International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2014

(05/2008)

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

Recommendation ITU-T Y.2014

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
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
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

Recommendation ITU-T Y.2014

Network attachment control functions in next generation networks

Summary

Recommendation ITU-T Y.2014 describes the network attachment control functions (NACF) component of the NGN functional architecture. This Recommendation also identifies relevant access scenarios related to the NACF.

Source

Recommendation ITU-T Y.2014 was approved on 7 May 2008 by ITU-T Study Group 13 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

Functional architecture, NGN, network attachment.

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/.

CONTENTS

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.

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

[ITU-T Y.2021] Recommendation ITU-T Y.2021 (2006), *IMS for Next Generation Networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), *Resource and admission control functions in Next generation Networks*.

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

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[ISO 7498-2] ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=14256>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authorization [ISO 7498-2]: The granting of permission based on authenticated identification.

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

3.1.2 nomadism [b-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 handover possible. It is assumed that normal usage pattern is that users shut down 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 – 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 explicit authentication: Authentication that requires that the party to be authenticated performs an authentication procedure (to verify the claimed identification of the party).

3.2.4 home gateway (HGW): Gateway between the customer premises network (CPN) and the access network.

NOTE – 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.

3.2.5 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.

3.2.6 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
AM-FE	Access Management Functional Entity
AN	Access Network
API	Application Programming Interface
AR-FE	Access Relay Functional Entity
ATM	Asynchronous Transfer Mode
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GTP	GPRS Tunnelling Protocol
HGW	Home Gateway
HGWC-FE	Home Gateway Configuration Functional Entity

HTTP	HyperText Transfer Protocol
ID	Identifier
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MAC	Media Access Control
MPLS	MultiProtocol Label Switching
NACF	Network Attachment Control Functions
NAC-FE	Network Access Configuration Functional Entity
NGN	Next Generation Network
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
PPP	Point-to-Point Protocol
QoS	Quality of Service
RACF	Resource and Admission Control Functions
SCF	Service Control Functions
SLA	Service Level Agreement
SUP-FE	Service User Profile Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TLM-FE	Transport Location Management Functional Entity
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

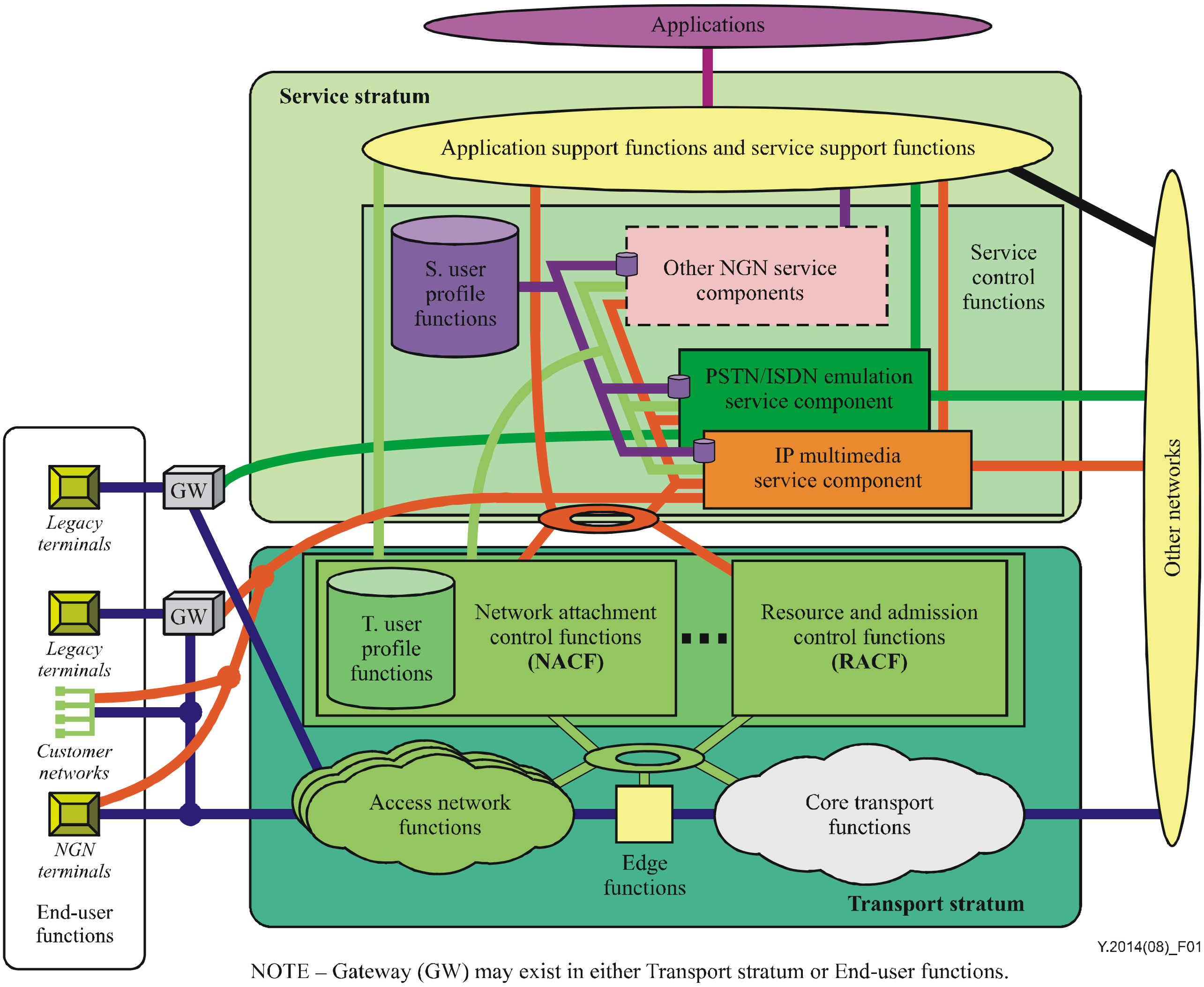
6.1 High level functional overview

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 this Recommendation.

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.


Applications
Service stratum
Application support functions and service support functions
S. user profile functions
Other NGN service components
Service control functions
PSTN/ISDN emulation service component
IP multimedia service component
Other networks
GW
Legacy terminals
GW
Legacy terminals
Customer networks
NGN terminals
End-user functions
T. user profile functions
Network attachment control functions (NACF)
Resource and admission control functions (RACF)
Access network functions
Edge functions
Core transport functions
Transport stratum
Y.2014(08)_F01

NOTE – Gateway (GW) may exist in either Transport stratum or End-user functions.

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).

This Recommendation does not require the support of handover and session continuity between access networks 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 and roaming, the NACF architecture can be mapped onto various functional network roles present in the fixed broadband access environment. The impact of nomadism and roaming 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 the network without an explicit authentication procedure.

Which implicit authentication method applies depends on the operator's 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.

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 (FQDNs) 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 the information flows related to network attachment, while Appendix III identifies potential physical configurations in which the functional NACF architecture can be applied.

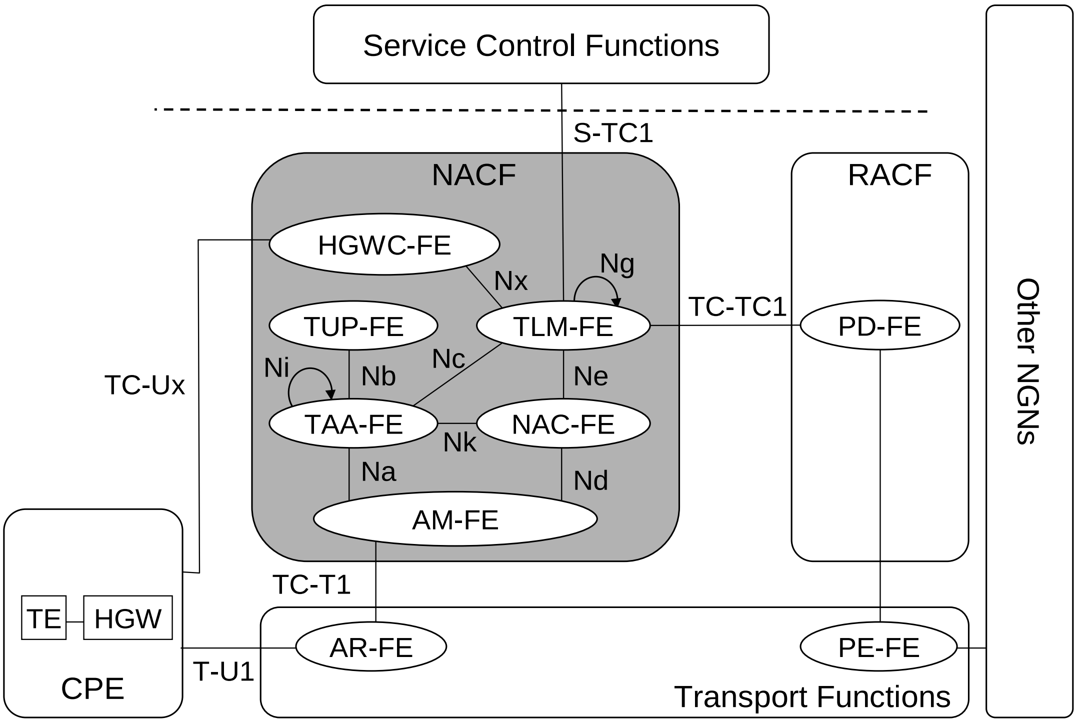


Figure 2 – NACF functional architecture

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 (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 TC-TC1 reference point for exporting transport subscription profile information;
- 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 TC-TC1 reference point between NACF and RACF is an intra-domain reference point ([ITU-T Y.2111]).

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., address of the P-CSCF when accessing to the IMS component [ITU-T Y.2021]).

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

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 interworking 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 [b-IEEE 802.1X]/PANA [b-IETF RFC 4058] 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.

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.

With respect to network attachment and as illustrated in Appendix I, 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 local TLM-FE is in the access network to which the terminal equipment is attached. The home TLM-FE is in the network designated by the transport user profile functional entity. Where these networks differ, communication between the local and home TLM-FE instances takes place over the Ng reference point (see clause 8.1.8).

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.

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 local TLM-FE interfaces with the NAC-FE to get the association between the IP address allocated by the NAC-FE to the CPE and the line ID (logical connection identifier).

The local TLM-FE registers also transport subscription profile information (received from the TAA-FE at authentication) to make this profile information available to the RACF at authentication of the CPE.

The local TLM-FE is able to correlate the information received from NAC-FE and TAA-FE based on the logical connection identifier.

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).
Privacy Indicator (Note 1)	Indicates whether location information can be exported to services and applications.
Transport Resource Subscription (Notes 2 and 3)	
– Transport Subscription Profile ID (Note 4)	The identifier of a set of Transport Subscription Profile information.

Table 1 – TLM-FE information model

Access session description	
– 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, etc.). It may include the QoS performance class (e.g., class defined in [b-ITU-T Y.1541]).
– 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	The list of destination IP addresses, ports, prefixes and port ranges to which traffic is denied by default. (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 Transport Network	The type of access network 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.

Table 1 – TLM-FE information model

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 on 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.

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.

7.2.3.2 TLM-FE state model

The behaviour of the TLM-FE when managing access records can be represented by the state model described in this clause. This state model is not intended to constrain implementations of a TLM-FE. Implementations may use a different model as long as they exhibit the same external behaviour.

