

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2012

(04/2010)

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

Next Generation Networks – Frameworks and functional
architecture models

Functional requirements and architecture of next generation networks

Recommendation ITU-T Y.2012



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

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

Recommendation ITU-T Y.2012

Functional requirements and architecture of next generation networks

Summary

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

History

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

Keywords

Functional architecture, functional entities, NGN.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2010

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

CONTENTS

	Page
1 Scope	1
2 References.....	1
3 Definitions	3
3.1 Terms defined elsewhere	3
3.2 Terms defined in this Recommendation.....	4
4 Abbreviations and acronyms	5
5 Conventions	10
6 General principles of the NGN functional architecture	11
6.1 General characteristics.....	11
6.2 Connectivity to the NGN.....	12
7 Overview of the NGN architecture.....	13
7.1 Transport stratum functions.....	15
7.2 Service stratum functions	17
7.3 End-user functions.....	18
7.4 Management functions	18
7.5 Identity management (IdM) functions.....	19
8 NGN concepts.....	20
8.1 Mobility levels in the NGN architecture	20
8.2 NGN service architecture	20
8.3 Network topology hiding functions and NAPT traversal functions.....	21
8.4 Overload control.....	21
8.5 Charging and accounting functions (CAF).....	22
9 Generalized NGN functional architecture	25
9.1 NGN functional architecture framework.....	25
9.2 NGN functional entities (FEs).....	26
9.3 Functional entity descriptions.....	27
9.4 Reference points	52
10 NGN components	57
10.1 NGN service-specific components	59
10.2 NGN transport-specific components	60
10.3 Management functions	60
11 Security considerations.....	60
Annex A – Differences between this edition and the 2006 edition of Recommendation ITU-T Y.2012.....	61

	Page
Annex B – Support of IPTV services	62
B.1 Overall functional mapping between NGN-based IPTV and NGN architectures.....	62
B.2 IMS-based IPTV functional architecture.....	63
B.3 Non-IMS-based IPTV architecture.....	65
Appendix I – Examples of NGN network configurations.....	68
I.1 Configurations and topology of the NGN	68
I.2 Relationship between the NGN and administrative domains.....	70
I.3 Relationship between the NGN and service domains	72
I.4 Enterprise role model	73
I.5 Functional roles	75
Appendix II – Transport-stratum access network scenarios	77
II.1 Introduction	77
II.2 Scenario 1: Multi-layered transport stratum.....	77
II.3 Scenario 2: Access aggregation using layer-2.....	78
II.4 Scenario 3: Access aggregation using layer-3.....	79
II.5 Scenario 4: Multistage policy enforcement.....	80
II.6 Scenario 5: Partitioning into transport-layer traffic subdomains	81
Appendix III – Instantiation of NGN reference points	82
III.1 Introduction	82
III.2 Scope	82
III.3 Rationale to consider SNI.....	82
III.4 Instantiation of NGN reference points	82
Appendix IV – Example illustrative deployment scenario for IdM in NGN.....	85
Bibliography.....	87

Recommendation ITU-T Y.2012

Functional requirements and architecture of next generation networks

1 Scope

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

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

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

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

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

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

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|----------------|---|
| [ITU-T G.722] | Recommendation ITU-T G.722 (1988), <i>7 kHz audio-coding within 64 kbit/s</i> . |
| [ITU-T G.8010] | Recommendation ITU-T G.8010/Y.1306 (2004), <i>Architecture of Ethernet layer networks</i> . |
| [ITU-T M.1400] | Recommendation ITU-T M.1400 (2006), <i>Designations for interconnections among operators' networks</i> . |
| [ITU-T M.3060] | Recommendation ITU-T M.3060/Y.2401 (2006), <i>Principles for the Management of the Next Generation Networks</i> . |

