Draft Recommendation ITU-T Y.FAid-loc-split

Functional architecture for the support of ID/locator separation in NGN

Summary

This Recommendation describes the functional architecture for the support of ID/locator separation in NGN. It covers only the host-based case of ID/locator separation. ID/LOC separation in NGN is decoupling the semantic of IP addresses into the semantics of identifiers (node IDs) and locators (LOCs) as described in [ITU-T Y.2015]. This recommendation defines the functional entities and reference points. It uses the node ID and locator as defined in [ITU-T Y.2015]. It draws heavily from [ITU-T Y.2015], but maps their content into the framework provided by [ITU-T Y.FRAr2].

CONTENTS

Page

Draft Recommendation ITU-T Y.FAid-loc-split

Functional architecture for the support of ID/locator separation in NGN

1 Scope

Based on requirements provided in [ITU-T Y.2015], this Recommendation describes the functional architecture for the support of ID/locator separation in NGN.

More specifically, this Recommendation addresses the following aspects:

- Functional architecture model for ID/locator separation in NGN;
- Identification of functions including the definition of functional entities and reference points;
- 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 and it focuses exclusively on layer 3 approaches.

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 Y.2001] ITU-T Recommendation Y.2001 (2004), *Next Generation Networks – Frameworks and functional architecture models*.

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2010), *Functional requirements and architecture for the NGN.*

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

[ITU-T Y.2091] ITU-T Recommendation Y.2091 (2006), *Terms and definitions for Next Generation Networks.*

[ITU-T Y.1241] ITU-T Recommendation Y.1241 (2001), *Support of IP-based services using IP transfer capabilities.*

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

[IETF RFC 5205] IETF RFC 5205 (2008), *HIP Domain Name System (DNS) Extensions.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 identifier [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).

3.1.2 address [ITU-T Y.2015]: An address is the identifier for a specific termination point and is used for routing to this termination point.

NOTE - This Recommendation only uses the term "address" in the case where it does not specifically refer to a locator or an identifier.

3.1.3 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 multi-homing.

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 multi-homing implications.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABG-FE Access Border Gateway Functional Entity

AM-FE Access Management Functional Entity

ID Identifier

ILCF ID/LOC Control Functions

ILC-FE ID/LOC Control Functional Entity

ILMF ID/LOC Mapping Functions

ILM-FE ID/LOC Mapping Functional Entity

ILMS-FE ID/LOC Mapping Storage Functional Entity

ILMU-FE ID/LOC Mapping Update Functional Entity

ILTF ID/LOC Transport Functions

IP Internet Protocol

LOC Locator

NACF Network Attachment Control Functions

NAC-FE Network Access Configuration Functional Entity

NGN Next Generation Networks

RACF Resource and Admission Control Functions

SAA-FE Service Authentication and Authorization Functional Entity

SCF Service Control Functions

SUP-FE Service User Profile Functional Entity

TAA-FE Transport Authentication and Authorization Functional Entity

TIL-FE Transport ID/LOC 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

UE User Equipment

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

5.1 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 is decoupling the semantic of IP addresses into the semantics of identifiers (node IDs) and locators (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 as well as applications.

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

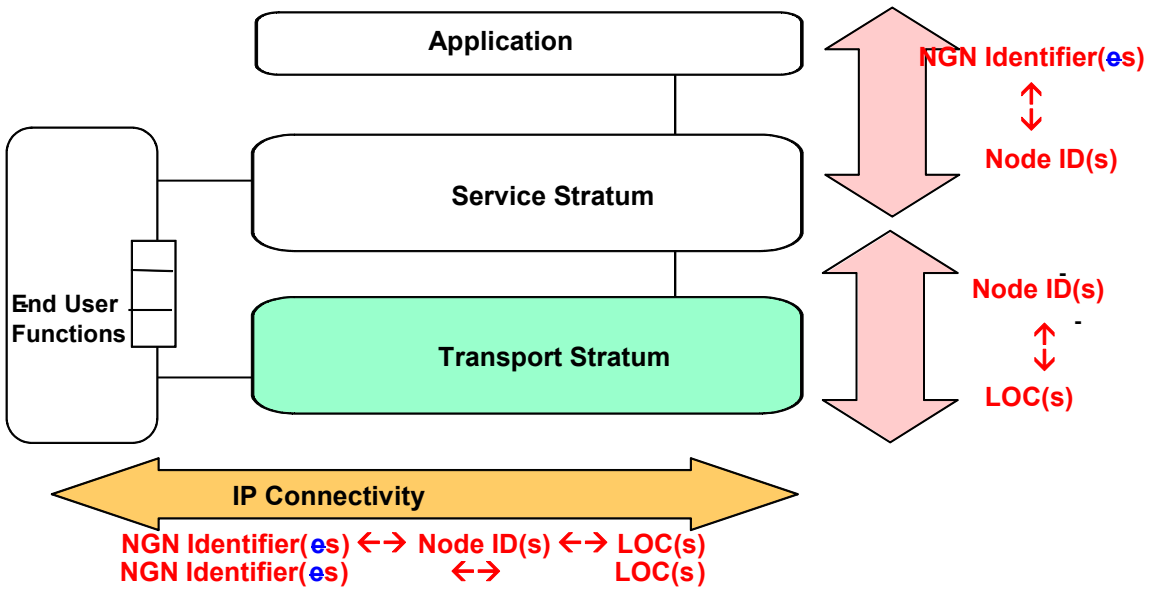

Figure 1- ID/LOCs separation in NGN

As shown in Figure 1, relationships between NGN identifier, Node IDs, and LOC(s) need to be considered in order to provide ID/LOC separation in the NGN architecture.

According to [ITU-T Y.2015], the two-stage mapping consists of a first stage mapping between the NGN identifier and a node ID and a second stage mapping between the node ID and the LOC. The two-stage mapping is the general functional case from which "any number of stages" or even the "no-stage" mapping can be seen as particular cases from an implementation view point. Therefore this Recommendation assumes that the two-stage mapping is used to support the ID/LOC separation in NGN.

5.2 Architecture overview

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

The NGN functional architecture supporting ID/locator split functions is shown in Figure 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 UE, respectively.

