Multimedia Content Distribution Over Next-Generation Heterogeneous Networks Featuring a Service Architecture of Sliced Resources

Ioannis M. Stephanakis[1] and Ioannis P. Chochliouros[2]

[1] Hellenic Telecommunication Organization (OTE) S.A.,
99 Kifissias Avenue, GR-151 24, Athens, Greece
stephan@ote.gr
[2] Research Programs Section,
Hellenic Telecommunications Organizations (OTE) S.A.,
99 Kifissias Avenue, GR-151 24, Athens, Greece
ichochliouros@oteresearch.gr

Abstract. Recent advancements of IP networks pave the way for Over-the-Top (OTT) applications. Evolved telecom platforms provide revenue potentials via Service Gateways (APIs) on top of VoIP/RCS (IMS), Machine Type Communication (MTC) and Smart Bit pipe approaches. QoS is achieved through over-provisioning in today's access and core networks since there are no flexible mechanisms that are available for end-users to influence the QoS level. Processes for user-demanded and operator-controlled QoS management as well as mechanisms for applications signaling their requirements on the data path into the network are far from being adequate. Novel approaches regarding end-to-end inter-domain flow-control architectures, i.e. network slicing, as well as machine-to-machine (M2M) virtualization platforms that handle such functions as device/communication management, session management and bearer and charging management are emerging promising enhanced multimedia communications and efficient utilization of network resources. They promote cloud services and they integrate the computer word into next generation telecommunications.

Keywords: network slicing; IP Multimedia Susystem (IMS); content delivery networks; cloud services; software defined networks (SDN); H.264/AVC

1 Introduction – Virtualized Next Generation Transport And Application Triggered Quality-of-Service (QoS)

Services in broadband *Next-Generation-Networks* (NGN) require end-to-end *Quality-of-Service* (QoS) over heterogeneous transportation and data networks and across multiple IP *Autonomous System* (AS) domains. *Quality-of-Service* is guarantied over sliced network resources that are parameterized on an automatic or semi-automatic basis by the end user or the application program. An application establishes a session that triggers the corresponding network setup which satisfies QoS requirements. This has the advantage to perfectly synchronize QoS requirements / setup and the usage of network resources by the application. *Machine-to-Machine* (M2M) communication according to the RESTful approach proposed by ETSI M2M assumes a virtualized transport layer consisting of routers, sliced network resources and virtual machines (VMs) that form the basis layer in a structured architecture that separates control, application and transport layers (see Fig. 1). Cloud services are straightforward commercial offerings that utilize such an architecture. The *Multiprotocol Label Switching* (MPLS) is an IP network protocol supported by many carriers including the *Hellenic Telecommunications Organization* (OTE). OTE supports transparent interconnection of client *Virtual Private Networks* (VPNs) through MPLS VPN (IETF RFC 2547bis) and MPLS Inter-AS. *Quality-of-Service* is supported through the implementation of the IETF recommendation RFC 3270 (MPLS *Support of Differentiated Services*).

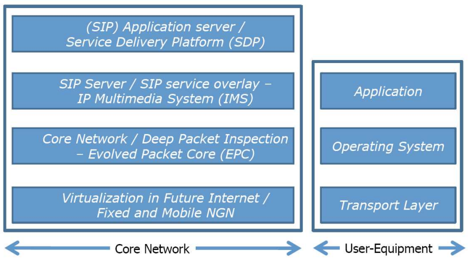

Fig. 1. A virtual transport layer forms the basis of structured models of future NGNs

1.1 Video-to-Video Delivery Over Content-Distribution-Networks (CDN)

A NGN has been defined by several standards bodies, including the ATIS IPTV Interoperability Forum (ATIS IIF), the ITU (*International Telecommunication Union*) and the ETSI TISPAN (*European Telecommunications Standards Institute - Telecoms & Internet Converged Services & Protocols for Advanced Networks*). In the definitions developed by all these organizations, NGN architectures and functional elements are similar and usually grouped into two layers:

- *NGN transport layer,* which contains transport processing functions that may include different access networks, a common *Network Attachment Subsystem* (NASS) and a common *Resource and Admission Control Subsystem* (RACS) [1].

