International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2022

(08/2011)

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

Next Generation Networks – Frameworks and functional architecture models

Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks

Recommendation ITU-T Y.2022

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
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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

Recommendation ITU-T Y.2022

Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks

Summary

Recommendation ITU-T Y.2022 describes the functional architecture for the support of host-based of ID/locator separation in NGN. ID/locator separation in NGN is concerned with decoupling the semantics of IP addresses into the semantics of identifiers (node IDs) and locators (LOCs) as described in Recommendation ITU-T Y.2015.

This Recommendation defines the functional entities and the related reference points, based on the framework architecture provided in Recommendation ITU-T Y.2012.

This Recommendation covers only the host-based case of ID/locator separation (the separation of node ID and locator is done in the user equipment and not in the network).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2022	2011-08-06	13

Keywords

Functional architecture, ID/LOC mapping, NGN.

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 not 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/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	3
6	Overview and architecture of ID/LOC separation in the NGN	4
	6.1 Overview of ID/LOC separation in the NGN	4
	6.2 Architecture overview	4
7	Functional architecture	5
	7.1 High level functions	6
	7.2 Functional entities	7
	7.3 Reference points	7
8	Procedures of ID/LOC split in NGN	10
	8.1 Attachment procedure	10
	8.2 Communication establishment using node ID	12
	8.3 Communication establishment for multihoming	12
	8.4 Communication update when the LOC is changed	13
	8.5 Detachment procedures	14
9	Security considerations	15
Bibliography		16

Recommendation ITU-T Y.2022

Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks

1 Scope

This Recommendation describes the functional architecture for the support of host-based node identifier (ID) and node locator (ID/locator) separation in next generation networks (NGN), based on the requirements provided in [ITU-T Y.2015].

This Recommendation addresses the following aspects:

– The functional architecture model for ID/locator separation in NGN.

– Identification of functions including the definition of functional entities and reference points.

– A description of relevant procedures and interactions with other components of the NGN functional architecture as defined in [ITU-T Y.2012].

This Recommendation covers only the host-based case of ID/locator separation, where the separation of node ID and locator is done in the user equipment (UE) and not in the network.

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 X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[ITU-T Y.2015] Recommendation ITU-T Y.2015 (2009), *General requirements for ID/locator separation in NGN*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 address [b-ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.2 credential [ITU-T Y.2720]: An identifiable object that can be used to authenticate the claimant is what it claims to be and to authorize the claimant's rights.

3.1.3 identifier [b-ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.4 ID/LOC mapping [ITU-T Y.2015]: ID/LOC mapping is an association between a node ID and one or more LOCs.

NOTE 1 – A single node ID or several node IDs can be associated with many LOCs associated with a single terminal. The node ID to LOC mapping can have the one-to-one, one-to-many, or many-to-one relationship.

NOTE 2 – ID/LOC mapping is also called ID/LOC binding.

3.1.5 ID/LOC mapping function [ITU-T Y.2015]: An ID/LOC mapping function gets mapping information from an ID/LOC mapping storage function and uses the corresponding node ID and/or LOC in packet headers. The ID/LOC mapping function works in a close correlation with the transport user profile associated with the transport control function.

NOTE – ID/LOC mapping functions can be physically located in an NGN terminal, an access border gateway, or any other NGN components.

3.1.6 ID/LOC mapping storage function [ITU-T Y.2015]: An ID/LOC mapping storage function stores the mapping of NGN identifiers, node IDs and LOCs. This function also updates mapping information, as well as provides mapping information to other functions on request. The mapping storage function can be physically located in an NGN terminal or with other NGN components.

3.1.7 ID/LOC separation [ITU-T Y.2015]: ID/LOC separation is decoupling the semantic of IP address into the semantics of node IDs and LOCs. Distinct namespaces are used for node IDs and LOCs so that they can evolve independently. LOCs are associated with the IP layer whereas node IDs are associated with upper layers in such a way that ongoing communication sessions or services shall not be broken by changing LOCs due to mobility and multihoming.

NOTE – In the context of this Recommendation, a completely new namespace for node IDs can optionally be created that would leave the IP address space more or less intact for LOCs, allowing routing technologies to be developed independently of end-host mobility and end-host multihoming implications.

3.1.8 locator (LOC) [ITU-T Y.2015]: A locator is the network layer topological name for an interface or a set of interfaces. LOCs are carried in the IP address fields as packets traverse the network.

NOTE – IP addresses can gradually become pure LOCs. However, on the contrary, it cannot be said that a LOC is an IP address. An IP address may associate with the IP layer as well as upper layer protocols (such as TCP and HTTP), whereas a LOC will associate with only the IP layer and be used in IP address fields.

3.1.9 node ID [ITU-T Y.2015]: A node ID is an identifier used at the transport and higher layers to identify the node as well as the endpoint of a communication session. A node ID is independent of the node location as well as the network to which the node is attached so that the node ID is not required to change even when the node changes its network connectivity by physically moving or

simply activating another interface. The node IDs should be used at the transport and higher layers for replacing the conventional use of IP addresses at these layers. A node may have more than one node ID in use.

NOTE – Unless otherwise specified, the term "ID" used in this Recommendation represents a node ID, not an NGN identifier specified in this or any other Recommendations.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AM-FE	Access Management Functional Entity
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GSC-FE	General Services Control Functional Entity
ID	Identifier
ILCF	ID/LOC mapping Control Functions
ILMF	ID/LOC Mapping Functions
ILM-FE	ID/LOC Mapping Functional Entity
ILMS-FE	ID/LOC Mapping Storage Functional Entity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LOC	Locator
NACF	Network Attachment Control Functions
NAC-FE	Network Access Configuration Functional Entity
NGN	Next Generation Networks
P-CSC-FE	Proxy Call Session Control Functional Entity
RACF	Resource and Admission Control Functions
SCF	Service Control Functions
TAA-FE	Transport Authentication and Authorization Functional Entity
TLM-FE	Transport Location Management Functional Entity
TUP-FE	Transport User Profile Functional Entity
UE	User Equipment

5 Conventions

None.

