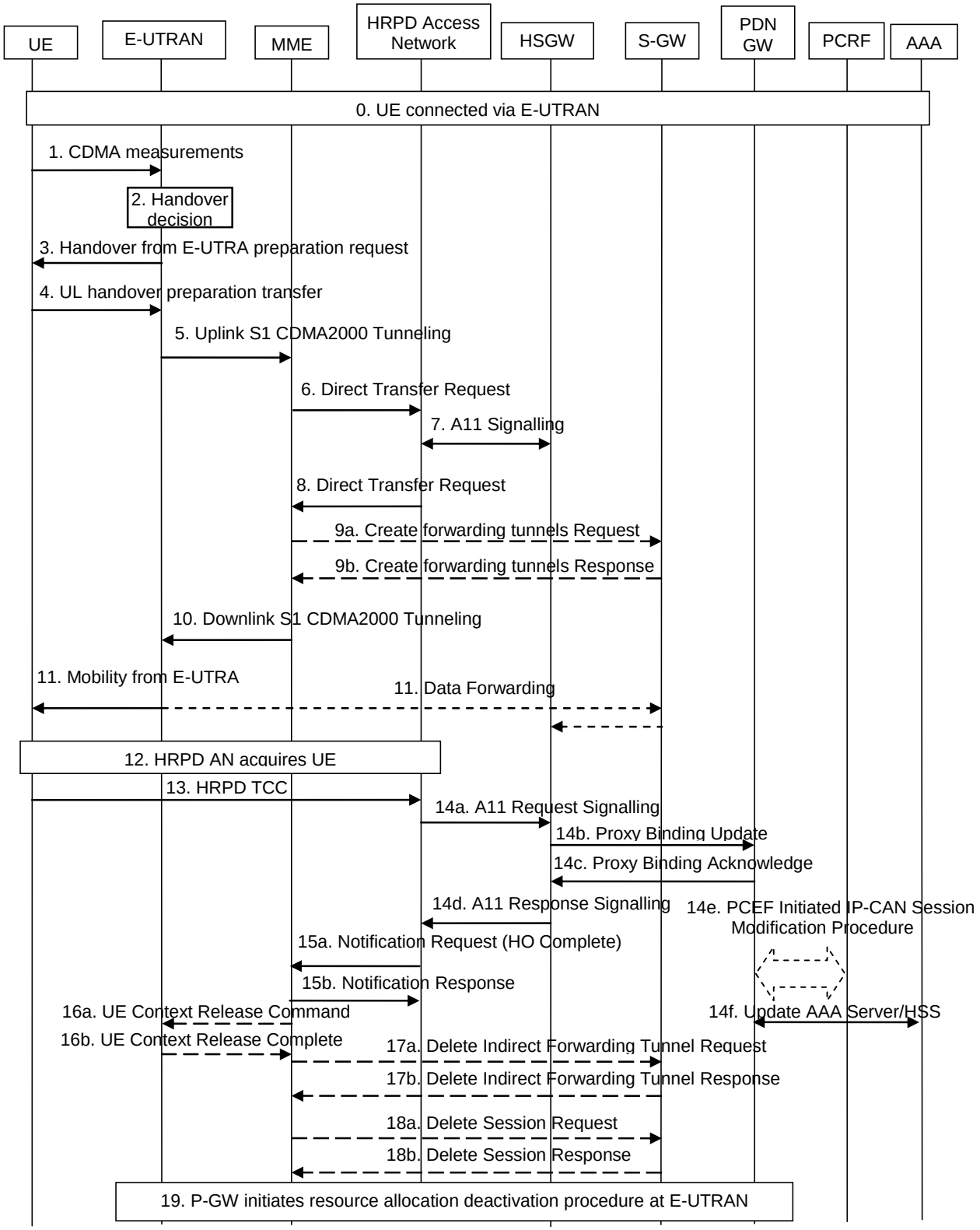


Figure 58 – E-UTRAN to HRPD handover [ETSI 123.402]

In the above diagram:

0 Ongoing session established over EPS/E-UTRAN access.

1 eNodeB receives measurement reports from UE.

2 eNodeB makes the handover decision.

3 The handover decision is signalled to UE with the handover from E-UTRA preparation request message.

4 UE sends an UL handover preparation transfer message (HRPD message starting HO access) to eNodeB. The HRPD message starting HO access is carried transparently to the HRPD access node, and its purpose is to request information for accessing HRPD traffic channel. The message indicates to eNodeB that UE is responding to the handover from E-UTRA preparation request message, and is requesting information for accessing HRPD traffic channel.

5 eNodeB sends the uplink S1 CDMA-2000 Tunnelling message (HRPD message starting HO access, and SectorID, CDMA-2000 HO required indication) to MME. The sector ID is statically configured in eNodeB. eNodeB will also include CDMA-2000 HO required indication IE to uplink S1 CDMA-2000 Tunnelling message, which indicates to MME that the handover preparation has started.

6 When receiving uplink S1 CDMA-2000 Tunnelling message with CDMA-2000 HO required indication, MME determines HRPD access node address based on the sector ID. An S101 session ID is used to identify signalling related to that UE on S101. MME sends a Direct Transfer Request message (S101 session ID, sector ID, PDN GW identity(ies), generic routing encapsulation (GRE) key(s) for uplink traffic, APN(s), HRPD message starting HO access) to the HRPD access node.

When GTP-based S5/S8 is used in EPS, MME creates the uplink generic routing encapsulation (GRE) keys from the uplink tunnel endpoint identifiers (TEIDs) of the default bearers using a standardized algorithm. In this way, only one GRE key per PDN connection is created. PDN GW shall be able to identify any PDN connection based on the GRE key created from the uplink TEID of the default bearer of that PDN connection.

NOTE – When PDN GW supporting both GTP and proxy MIP (PMIP) based interfaces allocates a TEID for GTP tunnel, it also allocates and memorizes a corresponding GRE key if the tunnel is created for a default bearer. Later on, PDN GW is able to identify the PDN connection based on the corresponding GRE key, i.e., PDN GW also assigns the corresponding GRE key to that particular PDN connection and it cannot use that GRE key for any other PDN connection.

7 HRPD access network allocates the requested radio access resources, and requests a forwarding address from HRPD serving gateway (HS-GW). The information sent in the request from the HRPD access network to HS-GW includes APN(s), PDN GW identity(ies) and GRE key(s) for uplink traffic. The response includes the HS-GW address and GRE key(s) for forwarded traffic on reference point S103. There is one GRE key for each PDN connection for which traffic is to be forwarded.

8 The HRPD access network sends the Direct Transfer Request message (S101 session ID, HRPD message with HO access information, HS-GW address and GRE key(s) for forwarded traffic, CDMA-2000 HO status) to MME. HS-GW address and GRE key(s) for forwarded traffic are sent if data forwarding applies. If the HRPD access network did not allocate the resources as requested, this will be indicated to MME and eNodeB with the CDMA-2000 HO status IE, and the embedded HRPD message indicates the failure to UE.

9a. If Direct Transfer Request message included HS-GW address and GRE key(s) for forwarded traffic, MME determines which of the S1-U bearers should be forwarded to HRPD and configures resources for indirect data forwarding by sending Create Forwarding Tunnel Request (HS-GW address, GRE key(s) for forwarded traffic, EPS bearer ID(s) subject to forwarding) to the serving GW.

MME shall select the same serving GW which is used as the anchor point for UE to perform the data forwarding.

9b. The serving GW confirms data forwarding resources for S103 and allocates a forwarding address for S1 in Create Forwarding Tunnel Response (cause, S-GW address, S1-U uplink TEID(s)). The S1-U uplink TEIDs are provided one per S1-U bearers subject to forwarding.

10 MME sends the Downlink S1 CDMA-2000 Tunnelling message (HRPD message with HO access information, S-GW address, S1-U uplink TEID(s), CDMA-2000 HO Status) to E-UTRAN. If the CDMA-2000 HO status indicates that handover preparation failed, the downlink S1 CDMA-2000 Tunnelling message will be sent with the appropriate cause, and the embedded HRPD message that indicates the failure to UE. The message from MME provides the eNodeB also with the data forwarding S1-U uplink TEIDs allocated at the serving GW if data forwarding applies.

11 E-UTRAN forwards the HRPD message with HO access information to UE in Mobility from E-UTRAN message. This is perceived by UE as a Handover Command message. If handover preparation failed, DL information transfer message will be sent instead, with the embedded HRPD message that indicates the failure to UE.

If data forwarding applies, E-UTRAN starts forwarding received downlink data to the S-GW on a per-S1-U bearer forwarding tunnel, which then forwards these packets on a per-PDN per-UE S103 tunnel to HS-GW. The forwarding starts at the same moment as the Mobility from E-UTRAN message is sent to UE.

12 UE retunes to the HRPD radio access network and performs traffic channel acquisition.

13 UE sends HRPD Traffic Channel Complete (TCC) message to the HRPD access network.

14a-14f E-UTRAN triggers switching the flow in EPC with the following sequence:

14a. The HRPD access network sends A11 request signalling to HS-GW, see [ETSI 123.402], to start setting up the U-plane connection between the HRPD access network and HS-GW.

14b. HS-GW sends a Proxy Binding Update (PBU) message to PDN GW. HS-GW sends the all zero IPv4 home address (0.0.0.0) or all zero IPv6 home prefix (0::/0) in the PBU message. In order to support session continuity, the P-GW performs the Binding Cache entry existence test based on NAI and assigns the same IPv4 home address and/or IPv6 home prefix to UE and acknowledge in the Proxy Binding Acknowledge (PBA) message.

14c. PDN GW switches the flow from serving GW to HS-GW, and sends Proxy Binding Acknowledge to HS-GW, including the Charging ID for the PDN connection.

14d. HS-GW responds with A11 Response Signalling to the HRPD access network.

14e. PDN GW executes a PCEF-initiated IP-CAN Session Modification procedure with PCRF as specified in [ETSI 123 203] to obtain the rules required for PDN GW to function as PCEF for all the active IP sessions UE has established with the new IP-CAN type. Otherwise, information configured with P-GW may be used to determine policy. Since steps 14c and 14e are both triggered by the Proxy Binding Update in step 14b, steps 14c and 14e may occur in parallel.

14f. PDN GW informs the 3GPP AAA server of its PDN GW identity and the access point name (APN) corresponding to UE's PDN connection and obtains authorization information from the 3GPP AAA server. The message includes information that identifies the PLMN in which PDN GW is located. The 3GPP AAA server may update the information registered in HSS.

For a multiple PDN connection, steps 14b-14f are performed for each PDN connection.

Multiple PDN connections for the same APN can be supported using PDN connection identities in the same way as it is specified for S2a procedures, see [ETSI 123.402].

15a. The HRPD access network sends a Notification Request (HO complete, S101 session ID) message to MME (including the S101 session ID to identify the UE context).

15b. MME responds by sending a Notification Response (S101 session ID) to the HRPD access network.

If data forwarding was not applied in step 9, MME shall skip step 17, and shall perform steps 16 and 18.

If data forwarding was applied in step 9, a timer in MME is started to supervise when the EPS bearer resources in the serving GW and the temporary resources used for indirect data forwarding in the serving GW shall be released. The uses of the timer are defined in [b-ETSI 123.401]. MME perform steps 16, 17 and 18 upon timer expiry.

