International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2012

(04/2010)

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

Next Generation Networks – Frameworks and functional architecture models

Functional requirements and architecture of next generation networks

Recommendation ITU-T Y.2012

ITU-T Y-SERIES RECOMMENDATIONS

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

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

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

Recommendation ITU-T Y.2012

Functional requirements and architecture of next generation networks

Summary

The objective of Recommendation ITU-T Y.2012 is to describe the functional requirements and architecture of the next generation network (NGN), taking into account the requirements and capabilities for ITU-T NGN as described in Recommendation ITU-T Y.2201. The functional architecture provided in this Recommendation allows a clear distinction between the definition and specification aspects of services provided by the NGN, and the actual specification of the network technologies used to support those services. In line with Recommendation ITU-T Y.2011 principles, an implementation-independent approach is adopted.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2012	2006-09-13	13
1.1	ITU-T Y.2012 (2006) Cor. 1	2008-01-25	13
1.2	ITU-T Y.2012 (2006) Amend. 1	2008-01-25	13
2.0	ITU-T Y.2012	2010-04-30	13

Keywords

Functional architecture, functional entities, NGN.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had 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

Page

Recommendation ITU-T Y.2012

Functional requirements and architecture of next generation networks

1 Scope

The objective of this Recommendation is to describe the functional requirements and architecture of the next generation network (NGN) [ITU-T Y.2001] taking into account the requirements and capabilities for ITU-T NGN as described in [ITU-T Y.2201]. This Recommendation defines functional entities (FEs) of the NGN and is a precursor to further identifying and designating reference points, and defining information flows across such reference points.

The functional architecture provided in this Recommendation allows a clear distinction between the definition/specification aspects of services provided by the NGN and the actual specification of the network technologies used to support those services. In line with [ITU-T Y.2011] principles, an implementation-independent approach is adopted. This Recommendation describes the functional architecture of the NGN by using the generic definitions, symbols, and abbreviations that are defined in related ITU-T Recommendations.

Although the scope of this Recommendation is targeted primarily at an NGN architecture, it is clear that the accommodation of legacy PSTN/ISDN terminals and/or interworking with the PSTN/ISDN is an important consideration with respect to NGN deployment. Thus, to provide a more comprehensive view, certain functional elements required to accommodate PSTN/ISDN terminals and interworking with the PSTN/ISDN are shown/described even though they are not strictly part of the NGN architecture itself.

This Recommendation provides support for nomadism between different network termination points as well as transport level mobility.

Administrations may require network operators and service providers to take into account national regulatory and national policy requirements in implementing this Recommendation.

Note that Annex A provides a high-level description of the main additional features provided in this Recommendation as compared to the 2006 edition of this Recommendation.

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 G.722] Recommendation ITU-T G.722 (1988), *7 kHz audio-coding within 64 kbit/s*.

[ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

[ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks*.

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of the Next Generation Networks*.

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

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions.*

[ITU-T Y.1291] Recommendation ITU-T Y.1291 (2004), *An architectural framework for support of quality of service in packet networks.*

[ITU-T Y.1453] Recommendation ITU-T Y.1453 (2006), *TDM-IP interworking – user plane interworking*.

[ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services.*

[ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture.*

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

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

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

[ITU-T Y.2017] Recommendation ITU-T Y.2017 (2009), *Multicast functions in next generation networks.*

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum.*

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

[ITU-T Y.2031] Recommendation ITU-T Y.2031 (2006), *PSTN/ISDN emulation architecture.*

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks.*

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in Next Generation Networks.*

[ITU-T Y.2171] Recommendation ITU-T Y.2171 (2006), *Admission control priority levels in Next Generation Networks.*

[ITU-T Y.2173] Recommendation ITU-T Y.2173 (2008), *Management of performance measurement for NGN.*

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN.*

[ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for NGN.*

[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.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 content provider [ITU-T Y.1910]: The entity that owns or is licensed to sell content or content assets.

3.1.3 control plane [ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control (see clause 8.1.1 of [ITU-T Y.2011] for some details).

3.1.4 data plane [ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.5 identity management [ITU-T Y.2720]: Set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes),
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects), and
- enabling business and security applications.

3.1.6 IPTV [ITU-T Y.1901]: Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.1.7 management plane [ITU-T Y.2011]: The set of functions used to manage entities in the stratum or layer under consideration, plus the functions required to support this management (see clause 8.1.2 of [ITU-T Y.2011] for some details).

3.1.8 mobility [ITU-T Q.1706]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.9 network operator [ITU-T M.1400]: An operator that manages a telecommunications network. A network operator may be a *Service Provider* and vice versa. A Network Operator may or may not provide particular telecommunications services.

3.1.10 NGN service stratum [ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications (see also clausse 7.1 of [ITU-T Y.2011]).

3.1.11 NGN transport stratum [ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities (see also clause 7.1 of [ITU-T Y.2011]).

3.1.12 nomadism [ITU-T Y.2201]: The ability of the user to change their network access point. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. It is assumed that normal usage pattern is that users shut down their service session before attaching to a different access point.

3.1.13 open service environment capabilities [ITU-T Y.2234]: Capabilities provided by an open service environment to enable enhanced and flexible service creation and provisioning based on the use of standards interfaces.

NOTE – Open service environment capabilities enable services reusability, portability across networks, and accessibility by application providers and user applications in NGN.

3.1.14 service [ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.15 service continuity [ITU-T Q.1706]: The ability for a moving object to maintain ongoing service over including current states, such as user's network environment and session for a service.

3.1.16 service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider may or may not be a customer of another service provider.

3.1.17 user plane [ITU-T Y.2011]: A synonym for data plane.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application network interface: Interface which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for realization of applications.

3.2.2 application provider: A general reference to a provider that offers applications to the customers making use of the services capabilities provided by the NGN.

3.2.3 cardinality: The numeric relationship between occurrences of the entities on either end of the relationship line.

3.2.4 functional architecture: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

3.2.5 functional entity: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.2.6 media: One or more of audio, video, or data.

3.2.7 media stream: A media stream can consist of audio, video, or data, or a combination of any of them. Media stream data conveys user or application data (i.e., a payload) but not control data.

3.2.8 mediated services: Services that are based on intermediate service stratum facilities provided by one or more service providers.

3.2.9 non-mediated services: Services that are not based on intermediate service stratum facilities provided by any service provider.

3.2.10 reference point: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

3.2.11 stream: A flow of real-time information of a specific media type (e.g., audio) and format (e.g., [ITU-T G.722]) from a single source to one or more destinations.

3.2.12 topology: Information that indicates the structure of a network. It contains the network address and routing information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ABG-FE	Access Border Gateway Functional Entity
ABMF	Account Balance Management Function
AG-FE	Application Gateway Functional Entity
AGC-FE	Access Gateway Control Functional Entity
ALG	Application Level Gateway
AM-FE	Access Management Functional Entity
AMG-FE	Access Media Gateway Functional Entity
AMR	Adaptive Multi-Rate
AN-FE	Access Node Functional Entity
ANI	Application Network Interface
APL-GW-FE	Application GateWay Functional Entity
APL-SCM-FE	Application Service Coordination Manager Functional Entity
APP-FE	Application Provisioning Functional Entity
AR-FE	Access Relay Functional Entity
AS	Application Server
AS-FE	Application Support Functional Entity
ASCM-FE	Application Service Coordination Manager Functional Entity
ASF&SSF	Application Support functions and Service Support functions
ASUP-FE	Application Support User Profile Functional Entity
ATM	Asynchronous Transfer Mode
BGC-FE	Breakout Gateway Control Functional Entity
BRAS	Broadband Remote Access Server
CAF	Charging and Accounting Functions
CCF	Charging Collection Function
CD&LC-FE	Content Distribution & Location Control Functional Entity
CDC-FE	Content Delivery Control Functional Entity
CDF	Content Delivery Functions
CDP-FE	Content Delivery Processing Functional Entity
CGCM-FE	CPN Gateway Configuration and Management Functional Entity

CGF	Charging Gateway Function
CGNA-FE	CPN Gateway Network Attachment Functional Entity
CGPD-FE	CPN Gateway Policy Decision Functional Entity
CGPE-FE	CPN Gateway Policy Enforcement Functional Entity
CGSC-FE	CPN Gateway Service Control Functional Entity
CIR	Charging Information Record
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CPR-FE	Content Preparation Functional Entity
CTF	Charging Trigger Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DTMF	Dial Tone Multi Frequency
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EAG	External Application Gateway
EC-FE	Elementary Control Functional Entity
EF-FE	Elementary Forwarding Functional Entity
EN-FE	Edge Node Functional Entity
EPG	Electronic Program Guide
FB	Functional Block
FE	Functional Entity
FMC	Fixed-Mobile Convergence
FP	Flow Point
FW	Firewall
GBA	Generic Bootstrapping Architecture
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSC-FE	General Services Control Functional Entity
HDC-FE	Handover Decision and Control Functional Entity
HGW	Home GateWay
HGWC-FE	Home GateWay Configuration Functional Entity
HSS	Home Subscriber Server
I-CSC-FE	Interrogating Call Session Control Functional Entity
IBC-FE	Interconnection Border Gateway Control Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
ICMP	Internet Control Message Protocol

ID	Identifier
IdM	Identity Management
IdMCC-FE	IdM Coordination and Control Functional Entity
IdP	Identity Provider
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
INNI	Internal Network-Network Interface
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IPCGF	Inter-Provider Charging Gateway Function
IPsec	Internet Protocol Security
IPTV	IP Television
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IVR	Interactive Voice Response
L2HE-FE	Layer 2 Handover Execution Functional Entity
L2TP	Layer 2 Tunnelling Protocol
L3HCF	Layer 3 Handover Control Function
L3HEF	Layer 3 Handover Execution Function
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
LS	Location Server
MGC-FE	Media Gateway Control Functional Entity
MLM-FE	Mobile Location Management Functional Entity
MMCF	Mobility Management and Control Functions
MPLS	Multi Protocol Label Switching
MPM	Management of Performance Measurement
MRB-FE	Media Resource Broker Functional Entity
MRC-FE	Media Resource Control Functional Entity
MRF	Multicast Replication Function
MRP-FE	Media Resource Processing Functional Entity
NAC-FE	Network Access Configuration Functional Entity
NACF	Network Attachment Control Functions
NAPT	Network Address and Port Translation
NAT	Network Address Translation

NE	Network Element
NID-FE	Network Information Distribution Functional Entity
NIR-FE	Network Information Repository Functional Entity
NGN	Next Generation Network
NNI	Network-Network Interface
NPF	NAPT Proxy Function
NSIW-FE	Network Signalling Interworking Functional Entity
OAMP	Operation, Administration, Maintenance and Provisioning
OCF	Online Charging Function
OSA	Open Service Architecture
OSE	Open Service Environment
P-CSC-FE	Proxy Call Session Control Functional Entity
PD-FE	Policy Decision Functional Entity
PDG	Packet Data Gateway
PE-FE	Policy Enforcement Functional Entity
PII	Personally Identifiable Information
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PS	Presence Server
PSTN	Public Switched Telephone Network
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RF	Rating Function
S-CSC-FE	Serving Call Session Control Functional Entity
SADS	Service and Application Discovery and Selection
SAA-FE	Service Authentication and Authorization Functional Entity
SC&CDF	Service Control and Content Delivery Functions
SCF	Service Control Functions
SCP	Service Control Point
SCP-FE	Service and Content Protection Functional Entity
SDH	Synchronous Digital Hierarchy
SG-FE	Signalling Gateway Functional Entity

SIP	Session Initiation Protocol
SL-FE	Subscription Locator Functional Entity
SLA	Service Level Agreement
SNI	Service Network Interface
SPAI	Service Provider Access Interface
SS-FE	Service Switching Functional Entity
STP	Spanning Tree Protocol
SUP-FE	Service User Profile Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TLM-FE	Transport Location Management Functional Entity
TMG-FE	Trunking Media Gateway Functional Entity
TRC-FE	Transport Resource Control Functional Entity
TRE-FE	Transport Resource Enforcement Functional Entity
TUP-FE	Transport User Profile Functional Entity
UDP	User Datagram Protocol
UE	User Equipment
UNG	User Network Gateway
UNI	User Network Interface
URI	Uniform Resource Identifier
USIW-FE	User Signalling Interworking Functional Entity
UT	User Terminal
VCR	Video Cassette Recorder
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
VR	Virtual Router
W-CDMA	Wideband-Code Division Multiple Access
WAG	WLAN Access Gateway
WDM	Wavelength Division Multiplexing
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WS	Web Server
WSG	Web Services Gateway
xDSL	x Digital Subscriber Line

5 Conventions

The following conventions apply:

1) This Recommendation uses the following conventions which are specific to this Recommendation and are used to facilitate referencing different relationships:

A-C_n: This term is used to indicate the relationship between functional entities in application support functions and service support functions, and functional entities in content delivery functions.

A-ON_n: This term is used to indicate the relationship between functional entities in application support functions and service support functions, and other networks.

A-S_n: This term is used to indicate the relationship between functional entities in application support functions and service support functions, and functional entities in service control functions.

A-T_n: This term is used to indicate the relationship between functional entities in application support functions and service support functions, and transport processing functional entities.

A-U_n: This term is used to indicate the relationship between functional entities in application support functions and service support functions, and end-user functions.

C-T_n: This term is used to indicate the relationship between functional entities in content delivery functions and transport processing functional entities.

C-U_n: This term is used to indicate the relationship between functional entities in content delivery functions and end-user functions.

I-A_n: This term is used to indicate the relationship between functional entities in identity management functions and functional entities in application support functions, and service support functions.

I-C_n: This term is used to indicate the relationship between functional entities in identity management functions and functional entities in content delivery functions.

I-M_n: This term is used to indicate the relationship between functional entities in identity management functions and functional entities in management functions.

I-S_n: This term is used to indicate the relationship between functional entities in identity management functions and functional entities in service control functions.

I-T_n: This term is used to indicate the relationship between functional entities in identity management functions and transport processing functional entities.

I-TC_n: This term is used to indicate the relationship between functional entities in identity management functions and transport control functional entities.

I-U_n: This term is used to indicate the relationship between functional entities in identity management functions and end-user functions.

S-C_n: This term is used to indicate the relationship between functional entities in service control functions and functional entities in content delivery functions.

S-ON_n: This term is used to indicate the relationship between functional entities in service control functions and other networks, including other NGNs.

S-T_n: This term is used to indicate the relationship between functional entities in service control functions and transport processing functional entities.

S-TC_n: This term is used to indicate the relationship between functional entities in service control functions and transport control functional entities.

S-U_n: This term is used to indicate the relationship between functional entities in service control functions and end-user functions.

T-ON$_n$: This term is used to indicate the relationship between transport processing functional entities and other networks, including other NGNs.

T-U$_n$: This term is used to indicate the relationship between transport processing functional entities and end-user functions.

TC-ON$_n$: This term is used to indicate the relationship between transport control functional entities and other networks, including other NGNs.

TC-T$_n$: This term is used to indicate the relationship between transport control functional entities and transport processing functional entities.

TC-TC$_n$: This term is used to indicate the relationship between the entities of network attachment control function (NACF), resource and admission control functions (RACF) and mobility management and control functions (MMCF). NACF, RACF and MMCF constitute the transport control functions.

TC-U$_n$: This term is used to indicate the relationship between transport control functional entities and end-user functions.

2) In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

3) In this Recommendation, the term "NGN operator" is used to refer to a network operator (as defined in clause 3.1.9) that manages one or more NGN(s). A NGN operator can also be a service provider (as defined in clause 3.1.16). Note also that the term "NGN provider", when used in this Recommendation, is equivalent to the term "NGN operator".

6 General principles of the NGN functional architecture

6.1 General characteristics

The NGN functional architecture incorporates the following principles:

- **Support for multiple access technologies**: The NGN functional architecture is required to offer the configuration flexibility needed to support multiple access technologies.
- **Distributed control**: This will enable adaptation to the distributed processing nature of packet-based networks and support location transparency for distributed computing.
- **Open control**: The network control environment is open to support service creation, service updating, and incorporation of service logic provision by third parties.
- **Independent service provisioning**: The service provisioning process is separated from transport network operation by using the above-mentioned distributed, open control mechanism. This is intended to promote a competitive environment for NGN development in order to speed up the provision of diversified NGN services.
- **Support for services in a converged network**: This is needed to generate flexible, easy-to-use multimedia services, by tapping the technical potential of the converged, fixed-mobile functional architecture of the NGN.

- **Enhanced security and protection**: This is the basic principle of an open architecture. It is imperative to protect the network infrastructure by providing mechanisms for security and survivability in the relevant layers.
- **Functional entity characteristics**: Functional entities incorporate the following principles:
  - Functional entities may not be distributed over multiple physical units but may have multiple instances.
  - Functional entities have no direct relationship with the layered architecture [ITU-T Y.2011]. However, similar entities may be located in different logical layers.

6.2 Connectivity to the NGN

Figure 6-1 shows the different connectivity, direct or indirect (i.e., through another network), that a NGN may support.

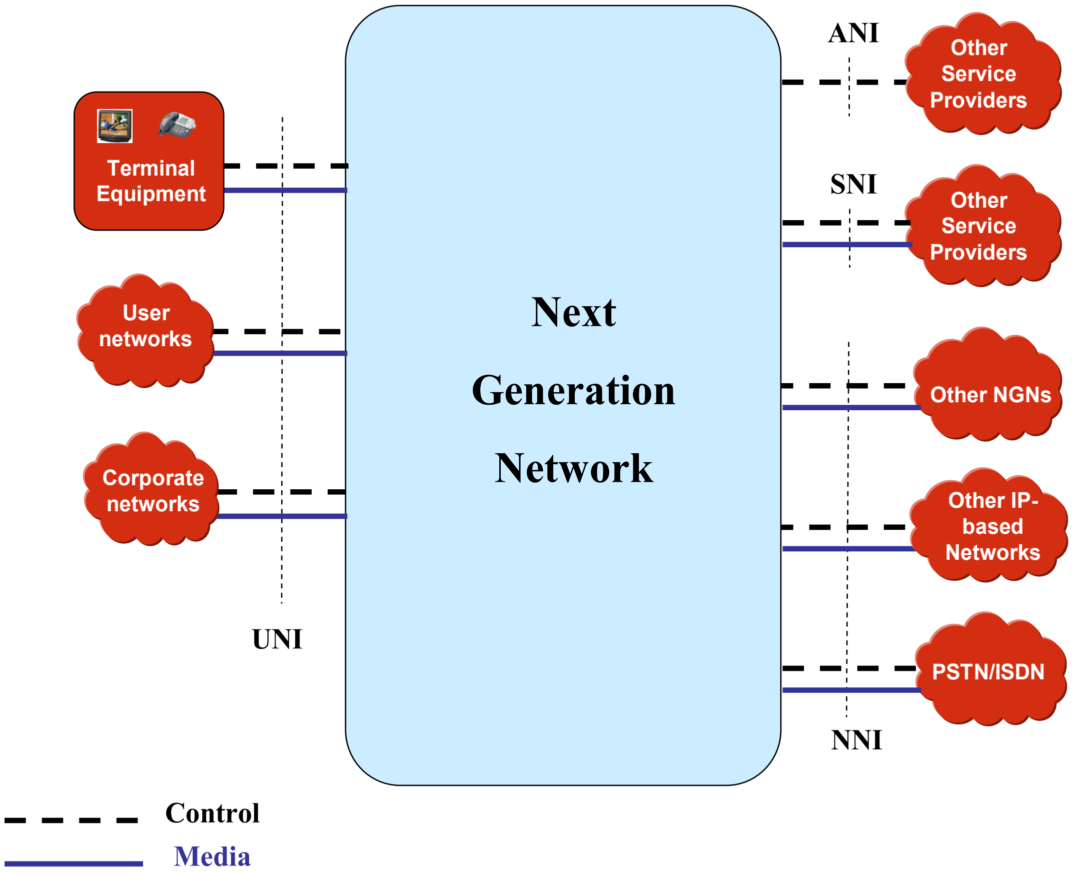


Figure 6-1 – Connectivity to the NGN

The UNI (user-network interface) is used to provide connectivity to:

- terminal equipments;
- user networks;
- corporate networks.

The UNI supports both a control level type of interaction and a media level type of interaction.

The NNI (network-network interface) is used to provide connectivity to:

- other NGNs (at the service stratum and/or transport stratum level);

- other IP-based networks;
- PSTN/ISDN.

The NNI supports both a control level type of interaction and a media level type of interaction.

The ANI (application network interface) is an interface which provides a channel for interactions and exchanges between a NGN and applications. The ANI offers capabilities and resources needed for realization of applications. The ANI supports only a control plane level type of interaction without involving media level (or data plane) interaction. The ANI is used to provide connectivity to other service providers, and their applications, also referred to as application providers in this Recommendation. It has to be noted that a NGN operator can also be an application provider as it may support "in-house" applications.

The SNI (service network interface) is an interface which provides a channel for interactions and exchanges between a NGN and other service providers (such as a content provider [ITU-T Y.1910]). The SNI supports both a control plane level type of interaction and a media level (or data plane) type of interaction.

Appendix III provides additional information regarding the UNI, NNI, ANI and SNI reference points.

7 Overview of the NGN architecture

Along with a new architecture, the next generation network brings an additional level of complexity beyond that of legacy networks. In particular, support for multiple access technologies and mobility results in the need to support a wide variety of network configurations. The specific configurations used in the NGN are not the subject of this Recommendation. Some examples of configurations are provided in Appendices I and II. Such examples serve to provide a context for the functional architecture described in this clause.

The NGN architecture provided in this Recommendation supports the delivery of services identified in the NGN [b-Y.2000-Sup.7], as well as the requirements and capabilities identified in [ITU-T Y.2201]. NGN services include multimedia services, such as conversational services, and content delivery services, such as IPTV services.

An aim of NGN is to support PSTN/ISDN replacement. Therefore, the NGN provides support for PSTN/ISDN emulation as well as PSTN/ISDN simulation.

Figure 7-1 shows an overview of the NGN functional architecture.

The NGN functional architecture supports the UNI, NNI, ANI and SNI reference points as described in clause 6.2.

The NGN functions are divided into service stratum functions and transport stratum functions according to [ITU-T Y.2011]. To provide these services, several functions in both the service stratum and the transport stratum are needed, as illustrated in Figure 7-1.

The delivery of services/applications to the end-user is provided by utilizing the application support functions and service support functions, and related control functions.

The transport stratum provides the IP connectivity services to the NGN users under the control of transport control functions, including the network attachment control functions (NACF), the resource and admission control functions (RACF) and mobility management and control functions (MMCF).

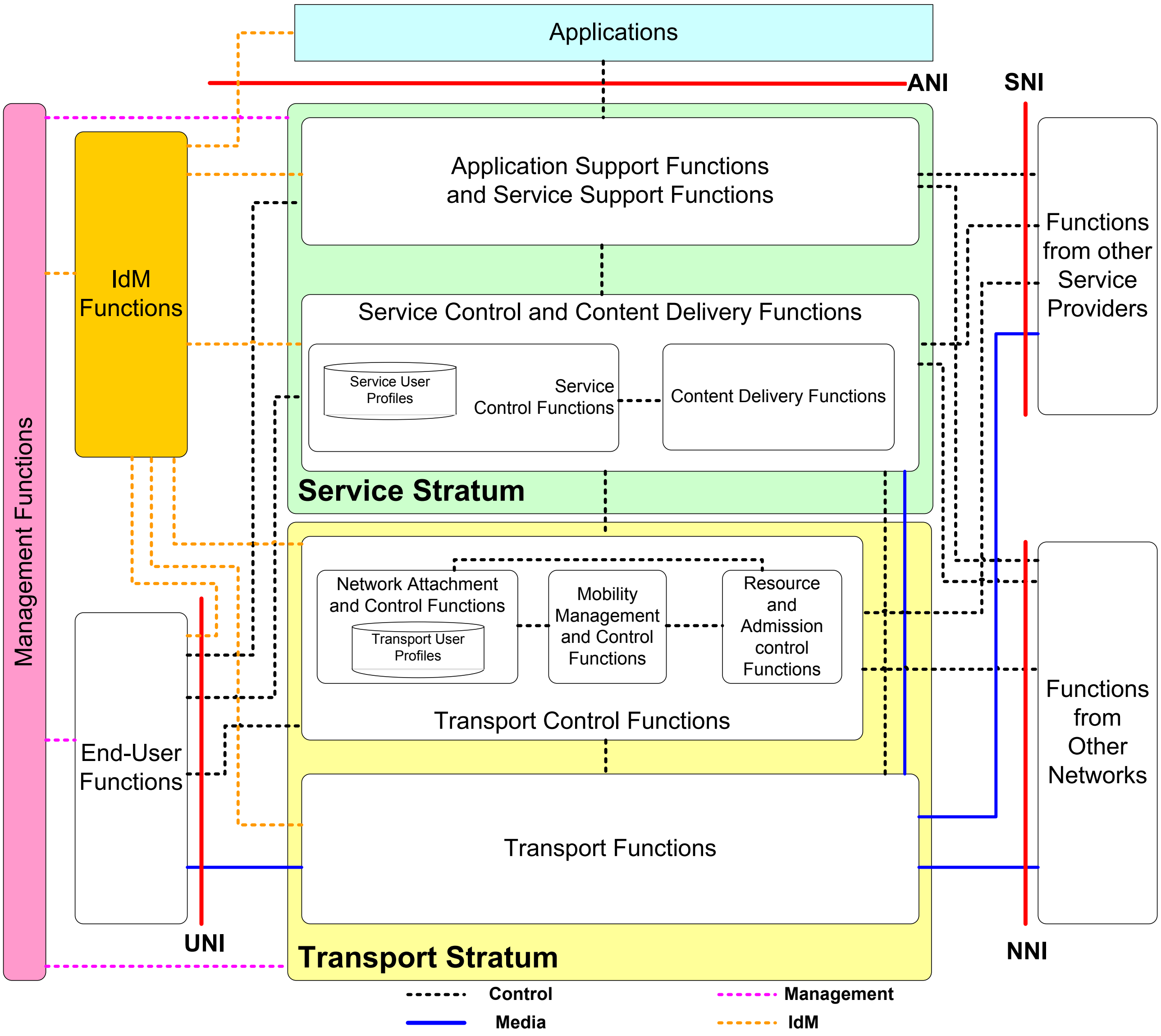

Applications
ANI
SNI
Management Functions
IdM Functions
Application Support Functions and Service Support Functions
Service Control and Content Delivery Functions
Service User Profiles
Service Control Functions
Content Delivery Functions
Service Stratum
Functions from other Service Providers
Network Attachment and Control Functions
Transport User Profiles
Mobility Management and Control Functions
Resource and Admission control Functions
Transport Control Functions
End-User Functions
Transport Functions
Functions from Other Networks
UNI
NNI
Transport Stratum
Control
Management
Media
IdM

Figure 7-1 – NGN architecture overview

NOTE 1 – The user network interface (UNI), the network network interface (NNI), the application network interface (ANI) and the service network interface (SNI) are to be understood as general NGN reference points that can be mapped to specific physical interfaces depending on the particular physical implementations.

NOTE 2 – Boxes in Figure 7-1 identify high-level functional groups, for which overall descriptions are given later in this clause.

NOTE 3 – The control links between the functional groups represent high-level logical interactions.

NOTE 4 – Some functional groups, such as resource and admission control functions (RACF), network attachment control functions (NACF), mobility management and control functions (MMCF), content delivery functions (CDF) and service control functions (SCF), can be distributed and instantiated over different NGN provider domains (e.g., access network, core network). The functional groups in the service stratum and the transport stratum can also be distributed between a visited network and a home network (refer to the NGN terminology [ITU-T Y.2091]). Refer to Appendix I for the details.

NOTE 5 – User profiles in both the service stratum and the transport stratum are shown as separate functional databases. Depending on the business model in place, these two functional databases can optionally be co-located. Note that other functional databases required for the support of NGN services (such as DNS) are not illustrated in Figure 7-1.

NOTE 6 – Since Figure 7-1 is drawn from a high-level conceptual point of view, instantiation of the NGN reference points, namely UNI, NNI, ANI and SNI, is useful to clarify the specific role of these different reference points in terms of service offering and the physical implementation entailed. The instantiation of NGN reference points is given in Appendix III.

NOTE 7 – The NGN-UNI line shows the functional aspect only and should not make any pre-decision about an ownership domain.

NOTE 8 – More precise location and distinction of possible NGN UNIs are for further study.

NOTE 9 – Although this Recommendation assumes that content delivery functions are provided by the NGN, these functions can optionally be provided outside of the NGN.

NOTE 10 – It is possible for IdM functions to reside in different planes (e.g., user, control and management) and different strata of the distributed architecture (e.g., service stratum and transport stratum). Although IdM functions are shown in a standalone group of functions, this is not intended to impose any implementation design and restrictions for IdM.

NOTE 11 – Although IdM functions are shown on the left side of Figure 7-1, this does not mean that IdM functions are located on the UNI side or part of the end-user functions.

NOTE 12 – Although not shown in Figure 7-1, IdM functions can be connected to functions from other service providers using the SNI reference point.

7.1 Transport stratum functions

The transport stratum functions include transport functions and transport control functions, per [ITU-T Y.2011].

7.1.1 Transport functions

The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for unicast and/or multicast transfer of media information, as well as the transfer of control and management information.

Transport functions include access network functions, edge functions, core transport functions, and gateway functions.