This state model defines a session state machine (SSM) that comprises five states:

- *Null*: This state represents a non-existing access record.
- *Wait_For_Bind_Indication_and_Profile*: This state is entered when an access record is created as a result of receiving a request for subscription to an event (e.g., the logon event), while no session record exists for the associated transport subscriber identifier or globally unique IP address information. A partial record is created and the TLM-FE waits for a Bind_Indication event.
- *Wait_For_Bind_Indication*: This state is entered when an access record is created as a result of receiving transport subscription profile information, while no session record exists for the associated transport subscriber identifier or globally unique IP address information. A partial record is created and the TLM-FE waits for a Bind_Indication event.
- *Wait_For_Profile_Information*: This state represents a partial session record where Transport subscription profile information is missing.
- *Active_Session*: This state represents a session record where the full description of an access session is available.

The TLM-FE sends and receives information flows at the S-TC1, TC-TC1, Ne and Nc reference points. Incoming information flows are routed to session state machines (SSM) based on the transport subscriber identifier or the globally unique IP address information they contain.

An SSM instance is created when Bind_Indication or an Event_Subscription_Indication event indicating an unknown transport subscriber identifier or globally unique IP address information occurs.

The following events are handled by the TLM-FE session state machine and cause transition between the states:

– *Event_Subscription_Indication*: This event occurs when an event registration request information flow (see clause 8.3.1) is received from an SCF.

  NOTE – When the actual TLM-FE event occurs, a notification event request information flow is sent back to the AF. This does not cause any state transition.

– *Bind_Indication*: This event occurs when the bind indication information flow is received at the Ne reference point (see clause 8.1.2).

– *Unbind_Indication*: This event occurs when the unbind indication information flow is received at the Ne reference point, or when a negative acknowledgement is received in response to a bind information query (see clause 8.1.2).

– *Subscription_Profile_Received*: This event occurs when a transport resource information indication information flow is received at the Nc reference point asynchronously or as a result of sending a transport resource information request information flow, or when internal configuration data indicate that a default transport subscriber profile applies.

– *Subscription_Profile_Removed*: This event occurs when a transport resource release notification information flow is received at the Nc reference point.

– *Session_Data_Requested*: This event occurs when a transport Resource information request information flow is received at the TC-TC1 reference point, or an information query Request information flow is received at the S-TC1 reference point. It causes an information query response or a transport resource information indication information flow to be sent over the S-TC1 or TC-TC1 reference point.

Figure 3 provides an overview of the state transitions based on the above events.

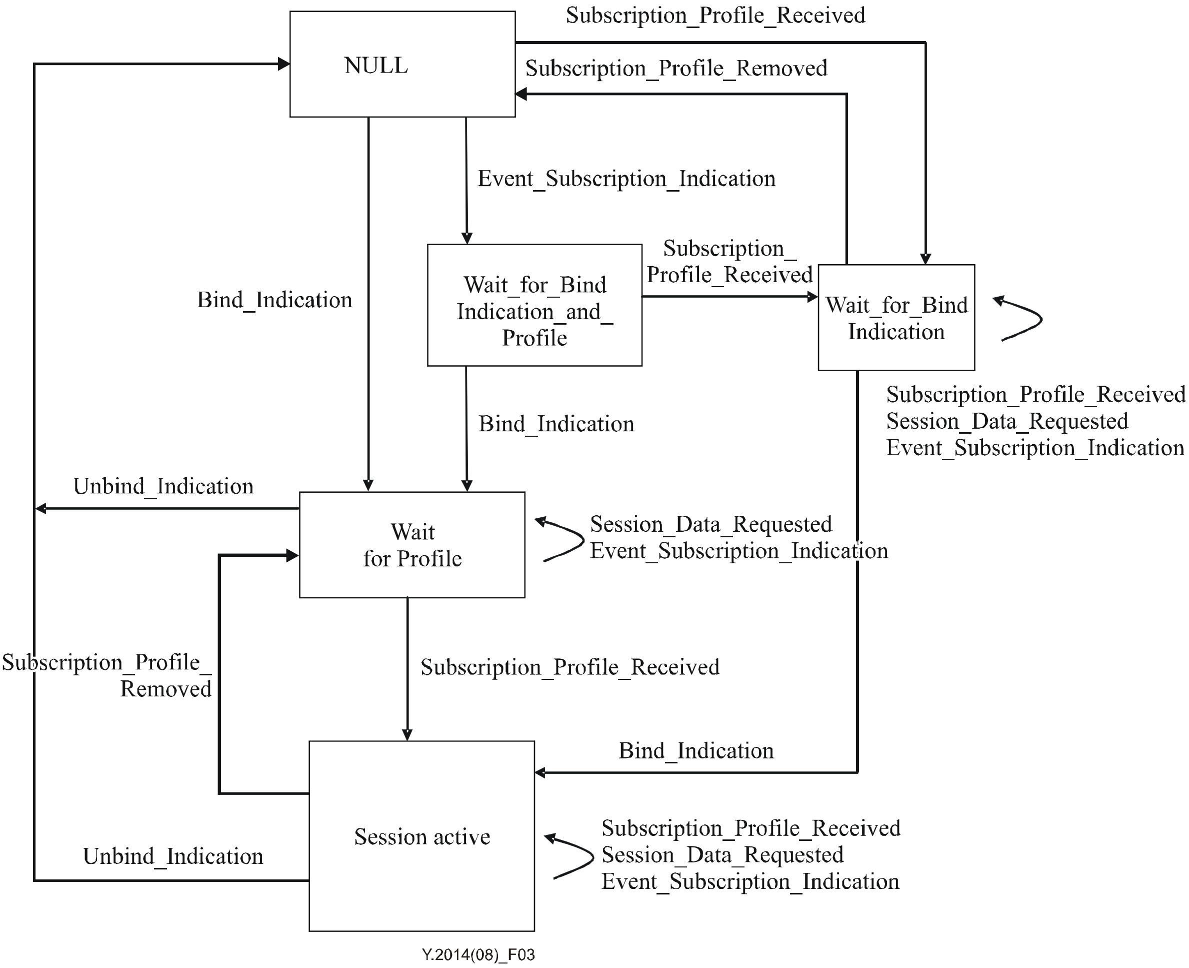

Subscription_Profile_Received
NULL
Subscription_Profile_Removed
Event_Subscription_Indication
Bind_Indication
Wait_for_Bind Indication_and_ Profile
Subscription_ Profile_Received
Wait_for_Bind Indication
Subscription_Profile_Received
Session_Data_Requested
Event_Subscription_Indication
Bind_Indication
Unbind_Indication
Wait for Profile
Session_Data_Requested
Event_Subscription_Indication
Subscription_Profile_ Removed
Subscription_Profile_Received
Bind_Indication
Session active
Unbind_Indication
Subscription_Profile_Received
Session_Data_Requested
Event_Subscription_Indication
Y.2014(08)_F03

Figure 3 – TLM-FE state model for access records management

7.2.4 Transport authentication and authorization functional entity (TAA-FE)

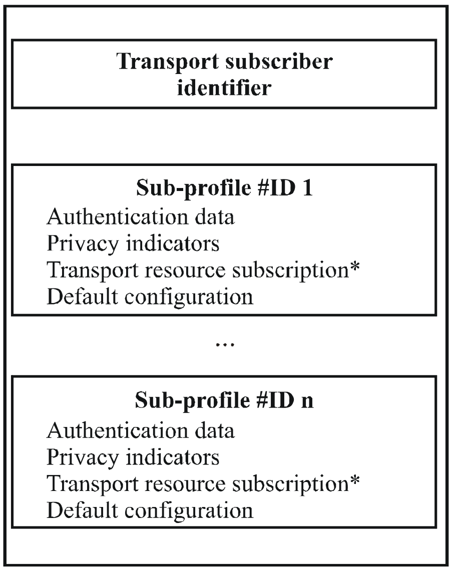
The TAA-FE performs user authentication, as well as authorization checking, based on transport subscription profiles, for network access. For each user, the TAA-FE retrieves authentication data and access authorization information from the transport subscription profile information contained in the TUP-FE. The TAA-FE may also perform the collection of accounting data for each user authenticated by NACF.

The TAA-FE can also act as a proxy. When acting as a proxy, the TAA-FE can locate and communicate with the TAA-FE acting as server which contains the TUP-FE subscription authentication data. The TAA-FE proxy can forward access and authorization requests, as well as accounting messages, received from the AM-FE, to the TAA-FE acting as server. Responses received back in return from the TAA-FE acting as server will be returned to the AM-FE via the TAA-FE proxy. Communication between the proxy TAA-FE and server TAA-FE passes across the Ni reference point.

NOTE 1 – In case PPP [b-IETF RFC 1661] is applied, the AM-FE terminates the PPP and translates it to signalling information on the Na reference point. The TAA-FE is assumed to be able to contact the NAC-FE via an internal reference point to obtain an IP address (TAA-FE and NAC-FE are in the PPP case internal functions). The Nd reference point does not carry DHCP signalling [b-IETF RFC 2131], instead the Na reference point is used to give the IP configuration information to the AM-FE.

7.2.5 Transport user profile functional entity (TUP-FE)

The TUP-FE is the functional entity that contains subscription authentication data (transport subscriber identifier, list of supported authentication methods, key materials, etc.) and information related to the required network access configuration: this data is called "transport subscription profile". The transport subscription profile may be sub-divided into sub-profiles (see Figure 4), each of which is associated to one or more logical connection identifiers. Support of the logical connection identifier is optional.



* Each sub-profile may contain more than one set of transport resource subscription.

Figure 4 – Transport subscription profile in the TUP-FE

The TUP-FE responds to queries from the TAA-FE on the full profile or on a particular sub-profile. In the latter case, it is the responsibility of the TAA-FE (or the Proxy-TAA-FE) to derive a sub-profile identifier from the logical connection identifier.

The TUP-FE can be co-located with the SUP-FE (as described in [ITU-T Y.2012]).

7.2.6 Home gateway configuration functional entity (HGWC-FE)

The HGWC-FE is used during initialization and update of the HGW. It also provides to the HGW with additional configuration information (e.g., configuration of a firewall internally in the HGW, QoS marking of IP packets, etc.). These data differ from the network configuration data provided by the NAC-FE.

Functions of the HGWC-FE also include:

– The HGWC-FE controls and monitors the current configuration of HGW.

– The HGWC-FE stores various configuration data, so it can decide which configuration parameters or profiles to be set or downloaded to the HGW. HGWC-FE is aware of the association between HGW and configuration profile based on subscriber information and/or application classes.

– The HGWC-FE has mechanisms to SET/GET configuration parameters to/from HGW.

The HGWC-FE is recommended to have a mechanism to facilitate profile downloads for a variety of purposes, such as firmware upgrade or vendor-specific configuration profiles.

The HGWC-FE may also handle notifications from the HGW on TE availability. The HGWC-FE may indeed provide configuration information for the TEs, indirectly via the HGW or directly to the TEs. It may also trigger maintenance tests and process results sent by the HGW or by the TEs.

The HGWC-FE may also interface with the TLM-FE in order to retrieve information on the HGW and on the access it is connected to. In such cases, the HGWC-FE uses the procedures described in clause 8.1.7. The information retrieved from the TLM-FE (e.g., physical connection identifier and/or transport subscriber identifier) may be used as input to the selection of configuration data to be delivered to the HGW.

