International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2018

(09/2009)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Mobility management and control framework and architecture within the NGN transport stratum

Recommendation ITU-T Y.2018

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2018

Mobility management and control framework and architecture within the NGN transport stratum

Summary

Recommendation ITU-T Y.2018 specifies the architecture and functional requirements for the management of logical location information, as defined in Recommendation ITU-T Q.1707 and control of mobility in the NGN transport stratum. It addresses all types of device mobility as defined in Recommendation ITU-T Q.1706. It draws heavily from Recommendations ITU-T Q.1707, ITU-T Q.1709, and ITU-T Q.1708, but maps their content into the framework provided by Recommendation ITU-T Y.2012.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2018	2009-09-12	13

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2018

Mobility management and control framework and architecture within the NGN transport stratum

1 Scope

This Recommendation describes an architecture of mobility management and control functions (MMCFs) for the NGN transport stratum. This architecture includes the definitions of the functional entities of MMCF and the scenarios for interactions with the other NGN functional components: NACF, RACF, SCF and the access and core transport functional blocks within the forwarding plane. This Recommendation considers the types of mobility management described in [ITU-T Q.1706]. This version of the Recommendation is limited to mobility of a single device, as opposed to the movement of sessions from one device to another (session mobility). It is further limited, as indicated by the Recommendation title, to support of IP-based mobility in the transport stratum. In this it differs from [ITU-T Q.1707] in that the latter also considers support of mobility in the service stratum. This Recommendation provides mechanisms to achieve seamless mobility if network conditions permit, but does not provide any mechanism to deal with service adaptation if the post-handover quality of service is degraded from the quality of service before handover.

This Recommendation uses the term "location information". That information is currently limited to logical location information as defined by clause 6.3.2 of [ITU-T Q.1707]. The management of physical (geographic) location information is for further study.

This Recommendation assumes that mobility is a service, explicitly specified by parameters in the user service profile. This Recommendation makes no assumption as to whether the mobility service parameters are located in the transport user profile or the service user profile, but assumes that they are accessible to the functional entities that need to use them.

This Recommendation is not dependent on specific access technologies, and supports handover across different technologies.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.1706] Recommendation ITU-T Q.1706 /Y.2801 (2006), *Mobility management requirements for NGN.*

[ITU-T Q.1707] Recommendation ITU-T Q.1707/Y.2804 (2008), *Generic framework of mobility management for next generation networks.*

[ITU-T Q.1708] Recommendation ITU-T Q.1708/Y.2805 (2008), *Framework of location management for NGN.*

[ITU-T Q.1709] Recommendation ITU-T Q.1709/Y.2806 (2008), *Framework of handover control for NGN.*

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*

[ITU-T Y.2014]	Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks*.
[ITU-T Y.2111]	Recommendation ITU-T Y.2111 (2008)*, Resource and admission control functions in next generation networks*.
[IETF RFC 4282]	IETF RFC 4282 (2005), *The Network Access Identifier*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 handover [ITU-T Q.1706].

3.1.2 seamless handover [ITU-T Q.1706].

3.1.3 service continuity [ITU-T Q.1706].

3.2 Terms defined in this Recommendation

NOTE – For convenience, this Recommendation uses the terms "mobility" and "mobile UE" to imply service continuity at a minimum, with the intent to achieve seamless handover. This is explicitly contrasted with nomadicity, although the latter is included in the broader definition of [ITU-T Q.1706].

This Recommendation defines the following terms:

3.2.1 access service authorizer: A network operator that authenticates a UE and establishes the UE's authorization to receive Internet service.

3.2.2 access service provider: The operator of the access network to which the UE is attached.

3.2.3 adaptive QoS resource management: The network capability which may afford dynamic QoS assurance to mobile UE according to network capability, user preference and service administration policies during handover. With this capability, the network may dynamically change the QoS resources granted to the individual flows of a session upward or downward within the range set by the application.

3.2.4 anchor point: A location in the forwarding plane above which movement of the terminal equipment within a certain topological scope is masked by the provision of mobility service at layer 3. "Above" means "on the side away from the user equipment (UE)". There may be more than one anchor point on the path between the UE and a correspondent entity.

3.2.5 anchoring network: The network within which an anchor point resides.

3.2.6 candidate access point (or network): An access point or network being evaluated as a possible new point of attachment (new serving access network) after handover.

3.2.7 handover latency: A delay in delivery of user data during handover due to the use of buffering as part of the handover procedure.

3.2.8 handover quality: The degree of impairment experienced by the user during the period of handover. This can range from cut-off (loss of service continuity) to a degree of impairment unnoticeable by most users. The latter condition is taken as the working definition of seamless handover.

3.2.9 host-based mobility: A mode of operation whereby the mobile UE takes an active role in the provision of mobility service at layer 3, in particular by contacting the mobile service provider directly to invoke this service after gaining network access.

3.2.10 integrated scenario: A scenario in which the same AAA infrastructure is used to authorize both transport and mobility service, so that a common set of user credentials is used to gain access to both services.

3.2.11 mobility service authorizer: A network operator that authenticates a UE and establishes the UE's authorization to receive mobility service. It is assumed in the network-based case that this authorization covers the affected components both in the anchoring network and in the access network.

3.2.12 mobility service provider: A network operator that provides mobility service. In the case of network-based mobility, this term refers specifically to the operator of the anchoring network, taking note that the access service provider is actually the operator of the equipment providing the tunnel lower end.

3.2.13 network-based mobility: A mode of operation whereby the mobile UE does not take an active role in the provision of mobility service at layer 3.

3.2.14 post-handover quality of service: The quality of service experienced after any transient conditions due to handover have passed.

3.2.15 proactive QoS reservation: Reservation of QoS resources in advance of handover.

3.2.16 serving access point (or network): The access point (or network) providing service to the UE before handover.

3.2.17 split scenario: A scenario in which mobility service is authorized by a separate AAA infrastructure from that which authorizes transport service. Thus, in general two sets of user credentials are required to complete the authorization process. This Recommendation assumes that the credentials for mobility service are obtained from the UE during the network attachment process, but leaves the details to other Recommendations.

3.2.18 target access point (or network): An access point or network which has been selected as the intended new point of attachment (new serving access network) after handover.

3.2.19 tunnel: An IP-in-IP tunnel as provided by the various varieties of mobile IP.

3.2.20 tunnel lower end: The end of the tunnel closest to the UE.

3.2.21 tunnel upper end: The end of the tunnel furthest from the UE, coinciding with the anchor point.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4.1 Functions

HCF	Handover Control Functions
HDF	Handover Decision Function
L2HCF	Layer 2 Handover Control Function
L3HCF	Layer 3 Handover Control Function
L3HEF	Layer 3 Handover Execution Function

4.2 Functional entities

ABG-FE	Access Border Gateway Functional Entity
AM-FE	Access Manager Functional Entity

AN-FE	Access Node Functional Entity
AR-FE	Access Relay Functional Entity
EN-FE	Edge Node Functional Entity
HDC-FE	Handover Decision and Control Functional Entity
HGWC-FE	Home Gateway Configuration Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
L2HE-FE	Layer 2 Handover Execution Functional Entity
MLM-FE	Mobile Location Management Functional Entity
NAC-FE	Network Access Configuration Functional Entity
NID-FE	Network Information Distribution Functional Entity
NIR-FE	Network Information Repository Functional Entity
PD-FE	Policy Decision Functional Entity
PE-FE	Policy Enforcement Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TLM-FE	Transport Location Management Functional Entity
TRC-FE	Transport Resource Control Functional Entity
TRE-FE	Transport Resource Enforcement Functional Entity
TUP-FE	Transport User Profile Functional Entity

4.3 Functional blocks

A-MMCF	MMCFs as they relate to the network providing access to the UE and to the lower tunnel end-point
C-MMCF	MMCFs as they relate to the mobile subscriber's home network and to the upper tunnel end-point
MMCF	Mobility Management Control Functions
NACF	Network Attachment Control Functions
RACF	Resource Admission and Control Functions
SCF	Service Control Function
TF	Transport Functions

NOTE – The TF are sub-components of the access transport and core transport blocks respectively. No functional entities are specified within the TF themselves.

4.4 Other

AAA	Authentication, Authorization, and Accounting.
HMIPv6	Hierarchical Mobile IP for IP version 6. See [b-IETF RFC 4140].
MIPv4	Mobile IP for IP version 4. See [b-IETF RFC 3344].
MIPv6	Mobile IP for IP version 6. See [b-IETF RFC 3775].
MLM-FE(C)	An instance of the MLM-FE performing the Central mobile location management role.

MLM-FE(P)	An instance of the MLM-FE performing the Proxy mobile location management role.
PMIPv6	Proxy mobile IP. See [b-IETF RFC 5213].
UE	User equipment

5 Conventions

May: In this Recommendation, "may" is a normative term indicating an optional condition or behaviour.

Can: In this Recommendation, "can" is an informative term indicating a condition or behaviour that will potentially be encountered within the environment to which this Recommendation applies.

6 Architecture model and concepts

6.1 General concepts

Figure 1 shows the incremental high-level functional architecture required for mobility management and control in the NGN transport stratum. Details of the general NGN architecture have been omitted to bring out the relevant points.

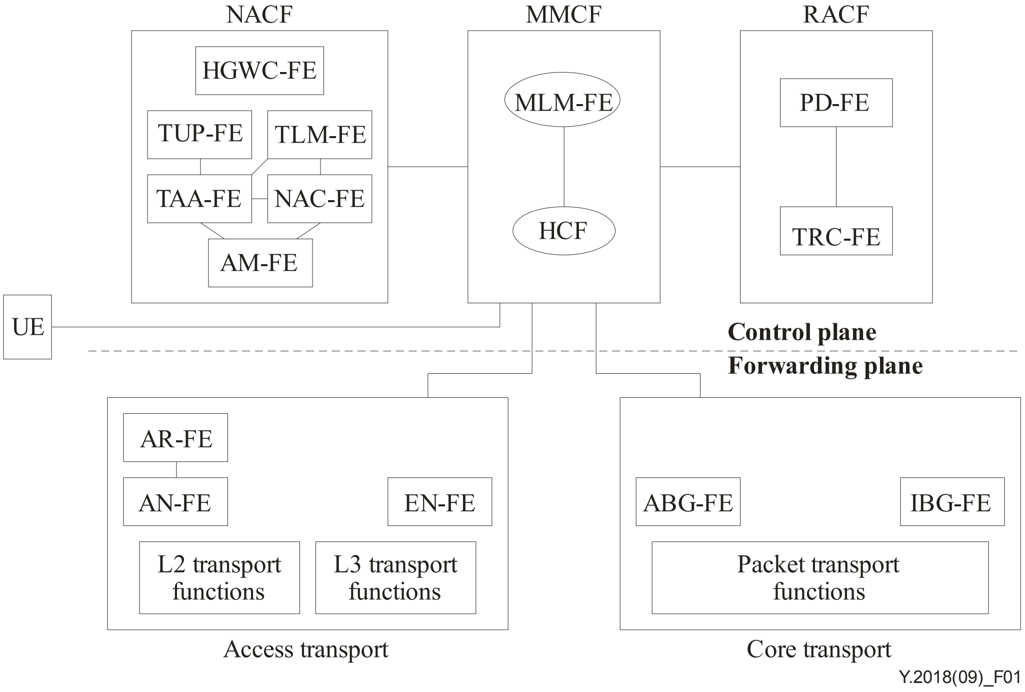


Figure 1 – Position of mobility management and control in the NGN transport stratum architecture

The mobility management and control function (MMCF) shown in Figure 1 is divided into two major functions: mobile location management and handover control.

The handover control functions (HCF) are used to provide session continuity for ongoing sessions of the moving UE. To provide good handover quality, the handover control operations must minimize data loss and handover latency during the handover of the UE.

Appendix I describes at a high level the application of the MMCF to a number of handover scenarios.

6.2 IP mobility management selection principles

The mobility mechanisms supported within an NGN operator's network and that of its roaming partner depend upon operator choice.

6.2.1 Static configuration of mobility mechanism

A statically configured mobility mechanism may be specific to the access type and/or roaming agreement. The information about the mechanism to be used in such a scenario is expected to be provisioned into the UE and the network. Mobility service with session continuity may not be possible if there is a mismatch between what the UE expects and what the network supports. For example, if a network only supports a host-based mobility protocol and the UE does not support it, mobility is not supported for the UE.

6.2.2 Dynamic configuration of mobility mechanism

If the network is able to support multiple IP mobility management mechanisms, the appropriate mechanism must be selected upon initial attachment and when handover occurs. Two cases are identified:

a) UE and network support a common mobility management mechanism:

In this case, one or more mobility management mechanisms may be supported by both UE and network. The choice of which one to use is determined by the operator's policy. This may be done as follows:

- If the UE indicates support of network-based mobility only and the network supports network-based mobility, then a network-based mobility protocol is used for providing connectivity, and persistent IP address preservation is provided.
- If the UE indicates support of both network-based and host-based mobility, the operator's policy decides which one will be used.

One possible way to indicate IP mobility mechanisms to be supported in the UE and network is through the AAA process, but the detailed mechanism for indicating the mobility mechanism is out of scope of this Recommendation.

b) UE and network do not support a common mobility mechanism, or UE support is not indicated:

In this case, there are two choices for the network, depending on the operator's policy: reject network access for the UE or enforce network-based mobility.

6.3 High level functions

6.3.1 Network attachment control functions (NACF)

6.3.1.1 Network access authentication

When a UE establishes a connection to an NGN access network, the user authentication and authorization procedure will be performed for the network access. In order to identify each UE, a user identifier associated with the UE will be offered in signalling. Various types of user identifier may be used as defined in [ITU-T Q.1707], and support of the network access identifier (NAI) based on [IETF RFC 4282] is required if 3GPP Evolved Packet Core compliance is needed. Authentication defines the process that is used for access control, i.e., to permit or deny a UE to attach to and use the resources of an NGN. Two authentication types are defined: implicit authentication and explicit authentication (see [ITU-T Y.2014]). In explicit authentication, the authentication signalling is executed between the UE and TAA-FE in NACF. Examples of authentication signalling and its procedures are described in [b-IETF RFC 3748] and [b-3GPP TS 33.234].

6.3.1.2 Mobility service authentication and authorization

Mobility service is separate from transport service, and is controlled by additional parameters in the user profile. In general, the user has separate identifiers for transport service and mobility service.

Mobility service authentication may be integrated into or separated from network access authentication. In the integrated scenario, mobility service and network access are authenticated by the same operator. The transport user identifier will be the same as the mobility service subscriber identifier.

In case of the split scenario, authentication for the mobility service and network access authentication are performed separately. In this scenario, after network access authentication is finished, mobility service authentication will be performed by the mobile service authorizer.

6.3.1.3 IP address allocation

IP address may be configured in two different approaches. In order to support mobility in the NGN, two kinds of IP addresses need to be allocated, a persistent IP address and, in the host-based case, a temporary IP address. The persistent IP address is allocated in the anchoring network while the temporary IP address is allocated when a UE attaches to an access network which has a different subnet prefix from the persistent IP address allocated to the UE. The persistent IP address is persistently maintained for a UE regardless of its movement within a given scope, which may be global or local to a given network, whereas the temporary IP address may be changed whenever the UE attaches to a new subnet.

The persistent IP address is a persistent logical location identifier and the temporary IP address is a temporary logical location identifier in terms of the definition in clause 6.3.2 of [ITU-T Q.1707].

Details of the address allocation process are provided in the sub-clauses of clause 7.2.

The NAC-FE in NACF may be responsible for retrieving both IP addresses in NGN. NAC-FE assignment of the persistent address is required only if none is present amongst the mobility service parameters retrieved by the TAA-FE. The NAC-FE may bind the information between the mobility service subscriber ID and both IP addresses and send the binding information to the MLM-FE(P) via the TLM-FE to trigger handover.

In network-based mobility, a UE always needs to be allocated and configured with a persistent IP address, but a temporary IP address is not required.

6.3.2 Resource and admission control functions (RACF)

RACF is responsible for resource and admission control in NGN. When a UE attaches to an access network or moves to another access network, an admission decision is required for the access network. If the decision is to admit, appropriate network resources must be reserved. Network resources should be dynamically configured according to the new access network that a mobile UE attaches to. The handover decision and control functional entity (HDC-FE) requests RACF to re-provision the resource and QoS for the flows of the moved UE. For that purpose, the HDC-FE is required to submit binding information for the flows of the moved UE to the PD-FE in RACF. If the original session information is not visible at the resource and QoS enforcement points of RACF, RACF is required to have the capability to provision resources and QoS for the aggregated flows.

NOTE – Some access technologies manage QoS locally rather than through RACF for movements within a limited scope.

The mobility architecture in this Recommendation supports:

- proactive QoS resource reservation;
- adaptive QoS resource management.

6.3.3 Mobility management and control functions (MMCF)

The MMCF are responsible for mobility management and control in NGN. As defined in [ITU-T Q.1707], MMCF is composed of two sub-functions, LMF and HCF for location management function and handover control function, respectively. The LMF and HCF as defined in [ITU-T Q.1707] are composed of several functional entities which are described in clause 6.4.

6.3.4 Mobility transport functions

In order to support mobility in the NGN network, mobility-specific transport functions are needed in the forwarding plane of the transport stratum. These functions are defined in order to provide handover enforcement in the transport nodes.

In this Recommendation, we define one functional entity to provide handover execution at layer 2, and a function embedded within the EN-FE, ABG-FE and IBG-FE to provide handover execution at layer 3. The definition of those mobility node functions makes it easier to explain forwarding plane procedures in mobility functional scenarios.

6.4 Functional entities

The functional entities required for support of mobility in the control plane of the transport stratum are:

- mobile location management functional entity (MLM-FE);
- handover decision and control functional entity (HDC-FE);
- network information distribution functional entity (NID-FE);
- network information repository functional entity (NIR-FE).

The following functional entity has been defined within the forwarding plane of the transport stratum for support of mobility:

- Layer 2 handover execution functional entity (L2HE-FE).

