



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2014

(03/2010)

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

Next Generation Networks – Frameworks and functional
architecture models

Network attachment control functions in next generation networks

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/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/>.

© ITU 2010

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T Y.2014

Network attachment control functions in next generation networks

Summary

This Recommendation describes the network attachment control functions (NACF) component of the NGN functional architecture. This Recommendation also identifies relevant access scenarios related to the NACF.

In particular, this edition includes extensions to Recommendation ITU-T Y.2014 (2008) to address the issues related to multicast and mobility in support of IPTV service and mobility service, respectively.

Keywords

NGN, functional architecture, network attachment

Contents

	Pages
1 Scope	4
2 References.....	4
3 Definitions	4
3.1 Terms defined elsewhere	4
3.2 Terms defined in this Recommendation.....	5
4 Abbreviations and acronyms	5
5 Conventions	7
6 General description	7
6.1 High level functional overview	7
6.2 High level concepts of NACF	8
6.3 Mobility, nomadism	8
6.4 Access network level registration.....	9
6.4.1 Implicit authentication.....	9
6.4.2 Explicit authentication.....	9
6.4.3 HGW remote network configuration.....	10
6.4.4 NGN service stratum components discovery	10
7. Functional architecture	10
7.1 Overview	10
7.2 Functional entities	11
7.2.1 Network access configuration functional entity (NAC-FE).....	11
7.2.2 Access management functional entity (AM-FE).....	12
7.2.3 Transport location management functional entity (TLM-FE).....	13
7.2.4 Transport authentication and authorization functional entity (TAA-FE).....	19
7.2.5 Transport user profile functional entity (TUP-FE).....	19
7.2.6 Home gateway configuration functional entity (HGWCFE)	20
7.2.7 Access relay functional entity (AR-FE)	21
8. Reference points	21
8.1 Internal NACF reference points	21
8.1.1 Reference point AM-FE – NAC-FE (Nd)	21
8.1.2 Reference point NAC-FE – TLM-FE (Ne)	21
8.1.3 Reference point AM-FE – TAA-FE (Na).....	24
8.1.4 Reference point TAA-FE – TLM-FE (Nc).....	24
8.1.5 Reference point NAC-FE – TAA-FE (Nk)	31
8.1.6 Reference point TAA-FE – TAA-FE (Ni).....	31

8.1.7	Reference Point HGWC-FE - TLM-FE (Nx)	33
8.1.8	Reference Point TLM-FE - TLM-FE (Ng)	34
8.1.9	Reference Point TUP-FE – TAA-FE (Nb)	37
8.2	Reference point between NACF and the Resource and Admission Control Functions (RACF)	37
8.2.1	Reference point between TLM-FE and RACF (Ru)	37
8.3	Reference points between NACF and the Service Control Functions	37
8.3.1	Reference point between TLM-FE and Service Control Functions (S-TC1)	37
8.4	Reference points between NACF and CPE	40
8.4.1	Reference points for authentication and IP address allocation (T-U1 and TC-T1)	40
8.4.2	Reference point between HGWC-FE and CPE (TC-Ux)	41
9.	Security considerations	42
Appendix I: Mapping to network roles		43
Appendix II: Information flows		46
II.1	High level information flows	46
II.2	PPP based authentication	47
II.3	DHCP mode	49
Appendix III: Physical configurations		50
III.1	PPP case	50
III.2	PPP with DHCP configuration	51
III.3	DHCP (option 1)	51
III.4	DHCP (option 2)	52
III.5	PANA-based configuration	52
Appendix IV: Overall mapping between ITU-T Recommendation Y.2014 and ETSI ES 282 004 v2.0.0		54
Bibliography		54

Recommendation ITU-T Y.2014

Network attachment control functions in next generation networks

1 Scope

This Recommendation describes the Network attachment control functions (NACF) component of the NGN functional architecture as defined in [ITU-T Y.2012]. This Recommendation also identifies relevant access scenarios related to the NACF.