NOTE – No assumptions are made about either the technologies to be used or the internal structure, e.g., the core transport network and the access transport network.

7.1.1.1 Access network functions

The access network functions take care of end-users' access to the network as well as collecting and aggregating the traffic coming from these accesses towards the core network. These functions also perform QoS control mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, and shaping. In addition, the access network provides support for mobility.

The access network includes access-technology dependent functions, e.g., for W-CDMA technology and xDSL access. Depending on the technology used for accessing NGN services, the access network includes functions related to:

1) Cable access;

2) xDSL access;

3) Wireless access (e.g., [b-IEEE 802.11] and [b-IEEE 802.16] technologies, and 3G RAN access);

4) Optical access.

7.1.1.2 Edge functions

The edge functions are used for media and traffic processing when aggregated traffic coming from different access networks is merged into the core transport network; they include functions related to support for QoS and traffic control.

The edge functions are also used between core transport networks.

7.1.1.3 Core transport functions

The core transport functions are responsible for ensuring information transport throughout the core network. They provide the means to differentiate the quality of transport in the core network.

These functions provide QoS mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, gate control, and firewall capability.

7.1.1.4 Gateway functions

The gateway functions provide capabilities to interwork with end-user functions and/or other networks, including other types of NGN and many existing networks, such as the PSTN/ISDN, the public Internet, and so forth.

Gateway functions can be controlled either directly from the service control functions (see clause 7.2.1) or through the transport control functions (see clause 7.1.2).

7.1.1.5 Media handling functions

The media handling functions provide specialized media resource processing for service provision, such as generation of tone signals and transcoding. These functions are specific to media resource handling in the transport stratum.

7.1.2 Transport control functions

The transport control functions include resource and admission control functions, network attachment control functions as well as mobility management and control functions.

7.1.2.1 Resource and admission control functions (RACF)

Within the NGN architecture [ITU-T Y.2011], the resource and admission control functions (RACF) act as the arbitrator between service control functions and transport functions for QoS [ITU-T Y.1291]. The decision is based on transport subscription information, SLAs, network policy rules, service priority (e.g., defined by [ITU-T Y.2171]), and transport resource status and utilization information.

The RACF provides an abstract view of transport network infrastructure to service control functions (SCF) and makes service stratum functions agnostic to the details of transport facilities, such as network topology, connectivity, resource utilization and QoS mechanisms/technology, etc. The RACF interacts with the SCF and transport functions for a variety of applications (e.g., SIP-based call, video streaming, etc.) that require the control of NGN transport resource, including QoS control, NAPT and firewall control and NAPT traversal.

The RACF performs the policy-based transport resource control upon the request of the SCF, determines the transport resource availability and admission, and applies controls to the transport functions to enforce the policy decision, including resource reservation, admission control and gate control, NAPT and firewall control, and NAPT traversal. The RACF interacts with transport functions for the purpose of controlling one or more of the following functions in the transport layer: bandwidth reservation and allocation, packet filtering; traffic classification, marking, policing, and priority handling; network address and port translation; and firewall.

The RACF takes into account the capabilities of transport networks and associated transport subscription information for subscribers in support of the transport resource control. Transport subscription information is the responsibility of the network attachment control functions (NACF). The RACF and the NACF interact to exchange relevant transport subscription information and information on the user terminal's point of attachment.

For delivering of those services across multiple service providers and/or network operators, SCF, RACF and transport functions may interact with the corresponding functions in other NGNs.

NOTE – The details and other aspects of the RACF are specified in [ITU-T Y.2111].

7.1.2.2 Network attachment control functions (NACF)

The network attachment control functions (NACF) provide registration at the access level and initialization of end-user functions for accessing NGN services. These functions provide transport stratum level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of NGN functions in the service stratum to the end user.

The NACF provides the following functionalities:

- Dynamic provisioning of IP addresses and other user equipment configuration parameters.
- By endorsement of user, auto-discovery of user equipment capabilities and other parameters.
- Authentication of end user and network at the IP layer (and possibly other layers). Regarding the authentication, mutual authentication between the 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 NACF includes the transport user profile which takes the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

NOTE – The details and other aspects of the NACF are specified in [ITU-T Y.2014].

7.1.2.3 Mobility management and control functions (MMCF)

The mobility management and control functions (MMCF) provide functions for the support of IP-based mobility in the transport stratum. These functions allow the support of mobility of a single device. The MMCF provides mechanisms to achieve seamless mobility if network conditions permit, but does not provide any mechanism to deal with service adaptation if the post-handover quality of service is degraded from the quality of service before handover.

The MMCF assumes that mobility is a service, explicitly specified by parameters in the user service profile. The MMCF is not dependent on specific access technologies, and supports handover across different technologies.

NOTE – The details and other aspects of the MMCF are specified in [ITU-T Y.2018].

7.2 Service stratum functions

This abstract representation of the functional grouping in the service stratum includes:

- the service control and content delivery functions including service user profile functions and,
- the application support functions and service support functions.

7.2.1 Service control and content delivery functions (SC&CDF)

The service control and content delivery functions include service control functions and content delivery functions.

7.2.1.1 Service control functions (SCF)

The service control functions (SCF) include resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services. They can also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level.

Regarding the authentication, mutual authentication between end user and the service is performed.

The service control functions accommodate service user profiles which represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of functional databases. These functional databases may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

7.2.1.2 Content delivery functions (CDF)

The content delivery functions (CDF) receive content from the application support functions and service support functions, store, process, and deliver it to the end-user functions using the capabilities of the transport functions, under control of the service control functions.

7.2.2 Application support functions and service support functions (ASF&SSF)

The application support functions and service support functions (ASF&SSF) include functions such as the gateway, registration, authentication and authorization functions at the application level. These functions are available to the "applications" and "end-user" functional groups. The application support functions and service support functions work in conjunction with the service control functions to provide end users and applications with the NGN services they request.

Through the UNI, the application support functions and service support functions provide reference points to the end-user functions. Application interactions with the application support functions and service support functions are handled through the ANI reference point.

7.3 End-user functions

No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. End-user equipment may be either mobile or fixed.

7.4 Management functions

Support for management is fundamental to the operation of the NGN. These functions provide the capabilities to manage the NGN in order to provide NGN services with the expected quality, security, and reliability.

These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in [ITU-T M.3060].

Management functions apply to the NGN service and transport strata. For each of these strata, they cover the following areas:

a) Fault management;

b) Configuration management;

c) Accounting management;

d) Performance management including what is specified in [ITU-T Y.2173];

e) Security management.

The accounting management functions also include charging and accounting functions (CAF). These interact with each other in the NGN to collect accounting information, in order to provide the NGN operator with appropriate resource utilization data, enabling the NGN operator to properly bill the users of the system.

A detailed description of the CAF functions can be found in clause 8.5.

7.5 Identity management (IdM) functions

7.5.1 Overview

[ITU-T Y.2720] provides a framework for identity management (IdM). IdM functions and capabilities are used to assure the identity information, assure the identity of an entity and support business and security applications (e.g., access control and authorization) including identity-based services. An entity is considered to be anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices.

In the NGN environment, a single entity may be associated with multiple types of identity information which can be grouped as follows:

– Identifiers, e.g., UserID, email addresses, telephone numbers, URI and IP addresses;

– Credentials, e.g., digital certificates, tokens and biometrics;

– Attributes, e.g., roles, claims, privileges, patterns and location.

IdM is a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

– assurance of identity information,

– assurance of the identity of an entity, and

– enabling and supporting business and security applications.

IdM services and capabilities also allow users/subscriber entities to control how their identity information is stored, used and disseminated. IdM also allows federated identity information to be shared and used by members of a federation (e.g., business partners) to support federated services (e.g., single sign-on and sign-off services).

7.5.2 IdM framework

[ITU-T Y.2720] provides a framework for IdM summarized as follows:

– Identity lifecycle management;

– Identity management (IdM) operation, administration, maintenance and provisioning (OAMP) functions;

– Identity management (IdM) signalling and control functions;

– Identity management (IdM) federated identity functions;

– Identity management (IdM) user and subscriber functions;

– Identity management (IdM) performance, reliability, and scalability;

– Identity management (IdM) security;

– Identity management (IdM) legal and regulatory rules;

NOTE – Legal and regulatory regulations are not within the scope of [ITU-T Y.2720] and this Recommendation. It is mentioned here only for completeness.

7.5.3 Architectural model

In the context of the NGN reference architecture model, it is possible for IdM related functions to reside in the different planes (e.g., user, control and management) and different strata of the distributed architecture (e.g., service stratum and transport stratum). From a realization or implementation perspective, support of IdM services and capabilities could involve the use of existing network elements or it could involve the use of additional network elements (e.g., specialized application servers) in a NGN.

Figure 7-1 illustrates the general concepts that the support of IdM services and capabilities may involve interaction with specific functional entities (FEs) to enable and support applications and services including identity services. This may include interactions with FEs in the following functional blocks, depending on the specific IdM service or capability being supported and the implementation design:

– applications;

– service stratum: application support functions and service support functions, service control functions and content delivery functions;

– transport stratum: transport control functions and transport functions;

– end-user functions;

– management functions.

8 NGN concepts

8.1 Mobility levels in the NGN architecture

The NGN architecture supports the capability to provide mobility within and between its various access network types and mobility technologies. This mobility may be supported at various levels in the NGN architecture. MMCF provides support for IP-based mobility in the transport stratum. Mobility in the service stratum is for further study.

Details are given in mobility management requirements for NGN [ITU-T Q.1706], while details of the functional architecture for MMCF are provided in [ITU-T Y.2018].

8.2 NGN service architecture

The service aspect of the NGN architecture, as shown in Figure 7-1, consists of three distinct functional areas:

a) "Applications";

b) "Application support functions and service support functions" in the service stratum of the NGN;

c) NGN resources and capabilities, including those in the transport stratum, capabilities such as presence, location information, charging function, security schemes, etc.

The "applications" functional area consists of two categories: those trusted by NGN operators, and those that are not. The former consists of applications provided by the NGN operators themselves and subordinate organizations or partners, while the latter may consist of applications provided by other independent service providers (also referred to as application providers), whose access to southbound resources is required to be authenticated, controlled and filtered by the functions in the service enablers.

As shown in Figure 7-1, through the ANI, the functional area of "application support functions and service support functions" offers service-enabling resources to the "applications" area, independently of the underlying network technologies. Through the ANI, the "applications" area benefits from the capabilities and resources of the "NGN infrastructure" functional area.

Specifically, the NGN service architecture has the following three main functional characteristics:

a) Agnosticism: application support and service support functions areas consist of functions that are agnostic with respect to their underlying NGN infrastructure.

b) Support for legacy capabilities and features: there are no limiting impacts on the NGN as a result of this NGN service architecture. On the contrary, the use of NGN capabilities such as session management, authentication, location information, charging is supported. For example, the legacy-IN-influenced features of the IMS, such as triggers, filter criteria, and the service capability interaction manager, are available through the abstraction of the IMS AS (application server) in the "application support functions and service support functions" area.

c) Support for open service interface: The NGN service platform is recommended to provide an open service interface, which provides an abstract of the network capabilities (i.e., the interface is network agnostic). This interface is recommended to provide access to such functions as authentication, authorization, and security to ensure that other service providers can make use of the network capabilities.

Based upon these main characteristics, [ITU-T Y.2234] further specifies functional requirements of the NGN open service environment (OSE) capabilities, as well as a service architecture for the support of the OSE in the NGN.

8.3 Network topology hiding functions and NAPT traversal functions

8.3.1 Service stratum topology hiding

Service stratum topology hiding is achieved by removing or modifying any topological information carried in application signalling packets to the peering network.

NOTE – For example, in SIP-based applications, topology information is present in SIP headers, like the via and Record Route headers.

8.3.2 Transport stratum topology hiding

Transport stratum topology hiding is achieved by modifying any topological information in media packets, or by blocking network control packets including any topological information.

Examples of transport stratum topology hiding are as follows:

- Change the IP addresses and/or port numbers of media packets that pass through the border between access and core transport network and/or the border between two core transport networks.
- Block the network control packet at the border of access/core transport networks, such as STP, ICMP and routing protocol.

8.3.3 Remote NAPT traversal

The network address and port translation (NAPT) traversal copes with the traversal of the far-end (remote) NAPT in access networks. The owner of the far-end NAPT is different from the owner of the service control functional entities (e.g., P-CSC-FE), i.e., the far-end NAPT cannot be controlled by the NAPT application level gateway (ALG) or other service control functional entities affiliated with the NGN operator domain.

8.4 Overload control

To defend session control functional entities such as S-CSC-FE, against the concentration of malicious or unexpected requests, the following functions are necessary at each boundary between access and/or core networks:

- Detection of the concentration of requests to an S-CSC-FE at each FE;
- Detection of the concentration of requests to an S-CSC-FE by gathering information from two or more FEs;
- Transmission of the detected information on the concentration of requests to other FEs;
- Traffic control according to the information on the concentration of requests.

More globally, the NGN architecture is required to allow for functions and mechanisms available to control overload that:

- automatically maximize effective throughput (i.e., admitted service requests/s) at an overloaded resource;
- achieve this throughout the duration of an overload event, and irrespective of the overloaded resource's capacity or of the number of sources of overload;
- are configurable so that, under processing overload, a high proportion of response times at overloaded resources are low enough so as not to cause customers to prematurely abandon service requests;
- are recommended to be applied within a NGN and between NGNs;
- are recommended to be applied within an NGN component (e.g., IP multimedia service component, PSTN/ISDN emulation service component, see clause 9) and between different NGN components.

NOTE – As a general rule, a NGN's call, session and command processing resources can experience prolonged processing overload under the appropriate circumstances (e.g., partial, or full, server failure, high rates of incoming service requests). Consequently, it needs to be equipped with some form of overload detection and control (including expansive controls such as load balancing and resource replication), in order to keep response times just low enough under such processing overload to preclude customers abandoning their service requests prematurely.

8.5 Charging and accounting functions (CAF)

The charging and accounting functions (CAF) are meant to represent a generalized architecture to support an NGN provider's need to collect and process information, such that customers can be charged for the services provided.

The CAF provide accounting data to the NGN provider regarding the utilization of resources in the network. They support the collection of data for later processing (offline charging), as well as near-real-time interactions with applications, such as for pre-paid services (online charging).

The CAF include a charging trigger function (CTF), an online charging function (OCF), a charging collection function (CCF), a rating function (RF), an account balance management function (ABMF), a charging gateway function (CGF) and an inter-provider charging gateway function (IPCGF).

Figure 8-1 shows a high-level view of the CAF.

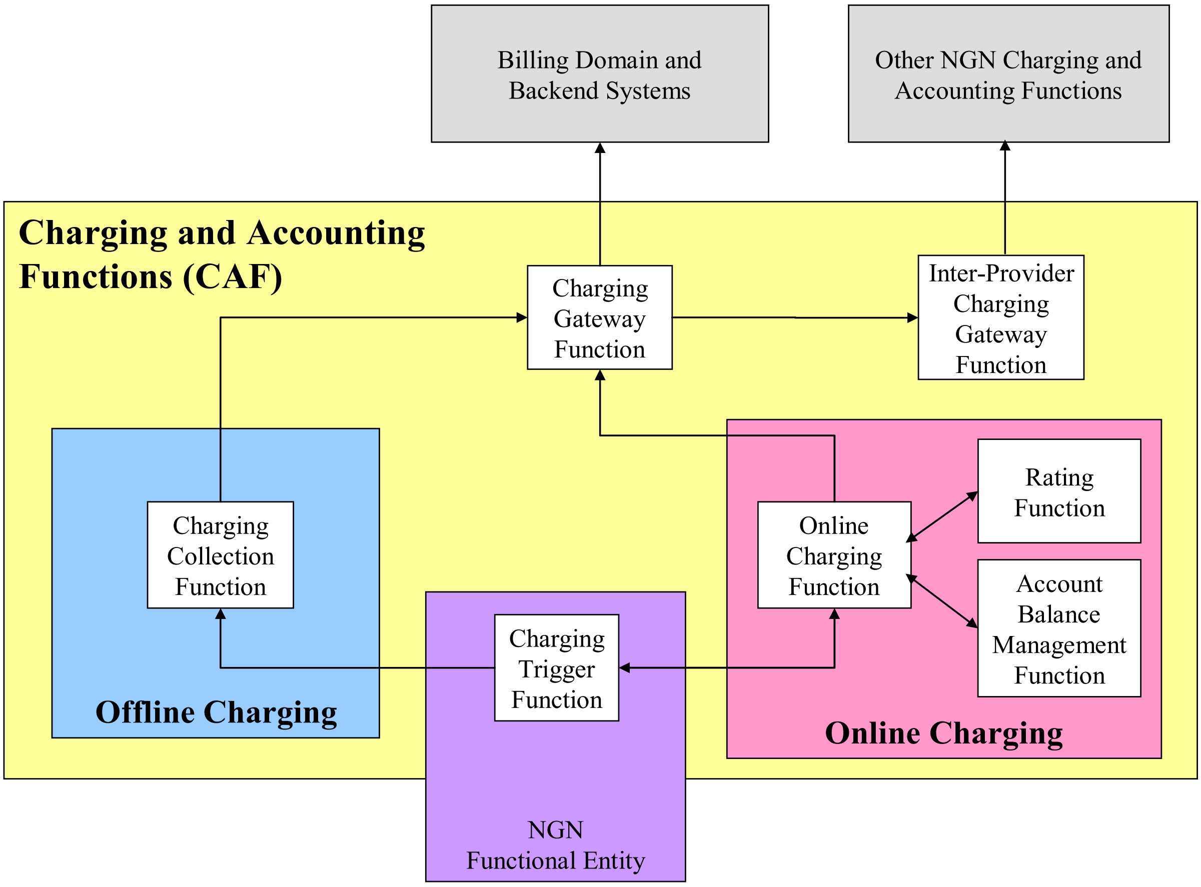

Billing Domain and Backend Systems
Other NGN Charging and Accounting Functions
Charging and Accounting Functions (CAF)
Charging Gateway Function
Inter-Provider Charging Gateway Function
Charging Collection Function
Offline Charging
Online Charging Function
Rating Function
Account Balance Management Function
Online Charging
Charging Trigger Function
NGN Functional Entity

Figure 8-1 – Charging and accounting functions

The following provides a description of the charging and accounting functions shown in Figure 8-1. For further details regarding the CAF functional architecture, related functions and corresponding reference points, please refer to [ITU-T Y.2233].

8.5.1 Charging trigger function (CTF)

The CTF generates charging events based on the observation of network resource usage. In every network and service element that provides charging information, the CTF is the focal point for collecting information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events to the charging collection function. The CTF is therefore a necessary component in all network elements that provide offline-charging functionality.

The CTF also creates the charging events used for online charging. The charging events are forwarded to the online charging function (OCF), in order to obtain authorization for the chargeable event or network resource usage requested by the user. It must be possible to delay the actual resource usage until permission has been granted by the OCF. The CTF must be able to track the availability of the resource usage permissions (i.e., quota supervision) during the network resource usage. It must also be able to enforce termination of the end user's network resource usage, when permission by the OCF is not granted or expires.

NOTE – The specific entities that contain charging trigger functionality are not defined in this Recommendation.

8.5.2 Charging collection function (CCF)

The CCF receives charging events from the CTF. It then uses the information contained in the charging events to construct charging information records (CIRs). The results of the CCF tasks are CIRs with well-defined content and format. The CIRs are later transferred to the billing domain.

8.5.3 Online charging function (OCF)

The OCF receives charging events from the CTF and executes them in near real time to provide authorization for the chargeable event or network resource usage requested by the user. The CTF must be able to delay the actual resource usage until permission has been granted by the OCF. The OCF provides a quota for resource usage, which must be tracked by the CTF. Subsequent interactions may result in an additional quota being provided according to the subscriber's account balance, or they may result in no additional quota being provided, in which case the CTF must enforce termination of the end user's network resource usage.

The OCF allows more than one user to share the same subscriber's account simultaneously. The OCF responds to the charging requests from various users at the same time and provides a certain quota to each user. The quota is determined by default or by certain policies. Users can resend requests for larger quotas during the same session. The maximum available quota, however, will not exceed the subscriber's account balance.

8.5.4 Rating function (RF)

The RF works with the online charging module. The RF determines the value of the network resource usage (described in the charging event received by the OCF from the network) on behalf of the OCF. To this end, the OCF furnishes the necessary information to the RF and receives the rating output.

8.5.5 Account balance management function (ABMF)

The ABMF stores the subscriber's account balance within the online charging system.

The subscriber's account balance could be represented by the remaining available traffic volume (e.g., bytes), time (e.g., minutes for calling), or content (e.g., a movie), as well as money.

Security and robustness should be emphasized by encrypting key data, providing backup and failure alarm capabilities, keeping detailed logs, and so forth.

8.5.6 Charging gateway function (CGF)

The CGF plays a gateway role between the NGN network and the billing domain or another NGN CGF. The CGF performs validation, consolidation, correlation, formatting, and error handling of CIRs. It also performs lifecycle management for CIR file creation, modification, and deletion.

When applicable, the CGF selects CIRs for inter-provider charging settlement per NGN provider and transfers them to the inter-provider charging gateway function (IPCGF).

8.5.7 Inter-provider charging gateway function (IPCGF)

The IPCGF constructs and transfers CIRs for inter-provider charging settlement. It determines the type of CIR (duration-based, volume-based, event-based, etc.) depending on the settlement policy between the involved NGN providers.

The IPCGF allows NGN providers to exchange CIRs in real-time over standardized interfaces.

9 Generalized NGN functional architecture

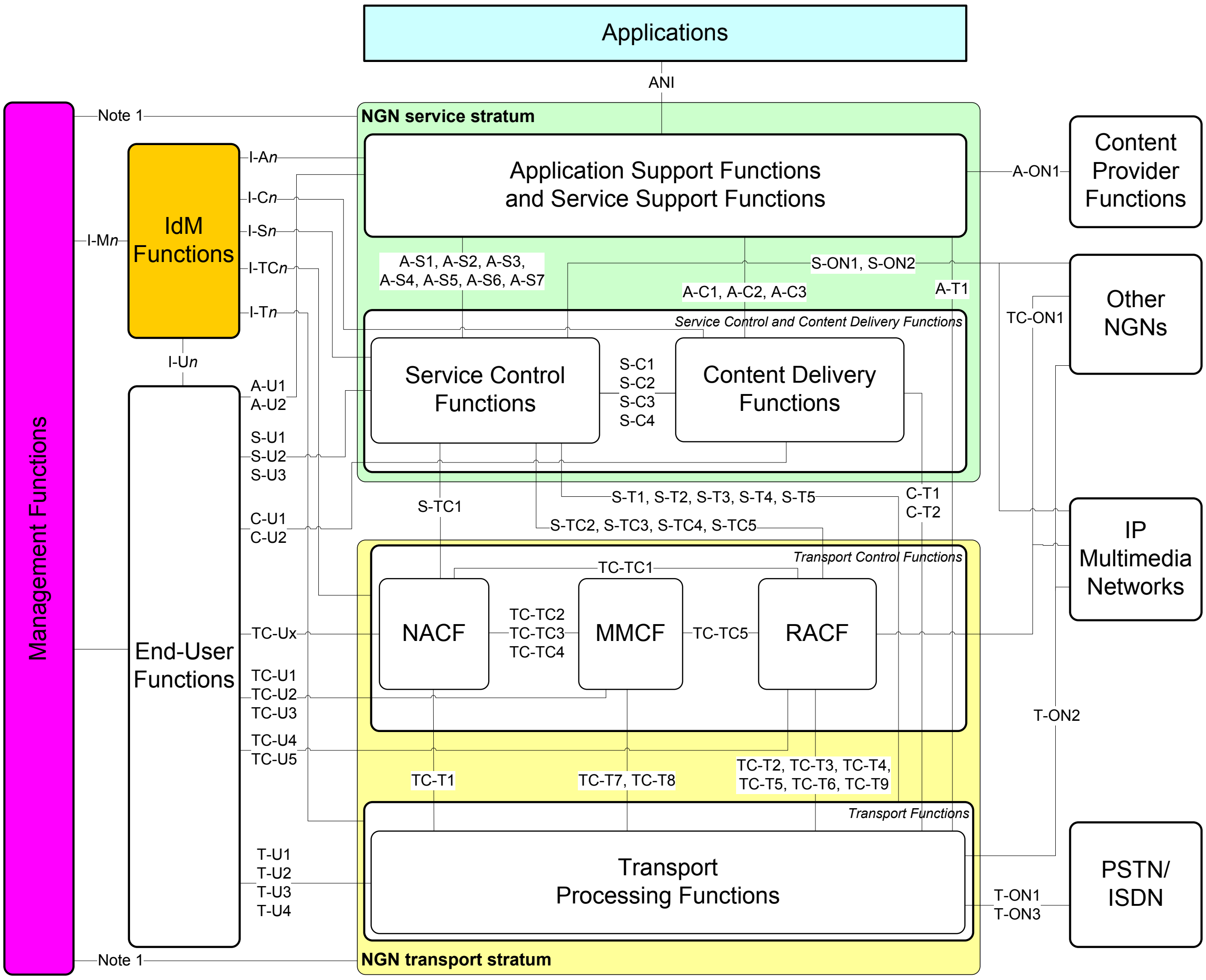
This clause describes the generalized functional architecture for the NGN, including the definitions of the generalized functional entities. This architecture is a general service- and technology-independent architecture that can be later instantiated in customized architectures that can respond to specific contexts in terms of the services offered and the technologies used.

9.1 NGN functional architecture framework

The NGN functional architecture framework shown in Figure 9-1 is based on the NGN architecture overview provided in clause 7. In particular, the functional groups identified in Figure 7-1 are used to structure the general layout of Figure 9-1. The functional groups shown in Figure 9-1 are groups of NGN functional entities which are further described in clause 9.3. Figure 9-1 also identifies NGN reference points between these functional groups, reference points which are also described later in this Recommendation.

As already mentioned in clause 7, the NGN architecture and, as a consequence, the generalized functional architecture described in this clause, are expected to provide functionality for all envisaged services over packet-based networks. More specifically, the NGN architecture described in this Recommendation is consistent with [b-ITU-T Y.2000-Sup.1] and [b-ITU-T Y.2000-Sup.7] that outline the scope of NGN and provides general support for the requirements and capabilities of the NGN identified in [ITU-T Y.2201].

In this sense, in line with the [ITU-T Y.2011] principles, most of the NGN transport stratum functions (such as RACF or NACF) are able to support different types of NGN services in a common way. NGN implementations do not, however, have to implement certain transport stratum functions, such as gateway functions with respect to PSTN/ISDN or MMCF functions with respect to mobility, if they do not require support for such capabilities.



NOTE 1 – This link corresponds to the multiple reference points that may exist between the management functions and the corresponding NGN stratum.

Figure 9-1 – NGN functional architecture framework

9.2 NGN functional entities (FEs)

In general, a FE is characterized by functions identified as sufficiently unique with respect to other FEs. In the case of the generalized NGN architecture, the functional entities, called NGN FEs, are to be understood as generic FEs to allow for their possible instantiation in more specific technology-oriented contexts. It is therefore possible that when NGN FEs are instantiated, they can be used and can behave in a slightly different manner depending on the context. For example, this may lead to the case where, at a given reference point (between the same NGN FEs), the interface and the associated protocols are different depending on the instantiation. This means that interfaces, as well as protocol descriptions, can only be provided on the basis of a specific instantiation of the generalized functional architecture.

In the NGN functional architecture, a given FE in a given NGN stratum is not necessarily constrained to a given layer in that stratum. For example, an FE in the NGN transport stratum may support functions involving different layers such as IP, TCP/UDP or transport layers used below the IP layer.