7.2.6.1 Optimized authentication in NACF

During the network attachment procedure, the HGW initiates access request to NACF, and TAA-FE performs the network access level authentication and authorization. If successful, security association (SA) used for protection between the HGW and the HGWC-FE can be negotiated between TAA-FE and the HGW.

The TAA-FE then pushes the SA to the TLM-FE via the Nc reference point, and after that the TLM-FE notifies the SA to the HGWC-FE via the Nx reference point.

The management information exchange between the HGW and the HGWC-FE is bidirectionally authenticated by the SA.

Note that this procedure is optional.

7.2.7 Access relay functional entity (AR-FE)

The AR-FE acts as a relay between the CPE and the NACF. It receives network access requests from the CPE and forwards them to the NACF. Before forwarding a request, the AR-FE may also insert local configuration information. The functionality of AR-FE is described in [ITU-T Y.2012].

NOTE – When using PPP [b-IETF RFC 1661], the AR-FE may act as a PPPoE relay. When using DHCP [b-IETF RFC 2131], the AR-FE acts as a DHCP relay agent.

8 Reference points

8.1 Internal NACF reference points

8.1.1 Reference point AM-FE – NAC-FE (Nd)

The Nd reference point allows the AM-FE to request the NAC-FE for the allocation of an IP address to a CPE as well as other network configuration parameters.

8.1.2 Reference point NAC-FE – TLM-FE (Ne)

The Ne reference point allows the NAC-FE to register in the TLM-FE the binding between an allocated IP address and a CPE as well as other transport related information, such as logical/physical port addresses.

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

- Bind indication
- Bind acknowledgment
- Unbind indication
- Bind information query
- Bind information query acknowledgement

8.1.2.1 Bind indication

Table 2 describes the elements contained in the bind indication information flow.

Table 2 – Bind indication (NAC-FE → TLM-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 allocated to the attached CPE.
– Address Realm	The addressing domain in which the IP address is significant.
Physical Connection Identifier (optional)	A local identifier for physical connection of the access transport network to which the CPE is attached (e.g., IP address of PE-FE device, and MAC address or Link ID and physical port ID).
Logical Connection Identifier (Note 1)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel or logical port).
CPE Type (Note 2) (optional)	The type of CPE.
NOTE 1 – If the NAC-FE is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-option 1 and 2 [b-IETF RFC 2131]. NOTE 2 – If the NAC-FE is implemented as a DHCP server, this parameter is mapped to the DHCP option 77 [b-IETF RFC 2131].	

8.1.2.2 Bind acknowledgement

The bind acknowledgment information flow conveys information that may be sent back to the CPE. The information returned by the TLM-FE in response to a bind indication is received from the TAA-FE or retrieved by the TLM-FE from the TUP-FE, via the TAA-FE.

Table 3 describes the elements contained in the bind acknowledgment information flow.

Table 3 – Bind acknowledgment (TLM-FE → NAC-FE)

HGWC-FE address (optional)	The address of the HGWC-FE entity from which configuration data may be retrieved by the CPE.
Geographic Location Information (optional)	Geographic location information.
P-CSCF Identity (optional)	The identifier of the P-CSCF for accessing IMS services [ITU-T Y.2021].

8.1.2.3 Unbind Indication

The Unbind Indication information flow is sent by the NAC-FE on expiry of the binding between an IP address and a CPE, or when an underlying PPP connection or layer 2 connection is released.

Table 4 describes the elements contained in the Unbind Indication information flow.

Table 4 – Unbind Indication (NAC-FE → TLM-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).

8.1.2.4 Bind information query

The bind information query information flow is used by the TLM-FE to request bind information (e.g., in the context of recovery procedures) from the NAC-FE.

Table 5 describes the elements contained in the bind information query information flow.

Table 5 – Bind information query (TLM-FE → 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).

8.1.2.5 Bind information query acknowledgement

The bind information query acknowledgement information flow is used by NAC-FE to inform the TLM-FE of the result of a bind information query request. When the information query is successful, the acknowledgement information flow contains the information described in Table 6.

Table 6 – Bind information query acknowledgement (NACF-FE → TLM-FE)

Physical Connection Identifier (optional)	A local identifier for physical connection of the 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 ID).
Logical Connection Identifier (Note 1)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel or logical port).
CPE Type (Note 2) (optional)	The type of CPE.
NOTE 1 – If the NAC-FE is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-option 1 and 2 [b-IETF RFC 2131]. NOTE 2 – If the NAC-FE is implemented as a DHCP server, this parameter is mapped to the DHCP option 77 [b-IETF RFC 2131].	

8.1.3 Reference point AM-FE – TAA-FE (Na)

The Na reference point allows the AM-FE to request the TAA-FE for user authentication and transport subscription information checking.

8.1.4 Reference point TAA-FE – TLM-FE (Nc)

The Nc reference point allows the TLM-FE to register the association between a subscriber and the corresponding preferences regarding the privacy of location information provided by the TAA-FE. Reference point Nc is also used to register transport resource subscription information. The TLM-FE may retrieve the transport resource subscription information from the TAA-FE.

The relationship between TAA-FE – TLM-FE may be operated in pull mode or push mode. The push mode is used when the TAA-FE is involved in the processing of network access requests in order to authorize or deny access to the network (e.g., when explicit authentication is used). The pull mode is used when implicit authentication is used or in support of TLM-FE recovery procedures.

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

- Transport resource information indication
- Transport resource information request
- Transport resource information response
- Transport resource release notification

8.1.4.1 Transport resource information indication

The transport resource information indication information flow is used to push transport subscription information from the TAA-FE to the TLM-FE, upon successful authentication of the user. The TAA-FE may decide to send in the same transport resource information indication information flow some transport subscription profiles in the form of a profile identifier (because the actual transport subscription profile information is assumed to be available in the TLM-FE) and some other transport subscription profiles in the form of full profile descriptions. This information is retrieved from the TUP-FE by the TAA-FE.

Table 7 describes the elements contained in the transport resource information indication information flow.

NOTE – In case PPP [b-IETF RFC 1661] is applied, the TAA-FE may provide the physical connection identifier to the TLM-FE.

Table 7 – Transport resource information indication (TAA-FE → TLM-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.
Globally Unique IP Address Information (Note 1)	A set of IP address information used for locating the access network in 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).
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).
Privacy Indicator	Indicates whether location information can be exported to services and applications.
Security Association (optional)	The security association negotiated between the HGW and the TAA-FE during the network access authentication and authorization procedure.
Transport Resource Subscription (Note 2) (optional)	
– Transport Subscription Profile ID (Note 3)	The identifier of a set of Transport Subscription Profile information.
– Transport Subscription Profile Description (Note 3)	
– Network Class of Service	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular, etc.). It may include the QoS performance class (e.g., class defined in [b-ITU-T Y.1541]).
– Subscribed Upstream Bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.
– Subscribed Downstream Bandwidth	The maximum amount of 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.

Table 7 – Transport resource information indication (TAA-FE → TLM-FE)

Default Configuration (Note 4) (optional)	
– Default Configuration Identifier (Note 5)	The identifier of a default configuration
– Default Configuration Description (Note 5)	
– Default Access Control List: allowed destinations	The list of default destination IP addresses and/or ports and/or prefixes and/or port ranges to which traffic can be sent. (Note 6)
– Default Access Control List: denied destinations	The list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. (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.
NOTE 1 – In case PPP [b-IETF RFC 1661] is applied, the TAA-FE is required to provide the globally unique IP address information to the TLM-FE. When DHCP [b-IETF RFC 2131] is applied, this parameter is optional. NOTE 2 – The transport resource subscription may contain multiple transport subscription profiles. NOTE 3 – Either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time. NOTE 4 – This information is used by the RACF to configure the transport functions, before resource reservation requests are received from services/applications. 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.	

8.1.4.2 Transport resource information request

The transport resource information request information flow is used by the TLM-FE to request the transport subscription profile information from the TAA-FE. This information flow is used when the relationship between TLM-FE and TAA-FE operates in pull mode or in the context of TLM-FE recovery procedures.

Table 8 describes the elements contained in the transport resource information request information flow.

Table 8 – Transport resource information request (TLM-FE → TAA-FE)

Globally Unique IP Address Information (Note 1)	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).
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).
Transport Subscriber Identifier (Note 2)	A globally unique identifier for the attached CPE. This identifier can be used for locating the transport subscription information for the CPE.
NOTE 1 – If the information flow is used for supporting recovery procedures and the reference point operates in push mode, the globally unique IP address information is required to be included. NOTE 2 – If the reference point operates in pull mode, the transport subscriber identifier is required to be included.	

8.1.4.3 Transport resource information response

The transport resource information response information flow is used to provide transport subscription information from the TAA-FE to the TLM-FE in response to a transport resource information request.

Table 9 describes the elements contained in the transport resource information response information flow.

NOTE – In case PPP [b-IETF RFC 1661] is applied, the TAA-FE may provide the physical connection identifier to the TLM-FE.

Table 9 – Transport resource information response (TAA-FE → TLM-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.
Globally Unique IP Address Information (Note 1)	A set of IP address information used for locating the access network in 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).
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).
Privacy Indicator	Indicates whether location information can be exported to services and applications.
Security Association (optional)	The security association negotiated between the HGW and the TAA-FE during the network access authentication and authorization procedure.
Transport Resource Subscription (optional) (Note 2)	
– Transport Subscription Profile ID (Note 3)	The identifier of a set of Transport Subscription Profile information.

Table 9 – Transport resource information response (TAA-FE → TLM-FE)

– Transport Subscription Profile Description (Note 3)	
– Network Class of Service	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular, etc.). It may include the QoS performance class (e.g., class defined in [b-ITU-T Y.1541]).
– Subscribed Upstream Bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.
– Subscribed Downstream Bandwidth	The maximum amount of 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 (Note 4) (optional)	
– Default Configuration Identifier (Note 5)	The identifier of a default configuration
– Default Configuration Description (Note 5)	
– Default Access Control List: allowed destinations	The list of default destination IP addresses and/or ports and/or prefixes and/or port ranges to which traffic can be sent. (Note 6)
– Default Access Control List: denied destinations	The list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. (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.

NOTE 1 – In case PPP [b-IETF RFC 1661] is applied, the TAA-FE is required to provide the globally unique IP address information to the TLM-FE. When DHCP [b-IETF RFC 2131] is applied, this parameter is optional.

NOTE 2 – The transport resource subscription may contain multiple transport subscription profiles.

NOTE 3 – Either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time.

NOTE 4 – This information is used by the RACF to configure the transport functions, before resource reservation requests are received from services/applications.

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.

8.1.4.4 Transport resource release notification

The transport resource release notification information flow is used by the TAA-FE to request the TLM-FE to delete the information it held about a CPE. This event occurs as a result of network management actions.

Table 10 describes the elements contained in the transport resource release notification information flow.

Table 10 – Transport resource release notification (TAA-FE → TLM-FE)

Globally Unique IP Address Information (Note 1)	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).
Logical Connection Identifier (optional)	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).
Transport Subscriber Identifier (Note)	A globally unique identifier for the attached CPE. This identifier can be used for locating the transport subscription information for the CPE.
NOTE – Either the Globally Unique IP Address Information or the Transport Subscriber Identifier is included.	