The Recommendation includes the reference points for the interactions with other NGN components (RACF, MMCF, and SCF) in order to provide the network attachment functions for the fixed, nomadic and mobile terminal/user.

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.2012] | ITU-T Recommendation Y.2012 (2006), <i>Functional requirements and architecture of the NGN</i> |
| [ITU-T Y.2021] | ITU-T Recommendation Y.2021 (2006), <i>IMS for Next Generation Networks</i> |
| [ITU-T Y.2111] | ITU-T Recommendation Y.2111 (2008), <i>Resource and admission control functions in Next generation Networks</i> |
| [ITU-T Y.2018] | ITU-T Recommendation Y.2018 (2009), <i>Mobility management and control framework and architecture within the NGN transport stratum</i> |
| [ITU-T Y.2701] | ITU-T Recommendation Y.2701 (2007), <i>Security requirements for NGN release 1</i> |
| [ITU-T Y.2702] | ITU-T Recommendation Y.2702 (2008), <i>NGN authentication and authorization requirements</i> |
| [ITU-T Q.1761] | ITU-T Recommendation Q.1761 (2004), <i>Principles and requirements for convergence of fixed and existing IMT-2000 systems</i> |
| [ITU-T Y.1541] | ITU-T Recommendation Y.1541 (2006), <i>Network performance objectives for IP-based services</i> |
| [ITU-T Y.1910] | ITU-T Recommendation Y.1910 (2008), <i>IPTV functional architecture</i> |
| [ISO/IEC 7498-2] | ISO/IEC 7498-2, <i>Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture</i> |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 authorisation** [ISO/IEC 7498-2]: the granting of permission based on authenticated identification.

NOTE - In some contexts, authorisation may be granted without requiring authentication or identification, e.g. emergency call services.

- 3.1.2 nomadism** [ITU-T Q.1761]: ability of the user to change his network access point on moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no session continuity or hand-over possible. It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

- 3.2.1 authentication:** a property by which the correct identifier of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network

- 3.2.2 customer premises equipment (CPE):** one or more devices allowing a user to access services delivered by NGN.

NOTE 1 - This includes devices under user control commonly referred to as Home Gateway (HGW) or Terminals (TE), etc, but not network controlled entities such as access gateways.

- 3.2.3 implicit authentication:** authentication based on a trusted relationship already established between two parties, or based on one or more outputs of an authentication procedure already established between two parties.

- 3.2.4 explicit authentication:** authentication that requires that the party to be authenticated performs an authentication procedure (to verify the claimed identification of the party).

- 3.2.5 home gateway (HGW):** gateway between the Customer Premises Network (CPN) and the Access Network.

NOTE 2 - A Home Gateway may be in its simplest form a bridged or routed modem, and in a more advanced form be an Integrated Access Device.

- 3.2.6 line identification:** a process that establishes the identifier of the line based on the trusted configuration.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
ABG-FE	Access Border Gateway Functional Entity
ACL	Access Control List
AM-FE	Access Management Functional Entity
AN	Access Network
AN-FE	Access Node Functional Entity
API	Application Programming Interface
AR-FE	Access Relay Functional Entity
ATM	Asynchronous Transfer Mode
CPE	Customer Premises Equipment
CPN	Customer Premises Network

CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EN-FE	Edge Node Functional Entity
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GTP	GPRS Tunnelling Protocol
HDC-FE	Handover Decision and Control Functional Entity
HGW	Home Gateway
HGWC-FE	Home Gateway Configuration Functional Entity
HTTP	Hyper Text Transfer Protocol
ID	Identifier
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
MAC	Media Access Control
MIP	Mobile Internet Protocol
MLM-FE	Mobile Location Management Functional Entity
MLM-FE(P) role	An instance of the MLM-FE performing the proxy mobile location management
MMCF	Mobility Management and Control Functions
MPLS	Multi-Protocol Label Switching
NACF	Network Attachment Control Functions
NAC-FE	Network Access Configuration Functional Entity
NGN	Next Generation Network
NID-FE	Network Information Distribution Functional Entity
PAA	PANA Authentication Agent
PaC	PANA Client
PANA	Protocol for Carrying Authentication for Network Access
P-CSCF	Proxy-Call Session Control Function
PD-FE	Policy Decision Functional Entity
PE-FE	Policy Enforcement Functional Entity
PIA	Persistent IP Address
PPP	Point-to-Point Protocol
QoS	Quality of Service
RACF	Resource and Admission Control Functions

