International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2201

(04/2007)

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

Next Generation Networks – Service aspects: Service capabilities and service architecture

NGN release 1 requirements

ITU-T Recommendation Y.2201

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.2201

NGN release 1 requirements

Summary

ITU-T Recommendation Y.2201 provides high-level requirements for services and capabilities of Next Generation Network (NGN) release 1.

Source

ITU-T Recommendation Y.2201 was approved on 27 April 2007 by ITU-T Study Group 13 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

accounting, addressing, authentication, authorization, capabilities, capability requirements, charging, identification, interoperability, interworking, management, mobility, naming, NGN release 1, numbering, OAM, open service environment, policy, privacy, profile, PSTN/ISDN emulation, PSTN/ISDN simulation, QoS, security, service enabler

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.2201

NGN release 1 requirements

1 Scope

This Recommendation specifies high-level requirements for the development of a set of ITU-T Recommendations which will constitute NGN release 1.

The high-level requirements and related capabilities specified in this Recommendation are aligned with the general goals and objectives captured in [ITU-T Y.2001] and are based on the objectives of NGN release 1 identified in [b-ITU-T Y-Sup.1]. NGN is required to provide at least one level of service that offers capabilities that are the same or better than those provided by circuit-switched networks.

More detailed requirements and service-specific requirements are outside the scope of this Recommendation. While requirements on user equipment are outside the scope of this Recommendation, requirements associated with access arrangements are within the scope.

It is recognized that a specific realization of NGN may be constituted by a set (or superset) of services supported in NGN release 1 and of capabilities as specified in this Recommendation.

Administrations may require 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 E.106] ITU-T Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[ITU-T E.107] ITU-T Recommendation E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[ITU-T E.164] ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*.

[ITU-T E.212] ITU-T Recommendation E.212 (2004), *The international identification plan for mobile terminals and mobile users*.

[ITU-T G.711] ITU-T Recommendation G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

[ITU-T G.780] ITU-T Recommendation G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[ITU-T G.808.1] ITU-T Recommendation G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T I.610] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[ITU-T M.3050.0] ITU-T Recommendation M.3050.0 (2007), *Enhanced Telecom Operations Map (eTOM) – Introduction*.

[ITU-T M.3050.1] ITU-T Recommendation M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework*.

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

[ITU-T Q.825] ITU-T Recommendation Q.825 (1998), *Specification of TMN applications at the Q3 interface: Call detail recording*.

[ITU-T Q.1703] ITU-T Recommendation Q.1703 (2004), *Service and network capabilities framework of network aspects for systems beyond IMT-2000*.

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

[ITU-T Q.1741.1] ITU-T Recommendation Q.1741.1 (2002), *IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network*.

[ITU-T Q.1741.2] ITU-T Recommendation Q.1741.2 (2002), *IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network*.

[ITU-T Q.1741.3] ITU-T Recommendation Q.1741.3 (2003), *IMT-2000 references to release 5 of GSM evolved UMTS core network*.

[ITU-T Q.1741.4] ITU-T Recommendation Q.1741.4 (2005), *IMT-2000 references to release 6 of GSM evolved UMTS core network*.

[ITU-T X.462] ITU-T Recommendation X.462 (1996), *Information technology – Message Handling Systems (MHS) Management: Logging information*.

[ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

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

[ITU-T Y.110] ITU-T Recommendation Y.110 (1998), *Global Information Infrastructure principles and framework architecture*.

[ITU-T Y.1271] ITU-T Recommendation Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-witched and packet-switched networks*.

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

[ITU-T Y.1710] ITU-T Recommendation Y.1710 (2002), *Requirements for Operation & Maintenance functionality in MPLS networks*.

[ITU-T Y.1730] ITU-T Recommendation Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

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

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

[ITU-T Y.2091] ITU-T Recommendation Y.2091 (2007), *Terms and definitions for Next Generation Network*.

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

[ITU-T Z.100] ITU-T Recommendation Z.100 (2002), *Specification and Description Language (SDL)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 accounting [ITU-T X.462]: The action of collecting information on the operations performed within a system and the effects thereof.

3.1.2 address [ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.3 application network interface (ANI) [ITU-T Y.2012]: 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.

3.1.4 billing [ITU-T Q.1703]: Administrative function to prepare bills to service customers, to prompt payments, to obtain revenues and to take care of customer reclaims.

3.1.5 charging [ITU-T Q.825]: The set of functions needed to determine the price assigned to the service utilization.

3.1.6 corporate network [ITU-T Y.2701]: A private network that supports multiple users and may be in multiple locations (e.g., an enterprise, campus).

3.1.7 customer [ITU-T M.3050.1]: The customer buys products and services from the enterprise or receives free offers or services. A customer may be a person or a business.

3.1.8 end user [ITU-T M.3050.1]: The end user is the actual user of the products or services offered by the Enterprise. The end user consumes the product or service. See also Subscriber.

3.1.9 handover [ITU-T Q.1706]: The ability to provide services with some impact on their service level agreements to a moving object during and after movement.

3.1.10 home network [ITU-T E.212]: The network of the service provider to which a given subscriber is subscribed.

3.1.11 identifier [ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.12 internet [ITU-T Y.101]: A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network.

3.1.13 mobility [ITU-T Y.2001]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment. The degree of service availability may depend on several factors including the access network capabilities, service level agreements between the user's home network and the visited network (if applicable), etc. Mobility includes the ability of telecommunication with or without service continuity.

NOTE – In [ITU-T Y.2001] this is called "generalized mobility".

3.1.14 mobility management [ITU-T Q.1706]: The set of functions used to provide mobility.

NOTE – These functions include authentication, authorization, location updating, paging, download of user information and more.

3.1.15 nomadism [ITU-T Q.1706]: 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.

3.1.16 personal mobility [ITU-T Q.1706]: This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

3.1.17 roaming [ITU-T Q.1706]: This is the ability of users to access services according to their user profile while outside of their subscribed home network, i.e., by using an access point of a visited network. This requires the capability for access to the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators.

3.1.18 seamless handover [ITU-T Q.1706]: It is a special case of mobility with service continuity since it preserves the ability to provide services without any impact on their service level agreements to a moving object during and after movement.

3.1.19 service [ITU-T Z.100]: A set of functions and facilities offered to a user by a provider.

3.1.20 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.

3.1.21 subscriber [ITU-T M.3050.1]: The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services.

3.1.22 terminal mobility [ITU-T Q.1706]: This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

3.1.23 user network [ITU-T Y.2701]: A private network consisting of terminal equipment that may have multiple users.

3.1.24 visited network [ITU-T Q.1706]: The network that is local to the customer in a roaming configuration.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 priority classification: Classification of traffic classes according to different levels of priorities.

3.2.2 priority enabling mechanisms: The mechanisms by which appropriate treatment of traffic according to priority classes may be enabled in the network.

3.2.3 priority signalling: Part of the priority enabling mechanisms using signalling.

3.2.4 single sign-on: The ability to use an authentication assertion from one network operator/service provider to another operator/provider for a user either accessing a service or roaming into a visited network.

3.2.5 terminal equipment identifier: A unique identifier of a terminal equipment.

3.2.6 user: A user includes end user [ITU-T Y.2091], person, subscriber, system, equipment, terminal (e.g., FAX, PC), (functional) entity, process, application, provider, or corporate network.

3.2.7 user attribute: A characteristic that describes the user (e.g., user identifier's lifetime, user status as being "available", "don't disturb", etc.).

3.2.8 user identifier: A type of password, image, or pseudonym associated with a user, assigned by and exchanged between operators and service providers to identify a user, to authenticate her/his identifier and/or authorize the use of service. Examples are identifiers such as SIP URI, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ANI Application Network Interface

API Application Programming Interface

ATM Asynchronous Transfer Mode

B2B Business-to-Business

CC Content of Communication

CD/DVD Compact Disk/Digital Versatile Disk

DNS Domain Name System

DTMF Dual Tone Multi Frequency

ENUM tElephone NUmber Mapping

ETS Emergency Telecommunications Service

IEPS International Emergency Preference Scheme

IM Instant Messaging

IMS IP Multimedia Subsystem

IN Intelligent Network

IP Internet Protocol

IP-CAN IP Connectivity Access Network

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IRI Intercept Related Information

ISDN Integrated Services Digital Network

IT Information Technology

LEA Law Enforcement Agencies

MMS Multimedia Messaging Service

MPLS Multi-Protocol Label Switching

NAI Network Access Identifier

NAPT Network Address Port Translation

NAT Network Address Translation

NGN Next Generation Network

NNI Network-Network Interface
OAM Operations, Administration and Maintenance
OMA Open Mobile Alliance
OS Operating System
OSA Open Service Access
OTN Optical Transport Network
QoS Quality of Service
PBX Private Branch Exchange
PC Personal Computer
PDA Personal Digital Assistant
PLMN Public Land Mobile Network
POTS Plain Old Telephone Service
PSTN Public Switched Telephone Network
RACF Resource and Admission Control Functions
SIP Session Initiation Protocol
SLA Service Level Agreement
SMS Short Message Service
SR Service Resiliency
TDR Telecommunications for Disaster Relief
TE Terminal Equipment
UDDI Universal Discovery, Description and Integration
UMTS Universal Mobile Telecommunications System
UNI User to Network Interface
URI Uniform Resource Identifier
VPN Virtual Private Network
xDSL Various types of Digital Subscriber Lines

5 Conventions

None

6 Capability requirements for NGN release 1

The high-level requirements and related capabilities to support the service objectives of the NGN release 1 scope identified in [b-ITU-T Y-Sup.1] are provided in the clauses that follow.

The requirements are mainly provided from a high-level perspective, and are not intended to constitute precise functional requirements for the different NGN entities.

More detailed requirements and service-specific requirements are not addressed by this Recommendation.

This Recommendation only addresses requirements for the capabilities of the network for NGN. While the requirements on user equipment are not addressed, requirements for access arrangements are addressed.

6.1 Transport connectivity

The NGN release 1 transport stratum [ITU-T Y.2012] is required to use the IP protocol for general, ubiquitous, and global public connectivity. The IP protocol may be carried over various underlying transport technologies in the access and core portions of the transport stratum (e.g., xDSL, ATM, MPLS, frame relay, OTN) according to the operator's environment.

NOTE – This does not prevent operators providing technology-specific services directly to users (e.g., ATM, MPLS, frame relay, OTN).

Connectivity is required to accommodate:

1) use of IPv4 and IPv6;
2) real-time and non-real-time communications;
3) one-to-one connectivity;
4) one-to-many connectivity.

6.2 Communication modes

NGN is required to support the following communication modes:

– one-to-one;
– one-to-many;
– many-to-many;
– many-to-one.

6.3 Media resource management

Media resource management mechanisms are traditionally used in conjunction with traditional voice processing services and user interactions via voice and DTMF. These have to be expanded in NGN in support of new data, video and content services.

NGN is required to support various media resources and media resource management capabilities to enable a wide range of applications.