8.1.5 Reference point NAC-FE – TAA-FE (Nk)

The Nk reference point is not specified in this Recommendation.

8.1.6 Reference point TAA-FE – TAA-FE (Ni)

This reference point is intended to be used between a TAA-FE-proxy and a TAA-FE-server, which may be in different administrative domains. This reference point allows the TAA-FE-proxy to request the TAA-FE-server for user authentication and authorization, based on transport subscription profiles. It also allows the TAA-FE-proxy to forward accounting data for the particular user session to the TAA-FE-server or to forward requests received from a TLM-FE.

The TAA-FE-proxy will forward access and authorization requests, as well as accounting messages, received over the Na reference point from the AM-FE, to the TAA-FE-server over the Ni reference point. Responses received back in return from the TAA-FE-server over the Ni reference point will be forwarded to the AM-FE over the Na reference point. A bilateral trust relationship will need to be set up between the TAA-FE-proxy and the TAA-FE-server in order to facilitate this exchange.

This reference point supports AAA message exchange between the TAA-FE-proxy and the TAA-FE-server.

NOTE – RADIUS [b-IETF RFC 2865] and Diameter [b-IETF RFC 3588] are two possible options for protocols on this reference point.

8.1.6.1 Information exchanged on Ni

Table 11 identifies the information components exchanged on the Ni reference point.

Table 11 – Ni reference point

Information component	Description
Transport Subscriber Identifier	A globally unique identifier of the CPE requesting IP connectivity. This identifier can be used for locating the transport subscription information for the CPE.
Privacy Indicator	Indicates whether location information can be exported to services and applications.
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).
Transport Resource Subscription (optional) (Note 1)	
– Transport Subscription Profile ID (Note 2)	The identifier of a set of Transport Subscription Profile information.
– Transport Subscription Profile Description (Note 2)	
– Network Class of Service	Represents the network service class subscribed by the attached CPE (e.g., Premium, Gold, Silver, Regular, etc.). It may include the QoS performance class (e.g., class defined in [b-ITU-T Y.1541]).
– Subscribed Upstream Bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.
– Subscribed Downstream Bandwidth	The maximum amount of 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) (Note 3)	
– Default Configuration Identifier (Note 4)	The identifier of a default configuration
– Default Configuration Description (Note 4)	
– Default Access Control List: allowed destinations	The list of destination IP addresses, ports, prefixes and port ranges allowed to cut through by default. (Note 5)
– Default Access Control List: denied destinations	The list of destination IP addresses, ports, prefixes and port ranges denied to cut through by default. (Note 5)

Table 11 – Ni reference point

Information component	Description
– 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.
NOTE 1 – The transport resource subscription may contain multiple profiles. NOTE 2 – Either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time. NOTE 3 – This information is used by the RACF to configure the transport functions, before resource reservation requests are received from services/applications. NOTE 4 – Either the default configuration identifier or the default configuration description may be included, but not both at the same time. NOTE 5 – If a destination does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACF.	

8.1.7 Reference point HGWC-FE – TLM-FE (Nx)

The Nx reference point enables the HGWC-FE to retrieve information from the TLM-FE. Note that the Nx reference point is similar in nature to the S-TC1 reference point (see clause 8.3.1), the HGWC-FE behaving in this case as a special type of service control function.

8.1.7.1 Information query request

Table 12 describes the information contained in the information query request information flow.

Table 12 – Information query request (HGWC-FE → TLM-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in which the CPE is attached.
– Unique IP Address	The IP address for identifying the CPE.
– Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).
SCF Identity	Indicates the Home Gateway Configuration application.

8.1.7.2 Information query response

Table 13 describes the information contained in the information query response information flow.

Table 13 – Information query response (TLM-FE → HGWC-FE)

Transport Subscriber Identifier	A globally unique identifier for the attached CPE. This identifier can be used for locating the transport subscription information for the CPE.
Physical Connection Identifier	A local identifier for physical connection of the access transport network to which the CPE is attached (e.g., IP address of PE-FE device, and MAC address or Link ID and physical port ID).
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).

8.1.7.3 Notification event request

The TLM-FE may notify the security association to the HGWC-FE using the notification event request information flow.

Table 14 describes the content of the notification event request information flow.

Table 14 – Notification event request (TLM-FE → HGWC-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE.
Event	Event-Type = Security Association
Security Association (SA)	The security association negotiated between the HGW and the TAA-FE during the network access authentication and authorization procedure.

8.1.7.4 Notification event acknowledgement

Table 15 describes the content of the notification event acknowledgement information flow.

Table 15 – Notification event acknowledgement (HGWC-FE → TLM-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE requesting the transport resource. This identifier can be used for locating the transport subscription information for the CPE.
Event	Event-Type = Security Association
Result	Result Code (e.g., success, permanent failure, etc.)

8.1.8 Reference point TLM-FE – TLM-FE (Ng)

The Ng reference point enables communication between local and home TLM-FEs.

Two operations may occur: location registration, in the direction from local TLM-FE to home TLM-FE, and location query, in the direction from home TLM-FE to local TLM-FE.

8.1.8.1 Location registration

Table 16 describes the content of the location registration information flow.

Table 16 – Location registration (Local TLM-FE → Home TLM-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the CPE requesting the IP connectivity.
Attached Access Domain Name	The access domain name or the provider's name of the network.
Index of Local NACF	The address of the Local NACF the user belongs to which is registered by TLM-FE.

8.1.8.2 Location query

Table 17 describes the content of the location query information flow.

Table 17 – Location query (Home TLM-FE → Local TLM-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE.
Attached Access Domain Name	The access domain name or the provider's name of the visited network.
Index of Local NACF	The address of the Local NACF the user belongs to which is registered by TLM-FE.

8.1.8.3 Location query response

The location query response information flow is identical to the information query response on the S-TC1 reference point (see clause 8.3.1.2).

8.1.9 Reference point TUP-FE – TAA-FE (Nb)

The Nb reference point is not specified in this Recommendation, i.e., TAA-FE and TUP-FE are either co-located or connected by a non-standardized interface.

8.2 Reference point between NACF and the resource and admission control functions (RACF)

8.2.1 Reference point between TLM-FE and RACF (TC-TC1)

The TC-TC1 reference point is equivalent to the Ru reference point as defined in [ITU-T Y.2111]. The TC-TC1 reference point allows PD-FE to interact with the NACF for checking on CPE transport subscription profile information and the binding information of the logical/physical port address to an assigned IP address.

The TC-TC1 reference point is an intra-domain reference point.

The TC-TC1 reference point allows information exchange as follows:

– The transport subscription profile information is pushed by the NACF to PD-FE.
– The transport subscription profile information is pulled by PD-FE from the NACF.

For further information, refer to clause 8.4 of [ITU-T Y.2111].

8.3 Reference points between NACF and the service control functions

8.3.1 Reference point between TLM-FE and service control functions (S-TC1)

The S-TC1 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 (e.g., network location information) from the TLM-FE. The form of location information that is provided by the TLM-FE depends on the requestor.

The following information flows are used on the S-TC1 reference point:

– Information query request
– Information query response
– Event registration request
– Event registration response
– Notification event request
– Notification event response

8.3.1.1 Information query request

Table 18 describes the information contained in the information query request information flow.

Table 18 – Information query request (SCF → TLM-FE)

Globally Unique IP Address Information (Note 1)	A set of IP address information used for locating the access network in 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). (Note 2)
Transport Subscriber Identifier (Note 1)	A globally unique identifier of the attached CPE.
SCF Identity	The identifier of the requesting Service Control Function.
NOTE 1 – Either the globally unique IP address information or the transport subscriber identifier is included. NOTE 2 – The addressing domain is known by the SCF either using configuration data (in which case, all terminal equipment served by the SCF belong to the same addressing domain), or from the physical or logical interface over which was received the service request that triggered the location query.	

8.3.1.2 Information query response

Table 19 describes the information contained in the information query response information flow.

Table 19 – Information query response (TLM-FE→ SCF)

Transport Subscriber Identifier (optional)	A globally unique identifier for the attached CPE. (Note 1)
Location Information (optional) (Note 2)	Location information (or a pointer to such information) in a form that is suitable for the requesting service control function.
RACF contact point (optional)	The FQDN or IP address of the RACF entity where resource request is sent (i.e., PD-FE address).
CPE Type (optional)	The type of CPE.
Type of Access Transport Network (optional)	The type of access network to which the CPE is attached.
Physical Connection Identifier (optional)	A local identifier for physical connection of access transport network to which the CPE is attached (e.g., IP address of PE-FE device, and MAC address or Link ID and physical port).
Logical Connection Identifier (optional)	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).
NOTE 1 – This identifier may be used by the SCF when interacting with the RACF. NOTE 2 – Location Information disclosure depends on the requesting application and the subscriber's privacy restrictions. Privacy restrictions are defined in the privacy indicator stored in the TLM-FE.	

8.3.1.3 Event registration request

Table 20 describes the information contained in the event registration request information flow. This information flow is not applicable if the SCF is a P-CSCF [ITU-T Y.2021].

Table 20 – Event registration request (SCF → TLM-FE)

Subscription Duration	Duration for which the subscription for a particular event will be active.
Transport Subscriber Identifier (optional) (Note 1)	A globally unique identifier of the attached CPE.
Event	Event-Type (e.g., user logon event) and Format for Event Relay/Notification description.
Globally Unique IP Address Information (optional) (Note 1)	A set of IP address information used for locating the access network in 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). (Note 2)
SCF Identity (optional)	The identifier of the requesting Service control Function.
NOTE 1 – At least one of the two identifiers ("transport subscriber identifier" or "globally unique IP address information") is required to be supplied. NOTE 2 – The addressing domain is known by the SCF either using configuration data (in which case, all user equipment served by the SCF belongs to the same addressing domain), or from the physical or logical interface over which a related service request was received.	

8.3.1.4 Event registration response

Table 21 describes the information contained in the event registration response information flow. This information flow is not applicable if the SCF is a P-CSCF [ITU-T Y.2021].

Table 21 – Event registration response (TLM-FE → SCF)

Update Action	Administrative Action/Information for an event: e.g., ACTIVATED (event registration successfully received and Event Notification for "Event" activated).
Transport Subscriber Identifier (Note)	A globally unique identifier for the attached CPE.
Event	Event-Type (e.g., user logon event)
Globally Unique IP Address Information (Note)	A set of IP address information used for locating the access network in 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).
NOTE – At least one of the two identifiers ("transport subscriber identifier" or "globally unique IP address information") is required to be supplied.	

8.3.1.5 Notification event request

Table 22 describes the information contained in the notification event request information flow. This information flow is not applicable if the SCF is a P-CSCF [ITU-T Y.2021].

Table 22 – Notification event request (TLM-FE → SCF)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE.
Event	Event-Type (e.g., user logon event)

8.3.1.6 Notification event response

Table 23 describes the information contained in the notification event response information flow. This information flow is not applicable if the SCF is a P-CSCF [ITU-T Y.2021].

Table 23 – Notification event response (SCF → TLM-FE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network in 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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE.
Event	Event-Type
Result	Result Code (e.g., success, permanent failure, etc.)