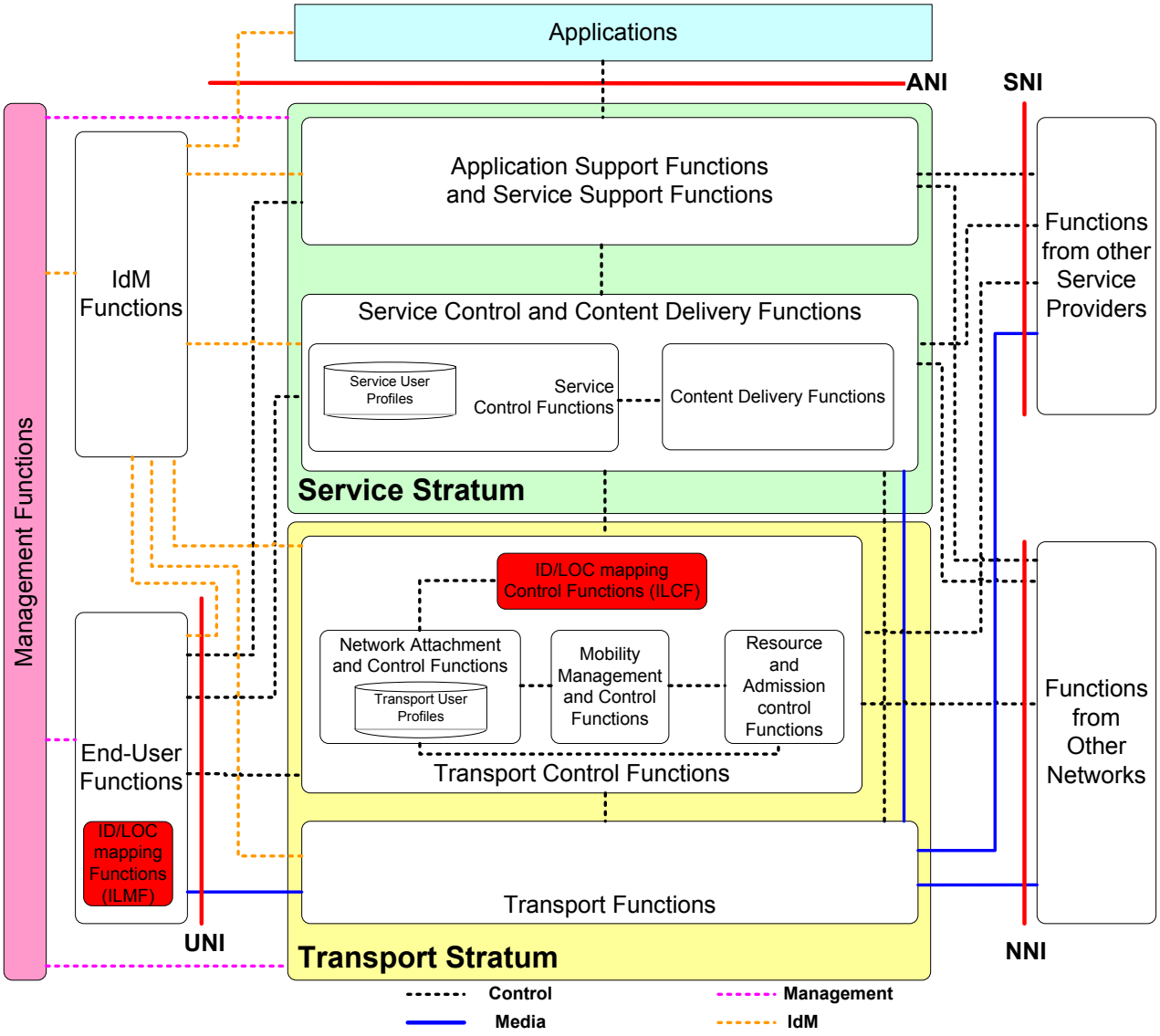

Figure 2 – Architecture overview for ID/LOC separation in NGN

The ILCF provides the control information and signaling required to implement IDLOC mapping functions in NGN. It collects, stores, updates, and distributes ID/LOC mapping information.

6 Functional architecture

Figure 3 shows the functional architecture for the support of ID/LOC separation in the NGN. Details of the general NGN architecture [ITU-T Y.2012] have been omitted to bring out the relevant points.

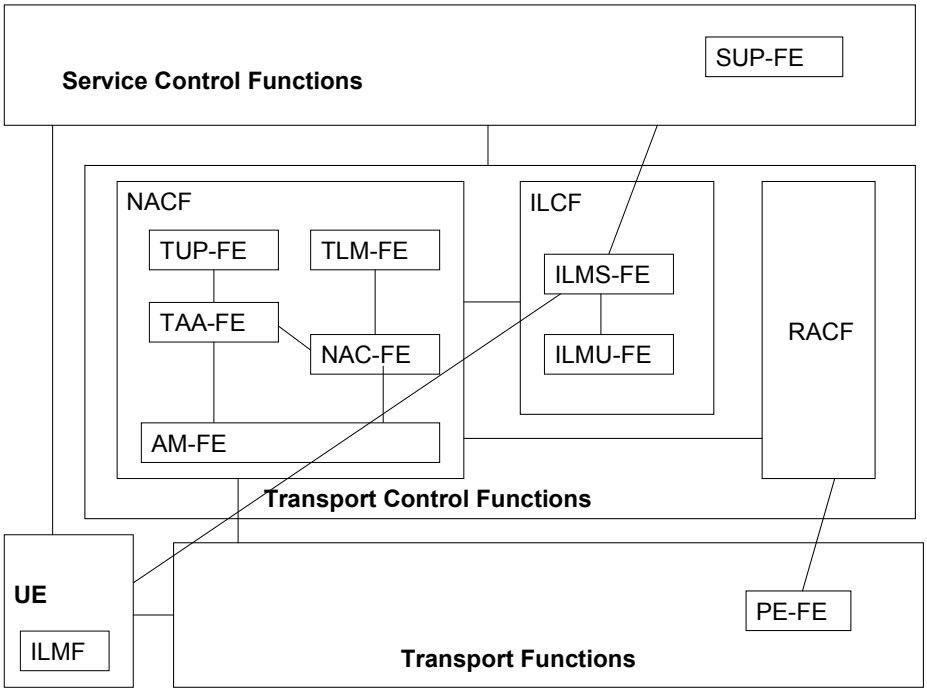

Figure 3–Functional architecture for ID/LOC separation in NGN

The ILCF includes two functional entities: ID/LOC Mapping Storage Functional Entity (ILMS-FE) and ID/LOC Mapping Update Functional Entity (ILMU-FE).

6.1 High level functions

At the highest level, this Recommendation involves the following functions:

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

6.1.1 Service control functions

The service control functions (SCF) accommodates service user profiles which represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of functional databases. In the NGN, the SCF interacts with ILCF to query the required node ID of UE.

6.1.2 Network Attachment Control functions

When a UE attaches to an NGN access network, the user authentication and authorization procedure will be performed for the network access. In the id-loc-split-based NGN, the Network Attachment Control Functions (NACF) interacts with the ILCF to exchange ID/LOC mapping information which is used for maintaining the transport user profile and for the transport stratum level identification/authentication.

- storing the credentials of the UE and the key of the Node ID;
- processing the registration messages sent from UE;
- maintaining the binding of the ID and the LOC assigned to the UE;
- updating the ID/LOC mapping dynamically.

6.1.3 Id-loc-split mapping control functions (ILCF)

The ID/LOC mapping control functions (ILCF) store, distribute and update ID/LOC mapping information. The ILCF has direct interactions with the TLM-FE within NACF to exchange ID/LOC mapping information of UE. The Id-loc-split control function (ILCF) has the following responsibilities:

- storing the credentials of the UE and the key of the Node ID;
- processing the attachment of the UE;
- processing the registration messages sent from UE;
- maintaining the binding of the ID and the LOC assigned to the UE;
- updating the ID/LOC mapping dynamically.