Media resource capabilities include:

– media recording (e.g., to support voice mail service);
– playing recorded media (e.g., to play voice mail, tones and announcements);
– DTMF recognition (e.g., to support interactive voice response services);
– advanced speech recognition (e.g., to support interactive voice response services);
– media conversion (e.g., to support text-to-speech, speech-to-text and fax-to-email services);
– transcoding;
– video/text/audio/data bridging (e.g., to support conferencing services);
– media duplication (e.g., to support lawful interception);
– media insertion.

6.4 Codecs

General requirements for codecs include the following:

1) Transcoding is required to be avoided wherever possible.

2) NGN is required to support end-to-end negotiation of any codec between NGN entities (terminals, network elements). It is the responsibility of entities at the rim of an NGN (e.g., NGN terminals and user equipment) and network equipment originating and terminating the IP media flows, to negotiate and select a common codec for each "end-to-end" media session. NGN is required to support end-to-end negotiation of text codecs, such as those currently specified in ITU-T Recommendations.

   NOTE 1 – A wideband audio codec is suggested to be used by NGN user equipment.

3) In order to enable interworking between NGN release 1 and other networks (including PSTN/ISDN, PLMN and other NGNs), the NGN is required to be capable of receiving and presenting G.711 [ITU-T G.711] coded speech when interconnected with another network.

4) When a packetization size is not selected by codec negotiation between terminals and/or network elements or agreed by bilateral arrangement, a speech packetization size of 10-ms samples should be used for G.711 [ITU-T G.711] coded speech; this is recommended as an optimum value balancing end-to-end delay with network utilization. It is recognized that there may be network constraints which require that a higher value is agreed by bilateral arrangement; in such cases a value of 20 ms is recommended.

   NOTE 2 – Where a packetization size is selected by codec negotiation between terminals and/or network elements, the present Recommendation places no requirements on the value to be selected.

NOTE 3 – As a deployment option, transcoding may be used in scenarios when end-to-end negotiation does not result in a common codec.

NOTE 4 – The requirements above do not mandate that any codec be supported by terminals, or that NGN support transcoding between any arbitrary audio codec and G.711 [ITU-T G.711].

6.5 Access network and network attachment

It is an NGN objective to support services and applications independently of the access network technologies. Thus:

1) NGN is required to support diverse access transport function technologies.

2) The transport stratum is required to be capable of providing IP connectivity between the end-user functions and core transport functions.

3) NGN is required not to preclude user networks of any level of configuration complexity.

4) NGN is required to support registration at the access network level, initialization of end-user functions for accessing the NGN services and management of the access network IP address space, including a NAT function.

5) The user profile is required to keep user access authentication data and information related to the required network access configuration.

6) NGN is required to support the re-configuration of services available to the user when the user is nomadic and accesses their services from a location other than the subscribed-to location. Services may be dependent on any or all of: the user device, the access network and arrangements (e.g., roaming agreements) between the service provider and the access network provider. The access network is required to allocate resources according to the services to be provided.

7) When multiple access networks are connected to a single NGN core network, an access network is required to be able to authenticate/authorize access by a user roaming on this access network from another access network.

8) To guarantee the availability of roaming services, the NGN access network attachment procedures are required to support access network authentication based on a standardized method for identifying users at access network level (e.g., the network access identifier (NAI) mechanism specified in [b-RFC 2486]).

6.6 User networks

The following are general requirements on NGN release 1 for access via user networks:

1) NGN is required not to preclude solutions for access via a user network to an NGN with NAT/NAPT and firewalls in the user environment where the assignment of IP addresses to user equipment may be done by the user network. These addresses need not be routable in the NGN.

2) Solutions for access via a user network to an NGN are required to have minimal impact on existing user network deployments.

3) Solutions for access via a user network to an NGN are required to support the following configurations:
   - direct connectivity and interaction between the individual terminals and the NGN;
   - indirect connectivity and interaction between the individual terminals and the NGN (e.g., via IP PBXs).

NGN release 1 should allow the simultaneous use of multiple types of access transport functions by a single terminal; however, there is no requirement to coordinate the communication. Such terminals may therefore appear to be two or more distinct terminals from the network point of view.

NOTE – Although the requirements in this Recommendation do not address terminal equipment, it is not intended to preclude the attachment of terminal equipment which could enable interface adaptation to varying user requirements, including the needs of people with disabilities, using commonly provided user interface devices.

6.7 Interconnection, interoperability and interworking

Interoperability and interworking are two distinct functions and are defined respectively in [ITU-T Y.101] and in the Y.1400-series Recommendations.

6.7.1 Interconnection

Two types of interconnection between release 1 NGNs are distinguished:

– "connectivity-oriented interconnection": It is based on simple IP connectivity irrespective of the levels of interoperability;

  NOTE 1 – An interconnection of this type is not aware of the specific end-to-end service and, as a consequence, network performance, QoS and security requirements specific to the service are not necessarily assured.

– "service-oriented interconnection": It allows carriers and service providers to offer services with defined levels of interoperability.

  NOTE 2 – For example, this is the case for G.711 services over IP interconnection. The defined levels of interoperability are dependent upon the service or QoS or security, etc.

The requirements for interconnection are the following:

1) Connectivity-oriented interconnection type between NGNs are required to be supported.

2) Service-oriented interconnection type between NGNs is not precluded.

6.7.2 Interoperability

In order to enable certain services to be provided across an end-to-end path comprising a single NGN domain or multiple NGN domains:

1) appropriate service components within a single NGN domain are required to interoperate;

2) interoperability of interconnected NGN domains which deploy identical sets of service capabilities is not precluded.

6.7.3 Interworking with non-NGN networks

NGN release 1 is required to interwork with various kinds of networks for provision of certain services. Services identified for interworking are required to operate seamlessly across the infrastructure provided by one or more network providers. NGN release 1 provides capabilities, including, among others, security, OAM, resiliency, quality of service and, where needed, media transcoding, for support of interconnection scenarios with other non-NGN networks in order to ensure seamless end-to-end operations.

In order to enable certain services to be provided across an end-to-end path comprising a combination of NGN and non-NGN networks:

– an NGN is required to be able to interwork with other non-NGN networks;

– an NGN should aim to support the following interworking capabilities:

  - Routing;
  - Signalling interworking;
  - Numbering, naming and/or addressing interworking;
  - Accounting and charging-related information exchange;
  - Security interworking;
  - QoS interworking;
  - User and terminal profile information exchange;
  - Media interworking;
  - Management interworking;
  - Policy management (e.g., according to inter-domain policies, some trusted domain internal information, including user-related information, may need to be hidden or removed from the information flow exchanged at the interface with another trusted or non-trusted domain), including resolution of differences in policy.

  NOTE – This does not imply that all services and/or service features can be interworked. These requirements may only apply to the interworking between certain specific (and most likely similar or identical) services and/or service features.

6.7.3.1 Interworking with PSTN/ISDN

When an NGN is connected to a PSTN/ISDN, it is required to support the following:

1) Interworking between PSTN/ISDN and PSTN/ISDN emulation services: Interworking is required to provide high-level of interoperability with the services in the PSTN/ISDN being emulated. The degree to which service interoperability is provided is a matter for operators and, in some cases, national regulators.

2) Interworking between PSTN/ISDN and PSTN/ISDN simulation services: Interworking is required to support the interoperability of PSTN/ISDN simulation services with PSTN/ISDN supplementary services, although this interworking may result in a limited service capability.

3) Interworking between PSTN/ISDN and NGN IP multimedia services, although this interworking may result in a limited service capability.

NOTE 1 – This does not imply that all NGN services and/or service features can be interworked with PSTN/ISDN services and vice versa. These requirements may only apply to the interworking between certain specific (and most likely similar or identical) services and/or service features offered by both the NGN and the PSTN/ISDN.

NOTE 2 – Circuit-switched-based corporate networks are supported in release 1 either by connection to the NGN via an existing PSTN/ISDN, or, when PSTN/ISDN emulation is deployed, through an interworking gateway.

6.7.3.2 Interworking with other networks

1) NGN is required to provide the capability for direct interconnection for circuit-switched-based networks, including at least cable networks, broadcast networks, and public land mobile networks. The requirements for interworking to all circuit-switched-based networks are the same as those for interworking to the PSTN/ISDN.

   NGN release 1 is required to provide the capability for connectivity-oriented interconnection with non-NGN but IP-based networks. NGN is required not to preclude the capability for service-oriented interconnection with non-NGN but IP-based networks.

   If the interconnected network provides all of the interworking capabilities, as identified in clause 6.7.3, such network interconnections may be supported in a deployment. The characterization and functionality of non-NGN but IP-based networks are sufficiently diverse and abundant that it is not possible to provide firm requirements for interconnection in release 1.

2) NGN is required not to deliberately exclude the interconnection with non-NGN but IP-based networks.

NOTE – Security requirements are contained in clause 6.13.

6.8 Routing

NGN is required to provide capabilities to select the proper routing paths between the traffic originating endpoint and the traffic receiving endpoint.

NGN is required to support routing schemes most suitable for NGN providers. In particular, NGN is required to support:

1) both static and dynamic routing schemes;
2) routing schemes which can effectively operate within an NGN domain;
3) routing schemes which can effectively operate between NGN domains, thereby allowing interoperability.

6.9 Quality of Service

NGN is required to support end-to-end QoS across different networks of varying infrastructure technologies provided by multiple operators to ensure the required service level for users or applications. NGN is required to support multiple levels of QoS, which may be negotiable between the user and provider. QoS service level support includes use of resource and admission control mechanisms, traffic class differentiation, priority management, QoS signalling mechanisms, performance measurement and management for quality insurance, and overload/congestion control.

6.9.1 General QoS requirements

The NGN is required to meet the following QoS requirements:

1) Allow different technologies and business models.
2) Support the different processes related to service lifecycle (e.g., subscription/provisioning, invocation, monitoring).
3) Support different terminal equipment capabilities (for example, some terminal equipment may support transport stratum QoS signalling, while others may not).
4) Control the QoS-related transport resources within packet networks and at the network boundaries in accordance with their capabilities.
5) Support resource and admission control within a single NGN domain and between NGN domains.
6) Support both relative QoS control and absolute QoS control.
7) Support application-driven QoS requirements.

6.9.2 Network QoS classes

1) NGN should take into consideration the network performance at the transport stratum.
2) NGN should support NGN QoS classes based on [ITU-T Y.1541].

6.9.3 Service/application priority

The NGN should support service/application priority as follows:

1) priority classification schemes for admission control and restoration;
2) signalling extensions that indicate priority levels across UNI and NNI;
3) priority enabling mechanisms that deliver the desired priority action.

6.9.4 QoS control

NGN should support:

1) per-flow, per-session, per-service-class QoS control granularity;
2) dynamic QoS behaviour (i.e., it should be possible to modify QoS attributes during an active session);
3) QoS resource control based on a distributed, centralized or a hybrid approach;
4) admission control and congestion control mechanisms;
5) mechanisms to guarantee the timely and reliable delivery of signalling and control packets;
6) mechanisms to prioritize the delivery of emergency telecommunications and priority telecommunications.