- *NGN service layer,* which contains IMS (IP *Multimedia Subsystem*), PSTN/ISDN *Emulation Subsystem* (PES) and common elements such as a *User Profiles Service Function* (UPSF).

Despite the fact that NGN specification includes several communication standards (like for example PES and IMS), it does not consider IPTV. Two approaches have been suggested to accommodate the addition of IPTV [2,3,4]:

- IMS-based IPTV, which extends IMS to support basic IPTV services
- NGN Integrated IPTV (IMS-integrated IPTV), which integrates IPTV alongside IMS

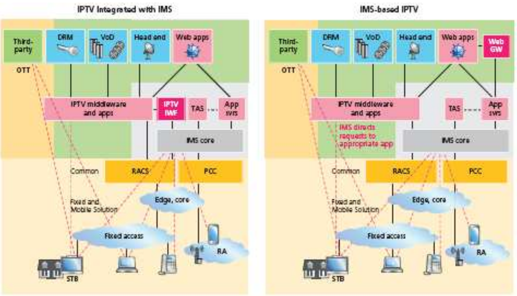

Fig. 2. IMS proposes two distinct ways of implementing an IPTV platform

Solutions based on the IMS-integrated (NGN Integrated IPTV) approach are well-suited for integration with web-based services (such as HTTP delivered content, Internet TV, adaptive streaming) because they have native support for web-based interfaces. IMS-based IPTV requires interworking between services not based on SIP (*Session Initiation Protocol*) via applications or a web gateway as shown in Fig. 2. An IMS-based IPTV approach requires extra SIP messages to access and control services, as well as “native” IPTV protocols, such as RTSP, IGMP and HTTP. NGN integrated IPTV requires three to four times fewer control messages for unicast services (VoD, restart TV, nPVR) and over eight times fewer messages for linear TV services (broadcast TV). Thus channel changes for IMS-based IPTV feature an overhead delay. IMS (*Section* 2.1) is designed as an end-to-end call management infrastructure that provides quality of service (QoS) between two call endpoints. Linear IPTV services are delivered using IP multicast. With IP multicast, the second IP endpoint is not known to IMS service control. Each multicast replication tree may end either at a multicast replicator in an access node or in network elements in the core network. Thus central-based admission control used by IMS cannot provide end-to-end QoS for linear services if the multicast tree is not available in the local access node. An additional overlay multicast control plane in the context of NGN architecture is required.

The current deployment of the IPTV platform of OTE utilizes VLANs for delivering IPTV services to users as well as for providing interconnection to content providers in a multi-source *Content Distribution Network* (CDN). The head-end includes encodes, receivers and transcoders as well as *Network Element Managers*, a *Conditional Access* and a *Digital Right Management System* (CA/DRM), a *Middleware Application Server* (MAS) and CDP (*Content Delivery Platform*) servers. Video compression protocols MPEG-2 and MPEG-4 are supported.

1.2 Cloud Services: Service Architecture and Taxonomy

There are the following distinct ways of cloud implementation:
- *Software as a service* (SaaS), in which case software is offered on-demand through the internet by the provider. The software may be parameterized remotely. Such examples are on-line word processors, spreadsheets, Google Docs and others.
- *Platform as a service* (PaaS), in which case customers are allowed to create new applications that are remotely managed and parameterized. The platform offers tools for development and computer interface restructuring. Such examples are Force, Google App Engine and Microsoft Azure.
- *Infrastructure as a service* (IaaS), in which case virtual machines, computers and operating systems may be controlled and parameterized remotely. Such examples are Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive, Rackspace Cloud, GoGrid, Joyent, AppNexus and others.