SADS	Service and Application Discovery and Selection
SCF	Service Control Functions
SLA	Service Level Agreement
SUP-FE	Service User Profile Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TLM-FE	Transport Location Management Functional Entity
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TIA	Temporary IP Address
TUP-FE	Transport User Profile Functional Entity
VC	Virtual Channel
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

5 Conventions

This Recommendation does not make use of specific conventions.

6 General description

6.1 High level functional overview

The NACF provides the following functionalities:

- Dynamic provisioning of IP addresses and other CPE configuration parameters.
- By endorsement of user, auto-discovery of CPE capabilities and other parameters.
- Authentication of end user and network at the IP layer (and possibly other layers). Regarding the authentication, mutual authentication between end user and the network attachment is performed.
- Authorization of network access, based on user profiles.
- Access network configuration, based on user profiles.
- Location management at the IP layer.

The user profiles mentioned above are related to the access transport network subscription only and are referred as "Transport Subscription Profiles" in the remaining part of the document.

The location of the NACF component in the overall NGN architecture can be found in [ITU-T Y.2012] and is placed here for information in Figure 1.

Figure 1 - NGN components including NACF

6.2 High level concepts of NACF

The NACF provides registration at access level and initialization of CPE for accessing to the NGN services. The NACF provides network level identification and authentication, manages the IP address space of the Access Network and authenticates access sessions. The NACF also announces the contact point(s) of the NGN Service stratum components to the CPE.

Network attachment through NACF is based on implicit or explicit user identification and authentication credentials stored in the NACF.

6.3 Mobility, nomadism

Mobility management functions provided by the NACF in this Recommendation are limited to the ability of a terminal to be moved to different access points and access networks (which may be owned by a different access network provider) and a user to utilize different terminal equipments, access points and access networks to retrieve their NGN services (even from another network operator).

The mobility in this Recommendation includes the support of handover and session continuity between access networks as well as nomadism and does not preclude the use of mobility capabilities provided within the access networks.

The NACF architecture does not assume any business roles. However to cope with the requirements for nomadism, roaming as well as mobility, the NACF architecture can be mapped onto various functional network roles present in the fixed broadband access environment. The impact of nomadism, roaming as well as mobility requirements are described in Appendix I.

6.4 Access network level registration

NACF registration involves the identification, authentication, and authorization procedures between the CPE and the NACF to control the access to the NACF. Two authentication types are defined for NACF: implicit authentication, for example based on line identification, and explicit authentication, for example based on EAP [b-IETF RFC 3748]. The relationship between the identifiers and the credentials used for authentication must be known to the NACF for any authentication solution to be possible.

Explicit authentication is operating between the CPE and the NACF. It requires a signalling procedure to be performed between the CPE and the NACF. Implicit authentication may be performed by the NACF based on the line identification of the connection to the CPE. It is a matter of operator policy which form of authentication is applied.

Both implicit authentication and explicit authentication may be used independently as NACF authentication mechanisms.

6.4.1 Implicit authentication

Depending on the access network configuration, especially for wired broadband access networks, the implicit access authentication may rely only on an implicit authentication through physical or logical identification of the layer 2 (L2) transport layer. A CPE can directly access to access network without an explicit authentication procedure.

Which implicit authentication method applies depends on the operator policies.