6.9.5 QoS signalling

NGN should use signalling mechanisms to support QoS.

Detailed requirements for QoS signalling are out of scope of this Recommendation and contained in other specific Recommendations.

6.9.6 Performance measurement and management

NGN is required to provide performance measurement and management to ensure QoS.

The network performance measurements and their management should support:

1) providers' assurance of performance delivery (for comparison against SLAs);
2) providers to supply performance information for prospective customers;

3) providers' troubleshooting among their networks along defined paths;

4) providers' internal indication of performance impacts due to changes within their networks;

5) providers' monitoring of each other's network performance;

6) providing information to other NGN functions, e.g., RACF.

Detailed requirements for performance measurement and management are out of scope of this Recommendation and contained in other specific Recommendations.

6.9.7 Processing and traffic overload management

In order to avoid processing and traffic overload and to keep response times reasonably low under such overload to preclude users abandoning their service requests, NGN release 1 should provide mechanisms for overload detection and control (including expansive controls such as load balancing and resource replication) within both the service and transport strata.

The NGN should have mechanisms available to control overload that:

1) convey indication of overload conditions and the degree of overload to other networks;

2) optimize effective throughput (e.g., admitted service requests/s or packets/s) subject to service priority considerations at an overloaded resource;

3) achieve this throughout the duration of an overload event, irrespective of the overloaded resource's capacity or of the number of sources of overload;

4) allow the network that receives the overload indication to control its traffic.

6.10 Accounting and charging

Accounting and charging capabilities are supported in NGN in order to provide accounting and charging data to the network operator regarding the utilization of resources in the network.

NGN requirements for accounting and charging are summarized below:

1) Accounting and charging capabilities are required to 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).

2) Open mechanisms are required to be available for charging management.

3) Various charging policies are required to be supported (e.g., fixed rate charging and usage based per-session charging).

4) Accounting and charging capabilities are required to support services with multicast functionality.

5) NGN is required to enable all possible types of accounting arrangements, including transfer of accounting/charging information between providers. This requirement also includes e-commerce arrangements.

   For example in content delivery services scenarios with multicast functionality, services may be provided by joint activities of multiple companies (e.g., several content service providers and a network provider): charging functionality between companies is necessary in addition to charging functionality to users.

NOTE – The usage of charging information collected by an NGN to enable billing arrangements is out of scope of this Recommendation.

6.11 Numbering, naming and addressing

NGN is intended to provide an efficient, secure and trustworthy numbering, naming and addressing environment for users, network operators and service providers. Regulatory requirements as well as interoperability with PSTN/ISDN will be taken into account where applicable.

Evolution to NGN is required to ensure that the sovereignty of ITU Member States with regard to numbering plan, naming plan, and addressing plans is fully maintained, in particular as described in [ITU-T E.164] and other relevant Recommendations and Specifications of other standard bodies.

The following are the requirements to support numbering, naming and addressing capabilities. Except where noted, they apply to both the transport and service strata.

6.11.1 General requirements for numbering, naming and addressing

1) Both dynamic and fixed address assignment modes are required to be supported.
2) Numbering, addressing and naming capabilities may be implemented by using an individual mapping scheme for each service, or via a mapping scheme that is common across different services.
3) Dynamic update of naming databases is required to be supported (for example, in case of a mobile terminal, addresses at one or more layers may dynamically change depending on the terminal's location).

6.11.2 Numbering

The numbering requirements applicable to NGN are the following:

1) Addressing mechanisms are required to support the ability to differentiate between the dialling plan, numbering and addressing plans.
2) Addressing mechanisms are required to support the ability to translate a dialling sequence into the numbering and addressing scheme.
3) NGN is required to support E.164 numbering (global numbers).
4) NGN should allow non-E.164 numbering (local numbers).
5) NGN should allow short numbers in national dialling plans.
6) NGN should not prevent private and corporate numbering (see clause 6.6).
7) When non-E.164 numbers (local numbers) or dialling sequences are used, NGN addressing is required to provide the scope within which the local numbers are valid.
8) NGN is required to support the ability to differentiate alphanumerical identifiers that happen to be consisting of only digits from those which are telephone numbers and should be treated as such in routing procedures.

6.11.3 Numbering, naming and addressing schemes

1) At the transport stratum, NGN release 1 is required to support IP addressing schemes based on IPv4 or IPv6 or both.

   NOTE 1 – It should be recognized that a mixture of IPv4 and IPv6 within a single domain may cause problems for service delivery.

2) NGN release 1 domains may support user equipment using IPv4 only, IPv6 only or both at the User-Network Interface.

   NOTE 2– It is assumed that IPv6 based user equipment can also support IPv4 at the User-Network Interface.

3) NGN release 1 is required to support IP multimedia communication establishment (in both the originating and terminating case) using at least E.164 telephone uniform resource identifiers (Tel URIs), e.g., tel: +4412345678, and SIP uniform resource identifiers (SIP URIs), e.g., sip:my.name@company.org, as a minimum. For Tel URIs:
   - global numbers are required to be supported;
   - local number form should be supported.

4) In some service scenarios, e.g., interworking with PSTN/ISDN, an NGN release 1 is required to support IP multimedia communication establishment (in both the originating and terminating case) using E.164 numbering with ENUM-like support where appropriate.

5) Numbering and addressing schemes are required to support unicast and multicast service types.

6) Numbering and addressing schemes should support broadcast service types.

7) Other numbering, naming and addressing schemes may be supported.

6.11.4 Name/number/address resolution

[ITU-T Y.2001] provides fundamental principles and requirements for name, number and address resolution. In line with those, the following requirements are provided.

1) scalability: NGN should be scalable in order to handle increased demand for name/number/address resolution;

2) reliability: name/number/address resolution capabilities are required to remain unaffected by a single-point of failure (using, for example, distributed resolution mechanisms);

3) security: security measures are required to be in place for name/number/address resolution capabilities.

NOTE – These capabilities may use databases that are internal or external to a NGN (e.g., an Internet DNS database). Examples of security measures include user access authentication, data security, data synchronization and fault recovery.

6.11.5 Numbering, naming and addressing interworking

The interworking functions perform translations of numbers, names and addresses when required in network interconnection scenarios.

1) NGN is required to support multiple transport stratum address interworking scenarios without affecting the service provided to users (i.e., interworking scenarios among different addressing domains, such as domains based on IPv4 or IPv6 addressing schemes, and domains based on public or private addressing schemes).

2) Where needed, address translation capabilities are required to be used to support address format differences, in both the transport and service strata, without affecting the service provided to users.

6.12 Identification, authentication and authorization

The requirements in this clause are not tied to any specific set of NGN services or applications.

NOTE – Specific authentication and authorization mechanisms are out of scope of this Recommendation.

6.12.1 General requirements

There are requirements for bilateral identification, authentication and authorization capabilities in both the transport and the service stratum. In the transport stratum there are requirements on how NGN transport resources can be used. In the service stratum requirements are on the association between a user and a service or between a user and another user, including the case when the two users are on different NGNs.

NOTE 1 – Sometimes the phrase "service provider" has been used to refer to the provider of transport stratum services. In this subclause, the network provider is usually shortened to "(the) NGN", and the "service provider" is exactly that, the "provider of the service": the service provider could be anywhere, and is not necessarily the network provider.

The following are general requirements for identification, authentication and authorization capabilities.

1) NGN is required to support bilateral authentication and authorization functions for both the transport and the service strata. Transport stratum authentication requires a user to be identified by the network in order to obtain access to the network and to privileged uses. An authentication function can be a significant factor in protection from unauthorized use of networks, such as prevention of unsolicited bulk telecommunications. An authorization function can set up access to network resources and prevent access violations.

2) NGN is required to uniquely identify users by one or both of the following types of user identifier:

   – public user identifier: The information that is normally used by one NGN user to contact or communicate with another NGN user;

   – private user identifier: A private NGN user identifier can be used to identify the NGN user to her/his NGN network or service provider. The private user identifier is one component used for authentication.

3) NGN is required to allow separate identification, authentication and authorization of users and terminal equipment.

4) NGN is required to allow verification of the association between the user and the user's terminal equipment for some specific services.

5) Authentication, authorization and accounting, performed by the NGN provider and the service provider, should be processed securely.

6) A service provider is required to provide mechanisms that allow presentation of the public identifier of the communication originator, where appropriate and where permitted.

7) A service provider is required to provide mechanisms to withhold the public identifier of the communication originator, if the presentation of this information is restricted by the communication originator or the network.

8) A service provider that performs authentication is required to support mechanisms to determine the authenticity of a public user identifier presented for an incoming communication.

9) A service provider that performs authentication is required to provide mechanisms that allow the presentation of the public user identifier of the connected party to the communication originator, if applicable and if this is not restricted by the connected party or the network.

10) An NGN is required to be able to verify the private identifier of users and terminals (if applicable). Additionally, it is required to be able to check the authentication and authorization of users and terminals to use resources of the NGN.

11) A service provider is required to be able to verify the private identifier of users of the services it provides. Additionally, the service provider is required to support the capability to check the authentication and authorization of users to use resources it manages.

12) Private and public identifiers of NGN users of transport stratum resources (identifiers used for authentication and authorization) are required to be administered by the relevant network provider.

13) Private and public identifiers of service users of service stratum resources (identifiers used for authentication, authorization and routing), are required to be administered by the relevant service provider and such administration is required to prevent the user from unauthorized changes to the public and private identifiers.

14) Private NGN user identifiers provided for authentication and authorization are required to be withheld from other users.

15) Public NGN user identifiers of service users may be visible to other users if no service intermediaries are involved and the user's permission is given.

16) A service provider may allow a user to access a service from multiple terminals in parallel using the same public and private user identifier.

17) As a single user may use multiple private user identifiers via a single subscription procedure, the NGN is required to support multiple private user identifiers via a single subscription procedure.

18) NGN may authenticate and authorize a single user for multiple services ("single sign-on").

NOTE 2 – Even when only a single authentication event is required, multiple authorization events may still be needed. In addition, single sign-on can be implemented on the client side, such that even though multiple authentications are required, the human user only needs to establish an authentication relationship once. NGN release 1 does not require support of single sign-on capabilities. However, where such support exists with current technologies, it is expected to be also used for NGN release 1.

Authentication of a subscriber's identifier or of a user's identifier is not intended to indicate positive validation of a person.

6.12.2 Requirements for identification

NGN release 1 provides capabilities for user identification, in order for network operators and service providers to identify the users of certain NGN services and use this information as required (e.g., for authentication and authorization procedures). NGN release 1 is required to provide capabilities for the user to identify NGN providers (on each stratum) where a direct relationship exists.

Requirements for identification capability include the following:

1) Multiple user identifiers

As an NGN user may have one or more public and private identifiers, NGN is required to segregate one identifier from another (e.g., for personal use and business use).

2) Identifier portability

NGN is required to provide capabilities that provide the equivalent of number portability in PSTN environments.