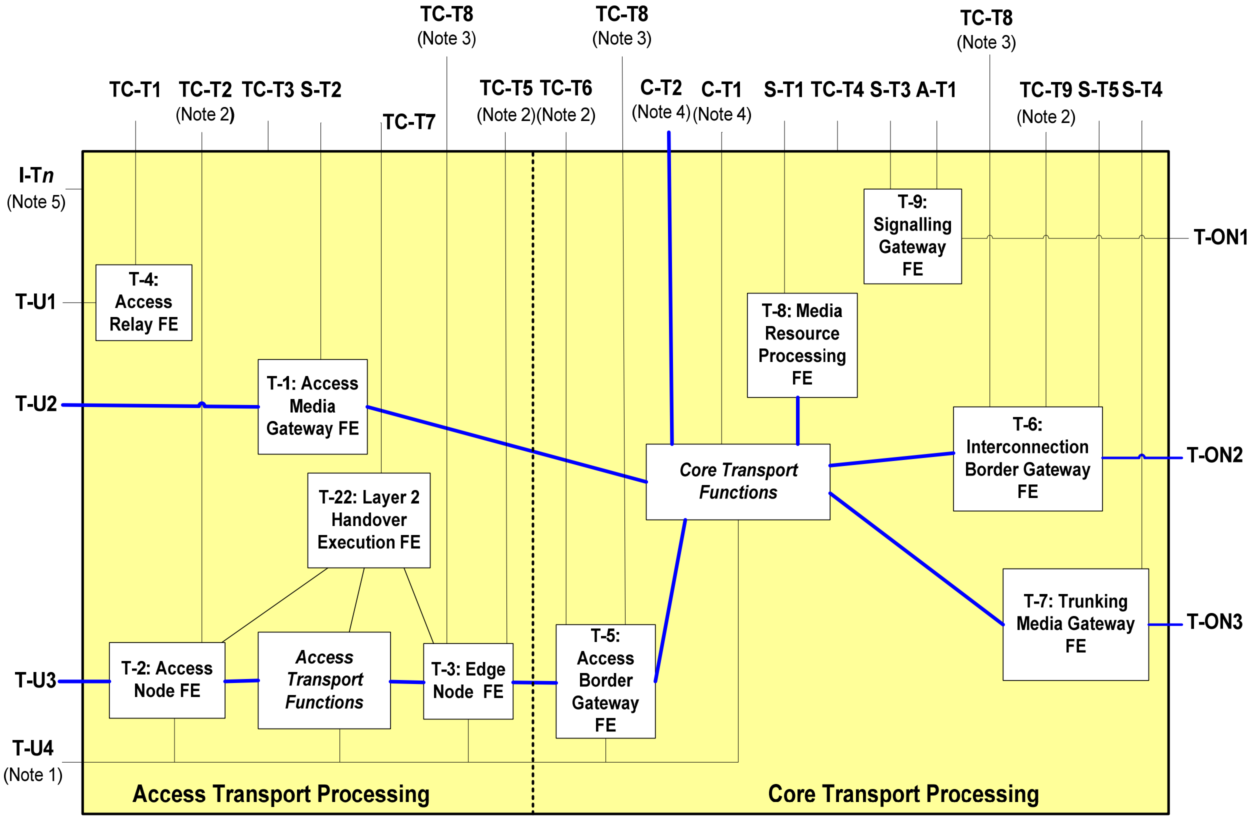
9.3 Functional entity descriptions

This clause provides a description of the NGN functional entities (FEs). The functional entities described are:

- Transport processing functional entities (covering access and core);
- Transport control functional entities;
- Service control and content delivery functional entities;
- Functional entities within the application support functions and service support functions;
- Functional entities within end-user functions;
- Functional entities within IdM functions.

9.3.1 Transport processing functional entities

Figure 9-2 shows the transport processing FEs. Since the generalized NGN functional architecture described in this Recommendation has a much broader sense, in particular, at the transport functions, distinction of access and core aspects is applied in Figure 9-2 regarding transport processing functional entities.



NOTE 1 – T-U4 is a reference point between end-user functions and the transport processing functions that is used for multicast control. Depending on the network configuration, the T-U4 reference point can terminate in either the AN-FE, or the EN-FE, or the ABG-FE or within the access or core transport functions. The entity terminating the T-U4 reference point includes EC-FE and EF-FE that are multicast capable, i.e., the EC-FE includes a multicast control point function (see [ITU-T Y.2017]), while the EF-FE includes a multicast replication function (see [ITU-T Y.2017]).

NOTE 2 – When used, the entity terminating the corresponding reference point includes a PE-FE.

NOTE 3 – When used, the entity terminating the corresponding reference point includes a Layer 3 handover execution function (L3HEF) as per [ITU-T Y.2018].

NOTE 4 – Although not shown in Figure 9-2 and depending on the network configuration, both C-T1 and C-T2 reference points can be connected to the access transport functions instead of the core transport functions.

NOTE 5 – This is to be understood as referring to the different I-T*n* reference points that may exist between IdM functions and relevant transport functional entities (see clause 9.3.7 for further information).

Figure 9-2 – Transport processing FEs

NOTE – Although the scope of this Recommendation is targeted primarily at a NGN architecture, it is clear that the accommodation of legacy PSTN/ISDN terminals and/or interworking with the PSTN/ISDN is an important consideration with respect to NGN deployment. Thus, to provide a more comprehensive view, AMG-FE required to accommodate PSTN/ISDN terminals is shown, even though it is not strictly part of the NGN architecture itself.

9.3.1.1 T-1: Access media gateway functional entity (AMG-FE)

The access media gateway functional entity (AMG-FE) provides interworking between the packet-based transport used in the NGN and analogue lines or ISDN access.

1) It provides bidirectional media processing functions for user plane traffic between PSTN/ISDN and the NGN under the control of the AGC-FE (see clause 9.3.3.1.8).
2) It provides adequate transfer functions for PSTN/ISDN user call control signalling to the AGC-FE for processing.
3) It optionally supports payload processing functions (e.g., codecs and echo cancellers).
4) It optionally provides the TDM/IP interworking function (refer to [ITU-T Y.1453]) to support ISDN emulation service in cases where an ISDN unrestricted bearer is needed.

9.3.1.2 T-2: Access node functional entity (AN-FE)

The access node functional entity (AN-FE) in IP access network directly connects to end-user functions and terminates the first/last mile link signals at the network side. Generally, it is a layer 2 device that can optionally be IP capable.

As one key injection node for support of dynamic QoS control, the AN-FE may perform packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the RACF.

When the AN-FE is IP capable, it is required to support the functions of elementary control functional entity (EC-FE) and elementary forwarding functional entity (EF-FE). In addition, it is recommended to support the functions of policy enforcement functional entity (PE-FE) and the transport resource enforcement functional entity (TRE-FE), which are controlled by the RACF as defined in [ITU-T Y.2111].

9.3.1.3 T-3: Edge node functional entity (EN-FE)

The edge node functional entity (EN-FE) in the access packet transport functions connects to core packet transport functions and terminates the layer 2 access session with the end-user functions. In case of connection to IP-based core transport functions, it is required to be a layer 3 device with IP forwarding capabilities.

The EN-FE performs QoS mechanisms dealing with the user traffic directly, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, and forwarding.

As one key injection node for support of dynamic QoS control, the EN-FE performs packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the RACF.

Since the EN-FE is IP capable, it is required to support the functions of elementary control functional entity (EC-FE) and elementary forwarding functional entity (EF-FE). It is recommended to support the policy enforcement functional entity (PE-FE) and the transport resource enforcement functional entity (TRE-FE), which are controlled by the RACF as defined in [ITU-T Y.2111].

In addition to the functions listed above, a layer 3 handover execution function (L3HEF) [ITU-T Y.2018] can optionally be embedded in the EN-FE for support of mobility.

9.3.1.4 T-4: Access relay functional entity (AR-FE)

The access relay functional entity (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 can optionally insert local configuration information.

NOTE 1 – When using PPP [b-IETF RFC 1661], the AR-FE can optionally act as a PPPoE relay. When using DHCP [b-IETF RFC 2131], the AR-FE acts as a DHCP relay agent.

NOTE 2 – For example, when using DHCP, the AR-FE acts as a DHCP relay agent and can optionally add information before forwarding a message, e.g., insertion of the identifier of the ATM virtual channel carrying IP traffic in a DHCP request.

9.3.1.5 T-5: Access border gateway functional entity (ABG-FE)

The access border gateway functional entity (ABG-FE) is a packet gateway between an access network and a core transport network used to mask a service provider's network from access networks, through which end-user functions are accessing packet-based services.

The functions of the ABG-FE include opening and closing gate, packet-filtering-based firewall, traffic classification and marking, traffic policing and shaping, network address and port translation, media relay (i.e., media latching) for NAPT traversal, and collecting and reporting resource usage information (e.g., start-time, end-time, octets of sent data).

As one key injection node for support of dynamic QoS control, NAPT/FW control and NAPT traversal, the ABG-FE is required to support the functions of PE-FE and TRE-FE which are controlled by the RACF as defined in [ITU-T Y.2111]. In addition, it is recommended to support the functions of elementary control functional entity (EC-FE) and elementary forwarding functional entity (EF-FE).

The ABG-FE can optionally support IPv4/IPv6 conversion.

In addition to the functions listed above, a layer 3 handover execution function (L3HEF) [ITU-T Y.2018] can optionally be embedded in the ABG-FE for support of mobility.

9.3.1.6 T-6: Interconnection border gateway functional entity (IBG-FE)

The interconnection border gateway functional entity (IBG-FE) is a packet gateway used to interconnect the core transport network of a NGN operator with that of another NGN operator. There may be one or multiple IBG-FEs in a core transport network.

The functions of the IBG-FE may be the same as that of the ABG-FE.

As one key injection node for support of dynamic QoS control, NAPT/FW control, the IBG-FE is required to support the functions of PE-FE (except for remote NAPT traversal) and TRE-FE which are controlled by the RACF as defined in [ITU-T Y.2111]. In addition, the IBG-FE is recommended to support the functions of elementary control functional entity (EC-FE) and elementary forwarding functional entity (EF-FE).

Alternative means of control, such as direct control by IBC-FE, need further study.

In addition, the IBG-FE can optionally support the following functions:

a) Media conversion (e.g., ITU-T G.711 and ITU-T T.38, ITU-T G.711 and AMR);

b) Inter-domain IPv4/IPv6 conversion;

c) Media encryption;

d) Fax/modem processing.

NOTE – Allocation of the above functions to the IBG-FE needs further study: the IBG-FE can optionally perform media conversion under the control of the IBC-FE. The direct link between the IBG-FE and the IBC-FE is for further study.

In addition to the functions listed above, a layer 3 handover execution function (L3HEF) [ITU-T Y.2018] can optionally be embedded in the IBG-FE for support of mobility.

9.3.1.7 T-7: Trunking media gateway functional entity (TMG-FE)

The trunking media gateway functional entity (TMG-FE) provides interworking between the packet-based transport used in the NGN and trunk lines from the circuit-switched network. It is under the control of the MGC-FE.

a) It can optionally support payload processing (e.g., codecs, echo cancellers, and conference bridges).

b) It can optionally provide the TDM/IP interworking function (refer to [ITU-T Y.1453]), in order to support the ISDN emulation service in case ISDN unrestricted bearer is needed.

9.3.1.8 T-8: Media resource processing functional entity (MRP-FE)

The media resource processing functional entity (MRP-FE) provides payload processing of packets used in the NGN.

a) It allocates specialized resources (such as announcement server, notification tone, and voice recognition resources, and voice menu and conference resources).

b) It provides media mixing functions under the control of the MRC-FE.

c) It receives and generates DTMF signals.

d) It generates tone signals (e.g., ring back).

e) It generates announcements.

f) It provides trans-coding, text-to-speech, video mixing, conference bridge, data conference, fax, voice and video recording, and voice recognition capabilities.

9.3.1.9 T-9: Signalling gateway functional entity (SG-FE)

The signalling gateway functional entity (SG-FE) is responsible for signalling transport interworking between the NGN and the existing networks, such as PSTN, ISDN, IN networks and signalling system No. 7.

9.3.1.10 Policy enforcement functional entity (PE-FE)

The policy enforcement functional entity (PE-FE) in the transport stratum enforces the network policy rules instructed by the PD-FE on a per-subscriber and per-IP flow basis. The PE-FE is typically included in packet-to-packet gateways at the boundary of different packet networks and/or between the CPE and the access network. It is the key injection node to enforce dynamic QoS and resource control, NAPT control and NAT traversal.

For further details, refer to [ITU-T Y.2111].

9.3.1.11 Transport resource enforcement functional entity (TRE-FE)

The transport resource enforcement functional entity (TRE-FE) in the transport stratum enforces the transport resource policy rules instructed by the TRC-FE at the technology-dependent aggregate level.

For further details, refer to [ITU-T Y.2111].

9.3.1.12 Elementary forwarding functional entity (EF-FE)

An elementary forwarding functional entity (EF-FE) forwards traffic data received on one flow point "In-FP" (flow point is used here similar to [ITU-T G.8010]) to one flow point "Out-FP" or optionally more flow point(s) "Out-FP(i)", i = 0..n of a transport element; where "In-FP" is not contained within the set of "Out-FP(i), i = 0..n". Consequently, for a unicast type of operation, there is exactly one Out-FP (i.e., i = 1), while for multicast type of operation, the set of "Out-FP(i)" can contain any number of flow points (including the case where "Out-FP(i)" equals the empty set). In the latter case, the EF-FE supports the multicast replication function (see [ITU-T Y.2017]).

9.3.1.13 Elementary control functional entity (EC-FE)

An elementary control functional entity (EC-FE) processes control protocol data (e.g., routing protocol data) for unicast, as well as multicast, data received on one flow point. As a result of this processing, the EC-FE might decide to:

a) send control protocol data (including events to trigger policy evaluation) to another EC-FE;

b) interact with one or more instances of EF-FE to establish new or modify existing forwarding behaviour of the EF-FE;

c) interact with one or more instances of TRE-FE and/or PE-FE. This includes the ability to create events to trigger policy evaluation in TRE-FE and/or PE-FE.

The EC-FE may also receive requests from PE-FE and/or TRE-FE to perform policy enforcement (e.g., trigger transport control protocol actions) and reply back to PE-FE and/or TRE-FE, indicating the result of the requested operation.

In case of multicast control, the EC-FE provides the multicast control point function [ITU-T Y.2017].

9.3.1.14 T-22: Layer 2 handover execution functional entity (L2HE-FE)

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

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

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

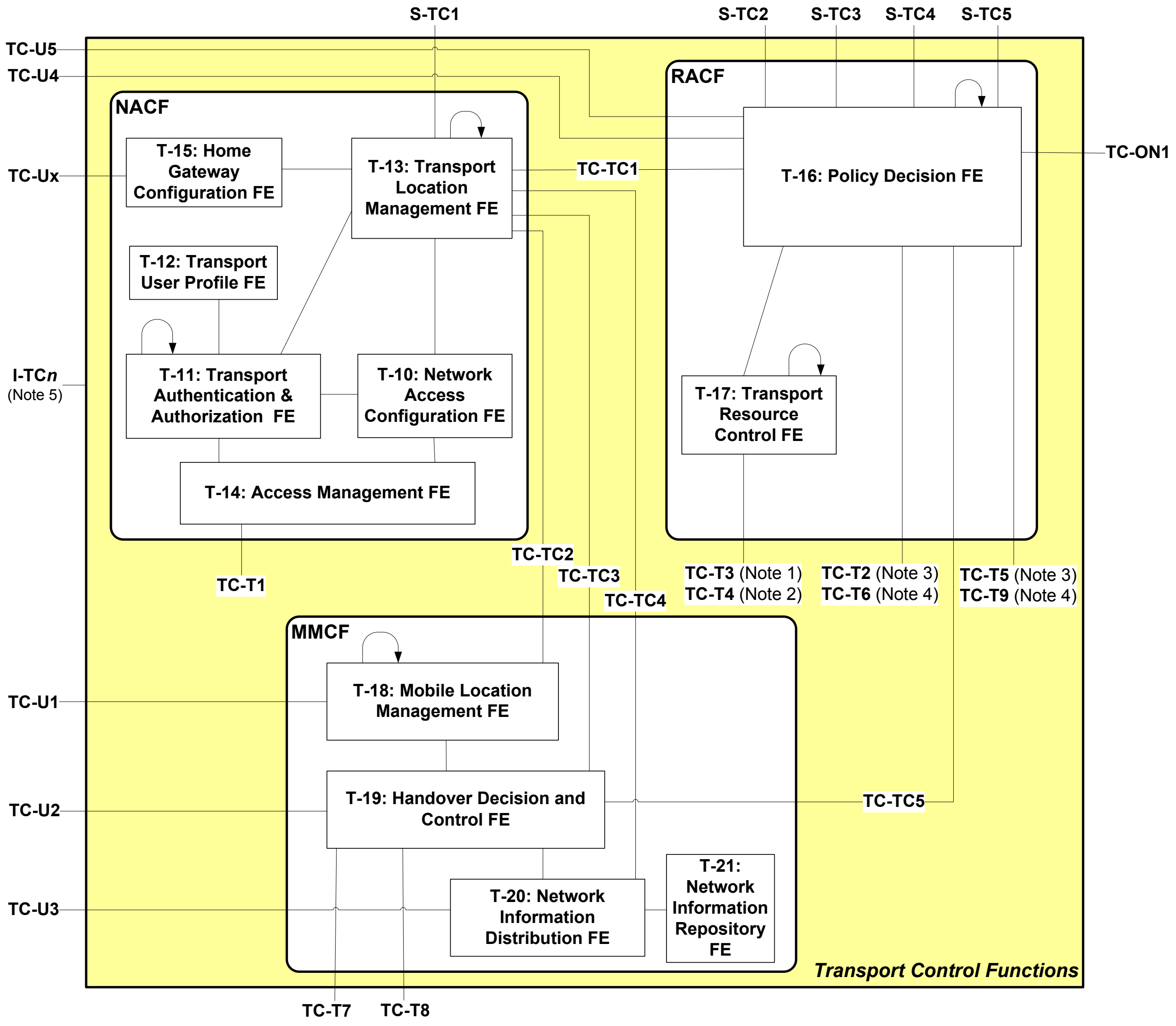
For further details, refer to [ITU-T Y.2018].

9.3.2 Transport control functional entities

Figure 9-3 shows the functional entities related to transport control.

Given that RACF [ITU-T Y.2111] does not make explicit distinction between access and core, the control of access and core transport processing entities described in clause 9.3.1 by RACF may vary.

At least one PD-FE is required to be deployed in each network administrative domain (e.g., access network domain and/or core network domain) with associated PE-FEs and TRC-FEs. Depending on the business model and the implementation choices, the RACF may be present in an access network domain or core network domain, or may be present in both access and core network domains. The implementation and physical configuration of the PD-FE and the TRC-FE are therefore flexible; they can be distributed or centralized, and may be a stand-alone device or part of an integrated device. Appendix I of [ITU-T Y.2111] depicts some implementation examples.


S-TC1
S-TC2
S-TC3
S-TC4
S-TC5
TC-U5
TC-U4
NACF
RACF
TC-Ux
T-15: Home Gateway Configuration FE
T-13: Transport Location Management FE
TC-TC1
T-16: Policy Decision FE
TC-ON1
T-12: Transport User Profile FE
I-TCn (Note 5)
T-11: Transport Authentication & Authorization FE
T-10: Network Access Configuration FE
T-17: Transport Resource Control FE
T-14: Access Management FE
TC-TC2
TC-TC3
TC-TC4
TC-T1
TC-T3 (Note 1)
TC-T4 (Note 2)
TC-T2 (Note 3)
TC-T6 (Note 4)
TC-T5 (Note 3)
TC-T9 (Note 4)
MMCF
T-18: Mobile Location Management FE
TC-U1
TC-U2
T-19: Handover Decision and Control FE
TC-TC5
TC-U3
T-20: Network Information Distribution FE
T-21: Network Information Repository FE
Transport Control Functions
TC-T7
TC-T8

NOTE 1 – This reference point is applicable when TRC-FE operates in the access network domain.
NOTE 2 – This reference point is applicable when TRC-FE operates in the core network domain.
NOTE 3 – This reference point is applicable when PD-FE operates in the access network domain.
NOTE 4 – This reference point is applicable when PD-FE operates in the core network domain.
NOTE 5 – This is to be understood as referring to the different I-TC*n* reference points that may exist between IdM functions and relevant transport control functional entities (see clause 9.3.7 for further information).

Figure 9-3 – Transport-control-related functional entities

9.3.2.1 T-10: Network access configuration functional entity (NAC-FE)

The NAC-FE is responsible for the IP address allocation to the CPE. It can optionally 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-CSC-FE when accessing to the IMS component [ITU-T Y.2021]).

For further details, refer to [ITU-T Y.2014].

NOTE – The T-10 network access configuration FE may reside in a visited network or a home network. It depends on the administrative domain and the business scenario.

9.3.2.2 T-11: 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 can optionally perform the collection of accounting data for each user authenticated by the NACF.

For further details, refer to [ITU-T Y.2014].

9.3.2.3 T-12: 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".

For further details, refer to clause 7.2.5 of [ITU-T Y.2014].

9.3.2.4 T-13: Transport location management functional entity (TLM-FE)

The TLM-FE registers the association between the IP address allocated to the CPE and the 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.

For further details, refer to [ITU-T Y.2014].

9.3.2.5 T-14: 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.

For further details, refer to [ITU-T Y.2014].

9.3.2.6 T-15: Home gateway configuration functional entity (HGWC-FE)

The HGWC-FE is used during initialization and update of the HGW (also called CPN gateway, see clause 9.3.6). It provides 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.

For further details, refer to [ITU-T Y.2014].

9.3.2.7 T-16: Policy decision functional entity (PD-FE)

The PD-FE provides a single contact point to the SCF and hides the details of transport network to the SCF. The PD-FE makes the final decision regarding network resource and admission control based on network policy rules, SLAs, service information provided by the SCF, transport subscription information provided by the NACF in access networks, and resource-based admission decision results provided by the TRC-FE. The PD-FE controls the gates in the PE-FEs at a per flow level. The PD-FE consists of transport technology-independent resource control functions and is independent of the SCF as well. The policy rules used by the PD-FE are service-based and are assumed to be provided by the NGN operators.

For further details, refer to [ITU-T Y.2111].

9.3.2.8 T-17: Transport resource control functional entity (TRC-FE)

The TRC-FE deals with the diversity of underlying transport technologies and provides the resource-based admission control decision results to the PD-FE. The TRC-FE is service-independent and consists of transport technology-dependent resource control functions. The PD-FE requests the TRC-FE instances in the involved transport networks to detect and determine the requested QoS resource along the media flow path. The TRC-FE may collect and maintain the transport network topology and the transport resource status information. It may also authorize resource admission control of a transport network based on network information, such as topology and/or connectivity, network and element resource availability, as well as the transport subscription information in access networks.

For further details, refer to [ITU-T Y.2111].

9.3.2.9 T-18: Mobile location management functional entity (MLM-FE)

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

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

For further details, refer to [ITU-T Y.2018].

9.3.2.10 T-19: Handover decision and control functional entity (HDC-FE)

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

For further details, refer to [ITU-T Y.2018].

9.3.2.11 T-20: Network information distribution functional entity (NID-FE)

The network information distribution functional entity (NID-FE) has the following responsibilities:

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

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

For further details, refer to [ITU-T Y.2018].

9.3.2.12 T-21: Network information repository functional entity (NIR-FE)

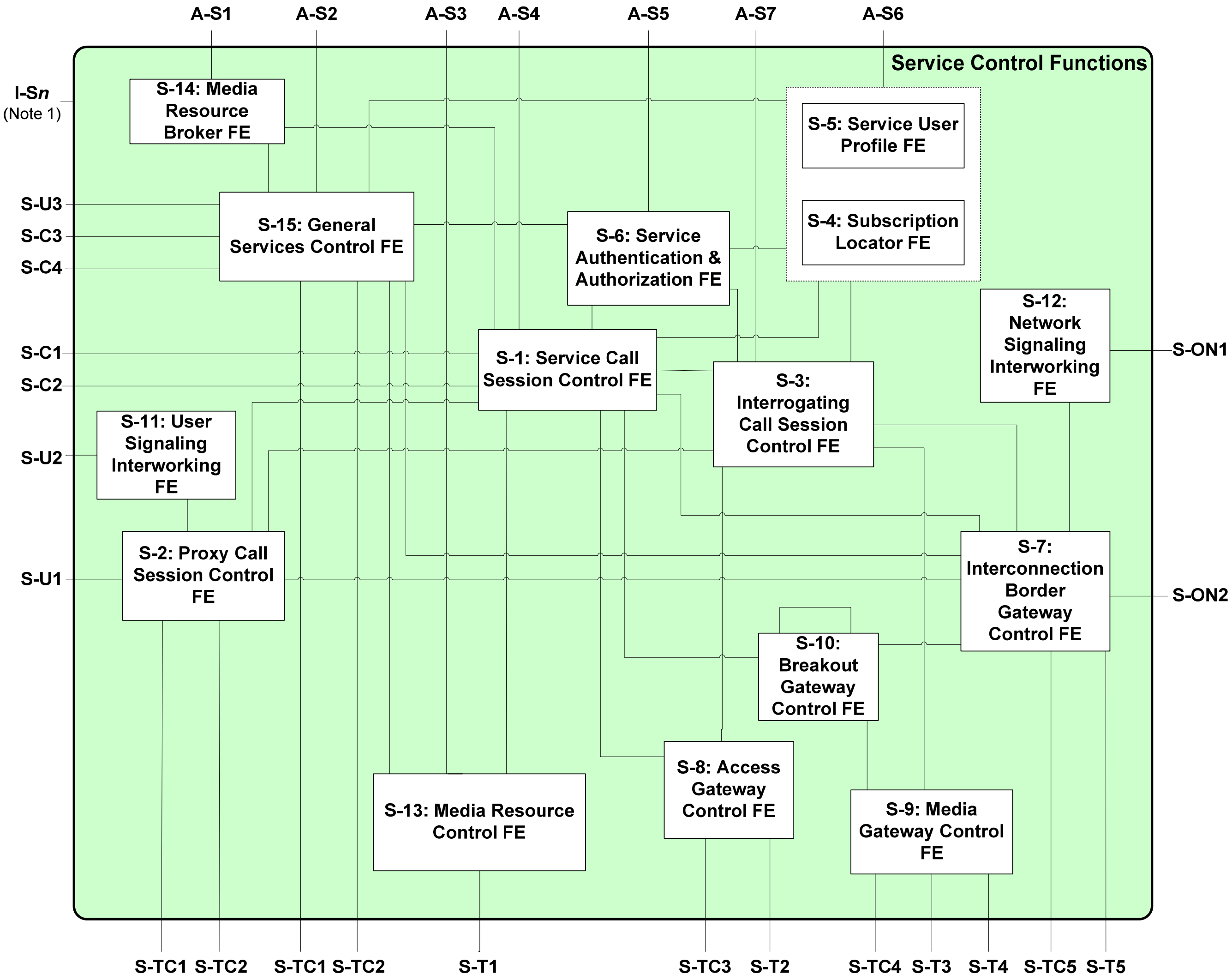
The network information repository functional entity (NIR-FE) provides static information on neighbouring networks to the NID-FE to assist the access network discovery and selection decision.

For further details, refer to [ITU-T Y.2018].

9.3.3 Service control and content delivery functional entities

9.3.3.1 Service control functional entities

Figure 9-4 shows the functional entities related to service control.


A-S1
A-S2
A-S3
A-S4
A-S5
A-S7
A-S6
Service Control Functions
I-Sn
(Note 1)
S-14: Media Resource Broker FE
S-5: Service User Profile FE
S-4: Subscription Locator FE
S-U3
S-C3
S-C4
S-15: General Services Control FE
S-6: Service Authentication & Authorization FE
S-12: Network Signaling Interworking FE
S-ON1
S-C1
S-C2
S-1: Service Call Session Control FE
S-3: Interrogating Call Session Control FE
S-11: User Signaling Interworking FE
S-U2
S-2: Proxy Call Session Control FE
S-U1
S-7: Interconnection Border Gateway Control FE
S-ON2
S-10: Breakout Gateway Control FE
S-8: Access Gateway Control FE
S-13: Media Resource Control FE
S-9: Media Gateway Control FE
S-TC1
S-TC2
S-TC1
S-TC2
S-T1
S-TC3
S-T2
S-TC4
S-T3
S-T4
S-TC5
S-T5

NOTE 1 – This is to be understood as referring to the different I-S*n* reference points that may exist between IdM functions and relevant service control functional entities (see clause 9.3.7 for further information).

Figure 9-4 – Service control functional entities

NOTE 1 – It is for further study whether functions not currently in S-1: S-CSC-FE, S-2: P-CSC-FE and S-3: I-CSC-FE should be added to them or accommodated by S-15: GSC-FE. Depending on the outcome of this study, S-15: GSC-FE may be revisited in the future.

NOTE 2 – Any line terminating on the dotted box around S-4 and S-5 implies an implicit connection to either S-4 or S-5 or both. Inclusion of these two FEs in the dotted box does not imply that they are co-located.

NOTE 3 – Although it is located in the service control functions, the MRB-FE could be viewed as a part of application support functions and service support functions.

9.3.3.1.1 S-1: Serving call session control functional entity (S-CSC-FE)

The serving call session control functional entity (S-CSC-FE) handles functionality related to session control, e.g., registration, origination of sessions (session setup, modification and teardown), and routing of session messages. It performs the following functions:

a) **Registration**: It can learn that a particular user and/or terminal identifier is currently in service and can interact with the SUP-FE (possibly via the SL-FE) to obtain relevant service profile and address information which will act as an input to the service triggering and routing functions of the S-CSC-FE.

b) **Service triggering**: Based on an analysis of the session control messages, it can route session control messages to appropriate application support and service support functions.

c) **Determination of routing of session control messages**: It can determine the routing for session control messages based on routing (location) information available to it in appropriate databases, NGN operator routing policy and address information obtained from SUP-FE via the "registration" function.

The S-CSC-FE maintains a session-related state as needed by the NGN operator for support of services. Within the network of a NGN operator, different S-CSC-FEs may have different functionalities.

For mediated session, the S-CSC-FE:

1) Is required to have the capability to accept session control requests and service them internally or forward them on, possibly after translation.

2) Is required to have the capability to terminate and independently generate session control messages.

3) Interacts with the AS-FE to support services and third-party applications.

4) Performs as follows for an originating endpoint (i.e., the originating user/UE or originating AS-FE):

   a) It obtains from a database the address of the contact point for the NGN operator serving the destination user from the destination name (e.g., a dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and it forwards the request or response to that contact point.

   b) When the destination name of the destination user (e.g., a dialled phone number or SIP URI) and the originating user belong to the same NGN operator, it forwards the session control request or response to an I-CSC-FE within the NGN operator's network.

   c) It forwards the session control request or response to a BGC-FE for call routing to the PSTN.

   d) In case the request is an originating request from an AS-FE:

      – It verifies that the request coming from the AS-FE is an originating request and applies procedures accordingly (e.g., it invokes interaction with the service platforms for the originating services, etc.).

