ETSI TR 102 806 V1.1.1 (2009-11)

Technical Report

User Group;
Analysis of current End-to-End QoS standardization state

Reference

DTR/USER-00031

Keywords

QoS, Interface

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 4

Foreword....4

Introduction 4

1 Scope 5

2 References 5
2.1 Normative references 5
2.2 Informative references....5

3 Definitions and abbreviations....7
3.1 Definitions....7
3.2 Abbreviations 9

4 NGN Context....11
4.1 User centric 12
4.2 Mobility....14
4.3 Heterogeneous environment....18
4.3.1 IMS Architecture (3GPP) 19
4.3.2 TISPAN NGN architecture....22
4.4 Conclusion....23

5 Requirement for QoS continuity 24

6 Analysis of related work for QoS....25
6.1 Control plane....25
6.1.1 MIH 26
6.1.2 MIPv6....30
6.1.3 NSIS....31
6.1.4 SIP 34
6.2 Management Plane 36
6.2.1 Policy control....36
6.2.2 Diameter 40
6.3 User plane (CPN: Customer Premises Network)....42
6.3.1 Service provided in CPN 42
6.3.2 CPN architecture model interacting with the NGN/IMS networks....44

7 Conclusion and next steps....46

Annex A: Bibliography....47

History 48

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI User Group (USER).

Introduction

This analysis of the current End-to-End (E2E) QoS standardization state was carried out as a preliminary work to the drafting of the multipart deliverable TR 102 805 "User Group; End-to-end QoS management at the Network Interfaces". Its publication was decided, considering that it could be useful to other ETSI TB.

1 Scope

The present document provides information on the standards and documents available in the area of end to end QoS.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
    - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] 3GPP TR 25.832 (V4.0.0): "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Manifestations of Handover and SRNS Relocation (Release 4)".

[i.2] ETSI TS 124 229 (V5.23.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 5.23.0 Release 5)".

[i.3] ETSI EG 202 132 (V1.0.0): "Human Factors (HF); User Interfaces; Guidelines for generic user interface elements for mobile terminals and services".

[i.4] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.5] ETSI ES 282 003 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[i.6] ETSI ES 282 004 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[i.7] ETSI ES 282 007 (V2.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[i.8] ETSI ES 283 003 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]".

[i.9] ETSI TR 102 805-1 (V1.1.1): "User Group; End-to-end QoS management at the Network Interfaces; Part 1: User's E2E QoS - Analysis of the NGN interfaces (user case)".

[i.10] ETSI TR 102 805-2 (V1.1.1): "User Group; End-to-end QoS management at the Network Interfaces; Part 2: Control and management planes solution - QoS continuity".

[i.11] ETSI TS 123 207 (V7.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) concept and architecture (3GPP TS 23.207 version 7.0.0 Release 7)".

[i.12] ETSI TS 123 228 (V8.6.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 8.6.0 Release 8)".

[i.13] ETSI TS 129 208 (V6.7.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) signalling flows (3GPP TS 29.208 version 6.7.0 Release 6)".

[i.14] ETSI TS 129 212 (V8.1.0): "Universal Mobile Telecommunications System (UMTS);Policy and charging control over Gx reference point (3GPP TS 29.212 version 8.1.0 Release 8)".

[i.15] ETSI TS 129 214 (V8.2.0): "Universal Mobile Telecommunications System (UMTS);Policy and charging control over Rx reference point (3GPP TS 29.214 version 8.2.0 Release 8)".

[i.16] ETSI TS 182 012 (V2.1.4): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[i.17] ETSI TS 182 027 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[i.18] ETSI TS 182 028 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; Dedicated subsystem for IPTV functions".

[i.19] ETSI TS 185 005 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[i.20] ETSI TS 185 006 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and interfaces and Reference Points".

[i.21] IEEE 802.11b: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band".

[i.22] IEEE 802.21: "Media Independent Handover; QOS Framework and parameters", February 17, 2006.

[i.23] ITU-T Recommendation Q.1706/Y.2801 (2006): "Mobility management requirements for NGN".

[i.24] IETF RFC 3261 (2002): "SIP(Session Initiation Protocol)".

[i.25] IETF RFC 3344 (2002): "Mobility Support in IPv4".

[i.26] IETF RFC 3753: "Mobility Related Terminology", June 2004. J. Manner, M. Kojo et al.

[i.27] IETF RFC 3775 (2004): "Mobility Support in IPv6".

[i.28] IETF RFC 4006 (2005): "Diameter Credit-Control Application".

[i.29] IETF RFC 4080: "NSIS Framework" June 2005.

[i.30] NLSP for QoS.

NOTE: Available at: http://www.ietf.org/html.charters/nsis-charter.html.

[i.31] QoS NSLP QSPEC Template.

NOTE: Available at: http://www.ietf.org/html.charters/nsis-charter.html

[i.32] TeleManagement Forum.

NOTE: Available at: http://www.tmforum.org.

[i.33] Gilles Bertrand: "The IP Multimedia Subsystem(IMS)-An overview".

[i.34] Th. Magedanz Senior Member IEEE, F.C. de Gouveia, "IMS-the IP Multimedia System as NGN Service Delivery Platform", Bektrotechnik & Informationstechnik (2006), pp. 271-276.

[i.35] IETF RFC 2475: "An Architecture for Differentiated Service".

[i.36] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers ".

[i.37] IETF RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[i.38] IEEE 802.11g: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".

[i.39] ETSI TS 129 207: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Policy control over Go interface (3GPP TS 29.207 Release 6)".

[i.40] ITU: "Study Group 19 - Contribution 25: Considerations of horizontal handover and vertical handover, 2007".

[i.41] ETSI TS 129 214 (V7.1.0): "Universal Mobile Telecommunications System (UMTS); Policy and charging control over Rx reference point (3GPP TS 29.214 Release 7)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

AmbientGrid: information inference (AmbientGrid) based on the profiles' matching, to structure with grid covering the needed user centric environment

Class of Service (CoS): way of traffic management in the network by grouping similar types of traffic and treating them as its own level of service priority

DiffServ networks: classify packets into one of a small number of aggregated flows or 'classes', based on the DiffServ codepoint (DSCP) in the packet's IP header

NOTE: This is known as behaviour aggregate (BA) classification (RFC 2475 [i.35]). At each DiffServ router, packets are subjected to a 'per-hop behaviour' (PHB), which is invoked by the DSCP (RFC 2474 [i.36])

horizontal handove: handover within homogeneous access networks

NOTE 1: Generally it is referred to as the Intra-AN handover.

NOTE 2: ITU: Study Group 19 - Contribution 25: Considerations of horizontal handover and vertical handover, 2007 [i.40]

infosphere: decisional knowledge base managing, in the real time, all the personalization and ambient environment information

IntServ (integrated services architecture): set of extensions to the traditional best effort model of the Internet with the goal of allowing end-to-end QoS to be provided to applications

NOTE 1: One of the key components of the architecture is a set of service; the current set of services consists of the controlled load and guaranteed services. The architecture assumes that some explicit setup mechanism is used to convey information to routers so that they can provide requested services to flows that require them. While RSVP is the most widely known example of such a setup mechanism, the IntServ architecture is designed to accommodate other mechanisms.

NOTE 2: See RFC 1633 [i.37].

multi-homing: user's services can be provided by more than one service or network provider

network mobility: network's ability, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself

policy control: adaptation and configuration of QoS according to particular goals dependent of user, network operator and service provider

QoS Classification: definition of class priority for QoS by describing traffic condition or performance parameters

QoS handover: ensures QoS state establishes when vertical/horizontal handover occurs

QoS Interworking: ensures the transfer of all different types of packet data with different QoS parameters in heterogeneous environment whenever the ANs and CNs are of different releases and types by mapping the QoS attributes

service mobility: ability to consistently provide services to the end-user, to maintain the expected QoS, at the system's initiative, regardless of the end-user's location, terminals, or networks.

NOTE: To maintain the service continuity, the session mobility is used.

terminal mobility: user uses his terminal to move across the same or different networks while having access to the same set of subscribed services

user mobility: ability for a subscriber to move to different physical locations and be able to use one or more devices connected to one or more access networks to gain access to their services without interruption

user session: period of communication between one user and another or other users or servers characterized by a starting time and a termination time, including setting up the relation of the user equipment, access network, core network and services

userware: innovative user centric middleware (Userware) enhancing the seamless feasibility along with the location and activity, personalization and user's ambient contexts

vertical handover: handover across heterogeneous access networks. Generally, it is referred to as the Inter-AN handover

NOTE: ITU STUDY GROUP 19 - CONTRIBUTION 25: Considerations of horizontal handover and vertical handover, 2007 [i.40].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	The 3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ACF	Admission Control Function
ACK	ACKnowledgement
AMF	Access Management Function
AN	Access Network
API	Application Programming Interface
A-RACF	Access Resource and Admission Control Function
ARF	Access Relay Function
AS	Application Server
ASF	Application Server Functions
ASP	Application Service Provider
AVP	Attribute-Value-Pair
BA	Binding Acknowledgement
BGCF	Breakout Gateway Control Function
BGF	Border Gateway Function
BU	Binding Update
CAC	Connection Admission Control
C-BGF	Core Border Gateway Function
CCA	Credit-Control Answer
CCR	Credit-Control Request
CDR	Charging Data Records
CN	Core Network
CND	Customer Network Devices
CNG	Customer Network Gateway
CNGCF	Customer Network Gateway Configuration Function
CoA	Care of Address
COPS	Common Open Policy Service
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
CTF	Charging Trigger Function
DCCP	Datagram Congestion Control Protocol
DiffServ	Differentiated Services
DSCP	DiffServ CodePoint
E2E QoS	End-to-End QoS
ETSI	European Telecommunications Standards Institute
FBC	Flow Based Charging
GIST	Generic Internet Signalling Transport
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HA	Home Agent
HHO	Horizontal HandOver
HLR	Home Location Register
HoA	Home Address
HSS	Home Subscriber Server
I/S CSCF	Interrogating/Serving CSCF
I-BGF	Interconnection Border Gateway Function
IEEE	Institute of Electrical & Electronic Engineers
IETF	Internet Engineering Task Force
IM	IP Multimedia
IMS	IP based Multimedia Subsystem
IN	Intelligent Network
IntServ	Integrated Services
IP-CAN	IP-Connectivity Access Networks
IPTV	Internet Protocol TeleVision

ISC	IP multimedia Service Control
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication standardization sector
IWU	InterWorking Unit
L2TF	Layer 2 Terminal Function
M2M	Machine-to-Machine
MAC	Medium Access Control
MGCF	Media Gateway Control Function
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIPv4	Mobile IP v4
MIPv6	Mobile IP v6
MN	Mobile Node
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
NACF	Network Access Configuration Function
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NGN	Next Generation Network
NGS	Next Generation Service
NSIS	Next Steps In Signalling
NSLP	NSIS Signalling Layer Protocols
NTLP	NSIS Transport Layer Protocol
OCS	Online Charging System
OSA	Open Service Access
OSI	Open System Interconnection
PCC	Policy and Charging Control
PCEF	Policy Enforcement Point
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy CSCF
PDA	Personal Digital Assistant
PDBF	Profile Data Base Function
PDG	Packet Data Gateway
PDP	Policy Decision Point
PDU	Protocol Data Unit
PEF	Policy Enforcement Function
PEP	Policy Enforcement Point
PES	PSTN/ISDN Emulation Subsystem
PHB	Per Hop Behaviour
PHY	PHYsical layer
PLMN	Public Land Mobile Network
PS	Proxy Server
PSTN	Public Switched Telephone Network
QNF	QoS NLSP Forwarder
QNI	QoS NLSP Initiator
QNR	QoS NLSP Responder
QoS	Quality of Service
QoSM	Quality of Service Managemer
QSPEC	QoS SPECification
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RMF	Resource Management Function
RS	Register Server
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
SBLP	Service Based Local Policy
SCIM	Service Capability Interaction Manager
SCP	Service Control Point
SCS	Service Capability Server

SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SID	Session IDentifier
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscription Locator Function
SLS	Service Level Specification
SP	Service Provider
SPDF	Service Policy Decision Function
SSF	Service Switch Function
TCP	Transmission Control Protocol
TE	Terminal Equipment
T-MGF	Trunk Media Gateway Function
TPF	Traffic Plane Function
UAAF	User Access Authorization Function
UDP	User Datagram Protocol
UE	User Equipment
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunications Systems
UMTSc	Universal Mobile Telecommunications Systems
URL	Universal Resource Locator
VHE	Virtual Home Environment
VHO	Vertical HandOver
VoIP	Voice over IP
WAG	Wireless Access Gateway
WLAN	Wireless Local Area Network

4 NGN Context

The successor of the 3G network is a single All-IP infrastructure which is referred to as NGN (Next Generation Network). A major characteristic of the Next Generation Network is its ability to handle heterogeneous and mobile environments for users and service providers.

One can consider four different types of mobility: User mobility, Terminal mobility, Network mobility and Service mobility. Moreover, heterogeneity exists in user's terminals, access networks, core networks as well as in services.

The ability to provide seamless mobility and adaptive quality of service in such a heterogeneous environment is THE key to the success of Next-Generation Networks.

Our analysis of the context led us to highlight innovative properties (clause 4.1).

Users wish to have a continuous multimedia service in a single session whether they are moving around (terminal mobility) or changing terminal (user mobility). This service session is user-centric, meaning that a user should have a continuity of service based on customization. Next service generation should have the self-management ability to dynamically accommodate user requests by adding or changing service components in a single service session.

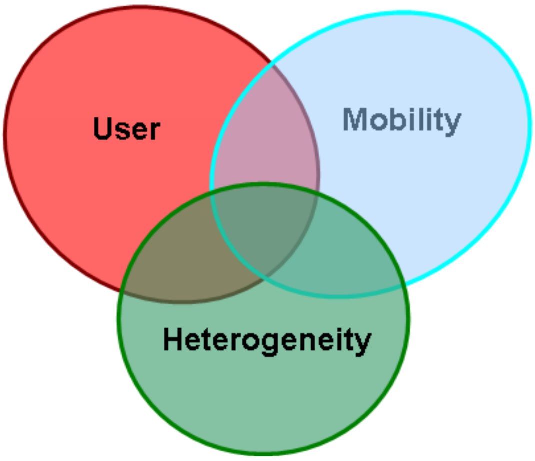


Figure 1: NGN context

In this clause, a basic introduction on the three main characteristics of NGN is provided: the User Centric conception (clause 4.1), the heterogeneous environment (clause 4.2), and the general mobility in NGN (clause 4.3). A conclusion is then proposed in clause 4.4.

4.1 User centric

Telecommunication evolved from system centric (user has to comply with various treatments) to network centric (user has to comply with various connections), and now to User centric. User information, QoS requirements and preferences are defined in the user's profile (Figure 2). In this new context, a common understanding about services, priorities, responsibilities, etc, is needed between the service provider and the user. This is expected to lead, in the case of business users, to a formal Service Level Agreement (SLA) or, in the case of the general public, to QoS commitments of the provider included in the service contract according to the relevant regulation.

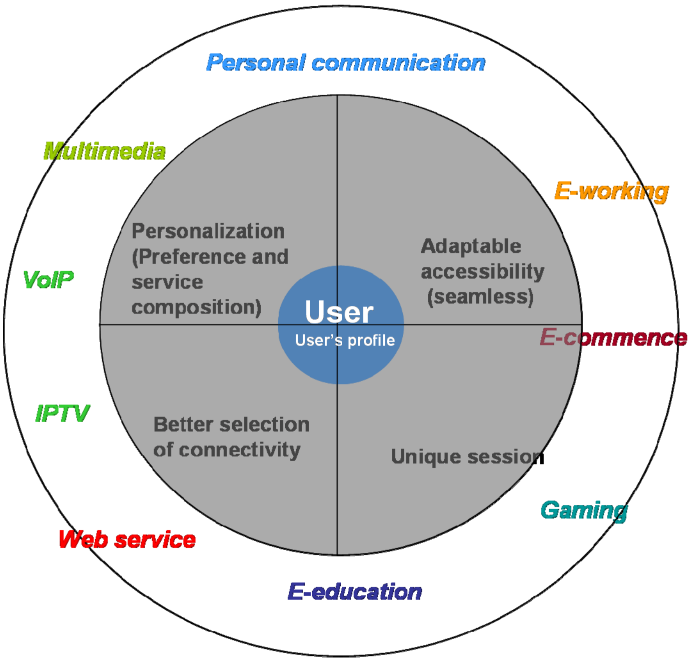


Figure 2: User centric

User centric means that users can access services, in a customized way with a single authentication and "always in a unique user session". This concept contains four essential requirements explained below:

- **Adaptable accessibility** to services regardless the terminal used
  End users may have several User Equipments (UE) in a Seamless Userware vision, for instance a computer, a PDA, a mobile telephone etc, all trying to access the same service. Each of these equipments has its specific context and conditions of use, and each user has his specific preferences.
  In such a situation, one key question is how to adapt services to a chosen terminal while complying to user's preferences.

- **Unique user session** for multimedia services (Continuity of service)
  During an on-going session, a user can enjoy different services from different providers. For example, during a telephone call, a user can add a Videophone service, and a movie program which may later on be transferred to a PDA. Users expect such service continuity to be provided via a unique user session.

- **Customization of service**
  The NGS (Next Generation Service) concept considers services as a flexible composition of autonomous service components customizable according to user's preferences and to the user profile. Thus, user's preferences should be taken into consideration while managing service composition across heterogeneous networks.

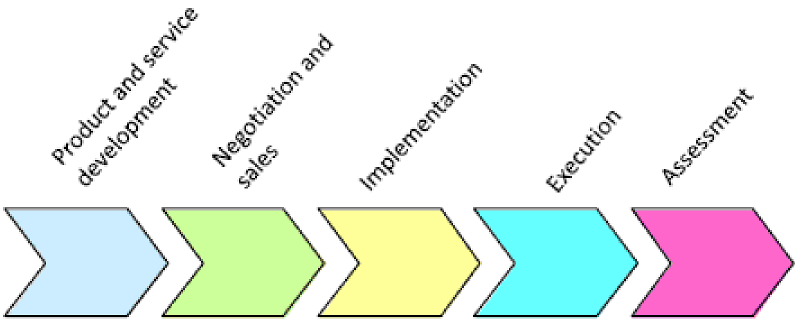
- **Better selection of connectivity with QoS**
  Today's technology allows a terminal to be able to access services through different access networks (WiFi, GSM, UMTS, etc.). This means that a user can switch from one access mode to another one in a dynamic manner according to user's preferences (QoS, location, availability, etc.).

All these four characteristics are subtended by the SLA concept.

SLA (Service Level Agreement) is an abbreviation often used in the context of contract between business users and their providers. In the present document, the meaning of SLA has been mapped to cover as well the case of the QoS commitments implied in the provision of telecommunication services to the general public.