Cloud computing may be divided into *Public cloud*, in which everyone may register and use the services, *Private cloud*, which is accessible through a private network, and *Partner cloud*, which offers services to specific partners/users. Cloud computing is an on-demand service whose size depends upon users' needs and should feature scale flexibility.

1.3 Current Implementations of Network Slicing And Virtualized Programmable Networks/Software Defined Networks (SDNs)

Current distributed control plane architectures do not grand switching nodes access to the full network topology neither do they allow for inter-domain QoS negotiation. One may enforce and monitor end-to-end QoS across multiple domains by defining priority flow paths and over-the-top switching controllers. *Software Defined Networks* (SDNs) are characterized by the ability to virtualize network resources. Such virtualized network resources are known as a "network slices". A slice can span several network elements including the network backbone, routers and hosts. *Software Defined Networks* decouple routing and switching of data flows and move the control of the flow to a separate network element namely, the flow controller that is implemented by the so-called *Service Control Point*. The concept of SDN originates from the academic community and there are multiple approaches adopted by the industry. Two approaches have risen to prominence with differences in their implementation making each applicable to different markets without prohibiting hybrid deployment.

- The *Open Flow solution* [5], which is proposed by the Open Networking Foundation and removes the entire control plane from the network equipment relegating it to a data-plane only role. New mechanisms of network control (discovery, path computation, path set up etc) are created and hosted on a server/cloud. The entities introduced in current implementations are the so-called *Open Flow controller*, which performs flow routing control, dynamic queue management and resource assignment, and the so-called *Open Flow switch*, which performs routing/packet forwarding and packet flow to queue assignment. Although applicable to telco/WAN environments, early work has focused on data centers and campus applications.

- The *Path Computation Element* (PCE) standardized by the IETF (IETF RFC 4655: PCE and RFC 5440: PCEP). PCE takes an evolutionary approach by migrating the path computation component of traditional networking devices to a centralized role. Much of the well established and proven software functions of the control plane are left untouched and remain integrated within the network element enabling a gradual migration to SDN. PCE has the added benefit of providing inter-domain networking, which is a key application for carrier networks. For true traffic engineered inter-domain data flows, it must be possible to calculate an optimal end-to-end path. PCE servers do have access, via interrogation of other PCE Servers, to path and traffic engineering information required in order to compute an optimal end-to-end path through different MPLS/IP aggregation networks. This feature makes PCE the preferred approach to SDN for telco/WAN environments.

Virtual Path Slices (VPS) and their corresponding controller have also been adopted in the context of [6]. We see currently two fundamental types of QoS services: Rate limiting at ingress and minimum bandwidth guarantee on egress. The first is typically done with a meter that is associated with ingress port or ingress flows; after a certain rate is exceeded packets are dropped according to some algorithm.

A virtualized *Machine-to-Machine* (M2M) transport layer envisages distributed applications across multiple virtual machines (VMs) that exchange traffic flows with each other. VM architecture migrates to optimize and rebalance server workloads, causing the physical end points of existing flows to change (sometimes rapidly) over time. VM migration challenges many aspects of traditional networking, from addressing schemes and namespaces to the basic notion of a segmented, routing-based design. It is interesting to mention the concept of para-virtualization, which is a technique of changing the kernel of the operating system in order to “port” it to an idealized virtual machine abstraction. This abstraction may lead to significant improvement in performance and efficiency. The basic architecture proposes a *hypervisor* or a virtual machine monitor which sits between the guest operating systems and the actual hardware. All hardware accesses are controlled by the *hypervisor*.