6.1.4 Id-loc-split mapping functions (ILMF)

The ILMF resides either in a UE or in a border access gateway, or in both. The ILMF performs ID/locator mapping functions using ID/locator mapping information obtained from the ILCF. The ILMF performs ID/LOC mapping function. The ILMF resides in UE performs ID/LOC mapping function using ID/LOC mapping information obtained from the ILMS-FE. After received the request to change the LOC, ILMS-FE/ILMU-FE sends response to ILM-FE carrying UE's LOC and its node ID. According to the mapping response the ILM-FE updates the ID/LOC mapping. The ILMS-FE/ ILMU-FE select the LOC of the UE from the updated ID/LOC mapping.

6.2 Functional entities

The functional entities required for support of id-loc-split in NGN are:

- ID/locator mapping functional entity (ILM-FE);
- ID/Locator Mapping Storage functional entity (ILMS-FE);
- ID/Locator Mapping Update functional entity (ILMU-FE);

6.2.1 ID/Locator Mapping – Functional Entity (ILM-FE)

An ID/LOC mapping functional entity (ILM-FE) is the major component of the ID/LOC separation architecture in NGN. It performs ID/LOC mapping function. It obtains ID/LOC mapping record from an ID/LOC mapping storage entity and uses the node ID and locator in communication protocols. The ILM-FE uses node ID in the transport and upper layer protocols and locators in the network layer protocol and packet header. Using the node ID as a reference value, the ILM-FE can dynamically change locators in the network layer protocol and packet header, while continuously using the same node ID in the transport and upper layers. The ILM-FE thus hides the effect of locator changes from the transport and upper layer services.

The ILM-FE resides in UE performs ID/LOC mapping function using ID/LOC mapping information obtained from the ILMS-FE.

6.2.2 ID/Locator Mapping Storage – Functional Entity (ILMS-FE)

An ID/LOC mapping storage functional entity (ILMS-FE) stores ID/LOC mapping record. It accepts an ID/LOC mapping record lookup request from the ILM-FE, searches the corresponding mapping record in its record, and forwards the mapping record to the ILM-FE. It also accepts an ID/LOC mapping record update request from authorized functional entities such as NACF, UE, and carries out corresponding updates.

6.2.3 ID/Locator Mapping Update functional entity (ILMU-FE)

A The ILMU-FE collects and updates ID/LOC mapping information. It interacts with the NACF, UEs or access border gateways. It distributes the updated mapping information to the ILMS-EF and the ILMF of UEs or access border gateways. That is, whenever UEs or access border gateways detect changes in their ID/locator mapping, they inform the ILMU-FE to update the mapping information in concerned entities such as the ILMS-EF and ILM-FE of UE.

6.3 Reference points

Figure 4 shows the functions and functional entities defined in the Y.FAid-loc-split. The links between the functions indicate required information flows, identified by reference points S1 through S4 are between ILCF entities and other entities. S5 is flow between entities of the ILCF.

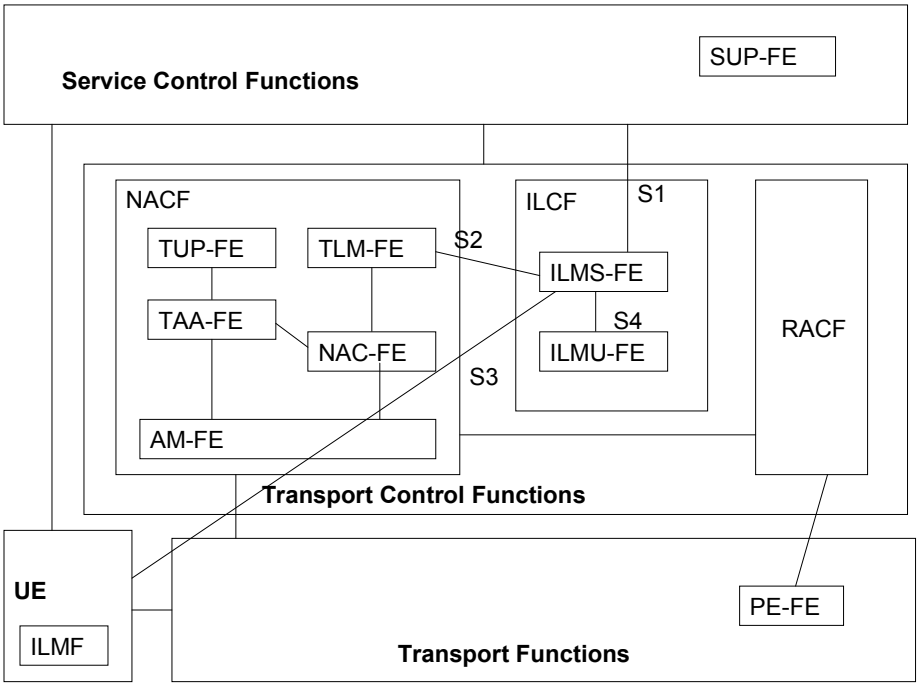

Figure 4 – Reference points and information flows involved in ID/locator mapping control functions

6.3.1 Reference point S1: between SCF and ILMS-FE

The S1 reference point enables Service Control Functions (SCF) to retrieve information about the characteristics of the IP-connectivity session used to access such Service Control Functions from the ILCF. The Node ID of UE is provided by the ILMS-FE. The following information flows are used on the S1 reference point:

- Information Query Request
- Information Query Response
- Event Registration Request
- Event Registration Response
- Notification Event Request
- Notification Event Response

6.3.1.1 Information Query request

Table 1 describes the information contained in the Information Query Request information flow.

Table 1 - Information Query Request (SCF -> ILMS-FE)

Information element	Explanation
Unique IP Address	The IP address allocated to the attached UE.
Node ID	The identifier of the UE

6.3.1.2 Information Query Response

Table 2 describes the information contained in the Information Query Response information flow.

Table 2 - Information Query Response (ILMS-FE -> SCF)

Information element	Explanation
Node ID	The identifier of the UE
Unique IP Address	The IP address allocated to the attached UE.

6.3.1.3 Event Registration Request

Table 3 describes the information contained in the Event Registration Request information flow.

Table 3: Event Registration Request (SCF -> ILMS-FE)

Information element	Explanation
Node ID	The identifier of the UE
Unique IP Address	The IP address allocated to the attached UE.

6.3.1.4 Event Registration Response

Table 4 describes the information contained in the Event Registration Response information flow.

Table 4: Event Registration Response (ILMS-FE -> SCF)

Information element	Explanation
Node ID	The identifier of the UE
Unique IP Address	The IP address allocated to the attached UE.

6.3.1.5 Notification Event Request

Table 5 describes the information contained in the Notification Event Request information flow.

Table 5: Notification Event Request (ILMS-FE -> SCF)

Information element	Explanation
Node ID	The identifier of the UE
Unique IP Address	The IP address allocated to the attached UE.