The TeleManagement Forum [i.32] defines a SLA as "a formal negotiated agreement between two parties, sometimes called a service level guarantee. It is a contract (or part of one) that exists between the service provider and its customer, to create a common understanding about services, priorities, responsibilities, etc..."

In fact, the SLA is considered from a service development point of view, as shown in its Life Cycle (Figure 3).



Source: Tele Management Forum

Figure 3: SLA Life Cycle

1) SLA **Development:** In this phase the SLA templates are developed.

2) **Negotiation** and **Sales**: The SLA is negotiated and the contracts are notified.

3) **Implementation:** The SLA is generated (activated).

4) **Execution:** The SLA is executed, monitored and maintained.

5) **Assessment (of the SLA performance):** A re-evaluation of the initial SLA template might be done.

SLA implementation helps service providers (including third-party service providers) and service users to clarify some of the services responsibilities regarding the expected quality. QoS (Quality of Services) indicators should avoid any ambiguity in understanding the quality of the service.

In addition, in the process of SLA, there is a commitment to quantify the quality of service (QoS indicators), and meanwhile, to perform regular statistics, analysis, reporting and management. These initiatives can guide the customer in exploring the potential settings, to achieve maximum "user benefit".

SLA is relevant to the management plane and to the informational dimension. This contract between the provider and the user is static. When dealing with the more complex context of NGN which encompasses mobility and heterogeneity, the trend will be to get a dynamic contract.

4.2 Mobility

Mobility gives users ability to connect from anywhere, anytime to any service with any type of terminal. In the NGN context, mobility allows users to communicate regardless of location, device, access mode and network across multiple spatial domains. The existing solutions for mobility include horizontal handover (HHO) and vertical handover (VHO). The horizontal handover is provided via mode L3 through the technology "Mobile IP". Media Independent Handover (MIH) is intended to manage seamless connectivity with different wireless networks in MAC and PHY layers.

Four kinds of mobility exist in such a NGN context:

- **User Mobility** refers to the ability for the user to move to different physical locations and be able to use one or more devices connected to one or more access networks to gain access to their services without interruption [i.3].

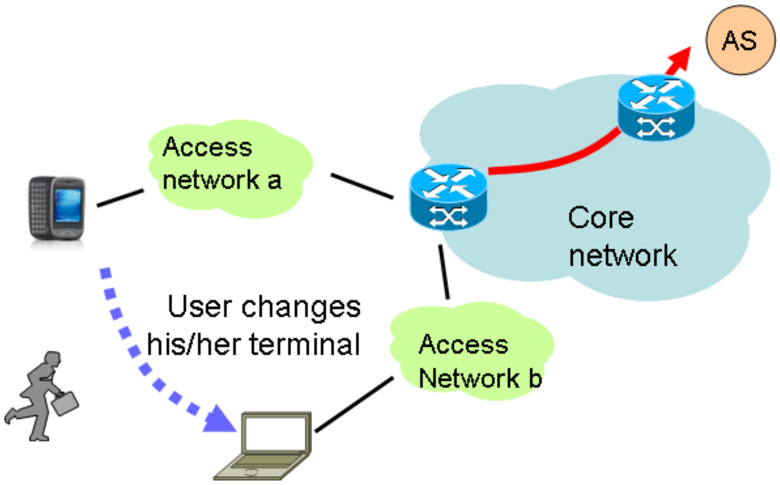


Figure 4: User Mobility

- **Network mobility** refers to the ability of networks, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself (this kind of mobility is out of our scope of research).

EXAMPLE: Ad-hoc network, military network.

- **Service Mobility** refers to the ability of services to be accessible and deliverable independently of network, terminal or geographical location attributes [i.3] It includes the ability of the service level to consistently provide customized services to the user, with the expected QoS, regardless of the user's location. This allows users to maintain access to their services even while moving or changing devices or network service providers.

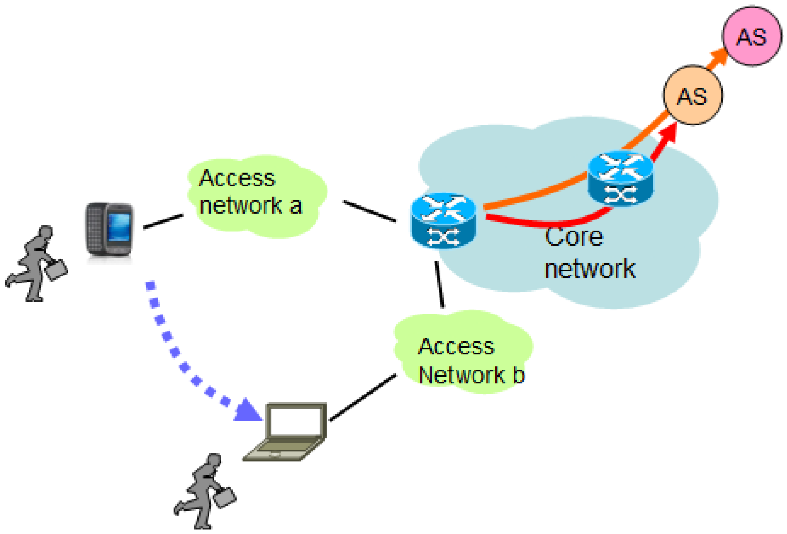
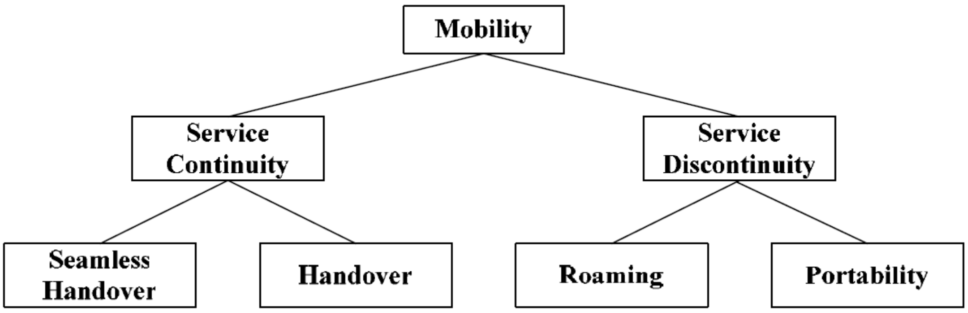


Figure 5: Service mobility

- **Terminal Mobility** refers to the ability of a terminal, while in motion, to access telecommunication services from same or different networks and the capability of the commercial networks to identify and locate that terminal [i.3].



NOTE: Source from ITU-T Recommendation Q.1706/Y.2801 [i.23].

Figure 6a: Mobility classifications according to network service quality

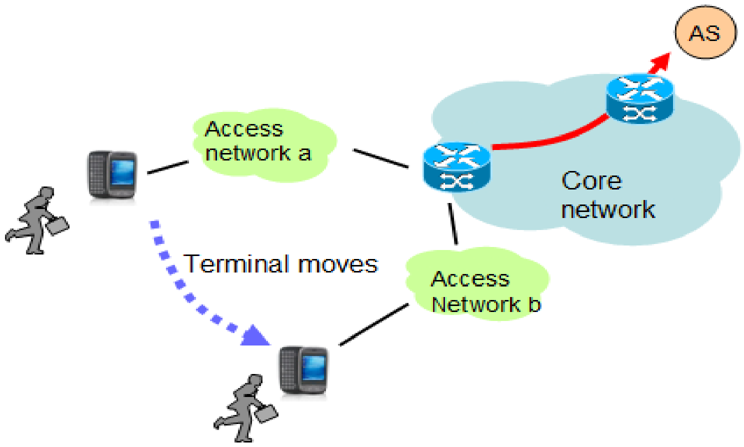


Figure 6b: Terminal Mobility

The key issue to achieve seamless mobility is for Service Providers to *comply with the QoS contract*.

Terminal mobility needs horizontal handover (HHO) in an homogenous network and vertical handover (VHO) in heterogeneous access networks. Generally, HHO is referred to as the Intra-AN handover while VHO is referred to as the Inter-AN handover [i.23]. Figure 7 illustrates both cases (HHO and VHO).

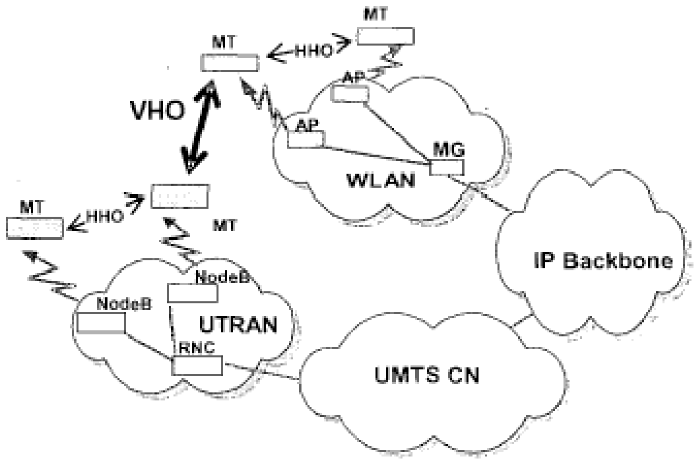


Figure 7: Horizontal handover and Vertical handover

Horizontal Handover (HHO) refers to a terminal whose location changes i.e. that moves across various access points in one network or moves across different network access points, while maintaining access to one set of services. Such mobility should allow the relocation of the terminal without any break. The change in the point of attachment may sometimes temporarily disconnect the mobile terminal and disrupt communications in progress while the objective is to ensure seamless communications.

The procedure for horizontal handover is handled mostly in layer 2. A layer 2 handover occurs when a mobile host's connection changes from one access point to another. The procedure of this type of handover involves releasing the connection from the former access point, establishing a connection to the new access point (though not necessarily in this order), and updating the binding between a mobile host's IP address and its temporary layer 2 identifier (e.g. a MAC address) on the sub-network at the access router. Two types of procedures are proposed [i.26]:

- **Break-before-make handover:** the former connection is released before the new connection is established; data reception is interrupted for a short period of time. The service disruption can be avoided.

- **Make-before-break handover:** if the mobile host is capable of establishing connections to multiple access points simultaneously, it can connect to the new access point before breaking its connection from the former access point.

Broadly speaking, the handover will be conducted by analyzing the signal received from the two related cells, frame by frame, involved and the best frame will be accepted. Several handover definitions have been proposed. For instance, in UMTS (Universal Mobile Telecommunications System) [i.1], three different handovers have been defined: hard handover, soft handover and softer handover.

a) Hard handover

It means that all the old radio links in the UE are removed before the new radio links are established. Hard handover can be seamless or non-seamless. Seamless hard handover means that the handover is not perceptible to the user. In practice a handover that requires a change of carrier frequency (inter-frequency handover) is always performed as hard handover.

b) Soft Handover

It means that the radio links are added and removed in a way that the UE always keeps at least one radio link to the UTRAN. Soft handover is performed by means of macro diversity, which refers to the condition that several radio links are active at the same time. Normally soft handover can be used when the mobile is going to another cell on the same frequency.

c) Softer Handover

Softer handover is a special case of soft handover where the radio links that are added and removed belong to the same Node B. In softer handover, macro diversity with maximum ratio combining can be performed in the Node B, whereas generally in soft handover on the downlink, macro diversity with selected combination is applied.

Vertical Handover (VHO) is the solution for mobility in a heterogeneous network. It refers to a terminal which location changes i.e. that moves among access points of a technology to another access point in a different technology while maintaining access to the set of services. Such mobility should be seamless.

Cellular and WLAN technologies are shortly discussed as basic technologies for vertical handover, especially, VHO between cellular technologies such as GPRS and WLAN such as IEEE 802.11b [i.21]/IEEE 802.11g [i.38]. Furthermore, the analysis can be extended to any combination of heterogeneous networks, including multiple overlapping (more than 2) radio technologies. 3GPP provides solution for VHO between Wimax and GPRS.

Often VHO between heterogeneous networks such as WLAN/GPRS is managed at IP level and Mobile IP is used see [i.25] and [i.27].

The interconnection between WLAN and GPRS in 3GPP architecture is represented below:

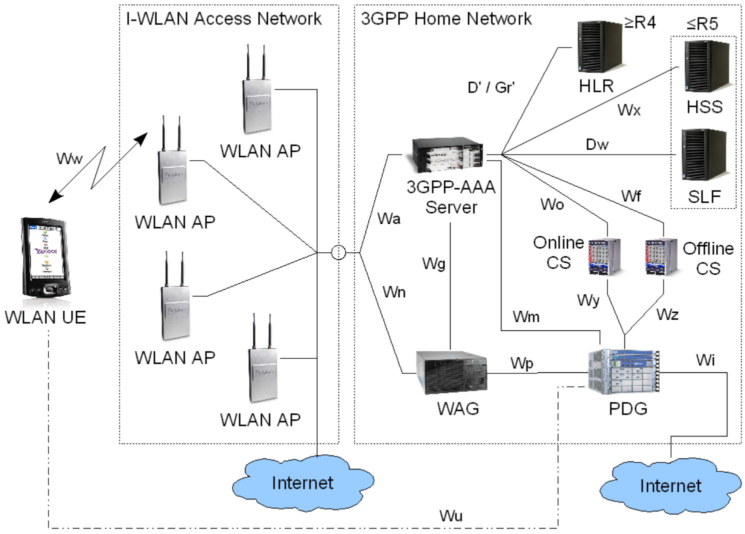


Figure 8: Interconnection between WLAN and GPRS in 3GPP architecture

Authentication, Authorisation and Accounting is managed by the HLR/HSS and Charging by the CS Online and Offline.

The WAG - Wireless Access Gateway provides interconnection between access and 3GPP network. The WAG manages IP tunnels, QoS mechanisms and it is responsible of roaming.

The PDG - Packet Data Gateway is the access point thru 3GPP network. It manages the tunnel for exchanges to the WAG. The PDG is responsible of packet routing between Internet and the User. It can implement certain functions such as NAT and QoS mechanisms.

The WLAN 3GPP IP proposes connection to Internet through the PLMN, and provides PLMN's services through WLAN access such as SMS, MMS, IMS Services, etc.

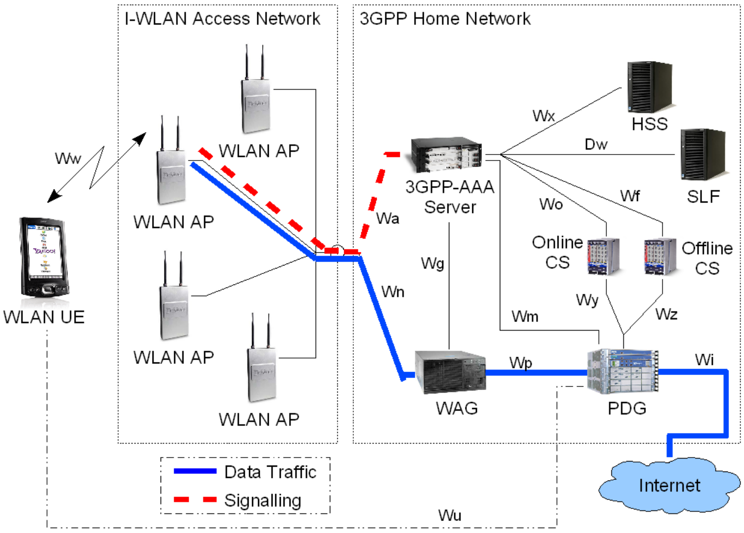
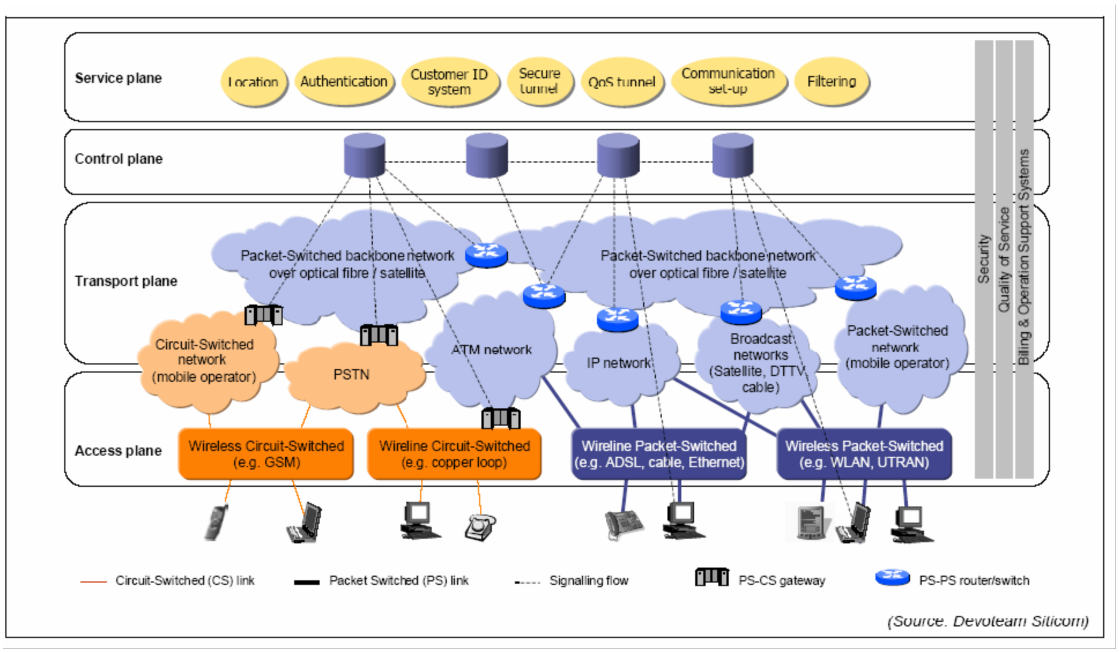


Figure 9: Data traffic and signalling between WLAN and GPRS in 3GPP architecture

4.3 Heterogeneous environment

With the continuous evolution of services and technologies, the world of telecommunication becomes more and more heterogeneous. Modern telecommunication networks consist of mobile network (such as GSM/GPRS/UMTS), fixed network (such as Public Switched Telephone Network/ISDN), satellite network and wireless access networks (such as wireless LAN (WiFi, WiMax) and Bluetooth networks), etc. The user devices are also becoming more diversified: PDAs, laptops, cell phones, etc. which are now commonly used by the general public.

The growing number of a variety of services and multimedia applications in converging fixed and mobile IP networks (called Next Generation Networks (NGN)) led to the definition of a Service Delivery Platform architecture known as an IMS (IP Multimedia Subsystem) (with associated protocols: SIP, Diameter and Policy control protocols). IMS was originally specified by 3GPP as part of the vision for evolving mobile networks beyond GSM and was extended later for supporting other networks such as fixed line, WLAN, etc. by a number of standardization organizations, such as the ITU-T and ETSI TISPAN; meanwhile the number of service providers and operators is growing in the NGN (Figure 10) heterogeneous environment.