6 Overview and architecture of ID/LOC separation in the NGN

6.1 Overview of ID/LOC separation in the NGN

According to the definition of NGN provided in [ITU-T Y.2001], the NGN framework is expected to support advanced architectural objectives over a unified IP network. NGN decouples IP-based services and transport, allowing them to be offered separately and evolve independently.

ID/LOC separation allows the decoupling of the IP addresses' semantics into the semantics of node IDs and LOCs as described in [ITU-T Y.2015]. LOC(s) are associated with the IP layer, whereas node IDs are associated with upper layers related to the NGN service stratum and applications.

Therefore, when ID/LOC separation is used in NGN, NGN specific functions are necessary to map the conventional NGN identifier to node IDs and to dynamically map the node ID to one or more LOCs. The relationship between the NGN identifier, node ID, and LOC(s), in order to support ID/LOC separation in the NGN functional architecture is described in Figure 6-1.

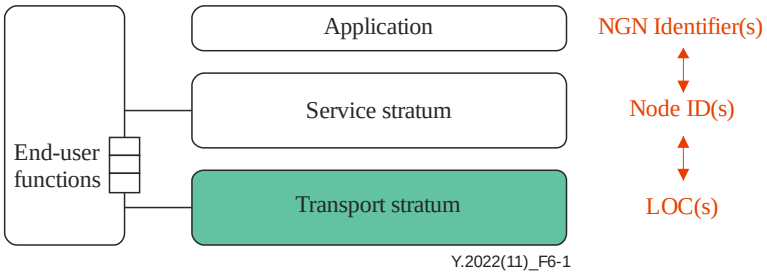

Figure 6-1 – ID/LOCs separation in NGN

Figure 6-1 shows the stage mappings between NGN identifiers, node IDs, and LOC(s) as used in the context of ID/LOC separation in NGN.

At the first stage, the mapping between the NGN identifier and the node ID takes place, while at the second stage the mapping between the node ID and the LOC takes place according to [ITU-T Y.2015].

In the case of host-based ID/LOC separation, the Node ID is an identifier used to identify the UE while the LOC(s) corresponds to the IP address(es) of the UE which is used for addressing and routing. As shown in Figure 6-1, applications are not bound by the locator of the UE, but bound by the node ID of the UE. So each UE has a node ID, and one or more LOCs are allocated to the UE by the network when the UE attaches to the network.

The network-based ID/LOC split approach (which is out of the scope of this Recommendation) means that the mapping of a node ID to a locator is not performed in the UE itself but in the network.

6.2 Architecture overview

This clause provides an overview of the architecture for the support of host based ID/LOC separation in NGN.

The NGN functional architecture supporting ID/LOC split functions is described in Figure 6-2. Two new functional groups, ID/LOC mapping control functions (ILCF) and ID/LOC mapping functions (ILMF) are added to the transport control functions and the end-user functions, respectively.

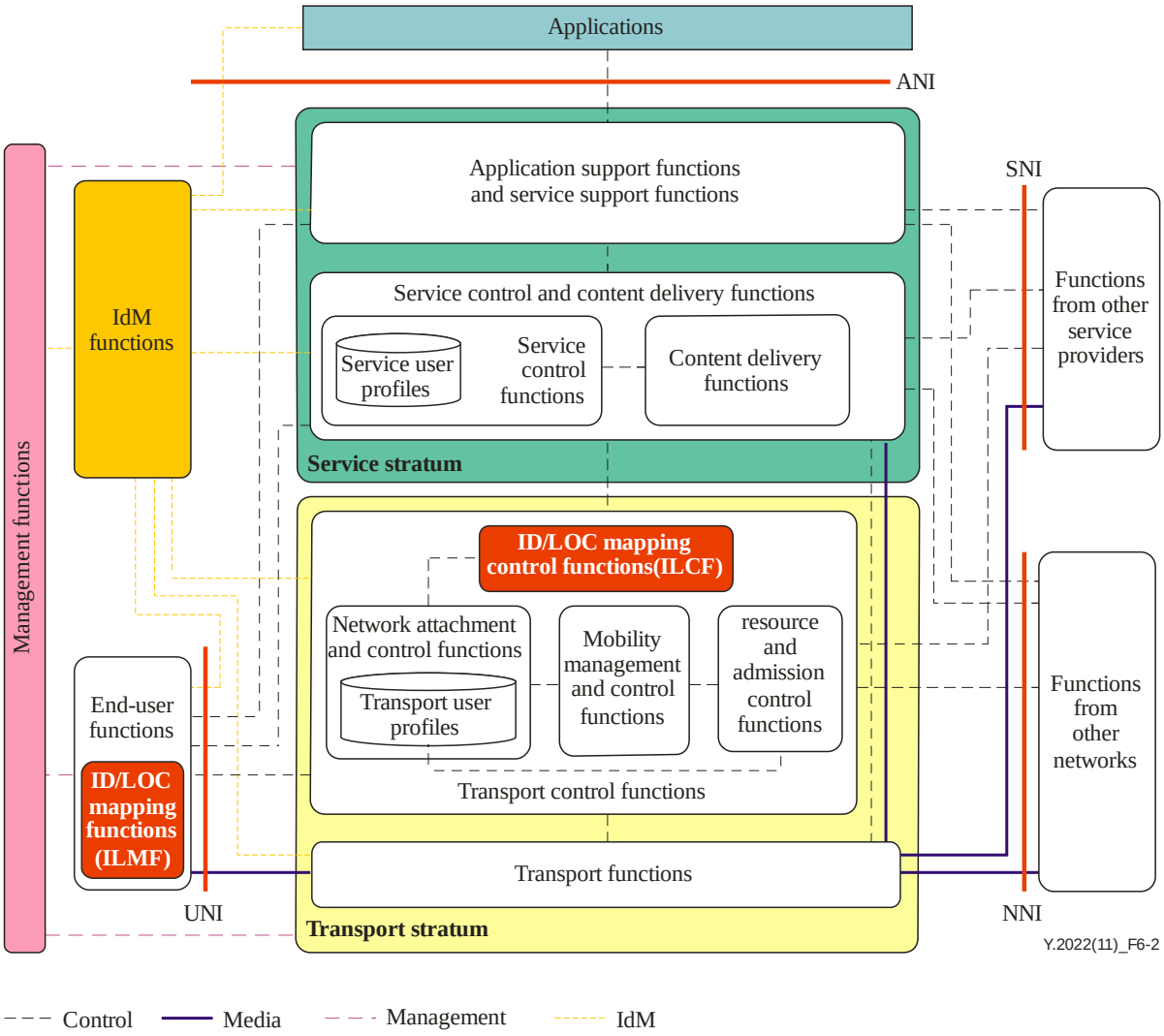

Figure 6-2 – Architecture overview for ID/LOC separation in NGN

The ILCF provides the control information and signalling required to implement ID/LOC mapping functions. It collects, stores, updates, and distributes ID/LOC mapping information. The ILMF performs ID/LOC mapping functions using ID/LOC mapping information obtained from the ILCF.