      – It processes and proceeds with the request even if the user on whose behalf the AS-FE had generated the request is unregistered.

      – It processes and proceeds with other requests to and from the user on whose behalf the AS-FE had generated the request.

      – It reflects in the charging information that an AS-FE had initiated the session on behalf of the user.

5) Performs as follows for a destination endpoint (i.e., the terminating user/UE).

This item identifies the procedures related to the destination endpoint. In the case that roaming is not deployed as a network capability, only those procedures in a) or b) related to terminating a session for a "home user" within a "home network" shall be mandated capabilities. Technology-specific functional architectures instantiating this FE are required to identify if roaming is supported in the technology.

a) It forwards the session control request or response to a P-CSC-FE or AGC-FE for a terminating session procedure for a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSC-FE in the path.

b) It forwards the session control request or response to an I-CSC-FE for a terminating session procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSC-FE in the path.

c) It forwards the session control request or response to a BGC-FE for call routing to the PSTN.

d) If the session control request contains preferences for the characteristics of the destination endpoint, it performs preference and capability matching.

9.3.3.1.2 S-2: Proxy call session control functional entity (P-CSC-FE)

The proxy call session control functional entity (P-CSC-FE) acts as the contact point to the user terminal for session-based services. Its address is discovered by terminals using mechanisms, such as static provisioning, a NACF, or other access-specific techniques. The P-CSC-FE has the capability to accept requests and services them internally or forward them on. It is required to have the capability to terminate and independently generate session control messages. However, as the key function of the P-CSC-FE is to proxy session control requests, this capability will likely only be used under abnormal conditions. The functions performed by the P-CSC-FE include the following:

a) It is required to have the capability of forwarding session control requests related to registration to an appropriate I-CSC-FE.

b) It is required to have the capability of forwarding session control requests received from the terminal to the S-CSC-FE.

c) It is required to have the capability of forwarding session control requests or responses to the terminal.

d) It is required to have the capability of detecting and handling emergency session establishment requests.

e) It is required to be able to maintain a security association between itself and each terminal.

f) It is required to have the capability of performing message compression/decompression.

g) It can optionally perform inter-domain topology hiding.

h) It can optionally perform inter-domain protocol repair (for further study).

In addition, the P-CSC-FE controls the access border gateway functional entities (ABG-FEs) via the RACF to accommodate access transport functions and end-user functions. The P-CSC-FE also controls access node functional entities (AN-FE) and edge node functional entities (EN-FEs) via the RACF to support access transport functions. The functions performed by the P-CSC-FE include the following:

i) It is required to have the capability of participating in the authorization of media resources and QoS management, e.g., by interacting with resource control when no explicit signalling (i.e., QoS signalling) is available. Application-specific intelligence is required to derive resource control commands from the application signalling.

j) It is required to support an NAPT proxy function (NPF) for network address hiding and remote NAPT traversal. It requests address mapping information and modifies the addresses and/or ports contained in the message bodies of application signalling messages, according to the address binding information provided by the RACF at the border of the access and core transport networks.

As an option, this FE interacts with MRC-FE in support of invoking transcoding.

9.3.3.1.3 S-3: Interrogating call session control functional entity (I-CSC-FE)

The interrogating call session control functional entity (I-CSC-FE) is the contact point within an NGN operator's network for all service connections destined to a user of that NGN operator. There may be multiple I-CSC-FEs within a NGN operator's network. The functions performed by the I-CSC-FE are as follows:

a) Registration

   – Assigning a S-CSC-FE to a user.

b) Session-related and session-unrelated flows

   – Obtaining from the SUP-FE the address of the currently assigned S-CSC-FE;

   – Forwarding a session control request or response to the S-CSC-FE determined by the above step for incoming sessions.

In performing the above functions, the NGN operator can optionally use the topology hiding function in the I-CSC-FE or other techniques to hide the configuration, capacity, and topology of the network from the outside. When an I-CSC-FE is chosen to meet the hiding requirement, for sessions traversing different network operators' domains, the I-CSC-FE may restrict the following information from being passed outside a NGN operator's network: the exact number of S-CSC-FEs, the capabilities of the S-CSC-FEs, and the capacity of the network.

9.3.3.1.4 S-4: Subscription locator functional entity (SL-FE)

The subscription locator functional entity (SL-FE) may be queried by the S-CSC-FE, the I-CSC-FE, or the AS-FE to obtain the address of the SUP-FE for the required subscriber. The SL-FE is used to find the address of the physical entity that holds the subscriber data for a given user identifier when multiple, separately addressable SUP-FEs have been deployed by the NGN operator. This resolution mechanism is not required in networks that utilize a single logical SUP-FE element.

9.3.3.1.5 S-5: Service user profile functional entity (SUP-FE)

The service user profile functional entity (SUP-FE) is responsible for storing user profiles, subscriber-related location data, and presence status data in the service stratum.

1) The SUP-FE performs basic data management and maintenance functions.

   - User profile management functions

     These functions require access to certain data, either "user subscription data" or "network data" (e.g., the current network access point and network location). The storage and update of this data are handled by the user profile management functions.

     A user profile is required to be provided in support of:

     - authentication
     - authorization
     - service subscription information
     - subscriber mobility
     - location
     - presence (e.g., online/offline status)
     - charging

     The user profile is stored in one database or separated into several databases.

2) The SUP-FE is responsible for responses to queries for user profiles.

   a) It provides access to user data.

      Other network functions require some user data in order to be appropriately customized. This data can be either "user subscription data" or "network data". This function provides filtered access to the user data, which is restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

   b) It can optionally be used for support of commonly used AAA and security schemes.

9.3.3.1.6 S-6: Service authentication and authorization functional entity (SAA-FE)

The service authentication and authorization functional entity (SAA-FE) provides authentication and authorization in the service stratum.

1) It ensures that the end-user has valid utilization rights for the requested service.
2) It performs policy control at the service level by using policy rules contained in a user profile database.
3) It works as the first step in the mobility management process and is used for authentication, authorization, and accounting of users/terminals.
4) The result of the authorization function is a yes/no response to a user connection request.

9.3.3.1.7 S-7: Interconnection border gateway control functional entity (IBC-FE)

The interconnection border gateway control functional entity (IBC-FE) controls interconnection border gateway functional entities (IBG-FEs) via the RACF to interwork with other packet-based networks. Alternative means of control, such as direct control of IBG-FE by IBC-FE, need further study.

The functions of the IBC-FE can optionally include:

1) Inter-domain network topology hiding;
2) Control of IBG-FEs to implement session-based processing (e.g., media conversion and NA(P)T) (This is for further study.);
3) Inter-domain protocol repair (This is for further study.);
4) Interaction with PD-FE for resource reservation, resource allocation and/or other resource related information (e.g., the available resource parameters if the required resources are not available, QoS label, etc.);
5) As an option, this FE interacts with MRC-FE in support of invoking transcoding.

NOTE – Information screening functions are for further study.

9.3.3.1.8 S-8: Access gateway control functional entity (AGC-FE)

The access gateway control functional entity (AGC-FE) controls one or more AMG-FEs to access PSTN or ISDN users and handles registration, authentication, and security for the user. The AGC-FE performs registration, authentication, and security for the AMG-FE.

a) It originates and terminates session control signalling.
b) It originates and terminates gateway control flows to control the AMG-FE.
c) It can optionally initiate and terminate UNI control flows, in order to provide ISDN (supplementary) services.
d) It forwards the session control flow to the S-CSC-FE.
e) It processes and forwards requests from the AMG-FE to the S-CSC-FE.
f) It can optionally process and forward service requests from the AMG-FE to the AS-FE through the S-CSC-FE. For example, a POTS user can request and use a multimedia 800 service provided by the AS-FE with media restrictions.

g) It can optionally participate in the authorization of media resources and QoS management, e.g., by interacting with resource control when no explicit signalling (i.e., QoS signalling) is available and application-specific intelligence is required to derive resource control commands from the application signalling.

h) It supports a NAPT proxy function (NPF) for network address hiding and remote NAPT traversal. This is done by requesting address mapping information and modifying the addresses and/or ports contained in the message bodies of application signalling messages, according to the address binding information provided by the RACF at the border of the access and the core transport networks.

i) Optionally, it ensures the transparent data transport between ISDN user side and IP side from the control level in media negotiation process, in order to support ISDN emulation service in case ISDN unrestricted bearer is needed.

9.3.3.1.9 S-9: Media gateway control functional entity (MGC-FE)

The media gateway control functional entity (MGC-FE) controls the TMG-FE to interwork with PSTN/ISDN.

a) It processes and forwards requests from the SG-FE to the S-CSC-FE through the I-CSC-FE;

b) It can optionally process and forward service requests from PSTN/ISDN to the AS-FE through the BGC-FE and the S-CSC-FE. For example, a PSTN user can request and use a multimedia 800 service provided by the NGN AS-FE with media restrictions.

c) Optionally, it ensures the transparent data transport between TDM side and IP side from the control level in media negotiation process, in order to support ISDN emulation service in cases where an ISDN unrestricted bearer is needed.

As an option, this FE interacts with the MRC-FE in support of invoking transcoding.

9.3.3.1.10 S-10: Breakout gateway control functional entity (BGC-FE)

The breakout gateway control functional entity (BGC-FE) selects the network in which PSTN breakout is to occur and selects the MGC-FE.

As an option, this FE interacts with the MRC-FE in support of invoking transcoding.

9.3.3.1.11 S-11: User signalling interworking functional entity (USIW-FE)

The user signalling interworking functional entity (USIW-FE) has the responsibility for the interworking and the information screening functions for different types of application signalling at the subscriber side (access-to-core), which can be located at the border of the access and core networks for subscriber-side signalling interworking.

9.3.3.1.12 S-12: Network signalling interworking functional entity (NSIW-FE)

The network signalling interworking functional entity (NSIW-FE) has the responsibility for the interworking for different types and profiles of application signalling at the trunking side (inter-network operator), which can be located at the border of the core networks for trunking-side signalling interworking.

NOTE – Information screening functions are for further study.

9.3.3.1.13 S-13: Media resource control functional entity (MRC-FE)

The media resource control functional entity (MRC-FE) controls the media resource processing functional entity (MRP-FE) by operating as a media resource control function.

The MRC-FE allocates/assigns MRP-FE resources that are needed for services such as streaming, announcements, and interactive voice response (IVR) support.

NOTE – As an option, P-CSC-FE, IBC-FE, BGC-FE, and MGC-FE interact with MRC-FE in support of invoking transcoding.

9.3.3.1.14 S-14: Media resource broker functional entity (MRB-FE)

The media resource broker functional entity (MRB-FE) does the following:

a) It assigns specific media server resources (i.e., MRC-FE and MRP-FE) to incoming calls at the request of service applications (i.e., an AS-FE); this happens in real time as calls come into the network.

b) It acquires knowledge of media server resource utilization that it can use to help decide which media server resources to assign to resource requests from applications.

c) It employs methods/algorithms to determine media server resource assignment.

d) It acquires knowledge of media server resource status related to in-service and out-of-service status and reservations via an operational type of reference point.

NOTE – Although it is located in the service control functions, the MRB-FE could be viewed as a part of application support functions and service support functions.

9.3.3.1.15 S-15: General services control functional entity (GSC-FE)

The NGN functional architecture also provides support for services that do not require initial network-mediated session establishment procedures using a proxy call session control functional entity, since it is expected to provide a platform for all envisaged services over packet-based networks.

The general services control functional entity (GSC-FE) acts as a contact point for application support and service support functional entities, as well as user terminals. The GSC-FE authenticates communications from these, and based on those communications, and optionally doing some processing functions, such as translating domain name to explicit the IP address for the end user's convenience, the GSC-FE authorizes and provides information on session flows and their required QoS characteristics to the PD-FE (either directly or via S-13, the media resource control FE), as well as to the IBC-FE when appropriate. The GSC-FE maintains session-related state as needed to assist in policy actions.

Communication from the terminal or application support and service support functions must include information to identify the targeted session flows (for example, source and destination IP address) plus the requested treatments. Depending on the service and implementation, it can optionally include:

- service priority information (to use, for example, if pre-emption is needed);
- a request for resource usage information.

The GSC-FE will respond to those communications and requests as appropriate and as information is available.

The GSC-FE can optionally obtain information from service user profiles and invoke service applications.

Communication from the GSC-FE to the PD-FE, and to the IBC-FE where applicable, will include at least session flow identification information and the requested treatments. Depending on the service and implementation, it can optionally include:

- an indication of when resources are to be committed (immediately or later);
- a request for resource usage information;
- a request to be notified when resources are reserved, modified and released.

The PD-FE will respond to those communications and requests as appropriate and as information is available.

Invocation of the MRC-FE and the MRP-FE, for transcoding, announcements, and so on, is for further study.

9.3.4 Content delivery functional entities

The content delivery functions (CDF) perform cache and storage functionalities and deliver the content according to the request from the end-user functions. The content delivery functions (CDF) can optionally process the content.

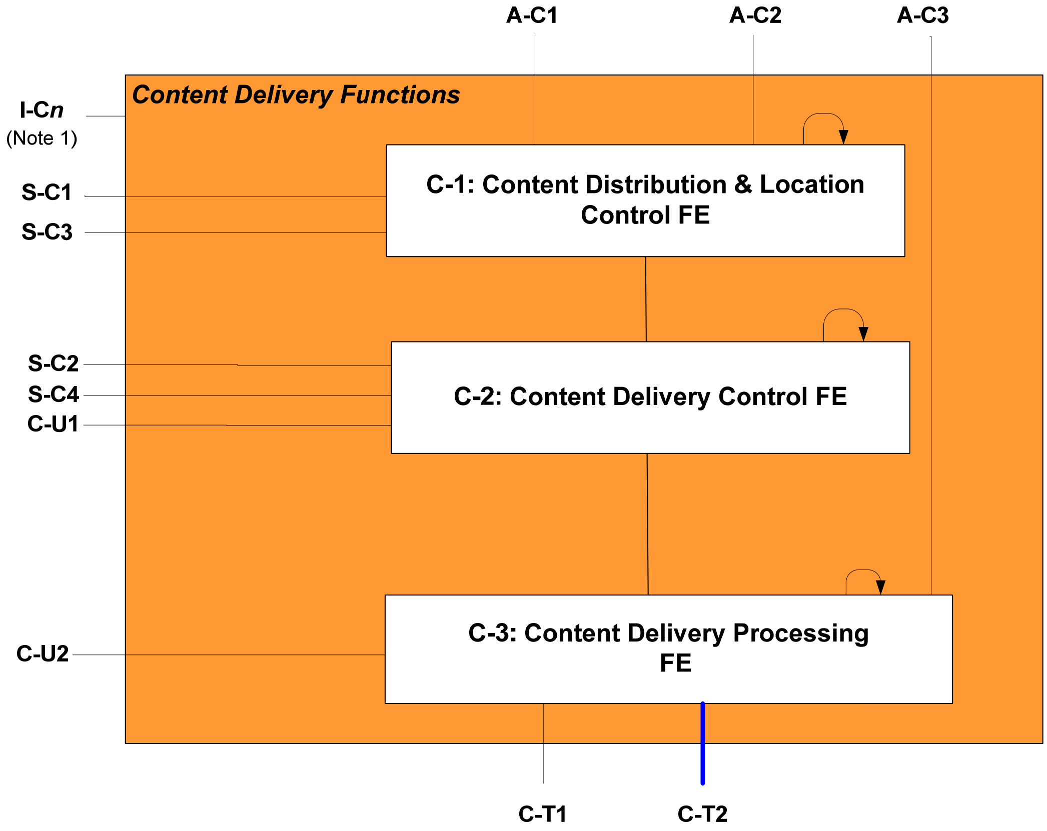
Multiple instances of storage and delivery functionalities can optionally exist. The content delivery functions select the suitable one(s). To maintain the same content at the multiple instances, the content delivery functions control the distribution of the content to multiple instances of storage and delivery functionalities.

The content is distributed to the content delivery functions before or during the service offering process.

The content delivery functions interact with end-user functions (e.g., trick mode play functionality).

The content delivery functions support unicast, multicast or both mechanisms.

Figure 9-5 shows the content delivery FEs.


A-C1
A-C2
A-C3
Content Delivery Functions
I-Cn
(Note 1)
S-C1
S-C3
C-1: Content Distribution & Location Control FE
S-C2
S-C4
C-U1
C-2: Content Delivery Control FE
C-U2
C-3: Content Delivery Processing FE
C-T1
C-T2

NOTE 1 – This is to be understood as referring to the different I-C*n* reference points that may exist between IdM functions and relevant content delivery functional entities (see clause 9.3.7 for further information).

NOTE 2 – Reference points S-C1 and S-C2 are meant to be used for the IMS IPTV case (i.e., connected to S-CSC-FE), while S-C3 and S-C4 reference points apply for the non-IMS IPTV cases (i.e., connected to GSC-FE). See Annex B for further details.

Figure 9-5 – Content delivery functional entities

9.3.4.1 C-1: Content distribution & location control functional entity (CD&LC-FE)

The content distribution & location control functional entity includes the following functions but is not limited to:

- Handling interactions with the service control functional entities;
- Controlling the distribution of content from the content preparation functional entity (CPR-FE) in the application support and service support functions to the content delivery processing functional entities (CDP-FEs);
- Gathering the information regarding content delivery processing functional entities (CDP-FEs), e.g., resource utilization, resources status (e.g., in-service and out-of-service), content distribution information and load status;
- Performing the selection of suitable content delivery processing functional entities (CDP-FEs) to serve end-user functions according to some criteria, e.g., the gathered information and the terminal capability.

  NOTE – This selection request can optionally be triggered by the service control functions or the application support functions and service support functions.

9.3.4.2 C-2: Content delivery control functional entity (CDC-FE)

The content delivery control functional entity (CDC-FE) handles control functions related to the content delivery processing functional entity (CDP-FE).

The CDC-FE includes but is not limited to:

- Control of the media resources delivery;
- Handling of recoding commands such as for video cassette recorder (VCR);
- Reporting status (e.g., load status and availability) to the content distribution and location control functional entity;
- Generating charging information.

9.3.4.3 C-3: Content delivery processing functional entity (CDP-FE)

The content delivery processing functional entity (CDP-FE) stores and caches the content, processes it under the control of the content preparation functional entity and the content delivery control functional entity. The CDP-FE distributes the content among instances of content delivery processing functional entities based on the policy of the content distribution & location control functional entity (CD&LC-FE).

The CDP-FE is responsible for delivering content to the end-user functions using the transport functions (e.g., unicast and/or multicast mechanisms).

The CDP-FE includes but is not limited to:

- Handling interaction with the service control functions;
- Handling content delivery to end-user functions;
- Caching and storing content and associated information;
- Insertion, transcoding and encryption of the content;
- Distributing content among content delivery processing functional entities;
- Managing interaction with the end-user functions (e.g., trick mode commands).

9.3.5 Application support functions and service support functions (ASF&SSF)

The application support functions and service support functions (ASF&SSF) provide control for services accessed by interacting with the S-CSC-FE, the GSC-FE, or the end-user directly. Application support functions and service support functions may reside either in the end-user's home network or in a third party location. The application support functions and service support functions include the following functional entities: application support FE, application gateway FE, application service coordination manager FE, service switching FE, application support user profile FE, application provisioning FE, content preparation FE and service and content protection FE.

The application support functions and service support functions can influence and impact the session on behalf of services through its interface with the S-CSC-FE.

It shall be possible for application support functions and service support functions to generate session control requests and dialogs on behalf of users. Such requests are forwarded to the S-CSC-FE serving the user, and the S-CSC-FE is required to perform regular originating procedures for these requests. Residing either as a trusted entity in the user's home network or as an un-trusted entity in a third-party location (requiring certain level of authentication), the application support functions and service support functions interact with other entities in the network, as shown in Figure 9-6.

The application support functions and service support functions do the following:

a) Execute service logic based on the subscriber's service profile and/or on the terminal capability (device profile);

b) Act via four session interaction models with respect to the S-CSC-FE:
   – as a terminating user agent;
   – as an originating user agent;
   – as a proxy;
   – as a third-party call control (back-to-back user agent);

c) Interact with the AGC-FE through the S-CSC-FE to provide access to the applications required to support the legacy terminal users;

d) Interact with the MRC-FE directly or via the S-CSC-FE in order to control MRP-FE;

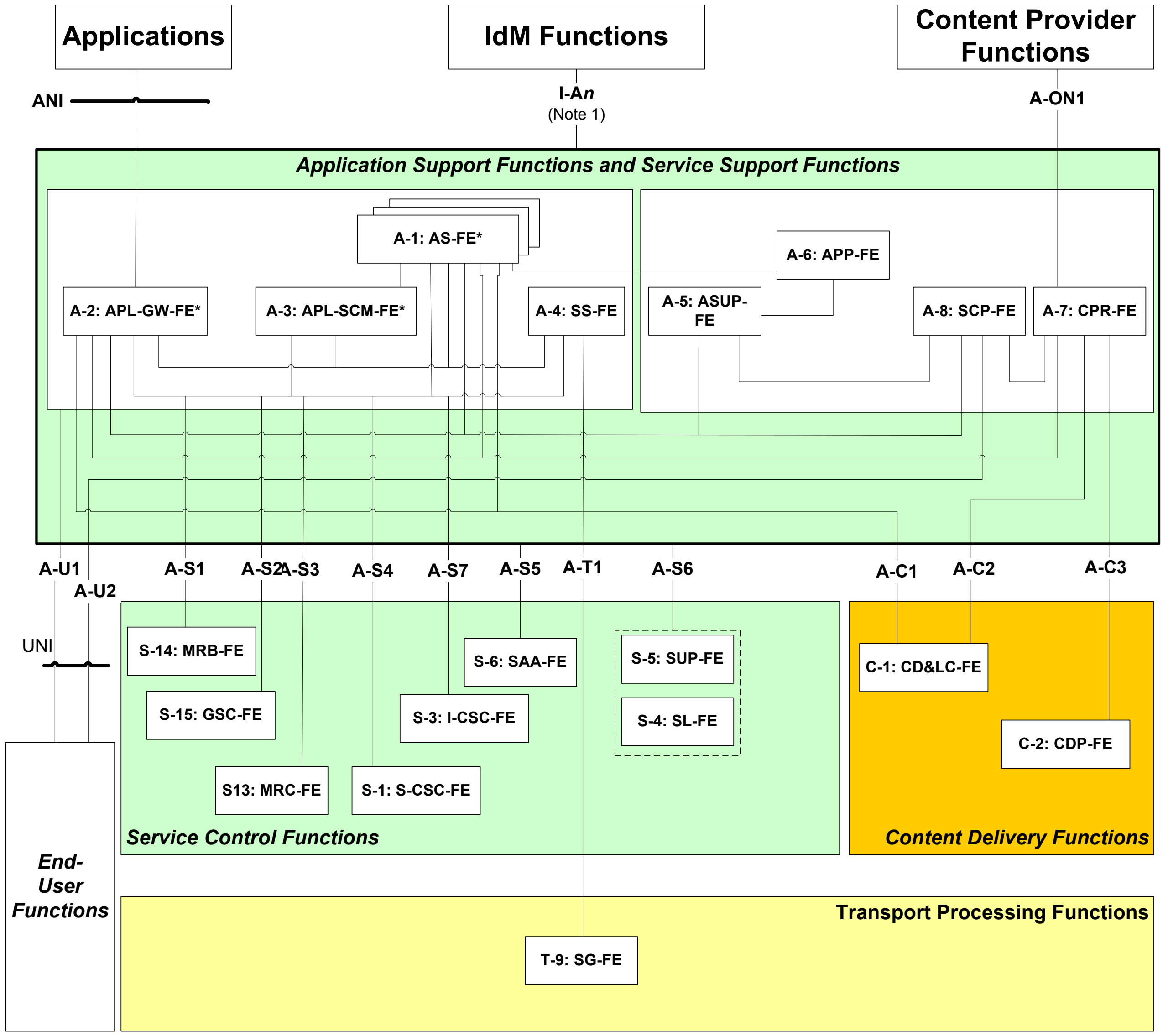
e) Optionally, interact with the MRB-FE in order to attain an MRC-FE resource;

f) Interact with the end-user functions (via UNI A-U1 reference point) to allow the end-users to securely manage and configure data for their services and applications;

g) Interact with the end-user functions (via UNI A-U2 reference point) for delivering security information (e.g., rights object or keys) from the SCP-FE to the end-user functions;

h) Interact with the content delivery functions to transfer content from CPR-FE to CDP-FEs (via A-C3 reference point), as well as to facilitate CPR-FE to configure policies such as content distribution rules, selection criteria, etc., in the CD&LC-FE (via the A-C2 reference point);

i) Interact with the content delivery functions (via the A-C1 reference point) to allow the AS-FE and/or the APL-GW-FE to request the CD&LC-FE to request the selection of a suitable CDP-FE for content delivery or to request other information such as service parameters to the CD&LC-FE.



NOTE 1 – This is to be understood as referring to the different I-A*n* reference points that may exist between IdM functions and relevant functional entities within application support functions and service support functions (see clause 9.3.7 for further information).

Figure 9-6 – Application/service support functions

NOTE 1 – Although the MRB-FE is located in the service control functions, it could be viewed as a part of the application support functions and the service support functions.

NOTE 2 – Note that content delivery functions may reside outside of the NGN (see Annex B), ASF&SSF FEs may also reside outside of the NGN, e.g., ASUP-FE, APP-FE, SCP-FE and CPR-FE.

9.3.5.1 A-1: Application support functional entity (AS-FE)

The application support functional entity (AS-FE) supports generic application server functions, including hosting and executing services. The examples of AS-FE are call feature application support servers, presence servers, various messaging servers, conferences servers, home application support servers, IPTV application support servers, service selection servers, service discovery servers, as well as charging and accounting servers.

9.3.5.2 A-2: Application gateway functional entity (APL-GW-FE)

The application gateway functional entity (APL-GW-FE) serves as an interworking entity between the applications and the S-CSC-FE of the service stratum. Appearing to the S-CSC-FE as if it were an AS-FE, the APL-GW-FE provides a secure open interface for the applications to use the capabilities and the resources of the NGN. Specifically, the APL-GW-FE is the interworking entity between various functions of NGN and all external application servers and service enablers. The applications connected to the APL-GW-FE are usually realized by OSA application servers.

9.3.5.3 A-3: Application service coordination manager functional entity (APL-SCM-FE)

The application service coordination manager functional entity (APL-SCM-FE) manages interactions between multiple applications and services. The functional entities of ASF&SSF might interwork with each other via the APL-SCM-FE to provide convergent services to the end users.

9.3.5.4 A-4: Service switching functional entity (SS-FE)

The service switching functional entity (SS-FE) provides access and interworking to a legacy IN SCP. For the IN services, the S-CSC-FE is connected through the SS-FE to the SG-FE to interact with a legacy IN SCP. The SS-FE provides IN service switching functions, including service trigger detection, service filtering, call state management, etc., and the protocol adaptation function between INAP and SIP, for example.

9.3.5.5 A-5: Application support user profile functional entity (ASUP-FE)

The application support user profile functional entity (ASUP-FE) can optionally include:

- End-user settings which include information related to the capabilities of the end-user's terminal devices. An end user may be associated with one or more terminals with different capabilities;
- Global settings (e.g., language preference);
- Application of specific settings (e.g., parental control level for VoD application);
- List of subscribed service packages;
- Service actions data which encompasses information related to the actions the user can optionally have taken while accessing services/applications, e.g., for IPTV, list of linear TV services (or programmes) that the user has paused and is hence likely to resume later, list of VoDs that the user has ordered and associated status, list of PVR contents that the user has asked to be recorded.

9.3.5.6 A-6: Application provisioning functional entity (APP-FE)

The application provisioning functional entity (APP-FE) adds or withdraws application support functional entities (AS-FEs) and manages the life-cycle of the applications supported by the AS-FEs.

9.3.5.7 A-7: Content preparation functional entity (CPR-FE)

The content preparation functional entity (CPR-FE) controls the preparation and aggregation of the contents such as VoD programs, TV channel streams, metadata, and EPG data, as received from the content provider functions. The content preparation functional entity can optionally pre-process (e.g., transcode or edit) the content in advance of passing it to the content delivery functions, associated application support functional entities and service protection and/or content protection functional entities.

The CPR-FE is comprised of content management, metadata processing, content processing control and content pre-processing functions. These functions can optionally be used to control the preparation and/or combination of the content, as delivered by the content owner(s), into the required delivery format.

The functions of the CPR-FE may be subject to commercial agreements with content owners. Note that not all contents are subject to the functions described below.

The metadata and rights information are delivered to the metadata processing function. Content can optionally be transcoded and encrypted by the content pre-processing function, before being delivered to the content delivery functions. The program related metadata is delivered to the corresponding application support functional entity. If the original content from the content owner is modified or transcoded in any way, it may be necessary to also edit the program related metadata.

9.3.5.8 A-8: Service and content protection functional entity (SCP-FE)

The service and content protection functional entity (SCP-FE) controls the protection of the services and content. Content protection includes control of accessing the content and the protection of content using methods such as encryption. Service protection includes authentication and authorization to access the services and, optionally, protection of the services using methods such as encryption.

The service and content protection functional entity (SCP-FE) includes a content protection function and a service protection function.