8.4 Reference points between NACF and CPE

8.4.1 Reference points for authentication and IP address allocation (T-U1 and TC-T1)

There is no direct reference point between the NACF and the CPE for supporting authentication and IP address allocation. Communication between the NACF and the CPE takes place via the access relay functional entity (AR-FE) in the transport functions, and involves both the T-U1 reference point between the CPE and the AR-FE and the TC-T1 reference point between the AR-FE and the NACF.

The T-U1 reference point at the CPE side may either be terminated on a HGW or a TE. The latter case applies when the TE has direct connectivity to the AR-FE.

The T-U1 reference point enables the CPE to initiate requests for IP address allocation and possible other network configuration parameters in order to access to the network. These requests are received by the AR-FE and are relayed to the AM-FE in the NACF via the TC-T1 reference point.

Requests for IP address allocation and network configuration parameters are either in the form of a DHCP [b-IETF RFC 2131] or PPP [b-IETF RFC 1661] request.

In case DHCP is used, the transport functions include an access relay functional entity (AR-FE) that is acting as a DHCP relay between the DHCP clients in the CPE and the DHCP server in the NACF.

Before sending a request to the NACF on the TC-T1 reference point, the AR-FE may add network location information to the information received from the CPE on the T-U1 reference point. The T-U1 reference point enables the CPE to provide user credentials (password, token, certificate, etc.) to the NACF in order to perform network access authentication. The T-U1 reference point may also enable the NACF to provide authentication parameter to the CPE to perform the network authentication when mutual authentication procedure is required. Based on the authentication result, the AM-FE authorizes or denies the network access to the CPE.

NOTE – When DHCP is used for IP address allocation and CPE configuration between the NACF and the CPE, [b-IEEE 802.1X] and PANA [b-IETF RFC 4058] are candidate protocols for authentication between the NACF and CPE.

8.4.2 Reference point between HGWC-FE and CPE (TC-Ux)

The TC-Ux reference point allows the HGWC-FE to configure the HGW, trigger maintenance tests, monitor the performance, and receive notifications. The TC-Ux reference point is used during initialization and update of the HGW to provide the HGW additional network configuration information when this information is not available over the T-U1 reference point, in order to allow the HGW to access to the NGN service control functions.

The HGWC-FE may also manage the TE devices connected to a HGW, indirectly via the HGW or directly to the TEs, for configuration, maintenance, performance monitoring, and notification purposes.

The TC-Ux reference point supports the following procedures:

- HGW identification/authentication to the HGWC-FE (e.g., in order to send appropriate configuration information (firmware upgrade) from the HGWC-FE).
- HGWC-FE authentication to the HGW before one HGW accepts a remote configuration for instance.
- Trigger maintenance tests from the HGWC-FE and report test results from the HGW.
- Configure the HGW.
- Notify the HGWC-FE about TE availability.
- Provide configuration and upgrade for the TEs.
- Trigger maintenance tests from the HGWC-FE and report test results from the TEs.

NOTE – [b-DSL Forum TR-069], HTTP [b-IETF RFC 2616], FTP [b-IETF RFC 959] and TFTP [b-IETF RFC 783] are candidate protocols for this reference point.

9 Security considerations

The security requirements within the functional requirements and architecture of the NACF are addressed by the security requirements for NGN [ITU-T Y.2701], as well as the security requirements for NGN authorization and authentication [ITU-T Y.2702].

Appendix I

Mapping to network roles

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

The NACF architecture does not assume any business roles. However to cope with the requirements for nomadism and roaming, the NACF architecture can be mapped onto various functional network roles present in the fixed broadband access environment as shown in Figure I.1.

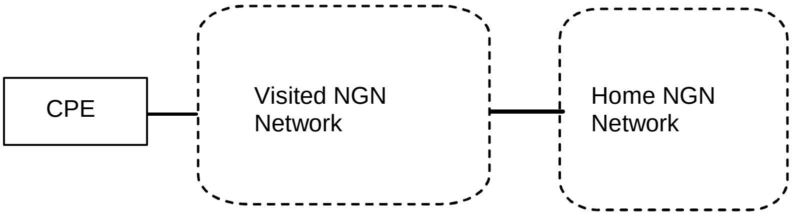


Figure I.1 – Functional network roles in NGN

Figures I.2 and I.3 give the mapping of NACF. Example of the access network in these figures is xDSL access network or a WLAN hotspot.

Figure I.2 shows the scenario 1 whereby the service control functions are (partly) provided by the visited NGN network. Figure I.3 clarifies a scenario 2 in which the home NGN network provides the service control functions.

Figures I.4 and I.5 both represent scenarios 3 and 4 in which a visiting CPE does not perform access authentication. In Figure I.4, the visiting CPE is able to access its home services via roaming agreement at the level of the service control functions. The definition of this is, however, outside the scope of this Recommendation. Figure I.5 gives a scenario in which service control functions of the home network access the TLM-FE in the visited network for location information via a proxy-TLM-FE in the home network. The Ng reference point is used here as a TLM-FE to TLM-FE reference point.

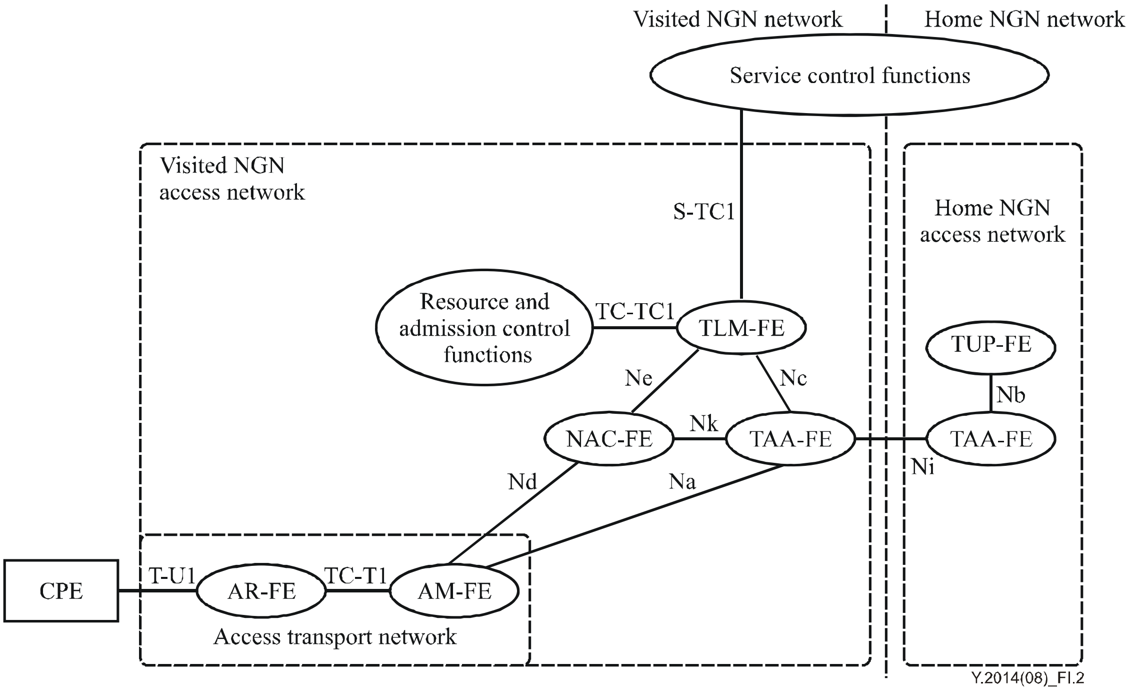


Figure I.2 – NACF mapped on functional network roles – scenario 1

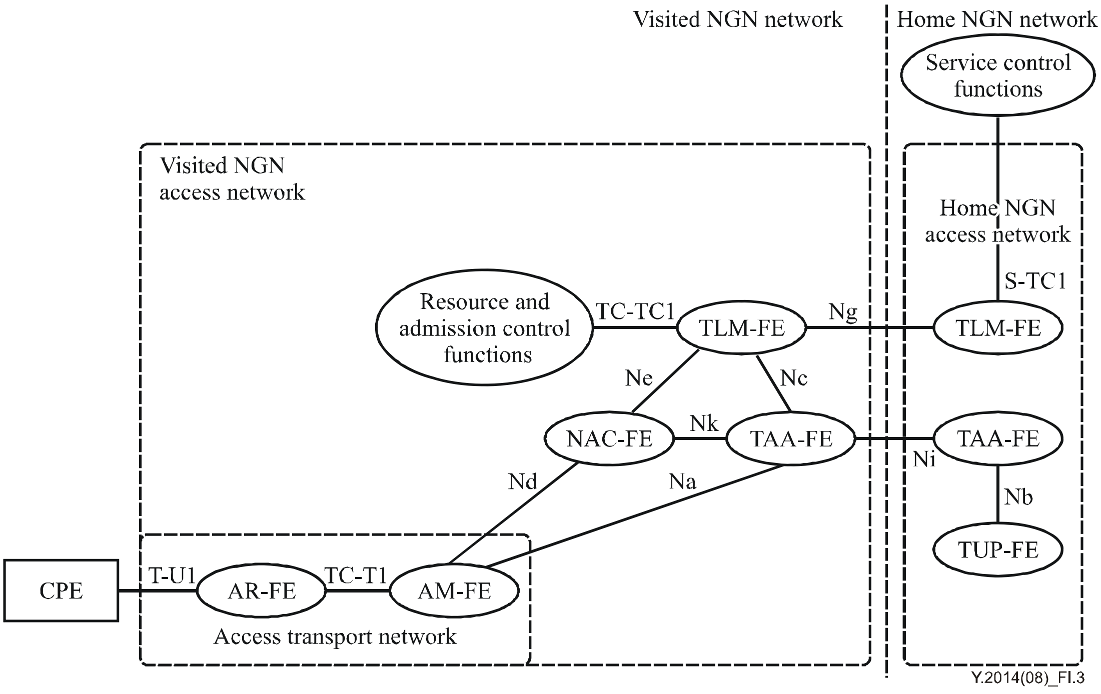


Figure I.3 – NACF mapped on functional network roles – scenario 2 (NGN services from the home network)