2 The IP Multimedia Subsystem (IMS)

2.1 IMS Architecture

The IMS architecture standardizes network functions and calling processes that are associated with the provisioning and the operation of multimedia services offered by telecom operators and are based upon the TCP/IP protocol suite described in IETF (*Internet Engineering Task Force*) recommendations. The IMS functional architecture [7] was initially designed by the 3GPP (3rd *Generation Partnership Project*) initiative for the communication models of wireless networks and it was intended for IP services over GPRS (*General Packet Radio Service*) mobile networks. The proposed functional architecture has been revised by 3GPP2 and the ETSI TISPAN workgroup in order to include *wireless LAN*, *CDMA2000* and *fixed line* networks. The IMS architecture defines a *control layer*, which is operated by the network provider and manages the underlying *access* and *transport layers* by performing *session control* of *data flows*. A *service layer* is defined as a higher layer that consists of application and multimedia servers. The core entities of the IMS architecture (see Fig. 3) are the *Call Session Control Functions* (CSCF) - i.e. the so called *Proxy*-CSCF, *Serving*-CSCF (S-CSCF) and *Interrogating*-CSCF (I-CSCF) – the *Home Subscriber Server* (HSS), application servers, media servers (like MRFC and MRFP), *Breakout Gateways*, IBCF (*Interconnection Border Control Function*), *Service Border Gateways* and *Application Layer Gateways* (ALG). The P-CSCF of the control layer supervises signaling, QoS, security and compression. The S-CSCF implements such functions as registration, routing (based on ENUM as in IETF RFC 3761), application routing (SSF) and network policies enforced by the operator. The I-CSCF communicates with the *Home Subscriber Server* (HSS), the *Subscriber Location Function* (SLF), the IBCF and the *Breakout Gateway Control Function* (BGCF). The IMS architecture supports user *authentication*, user *authorization* as well as quality-of-service functions [8, 9, 10] and communication security processes. These functions are supported by reliable, fault-tolerant servers at the application layer. This layer manages such service components as *user groups*, *presence*, *location* and others. IMS also controls the *Border Gateway Function* at the transport network.

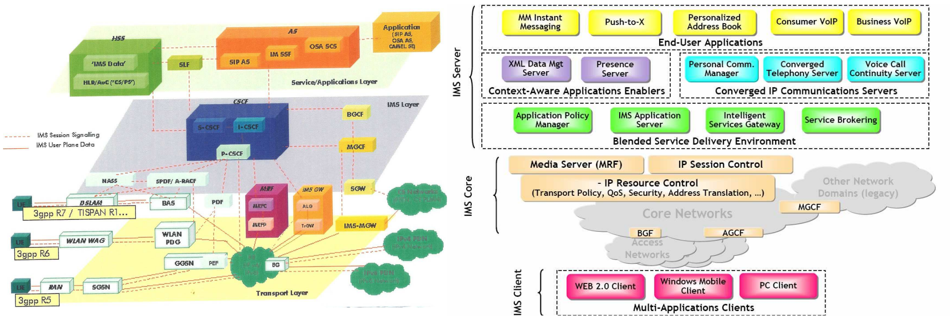

Fig. 3. IMS architecture assigns network functionalities into the so-called access layer, control layer and service layer

IMS defines two functions to police the signaling flows from IP-based networks entering the network core. On the access side, signaling between users and the IMS core is controlled by a *Proxy Call Session Control Function* (P-CSCF). Data flows per se are controlled by the NASS and the RACS modules. On inter-carrier links, signaling is controlled by the *Interconnect Border Control Function* (IBCF). The primary distinction between P-CSCF and IBCF is that devices that attach through a P-CSCF use SIP signaling to register their presence and subscribe for service (client-server), whereas the IBCF uses statically configured routing (peer-peer), such as DNS or ENUM (IETF RFC 3761). A single device may support both P-CSCF and IBCF modes, as both behaviors may be required, even over the same physical interface.

The current method of ensuring differentiated QoS in IMS networks is through two key network elements, namely the *Policy Decision Point* (PDP) and the *Policy Enforcement Point* (PEP). The PDP retrieves the necessary policy rules (flow parameters), in response to a RSVP message, which it then sends to the PEP. The PEP then executes these instructions. The *Policy Control Function* (PCF) associated with the P-CSCF plays the role of the PDP in IMS standards. The PEP resides in the

Gateway GPRS Support Node (GGSN) for mobile access or the module of RACF traffic control for next generation broadband access. In an IMS call flow, the SDP message is encapsulated within SIP and carries the QoS parameters. The PCF examines the parameters, retrieves appropriate policies and informs the PEP in the GGSN/RACS for the specific policy requirements associated with the traffic flow.