The content protection function controls the protection of the content and is responsible for the management of the content rights and the keys used to encrypt and decrypt the content. It acquires the content rights (or content license, originated from the content provider) indication from the content preparation functional entity, generates and distributes this security information (rights object or keys) to the end-user functions. It can optionally provide keys for content encryption.

For example, when it receives a request for security information from end-user functions, it interacts with the application support user profile functional entity for user related security subscription information (e.g., in case of IPTV, time limited, whether fast forward/fast rewind are allowed), generates the rights object and delivers it to the end-user functions.

It also provides keys for service and content protection to the associated application support functional entity, which then deliver the keys to relevant functions, e.g., end-user functions and the content preparation functional entity.

The service protection function controls the protection of services. Service protection includes authentication and authorization to access the services and protection of the services using methods such as encryption.

9.3.5.9 Guidelines for selecting functions as the AS-FE

The following guidelines for selecting functions as the AS-FE apply:

– A function that is used in common in two or more applications is recommended to be included in the AS-FE;

– From the viewpoint of personal information and privacy protection, a function that handles the user profile managed within NGN is recommended to be included in the AS-FE;

– From the viewpoint of security, a function that handles the inside network signal information is recommended to be included in the AS-FE;

– A function that can be located in application support functions and service support functions to provide an efficient service is recommended to be included in the AS-FE to improve QoE.

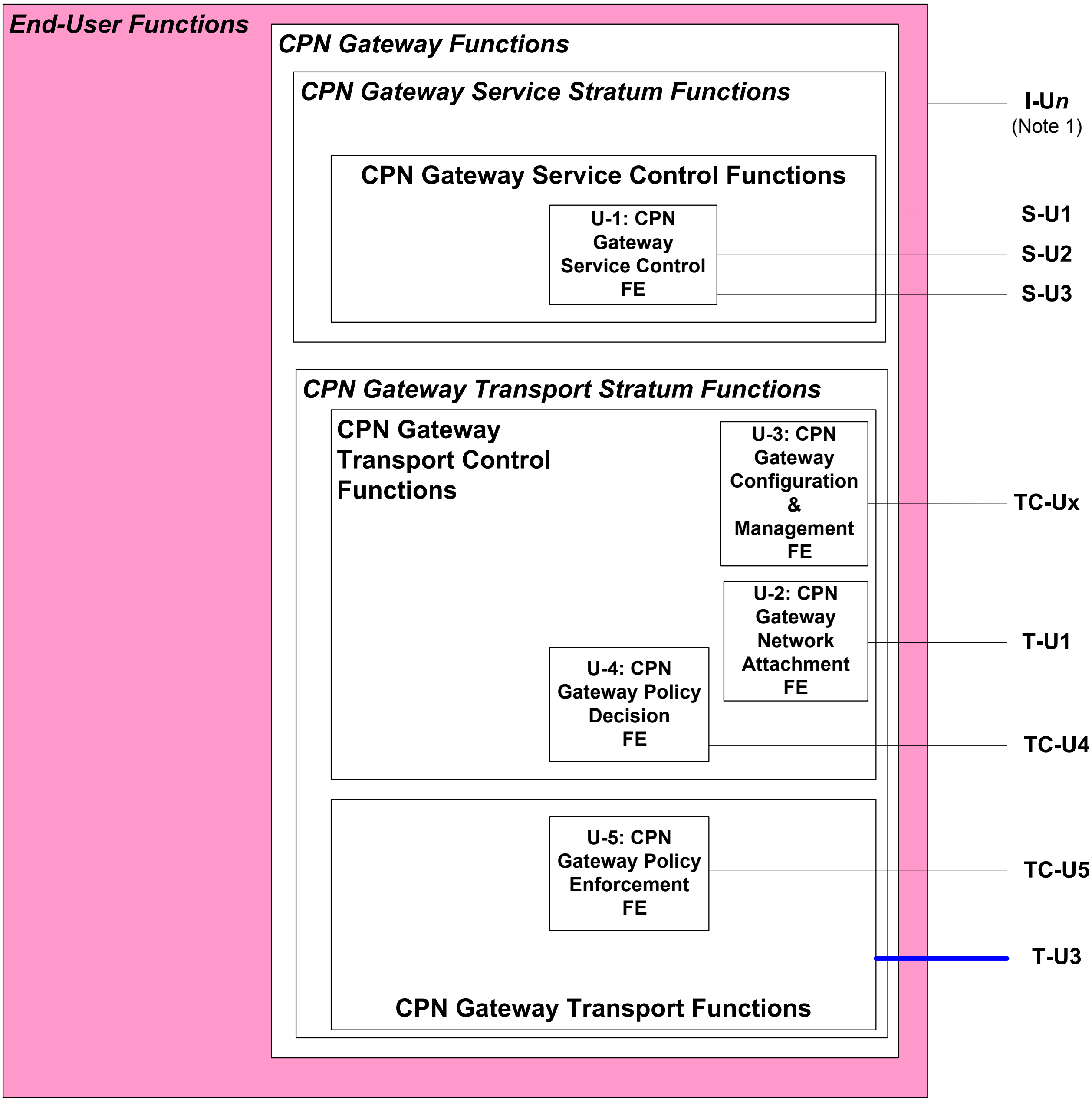
9.3.6 End-user functions

End-user functions include CPN gateway functions. Other functions, such as terminal functions, are not described in this Recommendation.

9.3.6.1 CPN gateway functions

CPN gateway functions (CGF) in this Recommendation concern CPN gateway's impact to the NGN, e.g., the impacts related to NACF, RACF, and functions inside the NGN service stratum.

CPN gateway functions are decomposed in a similar way than the NGN, i.e., in CPN gateway service stratum functions and CPN gateway transport stratum functions.


End-User Functions
CPN Gateway Functions
CPN Gateway Service Stratum Functions
CPN Gateway Service Control Functions
U-1: CPN Gateway Service Control FE
I-U*n*
(Note 1)
S-U1
S-U2
S-U3
CPN Gateway Transport Stratum Functions
CPN Gateway Transport Control Functions
U-3: CPN Gateway Configuration & Management FE
TC-Ux
U-2: CPN Gateway Network Attachment FE
T-U1
U-4: CPN Gateway Policy Decision FE
TC-U4
U-5: CPN Gateway Policy Enforcement FE
TC-U5
T-U3
CPN Gateway Transport Functions

NOTE 1 – This is to be understood as referring to the different I-U*n* reference points that may exist between IdM functions and relevant functional entities within end-user functions (see clause 9.3.7 for further information).

Figure 9-7 – End-user functional entities

Note that Figure 9-7 does not show reference points A-U1, A-U2 and T-U4. Further study is required regarding the termination of these reference points in the end-user functions. Regarding T-U2, this reference point is not applicable since used to connect PSTN/ISDN terminals to the AMG-FE. C-U1 and C-U2 reference points do not terminate in CPN-GW but in NGN terminals connected to the CPN-GW (e.g., IPTV terminal function in the case of IPTV services provided by NGN, see [ITU-T Y.1910]). TC-U1, TC-U2 and TC-U3 reference points terminate in NGN mobile capable UEs according to [ITU-T Y.2018].

9.3.6.1.1 U-1: CPN gateway service control functional entity (CGSC-FE)

The use of this functional entity is optional. Depending on the services supported, a CPN gateway may include one or more service control functional entities (CGSC-FE), such as a SIP based controlling entity acting as an outbound SIP proxy, a SIP access point to the NGN P-CSC-FE.

9.3.6.1.2 U-2: CPN gateway network attachment functional entity (CGNA-FE)

The CPN gateway network attachment functional entity (CGNA-FE) handles the allocation of IP address to the CPN gateway from the NAC-FE via the AR-FE.

9.3.6.1.3 U-3: CPN gateway configuration and management functional entity (CGCM-FE)

The CPN gateway configuration and management functional entity (CGCM-FE) enables the CPN gateway configuration and firmware upgrade. It also manages a mutual authentication between the HGWC-FE and the CPN gateway.

Through the TC-Ux reference point, it is possible to support a variety of functionalities to manage a collection of user equipments (CPN gateway and end-user devices).

9.3.6.1.4 U-4: CPN gateway policy decision functional entity (CGPD-FE)

The CPN gateway policy decision functional entity (PD-FE) makes decisions in the CPN gateway regarding network resource and admission control.

In particular, the CGPD-FE provides gate control functionality, i.e., dynamic NAPT and firewall functions at the boundary between the CPN gateway and the NGN.

For further details, refer to [ITU-T Y.2111].

9.3.6.1.5 U-5: CPN gateway policy enforcement functional entity (CGPE-FE)

The CPN gateway policy enforcement functional entity (CGPE-FE) in the end-user functions enforces the transport policy rules for upstream traffic instructed by the RACF PD-FE.

For further details, refer to [ITU-T Y.2111].

9.3.7 Identity management functions

The IdM functions provide the coordination and the control of the identity information and data (e.g., identifiers, credentials and attributes) for identity assurance purposes, enabling and supporting business, social networking and security services, and applications, including identity and federated identity services and applications.

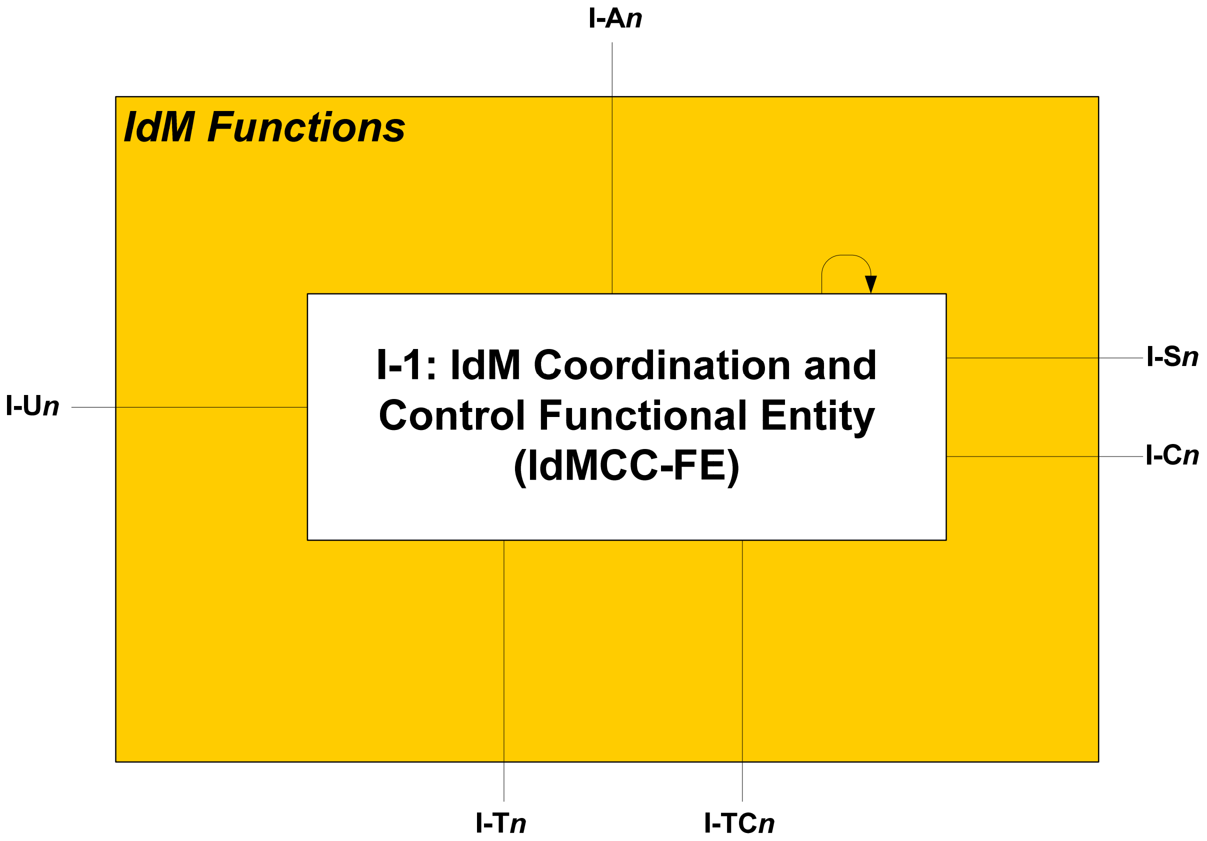

I-An
IdM Functions
I-1: IdM Coordination and Control Functional Entity (IdMCC-FE)
I-Un
I-Sn
I-Cn
I-Tn
I-TCn

Figure 9-8 – IdM functional entities

Appendix IV provides an example illustrative deployment scenario for IdM in NGN.

9.3.7.1 I-1: IdM coordination and control functional entity (IdMCC-FE)

The IdM coordination and control functional entity (IdMCC-FE) supports coordination and control functions and interactions with other FEs as appropriate to provide assurance of identity information (e.g., identifiers, credentials and attributes) associated to an entity such as user/subscriber, device, network element, data, object, service provider, or application process. Example of specific functions and capabilities provided by the IdMCC-FE include, but is not limited to:

- discovery of identity information within an NGN provider domain, among other networks (i.e., via NNI) and among other service providers (i.e., via SNI);
- correlation and binding of identity information (e.g., identity data from application support functions, service support functions, service control functions, content delivery functions, transport control functions, transport functions and end-user functions);
- communicate and exchange identity information and assertions (i.e., across UNI, ANI, NNI and SNI) to support IdM services and capabilities (e.g., single sign-on/single sign-off among multiple services and applications, and federated identity services among multiple service providers);
- enforcement of applicable policies and rules for IdM (e.g., protection of personally identifiable information (PII) and national regulatory rules);
- authentication assurance (e.g., functions and operational processes to provide confidence in authentication);
- bridging and interworking functions to facilitate interoperability between different types of IdM systems and federations that are using different semantics, schemas, mechanisms and technologies;

- end user/subscriber indications of preferences about the use and dissemination of their identity information.

Figure 9-8 illustrates the general concept that the IdMCC-FE may interact with specific functional entities (FEs) to enable and support services and applications including identity and federated identity services and applications. This may include interactions with FEs in the following functional blocks, depending on the specific IdM service or capability being supported and the implementation design:

a) Application support functions and service support functions: The IdMCC-FE may interact with the following functional entities via appropriate I-A*n* reference points:
   - A-1: Application support functional entity (AS-FE);
   - A-2: Application gateway functional entity – interfaces to external applications (APL-GW-FE);
   - A-3: Application service coordination manager functional entity (APL-SCM-FE);
   - A-5: Application support user profile functional entity (ASUP-FE);
   - A-8: Service and content protection functional entity (SCP-FE).

b) Service control functional entities: The IdMCC-FE may interact with the following service control functional entities via appropriate I-S*n* reference points:
   - S-1: Serving call session control functional entity (S-CSC-FE);
   - S-2: Proxy call session control functional entity (P-CSC-FE);
   - S-3: Interrogating call session control functional entity (I-CSC-FE);
   - S-4: Subscription locator functional entity (SL-FE);
   - S-5: Service user profile functional entity (SUP-FE);
   - S-6: Service authentication and authorization functional entity (SAA-FE);
   - S-7: Interconnection border gateway control functional entity (IBGC-FE);
   - S-8: Access gateway control functional entity (AGC-FE);
   - S-15: General services control functional entity (GSC-FE).

c) Content delivery functional entities: The IdMCC-FE may interact with the following content delivery functional entities via appropriate I-C*n* reference points:
   - C-1 Content distribution & location control functional entity (CD&LC-FE);
   - C-2 Content delivery control functional entity (CDC-FE).

d) Transport functional entities: The IdMCC-FE may interact with the following transport functional entities via an appropriate I-T*n* reference point:
   - T-5 Access border gateway functional entity (ABG-FE);
   - T-6 Interconnection border gateway functional entity (IBG-FE);
   - Policy enforcement functional entity (PE-FE) (see Figure 9-2).

e) Transport control functional entities: The IdMCC-FE may interact with the following transport control functional entities via an appropriate I-TC*n* reference point:
   - T-10: Network access configuration functional entity (NAC-FE);
   - T-11: Transport authentication and authorization functional entity (TAA-FE);
   - T-12: Transport user profile functional entity (TUP-FE);
   - T-13: Transport location management functional entity (TLM-FE);
   - T-14: Access management functional entity (AM-FE);
   - T-16: Policy decision functional entity (PD-FE);

- T-18: Mobile location management functional entity (MLM-FE);
- T-21: Network information repository functional entity (NIR-FE).

f) End user functional entities: The IdMCC-FE may interact with the following functional entities via an appropriate I-U*n* reference point:
   - U-1: CPN gateway service control functional entity (CGSC-FE);
   - U-2: CPN gateway network attachment functional entity (CGNA-FE);
   - U-3: CPN gateway configuration and management functional entity (CGCM-FE);
   - U-4: CPN gateway policy decision functional entity (CGPD-FE);
   - U-5: CPN gateway policy enforcement functional entity (CGPE-FE).

g) Management functions: The IdMCC-FE may interact with the management functions for OAMP via appropriate I-M*n* reference points.

9.4 Reference points

This clause provides the list of reference points defined in the NGN functional architecture. For each reference point, the involved functional entities are identified.

9.4.1 Reference points to/from ASF&SSF

9.4.1.1 Reference points between ASF&SSF and SC&CDF

9.4.1.1.1 Reference points between ASF&SSF and SCF

The reference points between ASF&SSF and SCF are as follows:

- Reference point A-S1 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and S-14 MRB-FE in SCF;
- Reference point A-S2 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and S-15 GSC-FE in SCF;
- Reference point A-S3 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and S-13 MRC-FE in SCF;
- Reference point A-S4 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and S-1 S-CSC-FE in SCF;
- Reference point A-S5 between the functional entities in ASF&SSF and S-6 SAA-FE in SCF;
- Reference point A-S6 between the functional entities in ASF&SSF and S-5 SUP-FE/S-4 SL-FE in SCF;
- Reference point A-S7 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and S-3 I-CSC-FE in SCF.

9.4.1.1.2 Reference points between ASF&SSF and CDF

The reference points between ASF&SSF and CDF are as follows:

- Reference point A-C1 between A-1 AS-FE and A-2 APL-GW-FE in ASF&SSF and C-1 CD&LC-FE in CDF;
- Reference point A-C2 between A-7 CPR-FE in ASF&SSF and C-1 CD&LC-FE in CDF;
- Reference point A-C3 between A-7 CPR-FE in ASF&SSF and C-2 CDP-FE in CDF.

9.4.1.2 Reference points between ASF&SSF and end-user functions

The reference points between ASF&SSF and end-user functions are as follows:

- Reference point A-U1 between A-1 AS-FE, A-2 APL-GW-FE, A-3 APL-SCM-FE and A-4 SS-FE in ASF&SSF and end-user functions;
- Reference point A-U2 between A-8 SCP-FE in ASF&SSF and end-user functions.

9.4.1.3 Reference points between ASF&SSF and content provider functions

The reference point between ASF&SSF and content provider functions is as follows:

- Reference point A-ON1 between A-7 CPR-FE and content provider functions.

9.4.1.4 Reference points between ASF&SSF and transport processing functions

The reference point between ASF&SSF and transport processing functions is as follows:

- Reference point A-T1 between A-4 SS-FE in ASF&SSF and T-9 SG-FE in the transport processing functions.

9.4.1.5 Reference points internal to ASF&SSF

The reference points within ASF&SSF are as follows:

- Reference point between A-1 AS-FE and A-3 APL-SCM-FE. Multiple A-1 AS-FEs can interwork with each other via APL-SCM-FE (application service coordination manager functional entity) to provide coordinated services to the end users;
- Reference point between A-1 AS-FE and A-6 APP-FE. With this reference point, the application provisioning functional entity (APP-FE) adds or withdraws application support functional entities (AS-FEs) and manages the life-cycle of the applications supported by the AS-FEs;
- Reference point between A-2 APL-GW-FE and A-5 ASUP-FE. This reference point allows the APL-GW-FE to interact with the ASUP-FE in order that APL-GW-FE provides a secure open interface for the applications to use the capabilities and resources of the ASUP-FE;
- Reference point between A-1 AS-FE and A-5 ASUP-FE. With this reference point, the AS-FE can access the profiles contained in the ASUP-FE;
- Reference point between A-5 ASUP-FE and A-8 SCP-FE. With this reference point, the service and content protection functional entity (SCP-FE) can interact with the application support user profile functional entity (ASUP-FE) to retrieve user related security subscription information;
- Reference point between A-7 CPR-FE and A-8 SCP-FE. With this reference point, the content preparation functional entity (CPR-FE) can optionally pre-process (e.g., transcode or edit) the content before passing it to the content delivery functions, associated with service and content protection functional entity (SCP-FE).

9.4.2 Reference points to/from SC&CDF

9.4.2.1 Reference points between SCF and end-user functions

The reference points between SCF and end-user functions are as follows:

- Reference point S-U1 between S-2 P-CSC-FE in SCF and end-user functions;
- Reference point S-U2 between S-11 USIW-FE in SCF and end-user functions;
- Reference point S-U3 between S-15 GSC-FE in SCF and end-user functions.

9.4.2.2 Reference points between SCF and transport processing functions

The reference points between SCF and transport processing functions are as follows:

- Reference point S-T1 between S-13 MRC-FE in SCF and T-8 MRP-FE in transport processing functions;
- Reference point S-T2 between S-8 AGC-FE in SCF and T-1 AMG-FE in transport processing functions;
- Reference point S-T3 between S-9 MGC-FE in SCF and T-9 SG-FE in transport processing functions;
- Reference point S-T4 between S-9 MGC-FE in SCF and T-7 TMG-FE in transport processing functions;
- Reference point S-T5 between S-7 IBG-FE in SCF and T-6 IBG-FE in transport processing functions.

9.4.2.3 Reference points between SCF and transport control functions

9.4.2.3.1 Reference points between SCF and NACF

The reference point between SCF and NACF is as follows:

- Reference point S-TC1 between S2 P-CSC-FE and GSC-FE in SCF and T-13 location management FE in NACF.

9.4.2.3.2 Reference points between SCF and MMCF

None identified in this Recommendation.

9.4.2.3.3 Reference points between SCF and RACF

The reference points between SCF and RACF are as follows:

- Reference point S-TC2 between S-2 P-CSC-FE/S-15 GSC-FE in SCF and T-16 PD-FE in RACF;
- Reference point S-TC3 between S-8 AGC-FE in SCF and T-16 PD-FE in RACF;
- Reference point S-TC4 between S-9 MGC-FE in SCF and T-16 PD-FE in RACF;
- Reference point S-TC5 between S-7 IBG-FE in SCF and T-16 PD-FE in RACF.

9.4.2.4 Reference points between SCF and other networks

The reference points between SCF and other networks are as follows:

- Reference point S-ON1 between S-12 NSIW-FE and other networks;
- Reference point S-ON2 between S-7 IBG-FE and other networks.

9.4.2.5 Reference points between CDF and transport processing functions

The reference points between CDF and transport processing functions are as follows:

- Reference point C-T1 between C-3 CDP-FE in CDF and transport processing functions. This reference point is used for multicast control;
- Reference point C-T2 between C-3 CDP-FE and transport processing functions. This reference point is used for both the transport of unicast and multicast.

9.4.2.6 Reference points between CDF and end-user functions

The reference points between CDF and end-user functions are as follows:

- Reference point C-U1 between C-2 CDC-FE in CDF and end-user functions;

- Reference point C-U2 between C-3 CDP-FE in CDF and end-user functions. This reference point is used for the support of error recovery mechanisms between the end-user functions and CDF.

9.4.2.7 Reference points between SC&CDF and ASF&SSF

Refer to clause 9.4.1.1.

9.4.2.8 Reference points internal to SC&CDF

The reference points between SCF and CDF are as follows:

- Reference point S-C1 between S-1 S-CSC-FE in SCF and C1 CD&LC-FE in CDF;
- Reference point S-C2 between S-1 S-CSC-FE in SCF and C2 CDC-FE in CDF;
- Reference point S-C3 between S-15 GSC-FE in SCF and C-1 CD&LC-FE in CDF;
- Reference point S-C4 between S-15 GSC-FE in SCF and C-2 CDC-FE in CDF.

NOTE – In the case of IPTV services, S-C1 and S-C2 are meant to be used for the IMS IPTV case (i.e., connected to S-CSC-FE), while S-C3 and S-C4 are meant to be used for the non-IMS IPTV (i.e., connected to GSC-FE).

9.4.3 Reference points to/from transport control functions

9.4.3.1 Reference points between transport control functions and end-user functions

The reference points between transport control functions and end-user functions are as follows:

- Reference point TC-Ux between T-15 HGWC-FE in NACF and end-user functions;
- Reference point TC-U1 between T-18 MLM-FE in MMCF and end-user functions;
- Reference point TC-U2 between T-19 HDC-FE in MMCF and end-user functions;
- Reference point TC-U3 between T-20 NID-FE in MMCF and end-user functions;
- Reference point TC-U4 between T-16 PD-FE in RACF and U-4 CGPD-FE in end-user functions.
- Reference point TC-U5 between T-16 PD-FE in RACF and U-5 CGPE-FE in end-user functions.

9.4.3.2 Reference points between transport control functions and transport processing functions

9.4.3.2.1 Reference points between NACF and transport processing functions

The reference point between NACF and transport processing functions is as follows:

- Reference point TC-T1 between T-14 AM-FE in NACF and T-4 AR-FE in transport processing functions.

9.4.3.2.2 Reference points between MMCF and transport processing functions

The reference points between MMCF and transport processing functions are as follows:

- Reference point TC-T7 between T-19 HDC-FE in MMCF and T-22 L2HE-FE in transport processing functions;
- Reference point TC-T8 between T-19 HDC-FE in MMCF and T-3 EN-FE, T-5 ABG-FE and T-6 IBG-FE in transport processing functions.

9.4.3.2.3 Reference points between RACF and transport processing functions

The reference points between RACF and transport processing functions are as follows:

- Reference point TC-T2 between T-16 PD-FE in RACF and T-2 AN-FE in transport processing functions;

- Reference point TC-T3 between T-17 TRC-FE in RACF and access transport processing functions;
- Reference point TC-T4 between T-17 TRC-FE in RACF and core transport processing functions;
- Reference point TC-T5 between T-16 PD-FE in RACF and T-3 EN-FE in transport processing functions;
- Reference point TC-T6 between T-16 PD-FE in RACF and T-5 ABG-FE in transport processing functions;
- Reference point TC-T9 between T-16 PD-FE in RACF and T-6 IBG-FE in transport processing functions.

9.4.3.3 Reference points between transport control functions and other NGNs

The reference point between transport control functions and other NGNs is as follows:

- Reference point TC-ON1 between T-16 PD-FE and other NGNs.

9.4.3.4 Reference points between transport control functions and other IP multimedia networks

The reference point between transport control functions and other IP multimedia networks is as follows:

- Reference point TC-ON1 between T-16 PD-FE and other IP multimedia networks. It is the same reference point as the one between T-16 PD-FE and other NGNs.

9.4.3.5 Reference points internal to transport control functions

The reference points internal to transport control functions are as follows:

- Reference point TC-TC1 between T-13 TLM-FE in NACF and T-16 PD-FE in RACF;
- Reference point TC-TC2 between T-13 TLM-FE in NACF and T-18 MLM-FE in MMCF;
- Reference point TC-TC3 between T-13 TLM-FE in NACF and T-19 HDC-FE in MMCF;
- Reference point TC-TC4 between T-13 TLM-FE in NACF and T-20 NID-FE in MMCF;
- Reference point TC-TC5 between T-16 PD-FE in RACF and T-19 HDC-FE in MMCF;
- Reference points inside NACF. These are described in [ITU-T Y.2014];
- Reference points inside RACF. These are described in [ITU-T Y.2111];
- Reference points inside MMCF. These are described in [ITU-T Y.2018].

9.4.3.6 Reference points to/from transport processing functions

9.4.3.6.1 Reference points between transport processing functions and end-user functions

The reference points between transport processing functions and end-user functions are as follows:

- Reference point T-U1 between T-4 AR-FE in transport processing functions and end-user functions;
- Reference point T-U2 between T-1 AMG-FE in transport processing functions and end-user functions;
- Reference point T-U3 between T-2 AN-FE in transport processing functions and end-user functions;
- Reference point T-U4 between AN-FE or EN-FE or any relevant FE in transport processing functions (which includes a multicast control point function [ITU-T Y.2017]) and end-user functions.

9.4.3.6.2 Reference points between transport processing functions and PSTN/ISDN

The reference points between transport processing functions and PSTN/ISDN are as follows:

- Reference point T-ON1 is between T-9 SG-FE in transport processing functions and PSTN/ISDN;
- Reference point T-ON3 is between T-7 TMG-FE in transport processing functions and PSTN/ISDN.

9.4.3.6.3 Reference points between transport processing functions and another NGN

The reference point between transport processing functions and another NGN is as follows:

- Reference point T-ON2 is between T-6 IBG-FE in transport processing functions and another NGN.