6.4.1.1 Line authentication

Line authentication is a form of implicit authentication. Line authentication ensures that an access line is authenticated and can be accessed from the HGW. Line authentication is based on the activation of the L2 connection between the HGW and the access network.

Line authentication ensures that an access line is authenticated and can be accessed from the HGW. The Line ID is used for line authentication. The operator's policy decides whether line authentication applies.

6.4.2 Explicit authentication

In case the HGW is a routing modem and the Customer Premises Network (CPN) is a private IP realm, authentication is initiated from the HGW. In case the HGW is a bridge, each TE authenticates with the NACF as the IP realm in the CPN is known to the Access Network (AN).

The relationship between the identifiers and the credentials used for authentication must be known to the NACF for any explicit authentication solution to be possible. The identifiers used for explicit authentication may depend on the authentication mechanism applied and on the access network to which the CPE is connected. Two examples of these identifiers are:

- User identifier and credentials.
- CPE identifier.

The type of explicit authentication mechanisms used depends on the access network configuration and on the operator policy.

6.4.3 HGW remote network configuration

This procedure is needed for the initialization of the HGWs accessing to the NGN service stratum components.

6.4.4 NGN service stratum components discovery

As part of the network registration process, the NACF is required to have the possibility to announce the contact information of the NGN Service stratum components to the CPE. In case the NGN service stratum component is the IMS service component [ITU-T Y.2021], the contact information provided by the NACF identifies the P-CSCF. On the other hand, in case of the IPTV service component [ITU-T Y.1910], the contact information provided by the NACF identifies the Service and Application Discovery and Selection (SADS) functional block.

The contact information provided by the NACF is recommended to be either in the form of the IP address of the contact point or in the form of the Fully Qualified Domain Name (FQDN) of the contact point (in which case the NACF provides the IP address of the DNS server that is able to resolve this FQDN into the IP address of the contact point).

Alternatively, the contact point(s) to the NGN Service stratum component(s) may be statically configured in the CPE, e.g. using Fully Qualified Domain Names (FQDN) and DNS resolution to retrieve the IP address(es) of the contact point(s). This option applies in the non-roaming case.

7. Functional architecture

7.1 Overview

Figure 2 describes the NACF functional architecture with the functional entities and the relevant reference points. Reference points to charging functions are not represented.

Appendix II describes information flows related to network attachment while Appendix III identifies potential physical configurations in which the functional NACF architecture can be applied.