If the EPS bearer resources release is triggered by a Delete Bearer Request message (from step 19) received before the timer expiry, MME shall stop the timer and skip steps 16, 17 and 18.

16a. MME releases the UE context in the source E-UTRAN by sending a UE Context Release Command message to eNodeB.

16b. The source eNodeB releases its bearer resources related to UE and responds with a UE Context Release Complete message.

17a. MME sends a Delete Indirect Data Forwarding Tunnel Request message to the serving GW.

17b. The serving GW releases the temporary resources used for indirect data forwarding which were allocated in step 9. The serving GW acknowledges with Delete Indirect Data Forwarding Tunnel Response message.

18a. MME releases the EPS bearer resources in the serving GW by sending a Delete Session Request message to the serving GW. MME shall indicate to the serving GW that the serving GW shall not initiate a delete procedure towards PDN GW.

18b. The serving GW acknowledges the resource removal with a Delete Session Response (Cause) message.

19. At any time after step 14c, PDN GW shall initiate the PDN GW-initiated PDN Disconnection procedure at E-UTRAN, see [ETSI 123.402] or the PDN GW-initiated Bearer Deactivation procedure as defined in clause 5.4.4.1 of [b-ETSI 123.401]. If data forwarding was applied, the forwarding tunnel established in step 9 shall be also released in this step.

Additional MM procedures for the S101 reference point are described in [ETSI 123.402], two of which are:

1 the HRPD to E-UTRAN handover with GTP-based S5/S8, and

2 S101 Tunnel Redirection procedure, used when UE performs TAU with MME change while UE has already triggered a pre-registration procedure from LTE to HRPD and the S101 session exists between MME and the HRPD access network, for idle and active cases.

20. Relationship between mobility management control function (MMCF) and NGN-FRA functions

In this clause, a high-level relationship between the mobility management control functions (MMCFs) and NGN-FRA (functional requirements and architecture of NGN) is described; see [b-ITU-T Y.2012]. The MM framework only describes the MM-related functions. The functional entities required to realize these functions are addressed in [b-ITU-T Q.1708] and [b-ITU-T Q.1709].

Figure 59 shows the generic relationship between MMCFs and NGN-FRA functions.

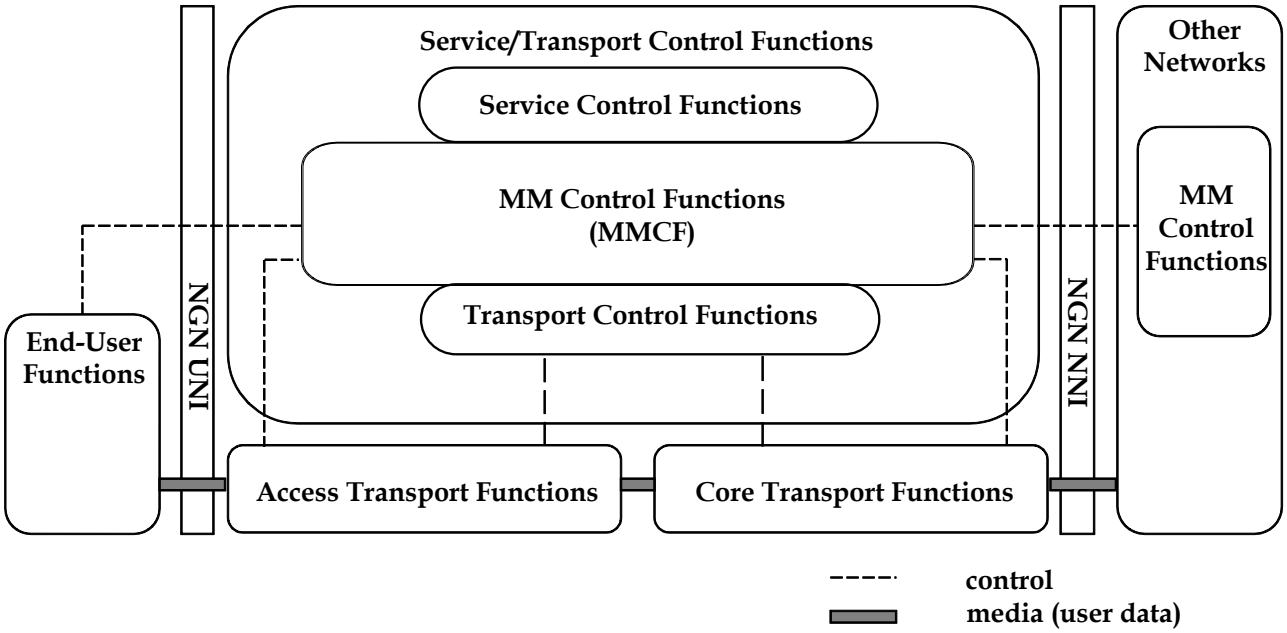


Figure 59 – Relationship between MMCF and NGN-FRA Functions [b-ITU-T Q.1707]

As shown in Figure 59, the service/transport control functions are associated to MMCF. MMCF in turn is associated with UE as well as with the network entities. Furthermore, the overall MM functionality interworks with other NGN networks, when required. Figure 59 also shows that MMCF interworks with the service and transport control functions as an integral part of NGN.

MMCF also interacts directly or indirectly with the transport function, wherever applicable.

The detailed mapping between MMCF functions and NGN-FRA functions such as NACF and RACF require more study.

21 High-level information flows

This clause describes the high-level information flows for MM within NGN, see [b-ITU-T Q.1707]. These include:

1 Network attachment.

2 Location management.

3 User data transport.

4 Handover support.

The high-level information flows are herein described based on MMCFs and UE.

For more detailed procedural information flows between MMCFs and the other NGN functional entities, e.g., AAA, DHCP, and policy servers, see [b-ITU-T Q.1708] and [b-ITU-T Q.1709].

The procedural information flows are provided after the following categories:

1) Roaming and non-roaming cases in the location management;

2) Hierarchical and non-hierarchical location and handover management;

3) Host-based and network-based location and handover management; and

4) Horizontal and vertical handover management.

21.1 Network attachment

This clause describes network attachment (see [b-ITU-T Q.1707]), which normally consists of:

1 Link establishment.

2 User authentication and authorization.

3 Location ID configuration

21.1.1 Link establishment

The MM control operations start when UE attempts to establish a connection to the network link. The network link, being a wired or wireless link, depends on the specific link-layer access technology, such as Ethernet, cdma2000, wideband code division multiple access (W-CDMA), WLAN, etc.

21.1.2 User authentication and authorization

After UE has established a connection to the network, the user authentication and authorization processes are performed, typically through the interaction of the AAA-related servers. In the user authentication/authorization process, a user ID (UID) is used associated with UE.

21.1.3 Location ID configuration

When or after UE is authenticated and authorized by the network (or service provider), it is given one or more location IDs, which must include a routable IP address. As LID, an IP address is configured using a DHCP server or an appropriate auto-configuration scheme.

When UE is connected to the network, it sends the information of UID to A-LMF for authentication and authorization. For this purpose, A-LMF may interact with NGN-NACF (network attachment control function), and it may also contact an appropriate user profile server. When the authentication/authorization is completed, LID will be assigned to UE.

21.2 Location registration and update

After UE has completed the network attachment, it performs the location registration and update procedures. By doing so, the information mapped between UID and LID is recorded and managed by the associated LM functions with the support of the relevant location database.

When UE is first attached to the network, it performs the location registration procedure, whereas it performs the location update procedure whenever it moves into another network and thus changes its LID.

21.2.1 Location registration

For the location registration in the host-based LM, when UE receives its LID, it registers LID and UID with the associated LM functional entities.

Figure 60 shows an abstract flow of the location registration for the non-roaming case.

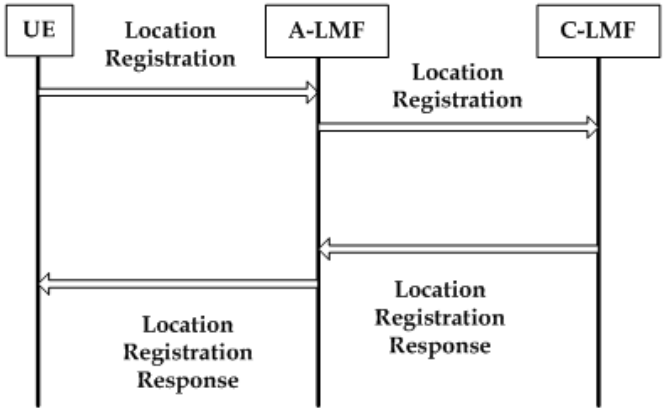


Figure 60 – Location registration for non-roaming cases [b-ITU-T Q.1707]

In Figure 60, UE registers its LID and UID with A-LMF by sending a location registration message. Based on the location registration message received from UE, A-LMF adds a new entry of the location information associated with UE and keeps the information related to the mapping between UID and LID. A-LMF then relays the message to C-LMF.

When C-LMF receives the location registration message from A-LMF, it also adds the associated location information into the location database (or user profile server) for UE. On the successful processing of the location database, C-LMF responds with a location registration response message to A-LMF. In turn, A-LMF responds to UE.

In the host-based LM, UE performs the location registration, whereas in the network-based LM, a network agent concerned with A-LMF is responsible for location registration. More detailed procedures for the location registration are described in [b-ITU-T Q.1708].

In the roaming case, in which UE moves into a different NGN operator's network, the location registration is performed with the support of the visited C-LMF and home C-LMF.

In the roaming case, the visited LMFs represent a set of A-LMFs and/or C-LMFs in the network of the NGN operator visited by UE. There may be a variety of location registration schemes in the roaming case; these are described in [b-ITU-T Q.1708].

21.2.2 Location update

After the initial location registration, UE may move around in the network. When UE moves into another network and changes its LID, it performs the location update operation.

When moving in the network, UE may change its LID and its corresponding A-LMF. In this case, UE updates its location information by sending the location update message to the new A-LMF.

If it is assumed that UE enters a new A-LMF, the location update message indicates that the operation is performed for re-registration of the location information. In the host-based LM, UE itself performs the location update procedures, whereas in the network-based LM, A-LMF is responsible for the location update procedures.

In the roaming case, UE may change its corresponding NGN operator with C-LMF. In this case, the location update messages are exchanged between the visited LMF and the home LMF, as the location registration flows for the roaming case. The detailed procedures for the location update are described in [b-ITU-T Q.1708].

21.3 Location query for user data transport

For user data transport, the corresponding UE performs the 'location query' operations to identify the location of the mobile UE. In the location query operation, UE tries to locate another UE by sending the location query message to LMFs. LMFs then respond to UE with the location query response message.

The location query operations are performed differently for the following two cases:

1 Location query without session set-up signalling;

2 Location query with session set-up signalling.

21.3.1 Location query without session set-up signalling

According to the application/session type, the location query and response operations may be done together with the session set-up signaling, e.g., SIP-based VoIP application, or without the session set-up signaling, e.g., e-mail.

If an application does not require any session set-up signalling, the calling UE obtains the location information of the concerned called UE using the location query and response operations.

Figure 61 provides high-level information flows for the location query and response operations without the session set-up signalling operation for the non-roaming case.