9.4.3.6.4 Reference points between transport processing functions and another IP multimedia network

The reference point between transport processing functions and another multimedia network is as follows:

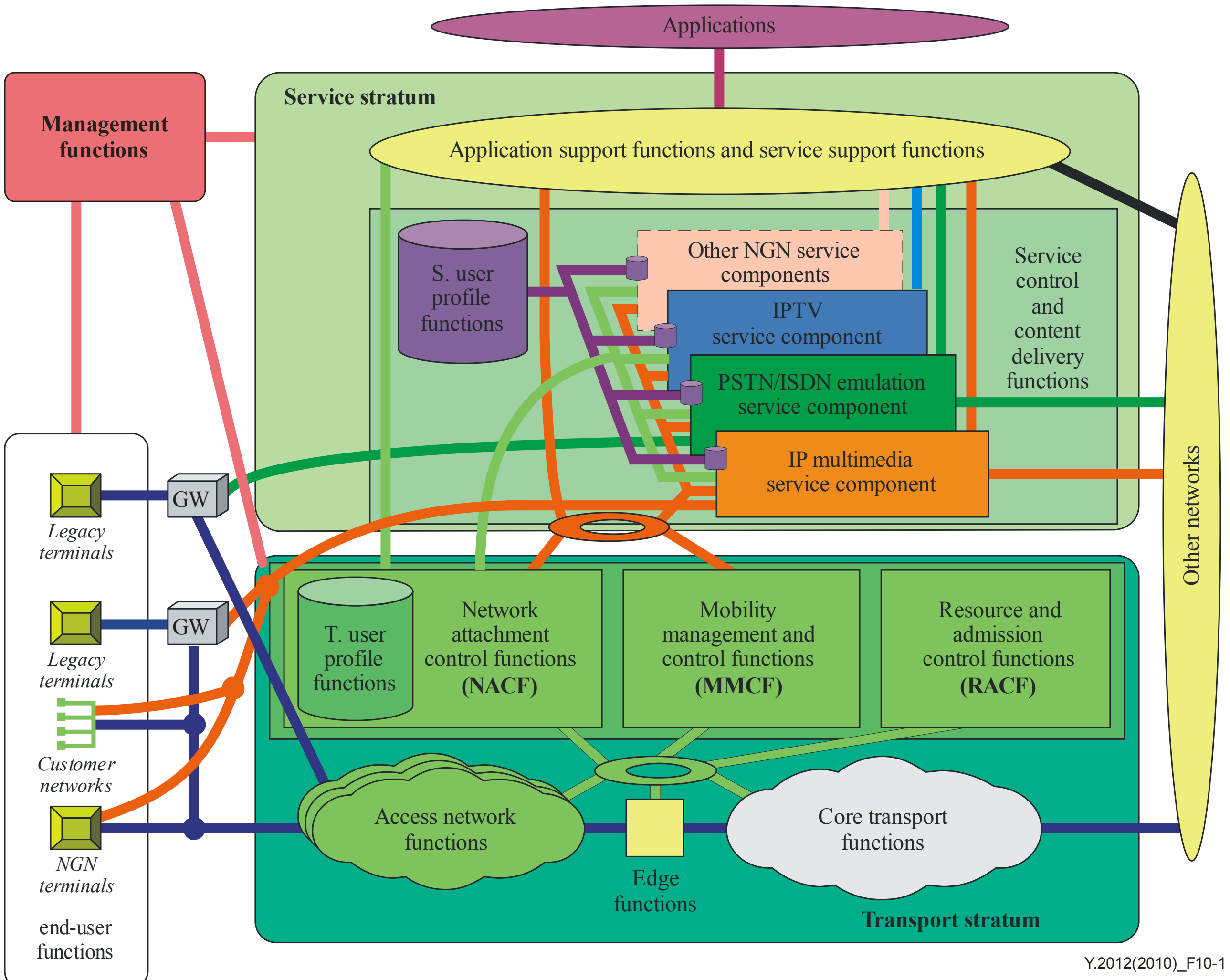
- Reference point T-ON2 is between T-6 IBG-FE in transport processing functions and another IP multimedia network.

10 NGN components

This clause introduces the concept of NGN components, derived from the generalized NGN functional architecture specified in clause 9.

Figure 10-1 shows a representation of NGN including these components. The components shown overlap and may share functionality.

The exact functionality and interface associated with each FE and the reference points in these components are described in other documents specifically covering each component.


Applications
Management functions
Service stratum
Application support functions and service support functions
S. user profile functions
Other NGN service components
IPTV service component
PSTN/ISDN emulation service component
IP multimedia service component
Service control and content delivery functions
Other networks
GW
Legacy terminals
GW
Legacy terminals
Customer networks
NGN terminals
end-user functions
T. user profile functions
Network attachment control functions (NACF)
Mobility management and control functions (MMCF)
Resource and admission control functions (RACF)
Access network functions
Edge functions
Core transport functions
Transport stratum
Y.2012(2010)_F10-1

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

Figure 10.1 – NGN components

For the sake of easy understanding, the representation shown in Figure 10-1 makes use of shading in a supplementary manner, to group and collate components in service control functions which are related.

The components are related to each other and may contain common or shared functionality. No assumptions should be made concerning their representation as separate components in the figure.

Three components are identified in the service stratum:

- The IP multimedia service component provides mediated services, including the control and delivery of real-time conversational services based on the use of the IMS. The IMS is extended in NGN to support additional access network types, such as xDSL and WLAN. PSTN/ISDN simulation service is also provided by this component.
- The PSTN/ISDN emulation service component provides all of the network functionality associated with supporting existing services for legacy end-user interfaces and equipment.
- The IPTV service component provides all of the network functionality associated with supporting IPTV services.

Other NGN service components (shown as a dotted box) will be defined in the future to address other services.

Three components are identified in the transport stratum: the network attachment control functions (NACF) component, the resource and admission control functions (RACF) component and the mobility management and control functions (MMCF) component.

Physical transport networks provide the connectivity for all components and physically separated functions within the NGN. Transport is divided into access transport networks and the core transport network, with a border gateway linking the two transport network categories.

IP connectivity is provided to the NGN end-user equipment by the transport functions, under the control of the NACF, the RACF and the MMCF components.

In the transport stratum, multiple configurations regarding access transport functions are possible. Figure 10-1 also represents the compilation of user information and other control-related data into two functions: "service user profile" and "transport user profile" functions. These functions may be specified and realized as a set of cooperating databases with functionality residing in any part of the NGN.

End-user interfaces are supported by both physical and functional (control) interfaces, and both are shown in the figure. No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. End-user equipment may be either mobile or fixed.

The NGN interface(s) to other networks includes many existing networks, such as PSTN/ISDN and the public Internet. The NGN interfaces other networks both at the service stratum level and at the transport stratum level, by using border gateways. The border gateways can optionally involve media transcoding and bearer adaptation. Interactions between the service stratum and the transport stratum may take place, either directly or through the RACF.

10.1 NGN service-specific components

10.1.1 IP multimedia service component

The IP multimedia service component supports mediated multimedia services. These services may include multimedia session services, such as voice or video telephony or PSTN/ISDN simulation, and some non-session services, such as subscribe/notify for presence information and the message method for message exchange. In contrast to the emulation service described in clause 10.1.2 below, the PSTN/ISDN simulation service refers to the provision of PSTN/ISDN-like services to advanced terminals such as IP phones.

The IP multimedia service component is specified further in [ITU-T Y.2021].

10.1.2 PSTN/ISDN emulation service component

The PSTN/ISDN emulation refers to the provision of PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure. The PSTN/ISDN emulation service component enables the support of legacy terminals connected through a gateway to an IP network. All PSTN/ISDN services remain available and identical (i.e., with the same operating characteristics), such that end users are unaware that they are not connected to a TDM-based PSTN/ISDN. Not all service capabilities and interfaces have to be present to provide PSTN/ISDN emulation.

By contrast, PSTN/ISDN simulation refers to the provision of PSTN/ISDN-like services to advanced terminals such as IP phones. The IP multimedia service component described in clause 10.1.1 may provide such simulation services.

The PSTN/ISDN emulation service component is specified further in [ITU-T Y.2031].

10.1.3 IPTV service component

The IPTV service component is described in Annex B.

10.1.4 Other NGN service components

The definition of other NGN service-specific components is for further study. Service specific components may be required in order for the NGN to support services such as push services, data retrieval applications, data communication services, online applications, sensor network services, remote control services, and over-the-network device management.

10.2 NGN transport-specific components

10.2.1 NACF component

The NACF component is specified in [ITU-T Y.2014].

10.2.2 RACF component

The RACF component is specified in [ITU-T Y.2111].

10.2.3 MMCF component

The MMCF component is specified in [ITU-T Y.2018].

10.2.4 Other NGN transport components

Because the NGN supports several types of access networks, specific components for access transport functions exist in the transport stratum. These include fixed access with a wire line, fixed access with a wireless LAN, and cellular access. Note that Appendix II identifies further transport stratum access network scenarios.

The definition of access specific transport components is for further study.

10.3 Management functions

Five different types of functions are included in this component, i.e., functions related to fault management, configuration management, accounting management, security management and performance management.

The MPM function as defined in [ITU-T Y.2173] provides functions within the performance management functions.

The charging and accounting functions defined in [ITU-T Y.2233] provide functions within the accounting management functions.

11 Security considerations

The security requirements within the functional requirements and architecture of the NGN are addressed by the security requirements for NGN in [ITU-T Y.2701].

Annex A

Differences between this edition and the 2006 edition of Recommendation ITU-T Y.2012

(This annex forms an integral part of this Recommendation)

This annex identifies the main differences between this edition and the 2006 edition of Recommendation ITU-T Y.2012.

This Recommendation provides the following additional functional features as compared to the 2006 edition of Recommendation ITU-T Y.2012:

– Introduction of the SNI reference point in the NGN architecture;

– Support for mobility in the transport stratum via the introduction of the MMCF component in the NGN architecture and related functional entities HDC-FE, MLM-FE, NID-FE and NIR-FE defined in [ITU-T Y.2018];

– Introduction of content delivery functions and related functional entities described in clause 9.3.4, i.e., CDP-FE, CDC-FE and CD&LC-FE;

– Introduction of new functional entities in the ASF&SSF (clause 9.3.5), i.e., CPR-FE, ASUP-FE, APP-FE and SCP-FE that can be used for the support of IPTV services;

– Details of CPN gateway functions and related functional entities as per clause 9.3.6;

– Introduction of identity management functions and related functional entities (i.e., IdMCC-FE) in the NGN architecture; a new appendix shows an example illustration of IdM in NGN;

– Introduction of a new annex regarding the support of IPTV services in NGN. This annex provides the mapping between functions and functional blocks defined in [ITU-T Y.1910] and NGN functions and functional entities defined in this Recommendation;

– Introduction of functional entities regarding forwarding in the transport functions, i.e., EF-FE and EC-FE. This Recommendation describes the use of these functional entities for the support of multicast in the NGN transport stratum and its relationship with [ITU-T Y.2017];

– Addition of the management of performance measurement (MPM) in the management functions. MPM functions are described in [ITU-T Y.2173].

Annex B

Support of IPTV services

(This annex forms an integral part of this Recommendation)

This annex describes the correspondence between the NGN functional architecture, as described in this Recommendation, and the NGN-based IPTV functional architectures, as described in [ITU-T Y.1910]. The NGN-based IPTV functional architectures considered in this annex are the IMS-based IPTV architecture and the non-IMS-based IPTV architecture. As a result, this annex provides an overall view of the IPTV service component as shown in Figure 10-1.

The IPTV functional architectures described in [ITU-T Y.1910] identify functions and functional blocks for the support of IPTV services, while this Recommendation describes NGN functions and functional entities.

B.1 Overall functional mapping between NGN-based IPTV and NGN architectures

The NGN-based IPTV architectures defined in [ITU-T Y.1910] are in accordance with this Recommendation for providing IPTV services. Therefore, the functionalities defined in [ITU-T Y.1910] have a corresponding relationship with the NGN architecture.

Application functions in NGN-based IPTV architecture [ITU-T Y.1910] are included in application support functions and service support functions of NGN shown in Figure 7-1. Service control functions and content delivery functions defined in [ITU-T Y.1910] are included in the NGN service control and content delivery functions as shown in Figure 7-1. Thus, application functions, service control functions, and content delivery functions are included in the service stratum of the NGN architecture. Although this Recommendation assumes that content delivery functions are located inside the NGN, content delivery functions can optionally reside outside of the NGN.

Table B.1 provides the relationship between the functions of NGN-based IPTV functional architecture [ITU-T Y.1910] and the NGN functional architecture described in this Recommendation.

Table B.1 – Functional mapping between NGN-based IPTV and NGN functional architectures

No.	NGN-based IPTV functional architectures [ITU-T Y.1910]	NGN functional architecture	Remarks
1	Network functions	Transport stratum	These correspond to each other.
2	End-user functions	End-user functions	These correspond to each other.
3	Management functions	Management functions	These correspond to each other.
4	Service control functions	Service control functions (in-service stratum)	IPTV service control functional block [ITU-T Y.1910] corresponds to NGN service control functions. However, NGN service control functions can optionally include other functionalities.

Table B.1 – Functional mapping between NGN-based IPTV and NGN functional architectures

No.	NGN-based IPTV functional architectures [ITU-T Y.1910]	NGN functional architecture	Remarks
5	Content delivery functions	Content delivery functions (in-service stratum)	Content delivery functions can optionally reside outside the NGN.
6	Application functions	Application support functions & service support functions (in-service stratum)	Application functions can optionally reside outside the NGN.
7	Content provider functions	Content provider functions	Content provider functions reside outside the NGN.

B.2 IMS-based IPTV functional architecture

B.2.1 Functional mapping

Table B.2 describes the functional mapping between the functional blocks and the functions defined in [ITU-T Y.1910], and the NGN functional entities or functions defined in this Recommendation for the support of the IMS-based IPTV functional architecture.

Table B.2 – IMS-based architecture

[ITU-T Y.1910]	NGN Functional Entity (FE)
Linear TV Application FB	Instantiation of A-1: Application Support FE for Linear TV
On Demand Application FB	Instantiation of A-1: Application Support FE for On Demand Application
Other Application FB	Instantiation of A-1: Application Support FE for Other IPTV Application
Service and Application Discovery and Selection FB	Instantiation of A-1: Application Support FE for Service and Application Discovery and Selection
Application Profile FB	A-5: Application Support User Profile FE
Application Provisioning FB	A-6: Application Provisioning-FE
Content Preparation Functions	A-7: Content Preparation FE
Service and Content Protection Functions	A-8: Service and Content Protection FE
Content Distribution and Location Control Functions	C-1: Content Distribution and Location Control FE
Content Delivery and Storage Functions	C-2: Content Delivery Control FE C-3: Content Delivery Processing FE
Core IMS Functions	Supported by the following: S-1: Serving Call Session Control FE S-2: Proxy Call Session Control FE S-3: Interrogating Call Session Control FE
Service User Profile FB	S-5: Service User Profile FE

Table B.2 – IMS-based architecture

[ITU-T Y.1910]	NGN Functional Entity (FE)
NACF	NACF
RACF	RACF
Multicast Replication FB	Multicast capable EF-FE in transport processing FEs
Multicast Control Point FB	Multicast capable EC-FE in transport processing FEs
Delivery Network Gateway FB	CPN Gateway Functions

B.2.2 Reference points

Table B.3 describes the mapping between reference points in [ITU-T Y.1910] and NGN reference points defined in this Recommendation for the support of the IMS-based IPTV architecture.

Table B.3 – Reference points – IMS based IPTV architecture

[ITU-T Y.1910] reference point	NGN reference point
E0	A-U1 reference point between instantiated AS-FE for SADS and end-user functions
E1	A-U1 reference point between instantiated AS-FE for IPTV application (e.g., Linear TV) and end-user functions
E2	A-U2 reference point between SCP-FE and end-user functions
E3	S-U1 reference point between P-CSC-FE and end-user functions
E4	C-U2 reference point between CDP-FE and end-user functions
E5	T-U4 reference point between relevant FE (e.g., AN-FE, EN-FE, etc.) in transport processing functions and end-user functions
E6	C-U1 reference point between CDC-FE and end-user functions
A0	A-S4 reference point between S-CSC-FE and instantiated AS-FE for SADS
A1	A-S4 reference point between S-CSC-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-2	AC-1 reference point between CD&LC-FE and instantiated AS-FE for IPTV application (e.g., linear TV)
A-3	Reference point between CPR-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-4	Reference point between APP-FE and instantiated AS-FE for SADS
A-5	Reference point between APP-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-6	Reference point between SCP-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
C-1	A-C2 reference point between CPR-FE and CD&LC-FE
C-2	A-C3 reference point between CPR-FE and CDP-FE
C-3	Reference point between CPR-FE and SCP-FE
D-1	Reference point between CD&LC-FE and CDC-FE
H-1	T-U1 reference point between end-user functions and AR-FE
H-2	T-U3 reference point between AN-FE and end-user functions (to transport multicast flows)

Table B.3 – Reference points – IMS based IPTV architecture

[ITU-T Y.1910] reference point	NGN reference point
H-3	T-U3 reference point between AN-FE and end-user functions (to transport unicast flows)
M-1	Reference point between SCP-FE and APP-FE
Mc	C-T1 reference point between CDP-FE and transport functions
Md	C-T2 reference point between CDP-FE and transport functions
S-1	S-C1 reference point between core IMS and CD&LC-FE
S-2	Reference point between S-CSC-FE and SAA-FE (Cx reference point)
S-3	Rs reference point between P-CSC-FE and RACF
S-4	S-TC1 reference point between P-CSC-FE and NACF
S-5	S-C2 reference point between core IMS and CDC-FE
T-1	TC-T1 reference point between P-CSC-FE and NACF
Ud	C-T2 reference point between CDP-FE and transport functions

B.3 Non-IMS-based IPTV architecture

B.3.1 Functional mapping

Table B.4 describes the functional mapping between the functional blocks and the functions defined in [ITU-T Y.1910], and the NGN functional entities or functions defined in this Recommendation for the support of the non-IMS-based IPTV architecture.

Table B.4 – Non-IMS-based IPTV architecture

[ITU-T Y.1910] Functional Block or Functions	NGN functional entity (FE) or NGN functions
Linear TV Application FB	Instantiation of A-1: Application Support FE for Linear TV
On Demand Application FB	Instantiation of A-1: Application Support FE for On Demand Application
Other Application FB	Instantiation of A-1: Application Support FE for Other IPTV Application
Service and Application Discovery and Selection FB	Instantiation of A-1: Application Support FE for Service and Application Discovery and Selection
Application Profile FB	A-5: Application Support User Profile FE
Application Provisioning FB	A-6: Application Provisioning-FE
Content Preparation Functions	A-7: Content Preparation FE
Service and Content Protection Functions	A-8: Service and Content Protection FE
Content Distribution and Location Control Functions	C-1: Content Distribution and Location Control FE
Content Delivery and Storage Functions	C-2: Content Delivery Control FE C-3: Content Delivery Processing FE
IPTV Service Control FB	Instantiation of S-15: General Services Control FE for IPTV service control
Service User Profile FB	S-5: Service User Profile FE

Table B.4 – Non-IMS-based IPTV architecture

[ITU-T Y.1910] Functional Block or Functions	NGN functional entity (FE) or NGN functions
NACF	NACF
RACF	RACF
Multicast Replication FB	Multicast capable EF-FE in transport processing FEs
Multicast Control Point FB	Multicast capable EC-FE in transport processing FEs
Delivery Network Gateway FB	CPN Gateway Functions

B.3.2 Reference points

Table B.5 describes the mapping between reference points defined in [ITU-T Y.1910] and NGN reference points defined in this Recommendation for the support of the non-IMS-based IPTV architecture.

Table B.5 – Reference points – non-IMS-based IPTV architecture

[ITU-T Y.1910] reference point	NGN reference point
E0	A-U1 reference point between instantiated AS-FE for SADS and end-user functions
E1	A-U1 reference point between instantiated AS-FE for IPTV application (e.g., Linear TV) and end-user functions
E2	A-U2 reference point between SCP-FE and end-user functions
E3	S-U3 reference point between instantiated GSC-FE for IPTV service control and end-user functions
E4	C-U2 reference point between CDP-FE and end-user functions
E5	T-U4 reference point between relevant FE (e.g., AN-FE, EN-FE, etc.) in transport processing functions and end-user functions
E6	C-U1 reference point between CDC-FE and end-user functions
A1	A-S4 reference point between instantiated GSC-FE for IPTV service control and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-2	AC-1 reference point between CD&LC-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-3	Reference point between CPR-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-4	Reference point between APP-FE and instantiated AS-FE for SADS
A-5	Reference point between APP-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
A-6	Reference point between SCP-FE and instantiated AS-FE for IPTV application (e.g., Linear TV)
C-1	A-C2 reference point between CPR-FE and CD&LC-FE
C-2	A-C3 reference point between CPR-FE and CDP-FE
C-3	Reference point between CPR-FE and SCP-FE
D-1	Reference point between CD&LC-FE and CDC-FE
H-1	T-U1 reference point between end-user functions and AR-FE
H-2	T-U3 reference point between AN-FE and end-user functions (to transport multicast

Table B.5 – Reference points – non-IMS-based IPTV architecture

[ITU-T Y.1910] reference point	NGN reference point
	flows)
H-3	T-U3 reference point between AN-FE and end-user functions (to transport unicast flows)
M-1	Reference point between SCP-FE and APP-FE
Mc	C-T1 reference point between CDP-FE and transport functions
Md	C-T2 reference point between CDP-FE and transport functions
S-1	S-C3 reference point between instantiated GSC-FE and CD&LC-FE
S-2	Reference point between instantiated GSC-FE and SAA-FE
S-3	Rs reference point between instantiated GSC-FE and RACF
S-4	S-TC1 reference point between instantiated GSC-FE and NACF
S-5	S-C4 reference point between instantiated GSC-FE and CDC-FE
T-1	TC-T1 reference point between instantiated GSC-FE and NACF
Ud	C-T2 reference point between CDP-FE and transport functions

Appendix I

Examples of NGN network configurations

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

NOTE – In this appendix, the terms "NGN core" and "NGN access" are used only for convenience and are not intended to define functional architecture of the NGN.

I.1 Configurations and topology of the NGN

Along with new architecture and services, the NGN brings an additional level of complexity over existing fixed networks. The addition of support for multiple access technologies and for mobility results in the need to support a wide variety of network configurations. Figure I.1 shows an NGN core network with a set of example access networks. In this figure, the core network is that part of the NGN that provides the telecommunications and/or multimedia services of the NGN to the user. It is distinguished from the access network(s) in that it provides common functions shared across one or more access networks. The NGN core network may be distinguished from other NGN core networks based on administrative needs or ownership. The access networks are distinguished from the core in that they do not provide end-user services directly (other than transport). The access networks may be distinguished from each other based on aspects such as technology, ownership, or administrative needs.

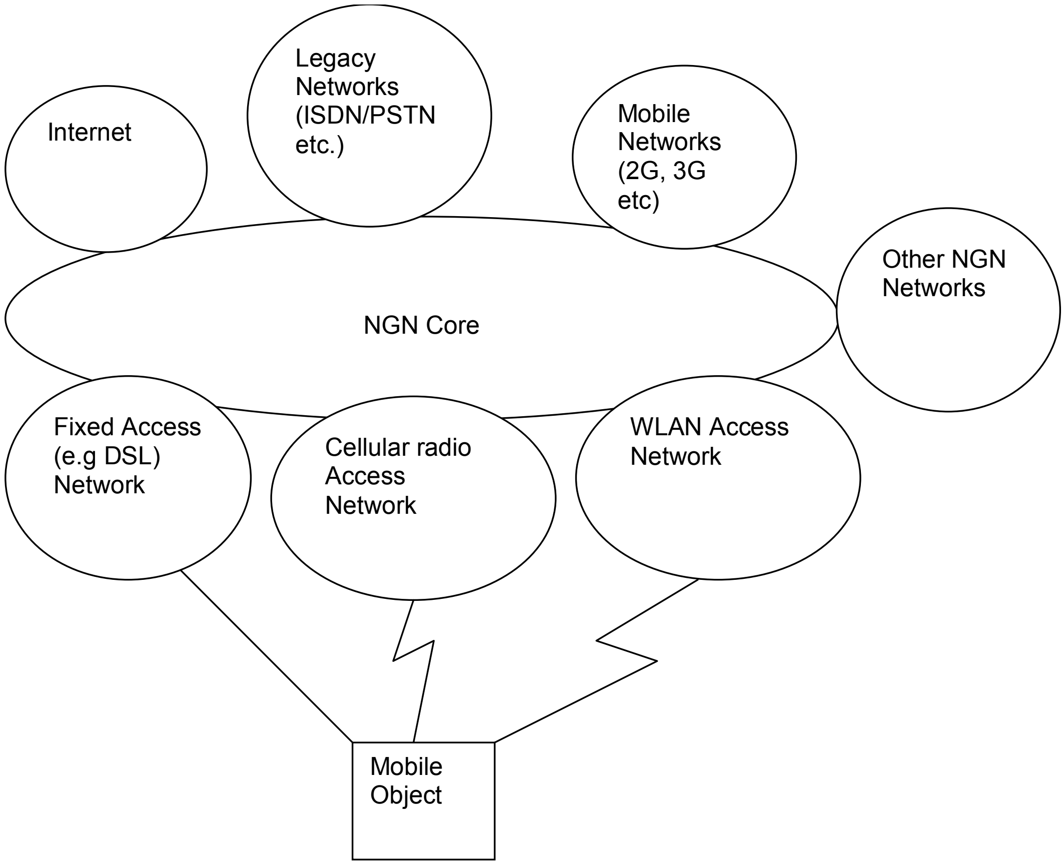

Internet
Legacy Networks (ISDN/PSTN etc.)
Mobile Networks (2G, 3G etc)
Other NGN Networks
NGN Core
Fixed Access (e.g DSL) Network
Cellular radio Access Network
WLAN Access Network
Mobile Object

Figure I.1 – NGN core and access networks

In addition to the need to distinguish between the NGN core and the access networks, the NGN support for roaming introduces another configuration aspect, that of a home network reached from a visited (sometimes called serving) network. Figure I.2 shows a configuration involving an end-to-end NGN session. In this example, user 1 is roaming outside his home network domain, viz. Home core NGN-1 and, thus, there is a need to distinguish between the home network and the visited network. User 2 in this case is in her home network, viz. Home core NGN-2.

It should be noted that the concept of a home network is not necessarily tied to the geographic location of a user's residence or workplace. Rather, it is based on the principle that a network operator holds a subscription for the service being offered to the user. This network operator is responsible for authorizing the user's access to the service and billing the user for this access. It is possible for an entire service to be provided by the visited network, for example, while still having a separate home network operator that authorizes the service through an appropriate business arrangement with the visited network operator. More typically in the NGN, the home network operator will provide the service control for the user while the visited network operator will provide only access-related capabilities, such as support for authentication, support for authorization, data integrity services, and QoS support.

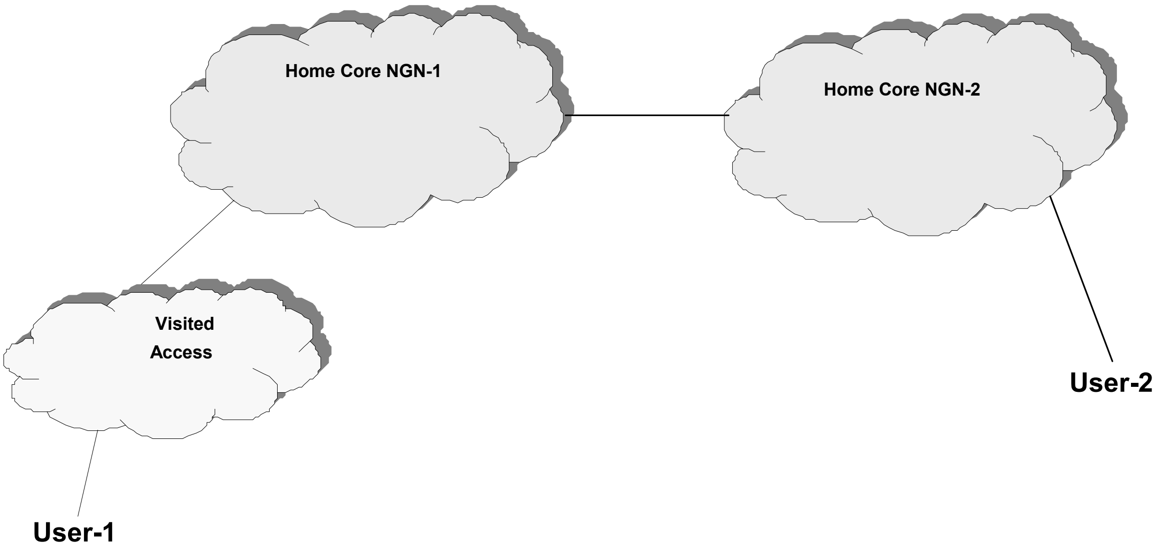


Figure I.2 – NGN example of home and visited networks

Figure I.2 also introduces the notion that multiple NGN core networks may interoperate to provide an end-to-end service to the user. In a simple case, an end-to-end session will have originating and terminating core networks. Depending on the network operator's particular configuration and whether or not roaming is involved, one or more separate access networks might be involved. In a more complex case, some visited core network capabilities may be used in a roaming situation. Figure I.3 shows such an example, where user 1 is roaming outside his home network and support for services such as location information or media transcoding, for example, is provided by the core network of the visited NGN operator.