Service plane
Location
Authentication
Customer ID system
Secure tunnel
QoS tunnel
Communication set-up
Filtering
Control plane
Transport plane
Packet-Switched backbone network over optical fibre / satellite
Packet-Switched backbone network over optical fibre / satellite
Circuit-Switched network (mobile operator)
PSTN
ATM network
IP network
Broadcast networks (Satellite, DTTV, cable)
Packet-Switched network (mobile operator)
Access plane
Wireless Circuit-Switched (e.g. GSM)
Wireline Circuit-Switched (e.g. copper loop)
Wireline Packet-Switched (e.g. ADSL, cable, Ethernet)
Wireless Packet-Switched (e.g. WLAN, UTRAN)
Security
Quality of Service
Billing & Operation Support Systems
Circuit-Switched (CS) link
Packet Switched (PS) link
Signalling flow
PS-CS gateway
PS-PS router/switch

(Source: Devoteam Siticom)

Figure 10: NGN heterogeneous environment

These heterogeneities have increased the complexity of the overall infrastructure. Problems of interoperability between the various systems and handover/roaming between different accesses and providers should be solved according to the QoS commitments.

The QoS problem in an heterogeneous environment is how to interoperate the QoS state. The policy could be used to adapt QoS according to particular goals in heterogeneous networks. Such policy could be used for:

- optimal access network selection in case of handover, routing and connection redirection;
- resource and service adaptation in heterogeneous network environment;
- management of the interactions between heterogeneous networks for QoS provisioning.

IP Multimedia Subsystem (IMS) has emerged as an overlay service provisioning platform that operates in an heterogeneous network environment. The IMS is defined by the 3rd Generation Partnership Projects (3GPP and 3GPP2) and is an overlay service architecture that enables the efficient provision of an open set of highly integrated multimedia services, combining web browsing, e-mail, instant messaging, VoIP, video conferencing, telephony, multimedia content delivery, etc.

4.3.1 IMS Architecture (3GPP)

The IP Multimedia Core Network (IM CN) subsystem enables PLMN operators to offer their subscribers multimedia services based on and built upon Internet applications, services and protocols. The IMS should enable the convergence of voice, video, messaging, data and web-based technologies for the wireless user, and combine the growth of the Internet with the growth in telecommunications. The complete solution for the support of IP multimedia applications consists of terminals, IP-Connectivity Access Networks (IP-CAN), and the specific functional elements of the IMS [i.12]. The IMS reference architecture including interfaces towards legacy networks and other IP based multimedia systems is represented in Figure 11. Details of the roles of these entities are described in the 3GPP IMS architecture is split into three layers: Service Layer, Control Layer and Connectivity Layer.

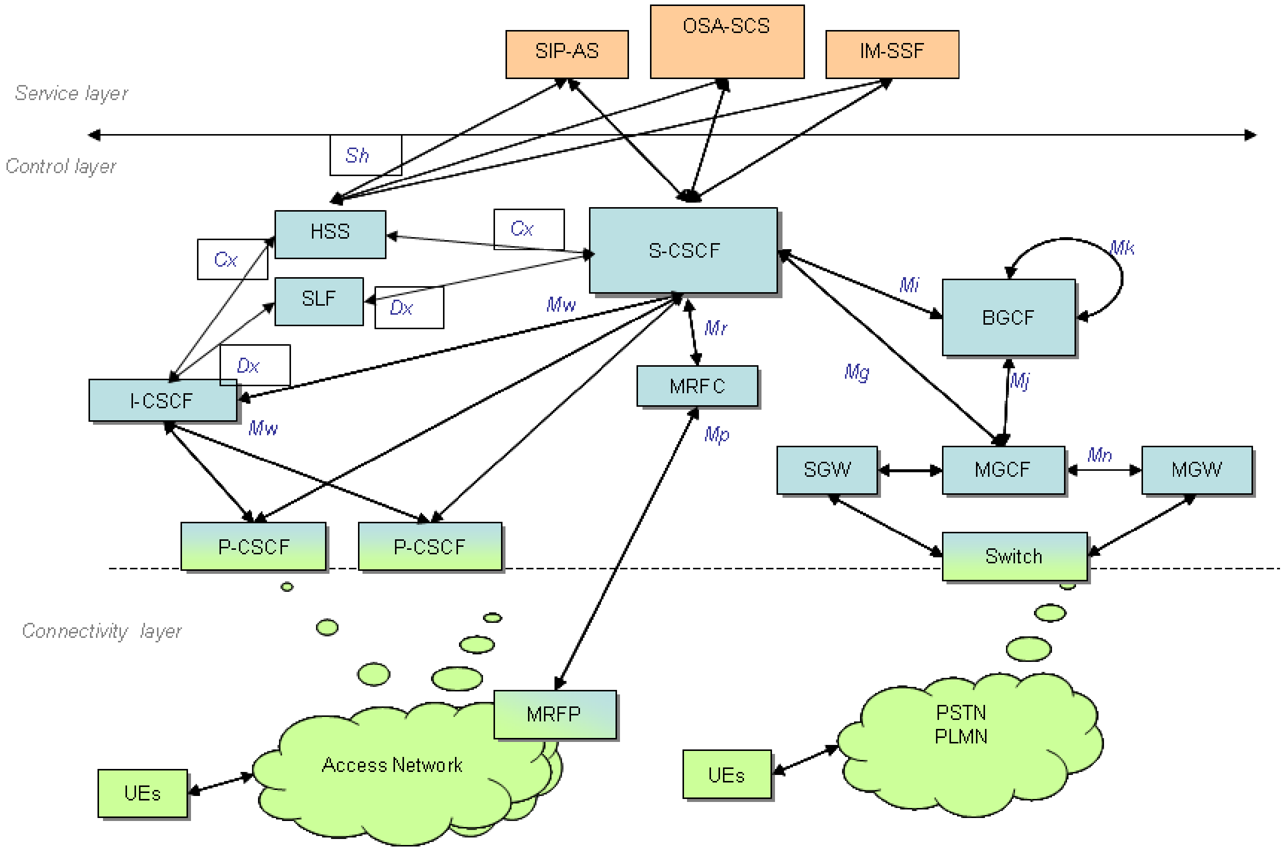


Figure 11: IMS architecture

The service layer consists of application and content servers to execute value-added services for the user. Three types of Application Server Functions (ASF) can be accessed by the IMS through the ISC or Ma reference point (Figure 11).

- SIP Application Servers (SIP AS); A SIP Application Server may contain "Service Capability Interaction Manager" (SCIM) functionality and other application servers. The SCIM functionality is an application which performs the role of interaction management.
- IM-SSF Application Server, it enables access to IN (intelligence network) service logic programs hosted in legacy SCPs (Service control point).
- OSA SCS Application Server (OSA Service Capability Server). It provides access to OSA applications, according to the OSA/Parlay framework

The control layer consists of network control servers for managing call or session set-up, modification and release. The most important of these is the Call Session Control Function (CSCF), also known as a SIP server. This layer also contains a full suite of support functions, such as provisioning, charging and operation and management. Inter-working with other operators' networks and or other types of networks is handled by border gateways.

At the core of this plane is the **Call Session Control Function** (CSCF), which consists of the following functions:

- The Proxy-CSCF (P-CSCF) is the first contact point within the IMS core. The P-CSCF behaves like a Proxy, i.e. it accepts requests and services them internally or forwards them on. The P-CSCF may behave as a User Agent, i.e. it may terminate and independently generate SIP transactions in abnormal conditions.
- Interrogating-CSCF (I-CSCF) is the contact point within an operator's network for all connections destined to a user of that network operator, or a roaming user currently located within that network operator's service area.
- The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services.

The signalling flow path for establishing a call session (Figure 12) based on UMTS network is shown below. The call signalling flows from the caller UE through the P-CSCF in the home network to his S-CSCF. The signalling then passes onto the UE called party via his S-CSCF.

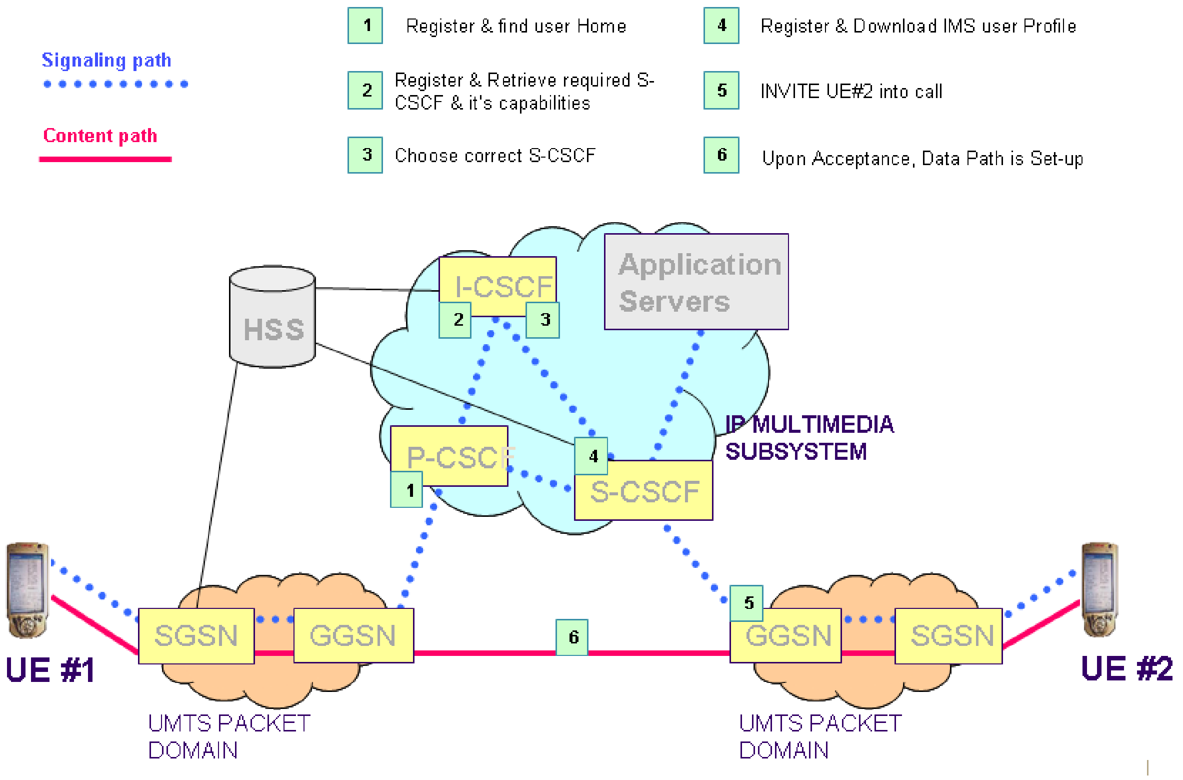


Figure 12: Signalling flow path for establishing a call session

Home Subscriber Server: The HSS contains a subscription database for the IMS, including subscription-related information to support the network entities that actually handle calls or sessions. The HSS is responsible for policing what information will be provided to each individual Application Server. The HSS also stores the currently assigned S-CSCF.

Subscription Locator Function: The SLF is needed to map user addresses when multiple HSSs are used. It may be queried by an I-CSCF during registration and session setup to get the name of the HSS containing the required subscriber-specific data.

Breakout Gateway Control Function: it determines the next hop for routing the SIP message. This determination may be based on information received in the protocol, administrative information, and/or database access. For PSTN terminations, the BGCF determines the network in which PSTN/CS Domain breakout is to occur. If the routing determination is such that the breakout is to occur in the same network in which the BGCF is located, then the BGCF shall select a MGCF that will be responsible for the interworking with the PSTN/CS Domain. If the routing determination results in break out in another network, the BGCF will forward this session signalling to another BGCF in the selected network. If the routing determination results in the session being destined for another IMS network, the BGCF forwards the message to an I-CSCF in this IMS network. If the BGCF determines that there is another IP destination for the next hop, it forwards the message to that contact point.

Media Resource Function Controller: The MRFC controls the media stream resources of the MRFP. It interprets information from an AS and S-CSCF, and controls the MRFP accordingly to support media services such as trans-coding and conferencing. The MRFC may generate the Charging Data Records (CDR).

Media Resource Function Processor: The MRFP controls the bearer on the Mb reference point, and provides resources to be controlled by the MRFC for media processing. It supports media stream mixing, announcement generation, trans-coding, media analysis, and management of access rights to shared resources in a conferencing environment.

Media Gateway Controller Function: The MGCF provides the ability to control a Trunk Media Gateway Function (T-MGF) through a standardized interface. Such control includes allocation and de-allocation of resources of the media gateway, as well as modification of the usage of these resources. The MGCF communicates with the CSCF, the BGCF and circuit-switched networks. The MGCF performs protocol conversion between ISUP and SIP.

The connectivity layer comprises routers and switches, both for the core network and the access network.

IMS reference points [i.12]:

Cx reference point: Supports information transfer between CSCF and HSS.

Dx reference point: The CSCF and SLF interface is used to retrieve the address of the HSS which holds the subscription date for a given user. Not required in a single HSS environment.

Gm reference point: Supports communication between the MT and the IMS.

Mn reference point: Communication interface between the MGCF and IMS-MGW. Equivalent to the Mc interface in the CS domain.

Mg reference point: Allows the MGCF to forward incoming session signalling (from the PSTN) to the CSCF for the purpose of inter-working with PSTN networks. The protocol used in this interface is SIP.

Mr reference point: allows the S-CSCF to relay signalling messages between an application server function and an MRFC. The protocol used in this interface is SIP.

Mp reference point: Allows an MRFC to control media stream resources provided by an MRF. Similar to the Mc interface in the CS domain.

Mw reference point: Allows the communication and forwarding of SIP signalling messaging between CSCFs. The protocol used in this interface is SIP.

Mi reference point: Allows the Serving CSCF to forward the session signalling to the BGCF for the purpose of inter-working with PSTN networks. The protocol used in this interface is SIP.

Mj reference point: Allows the BGCF to forward session signalling to the MGCF for the purpose of inter-working with PSTN networks. The protocol used in this interface is SIP.

Mk reference point: Allows the BGCF to forward session signalling to another BGCF. The protocol used in this interface is SIP.

Mb reference point: Used to access IPv6 network services for user data transport.

ISC reference point: The interface between the CSCF and application servers for access to IMS services.

Sh reference point: is used for communication from the SIP or OSA application server to the HSS.

Si reference point: is used for communication from the CAMEL application server to the HSS.

Go reference point: Allows the Policy Decision Function (PDF) to apply policy decisions to bearer usage in the GGSN. The Policy Decision Function (PDF) is a logical entity in the P-CSCF.

4.3.2 TISPAN NGN architecture

TISPAN uses IMS specified by 3GPP to enable fixed network operators to provide end to end IP based multimedia services. The TISPAN NGN functional architecture (Figure 13) can be divided into two layers [i.4]:

1) Service layer, consisting of Application Servers (AS).

2) Transport layer, consisting of the user equipment (UE), Access Network, Next Generation Network (NGN) core. TISPAN adds the transport control sub-layer for registration/initialization of user equipment (NASS: Network Attachment Subsystem) [i.6] and resource reservation from access network (RACS: Resource and Admission Control Subsystem) [i.5].

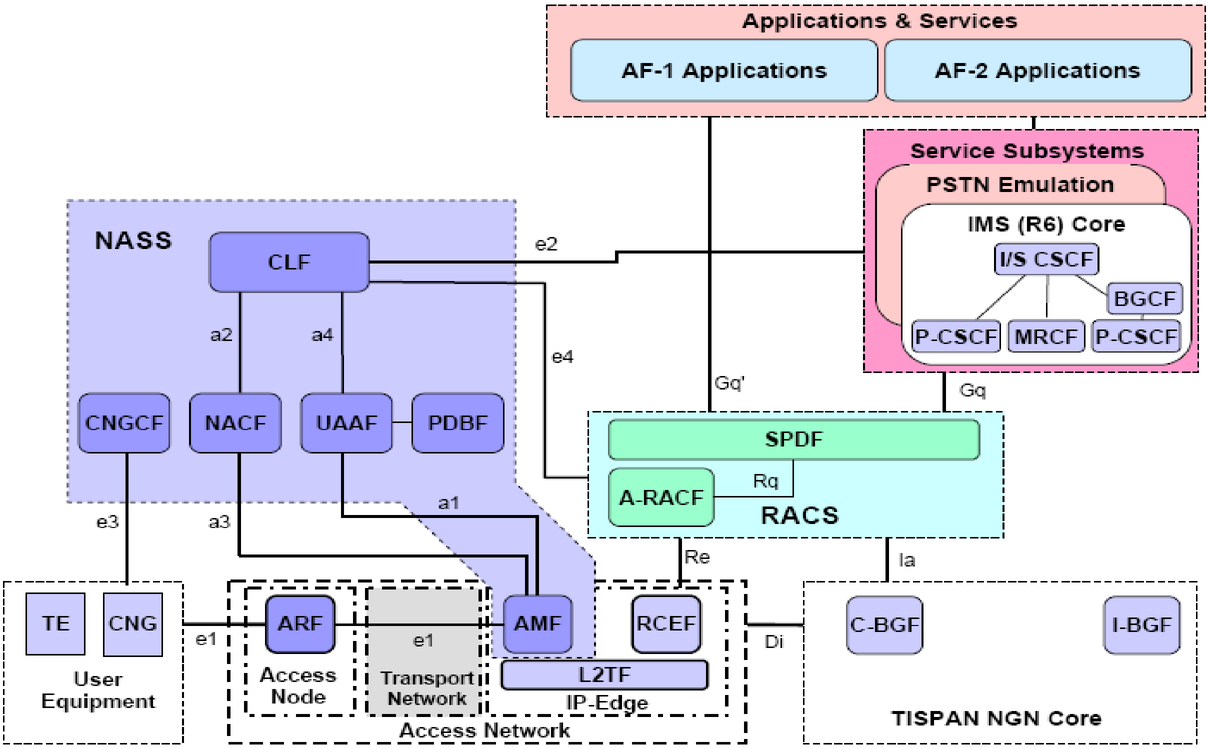


Figure 13: TISPAN NGN Architecture

The service layer is composed of the following components:

- The IP Multimedia subsystem core components. IMS Functional Architecture is specified in [i.7].
- The PSTN/ISDN Emulation Subsystem (PES) [i.16].
- Other multimedia subsystems (e.g. IPTV [i.18], etc.) and applications. It should be noted that the ETSI TC TISPAN also specified another option for the IPTV architecture than that defined in [i.17]. It is based on the support of the IPTV functions by the IMS subsystem described in the same document.

- Common components used by several subsystems such as those required for accessing applications, charging functions, user profile management, security management, routing databases, etc.