In addition to the functions contained within the above-listed functional entities, the following function has been identified for support of mobility:

- Layer 3 handover execution function (L3HEF), which is embedded within the EN-FE, ABG-FE, and IBG-FE in the forwarding plane and communicates with the HDC-FE.

These functional entities and functions are described in the following clauses.

6.4.1 Mobile location management functional entity (MLM-FE)

The mobile location management functional entity (MLM-FE) has the following responsibilities:

- in the case of network-based mobility, initiating location registration on behalf of the UE;
- processing location registration messages sent from or on behalf of the UE;
- optionally, maintaining the binding between the mobility service user ID and persistent IP address assigned to the UE;
- management of the binding between the persistent address assigned to the UE and its temporary address, in the case of host-based mobility, or the address of the lower tunnel end point, in the case of network-based mobility;
- optionally, holding two location bindings for the mobile UE by marking the binding for the serving network as active state and marking the binding for target network as standby state;
- supporting separation of control and data plane by allowing the MLM-FE address and data forwarding end point address (i.e., tunnelling end point address) to be different;
- indication of a new mobility location binding and distribution of binding information to the HDC-FE.

The MLM-FE has two roles, as proxy (MLM-FE(P)) and as the central instance (MLM-FE(C)). The MLM-FE(P) and MLM-FE(C) roles may be co-located in specific deployments providing only host-based mobility. The MLM-FE(C) provides a central point of contact for correspondent nodes (e.g., the SCF). The MLM-FE(P) and MLM-FE(C) together provide hierarchical location management. The MLM-FE(P) holds and updates the binding between mobile user ID, persistent address, and temporary/lower tunnel end point address. The MLM-FE(C) holds the binding between mobile user ID, persistent address, and address of the MLM-FE(P). The MLM-FE(P) may identify the corresponding MLM-FE(C) by extracting the home domain from the mobile user ID.

The MLM-FE(P) consists of the following functions:

- in the host-based case, it provides the first point of contact for location registration for mobile users. As such, it appears as a proxy for the MLM-FE(C) from the point of view of the UE, while appearing as a proxy for the UE from the point of view of the MLM-FE(C). The mobile UE obtains the address of the MLM-FE(P) in the attachment procedure;
- in the network-based mobility case, the MLM-FE(P) acts as a proxy for the UE from the point of view of the network side;
- the MLM-FE(P) supports IP-based paging to locate the mobile UE;
- in the host-based case, the MLM-FE(P) may interwork between different mobility signalling protocols (e.g., due to a difference in IP versions supported) at the UE and at the MLM-FE(C);
- signalling for location registration in the host-based case is secured through the security association between the UE and the MLM-FE(P). The security association is dynamically created based on the keying materials generated in the attachment procedure;
- the MLM-FE(P) is responsible for requesting the HDC-FE to perform handover control as a consequence of mobile location registration or update;
- the MLM-FE(P) may be the proxy of the UE for initiating route optimization, especially in the case of interworking between signalling protocols;
- if there is a second anchor point between the UE and the anchor point to which the MLM-FE(C) corresponds, the MLM-FE(P) carries the additional address binding;
- the MLM-FE(P) may be used to transform addresses within the signalling because of intervening NATs;
- the MLM-FE(P) may be used to provide address anonymity to the UE.

6.4.2 Handover decision and control functional entity (HDC-FE)

The handover decision and control functional entity (HDC-FE) has three sub-functions: handover decision (HDF), layer 2 handover control (L2HCF), and layer 3 handover control (L3HCF). Their relationship is shown in Figure 2.

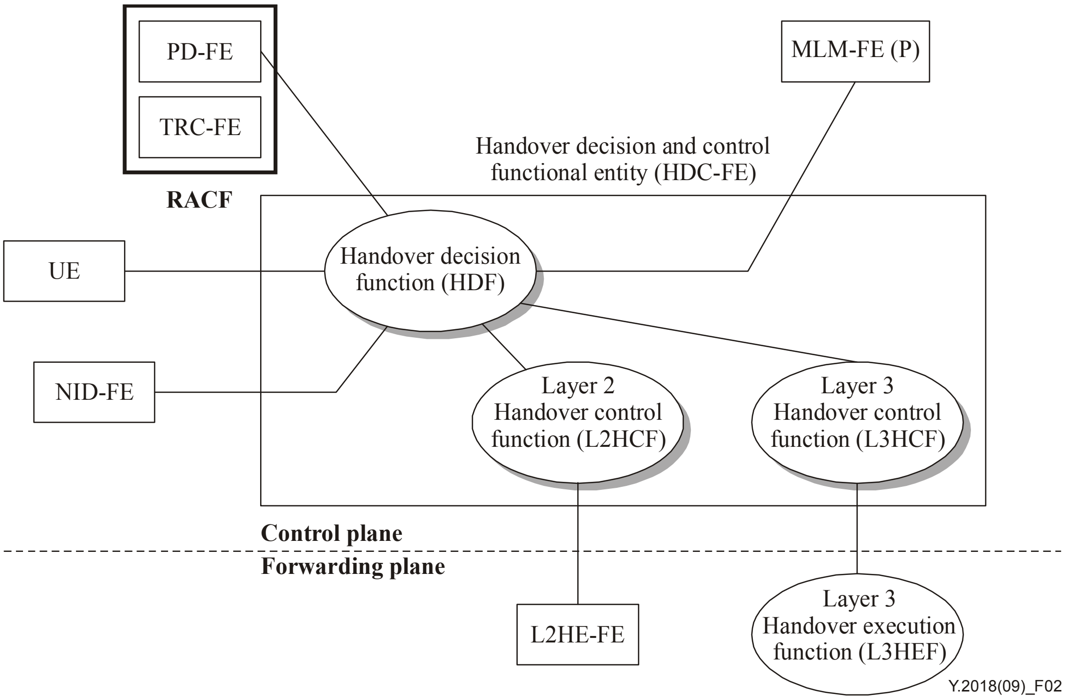

PD-FE
TRC-FE
RACF
MLM-FE (P)
Handover decision and control functional entity (HDC-FE)
UE
Handover decision function (HDF)
NID-FE
Layer 2 Handover control function (L2HCF)
Layer 3 Handover control function (L3HCF)
Control plane
Forwarding plane
L2HE-FE
Layer 3 Handover execution function (L3HEF)
Y.2018(09)_F02

Figure 2 – Relations of HDC-FE sub-functions

6.4.2.1 Handover decision function (HDF)

The handover decision function (HDF) has the following responsibilities:

- receiving a list of candidate access links for handover from the UE and invoking RACF to verify session QoS availability for each candidate access link for handover. In the case where the UE makes the handover decision, the HDF provides the acceptable subset of links to the UE;
- requesting RACF to re-provision the resource and QoS for the sessions of the moved UE by submitting binding information to the PD-FE in RACF with the following options:
  - requesting to release resource and QoS configuration for the previous data path while configuring resource and QoS for the new data path;
  - requesting to leave the previous data path as it is while configuring resource and QoS for the new data path, which makes make-before-break handover possible;
- requesting RACF to release resource and QoS for the data path which is verified not to be used anymore;
- triggering handover upon request from the UE, in the case of network-triggered handover;
- invoking handover action at the L2HCF in the case of intra-subnetwork handover, and at the L3HCF in the case of handover between subnetworks.

6.4.2.2 Layer 2 handover control function (L2HCF)

The layer 2 handover control function (L2HCF) communicates with the layer 2 handover execution functional entity (L2HE-FE) to perform the following:

- relay link layer reports to the handover decision function;
- upon request from the HDF, invoke handover action at the appropriate instance of the L2HE-FE.

For movement within the same subnetwork, handover is at layer 2. In this case, the L2HCF may communicate with L2HE-FE instances to create media paths between them during the handover process.

6.4.2.3 Layer 3 handover control function (L3HCF)

The layer 3 handover control function (L3HCF) communicates with the Layer 3 handover execution function (L3HEF) to perform the following:

- upon request from the HDF, invoke and coordinate handover action at the appropriate instances of the L3HEF.

6.4.3 Network information distribution functional entity (NID-FE)

The network information distribution functional entity (NID-FE) communicates with the entity making the handover decision during the network discovery phase described in clause 7.1. The handover decision may be made either by the UE or by the HDC-FE. The NID-FE has the following responsibilities:

- distributing handover policy, which is a set of operator-defined rules and preferences that affect the handover decisions taken by the UE or HDC-FE.

  For example, a handover policy can indicate that vertical handover from E-UTRAN access to WLAN access is not allowed. It can also indicate e.g., that WiMAX access is preferable to WLAN access;
- distributing other information provided by the NIR-FE.

6.4.3.1 Network information repository functional entity (NIR-FE)

The network information repository functional entity (NIR-FE) provides static information on neighbouring networks to the NID-FE to assist the access network discovery and selection decision. The information provided by the NIR-FE may include:

- information on neighbouring access networks in the vicinity of the UE. These access networks are possible target networks for the potential handover from the current UE location. The information may include access network identifier, access type, operator who runs the network, security and network QoS capabilities, etc.;
- information on attachment points (base stations, NodeB, access points, etc.) such as attachment point identifiers, L1/L2 address, bit rates supported, and network address configuration policy;
- operator policies such as charging mode and rates (cost for the usage of the network), roaming agreements, mobility mechanism selection policies, etc.

The means by which the NIR-FE acquires its information is out of the scope of this Recommendation.

6.4.4 Additional functions required in the forwarding plane

6.4.4.1 Layer 2 handover execution functional entity (L2HE-FE)

The layer 2 handover execution functional entity (L2HE-FE) resides in the access transport functional block. It acts on commands from the HDC-FE to:

- take access-technology-specific action as required to preserve flow continuity during handover;
- complete handover execution in the direction toward the UE when it has determined that the UE has executed handover.

In support of media independent handover (see [b-IEEE 802.21]), it also reports link layer events to the HDC-FE.

6.4.4.2 Layer 3 handover execution function (L3HEF)

The layer 3 handover execution function (L3HEF) resides in the access transport and core transport functional blocks. It acts on commands from the HDC-FE to:

- execute tunnel set-up, modification, or take-down during handover;
- buffer user packets as required to preserve flow continuity during handover;
- following handover, encapsulate user packets received from the UE (at the tunnel lower end in the case of network-based mobility) or from correspondent nodes (at the tunnel upper end) and forward them through the tunnel; similarly, decapsulate packets received from the tunnel and forward them to the UE (at the tunnel lower end in the case of network-based mobility) or to the correspondent node (at the tunnel upper end).

6.5 Reference points

Figure 3 shows the functions and functional entities described above along with the functional blocks and entities already defined in [ITU-T Y.2012]. The links between the functions indicate required information flows, identified by reference points M1 through M13. M1 through M8 and M13 are between MMCF entities and other entities. M9 through M12 are flows between entities of the MMCF. The set of links shown in Figure 3 is the superset of the links shown for individual scenarios in clause 7.

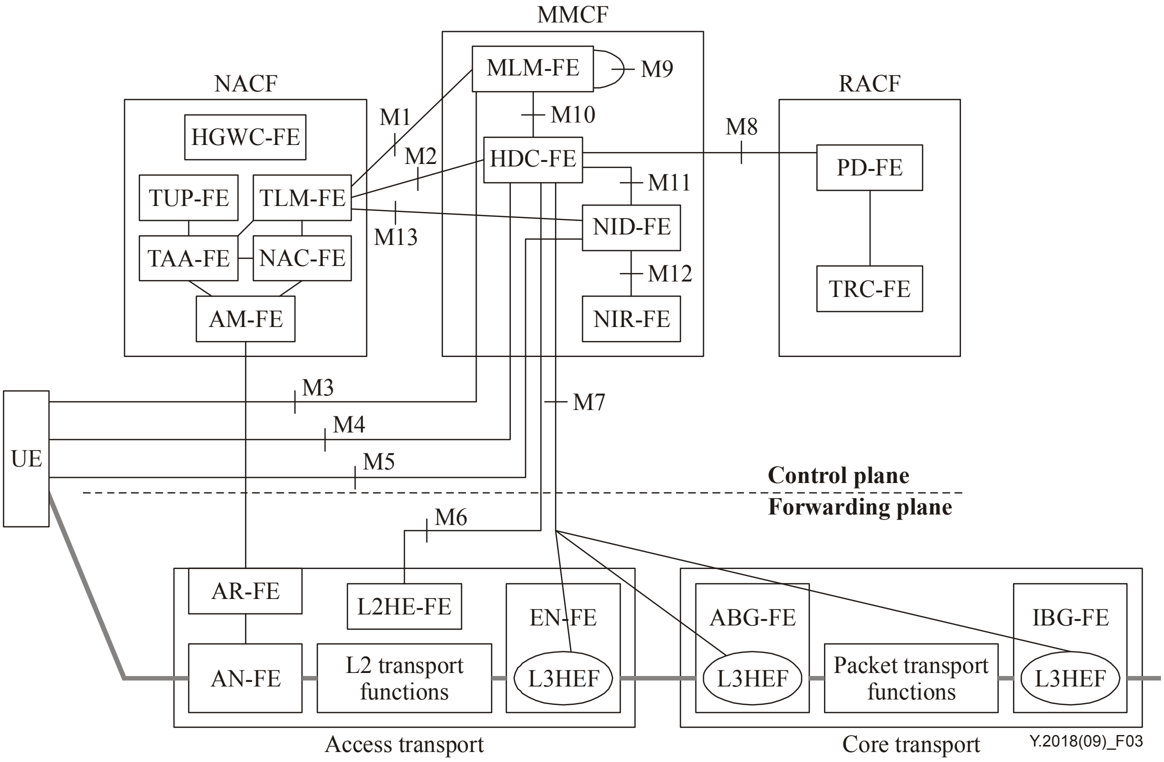


Figure 3 – Reference points and information flows involved in mobility management and control

6.5.1 Reference point M1 between TLM-FE and MLM-FE(P)

This information flow is used to distribute several types of information from the TLM-FE to the MLM-FE(P). The TLM-FE is assumed to be able to contact the NAC-FE via an internal reference point to obtain the persistent and temporary IP addresses (see clause 8.1.2 of [ITU-T Y.2014]).

6.5.1.1 Indication of host-based mobility

In the host-based mobility case, the information transferred includes the keying material derived from the UE authentication procedure (see clause 7.3.2), in support of the security association required between the MLM-FE(P) and the UE. The information passed from the TLM-FE to the MLM-FE(P) may also include:

- mobility service user ID;
- persistent IP address of the user;
- binding between mobile user ID and persistent IP address.

The TAA-FE obtains these mobility service parameters from an AAA entity in the mobile subscriber's home network. The means by which the TAA-FE determines that mobility service is to be provided and that mobility service parameters are required is out of scope of this Recommendation.

The contents of the "indication of host-based mobility" primitive are shown in Table 1.

Table 1 – Indication of host-based mobility (TLM-FE → MLM-FE(P))

Information element	Explanation
Transport subscriber identifier (optional) (Note)	The user/UE identifier authenticated for attachment.
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information (optional) (Note)	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Keying material	The material used for the security association between the UE and MLM-FE(P).
RACF contact point (optional)	The FQDN or IP address of the RACF entity where the resource requests are required to be sent (i.e., PD-FE address).
Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
NOTE – Either the UE identifier or the persistent IP address must be present.	

6.5.1.2 Indication of network-based mobility

The information transferred in the case of network-based mobility includes the identifier or persistent address, the address of the MLM-FE(C) instance for this connection, and may include the lower tunnel end point address and other parameters relating to mobility service. The "indication of network-based mobility" primitive is shown in Table 2.

When the TLM-FE indicates network-based mobility service to the MLM-FE(P), this indication will trigger the mobile location registration procedure, and indirectly trigger handover.

Table 2 – Indication of network-based mobility (TLM-FE → MLM-FE(P))

Information element	Explanation
Transport subscriber identifier (optional) (Note 1)	The user/UE identifier authenticated for attachment.
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information (optional) (Note 1)	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Address of MLM-FE(C)	The address of the instance of the MLM-FE containing the mobile address binding information.
Tunnel end-point address (optional) (Note 2)	The tunnelling end point address for the network node which works as UE's proxy (lower tunnel end point).
RACF contact point (optional)	The FQDN or IP address of the RACF entity where resource requests shall be sent (i.e., PD-FE address).
Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
NOTE 1 – Either the UE identifier or the persistent IP address must be present. NOTE 2 – If the tunnel end-point address is statically provisioned or the MLM-FE can obtain it with its own mechanisms, this information is not required.	

6.5.2 Reference point M2 between TLM-FE and HDC-FE

This information flow provides the keying material derived from the UE authentication procedure (see clause 7.3.2), in support of the security association required between the HDC-FE and the UE. This security association is required for the ongoing network selection and decision process subsequent to attachment.

Reference point M2 supports the "network selection key transfer indication" primitive, as shown in Table 3.

Table 3 – Network selection key transfer indication (TLM-FE → HDC-FE)

Information element	Explanation
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Keying material	The material used for security association between the UE and HDC-FE.

6.5.3 Reference point M3 between UE and MLM-FE(P)

This information flow is used by the UE to register and update its mobility location information in the case of host-based mobility management. Reference point M3 supports the following primitives:

- mobility location binding update, shown in Table 4;
- mobility location binding acknowledgement, shown in Table 5.

It is a requirement that mobility signalling between the UE and the MLM-FE(P) shall be protected by a security association. For more details see clause 8.

Table 4 – Mobility location binding update (UE → MLM-FE(P))

Information element	Explanation
Mobility service subscriber identifier (Note)	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Temporary IP address information	A set of IP address information used for locating the access network to which the UE is attached.
– Unique IP address	The temporary IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
NOTE – Subscriber identifier is required if either persistent or temporary address is private.	

Table 5 – Mobility location binding acknowledgement (MLM-FE(P) → UE)

Information element	Explanation
Mobility service subscriber identifier (Note 1)	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information	A set of IP address information used for locating the mobile UE
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Anchor point address (conditionally mandatory) (Note 2)	The address of the upper data tunnelling end point, from the point of view of the UE.
Binding request result	Indication of the success or failure of the binding update.
NOTE 1 – UE identifier is required if persistent address is private. NOTE 2 – Anchor point address is required for initial tunnel installation.	

