# An Improved Model for Next Generation Networks with Guaranteed End-to-End Quality of Service

Cherif Ghazel and Leila Saïdane
The National School of Computer Sciences.
University of Manouba - Tunisia
E-mail: {Cherif.Ghazel@Email.ati.tn, Leila.Saidane@Ensi.rnu.tn}

*Abstract* - **The quality of service (QoS) in the Next Generation Networks (NGN) has been of a particular interest to researchers, system designers, standardization organizations and various industries affected by these networks. In this paper, we propose and outline a control and signalling model which guarantees an end-to-end QoS for multi-service traffics in the NGN networks based on IP/MPLS transport. This work is based on previous works of various standardization bodies such as PacketCable, 3GPP, ETSI, MSF, and ITU-T. The proposed model treats the RACM as a basis component for a large scale QoS guarantee architecture. A key aspect of this model lies in its capacity to integrate the MPLS traffics engineering which offers a scalability and resilience to the transport network and guarantees the requested QoS.**

## I. Introduction

In spite of their numerous practical advantages, the NGN are not without limitations. The main deficiency of the modern NGN model lies in the fact that it may not sufficiently guarantee an end-to-end QoS for multi-service traffics. Consequently, current NGN networks may require more advanced control mechanisms in the control and transport levels to overcome some of these deficiencies. In particular, the QoS signalling and control structure of the current NGN model is the aspect that requires improvement to harmonize the QoS needs with the network capacity. In this work, we propose an alternative NGN model which provides the desired improvement to satisfy the QoS requirements.

Currently, the QoS signalling and the NGN networks control solutions are still at the development stages. PacketCable, which supports QoS in packet-based cable access networks for telephony services, proposed a QoS solution, as outlined in [1]. This solution focuses mainly on some specific problems related to packet-based cable access networks. Similarly, the 3GPP also proposed an end-to-end QoS solution for the 3rd generation mobile networks, as described in [2]. It was developed for specific category of networks and lacks several functionalities that can be deemed necessary for a standard NGN QoS model (core network resource control, topology knowledge, path selection, etc.). Also, the choice of Diameter protocol for Gq interface must be more argued for what this protocol is generally used to perform resource reservation requests. Unlike what has been represented in [1], our proposed model splits the call management and gate control functionalities into Call Server (CS) and Resource and Admission Control Manager (RACM) in order to apply call admission control (CAC), reach reliable and accurate resource management and improve the transport network scalability and resilience. Furthermore, it decomposes the RACM into distinct Service Policy Decision Manager (SPDM) and Transport Resource Control Manager (TRCM) entities in order to enable the coverage of large domains. The proposed model also takes into account different QoS negotiation capabilities for various categories of User Equipments (UE). It presents methods for call admission and resource based QoS control, Network Address Port Translation (NAPT) control and subscriber mobility management and control. In order to guarantee the QoS requirements, while at the same time maintaining fair and high utilization of transport resources, a scheme for resource management is proposed. This scheme is based specifically on the concepts of resource reservation and allocation during admission, MPLS-Tunnelling, call admission control, traffic aggregation, traffic engineering (TE) and fast rerouting (FRR). Moreover, we will define the necessary interfaces and attempt to fix the corresponding open and mature standards for this purpose.

The organization of this paper follows a standard methodology of development in five sections. The first section outlines the need in term of QoS for the NGN multi-service traffics. The architecture of the QoS model, where we describe the end-to-end QoS control and signalling model as well as define the communication interfaces and the architecture components, is outlined in second section. The third section is dedicated to the resource management in NGN transport network and the MPLS contribution in the improvement of the QoS. In the fourth section, the call admission and resource based QoS control, the application of NAPT control and the subscriber mobility management and control are described. Brief summary and concluding remarks are presented in the last section where some additional future works and directions are also outlined.

## II. NGN Traffics Requirements in Terms of QoS

Once a call is accepted by the call control mechanisms and is assigned the necessary resources, it should be kept and established with the required QoS [3]. The established calls must be protected from network disruptions caused by abrupt overloads and traffic re-routing. In order to protect the network capacity and the established calls, the network must be equipped with mechanisms for resource-based admission control. It shall also support a large number of busy-hour call attempts and offer acceptable call setup latency. Mechanisms that guarantee the emergency call setup, ensure call pre-emption and offer a specific treatment for the priority calls are also required, as in [4]. The network must be protected from attacks, theft of services and illegal access to resources.