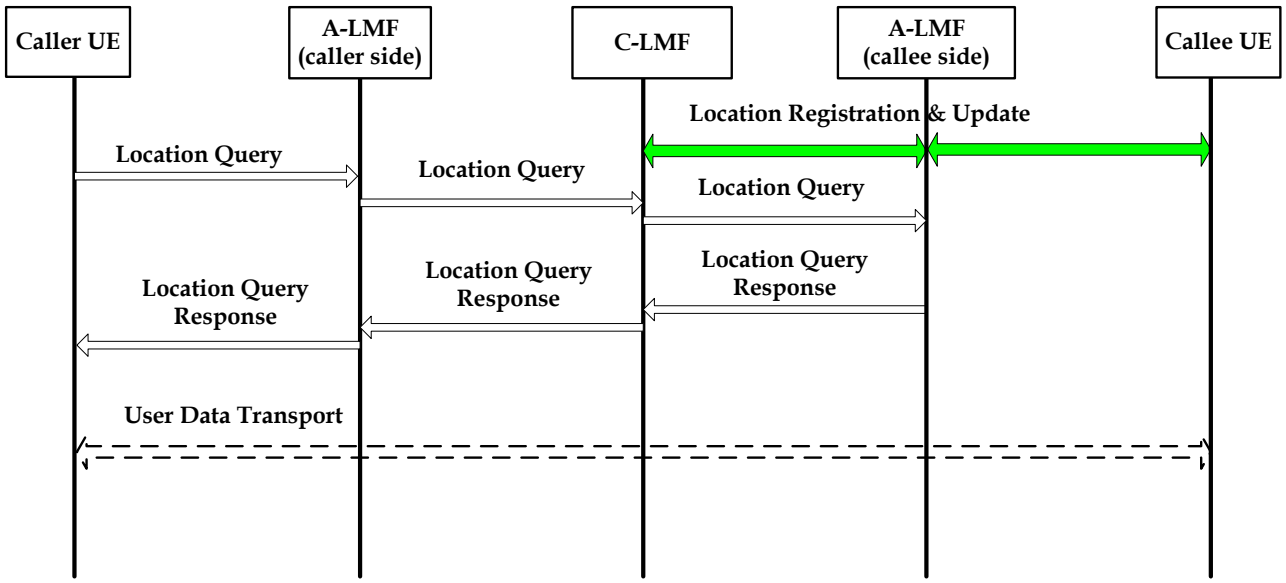


Figure 61 – Location query without session set-up signalling when non-roaming

It is assumed in the flow that the calling UE has already registered its current location information with the associated A-LMF as well as with C-LMF. It is also assumed that the calling UE and the called UE are registered with different A-LMFs, in which A-LMF in the calling UE side manages the location information of the calling UE, whereas A-LMF in the called side manages the location information of the called UE. Depending on the specific LM scheme, some of the signalling may be omitted in Figure 61.

Figure 61 also shows that the calling UE first tries to find the location information of the called UE by contacting A-LMF in the calling side. If the called UE has not registered with A-LMF of the calling UE, A-LMF in the calling side will consult with C-LMF. C-LMF may then find the location of the called UE by contacting A-LMF in the called side. The location information of the called UE is then delivered to the calling UE with the location query response message. After this procedure has taken place, the user data transport begins.

On the other hand, Figure 62 shows an abstract information flow for the location query and response operations when roaming.

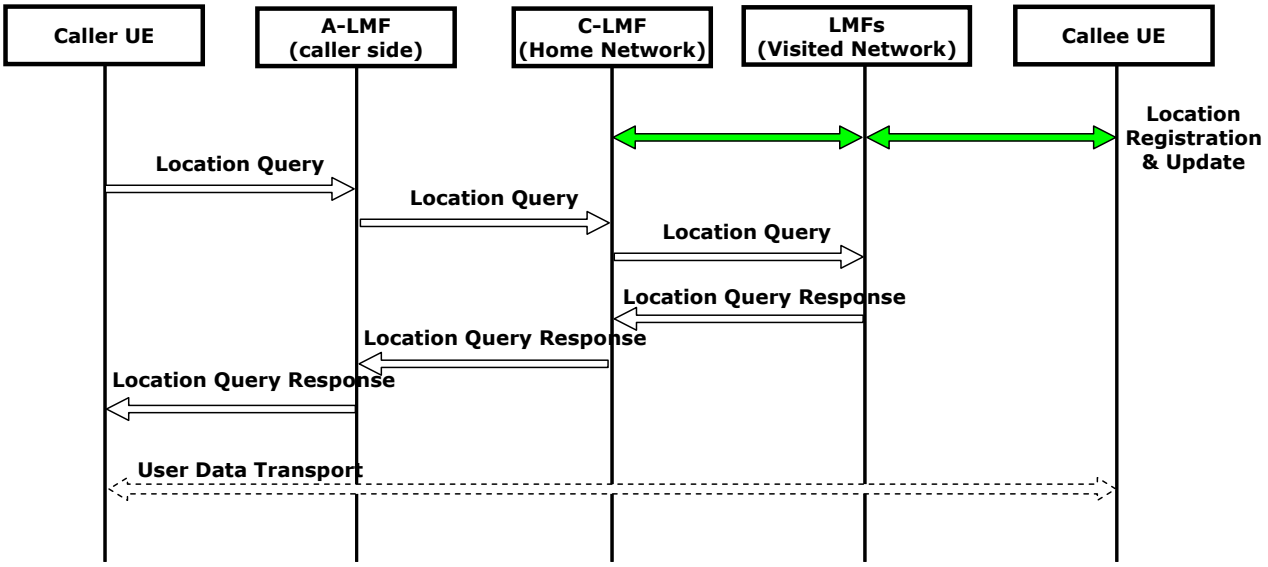


Figure 62 – Location query without session set-up signalling when roaming [b-ITU-T Q.1707]

Figure 62 also shows an option in which the calling UE is in the visited network and has already registered its current location information with the associated home C-LMF, possibly via the visited LMFs.

In this case, the calling UE obtains the location information of the called UE by sending a location query to A-LMF in the calling side. In turn, A-LMF of the calling UE sends a location query to the home C-LMF of the called UE. The home C-LMF then consults with the visited LMFs of the called UE.

21.3.2 Location query with session set-up signalling

For applications requiring a session set-up signalling operation, e.g., SIP-based application, the location query and response operations may be performed together with the session set-up signalling operations. In this case, the messages for session set-up signalling may contain the location query/response information, as shown in the SIP INVITE and OK messages.

Figure 63 below provides an example of the information flow for the location query/response operation with the session set-up signalling when UE is not roaming.

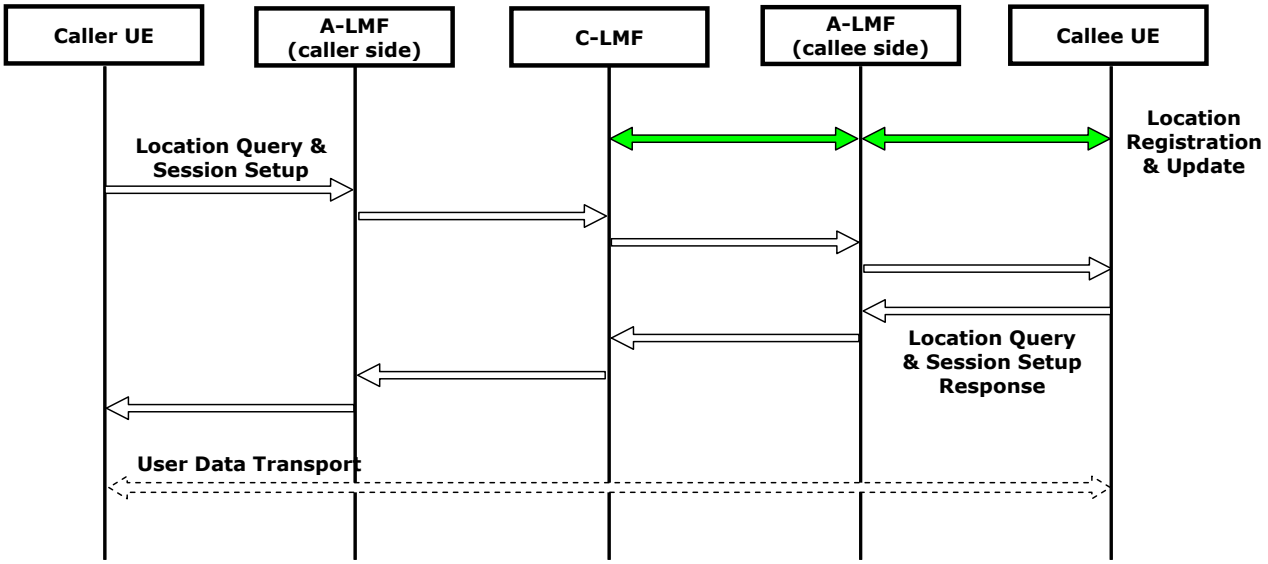


Figure 63 – Location query with session set-up signalling when UE is not roaming [b-ITU-T Q.1707]

In Figure 63, it is assumed that the calling UE has already registered its current location information with the associated A-LMF (at the calling side) as well as with C-LMF. In case of IMS-based applications, A-LMF may work with the proxy call session control function (CSCF), and C-LMF may be with S-CSCF (serving-CSCF).

An abstract information flow for the location query and response, with session set-up signalling operations when UE is roaming, is shown in Figure 64. More detailed information flows are described in [b-ITU-T Q.1708].

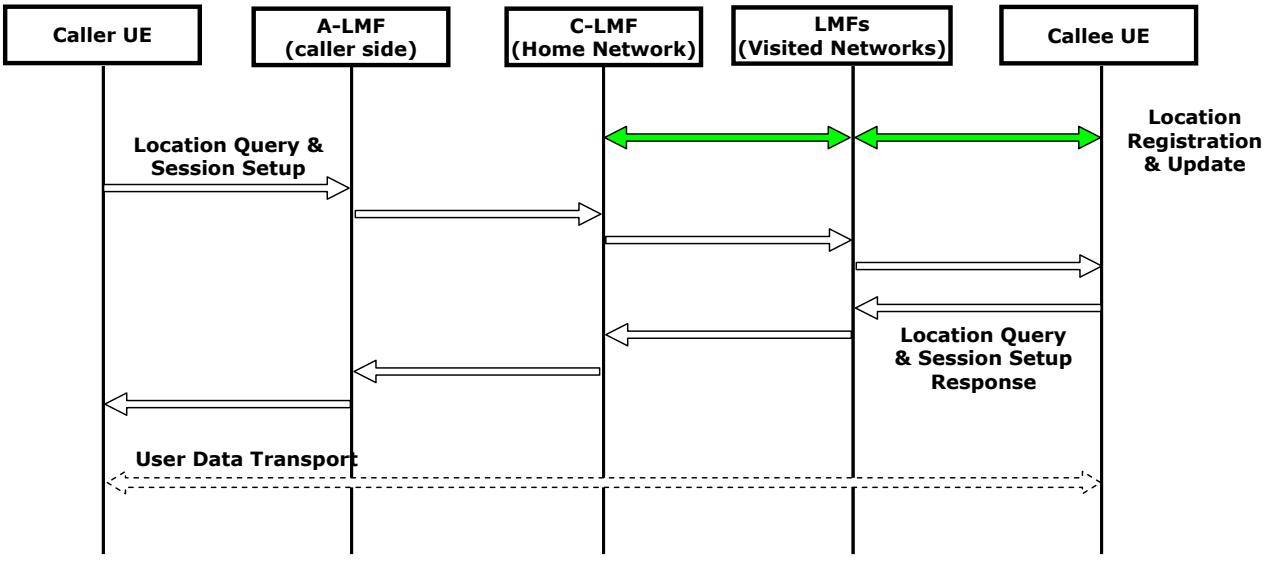


Figure 64 – Location query with session set-up signalling when UE is roaming [b-ITU-T Q.1707]

21.4 Handover support

After the location query and response operations have been performed, the user data transport operations begin. The data packets are exchanged between the two concerned UEs using the standard IP routing scheme, see [b-ITU-T Q.1707].