6.5.4 Reference point M4 between UE and HDC-FE

This information flow is used to carry handover event or command messages between the HDC-FE and the UE.

6.5.4.1 Initiation of handover sequence

The handover sequence begins when the UE detects that it will need to perform handover in the near future. It alerts the HDC-FE and provides a list of alternative access points that it has detected, using the "handover candidate indication" primitive (Table 6). The HDC-FE responds with the "handover candidate response" (Table 7).

Table 6 – Handover candidate indication (UE → HDC-FE)

Information element	Explanation
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Access point list	A list of attachment point identifiers suggesting new access networks to which handover initiation will be considered. The list is sorted from most preferred first to least preferred last.
Preferred handover decision maker (optional)	Indicates whether the UE prefers the network to select the target access point or prefers to do the selection itself.
Preferred triggering entity (optional)	Indicates whether the UE prefers the network to trigger handover or whether the UE prefers to do so itself.

Table 7 – Handover candidate response (HDC-FE → UE)

Information element	Explanation
Handover decision maker	Indicates whether the choice of target link will be made by the network or by the UE.
Triggering entity	Indicates whether triggering will be done by the network or the UE.
Preferred access point list (Note)	A list of attachment points suggesting new access networks to which handover initiation will be considered. This may be different from the networks that were suggested in the candidate query. The list is sorted from most preferred first to least preferred last.
Address of NID-FE (Note)	Address of the entity from which the UE may obtain static network information for the networks under consideration.
NOTE – These parameters are included only if the handover decision maker will be the UE.	

6.5.4.2 Handover decision

If the network has indicated that the network will make the handover decision, the UE waits until the network sends a "network handover decision request" (Table 8); the UE responds by sending a "network handover decision response" (Table 9). Conversely, if the UE is the decision maker, the network waits until the UE sends a "UE handover decision request" (Table 10); the network responds with a "UE handover decision response" (Table 11).

Table 8 – Network handover decision request (HDC-FE → UE)

Information element	Explanation
Target access point	Identifies the target access point selected by the network.
Target network information	Information about the target network to assist the mobile node to perform a handover.
Handover execution delay (Optional) (Note)	The amount of time (in ms) to elapse before an action needs to be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instant the command arrives until the time when the execution of the action is carried out.
NOTE – May be present if the UE has previously been identified as the triggering entity.	

Table 9 – Network handover decision response (UE → HDC-FE)

Information element	Explanation
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Status	One of: handover not possible, ready to trigger, awaiting trigger.
Handover execution delay (Optional) (Note)	The amount of time (in ms) to elapse before an action needs to be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instant this response arrives until the time when the execution of the action is carried out.
NOTE – May be present if the network has previously been identified as the triggering entity and status is "awaiting trigger".	

Table 10 – UE handover decision request (UE → HDC-FE)

Information element	Explanation
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Target access point	Identifies the target access point selected by the network.
Target network information	Information about the target network to assist the mobile node to perform a handover.
Handover execution delay (Optional) (Note)	The amount of time (in ms) to elapse before an action needs to be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instant the command arrives until the time when the execution of the action is carried out.
NOTE – May be present if the network has previously been identified as the triggering entity.	

Table 11 – UE handover decision response (HDC-FE → UE)

Information element	Explanation
Status	One of: handover not possible, ready to trigger, awaiting trigger.
Handover execution delay (Optional) (Note)	The amount of time (in ms) to elapse before an action needs to be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instant this response arrives until the time when the execution of the action is carried out.
NOTE – May be present if the UE has previously been identified as the triggering entity and status is "awaiting trigger".	

6.5.5 Reference point M5 between UE and NID-FE

This information flow is used to carry information needed to make the handover decision from the NID-FE to the UE when the UE is the entity that makes the handover decision. Reference point M5 supports two primitives:

- access network information query (Table 12);
- access network information query response (Table 13).

Note that these are the same primitives supported across reference point M11 (HDC-FE ↔ NID-FE, Tables 23 and 24).

Table 12 – Access network information query (UE → NID-FE)

Information element	Explanation
Serving access point identifier(s)	The identifiers of the access point(s) to which the UE is currently connected.
– access point identifier	Identifier of the specific access point within the serving access network.
– network identifier	Identifier of the serving access network.

Table 13 – Access network information query response (NID-FE → UE)

Information element	Explanation
Static neighbouring network info	Static neighbouring network information (e.g., local policies, cost) for networks neighbouring the serving network(s) specified in the original query.

6.5.6 Reference point M6 between HDC-FE and L2HE-FE

This information flow is used by the HDC-FE to achieve handover at layer 2 in the forwarding plane. The details of this information flow are technology specific and out of scope of this Recommendation.

6.5.7 Reference point M7 between HDC-FE and L3HEF

This information flow is used by the HDC-FE to achieve handover at layer 3 in the forwarding plane. The details of this information flow are implementation specific and out of scope of this Recommendation. As a generality, the information sent to the L3HEF will include information by which the tunnel can be identified, the address of the other tunnel end point, and either the address given to this tunnel end point or information from which it can be generated.

6.5.8 Reference point M8 between HDC-FE and PD-FE

Reference point M8 supports the operations described in clause 6.3.2.

6.5.8.1 Verification of resource availability

The HDC-FE queries RACF to verify that resources are available to serve the user prior to handover. For this purpose, reference point M8 supports two primitives:

- available resource query (Table 14);
- available resource query response (Table 15).

The "available resource query" primitive is used by the HDC-FE to check with RACF in candidate networks to verify available resources on the candidate access links.

Table 14 – Available resource query (HDC-FE → PD-FE)

Information element	Explanation
Transport subscriber identifier	The user/UE identifier authenticated for attachment.
Candidate attachment point list	A list of attachment points, suggesting the new access networks to which handover initiation will be considered. The access networks towards the top of the list are preferred over those towards the bottom of the list.

Table 15 – Available resource query response (PD-FE → HDC-FE)

Information element	Explanation
Transport subscriber identifier	The user/UE identifier authenticated for attachment.
Status	Specifies whether requested resources are available or not for each candidate link.

6.5.8.2 Resource re-provisioning

This information flow is used by the HDC-FE to reserve session QoS resources by providing address binding information to PD-FE, and to deallocate QoS on the old path once handover is complete. Reference point M8 supports two primitives for the purpose:

- resource re-provisioning request (Table 16);
- resource re-provisioning response (Table 17).

Table 16 – Resource re-provisioning request (HDC-FE → PD-FE)

Information element	Explanation
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Transport user identifier (conditionally mandatory) (Note)	The user/UE identifier authenticated for attachment.
Temporary IP address information	A set of IP address information used for locating the access network to which the UE is attached. In the host-based mobility case this is the temporary address. In the network-based mobility case it is the address of the lower tunnel end point.
– Unique IP address	The temporary IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Operation type	Indication of resource reservation operation type: resource reservation or resource release.
Gateway Address (optional)	The address of ABG-FE/IBG-FE containing the anchor point.
NOTE – Transport user identifier is required if either persistent or temporary address is private.	

Table 17 – Resource re-provisioning response (PD-FE → HDC-FE)

Information element	Explanation
Transport user identifier	The user/UE identifier authenticated for attachment.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Status	The status of operation.

It is assumed that RACF retains the binding between persistent address and the QoS resources allocated to sessions associated with the UE.

6.5.9 Reference point M9 between MLM-FE(P) and MLM-FE(C)

6.5.9.1 Mobility location binding registration/update request

This information flow is used to register and update mobility location information in both the host-based and network-based mobility cases. In the network-based mobility case, the MLM-FE(P) will send the location registration/update request to the MLM-FE(C). In the host-based mobility case, the UE will send the location registration/update request to the MLM-FE(P), which will pass it on to the MLM-FE(C).

The mobility service subscriber ID and information providing the location binding between the persistent location identifier and the location of the MLM-FE(P) are included in the messages for both host-based and network-based mobility.

Reference point M9 supports two primitives for this operation:

- mobility location binding registration/update request (Table 18);
- mobility location binding registration/update response (Table 19).

Table 18 – Mobility location binding registration/update request (MLM-FE(P) → MLM-FE(C))

Information element	Explanation
Mobility service subscriber identifier (conditionally mandatory) (Note)	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Address of MLM-FE(P)	The address of the MLM-FE instance which sends the location registration.
NOTE – Mobility service subscriber identifier is required if persistent address is private.	

Table 19 – Mobility location binding registration/update response (MLM-FE(C) → MLM-FE(P))

Information element	Explanation
Mobility service subscriber identifier	The identifier of the subscriber for which the mobility service is to be provided.
Binding request result	Indication of the success or failure of the binding request.

6.5.9.2 Mobility location query

In the routing optimization case (see clause 7.3.5), the MLM-FE(C) may query and obtain the mobile UE's current binding location information through this reference point in order to pass it to the MLM-FE(C) associated with a correspondent UE.

If a related entity (e.g., a correspondent node) requests the MLM-FE(C) to provide an indication regarding UE's reachability, the MLM-FE(C) may send a request to the MLM-FE(P) through this reference point to get that information. The MLM-FE(P) will send the location binding information to the related entity (e.g., correspondent node) via the MLM-FE(C).

Reference point M9 supports two primitives for this purpose:

- mobility location query (Table 20);
- mobility location query response (Table 21).

Table 20 – Mobility location query (MLM-FE(C) → MLM-FE(P))

Information element	Explanation
Mobility service subscriber identifier (Note)	The identifier of the subscriber for which the mobility service is to be provided.
Persistent IP address information (Note)	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
NOTE – Either the mobility service subscriber identifier or the persistent address is required.	

Table 21 – Mobility location query response (MLM-FE(P) → MLM-FE(C))

Information element	Explanation
Mobility service subscriber identifier	The identifier of the subscriber for which the mobility service is to be provided.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Temporary IP address information	A set of IP address information used for locating the access network to which the UE is attached.
– Unique IP address	The temporary IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.

6.5.10 Reference point M10 between MLM-FE(P) and HDC-FE

This information flow is used to carry handover indications from the MLM-FE(P) to the HDC-FE and responses from the HDC-FE to the MLM-FE(P) when handover execution is complete in the host-based mobility case.

Reference point M10 supports the "handover indication" primitive (Table 22) for this purpose.

Table 22 – Handover indication (MLM-FE → HDC-FE)

Information element	Explanation
Transport subscriber identifier (optional) (Note 1)	The user/UE identifier authenticated for attachment.
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.

Table 22 – Handover indication (MLM-FE → HDC-FE)

Information element	Explanation
Temporary IP address information (conditionally mandatory) (Note 2)	A set of IP address information used for locating the UE within the network to which the UE is attached.
– Unique IP address	The temporary IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
RACF contact point (optional) (Note 3)	The FQDN or IP address of the RACF entity where resource requests shall be sent (i.e., PD-FE address).
Upper tunnel end point (optional) (Notes 3 and 4)	Address of the upper tunnel end point.
Mobility service parameters	Details are for further study.
NOTE 1 – UE identifier is required if either persistent or temporary address is private. NOTE 2 – Required always for host-based case, and required in network-based case only when L3HEF in EN-FE is unable to allocate that address. NOTE 3 – Provided only if supplied by the TLM-FE (see Tables 1 and 2). NOTE 4 – Not required if available by local means.	

6.5.11 Reference point M11 between HDC-FE and NID-FE

This information flow is used by the HDC-FE to query neighbouring network information from the NID-FE in the case where the HDC-FE makes the handover decision.

Reference point M11 supports two primitives:

- access network information query (Table 23);
- access network information query response (Table 24).

It is assumed that the NID-FE is configured with the topological information that allows it to determine which networks are neighbours to (and have the same access technology as) a given serving network.

Table 23 – Access network information query (HDC-FE → NID-FE)

Information element	Explanation
Serving access point identifier(s)	The identifiers of the access point(s) to which the UE is currently connected.
– access point identifier	Identifier of the specific access point within the serving access network.
– network identifier	Identifier of the serving access network.

Table 24 – Access network information query response (NID-FE → HDC-FE)

Information element	Explanation
Static neighbouring network info	Static neighbouring network information (e.g., local policies, cost) for networks neighbouring the serving network(s) specified in the original query.

6.5.12 Reference point M12 between NID-FE and NIR-FE

The information flow through reference point M12 allows the NID-FE to retrieve the neighbouring network information that it then provides to the UE or HDC-FE. Reference point M12 supports two primitives:

- access network information query (Table 25);
- access network information query response (Table 26).

Table 25 – Access network information query (NID-FE → NIR-FE)

Information element	Explanation
List of neighbouring networks	The list of identifiers of networks for which NID-FE wants access network information.

Table 26 – Access network information query response (NIR-FE → NID-FE)

Information element	Explanation
Static neighbouring network info	Static neighbouring network information (e.g., local policies, cost) for each network identified in the query.

6.5.13 Reference point M13 TLM-FE and NID-FE

This information flow provides the keying material derived from the UE authentication procedure (see clause 7.3.2), in support of the security association required between the NID-FE and the UE. This security association is required for the ongoing network selection and decision process subsequent to attachment.

Reference point M13 supports the "network selection key transfer indication" primitive, as shown in Table 27.

Table 27 – Network selection key transfer indication (TLM-FE → NID-FE)

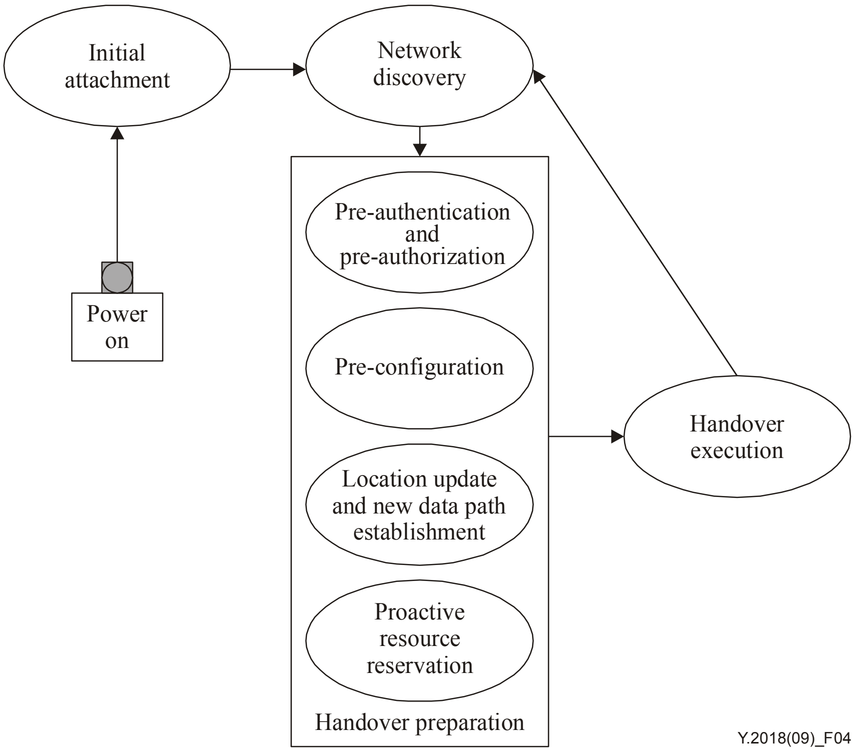
Information element	Explanation
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Keying material	The material used for security association between the UE and NID-FE.

7 Procedures

This clause describes the information flows required to achieve initial attachment, network discovery and handover for a mobile UE. In each stage, the procedures vary depending on UE capabilities and network arrangements, and the scenarios in this Recommendation, therefore, can be referred to only as examples.

7.1 Overview of mobility procedures

Figure 4 shows the key procedures involved in the whole mobility process and their general sequence. It should be noted that depending on different deployment requirements, the handover preparation can vary slightly.



Initial attachment
Network discovery
Power on
Pre-authentication and pre-authorization
Pre-configuration
Location update and new data path establishment
Proactive resource reservation
Handover preparation
Handover execution
Y.2018(09)_F04

Figure 4 – Overview of the handover process

1) *Initial attachment*

When a UE is powered on it will perform the initial attachment process defined in [ITU-T Y.2014]. For mobile UE, mobility authentication will be performed along with network access authentication. Also mobility location registration and binding will be done at the end of the phase.

After the initial attachment procedure, IP connectivity exists between the UE and the network.

2) *Network discovery*

Network discovery is performed by the mobile UE. Once a mobile UE is powered on, it may periodically scan for potential attachment points. The handover threshold can be triggered by multiple reasons such as link deterioration, etc. When this happens, the UE sends its current list of candidate attachment points to the HDC-FE to initiate the handover decision process. This process results in the selection of the target access point.

3) *Authentication*

The UE needs to perform authentication for the target access network chosen in the network discovery procedure. In order to reduce authentication latency, pre-authentication and/or optimized re-authentication methods may be performed while the UE is still attached to the serving access point. As a result of authentication, keying material is passed to the UE and the entities to which the UE signals (HDC-FE, MLM-FE(P) in the host-based mobility case, and the NID-FE in the case where the UE makes the handover decision).

4) *Configuration*

Once (pre-)authentication is successfully performed, the UE and the target network will be configured with parameters such as UE address(es), MLM-FE(P) address, etc. In addition, NACF will push the transport profile of the target network to RACF for QoS resource allocation.

5) *Location update and new data path establishment*

After the new IP addresses are configured, the UE is ready for mobility location update and new data path creation for the target network. If successful, the user traffic towards mobile UE may be forwarded to the serving network and the target network simultaneously. The MLM-FE may hold two location bindings for the mobile UE; the binding for the serving network is marked as active while the binding for target network is marked as in standby state. To support separation of control and data plane, the MLM-FE address and the data forwarding end point address (i.e., tunnelling end point address) may be different.

6) *Proactive resource reservation*

Proactive resource reservation is also an important step in handover preparation. Proactive resource reservation can assure QoS in the target network thus helping to assure seamless handover.

Proactive resource reservation may be initiated by MMCF after the mobility location update or triggered through the transport function.

7) *Handover execution*

In handover execution, the packet delivery path is switched to the new data path only and the old data path is released accompanied with the deletion of the old location binding.