6.3.1.6 Notification Event Response

Table 6 describes the information contained in the Notification Event Response information flow.

Table 6: Notification Event Response (SCF -> ILMS-FE)

Information element	Explanation
Node ID	The identifier of the UE
Unique IP Address	The IP address allocated to the attached UE.

6.3.2 Reference point S2: between TLM-FE and ILMS-FE

The S3 reference point allows the TLM-FE to register in the ILMS-FE the binding between the LOC allocated to UE and the Node ID.

The following information flows are used on the ILMS-FE to TLM-FE reference point:

- Bind Indication
- Bind Acknowledgment
- Unbind Indication
- Bind Information Query
- Bind Information Query Acknowledgement

6.3.2.1 Bind Indication

Table 8 describes the elements contained in the Bind Indication information flow.

Table 8 – Bind Indication (TLM-FE → ILMS-FE)

Information element	Explanation
Node ID	The identifier of the UE.
LOC	The IP address allocated to the attached UE.

6.3.2.2 Bind Acknowledgement

The Bind Acknowledgment information flow conveys information that may be sent back to the UE. The information returned by the TLM-FE in response to a bind indication is received from the ILM-FE. Table 9 describes the elements contained in the Bind Acknowledgment information flow.

Table 9 - Bind Acknowledgment (ILMS-FE -> TLM-FE)

Information element	Explanation
Node ID	The identifier of the UE
Binding Request Result	Indication of the success or failure of the binding.

6.3.3 Reference point S3: between UE and ILMS-FE

The S4 reference point allows the UE to authentication, monitoring, receive notifications and allots the node ID to the traditional UE when the traditional UE communicates with the id-loc-split-based UE. The S4 reference point is used during initialization and updating the ID/LOC binding in the ILM-FE in order to allow the UE to access to the NGN Service Control Functions.
The S4 reference point supports the following procedures:

- UE identification/authentication;

- Provide configuration and upgrade for the ILMS-FE;

-The address of the ILMS-FE instance which sends the location registration.

- allots the node ID to the traditional UE when the traditional UE communicates with the id-loc-split-based UE.

6.3.5 Reference point S4: between ILMS-FE and ILMU-FE

The information flow through reference point S5 allows the ILMU-FE to retrieve the ID/LOC mapping information that it then provides to the UE. Reference point S5 supports two primitives for this operation:

- ID/LOC binding registration/update request;
- ID/LOC binding registration/update response.

Table 10 –ID/LOC binding registration/update request (ILMU-FE -> ILMS-FE)

Information element	Explanation
Node ID	The identifier of the UE
LOC	The persistent IP address allocated to the attached mobile UE.

Table 11 –ID/LOC binding registration/update response (ILMS-FE -> ILMU-FE)

Information element	Explanation
Node ID	The identifier of the UE
LOC	The persistent IP address allocated to the attached mobile UE.
Binding request result	Indication of the success or failure of the Binding Request.

7 Procedures

This clause describes the information flows required to the id-loc-split network.

7.1 Attach procedure

7.1.1 UE initiates the ID/LOC mapping

In the id-loc-split-based NGN, when UE attaches a network, User identity node ID is used in the processing of authentication and authorization, UE attaches the network through the ILMU-FE/ILMS-FE.

The steps included as following:

- In the processing of the authentication and authorization, node ID is authenticated and authorized through ILMU-FE/ILMS-FE;
- Through the processing of configuration, UE allocated the IP address;
- UE does the ID/LOC mapping through ILMU-FE/ILMS-FE

Figure 5 shows the message flow.

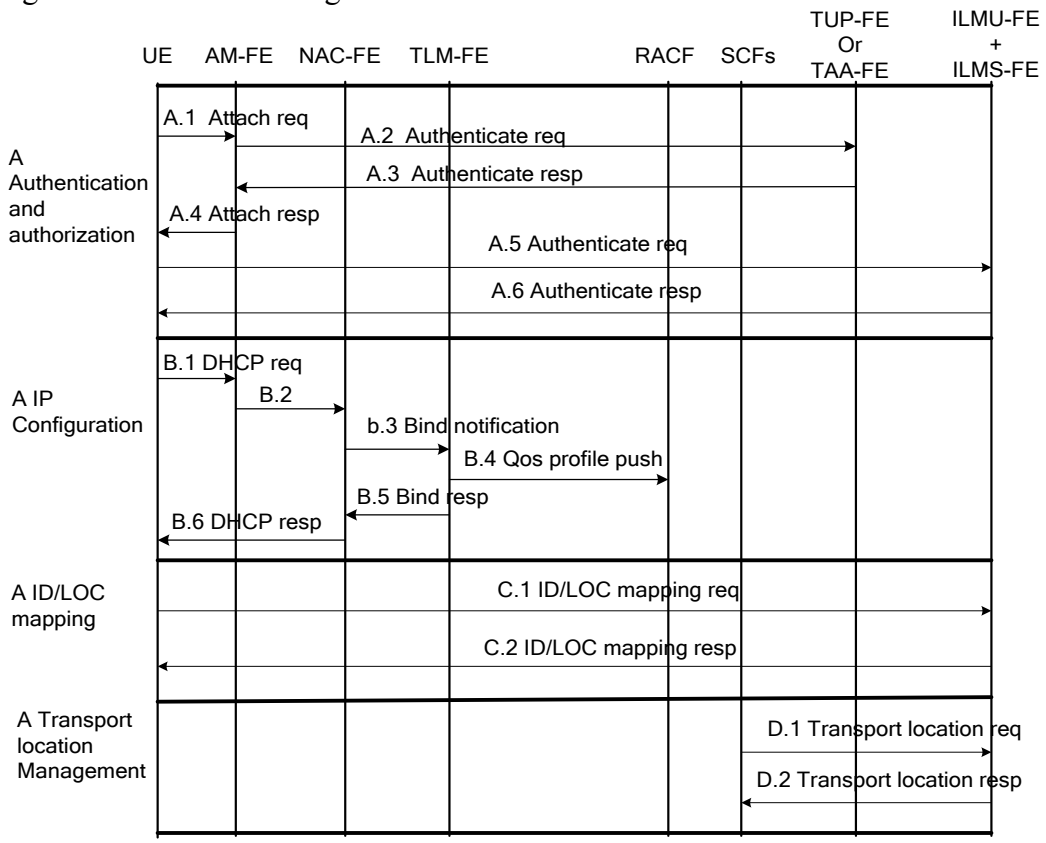

Figure 5- Information flows for Id-loc-split-based network attachment

Phase A: authentication and authorization

A.1 The UE requests attachment to the network.

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

A.3-A.4 The TAA-FE in the target network responds to the AM-FE, which in turn responds to the UE's attachment request and node ID is authenticated and authorized.

A.5 The UE sends authenticate request to ILMU-FE/ILMS-FE, ILMU-FE/ILMS-FE can generate authentication vector according to the UE identifier.