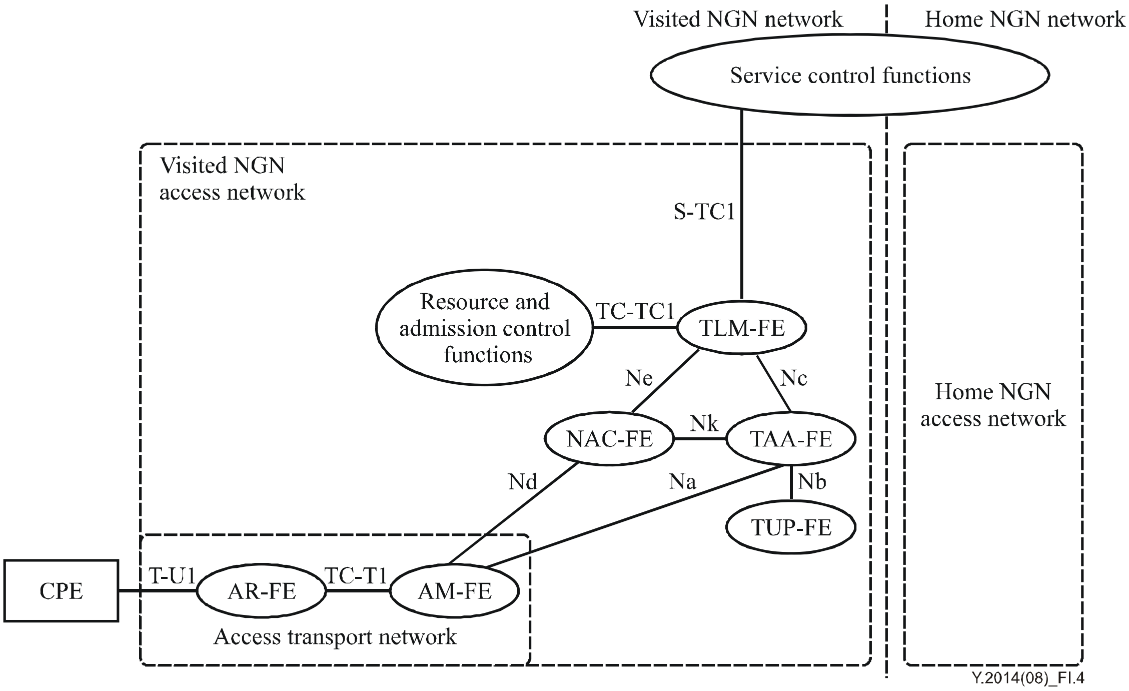


Figure I.4 – NACF mapped on functional network roles – scenario 3

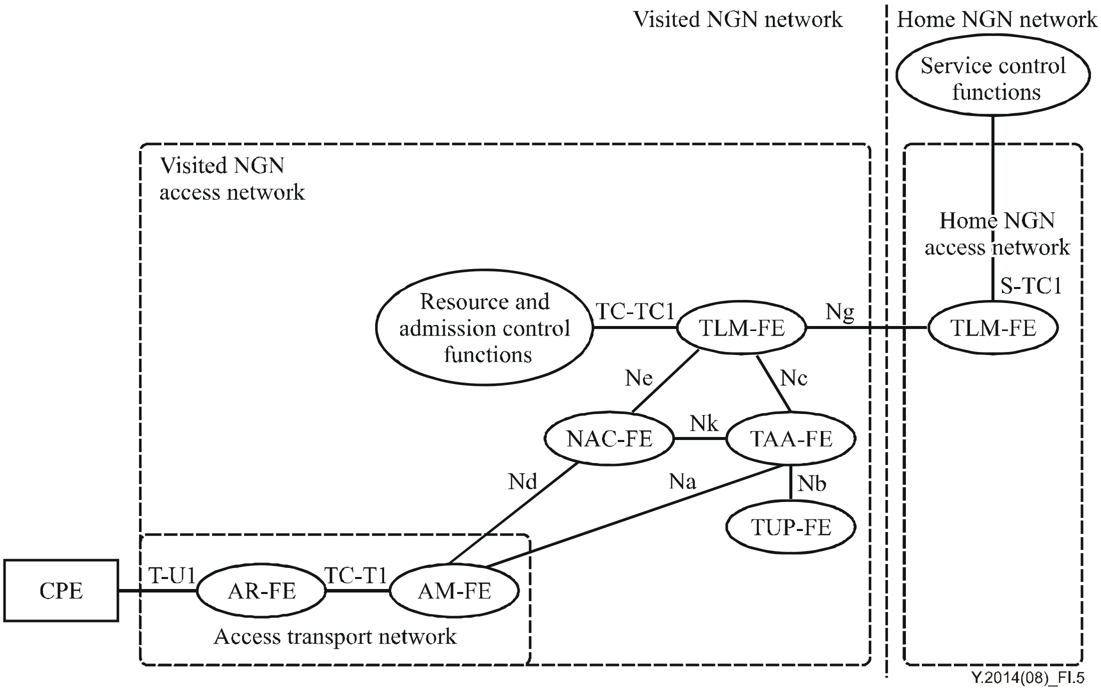


Figure I.5 – NACF mapped on functional network roles – scenario 4

Appendix II

Information flows

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

II.1 High-level information flows

This clause provides high-level information flows that define the network attachment process and the distribution of transport subscription profile information in the NACF and towards the RACF.

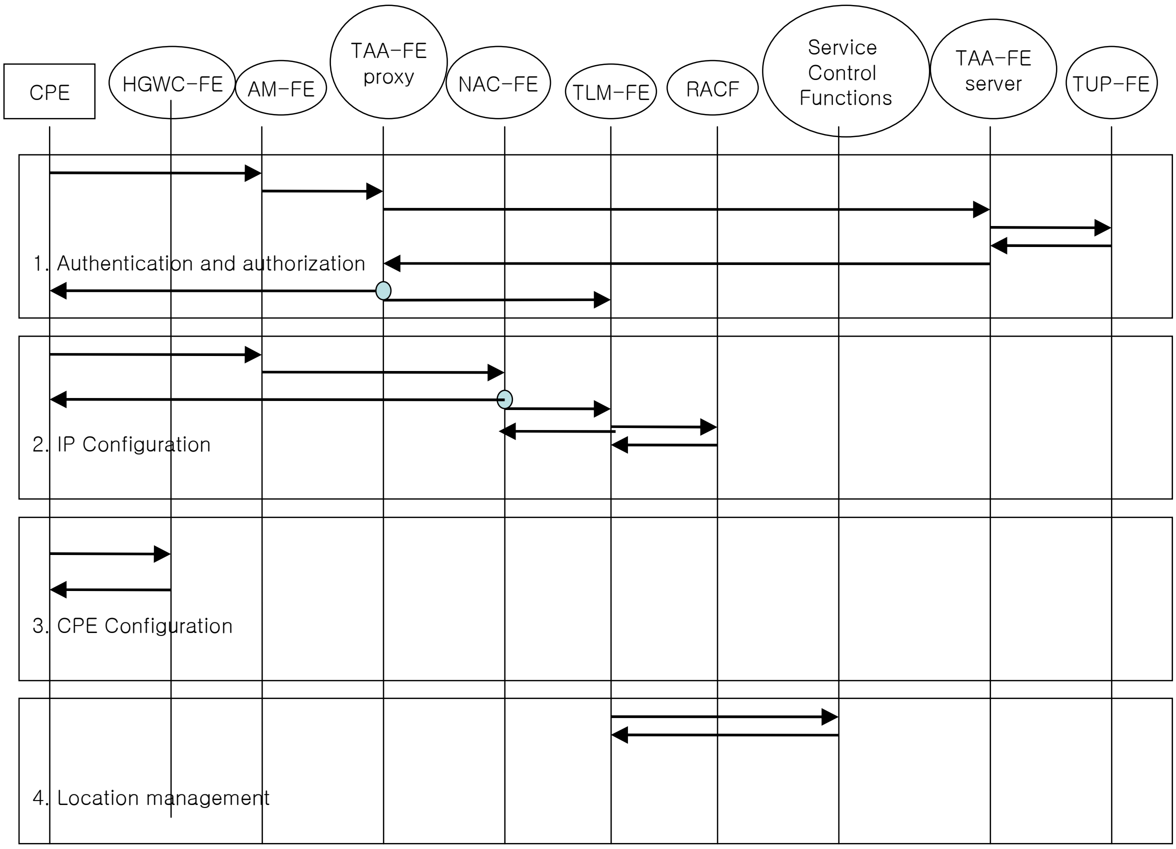


Figure II.1 – High-level information flows

The NACF relies on several stages in the network attachment process. Figure II.1 shows the high level information flows and the different procedures of NACF. Depending on the technology (e.g., [b-IEEE 802.1X], [b-IETF RFC 4058], etc.) and configuration used, these stages can be applied in a different order than presented in Figure II.1:

1) In the first stage of the network attachment process, the CPE will be authenticated and authorized. The authentication process relies on the mechanisms and identities described in clauses 6, 7 and 8. This implies that line authentication and/or access authentication is used. The applicable identifiers are: user identifier and credentials provided by the user or CPE identifier. Step 1 also involves the authorization for access to the network based on the Transport Subscription Profile. A specific transport subscription profile, related, for example, to QoS, may be downloaded from the home NGN network to the visited NGN network (from the TAA-FE-server to the TAA-FE-proxy mode). When the authentication is

successful and the CPE is authorized to use access network resources, configuration of access network based on Transport Subscription Profile is performed. This implies also that the transport subscription profile information specific for the authenticated user is required to be forwarded to the TLM-FE via the Nc reference point. The profile information includes at least the logical connection identifier (i.e., line ID), transport subscriber identifier and the transport resource subscription information, which may be the QoS profile downloaded from the home NGN network or a default configuration profile, and the identification of the edge PE-FE device.

NOTE – Step 1 may occur prior or during the IP address allocation procedure (step 2).

2) Dynamic provision of IP address and provisioning of IP configuration information to the CPE. During step 2, the NAC-FE allocates the IP configuration information. The NAC-FE receives from signalling via TC-T1 reference point the logical connection identifier (i.e., line ID) and establishes the mapping between the allocated IP configuration information and the logical connection identifier. This mapping information is forwarded to the TLM-FE (via the Ne reference point), which correlates this with the transport subscriber identifier and transport subscription profile and pushes this information to RACF via TC-TC1 reference point (i.e., Ru reference point [ITU-T Y.2111]). The RACF configures its functionality in line with the transport subscription profile information it receives from TLM-FE.

3) The HGWC-FE may configure HGW parameters.

4) The NGN service control functions retrieve location information from the TLM-FE via the S-TC1 reference point. In case the NGN service control functions need to access location information in a different domain, the signalling to retrieve the location information is required to be forwarded via a TLM-FE proxy, which is located in the same network as the NGN service control functions that retrieve the information. The primary parameter to retrieve the location information is the transport subscriber identifier and/or the IP address allocated to the CPE by NACF.

II.2 PPP-based authentication

This clause provides example information flows of NACF in case PPP is applied [b-IETF RFC 1661]. These examples are not intended to cover the complete functionality of NACF in case of PPP-based authentication.

NOTE – This is intended as an example only.

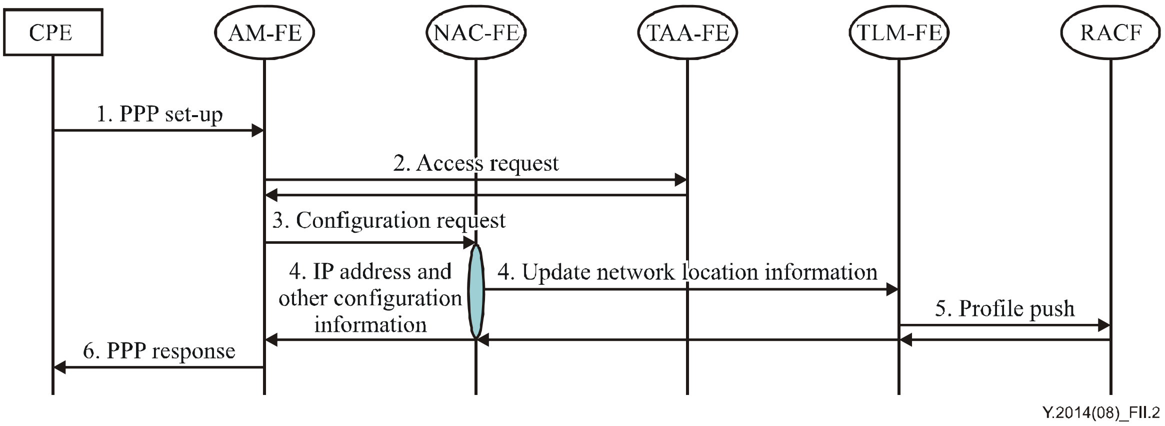


Figure II.2 – PPP-based network attachment

1) CPE initiates a PPP request to apply for an IP address. PPP is used for access and line authentication.