7.2 Network attachment, IP configuration, and mobility location management

The procedures for network attachment of a mobile UE differ from those for a fixed or merely nomadic terminal because:

- the part of the user profile that specifies the mobility service to be granted to the UE must be made available to the access network; and
- the functions related to mobility service must be engaged.

In the integrated scenario, the user identifier presented for transport authentication and authorization is sufficient to accomplish these two requirements. In the split scenario, because there are two authorizing entities, some extra steps are required. The first is to obtain the user identifier for the purpose of authorizing mobility service. From this, the access network may initiate authentication and authorization at the authorizing entity for mobility service, which will be an AAA entity in the mobile subscriber's home network. This will, in general, lead to an authentication exchange between the UE and that entity, relayed by the TAA-FE.

7.2.1 Procedures for attachment in the case of host-based mobility

As noted in clause 6.4.1, the MLM-FE(P) is the first point of contact for mobility location management signalling. In this scenario, mobility location registration messages pass from the host through the MLM-FE(P), and are then relayed to the MLM-FE(C). If a hierarchical mobility mechanism is adopted and the UE moves within the scope of a single MLM-FE(P), the MLM-FE(P) will update its own mobility location bindings but does not need to notify the MLM-FE(C). Figure 5 shows the message flow, which is divided into four phases: (pre-)authentication and (pre-)authorization, IP address configuration, mobility location management, and transport location management.

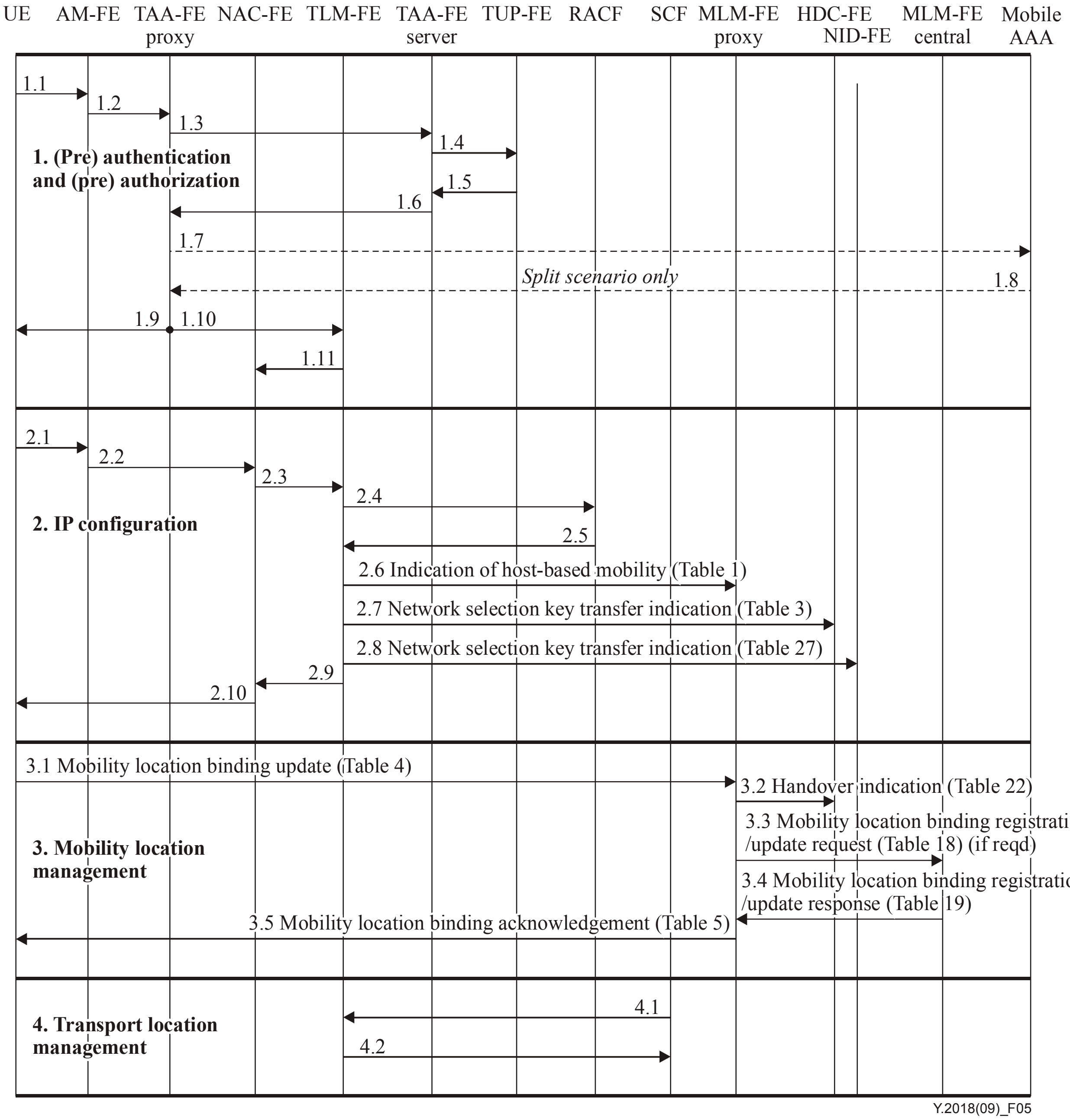

UE
AM-FE
TAA-FE proxy
NAC-FE
TLM-FE
TAA-FE server
TUP-FE
RACF
SCF
MLM-FE proxy
HDC-FE
NID-FE
MLM-FE central
Mobile AAA
1.1
1.2
1.3
1.4
1. (Pre) authentication and (pre) authorization
1.5
1.6
1.7
Split scenario only
1.8
1.9
1.10
1.11
2.1
2.2
2.3
2.4
2. IP configuration
2.5
2.6 Indication of host-based mobility (Table 1)
2.7 Network selection key transfer indication (Table 3)
2.8 Network selection key transfer indication (Table 27)
2.9
2.10
3.1 Mobility location binding update (Table 4)
3.2 Handover indication (Table 22)
3.3 Mobility location binding registration /update request (Table 18) (if reqd)
3. Mobility location management
3.4 Mobility location binding registration /update response (Table 19)
3.5 Mobility location binding acknowledgement (Table 5)
4.1
4. Transport location management
4.2
Y.2018(09)_F05

Figure 5 – Information flows for attachment in the case of host-based mobility

Phase 1: (Pre-)authentication and (pre-)authorization

The procedure is as described in clause II.1, numeral 1) of [ITU-T Y.2014], with the following modifications:

1.1 In its attachment request, the UE indicates that it requires mobility services, and may indicate whether it supports host-based and/or network-based mobility. In the split scenario, it provides its mobility service credentials either at this stage or at a later stage (not shown) in an additional dialogue with the TAA-FE (proxy) before step 1.7.

1.2 The AM-FE forwards the additional mobility-related information provided by the UE to the TAA-FE along with the information defined in [ITU-T Y.2014].

1.3-1.4 No change from [ITU-T Y.2014].

1.5 In the integrated scenario, the TUP-FE returns mobility service parameters as well as the user transport profile.

After successful authentication, the entities in the home network may allocate a persistent IP address for the mobile node (e.g., using a DHCP server) based on the mobile user location information, and store it with other mobility service parameters for the UE. This allocation is required only if no persistent address has already been allocated to the UE.

1.6 The user transport profile and mobility service parameters (in the integrated scenario) are sent from the TAA-FE (server) in the home network to the TAA-FE (proxy) in the target network. The mobility service parameters include the persistent address, and the address of the MLM-FE(C).

After successful authentication, the TAA-FE (proxy) also has the keying material needed to establish a security association between the UE and the MLM-FE(P). Further details on generation of keying material at this stage are provided in clause 7.3.2.

1.7-1.8 These steps are necessary only in the split scenario. The TAA-FE (proxy) forwards the user's mobility service credentials to an AAA server in the user's home network for mobility services. The AAA server authenticates the user for mobility services and returns the mobility service parameters. As part of this process, the AAA server ensures that a persistent address is allocated if this is necessary.

1.9 No change from [ITU-T Y.2014].

1.10 The profile information passed to the TLM-FE includes the mobility service parameters.

1.11 The TLM-FE configures the NAC-FE with the mobile subscriber's persistent address and an indication that host-based mobility will be used. It also passes the address of the instance of the MLM-FE(P) that the UE will use, and keying material for the security associations with the MLM-FE(P), HDC-FE, and, if required, the NID-FE.

NOTE – This is an entirely new information flow that must be added to [ITU-T Y.2014].

Phase 2: IP configuration

The procedure is as described in clause II.1, numeral 2) of [ITU-T Y.2014], with the following modifications:

2.1-2.2 No change from [ITU-T Y.2014].

2.3 No change from [ITU-T Y.2014]. However, because it was pre-configured for mobility services, the NAC-FE defers its response to the UE (which Figure II.1 of [ITU-T Y.2014] shows as happening at the same time as step 2.3) until it receives a response from the TLM-FE. This prevents a race between completion of the next few steps by the TLM-FE and the sending of the mobility location binding update message by the UE.

2.4-2.5 No change from [ITU-T Y.2014].

2.6 The TLM-FE pushes the user identity and keying materials to the MLM-FE(P), indicating host-based mobility.

2.7-2.8 The TLM-FE pushes keying material for communication with the UE during network discovery and selection to the HDC-FE and NID-FE.

2.9 The TLM-FE responds to the NAC-FE only after completing steps 2.6-2.8.

2.10 The NAC-FE responds to the UE only after receiving acknowledgement from the TLM-FE (step 2.9). As well as its new temporary IP address, the UE is configured with its persistent IP address, the new MLM-FE(P) address, and keying material for the security associations with the MLM-FE(P), HDC-FE, and, if required, the NID-FE. It is also given an indication that host-based mobility is to be used.

Phase 3: Mobility location management

3.1 The UE initiates mobility location registration at the MLM-FE(P). The UE is able to send its message protected by the security association set up implicitly by the distribution of the keying material to it and the MLM-FE(P), without the need for additional messaging for this purpose,

3.2 The MLM-FE(P) records or updates its mobility bindings based on the received information. The MLM-FE(P) sends an indication to the HDC-FE that a mobile location update has occurred. This initiates the layer 3 path establishment procedure described in clause 7.3.3 and shown in Figure 9.

3.3 The MLM-FE(P) modifies the binding request from the UE before relaying it to the MLM-FE(C). Steps 3.3-3.4 are unnecessary if the MLM-FE(P) is associated with a previously-established intermediate anchor point.

3.4 The MLM-FE(C) records or updates its own binding information and responds to the MLM-FE(P).

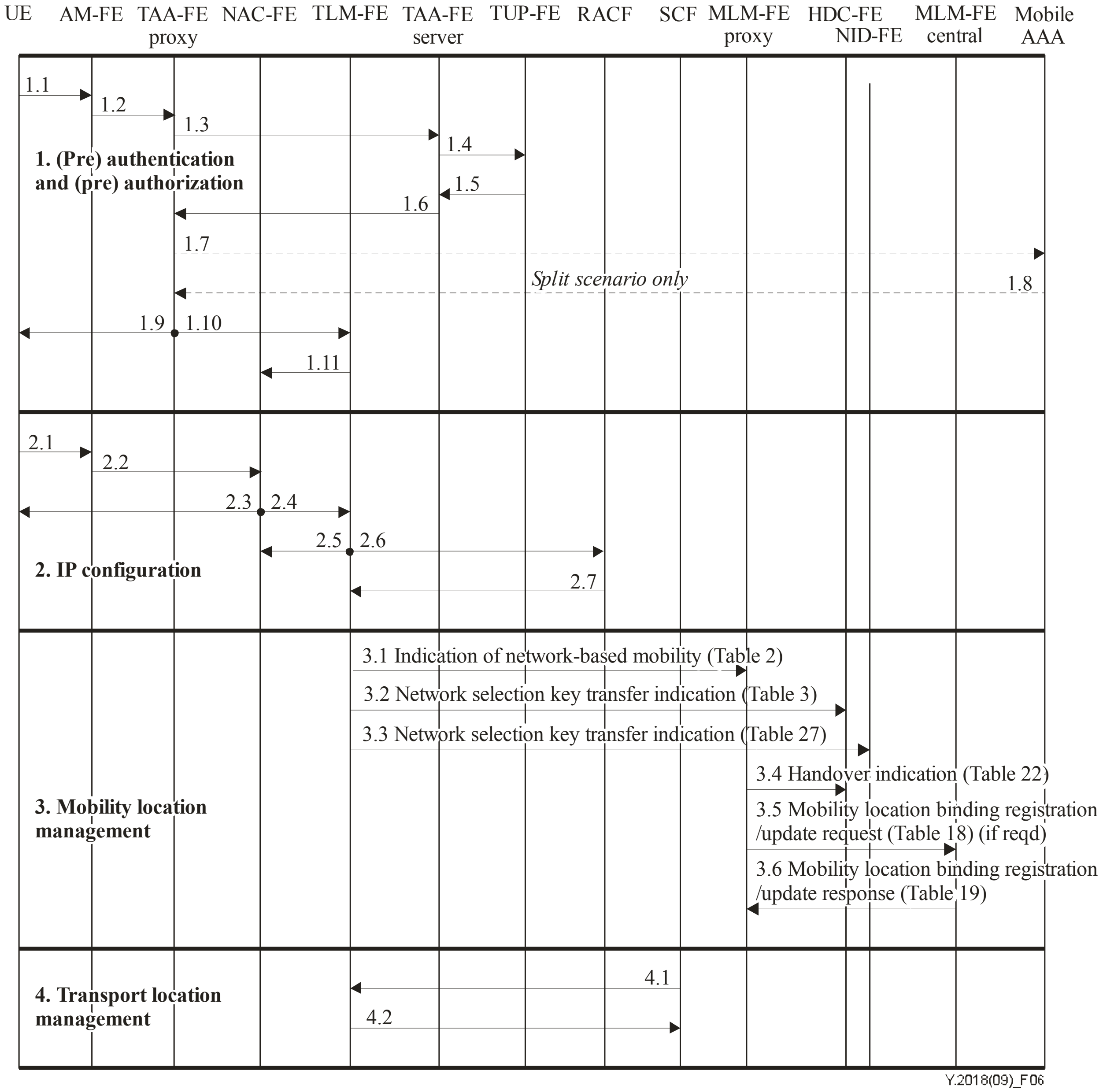
3.5 The MLM-FE(P) responds to the UE.

Phase 4: Transport location management

As described in clause II.1, numeral 4) of [ITU-T Y.2014].

7.2.2 Procedures for attachment in the case of network-based mobility

Figure 6 shows the information flows in the case of network-based mobility. The same four phases apply as for the host-based case. However, because there is no potential race between a binding update from the UE and the configuration of the MLM-FE(P), the need for coordination between the NAC-FE and TLM-FE in the IP configuration stage is eliminated. The preconfiguration of the mobility management functions is therefore shown as part of the mobility location management phase in Figure 6.



UE
AM-FE
TAA-FE proxy
NAC-FE
TLM-FE
TAA-FE server
TUP-FE
RACF
SCF
MLM-FE proxy
HDC-FE
NID-FE
MLM-FE central
Mobile AAA
1. (Pre) authentication and (pre) authorization
1.1
1.2
1.3
1.4
1.5
1.6
1.7
Split scenario only
1.8
1.9
1.10
1.11
2. IP configuration
2.1
2.2
2.3
2.4
2.5
2.6
2.7
3. Mobility location management
3.1 Indication of network-based mobility (Table 2)
3.2 Network selection key transfer indication (Table 3)
3.3 Network selection key transfer indication (Table 27)
3.4 Handover indication (Table 22)
3.5 Mobility location binding registration /update request (Table 18) (if reqd)
3.6 Mobility location binding registration /update response (Table 19)
4. Transport location management
4.1
4.2
Y.2018(09)_F06

Figure 6 – Information flows for attachment, case of network-based mobility

Phase 1: Authentication and authorization

The procedure is as described in clause II.1, numeral 1) of [ITU-T Y.2014], with the following modifications:

1.1-1.10 As in the previous clause.

1.11 The TLM-FE configures the NAC-FE as in step 1.11 of the previous clause, except that network-based mobility is indicated. In addition, the address of the MLM-FE(P) and keying material associated with the MLM-FE(P) are unnecessary and are not passed.

Phase 2: IP configuration

The procedure is as described in clause II.1, numeral 2) of [ITU-T Y.2014], with the following modifications:

2.1-2.2 No change from [ITU-T Y.2014].

2.3 The UE is configured with its persistent IP address as its new local address. It is also configured with keying material for the security associations with the HDC-FE and, if required, the NID-FE. If it indicated support for host-based mobility, it may also be given an indication that network-based mobility is to be used.

2.4 Depending on local arrangements, the NAC-FE may pass the persistent address or the address of the lower tunnel end point back to the TLM-FE with the profile information.

Phase 3: Mobility location management

3.1 After the (Pre)authentication and (pre)authorization procedure, the TLM-FE pushes an indication to the MLM-FE(P) that network-based mobility is to be provided.

3.2-3.3 The TLM-FE pushes keying material for communication with the UE during network discovery and selection to the HDC-FE and NID-FE.

3.4 The MLM-FE(P) notifies the HDC-FE to begin handover. The HDC-FE oversees creation of a new tunnel as described in clause 7.3.3 and returns the address of the tunnel end point at the lower end.

3.5 The MLM-FE(P) initiates the mobility location management procedure at the MLM-FE(C).

3.6 The MLM-FE(C) records the binding information, notifies the old MLM-FE(P) to delete its mobile location bindings and responds to the new MLM-FE(P).

Phase 4: Transport location management

As described in clause II.1, numeral 4) of [ITU-T Y.2014].

7.3 Handover

7.3.1 Network discovery and decision

Before the UE can achieve handover to a new access point or network, the network discovery and decision procedure must be performed. The information needed to make the handover decision includes:

- radio signal strength, from the UE;
- link events, from the L2HE-FE (in the case where the HDC-FE makes the decision);
- static neighbouring network information (e.g., local policies, cost), from the NID-FE;
- resource availability in candidate networks, from RACF;
- applicable UE-specific policy, from the user mobility service profile.