2.2 Media Gateways, Session Border Controllers (SBC) and Home Gateways

A *Session Border Controller* [7] implements the following signaling and control functions in the context of the IMS architecture: P-CSCF, IBCF, BGF and TrGW (*Translation Gateway*). The IBCF/TrGw provides the necessary functions for codec transcoding, when required by interworking agreement and session information, in order to establish communication between end points belonging to different IMS domains. The standardized border functions P-CSCF and IBCF form the signaling core of the *Access* and *Interconnect Session Border Controllers* (SBCs). They provide routing and authentication of the signaling, and communicate with devices within the IMS core over the standardized Mw (SIP) interface. SBCs are also required to support functions outside the IMS standards, such as *Denial-of-Service* protection and interworking with non-IMS devices. SBCs also allow operators to monitor and tune performance to meet agreed SLAs, tailor the service bundle to each customer with multi-level, fine-grained policy rules, facilitate services between incompatible equipment and through NATs and firewalls, and comply with legal regulations regarding privacy, reliability and lawful intercept.

The I-CSCF of the IMS architecture communicates with home networks after verifying user authentication by exchanging SIP messages with S-CSCF. *Home* IMS *Gateway* (HIGA) [11] uses client software to identify a user in an IMS network (ISIM/IP *Multimedia Services Identity Module*). It interworks with home DLNA (*Digital Living Network Alliance*) networks. DLNA networks support multimedia management in home networks. They define the following home servers and equipment: *Digital Media Servers* (DMS), *Digital Media Players* (DMP), *Digital Media Controllers* (DMC) and *Digital Media Renderers* (DMR).

2.3 End-to-End Flow Control Architecture

Sliced network resources such as dedicated paths may be defined in the context of *over-the-top* application models. Dedicated paths are defined either on a per flow basis or as aggregate trunks. Two main approaches are considered in establishing such paths: The multi-domain approach (or the so-called "*hard*" model) and the per domain approach (the so-called "*loose*" model). The data path is determined by some routing protocol on a *hop-by-hop* basis satisfying simple continuity *Per Hop Behavior* (PHB) for a deployment according to the "*loose*" model. The "*hard*" model establishes data paths a priori (see Fig. 4). There is no need of border router configuration via a resource allocator for the multi-domain case. Per flow CAC (*Connection Admission Control*) is done only in the access since the end-to-end path is well-known. Cooperation between all operators is required in order to build and maintain end-to-end paths - that do not scale easily - in order to accommodate more traffic. The per domain approach on the other hand is scalable and more flexible since each operator can merge and aggregate traffic from one path to another and may independently setup paths between border routers. Per flow CAC needs to be performed by each domain *Resource Manager* (RM) to verify the traffic entering in each BR-to-BR path. A *Resource Manager* (RM) is the key ingredient in building data paths. The RM configures the border router according to the required QoS parameters in the case of the "*loose*" model. The best intra-domain (AS) path is estimated and the routing table is updated after a communication between the *Resource Manager* and the border router. Each RM processes the QoS requirements and exchanges this information in the case of the "*hard*" model. The best AS path is computed and routing is enforced by means of tunnels between dedicated access resources after each RM has received all QoS requirements.