During the user data session, whenever an UE moves into another network region, the handover support operations are activated to provide seamless session continuity with the support of the handover control functions (HCFs).

The handover support operations may be classified into two phases:

1 Handover preparation, and

2 Handover execution.

21.4.1 Handover preparation

The first step in the handover preparation procedure is the handover (or movement) detection in order to recognize that a link-layer handover of a mobile UE is imminent.

This can be achieved with the help of an associated link-layer notification. For instance, a link trigger such as link-going-down may be used for notification of an imminent link-layer handover.

Thus an important feature in this process is to align the link-layer triggers provided by different access technologies into an integrated open service interface between the link-layer protocols and the upper-layer mobility management schemes, as for instance in the media independent handover (MIH) services.

The next step takes place when the network discovery operation searches the access networks to which UE is able to connect to. This step may be performed, from UE point of view, by scanning all accessible links to UE. In support to UE, the neighbouring network information may be periodically announced from the access network to UE.

The network discovery may be followed by the network selection, in order to choose the target access network (or PoA) to achieve the handover operation. An UE may select one of the accessible links found in the network discovery according to a predefined handover policy.

If sufficient network information is provided for network selection, UE and/or HCF may choose a target network which is the most profitable one as per the predefined policy. Policies or factors to be considered for network selection may include the available resources, estimated handover latency, QoS support, types of MM protocols, wireless cell coverage, etc. HCF may interact with other NGN functions, i.e., RACF or NACF, to negotiate the QoS-related parameters or to perform the proactive operations to perform a fast handover.

The handover procedure may be enhanced by proactively performing some of the network-layer handover operations before a link-layer handover is completed.

While the target network for handover is selected, UE may obtain the information to perform the proactive handover toward the target network. Proactive operations may reduce the handover latency required for the allocation of a new LID, authentication/authorization, and handover signalling between UE and HCFs. Issues concerning proactive handover operation are described in [b-ITU-T Q.1709].

Figure 65 shows high-level information flows for the handover preparation procedure.

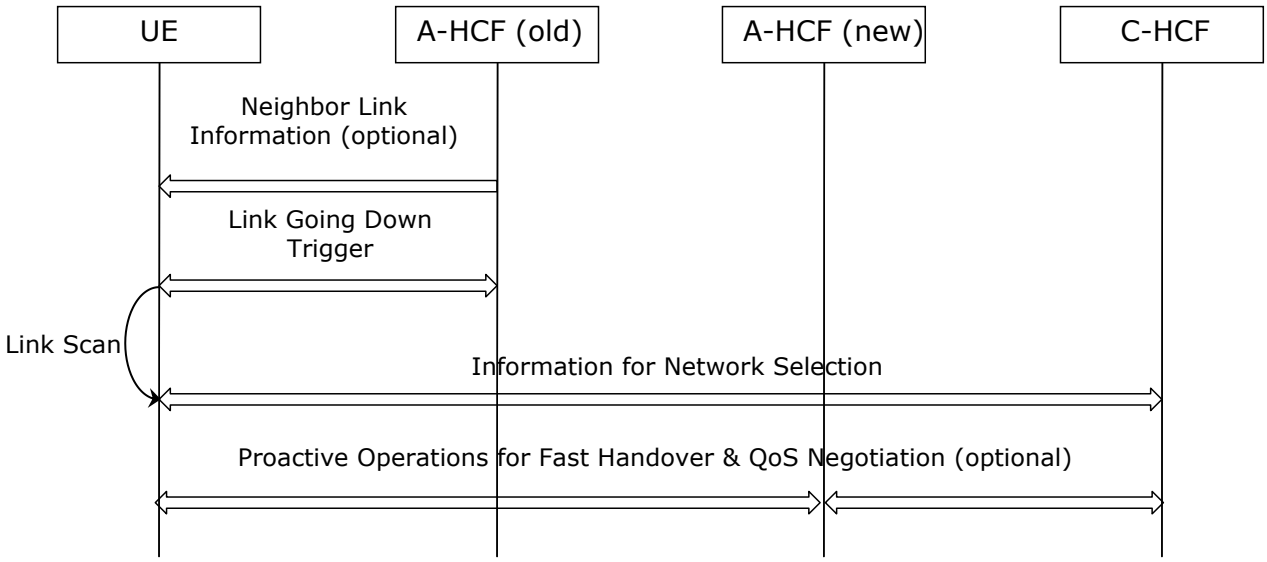


Figure 65 – Example of information flow for handover preparation procedure [b-ITU-T Q.1707]

When UE perceives an imminent disconnection, from the currently attached link, it scans all the accessible links (or networks) and selects one of those detected links as the target for a handover. Optionally, the information of adjacent links may be delivered from A-HCF to UE in order to reduce scanning latency, as shown in Figure 65. The link scanning process is performed with the support of a link-layer trigger.

In the selection of the target network, the necessary information may be exchanged between UE and C-HCF with additional support of A-HCFs. This network selection may be performed either via a UE-controlled procedure or through a network-controlled procedure. When the target network is selected, some proactive operations for fast handover and QoS negotiation may be performed. They depend on specific handover schemes.

Figure 65 illustrates the case of host-based handover control. If a network-based handover control procedure takes place, A-HCF may play the role of UE.

21.4.2 Handover execution

The handover execution phase starts by determining the necessary support of layer 3 (L3) handover control. UE (or HCF) checks whether a handover should be handled at L2 or at a higher layer; afterwards, it initiates the corresponding handover control procedures.

When UE moves within the same access-mobility management control function (A-MMCF) domain, it requires only the layer 2 (L2) handover control that is generally provided by each access technology. However, when UE moves between different A-MMCF domains (or different networks), it is further required to configure a new location ID (LID) and to invoke the subsequent location management procedure.

The configuration of a new location ID may be done using the state scheme, using the dynamic host configuration protocol (DHCP server), or the stateless (auto- or manual configuration) schemes. Specific handover schemes are associated with specific location ID configuration operations, i.e., a specific handover scheme may use a different scheme to configure the location ID.

During handover, HCF may trigger the L3 location management procedure by interworking with the associated LMF. This is done in order to reduce the handover detection latency, since HCF may usually detect the L3 handover event of UE earlier than LMFs.

A handover typically changes the data delivery path between the two UEs in a session. HCF adjusts the routing path from/to a UE according to the change of location by interworking with the core/access transport functions in NGN.

The network access authentication and authorization operations are required to mitigate the threats associated with unauthorized access. When UE turns on the power and it connects to an access network, an authentication is performed. Moreover, when UE performs a handover and it connects to the new access network, an authentication is also performed. Accordingly, an important factor related to the handover control for the seamless service is to reduce the delay time associated with the authentication during the handover procedure.

Figure 66 provides a high-level example of the information flow at handover execution.

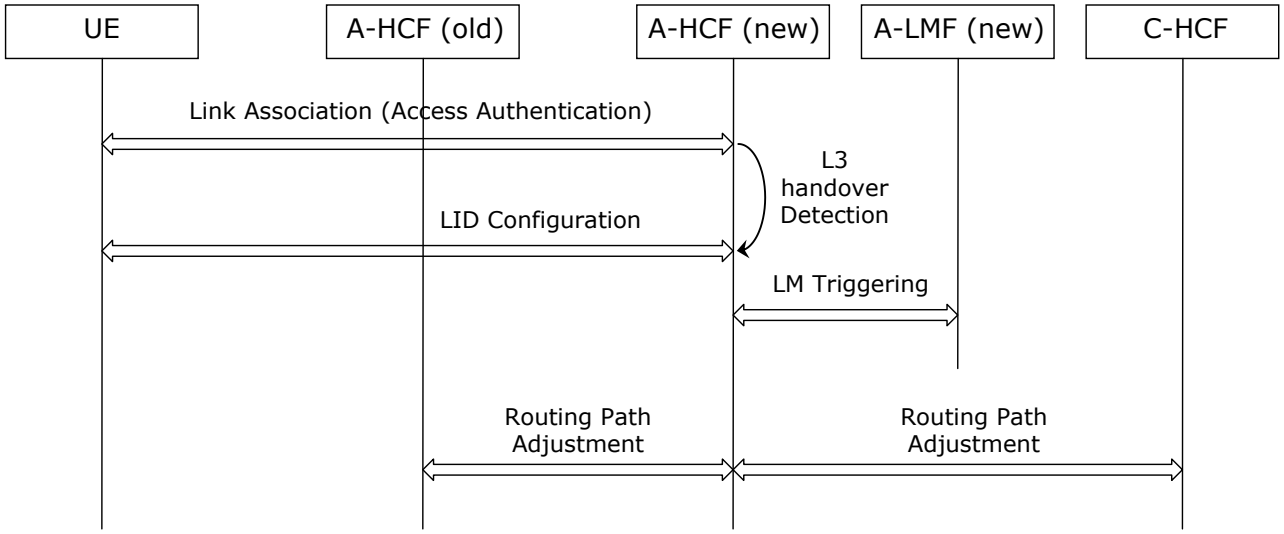


Figure 66 – Example of information flow for handover execution [b-ITU-T Q.1707]

As mentioned before, the handover execution operations such as handover detection, configuration of a new LID, routing path adjustment and authentication may be performed before the L2 handover is completed in order to improve the handover performance.

Handover signalling for routing path adjustment may be performed to establish the handover tunnel or to perform bicasting between the concerned network entities, therefore minimizing data loss and latency associated with the handover operation.

In the host-based handover control, UE is involved in the handover signalling operations; whereas in the network-based handover, a network agent concerned with A-HCF may perform and complete the handover signalling operations.

There are many types of handover in the network, such as vertical handover and horizontal handover, and also handover for the hierarchical and non-hierarchical network. The detailed information flows for those types of handover are described in [b-ITU-T Q.1709].

22 Conclusions

Mobile and NGN networks are presently world-wide deployed with conforming releases. Therefore, their mobility management (MM) mechanisms should be compatible with the present and future releases; in this way, networks and their corresponding user equipment (UE) may execute location management, handover, and roaming freely across networks and countries – paving the road towards ubiquitous networks.

MM procedures, nodes, reference points, identifiers, and interfaces are an integral part of these networks' infrastructures. SG13 in ITU-T, following the initiation of the nomadicity and mobility concepts in SG19, have concluded in the study period 2009-2012 a remarkable effort to adhere to NGN the MM capabilities to hurdle into the Future Network arena.

With the increasing provision of various radio and fixed accesses released to NGN and mobile networks alike, and their corresponding UEs, the complexity of MM mechanisms tend to increase. A fact additionally fuelled by the sequential and parallel new accesses between UE and the networks supporting the communication of a variety of new services. The new services involving mobility thus need to be explored in detail, in terms of MM, utilizing the standardization methods backing mobility and ubiquity features congruent to future networks and services such as the smart ubiquitous network (SUN) and cloud computing, among others.