7 Functional architecture

Figure 7-1 shows the functional architecture for the support of ID/LOC separation in NGN. Details of the general NGN architecture [ITU-T Y.2012] have been omitted to bring out only the relevant points.

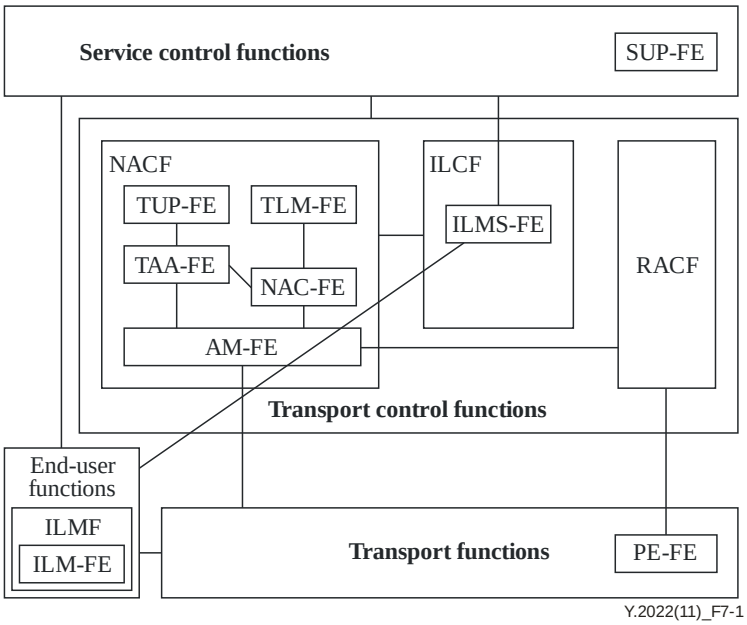

Figure 7-1 – Functional architecture for host-based ID/LOC separation in NGN

The ILCF includes the ID/LOC mapping storage functional entity (ILMS-FE), whereas the ILMF includes the ID/LOC mapping functional entity (ILM-FE).

7.1 High level functions

ID/LOC separation involves the following functions:

- service control functions (SCF);
- network attachment control functions (NACF);
- ID/LOC mapping control functions (ILCF);
- ID/LOC mapping functions (ILMF).

7.1.1 Service control functions (SCF)

The SCF accommodates service user profiles. The SCF interacts with the ILCF to obtain the node ID of the UE.

The procedure is as follows:

- the SCF retrieves node locators and relevant session information from the ILCF;
- the SCF sends a LOC query request to the ILCF, which responds with the LOC query response information containing the LOC and additional information relevant to the format of location information provided by the ILCF.

NOTE – In an IMS-based architecture, the SCF interacts with the ILCF through P-CSC-FE, but in a non-IMS-based architecture, the SCF interacts with the ILCF through GSC-FE [ITU-T Y.2012].

7.1.2 Network attachment control functions (NACF)

When a UE attaches to the access network in NGN, the user authentication and authorization procedure is performed. When NGN supports host-based ID/LOC separation, the NACF allocates LOC to the UE and interacts with the ILCF to exchange ID/LOC mapping information.

NOTE – The support of ID/LOC by NACF [ITU-T Y.2014] is for further study.

7.1.3 ID/LOC mapping control functions (ILCF)

ILCF stores, distributes and updates ID/LOC mapping information. The ILCF has direct interactions with the TLM-FE within NACF to exchange ID/LOC mapping information of the UE. The ILCF has the following responsibilities:

- storing the authentication credentials [ITU-T Y.2720] of the UE, such as encryption keys [ITU-T X.509] and node IDs. The public cryptographic key, of a public/private key pair, is used to authenticate that the UE possesses the node ID, which in turn can be used to securely associate different locators with the same UE;
- processing the registration information sent from the UE;
- maintaining the binding of the node ID and LOC assigned to the UE;
- updating the ID/LOC mapping dynamically.

7.1.4 ID/LOC mapping functions (ILMF)

The ILMF is located in the end-user functions. The ILMF performs ID/LOC mapping functions using ID/LOC mapping information obtained from the ILCF.

7.2 Functional entities

The functional entities required for the support of ID/LOC separation in NGN are as follows:

- ID/LOC mapping functional entity (ILM-FE);
- ID/LOC mapping storage functional entity (ILMS-FE).

7.2.1 ID/LOC mapping functional entity (ILM-FE)

The ILM-FE is located in the ILMF and performs the ID/LOC mapping function in the UE. It obtains the ID/LOC mapping record from an ID/LOC mapping storage functional entity (ILMS-FE). The ILM-FE uses node IDs in the service stratum and applications and locators in layer 3 within the transport stratum. Using the node ID as a reference value, the ILM-FE can dynamically change, while continuously using the same node ID.

7.2.2 ID/LOC mapping storage functional entity (ILMS-FE)

ILMS-FE stores ID/LOC mapping records. It handles requests for ID/LOC mapping received from the ILM-FE, searches for the corresponding mapping in its record, and forwards the mapping information to the ILM-FE. It also handles update requests for ID/LOC mapping from authorized functional entities such as the NACF and UE, and carries out corresponding updates.

7.3 Reference points

Figures 7-2.a and 7-2.b show the functions, the functional entities and the related reference points defined in this Recommendation.