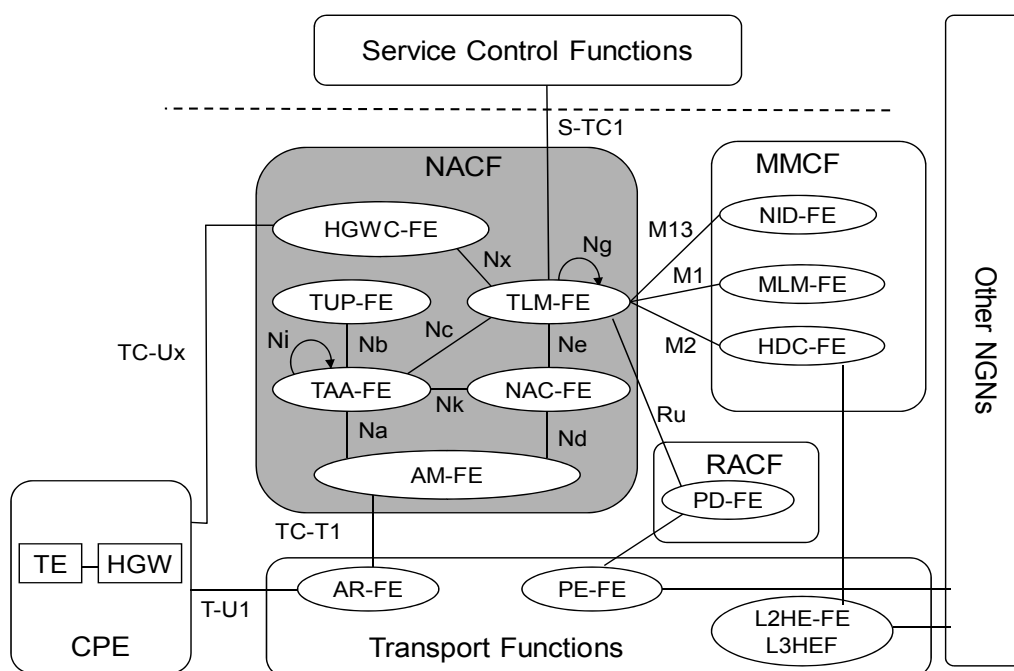


Figure 2 – NACF functional architecture

The NACF comprises the following functional entities:

- Network access control functional entity (NAC-FE)
- Access management functional entity (AM-FE)
- Transport location management functional entity (TLM-FE)
- Transport authentication and authorization functional entity (TAA-FE)
- Transport user profile functional entity (TUP-FE)
- Home gateway configuration functional entity (HGWC-FE)

The NACF has interaction with the following NGN components and entities:

- Service control functions (SCF) (e.g. such as those of the IMS service component [ITU-T Y.2021]) at the S-TC1 reference point for exporting information on access sessions;
- Resource and admission control functions (RACF) [ITU-T Y.2111] at the Ru reference point for exporting Transport Subscription Profile information;
- Mobility management control functions (MMCF) [ITU-T Y.2018] at the M1, M2 and M13 reference points for exporting several types of information on mobility management;
- Transport functions (i.e. Access Relay Functional entity (AR-FE) [ITU-T Y.2012]) acting as relays to/from the CPE for address allocation, authentication and authorization purposes (TC-T1 and T-U1 reference points);
- The customer premises equipment (CPE) at the TC-Ux reference point for configuration purposes.

One or more functional entities may be mapped onto a single physical entity. If one functional entity is implemented by two physical entities, the interface between these physical entities is outside the scope of standardization.

Administrative domains are not represented in Figure 2. Functional entities in the NACF may be distributed over two administrative domains. Appendix I illustrates the impacts of nomadism and roaming on the distribution of NACF, i.e. NACF distribution between Visited NGN and Home NGN access network domains. Note that the Ru reference point between NACF and RACF [ITU-T Y.2111], and the M1, M2 and M13 reference points between NACF and MMCF [ITU-T Y.2018] are an intra-domain reference points.

The NGN architecture does not require a single NACF instance to support multiple access networks. This does not prevent operators from deploying NACF functions that are common to multiple access networks (e.g. one user profile database common to different access networks).

7.2 Functional entities

7.2.1 Network access configuration functional entity (NAC-FE)

The NAC-FE is responsible for the IP address allocation to the CPE. It may also distribute other network configuration parameters such as address of DNS server(s), address of signalling proxies for specific service stratum components (e.g. addresses of the P-CSCF and the SADS when accessing to the IMS service component [ITU-T Y.2021] and IPTV service component [ITU-T Y.1910], respectively).

The NAC-FE should be able to provide to the CPE access network information. This information uniquely identifies the access network to which the CPE is attached. The CPE may send this information to SCFs as a hint to locate the TLM-FE.

SCFs locate the TLM-FE based on the CPE's IP address or/and based on the information of the access network from which the SCFs receive the IP packet (for example P-CSC-FE may have several logical/physical interfaces toward different access networks). SCFs perform a "Location Information Query" towards the TLM-FE over the reference point S-TC1. The key for the query is the IP address used by the CPE.

The NAC-FE may be able to allocate two kinds of IP addresses; Persistent IP address (PIA) and temporary IP address (TIA), to the TE in order to support mobility. Persistent IP address is not changed during the movement of TE, after it has once been allocated to TE. However, it is noted that a different persistent IP address can be allocated to the same TE in certain cases, for example, when the TE is rebooted. The home address of MIP [b-IETF RFC 3220] is an example of the persistent IP address. On the other hand, a different temporary IP address is allocated to a TE whenever the TE moves into a new subnet. The care-of address of MIP is an example of the temporary IP address. The NAC-FE may allocate IP addresses with associated TAA-FE, if an address needs to be allocated during the process of authentication.