This fact creates at least a two-dimensional vertical and horizontal composite environment, i.e., new services in one dimension, and new concurrent accesses in the other dimension. Reflecting this complexity in the MM procedures conveys to the integration of additional reference points, interfaces, identities, and related nodes managing location and mobility instances. Besides, it should be considered that enterprise market segments as well as vertical markets need new applications for their areas and industries, such as banking, health, manufacturing, machine-to-machine, education, real estate, government, etc.

ITU-T have started to cover some of these challenges by including MM interworking between heterogeneous access - 3GPP and non-3GPP - like Wi-MAX, WLAN, and UMTS, see for instance [b-ITU-T Y.2812]. In the new study period 2013-2016, The ITU-T MM set tool should continue developing robust MM mechanisms with compatibility and interoperability characteristics taking the above challenges into consideration.

It is important to bear in mind as well that the combination of enterprise market segments, vertical markets with their respective new services, and legacy services (including streaming) provide an exciting palette of variations provided to mobile users. Combinations of these services, sequentially or in parallel (supported by several active radio access technologies), imply that additional MM techniques from external forums might be used to organize and optimize the current ITU-T MM mechanisms, see [b-ITU-T Y.2027]. Among these mechanisms, there are the policy and charging control (PCC), IP flow mobility, and QoS, among others. Robust MM techniques might then evolve designed after new requirements drawn from real-time and non-real-time latency characteristics in those service combinations, blends of these services not considered previously.

Annex A

Mobility management for IP multicast in NGN

This annex provides excerpts from [b-ITU-T Y.2810] on the important topic of the mobile networks in the context of multimedia-streaming services, specifically covering personal broadcasting like video conferencing and Internet protocol television (IPTV) as some of the primary applications. These applications are based on group communications and IP multicast.

Multicast plays a particularly important role and possesses many distinct advantages in mobile environments because it enables scalable and global multimedia streaming services.

[b-ITU-T Y.2810] aims to develop a mobility management (MM) framework to support multicast communications in NGN by providing multicast-based services and their related MM capabilities needed to interoperate efficiently. These capabilities enable UE to receive multicast data continuously even while moving among different access networks.

Mobility management for IP multicast in NGN [b-ITU-T Y.2810] encompasses:

1 Design considerations
   a. Target applications and services,
   b. Generic network models:
      i. Separated transport model for multicast and unicast flows,
      ii. Unified transport model for multicast and unicast flows.
   c. Functional requirements.

2 Functional architecture for mobile multicast in NGN
   a. Service stratum:
      i. Mobile multicast capable service control functions,
      ii. Mobile multicast capable application support and service support functions.
   b. Transport stratum:
      i. Mobile multicast capable transport control functions,
      ii. Mobile multicast capable transport functions.
   c. Management functions,
   d. End-user functions.

3 Information flows for mobile multicast management
   a. Information flows for the separated transport model:
      i. Multicast receiver mobility:
         1 Multicast receiver joining procedure,
         2 Multicast receiver prune procedure,
         3 Multicast receiver handover procedure.
      ii. Multicast source mobility:
         1 Multicast source registration procedure,
         2 Multicast receiver joining procedure,
         3 Multicast source handover procedure,
         4 Multicast source prune procedure.
   b. Information flows for the unified transport model:
      i. Multicast receiver mobility:
         1 Multicast receiver joining procedure,
         2 Multicast receiver handover procedure,
         3 Multicast receiver prune procedure.
      ii. Multicast sender mobility:

1 Multicast source registration procedure,
2 Multicast source handover procedure,
3 Multicast source prune procedure.

4 Security considerations.

Only some of these topics are covered in the following clauses. For more details, see [b-ITU-T Y.2810].

A.1 Target applications and services

The typical understanding of mobile multicast services refers to a service provider supporting various multimedia services for a restricted user group in a mobile environment. A user joins the multicast-group to access services offered by the multicast source, see [b-ITU-T Y.2810]. Once the user is a member of the multicast group, a multicast delivery path is constructed between the multicast source and the user using a multicast protocol such as protocol-independent multicast (PIM). When leaving the multicast group, a user cannot receive any multicast traffic from the source. When a user moves to another network, the corresponding procedures, unlike the unicast service, should be followed for seamless multicast service. To satisfy these requirements, some technical issues different from those applied to the fixed network are considered.

In this context, [b-ITU-T Y.2810] supports the following IP-based multimedia multicast applications:

a) Multicast applications and/or services with receiver mobility, and

b) Multicast applications and/or services with source mobility.

A.1.1 Multicast applications and/or services with receiver mobility

Personal broadcasting is a service wherein the mobile multicast framework is applicable. The user acts as a multicast source, and other users who want to use the multicast service get source information, including group addresses, by online or offline advertisement, in order to provide the mobile multicast services, MM capabilities (including A-MMCFs and C-MMCFs) and interwork with multicast capabilities, such as multicast routers (MRs). After the users join the multicast group, they can receive multicast traffic from the source. The delivery path may be changed dynamically as handovers between the access networks occur, see Figure A.1 below. The mobile multicast framework may be adopted not only for a given service but for any application with multiple mobile receivers.

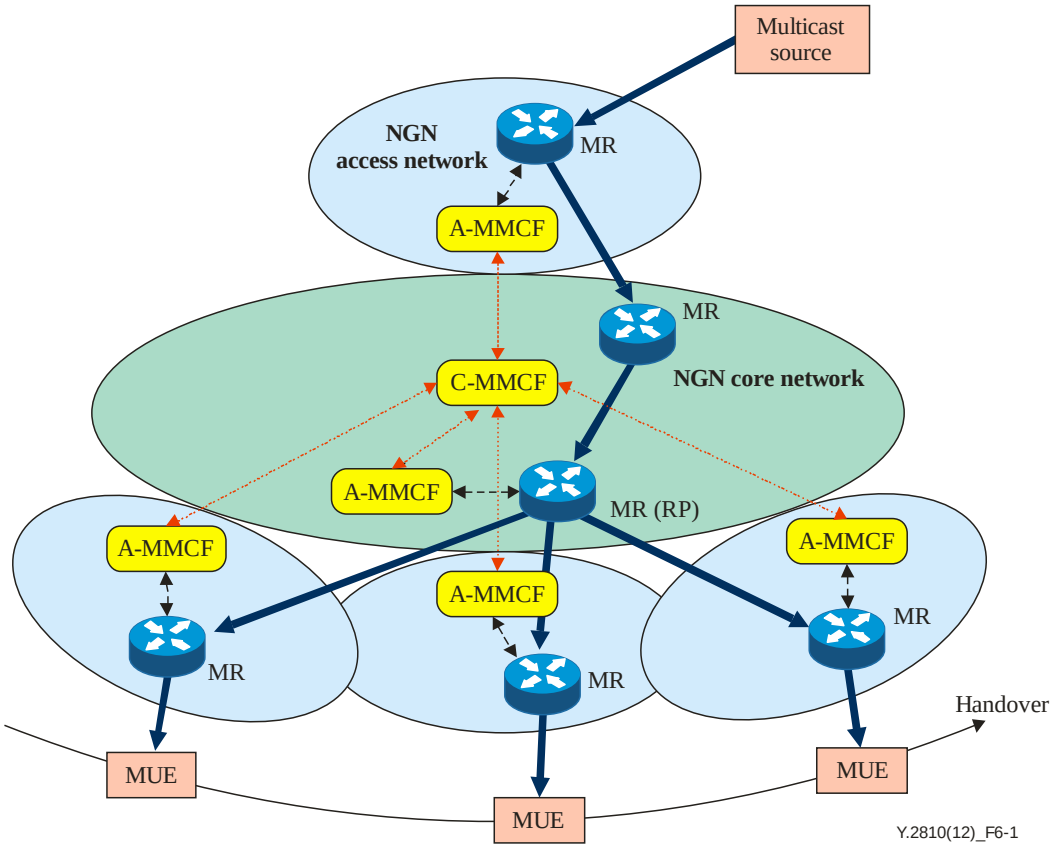


Figure A.1 – Multicast applications and/or services for receiver mobility [b-ITU-T Y.2810]

A.1.2 Multicast applications and/or services with source mobility

[b-ITU-T Y.2810] suggests to support the handover multicast source scenario, see Figure A.2 below, in applications such as video conferencing and mobile broadcasting, where the participating user may be both the multicast data sender and the receiver.

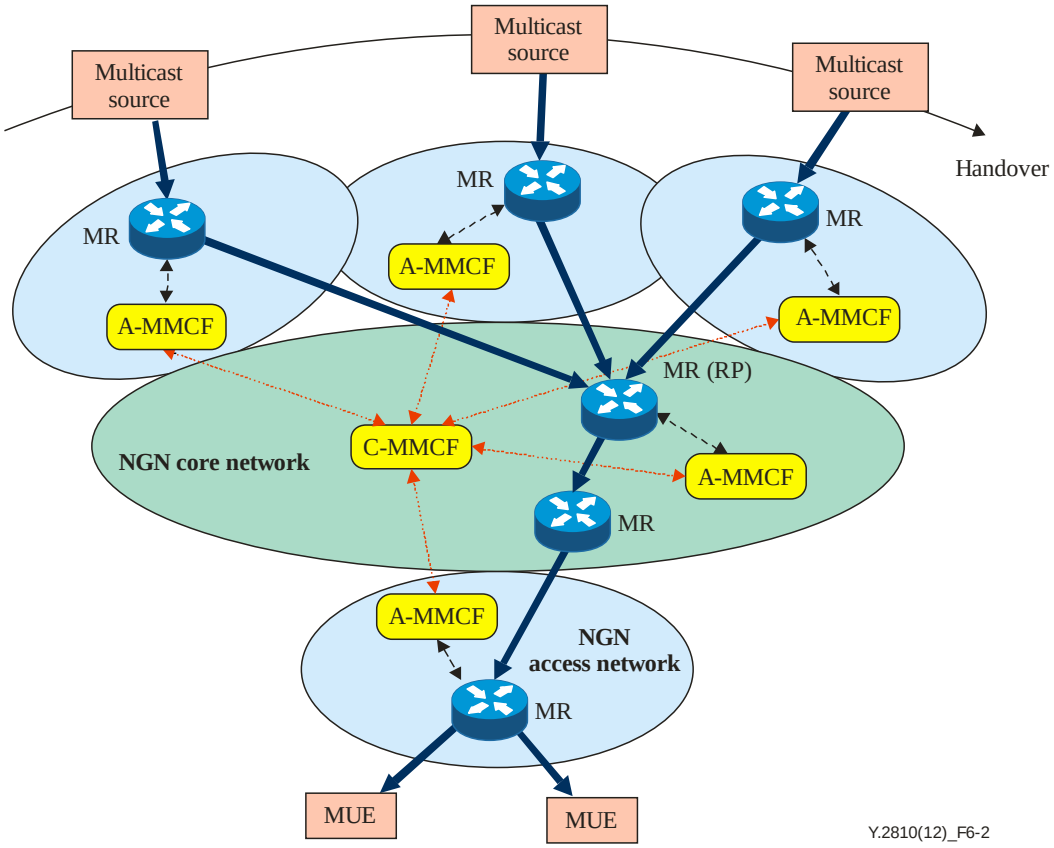


Figure A.2 – Multicast applications and/or services for source mobility [b-ITU-T Y.2810]

A.2 Multicast source handover procedure information flow for the unified transport model

Figure A.3 below describes the information flow for the multicast source handover procedure for the unified transport model.