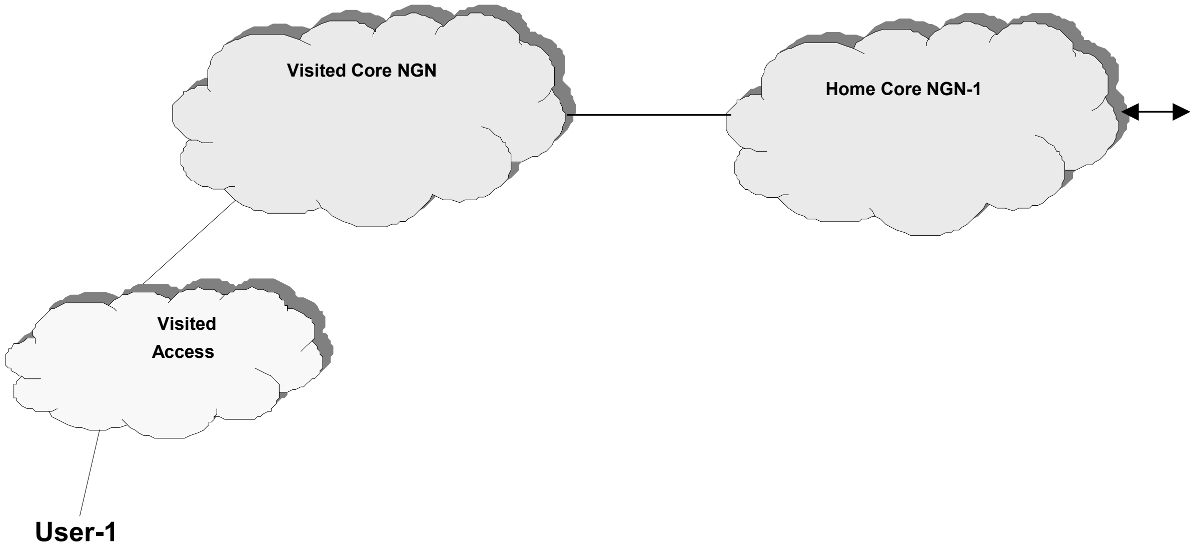


Figure I.3 – NGN example of visited NGN core network support

Since, in many cases, the specific division of functionality between the core and the access networks, between the home and the visited networks, and between the originating and the terminating networks is based on the network operators' business decisions, it is difficult to precisely define the attributes that make up each of these configuration elements. Rather than hard points of separation in the architecture, these aspects should be thought of as configurable topology elements that may be mixed and matched in many different ways. The specification of the NGN architecture should not place any limitations on the network operator's freedom to deploy capabilities or to use the capabilities of other business partners.

I.2 Relationship between the NGN and administrative domains

The NGN network can be logically decomposed into different sub-networks, as shown in Figure I.4. The emphasis on logical decomposition instead of physical decomposition is based on the fact that, in the future, physical equipment may have features of both the access network and the core network. A pure physical decomposition will encounter difficulties when such features are combined into a single network element.

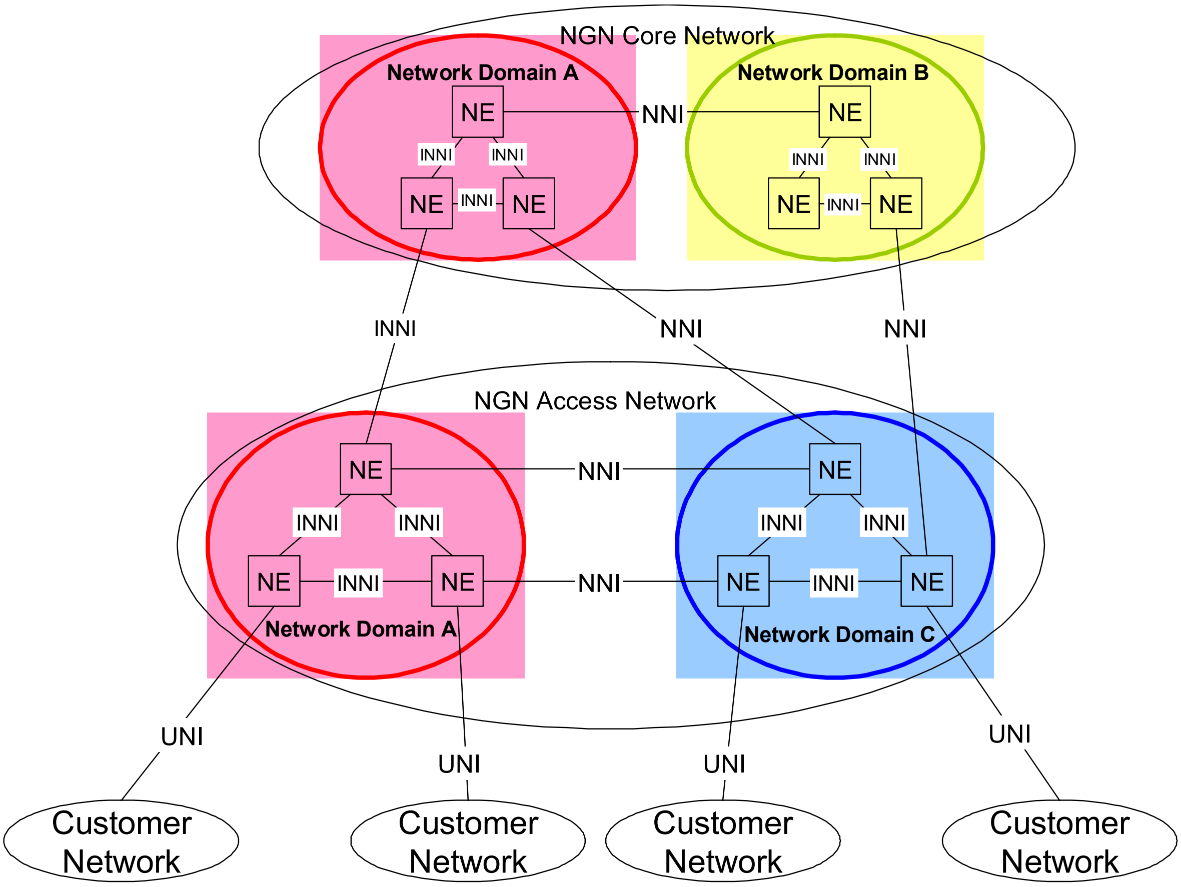


Figure I.4 – Major components of the NGN at the network level

The major components of an NGN network are as follows:

- Customer network: A customer network can be a network within a home or an enterprise network. It is connected to the NGN provider's network via a UNI (user-to-network interface). The UNI is also the demarcation point between the NGN provider and the user. A customer network may obtain its content service from:
  - the core network,
  - another instance of the customer network providing public services, or
  - another instance of the customer network providing private services, possibly with a private addressing scheme.
- Access network: An access network collects end-user traffic from the end-user network to the core network. The access network provider is responsible for the access network. The access network can be further partitioned into different domains, with the intra-domain interface being termed an INNI (internal network-network interface) and the inter-domain interface being termed a NNI (network-network interface). The access network belongs to the transport stratum.
- Core network: The core network belongs to both the transport stratum and the service stratum. The core network provider is responsible for the core network. The interface between the core network and the access network or between core networks can be an INNI (in the case of partitioning as a single domain) or a NNI.

The concept of an NGN domain is introduced to outline the administrative boundaries. Detailed topology information may or may not be shared across the NNI, but may be shared if available for

INNI links. As depicted in Figure I.4, the access network and the core network may or may not belong to the same NGN domain.

I.3 Relationship between the NGN and service domains

The NGN provides access to a wide variety of services. The specific services offered by any NGN operator are determined by business needs and customer needs. Figure I.5 shows an example of an NGN configuration to illustrate multiple domains within which services may be accessed.

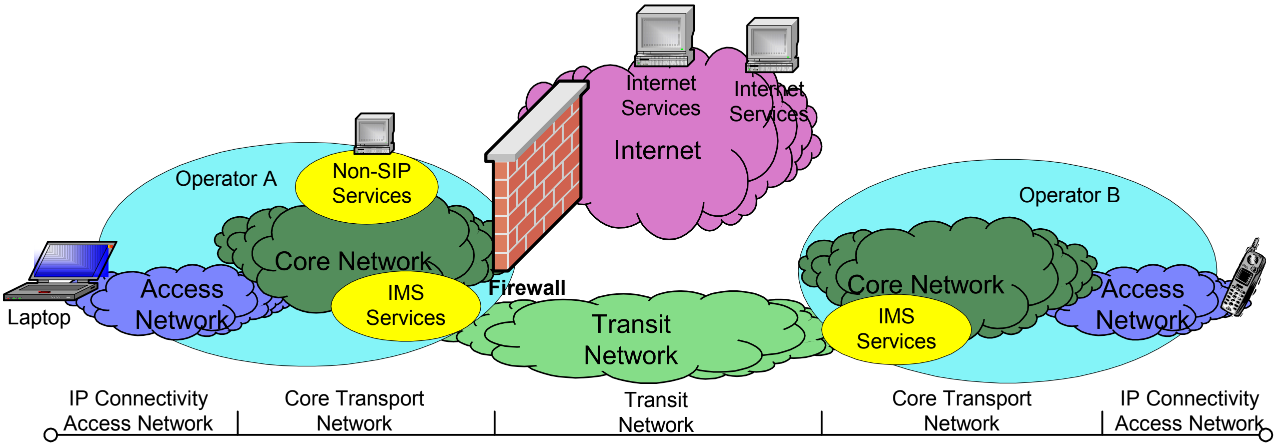


Figure I.5 – NGN example of service domains

In this example, NGN operator A supports a single access network technology that provides access to three service domains via its core network.

One service domain is that provided by the IMS services bubble. These services may be completely within NGN operator A's domain or may support end-to-end services to other network operators. In this example, NGN operator A supports end-to-end IMS services along with NGN operator B's IMS. They are interconnected through a trusted transit network. Other transit network configurations are of course allowed, and the transit network may be null in the case where NGN operator A is directly connected to the other endpoint network. In some cases, firewalls or other gateway elements might be used to protect the NGN operator from the transit network. It should also be noted that the network on the other side of the transit network might be another type of external network, such as the PSTN.

A second service domain in this example is the non-SIP services bubble of NGN operator A. This would provide services such as streaming video. These service entities may be attached directly to the core network of NGN operator A, or may be provided by third parties through trusted security arrangements.

NOTE – Streaming video is chosen as an example of the non-SIP services. Streaming video may be provided either as non-SIP or SIP services.

A third service domain shown here is access to Internet-based services. These services are neither part of NGN operator A's domain, nor are they provided by business arrangements with NGN operator A. These services are accessed by NGN operator A providing a transport connection to the Internet. Such a connection by NGN operator A may only be allowed via firewall techniques.

As mentioned earlier, this example shows only a small set of the possible configurations that might be supported by NGN operators. It illustrates the three basic domains of service access that are provided by the NGN.

I.4 Enterprise role model

The primary purpose of an enterprise model is to identify interfaces that are likely to be of general commercial importance. To do this, a number of roles are identified, which describe reasonably well-defined business activities that are unlikely to be subdivided between a number of players [b-ITU-T Y.110]. The players may aggregate roles as they see fit. Therefore an enterprise model does not limit players in anyway, but it does identify the roles that the architecture should enable.

A basic role model for NGN is shown in Figure I.6. The model itself is taken from [b-ETSI TS 122 101], but we have modified the names to better align it with the current NGN terminology. It identifies the following roles:

- *Customer*: The role denoting a person or other entity that has a contractual relationship with a service provider on behalf of one or more users.
- *User*: The role in which a person or other entity authorized by a customer uses services subscribed to by the customer.
- *Retailing service provider*: The role that has overall responsibility for the provision of a service or set of services to users associated with a subscription as a result of commercial agreements established with the users (i.e., subscription relationships). The user profile is maintained by the retailing service provider. Service provision is the result of combining wholesale network services and service provider service capabilities.
- *Wholesale service provider*: The role that combines a retailing service provider's service capabilities with its own network service capabilities to enable users to obtain services.
- *Value added service provider*: The role that provides services other than basic telecommunications service (e.g., content provision or information services) for which additional charges may be incurred. These may be billed via the customer's service provider or directly to the customer.

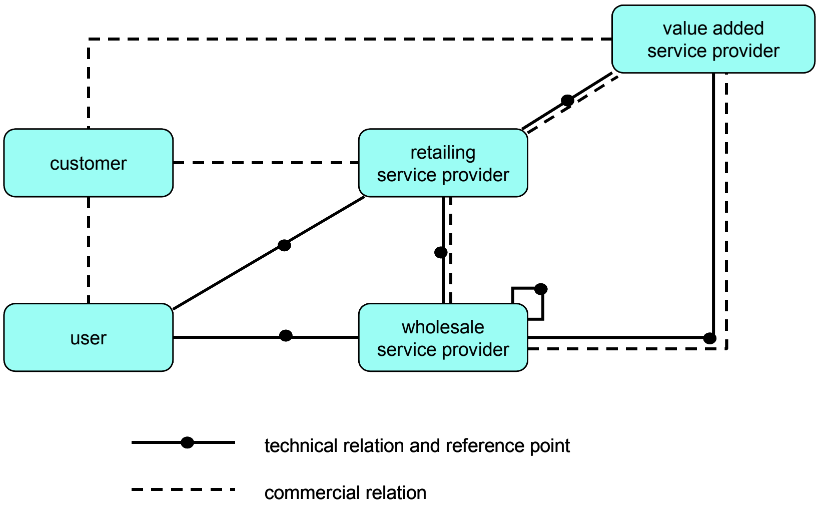

value added service provider
customer
retailing service provider
user
wholesale service provider
technical relation and reference point
commercial relation

Figure I.6 – Basic NGN roles

This basic model provides a kind of superclass for roles and their relations. Wholesale service provider players may need to combine their services to provision an end-to-end service. This is illustrated by the looped line and reference point in the figure. The figure further illustrates whether a relationship between roles is technical or commercial. In the latter case, the relationship may or may not be supported by a technical reference point. Such a reference point would be in the management plane, which is not detailed in this Recommendation. We have therefore limited further elaboration of the model to the technical relationships and the roles that have at least one technical relationship. Hence, the customer role is not shown in the following figures.

The basic model can be extended to reflect the types of specialization that are already visible in the marketplace. To date, we mainly see specialization for the wholesale service provider role, and this is the only one we will consider in the following description. Specialization of the retailing and value-added service provider roles may be considered at a later stage.

The first specialization step is based on the domains as they have been defined by 3GPP (3rd Generation Partnership Project) in [b-ETSI TS 123 101]. Unfortunately, it is not possible to reuse the terminology, as the distinction between serving and home network domains is functional, rather than an enterprise role distinction. The same player will support both functions, depending on the subscription of the user. For lack of a better term, we have used the term "core" for the server/home network role. The access and transit service provider roles map directly to the respective domains in [b-ETSI TS 123 101]. Note that 3GPP uses the term "core network domain" for the combination of server, home, and transit network domains.

At this point it is also worth noting that [b-ETSI TS 123 228] defines an IP connectivity access network (IP-CAN) as the non-IMS part of a complete network solution, excluding terminals. It is neither an access network domain as defined in [b-ETSI TS 123 101], nor does it map to the access service provider role.

The first step in wholesale provider specialization (sub-classing) is shown in Figure I.7.

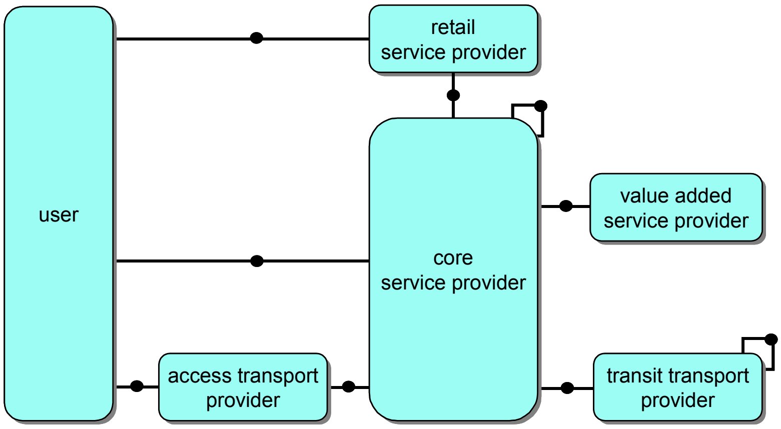

retail service provider
user
value added service provider
core service provider
access transport provider
transit transport provider

Figure I.7 – NGN roles: first level of specialization

A basic tenet of the NGN architecture is the separation of transport and service stratum functions. The main motivation for this is the requirement for the transport stratum to support different types of service control systems, not just IMS. This will be a functional requirement from any player, including cases where the transport and service stratum functions are combined in the core service provider role. This can be taken one step further by specializing the core service provider into a "core transport" and a "service control and integration" provider role. The implication is that the reference points between functions in the transport stratum and the service stratum become trust boundaries and will have to support inter-network operator security requirements.

For completeness, the service control and integration provider role has been split into separate service control provider and integration service provider roles. Virtual network operators are players who perform this role, and these are so well established that it is deemed appropriate to reflect this in the second level of specialization. The resulting role model is depicted in Figure I.8.

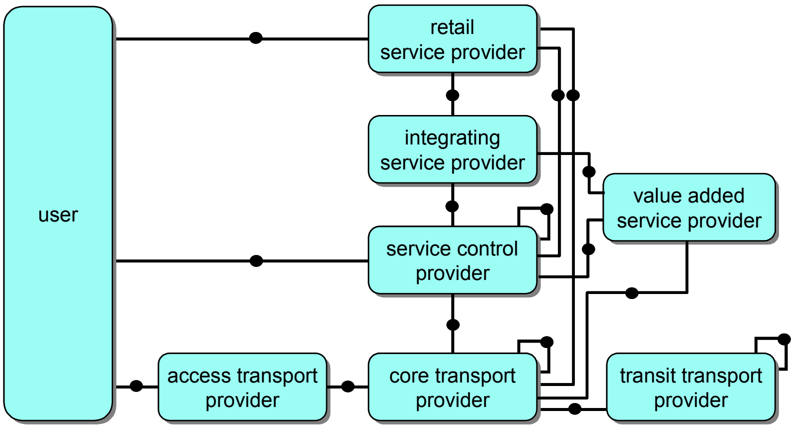

retail service provider
integrating service provider
user
value added service provider
service control provider
access transport provider
core transport provider
transit transport provider

Figure I.8 – NGN roles: second level of specialization

Each of the new roles has a relationship with the retailing service provider role that holds the user profile database. A retailing role player may hold the user information for all three roles, or a user may have a relationship with multiple retailing role players. This cannot be derived from the figure, because it does not show the cardinality of these relationships.

In summary, the second level of specialization of the NGN enterprise model defines the following roles:

- *User*: The role in which a person or other entity authorized by a customer uses services subscribed to by the customer.
- *Retailing service provider*: The role that has overall responsibility for the provision of a service or set of services to users. The user profile is maintained by the retailing service provider. Service provision is the result of combining retailing service provider services with wholesale services from, at least, the access and core transport provider roles and, at most, from all other provider roles.
- *Integrating service provider*: The role that creates unique new service offerings from the wholesale services provided by other roles.
- *Service control provider*: The role that provides session and call control and related services, such as registration, presence, and location, wholesale to retailing and integrating service providers.
- *Value added service provider*: The role that provides value added services (e.g., content provision or information services) on top of the basic telecommunications service provided by the service control provider role. It does not provide a complete service on its own.
- *Core transport provider*: The role that provides connectivity either end-to-end or in part, and related services such as registration for connectivity service, by combining its own services with those of the access transport provider and transit provider roles as necessary.
- *Access transport provider*: The role that provides a wholesale connectivity service between the user and a core transport provider.
- *Transit transport provider*: The role that provides a wholesale connectivity service between core transport providers, in conjunction with other transit transport providers as necessary. It also provides related DNS services.

I.5 Functional roles

Clause I.4 suggests that the core service provider role shown in Figure I.7 will, in general, support both home network as well as serving network functionality. If a strict separation between the transport and the service stratum functions is applied as represented in the functional requirements and architecture model, and implied by the NGN enterprise model shown in Figure I.8, both the service control provider and the core transport provider have to independently support home and serving network functions.

The requirement to support user networks with nomadic terminals is another reason why the home network function of the user terminal in the service stratum may need to be supported by a different player than the one that supports the home network function for the user network gateway (UNG) in the transport stratum. The UNG is connected to a fixed network, which means that the access network will connect it directly to the core transport provider that provides the home network functionality. For moving networks this is no longer the case, and the UNG may roam as well.

The wide range of possibilities this creates is illustrated in Figure I.9. The UNG may be at a location where it has potential access to more than one access transport provider. Each access network may in turn be connected to multiple core transport providers. This scenario is already recognized and supported for WLAN interworking [b-ETSI TS 124 234]. The additional complexity that is introduced by transport and service stratum independence significantly increases the number of routing possibilities, and it still needs to be verified whether this is fully supported by the current architecture.

The need to provide this flexibility should not be questioned, since it will be required to support moving networks anyway. It will, however, undoubtedly increase the complexity, if it has to support the business model shown in Figure I.8, as opposed to the simpler one shown in Figure I.7.

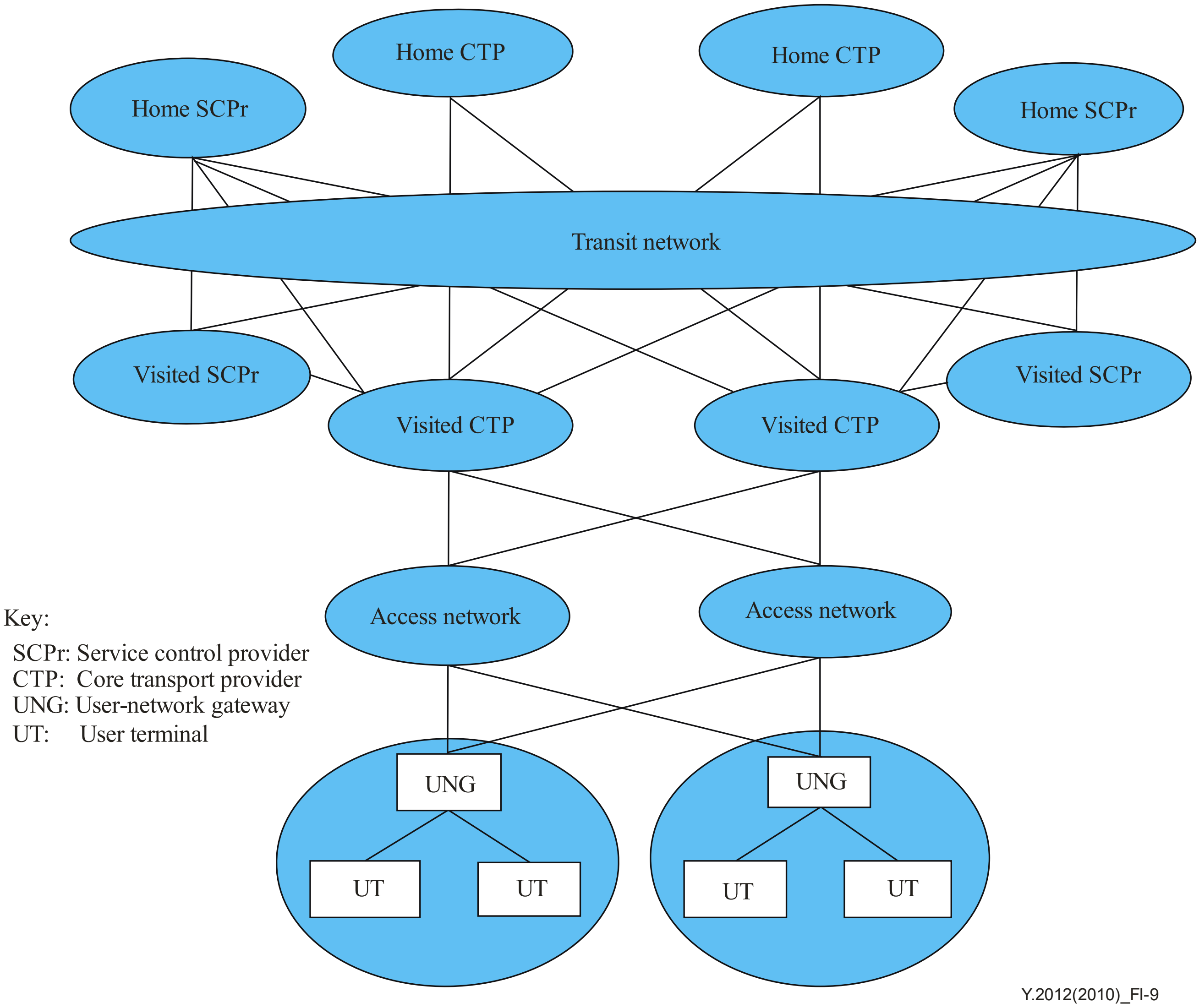


Figure I.9 – Home and visited network functional roles

Appendix II

Transport-stratum access network scenarios

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

II.1 Introduction

This appendix describes some transport-layer access network deployment scenarios that show user equipment accessing the NGN. The figures used to illustrate these scenarios show physical devices and indicate high-level functionality but do not indicate business models, enterprise roles, or network operator domain boundaries. In general, many different business models may be used with each functional scenario. Some of the text used to describe the figures contains examples of such business model considerations.

Also, note that the term "policy enforcement" as used here covers generalized transport-layer user-plane policy enforcement actions, such as QoS traffic conditioning, packet filtering, NAPT binding manipulation, usage metering, flow-based charging, and policy-based forwarding, which may in some cases be broader in scope than NGN. In this discussion, the terms "link layer" and "layer 2" are used synonymously. In the diagrams, some link-layer segments are shown with a specific type (e.g., VLAN (Virtual LAN)), but in general any type of link layer can be used (e.g., SDH (synchronous digital hierarchy), ATM, MPLS (multi protocol label switching)).

II.2 Scenario 1: Multi-layered transport stratum

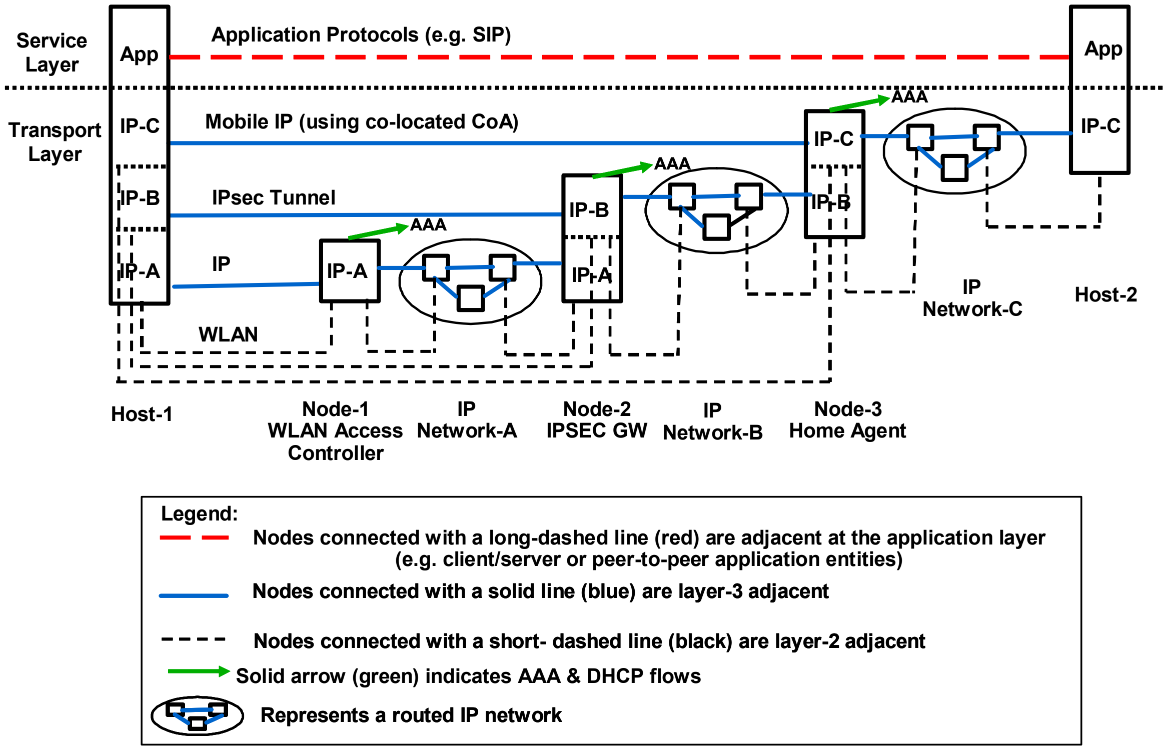

Service Layer
Transport Layer
App
IP-C
IP-B
IP-A
Application Protocols (e.g. SIP)
Mobile IP (using co-located CoA)
IPsec Tunnel
IP
WLAN
AAA
AAA
AAA
IP-A
IP-B
IP-A
IP-C
IP-B
App
IP-C
IP Network-C
Host-2
Host-1
Node-1 WLAN Access Controller
IP Network-A
Node-2 IPSEC GW
IP Network-B
Node-3 Home Agent
Legend:
Nodes connected with a long-dashed line (red) are adjacent at the application layer (e.g. client/server or peer-to-peer application entities)
Nodes connected with a solid line (blue) are layer-3 adjacent
Nodes connected with a short- dashed line (black) are layer-2 adjacent
Solid arrow (green) indicates AAA & DHCP flows
Represents a routed IP network

Figure II.1 – Multi-layered transport stratum

The transport stratum may be multi-layered, with a number of different access technologies layered on top of each other. For example, IP can run over a stack of link-layer technologies, such as IP/Ethernet/ATM/SDH/WDM (wavelength division multiplexing). IP itself can also be used as a link-layer technology via IP tunnelling, and these IP tunnels can form part of a stack of link layers.