2) AM-FE relays and translates the PPP request to an access request to the TAA-FE for authentication.

3) AM-FE sends the configuration request to NAC-FE to obtain IP address and other parameters including, in this scenario, the IP address of a NGN service control function (e.g., P-CSCF).

4) The NAC-FE allocates an IP address and replies to the AM-FE. The NAC-FE also sends to the TLM-FE the binding information of allocated IP address, line ID and identification of the edge PE-FE device.

5) The TLM-FE pushes the binding information to the RACF via the TC-TC1 reference point (equivalent to the RACF Ru reference point in [ITU-T Y.2111]).

6) The AM-FE sends a PPP response, including the allocated IP address and other parameters, such as the IP address of a NGN service control function (e.g., P-CSCF), to the CPE.

II.3 DHCP mode

This clause provides example information flows of NACF in case DHCP is used. These examples are not intended to cover the complete functionality of NACF in case of DHCP mode.

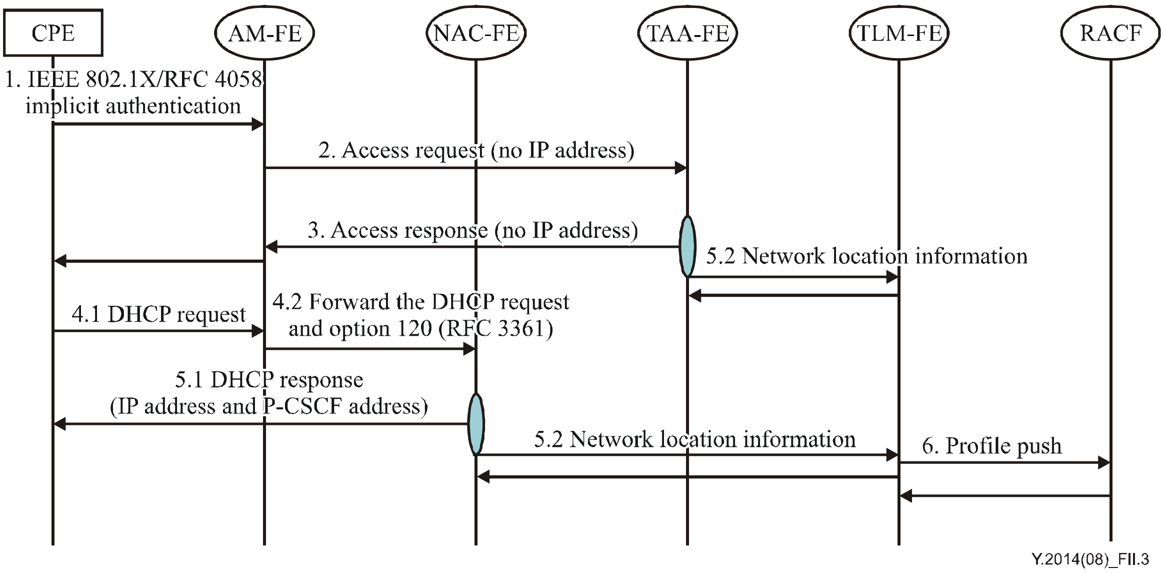

CPE
AM-FE
NAC-FE
TAA-FE
TLM-FE
RACF
1. IEEE 802.1X/RFC 4058
implicit authentication
2. Access request (no IP address)
3. Access response (no IP address)
5.2 Network location information
4.1 DHCP request
4.2 Forward the DHCP request
and option 120 (RFC 3361)
5.1 DHCP response
(IP address and P-CSCF address)
5.2 Network location information
6. Profile push
Y.2014(08)_FII.3

Figure II.3 – DHCP-based network attachment with [b-IEEE 802.1X]/ [b-IETF RFC 4058]/implicit access authentication

1) CPE initiates authentication based on [b-IEEE 802.1X]/[b-IETF RFC 4058]. Alternatively line authentication may be implicitly performed in case no nomadism applies.

2) The AM-FE contacts the TAA-FE for authentication.

3) After successful authentication, the TAA-FE responds with the authentication result. The TAA-FE informs the TLM-FE that a CPE is authenticated.

4) DHCP request is used by CPE to request an IP address (as per flow 4.1) and through DHCP option No. 120 the address of a NGN service control function (e.g., P-CSCF) (as per flow 4.2). This request is relayed by the AM-FE to the NAC-FE, which operates a DHCP server.

5) The NAC-FE allocates an IP address and replies to the CPE. The NAC-FE also informs the TLM-FE that an IP address is allocated the CPE indicated in (3).

6) The TLM-FE pushes the binding information between the allocated IP address, line ID and identification of edge PE-FE device to the RACF via the TC-TC1 interface (equivalent to the RACF Ru reference point in [ITU-T Y.2111]).

NAC-FE provides the FQDN or IP address of the NGN service control function contact point (e.g., P-CSCF), which is relayed by the AM-FE to the CPE.

Appendix III

Physical configurations

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

In this appendix, reference is made to EAP [b-IETF RFC 3748] as an authentication method. Which authentication mechanism is used for NACF is for further study.

III.1 PPP case

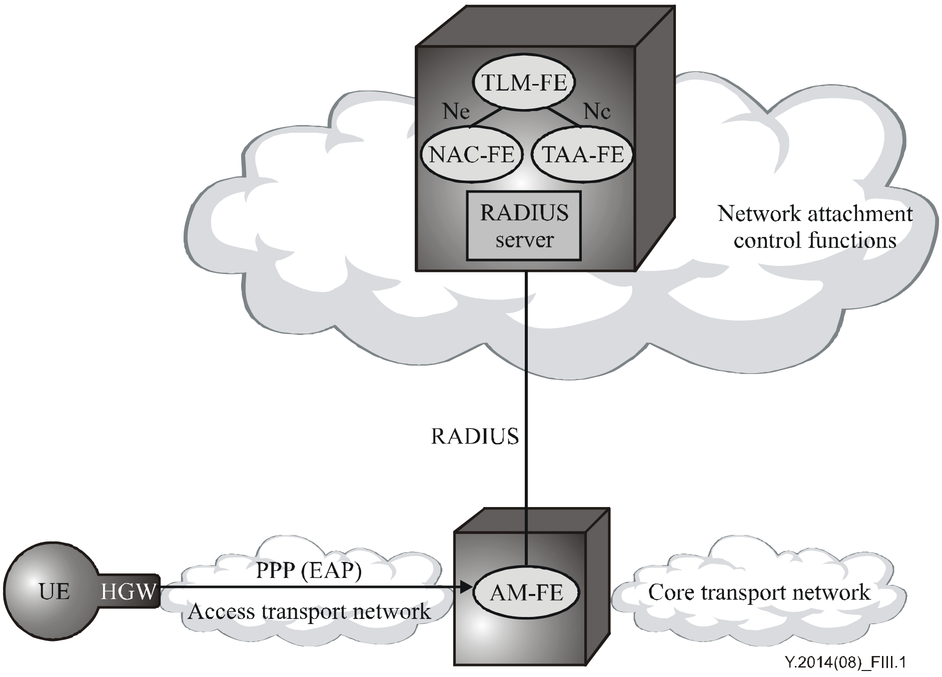


Figure III.1 – PPP-based configuration

NOTE – For the sake of simplicity, interfaces to the RACF are not represented.

III.2 PPP with DHCP configuration

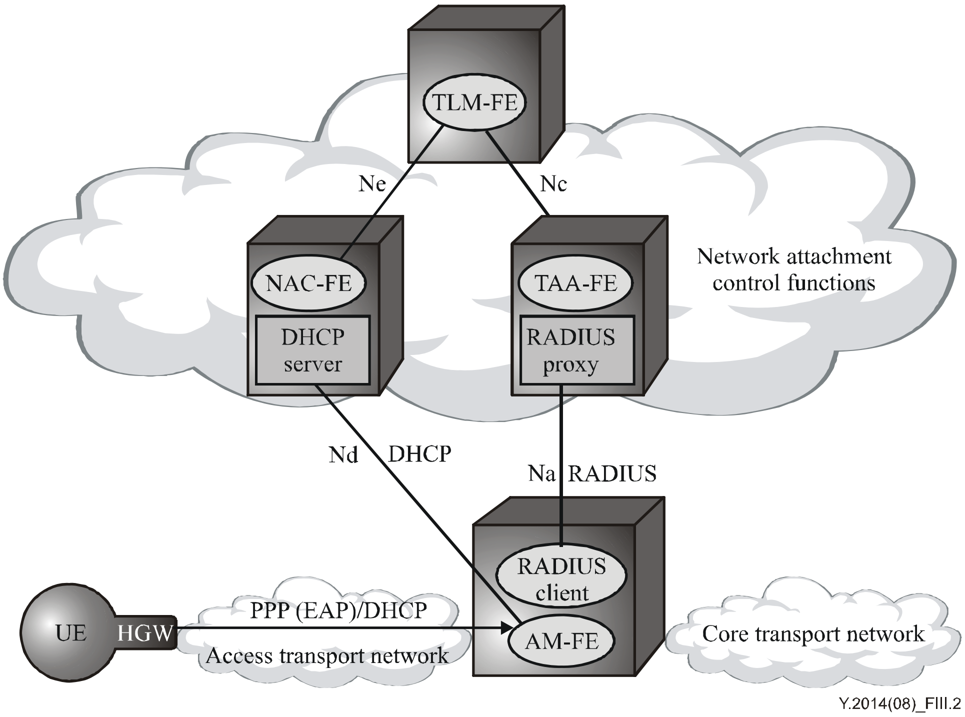


Figure III.2 – PPP-based configuration with DHCP-based IP configuration (allocation of the NGN service control functions contact point to the HGW)

III.3 DHCP (option 1)

