International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2012

(09/2006)

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 the NGN release 1

ITU-T Recommendation 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
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.2012

Functional requirements and architecture of the NGN release 1

Summary

The objective of ITU-T Recommendation Y.2012 is to describe the functional requirements and architecture of the next generation network (NGN) for release 1, as described in ITU-T Rec. Y.2201 (NGN release 1 requirements) and Supplement 1 to ITU-T Y.2000-series Recommendations (NGN release 1 scope). The functional architecture provided in this Recommendation allows a clear distinction between the definition and specification aspects of the services provided by the NGN and the actual specification of the network technologies used to support those services. In line with Y.2011 principles, an implementation-independent approach is adopted.

Source

ITU-T Recommendation Y.2012 was approved on 13 September 2006 by ITU-T Study Group 13 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation Y.2012

Functional requirements and architecture of the NGN release 1

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] for release 1, as described in NGN release 1 scope [b-ITU-T Y.2000-series Sup.1] and NGN release 1 requirements [b-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 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.

The scope of release 1 specifies that nomadism shall be supported between different network termination points. While no major new reference points for mobility are proposed for development as part of release 1, other mobility-related functionalities beyond nomadism, such as handover, are not precluded and may be supported through the use of existing technologies. Thus, any mobility-related functions or functional entities described here that support capabilities beyond nomadism are only included because they represent functionalities that already exist in the mobile environment. They should be applied in the areas related to mobility within the architecture.

Administrations may require operators and service providers to take into account national regulatory and national policy requirements in implementing 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 M.3060/Y.2401] ITU-T Recommendation M.3060/Y.2401 (2006), *Principles for the management of Next Generation Networks*.

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

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

[ITU-T Y.1453]	ITU-T Recommendation Y.1453 (2006), *TDM-IP interworking – User plane interworking*.
[ITU-T Y.2001]	ITU-T Recommendation Y.2001 (2004), *General overview of NGN*.
[ITU-T Y.2011]	ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.
[ITU-T Y.2021]	ITU-T Recommendation Y.2021 (2006), *IMS for Next Generation Networks*.
[ITU-T Y.2031]	ITU-T Recommendation Y.2031 (2006), *PSTN/ISDN emulation architecture*.
[ITU-T Y.2091]	ITU-T Recommendation Y.2091 (2007), *Terms and definitions for Next Generation Networks*.
[ITU-T Y.2111]	ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.
[ITU-T Y.2171]	ITU-T Recommendation Y.2171 (2006), *Admission control priority levels in Next Generation Networks*.

3 Definitions

This Recommendation defines the following terms:

3.1 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 the realization of applications.

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

3.3 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.

3.4 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.

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

3.6 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.

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

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

3.9 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.

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

3.11 **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 and acronyms:

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ABG-FE	Access Border Gateway Functional Entity
AGC-FE	Access Gateway Control Functional Entity
ALG	Application Level Gateway
AMF	Account Management Function
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
AR-FE	Access Relay Functional Entity
AS	Application Server
ASF&SSF	Application Support Function and Service Support Function
AS-FE	Application Support Functional Entity
ATM	Asynchronous Transfer Mode
BG-FE	Border Gateway Functional Entity
BGC-FE	Breakout Gateway Control Functional Entity
CAF	Charging and Accounting Function
CCF	Charging Collection Function
CDR	Call Detail Record; Charging Data Record
CTF	Charging Trigger Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DTMF	Dual Tone Multi Frequency
EN-FE	Edge Node Functional Entity

FE	Functional Entity
FW	Firewall
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSC-FE	General Services Control Functional Entity
HGW	Home GateWay
HGWC-FE	Home GateWay Configuration Functional Entity
IBC-FE	Interconnection Border Gateway Control Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
ICMP	Internet Control Message Protocol
I-CSC-FE	Interrogating Call Session Control Functional Entity
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IPTV	IP Television
ISDN	Integrated Services Digital Network
IVR	Interactive Voice Response
L2TP	Layer 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MGC-FE	Media Gateway Control Functional Entity
MPLS	Multi Protocol Label Switching
MRB-FE	Media Resource Broker Functional Entity
MRC-FE	Media Resource Control Functional Entity
MRP-FE	Media Resource Processing Functional Entity
NACF	Network Attachment Control Function
NAC-FE	Network Access Configuration Functional Entity
NAPT	Network Address and Port Translation
NE	Network Element
NGN	Next Generation Network
NNI	Network Network Interface
NPF	NAPT Proxy Function
NSIW-FE	Network Signalling Interworking Functional Entity
OCF	Online Charging Function
OSA	Open Service Architecture

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
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACF	Resource and Admission Control Function
RAN	Radio Access Network
RF	Rating Function
SAA-FE	Service Authentication and Authorization Functional Entity
SCF	Service Control Function
SCP	Service Control Point
S-CSC-FE	Serving Call Session Control Functional Entity
SDH	Synchronous Digital Hierarchy
SG-FE	Signalling Gateway Functional Entity
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SL-FE	Subscription Locator Functional Entity
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
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
TUP-FE	Transport User Profile Functional Entity
UE	User Equipment
UNI	User Network Interface
URI	Uniform Resource Identifier
USIW-FE	User Signalling Interworking Functional Entity
W-CDMA	Wideband-Code Division Multiple Access
WLAN	Wireless LAN
xDSL	x Digital Subscriber Line

5 Conventions

This Recommendation uses the following conventions. These conventions are specific to this Recommendation and are used to facilitate referencing different relationships.

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 function.

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

S-T_n: This term is used o indicate the relationship between service stratum functional entities and transport processing functional entities.

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

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

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 function.

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) and resource and admission control functions (RACF). NACF and RACF constitute transport control function.

6 General principles of the NGN functional architecture

The NGN functional architecture shall incorporate the following principles:

Support for multiple access technologies: The NGN functional architecture shall 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 interface should be open to support service creation, service updating, and incorporation of service logic provision by third parties.

Independent service provisioning: The service provisioning process should be 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 should 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. However, similar entities may be located in different logical layers.

7 Overview of the NGN architecture

Along with a new architecture, the next generation network will bring an additional level of complexity beyond that of existing 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, however, 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 release 1 scope [b-ITU-T Y.2000-series Sup.1], as well as the requirements identified in the NGN release 1 requirements [b-ITU-T Y.2201]. NGN services include multimedia services, such as conversational services, and content delivery services, such as video streaming and broadcasting.

The 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 1 shows an overview of the NGN functional architecture that allows the support of the release 1 services. 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 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 NGN supports a reference point to the applications functional group called application network interface (ANI), which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for the realization of applications.

The transport stratum provides IP connectivity services to NGN users under the control of transport control functions, including the network attachment control functions (NACFs) and resource and admission control functions (RACFs).

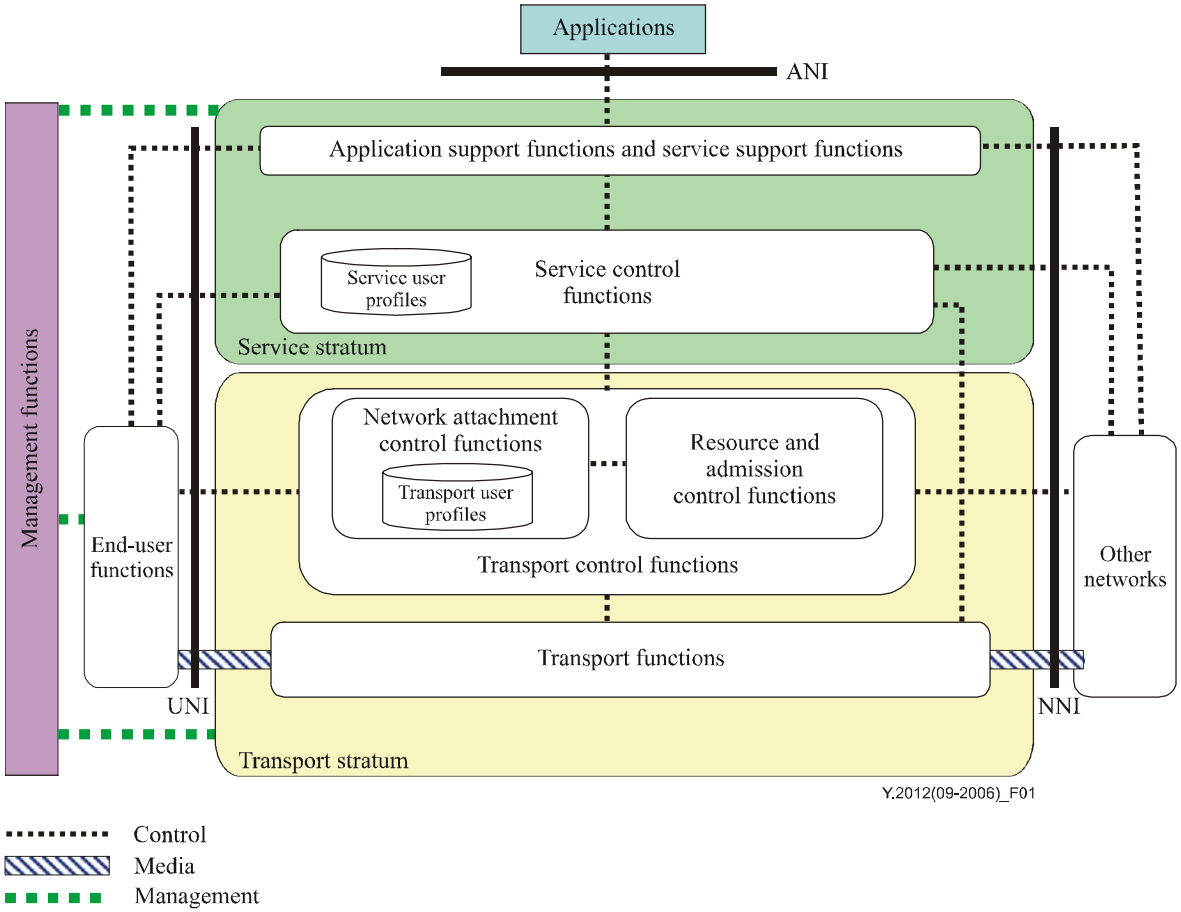


Figure 1 – NGN architecture overview

NOTE 1 – The user network interface (UNI), network network interface (NNI), and application network interface (ANI) should 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 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 (RACFs), network attachment control functions (NACFs), and service control functions, may be distributed and instantiated over different NGN provider domains. The functional groups in the service stratum and the transport stratum may be distributed between a visited network and a home network (refer to 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 be co-located. Note that other functional databases required for the support of NGN release 1 services (such as DNS) are not illustrated in Figure 1.