## III. NGN QoS Architecture Model

The proposed NGN model defines the QoS signalling and control framework for an end-to-end QoS through the originating, transit and terminating architectures that an operator can play. This model exploits, to a certain extent, the SIP control and signalling model, as in [5]. It also addresses the admission control policy architecture, as in [6]. The core network is based on IP/MPLS which offers a QoS guarantee for traffic aggregations. The deployment of DiffServ offers QoS improvement and traffic classification. The traffic policies in the transport data plane are ensured by the DiffServ and MPLS integration QoS mechanisms. The choice of IntServ in the access level, offers a strict resources reservation and better QoS guarantee. The resource allocation is going to be applied in two phases: The first consists of resource authorization and reservation at the call initialization while the second resides in resource commitment once the physical path is established. This two-phase resource control scheme is suitable for interactive applications, which require performance and transport resources availability. The reserved resource can be used for transporting *best effort* traffics. The resulting architecture illustrated in Figure 1 is proposed mainly for large scale networks with multiple domains. It addresses different QoS requirements of multiservice high load traffics generated by various categories of users. The evaluation of the defined model will appear in further works.

### *A. Functional entity descriptions*

The functionalities of the different QoS components presented in the architecture depicted in Figure 1 are defined in the following subsections:

*1) Originating User (OU):* This is an application installed at the calling user's terminal which instigates the service request and asks for the establishment of end-to-end calls, as in [7]. It may support the multimedia sessions and the video-conferencing. Depending on the type of the utilized terminal, it negotiates the QoS in the control or the transport levels at service setup, as in [1], [2] and [8].

*2) Originating Call Server (CS-Orig):* Performs the call signalling control functions and identifies the originating and terminating points in the network [9]. It controls the calling user's authentication and authorization based on information bound to the call as well as other aspects indicated in the user's Service Level Agreement (SLA). It determines whether the user is permitted to establish a call with the specified QoS, as in [7]. It treats the end-to-end QoS signalling by consulting the RACMs and determines if the current policy guarantees the required QoS. Accordingly, it rejects or initializes the call towards the destination address. The Call Control and Signalling Function (CCSF) and the QoS Control and Policy Function (QCPF) represent the main functions offered by this entity. They intervene in the QoS control and guarantee.

*3) Transit Call Server (CS-Tr):* Provides the call signalling control and treatment functions in order to guarantee the requested QoS in the transit level. It routes any incoming call towards the terminating CS and informs it of its required QoS, as described in [7]. In practice, the transit level does not need to install a CS-Tr except if it directly service attached end users belonging to its domain.

*4) Terminating Call Server (CS-Term):* Provides the call signalling control and treatment functions in order to guarantee the specified QoS in the terminating level. It also routes the incoming call towards its destination (called user) and informs him of the associated QoS, as outlined in [7].

*5) Originating Resources and Admission Control Manager (RACM-Orig):* Provides the required QoS on the transport level. In accordance with the NGN concept, the RACM separates the call control functions from the specific transport functions. It permits the exchange of the QoS signalling between the control and the transport interfaces. It ensures the authorization, reservation, commitment and release of network resources as well as the incoming call admission control [8]. It also identifies and addresses problems in the transport level, installs the appropriate policies and control mechanisms in nodes. It decides whether it is necessary to modify some resources in order to preserve QoS for the established calls. It ensures the pre-emption of low priority traffics to the benefit of high priority traffics and interrupts calls that did not respect traffic parameters. It ensures the NAPT control and applies firewalls in order to secure network resource [10]. In practice, it consists of two functional entities: the SPDM and the TRCM. This decomposition offers a better scalability and robustness and enables the coverage of large core networks. Note that, in this work, we suppose that a RACM may cover a domain, a TRCM may cover a sub domain and an NGN network may cover multiple domains.