A.6 The ILMU-FE/ILMS-FE sends response to the UE carrying the authentication information.

Phase B: IP configuration

B.1 The UE issues a DHCP request to the AM-FE.

B.2 The AM-FE forwards the request to the NAC-FE.

B.3 The NAC-FE pushes a Bind Indication to the TLM-FE containing the temporary address it has allocated and other transport related information such as logical/physical port addresses.

B.4 The TLM-FE pushes the profile information to RACF.

B.5 The TLM-FE pushes the profile information to the NAC-FE.

B.6 The NAC-FE configures the UE with its new IP address.

Phase C3: ID/LOC mapping

C.1 The UE sends ID/LOC mapping request to ILMU-FE/ILMS-FE.

C.2 The ILMU-FE/ILMS-FE responses the ID/LOC mapping to the UE.

Phase D: Transport location management

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

D.2 The ILMU-FE/ILMS-FE responses the location information to SCF.

In the id-loc-split network, the NGN service control function retrieves location information from the ILM-FE. Service control functions (SCF) retrieves information about the characteristics of the IP-connectivity session used to access such service control functions (e.g. network location information) from the ILMU-FE/ILMS-FE. SCF sends location query request to ILMU-FE/ILMS-FE, which in return responses to SCF the location query request, the response message carries the location information and/or information about the characteristics of the IP-connectivity session used to access such service control functions. The form of location information is provided by the ILMU-FE/ILMS-FE depends on the requestor. The primary parameter to retrieve the location information is the Transport Subscriber Identifier, UE identifier, SCF Identity and the IP address allocated to the UE.

According to Figure 5, the AM-FE sends the configuration request to NAC-FE to obtain IP address. The UE sends the mapping of the allocated IP address and its identifier to ILMU-FE/ILMS-FE after the new IP address is configured. That is, the UE initiates the ID/LOC mapping. But there is another case which the network sends the ID/LOC mapping request to ILMU-FE/ILMS-FE after the new IP address is allocated by network. That is the TLM-FE initiates the ID/LOC mapping. The TLM-FE sends ID/LOC mapping request to ILMU-FE/ILMS-FE after the new IP address is allocated. After receiving the request to do the ID/LOC mapping, the ILMU-FE/ILMS-FE responses the ID/LOC mapping to the TLM-FE with the mapping information. Figure 6 is the network initiates the ID/LOC mapping message flow.

7.1.2 The network initiates the ID/LOC mapping

Figure 6 shows the message flow of the network initiates the ID/LOC mapping.

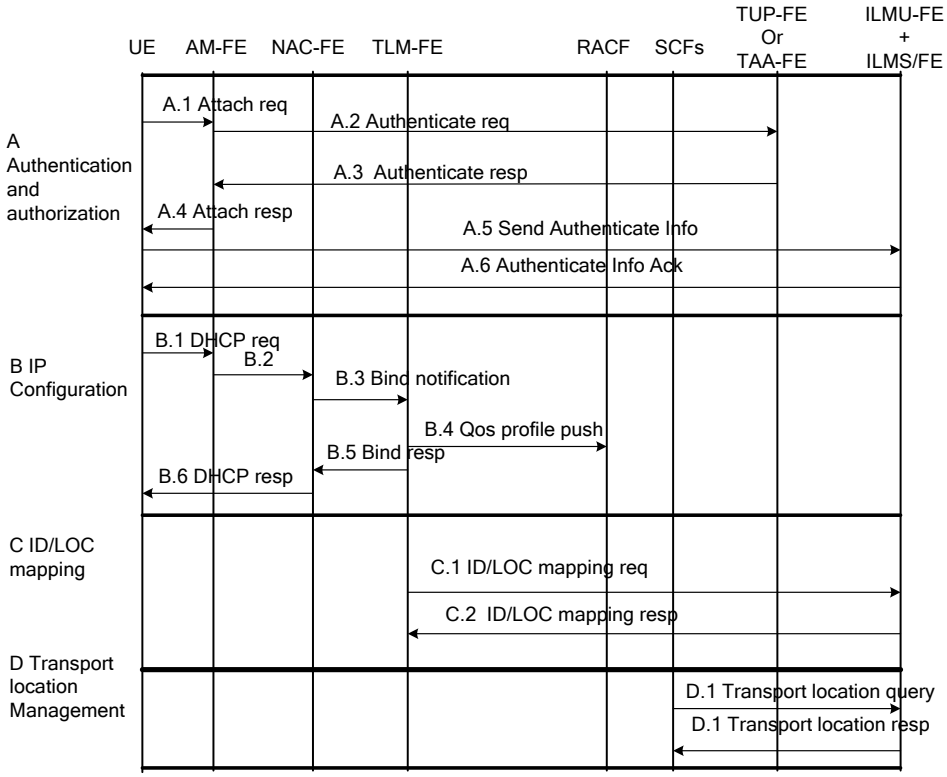

Figure 6- The network initiates the ID/LOC mapping

Phase A: authentication and authorization

A.1 The UE requests attachment to the network.

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

A.3-A.4 The TAA-FE in the target network responds to the AM-FE, which in turn responds to the UE's attachment request.

A.4 The UE sends authenticate information to ILM-FE, ILM-FE can generate authentication vector according to the UE identifier.

A.5 The ILM-FE sends response to the UE carrying the authentication vector.

Phase B: IP configuration

B.1 The UE issues a DHCP request to the AM-FE.

B.2 The AM-FE forwards the request to the NAC-FE.

B.3 The NAC-FE pushes a Bind Indication to the TLM-FE containing the temporary address it has allocated and other transport related information such as logical/physical port addresses.

B.4 The ILMU-FE/ILMS-FE pushes the profile information to RACF.

B.5 The ILMU-FE/ILMS-FE pushes the profile information to the NAC-FE.

B.6 The NAC-FE configures the UE with its new temporary IP address.

Phase C: ID/LOC mapping

C.1 The TLM-FE sends ID/LOC mapping request to ILMU-FE/ILMS-FE.

C.2 The ILMU-FE/ILMS-FE responses the ID/LOC mapping to the TLM-FE.

Phase D: Transport location management

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

D.2 The ILMU-FE/ILMS-FE responses the location information to SCF.

7.2 Connection procedures using node ID

In the id-loc-split network, the transport and higher layers are required to use the node ID for an application service or transport session. UE uses the node ID to associate with the peer after which has registered and been authenticated. When UE1 wants to initiate a communication with UE2, Initiator obtains IP of ILMS-FE/ILMU-FE through a DNS lookup, the ILMS-FE/ILMU-FE is the mapping server of the UE2. Initiator obtains the LOC of the responder's through the ID/LOC mapping lookup response via ILMS-FE/ILMU-FE .Then UE1 obtains the node ID of UE2 through the ID/LOC mapping query. Initiator creates connection with the responder. The connection procedures using node ID is illustrated in Figure 7.