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 the 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.

Access network functionality beyond collecting and aggregating the traffic (e.g., switching or routing) needs further study.

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., IEEE 802.11 and 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

This series of functions provides 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 and network attachment control functions.

7.1.2.1 Resource and admission control functions (RACF)

Within the NGN architecture [ITU-T Y.2001] and [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] related transport resource control within access and core networks. 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 (SCFs) and makes service providers 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/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 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 (NACFs). The RACF and NACF interact to exchange relevant transport subscription information.

For delivering of those services across multiple providers or 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 (NACFs)

The network attachment control functions (NACFs) 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 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 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.

7.2 Service stratum functions

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

- the service control functions including service user profile functions; and
- the application support functions and service support functions.

7.2.1 Service control functions

The service control functions 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.

7.2.2 Application support functions and service support functions

The application support functions and service support functions 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 a reference point 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 ability 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/Y.2401].

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;

e) security management.

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

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

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.

Details are given in mobility management requirements for NGN [ITU-T Q.1706/Y.2801].

8.2 NGN service architecture

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

i) "Applications";

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

iii) certain 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 may break into two categories: those trusted by network/server providers, and those that are not. The former may consist of network/server providers themselves and subordinate organizations or partners, while the latter may consist of independent service providers, whose access to southbound resources must be authenticated, controlled, and filtered by the functions in the service enablers.

As shown in Figure 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. Also 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 shall consist of functions that are agnostic with respect to their underlying NGN infrastructure.

b) Support for legacy capabilities and features: There shall not be any 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, and so forth shall be supported. For example, the legacy-IN-influenced features of IMS,

such as triggers, filter criteria, and the service capability interaction manager, will be 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 should provide an open service interface, which provides an abstract of the network capabilities (i.e., the interface is network agnostic). This interface should provide access to such functions as authentication, authorization, and security to ensure that third-party service providers can make use of the network capabilities.

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. 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

Network address and port translation (NAPT) traversal copes with the traversal of 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 NAPT application level gateway (ALG) or other service control functional entities affiliated with the service provider 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.

8.5 Charging and accounting functions (CAFs)

The CAFs described in this clause are meant to represent a generalized architecture to support an NGN provider operator's need to collect and process information, such that customers can be charged for the services provided.

The CAFs provide accounting data to the network operator 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 CAFs include a charging trigger function (CTF), an online charging function (OCF), a charging collection function (CCF), a rating function (RF), and an account management function (AMF).

Figure 2 shows the functions that comprise the CAF.

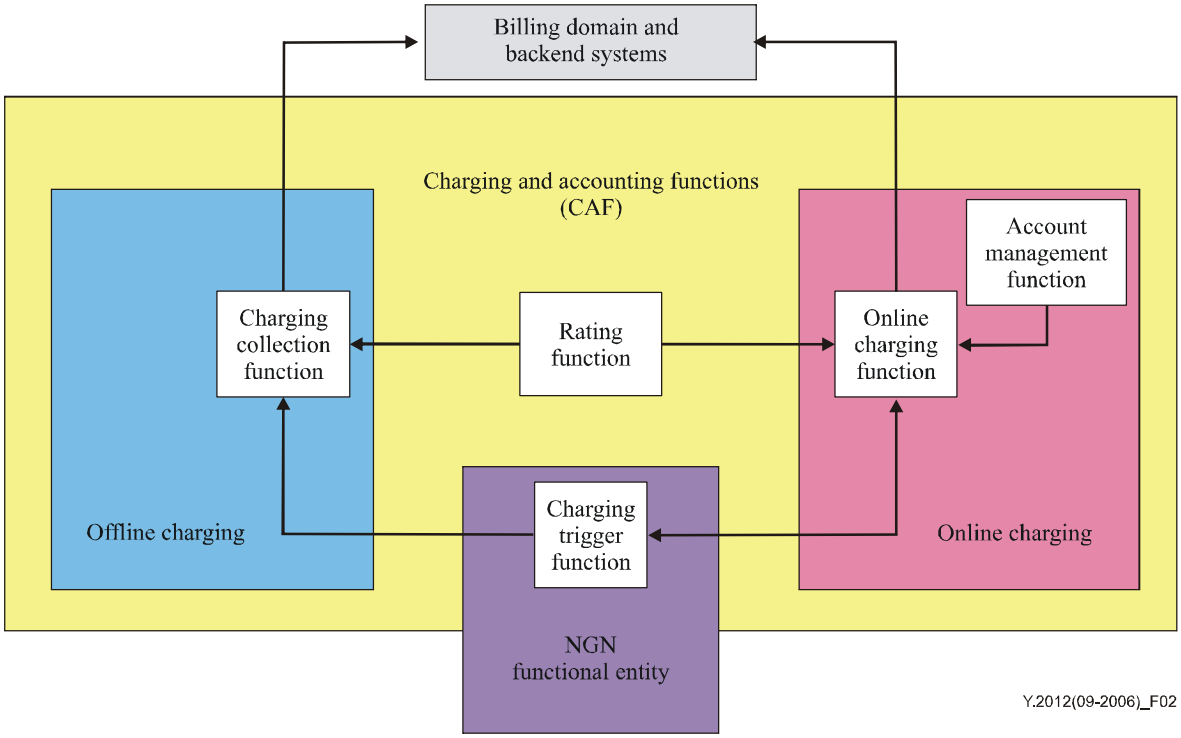


Figure 2 – Charging and accounting functions

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 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 data records (CDRs). The results of the CCF tasks are CDRs with well-defined content and format. The CDRs are later transferred to the billing domain.

8.5.3 Online charging function (OCF)

The OCF receives charging events from the CTF and executes 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 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.

The RF also works with the offline charging module, and it determines the value of the network resource usage (described in the charging event received by the CCF from the network).

8.5.5 Account management function (AMF)

The AMF 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.

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 entities (FEs)

In general, an 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.

9.2 Generalized functional architecture

The generalized NGN functional architecture shown in Figure 3 is based on the NGN architecture overview provided in clause 7. In particular, the functional groups identified in Figure 1 are used to structure the general layout of Figure 3.

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. [b-ITU-T Y.2000-series Sup.1] outlines the scope of NGN release 1. [b-ITU-T Y.2201] specifies the service capability requirements of the NGN. The NGN architecture is consistent with the scope and requirements specified in these Recommendations.

In this sense, it is expected that, in line with Y.2011 principles, most of the NGN transport stratum functions (such as RACF or NACF) will be able to support these different types of NGN services in a common way. NGN implementations do not, however, have to implement certain transport stratum FEs, such as gateway FEs with respect to PSTN/ISDN, if they do not require support for such capabilities.

Resource and admission control functions (RACF) architecture described in [ITU-T Y.2111] characterizes transport functions focusing on QoS, NAPT, and firewall control aspects. Since the generalized NGN functional architecture described in this Recommendation has much broader sense, in particular, at the transport functions, another model showing distinction of access and core aspects is used. In Figure 3, two RACF instances are shown to express independent control of associated underlying access and core transport respectively. RACF itself has no distinction between access and core and the same conventions are used.