3) Identifier independency

The public user identifier should be assigned to the user independent of its repository, the user terminal and the underlying network technologies. However, backward compatibility (e.g., for POTS handset) may be achieved via proper interworking functions.

4) Support for identifier attributes

Private identifier attribute, such as the lifetime of that identifier for the user, the subscriber, the network in use, etc., may be associated with a user identifier.

5) Support for attribute conditions

Conditions (e.g., setting timer as validity conditions) for a user attribute may be associated with a user identifier by an attribute provider (e.g., network, principal user, end user).

6) Selective attribute authorization

NGN is required to support selective authorization of user's private identity attribute information by an attribute provider (e.g., identifier lifetime).

7) Support for subscriber programming

NGN should support subscriber's programming of different permissions for different attribute information, e.g., access to and usage of private identity attribute information, on a per attribute basis.

8) User and terminal binding

NGN is required to support a dynamic binding of the public user identifier and the terminal equipment identifier for certain services.

9) Multiple terminal association

NGN is required to allow association of a user public or private identifier to multiple (mobile or fixed) terminal equipment identifiers for certain services. The user may be allowed to use multiple terminals at any given time.

10) Identifier information transfer

NGN is required to support the transfer of the user identifier information by NGN users if permission is given by the user providing input either on their own terminal or on the receiving terminal for certain services (e.g., point of sale terminal).

6.12.3 Requirements for authentication

Authentication is the process of establishing confidence in user and terminal equipment identifiers as well as network attachment and service offers. From the point of view of providers, NGN may distinguish between transport network authentication and service authentication. From the perspective of subscribers, NGN may distinguish between user authentication and terminal equipment authentication. Network authentication is the process of verifying user/terminal equipment identifiers for transport network access only by network providers. Service authentication is responsible for verifying user/terminal equipment identities for service usage purpose. From the perspective of subscribers, NGN is required to provide the capability for a user to authenticate and identify a transport network provider.

From the perspective of subscribers, NGN is also required to provide the capability for a user to authenticate and identify a service provider.

NGN should allow for these capabilities to be independent.

These distinct authentication concepts may be unified into a single concept or be applied separately, depending on the transport technology or business model. For example, a single authentication flow may be processed if a network provider is also a service provider.

Requirements for authentication capability include the following:

1) NGN is required to allow various network authentication mechanisms appropriate to the underlying access network technologies.
2) Service authentication should aim to be independent of the NGN access network technologies and maintain a consistent service authentication mechanism.
3) An NGN is required to request user/terminal equipment to input authentication information either in an explicit or implicit manner.
4) NGN should support both software-based and hardware-based authentication mechanisms.
5) Terminal equipment authentication that uses device profile information is required to be supported.
6) NGN should provide capabilities of bilateral authentication between service provider and user.
7) NGN should provide capabilities of bilateral authentication between transport network provider and user.

6.12.4 Requirements for authorization

Requirements for authorization capability include the following:

1) NGN is required to provide service access to authenticated users and/or devices based on their access rights, user profiles and network policy.

2) Service authorization should aim to be independent of the NGN access network technologies.

3) Authorization capability should support NGN release 1 mobility scenarios where applicable.

6.13 Security

NGN release 1 is required to contain the security features incorporated in existing networks and allow for secure interconnection with other NGNs or non-NGN networks. The requirements are based on the application of [ITU-T X.805] to NGN and thus address the following dimensions of NGN security: access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy.

NGN is required to provide:

1) protection against unauthorized use of network resources and unauthorized access to information flows and applications;

2) authentication of the communication entities if policy requests;

3) mechanisms for data confidentiality;

4) mechanisms for data integrity;

5) a means for accountability, whereby individuals are held responsible for the effect of any of their actions;

6) availability and accessibility of the network, upon demand by an authorized entity;

7) mechanisms of non-repudiation for preventing one of the entities or parties in a communication from falsely denying having participated in the whole or part of the communication;

8) privacy of the user's data, e.g., preferences, profiles, presence, availability and location information. This is required to be protected by revealing information only when valid authorization is provided;

9) protection to minimize network attacks, from within or outside;

10) protection against cybercrime by enabling the user to identify the transport network provider and the service provider.

6.14 Mobility management

Mobility management involves the ability of mobile objects, such as users, terminals and networks, to be able to roam between different networks (NGN or non-NGN). In NGN release 1, two distinct types of mobility are considered: personal mobility and terminal mobility [ITU-T Q.1706].

For NGN release 1, personal mobility exists where users can use registration mechanisms to associate themselves with a terminal that the network can associate with the user. Where interfaces between users and terminals, and users and networks for user registration exist, it is assumed these interfaces will be used for NGN release 1.

For NGN release 1, terminal mobility exists within and among networks where registration mechanisms are used to associate the terminal to the network. Where support for terminal mobility with service continuity exists, such support is expected to also be used for NGN release 1.

The following provides general requirements for mobility management, focused on support of customer needs.

For the services to which mobility is appropriate, NGN release 1 is required to provide:

1) nomadism for personal mobility and terminal mobility;
2) mobility support for existing access technologies, existing QoS capabilities and existing security capabilities;
3) location management support for registration, location update and address translation to enable mobility across providers' network boundaries;
4) support for roaming subscription and authentication management;
5) support for security to prevent unauthorized access and ensure user privacy, taking account of service continuity and handover where applicable;
6) support for location confidentiality to conceal location information from non-trusted entities;
7) support for paging capability for set-up of incoming calls, in order to save power in mobile terminals and reduce signalling in the network.

6.15 OAM

It is recognized that OAM capabilities are important in public networks for ease of network operation, for verifying network performance, and to reduce operational costs by minimizing service interruptions, service degradation and operational downtimes. OAM capabilities are especially important for networks that are required to deliver (and hence be measurable against) network performance and availability objectives [ITU-T Y.1710], [ITU-T Y.1730].

NGN release 1 is required to provide OAM functions for both service and transport strata.

In order to offer reliable NGN services that can support the requirements of SLAs, NGN services are required to have their own OAM capabilities.

NOTE – The OAM capabilities described in this clause are complementary to the management capabilities described in clause 6.17.

6.15.1 General OAM requirements

The following provides OAM requirements of NGN:

1) The capability to choose the desired OAM functions by the service or network provider is required to be supported.
2) OAM functions are required to be applicable to point-to-point, point-to-multipoint and multipoint-to-multipoint applications.
3) OAM functions are required to allow efficient scaling to large network sizes.
4) The capability to support detection of faults, defects and failures is required to be supported.
5) The capability to diagnose, localize and notify the network management entities and take appropriate corrective actions is required to be supported.
6) The capability to allow an NGN to prevent the customer from triggering any service/network provider OAM function is required to be supported.
7) The capability to allow an NGN to prevent the customer from detecting or localizing failures (since this is part of service provider or network provider's responsibility) is required to be supported.
8) OAM traffic is required to follow the same path as the user traffic.

9) The following anomalies are required to be automatically detected:
   - lost data;
   - loss of connectivity;
   - errored data;
   - unintentionally self-replicated data;
   - misinserted data [ITU-T Y.1730].

10) OAM functions are required to be backward compatible. NGN is required to be capable of activating OAM functions transparently without disturbing the user traffic or causing unnecessary actions.

11) OAM functions are required to perform reliably even under degraded transmission conditions, e.g., error events.

12) Connectivity status assessment is required to be independent of the dynamic behaviour of user traffic [ITU-T Y.1710], [ITU-T Y.1730].

13) Server-client layer OAM relationships between lower layers and higher layers (e.g., signal fail/signal degrade) in case of a multi-layer network is required to be supported.

14) In case of a multi-layer network, a defect event in a given server layer network is required to avoid causing multiple alarm events to be raised, and is required to avoid unnecessary corrective actions to be taken, in any higher client layer network. Client layer networks should support alarm suppression for server layer sourced defects whose presence have been communicated by forward defect indication means. Client layer networks are required to support forward defect indication capability [ITU-T Y.1710], [ITU-T Y.1730].

15) In case of a multi-layer network, OAM functions in a given layer network are required to be independent of any specific lower or higher layer network. This is architecturally critical to ensure that layer networks can evolve, be added and removed without impacting other layer networks.

16) In case of a multi-layer network, OAM functions in a given layer network are required to be sufficiently independent of any specific control plane such that control plane changes do not impose changes in user plane OAM. This is architecturally critical to ensure that user plane and control plane can evolve without impacting each other.

17) OAM functions are required to be supported in multiple service/network provider environments.

18) When NGN services are provided in multiple service/network provider environments, it is required to detect and notify which service/network provider is responsible for the defect so that a quick action can be taken. Additionally, the service/network provider that offers the service to the user is required to be made aware of the service fault, even if the fault and detection point are located in the network of another service/network provider.

19) NGN is required to have mechanisms that make sure that service/network providers' OAM flows, which are meant for their internal use, are confined within their networks and do not leak out to customers or other service/network providers.

20) In order to realize OAM functions in hybrid networks, so that services can be provided across an end-to-end path comprising a combination of NGN and non-NGN networks, OAM functions are required to be supported in interworking scenarios (clause 6.7.3).

21) In order to allow managing separately a portion of a network which is under the responsibility of a provider, and to allow defining maintenance entities flexibly, both "segment" OAM functions and "end-to-end" OAM functions are required to be supported.

NOTE – Segment means a part of an end-to-end connection which is defined for operation and maintenance purposes.

22) Recording of service downtime for performance and availability measurements is required to be supported.

23) The information produced by OAM functions is required to be managed so as to provide the appropriate indications to the maintenance staff for maintaining the quality of service level offered to customers [ITU-T I.610].

24) Capabilities for performance monitoring are required to be supported.

6.16 Survivability

Survivability functions are necessary to realize highly reliable networks.

6.16.1 Protection switching requirements

NGN is required to support protection switching capabilities to implement fast and deterministic survivability functions for all traffic paths.

The following are general requirements for NGN transport protection switching:

1) Capabilities to prevent a higher layer defect from triggering lower layer protection switching is required to be supported.

2) When more than one layer is involved in protection switching, the lower layers are required to have priority over the higher layers (this is known as inter-layer escalation strategy).

3) Both 1+1 and 1:n protection switching should be provided.

4) Unutilized transport protection resources may be used to carry best effort traffic.

5) Impacts on network performance (e.g., additional delay, delay variation, bit errors, packet losses, etc.) due to protection switching should be minimized.

6) Operator control functions, such as lockout of protection, forced switch and manual switch commands, are required to be supported.

Detailed requirements for specific technologies are provided in various Recommendations such as [ITU-T G.808.1].

6.16.2 Rerouting requirements

When serious accidents or special events occur, network degradation or in the worst case failure may occur. Capabilities such as rerouting, with possible downgrading of performance or quality of service, and traffic control mechanisms are therefore required.

NOTE – These capabilities can also be regarded as part of network integrity functions.

General requirements for NGN rerouting are as follows:

1) When more than one layer is involved in rerouting, the lower layers may have priority over the higher layers (inter-layer escalation strategy).