Figure II.1 shows a host running a stack of mobile IP/IPsec/WLAN. For example, a terminal could connect to a public WLAN hotspot, establish an IPsec tunnel to an IPsec gateway located in a service provider domain, and then perform a mobile IP registration with a home agent also in the service provider domain. In this example, a co-located care-of address is used, so there is no foreign agent. Here, the terminal has three IP addresses, one for each layer. The first IP address is assigned when the terminal connects to the WLAN network; the second, when the terminal connects to the IPsec gateway; and the third, when the mobile IP registration is performed. Also, an AAA request may be issued independently at each layer for the purposes of user authentication and authorization.

The terminal may send all application traffic over mobile IP, or it can bypass one or more layers in the stack and send application traffic via a lower layer. For example, split IPsec tunnelling could be used, whereby only traffic destined to the service provider domain is sent via IPsec, with general Internet traffic bypassing IPsec.

Transport-layer user-plane policy enforcement may be performed at each layer. For example, when a user connects to the WLAN, a packet filter for that user may be installed in the WLAN access controller that restricts traffic to a set of IPsec gateways. In turn, the IPsec gateways may have a packet filter for that user that restricts traffic to a set of mobile IP home agents, such that the user is required to run mobile IP. In turn, the home agents may have packet filters that allow the user to access some service platforms but not others.

When this scenario is mapped to a 3GPP WLAN IP access environment, the WLAN access gateway (WAG) functionality is located in Node-1, and the packet data gateway (PDG) functionality is located in Node-2.

Mappings onto NGN functional architecture

In this scenario, Node-1 acts as an EN-FE (e.g., handling QoS enforcement for the WLAN network). Node-1 may also act as an ABG-FE (e.g., performing NAPT). Node-2 and Node-3 act as ABG-FEs, handling policy enforcement for their respective IP layers. This scenario illustrates that ABG-FE and EN-FE functionality may be performed independently at each IP layer in a transport stratum which contains multiple IP layers. Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the IP tunnels for which they are performing a layer-2 termination function. This scenario illustrates that ABG-FE and EN-FE functionality may be performed independently at each IP layer in a transport stratum which contains multiple IP layers.

II.3 Scenario 2: Access aggregation using layer-2

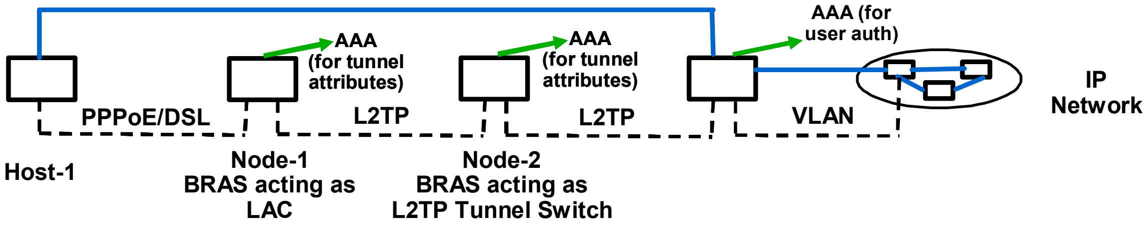

AAA (for user auth)
AAA (for tunnel attributes)
AAA (for tunnel attributes)
PPPoE/DSL
L2TP
L2TP
VLAN
IP Network
Host-1
Node-1 BRAS acting as LAC
Node-2 BRAS acting as L2TP Tunnel Switch

Figure II.2 – Access aggregation using layer-2

Within a single layer of the transport stratum, there may be multiple points where access traffic is aggregated. Traffic forwarding between different aggregation segments may be done at layer-2 or layer-3.

Figure II.2 shows a host running PPPoE connected over DSL (digital subscriber line) to a BRAS (broadband remote access server). This BRAS acts as a LAC (L2TP access concentrator) and forwards the traffic by using L2TP to a second BRAS acting as an LNS (L2TP network server). Node-1 may issue a RADIUS request to obtain attributes for the tunnel to be established (e.g., [b-IETF RFC 2868]). The second BRAS performs L2TP tunnel switching and, in turn, acts as a LAC and forwards the traffic to a third BRAS acting as an LNS. Node-2 may also issue a RADIUS request to obtain attributes for the tunnel to be established. The third BRAS terminates the PPP state machine and may issue a RADIUS request to perform user authentication. Forwarding at Nodes-1 and 2 is done at layer-2, with traffic being switched between two link-layer segments: IP header information is not examined in making forwarding decisions. Policy enforcement (e.g., traffic conditioning, packet filtering, NAPT, etc.) is generally only done in Node-3, though there are cases where some policy enforcement may be done at Nodes-1 or 2. For example, a similar scenario can be used in a mobile environment with a mobile network operator providing a network-based VPN service and backhauling traffic to a corporate LNS. If a pre-paid charging model is used, service termination upon reaching a zero-balance condition may be enforced at Nodes-1 or 2.

The scenario shown here may be used in a wholesale business model, where one party owns the physical DSL lines and aggregates traffic to a second party acting as a wholesaler, who in turn aggregates traffic to a third party acting as a service provider (e.g., an ISP). By introducing a wholesale intermediary, the party dealing with the physical lines (or more generally, the party operating the access-technology-specific equipment) does not need to maintain a business relationship with all the service providers, and a party acting as a service provider does not need to maintain a business relationship with multiple network operators each handling some specific access technology, such as DSL, 2G/3G, or WiMax (Worldwide Interoperability for Microwave Access).

Mappings onto NGN functional architecture

In this scenario, Node-1 acts as an EN-FE (e.g., handling QoS enforcement for the DSL aggregation network). Node-3 acts as an ABG-FE (e.g., performing traffic conditioning, packet filtering, NAPT, etc.) Node-3 may also act as an EN-FE, handling QoS enforcement for the L2TP tunnels it terminates. Typically Node-2 is acting as a pure layer-2 relay and is not playing either an EN-FE or an ABG-FE role. Node-2 acts as an ABG-FE if it is performing IP-level policy enforcement (e.g., accounting).

II.4 Scenario 3: Access aggregation using layer-3

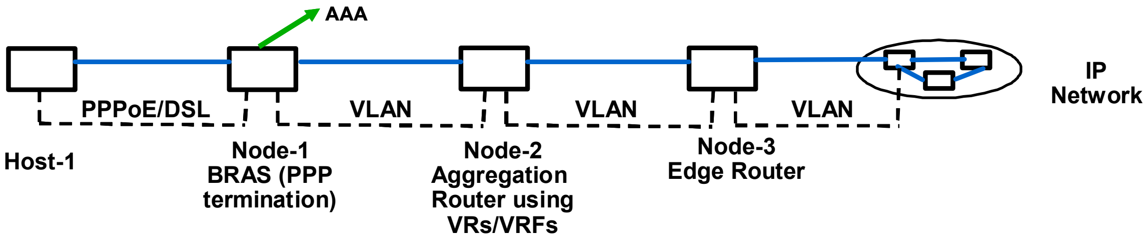

AAA
IP Network
PPPoE/DSL
VLAN
VLAN
VLAN
Host-1
Node-1 BRAS (PPP termination)
Node-2 Aggregation Router using VRs/VRFs
Node-3 Edge Router

Figure II.3 – Access aggregation using layer-3

This is similar to scenario 2, except that forwarding between different aggregation segments is done at layer-3. Node-1 terminates PPP and associates the traffic for a PPP session with a particular domain (e.g., using the realm part of the PPP username to identify the domain). In the upstream direction, policy-based forwarding is used, so that traffic for different domains is segregated and the correct IP next-hop for each domain is chosen. In the downstream direction, Node-1 performs regular IP forwarding based on the longest match prefix. Node-2 implements multiple virtual routers, one for each domain. Again, policy-based forwarding is done in the upstream direction, such that all traffic for a given user is sent upstream to Node-3, and regular IP forwarding is done in the downstream direction. In this example, Nodes-1, 2, and 3 see all the traffic for a given subscriber. Node-1 may issue a RADIUS request to perform user authentication. This request may be sent via a RADIUS proxy, or directly over the virtual routed network itself, thus avoiding the need for a RADIUS proxy.

Aggregation at layer-3 may simplify Node-3, since it does not need to terminate large numbers of L2TP tunnels and associated PPP state machines, but it instead receives an aggregated traffic stream delivered over a single VLAN. Note that Node-3 can still identify individual subscriber traffic flows for the purposes of performing subscriber-specific policy enforcement actions, but on the user plane this is done using layer-3 information (e.g., the source IP address), rather than by maintaining an individual link-layer connection for each subscriber. Policy enforcement actions (e.g., traffic conditioning, packet filtering, NAPT, etc.) may be carried out in all nodes, and this may be done at the subscriber-flow level or at coarser granularities, such as at the virtual router level (e.g., some VRs may have a higher level of QoS than others).

Mappings onto NGN functional architecture

In this scenario, Node-1 acts as an EN-FE (e.g., handling QoS enforcement for the DSL aggregation network). Node-3 acts as an ABG-FE (e.g., performing traffic conditioning, packet filtering, NAPT, etc.). Node-1 and Node-2 act as ABG-FEs if they are performing IP-level policy enforcement (e.g., NAPT or support of different QoS classes). Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the VLANs they terminate.

II.5 Scenario 4: Multistage policy enforcement

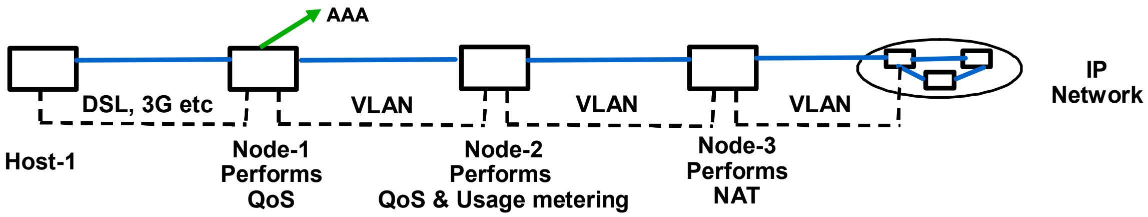


Figure II.4 – Multistage policy enforcement

Within a single layer of the transport stratum, the set of policy enforcement actions carried out for traffic for a given subscriber may be distributed across a sequence of devices, with each device doing a subset of the total work. This may reflect a network deployment strategy where there is a set of access-technology-specific edge devices (e.g., GGSNs or BRASs) and one or more devices behind these that perform policy enforcement in an access-technology-independent manner. Different devices may have different capabilities or be optimized for a certain type of policy enforcement action.

Figure II.4 shows an example where policy enforcement is distributed across a sequence of devices. Here, Node-1 terminates some access technologies and performs QoS functions that require visibility of link-layer technology-specific parameters, such as the mapping of DiffServ codepoints to 802.1p priorities or GPRS traffic classes. Node-2 performs QoS functions that operate at layer-3 and above and also performs usage metering. Node-3 is used as a NAPT traversal gateway. Node-3 could either be layer-3 adjacent to Node-2, or it could be used as a user-plane/media relay and located anywhere in the IP network. In the relay case, packets from Host-1 are explicitly addressed to Node-3, and when Node-3 forwards the traffic onwards, it re-originates the traffic with an IP address belonging to Node-3. Similarly in the reverse direction, packets are explicitly addressed to Node-3 and re-originated with a Node-3 IP address.

Mappings onto NGN functional architecture

In this scenario, Node-1 acts as an EN-FE (e.g., handling QoS enforcement for the access network). Node-2 and Node-3 are acting as ABG-FEs, handling IP-level policy enforcement. Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the VLANs they terminate.

II.6 Scenario 5: Partitioning into transport-layer traffic subdomains

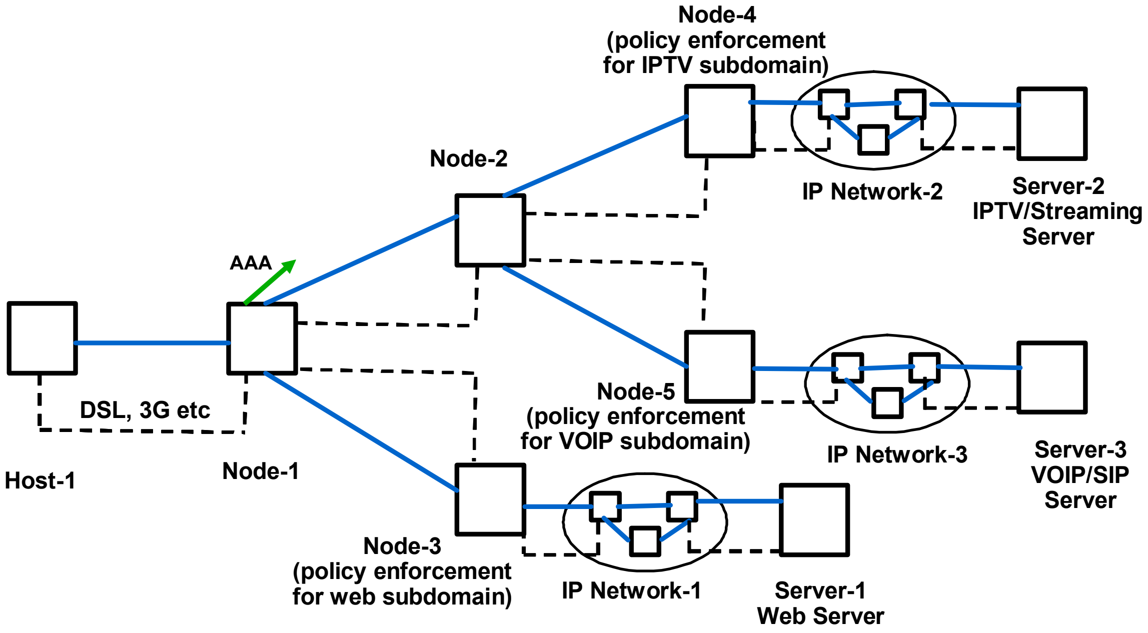


Figure II.5 – Partitioning into transport-layer traffic subdomains

Within a single layer of the transport stratum, traffic may be partitioned into multiple subdomains, such that policy enforcement may be carried out separately in each subdomain. Certain nodes act as branch points, whereby traffic for a given subdomain is identified and then subjected to a certain traffic treatment, such as being forwarded to a next-hop node through policy-based forwarding. A transport-layer-traffic sub-domain may be associated with a specific set of service-layer services and applications (e.g., IPTV (IP television), VoIP (voice over IP), or Internet traffic). A transport-layer-traffic subdomain could also be associated with peer-to-peer traffic, with the NGN providers only supplying transport-layer services, such as a QoS-enabled path between two customer hosts.

Figure II.5 shows such an example where traffic for a given user is split at Node-1 into two subdomains: one for web or non-real-time traffic, and the other for real-time traffic. The real-time traffic in turn is split at Node-2 into an IPTV/streaming subdomain and a communications subdomain used for VoIP, video telephony, and so forth. This could map to a business model where one service provider is used for internet traffic, another for IPTV, and another for communications services, and each independently performs policy enforcement on its respective traffic subdomain. Note that many variants of this scenario are possible; for example, Nodes-1 and 2 could be collapsed so that there is a 3-way split at Node-1. Also, Nodes-2 and 5 could be collapsed so that both the branching of traffic between domains (IPTV and VoIP) and the policy enforcement for a specific domain (VoIP) occur at the same node.

Mappings onto NGN functional architecture

In this scenario, Node-1 acts as an EN-FE (e.g., handling QoS enforcement for the access network). Node-1 also acts as an ABG-FE, steering upstream traffic to the right subdomain. Node-2, Node-3, Node-4 and Node-5 are acting as ABG-FEs, handling traffic steering and/or IP-level policy enforcement. Node-2, Node-3, Node-4 and Node-5 may also act as EN-FEs, handling QoS enforcement for the link layers they terminate.

Appendix III

Instantiation of NGN reference points

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

III.1 Introduction

Figure 7-1 shows an overview of the NGN functional architecture that allows the support of NGN services. Since Figure 7-1 is drawn from a high-level conceptual point of view, instantiation of the NGN reference points is useful to clarify the specific role of the different NGN reference points in terms of service offering and the physical implementation entailed.

III.2 Scope

The purpose of this appendix is to help understand the four reference points contained in Figure 7-1, i.e., UNI, NNI, ANI and SNI reference points.

In particular, this appendix also describes the service-network interface (SNI) which is a new reference point in this Recommendation as compared to the previous edition of this Recommendation. This instantiation of the SNI is effective only when a service partner is classified separately from ordinary customers. The SNI does not preclude any use of UNI, NNI and ANI, when such classification is not considered as relevant.

III.3 Rationale to consider SNI

In comparison to an ordinary customer connected at a UNI, this clause identifies support service partners connected at the SNI. Service partners include content providers, data information providers, and other service providers different from the NGN operator.

The following requirements apply regarding service partners connected at the SNI:

1) Larger capacity than ordinary customers in terms of transport and signalling resources, such as physical transmission capacity, maximum number of simultaneous sessions, and maximum session establishment/release rate.
2) Media flow injection that should be multicast in the network; this injection allows a connected entity to play the role of a multicasting source (root) in addition to an ordinary sink (leaf) role.
3) Customized policy different from that for ordinary customers; this includes the level of trust which is derived from different physical configurations (hosting, connection with dedicated and secured lines, and so on).
4) Unrestricted server role in terms of client/server model; for instance, SIP is modelled by the client/server model. An ordinary customer does not need or must not play the role of a server for specific functions, such as registrar and presence server, whereas a server residing in a service partner should be allowed to do so.

III.4 Instantiation of NGN reference points

Figure III.1 describes an illustrative instantiation of NGN reference points, which are derived from the overview architecture in Figure 7-1.

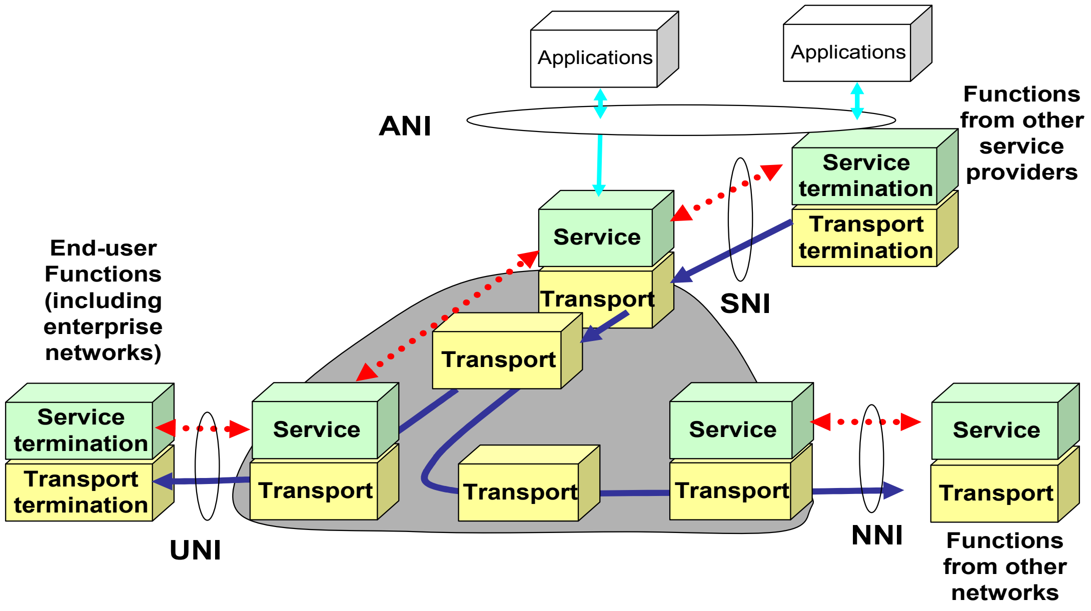


Figure III.1 – Instantiation of NGN reference points

NOTE 1 – In Figure III.1, boxes labelled "Service" correspond to boxes that include "NGN service stratum" functions, while boxes labelled "Transport" correspond to boxes that include "NGN transport stratum" functions.

NOTE 2 – In Figure III.1, "termination" at "End-user functions" and at "Functions from other service providers" highlight the specific nature of these functions, which is the absolute source or sink of the media stream.

III.4.1 Instantiation of UNI reference point

The NGN supports a reference point to the end-user functions called the "user-to-network interface (UNI)", which provides a channel for interactions and exchanges between end-user functions and NGN elements.

In this instantiation, UNI is assumed to support enterprise customers as well, which requires aggregation of multiple end users. Further instantiation of UNI dedicated for enterprise customers is under study.

III.4.2 Instantiation of NNI reference point

The NGN supports another reference point to other networks called the "network-to-network interface (NNI)", which provides a channel for interactions and exchanges between the NGN and other networks.

III.4.3 Instantiation of SNI reference point

In addition to UNI and NNI, the NGN can support a reference point called the "service-to-network interface (SNI)", which provides a channel for transport-level media exchange and service-level signalling interaction between functions of other service providers and NGN elements. The functions of other service providers include a content-generating function, which is an ultimate source or sink of multimedia content, such as a server device that acts as a content source, data storage, or application.

The SNI is a realization of a service provider access interface (SPAI), which is specified in [b-ITU-T Y.140]. In particular, the SNI corresponds to the SPAI for Class 2 service providers and brokers.

The SNI has the following characteristics at least:

- It allows the connected entities to exchange media flows.
- It allows the connected entities to exchange signalling flows at the service control level.
- It accommodates content source as a connected entity, which expects the network to multicast the injected media flow.
- It allows flexible and customizable configurations and policy rules to meet a wide range of requirements of service providers connected to the NGN, in terms of resource capacity, signalling profile, and operational rules, including security.
- It allows the connected entities to play full server roles in a client/server model, in particular in signalling interaction.

The way to implement the SNI at the detailed functional entity level needs further study.

III.4.4 Instantiation of ANI reference point

Clause 6.2 defines the application network interface (ANI) as follows:

"Application network interface: Interface which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for realization of applications."

Since Figure 7-1 shows no media flow across the ANI, the ANI is interpreted as a control-level interaction without media interactions such as voice and video. The ANI should be interpreted as a point of vertical interactions between different layers, which allows media injection. On the other hand, UNI, NNI, and SNI are a point of horizontal interactions between different entities consisting of a couple of layers.

Appendix IV

Example illustrative deployment scenario for IdM in NGN

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

NGN may deploy IdM infrastructure with capabilities supporting identity-based services to its users leveraging web services capabilities and specifications defined by the Liberty Alliance Project and OpenID. For example, IdM capabilities to allow its users to access services among different service and application providers including federated services and applications. Also, NGN may support IdM capabilities to offer Identity Provider (IdP) services to other applications and service providers (e.g., assertion of user device identity and authentication, location and other relation identity information).

Support of IdM capabilities to offer IdP services and or partner with other application and service providers that are using different types of IdM systems based on different semantics, schemas, mechanisms and technologies, would require appropriate bridging and interworking functions to facilitate interoperability. For example, to support IdM services and capabilities with other applications and service providers (e.g., web services and content providers), NGN could support capabilities for the following:

- 3GPP GBA interworking with Liberty Alliance Framework;
- 3GPP GBA interworking with OpenID.

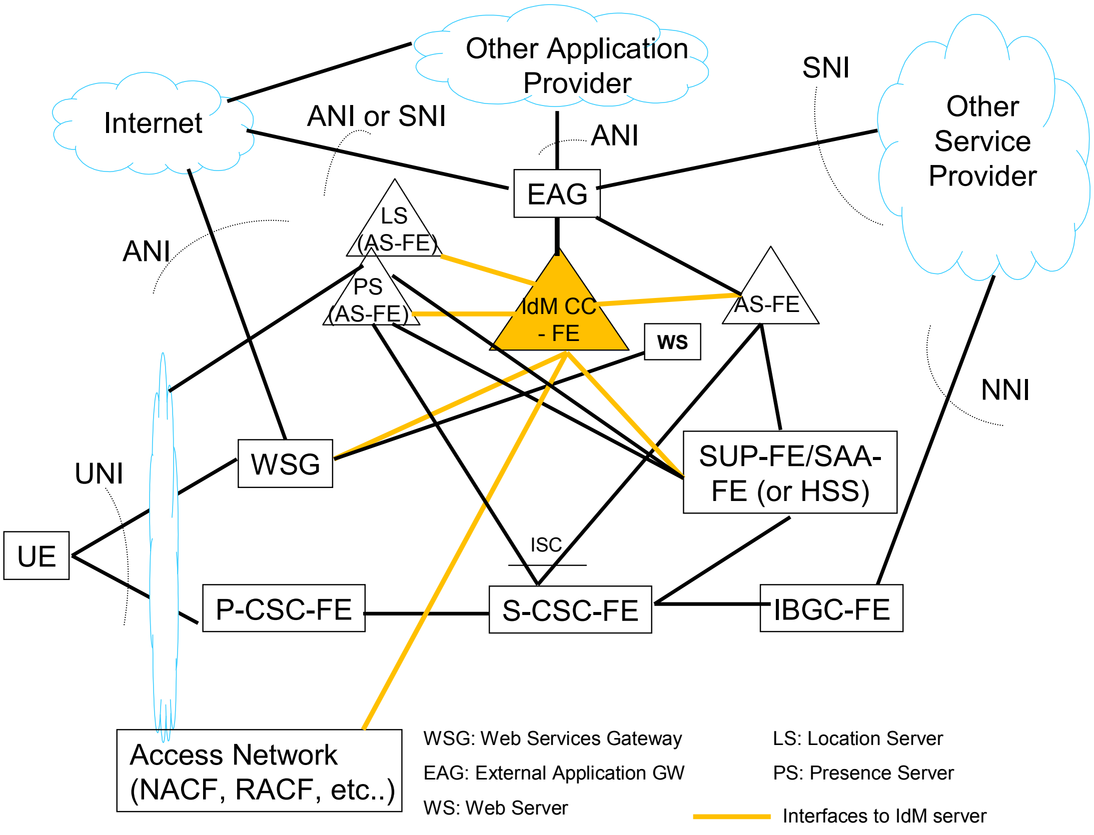


Figure IV.1 – Example IdM deployment in NGN

Figure IV.1 illustrates an example of IdM deployment for NGN. This example shows the use of an IdM server which may be a standalone box, or a set of functions that are distributed, and/or located in the HSS. The IdM server interfaces and interacts with network elements support functional entities defined for the NGN. For example, the IdM server may interface with:

- service enabling application servers (ASs), such as a location server (LS) or a presence server (PS), or other applications in order to provide a higher level of authentication assurance and to support identity based services and applications;
- policy and network attachment and control servers for authentication assurance and policy management.

In order to support certain IdM services for users/subscribers and to offer IdP services or partner with other application providers and/or other service providers, the NGN would need to support specific capabilities to control access and IdM exchanges with other application providers and/or other service providers (e.g., web services providers and content providers). This illustrative example shows the use of a web services gateway (WSG) and an external application gateway (EAG) to support certain IdM services leveraging or partnering with other application providers and/or other service providers. Specifically, Figure IV.1 shows the IdM server interfacing with the user via a web services gateway (WSG) which authenticates the user and provides the user with an interface to manage his/her identity profile. The IdM server also interfaces with an external application gateway (EAG) that allows the user to access web-based services in the NGN or from other application providers and/or other service providers.

Bibliography

[b-ITU-T Y.2000-Sup.1]	ITU-T Y-2000 series Recommendations – Supplement 1 (2006), *ITU-T Y.2000 series – Supplement on NGN release 1 scope.*
[b-ITU-T Y.2000-Sup7]	ITU-T Y-2000 series Recommendations – Supplement 7 (2008), *ITU-T Y.2000 series – Supplement on NGN release 2 scope.*
[b-ITU-T Y.110]	Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture.*
[b-ITU-T Y.140]	Recommendation ITU-T Y.140 (2000), *Global Information Infrastructure (GII): Reference points for interconnection framework.*
[b-ETSI TS 122 101]	ETSI TS 122 101 V9.6.0 (2010), *Universal Mobile Telecommunications System (UMTS); LTE; Service aspects, Service principles (3GPP TS 22.101 version 9.6.0 Release 9).*
[b-ETSI TS 123 101]	ETSI TS 123 101 V8.0.0 (2009), *Universal Mobile Telecommunications System (UMTS); LTE; General UMTS Architecture (3GPP TS 23.101 version 8.0.0 Release 8).*
[b-ETSI TS 123 228]	ETSI TS 123 228 V8.10.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 8.10.0 Release 8).*
[b-ETSI TS 124 234]	ETSI TS 124 234 V8.3.0 (2009), *Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3 (3GPP TS 24.234 version 8.3.0 Release 8).*
[b-IEEE 802.11]	IEEE Std 802.11-2007, *IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements – Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*
[b-IEEE 802.16]	IEEE Std 802.16-2009. *IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Broadband Wireless Access Systems.*
[b-IEEE 802.21]	IEEE Std 802.21-2008, *IEEE Standard for Local and metropolitan area networks – Part 21: Media Independent Handover Services.*
[b-IETF RFC 1661]	IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP).*
[b-IETF RFC 2131]	IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*
[b-IETF RFC 2868]	IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support.*

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2010