# Adaptive Quality of Service Management for Next Generation Residential Gateways

Iván Vidal, Jaime García, Francisco Valera, Ignacio Soto, and Arturo Azcorra

Universidad Carlos III de Madrid
Avda. Universidad 30, 28911 Leganes - Madrid, Spain
{ividal, jgr, fvalera, isoto, azcorra}@it.uc3m.es

**Abstract.** The TISPAN workgroup inside ETSI is currently working on accommodating the IMS (IP Multimedia Subsystem) architecture, which has been created for the mobile world, to the fixed scenario where there is a new important element to be taken into account: the Residential Gateway (RGW). This element is typically considered as a customer device where providers do not usually have anything to configure. However, in order to achieve real end-to-end Quality of Service (QoS) this cannot be true anymore.

This paper focuses on the way that a RGW is capable of configuring itself (an interface with the providers is also available), regarding Quality of Service parameters, into a Next Generation Network (NGN) scenario. The proposed RGW architecture is also flexible enough so as to adapt the QoS management mechanism to different possible scenarios, e.g. configured by the provider, by the customer or even autoconfigured by the RGW itself. A specific scenario, where a RGW is deployed in the TISPAN NGN architecture, will be explained and validated to proof the concept of the RGW architecture.

## 1 Introduction

Nowadays a lot of work around Next Generation Networks (NGN) has been done by the scientific community to achieve a real integration of every access technology actually deployed to provide triple-play services (video, data and voice). This work is still unfinished due to the high complexity of the problem and there are in fact many initiatives in progress. ETSI TISPAN is one of them and its philosophy is to try to conjugate different standards together and improve them to be fully compatible with the NGN architecture. The TISPAN defined what a NGN is in [1]:

> "A Next Generation Network is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service related functions are independent from underlying transport related technologies. It offers unrestricted access by users to different service providers. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users."

As a result of the ongoing work, the first release for TISPAN Next Generation Network (NGN) [2] was published at the beginning of 2006. The core network of TISPAN NGN is based upon the IMS, as defined in 3GPP Release 6 and 3GPP2 revision A for IP-based multimedia applications (although IMS is conceptually designed to be independent from the technology used in the access network, the standards developed by the 3GPP from release 5 are mainly focused on the UMTS IP connectivity access network). Due to this decision, TISPAN architecture obtains many advantages from merging both wireless and wired worlds because the only need fact is an IMS adaptation to the fixed world. But this work is not an easy task and a lot of discussions are still open. One of these discussions is related with the RGW configuration, because in the mobile world this entity does not exist. To date, there is no way to remotely configure the RGW QoS parameters by a NGN operator so there is still a gap in the architecture. Actually, the RGW is considered by the TISPAN as a customer equipment with no logical interfaces towards the network so as to be able to configure it. In this paper a flexible RGW architecture is proposed allowing the own gateway to autoconfigure itself using the signalling interchanged by the customer devices and the network. This architecture extends and demonstrate the concepts published in a previous work [3] where just the basic functionality was described, in order to explain the work developed in the MUSE European Project [4] where the main goal is to research the European next generation network. In MUSE the RGW is considered a key component and an entire Task Force is focused in its study and definition.

The rest of this article is organised as follows. The TISPAN NGN QoS management architecture is reviewed in next Sect. 2. The complete RGW architecture is proposed in Sect. 3 while the particular part where the QoS autoconfiguration is extended is analysed in Sect. 4. Section 5 concludes the article with the main contributions of this work.

## 2    TISPAN NGN QoS Management Overview

In this section, just a brief overview of TISPAN NGN QoS management is presented. The functional architecture of TISPAN NGN in release 1 is described in detail in [5] and the rest of the article follows the terminology defined by TISPAN. Figure 1 covers a simplified overview of this architecture to facilitate the reading of this document.