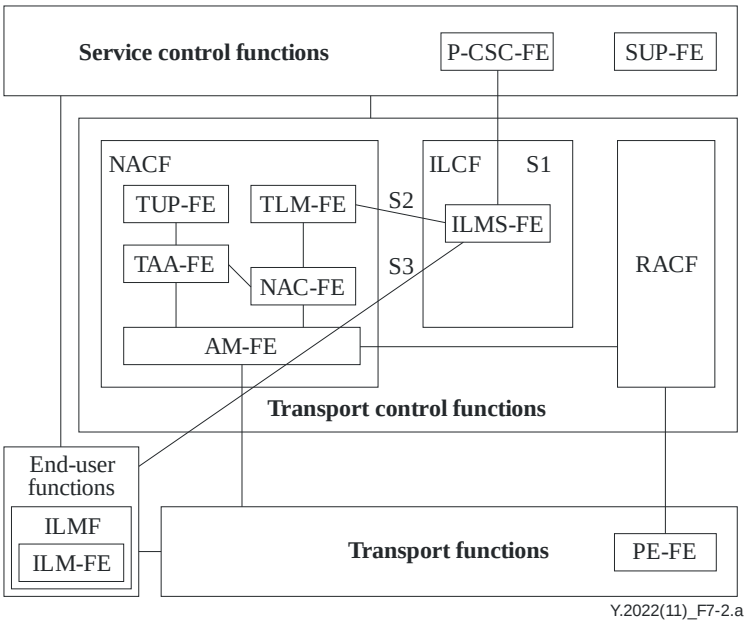

Figure 7-2.a – Reference points involved in ID/LOC mapping control functions in the IMS-based architecture

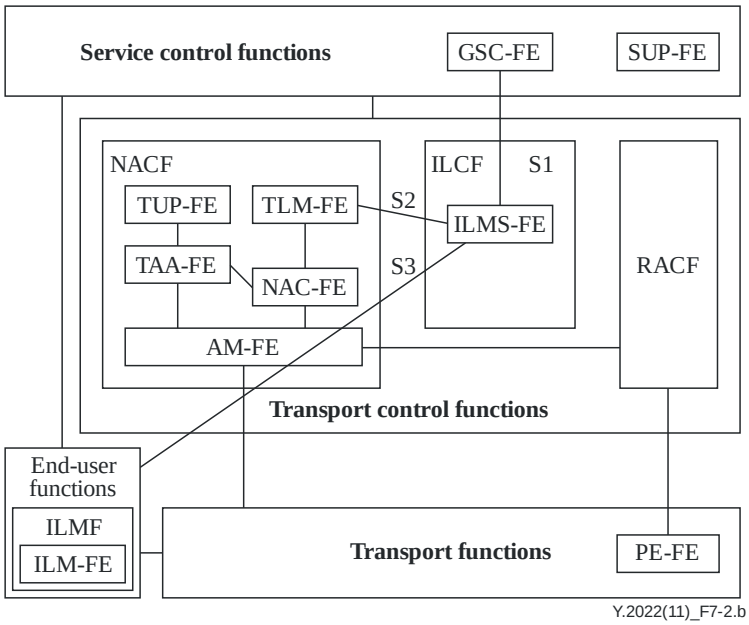

Figure 7-2.b – Reference points involved in ID/LOC mapping control functions in the non-IMS-based architecture

In an IMS-based architecture the SCF interacts with the ILCF through P-CSC-FE, but in a non-IMS-based architecture the SCF interacts with the ILCF through GSC-FE [ITU-T Y.2012].

7.3.1 Reference point S1 between SCF and ILMS-FE

S1 reference point enables SCF to retrieve information about the characteristics of the IP connectivity session from the ILCF. In an IMS-based architecture the S1 reference point is between the P-CSC-FE and ILMS-FE, but in a non-IMS-based architecture the S1 reference point is between the GSC-FE and ILMS-FE. The node ID of the UE is provided by the ILMS-FE. The following information flows are used on the S1 reference point:

– Information query request: This information flow contains the node ID and locator of the UE and flows from the SCF to the ILMS-FE.

– Information query response: This information flow contains the node ID and locator of the UE and flows from the ILMS-FE to the SCF.
– Event registration request: This information flow also contains the node ID and locator of the UE and flows from the SCF to the ILMS-FE.
– Event registration response: This information flow contains the node ID and locator of the UE and flows from the ILMS-FE to the SCF.
– Notification event request: This information flow also contains the node ID and locator of the UE and flows from the SCF to the ILMS-FE.
– Notification event response: This information flow contains the node ID and locator of the UE and flows from the ILMS-FE to the SCF.

7.3.2 Reference point S2 between TLM-FE and ILMS-FE

The S2 reference point allows the TLM-FE to register in the ILMS-FE the mapping between the LOC allocated to the UE and the node ID.

The following information flows are used on the S2 reference point:

– Mapping indication: This information flow contains the ID/LOC mapping of the UE and flows from the TLM-FE to the ILMS-FE to register the ID/LOC mapping in the ILMS-FE's record.
– Mapping acknowledgment: This information flow contains the result of the operation of the mapping indication and flows from the ILMS-FE to the TLM-FE.
– Mapping delete indication: This information flow contains the node ID and locator of the UE and flows from the TLM-FE to the ILMS-FE to delete the ID/LOC mapping in the latter's record.
– Mapping delete acknowledgment: This information flow contains the result of the operation of the mapping delete indication and flows from the ILMS-FE to the TLM-FE.

7.3.3 Reference point S3 between UE and ILMS-FE

The S3 reference point between the UE and the ILMS-FE allows the UE to authenticate with the ILMS-FE, and to update the ID/LOC mapping in the ILMS-FE by exchanging the following information flows.