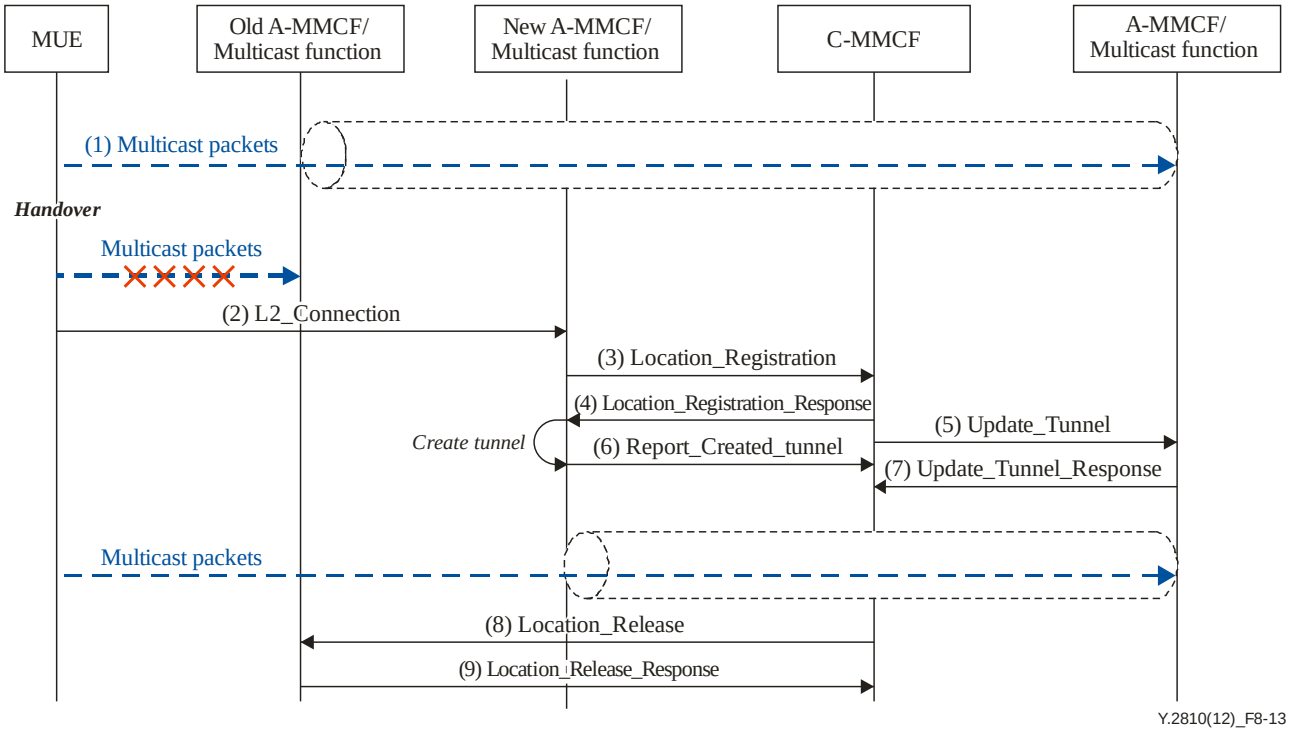


Figure A.3 – Multicast source handover procedure [b-ITU-T Y.2810]

Where:

1) UE (MUE in the figure) transmits multicast packets to NGN;

2) When UE moves to another network, it establishes L2_Connection to the new A-MMCF;

3) The new A-MMCF sends a Location_Registration message to C-MMCF to request the location registration of UE;

4) C-MMCF checks the information of UE and recognizes that UE is a multicast source, and that the multicast group has a receiver. Thus, C-MMCF sends a Location_Registration_Response message including the multicast source information to the new A-MMCF;

5) Likewise, C-MMCF sends an Update_Tunnel message including the multicast source information to the multicast function;

6) Upon receiving the Location_Registration_Response message, the new A-MMCF establishes a tunnel to the multicast function and sends the multicast packets through the created tunnel. After that, the new A-MMCF reports it to C-MMCF by sending a Report_Created_Tunnel message;

7) Meanwhile, the multicast function establishes a tunnel to the new A-MMCF and sends an Update_Tunnel_Response message to C-MMCF;

8) C-MMCF sends a Location_Release message to the old A-MMCF for the location release of UE. Upon receiving this message including the multicast source information of UE, the old A-MMCF deletes the tunnel used for the multicast packet transmission of UE;

9) The old A-MMCF sends a Location_Release_Response message to C-MMCF in response to the Location_Release message.

Other information flows related to handover, joining, prune, and registration procedures for multicast receiver mobility for the separated transport model are described in [b-ITU-T Y.2810].

Annex B

Further considerations for handover control in ITU-T

In this annex, additional issues on handover control in ITU-T are discussed. The topics were considered for further study within the scope of the Study Period 2009-2012.

B.1 Vertical handover

One of the major requirements when initiating the specifications for mobility management in NGN was to support mobility across a variety of heterogeneous access networks. Accordingly, handovers may be classified as follows:

1 Horizontal handover: A handover within homogeneous access networks.

2 Vertical handover: A handover across heterogeneous access networks.

The main concern of horizontal handover is to maintain ongoing service despite the change of location identifier (LID) due to the movement of UE. In vertical handover, the underlying access technology also changes together with the LID of UE. Thus, vertical handover needs to consider the change of network characteristics, e.g., link characteristics, MM protocol types, QoS factors, as well as the change of LID. The HC scheme for vertical handover also needs to consider multiple network interfaces used by a single UE. The link layer handover may be performed based on 'make-before-break' as well as 'break-before-make'. The details of vertical handover control are for further study. A comparison between horizontal and vertical handover is given in Table B.1, see [b-ITU-T Q.1709].

Table B.1 – Comparison between horizontal and vertical handover [b-ITU-T Q.1709]

	Horizontal handover	**Vertical handover**
Access technology	Homogeneous	Heterogeneous
Network interface	Single	Multiple

B.2 Inter-core network handover

The inter-CN handover represents the handover of UE to a different NGN network. In this type of handover, a number of issues on roaming agreement, authentication and authorization, agreement for handover support between the different NGN providers, among others, play an important role. The details of inter-CN handover are for further study.

Annex C

Practical scenarios for seamless handover using media independent handover (MIH)

This annex covers media independent handover (MIH) mechanisms to support and enhance mobility management in NGN networks. It covers:

1 Seamless real-time services with MIH, and

2 MIP-based handover based on media independent handover (MIH), including two sub-cases:

- a Network controlled handover, and
- b Terminal controlled handover.

C.1 Seamless real-time services with media independent handover (MIH)

Additional support is needed to realize faster handovers to allow seamless real-time services. Therefore, further practical scenarios are explored, in the framework of mobility management in NGN, where 2G/3G/long term evolution (LTE) in cellular networks, and WLAN (Wi-Fi and WiMAX) handovers also may take place. Specifically, IETF working groups like MIPv6 signalling and handoff optimization (MIPSHOP) have been involved in activities related to the use of mechanisms to reduce and eliminate signalling overhead and packet loss due to handover latency incurred by MIPv6. These related issues are taken as a whole into consideration since both link layer connectivity and layer 3 mobility management protocols interact at these two different layers for a number of purposes, i.e., new links configuration, router discovery, and exercise of new care-of-address, see [b-ITU-T Q.1709].

NOTE 1 – On the specific topic of WLAN-WiMAX mobility management, which describes a MM functional architecture to interact between WLAN and WiMAX. In such a framework, each access network is operated by different service providers. Specifically, IP mobility is supported among UEs moving between these two access networks and the interworking needed for mutual authentication between service providers.

NOTE 2 – Regarding WiMAX and UMTS mobility management interworking, [ITU-T Y.2812] describes a functional architecture to interwork between the two networks. [b-ITU-T Y.2812] strives to harmonize this interworking as part of the NGN infrastructure. A thorough analysis is offered therein. Thus refer to [b-ITU-T Y.2812] to consider the WiMAX and UMTS network component interactions in the context of the NGN MM functional architecture.

Intelligent terminals are frequently used to access the Internet while the user is moving. Handover thus becomes an important issue when users move across different access technologies, especially during active applications such as voice over IP (VoIP), video on demand (VoD), IP television (IPTV), etc. The mobile IP protocol can achieve service continuity across different IP networks, but some delay and packet loss are intrinsic to the procedures of the protocol.

Other standardization activities help to achieve faster mobile IP handovers. One important activity is the IEEE 802.21 media independent handover services standard. This standard provides lower layer enhancements to mobile IP for IEEE 802-based technologies to enable seamless handover.

From the user point of view, a terminal may be considered a multifunctional device with one or more of the following features: wireless phone, cloud terminal, PDA, camera, music player, web browser, TV service, global positioning system (GPS), etc. From a technical point of view, a terminal can be considered as a mobile device that supports an IP stack, and multiple wired or wireless access modes, e.g., radio frequency (RF) interfaces, Ethernet, and infrared. Terminals must provide seamless mobility with no application interruption as a user moves between heterogeneous technologies. Thus, an efficient mobility protocol is required to hand off services across such networks with minimal delay, minimal data loss, and minimal user perception of the event.

More specifically, mobile IP is essentially a layer 3 (L3) protocol for terminal mobility across IP networks. [b-IEEE 802.21] resides between layer 2 and layer 3. This protocol provides lower layer

support for terminal mobility across networks involving IEEE technologies such as [b-IEEE 802.11] (Wi-Fi), [b-IEEE 802.16] (WiMAX) and [b-IEEE 802.3] (Ethernet), as well as 3GPP.

Mobile IP is a well-known mobility protocol that maintains the network connection of a terminal despite changes in its network point of attachment. It supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. However, when a terminal moves to a different type of layer 1 (L1)/layer 2 (L2) connection, mobile IP by itself cannot achieve seamless handover, especially for real-time services, because of the latency in setting up the new L1/L2 connection. [b-IEEE 802.21] is a key lower layer enhancement for mobile IP in heterogeneous environments.

[b-IEEE 802.21] consists of a media independent handover function (MIHF), shown in Figure C.1, providing three services to achieve efficient handover decisions.

1 The event service (ES) notifies upper layer users about dynamic events such as link up, link down, link parameter change, etc.

2 The command service (CS) enables higher layers to control the L1 and L2 of the terminals. Examples include get status of link, scan for new link, switch link, etc.

3 The information service (IS) provides information about surrounding networks such as neighbour list technology, neighbour operator list, etc.