### 2.1    Resource and Admission Control in TISPAN NGN

The Resource and Adsmission Control Subsystem (**RACS**) is the TISPAN NGN subsystem that provides QoS reservation mechanisms over the transport layer. In this way, RACS provides the ASFs and the Service Control Subsystems with means to request and reserve resources from the transport networks which are under its control.
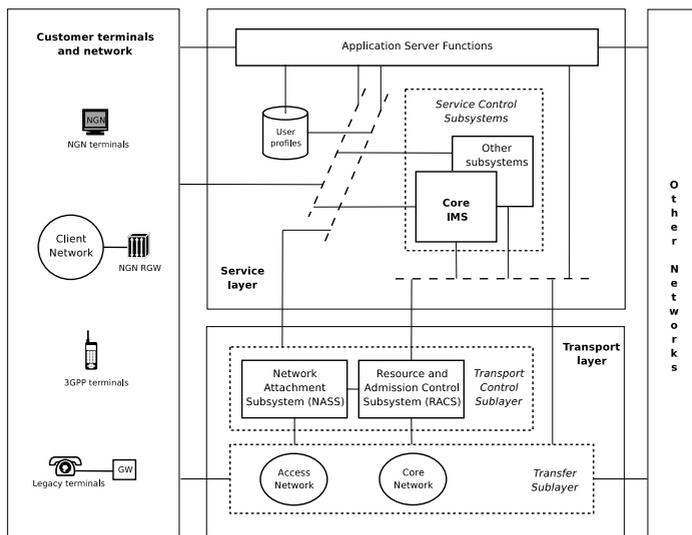
**Fig. 1.** Functional architecture of TISPAN NGN, release 1

On the other hand, in the NGN scope, the access network is viewed as the most critical segment to provide end-to-end QoS. For this reason, Release 1 of TISPAN NGN is mainly focused on this segment of the transport network in respect to QoS provision, assuming that QoS in the Core Network is provided by other means.

Therefore, RACS scope in TISPAN NGN Release 1 is limited to the access network, to the interconnection point between the access network and the Core Network and to the interconnection point between Core Networks. The release does not require the RACS subsystem to cover the Core Network itself or any equipment located in client premises.

The basic RACS functionalities in TISPAN NGN are indicated below:

- **Policy Control.** RACS applies to resource reservation requests a set of policy rules to check if these requests can be authorised and to determine how must they be served. Policy control is also performed in the access network, applying network policies specific to each particular access line.
- **Admission Control.** RACS verifies the authorisation to reserve resources on the access network based on user profiles, the access network policies and the resource availability.
- **Resource reservation.** RACS provides the means to reserve bearer resources on the access network.
- **NAT/Gate Control.** RACS controls NAT and NAT-T functionalities and performs gate control functions, at the limit between the access and the core networks and in the limit between core networks.

So, RACS provides the Service Layer with a single interface to request transport control services, acting as an intermediary between the service layer entities

(ASFs and Service Control Subsystems) and the functional entities in the transfer sublayer. In this way, RACS ensures that service layer entities do not need to be concerned with transport network details, like the topology and transmission technologies.

In addition, the RACS subsystem supports a *QoS Push Model* for the transport control service requests, where the resource reservation requests are "pushed" from ASFs and service control subsystems to RACS. If the requests can be satisfied, RACS "pushes" the requests to the transport layer to reserve the resources.

Finally, RACS supports several modes of operation in respect to resource management, two of which are explained below:

- A Reserve-commit resource management schema, where resources are reserved in a first phase and are finally made available after a commit procedure.
- A single-stage resource management schema, where reservation and commit procedures are performed at the same time.

**QoS Control Models.** The RACS subsystem supports two different models for QoS control over the transport network. These models are the following:

- **Guaranteed QoS.** In this model the QoS is guaranteed with absolute bounds on some or all of its parameters, like throughput or jitter. Guaranteed QoS is configured on the access network with the application of techniques such as throughput control and traffic policing in the IP edge node. These techniques may also be applied to the Access Node or to the equipments in the client premises.
- **Relative QoS.** In this model the QoS is provided by class based differentiation. This QoS differentiation is configured in the IP edge node of the access network, where functionalities like packet marking are provided. RACS should be aware that some equipment in the client premises may also provide QoS differentiation, for example through packet marking. This marking should only have effect if it is required by the operator.