Network discovery is performed by the UE, when it detects alternative access points to which it may move. The handover decision is the process of choosing an access point to which to move. Network discovery and the handover decision must consider three cases:

- the network makes the handover decision with input from the UE;
- the UE makes the handover decision with the assistance of information from the network;
- the UE makes the handover decision without assistance from the network.

In the latter two cases the UE can request user input or can be constrained by user intervention.

When the UE is acting together with the network, the handover decision process begins when the UE reports a list of alternative access points to the HDC-FE. The UE may indicate its preference at this time regarding which entity makes the handover decision and which entity actually triggers the handover. Based on the information the UE has provided, the HDC-FE requests RACF to check network resource availability on the potential path through each candidate network and receives the resource check result from RACF. The HDC-FE then responds to the UE, indicating its choice of deciding entity and triggering entity. If it has chosen the UE to make the decision, it returns a candidate access point list which is based on the UE's input but reflects the results of the resource check and perhaps of local policy. If it has chosen to make the decision itself, its response includes no candidates.

The next step depends on which entity the HDC-FE has nominated to make the handover decision. If it is the HDC-FE, then the HDC-FE retrieves static network information for the candidate access points from the NID-FE. Based on that information, it makes a final decision on the identity of the target access point. It prepares for handover to that target access point as described in the next two clauses. It then informs the UE of its decision. The UE responds when it is ready for the handover. Alternatively, the UE may respond that handover to the selected access point is not possible (e.g., because it is no longer 'visible' to the UE). In this latter case, the whole network discovery and decision process must begin again.

If the UE is the one to make the decision, it is the one to retrieve static network information about the target networks from the NID-FE. It makes its selection, then informs the HDC-FE. The HDC-FE prepares the new access point as described in the next two clauses, then responds to the UE.

The actual triggering of handover execution is done by the entity nominated by the HDC-FE. The complete discovery and decision process is illustrated in Figure 7.

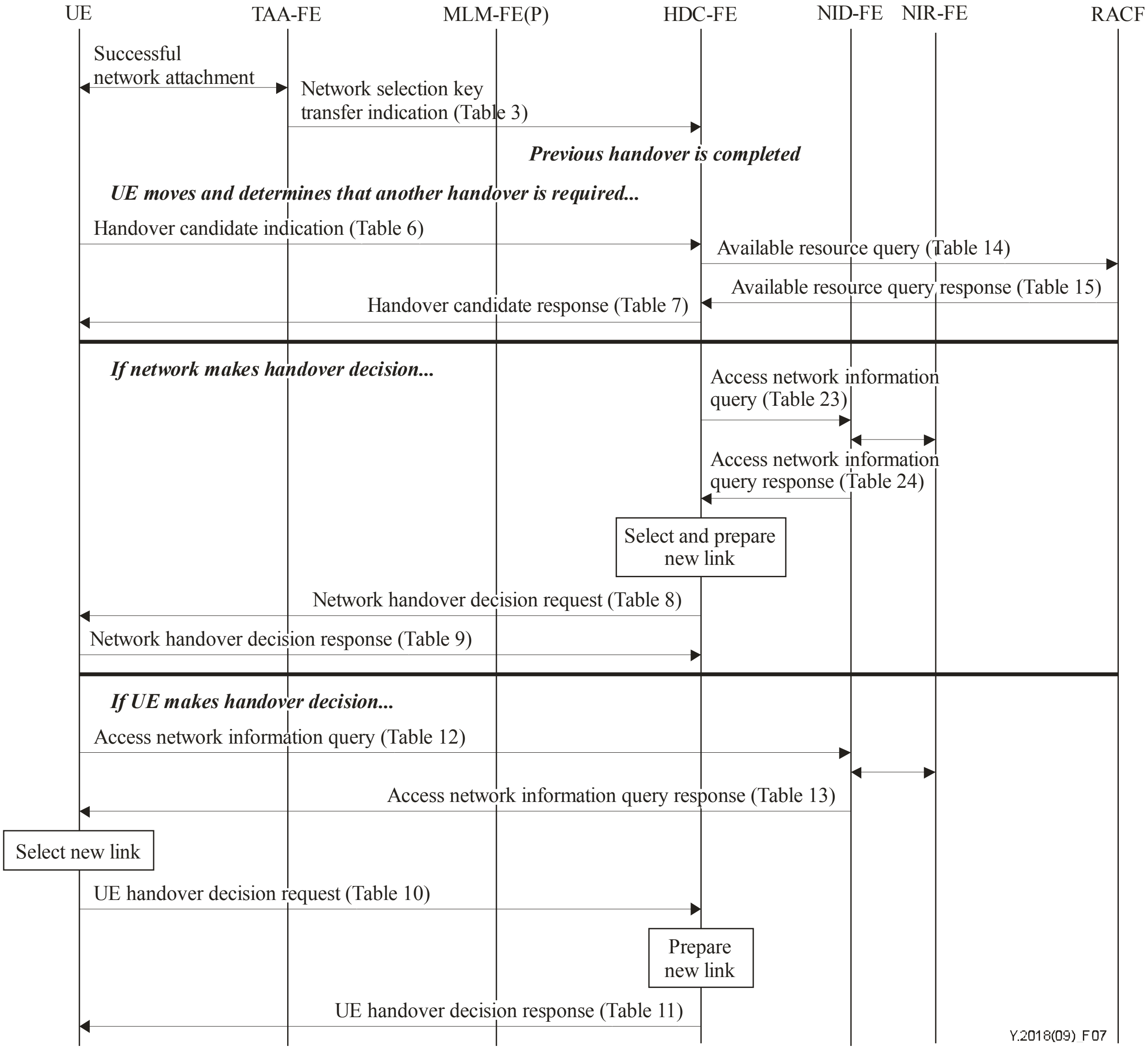

UE
TAA-FE
MLM-FE(P)
HDC-FE
NID-FE
NIR-FE
RACF
Successful network attachment
Network selection key transfer indication (Table 3)
Previous handover is completed
UE moves and determines that another handover is required...
Handover candidate indication (Table 6)
Available resource query (Table 14)
Available resource query response (Table 15)
Handover candidate response (Table 7)
If network makes handover decision...
Access network information query (Table 23)
Access network information query response (Table 24)
Select and prepare new link
Network handover decision request (Table 8)
Network handover decision response (Table 9)
If UE makes handover decision...
Access network information query (Table 12)
Access network information query response (Table 13)
Select new link
UE handover decision request (Table 10)
Prepare new link
UE handover decision response (Table 11)
Y.2018(09)_F07

Figure 7 – Illustration of network discovery and decision procedure – Network-triggered handover

7.3.2 Pre-authentication and pre-authorization

NOTE – The procedures of this clause require changes to [ITU-T Y.2014].

As the result of the network discovery and decision process, one target network is selected for the upcoming handover. Before the handover, pre-authentication and pre-authorization in the new target network will be performed while still connecting to the serving network. Figure 8 shows three cases.

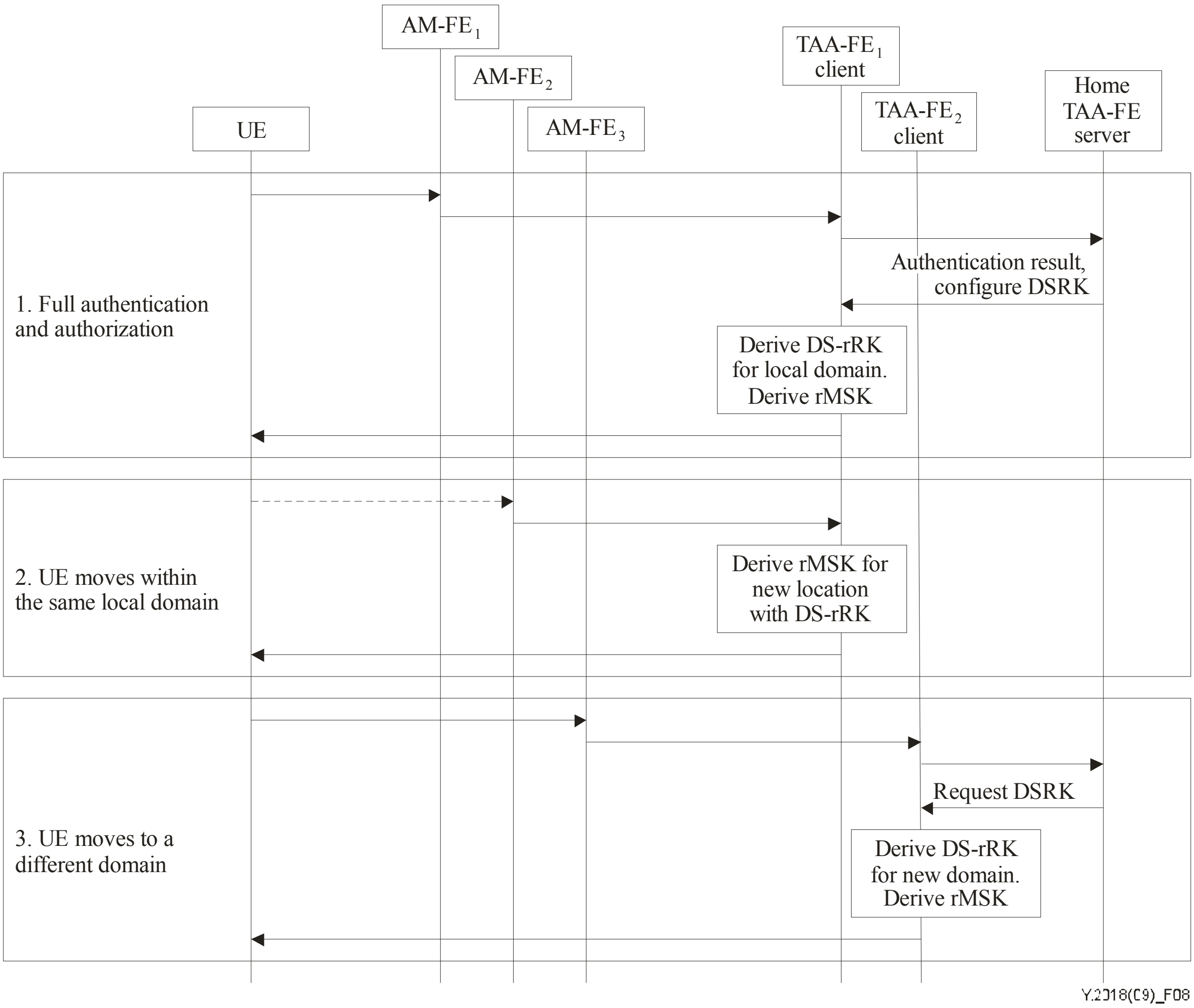

AM-FE$_1$
TAA-FE$_1$ client
AM-FE$_2$
Home TAA-FE server
TAA-FE$_2$ client
UE
AM-FE$_3$
Authentication result, configure DSRK
1. Full authentication and authorization
Derive DS-rRK for local domain. Derive rMSK
2. UE moves within the same local domain
Derive rMSK for new location with DS-rRK
Request DSRK
3. UE moves to a different domain
Derive DS-rRK for new domain. Derive rMSK
Y.2018(09)_F08

Figure 8 – Information flow for pre-authentication

The first time UE attaches to the network, it will perform the full authentication process. In order to improve handover performance with lower authentication latency, fast authentication and/or re-authentication is needed for subsequent attachments. That means that when a mobile user hands over from the serving AM-FE to the target AM-FE, the TAA-FE will receive the user authentication request from the target AM-FE and derive an authentication key for it. The user is authenticated based on the authentication key. If TAA-FE identifies that the serving AM-FE and target AM-FE belong to different security domains (i.e., controlled by different local TAA-FE), the TAA-FE will request a domain-specific root key (DSRK) from the AAA server for the new security domain, providing appropriate parameters such as domain name and sequence number in the request, depending on the authentication algorithm. The AAA server uses the handover root key generated in the original full authentication and the received domain-related parameters to generate a DSRK for the local domain. This is shown in the first and third cases of Figure 8. Note that in the case of split mode it may be necessary to carry out this process twice, once for the keying material related to network access authentication and a second time for keying material related to mobility service authentication.

If the UE moves within a local security domain, e.g., the UE just moves to a different access link, the TAA-FE in the local domain may re-authenticate the UE in a single round trip. In this case the target AM-FE shares the handover root key with the serving AM-FE and only the session key needs to be re-negotiated. The TAA-FE may use this root key to authenticate the user. This is shown in the second case of Figure 8.

The pre-authentication process may include generation of keying material for protection of user plane traffic between the UE and the EN-FE, if such protection is required by the user profile.

7.3.3 New path establishment and resource reservation

This clause applies only to handover at layer 3.

New path creation and resource reservation along that path are triggered by a bind indication from the MLM-FE(P) to the HDC-FE. This indication must contain the information required for both path creation and for retrieval by RACF of the session QoS descriptor for the old path.

With this information, the HDC-FE sends a request to RACF to allocate QoS resources on the new path matching the session QoS allocated to the old path. When this operation is complete, the HDC-FE locates the appropriate instance(s) of the L3HEF and issues a request to them to establish a tunnel between the new endpoints. When the tunnel is complete, the L3HEF instance at the anchor point begins to monitor for data flows from the UE through the new tunnel, and decapsulates and forwards them as well as packets received from the old tunnel. In the case of network-based mobility it is possible that a temporary tunnel is established between the old and new tunnel lower end points, in support of seamless handover.

Figure 9 illustrates this procedure.

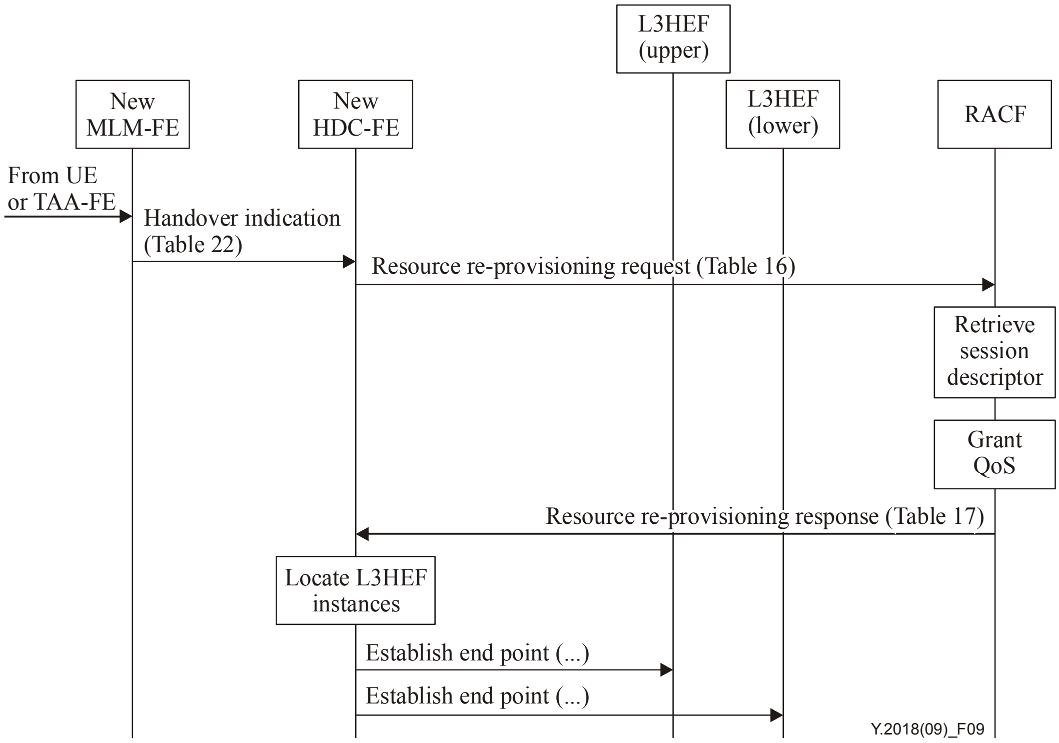

L3HEF (upper)
New MLM-FE
New HDC-FE
L3HEF (lower)
RACF
From UE or TAA-FE
Handover indication (Table 22)
Resource re-provisioning request (Table 16)
Retrieve session descriptor
Grant QoS
Resource re-provisioning response (Table 17)
Locate L3HEF instances
Establish end point (...)
Establish end point (...)
Y.2018(09)_F09

Figure 9 – Procedure for establishing a new layer 3 path

7.3.4 Handover execution

This clause applies only to handover at layer 3.

Handover execution may be initiated in three ways:

a) if the UE has the required capabilities or the tunnel lower end lies in the network (network-based mobility), handover execution is carried out under the explicit control of the HDC-FE; or

b) the L2HE-FE instance monitoring the old access link detects and reports a 'link down' event; or

c) the MLM-FE(P) on the old path receives an unbind indication from the UE and notifies the HDC-FE.

In case a), the HDC-FE receives direct confirmation from the tunnel lower end that it has executed handover. In case b) or c), UE readiness is inferred from its actions.

7.3.4.1 Explicit control of handover execution at the UE

In this case, when the HDC-FE has finished preparation of the new path as described in clause 7.3.3, it issues requests to the tunnel upper and lower ends to commit to the new path. Details of the protocol required to do this without losing packets are out of scope. Once the HDC-FE is informed that commitment is complete, the HDC-FE issues requests to the tunnel upper and lower ends to delete the old tunnel. It sends a request to RACF to deallocate the QoS resources assigned to the old path, from the old access point to the anchor point.

7.3.4.2 Link down indication or unbind indication

If the HDC-FE receives a 'link down' indication from the L2HE-FE instance associated with the old link, or an unbind indication from the MLM-FE, the procedure is similar to the procedure just described, with the exception that if the tunnel lower end was the UE, it does not have to be directed to commit to the new path or to delete the old tunnel. The details of the protocol required to avoid packet loss in this case are out of the scope of this Recommendation. They may differ from what is required in the case described by clause 7.3.4.1.