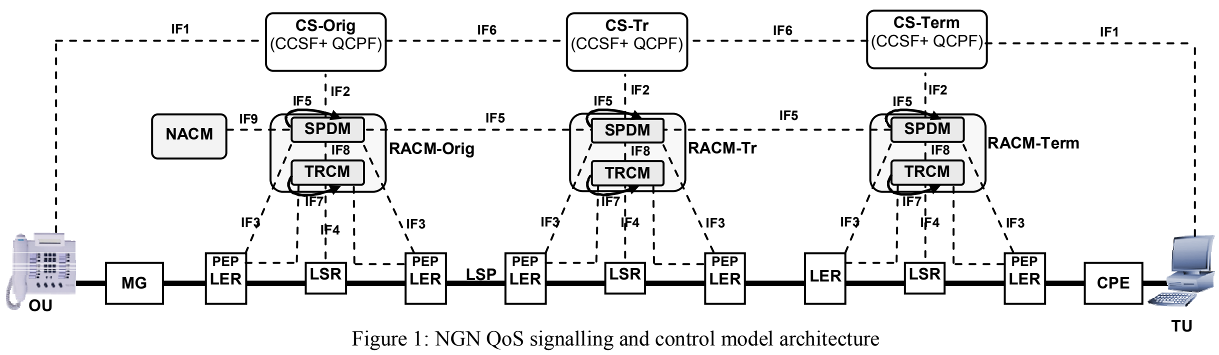


Figure 1: NGN QoS signalling and control model architecture

*The SPDM*: Provides a single contact point and hides the transport network details to the CS and is independent of the transport technology. The policy rules used by the SPDM are service-based. It makes the final decision regarding the network resource and admission control based on network policy rules, SLAs, service information provided by the CS, transport subscription information provided by the NACM and resource-based admission decisions and resource availability state offered by the TRCMs [4]. It also maps the service QoS parameters and priority received from the CS to network QoS parameters and classes based on the network policy rules. The SPDM controls gates in the Policy Enforcement Points (PEP) at per flow basis and installs appropriate policies to control the call flow [9]. It requests the TRCM instances to determine the necessary QoS resource along the media flow path. In practice, one SPDM may control all or a subset of LERs belonging to the same domain.

*The TRCM*: Provides the resource based-admission control decisions to the SPDM and is dependent of the transport technology. It maps the network QoS parameters and classes received from the SPDM to transport QoS parameters and classes based on transport policy rules. Each TRCM establishes aggregated physical paths for supporting the requested QoS between end points in its sub domain. The TRCM maintains the network topology and keeps track of the transport resource occupation status. It determines the resource-based admission control based on transport network information such as the topology, resource availability and the transport subscription information [10].

*6) Transit Resources and Admission Control Manager (RACM-Tr):* Ensures the QoS guarantee and coordination functions in the transit domain to the profit of the RACM-Orig. It establishes physical connections and ensures resource provisions relative to the specified QoS and forwards the call toward the RACM-Term, as in [7] and [9]. It consists of two functional entities: the SPDM and the TRCM. Some of these functionalities are similar to those of the RACM-Orig.

*7) Terminating Resources and Admission Control Manager (RACM-Term):* Serves the called user and ensures the QoS guarantee and coordination functions in the termination domain to the benefit of the RACM-Orig. It also establishes physical connections and ensures resource provisions relative to the requested QoS. It consists of two functional entities: the SPDM and the TRCM. Some of these functionalities are similar to those of the RACM-Orig.

*8) Edge Router:* Provides the border functions offered by DiffServ and MPLS and applies the appropriate policies per individual flow basis. It executes the edge control and security functions based on the defined QoS classes to enable compliant flow to use the network resources. It also informs the RACM of the established connection status changes. It applies the CAC, gate control, resource allocation and pre-emption, NAPT, session information collection and QoS mapping. The RACM connects to the edge routers to execute the flow control procedures and select traffic paths, as in [9].

*9) Core Router:* Ensures the routing and forwarding, in differentiated mode, of large volume of aggregated traffics through the core network and applies DiffServ and MPLS functionalities. These routers support separate internal traffic queues per DiffServ class to differentiate traffics in different QoS classes. They inform the RACM of the established call status changes occurred in the core level. The RACM connects to the core routers to determine the network topology, ensure tunnel provision, modify resource allocations, address problems, apply QoS guarantee rules, collect information on the resource reservation state and select paths, as in [3] and [9].

*10) Terminating User (TU):* An application installed in the called user terminal which terminates the service request. It accepts the call with the specified end-to-end QoS, as in [7].