– UE authentication request: This information flow from the UE to the ILMS-FE contains the node ID and authentication parameter generated by encrypting the node ID by the UE's private key.
– UE authentication response: This information flow from the ILMS-FE to the UE contains the node ID and the result (success or failure) of the authentication request.
– ID/LOC mapping registration request: This information flow is sent from the UE to the ILMS-FE to register the ID/LOC mapping in the ILMS database.
– ID/LOC mapping registration response: This information flow contains the node ID and the result of the registration request is sent from the ILMS-FE to the UE.
– ID/LOC mapping update request: This information flow containing the updated ID/LOC mapping is sent from the UE to the ILMS-FE when the UE changes its locator (e.g., as a result of mobility).
– ID/LOC mapping update response: This information flow containing the node ID and the result of the update request is sent from the ILMS-FE to the UE.

8 Procedures of ID/LOC split in NGN

This clause describes the procedures related to host-based ID/LOC separation in NGN.

8.1 Attachment procedure

8.1.1 ID/LOC mapping update initiated by the UE

When a UE attaches to a network, the UE's node ID is used during authentication and authorization processes. The UE attaches to the network through the involvement of the ILMS-FE and the NACF.

Figure 8-1 describes the signalling flow sequence related to ID/LOC mapping initiated by the UE.

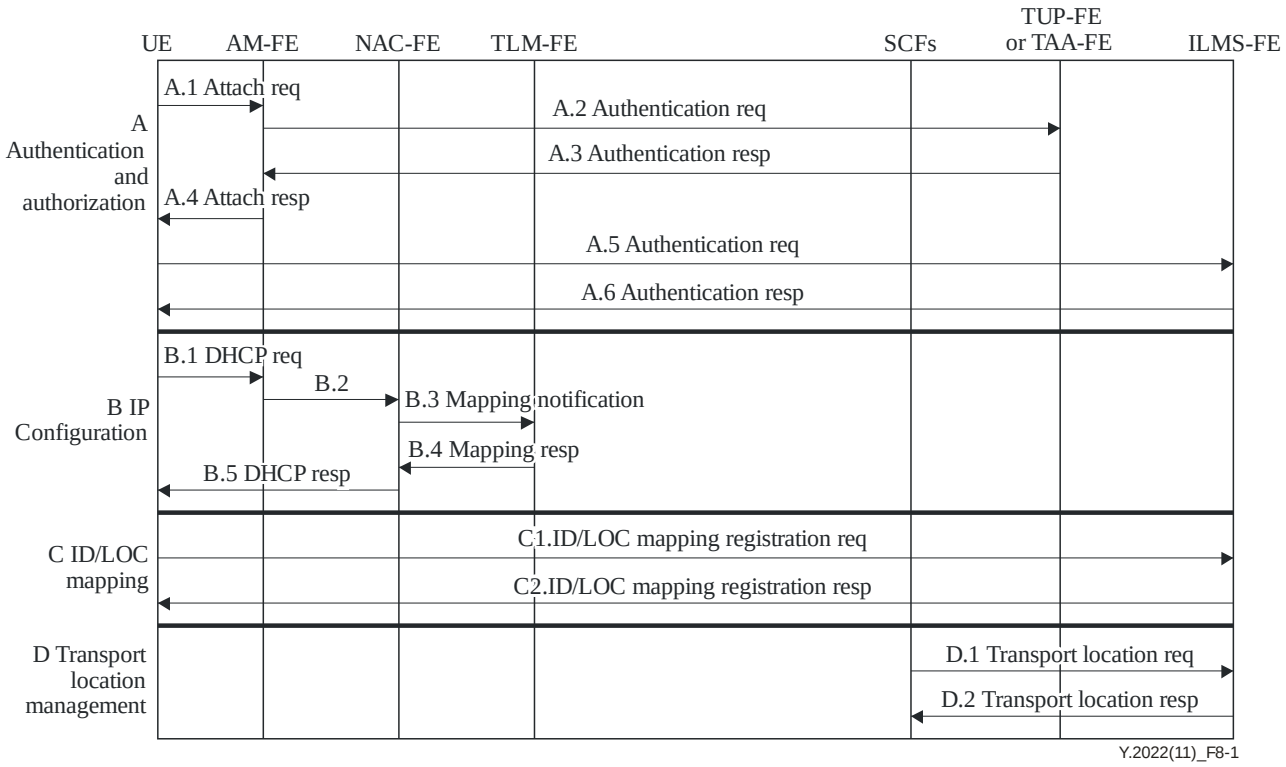

Figure 8-1 – Signalling flow sequence in the UE initiated ID/LOC mapping registration

Phase A: authentication and authorization

A.1) The UE sends an attachment request containing the node ID and user credential to the network with node ID.

A.2) The AM-FE forwards the user credential to the TAA-FE for authentication.

A.3, A.4) The TAA-FE responds to the AM-FE, which in turn responds to the UE with an attachment response.

A.5) The UE sends to the ILMS-FE an authentication request containing the encryption of the node ID by the UE's public key.

A.6) The ILMS-FE sends to the UE an authentication response containing the result of the authentication process.

Phase B: IP configuration

B.1) The UE issues a DHCP request containing its node ID to the AM-FE.

B.2) The AM-FE forwards the request to the NAC-FE, which allocates the LOC.

B.3) The NAC-FE pushes a mapping notification message to the TLM-FE, containing the allocated LOC and other transport related parameters such as logical/physical port addresses.

B.4) The TLM-FE replies to the NAC-FE with the mapping notification response message.

B.5) The NAC-FE configures a new LOC and assigns it to the UE. The UE is now aware of the mapping between the node Id and the LOC.

Phase C: ID/LOC mapping

C.1) The UE sends an ID/LOC mapping registration request to the ILMS-FE to register the ID/LOC mapping storage record.

C.2) The ILMS-FE replies to the UE with the ID/LOC mapping registration response.

Phase D: Transport location management

D.1) The SCF queries the ILMS-FE for location information.

D.2) The ILMS-FE sends the location information to the SCF.

8.1.2 ID/LOC mapping initiated by the network

This procedure enables the NACF to send the ID/LOC mapping registration request to the ILMS-FE after a new LOC has been allocated by the NACF.

Figure 8-2 describes the signalling flow sequence where the network initiates the ID/LOC mapping signalling flow sequence.