7.3.5 Routing optimization considerations for network-based handover

When a correspondent UE communicates with the mobile UE, normally packets from the correspondent UE will be intercepted by the transport function associated with the MLM-FE(C) (i.e., the L3HEF at the anchor point), then encapsulated and tunneled to the current location of UE. For data path optimization, the MLM-FE(P) to which a correspondent UE is associated may, based on administrative policies, cooperate with the MLM-FE(P) to which the mobile UE is associated to establish a direct tunnel between their respective networks. At that point the L3HEF at each end will encapsulate packets based on the location binding information exchanged between the two MLM-FE(P)s and forward them directly to its peer L3HEF through the tunnel between them. The peer L3HEF delivers the decapsulated packets to the correspondent or mobile UE respectively.

The L3HEF is required to be aware of active communication between the mobile UE and correspondent UE. The process is triggered when it detects a flow that matches policy indicating that routing optimization may be attempted. It then indicates route optimization to its associated MLM-FE(P) via the HDC-FE. The MLM-FE(P) sends a location management message to the MLM-FE(C) which contains a routing optimization (RO) indication.

Upon receiving an RO request message from the MLM-FE(P), the MLM-FE(C) will perform routing optimization operation not only with the MLM-FE(P) associated with the mobile UE, but also with the MLM-FE(P) associated with the correspondent UE. The MLM-FE(C) may look up its location binding list and determine whether the two MLM-FE(P) instances have both registered to it. In the case where both MLM-FE(P) instances are registered to the same MLM-FE(C) instance, the latter will pass the location of each MLM-FE(P) to the other.

If the two MLM-FE(P) instances register to different MLM-FE(C) instances, the MLM-FE(C) associated with the mobile UE and MLM-FE(C) associated with the correspondent UE will coordinate with each other to provide the location of each MLM-FE(P) instance to the other. If the MLM-FE(C) associated with the mobile UE fails to retrieve the location of the MLM-FE(C) associated with the correspondent UE, it will notify the MLM-FE(P) associated with the mobile UE that route optimization is not available.

After routing optimization operations are completed between the two MLM-FE(P)s, the location binding cache in each MLM-FE(P) is updated and the optimized tunnel is installed. The details for the common MLM-FE(C) case are shown in Figure 10.

NOTE 1 – The messages required for routing optimization are shown in Figure 10, but their detailed definition is for further study.

NOTE 2 – The HDC-FE is shown as a centralized function for convenience, and MLM-FE(P) A is arbitrarily chosen as the initiating entity to start tunnel set-up. It is more realistic to assume that both MLM-FE(P) instances will notify HDC-FE and tunnel set-up and take-down will proceed in a more distributed fashion.

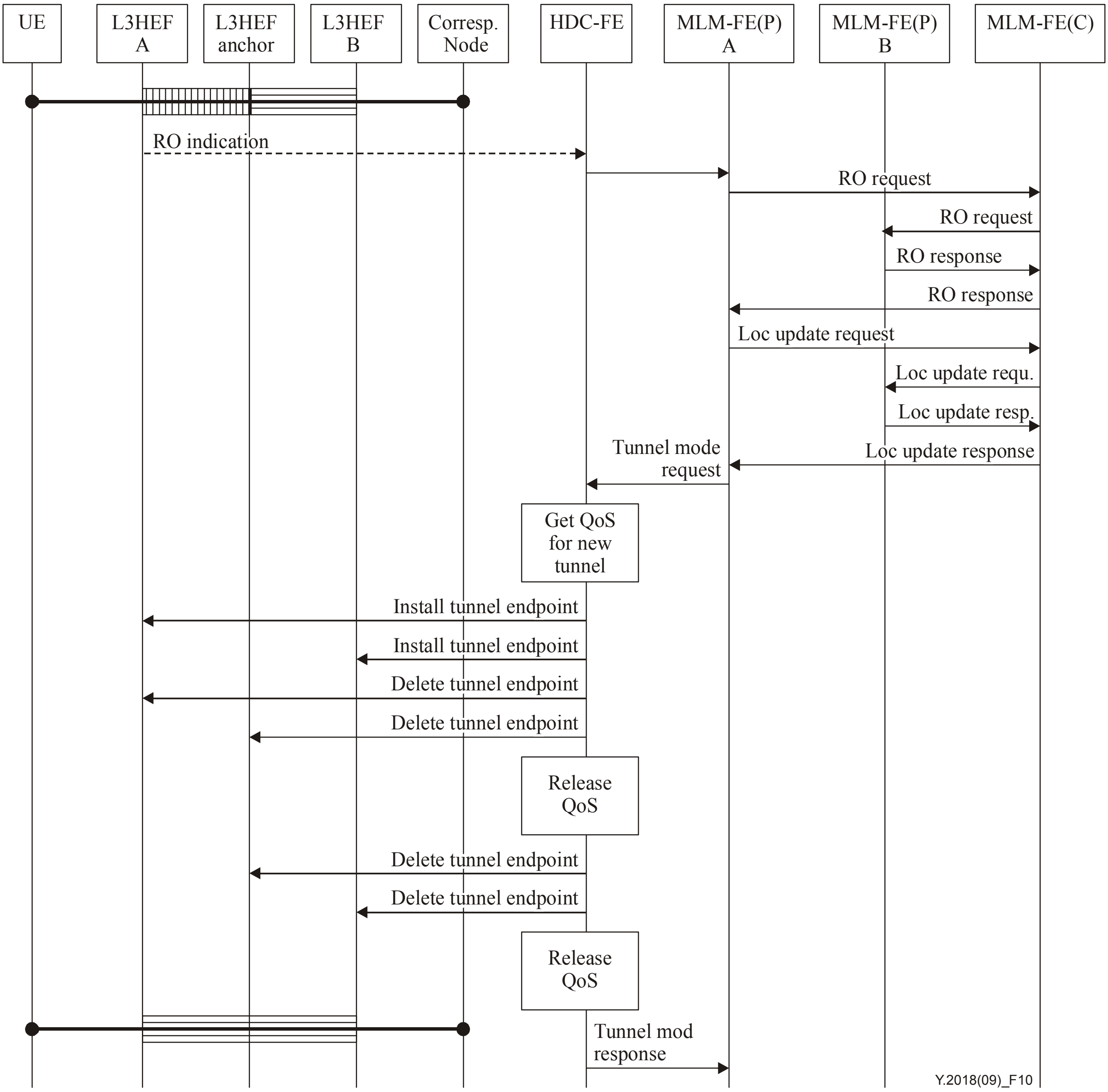


Figure 10 – Routing optimization assuming network-based mobility at each end

8 Security considerations

The path between the UE and the network can pass over a variety of technologies, many of which are open to attack. While the MMCF is considered to be in the trusted zone, the UE and the path from the UE to the MMCF are considered untrusted. The following considerations govern the design of the architecture as it relates to communications between the UE and the MMCF:

8.1 Security threats

T1 UE can be unauthorized to initiate the mobility signalling with MLM-FE.

T2 Mobility signalling can be tampered by intruders.

T3 MLM-FE can be impersonated to provide false information to UE.

T4 UE location can be eavesdropped by intruders.

T5 Traffic redirection attack can happen.

T6 Attacker can insert itself on-path by man-in-the-middle attack.

T7 DDoS attack can consume a large quantity of network resources.

T8 UE can be unauthorized to get information from HDC-FE or NID-FE.

T9 HDC-FE or NID-FE can be impersonated to push false information to UE.

T10 The signalling between UE and HDC-FE or NID-FE can be modified or eavesdropped.

T11 The user plane data can be eavesdropped or modified.

8.2 Security requirements

R1 UE and NID-FE are required to be mutually authenticated.

R2 Signalling between UE and MLM-FE is required to be integrity and confidentiality protected.

R3 Signalling between UE and MLM-FE is required to be protected against replay attacks.

R4 The location privacy of UE is required to be provided.

R5 UE and HDC-FE are required to be mutually authenticated.

R6 Signalling between UE and HDC-FE is required to be integrity and confidentiality protected.

R7 Signalling between UE and HDC-FE is required to be protected against replay attacks.

R8 Low-latency authentication and signalling protection is required to be provided.

R9 Security context transfer is required to be optimized.

R10 The mobility security solution is required to be media independent.

R11 Mechanisms are required to be available to protect user plane traffic between the UE and the EN-FE when the user profile so indicates.

Appendix I

Architecture reference model

(This appendix does not form an integral part of this Recommendation)

The architecture reference models are explained considering both the non-roaming case and the roaming case. The aggregated reference points, m1 through to m4 are used to explain the relationship among UE, A-MMCF and C-MMCF in home and visited networks. m1 is the interface between A-MMCF and C-MMCF, m2 is the interface between UE and A-MMCF, m3 is the interface between UE and C-MMCF, and m4 is the interface between the two C-MMCF in home and visited networks. The MMCF is composed of several functional entities and the detailed reference points between those functional entities and the other functional entities in NGN are defined in clause 6.5.

I.1 Non-roaming architecture and scenarios

The non-roaming architecture in NGN can have two different architectures according to the type of mobility management protocols supported, host-based or network-based mobility management protocols.

Figure I.1 shows a non-roaming architecture when a network-based mobility management protocol is considered while using an interface between A-MMCF and C-MMCF.

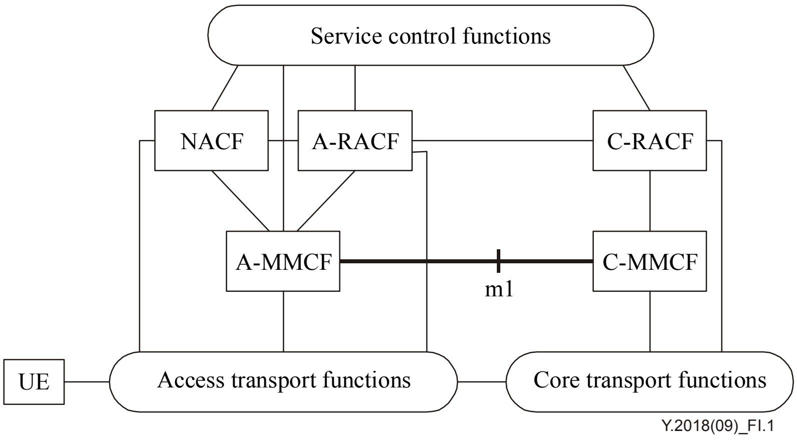


Figure I.1 – Non-roaming architecture for network-based mobility using m1

Figure I.2 shows a non-roaming architecture when a host-based mobility management protocol is considered while having a direct relationship between UE and C-MMCF without involving A-MMCF.

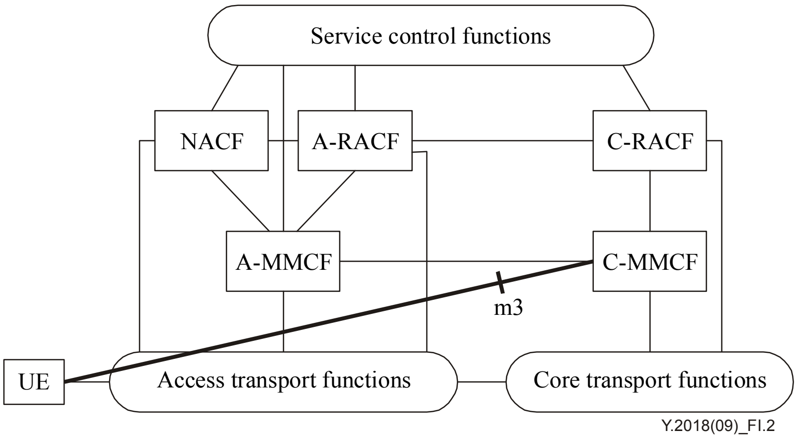


Figure I.2 – Non-roaming architecture for host-based mobility using m3

Figure I.3 shows a non-roaming architecture when host-based mobility management protocol is considered while having the interfaces between UE and A-MMCF and between A-MMCF and C-MMCF.

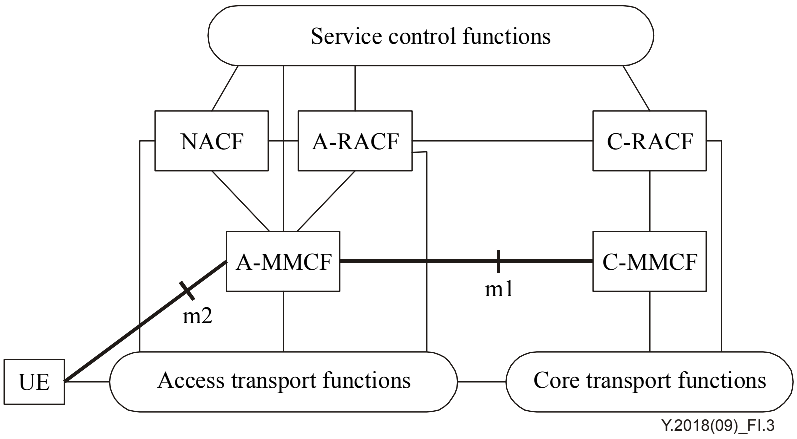


Figure I.3 – Non-roaming architecture for host-based mobility using m1 and m2

I.2 Roaming architecture and scenarios

The roaming architecture in NGN can also have two different architectures according to the type of mobility management protocols supported, host-based or network-based mobility management protocols.

Figure I.4 shows a roaming architecture when a network-based mobility management protocol is considered while using the direct interface between the A-MMCF in the visited network and the C-MMCF in the home network.

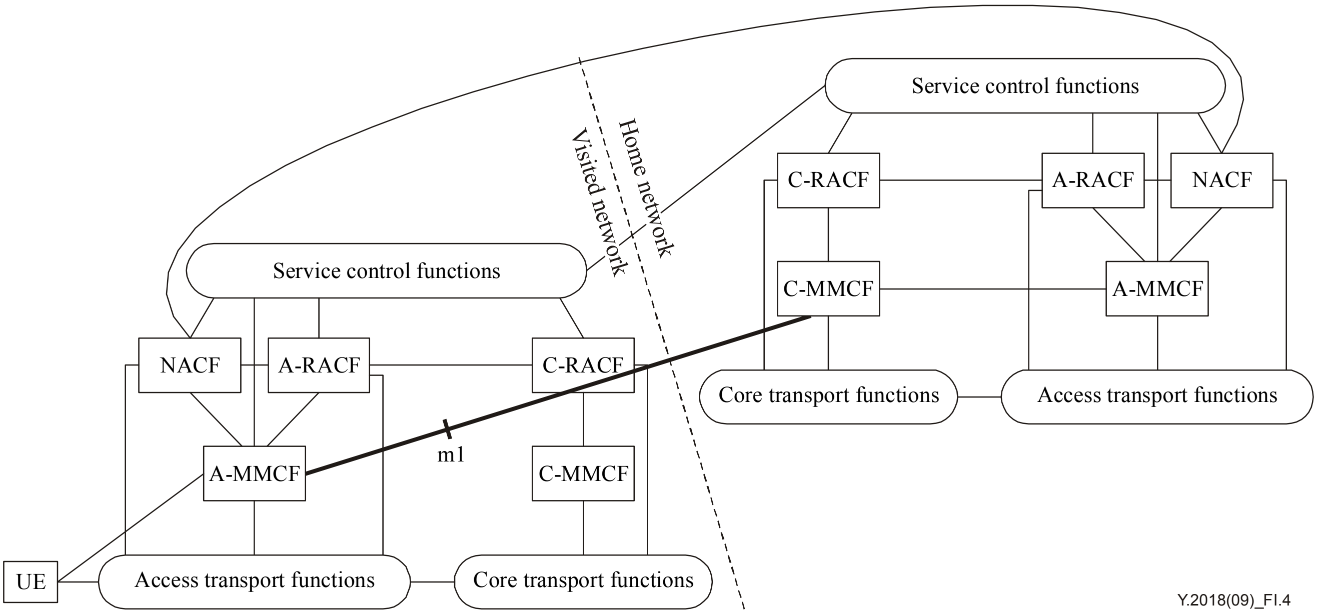


Figure I.4 – Roaming architecture for network-based mobility using m1

Figure I.5 shows a roaming architecture when a network-based mobility management protocol is considered while using the interfaces between the A-MMCF and the C-MMCF in the visited network and between the C-MMCF in the visited network and the C-MMCF in the home network.

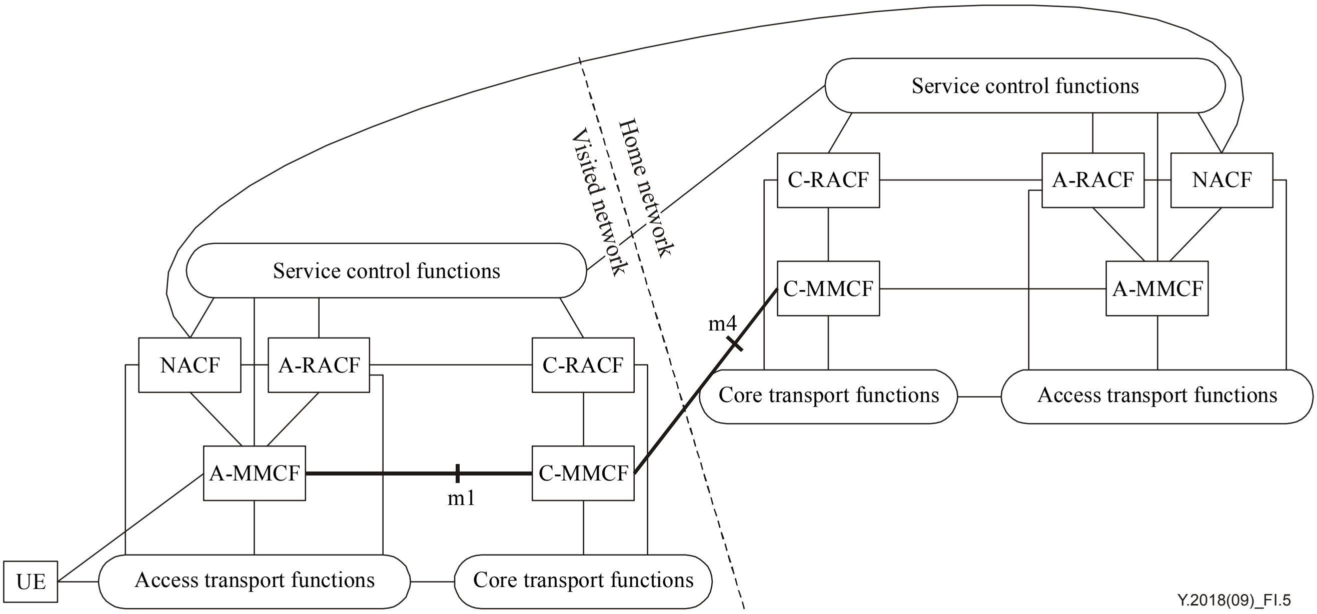


Figure I.5 – Roaming architecture for network-based mobility using m1 and m4

Figure I.6 shows a roaming architecture when a host-based mobility management protocol is considered while using a direct interface between UE and the C-MMCF in the home network.