**RACS Functional Architecture.** Figure 2 shows the functional architecture of the RACS subsystem.

The Application Function (**AF**) interacts with the RACS subsystem to request transport-layer control services for QoS provisioning to services. This function is implemented in some functional entities from the service layer, such as the ASF and the P-CSCF of the Core IMS. The AF converts QoS information from the application layer to QoS information which is suitable for the RACS subsystem, and includes this information in a request message, which is sent to the SPDF through the Gq' interface. The details of the protocol used in the interface Gq' are specified in [6].

The Service Policy Decision Function (**SPDF**) authorises the request, checking the information contained on it against the local policy established for the
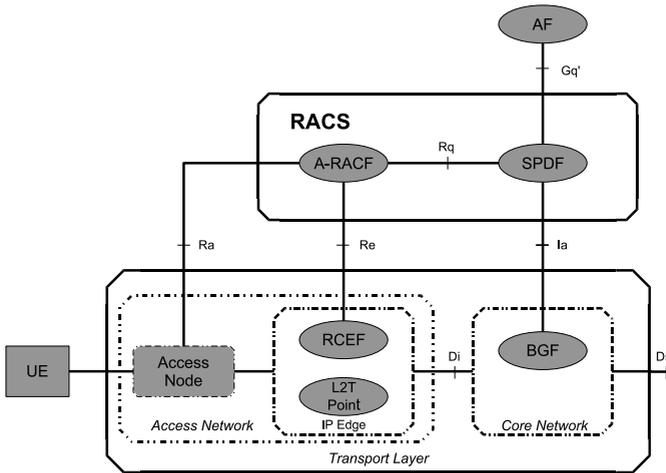
**Fig. 2.** Functional architecture of RACS

requester AF. If the request is successfully authorised, the SPDF determines if it must contact the A-RACF and/or the BGF to provide the transport-layer control service.

The Access-Resource and Admission Control Function (**A-RACF**) is always in the access network, and provides the functionality for admission control and resource reservation over the access network to the SPDF. The A-RACF can accept or reject the requests received from the SPDF based on the admission control mechanisms.

The Resource Control Enforcement Function (**RCEF**) is located in the IP edge node of the access network, and provides the RACS with the means to apply the traffic policies that guarantee the resource reservation. The Border Gateway Function (**BGF**) provides the interface between two IP domains. Release 1 of TISPAN NGN identifies two types of BGF: the Core BGF (**C-BGF**), which is located between the access and the core network (in the Core Network side), and the Interconnection BGF (**I-BGF**), which is located in the limit between two Core Networks.

Table 1 offers an overview of the functionalities provided by the RCEF, C-BGF and I-BGF, as they are explained in [7].

## 2.2   Session Establishment and Resource Reservation

The session establishment process in IMS is based on the Session Initiation Protocol (SIP), and involves an end-to-end signalling dialogue between the terminals participating in the session. To negotiate the parameters associated with the media which is going to be transferred during the session, such us the type of media streams, codecs or IP addresses and ports, the Offer/Answer model of

**Table 1.** Functionality of RCEF, C-BGF and I-BGF

| RCEF | C-BGF | I-BGF |
|---|---|---|
| Open/Close Gates | Open/Close Gates | Open/Close Gates |
| Packet marking | Packet marking | Packet marking |
|  | Resource allocation (per flow) | Resource allocation (per flow) |
|  | NAT | NAT |
|  | Hosted Nat traversal |  |
| Policing of down/uplink traffic | Policing of down/uplink traffic | Policing of down/uplink traffic |
|  | Usage metering | Usage metering |

the Session Description Protocol (SDP) is used. SDP provides the support to describe multimedia sessions, and the Offer/Answer model applied to this protocol allows the end terminals to reach an agreement about the session description. The complete specification of SIP can be found in [8], whereas the Offer/Answer model with SDP is detailed in [9].