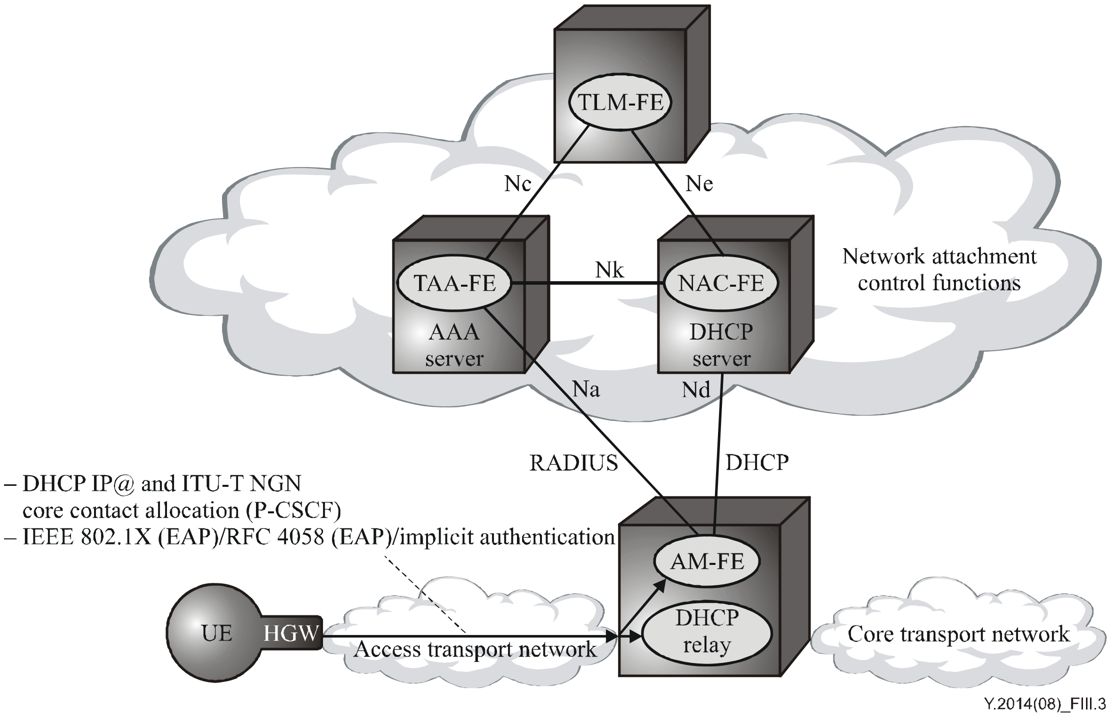

TLM-FE
Nc
Ne
TAA-FE
AAA server
Nk
NAC-FE
DHCP server
Network attachment control functions
Na
Nd
RADIUS
DHCP
– DHCP IP@ and ITU-T NGN core contact allocation (P-CSCF)
– IEEE 802.1X (EAP)/RFC 4058 (EAP)/implicit authentication
AM-FE
DHCP relay
UE
HGW
Access transport network
Core transport network
Y.2014(08)_FIII.3

Figure III.3 – DHCP-based configuration (option 1)

NOTE – For the sake of simplicity, interfaces to the RACF are not represented.

III.4 DHCP (option 2)

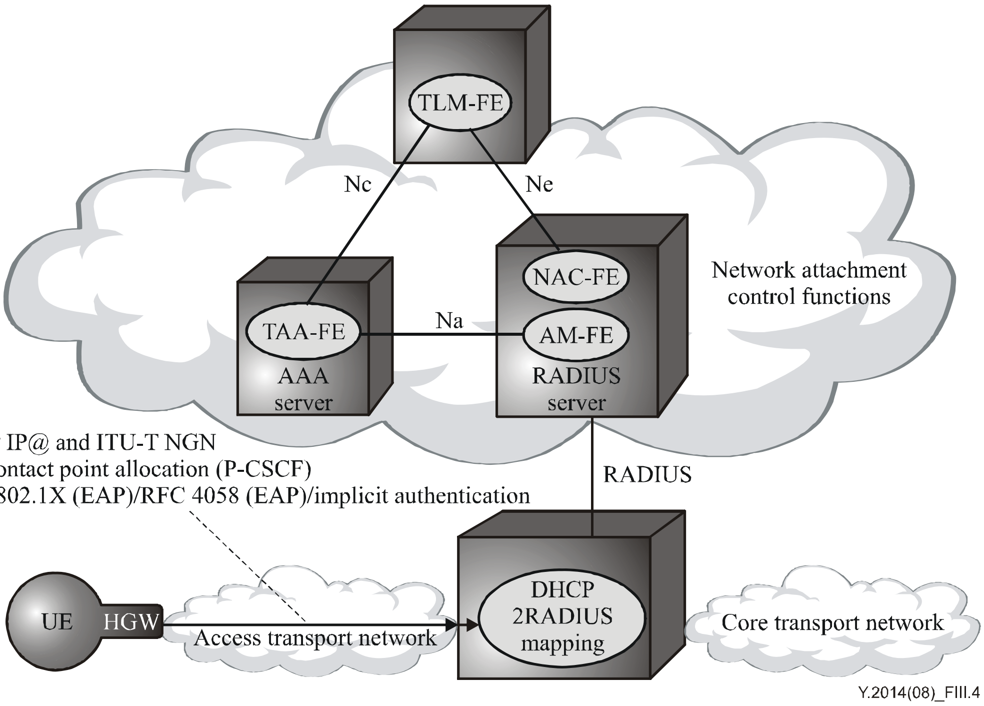


Figure III.4 – DHCP-based configuration (option 2)

NOTE – For the sake of simplicity, interfaces to the RACF are not represented.

III.5 PANA-based configuration

With a DHCP-based implementation, the user authentication may be provided at the IP layer by using PANA (protocol for carrying authentication for network access) defined within [b-IETF RFC 4058]. This IP protocol carries EAP [b-IETF RFC 3748] between a PANA client (PaC) residing in the end user equipment and a PANA authentication agent (PAA) in the transport plane. This PANA signalling goes through an enforcement point (EP) that controls the access of unauthorized users to the network.

The PAA consults an authentication server in order to verify the credentials and rights of a PaC. If the authentication server resides on the same physical equipment as the PAA, an API is sufficient for this interaction. When they are separated, RADIUS or Diameter may be used for this purpose.

Once the user is successfully authenticated and authorized to access to the network, the PAA sends to the EP configuration information to modify the per-packet enforcement policies (i.e., filters) applied on the inbound and outbound traffic of the end user equipment.

Figure III.5 describes a PANA-based implementation for the physical configuration of NACF:

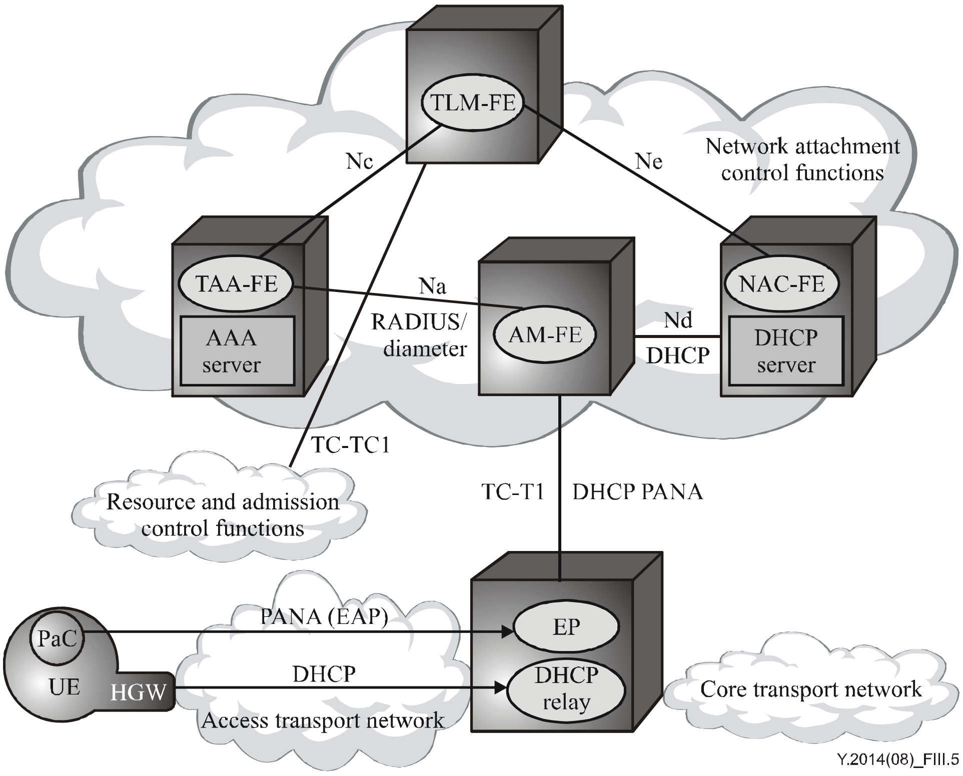


Figure III.5 – PANA-based configuration

Appendix IV

Overall mapping between Recommendation ITU-T Y.2014 and ETSI ES 282 004 v2.0.0

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

Table IV.1 provides a high-level mapping between NACF as specified in this Recommendation and the network attachment sub-system (NASS) as specified in [b-ETSI ES 282 004].

Table IV.1 – Terminology relationships

ETSI ES 282 004 v2.0.0	Recommendation ITU-T Y.2014
Functional entities	
ARF	AR-FE [ITU-T Y.2012]
AMF	AM-FE
NACF	NAC-FE
UAAF	TAA-FE
PBDF	TUP-FE
CLF	TLM-FE
CNGCF	HGWC-FE
CNG	HGW
Reference points	
NACF-AMF: a1	NAC-FE/AM-FE: Nd
NACF-CLF: a2	NAC-FE/TLM-FE: Ne
AMF-UAAF: a3	AM-FE/TAA-FE: Na
UAAF-CLF: a4	TAA-FE/TLM-FE: Nc
UAAF-PBDF: not defined	TAA-FE/TUP-FE: Nb. Details are for further study.
NACF-UAAF: not defined	NAC-FE/TAA-FE: Nk. Details are for further study.
ARF-AMF: e1	AR-FE-AM-FE: TC-T1
UE-ARF: e1	CPE/AR-FE: T-U1 [ITU-T Y.2012]
AF (e.g., P-CSCF)-CLF: e2	Service Control Functions (SCF)/ TLM-FE: S-TC1
CLF-CLF: e2	TLM-FE/TLM-FE: Ng
CNGCF-CLF: e2	HGWC-FE/TLM-FE: Nx
CNGCF-UE: e3	HGWC-FE/CPE: TC-Ux
CLF-RACS: e4	TLM-FE/RACF: TC-TC1 also called Ru in (RACF) [ITU-T Y.2111]
UAAF-UAAF: e5	TAA-FE/TAA-FE: Ni

Bibliography

[b-ITU-T Q.1761] Recommendation ITU-T Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

[b-ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services*.

[b-ETSI ES 282 004] ETSI ES 282 004 V2.0.0 (2008-02), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25226>

[b-IETF RFC 783] IETF RFC 783 (1981), *The TFTP Protocol (Revision 2)*. <http://www.ietf.org/rfc/rfc0783.txt?number=783>

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*. <http://www.ietf.org/rfc/rfc0959.txt?number=959>

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*. <http://www.ietf.org/rfc/rfc1661.txt?number=1661>

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*. <http://www.ietf.org/rfc/rfc2131.txt?number=2131>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*. <http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*. <http://www.ietf.org/rfc/rfc2865.txt?number=2865>

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*. <http://www.ietf.org/rfc/rfc3588.txt?number=3588>

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*. <http://www.ietf.org/rfc/rfc3748.txt?number=3748>

[b-IETF RFC 4058] IETF RFC 4058 (2005), *Protocol for Carrying Authentication for Network Access (PANA) Requirements*. <http://www.ietf.org/rfc/rfc4058.txt?number=4058>

[b-IEEE 802.1X] IEEE 802.1X (2004), *IEEE Standard for Local and metropolitan area networks – Port Based Network Access Control*. <http://www.ieee802.org/1/pages/802.1x.html>

[b-DSL Forum TR-069] DSL Forum TR-069 (2004), *CPE WAN Management Protocol*. <http://www.broadband-forum.org/technical/download/TR-069.pdf>

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	Telephone transmission quality, telephone installations, local line networks
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, 2009