2) The rerouting mechanism is required to be capable of finding an alternative route within an acceptable time.

3) Impacts on network performance (e.g., additional delay, delay variation, bit errors, packet losses, etc.) due to rerouting should be minimized.

4) NGN is required not to preclude operator control.

5) Network re-optimization is required to be supported, where necessary, after restoration of the impaired traffic.

6) After recovery from fault or degraded conditions, the performance and quality of service levels preceding the fault or degraded conditions are required to be restored.

6.16.3 Service resiliency requirements

Resiliency conditions depend on the specific service; therefore, they are required to be described for each service as required.

General requirements for service resiliency (SR) are as follows:

1) NGN is required to be able to independently assign different SR levels to different services.
2) NGN is required to be able to independently assign different SR levels to different services on a per flow basis.
3) Depending on the assigned SR level, NGN is required to support the capability for the services covered by SR to experience the same level of service quality experienced prior to the failure event.
4) Terminal equipment may optionally signal SR levels to the NGN.
5) NGN is required to be able to assign and support SR from the point of ingress to the point of egress of the service provider network.
6) NGN is required to be able to differentiate among user plane and control plane SR-enabled flows.
7) NGN is required to support the capability to notify the application/user if the required SR level cannot be met by the NGN.

6.17 Management

NGN management capabilities support management areas which cover the planning, installation, operations, administration, maintenance and provisioning of networks and services. The high-level goal is to provide survivable and cost-effective networks.

NGN management capabilities also support the monitoring and control of NGN services and transport components via the communication of management information across interfaces between NGN components and management systems, between NGN supportive management systems, and between NGN components and personnel of service and network providers.

NGN management capabilities support the aims of the NGN by:

1) providing the ability to manage, through their complete life cycle, NGN components, both physical and logical. This includes resources in the transport stratum and the service stratum, access transport functions, interconnect components and user networks and terminals;
2) providing the ability to manage NGN service components independently from the underlying NGN transport components and enabling organizations offering NGN services (potentially from different service providers) to build distinctive service offerings to customers;
3) providing the management capabilities which enable organizations offering NGN services to offer users the ability to personalize user services and to create new services from NGN capabilities (potentially from different service providers);
4) providing the management capabilities which enable organizations offering NGN service improvements including user self-service (e.g., provision of service, reporting faults, online billing reports);
5) developing a management architecture and management services which enable service providers to reduce the time-frame for the design, creation and delivery of new services;
6) supporting the security of management information, including customer and user information;

7) supporting the availability of management services any place any time to any authorized organization or individual;

8) supporting eBusiness networks based upon concepts of business roles (customer, service provider, complementor, intermediary, supplier (e.g., equipment vendor)) [ITU-T Y.110], [ITU-T M.3050.0];

9) allowing an enterprise and/or an individual to adopt multiple roles in different networks and also multiple roles within a specific network (e.g., one role as a retail service provider and another role as a wholesale service provider) [ITU-T M.3050.0];

10) supporting B2B processes between organizations providing NGN services and capabilities;

11) allowing the management of hybrid networks comprising NGN and non-NGN resources;

12) integrating an abstracted view on resources (network, computing and application), which is hiding complexity and multiplicity of technologies and domains.

Detailed requirements for NGN management are beyond the scope of this Recommendation and are provided in management-specific recommendations, such as [ITU-T M.3060].

NOTE – See also the requirements in clause 6.10 "Accounting and charging".

6.18 Open service environment

Open service environment capabilities stem from the general characteristics of the NGN in supporting and establishing an environment for enhanced, flexible and open service creation and provisioning within the service stratum.

Implementing new functionalities in current networks may be limited or impossible due to the capabilities of the installed equipment. Software provisioning to implement new functionalities is essentially restricted to equipment vendors, since the application programming interfaces (APIs) are typically proprietary (i.e., not open).

NGN is required to enable new capabilities and support a wide range of emerging services, including services with advanced and complex functionalities. Due to a drive from third-party application and service providers to develop new applications and capabilities accessible via open and standard interfaces, there is an increasing need for network and service providers to cooperate in the development of standard application network interfaces (ANI). Furthermore, software reusability and portability, and use of commercial software should be supported to facilitate cost effective development.

Some general benefits of an open service environment are as follows.

– Applications and capabilities can be easily developed by network providers as well as by third parties.

– Capabilities can be made portable and/or reusable across networks.

– Open and standard ANIs will accommodate interactions between NGN entities and applications (e.g., for service creation).

Within an open service environment, each capability is required to be able to function either independently or in conjunction with other capabilities for the realization of applications. Each capability performs all corresponding service functions for the requesting entity (e.g., third party). Applications may be provisioned in different networks, so the capabilities have to be able to function independently from the underlying network technologies.

NGN is required to satisfy the following open service environment general requirements:

1) Independence from transport network providers: Functionalities, operations and management of applications and services are required to be independent from the underlying transport network providers' infrastructure and network technologies;

2) Independence from manufacturers: A multi-vendor open service environment is required to be supported, providing users with a wide range of services and applications in a competitive environment;

3) Location transparency: In a distributed environment, service providers are required to be able to access capabilities from anywhere, regardless of the actual physical location of such capabilities;

4) Network transparency: The open service environment is required to allow applications and services to be technology and terminal agnostic;

5) Protocol transparency: Protocol transparency is required to be achieved by providing open standardized protocol programming interface tools for realizing independent service control process and shielding complex network technical details to the open service environment;

6) Secure access to open service environment capabilities is required to satisfy the general NGN security requirements as specified in clause 6.13.

The following subclauses provide open service environment capabilities.

6.18.1 Service coordination

Requirements for service coordination of the open service environment include the following:

1) NGN is required to offer coordination of applications and services with capabilities.

2) NGN capabilities or service components from various service providers, and the relationship between these capabilities or service components, should be tracked.

3) Information on state changes of capabilities or service components (for example, due to upgrades) should be made available to applications and services.

6.18.2 Interworking with service creation environments

1) The NGN open service environment is required to allow interworking between service creation environments and network entities for creation and provisioning of applications and services.

2) NGN release 1 should support the following three classes of service creation environments:
   - Open service creation environment: Examples of this class of environment using ANI include OSA/Parlay, Parlay X, OMA;
   - IP Multimedia Subsystem (IMS)-based service creation environment [ITU-T Q.1741.X];
   - Intelligent network (IN)-based service creation environment: Examples of relevant interface protocols for this class of environment include IN application protocol (INAP), customized application for mobile network enhanced logic (CAMEL) and wireless intelligent network (WIN).

6.18.3 Service discovery

Service discovery is often the first step to locate capabilities, and/or services and applications. A service discovery capability is essential in several scenarios, such as mobility scenarios (to locate services in the visited network) and user device independent access to services.

As an example, when this capability is implemented in web services, public web service registries (e.g., the universal discovery, description and integration (UDDI) registry) can be used to implement service discovery and enable access to services.

Requirements for service discovery are the following:

1) NGN is required to support a service discovery capability to allow users to discover services of their interest over any underlying networking technology.

2) Service discovery mechanisms are required to be independent of the underlying networking technologies so that they can support heterogeneous and changing network technologies.

3) The service discovery capability is required to allow discovery of both human interest and device-interest services:

   – Human interest services can be directly used by users. Examples of user-interest services include directory services, translation services and shared facilities (e.g., IT support information).

   – Device-interest services can be directly accessed by devices (e.g., mobile handsets or portable PCs). Examples include printers, backup devices, CD/DVD-writers, authentication servers, IP address allocation servers. Device-interest services and network information may not be directly usable by human users.

4) The service discovery mechanisms should not be limited only to the traditional client-server based technologies.

   NOTE – Service discovery may be implemented using peer-to-peer technologies or a combination of client-server and peer-to-peer technologies.

5) The service discovery capability should support a variety of scoping criteria (e.g., location and cost) to provide appropriate scaling.

6) The service discovery capability is required to support appropriate mechanisms to ensure security and privacy.

7) The service discovery capability is required to take into account scalability (e.g., broadcast mechanisms should be avoided).

6.18.4 Service registration

This capability allows the registration of other capabilities, services and applications in directories of the open service environment which are accessible by capabilities, services and applications. As an example, the registration capability may be implemented in web services when it is wished to expose a web service: web services may be registered in public web service "registries" (a registry is a special directory that not only points users to a resource, but also lets them register services with it).

Requirement for service registration is as follows:

1) The open service environment is required to provide the means to manage the registration of capabilities, services and applications. The technology choice is required to ensure functions for service registration and deregistration, including configuration, activation, publication.

6.18.5 Development support for services

Development support for services is a key aspect of the service delivery chain, both within the service provider and within third parties who can extend the set of capabilities and broaden the overall service offering. Developers' needs include collection and publication of data, plus availability of a means to articulate and specify their needs, and identify interfaces for the development of services.

NGN should offer development support for:

1) construction of applications and services;

2) trialing of applications and services (e.g., tracing and debugging);

3) deployment of applications and services;

4) removal of applications and services.

Development support should include:

1) (software) component re-usability and interchangeability;

2) ability of mixing-and-matching of components by management of interfaces and having consistent semantics of shared data/schema across these components;

3) support for the full life cycle of components, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal;

4) support for delivery-agnostic application design to allow applications to be implemented without requiring re-design for each development scenario;

5) tracking of dependencies among components.

6.19 Profile management

6.19.1 User profile

A user profile is a set of stored information related to a user (or a subscriber). In an NGN environment, the management of the user profile attributes is especially important since the user information is required to implement a number of capabilities, including authentication, authorization, mobility, location, charging, etc. User profiles include transport-related information and service-related information. User profiles can be stored in separate databases in the service stratum and in the transport stratum and may have data exchange functions between them.

General requirements for user profile are as follows:

1) For each user, a user profile is required to exist by a related provider, which may consist of several 'components'.

2) These components may be distributed in the home network and service provider's environment; criteria of privacy and data protection are required to be fulfilled.

3) Within the domain of the home network, the components may be distributed in various entities.

4) Within the home network, a functionality that is able to locate user profile components is required. This functionality allows services/applications to be unaware of the actual location of the components and is required to be under the control of the home network.

5) Services, applications and other NGN entities are required to be able to retrieve the related user profile or selected parts of it (as required) in one transaction; criteria of privacy and data protection are required to be fulfilled.

6) Effective means to retrieve individual user profile components are required with acceptable delay for real-time services.

NOTE – Although user profile management does not attempt to provide any classification of the data a user profile may contain, categorizations such as general user information, service-specific information, etc. may be applied.

The detailed requirements relating to user profile, its usage and management are expected to be contained in further ITU-T Recommendation(s).

6.19.2 Device profile

A device profile is a set of stored information related to a user equipment. In an NGN environment, the management of the device profile attributes is also important since the device information is required in conjunction with "user profile" by a number of capabilities, including authentication, authorization, mobility, location, charging, etc. Device profiles may contain transport-related information or service-related information. Device profiles can be stored in separate databases in

the service stratum and in the transport stratum and may have data exchange functions.