In the IMS architecture, the P-CSCF (Proxy-Call Session Control Function) is the functional entity which acts as the entry point for the users to the system. So, all the SIP signalling messages that come from or go to the user terminal must necessarily pass through this functional entity.

In TISPAN NGN Release 1, the P-CSCF in the Core IMS implements the AF functionality indicated in section 2.1, interacting with RACS to request QoS provision for the services negotiated between the end users. As it is detailed in [6], the P-CSCF sends service information to the RACS subsystem (i.e. to the SPDF) after receiving every SIP message with a SDP answer payload. This service information is derived from that SDP answer and from its corresponding SDP offer. Jointly, the SDP *offer* and SDP *answer* contain enough information to describe the session as it has been negotiated up to that moment, such us the IP addresses, ports and bandwidth requirements for the IP flows that will be transferred. Annex B in document [6] describe the mapping process that must be performed to convert SDP information to relevant service information to be transferred to the RACS subsystem.

As an example, consider the scenario proposed in Fig. 3 where it is assumed that two users want to establish a VoIP call through the TISPAN NGN, being both of them connected to the NGN through different xDSL access networks, and that only public IP addressing schemes are in use. The figure only shows the signalling and the QoS reservation process from the point of view of the user originating the call. The example assumes a reserve-commit resource management schema.

The procedure is as follows:

1-3. The terminal sends a SIP INVITE request, including a SDP offer, to the P-CSCF. The P-CSCF processes the request and forwards it to the
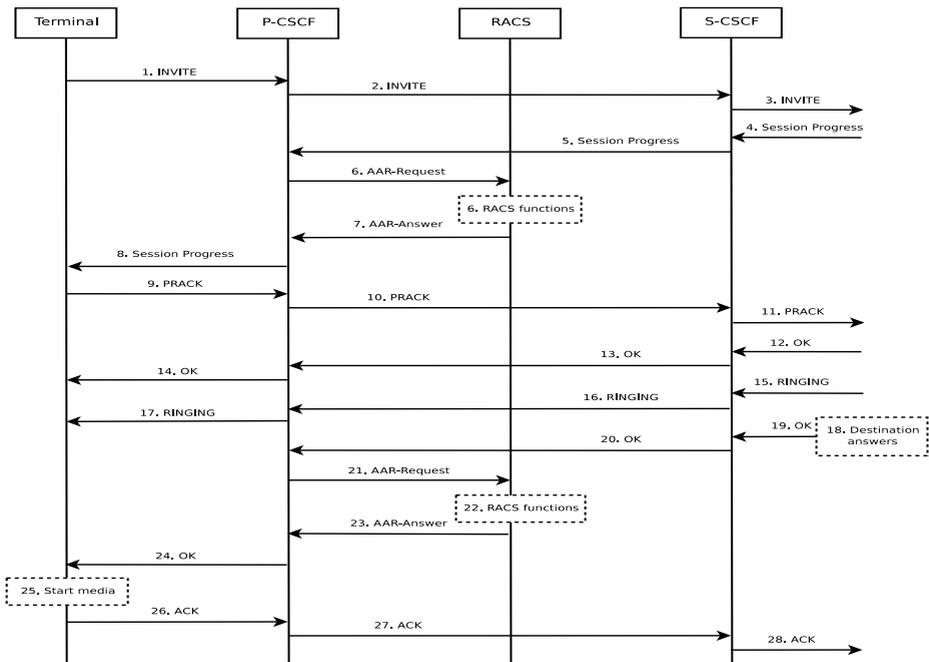
**Fig. 3.** Example of IMS signalling and QoS reservation

proper S-CSCF. After that, the S-CSCF processes the request and forwards it to the IMS domain of the destination user.

4-5. The destination terminal answers back with a Session Progress message, which is received in the S-CSCF. The S-CSCF processes it and forwards it to the P-CSCF.