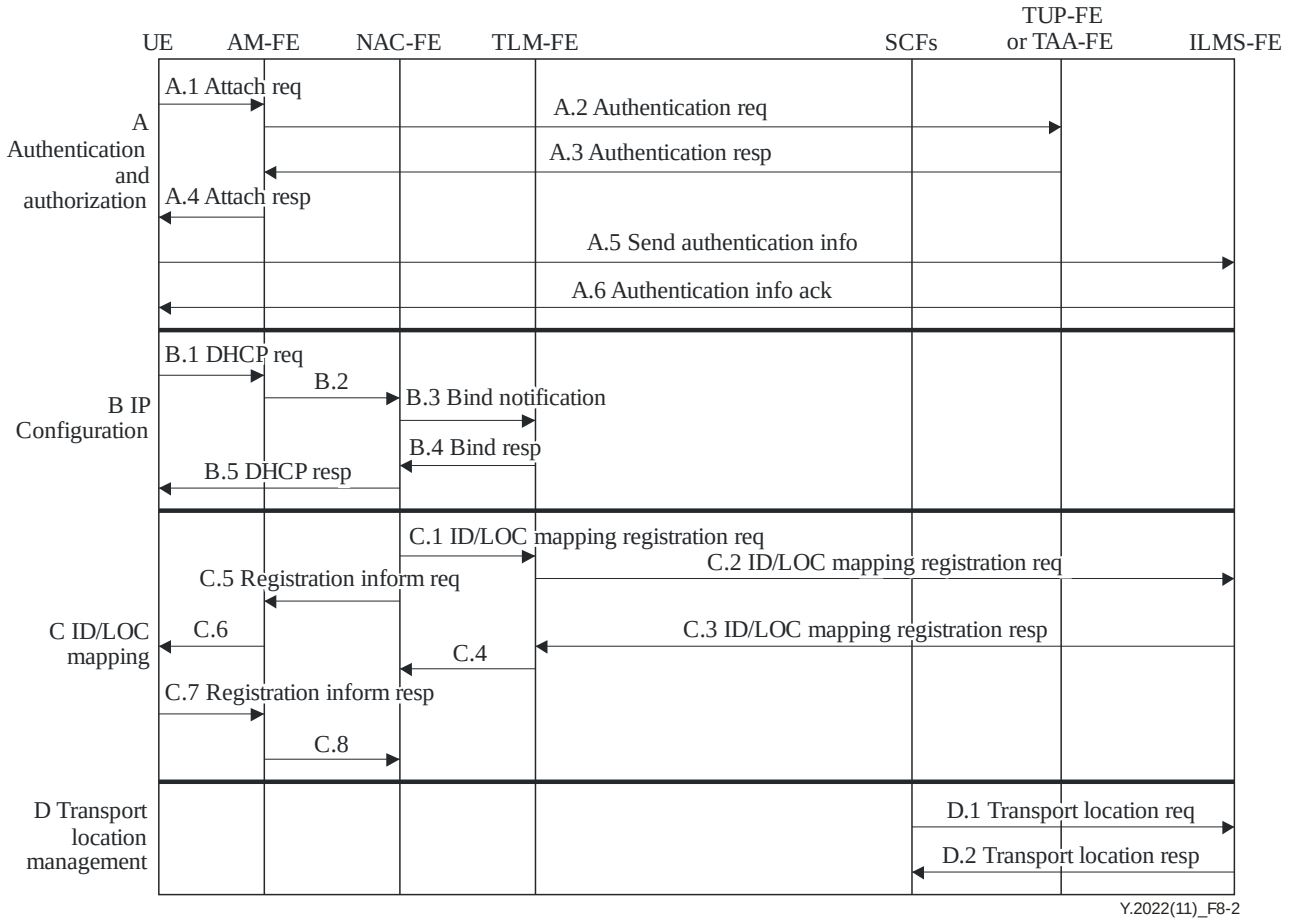

Figure 8-2 – ID/LOC mapping initiated by the network

As in Figure 8-1, Figure 8-2 also includes four phases. All the phases, except phase C, are similar in both figures.

In phase C, ID/LOC mapping registration takes place. In Figure 8-1 the registration was initiated by the UE whereas in Figure 8-2, it is initiated on the network side by the TLM-FE.

NOTE – Phases A, B and D are the same as the ones described in clause 8.1.1.

Phase C: ID/LOC mapping

C.1) The NAC-FE sends an ID/LOC mapping registration request to the TLM-FE.

C.2) The TLM-FE sends an ID/LOC mapping registration request to the ILMS-FE to register the ID/LOC mapping storage record.

C.3) The ILMS-FE replies to the TLM-FE with the ID/LOC mapping registration response.

C.4) The TLM-FE replies to the NAC-FE with the ID/LOC mapping registration response.

C.5, C.6) After step C.1 the NAC-FE sends an ID/LOC mapping registration inform request to the AM-FE, which then sends an ID/LOC mapping registration inform request to the UE to inform it that the registration has been initiated by the network.

C.7, C.8) The UE replies to the AM-FE with the ID/LOC mapping registration inform response, then the AM-FE sends an ID/LOC mapping registration inform response to the NAC-FE.

8.2 Communication establishment using node ID

Figure 8-3 describes the communication establishment procedure using the node ID.

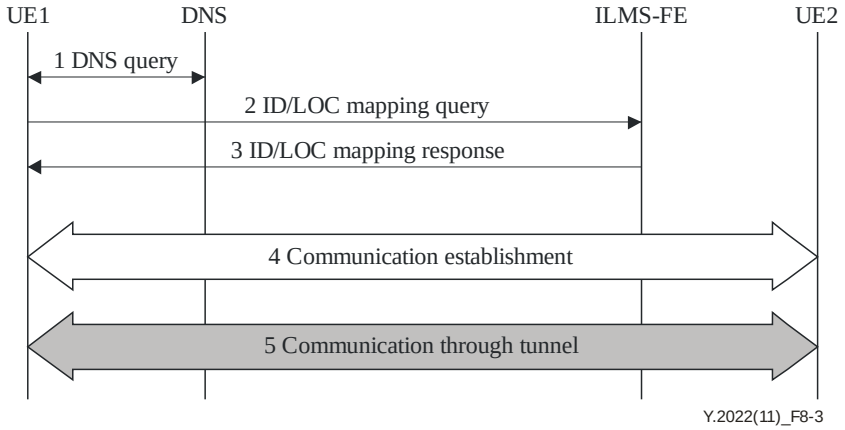

Figure 8-3 – Communication establishment procedures using node ID

The procedure described in Figure 8-3 includes the following:

1) UE1 sends a DNS query towards the DNS server [b-IETF RFC 5205] to find the ILMS-FE of UE2.

