A broadcasting enabled Residential Gateway for Next Generation Networks

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

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

Abstract. To date, broadcasting traffic data represents a low percentage of the total traffic in the Internet when compared to other kinds of information. This may be caused by difficulties with multicast transmissions (i.e filtering by ISPs), low bandwidth rates in the last mile access, quality of service (QoS) and the use of Network Address Translation (NAT) boxes in SME's and home offices (SOHOs). Research efforts in Next Generation Networks (NGN) are under way to create networks with true triple-play capabilities to overcome these problems. Several standardisation bodies like ITU-T and ETSI have working groups aimed at developing a general NGN architecture able to transport any type of traffic with an associated QoS. There are several results available (for example, ETSI TISPAN has published its Release 1) but there is still on-going work on different subjects, such as broadcasting transport in NGNs, where ETSI TISPAN has approved the study of IPTV in NGN as a high priority issue. This article focuses on the problems and solutions of a flexible, easily upgradeable broadcast enabled RGW (Residential Gateway) designed to work in an NGN scenario where multicast traffic, NAT boxes and QoS must be taken into consideration.

1 Introduction

There are several initiatives focused on standardizing Next Generation Networks (NGN) with triple-play capabilities. NGN is not a fixed concept and several authors or even standardisation bodies have different definitions. For example, ETSI TISPAN defines an NGN as *"... 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"*. From this definition one can extract a key concept of the NGN idea: the service layer is independent from the underlying transport technology. It is important for applications such as IPTV, VoD, VoIP, or any jitter/delay-sensitive application.

A challenge when defining a new protocol or architecture is not to forget about legacy applications. In this respect, the ETSI TISPAN NGN architecture considers previous transport technologies and applications, and introduces several blocks of functionalities to handle Streaming Services (RTSP based), PSTN/ISDN emulation (SIP-I based) or the IP Multimedia Subsystem (IMS). Still, in order to be fully operative, it could be enhanced in specific areas. For example, TISPAN uses SIP as the signalling protocol to reserve network resources. SIP difficulties with NAT are well known, and the TISPAN proposal is to introduce a NAT box in the Core Network boundary and use an Application Level Gateway (ALG) to handle SIP messages. However, there are some concerns about scalability issues that may arise in such a scenario. Another problem that must be solved is the integration in IMS of legacy applications together with other signalling protocols different than SIP, such as IPTV (IGMP multicast) or VoD (RTSP), in order to inform the IMS core about flows with certain bandwidth requirements.

This article proposes to follow the TISPAN architecture to configure the NAT but in the RGW instead of in a network device due to these scalability issues. The idea is to use an ALG in the RGW to force SIP frames to change the SDP payload and open and close the proper ports in the Firewall block. In order to solve the previously commented integration problem, an IGMP and RTSP snooping will be introduced in the RGW which will generate SIP messages to the IMS core to reserve and modify bandwidth resources. Moreover, other kind of NAT traversal mechanism will be implemented to complement the ALG one.

The rest of the article is organised as follows: next section describes a broadcasting scenario in an NGN to detect problems associated to broadcasting applications. Section 3 presents the whole concept, problems and solutions of NAT in a broadcasting enabled NGN while Section 4 takes into consideration the IPTV and VoD problems in the same scenario. Section 5 gathers the solution proposed to automatically manage the NAT, IPTV and VoD in the RGW and, finally, Section 6 presents the concluding remarks.

2 Broadcasting and NGN concepts

2.1 Broadcasting

The broadcasting concept has its roots in the analogue world of radio and TV. In the Internet it is used to define the same behaviour, even though the underlying technology is quite different: terrestrial radio or TV transmits their signal into the air and any receiver in the surroundings can demodulate it and present the information to the end user. In the Internet, however, the end user must first request the transmission. The server (transmitter) has two possibilities when sending packets: unicast transmission or multicast transmission. If the former is used, every end user will receive a fresh copy of a packet originated in the source while in the latter the server just generates one packet independently from the number of end users.

Peer-to-Peer (P2P) applications have a different transmission philosophy since all nodes involved in the data exchange are both servers and clients. When P2P applications are used to transmit video or audio, one point assumes the super-seed role (the one that just sends the packets) and then a tree topology is generated to propagate the packets to the group members.