In the transport layer:

The NASS provides the following functionalities [i.6]:

- Dynamic provision of IP addresses and other terminal configuration parameters.
- Authentication taking place at the IP layer, prior or during the address allocation procedure.
- Authorization of network access based on user profiles.
- Access network configuration based on user profiles.
- Location management taking place at the IP layer.

RACS [i.5] is the TISPAN NGN subsystem responsible for the implementation of procedures and mechanisms handling policy-based resource reservation and admission control for both unicast and multicast traffic in access networks and core networks.

Besides acting as a resource control framework, RACS also includes support for controlling Network Address Translation (NAT) at the edge of networks and assisting in remote NAT traversal. Furthermore, RACS also covers aspects related to the setting and modification of traffic policies, end-to-end quality of service and transport-level charging.

In core network, there are two main types of Border Gateway Function (BGF):

- The Core BGF (C-BGF) that sits at the boundary between an access network and a core network, at the core network side.
- The Interconnection BGF (I-BGF) that sits at the boundary between two core networks.

On the user side, the User Equipment (UE) consists of one or more user controlled devices allowing a user to access services delivered by NGN networks. Different components of the customer equipment may be involved depending on the subsystem they interact with. As for the Custom Network Gateway (CNG), it will be introduced in detail in clause 6.3.1.

4.4 Conclusion

As networks become more and more complex and as new services emerge continuously, the requirement for an end to end QoS management offering a transparent experience to the end user is growing.

These new services (e.g. data services, multimedia services) can be used by different users in different manners. Users are no longer satisfied with a simple phone call service but are interested to have as many services available as possible included in a customized service composition. These requirements imply not only the possibility to always have these services accessible in a unique session when the user is moving in an heterogeneous environment but also to have the QoS guaranteed for different types of applications simultaneously.

To maintain E2E QoS continuity for users, as expected, the means to provide cooperation between the different environments are needed.

5 Requirement for QoS continuity

As networks are evolving towards Next Generation Network (NGN), the network environment is becoming more and more complex. Heterogeneity and mobility are two specific characteristics in NGN that take into account end-user terminals, access networks, core networks and services. Mobility allows end-users to communicate regardless of location, device used, access mode or network across multiple spatial domains.

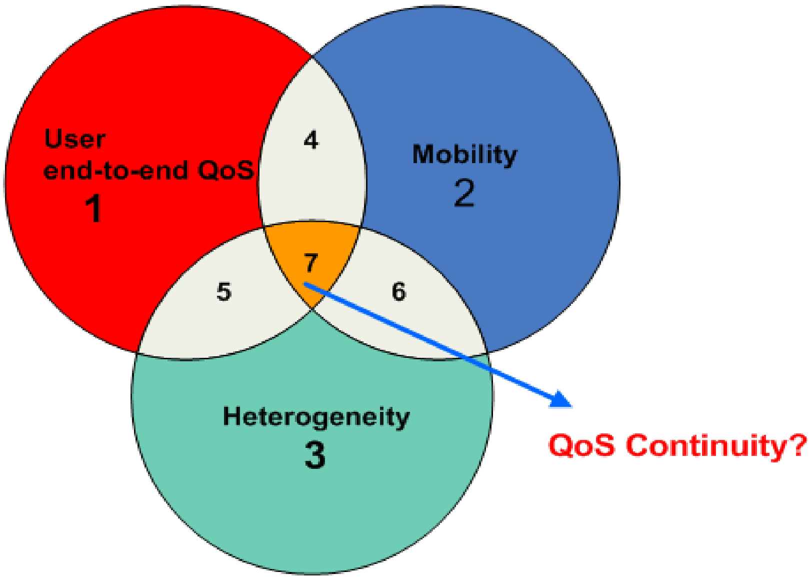


Figure 14: From existences to concerned problem

The following numbers are referring to the ones in the domains in Figure 14:

1) User requirements and preferences: In terms of continuity of multimedia services and all personal information (usage, SLA, security, etc.).

2) Mobility, which refers to terminal mobility, user mobility, service mobility and network mobility.

3) Heterogeneity, which represents the heterogeneity of networks and terminals, as well as the heterogeneity of services which contribute to the heterogeneity of QoS mechanisms.

QoS issues are then analyzed between each two sub fields:

4) A proper E2E QoS signalling which insures user continuous services within a mobile environment.

5) The user connectivity to heterogeneous networks which is expected to always comply with the SLA where the user preferences are defined.

6) An inter-working QoS to enable terminal mobility across heterogeneous networks.

7) **QoS continuity** taking into consideration the mobility across heterogeneous environments. The advanced management information covers the mobility management information (User mobility, terminal mobility, service mobility, network mobility and session mobility), QoS information and AAA information (Authentication, Authorization and Accounting).

6 Analysis of related work for QoS

The work related to QoS was analyzed through the three planes. In the heterogeneous environment, technologies differ in the bandwidth, latency, cost and QoS classification used. Mobility occurs between these environment to maintain minimum QoS contracts for different applications. Supporting this seamless mobility, or interconnection and interoperation across the heterogeneous environment (QoS signalling and QoS interworking) is seen as one of the key issues in heterogeneous environment.

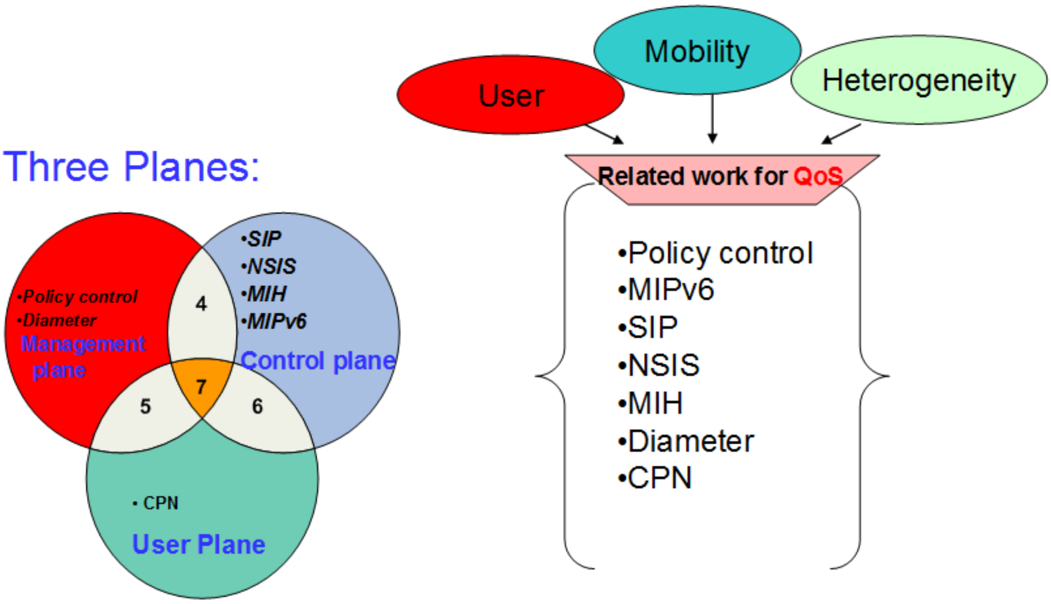


Figure 15: Related work for QoS

6.1 Control plane

Some work related to this issue has already been done in control plane. Media Independent Handover manages the seamless connectivity with different wireless networks (clause 6.1.1), while Mobile IPv6, which is a protocol working on network layer, supports not only horizontal but also vertical handover (clause 6.1.2). IETF has proposed Next Steps in Signalling (NSIS) as the signalling protocol for network which have its own way to transfer the QoS parameters (clause 6.1.3) and Session Initiation Protocol (SIP) as the session-base signalling protocol working on application layer to support session mobility (clause 6.1.4).

These protocols work on respective layer of Open System Interconnection OSI (OSI) are shown in Figure 16.

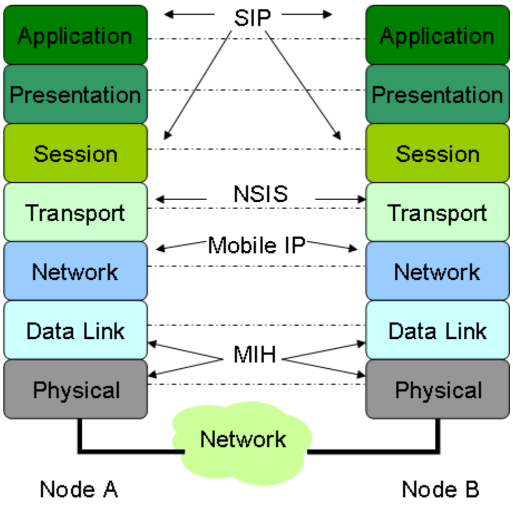


Figure 16: Related work in mobility control in OSI architecture

6.1.1 MIH

IEEE 802.21 [i.22] introduces the concept of MIH (to carry out the handover between heterogeneous technologies). This standard is under development. Its main purpose is to manage seamless connectivity across different wireless networks. This standard is managing the handover between cellular networks, WiFi and Bluetooth, etc.

In the context of heterogeneous networks, the vertical handover has to be considered because it allows adaptation between different network technologies in a flexible manner. Mobility management is primarily concerned with handover initiation and network selection. Admission control is an inherent part of the handover execution stage and governs access to the chosen network. The MIH is in the scope of the first two steps: handover initiation and handover preparation, as shown in Figure 17. The IEEE 802.21 [i.22] standard defines the framework that is needed to exchange information between handover participants to provide mobility. It also defines functional components taking handover decision.

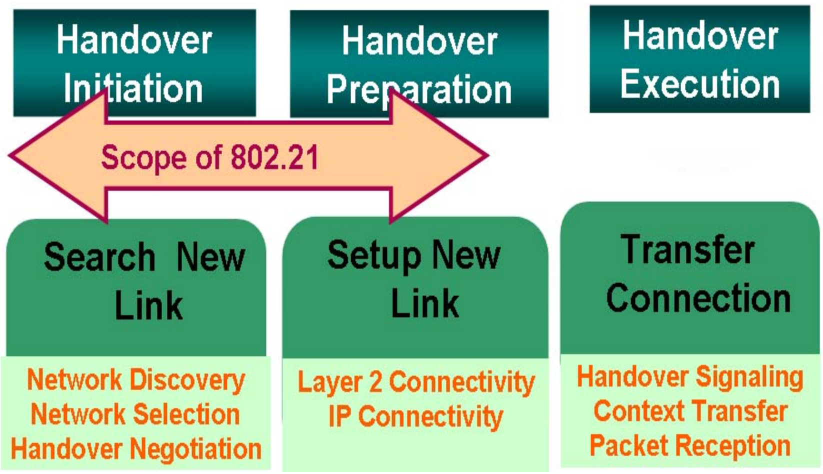


Figure 17: 802.21 scope

The IEEE 802.21 [i.22] framework offers the method and procedure for handover between heterogeneous networks. This handover procedure uses the information from both mobile terminal and network infrastructures. The IEEE 802.21 [i.22] framework informs the available networks close to the mobile terminal and helps the mobile terminal to detect and select the appropriate network. This information includes link layer information.

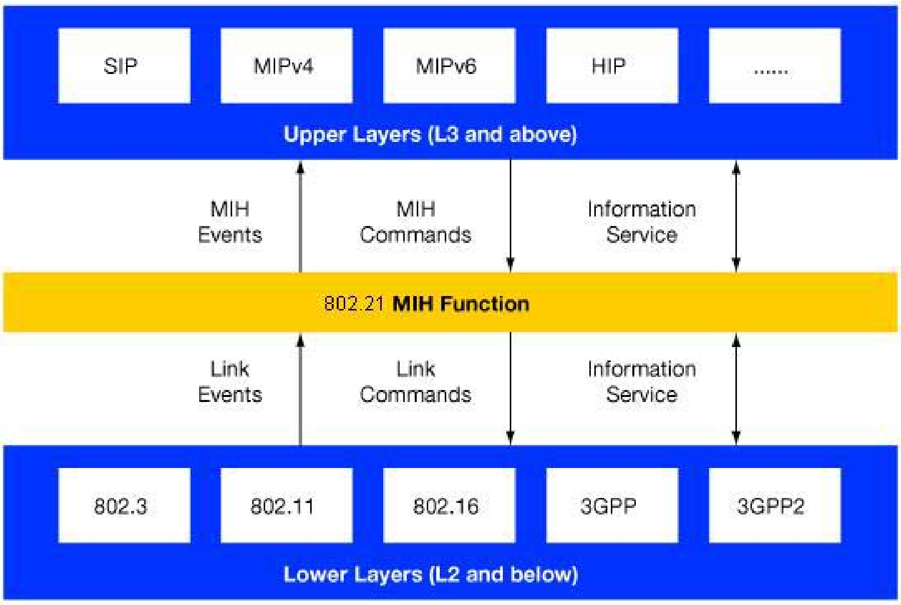


Figure 18: 802.21 Functional Components

The core of 802.21 lies in Media Independent Handover Function (MIHF) which plays the role of intermediate operation between layer 2 and layer 3. It presents homogeneous interfaces independent from access technologies. This interface is in charge of the communication between the upper layer and the lower layer with the functional components (Figure 18). MIH Function provides three services: Media Independent Event Service (MIES), Media Independent Command Service (MICS), and Media Independent Information Service (MIIS).

MIES

MIES provides the local or remote event to the upper layer. The MIES supports the transfer, filtering and classification of dynamic changes on the link layer. It may transfer the link level event to the proper application or process and then passes on to the higher layers. The events are generated locally or by a remote peer MIHF entity. The framework for both local and remote event exchanges is shown in Figure 19.

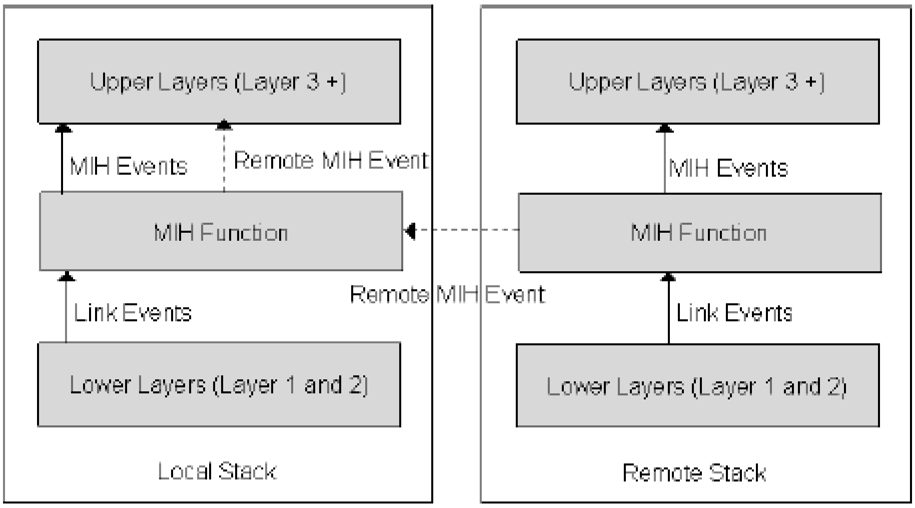


Figure 19: Media Independent Event Service

Link Events are classified into four categories:

- *State change event*: for example, MAC and Physic state change event (Link_up or Link_down) and Link parameter events which are generated due to change in link parameters (Link Parameter Change).
- *Predictive events*: which provide the likelihood of change in the link properties in future based on present and past conditions (Link Going Down).
- *Link Synchronous events:* which provide information about actual link layer activities, like handover decision at the link layer.
- *Link transmission events*: which indicate the status of the transmission of higher layer PDUs by the link layer.

Example link events which are proposed in 802.21 are shown in table 1.

Table 1: Proposed link events in 802.21

No	Event Type	Event Name	Description
1	State Change	Link Up	L2 Connection established
2	State Change	Link Down	L2 Connection is broken
3	Predictive	Link Going Down	L2 connection breakdown imminent
4	State Change	Link Detected	New L2 link has been found
5	State Change	Link Parameters Change	Change in specific link parameters has crossed pre-specified thresholds (link Speed, Quality metrics
6	Administrative	Link Event Rollback	Event rollback
7	Link Transmission	Link SDU Transmit Status	Improve handover performance through local feedback as opposed to waiting for end-to-end notifications
8	Link Synchronous	Link Handover Imminent	L2 intra-technology handover imminent (subnet change). Notify Handover information without change in link state
9	Link Synchronous	Link Handover Complete	Notify handover state

MICS

The MICS offers the functions to control and manage the link layer. If the MIH application wants handover and mobility, it can control the MAC layer by using MICS to configure, control and get information. Commands flow from higher to lower layers. The MICS function framework is shown in Figure 21. MIH users use MIH commands to determine the status of a link. This service enables users to implement an optimal handover policy.

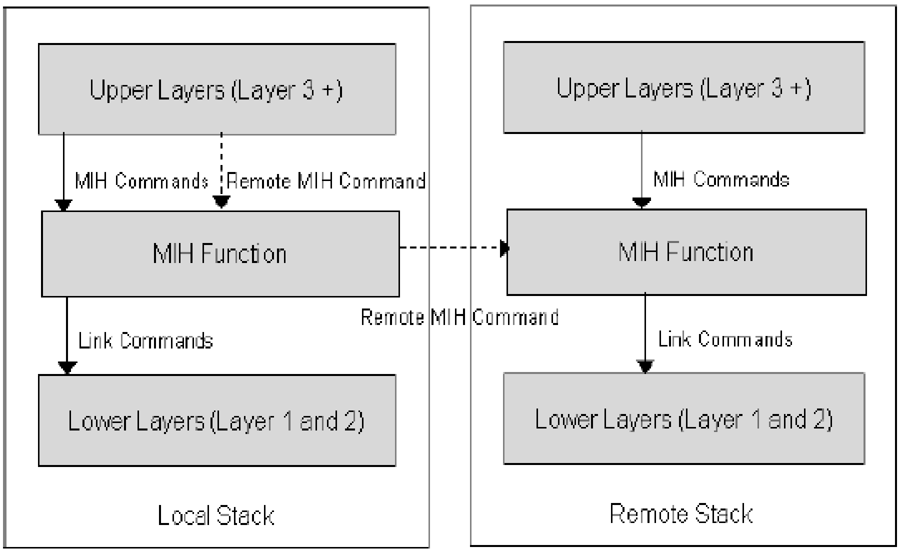


Figure 20: Media Independent Command Service

MIIS

The MIIS offers information that is needed to perform the handover. Information is maintained in Information Server in the network (Figure 21). This information includes the name of network and operator, supported QoS, address of point of attachments, available applications and nearby available access networks etc. Information Service can help with Network Discovery and Selection for specific QoS leading to more effective Handover decisions. The information elements defined in MIIS is shown in Table 2.