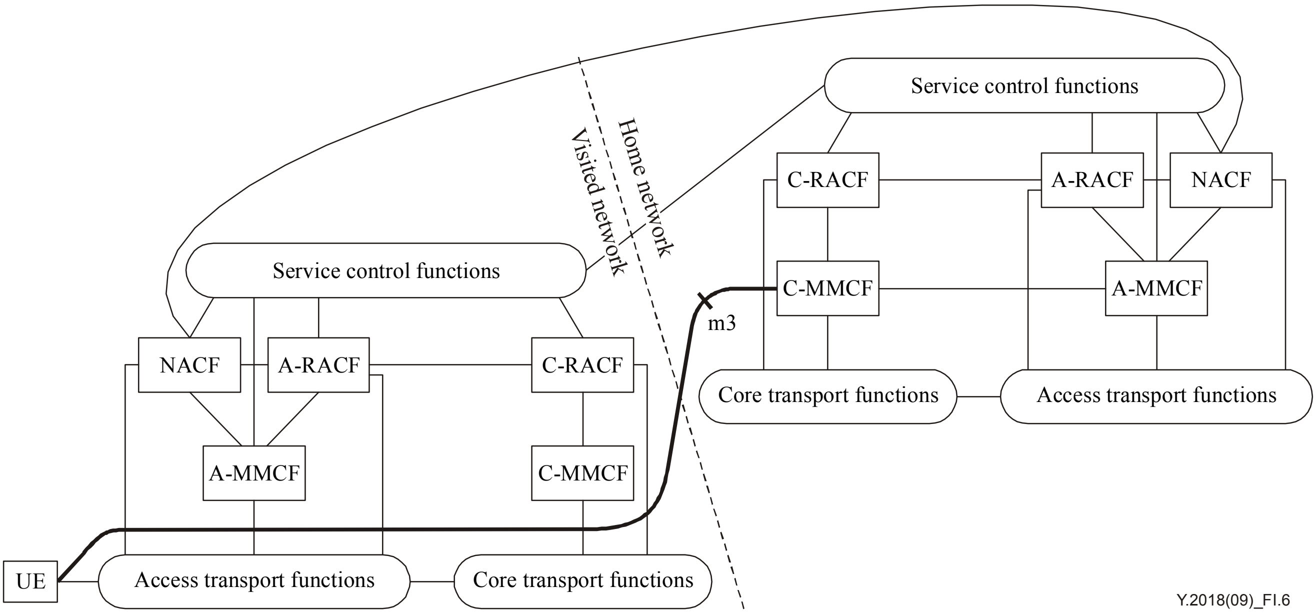


Figure I.6 – Roaming architecture for host-based mobility using m3

Figure I.7 shows a roaming architecture when a host-based mobility management protocol is considered while using the interfaces between UE and the A-MMCF in the visited network and between the A-MMCF in the visited network and the C-MMCF in the home network.

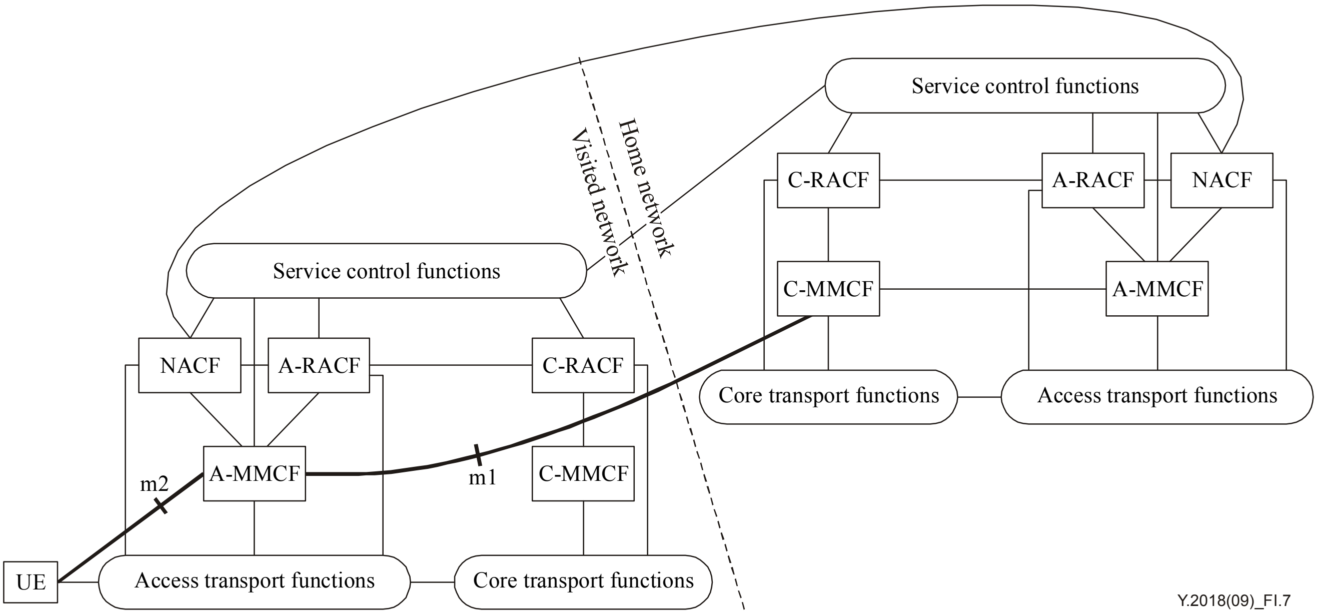


Figure I.7 – Roaming architecture for host-based mobility using m1 and m2

Figure I.8 shows a roaming architecture when a host-based mobility management protocol is considered while using the interfaces between UE and the C-MMCF in the visited network and between the C-MMCF in the visited network and the C-MMCF in the home network.

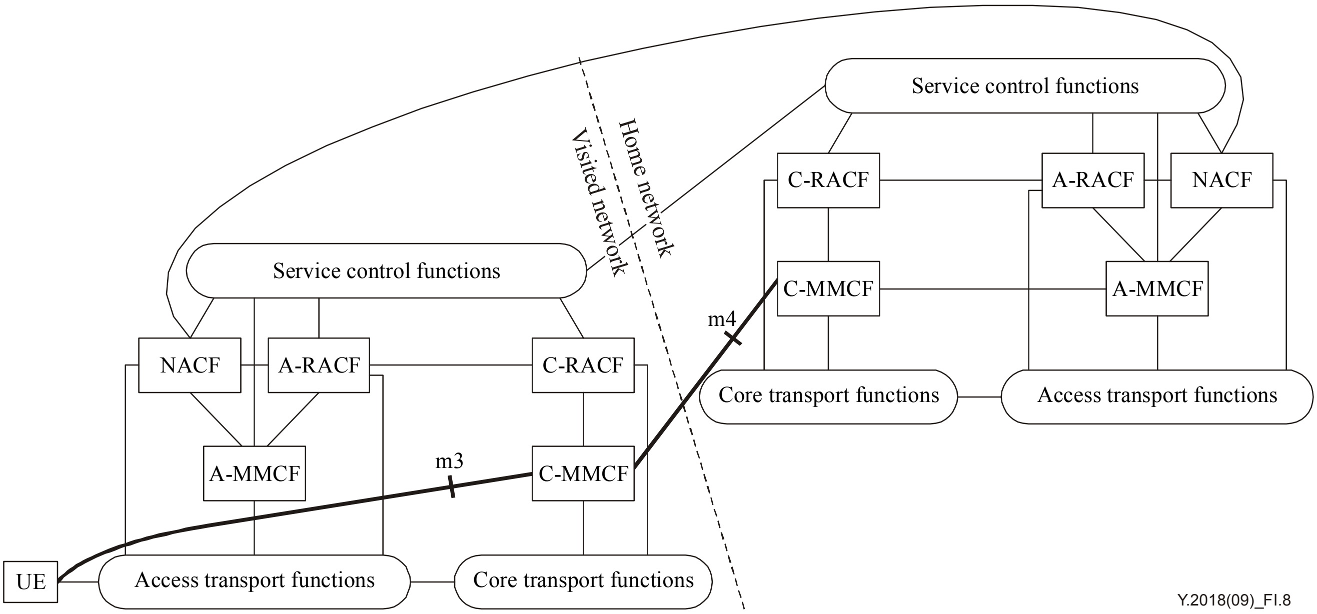


Figure I.8 – Roaming architecture for host-based mobility using m3 and m4

Figure I.9 shows a roaming architecture when a host-based mobility management protocol is considered while using the interfaces between UE and the A-MMCF in the visited network, between the A-MMCF and the C-MMCF in the visited network, and between the C-MMCF in the visited network and the C-MMCF in the home network.

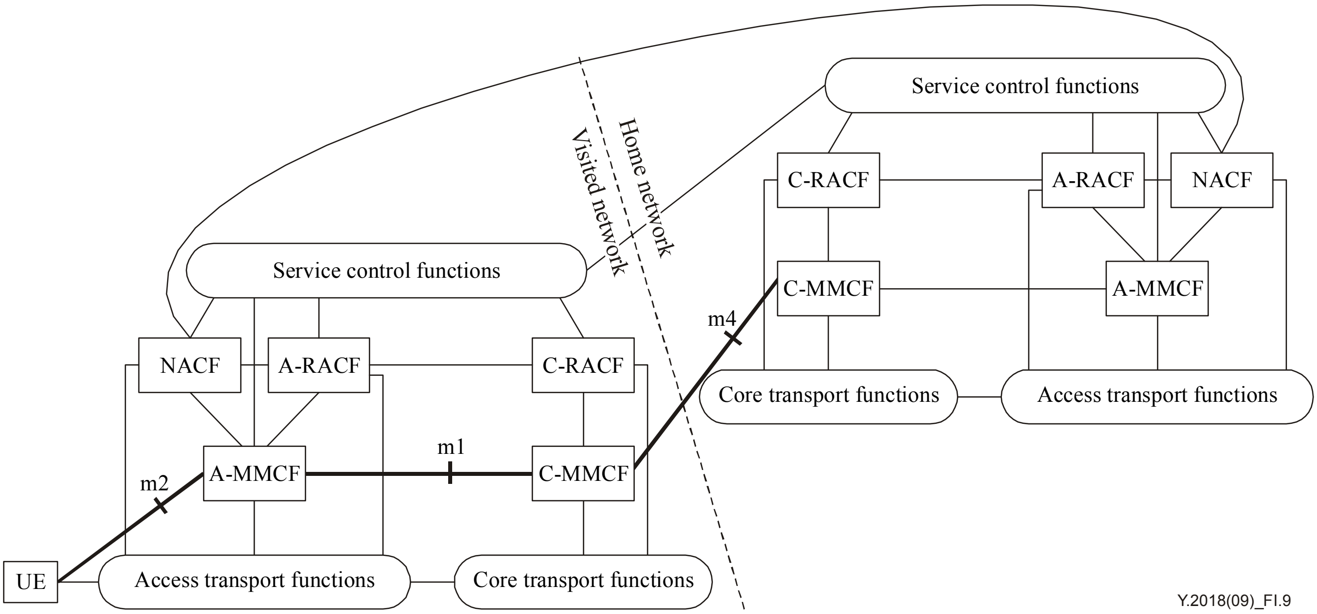


Figure I.9 – Roaming architecture for host-based mobility using m1, m2 and m4

Appendix II

Mapping between functions defined in this Recommendation and IETF entities

(This appendix does not form an integral part of this Recommendation)

II.1 The IETF mobility architectures

The IETF has been working on mobility at the IP level for several years, beginning with MIPv4 ([b-IETF RFC 3344]), working through MIPv6 ([b-IETF RFC 3775]), and a variety of optimizations and extensions including proxy mobile IP (PMIP) ([b-IETF RFC 5213]) and hierarchical mobile IP (HMIP) ([b-IETF RFC 4140]). Each of the variants just mentioned introduces its own architectural elements. The only network element common to all of these architectures, which are individually described below, is the home agent. However, this appendix demonstrates that the IETF architectural components can be shown to share certain sets of functions in common. These functions are the same as the ones identified in clause 6.4.

Note that each of these architectures includes the mobile node and the correspondent node as well as the network elements it identifies. For our purpose, the mobile node can be identified with the UE, and the correspondent node, most conveniently, with the SCF.

II.1.1 MIPv4

Mobile IP v4 (MIPv4) requires the UE to support functions specific to mobility. It identifies two network entities: the foreign agent (FA) and the home agent (HA). The FA can be collocated with the UE, creating a scenario similar to MIPv6. The IETF architecture for MIPv4 is shown in Figure II.1.

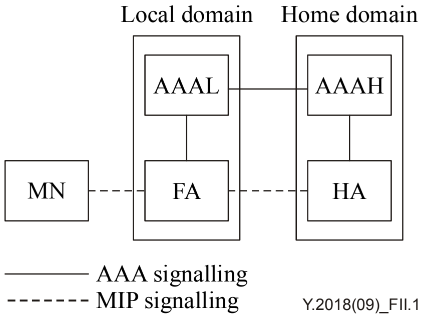


Figure II.1 – MIPv4 architecture according to the IETF

Mobile IP requires every registration to be handled between the home agent (HA) and the foreign agent (FA), as shown by the dashed line in Figure II.1. During the initial registration, some operations happen (such as allocating HoA, HA address, derive MSAs) that enable the home agent and foreign agent to perform subsequent mobile IP registrations. After the initial registration, the AAAH and AAAL in Figure II.1 will not be needed, and subsequent mobile IP registrations will only follow the lower control path between the foreign agent and the home agent.

Table II.1 lists the functions that must be supported by the FA and the HA, and matches these functions to those defined in clause 6.4.

Table II.1 – Mapping of MIPv4 network entities with MMCF functions

Entity	Functional description	Function
FA	Initiates location update signalling	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF
HA	Binds the local mobility information	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF

II.1.2 MIPv6

Mobile IP v6 (MIPv6) requires the UE to support functions specific to mobility. It identifies one network entity: the home agent (HA).

Table II.2 lists the functions that must be supported by the HA, and matches these functions to those defined in clause 6.4.

Table II.2 – Mapping of MIPv6 network entities with MMCF functions

Entity	Functional description	Function
HA	Binds the local mobility information	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF

II.1.3 Proxy MIP

Proxy mobile IP (PMIPv6) does not require the UE to support functions specific to mobility. It identifies two network entities: the mobility access gateway (MAG) and the local mobility anchor (LMA).

Figure II.2 shows the message flow defined by PMIPv6 for initial attachment. Figure II.3 shows the PMIPv6 signalling for handover.

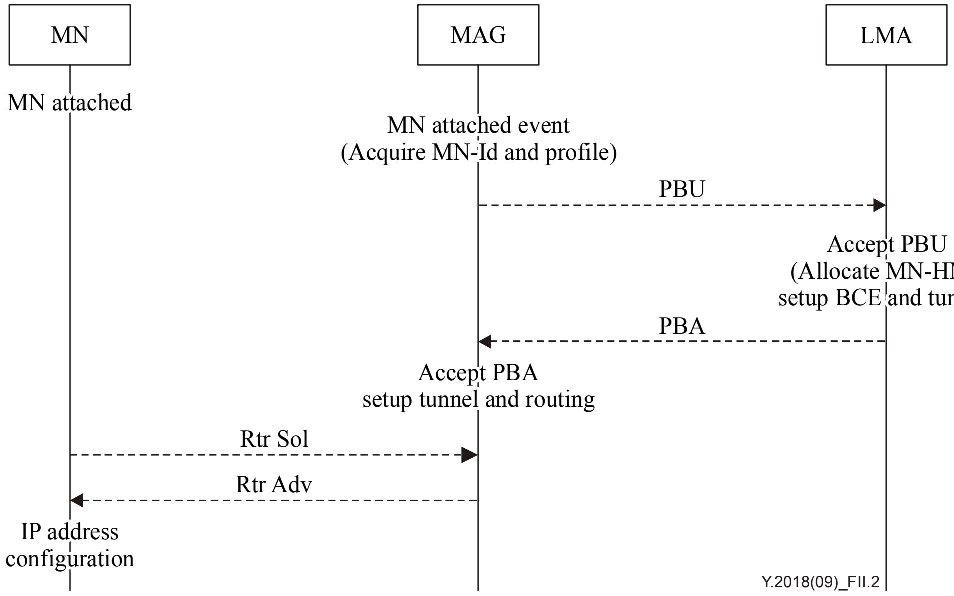


Figure II.2 – Signalling flows for PMIPv6 initial attachment

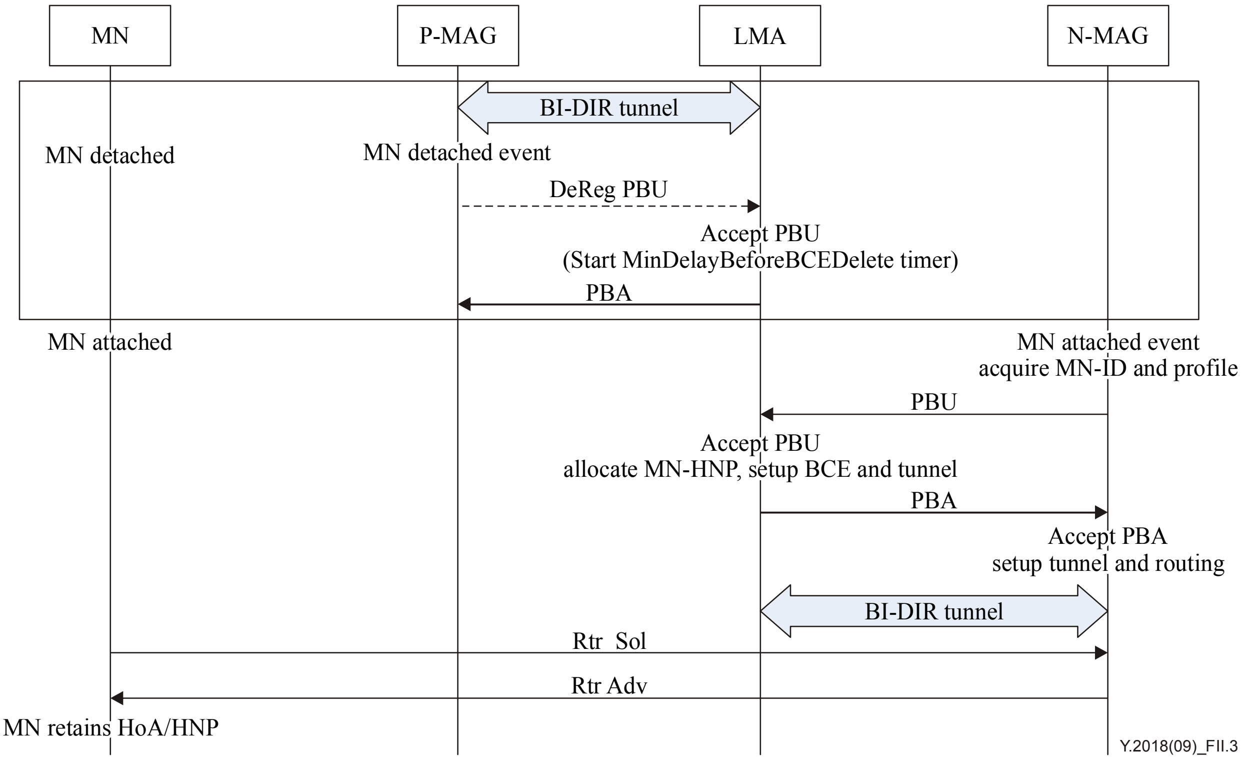


Figure II.3 – PMIPv6 signalling flows for handover

Table II.3 lists the functions that must be supported by the MAG and the LMA, and matches these functions to those defined in clause 6.4.