NOTE 1 - The transport of the access network identifier to the CPE depends on extension in existing protocols (e.g. new DHCP option or usage of DHCP option 120 [b-IETF RFC 2131]).

NOTE 2 - DHCP servers or RADIUS servers are typical implementations of the NAC-FE.

7.2.2 Access management functional entity (AM-FE)

The AM-FE terminates the layer-2 transport connection between the CPE and the NACF for registration and initialization of the CPE. The layer 2 connection may be used for detecting the network attachment at the network layer. In this case, the layer 2 connection between the CPE and the AM-FE can constitute a unified framework to the higher layer entities across the heterogeneous network environment to facilitate discovery and selection of multiple types of access networks existing within a geographical area. It is important to note that each of the communication relationships between the CPE and the AM-FE does not imply a particular transport mechanism.

Based on this connection, the AM-FE can collect the access network information about link identifier, link parameters, location of TEs, host configuration parameters, etc. The host configuration information may also include the previously assigned authenticated data and location management with the Transport Subscription Profile information that has been served at the previous access network. In the larger scope, the objective of the access network information is to help the higher layer mobility management functions to acquire a global view of the heterogeneous networks in order to realize nomadism across these networks.

The AM-FE translates network access requests issued by the CPE into a format that can be understood by NACF. It forwards the requests for allocation of an IP address and possibly additional network configuration parameters to/from the TAA-FE and the NAC-FE according to the type of request. The AM-FE forwards requests to the TAA-FE to authenticate the user, authorize or deny the network access, and retrieve user specific access configuration parameters. The AM-FE may also add link layer parameters and host configuration parameters to the forwarded requests.

The access network information may help in network discovery/registration in the NAC-FE and the TAA-FE. Both the CPE and the AM-FE may make decisions about connectivity for mobility management and reuse the network registration/authentication data for fast recovery without performing the whole procedures of the registration/authentication/configuration repeatedly. The network information can be further used for the CPE to perform mobility management procedure in the CPE.

NOTE 1 - In case PPP [b-IETF RFC 1661] is applied, the AM-FE terminates the PPP connection and provides the inter-working with the reference point to the NACF e.g. using an AAA protocol (RADIUS [b-IETF RFC 2865] or Diameter [b-IETF RFC 3588]). The AM-FE acts as a RADIUS

client if the TAA-FE is implemented in a RADIUS server (the AM-FE terminates the PPP and translates it to signalling information on the Na reference point).

NOTE 2 - In case IEEE 802.1X [b-IEEE 802.1X]/PANA [b-IETF PANA] is applied, the line authentication may be implicitly performed. The implicit authentication may rely only on the access line to the CPE through physical or logical identification of the layer 2 transport layer.

NOTE 3 - In case mobile access network (e.g., 3GPP access [b-3GPP TS 23.401, b-3GPP TS 23.402]) is connected, the authentication may be performed after translating network access requests in AM-FE. The details are further the study.

7.2.3 Transport location management functional entity (TLM-FE)

The TLM-FE registers the association between the IP address allocated to the CPE and related network location information provided by the NAC-FE, e.g. access transport equipment characteristics, Logical Connection Identifier, identification of the edge PE-FE device, etc. The TLM-FE registers the association between transport location information received from the NAC-FE and geographical location information. The TLM-FE may also store identifier(s) of the user/CPE to which the IP address has been allocated (information received from the TAA-FE), as well as the Transport Subscription profile information and preferences regarding the privacy of location information. In case the TLM-FE does not store the identifier/profile of the user/CPE, the TLM-FE is required to be able to retrieve this information from the TAA-FE. For detailed TLM-FE information model, see clause 7.2.3.1.