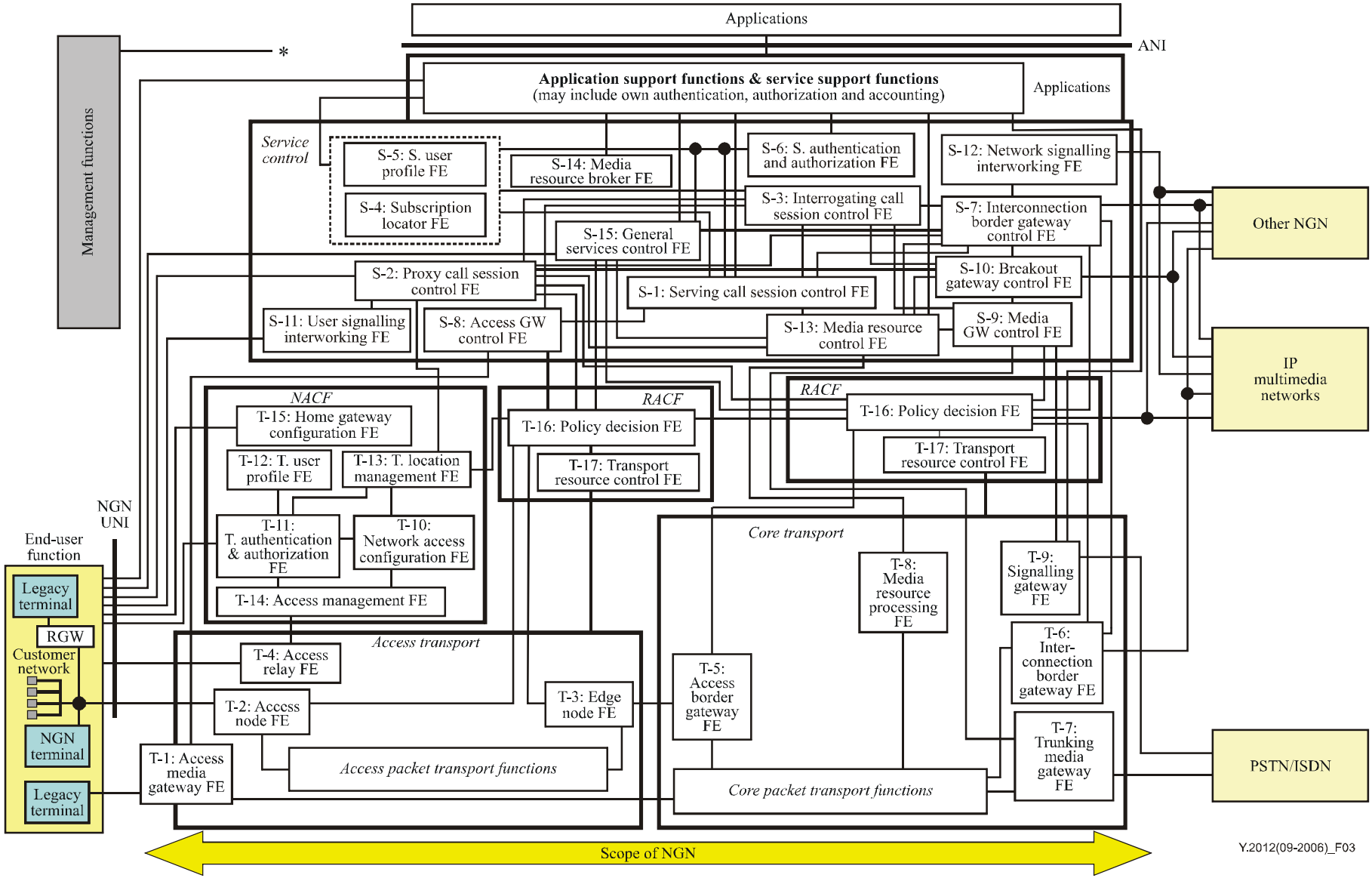


Figure 3 – NGN generalized functional architecture (Refer to Notes below)

NOTE 1 – 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.

NOTE 2 – Lines terminating on the dotted box around S-4 and S-5 indicate connection to both internal FEs. Inclusion of these two FEs in the dotted box does not imply that they are co-located.

NOTE 3 – The need for allocation of some functions to the IBG-FE is for further study: IBG-FE may/may not perform media conversion under the control of IBC-FE. A direct link between IBG-FE and IBC-FE is for further study. (Refer to clause 9.3.1.6 on T-6 IBG-FE.)

NOTE 4 – The NGN-UNI line shows the functional aspect only and should not make any pre-decision about an ownership domain.

NOTE 5 – More precise location and distinction of possible NGN-UNIs are for further study.

NOTE 6 – As an option, P-CSC-FE, IBC-FE, BGC-FE, and MGC-FE interact with MRC-FE in support of invoking transcoding.

NOTE 7 – 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.

NOTE 8 – 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, AMG-FE required to accommodate PSTN/ISDN terminals is shown even though they are not strictly part of the NGN architecture itself.

NOTE 9 – * indicates multiple links from management functions towards applications, service control, NACF, RACF, access transport, and core transport.

NOTE 10 – This figure does not show any linkage from an FE to itself, though it is not precluded.

NOTE 11 – Relationship between S-7 and S-12 needs further study with regard to interaction with other networks. Relationship of S-7 and S-12 with other NGN needs further study.

In this functional architecture, some FEs include functions relating to the NGN service stratum and the NGN transport stratum. On the one hand, the transport stratum covers transport functions and associated control functions up to the IP layer. On the other hand, the service stratum includes functions that handle the layers above the IP layer. Attention needs to be paid to which layer is addressed by each relationship (i.e., linkage in Figure 3) between FEs. For instance, there are several relationships between end-user functions and the transport stratum. There are IP-based relationships and PSTN/ISDN relationships related to media transport, and there are also some signalling relationships. The relationships between the end-user functions and service functions represent service protocol layer relationships. The relationships to the application functions represent application layer protocol relationships.

9.3 Functional entity descriptions

This clause describes each FE with figures.

9.3.1 Transport processing FEs

Figure 4 shows the transport processing FEs.

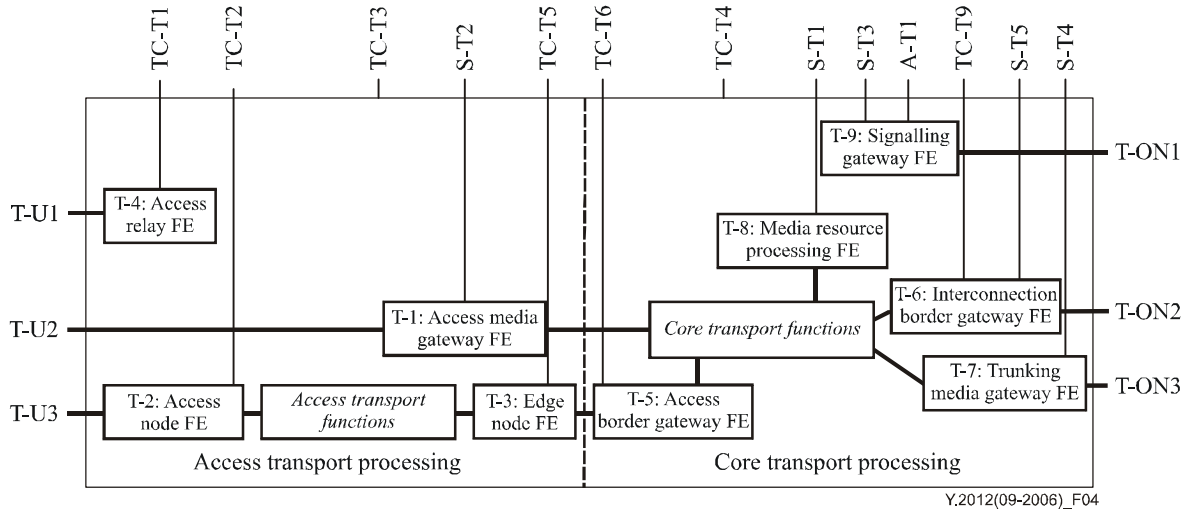


Figure 4 – Transport processing FEs

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.

a) 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 9.3.3.8).

b) It provides adequate transfer functions for PSTN/ISDN user call control signalling to the AGC-FE for processing.

c) It optionally supports payload processing functions (e.g., codecs and echo cancellers).

d) 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 may 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.

Since the AN-FE may be IP capable, it should support the functions of policy enforcement functional entity (PE-FE) and 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 shall 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 should support the functions of policy enforcement functional entity (PE-FE) and controlled by the RACF as defined in [ITU-T Y.2111].

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

The AR-FE is a relay between end-user functions and the NAC-FE that inserts local pre-configuration information when necessary.

NOTE – For example when using DHCP, the AR-FE acts as a DHCP relay agent and may 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 access packet-based services.

The functions of the ABG-FE may 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 shall support the functions of PE-FE controlled by the RACF as defined in [ITU-T Y.2111].

ABG-FE may support IPv4/v6 conversion.

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 an operator's core transport network with another operator's core transport network supporting the packet-based services. There may be one or multiple IBG-FE 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 shall support the functions of PE-FE (except for remote NAPT traversal) controlled by the RACF as defined in [ITU-T Y.2111].

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

In addition, the IBG-FE may support the following:

1) media conversion (e.g., G.711 and AMR, T.38 and G.711);
2) inter-domain IPv4/IPv6 conversion;
3) media encryption;
4) fax/modem processing.

NOTE – Allocation of the above functions to the IBG-FE needs further study: IBG-FE may/may not perform media conversion under the control of IBC-FE. The direct link between IBG-FE and IBC-FE is for further study.

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 may support payload processing (e.g., codecs, echo cancellers, and conference bridges).

b) It optionally provides the TDM/IP interworking function (refer to [ITU-T Y.1453]) in order to support 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.

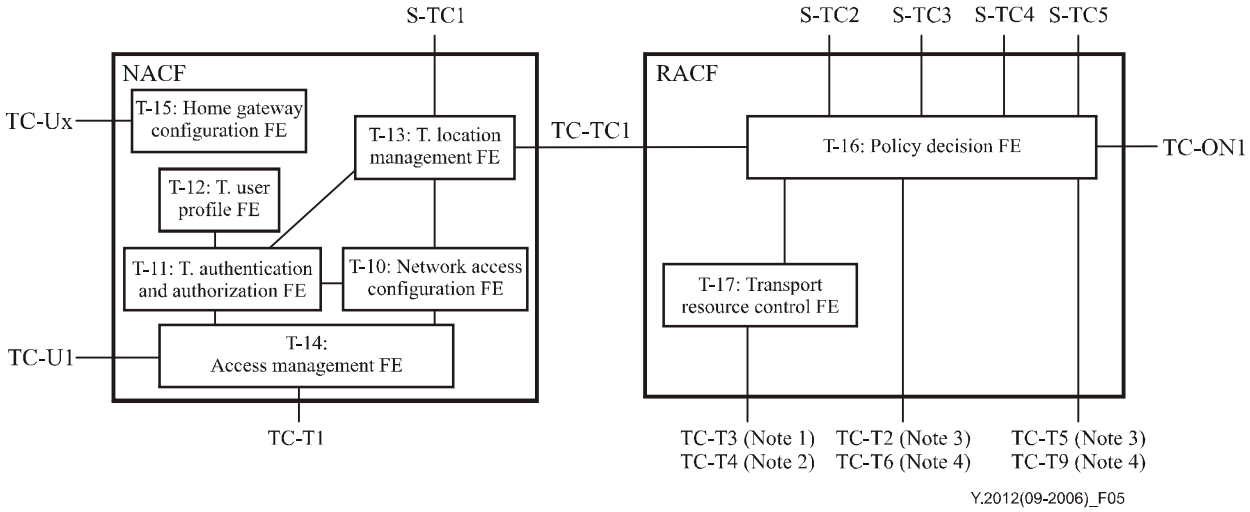
f) It provides transcoding, text-to-speech, video mixing, conference bridge, data conference, fax, voice and video recording, and voice recognition capabilities.