*11) Network Attachment control Manager (NACM):* Consists of a collection of functional entities that provide a variety of functions for user access network management and configuration based on user profile. It includes network access registration, authentication, authorization and configuration parameters. It manages the IP address space of the access network and ensures a dynamic provision and allocation of IP address (DHCP mode). The NACM ensures the user location management, announces the contact point to the UE and initialize it for accessing the NGN services [10].

### *B. Communication interfaces*

One of the key elements is the definition of the interfaces and the corresponding protocols between the different functional entities. Therefore, we consider each interface indicated in the architecture defined in Figure 1 and analyze the role and identify the appropriate protocol for it.

*1) Interface IF1:* The intra domain IF1 interface exists between the calling user and the CS. It is used for the call signalling establishment and terminal synchronization [1]. It ensures the transport of the QoS control signalling messages. SIP is considered the suitable protocol for this interface.

*2) Interface IF2:* The intra domain IF2 interface exists between the CS and the RACM and is used to perform the call control functions. Its role is to separate the call control functions bound to the CS from the specific functions bound to the RACM [3]. It is used by the CS to send the session establishment information to the RACM which translate them into physical establishment decisions. The call control level use this interface to reserve bandwidth between two end points, ensure the QoS control, apply priority and gather information on the resource usage. It is also used to exchange information regarding the resource authorization, reservation, commitment and liberation. It permits the RACM to exchange control information with the CS relating to the undergoing calls, the resource synchronization, the NAPT, the Firewall application, the overload and failure event recovery. According to the model usage orientation, there are several protocols that can be suitable for this interface such as: SIP, COPS and NRCP.

*3) Interface IF3:* The intra domain IF3 interface, which firmly depends on transport technologies, is established between the LER and the RACM (with the SPDM). It allows the RACM to control the edge routers on a per call basis [3]. The RACM uses IF3 to push the CAC decision, reserve and commute resources, update its resource database, ask for authorized QoS and control gates. Through this interface, the

RACM imposes label stacks in the edge level in order to define the session path. It allows the RACM to allocate the QoS mechanisms [10] and to enforce QoS constraints to the established sessions. It permits the RACM to control QoS, collect information on resource usage and apply NAPT in the LERs [8]. It allows the LER to request information bound to the established sessions, and to inform the RACM of any reserved resource or network topology changes. It authorizes the RACM to control the network failure and to intervene for maintenance. The mature protocols for this interface are: H.248 and COPS. Except that, H.248 supports an MPLS package which allows label stacks to be pushed to the edge nodes in order to initiate tunnels. It also offers better traffic management and conditioning in the Edge level.

*4) Interface IF4:* The intra domain IF4 interface is implemented between the LSR and the RACM (with the TRCM). It is used for the control of functional entities in the IP/MPLS core network. It allows the RACMs to establish, release and modify bandwidth for traffic aggregations within DiffServ QoS classes. The network elements use this interface to inform the RACMs of resource reservation state and changes occurred during current sessions as well as to reject demands while being based on the TE-tunnels occupation state. It permits the RACMs to collect information on network topology [10], reservation state, traffic routing, network failure and tunnel management. The selected protocol for this interface shall depend firmly on the IP/MPLS transport technology [3]. The H.248 protocol supports an MPLS package that allows the RACM to impose label stacks in the transport level in order to manage tunnels. It also offers a package for the NAT traversal as well as a mechanism allowing the RACM to recover from failure situations [9].

*5) Interface IF5:* The inter domain IF5 interface which links the RACMs (inter SPDMs), is necessary when two or more RACMs need to interact directly without the CS control in order to determine the QoS resource along the call path. In such case, it may be possible when two NGN domains, each controlled by a CS, need to exchange traffics through a transit domain controlled exclusively by a RACM [3]. Furthermore, in order to ensure scalability in networks with multiple domains, it is necessary to implement multiple RACMs; each one controls a network domain. The interaction between these RACMs restricts the contact of the CS to a single RACM and decreases the call handling load [9]. For a session, the signalling path may not be associated with the data path and generally only the CS in the originating and terminating domains are involved in the control signalling. Accordingly, it could be difficult for a CS to identify the call path details and the transport resource status to determine the requested QoS resource. Therefore, the transit RACMs need to establish their own connections and process the QoS signalling. In addition, for scalability inside large domains, multiple SPDMs may be deployed; each one handles a subset of LERs and interacts with others SPDMs over IF5 to guarantee QoS. This interface may also be used to exchange MPLS label stacks and additional parameters to establish MPLS tunnels and Label Switching Paths (LSP), as in [9]. Since, the IF2 and IF5 have similar functionalities, we decided to select for IF5 the same protocols defined for IF2.