2.2 TISPAN-NGN overview

In 2004 ETSI and 3GPP started working in cooperation, in the ETSI TISPAN group, researching on how to apply IMS over other access networks different than the 3GPP IP-CAN. As a result of this joint work, the first release for TISPAN Next Generation Network (NGN) was published at the beginning of 2006. The main objective of this release is to provide an extensible platform for the development of future services and architecture for the NGN. In addition, it confronts two key objectives: to extend the services provided in IMS to access networks based on different technologies and capabilities (e.g. xDSL, Ethernet, cable networks or wireless LAN) and to enable ISDN/PSTN replacement. TISPAN NGN will support a variety of user equipment, from simple legacy telephones to client networks connected through a residential gateway.

TISPAN NGN functional architecture As it is shown in Figure 1, the functional architecture of TISPAN NGN [1] is structured in two layers, the transport layer and the service layer. Both layers are constituted by a set of subsystems and functional entities.

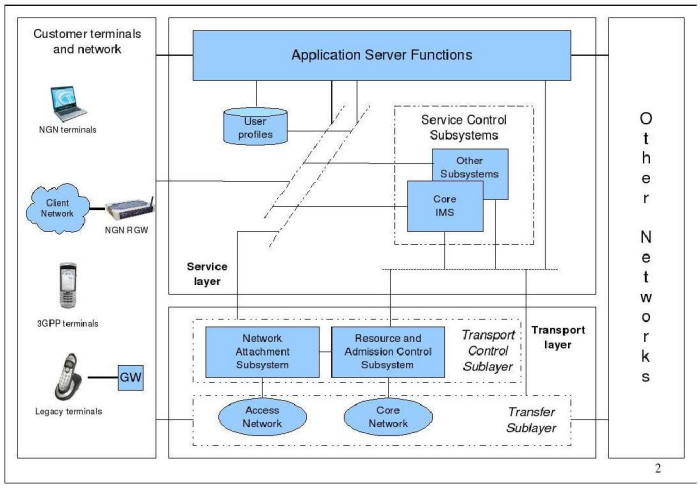

Fig. 1. Functional architecture of TISPAN NGN, release 1.

Transport layer The transport layer provides IP connectivity to the user equipment in the client premises. The functionality supported by this layer is divided in two sublayers: a transport control sublayer and a transfer sublayer. The transport control sublayer comprises the following subsystems:

- The Resource Reservation and Admission Control Subsystem (RACS) provides policy control, resource reservation and admission control in the NGN. The RACS subsystem provides the applications with means for requesting and reserving resources from the transport networks (in Release 1, the RACS is only defined for fixed access networks), supporting QoS provision for NGN services. The RACS also controls the transversal of remote and near-end NATs on the NGN core network and at the border between core and access network. Further details about the architecture of the RACS can be found in [2].
- The Network Attachment Subsystem provides initialisation of user equipment for accessing to NGN services (for example, dynamic provision of IP addresses), network level authentication, authorisation of network access, access network configuration and location management.

Service layer The service layer comprises a set of subsystems that provide service control functionalities. The following service control subsystems have been proposed in TISPAN NGN Release 1: the IP Multimedia Subsystem Core (Core IMS), the PSTN/ISDN Emulation Subsystem (PES), the Streaming Subsystem and the Content Broadcasting Subsystem. The IP Multimedia Subsystem Core provides the means to negotiate SIP-based multimedia services to NGN terminals. It is a subset of the IMS as it was defined in the 3GPP Release 6 specifications, simply restricted to the session control functionalities. The architecture of the Streaming Subsystem and the Content Broadcasting Subsystem is outside the scope of TISPAN NGN Release 1.

3 The NAT problem

3.1 The NAT concept

The basic NAT [3] operation is a method by which some IP addresses are mapped (translated) into some other IP addresses. This mechanism is nowadays available in many business environments and in almost every residential environment with an Internet connection since the most important need for address translation appears when multiple devices belonging to a private address domain want to share a public IP address.

3.2 NAT traversal problems with SIP signalling

Although NATs are very useful and some times mandatory elements, they break many existing applications and working protocols and the main problem is common to all of them: NATs are only capable of changing transport addresses

located in the header of the packets and there are protocols (FTP, SIP, RTSP, etc.) that send their information about transport addresses in the payload of the protocol messages so when the destination retrieves this information, it finds there the untouched private address and port that are unreachable and causes the protocol to fail.