NOTE 1 – This information may contain terminal identification attributes, like address, name, static attributes such as supported media and protocols, screen details (size in pixels, colour resolution, response time, etc.), transmission speed, bandwidth, and processing power, and dynamically changing attributes such as the user using the terminal, geographical location, running applications on the terminal.

Device profiles may be used for the following purposes:

– to track stolen or misappropriated devices;

– to determine the type and level of service than may be provided to the user (based on device capabilities);

– to determine the required quality of service for a connection between terminals (based on device capabilities).

The requirements for device profiles are as follows.

1) For each user equipment, one device profile may exist, which may consist of several "components".

2) These components may be distributed in the home network and/or service provider's environment.

3) Within the home network, the components may be distributed in various entities.

4) Within the home network, a functionality that is able to locate device profile components is required. This functionality allows services/applications to be unaware of the actual location of the components and is required to be under the control of the home network.

5) By endorsement of the user, services, applications and other NGN entities may be able to retrieve the whole device profile or selected parts of it (as required) in one transaction; criteria of privacy and data protection are required to be fulfilled.

6) An effective means to retrieve individual device profile components is required with acceptable delay for real-time services.

NOTE 2 – Although device profile management does not attempt to provide any classification of the data a device profile may contain, categorizations such as general device information, service specific information, etc., may be applied.

– The detailed requirements relating to device profile, its usage and management are expected to be contained in further ITU-T Recommendation(s).

6.20 Policy management

Policy management may be used in NGN to:

1) ensure service consistency across a range of access and core network technologies. This can be also applied across multiple service provider networks;

NOTE 1 – The policy applied to each network depends on the network technologies and it may be specific to each network technology.

2) provide admission control with respect to usage of network capabilities and network resources by services and applications;

3) provide network resource usage logging;

NOTE 2 – This can be viewed as the function that produces information which may be used by other network capabilities, such as accounting and charging functions.

4) shield services and applications from the intricate details of transport network implementation.

NOTE 3 – Policy control can be used to serve the needs of applications, while remaining agnostic about the network technologies deployed.

With the basic areas of applicability indicated above, and policy operating in conjunction with connectivity, QoS, and security, many actions can be taken in the policy management space that can benefit NGN services. For example, policy management may be applied to:

– service provisioning;

– service configuration;

– authorization (i.e., entitlements);

– service delivery;

– accounting and charging.

Policy management can invoke policy rules to provide reliable, consistent, deterministic outcomes called policy decisions. The complexity of these rules will be a function of their intended use.

NOTE 4 – QoS management capabilities such as resource and admission control (clause 6.9) may be seen as part of the global policy management capability set.

NGN release 1 policy management general requirements are as follows:

1) Policy management capabilities are required to be supported in order to ensure service access, provisioning and management.

2) Policy management capabilities are required to work within specific services, and within specific provider domains or across multiple provider domains.

3) Policy management capabilities are required to refuse or not respond to unauthorized requests, and respond to authorized requests.

6.21 Service enablers

The "service enablers" category groups capabilities providing features for specific or advanced services and applications, and/or enabling access to, and/or handling of, the specific information provided by these same capabilities.

6.21.1 Group management

This capability provides functionalities related to the secure and efficient management of groups of network entities (terminals, users, network nodes, etc.). It may be used by applications and services for different purposes, including VPN applications, video content distribution, device management, transport and service provisioning and management, emergency (community notification) services, etc.

A typical case which requires group management is a VPN service provided by a provider. In the VPN case, a closed group has to be defined with a member list of service users, and communications within this group should be securely protected from other users. NGN should manage such groups and provide secure group communications.

Another example is simultaneous distribution of video contents by multicast from a source to multiple users in a group. For such an application, the group management capability is also essential. Requirements of group management are as follows.

1) NGN is required to provide a capability which enables the creation of transport stratum groups.

2) NGN is required to provide a capability which enables the creation of service group and/or service-specific groups (service stratum).

3) NGN is required to manage groups, and provide secure group communications.

6.21.2 Personal information management

This capability provides management of application-specific static and dynamic information (user-related and communication-context-related). Examples of application-specific information include user contact information, application membership (passwords, etc.), default application parameters, bandwidth/QoS preferences (e.g., according to available access networks), media preferences, user-specified data, etc. Delivered by applications (e.g., notification and information services) according to pre-defined user preferences and policy attributes (e.g., across various mobile devices and access network types), this information may be stored and managed by the personal information management capability on behalf of the users. The personal information management capability, acting as user proxy with respect to applications, may also retrieve this information from applications on behalf of the users.

The following are requirements for the personal information management capability.

1) A personal information management capability may be provided. The personal information management capability may store and manage application-specific static and dynamic information on behalf of the users; it may also retrieve this information from applications on behalf of the users.
2) The information managed by the personal information management capability is required to be protected against unauthorized access/retrieval or manipulation, etc.
3) The personal information management capability should support different communication contexts.

6.21.3 Message handling

In today's networks, some services are supported in both wired and wireless environments, others are only found in one. For example, short message service (SMS) has been designed for a wireless environment, although it can now be found in some fixed networks, whereas instant messaging (IM) has been designed for a wired environment, although some mobile networks have implemented IM services. The expectations of the various services also differ in that some services are designed to be used in what is perceived as 'real time' and others are designed as a 'mailbox' service where the message is stored ready for delivery at a later time.

The message handling capability provides functionalities for message-based services. Functionalities include real-time and non-real-time messaging service control. Examples of real-time messaging are IM and Chat, non-real-time examples being electronic mail, SMS and multimedia messaging service (MMS).

General requirements are as follows.

1) NGN message handling capability is required to support messaging services accessible by both types of terminals, those which are for use of wired transport access and those for use of wireless transport access.
2) NGN message handling capability is required to support both real-time and non-real-time messaging services.

NOTE – The group management capability may be also necessary for supporting messaging services.

In addition, there are user requirements for the message handling capability to enable configuration features of messaging services, such as selection, filtering, formatting, group management and processing (e.g., isolation of unsolicited bulk telecommunications).

6.21.4 Multicast support

These capabilities enable applications to deliver content to multiple users at the same time using multicast mechanisms.

In addition to unicast, multicast mechanisms should be supported for efficient network resource usage.

For providing broadcast/multicast services, both the transport and the service strata should provide the related capabilities.

General requirements include the following:

1) NGN is required to support multicast capabilities in order to realize efficient and scalable data delivery.

2) NGN should provide capabilities to realize broadcast/multicast services in a single NGN or across multiple NGNs.

6.21.5 Presence

The presence capability (service) provides access to presence information and its availability to users or services. Presence is a set of attributes characterizing the current properties (e.g., status, location, etc.) of an entity.

An entity in this respect is any device, service, application, etc., that is capable of providing presence information. Availability, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity – e.g., time of day, device capabilities, media preferences and capabilities, etc. The terms "presence" and "availability" are almost always used together to provide a complete set of presence information.

NGN is required to support both a user as the supplier of presence information (sometimes called presentity [b-121.905]), and a user as the requester of presence information (watcher).

Presence is enabled by three capability groupings. Requirements for each capability grouping are described below.

Presence collection

1) NGN is required to provide a capability to collect information describing the connectivity state of the presentity on permission of the user, e.g., the device(s) used by a user.

2) NGN is required to provide a capability to collect information concerning the location of the presentity according to national regulations and laws.

Presence distribution

3) NGN is required to provide a capability to enable an entity, e.g., a user, to be informed of current presence status of the presentity. Another example is the usage of this capability to enable another service to access the users' presence information depending on the permission of the user.

Presence management

4) NGN is required to provide presence management, a set of capabilities to manage the presence information collected.

5) Access control to the presence information (using the presence distribution capabilities) is required to be managed in compliance with presentity privacy and access rules requirements.

6) The presence management capabilities are required to enable the distribution capability to supply only part of the presence information where required.

7) The presence management capabilities are required to enable collection of requests from certain entities to receive presence information for other entities. The presence management also provides the presentity with the ability to determine the distribution of its presence information, e.g., to accept or reject requests for presence information on a per watcher basis.

6.21.6 Location management

Location management is an enabling capability for provisioning of location-based applications and services, which use information regarding the location of users and devices within networks. The location of users and devices within networks may be related to their physical positioning, hence enhancing applications with local context and relevance.

Mechanisms to determine and report location information often depend on the access network technology. This means that support for location-based applications and services should be implemented within each access network technology.

The following are requirements for location management.

1) NGN is required to provide a location management capability to determine and report information regarding the location of users and devices within NGN according to national regulations and laws.
2) NGN is required to provide additional functionalities to ensure the correctness and authenticity of location information used by applications and services to mitigate any adversary effects due to fraudulent or false location information.
3) Privacy issues are required to be fulfilled by provisioning location-based services and applications.
4) The location management capability is required to provide a means to release location information according to the information contained in user/device profiles.

6.21.7 Push

Push is an enabler that provides the capability to transmit data from a sender to a recipient without previous request by the recipient, e.g., via SIP-based push mechanisms.

Whereas the user typically has the ability to configure push services from a range of services provided by service providers, the recipient does not have to issue a specific request but a general request for the data to be sent. Data can be sent either as a result of a single invocation application-dependent trigger or periodically.

As an example, push may be used to provide notification that a MMS message is available.

The push requirement is as follows:

1) NGN is required to support a push capability according to national regulations and laws.

NOTE – Invocation of push services may require user agreement.

6.21.8 Device management

Device management is an enabler that provides the network capabilities to manage and control devices. Device management capabilities may be used for:

– hardware/software configuration management, such as device hardware information, media capabilities, software version;
– remote software upgrades, both with and without user intervention, such as bug-fixes, features, OS, firmware, application clients;
– remote fault diagnosis.

General requirements for device management are as follows:

1) NGN is required to support device upgrades.
2) NGN is required to support device auto-configuration.
3) NGN is required to support gathering device connection information according to national regulations and laws, such as IP address and location.

4) Device management may provide functions for registering, managing and updating device information.

5) Device management may provide functions for remotely checking device status, including status changes and upgrades, and generating diagnostic reports.

6) Device management procedure is required to be secure, always carried out by a trusted entity according to national regulations and laws.

NOTE 1 – Device management should allow installation of user preferences and applications.

NOTE 2 – Invocation of device management services normally requires user agreement.

6.21.9 Session handling

NGN is required to provide the capabilities to set up, manage, and terminate end-to-end service sessions that involve, for example, multiple parties, a group of endpoints associated with those parties, and a description of multimedia connections among the endpoints. These session handling capabilities are required to be provided in both fixed and mobile environments in order to accommodate different service requirements, as well as to use the appropriate application servers for service operation.

The session handling functions include:

– session establishment;

– presentation of the identifier of originating party and connected-to party of a session;

– suppression of the identifier of originating party and connected-to party of a session;

– delivery and suppression of user-provided optional information (e.g., picture, video or text during session establishment);

– handling of an incoming session by the terminating party;

– negotiation of capabilities for an incoming session;

– accepting, ignoring, re-directing or rejecting an incoming session;

– negotiation of media and media components during session establishment;

– handling of an ongoing session;

– modification of media and media components in an ongoing session;

– suspending and resuming an ongoing session;

– ending a session;

– network-controlled session termination.