2) UE1 then issues an ID/LOC mapping query to the ILMS-FE including the Node ID of UE2 in order to obtain the LOC of UE2.

3) The ILMS-FE sends a response to UE1 which includes the LOC of UE2.

4) UE1 establishes communication with UE2 using the LOC of UE2.

5) UE1 is able to communicate with UE2.

8.3 Communication establishment for multihoming

In the case of multihoming, the UE may have multiple valid LOCs. However, the UE still uses the same node ID to communicate with other UEs. The corresponding procedure for communication establishment is described in Figure 8-4.

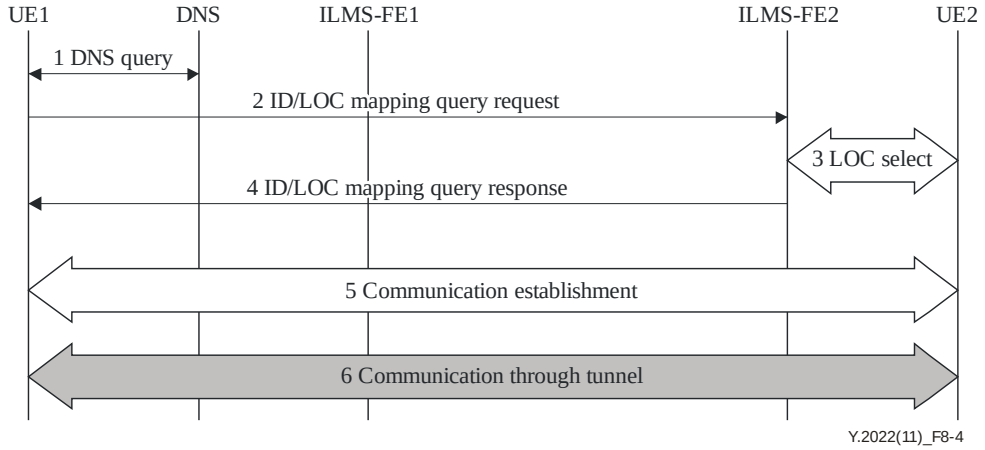

Figure 8-4 – Communication establishment procedures using node ID when multihoming

In Figure 8-4, UE2 is multihomed. The procedure for communication establishment from UE1 to UE2 includes the following steps:

1) UE1 sends a DNS query towards the DNS server in order to obtain the LOC of ILMS-FE associated with UE2.
2) UE1 then issues an ID/LOC mapping query to ILMS-FE2 (i.e., the ILMS-FE associated with UE2).
3) As it is multihomed, UE2 selects the LOC to be used for the communication with UE1 and indicates the selected LOC to ILMS-FE2.
4) ILMS-FE2 sends a response to UE1 including the selected LOC of UE2.
5) UE1 establishes a connection with UE2 using the selected LOC of UE2.
6) Communication is established between UE1 and UE2.

8.4 Communication update when the LOC is changed

When the LOC of a UE changes (e.g., as a result of UE moving), the UE requests the ILCF to update its ID/LOC mapping. If the UE is communicating with another UE, it updates the communication with the new LOC.

The related procedure is described in Figure 8-5.

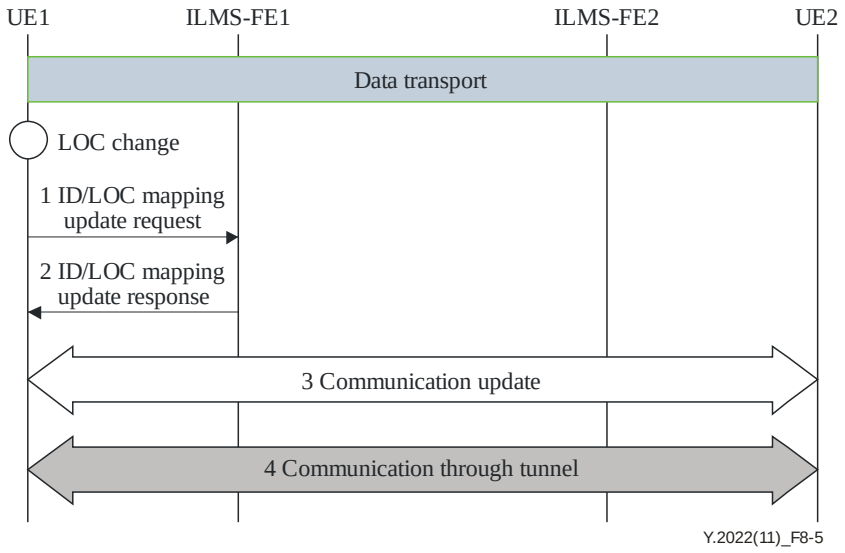

Figure 8-5 – Communication update when the LOC is changed

The procedure described in Figure 8-5 includes the following four steps:

1) After UE1 changes its LOC (e.g., as a result of mobility), UE1 sends an ID/LOC mapping update request to its ILMS-FE1, including its new LOC.

2) ILMS-FE1 sends a response to UE1 after having updated the ID/LOC mapping record.

3) UE1 updates its communication with UE2 in order to use the new LOC of UE1 and establishes a tunnel between them.

4) UE1 communicates with UE2.

8.5 Detachment procedures

The detachment procedures allow:

– a UE to inform the network that it does not want to access the network any longer; and

– the network to inform the UE that it does not have access to the network any longer.

8.5.1 Detachment procedure initiated by the UE

The UE initiated detachment procedure is described in Figure 8-6.