Table II.3 – Mapping of Proxy MIP network entities with MMCF functions

Entity	Functional description	Function
MAG	Initiates location update signalling	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF
LMA	Binds the local mobility information	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF

II.1.4 Hierarchical MIP

Hierarchical MIP [b-IETF RFC 4140] identifies two network entities: the home agent (HA) and the mobility anchor point (MAP).

Table II.4 – Mapping of hierarchical MIP network entities with MMCF functions

Entity	Functional description	Function
MAP	Initiates location update signalling	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF
HA	Binds the local mobility information	MLM-FE
	Indicates tunnel set-up	HDC-FE
	Provides a tunnel end point	L3HEF

Appendix III

Mapping between this Recommendation and 3GPP functions

(This appendix does not form an integral part of this Recommendation)

III.1 Introduction

This appendix demonstrates the consistency of the architecture presented in the body of this Recommendation with the architecture being specified for the 3GPP evolved packet system (EPS).

III.2 References

The 3GPP entities and the functions they perform are taken from [b-3GPP 23.401], [b-3GPP 23.402] and [b-3GPP 36.300].

III.3 Architectural scenarios

This clause presents representative architectural arrangements to aid in the understanding of the mapping presented in clause III.4.

III.3.1 Non-roaming architecture for 3GPP accesses within EPS using PMIP-based S5

The relevant 3GPP architectural reference diagram for this scenario is shown in Figure III.1. It is assumed in the mapping that follows that the dashed oval encloses the access network as understood within the ITU-T NGN architecture.

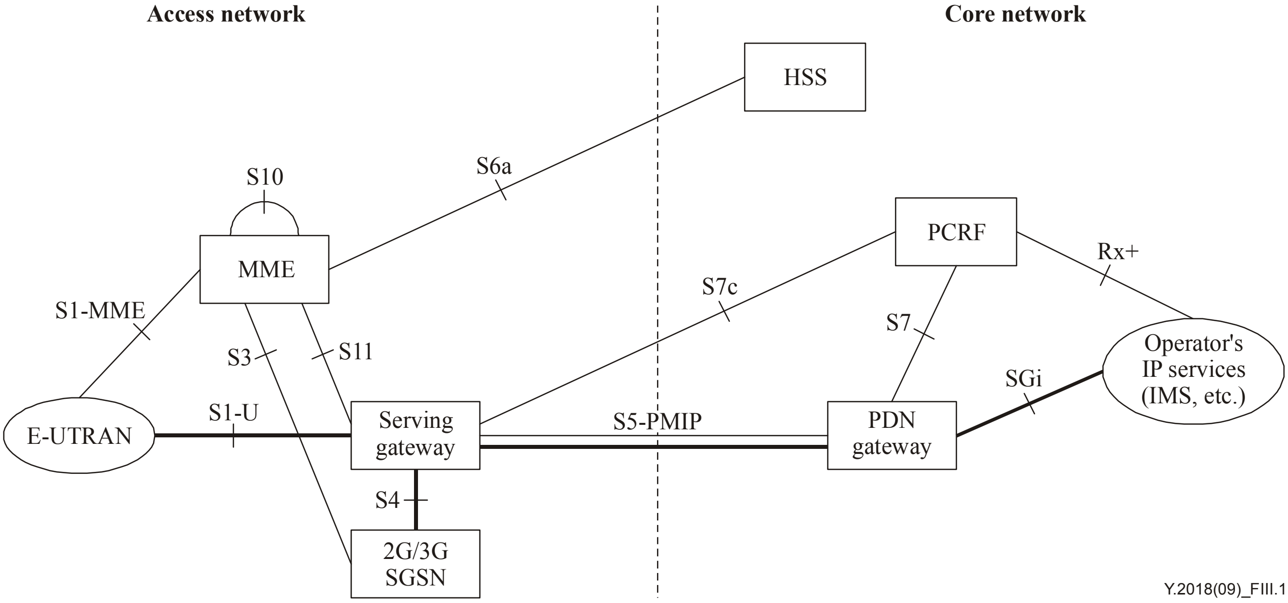


Figure III.1 – Non-roaming architecture for 3GPP accesses within EPS using PMIP-based S5

III.3.2 Roaming architecture for 3GPP accesses within EPS using PMIP-based S8

The relevant 3GPP architectural reference diagram for this scenario is shown in Figure III.2.

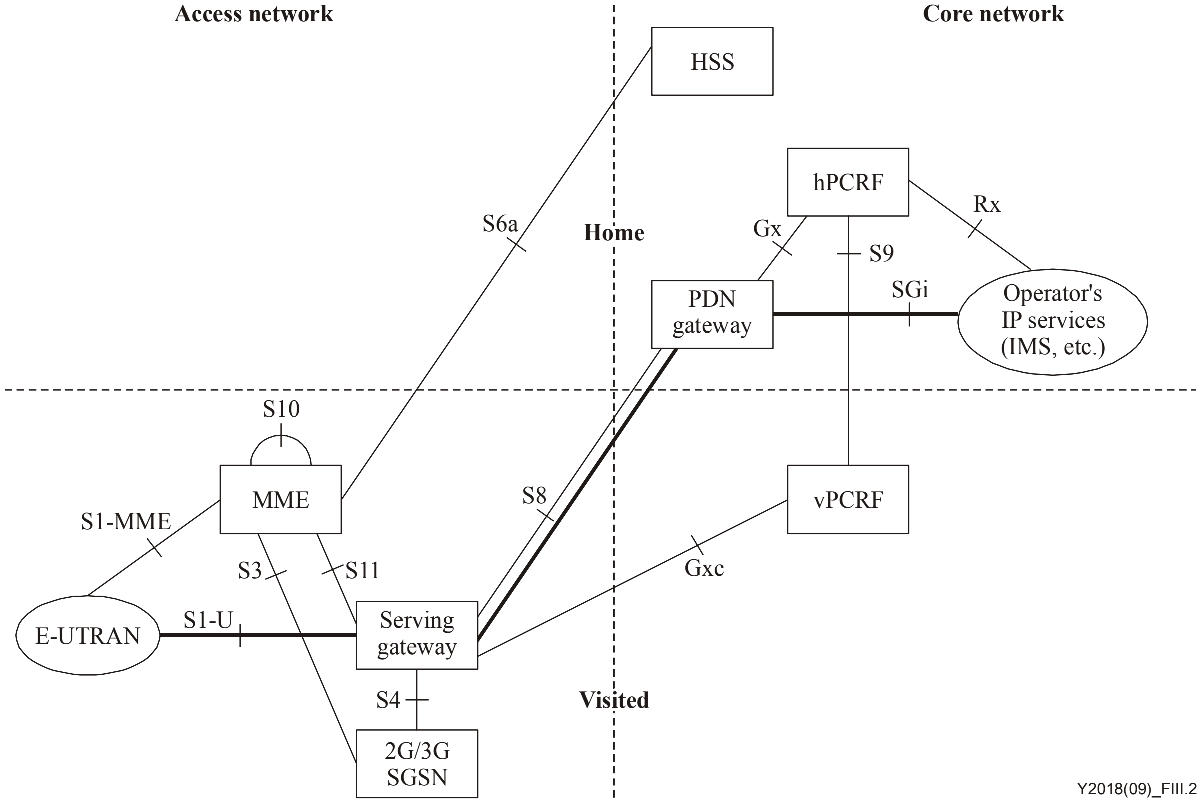


Figure III.2 – Roaming architecture for 3GPP accesses within EPS using PMIP-based S8

The mapping of functional components in this case is the same as in the non-roaming case, with the exception that the visited network policy and charging rules function (vPCRF) must now be considered. Aside from its relay function, the vPCRF is really a source of policy for connection to the backbone network lying between the visited public land mobile network (VPLMN) and home public land mobile network (HPLMN).

III.3.3 Roaming architecture for EPS using S5, S2c – Local breakout

Figure III.3 shows the architecture for this case. Host-based mobility service is provided, with UE signalling via the S2c interface.

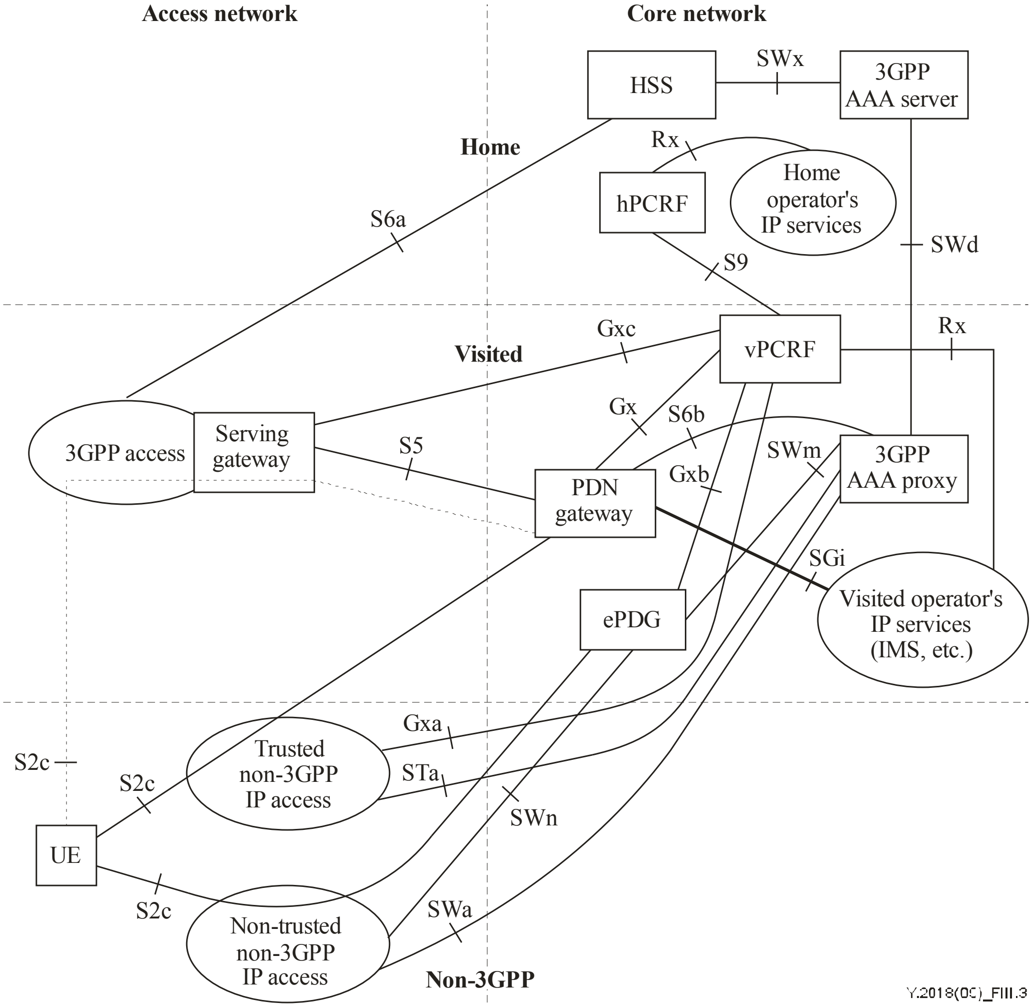


Figure III.3 – Roaming architecture for EPS using S5, S2c – Local breakout

III.4 Mapping from 3GPP entities to ITU-T Y.2018 entities

Table III.1 lists key entities in the 3GPP EPS architecture, their functions, and the ITU-T Y.2018 entities responsible for those functions.

Table III.1 – Mapping from 3GPP to ITU-T Y.2018 entities

3GPP entity	Functions performed	ITU-T Y.2018 entity responsible
eNodeB	Functions for radio resource management: radio bearer control, radio admission control, connection mobility control, dynamic allocation of resources to UEs in both uplink and downlink (scheduling)	AN-FE
	IP header compression and encryption of user data stream	AN-FE
	Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE	AR-FE
	Routing of user plane data towards serving gateway	AN-FE
	Scheduling and transmission of paging messages (originated from the MME)	AN-FE
	Scheduling and transmission of broadcast information (originated from the MME or O&M)	AN-FE
	Measurement and measurement reporting configuration for mobility and scheduling	AN-FE
	Scheduling and transmission of ETWS messages (originated from the MME)	AN-FE
Mobility management entity (MME)	NAS signalling	NACF
	NAS signalling security	NACF
	AS security control	NACF
	Inter CN node signalling for mobility between 3GPP access networks	NACF
	Idle mode UE reachability (including control and execution of paging retransmission)	TBD*
	Tracking area list management (for UE in idle and active mode)	TBD (Note 1)
	PDN GW and serving GW selection	TBD (Note 2)
	MME selection for handovers with MME change	NACF
	SGSN selection for handovers to 2G or 3G 3GPP access networks	NACF
	Roaming	NACF (TAA-FE)
	Authentication	NACF (TAA-FE)
	Bearer management functions including dedicated bearer establishment	HDC-FE
	Support for ETWS message transmission	NACF

Table III.1 – Mapping from 3GPP to ITU-T Y.2018 entities

3GPP entity	Functions performed	ITU-T Y.2018 entity responsible
Serving gateway	The local mobility anchor point for inter-eNB handover	L2HE-FE
	Mobility anchoring for inter-3GPP mobility	L2HE-FE
	E-UTRAN idle mode downlink packet buffering and initiation of network triggered service request procedure	L2HE-FE
	Lawful interception	EN-FE
	Packet routing and forwarding	EN-FE
	Transport level packet marking in the uplink and the downlink	EN-FE
	Accounting on user and QCI granularity for inter-operator charging	EN-FE
	UL and DL charging per UE, PDN, and QCI	EN-FE
	Originator of PMIP signalling. Proxy point for PMIP signalling (chained PMIP)	MLM-FE(P)
	Lower IP tunnel end point	L3HEF
Packet data network (PDN) gateway	Per-user based packet filtering (by e.g., deep packet inspection)	ABG-FE
	Lawful interception	ABG-FE
	UE IP address allocation	NACF
	DHCPv4 (server and client) and DHCPv6 (client and server) functions	NACF
	UL and DL service level charging, gating and rate enforcement	ABG-FE
	DL rate enforcement based on AMBR	ABG-FE
	Transport level packet marking in the downlink	ABG-FE
	Terminator of PMIP signalling	MLM-FE(C)
	Upper tunnel end point	L3HEF
	Terminator of DSMIPv6 signalling from the UE	MLM-FE(P) collocated with MLM-FE(C)

* TBD: to be defined.

NOTE 1 – TLM-FE is a candidate.

NOTE 2 – TUP-FE is a candidate.

Bibliography

[b-3GPP 23.401] 3GPP TS 23.401 V8.5.0 (2009), *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 8)*.

[b-3GPP 23.402] 3GPP TS 23.402 V8.5.0 (2009), *Architecture enhancements for non-3GPP accesses (Release 8)*.

[b-3GPP TS 33.234] 3GPP TS 33.234 V8.1.0 (2008), *3G security; Wireless Local Area Network (WLAN) interworking security*.

[b-3GPP 36.300] 3GPP TS 36.300 V8.8.0 (2009), *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 8)*.

[b-IEEE 802.21] IEEE 802.21 (2008), *IEEE Standard for Local and Metropolitan Area Networks – Media Independent Handover Services*.

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 4140] IETF RFC 4140 (2005), *Hierarchical Mobile IPv6 Mobility Management (HMIPv6)*.

[b-IETF RFC 4283] IETF RFC 4283 (2005), *Mobile Node Identifier Option for Mobile IPv6*.

[b-IETF RFC 4640] IETF RFC 4640 (2006), *Problem Statement for bootstrapping Mobile IPv6 (MIPv6)*.

[b-IETF RFC 5026] IETF RFC 5026 (2007), *Mobile IPv6 Bootstrapping in Split Scenario*.

[b-IETF RFC 5149] IETF RFC 5149 (2008), *Service Selection for Mobile IPv6*.

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010