General requirements for session handling are as follows:

1) Session handling is required to be able to use the appropriate application servers for service operation.

2) The NGN is required to support the users' ability to invoke one or multiple sessions, and to activate concurrent multimedia applications within each session.

3) Session handling is required to support sessions with a variety of media types.

4) Session admission control based on defined levels of QoS and security is required to be supported.

5) Session admission control mechanisms are required to span multiple service types (e.g., voice, text and video).

6) If there are one or two participants in the session, the network is required to end a session at any time during the session, when requested by any of the session users. The network may end a session at any time during the session (e.g., in failure conditions).

7) If there are more than two participants in the session, the network may end a session at any time during the session, when requested by any of the session users. The network may end a session at any time during the session (e.g., in failure conditions).

6.21.10 Web-based application support

The web-based application support enablers allow enhanced utilization of device capabilities and network characteristics for web-based applications.

Web-based application support capabilities provide users with a consistent web environment which spans multiple network environments and multiple devices (PC, laptop, PDA, cell phone, etc.).

Web-based application support includes the following interactions:

– (application) server-to-server;

– server-to-terminal;

– terminal-to-server;

– terminal-to-terminal (or peer-to-peer).

NGN is required to provide web-based application support satisfying with the following:

1) interoperability across wired and wireless network environments;

2) secure access to applications;

3) nomadism;

4) low time delays and efficient bandwidth use.

NGN should provide web-based application support satisfying with the following:

5) re-use of existing technologies and NGN components (e.g., authentication) for web-based application provisioning;

6) re-use of authoring and integration tools;

7) consistent user experience across networks;

8) support of service composition techniques;

9) scalability of web-based applications;

10) non-degradation of NGN reliability.

NOTE – NGN release 1 may be limited in respect of web-based application support capabilities.

6.21.11 Data synchronization

Data synchronization is defined as the act of establishing equivalence between two data sets. The data synchronization enabler synchronizes networked data of different terminals, including handheld computers, mobile phones, laptop PCs and desktop PCs. Applications which may utilize the data synchronization enabler include calendar, contact information management, management of enterprise data stored in databases, and management of web documents.

NGN should support a data synchronization enabler with the following features:

1) synchronization of networked data with terminals supporting this capability;

2) synchronization of a terminal with appropriate networked data;

3) synchronization of networked data among terminals.

If a data synchronization enabler is supported, the following requirements apply:

1) The data synchronization enabler is required to be independent from transport protocols.

2) Arbitrary networked data is required to be supported.

3) Data synchronization should be aware of the resource limitations of terminals.

6.22 PSTN/ISDN emulation and simulation

Evolution of networks to NGN is dependent on provider's choices and their needs. Network providers may choose an evolution path depending on their actual resources, business plans and strategies. Therefore, they may choose different technologies and time-frames.

For the transition period from PSTN/ISDN to NGN, NGN is required to provide the following capabilities:

1) PSTN/ISDN emulation capabilities;

2) PSTN/ISDN simulation capabilities.

Requirements for these capabilities are described below.

6.22.1 PSTN/ISDN emulation requirements

6.22.1.1 General requirements for PSTN/ISDN emulation

NGN is required to provide at least one level of service of PSTN/ISDN emulation service that offers capabilities that are the same or better than those provided by circuit-switched networks.

6.22.1.2 Terminal requirements for PSTN/ISDN emulation

NGN is required to support legacy terminals (e.g., traditional PSTN phones, text phones, facsimile machines, and other types of existing PSTN/ISDN terminals) which are not attached via a NGN UNI but via a PSTN/ISDN like UNI.

NOTE – Emulation of the full PSTN/ISDN service set may not be possible and service support may be restricted to certain terminal types, i.e., legacy terminals or user equipment that behave like legacy terminals.

6.22.1.3 Service requirements for PSTN/ISDN emulation

Service requirements for PSTN/ISDN emulation are the following:

1) NGN is required to support the ability for service providers to emulate one or more of their PSTN/ISDN services.

2) NGN is required to support capability definitions inherited from existing PSTN/ISDN specification.

NOTE – A specific NGN deployment need not support all possible capabilities and interfaces which are present in PSTN/ISDN.

6.22.2 PSTN/ISDN simulation requirements

6.22.2.1 General requirements for PSTN/ISDN simulation

NGN is required to support PSTN/ISDN simulation services that provide the user with a PSTN/ISDN-like experience.

6.22.2.2 Terminal requirements for PSTN/ISDN simulation

NGN is required to support non-legacy terminals for PSTN/ISDN simulation services. It may also support adaptation devices to allow legacy terminals to connect via adaptation devices to NGN (e.g., black phones, text phones and facsimile machines).

6.22.2.3 Service requirements for PSTN/ISDN simulation

Service requirements for PSTN/ISDN simulation are the following:

1) NGN is required to support PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

2) NGN should provide the ability for a service provider to simulate PSTN/ISDN services.

3) NGN is not required to provide services identical to those in PSTN/ISDN.

NOTE – It is assumed that the PSTN/ISDN simulation services do not utilize PSTN/ISDN call models or signalling protocols.

6.23 Public interest aspects

NGN is required to provide capabilities for the support of public interest services required by regulations or laws of national or regional administrations and international treaties. These public interest services may include, among others, the services described in the following subclauses within this clause.

6.23.1 Lawful interception

1) An NGN transport provider and/or NGN service provider are required to respond to lawful interception requirements. Therefore, an NGN is required to provide mechanisms that make lawful interception possible where required by regulation or law of a country in their application area.

2) The lawful interception mechanisms are required to provide access to content of communication (CC) and intercept related information (IRI) by law enforcement agencies (LEA), as per the requirements of administrations and international treaties.

Because the nature of lawful interception is dependent upon national/regional customs and laws, requirements are dependent upon the regulatory environment of each country.

6.23.2 Malicious communication identification

NGN is required to include the capability to identify the source of a malicious communication, e.g., obtaining the identifier of the terminal involved or the location of the originator of the communication.

6.23.3 Unsolicited bulk telecommunications

NGN is required to provide capabilities to prevent unsolicited bulk telecommunications.

6.23.4 Emergency telecommunications

Emergency telecommunications (including support of early warning) include:

– individual-to-authority telecommunications, e.g., calls to emergency service providers;

– authority-to-authority telecommunications, e.g., telecommunications for disaster relief (TDR);

– authority-to-individual telecommunications, e.g., community notification services.

NOTE – In addition to being used for authority-to-authority telecommunications, TDR and emergency telecommunications service (ETS) may also be used for authority-to-individual telecommunications.

[ITU-T Y.1271], [ITU-T E.106] and [ITU-T E.107] provide *"Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks"*, *"International Emergency Preference Scheme (IEPS) for disaster relief operations"* and *"Emergency Telecommunications Service and interconnection framework for national implementations of ETS"*, respectively.

NGN is required to make network capabilities available to early warning applications, e.g., to provide geographical location information to support provision of warning messages only to those possibly affected by an impending disaster.

The support of emergency telecommunications and early warning requires the NGN to be operationally robust and have high availability.

NGN is required to:

1) include service and transport level capabilities to allow emergency telecommunications to be supported using priority/preferential schemes. Call/session control of emergency telecommunications and emergency telecommunications bearer traffic is required to receive priority treatment during congestion/failure conditions;

2) provide as necessary the interworking and mapping of priority mechanisms between the various components of NGN (e.g., between the access and the core network, and between the service stratum and the transport stratum) and between NGNs (e.g., between two core service provider networks) to assure appropriate end-to-end priority/preferential telecommunications;

3) support existing telecommunication services, including an equivalent to all existing PSTN/ISDN emergency telecommunication services, even when one or more of communicating entities are attached to an NGN and one or more are attached to a PSTN/ISDN;

4) enable new emergency telecommunication means (e.g., instant messaging) to be supported in future deployments by authorities (such as emergency service providers);

5) provide seamless interworking of emergency telecommunications across all public networks within an administrative (emergency) domain;

6) provide routing of emergency telecommunications to appropriate authorities;

7) provide routing of emergency telecommunications from the authority to individuals;

8) provide, where possible, continuation of emergency telecommunication between the authority and individuals until the authority terminates the session, even though the individual may have hung up;

9) provide to the authority information regarding the individual's geographical location as well as their identifier according to national or regional regulation requirements. When required by regulation or law, this information can be acquired by the authority even though the individual requested withholding this information;

10) provide the ability for both authenticated and unauthenticated access to emergency telecommunication services according to national or regional regulation requirements. For example, NGN is required to provide the ability to authenticate user access to ETS/TDR telecommunications;

11) support exemption of emergency telecommunications from certain restrictive network management functions;

12) support emergency telecommunications with alternative and multiple media when required (e.g., by regulation or law). Video, text and voice and any combination thereof, as well as various forms of messaging, are essential for telecommunication with the emergency services for people with disabilities;

13) provide capabilities to ensure that only authorized early warning messages are distributed;

14) provide capabilities to prevent untargeted and unnecessary early warning-like messages.

6.23.5 User identifier presentation and privacy

1) NGN is required to have the capability to present the identifier of the originating party.

2) NGN is required to have the capability to present the identifier of the terminating party.

3) NGN shall have the capability to suppress the presentation of the identifier of the originating party.

4) NGN shall have the capability to suppress the presentation of the identifier of the terminating party.

NOTE – The requirements for support of emergency telecommunications may override the suppression.

6.23.6 Network or service provider selection

NGN is required to support the capability for provider selection, where required (e.g., by regulation or law).

6.23.7 Users with disabilities

Users with disabilities have a general need to be provided with means to control and use terminals and services in alternative ways and modes, suiting varied capabilities and preferences. Such requirements are best met by inclusive design of the general provision of terminals and services.

1) NGN is required to provide the means needed for invocation of relay services. Relay services translate between various modes of telecommunication that are of interest for people with disabilities (e.g., sign language, lip reading, text, voice). Invocation of relay services may be based on user preferences, address resolution or user commands.

2) NGN is required to have the capability to invoke relay services by either party in an emergency telecommunication.

   NOTE 1 – Other needs for users with disabilities to use emergency telecommunication services are handled in clause 6.23.4.

NOTE 2 – See also in Bibliography [b-ITU-T TP.TACL] and [b-ITU-T F.790].

6.23.8 Number portability

Number portability is a PSTN/ISDN network capability.

The equivalent capability in NGN is identifier portability (clause 6.12.2). PSTN/ISDN emulation places no new requirements to support number portability because emulated services are inherited from the PSTN/ISDN (see clause 6.22.1.3).

6.23.9 Service unbundling

In many national jurisdictions, it is required that service providers "unbundle" their offerings to allow customers a choice of providers for diverse services, as well as allow providers to competitively offer their services to customers.