*6) Interface IF6:* The inter domain IF6 interface exists between CS. It ensures peer to peer call control and signalling exchanges. The protocol selected for this interface is SIP.

*7) Interface IF7:* The intra domain IF7 interface exists between the TRCMs. Since a domain may have multiple sub domains, it may deploy multiple TRCM instances, each one controls a sub domain [9]. For large domains, some intermediate sub domains may not have SPDMs and they only ensure the transport functions. Accordingly, a SPDM has no knowledge of the media flow path details and the transport resource status. Hence, it is necessary to use multiple TRCMs within the same domain which interact via IF7 to determine the requested QoS resources. This interaction between multiple TRCMs enables the SPDM to only contact a single TRCM. Because of the majority of functionalities provided by IF7 are similar to those of IF2, we decided to use the same protocols defined for IF2 for this interface.

*8) Interface IF8:* The intra domain IF8 interface provides interaction between the SPDM and the TRCM to determine the requested QoS resource reservation in the involved core domain along the media flow path [8]. Via IF8, the SPDM requests the TRCM entities to determine the specified QoS resource or to retrieve the path selection information. The TRCM uses this interface to provide the resource reservation tracking and the resource based admission control. Since, the IF8 and IF2 have similar functionalities; we decided to select the same protocols defined for IF2 for this interface as well.

*9) Interface IF9:* The intra domain IF9 interface provides interaction between the SPDM and the NACM for checking on the transport subscription and information binding. It is used for retrieving the access transport subscription and configuration information to locate the access transport network for UE and to perform resource based admission control. A convenient protocol for this interface that enables the exchange of the transport subscription and information binding and IP session connectivity is Diameter, as in [11].

### *C. Resource control and allocation management*

In the same context of the QoS model previously presented, we discuss the resource control and allocation management. The RACM entity, which represents the main component in this issue determines the resource availability, the network topology and performs the CAC procedures. In practice, this component takes a distributed or hierarchical architecture. It communicates with edge and border routers to perform the flow control procedures and select flow paths. It connects with core routers in order to reserve resources for traffic aggregations, collect information on resource reservation states, apply QoS guarantee rules, discover the IP/MPLS core network topology and manage TE-tunnels. The transport network partitioning and TE-tunnels provisioning simplify the application of the CAC and ensure an enhanced resource management. The RACM determines the transport network topology by participating in the traffic routing using protocols such as OSPF-TE which supplies the transport network information to the control plane. This may also be ensured by receiving information sent by the core routers concerning the routing tables, the link and node states as well as the used traffic QoS management mechanisms. The RACMs interact to exchange information regarding the resource reservations, the selected local and transit MPLS LSPs and the QoS control.

### C.1. RACMs architecture

The flexibility of the proposed architecture offers the RACM the possibility to be deployed in different structures in order to provide high performance, scalability and resilience to large network domains. Firstly, as depicted in Figure 2, a RACM can be implemented in a hierarchical structure. In this case, the SPDMs in the top level of the hierarchy reserve resources from the TRCMs in the sub level of the hierarchy and apply the CAC in the Edge level. Secondly, as depicted in Figure 3, a RACM can also be represented in a peering structure. In this architecture, the SPDMs are implemented in the border of the RACM. They reserve resources from the peering TRCMs and apply the CAC in the Edge level. In the two cases, the edge SPDM offers a single contact point to the CS, hides details of the transport network, identifies the sub domains that the session path is going to cross and requests resource from its peering SPDMs of adjacent domains. They decreases the CS load relative to the traffic routing and distribution, the resource reservation, the topology discovery, the QoS control and the call path selection. The TRCMs are responsible of the resource control and management in the different sub domains. They interact to ensure the resource provision along the call path [9]. In the same domain, the multiple TRCMs directly communicate via the IF7 interface. However, in different domains they interact indirectly through the SPDM instances. Note that, the deployment of multiple SPDMs scales the reservation request load and the deployment of multiple TRCMs offers scalability, robustness in large domain and scales the resource reservation load.