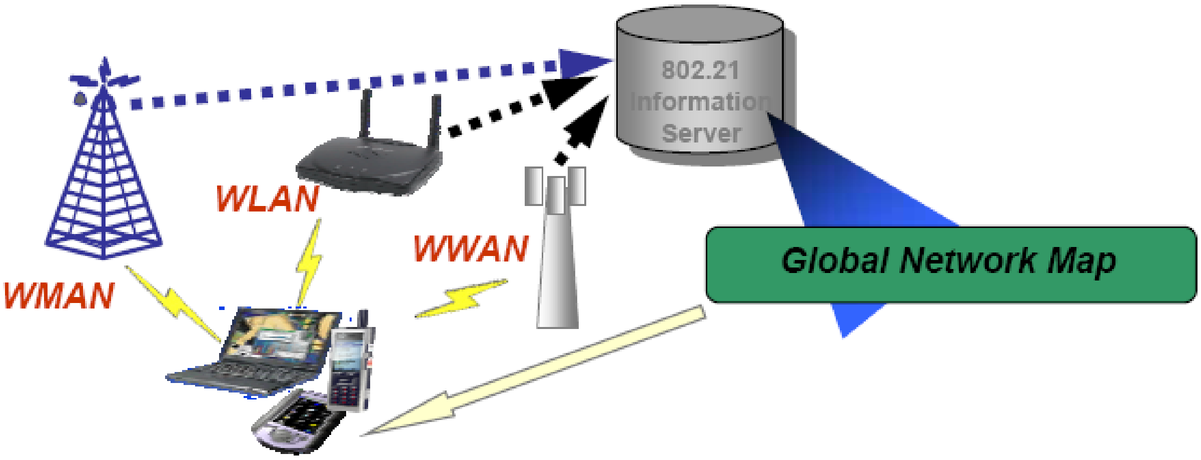


Figure 21: Media Independent Information Service

Table 2: Information elements

Information Element	Description	Comments
List of networks available	List of all network types that are available given client location	E.g. 802.11, 802.16, GSM, GPRS/EDGE, UMTS networks
Location of PoA	Geographical Location, Civic address, PoA Id	E.g. GML format for LBS or network management purpose
Operator ID	Name of the network provider	E.g Could be equivalent to Network ID
Roaming Partners	List of direct roaming agreements	E.g. in form of NAIs or MCC+MNC
Cost	Indication of costs for service/network usage	E.g, Free/Not free or (flat rate, hourly, day or weekly rate)
Security	Link layer security supported	Cipher Suites and Authentication Methods, Technology specific, e.g. WEP in 802.11, 802.11i, PKM in 802.16, etc.
Quality of Service	Link QoS parameters	802 wide representation, application friendly
PoA Capabilities	Emergency Services, IMS Services, etc.	Higher Layer Services
Vendor Specific IEs	Vendor/Operator specific information	Custom Information

The information is represented in a common form across different networks using TLV (Type, Length, and Value). An example of a MIIS message is shown in Figure 22.

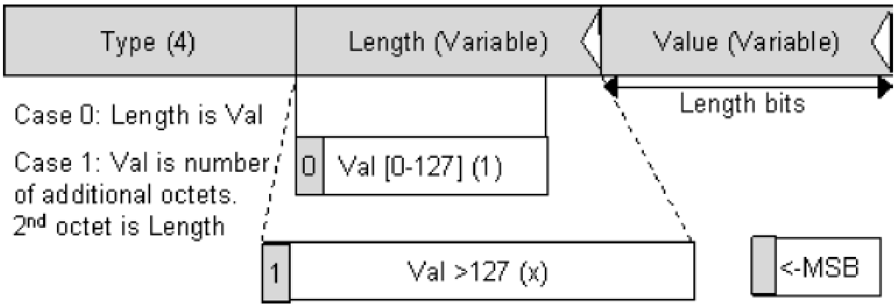


Figure 22: MIIS Message

Conclusion

IEEE 802.21 [i.22] helps with Handover Initiation, Network Selection and Interface Activation during Vertical Handovers for next generation wireless All-IP networks. The 802.21 enables Co-operative Handover decision making between Clients and Network. However, how to solve the vertical handover in the wireless and fix network is not covered in the scope of MIH.

6.1.2 MIPv6

Mobile IPv6 allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications. One can think of the Mobile IPv6 protocol as solving the network-layer mobility management problem. The Mobile IPv6 topology is shown in Figure 23.

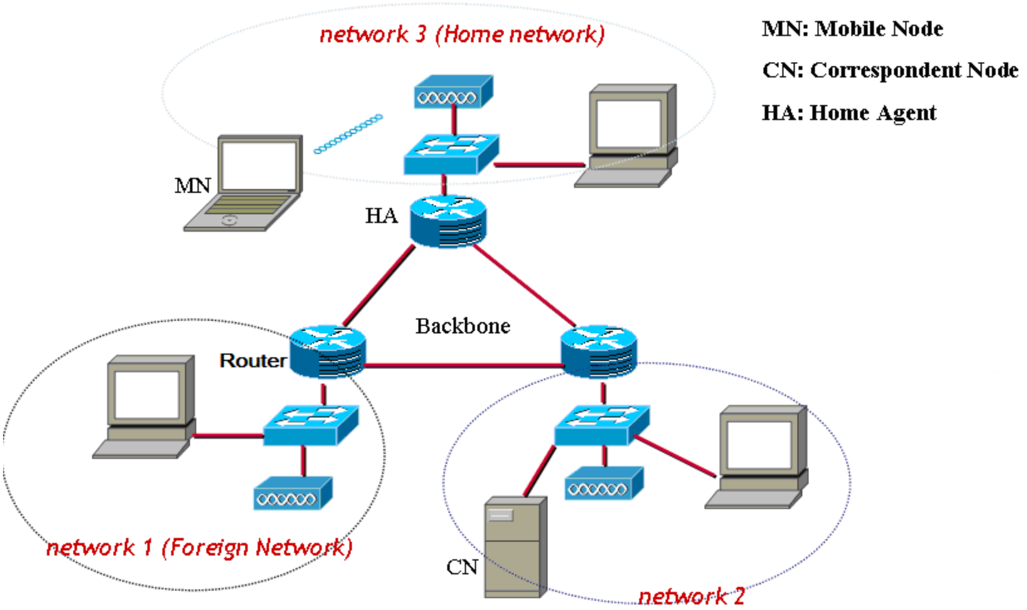


Figure 23: Mobile IPv6 Topology

- Home Agent (HA): A router on the home network which represents the MN while it is not attached with the home network.
- Home Address (HoA): A (static) IP address out of the mobile nodes home network.
- Mobile Node (MN): Could change its point of attachment while still being reachable via HoA.
- Care of Address (CoA): The physical IP address of a MN while visiting a foreign network.
- Correspondent Node (CN): A peer node with which a MN is communicating, the CN may be either mobile or stationary.
- Binding: Association of the home address with the Care-of address of a MN.

Mobile IPv6 identifies each node by its unchanging global home address, regardless of its current point of attachment to the Internet.

The process of handover when the MN moves between different access networks based on Mobile IPv6 is shown in Figure 24.

Once MN moves to visited network, it gets a Care of Address for this network, and then MN sends a Binding Update message (BU) to an HA on previous network to notify its mobility events and CoA.

When the HA gets the BU message, it returns a Binding Acknowledgement (BA).

The HA intercepts packets addressed to the mobile node's home address and tunnels them to the mobile node's current location.

MN sends a Binding Update to CN.

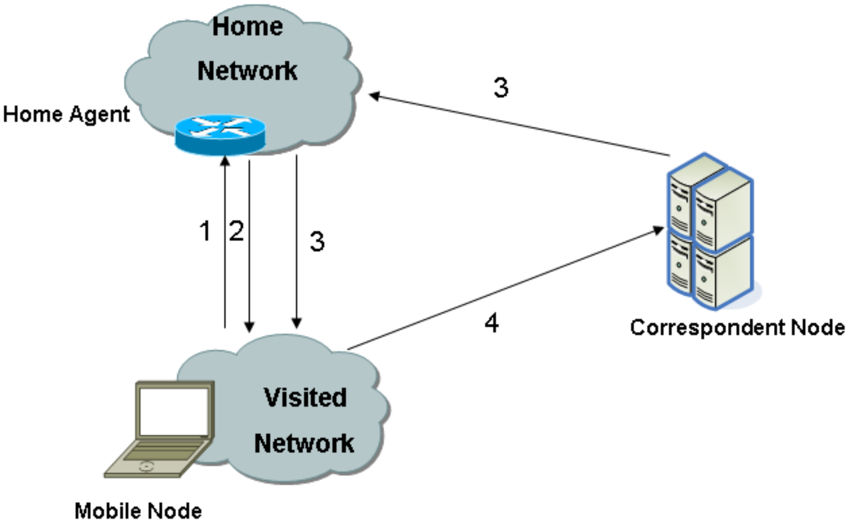


Figure 24: Mobile IPv6 handover process

The IPv6 header has two QoS-related fields. They are:

- 20-bit Flow Label.

Used by a source to label sequences of packets for which it requests special handling by the IPv6 routers Geared to IntServ and RSVP.

- 8-bit Traffic Class Indicator.

Used by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets Geared to DiffServ.

Moreover, Mobile IPv6 has a new IPv6 option: QoS Object. QoS Object describes QoS requirement, traffic volume and packet classification parameters for MN's packet stream Included as a Destination Option in IPv6 packets carrying Binding Update and Biding Acknowledgment messages.

Conclusion

Mobile IPv6 allows easier configuration, better security and optimization; it minimizes the control traffic needed to effect mobility. But Mobile IP is not a complete mobility solution; it needs to cooperate with other mobility management protocol.

6.1.3 NSIS

To fulfill the needs of signalling over IP-based networks, the Internet Engineering Task Force (IETF) developed the Resource Reservation Protocol (RSVP) which is designed and applied to resource reservation for both Integrated Services (IntServ) and later Differentiated Services (Diff-Serv), rather than more general signalling services. In 2001, the IETF formed a new working group (Next Steps in Signalling (NSIS)), to search for a flexible IP signalling architecture and protocols.

As a result, an extensible IP signalling architecture [i.29] was developed also referred to as NSIS (Figure 25). It consists of two layers: the lower layer provides a generic transport service for different signalling applications (QoS NSLP, NAT/Firewall NSLP, Metering NSLP), which reside in the upper layer. This kind of two-layer model is used to separate the transport signalling from the application signalling. This allows more flexibility, such as the ability to use standard transport layer and security protocols.

In the transport layer of NSIS (NSIS Transport Layer Protocol (NTLP)), the main composition is known as GIST (General Internet Signalling Transport Protocol). It ensures the transport of signalling messages. The GIST runs on standard protocols for transportation and security. Examples of such transport protocols are UDP, TCP, Stream Control Transmission Protocol (SCTP), and Datagram Congestion Control Protocol (DCCP). In signalling layer of NSIS (NSLPs: NSIS Signalling Layer Protocols), the protocols execute the application-specific signalling. For instance QoS NSLP for reserving resource, NAT / firewall NSLP for configuring middle box etc.

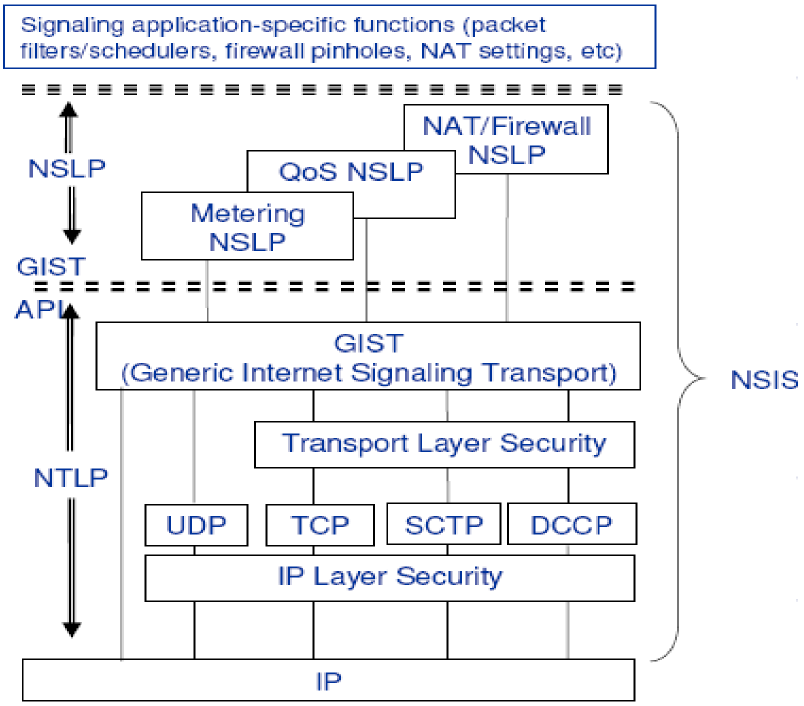

Signaling application-specific functions (packet filters/schedulers, firewall pinholes, NAT settings, etc)
NSLP
NAT/Firewall NSLP
QoS NSLP
Metering NSLP
GIST API
GIST (Generic Internet Signaling Transport)
NSIS
Transport Layer Security
NTLP
UDP
TCP
SCTP
DCCP
IP Layer Security
IP

Figure 25: Organisation of NSIS

A logical model (Figure 26) for the operation of the QoS NSLP and associated provisioning mechanisms within a single node are presented below.

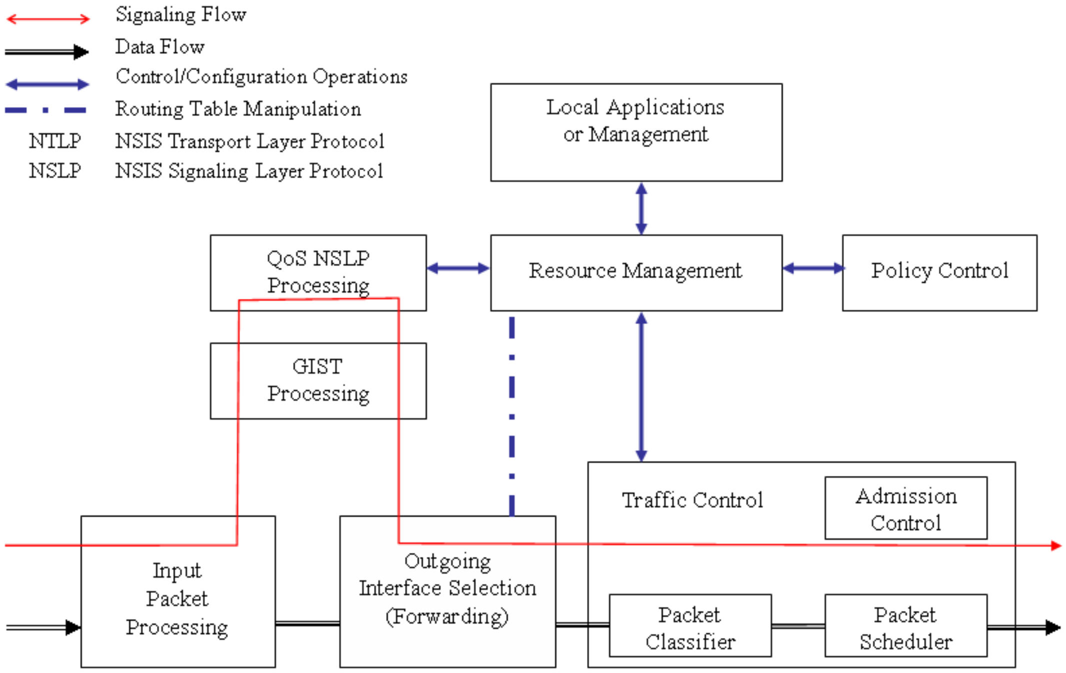

Signaling Flow
Data Flow
Control/Configuration Operations
Routing Table Manipulation
NTLP NSIS Transport Layer Protocol
NSLP NSIS Signaling Layer Protocol
Local Applications or Management
QoS NSLP Processing
Resource Management
Policy Control
GIST Processing
Traffic Control
Admission Control
Input Packet Processing
Outgoing Interface Selection (Forwarding)
Packet Classifier
Packet Scheduler

Figure 26: Logic model for the operation

Incoming messages are captured during input packet processing and handled by GIST. Only messages related to QoS are passed on to the QoS NSLP. GIST may also generate triggers to the QoS NSLP (e.g. indications that a route change has occurred). The QoS request is handled by the RMF (Resource Management Function), which coordinates the activities required to grant and configure the resources. It also handles policy-specific aspects of QoS signalling [i.30].

The grant processing involves two local decision modules: policy control and admission control. Policy control determines whether the user is authorized to make the reservation. Admission control determines whether the network of the node has sufficient available resources to supply the requested QoS. If both checks succeed, parameters are set in the packet classifier and in the link layer interface (e.g. in the packet scheduler) to obtain the desired QoS. Error notifications are passed on back to the request originator.

Admission control, packet scheduling, and any part of policy control beyond simple authorization have to be implemented using specific definitions for types and levels of QoS. A key assumption is made that the QoS NSLP is independent of the QoS parameters. These are captured in a QoS Model and interpreted only by the resource management and associated functions, and are opaque to the QoS NSLP itself.

The final stage of processing for a resource request is to indicate to the QoS NSLP protocol processing that the required resources have been configured. The QoS NSLP may generate an acknowledgment message in one direction and may forward the resource request in the other.

The QoS NSLP uses four message types:

RESERVE: The RESERVE message is the only message that manipulates QoS NSLP reservation state. It is used to create, refresh, modify and remove such state. The result of a RESERVE message is the same whether a message is received once or many times.

QUERY: A QUERY message is used to request information about the data path without making a reservation. This functionality can be used for reservations or for the support of certain QoS models.

RESPONSE: The RESPONSE message is used to provide information about the result of a previous QoS NSLP message. This includes explicit confirmation of the state manipulation signalled in the RESERVE message, the response to a QUERY message or an error code if the QNE or QNR is unable to provide the requested information or if the response is negative. The RESPONSE message does not cause any reservation state to be installed or modified.

NOTIFY: NOTIFY messages are used to convey information to a QNE. They differ from RESPONSE messages in that they are sent asynchronously and need not refer to any particular state or previously received message. The information conveyed by a NOTIFY message is typically related to error conditions. Examples would be notification to an upstream peer about state being torn down or to indicate when a reservation has been pre-empted.

QoS NSLP messages are sent peer-to-peer. This means that a QNE considers its adjacent upstream or downstream peer to be the source of each message.

QoS NSLP messages contain three types of objects:

- Control Information: Control information objects carry general information for the QoS NSLP processing, such as sequence numbers or whether a response is required.
- QoS specifications (QSPECs): QSPEC objects describe the actual resources that are required and depend on the QoS model being used. Besides any resource description they may also contain other control information used by the RMF's processing.
- Policy objects: Policy objects contain data used to authorize the reservation of resources.