6-8. The P-CSCF derives the service information from the SDP offer and answer, and then sends a resource reservation request to the RACS subsystem. RACS authorises the request and performs the corresponding admission control procedures, reserving the necessary resources from the transport network. Finally, it confirms to the P-CSCF that the resource reservation procedure has succeed. Finally, the P-CSCF forwards the Session Progress message to the terminal.

9-11. The terminal decides the final parameters for the session and confirms the reception of the Session Progress with a PRACK message. This message may also contain a SDP payload, that may be the same as the one that was received in the previous message or a subset. The terminal can make a new SDP offer in this message, or later using SIP UPDATE messages. Anyway, each SDP offer/answer pair will cause a new interaction with RACS from the P-CSCF.

12-14. The destination terminal acknowledges the PRACK with an OK message and if the PRACK message included an SDP offer, the OK message will

also contain a SDP answer. If the session description has changed, a new
interaction with the RACS must be performed.

15-17. The destination terminal alerts the user about the incoming call and
sends a SIP RINGING message to the originator terminal.

18-20. When the destination user answers the phone, the destination terminal
sends a SIP OK message to the originator terminal, that arrives at the
P-CSCF.

21-23. The P-CSCF interacts with the RACS subsystem to commit the previous
resource reservations.

24-28. The SIP OK message arrives to the originator terminal, and the user can
start to send media. The terminal responds the SIP OK message with an
ACK message, which is sent to the IMS domain of the destination user.

## 3  RGW Architecture

This section describes the architecture of the prototype already implemented
from the point of view of the development environment and this description will
be classified using a bottom-up view starting at the data level and then defining
the configuration process.

Figure 4 represents the complete picture at the bottom level where all func-
tional blocks and their relationships are depicted[1]. Incoming and outgoing traffic
flows are represented and the two separate paths show that these two flows never
use the same resources at Click! level. Dotted arrows represent unknown outgoing
traffic. Click! level sends these packets to the CSD (Click! Signalling Dispatcher)
to treat them and then it sends the packets to the corresponding Signalling Pro-
cess (SP) to handle it. Finally, the SP returns the packets to Click! level. Dashed
arrows are frame copies that Click! sends to the CSD or the IMS due to special
characteristics (signalling frames, for example).

These are the functional blocks for this level:

- **User Classifier:** The function of this block is to recognise flows depending
on the user (administrator) preferences. The user can add, reorder or remove
flow definitions and this change will modify the functionality of this block.
In the downstream direction, the user can select that a particular flow can
be replicated to all in-home interfaces selecting the multicast option.
- **Dispatcher:** Based on the p-bits field, this module introduces a packet in
one of the four possible queues.
- **Queues:** In Click!, the implementation of these queues is based on the in-
vocation of four different queue elements. Each queue represents a different
CoS. There are several ways to accomplish the requirements imposed by a
specific CoS. For example, a fix size queue can be used to avoid queue delays.
- **Scheduling:** Working with two or more queues implies the use of some
algorithm to extract a packet from one queue at each time. It is even more
complex to select the right one when priority queues exist. There are many

---

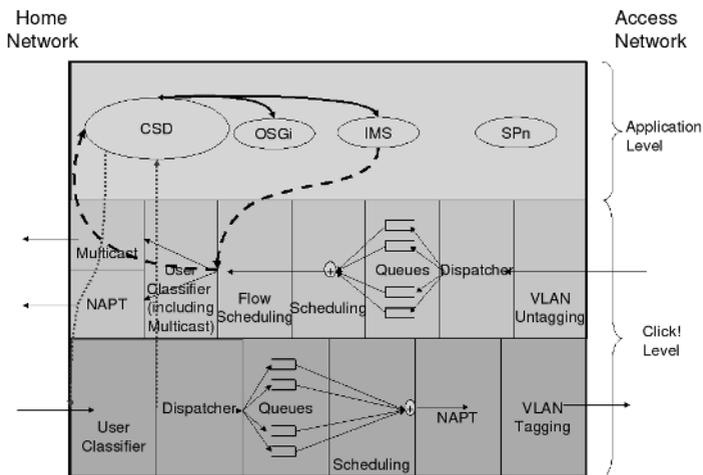[1] The core of this prototype is implemented using the Click! modular router [10].