*1) Hierarchical architecture:* In this architecture, a SPDM instance may interact with multiple TRCM instances and a TRCM instance may interact with multiple SPDM instances to satisfy the QoS resource requirements from edge to edge in the involved domain [9]. The TRCMs receive reservation requests from SPDMs and apply resource reservation and allocation control to sub domains based on resource availability states. They interact with the SPDMs in order to share the domain resources and reserve bandwidth aggregations. The SPDM ensures the CAC based on the resource occupation state received from the TRCMs.

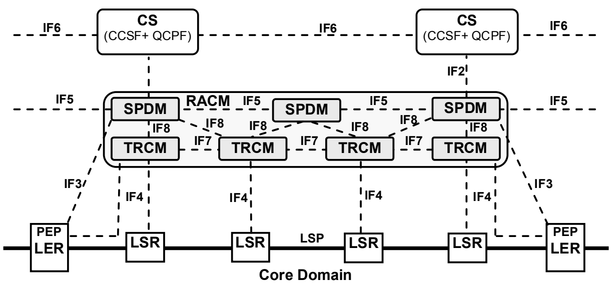


Figure 2: Hierarchical Architecture

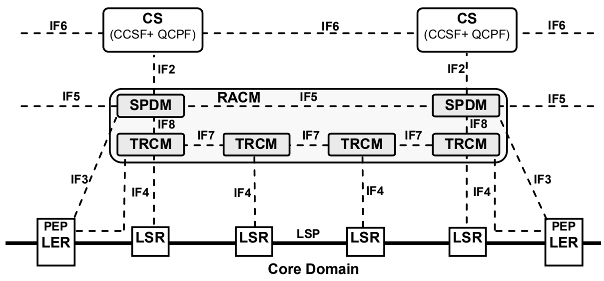


Figure 3: Peer to peer Architecture

*2) Peer to peer architecture:* In this architecture, the SPDMs and the peering TRCMs are implemented respectively in the borders and the core domains. The SPDM may communicate on equal terms with the SPDMs of adjacent domains and with the first TRCM of the peering TRCMs of its domain. It identifies the TRCMs of the adjacent sub domains that the session crosses. The first TRCM instance interacts with its neighbouring TRCMs to detect and determine the requested edge to edge QoS resource in the involved domain. They assign bandwidth aggregations along the adjacent sub domains.

### C.2. Resource control and allocation in the IP/MPLS level

The proposed NGN QoS model depends firmly on the transport network capacity and technology. As a result, this model is mainly based on open standards formed by DiffServ and MPLS in an IP environment. The use of IP/MPLS as transport technologies is justified by its simplicity, the QoS guarantee and the offered performances features such as: TE, FRR, VPN, unit-cast and multi-cast routing, security, etc.

Currently, MPLS traffic engineering provides the better approach for applying a rigorous QoS in IP packet switched networks. The use of the RACMs associated with MPLS-TE solves problems regarding the traffic routing and the network scalability and simplifies the core network complexity to a set of tunnels. These tunnels can be instantiated in the edge and the core network by the RACMs. For this aim, the RACMs exchange information concerning the resource reservation state, the local and transit LSP occupation state and the MPLS label stacks. Accordingly, the bandwidth management in the core network may be accomplished, through an equitable sharing of the available bandwidth between a pool of MPLS TE-tunnels which may be solicited by the RACMs to assign bandwidth to the authorized sessions.

This use of the TE-tunnels associated with the RACMs, may be consolidated by existing effective techniques which improve the core network scalability by offering more efficient bandwidth allocation and ensuring an accurate resource sharing. Such techniques include the Edge to edge TE-tunnels with differentiation class of services, the Hierarchical TE-tunnels with differentiation class of services and Hierarchical bandwidth tunnels, as in [9].

It is also possible to avoid the transient congestion problems due to network element failures and unexpected reserved resource degradations and sudden traffic variation, by using MPLS TE-tunnels with FRR and specified bandwidths in order to protect real time services, as in [12].

*D. Call admission and resource based QoS control*

This model defines a scheme using the push mode for the QoS resource and admission control which takes into account the different QoS negotiation capabilities of diverse UE:

1. The UE sends a service request to the CS. Depending on the used UE; the demand may or may not specify the QoS parameters in the transport or service level.
2. The CS processes the demand of service as well as the QoS associated parameters, and sends a QoS resource authorization and reservation request containing the requested QoS parameters to the RACM.
3. The RACM executes the admission and authorization controls based on the policy rules, resource based admission decision and transport subscription profile. If the demand is granted, the RACM enables an access gate and applies the traffic control rules in the Edge level and the bandwidth allocation in the transport level. The gate will be committed by the RACM, in response to an instruction from the CS, when the call has reached a state where the media path should be opened [9]. This results in previously reserved resources being opened by sending an instruction from the RACM to the edge node.