This problem is particularly significant nowadays in a protocol such as SIP [4] that is becoming the basic signalling protocol in Next Generation Networks since it is capable of locating persons and setting up point to point sessions.

The main problems associated with SIP NAT traversal are the following:

- SIP uses a special notation, SDP, Session Description Protocol, to describe multimedia sessions and since addresses are also included in SDP they remain hidden for NATs.
- Other important information typically included in the SDP message are the RTP/RTCP ports to be used in subsequent exchanges. In order to be able to receive data on these ports the NAT should open them (forward incoming connections on those port towards the corresponding client), but it is impossible for the NAT to do so since they are hidden in the SDP message.

3.3 NAT solutions to date

There are several solutions that have been proposed in order to allow different protocols to operate through NATs but similarly to what happens with NAT behaviours, they are usually non standardized proposals. Some of these alternatives are: manual configuration, tunnelling mechanisms, the Simple Traversal of UDP through NATs, the Stun Relay Usage, the Interactive Connectivity Establishment, the Realm Specific IP, application level gateways, etc.

All these solutions have their own advantages and disadvantages and are certainly valid in some specific situations and topologies although in some others they fail and do not perform effectively.

However, it is important to notice that independently of the chosen mechanism there are two main ways to perform NAT traversal: to rely on an external server to perform different actions or to enhance the NAT itself by the provisioning of an application level entity capable of treating the signalling messages before the NAT operation. In the following subsections the most representative solutions are presented and both NAT traversal philosophies are compared (see Figure 2).

- STUN: the idea behind the Simple Traversal of UDP through NATs (STUN) solution is that if it is possible to inform the client in advance about the NAT binding that would be issued in case a SIP message was sent towards the destination it would be possible for the client to include these details (public address and port) into the SDP information when sending the SIP message and there would be then no problem to locate it from the server side.

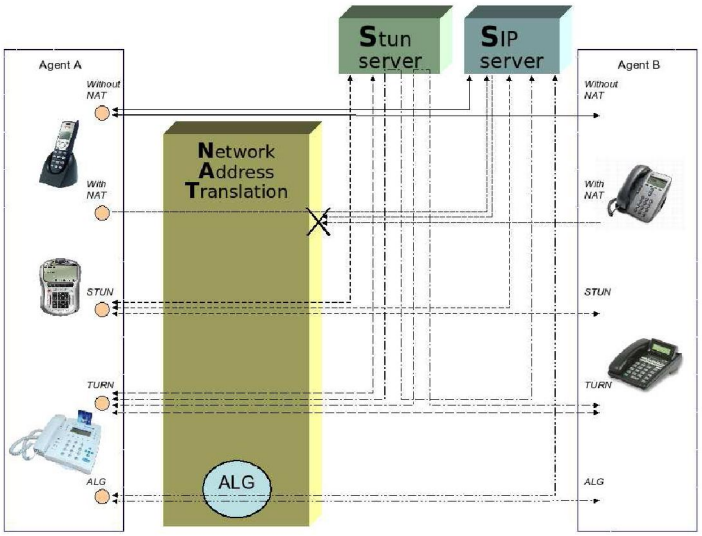

Fig. 2. NAT traversal techniques

- TURN: the Traversal Using Relay NAT (originally known as TURN but now understood as an extension of STUN with relying possibilities) solution is proposed by the same authors as STUN in order to cover the problems that the simple traversal solution presents. In the introduction of the RFC it is clearly stated that even although TURN is capable of providing connectivity in almost every situation it is at a high cost for the provider of the TURN server and should only be used as a last resort.
- ICE: the TCP Candidates with Interactive Connectivity Establishment (ICE) is not a new mechanism itself but a combination of different existing mechanisms like STUN and TURN. ICE claims to be making use of these existing solutions in order to create a generic mechanism for NAT traversal not so topology dependent and to be able to dynamically determine the way to proceed with STUN messages depending on the detected environment.
- Application Level Gateways (ALG): instead of relying on external servers, the idea of the ALG related to SIP (although it can be applied to any protocol) is to work in concordance with the NAT so that it is possible to derive certain packets to it in order to inspect and modify the payload before sending them through the NAT. In the particular case of SIP, the ALG is responsible for changing the IP addresses in the SDP message so as to show there the public address of the NAT instead of the private address of the host, retrieving the ports to be used in the RTP/RTCP media sessions and opening these ports in the NAT, etc. This mechanism is completely transparent to the end user since it does not require the installation of any additional software other than a normal SIP client. It is also a self-sufficient mechanism since it does not imply the installation of any external server

or any external relay. This absence of relays and additional exchanges of messages with external servers allows a faster signalling procedure.