[ITU-T Q.1706]	Recommendation ITU-T Q.1706/Y.2801 (2006), <i>Mobility management requirements for NGN.</i>
[ITU-T Y.101]	Recommendation ITU-T Y.101 (2000), <i>Global Information Infrastructure terminology: Terms and definitions.</i>
[ITU-T Y.1291]	Recommendation ITU-T Y.1291 (2004), <i>An architectural framework for support of quality of service in packet networks.</i>
[ITU-T Y.1453]	Recommendation ITU-T Y.1453 (2006), <i>TDM-IP interworking – user plane interworking.</i>
[ITU-T Y.1901]	Recommendation ITU-T Y.1901 (2009), <i>Requirements for the support of IPTV services.</i>
[ITU-T Y.1910]	Recommendation ITU-T Y.1910 (2008), <i>IPTV functional architecture.</i>
[ITU-T Y.2001]	Recommendation ITU-T Y.2001 (2004), <i>General overview of NGN.</i>
[ITU-T Y.2011]	Recommendation ITU-T Y.2011 (2004), <i>General principles and general reference model for Next Generation Networks.</i>
[ITU-T Y.2014]	Recommendation ITU-T Y.2014 (2010), <i>Network attachment control functions in next generation networks.</i>
[ITU-T Y.2017]	Recommendation ITU-T Y.2017 (2009), <i>Multicast functions in next generation networks.</i>
[ITU-T Y.2018]	Recommendation ITU-T Y.2018 (2009), <i>Mobility management and control framework and architecture within the NGN transport stratum.</i>
[ITU-T Y.2021]	Recommendation ITU-T Y.2021 (2006), <i>IMS for Next Generation Networks.</i>
[ITU-T Y.2031]	Recommendation ITU-T Y.2031 (2006), <i>PSTN/ISDN emulation architecture.</i>
[ITU-T Y.2091]	Recommendation ITU-T Y.2091 (2008), <i>Terms and definitions for Next Generation Networks.</i>
[ITU-T Y.2111]	Recommendation ITU-T Y.2111 (2008), <i>Resource and admission control functions in Next Generation Networks.</i>
[ITU-T Y.2171]	Recommendation ITU-T Y.2171 (2006), <i>Admission control priority levels in Next Generation Networks.</i>
[ITU-T Y.2173]	Recommendation ITU-T Y.2173 (2008), <i>Management of performance measurement for NGN.</i>
[ITU-T Y.2201]	Recommendation ITU-T Y.2201 (2009), <i>Requirements and capabilities for ITU-T NGN.</i>
[ITU-T Y.2233]	Recommendation ITU-T Y.2233 (2008), <i>Requirements and framework allowing accounting and charging capabilities in NGN.</i>
[ITU-T Y.2234]	Recommendation ITU-T Y.2234 (2008), <i>Open service environment capabilities for NGN.</i>
[ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), <i>Security requirements for NGN release 1.</i>
[ITU-T Y.2702]	Recommendation ITU-T Y.2702 (2008), <i>Authentication and authorization requirements for NGN release 1.</i>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

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



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

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

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

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

5 Conventions

The following conventions apply:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2) In this Recommendation:

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

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

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

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

6 General principles of the NGN functional architecture

6.1 General characteristics

The NGN functional architecture incorporates the following principles:

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

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

6.2 Connectivity to the NGN

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

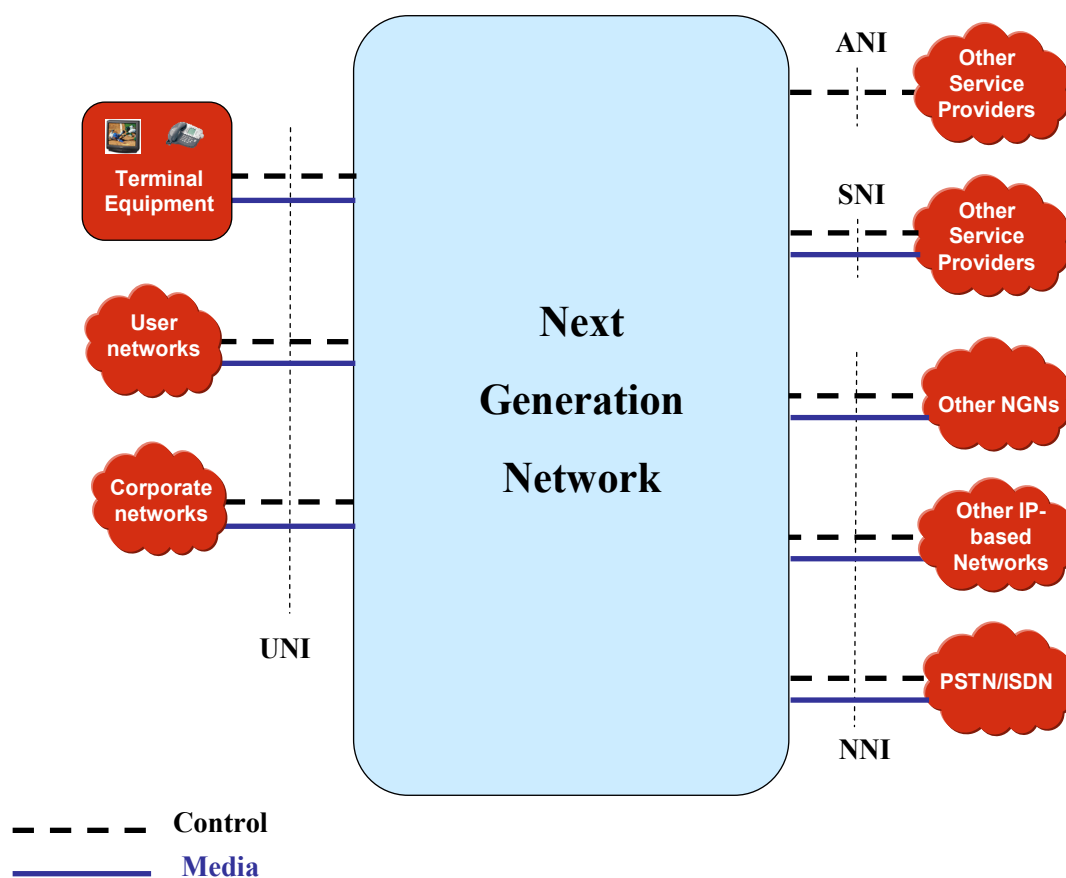


Figure 6-1 – Connectivity to the NGN

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

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

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

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

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

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

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

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

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

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

7 Overview of the NGN architecture

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

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

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

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

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

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

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

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

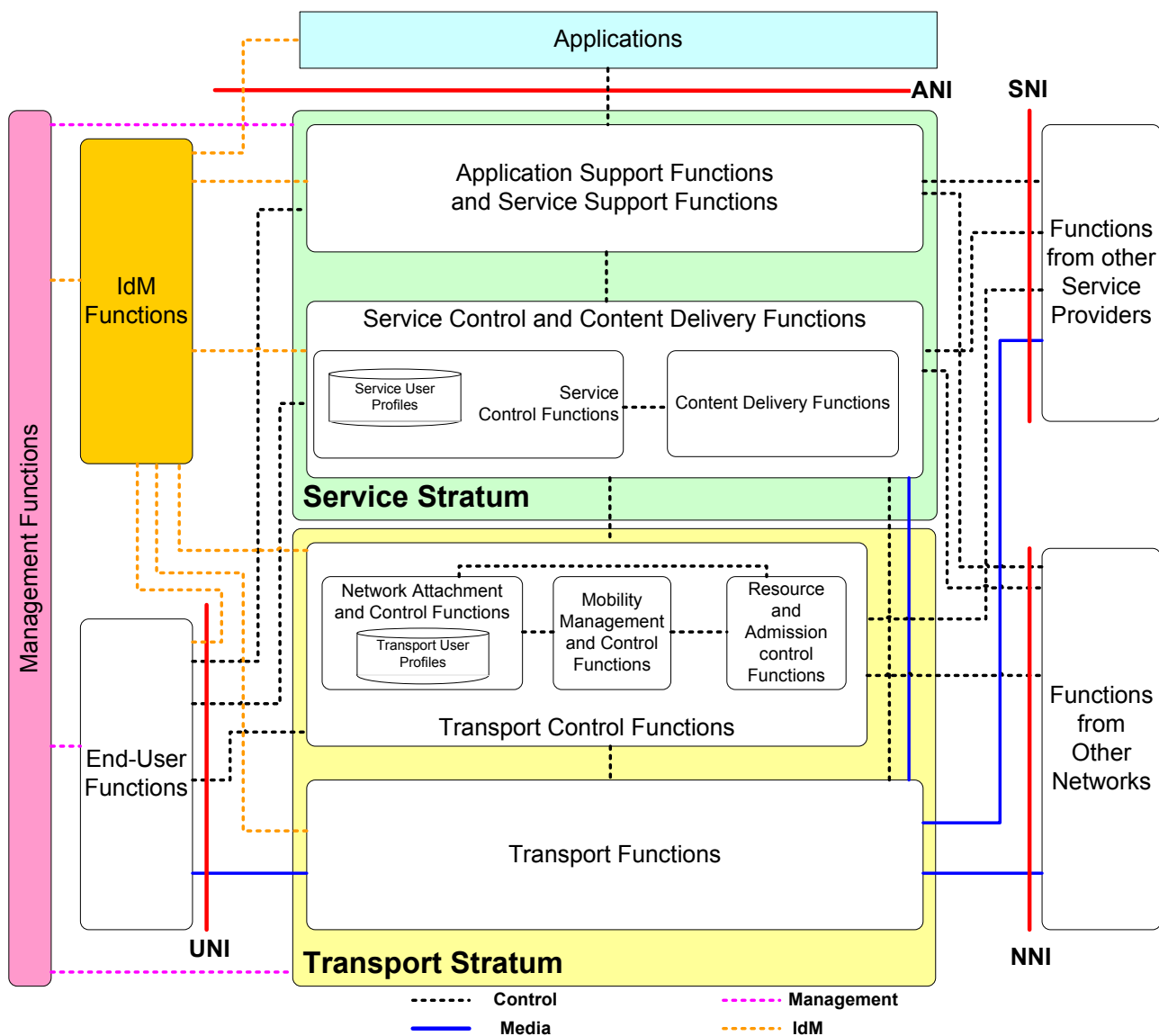


Figure 7-1 – NGN architecture overview

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

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

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

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

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

NOTE 6 – Since Figure 7-1 is drawn from a high-level conceptual point of view, instantiation of the NGN reference points, namely UNI, NNI, ANI and SNI, is useful to clarify the specific role of these different

reference points in terms of service offering and the physical implementation entailed. The instantiation of NGN reference points is given in Appendix III.

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

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

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

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

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

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

7.1 Transport stratum functions

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

7.1.1 Transport functions

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

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

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

7.1.1.1 Access network functions

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

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

- 1) Cable access;
- 2) xDSL access;
- 3) Wireless access (e.g., [b-IEEE 802.11] and [b-IEEE 802.16] technologies, and 3G RAN access);
- 4) Optical access.

7.1.1.2 Edge functions

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

The edge functions are also used between core transport networks.

7.1.1.3 Core transport functions

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

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

7.1.1.4 Gateway functions

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

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

7.1.1.5 Media handling functions

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

7.1.2 Transport control functions

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

7.1.2.1 Resource and admission control functions (RACF)

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

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

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

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

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

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

7.1.2.2 Network attachment control functions (NACF)

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

The NACF provides the following functionalities:

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

The NACF includes the transport user profile which takes the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

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

7.1.2.3 Mobility management and control functions (MMCF)

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

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

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

7.2 Service stratum functions

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

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

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

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

7.2.1.1 Service control functions (SCF)

The service control functions (SCF) include resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services. They can

also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level.

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

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

7.2.1.2 Content delivery functions (CDF)

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

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

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

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

7.3 End-user functions

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

7.4 Management functions

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

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

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

- a) Fault management;
- b) Configuration management;
- c) Accounting management;
- d) Performance management including what is specified in [ITU-T Y.2173];
- e) Security management.

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

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

7.5 Identity management (IdM) functions

7.5.1 Overview

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

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

- Identifiers, e.g., UserID, email addresses, telephone numbers, URI and IP addresses;
- Credentials, e.g., digital certificates, tokens and biometrics;
- Attributes, e.g., roles, claims, privileges, patterns and location.

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

- assurance of identity information,
- assurance of the identity of an entity, and
- enabling and supporting business and security applications.

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

7.5.2 IdM framework

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

- Identity lifecycle management;
- Identity management (IdM) operation, administration, maintenance and provisioning (OAMP) functions;
- Identity management (IdM) signalling and control functions;
- Identity management (IdM) federated identity functions;
- Identity management (IdM) user and subscriber functions;
- Identity management (IdM) performance, reliability, and scalability;
- Identity management (IdM) security;
- Identity management (IdM) legal and regulatory rules;

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

7.5.3 Architectural model

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

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

- applications;
- service stratum: application support functions and service support functions, service control functions and content delivery functions;
- transport stratum: transport control functions and transport functions;
- end-user functions;
- management functions.

8 NGN concepts

8.1 Mobility levels in the NGN architecture

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

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

8.2 NGN service architecture

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

- a) "Applications";
- b) "Application support functions and service support functions" in the service stratum of the NGN;
- c) NGN resources and capabilities, including those in the transport stratum, capabilities such as presence, location information, charging function, security schemes, etc.