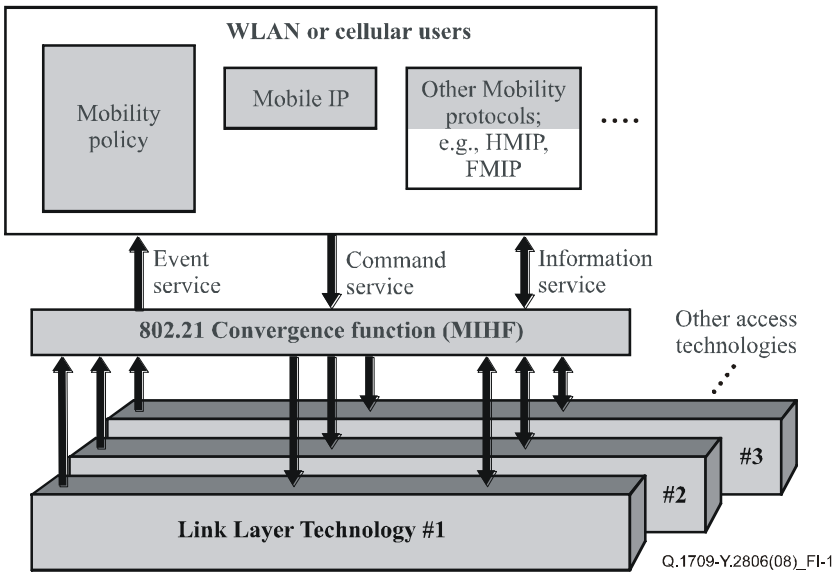


Figure C.1 – IEEE 802.21 MIH and mobile IP on different access technologies [b-ITU-T Q.1709]

Using this architecture, [b-IEEE 802.21] handover latency may be minimized to support real-time services by providing the following six standardized services to upper layer mobility protocols such as mobile IP:

1 Triggering fast detection (discovery) of neighbouring L2 networks of different technologies;

2 Detecting current L2 link status;

3 Informing quickly the upper layers of new L2 network point of attachment;

4 Allowing set-up of multiple L2 links for make-before-break handling;

5 Allowing quick teardown of unused L2 links; and

6 Allowing QoS parameter-mapping among different access technologies.

The overall result is faster handovers since the protocol specifically minimizes the time between link layer connection set-ups and mobile IP signalling.

Interaction between cellular networks and WLAN technology is one of the most important handover scenarios to be considered. 3GPP LTE defines the evolution of 3GPP cellular towards an "All IP" network. LTE employs new air interface technologies, such as orthogonal frequency division multiplexing (OFDM) and multiple-input multiple-output (MIMO) for higher throughput. Both mobile IPv4 and mobile IPv6 are supported in LTE. Detailed description of MIH signalling and data flows for WLAN-3GPP handovers can be found in other ITU-T MM framework Recommendations.

C.2 MIP-based handover based on media independent handover (MIH)

In this clause, two example scenarios are covered involving 3GPP LTE and WLAN network architectural configurations, based on the degree of IEEE 802.21 support in different network entities.

In the first scenario, the IEEE 802.21 network server manages the handover process with the support from the IEEE 802.21 peer in UE (network-controlled handover). In the second scenario, the handover is accomplished with total control by the IEEE 802.21 client in UE (terminal-controlled handover), with no IEEE 802.21 support anywhere else in the network.

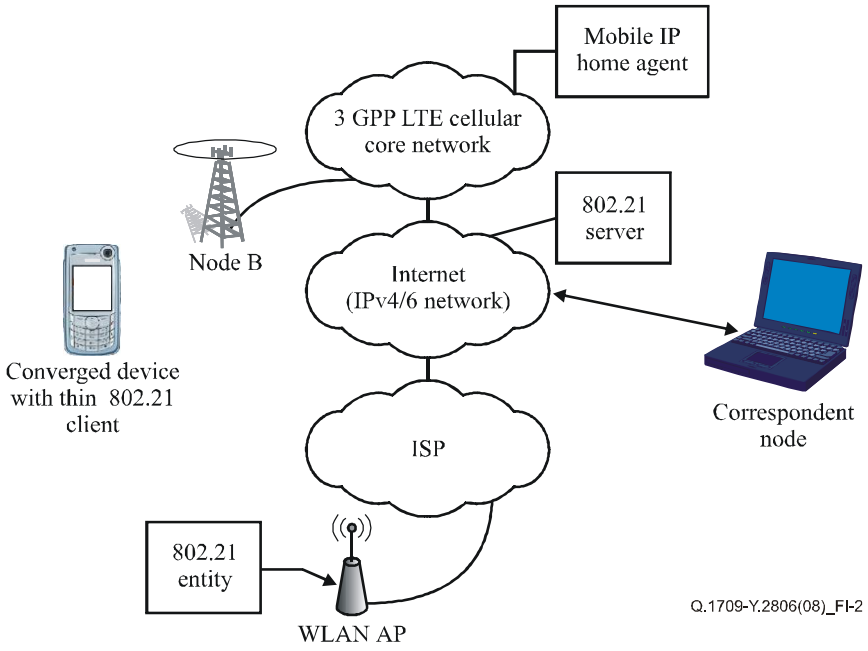


Figure C.2 – Handover between 3GPP and WLAN technologies based on media independent handover (MIH) [b-ITU-T Q.1709]

In the first scenario or network-controlled handover, the inter-system handover is completely controlled by the network. In this architecture, the terminal has a thin IEEE 802.21 client. The WLAN access point (AP) also has an IEEE 802.21 entity and connects to the Internet, IPv4 or IPv6, through the local Internet service provider (ISP). The 3GPP LTE cellular core network contains the mobile IP home agent and also connects to the Internet. Finally, also connected to the Internet is an IEEE 802.21 server that is easily accessible by both the WLAN and 3GPP LTE networks via IP. Note that the IEEE 802.21 server only needs IP connectivity to deliver its services. Hence, it could also be connected directly to the 3GPP LTE core network – for instance, as part of the IP

multimedia subsystem (IMS) platform, or to ISP. In addition, all messages between the IEEE 802.21 server and the terminal are carried over IP packets.

From the network IEEE 802.21 server, the terminal client IEEE 802.21 may be provided with information such as the neighbour list technology. The terminal client may then be asked by the IEEE 802.21 network server, via the command service, to scan the different technologies so as to identify the best possible L1/L2 network. In addition, event services, such as link going down or link detected, can be used to make efficient handover decisions. Specifically, the terminal can be asked to report these events to the IEEE 802.21 network server as a basis for making handover decisions. Finally, the command service such as switch link can be sent by the IEEE 802.21 network server to the terminal client to execute the L1/L2 handover.

In the second scenario or terminal controlled handover, the terminal contains a "smart" IEEE 802.21 client that fully controls the inter-technology handover process. The WLAN AP, via ISP, connects to the Internet, IPv4 or IPv6, which also has the 3GPP LTE cellular core network connected to it. The 3GPP LTE network also contains the mobile IP home agent. However, there are no IEEE 802.21 entities anywhere outside of UE.

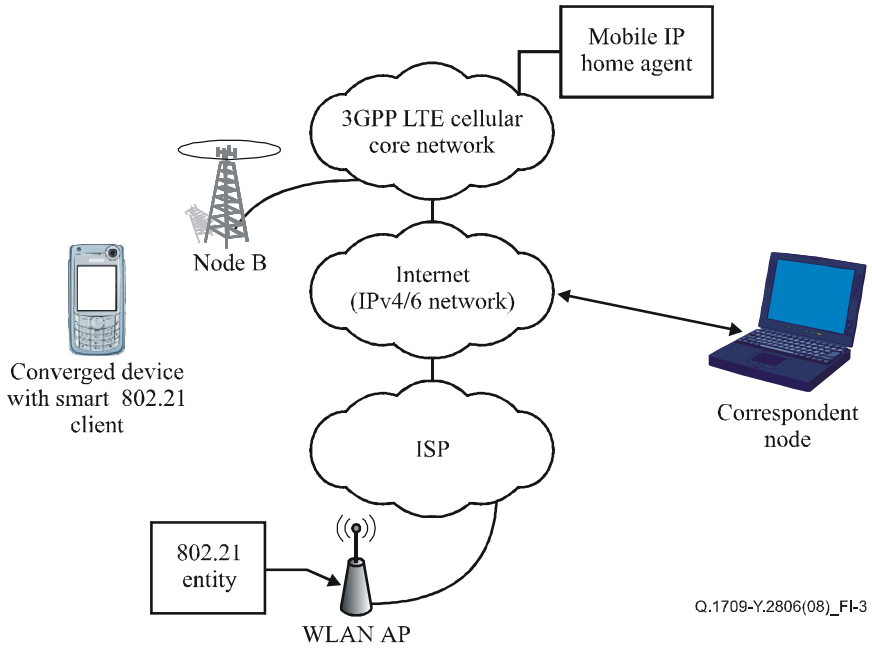


Figure C.3 – Terminal controlled handover between 3GPP and WLAN technologies [b-ITU-T Q.1709]

In this architecture, all the IEEE 802.21 services are generated locally and are exchanged between the different layers of UE. Upper layer command services can be used to gather link status using the get status command. Lower layers can report new link detection with the Link_Detected event or can relay predictive events about link degradation with the Link_Going_Down event service. These services are locally provided within the terminal without any service support from an IEEE 802.21 network entity.

Both scenarios above highlight the importance of "All IP" networks, such as 3GPP LTE mobile and WLAN networks. They require the interaction of mobility protocols at different layers to achieve seamless handovers across heterogeneous networks. While mobile IP supports mobility at the network level, the IEEE 802.21 standard provides standardized L1/L2 enhancements, which enables

faster inter-technology handovers. [b-IEEE 802.21] may thus complement mobile IP for mobile and WLAN mobility.

Annex D

Advanced issues for handover control

This annex covers the following techniques to support and enhance mobility management in NGN networks, see [b-ITU-T Q.1709]. It covers:

1 Authentication procedure for fast handover,

2 Policy-based handover control, and

3 Fast handover control for multi-interfaced UE.

D.1 Authentication procedure for fast handover

Network access authentication and authorization capabilities may be added to the NGN MM scenarios to mitigate threats associated with unauthorized access. They verify the identities and determine whether access should be granted to customer premises equipment (CPE) and customer premises equipment – border element (CPE-BE) requesting network connectivity to NGN.

When UE turns on the power and initially connects to an access network, an authentication procedure is performed. When UE performs the handover to new access network, the authentication procedure is also performed. The handover of UE between different access networks incurs into a time delay that includes the re-authentication procedure. Many discussions took place around the key issue of MM for seamless service offer to reduce the delay due to the authentication procedure during handover. There are various methods to reduce such delay.

For example, when the pre-authentication method performs the authentication procedure before the UE moves. UE requests its pre-authentication to neighbouring access functions, thus each neighbouring access function performs a pre-authentication procedure in advance. The pre-authentication method shall be optional to reduce the time delay of the authentication during handover.

There are two approaches in the pre-authentication method for handover:

1 Pre-authentication method via AAA server, and

2 Pre-authentication method using context transfer.

Refer to Figures II.1 to II.3 in [b-ITU-T Q.1709] to consider the network-based MM as well as the host-based MM. In details, Figure II.1 shows the pre-authentication procedure via the AAA server for fast handover. At first, UE requests its handover in advance to the old A-MMCF, the old A-MMCF responds with candidates for new A-MMCF. Then, UE requests pre-authentication to the AAA server via the new A-MMCF. The AAA server performs the pre-authentication procedure. After the pre-authentication of UE, UE can move to the new A-MMCF without incurring into a time delay.

The context transfer method may be considered as the alternative method for fast authentication. The authentication contexts of UE may be transferred from the AAA server to the relevant MMCFs. Thereafter, the authentication process for UE may be performed by MMCFs using the authentication contexts received from either the AAA server or neighbouring MMCFs.

The pre-authentication method using context transfer consists of two cases, see clause II.1 of [b-ITU-T Q.1709] for further details. These are considered in case the handover of UE occurs within the same core network.