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 existing networks such as PSTN, ISDN, IN networks, and signalling system No. 7.

9.3.2 Transport control functional entities

Figure 5 shows the functional entities related to transport control.



NOTE 1 – Applicable when TRC-FE operates in the access network domain.
NOTE 2 – Applicable when TRC-FE operates in the core network domain.
NOTE 3 – Applicable when PD-FE operates in the access network domain.
NOTE 4 – Applicable when PD-FE operates in the core network domain.

Figure 5 – Transport-control-related functional entities

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

The network access configuration functional entity (NAC-FE) is responsible for IP address allocation to terminals. It may also distribute other network configuration parameters, such as the addresses of DNS servers and signalling proxies (e.g., the address of the P-CSC-FE in order to have access to service stratum functions).

The NAC-FE should be able to provide an access network identifier to a terminal. This information uniquely identifies the access network to which the terminal is attached. With this information, applications should be able to locate the TLM-FE.

NOTE – DHCP servers, RADIUS servers, or DIAMETER servers are typical implementations of the NAC-FE.

The NAC-FE is responsible for the discovery function to support auto configuration. The discovery function is a transport control function to detect the identity of its currently attached network, collect the appropriate network configuration parameters, and ascertain the validity of configuration of its currently attached network based on user profiles.

9.3.2.2 T-11 Transport authentication and authorization functional entity (TAA-FE)

The transport authentication and authorization functional entity (TAA-FE) provides authentication and authorization functions in the transport stratum. The TAA-FE performs user authentication, as well as authorization checking, based on user profiles, for network access. For each user, the TAA-FE retrieves authentication data and access authorization information from the user profile information contained in the TUP-FE.

The TAA-FE acting as a proxy can locate and communicate with the TAA-FE acting as a server which can access the TUP-FE user authentication data, and forward access and authorization requests, as well as accounting messages, received from the AM-FE, to the TAA-FE acting as a server. Responses received back in return from the TAA-FE acting as a server will be forwarded to the AM-FE.

9.3.2.3 T-12 Transport user profile functional entity (TUP-FE)

The transport user profile functional entity (TUP-FE) is responsible for storing user profiles (e.g., QoS profile, P-CSC-FE address, and HGWC-FE address) related to the transport stratum.

The TUP-FE is responsible for responses to TAA-FE queries for user profiles, i.e.:

a) It provides access to user data. This function provides filtered access to the user data, which may be restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

b) It may also be used for support of commonly used AAA and security schemes.

The TUP-FE performs basic data management and maintenance functions, e.g., user profile management functions for handling the storage and update of the user profiles data.

NOTE 1 – The transport user profile may be stored in one database or separated into several databases. The TUP-FE and the TAA-FE can be co-located. The TUP-FE can be co-located with the SUP-FE.

NOTE 2 – The transport user profile may reside in the visited or home networks.

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

The transport location management functional entity (TLM-FE) registers the association between the IP address allocated to the user equipment and related network location information provided by the NAC-FE (e.g., access line identifier). The TLM-FE registers the association between network location information received from the NAC-FE and geographical location information.

The TLM-FE may also store the identifier of the user/UE to which the IP address has been allocated (information received from the TAA-FE), as well as the user network QoS profile and user preferences regarding the privacy of location information. In case the TLM-FE does not store the identifier/profile of the user/user equipment (UE), the TLM-FE shall be able to retrieve this information from the TAA-FE.

The TLM-FE responds to location queries from service control components and applications.

The TLM-FE interfaces with the NAC-FE to get the association between the IP address allocated by the NAC-FE to the end user equipment and the identity of the logical access used by the attached user equipment (i.e., logical access ID).

The TLM-FE registers also user network profile information (received from the TAA-FE at authentication) to make this profile information available to the RACF at authentication of the user equipment.

The TLM-FE is able to correlate the information received from NAC-FE and TAA-FE based on the access logical line identification.

NOTE – Further flexibility may be required in the future regarding the location of TLM-FE temporary data in the network attachment control functions (NACF), e.g., in order for NACF to be applicable for both fixed and mobile environments.

9.3.2.5 T-14 Access management functional entity (AM-FE)

The access management functional entity (AM-FE) translates network access requests issued by the user equipment. It forwards the requests for allocation of an IP address and possibly additional network configuration parameters to/from the NAC-FE.

AM-FE forwards requests to the TAA-FE to authenticate the user, authorize or deny the network access, and retrieve user-specific access configuration parameters.

NOTE – In case PPP is applied, the AM-FE terminates the PPP connection and provides the interworking with the interface to the network attachment subsystem, e.g., using an AAA protocol (e.g., RADIUS or DIAMETER). The AM-FE acts as a RADIUS client if the TAA-FE is implemented in a RADIUS server (i.e., the AM-FE terminates the PPP and translates it to signalling on the reference point between the AM-FE and the TAA-FE).

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

The home gateway configuration functional entity (HGWC-FE) is used during initialization and update of the home gateway (HGW). The HGWC-FE provides the HGW with additional configuration information (e.g., configuration of a firewall internally in the HGW, QoS marking of IP packets, etc.). This data differs from the network configuration data provided by the NACF-FE.

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

Refer to [ITU-T Y.2111].

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

Refer to [ITU-T Y.2111].

9.3.3 Service control functional entities

Figure 6 shows the service stratum FEs.

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

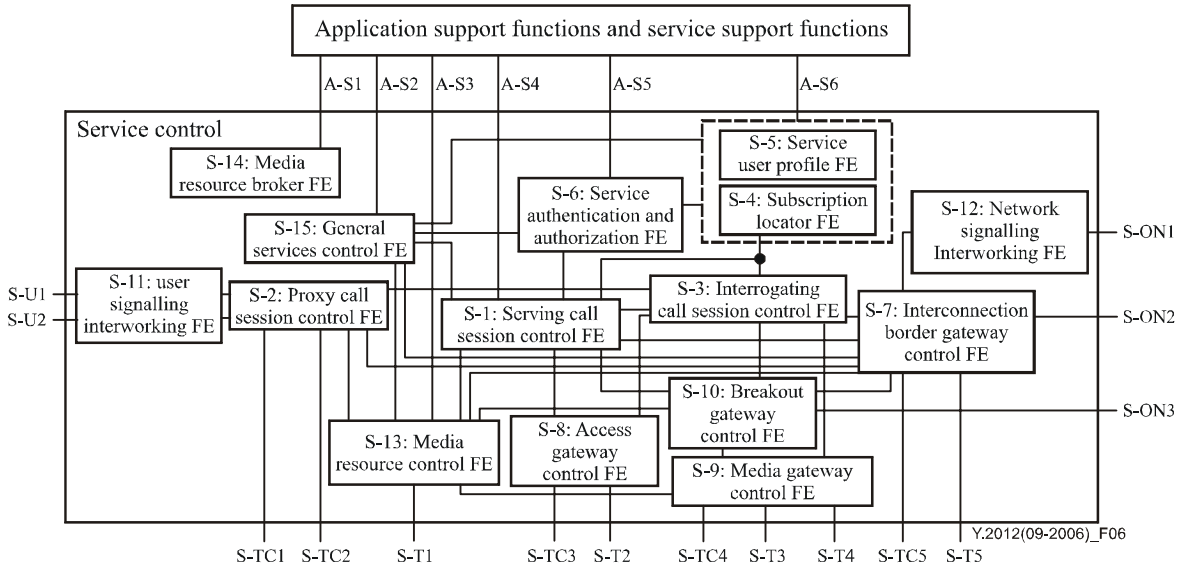


Figure 6 – Service stratum functional entities

9.3.3.1 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 set-up, 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, operator routing policy and based on address information obtained from SUP-FE via the "registration" function.

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

For mediated session the S-CSC-FE:

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

2) Shall 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 network 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 network operator, it forwards the session control request or response to an I-CSC-FE within the 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" on a "home network" shall be mandated capabilities. Technology-specific functional architectures instantiating this FE shall 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.

9.3.3.2 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, an NACF, or other access-specific techniques. The P-CSC-FE has the capability to accept requests and service them internally or forward them on. It shall 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 shall have the capability to forward session control requests related to registration to an appropriate I-CSC-FE.

b) It shall have the capability to forward session control requests received from the terminal to the S-CSC-FE.

c) It forwards session control requests or responses to the terminal.

d) It shall have the capability to detect and handle emergency session establishment requests.

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

f) It shall have the capability to perform message compression/decompression.

g) It may perform inter-domain topology hiding.

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

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

i) It shall have the capability to 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.

j) It supports 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.

9.3.3.3 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 operator's network for all service connections destined to a user of that network operator. There may be multiple I-CSC-FEs within an operator's network. The functions performed by the I-CSC-FE are as follows:

Registration:

– Assigning an S-CSC-FE to a user.

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 operator may use the optional 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 operators' domains, the I-CSC-FE may restrict the following information from being passed outside an operator's network: the exact number of S-CSC-FEs, the capabilities of the S-CSC-FEs and the capacity of the network.

9.3.3.4 S-4 Subscription locator functional entity (SL-FE)

The subscription locator functional entity (SL-FE) may be queried by the S-CSC-FE, I-CSC-FE, or 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 network operator. This resolution mechanism is not required in networks that utilize a single logical SUP-FE element.

9.3.3.5 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 shall be provided in support of:

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

   The user profile may be 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 may be restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

   b) It may also be used for support of commonly used AAA and security schemes.

9.3.3.6 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.

9.3.3.7 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 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 may 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.).

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

NOTE 1 – Information screening functions are for further study.

NOTE 2 – Relationship between S-7 and S-12 needs further study with regard to interaction with other networks. Relationship with other NGNs needs further study.