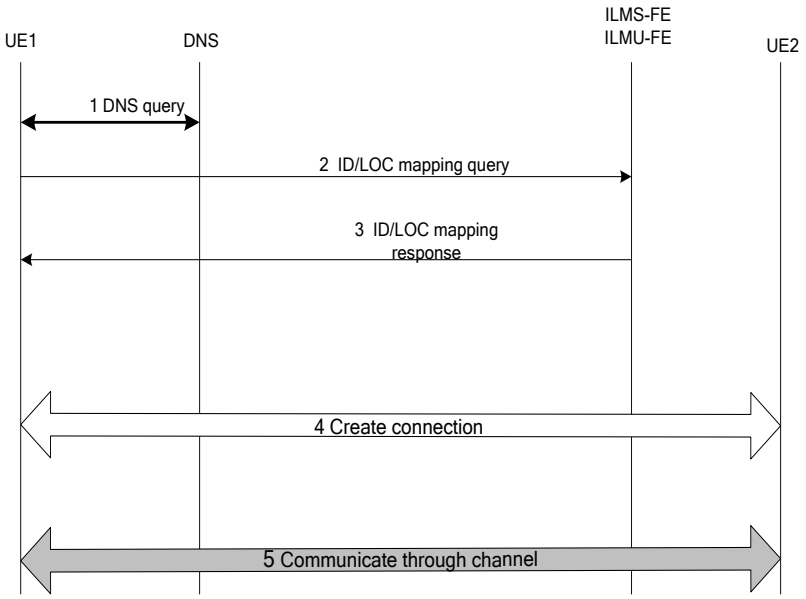

Figure 7- Connection procedures using node ID

1. UE1 sends DNS query towards DNS server to obtain the LOC of ILMS-FE/ILMU-FE.
2. UE forwards ID/LOC mapping query to ILMS-FE/ILMU-FE to obtain the node ID of UE2.
3. The ILMS-FE/ILMU-FE responses to UE2 the node ID of UE2.
4. UE1 creates connection between UE2.
5. Initiator communicates the peer by tunnel.

7.3 Connection procedures using node ID when multihoming

In the multihoming case, UE may sometimes have more than one interface or global address. The transport and higher layers are required to use the node ID for application service or transport session. UE may also have multiple valid LOCs to use, but the UE uses the same node ID to associate with the peer. In practice, UE in a multihoming configuration may have both a preferred peer LOC and a preferred local LOC. When more than one LOC is provided to the UE, the network must select the suitable LOC of UE in communication. To create a connection when the UE is multihoming, ILMS-FE/ILMU-FE stores the ID/LOC mapping. UE1 obtains the IP of ILMS-FE/ILMU-FE through a DNS lookup. UE1 obtains the LOC can be used by UE2 through the

ID/LOC mapping update process. UE1 creates connection between UE2 by the LOC of UE2 it had obtained. The connection procedures using node ID when multihoming is illustrated in Figure 8.

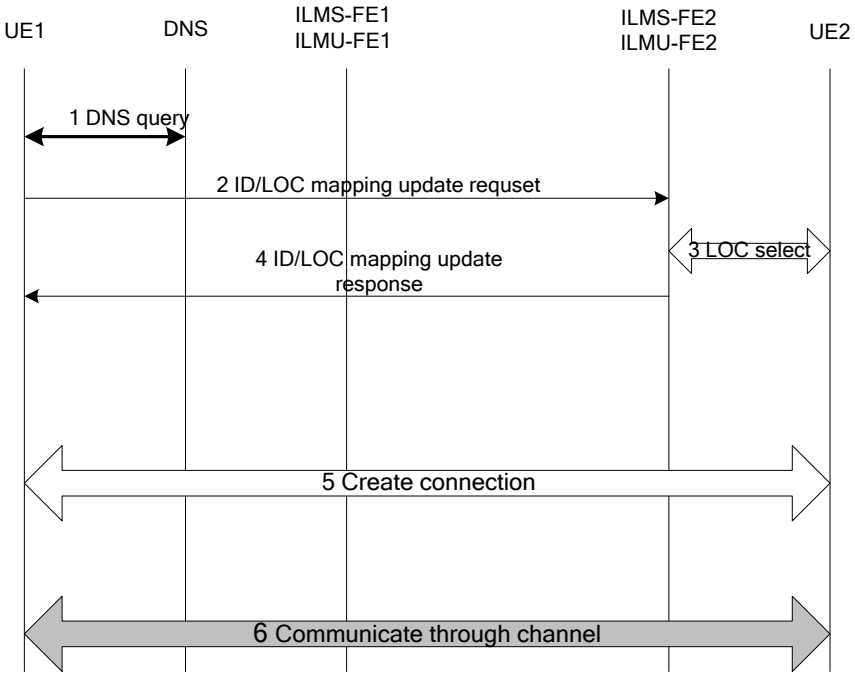

Figure 8- Connection procedures using node ID when multi-homing

1. UE1 sends DNS query towards DNS server obtains the IP of ILMS-FE2/ILMU-FE2;
2. UE1 forwards ID/LOC mapping update request to ILMS-FE2/ILMU-FE2;
3. UE2 selects the LOC can be use and responses to ILMS-FE2/ILMU-FE2;
4. The ILMS-FE2/ILMU-FE2 responses to UE1 the selected LOC of UE2;
5. UE1 creates connection between UE2；
6. Initiator communicates the peer by tunnel.

7.4 Handover procedures using node ID

When UE changes its position in the communicating process, UE requests the ID/LOC split mapping control function to update the ID/LOC mapping of UE. UE updates the connection with the peer side and establishes a channel with which to communicate.
The procedure described in Figure 9.