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

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

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

- a) Agnosticism: application support and service support functions areas consist of functions that are agnostic with respect to their underlying NGN infrastructure.
- b) Support for legacy capabilities and features: there are no limiting impacts on the NGN as a result of this NGN service architecture. On the contrary, the use of NGN capabilities such as session management, authentication, location information, charging is supported. For example, the legacy-IN-influenced features of the IMS, such as triggers, filter criteria, and

the service capability interaction manager, are available through the abstraction of the IMS AS (application server) in the "application support functions and service support functions" area.

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

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

8.3 Network topology hiding functions and NAPT traversal functions

8.3.1 Service stratum topology hiding

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

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

8.3.2 Transport stratum topology hiding

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

Examples of transport stratum topology hiding are as follows:

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

8.3.3 Remote NAPT traversal

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

8.4 Overload control

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

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

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

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

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

8.5 Charging and accounting functions (CAF)

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

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

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

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

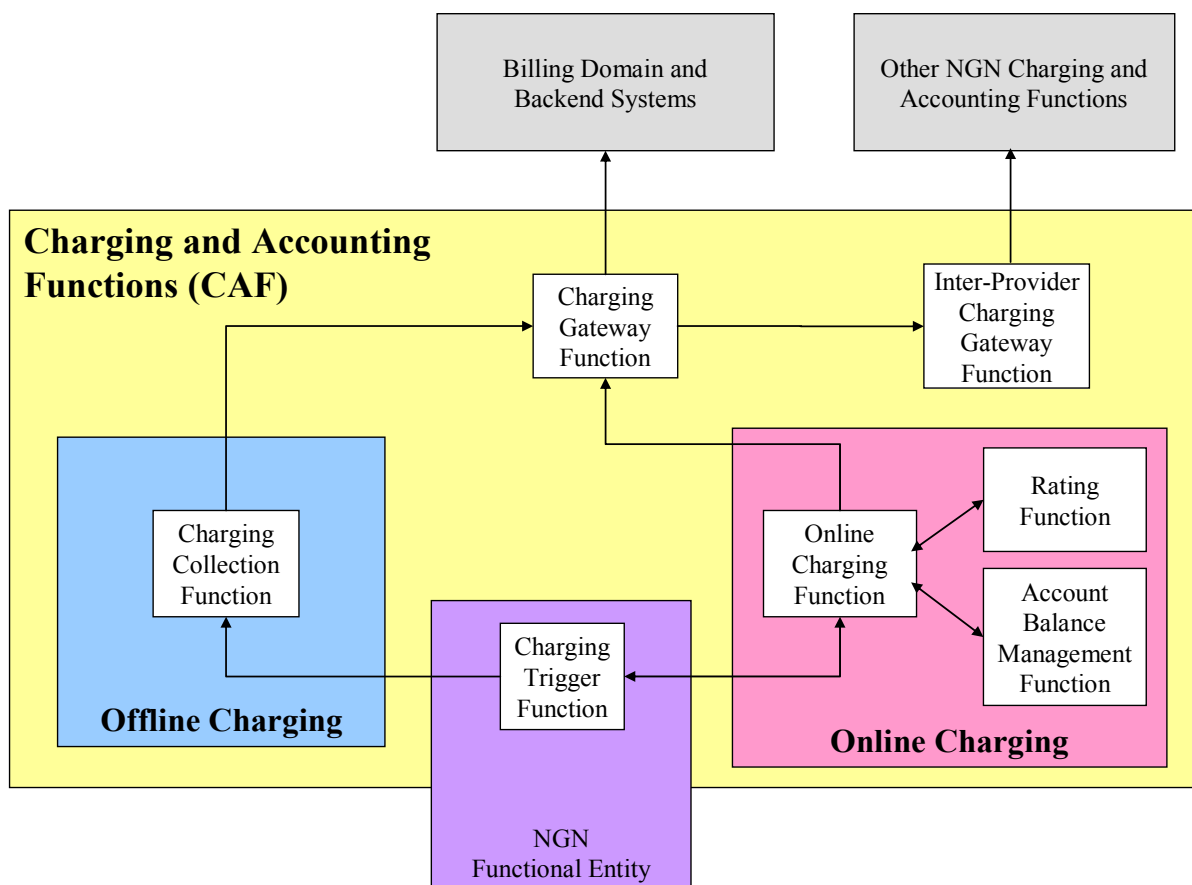


Figure 8-1 – Charging and accounting functions

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

8.5.1 Charging trigger function (CTF)

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

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

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