*E. Network address and port translation*

In order to mask the network addresses between different sub networks and use private addresses to remedy the lack of public addresses or to protect the customer promise networks, the use of NAPT is necessary. The RACM interacts with the CS and the transport entities in order to execute the NAPT control and the NAT traversal as follows [10]:

1. The CS modifies the address and the port in the session signalling messages to reflect the port and address binding performed in the transport edge level.
2. The RACM gets the port and address binding information and performs the NAPT control during the lifetime of the session. Thus, it interacts with the CS for the session signalling message modification and with the edge router to collect information bound to the network address and port translations.
3. The edge router applies the NAPT by modifying the session packet port and address values.

*F. Subscriber mobility management and control*

In the proposed model, the user's mobility may be ensured firstly by using SIP protocol. The calling user localizes the SIP server which will be the destination of its invitation message. The server either knows the physical address of the called user, or redirects the request toward another server. Since SIP points to a server and not to the user's terminals, this offers a flexible mobility and relieves DNS servers which need to know only the server's address and not the terminal addresses. The usage of DHCP mode for session initiation offers more flexibility in address allocation.

The user's mobility can also be offered by using of NACM functionalities associated with DHCP mode. After successful authentication procedures, the UE initiates a DHCP request for demanding an IP address. This request is then relayed to the NACM which operates as a DHCP server. The latter treats the request and informs the UE that an IP address is allocated. Thereafter, the NACM pushes the binding information to the RACM via the IF9 interface in order to perform access rules on the relevant UE in the Edge level.

## IV. CONCLUSION

In this paper, we proposed a model-based QoS architecture which guarantees the necessary QoS for the transport of multiservice traffics and real time flow in the next generation networks. This end-to-end QoS control and signalling structure is based mainly on the QoS signalling and control architecture. The choice of DiffServ, IP and MPLS protocols in the transport level offers scalability, reliability, and high performance. It also forces operators to use existing mature protocols. This model uses RACM as a basis component for a large scale QoS guarantee architecture. It is based on DiffServ, MPLS and native IP networks, and can even support DiffServ and IPv6 environments. A key aspect of this model is its capacity to integrate the MPLS traffics engineering which offers a scalability and resilience to the transport network and guarantees the requested QoS.

Our on-going work focuses on the complementary survey and further investigation and enhancement of the next issues:

1. Ensuring the evaluation of the defined model architecture.
2. Defining a more advanced and adequate standard between the transport and the control levels.
3. Surveying the selected protocol interpretabilities for different interfaces.

## REFERENCES


[1] PacketCable™ 1.5 Specifications PK-TSP-DQOS1.5-I02-050812, "Dynamic Quality-of-Service", PacketCable, August 2005.

[2] 3GPP TS 23.207, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; End-to-end Quality of Service (QoS) concept and architecture", 3GPP, September 2004.

[3] C. Gallon and O. Schelén, "Quality of Service for Next Generation Voice Over IP Networks", MultiService Forum, February 2003.

[4] ITU-T Recommendation Y.2171, "Admission control priority levels in Next Generation Networks".

[5] R. Yavatkar, D. Pendarakis and R. Guerin, "A Framework for Policy-based Admission Control", IETF RFC 2753, January 2000.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002

[7] ETSI TS 102 024-3 V4.1.1, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; End-to-end Quality of Service in TIPHON Systems; Part 3: Signalling and Control of end-to-end Quality of Service", ETSI, January 2003.

[8] ETSI ES 282 003 V1.1.1, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture", ETSI, June 2006.

[9] C. Gallon and O. Schelén, "Bandwidth Management in Next Generation Packet Networks", MultiService Forum, August 2005.

[10] ITU-T Recommendation Y.2012, "Functional requirements and architecture of the NGN".

[11] ETSI ES 283 034 V1.2.0, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol", ETSI, March 2007.

[12] J. Evans, "Network Engineering to Support the Bandwidth Manager Architecture", MultiService Forum, May 2006.