Where required, e.g., by regulation or law, NGN is required to support mechanisms to realize service unbundling.

6.24 Critical infrastructure protection

Service providers should have capabilities to protect their NGN infrastructure from malicious attacks, such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection may include prevention, detection and recovery from attacks, and measures to prevent service outages.

Security requirements are provided in clause 6.13.

6.25 Non-disclosure of information across NNI interfaces

Where required e.g., by regulation, law, country or regional conditions, NGN is required to have capabilities to enable:

– service providers to prevent disclosure of internal information or service users' information to other entities across NNI interfaces;

– network providers to prevent disclosure of internal network information as well as network users' information to other entities across NNI interfaces.

6.26 Inter-provider exchange of user-related information

Where required, e.g., by regulation or law, NGN is required to support mechanisms to exchange user-related information between NGNs for service interoperability.

Appendix I

Mapping of services to service enablers

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

This appendix provides an example mapping of selected services to selected service enablers (clause 6.21). The mapping is not meant to be exhaustive nor represent requirements for support.

Table I.1 – Illustrative mapping of services to service enablers

Services\Service Enablers	Presence	Location management	Group management	Message handling	Multicast support	Push	Session handling
Real-time conversational voice services							X
Real-time text							X
Messaging services	X		X	X			X
Push to talk over NGN	X		X				X
Point-to-Point interactive multimedia services			X				X
Collaborative interactive communication services		X	X				X
Content delivery services		X				X	
Push-based services		X				X	
Broadcast/multicast services					X		
Hosted and transit services for enterprises			X				X
Information services	X	X				X	
Presence and general notification services	X	X	X				
3GPP release 6 and 3GPP2 release A OSA-based services	X	X	X	X	X	X	X
Data retrieval applications	X					X	
VPN services			X		X		

Bibliography

The following documents contain information that may be valuable to the reader of this Recommendation. They provide additional information about topics covered within this Recommendation, but are not essential for an understanding of this Recommendation.

ITU Recommendations

[b-ITU-R M.1645] ITU-R Recommendation M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-T E.351] ITU-T Recommendation E.351 (2000), *Routing of multimedia connections across TDM-, ATM- and IP-based networks*.

[b-ITU-T F.703] ITU-T Recommendation F.703 (2000), *Multimedia conversational services*.

[b-ITU-T F.724] ITU-T Recommendation F.724 (2005), *Service description and requirements for videotelephony services over IP networks*.

[b-ITU-T F.733] ITU-T Recommendation F.733 (2005), *Service description and requirements for multimedia conference services over IP networks*.

[b-ITU-T F.741] ITU-T Recommendation F.741 (2005), *Service description and requirements for audiovisual on-demand services*.

[b-ITU-T F.742] ITU-T Recommendation F.742 (2005), *Service description and requirements for distance learning services*.

[b-ITU-T F.790] ITU-T Recommendation F.790 (2007), *Telecommunications accessibility guidelines for older persons and persons with disabilities*.

[b-ITU-T G.722.2] ITU-T Recommendation G.722.2 (2003), *Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)*.

[b-ITU-T G.729] ITU-T Recommendation G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[b-ITU-T G.729A] ITU-T Recommendation G.729 Annex A (1996), *Reduced complexity 8 kbit/s CS-ACELP speech codec*.

[b-ITU-T G.780] ITU-T Recommendation G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[b-ITU-T G.799.1] ITU-T Recommendation G.799.1/Y.1451.1 (2004), *Functionality and interface specifications for GSTN transport network equipment for interconnecting GSTN and IP networks*.

[b-ITU-T G.805] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[b-ITU-T G.809] ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks*.

[b-ITU-T G.1000] ITU-T Recommendation G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

[b-ITU-T G.1010] ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories*.

[b-ITU-T H.263] ITU-T Recommendation H.263 (2005), *Video coding for low bit rate communication*.

[b-ITU-T H.264] ITU-T Recommendation H.264 (2005), *Advanced video coding for generic audiovisual services*.

[b-ITU-T H.510] ITU-T Recommendation H.510 (2002), *Mobility for H.323 multimedia systems and services*.

[b-ITU-T H-supp1] ITU-T H-series Supplement 1 (1999), *Application profile – Sign language and lip-reading real-time conversation using low bit-rate video communication*.

[b-ITU-T I.230] ITU-T Recommendation I.230 (1988), *Definition of bearer service categories.*

[b-ITU-T I.250] ITU-T Recommendation I.250 (1988), *Definition of supplementary services.*

[b-ITU-T M.3017] ITU-T Recommendation M.3017 (2003), *Framework for the integrated management of hybrid circuit/packet networks*.

[b-ITU-T Q.833.1] ITU-T Recommendation Q.833.1 (2001), *Asymmetric digital subscriber line (ADSL) – Network element management: CMIP model*.

[b-ITU-T Q.1200] ITU-T Recommendation Q.1200 Series (1997), *General series Intelligent Network Recommendation structure*.

[b-ITU-T Q.1236] ITU-T Recommendation Q.1236 (1999), *Intelligent Network Capability Set 3 – Management Information Model Requirements and Methodology*.

[b-ITU-T Q.1702] ITU-T Recommendation Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000.*

[b-ITU-T Q.1742.4] ITU-T Recommendation Q.1742.4 (2005), *IMT-2000 references (approved as of 30 June 2004) to ANSI-41 evolved core network with cdma2000 access network.*

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

[b-ITU-T T.140] ITU-T Recommendation T.140 (1998), *Protocol for multimedia application text conversation.*

[b-ITU-T Y.1411] ITU-T Recommendation Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*.

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

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

ITU-T Guidelines

[b-ITU-T TP.TACL] ITU-T Technical paper: Accessibility Checklist for use in ITU-T standardisation work (2006). (available at www.itu.int/ITU-T/studygroups/com16/accessibility/docs/tacl.pdf)

ETSI Technical Specifications

[b-101.331] ETSI TS 101 331 V1.2.1 (2006-06), *Requirements of Law Enforcement Agencies*.

[b-102.71] 3GPP TS 22.071 3rd Generation Partnership Project; Technical specification Group Services and System Aspects; *Location Services (LCS); Service description; Stage 1* (Release 1999).

[b-121.905] ETSI TR 121 905 V7.3.0 (2007-03), *Vocabulary for 3GPP Specifications*.

[b-122.057] ETSI TS 122 057 V6.0.0 (2005-01), *Mobile Execution Environment (MExE) service description; Stage 1*.

[b-122.127] ETSI TS 122 127 V7.1.0 (2006-03), *Service requirement for the Open Services Access (OSA); Stage 1*.

[b-122.140] ETSI TS 122 140 V6.7.0 (2005-03), *Multimedia Messaging Service (MMS); Stage 1*.

[b-122.146] ETSI TS 122 146 V7.2.0 (2006-09), *Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.

[b-122.174] ETSI TS 122 174 V6.2.0 (2005-01), *Push service; Stage 1*.

[b-122.240] ETSI TS 122 240 V6.5.0 (2005-01), *Service requirements for 3GPP Generic User Profile (GUP); Stage 1*.

[b-122.250] ETSI TS 122 250 V6.0.0 (2005-01), *IP Multimedia Subsystem (IMS) Group Management; Stage 1*.

[b-122.708] ETSI TS 122 078 V7.6.0 (2005-12), *Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description*.

[b-123.141] ETSI TS 123 141 V7.2.0 (2006-09), *Presence service; Architecture and functional description; Stage 2*.

[b-123.228] ETSI TS 123 228 V7.7.0 (2007-03), *IP Multimedia Subsystem (IMS); Stage 2*.

[b-126.235] ETSI TS 126 235 V6.4.0 (2005-03), *Packet switched conversational multimedia applications; Default codecs*.

[b-133.106] ETSI TS 133 106 V7.0.1 (2006-01), *Lawful interception requirements*.

[b-142.033] ETSI TS 142 033 V7.0.0 (2007-06), *Lawful interception – Stage 1*.

[b-181.005] ETSI TS 181 005 V1.1.1 (2006-03), *Services and Capabilities Requirements*.

American National Standards Institute (ANSI) Standards

[b-JSTD025] ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA)*.

[b-T1.678] ANSI ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*.

[b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception, March, 2004*.

[b-TIA-1066] TIA-1066 (2006), *Lawfully Authorized Surveillance (LAES) for cdma2000 Voice Over IP (VoIP)*.

[b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular*.

[b-TIA-1016-A] *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems (TIA-1016-A-2006)*.

[b-TIA-127-A] *Enhanced Variable Rate Codec Speech Service Option 3 for Wideband Spread Spectrum Digital Systems (ANSI/TIA-127-A-2004)*.

IETF Specifications

[b-RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier*.

[b-RFC 4594] IETF RFC 4594 (2006), *Configuration guidelines for DiffServ Service Classes*.

Open Mobile Alliance Specifications

[b-OMA-DS] OMA Data Synchronization V1.2 – **Status**: Approved Enabler – **Release Date**: 2006-07-10.

[b-OMA-DM] OMA Device Management V1.2 – **Status**: Approved Enabler – **Release Date**: 2007-02-09.

[b-OMA-OSE] OMA Service Environment V1.0 – **Status**: Candidate Release – **Release Date**: 2007-03-13.

[b-OMA-PoC] OMA Push to talk over Cellular V1.0.1 – **Status**: Approved Enabler – **Release Date**: 2006-11-28.

[b-OMA-PS] OMA Presence Simple V1.0.1 – **Status**: Approved Enabler – **Release Date**: 2006-11-28.

[b-OMA-WS] OMA Web Services V1.1 – **Status**: Approved Enabler – **Release Date**: 2006-03-28.

[b-OMA-XML] OMA XML Document Management V1.0.1 – **Status**: Approved Enabler – **Release Date**: 2006-11-28.

[b-OMA-LS] OMA Mobile Location Service V1.1 – **Status**: Candidate Enabler – **Release Date**: 2006-10-20.

[b-OMA-XDM] OMA XML Document Management V1.0.1 – **Status**: Approved Enabler – **Release Date**: 2006-11-28.

[b-OMA-Push] OMA Push V2.1 – **Status**: Candidate Enabler – **Release Date**: 2005-11-22.

Open Service Access (OSA)

[b-OSA-Parlay-X] *Open Service Access (OSA), Parlay X Web Services, Parts 1-14*, ETSI ES 202 391-[1-14] V1.1.1 (2006-12).

[b-OSA-Parlay-4] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-14*, ETSI ES 202 915-[1-14] V1.3.1 (2006-12).

[b-OSA-Parlay-5] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-15*, ETSI ES 203 915-[1-15] V1.1.1 (2007-01).

IN Services

[b-TIA-771] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001)*.

[b-TIA-873] TIA/EIA 873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2*.

UDDI Specifications

[b-UDDI] UDDI Specification Technical committee, *UDDI Specification*, Version 3.0.2.

SOA Specifications

[b-OASIS-SOA] *OASIS, Reference Model for Service Oriented Architecture 1.0*, Committee Specification 1. 2 August 2006.

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