9.3.3.8 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 AMG-FE.

a) It originates and terminates session control signalling.

b) It originates and terminates gateway control flows to control AMG-FE.

c) It may 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 may 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 may 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 an 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 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.

9.3.3.9 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 may process and forward service requests from PSTN/ISDN to the AS-FE through the BG-FE and 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 MRC-FE in support of invoking transcoding.

9.3.3.10 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 MRC-FE in support of invoking transcoding.

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

The user signalling interworking functional entity (USIW-FE) has the responsibility for the interworking and 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.

9.3.3.12 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-operator), which can be located at the border of the core networks for trunking-side signalling interworking.

NOTE 1 – Information screening functions are for further study.

NOTE 2 – Relationship between S-7 and S-12 needs further study with regard to interaction with other networks. Relationship with other NGNs needs further study.

9.3.3.13 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.

9.3.3.14 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.

9.3.3.15 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, the GSC-FE 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 may 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 may 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 may 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 Application support functions and service support functions

The application support functions and service support functions provide control for services accessed by interacting with the S-CSC-FE, GSC-FE, or 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 may comprise the following functional entities: application support FE, application gateway FE, application service coordination manager FE, and service switching functional entity.

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 shall 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 7.

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;

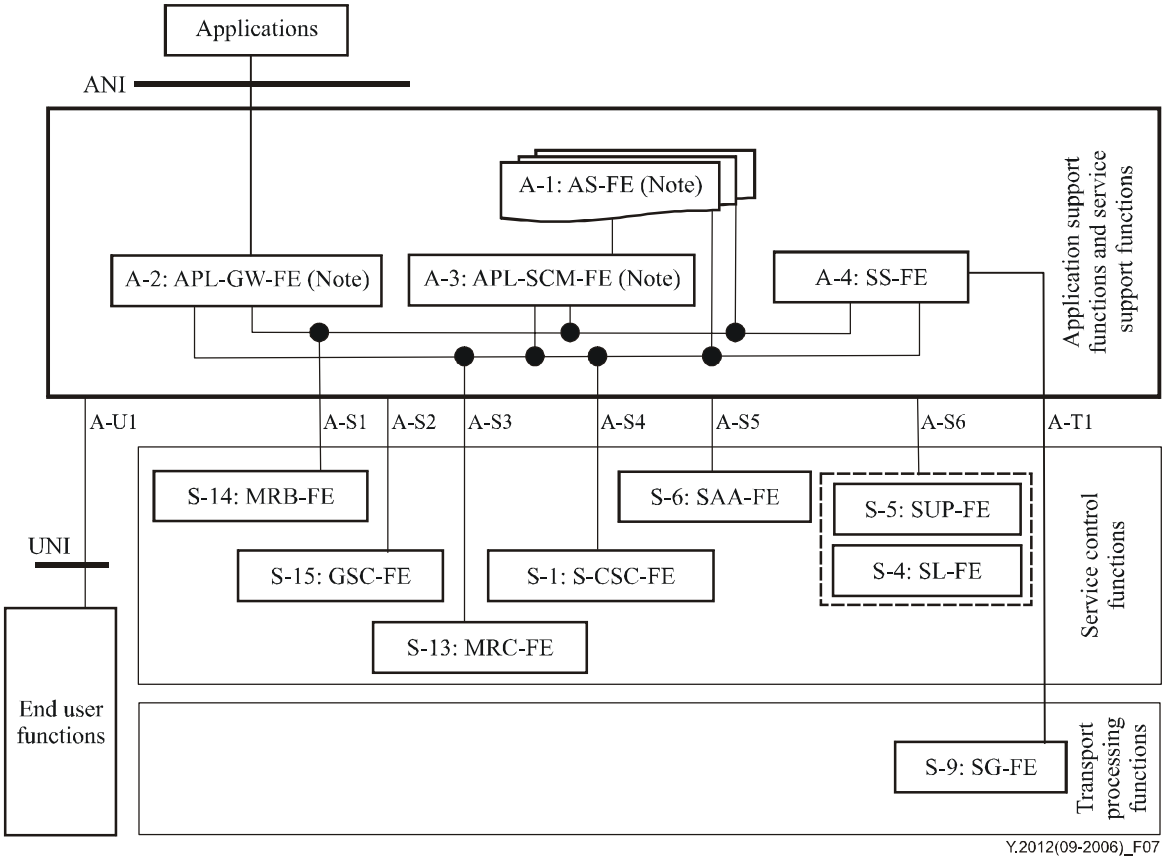
– as a third-party call control (back-to-back user agent).

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 to allow the end-users to securely manage and configure data for their application services.



NOTE – May include authentication, authorization and accounting.

Figure 7 – Application/service support functions

NOTE – 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.

9.3.4.1 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, and so on.

9.3.4.2 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 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 APL-GW-FE are usually realized by OSA application servers.

9.3.4.3 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 application services (or servers). The functional entities of ASF&SSF might interwork with each other via APL-SCM-FE to provide convergent services to the end users.

9.3.4.4 A-4 Service switching functional entity (SS-FE)

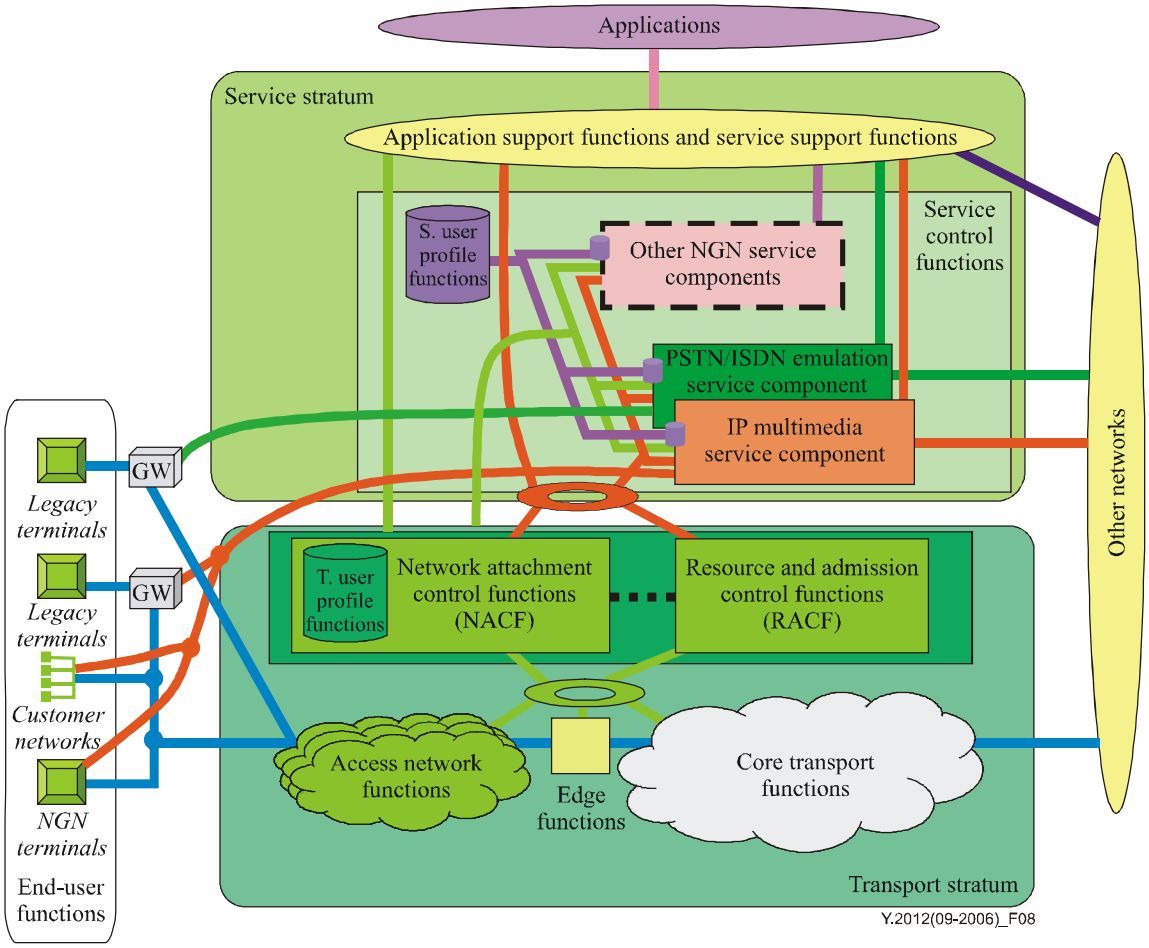
The service switching functional entity (SS-FE) provides access and interworking to a legacy IN SCP. For the IN services, the S-CSC-FE is connected through the SS-FE to the SG-FE to interact with a legacy IN SCP. The SS-FE provides IN service switching functions including service trigger detection, service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

10 NGN components

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

Figure 8 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.



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

Figure 8 – NGN components

For the sake of easy understanding, the representation shown in Figure 8 makes use of colour 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.

In release 1, two components are identified in the service stratum:

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

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

In release 1, two components are identified in the transport stratum: the network attachment control functions (NACF) component and the resource and admission control functions (RACF) 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 and the RACF components.

In the transport stratum, multiple configurations regarding access transport functions are possible. Figure 8 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 may involve media transcoding and bearer adaptation. Interactions between the service stratum and 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, 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

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 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 content delivery services, multimedia multicast or broadcast services, 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 release 1 NACF component may be further specified in a separate Recommendation.

10.2.2 RACF component

The release 1 RACF component is specified in [ITU-T Y.2111].

10.2.3 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.

11 Security considerations

The security requirements within the functional requirements and architecture of the NGN are addressed by the security requirements for NGN release 1 [b-ITU-T Y.2701].

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 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.