QoS Specifications and QoS Models

The QoS NSLP provides flexibility over the exact patterns of signalling messages that are exchanged. Various QoS models can be designed, and these do not affect the specification of the QoS NSLP protocol. Only the RMF specific to a given QoS model will need to interpret the QSPEC. A QoS Model defines the behaviour of the RMF, including inputs and outputs, and how QSPEC information is used to describe resources available, resources required, traffic descriptions, and control information required by the RMF. A QoS Model also describes the minimum set of parameters QNEs should use in the QSPEC when signalling about this QoS Model.

The QSPEC carries a collection of objects that can describe QoS specifications in a number of different ways. A generic template is defined in [i.31] and contains object formats for generally useful elements of the QoS description, which is designed to ensure interoperability when using the basic set of objects.

All QSPECs should follow the design of the QSPEC template (Figure 27) which is composed of four QSPEC objects, namely QoS Desired, QoS Available, QoS Reserved and Minimum QoS.

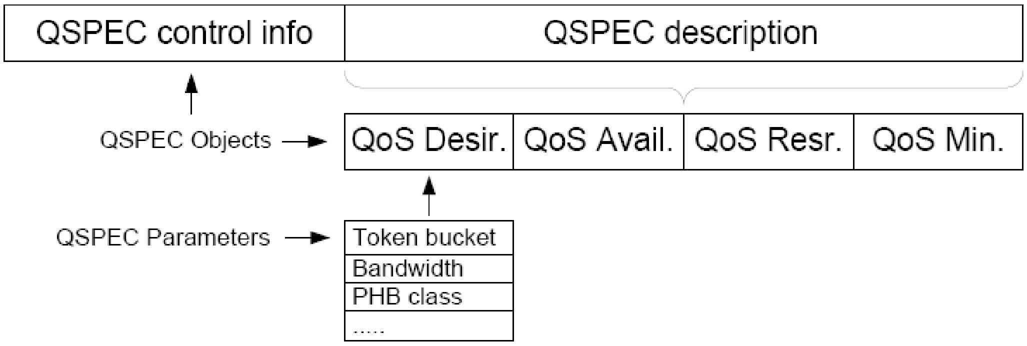


Figure 27: QSPEC Template

- QoS Available: it contains parameters describing the available resources. They are used to collect information along a reservation path.
- QoS Desired: it contains parameters describing the desired QoS for which the sender requests reservation.
- QoS Minimum: it allows the QNI to define a range of acceptable QoS levels by including both the desired QoS value and the minimum acceptable QoS in the same message.
- QoS Reserved: it contains parameters describing the reserved resources and related QoS parameters.

At each QNE, the content of the QSPEC is interpreted by the Resource Management Function and the Policy Control Function for the purposes of traffic and policy control (including admission control and configuration of the packet classifier and scheduler).

Conclusion

NSIS assumes a scalable architecture signalling in two layers and reuses the existing transport and security. It uses session ID independent of the flow identifier for the state management. The Session ID (SID) used in NSIS signalling enables the separation of the signalling state and the IP addresses of the communicating hosts. This makes it possible to directly update a signalling state in the network due to mobility without being forced to first remove the old state and then re-establish a new one.

In the NGN context, the change of route or IP addresses in mobile environments is typically much faster and more frequent than traditional route changes caused by node or link failure. Is NSIS sufficient for the self-management and self-adaptation to whatever change in the user-centric session is yet a pending question.

6.1.4 SIP

SIP is an application-layer control protocol to create, modify and terminate sessions with one or more participants. It has been designed and developed within the IETF.

The specification is available through several RFCs, the most important one being RFC 3261 [i.24] which contains the core protocol specification. It should be noted that 3GPP specified a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP) [i.2]. This specification has been endorsed by the ETSI TC TISPAN [i.8]. Here, the necessary modifications to [i.2] are provided with respect to the use of SIP/SDP in the NGN.

In the context of the present document, session stands for a set of senders and receivers that communicate and the state of which is kept during the communication. Examples of a session can include Internet telephone calls, delivery of multimedia, multimedia conferences, distributed computer games, etc.

SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility - users can maintain a single externally visible identifier regardless of their network location.

SIP supports five facets of establishing and terminating multimedia communications:

- **User location:** determination of the end system to be used for communication.
- **User availability:** determination of the willingness of the called party to engage in communications.
- **User capabilities:** determination of the media and media parameters to be used.
- **Session setup:** "ringing", establishment of session parameters at both called and calling party.
- **Session management:** including transfer and termination of sessions, modifying session parameters, and invoking services.

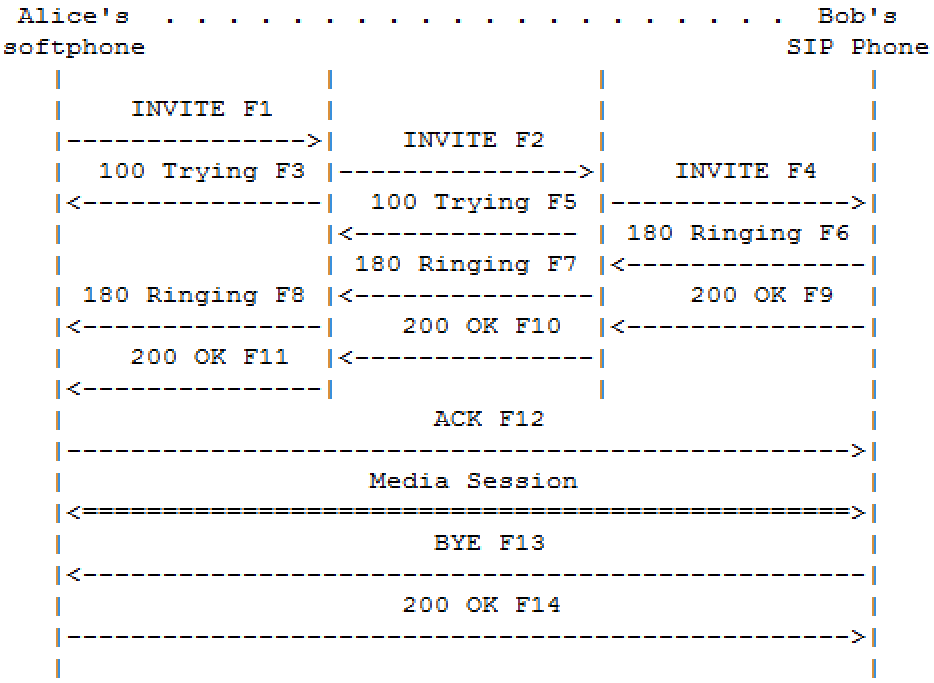
SIP uses server/client architecture, the entities in the establishment of a SIP session can be classified into two categories: user agents (terminal) and intermediate servers.

Agents (User Agents (UA)): These agents usually reside on end-user equipment in form of an application, but can be also user's terminal, such as phones, PDAs and so on.

Intermediate servers: These intermediaries are logical entities through which pass SIP messages to reach the destination. They are used to route and redirect these messages. These servers include:

- Register Server (RS) is a database that contains location information of a UAs area.
- Proxy Server (PS) is the link between the UA and the RS. It decides next hop and forwards request, relays call signalling, operates in a transactional manner, saves no session state.
- Redirect Server that enables proxy server to redirect queries to recipients who are in different domains.

SIP provisioning messages are exchanged for the establishment of the session. During this procedure of initialization (application resources reservation), the negotiation of application types, parameters of the session and capacity of the two interlocutors (end-users) is done (F1 to F12 shown in Figure 28). At the end of the reservation procedure of application resources starts the transmission of media data.



```
  Alice's  . . . . . . . . . . . . . . . . . . . .  Bob's
 softphone                                        SIP Phone
    |                |                |                |
    |    INVITE F1   |                |                |
    |--------------->|    INVITE F2   |                |
    |  100 Trying F3 |--------------->|    INVITE F4   |
    |<---------------|  100 Trying F5 |--------------->|
    |                |<-------------- | 180 Ringing F6 |
    |                | 180 Ringing F7 |<---------------|
    | 180 Ringing F8 |<---------------|     200 OK F9  |
    |<---------------|    200 OK F10  |<---------------|
    |    200 OK F11  |<---------------|                |
    |<---------------|                |                |
    |                     ACK F12                      |
    |------------------------------------------------->|
    |                  Media Session                   |
    |<================================================>|
    |                     BYE F13                      |
    |<-------------------------------------------------|
    |                    200 OK F14                    |
    |------------------------------------------------->|
    |                                                  |
```

Figure 28: Session establishment procedure

Two protocols that are most often used with SIP are RTP and SDP. RTP protocol is used to carry the real-time multimedia data (including audio, video and text) and makes it possible to encode and split the data into packets and to transport such packets over the Internet.

SDP

Another important protocol is SDP, which is used to describe and encode capabilities of session participants. Such a description is then used to negotiate the characteristics of the session so that all the devices can participate (that includes, for example, negotiation of codec used to encode media so that all participants will be able to decode it, to negotiate the transport protocol used and so on).

The purpose of SDP is to convey information about media streams in multimedia sessions to allow the recipients of a session description to participate in the session. SDP is primarily intended for use in an internetwork, although it is sufficiently general that it can describe conferences in other network environments.

Thus SDP includes:

- Session name and purpose.
- Time(s) the session is active.
- The media comprising the session.
- Information to receive those media (addresses, ports, formats and so on).

As resources which are necessary to participate in a session may be limited, some additional information may also be useful:

- Information about the bandwidth to be used by the service.
- Contact information for the person responsible for the session.

In general, SDP will convey sufficient information for a user to be able to join a session (with the possible exception of encryption keys) and to announce the needed resources to non-participants who may need to know.

Conclusion

SIP has been designed in conformance with the Internet model. It is an end-to-end oriented signalling protocol which means, that all the logic is stored in the end devices (except routing of SIP messages).

For QoS, although the SDP describes the session and negotiates the QoS requested, it will nevertheless integrate QoS signalling protocol to achieve QoS guarantee for the session.

Moreover, the SIP can filter (select) according to User Profile to implement application servers before establishment of the session but cannot re-select services during a call.

6.2 Management Plane

There is already a lot of work done related to QoS issues in management plane. The policy control in IMS architecture ensures available resource with proper defined policy rules (clause 6.2.1), and DIAMTER which is a protocol to carry the QoS and management related information (clause 6.2.2).

6.2.1 Policy control

In the IMS, the procedure of reserving resources for the purpose of QoS provisioning starts with the application indicating its requirements and ends with the resources being committed over the radio channel and into the core network. The IMS will implement resource policy control in the management plane, admission control in the control plane, and makes sure that proper policy enforcement is available in the network for the QoS guaranteed issue. By these network functions, it is ensured that IMS sessions can only be established when enough resources are available.

Using CoS (Class of Service), the packets can receive different treatments with respect to various QoS aspects such as flow priority or packet drop precedence. In addition, policy can be used to specify the packet forwarding based on various classification criteria. The policy controls the set of configuration parameters and forwarding for each class or admission conditions for flow reservations depending on the QoS scheme used e.g. RSVP, DiffServ. Once the policies for a domain are specified, all new sessions should enforce the QoS policies on the routers before the User Equipment is registered in the IMS. The policy-based control (Figure 29) in IMS [i.13] and the message flows (Figure 30) during the process of one policy-based session's establishment with the QoS guarantee [i.34] are shown below.

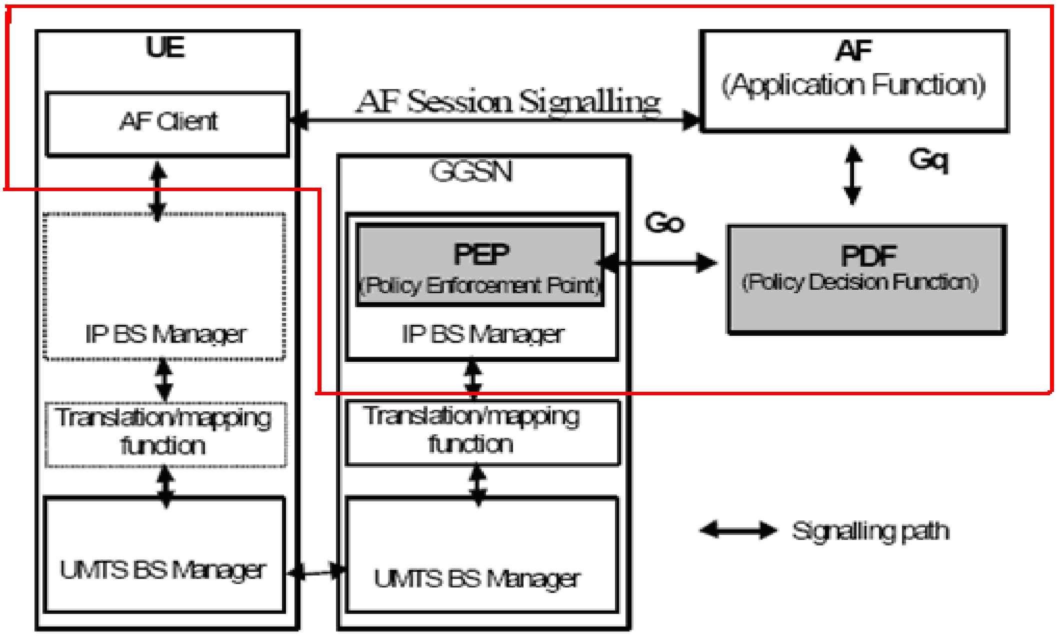


Figure 29: Go interface architecture model (TS 129 207 [i.39] R6)

The network policy rules are defined by the operator in the Policy Decision Point (PDP). This network element is used for taking policy decisions. It answers to the requests emitted by a Policy Enforcement Point (PEP). As was mentioned in the paragraph above, the interface Go can be used to carry admission control related information between the PDP and the PEP, and the interface Gq can be used to carry the policy set-up information between the PDP and the AF. Therefore, these two interfaces play a very important role in the QoS control of the policy-based services. In TR 102 805-1 [i.9], these two interfaces will be taken as the beginning of the convergence of the protocol.

Table 3: Policy based control in the IMS

Interface	Function	Protocol
Go	Provides information to support: - Control of service-based policy "gating" function in GGSN - UMTS bearer authorization - Charging correlation related function	**COPS**
Gq	Transports policy set-up information between the application function(P-CSCF) and the PDF	**Diameter**

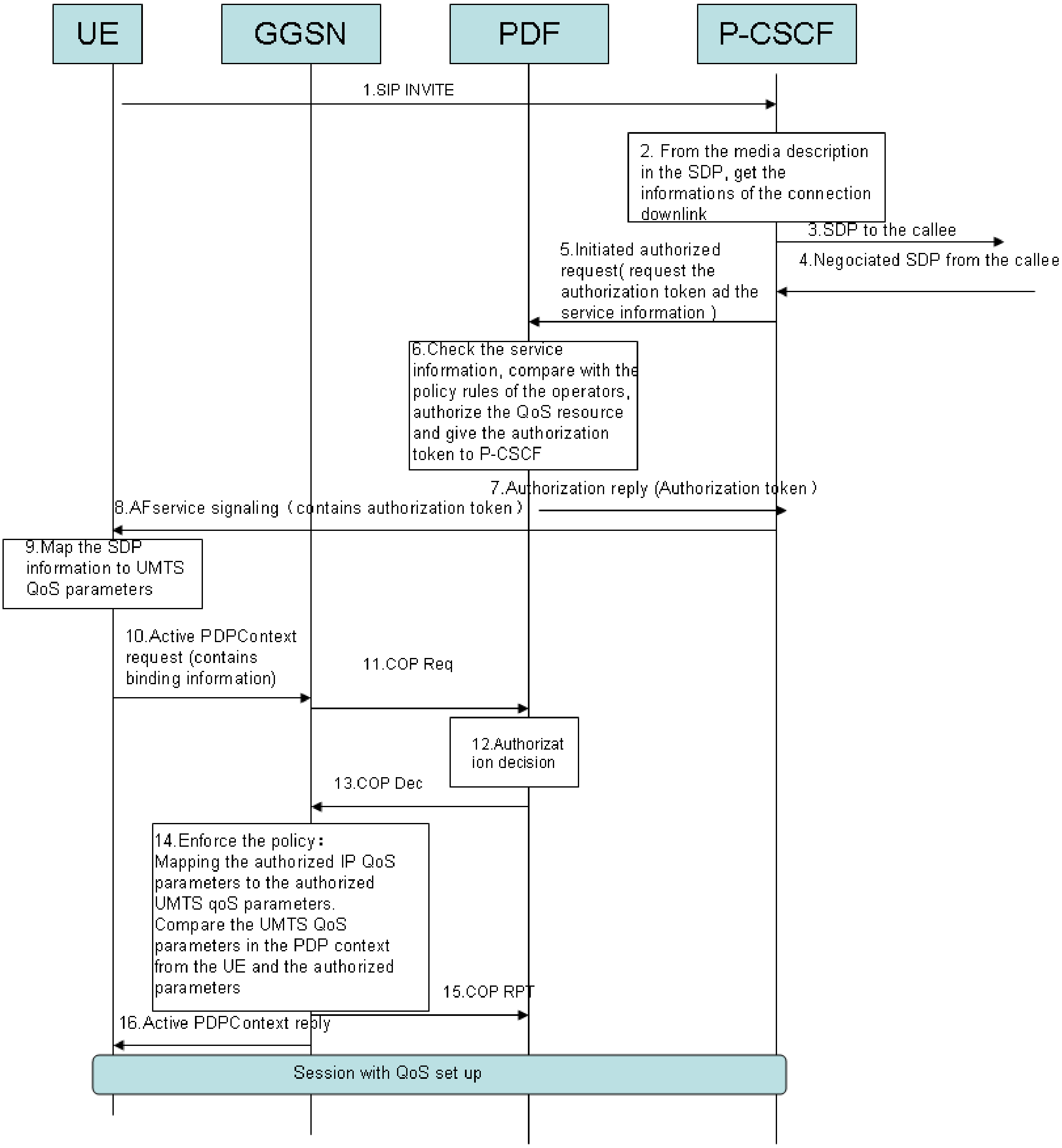

UE
GGSN
PDF
P-CSCF
1.SIP INVITE
2. From the media description in the SDP, get the informations of the connection downlink
3.SDP to the callee
4.Negociated SDP from the callee
5.Initiated authorized request(request the authorization token ad the service information)
6.Check the service information, compare with the policy rules of the operators, authorize the QoS resource and give the authorization token to P-CSCF
7.Authorization reply (Authorization token)
8.AFservice signaling（contains authorization token）
9.Map the SDP information to UMTS QoS parameters
10.Active PDPContext request (contains binding information)
11.COP Req
12.Authorization decision
13.COP Dec
14.Enforce the policy：Mapping the authorized IP QoS parameters to the authorized UMTS qoS parameters. Compare the UMTS QoS parameters in the PDP context from the UE and the authorized parameters
15.COP RPT
16.Active PDPContext reply
Session with QoS set up

Figure 30: Message flows for QoS provisioning

1) The P-CSCF receives the SDP (Session Description Protocol) parameters defined by the User Equipment within an SDP offer in SIP signalling.