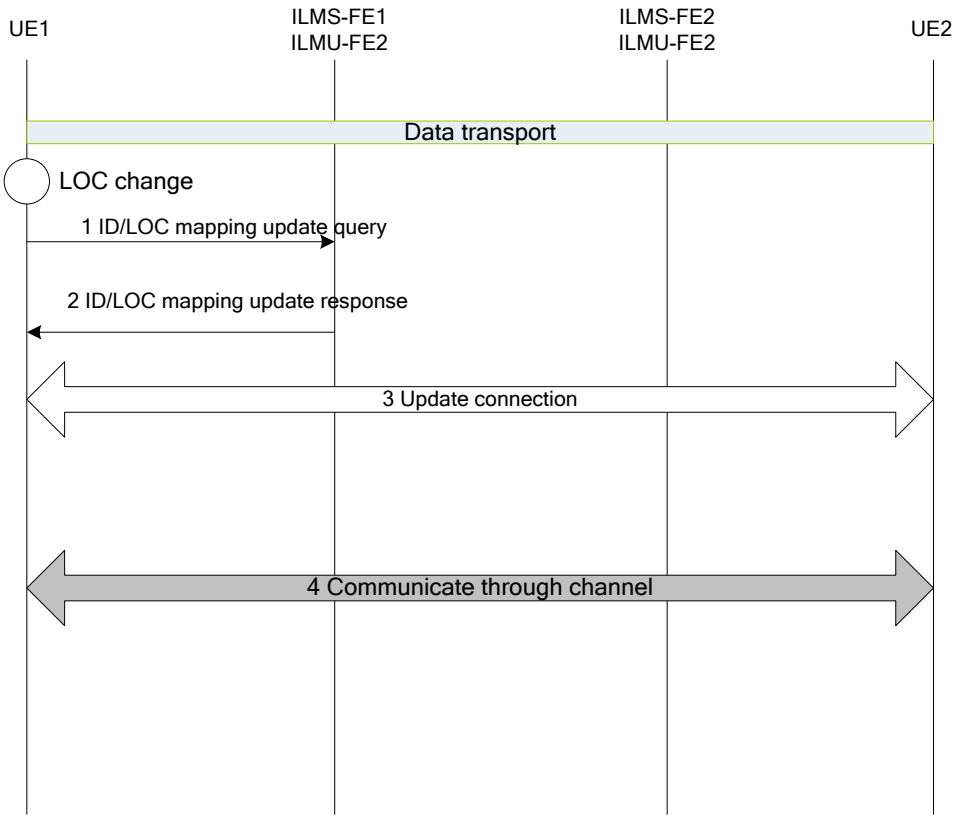

Figure 9- Handover procedures using node ID

When UE1 changes its LOC in data transporting, it may update its ID/LOC mapping in its ILMS-FE/ILMU-FE, and UE1 update connection between UE2, at the same time that it is notifying the peer of the new address. The UPDATE connection message sent from the UE1 to UE2 includes the "Old LOC" and a key parameter. After receiving the update message UE2 responses to UE1 with the new LOC.

1, 2 After UE1 changed its LOC in data transporting, UE1 sends ID/LOC mapping update request to ILMS-FE/ILMU-FE, which responses to UE1 after it updated its ID/LOC mapping.

3. UE1 updates its connection between UE2.
4. Initiator communicates the peer by tunnel.

7.5 Detach procedure

The detach procedure allows:

UE to inform the network that it does not want to access the network, and
The network to inform UE that it does not have access to network any longer.

7.5.1 UE initiated Detach procedure

Detach procedures are provided when UE to inform the network that it does not want to access the network any longer. The detach procedure is initiated by the UE. UE sends detach request to the network attachment control function. After received the detach request the network attachment control function send the ID/LOC mapping delete request to the ID/LOC split mapping control function, which then sends the detach response to UE. After received the ID/LOC mapping delete request the ID/LOC split mapping control function deletes the UE's ID/LOC mapping that has stored in it. The UE initiated detach procedure when initiated by the UE is illustrated in Figure 10.

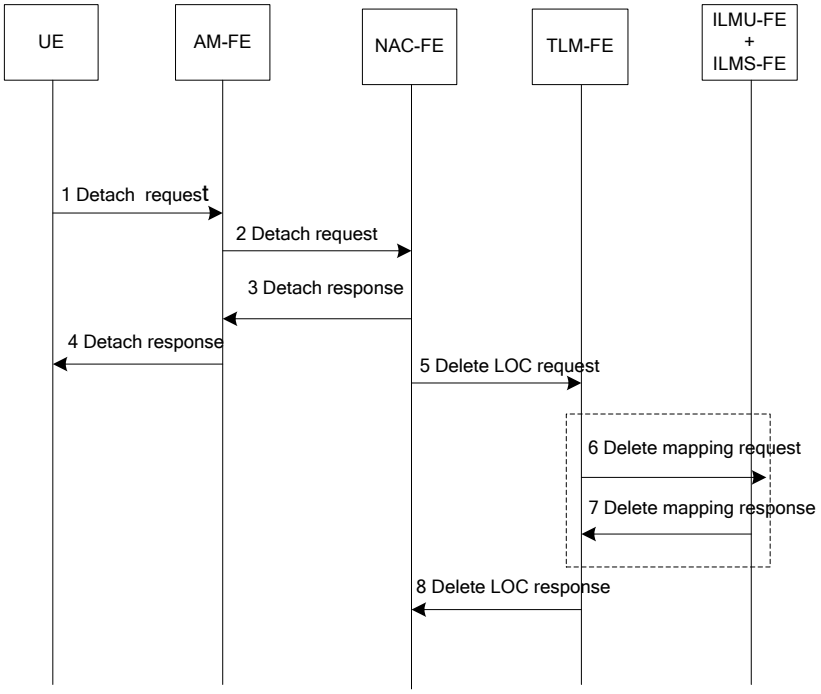

Figure 10- UE Initiated Detach Procedure

1,2 UE sends detach request to the AM-FE, and the AM-FE sends Detach Request to NAC-FE.

3,4. After received the detach message from the AM-FE, the NAC-FE releases the related Bearer context information and sends the detach response with delete Session Response and Detach Indication (Cause) message to the associated AM-FE, which in turn responds to the to UE.

5. The NAC-FE/ sends delete LOC request to TLM-FE.

6. The TLM-FE sends delete ID/LOC mapping request to ILMS-FE/ ILMU-FE.

7. After received the request, the ILMS-FE/ILMU-F responses the delete ID/LOC mapping response to the TLM-FE.

5. The TLM-FE responses the delete LOC response to the NAC-FE.

7.5.2 Network initiated Detach procedure

Detach procedures are provided by network when the network to inform UE that it does not have access to the network any longer. The NAC-FE initiated detach procedure is illustrated in Figure 11.

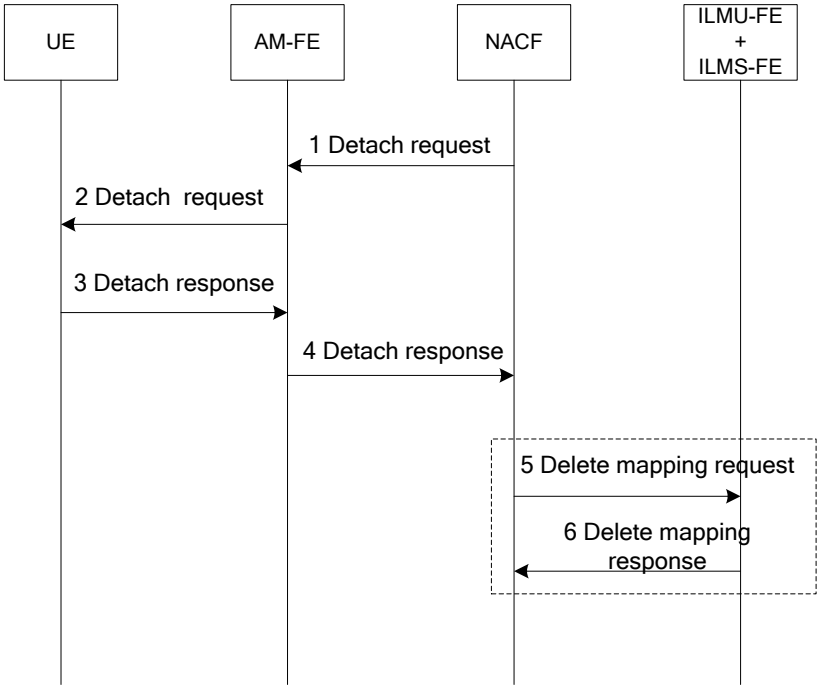

Figure 11- Network Initiated Detach Procedure

As a result of the contract changes or UE charges owed or the network no longer receive the periodically update messages from UE, the network can inform UE that it cannot access to the network, the network sends the Detach message to UE, the network sends the ID/LOC mapping delete request to the ID/LOC split mapping control function to request deleting the ID/LOC mapping of UE. After received the D/LOC mapping delete request the ID/LOC spilt mapping control function deletes the UE's ID/LOC mapping that has stored in it. The network initiated detach procedure is either explicit or implicit. The network may implicitly detach a UE, if it has not had communication with UE for a long period of time.