**Fig. 4.** RGW Functional Blocks

scheduling algorithms to treat this problem: Priority Queuing, Weighted Fair Queuing, Class-based Weighted Fair Queuing, etc. and a Click! element called PrioSched that implements a Priority-like Queuing is used.

- **Policing:** The aim of this functional block is to limit the flows rate for every CoS. When an excess rate is detected, this block can either discard packets or change their CoS tag.
- **VLAN untagging:** Removes the 802.1Q/p tags from the packets.
- **Flow scheduling:** Detects "important" packets as signal packets and send copies to the CSD. It is useful to detect new flows and their characteristics (CoS for example).
- **NAPT:** For the upstream traffic it detects new sessions and then creates new entries in the NAPT table to change the original source port with the corresponding identification. For the downstream direction, this box just has to change the destination port and IP address with the matching entry from the NAPT table. Upstream and downstream directions are not different boxes because they must share the NAPT table.
- **VLAN tagging:** Depending on the user/administrator preferences, outgoing packets will be marked with 802.1Q/p tags and bits to add a priority to the frames. This information (the corresponding p-bit assignment) is pre-configured in the first stage and configured by the network in the final prototype. When a flow is not configured, this block forwards the packet to the CSD. The CSD can then discard the packet or reconfigure the VLAN tagging functional block (to recognise this new flow) and inject the packet again.
- **Multicast:** This block copies all incoming frames to all in-home interfaces (like most Ethernet switches do).
- **CSD:** This software has been developed in Java to allow an easy and quick portability to other platforms. The CSD will configure and reconfigure the

Click! level when signalling packets arrives. It is also possible to redirect this kind of packets to the corresponding Signalling Process (SP).

– **IMS:** MUSE plans to adopt SIP, which is used as the prominent signalling protocol in IMS, as its QoS signalling standard. Because the RGW is the access network and home network interconnection point, it must couple both worlds and allow an end-to-end QoS. To accomplish this requirement, the RGW must be configured as any network node.

## 4   QoS Management in the RGW

The specifications of TISPAN NGN Release 1 are mainly focused on the QoS provision in the access network. Nevertheless, a complete service architecture with QoS support will necessarily require to extend to QoS scope to the client premises, to provide end-to-end QoS. In this respect, this section describes an architecture which supports adaptive QoS management in a RGW connected to a NGN compliant with TISPAN NGN Release 1. The proposed architecture for the RGW, from the point of view of QoS management, is shown in Fig. 5.

The **NGN SP** is the Signalling Process that will manage, in the RGW, the SIP signalling used to negotiate end-to-end services over the TISPAN NGN. It will process all the SIP signalling messages interchanged between the NGG core IMS and the customer equipment. The NGN SP will provide the following functionalities:

– **P-CSCF functionality:** After receiving every SIP message containing a SDP answer, it will derive the corresponding service information from the SDP offer and the SDP answer as it is specified in annex B of [6]. This information will be provided to the A-RACF functionality of the NGN SP. On the other hand, after receiving a SIP OK message corresponding to a SIP INVITE message, it will contact the A-RACF functionality of the NGN SP to start the commitment process for the reserved resources.

– **A-RACF functionality:** With the service information provided by the P-CSCF functionality, the A-RACF functionality will perform admission control functions, verifying if the QoS demands can be satisfied in the RGW and the home network with the available resources. The A-RACF functionality will support a reserve-commit resource management schema and the QoS control models defined for the RACS in [7], i.e. guaranteed QoS and relative QoS.

– **SIP signalling proxy:** This functionality is necessary in the Signalling Proxy Scenario (SPS) proposed in [3]. In this scenario the NGN SP would behave as a signalling proxy on behalf of legacy terminals, by generating the SIP signalling associated with the upstream and the downstream traffic.