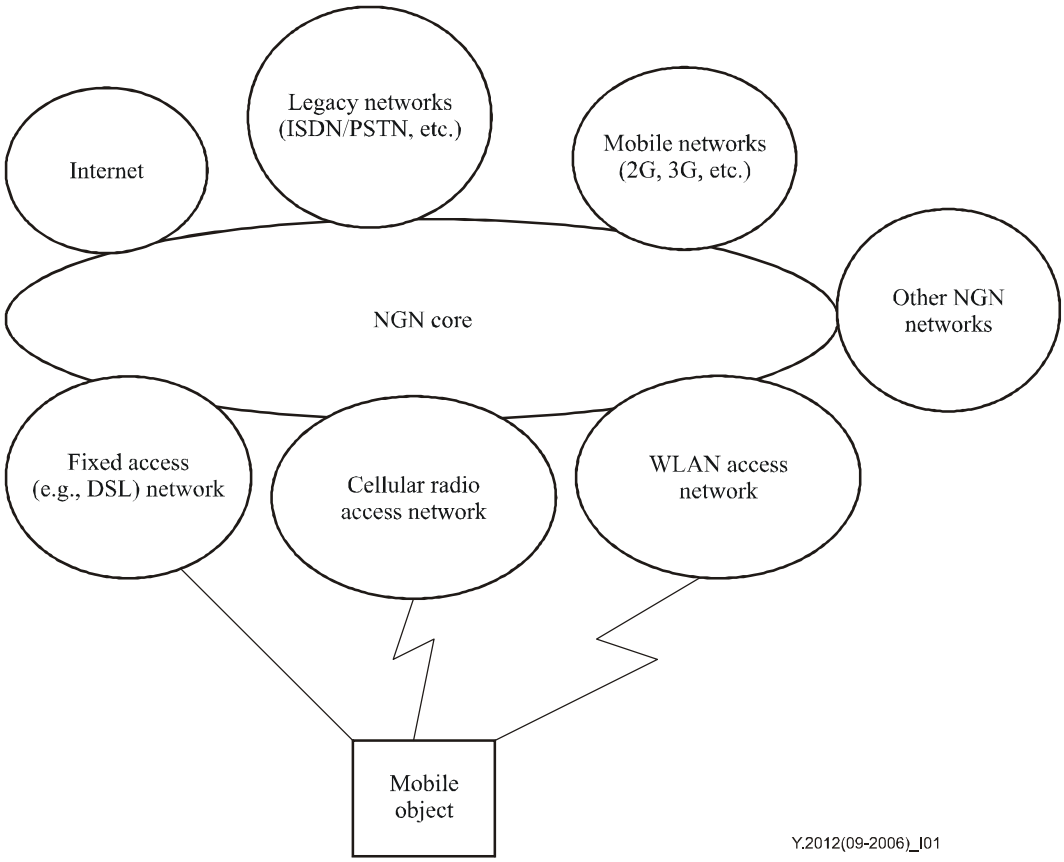


Figure I.1 – NGN core and access networks

In addition to the need to distinguish between the NGN core and 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 an operator holds a subscription for the service being offered to the user. This 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 operator. More typically in the NGN, the home operator will provide the service control for the user while the visited operator will provide only access-related capabilities, such as support for authentication, support for authorization, data integrity services, and QoS support.

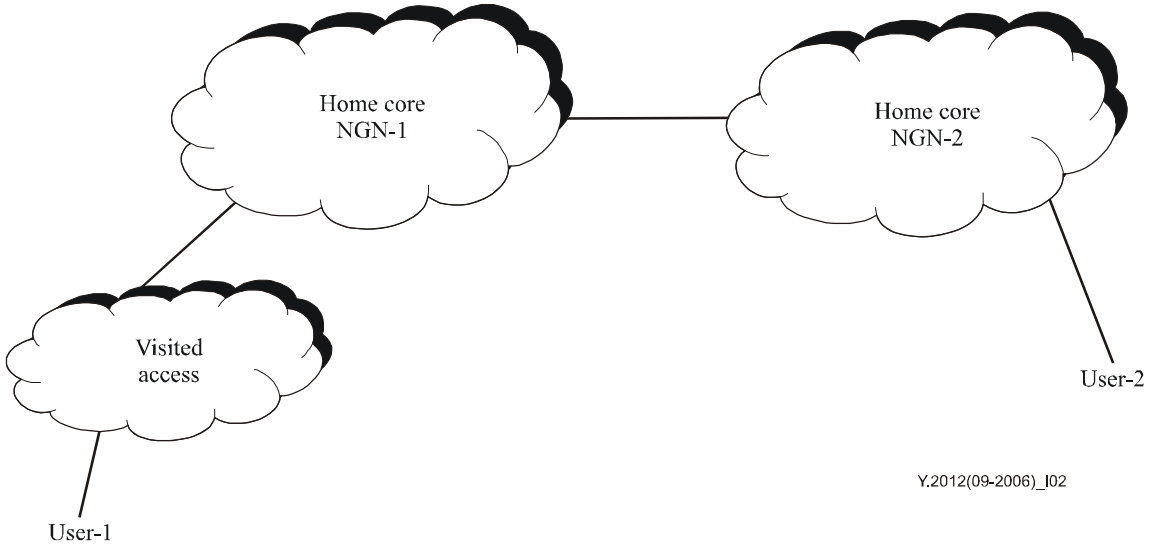


Figure I.2 – NGN example of home and visited networks

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 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 visited operator's NGN core network.

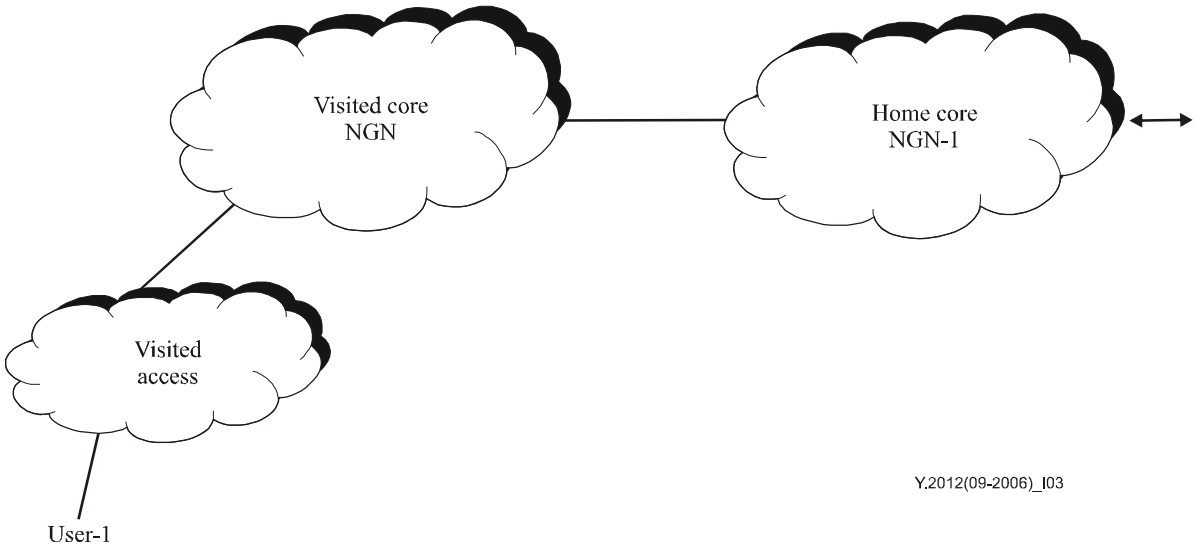


Figure I.3 – NGN example of visited NGN core network support

Since, in many cases, the specific division of functionality between the core and access networks, between the home and visited networks, and between the originating and terminating networks is based on the 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 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 subnetworks, 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.

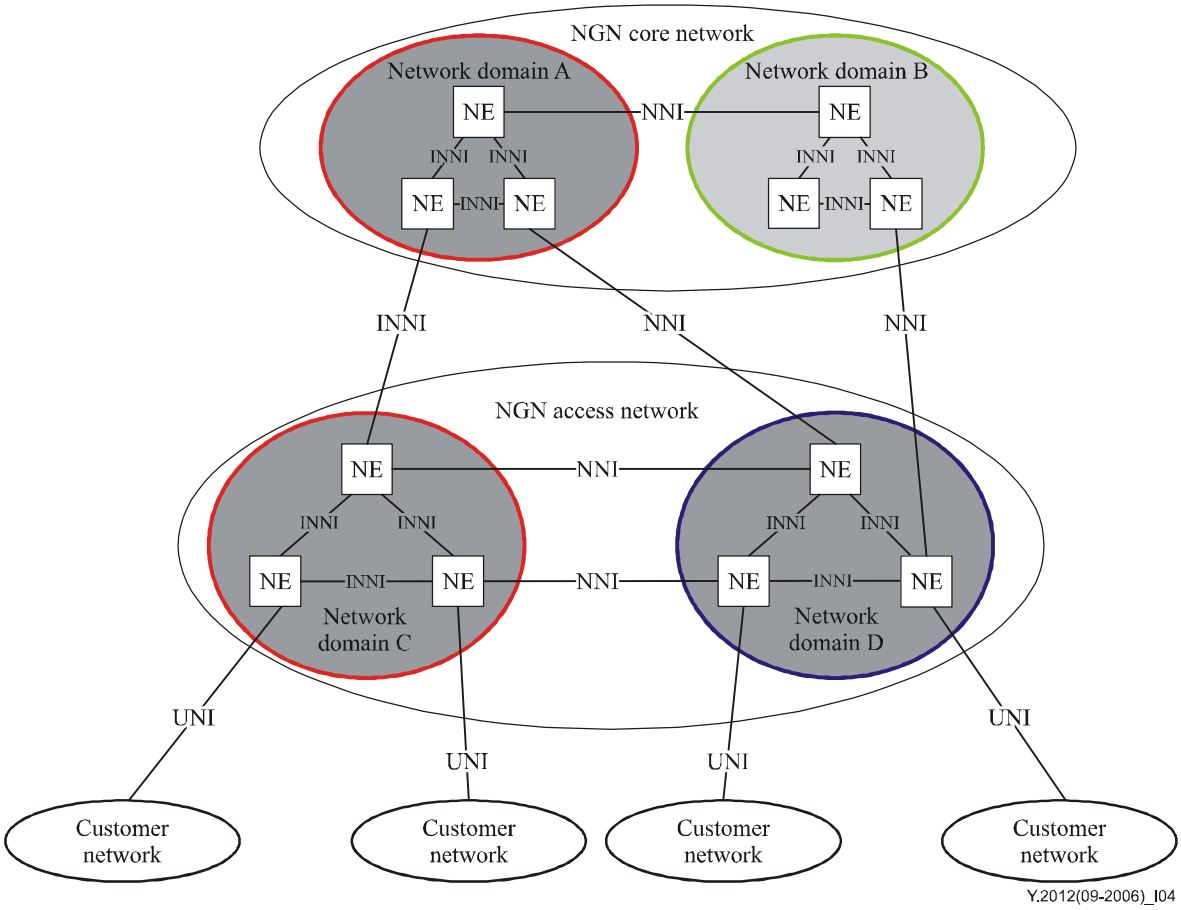


Figure I.4 – Major components of the NGN at the network level

The major components of an NGN network are as follows:

- End-user network: An end-user network can be a network within a home or an enterprise network. It is connected to the service provider's network via a UNI (user-to-network interface). The UNI is also the demarcation point between the service provider and the user. An end-user network may obtain its content service from:
  - the core network;
  - another instance of the end-user network providing public services; or
  - another instance of the end-user 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 service 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 an 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 service 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 an 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 above, 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 service provider 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.

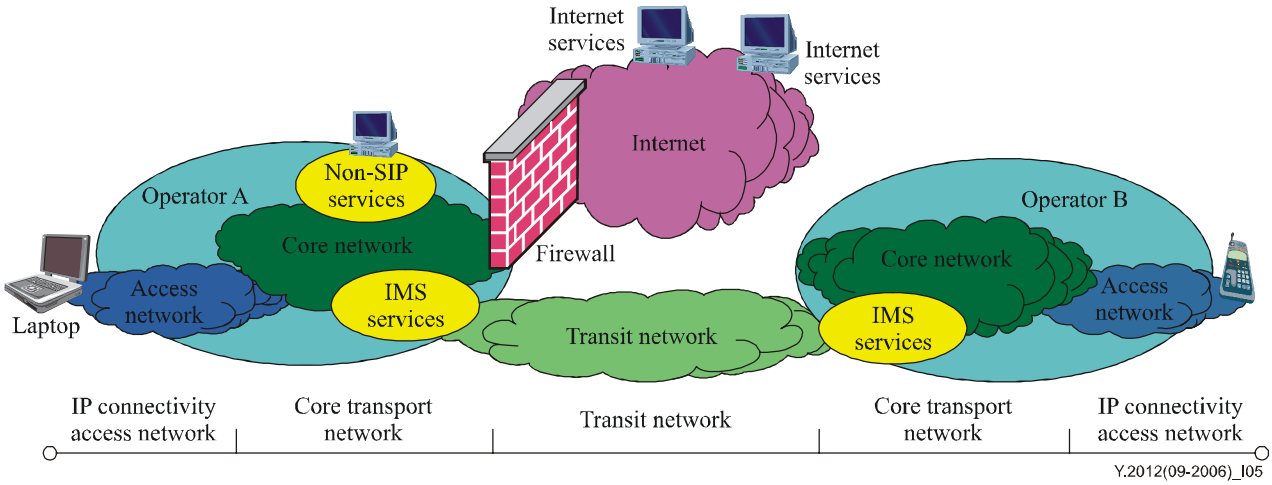


Figure I.5 – NGN example of service domains

In this example, 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 operator A's domain or may support end-to-end services to other operators. In this example, operator A supports end-to-end IMS services along with 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 operator A is directly connected to the other endpoint network. In some cases, firewalls or other gateway elements might be used to protect the 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 operator A. This would provide services such as streaming video. These service entities may be attached directly to operator A's core network 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 not part of operator A's domain, nor are they provided by business arrangements with operator A. These services are accessed by operator A providing a transport connection to the Internet. Such a connection by 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-ITU-T UMTS 22.01], but we have modified the names to better align 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.

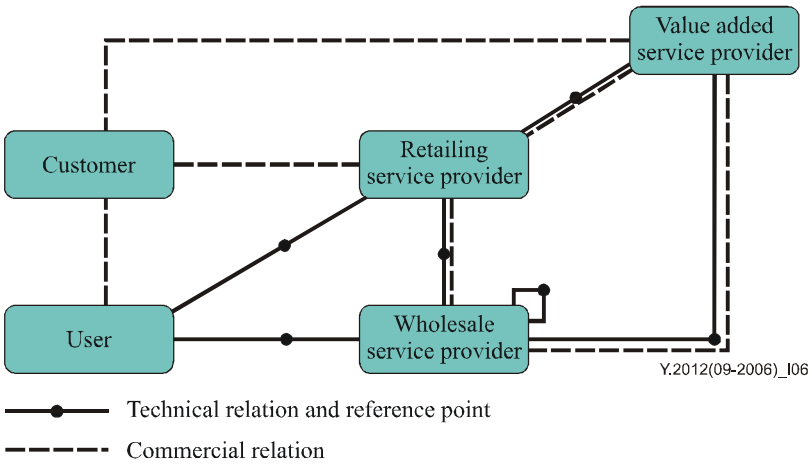


Figure I.6 – Basic NGN roles

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 the FRA. 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 123101]. 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 123101]. 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 123228] defines an IP connectivity access network (IP-CAN) as the non-IMS part of a complete network solution, excluding terminals. It is not an access network domain as defined in [b-ETSI TS 123101], nor does it map to the access service provider role.

The first step in wholesale provider specialization (subclassing) is shown is Figure I.7.

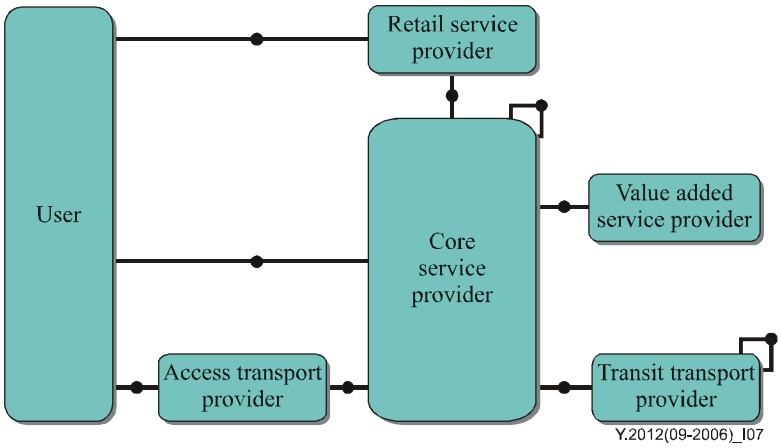


Figure I.7 – NGN roles: First level of specialization

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-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.

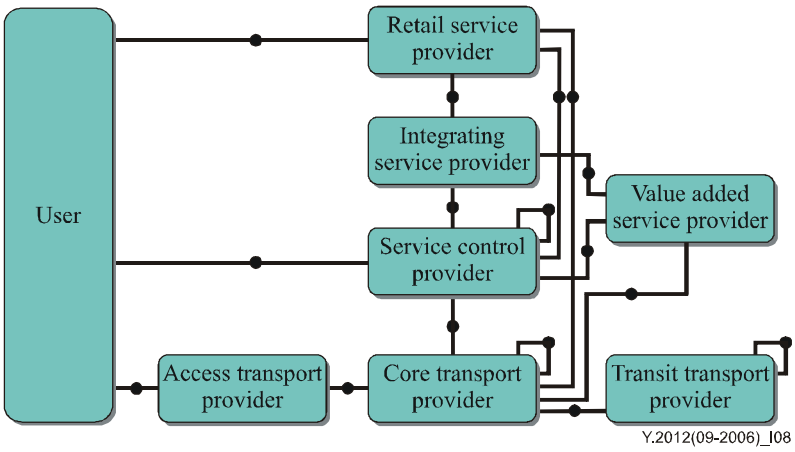


Figure I.8 – NGN roles: Second level of specialization

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.

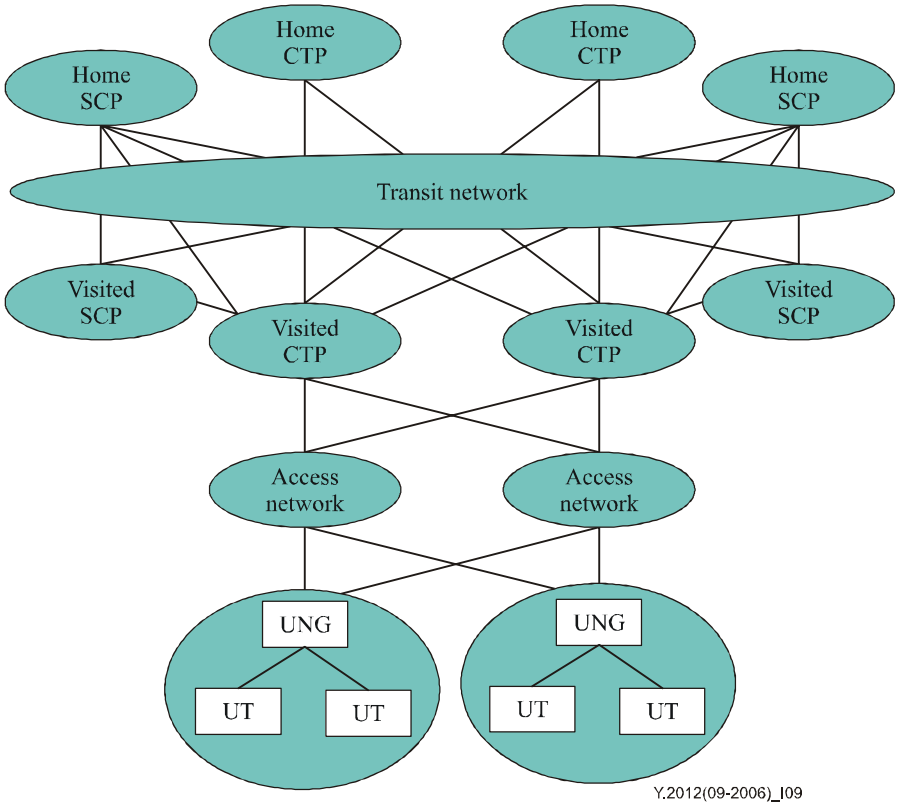
I.5 Functional roles

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 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. In release 1, the UNG will be 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-3GPP 24.234]. 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, and release 1 will take longer to complete if it has to support the business model shown in Figure I.8, as opposed to the simpler one shown in Figure I.7.