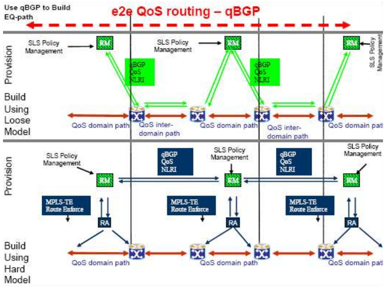

Fig. 4. Loose and hard forward models over multiple QoS domains

3 Traffic Control, Quality-of-Service (QoS) and Policy Considerations for Video-to-Video Delivery Over Heterogeneous Networks

Heterogeneous technologies as well as IP networks belonging to multiple AS (*Autonomous Systems*) may serve as access or transport layers in the context of NGN and IMS structured architecture. Metro Ethernet [12] may be used as an access network that aggregates user traffic from ADSL and VDSL DSLAMs (*Digital Subscriber Line Access Multiplexers*). On the other hand MPLS/MPLS-TP (IETF RFC 5654/5921/5960) supporting MPLS-TE IP networks (according to IETF RFC 4124/4125/4127: *Diffserv-aware* MPLS *Traffic Engineering*) may provide backbone networks for both fixed and mobile access. QoS path finding based on overlay topologies is not like traditional routing process since it is based on an overlay virtual topology described at inter-domain level. Together with the intra-domain QoS routing available inside each network domain one obtains end-to-end QoS routing paths. QoS routing in such cases is described in [13, 14]. Conventional intra-domain QoS routing protocols run on the routers and find paths with QoS constraints from source to destination. This approach does not offer an image of the available resources at the domain level. A centralized solution is better for mid-long term paths with QoS guarantees. This introduces a domain central manager having knowledge of the total resource allocation inside the domain. A dedicated module of the domain manager determines QoS routes between source and destination according to specific algorithms. Usually the QoS routing process is triggered by a new request addressed to the manager for a QoS path through the domain. One distinguishes between two approaches for inter-domain QoS routing as well. The first one proposes enhancements for the BGP protocol in order to support QoS features. The BGP advertises QoS related information between autonomous systems (AS), and the routing table is build taking into consideration this additional QoS information. The Q-BGP protocol is proposed in the MESCAL project [15]. The other approach of inter-domain QoS routing solutions is based on the overlay *Virtual Topology* (VT) solution, which abstracts each domain with a node, represented by the domain service manager, or with several nodes represented by the egress routers from that domain [16]. The VT is formed by a set of virtual links that map the current link state of the domain without showing internal details of the physical network topology. These solutions are based on an end-to-end QoS negotiation process. After the QoS path is found, the negotiation process is started. The QoS routing process performed in advance would increasing the chance of negotiation success. The overall process implies two QoS–related searching processes: building the QoS topology and secondly negotiation in order to reserve resources.

A two stage process while building *End-to-End Quality-of-Service Paths* is outlined as follows [17, 18] :

- **`Provisioning`**
- **`Invocation`**
- **`Operating and Maintenance (OAM)`**

Such an approach is adopted by the EuQoS consortium. The architectural framework described in [19] allows inter-domain *Traffic Engineering Label Switched Paths* (TE-LSPs) with guaranteed quality of service (QoS) to be setup. Such TE-LSPs, called EQ-links, are setup by coordinating path computation elements (PCEs) of neighboring autonomous systems (ASs) along a pre-determined inter-AS path, computed through cooperative interaction between pairs of neighboring ASs. IETF has standardized a backwards recursive algorithm (IETF RFC 5441: BRPC) in order to establish *End-to-End Quality-of-Service Paths* that initiate from the destination according to the proposed PCE architecture (as in IETF RFC 4655: PCE and in RFC 5376: *Inter-AS Requirements for* PCECP).

An alternative resource control mechanism that utilizes *Open Flow* switches is the *Generic-Adaptive-Resource-Control Function* (GARC). It extends 3GPP and non-3GPP architectures in order to introduce flexible QoS treatment. It guarantees a user demanded bandwidth of 40 kbps for VoIP calls over the internet. It is to be integrated as an additional component in the telco network operator plane with interfaces to application provider and UE directly. It allows QoS requests by static predefined lists or by dynamic and individual statements. It features granularity per single flow, per individual service, per type of service, per user profile, per device and per context. Charging is based on demanded QoS level per bearer, duration, volume of data traffic and number of service invocations.