2) The P-CSCF identifies the connection information needed (IP address of the down link IP flow(s), port numbers to be used, etc.).

3) The P-CSCF forwards the SDP offer in SIP signalling.

4) The P-CSCF gets the negotiated SDP parameters from the callee side through SIP signalling interaction.

5) The P-CSCF identifies the connection information needed (IP address of the up-link media IP flow(s), port numbers to be used, etc.). The P-CSCF forwards the derived session information to the PDF and requests an authorization token by sending a request for authorization (using Gq Interface).

6) The PDF checks the service information and compares with the operator's policy rules. Then the PDF authorizes every component negotiated for the session. An authorization token is generated by the PDF.

7) The PDF sends the authorization token to the P-CSCF (using Gq Interface).

8) Upon successful authorization of the session, the SDP parameters and the authorization token are passed to the UE in SIP signalling.

9) The UE mapping the SDP information to UMTS parameters.

10) UE sends an Activate PDP (Packet Data Protocol) Context request to receive the authorization token.

11) Policy Enforcement Point sends a COPS request to the PDF using the Go Interface.

12) PDF takes the authorization decision.

13) The PDF sends the configuration parameters to be enforced by the PEP through the Go Interface.

14) The PEP enforces the policies.

15) The GGSN sends COPS RPT message back to the PDF and reports its success or failure in carrying out the PDF decision.

16) The GGSN accepts the PDP context request based on the results of the authorisation policy decision enforcement.

In the IMS R7 [i.11], the policy control function (SBLP) and the Flow Based Charging function (FBC) are combined as an entity Policy and Charging Control function (PCC). The COPS based interface (Go) is replaced by DIAMETER based interface (Gx+).

The PDF and CRF are integrated into one entity which is called the PCRF. The Policy Enforcement Function (PEF) and Traffic Plane Function (TPF) are enforced in the PCEF. The Gq interface and the Rx interface are integrated as the Rx+ interface, and the Go interface and Gx interface are integrated as the Gx+ interface.

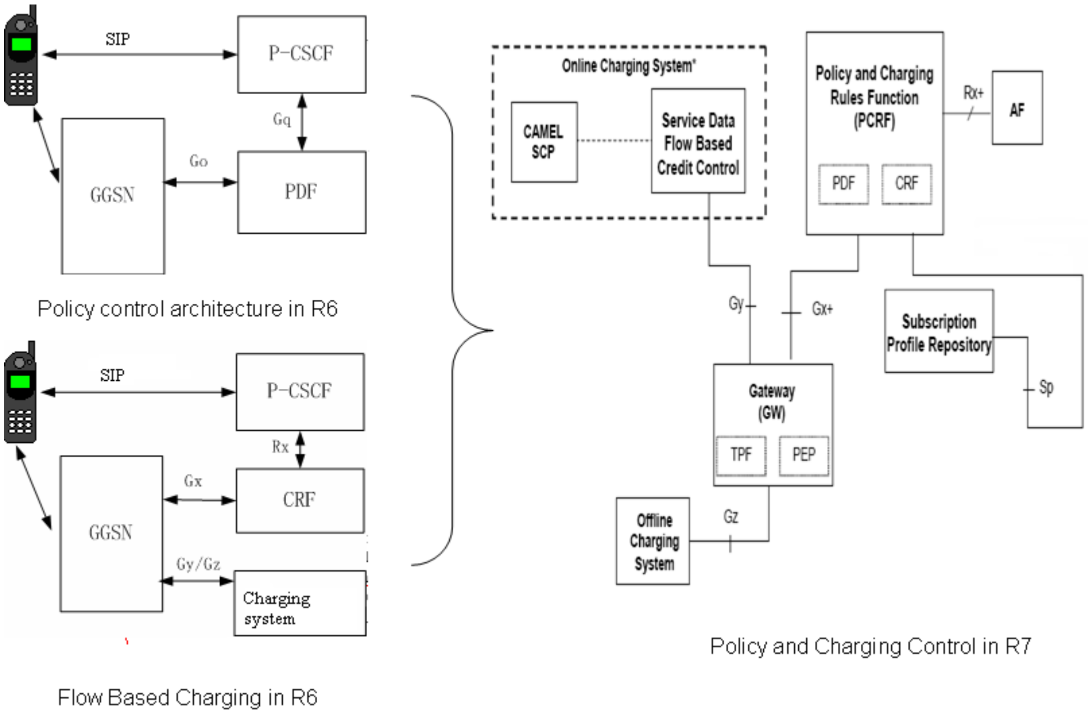

SIP
P-CSCF
Gq
Go
GGSN
PDF
Policy control architecture in R6
SIP
P-CSCF
Rx
Gx
GGSN
CRF
Gy/Gz
Charging system
Flow Based Charging in R6
Online Charging System
CAMEL SCP
Service Data Flow Based Credit Control
Policy and Charging Rules Function (PCRF)
PDF
CRF
Rx+
AF
Gy
Gx+
Subscription Profile Repository
Sp
Gateway (GW)
TPF
PEP
Offline Charging System
Gz
Policy and Charging Control in R7

Figure 31: Evolution of IMS R7

The effect of such convergence goes beyond the simple addition of the two functions. Indeed, by the fusion of the two functions, it will be possible to charge according to the strategic decision. For example, it will be possible to define a rule indicating the charging change on real-time when any QoS change occurs.

Convergence of policy decision and charging (PCRF and PCEF) entities in the Rel-7 makes it possible to transfer the QoS and charging information at the same time. The related charging protocols and interfaces are Diameter-based reference point Rx+, Gx+, Gy and Ro. The Gy and Ro interfaces are used for the online charging.

Conclusion

Policy control management in IMS allows a network operator to easily define policy control rules in the network equipments. It facilitates the translation of business level agreements like Service Level Specifications (SLSs) and Service Level Agreements (SLAs) into network level policies. From Release 7, several mechanisms are given in order to offer convergence in IMS architecture. The effect of such convergence makes dynamic decision coherent with the strategy.

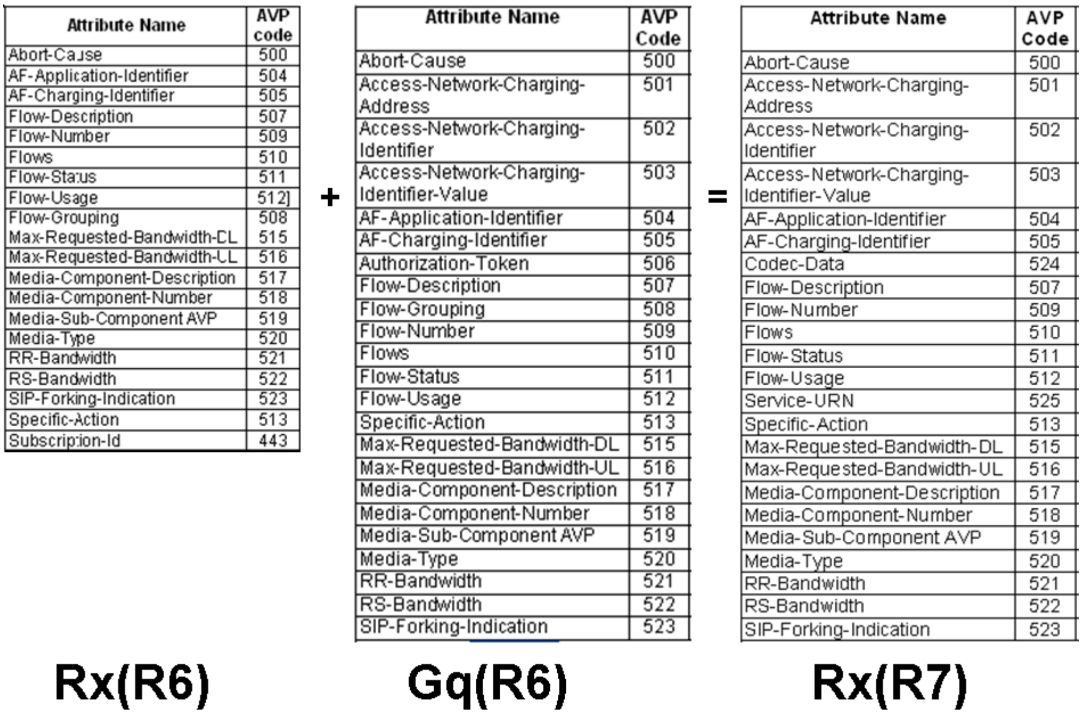
6.2.2 Diameter

In this clause the messages and the AVPs (Attribute-Values-Pairs) used in the corresponding interfaces are detailed.

Reference point Rx+ [i.41] is between the entities P-CSCF (AF) and PCRF. It enables the transport of application level session information from AF to PCRF, i.e. IP filter information to identify the service data flow for policy control, differentiated charging and media/application bandwidth requirements for QoS control.

Four pairs of messages are used in this interface: AA-Request/Answer is used to transfer the session information; Re-Auth-Request/Answer is used to indicate specific re-authorization actions; Session Termination-Request/Answer is used to indicate a session should be terminated. And Abort-Session-Request/Answer is used to indicate that the bearer of the established session is unavailable.

As mentioned before, the interface Rx and interface Gq are integrated into the interface Rx+. The former interfaces Rx and Gq are both diameter-based. Therefore, most of AVPs' definitions in Rx+ are based on TS 129 214 (V7.1.0) [i.41]: Policy and Charging Control over Rx reference point R7, June 2007.



Attribute Name	AVP code
Abort-Cause	500
AF-Application-Identifier	504
AF-Charging-Identifier	505
Flow-Description	507
Flow-Number	509
Flows	510
Flow-Status	511
Flow-Usage	512]
Flow-Grouping	508
Max-Requested-Bandwidth-DL	515
Max-Requested-Bandwidth-UL	516
Media-Component-Description	517
Media-Component-Number	518
Media-Sub-Component AVP	519
Media-Type	520
RR-Bandwidth	521
RS-Bandwidth	522
SIP-Forking-Indication	523
Specific-Action	513
Subscription-Id	443

Rx(R6)

+

Attribute Name	AVP Code
Abort-Cause	500
Access-Network-Charging-Address	501
Access-Network-Charging-Identifier	502
Access-Network-Charging-Identifier-Value	503
AF-Application-Identifier	504
AF-Charging-Identifier	505
Authorization-Token	506
Flow-Description	507
Flow-Grouping	508
Flow-Number	509
Flows	510
Flow-Status	511
Flow-Usage	512
Specific-Action	513
Max-Requested-Bandwidth-DL	515
Max-Requested-Bandwidth-UL	516
Media-Component-Description	517
Media-Component-Number	518
Media-Sub-Component AVP	519
Media-Type	520
RR-Bandwidth	521
RS-Bandwidth	522
SIP-Forking-Indication	523

Gq(R6)

=

Attribute Name	AVP Code
Abort-Cause	500
Access-Network-Charging-Address	501
Access-Network-Charging-Identifier	502
Access-Network-Charging-Identifier-Value	503
AF-Application-Identifier	504
AF-Charging-Identifier	505
Codec-Data	524
Flow-Description	507
Flow-Number	509
Flows	510
Flow-Status	511
Flow-Usage	512
Service-URN	525
Specific-Action	513
Max-Requested-Bandwidth-DL	515
Max-Requested-Bandwidth-UL	516
Media-Component-Description	517
Media-Component-Number	518
Media-Sub-Component AVP	519
Media-Type	520
RR-Bandwidth	521
RS-Bandwidth	522
SIP-Forking-Indication	523

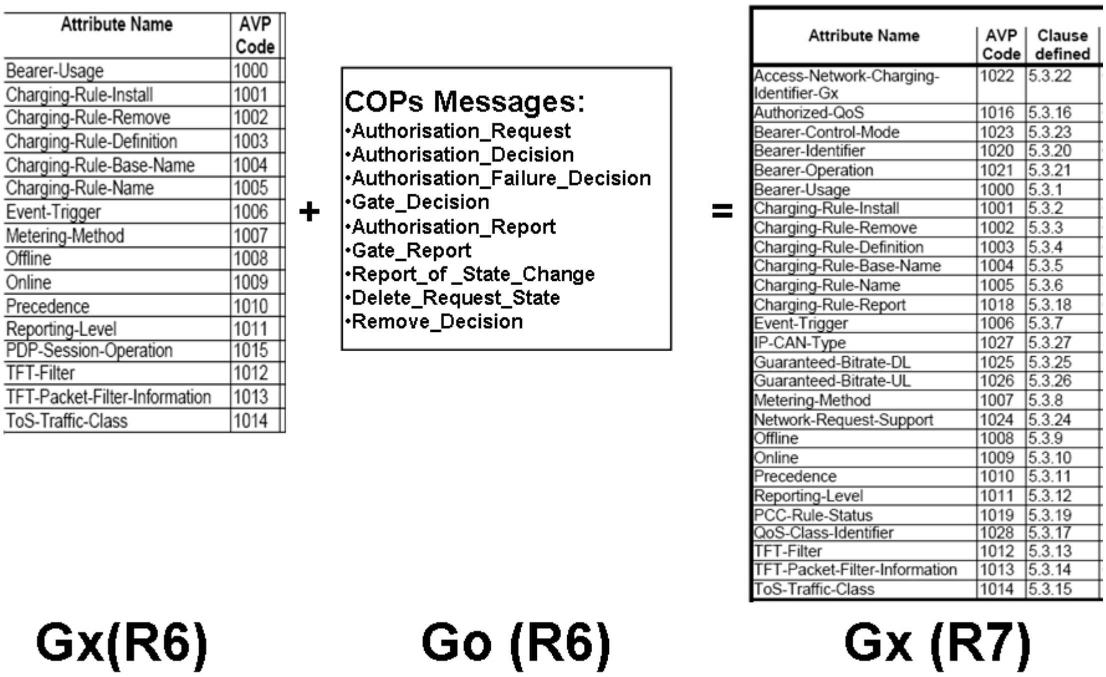
Rx(R7)

Figure 32: AVPs in Rx+

Reference point Gx [i.14] is located between the PCEF and the PCRF. It enables a PCRF to have dynamic policy and charging control over the PCC behaviour at a PCEF.

Two pairs of messages are used in this interface are: Credit-Control-Request/Answer is used to indicate bearer or PCC rule related events or the termination of the IP CAN bearer, etc. Re-Auth-Request/Answer is used to do the PCC rules provisioning and event triggers for the session, etc.

Gx and Go interfaces are integrated into interface Gx+. Go and Gx use different protocols. Go is COPS-based and Gx is diameter-based. Thus the messages used in the Go should be changed into the Gx diameter-based messages. Furthermore, the Gx+ application has its own specific Diameter application (Diameter Credit Control session for an IP-CAN session).


+
=
Gx(R6)
Go (R6)
Gx (R7)

Attribute Name	AVP Code
Bearer-Usage	1000
Charging-Rule-Install	1001
Charging-Rule-Remove	1002
Charging-Rule-Definition	1003
Charging-Rule-Base-Name	1004
Charging-Rule-Name	1005
Event-Trigger	1006
Metering-Method	1007
Offline	1008
Online	1009
Precedence	1010
Reporting-Level	1011
PDP-Session-Operation	1015
TFT-Filter	1012
TFT-Packet-Filter-Information	1013
ToS-Traffic-Class	1014

COPs Messages:

- Authorisation_Request
- Authorisation_Decision
- Authorisation_Failure_Decision
- Gate_Decision
- Authorisation_Report
- Gate_Report
- Report_of _State_Change
- Delete_Request_State
- Remove_Decision

Attribute Name	AVP Code	Clause defined
Access-Network-Charging-Identifier-Gx	1022	5.3.22
Authorized-QoS	1016	5.3.16
Bearer-Control-Mode	1023	5.3.23
Bearer-Identifier	1020	5.3.20
Bearer-Operation	1021	5.3.21
Bearer-Usage	1000	5.3.1
Charging-Rule-Install	1001	5.3.2
Charging-Rule-Remove	1002	5.3.3
Charging-Rule-Definition	1003	5.3.4
Charging-Rule-Base-Name	1004	5.3.5
Charging-Rule-Name	1005	5.3.6
Charging-Rule-Report	1018	5.3.18
Event-Trigger	1006	5.3.7
IP-CAN-Type	1027	5.3.27
Guaranteed-Bitrate-DL	1025	5.3.25
Guaranteed-Bitrate-UL	1026	5.3.26
Metering-Method	1007	5.3.8
Network-Request-Support	1024	5.3.24
Offline	1008	5.3.9
Online	1009	5.3.10
Precedence	1010	5.3.11
Reporting-Level	1011	5.3.12
PCC-Rule-Status	1019	5.3.19
QoS-Class-Identifier	1028	5.3.17
TFT-Filter	1012	5.3.13
TFT-Packet-Filter-Information	1013	5.3.14
ToS-Traffic-Class	1014	5.3.15

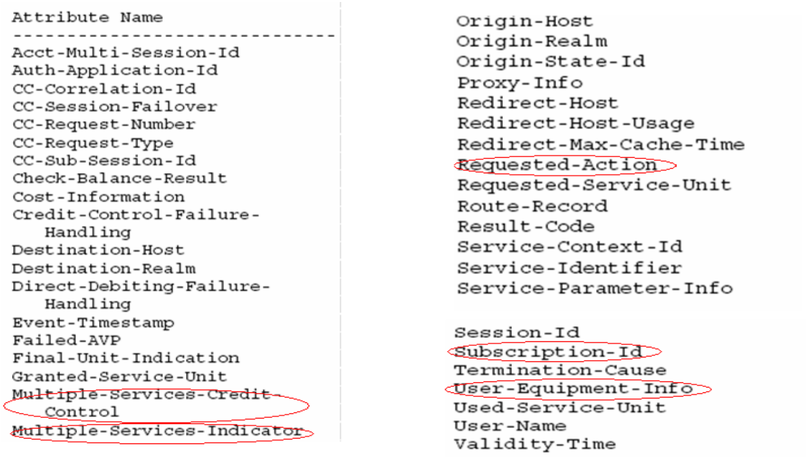
Figure 33: AVPs in Gx+

The Gy reference point resides between the OCS and the PCEF. The Ro reference point is used between the OCS and CTF (IMS-GW, MRFC, AS). The two reference points allow online credit control for service data flow based charging [i.28].

There are six pairs of messages in Ro interface:

- Credit-Control-Request/Answer;
- Re-Auth-Request/Answer;
- Capabilities-Exchange-Request/Answer;
- Device-Watchdog-Request/Answer;
- Disconnect-Peer-Request/Answer;
- Abort-Session-Request/Answer.