CTP Core transport provider
SCP Service control provider
UNG User network gateway
UT User terminal

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 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 release 1. 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

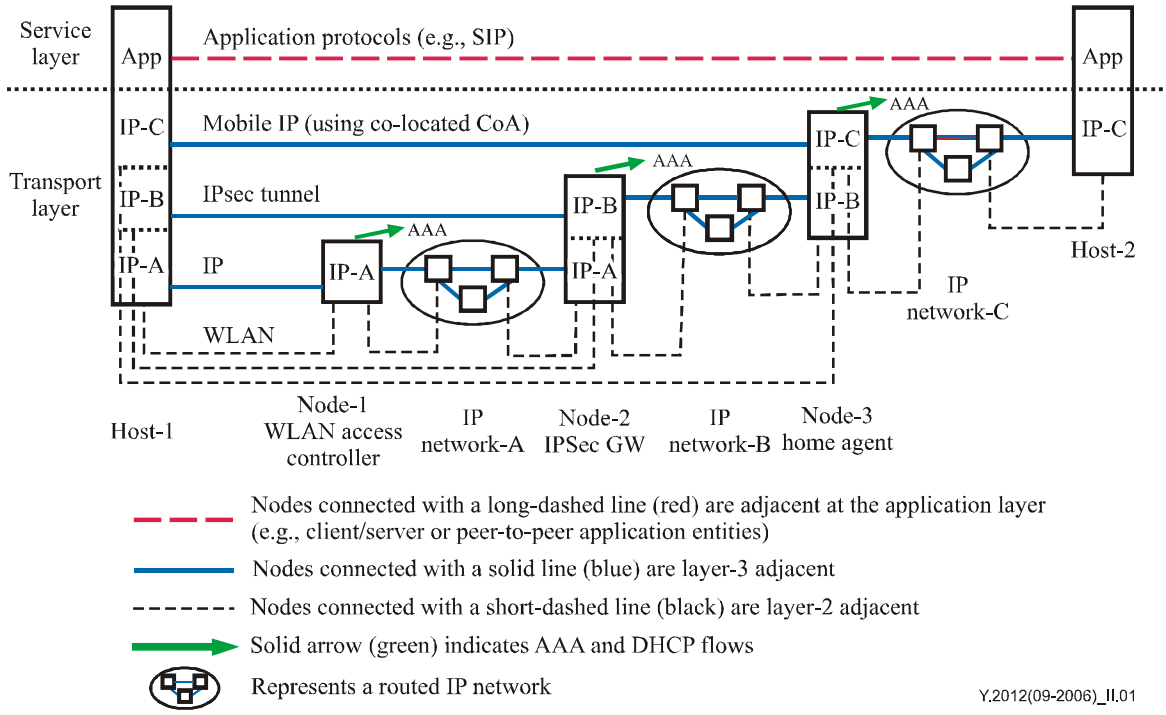


Figure II.1 – Multi-layered transport stratum

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 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 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

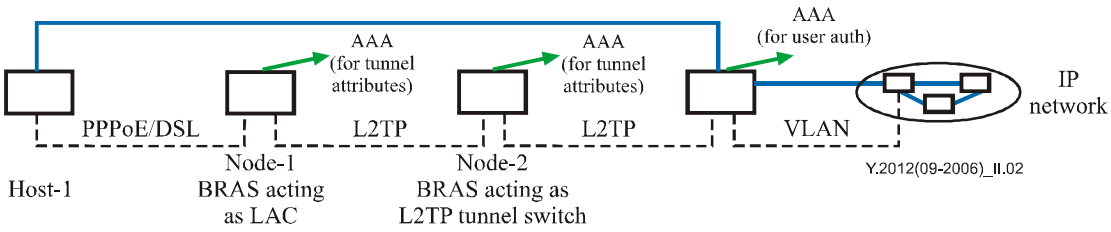


Figure II.2 – Access aggregation using layer-2

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., 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 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 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 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

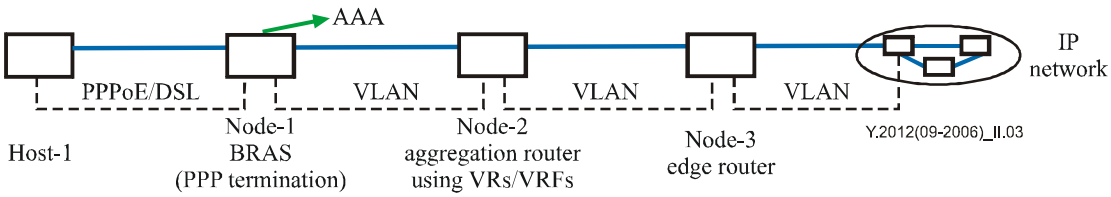


Figure II.3 – Access aggregation using layer-3

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 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: Multi-stage policy enforcement

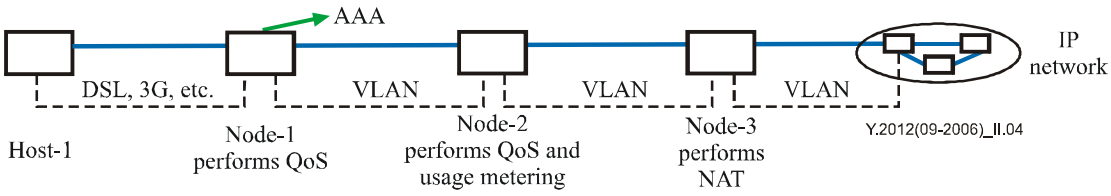


Figure II.4 – Multi-stage policy enforcement

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

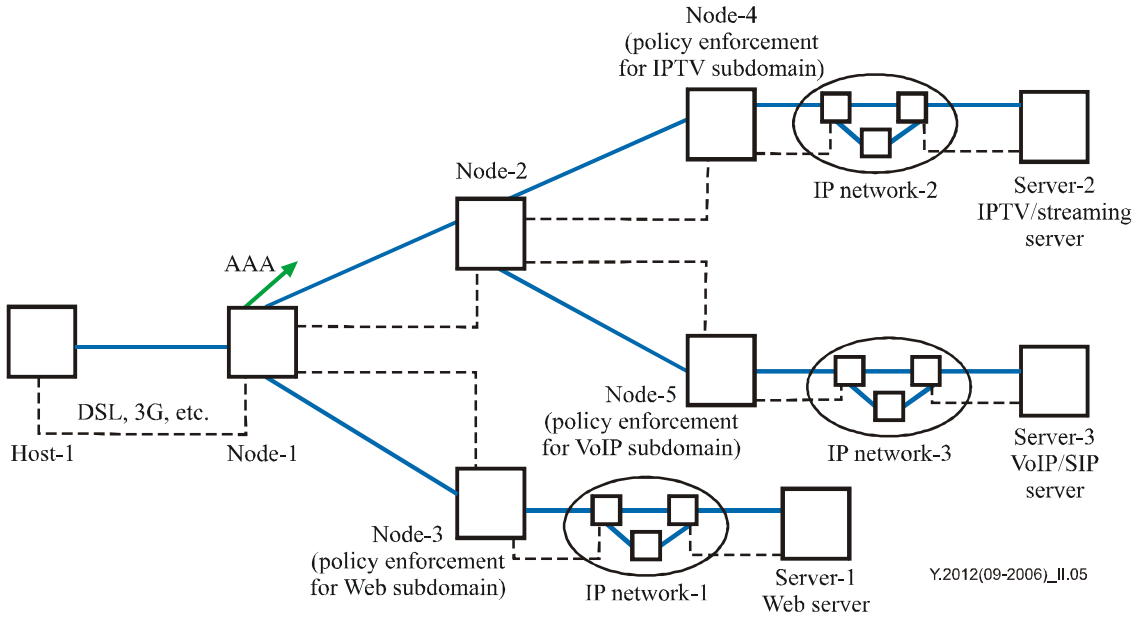


Figure II.5 – Partitioning into transport-layer traffic subdomains

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 subdomain 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 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.

Bibliography

[b-ITU-T Y.110] ITU-T Recommendation Y.110 (1998), *Global information infrastructure principles and framework architecture*.

[b-ITU-T Y.2000-series Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *NGN release 1 scope*.

[b-ITU-T Y.2201] ITU-T Recommendation Y.2201 (2007), *NGN release 1 requirements*.

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

[b-ITU-T UMTS 22.01] UMTS 22.01, *Universal Mobile Telecommunications System (UMTS); Service aspects, Service principles*.

[b-ETSI TS 123101] ETSI TS 123 101 V6.0.0 (2004), *Universal Mobile Telecommunications System (UMTS); General UMTS Architecture*.

[b-ETSI TS 123228] ETSI TS 123 228 V6.16.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2*.

[b-3GPP 24.234] 3GPP TS 24.234 v6.4.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3GPP system to WLAN Interworking; System description*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007