Figure II.2 in [b-ITU-T Q.1709] shows one of the pre-authentication procedures using context transfer for fast handover. In this case, the central HC-FE (CHC-FE) in C-MMCF substitutes for the function of AAA server. The authentication contexts of UE may be transferred from the AAA server to C-MMCF during initial authentication procedure. Thereafter, CHC-FE in C-MMCF helps the authentication process for UE by using the received contexts in case UE moves to another

network region within the same core network. For this, C-MMCF needs to have the function that stores the information about UE received from the AAA server.

Figure II.3 in [b-ITU-T Q.1709] shows another pre-authentication procedure using context transfer for fast handover. In this case, the access HC-FE (AHC-FE) in A-MMCF substitutes the function of AAA server. The authentication contexts of UE may be transferred from the AAA server to C-MMCF during the initial LBU procedure. If the information of a new A-MMCF can be provided to C-MMCF in the process where UE starts the handover through the old A-MMCF, the authentication context of UE may be transferred from C-MMCF to the new A-MMCF. Thereafter, AHC-FE in the new A-MMCF helps the authentication process of UE by using the received contexts, in case UE moves to another network region within the same core network. For this, A-MMCF needs to have the function that stores the information about UE received from C-MMCF. This mechanism accelerates the authentication process for UE's handover, by reducing the signalling latency between UE and the AAA server.

D.2 Policy-based handover control

NGN may have many access networks and UE may want to access the best network for a specific service. The policy-based handover control relates to network selection and handover decision. The network selection and handover decision may be controlled by a user/operator policy. The core network in NGN may have a policy entity. [b-ITU-T Y.2111] defines the policy decision functional entity (PD-FE) and the policy enforcement functional entity (PE-FE) to support QoS. These identities may be extended for mobility management policy usage. For more details on the architecture, see [b-ITU-T Y.2027].

PD-FE, which is placed at the service/transport control function in the core network, decides the policy rules, handles network selection for UE, and triggers the handover. PE-FE, which is placed at UE, triggers handover and performs handover according to the received policy rules.

The HC procedure is divided into two cases:

1 Host-based handover, and

2 Network-based handover.

In the host-based handover, UE triggers a handover based on the received signal strength or QoS level required for a particular service. In the network-based handover, the network, i.e., A-MMCF, triggers a handover based on current network states such as traffic load or operator's policies. These details for policy-based handover in the context of MM were proposed for further study in the ITU-T Study Period 2009-2012.

D.3 Fast handover control for multi-interfaced UEs

UE may have multiple interfaces to maintain continuous and wide area network connectivity. Depending on the user preference or network environment, only one interface or multiple interfaces may be used in parallel, see [b-ITU-T Y.2027] for more information on these types of multiple-radio access technology scenarios. The multiple interfaces in UE can be utilized efficiently to minimize the handover delay. 'Make-before-break' handover can be achieved by activating a new interface before breaking from the current active interface.

If multiple interfaces are active and simultaneously used for data traffic delivery, the data traffic from an interface may be handed over to another active interface. However, if only one interface is active at one time, at least one of the other interfaces may be prepared to receive the data traffic seamlessly, as fast as possible after detecting that the current active interface is about to go down. The preparation in this context may include TLID (IP address) allocation, LID binding update, and data tunnel creation, which allow for a fast handover by just switching one data tunnel to the other one.

Clause II.3 of [b-ITU-T Q.1709] presents an example scenario of UE with two interfaces. In the example, one interface (active) is used to deliver the data traffic while the other one (standby) is just prepared to deliver the data traffic when the active interface is about to go down.

The flow in Figure II.4 of [b-ITU-T Q.1709] shows the case in which a data tunnel for UE is established between two endpoints controlled by CHC-FE and AHC-FE (case 1). For each interface, the procedure is the same as in Figure 7-2 of [b-ITU-T Q.1709]. The difference from Figure 7-2 of [b-ITU-T Q.1709] consists in that the LBU procedure and tunnel set-up are done for each interface.

To simplify the description, the tunnel endpoints are illustrated as HC functional entities (HC-FEs) in Figure II.4 of [b-ITU-T Q.1709], where the real endpoints of a tunnel are NGN transport functions controlled by those HC-FEs. This simplification is applied to all the figures presented in clause II.3 of [b-ITU-T Q.1709].

Figure II.5 of [b-ITU-T Q.1709] shows the case in which a data tunnel for UE is established between UE and an endpoint controlled by CHC-FE (case 2). For each interface, the procedure is the same as in Figure 7-3 of [b-ITU-T Q.1709]. The difference from Figure 7-3 of [b-ITU-T Q.1709] consists in that the LBU procedure and tunnel set-up are done for each interface.

Figure II.6 of [b-ITU-T Q.1709] illustrates an information flow to control UE's handover between two A-MMCFs' regions for UEs with multiple interfaces. It describes the case in which two data tunnels are established for UE between an endpoint controlled by CHC-FE and AHC-FE1 and also between an endpoint controlled by CHC-FE and AHC-FE2 (case 1). If an active interface (interface 1 in the example of clause II.3 of [b-ITU-T Q.1709]) goes down, one of the standby interfaces (interface 2 in the example) goes up to become an active interface. If the previous active interface (interface 1) is attached to the other access network (ALM-FE3), UE proceeds with the LBU procedure to set up a tunnel between the endpoints controlled by AHC-FE3 and CHC-FE.

Figure II.7 of [b-ITU-T Q.1709] shows another information flow for UEs with multiple interfaces. It represents the case in which two data tunnels for UE are established through each interface between UE and an endpoint controlled by CHC-FE (case 2). If an active interface (interface 1 in the example of clause II.3 of [b-ITU-T Q.1709]) goes down, one of the standby interfaces (interface 2 in the example) goes up to become an active interface. If the previous interface (interface 1) is attached to the other access network (ALM-FE3), UE proceeds with the LBU procedure to set up a new tunnel between UE and CHC-FE.

Bibliography

Note - At the time of publication, the editions indicated below were valid. All these references are subject to revision; therefore, users of this technical paper are encouraged to investigate the possibility of applying the most recent edition of the references listed below.

[1] [b-ITU-T E.164] Recommendation ITU-T E.164 (2005), The international public telecommunication numbering plan.

[2] [b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), Mobility management requirements for NGN.

[3] [b-ITU-T Q.1707] Recommendation ITU- T Q.1707/Y.2804 (2008), Generic framework of mobility management for next generation networks.

[4] [b-ITU-T Q.1708] Recommendation ITU-T Q.1708/Y.2805 (2008), Framework of location management for NGN.

[5] [b-ITU-T Q.1709] Recommendation ITU-T Q.1709/Y.2806 (2008), Framework of handover control for NGN.

[6] [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), Functional requirements and architecture of next generation networks.

[7] [b-ITU-T Y.2027] Recommendation ITU-T Y.2027 (2012), Functional architecture of multi-connection.

[8] [b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), Terms and definitions for next generation networks.

[9] [b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), Resource and admission control functions in next generation networks.

[10] [b-ITU-T Y.2809] Recommendation ITU-T Y.2809 (2011), Framework of mobility management in the service stratum for next generation networks.

[11] [b-ITU-T Y.2810] Recommendation ITU-T Y.2810 (2012), Mobility management framework for IP multicast communications in next generation networks.

[12] [b-ITU-T Y.2811] Recommendation ITU-T Y.2811 (2012), Framework for the mobile virtual private network service in next generation networks.

[13] [b-ITU-T Y.2812] Recommendation ITU-T Y.2812 (2012), Mobility management for interworking between WiMAX and UMTS.

[14] Draft Recommendation ITU-T Y.MM-MD, Mobility Management Framework for Communications between Users with Multiple Terminal Devices.

[15] Draft Recommendation ITU-T Y.MM-WAW, Mobility Management for Interworking between WiMAX and WLAN.

[16] [b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.

[17] [b-ETSI 121.905] LTE, Vocabulary for 3GPP Specifications, version 11.3.0 Release 11.

[18] [b-ETSI TS 123 002] LTE, Network architecture, version 11.6.0 Release 11.

[19] [b-ETSI TS 123 003] Numbering, addressing and identification, version 11.8.0 Release 11

[20] [b-ETSI 123 008] Organization of subscriber data, version 11.9.0 Release 11.

[21] [b-ETSI 123 060] General Packet Radio Service (GPRS); Service description; Stage 2, version 10.12.0 Release 10.

[22] [b-ETSI 123 122] Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode, version 11.4.0 Release 11.

[23] [b-ETSI 123 203] Policy and charging control architecture, version 11.9.0 Release 11

[24] [b-ETSI 123.216] Single Radio Voice Call Continuity (SRVCC); Stage 2, version 11.10.0 Release 11.

[25] [b-ETSI 123.221] Architectural requirements, version 11.2.0 Release 11.

[26] [b-ETSI 123.234] 3GPP system to Wireless Local Area Network (WLAN) interworking; System description, version 11.0.0 Release 11.

[27] [b-ETSI 123.271] Functional stage 2 description of Location Services (LCS), version 9.8.0 Release 9

[28] [b-ETSI 123.401] LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, version 11.8.0 Release 11

[29] [b-ETSI 123.402] Architecture enhancements for non-3GPP accesses, version 11.8.0 Release 11

[30] [b-ETSI 124.002] Public Land Mobile Network (PLMN) Access Reference Configuration, version 11.0.0 Release 11.

[31] [b-ETSI 124.008] Organization of subscriber data, version 11.9.0 Release 11

[32] [b-ETSI 124.301] Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, version 11.9.0 Release 11

[33] [b-ETSI 125.304] User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode, version 11.5.0 Release 11.

[34] [b-ETSI 125.331] Radio Resource Control (RRC); Protocol specification, version 11.9.0 Release 11

[35] [b-ETSI 125.410] UTRAN Iu interface: General aspects and principles, version 11.0.0 Release 11.

[36] [b-ETSI 129.002] Mobile Application Part (MAP) specification, version 11.9.0 Release 11

[37] [b-ETSI 129.272] LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol, version 11.9.0 Release 11

[38] [b-ETSI 129.274] LTE; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3, version 11.9.0 Release 11.

[39] [b-ETSI 133.401] LTE; 3GPP System Architecture Evolution (SAE); Security architecture, version 11.7.0 Release 11

[40] [b-ETSI 136.300] LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2, version 11.9.0 Release 11.

[41] [b-ETSI 136.401] Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Architecture description, version 11.2.0 Release 11.

[42] [b-ETSI 136.413] LTE, Evolved Universal Terrestrial Access Network (E-UTRAN); S1 Application Protocol (S1AP), version 11.6.0 Release 11.

[43] [b-3GPP TS 43.051] 3GPP TS 43.051, Technical Specification Group GSM/EDGE Radio Access Network; Overall description, Stage 2.

[44] [b-ETSI 148.002] Base Station System - Mobile-services Switching Centre (BSS - MSC) interface; Interface principles, version 11.0.0 Release 11

[45] [b-IEEE 802.3] IEEE 802.3

[46] [b-IEEE 802.11] IEEE 802.11

[47] [b-IEEE 802.16] IEEE 802.16

[48] [b-IEEE 802.21] IEEE 802.21 (2008), IEEE Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover.

[49] [b-IETF RFC 768] IETF RFC 768 (1980), User Datagram Protocol.

[50] [b-IETF RFC 3588] IETF RFC 3588 (2003), Diameter Base Protocol.

[51] [b-IETF RFC 4960] IETF RFC 4960 (2007), Stream Control Transmission Protocol.