Credit Control AVPs



```
Attribute Name
------------------------------
Acct-Multi-Session-Id
Auth-Application-Id
CC-Correlation-Id
CC-Session-Failover
CC-Request-Number
CC-Request-Type
CC-Sub-Session-Id
Check-Balance-Result
Cost-Information
Credit-Control-Failure-
   Handling
Destination-Host
Destination-Realm
Direct-Debiting-Failure-
   Handling
Event-Timestamp
Failed-AVP
Final-Unit-Indication
Granted-Service-Unit
Multiple-Services-Credit-
   Control
Multiple-Services-Indicator

Origin-Host
Origin-Realm
Origin-State-Id
Proxy-Info
Redirect-Host
Redirect-Host-Usage
Redirect-Max-Cache-Time
Requested-Action
Requested-Service-Unit
Route-Record
Result-Code
Service-Context-Id
Service-Identifier
Service-Parameter-Info

Session-Id
Subscription-Id
Termination-Cause
User-Equipment-Info
Used-Service-Unit
User-Name
Validity-Time
```

Figure 34: Credit control AVP

All of the Diameter AVPs defined in the credit-control application are shown in Figure 34. These AVPs could be used in the Credit-Control messages, i.e. CCR/CCA. The four AVPs related to user equipment and multiple service are circled in red as the most interesting in this context: Multiple-Service-Credit-Control; Multiple-Service-Indicator; Requested-Action and User-Equipment-Info.

Conclusion

The IMS standard is being adopted by a growing number of companies of the telecom community. IMS provides a standardized, well-structured way of delivering services, legacy inter-working and fixed-mobile convergence. IMS uses DIAMETER to carry the information of authorization, charging,etc. The QoS related information can also be mapped to DIAMETER AVP.

6.3 User plane (CPN: Customer Premises Network)

In clause 4, the user-centric requirements for the Next Generation Service have been identified. The QoS research should be extended from core to edge. In such End-to-End session, the user connectivity to heterogeneous network for the service with QoS is considered as an important part of resolving the E2E QoS in the NGN. TISPAN has proposed the Home Networking conception which contains Customer Network Device (CND) and Customer Network Gateway (CNG), to interact with TISPAN NGN for variety of services in the home environment [i.19].

TISPAN began to cover home devices and home networking issues from 2006 and a specific working group (WG5) was created in TISPAN to develop service requirements, functional architectures and protocols for the entities involved in the home network environment.

In this clause, an overview is given on services provided in Home Networking (also named customer premises network or CPN in TISPAN) (clause 5.3.1), on the way it interacts with the NGN-IMS networks which is described in the ETSI TISPAN Release 1 standards [i.4] and on the QoS related blocks in the CPN architecture (clause 5.3.2).

6.3.1 Service provided in CPN

The use cases can be grouped in the following categories [i.19]:

1) **Broadband connection**

The user wants to access the Internet from a number of PCs at home, and may also decide to subscribe to new services (e.g. parental control, online audio streaming, etc.) offered by his Internet Service Provider (ISP) or an Application Service Provider (ASP), via email or online.

From the service provider point of view, the service will be remotely activated via auto-provisioning, the necessary connectivity to deliver the service, including QoS should be guaranteed and there should be the possibility of remotely debug the customer problems.

2) Communication

There are three categories of communication services:

- Person-to-Person communication (P2P): voice or voice/video communication, text service, and computer-originated text communication to PSTN. The service provider should guarantee the necessary connectivity to deliver the service with QoS.
- Person-to-Machine communication (P2M): A typical P2M communication use case is, for example to remotely access a device to access the home media server and upload or download one's photos.
- Machine-to-Machine communication (M2M): A typical M2M communication use case is from the customer network and NGN standpoints the automatic electricity meter reading business. With this approach, network operators can reuse the NGN security functions in CNG (Customer Network Gateway) and electricity charging server to deliver secure data service between customers' electricity meters and electricity companies' charging servers.

3) Home worker

In this use case various members of a family simultaneously use the broadband infrastructure. In particular, parents are connected to their respective corporate intranets over a secure link and perform a number of actions, including upload and download of documents, placing VoIP calls for work. They expect to have a simple mechanism by which they can easily switch from private to corporate calls (billing will be different). While the parents are working, children should be able to watch video streaming, or browse the Internet. All these simultaneous applications have to live up to the experiential expectations of the user. Hence the necessary priorities have to be taken into account within the customer network environment.

4) Home Management and Security

Two different sub cases are proposed for this category.

The first sub case is related to the *access/parental control*. The user wants to make sure that he has an overview on the children communication and entertainment activities and that he is able to control the access to these activities. An access control service can be built up with the following capabilities: Content check, Cost check, Usage check, Time check. The user should have the capability to check the configuration of the access control service via a terminal (e.g. a PC) and to change the parental control configurations by himself as administrator. From the service provider point of view, a number of mechanisms for service activation, billing and web based consumer support in case of problems should be ensured.

The second sub case is to the *personal monitoring*. In this use case the user should be able to access images coming from a camera installed at home, via an Internet browser on a remote PC or/and via a mobile Internet connection.

5) Provisioning and Service configuration

A set of parameters should be configured on UE (device that contains the SIP UA) to access to IMS network. These parameters should be provisioned on UE in order to the user to make seamlessly the UE registration to IMS. There are four kinds of configurations:

- First Provisioning (Manual).
- First Provisioning (Automatic).
- Manual Re-Configuration.
- Self Re-Configuration Service.

6) Entertainment and information

Three specific use case scenarios are proposed for this category. The first one is related to the broadcast IPTV service usage inside the house, the second one to the access the contents stored in a media gateway and the third one to gaming.

7) **Remote Access**

When a user is away from its customer network, it is in many situations valuable to be able to access services on the customer network. Remote access can be divided into two categories: access of devices and access of services. An example of the first category is uploading the latest vacation pictures or films to a storage server on the customer network or when a user sends a message to his home to turn on/off a device. An example of the second category includes accessing a surveillance camera service to check that everything is in order.

6.3.2 CPN architecture model interacting with the NGN/IMS networks

In this clause, the TISPAN Architectural Model for the CPN and interactions with NGN-IMS entities is detailed. The CPN is composed of Customer Network Gateway (CNG) and Customer Network Device (CND) entities. Examples of Customer Network Devices which may be connected to the CNG:

a) analogue phones connected through the CNG to the NGN network;

b) IMS Customer Network Devices connected through a CNG to the NGN network;

c) non IMS SIP IETF Customer Network Devices;

d) ISDN Customer Network Devices connected through the CNG to the NGN network.

Different types of Customer Network Devices may be involved in Intra CPN communication through a CNG. The list of Customer Network Devices which are likely to be connected to the CNG is provided by the TS 185 006 [i.20].

The CNG functional entities which are used to interact with TISPAN NGN network are shown in Figure 35, as well as the reference points between each function.

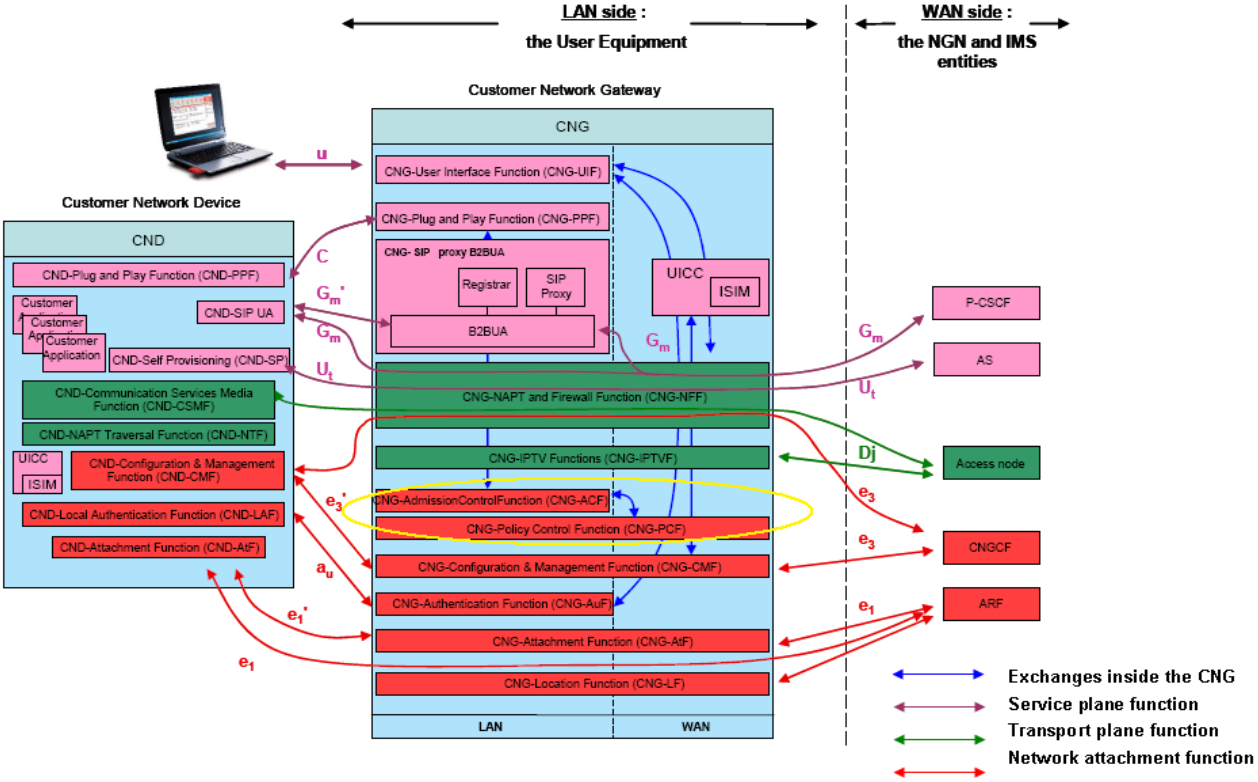

LAN side :
the User Equipment
WAN side :
the NGN and IMS entities
Customer Network Gateway
CNG
CNG-User Interface Function (CNG-UIF)
CNG-Plug and Play Function (CNG-PPF)
CNG- SIP proxy B2BUA
Registrar
SIP Proxy
B2BUA
UICC
ISIM
CNG-NAPT and Firewall Function (CNG-NFF)
CNG-IPTV Functions (CNG-IPTVF)
CNG-AdmissionControlFunction (CNG-ACF)
CNG-Policy Control Function (CNG-PCF)
CNG-Configuration & Management Function (CNG-CMF)
CNG-Authentication Function (CNG-AuF)
CNG-Attachment Function (CNG-AtF)
CNG-Location Function (CNG-LF)
LAN
WAN
Customer Network Device
CND
CND-Plug and Play Function (CND-PPF)
Customer Application
Customer Application
Customer Application
CND-SIP UA
CND-Self Provisioning (CND-SP)
CND-Communication Services Media Function (CND-CSMF)
CND-NAPT Traversal Function (CND-NTF)
UICC
ISIM
CND-Configuration & Management Function (CND-CMF)
CND-Local Authentication Function (CND-LAF)
CND-Attachment Function (CND-AtF)
u
C
G_m'
G_m
U_t
e_3'
a_u
e_1'
e_1
G_m
G_m
U_t
Dj
e_3
e_3
e_1
P-CSCF
AS
Access node
CNGCF
ARF
Exchanges inside the CNG
Service plane function
Transport plane function
Network attachment function

Figure 35: IMS Customer Network Device connected to the NGN-IMS network through a CNG

The entities and interfaces in red are network attachment functions, admission control function, policy control function, authentication function, and location function etc. The entities and interfaces in green are for the transport of the service media. The entities and interfaces in pink are dedicated to the service layer functions. Meanwhile, in the CNG, there are interfaces among the three level entities to allow for exchanges of pieces of information.

- CNG-User Interface Function: The CNG-UIF entity should allow the user to configure many CNG parameters for the transport layer:
  - firewall rules, possibly defined for each user (e.g. parental control);
  - CNDs authorized within the CPN, with possible bandwidth restrictions.

The operator should be able to prevent a user from modifying a specific subset of CPN parameters. Thus this entity may have reference points with the CNG-AuF and the CNG-NFF of the CNG.

- CNG-Policy Control Function: The CNG-PCF may integrate a database containing the access profile. This includes bandwidth and QoS parameters for the CNG Customer Network Device side applications and terminals, which could be configured by a user. For instance, congestion issues within the CPN may be solved defining resources for several SSID.

- CNG-Admission Control Function: The CNG-ACF (Figure 36) should receive and send QoS messages from/to the CNG-SIP proxy B2BUA Function. In particular it should:
  - check resources availability on each link/device involved in the communication requesting a QoS reservation/allocation, through an internal database;
  - perform the appropriate resources reservation, through the CNG-PCF.

Thus, the CNG-ACF should manage session limitations for instance or the priority of media streams. This applies to upstream flows but there may also be an opportunity to do so for downstream flows. The module is considered as optional (as Gm' and Gm interfaces related to the SIP proxy).

The objective is to guaranty the quality of service for each new session and existing sessions previously established. The B2BUA extracts from SIP messages the SDP offer and announced capabilities (codec audio, video, etc.). It asks to the CNG-ACF if announced capabilities are compliant with the available resources.

The CNG-ACF module can return 3 different responses:

a) OK:
   - the resource is available for all announced codecs;
   - the initial SIP message is forwarded without any change on SDP part.

b) OK with restriction:
   - the initial SIP message is modified (incompatible codecs are suppressed from SDP part) and then forwarded;
   - the session can be established with an acceptable codec for network resource.

c) Not OK:
   - the B2BUA rejects the session establishment.

Below is the procedure of admission control in CNG (Figure 36):

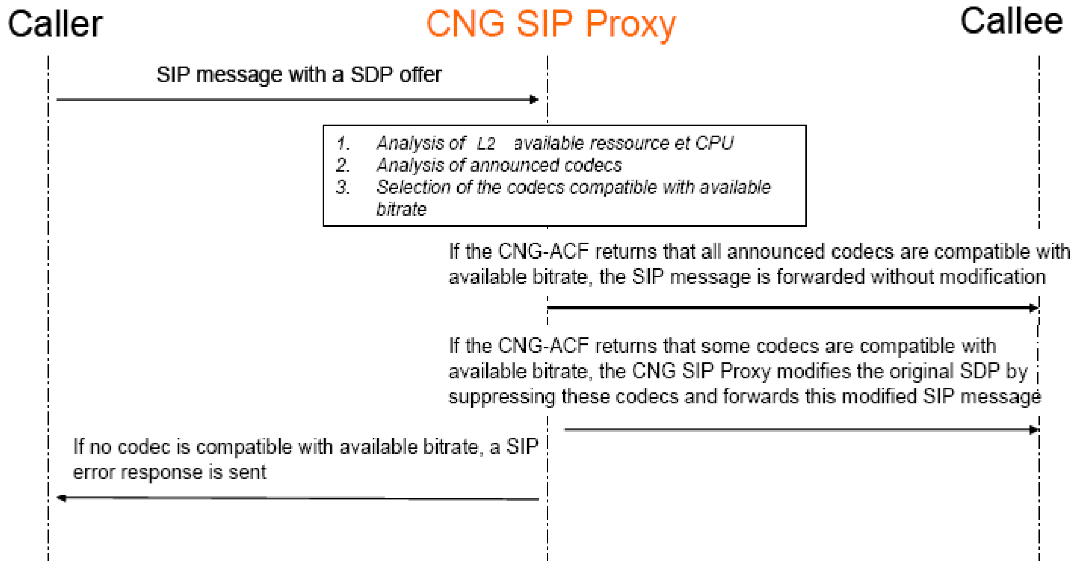

Caller
CNG SIP Proxy
Callee
SIP message with a SDP offer
1. Analysis of L2 available ressource et CPU
2. Analysis of announced codecs
3. Selection of the codecs compatible with available bitrate
If the CNG-ACF returns that all announced codecs are compatible with available bitrate, the SIP message is forwarded without modification
If the CNG-ACF returns that some codecs are compatible with available bitrate, the CNG SIP Proxy modifies the original SDP by suppressing these codecs and forwards this modified SIP message
If no codec is compatible with available bitrate, a SIP error response is sent

Figure 36: Admission control within the CNG

Conclusion

For the service and network providers, the CPN speeds up broadband deployment and multi-service implementation. More important, the QoS related entities in the CPN give the possibility to deal with the QoS issue on the user side in an End-to-End session with QoS continuity. Therefore, this will be taken it into account in the drafting of the TR 102 805 set [i.9] and [i.10].

7 Conclusion and next steps

Evolution of networks and services requires to consider end to end flow while offering transparency of information to the end users.

Users and services are interconnected by several networks which may be trans-organizations.

In order to achieve the expected behaviour (end-user), means are needed to provide cooperation between different environment in order to achieve end to end QoS.

Today, the end-user wishes to choose any terminal or any access as a mean to use any service in a heterogeneous environment. Meanwhile, the end-user expects to have a continuous comprehensive service throughout the whole session while moving (terminal mobility) or changing terminal (user mobility). During this session, service connectivity is considered as a composition of elements in each layer (User, Terminal, Network and Service).

To achieve the E2E QoS, considering these new paradigms, the control plane (signalling based solution, such as SIP/SDP, NSIS) and the management plan (management based solution, such as DIAMETER or Policy Control) through converged interfaces, should be considered.

The goal of next steps is now to identify at which point end-users could and should enter their choices and preferences and which components play a key role in the interactions with the end-users in order to take dynamic decision at right place and right moment.

Annex A: Bibliography

- ETSI ES 282 002 (V1.1.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture" (see also TS 182 012).

- ETSI TS 123 234 (V7.7.0): "Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (current version: 3GPP TS 23.234 version 7.7.0 Release 7)".

- ETSI TS 129 213 (V8.1.1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping (current version: 3GPP TS 29.213 version 8.1.1 Release 8)".

- IEEE 802.11g-2003 Part II: "Wireless LAN MAC and PHY specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band".

- ITU-T Recommendation H.360 (2004): "An architecture for end-to-end QoS control and signalling".

- ITU-T Recommendation Y.1251 (2002): "General architectural model for interworking".

- ITU-T Recommendation Y.1540 (2007): "Internet protocol data communication service - IP packet transfer and availability performance parameters".

- ITU-T Recommendation Y.1541 (2006): "Network Performance objectives for IP-based services",.

- IETF Y.1541-QOSM - Y.1541 (2008): "QoS Model for Networks Using Y.1541 QoS Classes".

NOTE: See http://tools.ietf.org/html/draft-ash-nsis-y1541-qosm-00.

- IETF RFC 2327 (1998): "SDP (Session Description Protocol)".

- IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol" IETF, Tech. Rep., 2000.

- IETF RFC 4094: "Analysis of Existing Quality-of-Service Signalling Protocols" May 2005.

History

Document history		
V1.1.1	November 2009	Publication