In order to support hierarchical structure for location query, the TLM-FE may play several roles, i.e. the Home role, the Local role, or both. In its Home role the TLM-FE stores a pointer to the TLM-FE instance that is playing the Local role for the attachment. The current location information of the user/CPE in the access domain is stored and bound in the Local TLM-FE. So when the user/CPE moves in the same access domain, only the location binding information of the Local TLM-FE needs to be updated; the location binding information of the Home TLM-FE does not need to be updated.

The TLM-FE responds to location queries from Service Control Functions. When one of these functions (e.g., P-CSCF) needs to query the location information of the terminal equipment, it will first query the Home TLM-FE. The Home TLM-FE will then query the Local TLM-FE about the detailed location information of the terminal equipment in the network to which it is attached, based on the index of the Local TLM-FE the terminal equipment belongs to. The actual information delivered by the TLM-FE may take various forms (e.g. network location, geographical coordinates, post mail address etc.), depending on agreements with the requestor and on user preferences regarding the privacy of its location.

On the other hand, in order to support nomadism/roaming, SCFs of the home network access the TLM-FE in the visited network for location information via a TLM-FE-proxy in the home network as shown Figure I-5.

In addition, to support mobility, the interaction between Local TLM-FEs takes place over the Ng reference point.

NOTE 1 - The retrieval by the TLM-FE of geographical information from related user network location characteristics is outside of the scope of this Recommendation.

NOTE 2 - Geographical information may take several different forms depending on the access type and the application.

The TLM-FE identifies the current network location of a TE and keeps track of it as it moves. When the point of attachment of a TE is changed in network, TLM-FE updates the association between the IP address allocated to the TE and related network location information. At the same

time it updates the association between network location information and geographical location information.

When a TE is attached to a new access network and a new temporary IP address is allocated and the location information is stored in new TLM-FE, old TLM-FE may transfer the related context information to new TLM-FE, where the context information includes QoS profile, user preference, etc. At this moment the new TLM-FE may inform Service Control Function of the updated binding information.

The TLM-FE could be informed of Access Control Lists (ACLs), which are could be generated by Service Control Functions and/or management entities, based on user profile in TUP-FE. Whether user subscribes to a certain multicast group or not is an example of user profile. ACLs may consist of packet source address, packet destination address or upper-layer protocol and port number. The TLM-FE informs PD-FE of ACLs to be downloaded to the AN-FE, EN-FE and ABG-FE.

The AN-FE, EN-FE or ABG-FE decides whether to forward or block each packet based on ACLs from PD-FE. In case a user seeks to join a multicast group, the AN-FE, EN-FE or ABG-FE forwards or/and processes the request. If not, the request is discarded and the service request will eventually fail.

7.2.3.1 Information model

The TLM-FE holds a number of records representing active access sessions. These records contain information received from the NAC-FE and the TAA-FE, information on the list of SCFs having subscribed to particular events and additional statically configured data. Table 1 identifies which information elements are stored for each of these access sessions.

NOTE - In case PPP [b-IETF RFC 1661] is used, the Physical Connection Identifier may be provided from the TAA-FE to the TLM-FE.