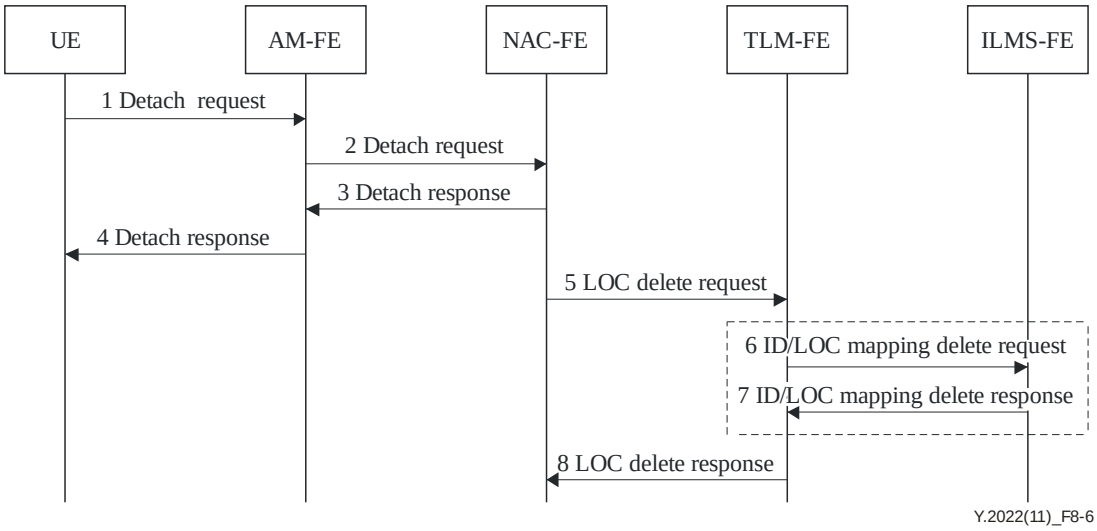

Figure 8-6 – Detachment procedure initiated by the UE

The procedure described in Figure 8-6 includes the following steps:

1, 2) UE sends a detach request to the AM-FE, and the AM-FE forwards the detach request to the NAC-FE.

3, 4) The NAC-FE releases the related attachment information and sends a detach response to the AM-FE, which in turn responds to the UE.

5) The NAC-FE sends a LOC delete request to the TLM-FE.

6, 7) The TLM-FE sends an ID/LOC mapping delete request to the ILMS-FE to delete the ID/LOC mapping stored in the ILMS-FE. After deleting the record, the ILMS-FE sends an ID/LOC mapping delete response to the TLM-FE.

8) The TLM-FE sends a LOC delete response to the NAC-FE.

8.5.2 Detachment procedure initiated by the network

The detachment procedure initiated by the network is described in Figure 8-7.

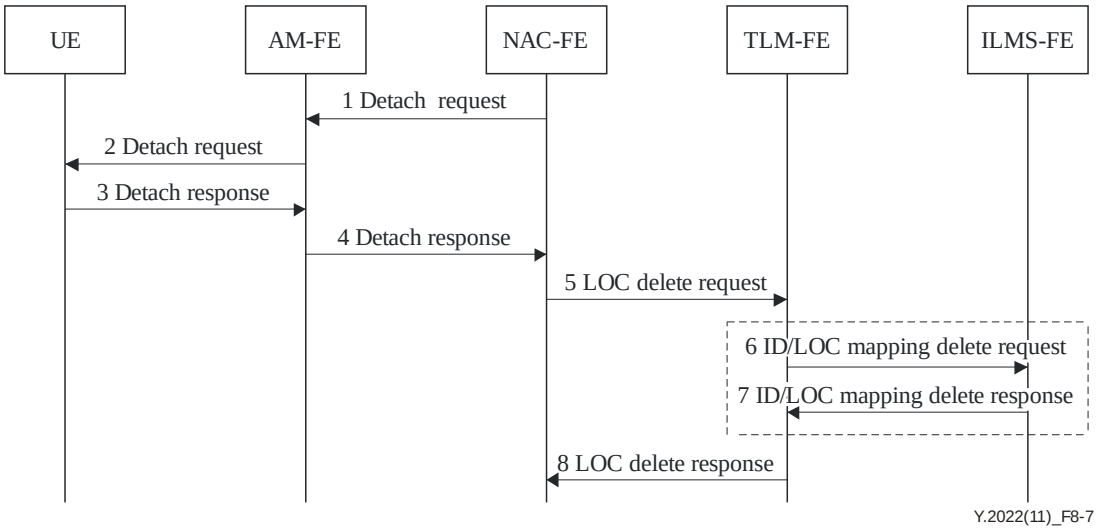

Figure 8-7 – Detachment procedure initiated by the network

The procedure described in Figure 8-7 includes the following steps:

1, 2) The NAC-FE sends a detach information request to the AM-FE. After receiving the request, the AM-FE sends the detach information request to the UE.

3, 4) After receiving the detach information request from the AM-FE, the UE sends a detach response to the AM-FE, which in turn responds to the NAC-FE.

5) The NAC-FE sends a LOC delete request to the TLM-FE.

6, 7) The TLM-FE sends an ID/LOC mapping delete request to the ILMS-FE. After deleting the record, the ILMS-FE sends an ID/LOC mapping delete response to the TLM-FE.

8) The TLM-FE sends a LOC delete response to the NAC-FE.

9 Security considerations

The UE and the communication path between the UE and the ILCF may not be secured. So this communication could be subjected to attacks. The UE is required to use secured mechanisms when retrieving ID/LOC mapping records from the authenticated ID/LOC mapping storage functions.

Security requirements are as follows:

R1 The ILMS-FE is required to be secured as per [ITU-T Y.2701].

R2 The ILM-FE is required to be secured as per [ITU-T Y.2701].

R3 The communication path between the ILM-FE and ILMS-FE is required to be secured as per [ITU-T Y.2701].

Bibliography

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks.*

[b-IETF RFC 5201] IETF RFC 5201 (2008), *Host Identity Protocol (HIP).*

[b-IETF RFC 5205] IETF RFC 5205 (2008), *Host Identity Protocol (HIP) Domain Name System (DNS) Extensions*.

[b-IETF RFC 5206] IETF RFC 5206 (2008), *End-Host Mobility and Multihoming with the Host Identity Protocol.*

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, 2012