The **RCEF** will implement the functionality of a Resource Control Enforcement Function as it is detailed in [5] and [7], i.e. opening/closing gates, packet marking and policing of down/uplink traffic. The RCEF will apply the traffic
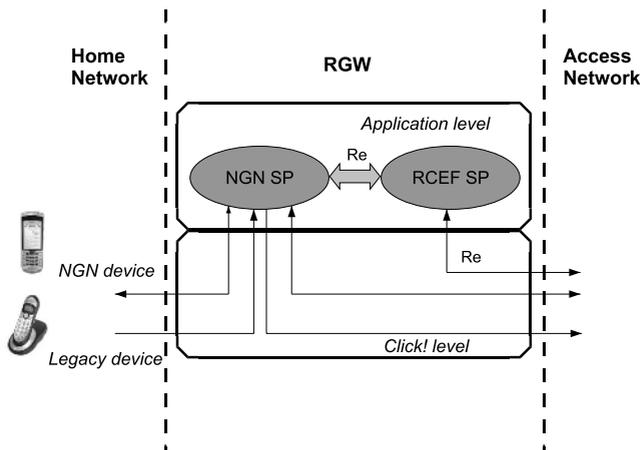
**Fig. 5.** RGW QoS management architecture

policies established by the A-RACF functionality of the NGN SP, guaranteeing the reservation of resources in the RGW.

Finally, the RCEF will provide a interface fully compatible with the Re interface defined in the RACS architecture detailed in [7]. This way, it will be possible a future scenario where the RACS subsystem in the NGN access network may directly access the RCEF function in the RGW to manage the QoS configuration in the client premises.

## 5   Conclusions

To date, there are a lot of telecommunications infrastructures capable of carrying different types of information: a specific one for the fixed telephone, a different technology for the mobile phones (moreover GSM, GPRS, UMTS, etc. are totally different) and other equipments to transport data (the Internet network). A telecommunications operator providing voice, video and data services needs to bring together all these technologies in a more efficient one to reduce costs. The IP protocol could be used to bring Triple Play services but many problems have to be solved first and the QoS is one of them. ETSI TISPAN Release 1 defines how to achieve QoS deliveries up to the access network but, since the RGW is not considered part of the access network by TISPAN, the end user would not perceive that QoS when its own home network is a bottleneck.

In this article we presented a flexible RGW architecture where both, the RGW resources and the home network available bandwidth are taken into account to accept or not a given connection. The schema proposed is valid for a RGW aware NGN architecture, where the access and reservation systems configure the RGW and in a RGW unaware one. For the later, the RGW intercepts SIP requests

and responses to perform some actions in the same way as in the TISPAN NGN devices (P-CSCF, A-RACF, etc.). How the RGW manages NAPT scenarios and updates the parameters of a certain established connection are let for further study.

## Acknowledgements

## References

1. TISPAN: ETSI TR 180 000 V1.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology." (2006)
2. TISPAN: ETSI TR 180 001 V1.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition." (2006)
3. Guerrero, C., Garcia-Reinoso, J., Valera, F., Azcorra, A.: Qos management in fixed broadband residential gateways. LNCS **3754** (2005) 338–349 8th International Conference on Management of Multimedia Networks and Services (MMNS 2005).
4. MUSE: Multi Service Access Everywhere. Internet (2006) http://www.ist-muse.org/.
5. TISPAN: ETSI ES 282 001 V1.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1" (2005)
6. TISPAN: ETSI TS 183 017 V1.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF): Protocol specification." (2006)
7. TISPAN: 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." (2006)
8. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard) (2002) Updated by RFCs 3265, 3853, 4320.
9. Rosenberg, J., Schulzrinne, H.: An Offer/Answer Model with Session Description Protocol (SDP). RFC 3264 (Proposed Standard) (2002)
10. Kohler, E., Morris, R., Chen, B., Jannotti, J., Kaashoek, M.F.: The Click Modular Router Project. Internet (2006) http://www.read.cs.ucla.edu/click/.