1, 2 The NACF sends a detach request message to the AM-FE. This message includes an indication that all bearers belonging to that PDN connection shall be released. After received the request the AM-FE sends the detach request message to UE.

3,4 If the UE receives the Detach Request message from the AM-FE in the step2, UE sends a detach response to the AM-FE any time after step2, which in turn responds to UE.

5. The NAC-FE sends delete ID/LOC mapping request to ILMS-FE/ ILMU-FE.

6. After received the request, the ILMS-FE/ ILMU-F responses the delete ID/LOC mapping response to the UE.

7.6 Id-loc-split-based multi-homing

In the scenario of the host-based multihoming, the UE has multiple network addresses with network or the UE supports multiple network access points, then the UE shall use multiple connections simultaneously or in different time. After the UE is authenticated and authorized, the ID/LOC mapping is done through ILMS-FE, ILMU-FE and NACF. When the UE changes its LOC, the ID/LOC mapping is updated through ILMS-FE, ILMU-FE. There are multiple addresses available when the UE tries a connection, the Id-loc-split-based NGN network must makes possible for the UE to select the preferred address to be used. By default, the addresses used are the preferred until indicated otherwise. In the scenario of the multi-homing, after the UE is authenticated and authorized, the UE sends the ID/LOC mapping request to the ILMU-FE via the ILM-FE, then the

ILMU-FE forwards the ID/LOC mapping request to the NACF. The NACF responses to the ILMU-FE carrying the mapping information after NACF allocated the new IP address. The ILMU-FE responds to UE with the ID/LOC mapping information via ILM-FE. When the UE changes its LOC, the UE requests the ID/LOC mapping update query to the ILMS-FE, the ILMS-FE sends the ID/LOC mapping update query to the ILMU-FE. After receiving the ID/LOC napping update query the ILMU-FE responses to the ILMS-FE with the updated ID/LOC mapping, which responds to the UE. Figure 12 shows the scenario of the host-based multihoming.

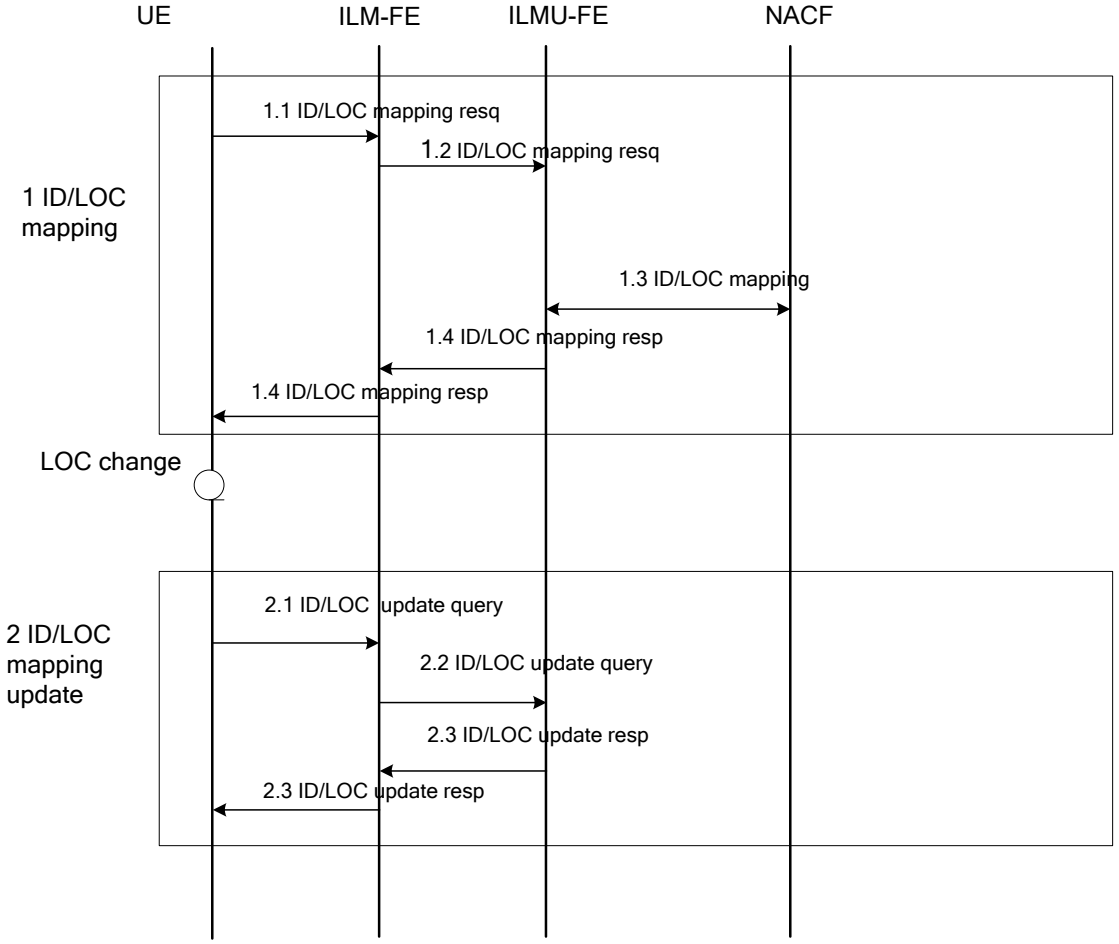

Figure 12- The scenario of the host-based multihoming

After received the request to change the LOC, ILMU-FE sends response to ILMS-FE carrying UE's LOC and its node ID. According to the mapping response the ILM-FE updates the ID/LOC mapping. The ILM-FE selects the LOC of the UE from the updated ID/LOC mapping.

8 Security consideration

The UE and the path from the UE to the ILCF are considered untrusted. The path between the UE is open to attack. UE is required to use secured mechanisms to retrieve ID/LOC mapping data from authenticated ID/LOC storage functions. Security requirements are as below.

R1 The ILMS is required to be secured.

R2 The ILMU is required to be secured.

R3 ILMF is required to be secured.

Annex A

<Annex Title>

(This annex forms an integral part of this Recommendation)

<Body of annex A>

Bibliography

[b-ITU-T X.yyy] ITU-T Recommendation X.yyy (date), *Title*

_____