4 Conclusion

The actual traffic processing in real internet deployments is still mostly best effort. *End-to-end Quality-of-Service* for multimedia flows over multi-domain heterogeneous environments involves initial provisioning - usually solved in the management plane - and subsequent monitoring and adjustments in the control plane (IntServ, Diffserv, TBAC etc). Combining intelligent cloud services with multimedia content requires synchronization between service and control in order to reserve network resources. Several resource control mechanisms that are defined in the context of such novel architectures as IMS and next generation IPTV models are presented in the context of this review paper. Interconnecting private clouds with *Over-The-Top* Service Application Platforms (EuQoS), MPLS-TE/IP tunnels and tunnel based aggregation control (TBAC/RSVP as in IETF RFC 4804), prioritized flow forwarding from specific reserved switching resources (*Open Flow* proposal), PCE architecture/SDN and specific network attachment control functions all offer distinct possible deployments whose effectiveness depends upon the installed infrastructure and the business model to be adopted for the cloud services by the provider.

Acknowledgments. The present work has been performed in the scope of the *LiveCity* ("*Live Video-to-Video Supporting Interactive City Infrastructure*") European Research Project and has been supported by the Commission of the European Communities - *Information Society and Media Directorate General* (FP7-ICT-PSP, Grant Agreement No.297291).

References

1. ETSI TS 183 060 V2.1.1. Resource and Admission Control Subsystem (RACS) (2009-04).
2. ITU-T Y.1910: IPTV functional architecture. http://www.itu.int/rec/T-REC-Y.1910-200809-I
3. ITU-T Y.1991: Terms and definitions for IPTV. http://www.itu.int/rec/T-REC-Y.1991-201003-P
4. Open IPTV Forum White Paper. http://www.oipf.org/docs/OIPF-T2-Whitepaper_V2_0.pdf (January 2009).
5. Open Networking Foundation (ONF). OpenFlow Switch Specification. http://www.opennetworking.org.
6. Sixth Framework Programme: http://cordis.europa.eu/fp6/whatisfp6.htm.
7. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 10): 3GPP TS 23.228 V10.1.0 (2010-6).
8. 3GPP TS 23.207 V9.0.0: End-to-end Quality of Service Concept and Architecture. Release 9 (2009-12).
9. 3GPP TR 23.802 V7.0.0: Architectural Enhancements for End-to-end Quality of Service (QoS). Release 7 SA2 (2005-09).
10. 3GPP TS 29.213 V9.3.0: Policy and Charging Control Signaling Flows and Quality of Service (QoS) parameter mapping. Release 9 (2010-06).
11. Home Gateway Initiative: http://www.homegatewayinitiative.org and ETSI TISPAN: http://www.etsi.org/tispan
12. Metro Ethernet Forum. http://metroethernetforum.org
13. Fabio, Verdi, L., Maurıcio, F.: Using Virtualization to Provide Interdomain QoS-enabled Routing, Journal of Networks. April 2007.
14. D. Griffin, J. Spencer, J. Griem, M. Boucadair, P. Morand, M. Howarth, N. Wang, G. Pavlou, A. Asgari, P. Georgatso: Interdomain routing through QoS-class planes, Communications Magazine, IEEE, Feb.2007.
15. E. Borcoci, A. Asgari, N. Butler, T. Ahmed, A. Mehaoua, G. Kourmentzas, S. Eccles, 2005 Service Management for End-to-End QoS Multimedia Content Delivery in Heterogeneous Environment, AICT Conference Proceedings, July 2005, Lisbon.
16. Fabio L. Verdi, F. Maurıcio, 2007 Magalhaes Using Virtualization to Provide Interdomain QoS-enabled Routing, Journal of Networks, April 2007
17. *eTOM Solution Suite*. http://www.tmforum.org
18. EuQoS consortium. http://www.euqos.org
19. Braun, T., Diaz, M., Gabeiras, J. E., Staub, Th.: End-to-End Quality of Service Over Heterogeneous Networks. Springer, ISBN: 978-3-540-79119-5.