Table 1 – TLM-FE information model

Access Session Description	
Information component received from the NAC-FE	
Globally Unique IP Address Information	A set of IP address information used for locating the access network to which the CPE is attached.
- Unique IP Address	The IP address for identifying the attached CPE.
- Address Realm	The addressing domain of the IP address (e.g. Subnet prefix or VPN ID).
Physical Connection Identifier (optional)	A local identifier for physical connection of access transport network to which the CPE is attached to (e.g., IP address of PE-FE device, and MAC address or Link ID and physical port)
Logical Connection Identifier	A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel and logical port). It can be used to locate the layer 2 connection and pertinent network devices for a particular attached CPE.
CPE Type	The type of CPE to which the IP address has been allocated.
Information received from the TAA-FE/TUP-FE	
Transport Subscriber Identifier	A globally unique identifier of the attached CPE. This identifier can be used for locating the transport subscription information for the CPE.
Logical Connection Identifier	A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel and logical port).
Mobility Service Parameters (optional) (Note 8)	
- Address of MLM-FE(C) (Note 9)	The address of the instance of the MLM-FE containing the mobile address binding information.
- Address of MLM-FE(P) (Note 9)	The address of the MLM-FE instance which sends the location registration.
- Keying Material (Note 9)	The material used for the security association between the UE and MMCF.
- Mobility Protocol Type	The type of mobility protocol that TE or CPE could support, for example host-based or network-based mobility.
- Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
- Tunnel end point address (optional) (Note 10)	The tunnelling end point address for the network node which works as UE's proxy (lower tunnel end point).
Privacy Indicator (Note 1)	Indicates whether location information can be exported to services and applications.
Transport Resource Subscription (Note 2, Note 3)	
- Transport Subscription Profile ID (Note 4)	The identifier of a set of Transport Subscription Profile information.
- Transport Subscription Profile Description (Note 4)	
- Network Class of Service	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular...). It may include the QoS performance class (e.g., class defined in [ITU-T Y.1541] class).
- Subscribed Upstream Bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.
- Subscribed Downstream Bandwidth	The maximum bandwidth subscribed by a CPE for the downstream connections.
- Level of priority	The maximum level of priority permitted for any reservation request.
- Requestor Name	Identifies the requestor(s) that are allowed by the Transport Resource

	Subscription.
Default Configuration (optional)	
- Default Configuration Identifier (Note 5)	The identifier of a default configuration
- Default Configuration Description (Note 5)	
- Default Access Control List: List of allowed destinations	The list of destination IP addresses, ports, prefixes and port-ranges allowed to cut through by default. (Note 6)
- Default Access Control List: List of denied destinations as well as multicast flows	The list of destination IP addresses, ports, prefixes and port ranges to which traffic is denied by default. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached user equipment must be denied. Address ranges are supported within the list. (Note 6)
- Default Upstream Bandwidth	The maximum bandwidth that can be used for the upstream connections by default.
- Default Downstream Bandwidth	The maximum bandwidth that can be used for the downstream connections by default.
Static Information derived from the Physical Connection Identifier	
Location Information	
Default Transport Subscriber Identifier	
Static Information Derived from the Logical Connection Identifier	
RACF point of contact	The address of the RACF element where the Transport Subscription Profile is to be pushed.
Type of Access Network	The type of access network to which the CPE is attached.
Attached Access Domain Name	The access domain name or the provider's name to which the CPE is attached.
Event Management Information	
Event Management Information (Note 7)	
- Event	The type of event to be monitored
- SCF Identities	The list of SCF to be notified of the occurrence of this event
NOTE 1: An indication whether applications can access location information, depending on their security level. NOTE 2: The access session may contain the description of multiple Transport Resource Subscriptions. NOTE 3: The actual available bandwidth is not known by the NACF. This information can be derived by the RACF based the Logical Connection Identifier. NOTE 4: Either the Transport Subscription Profile ID or the Transport Subscription Profile Description may be included, but not both at the same time. NOTE 5: Either the Default Configuration Identifier or the Default Configuration Description may be included, but not both at the same time. NOTE 6: If a destination does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACF. NOTE 7: More than one Event and associated SCF Identities may be stored. NOTE 8: It is available only if the mobility service is applied. NOTE 9: It is available only if the host-based mobility is applied. NOTE 10: 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. It is available only if the network-based mobility is applied.	

Several records may contain the same Physical Connection Identifier and/or Logical Connection Identifier and/or Transport Subscriber Identifier, as a subscriber may establish more than one IP access session, over the same or different access logical connection (e.g. ATM VC) using the same or different access physical connection. The TLM-FE does not need to establish any link between such records, although it may do it for the purpose of optimizing its storage capacity.