ETSI TISPAN uses an ALG for SIP messages but in the Core Network. Section 5 describes a better solution where the ALG is done in a RGW, but before, next section introduces other problems of the broadcasting applications in NGNs.

4 IPTV and VoD

4.1 IPTV

Several TV companies and other enterprises have streaming-capable servers in the Internet to distribute live events or stored videos. They can provide these services using for example a pay-per-view scheme (by means of an authentication method to allow its customers to access their services) or even distribute them totally free, but there are no delay or jitter guarantees because these service providers have no specific traffic contracts with their ISPs. This is a problem with streaming services and although some workarounds are used to overcome it (buffering, multi-layer encoding, interleaving, etc.) no one of them solves the main issue: all packets in the Internet share the medium in a best effort way.

Nowadays, there are several telcos in many countries providing the same service, but with a QoS differentiation because they own the access network. So, it is possible for them to prioritise the video/audio signal over other kinds of traffic. Another possibility is the video storage, replication or other schemes to increase the video/audio quality.

As stated before, the control of the access network has competitive advantages over a simple service provider. Indeed, the provision of video/audio distribution using IP multicast is crucial to succeed in this game. Another advantage is the possibility to easily use recent access technologies such as xDSL, allowing telcos to provide one channel for the Internet and a separate one for the TV traffic.

4.2 VoD

Video on Demand has important differences with IPTV due to the unicast behaviour of the former and the mechanisms used to distribute it. In VoD the end user requests a video and can program the starting time of the transmission. In contrast with IPTV, this user could be the only one receiving that video so a multicast transmission is not the optimum distribution scheme. Even if two or more users request the same video, the probability of time coincidence is very low (some service providers allow the users to receive the video only at programmed time slots, even though this does not represent the true video on demand concept).

Existing solutions proposed to overcome these issues, such as bringing the video servers near the end users replicating the video pools in all the servers, are

expensive in terms of equipment and maintenance and therefore other alternatives are needed in order to be able to decrease the final price to the users.

5 An NGN-Residential Gateway for broadcasting applications

5.1 The role of residential gateways in NGN

ETSI TISPAN Release 1 does not include the RGW specifications nor its interface with the access network, but these definitions will be studied in Release 2 as it is clear that the RGW is a key device in NGNs.

Regarding the NAT issue, TISPAN Release 1 describes a situation where the CPE has a NAT functional block. In the scenario described in [2] the CPE does not include an ALG so the access network elements have to emulate its behaviour by means of a proposed a method called "addressing latching" to handle private IPs from the SIP message and learn the public IP which corresponds to the CPE.

TISPAN NGN Release 1 does not consider multicast but it is foreseen in next releases. The mechanism to request multicast services should also be taken into account, to extend SIP capabilities. Meanwhile, some workarounds have to be deployed to allow for IPTV services in the NGN. Moreover, the QoS request in this scenario has to be studied in depth to follow the overall model.

Another question with NGNs and multimedia legacy applications is the QoS control in one session. With RTSP, a client could pause the reception or even change its available bandwidth and therefore, these changes must be communicated to the network. If RTP is used then RTCP could inform about the modifications and the sender could switch the codecs.

5.2 NAT in the RGW

ETSI TISPAN defines the possibility to do NAT functionalities at the border of the access and core network to allow the access network to work with private IP addresses (or other items). When NAT is used, the SIP INVITE message is accordingly changed, after the RACS subsystem has obtained the proper mapping from the NAT box. This must be done for every SIP message with a SDP load with IP or port addresses (INVITE, OK, REQUEST, etc.). This behaviour has several scalability problems. Moreover, there are other problems when a NAT box with ALG functionalities or any other external proxy server that helps in the NAT traversal problem is in between the UE (User Equipment) and the BGF (Border Gateway Function), for example when the CPE has a NAT box. In this case, the SDP load does not have the WAN IP or port addresses so the functional elements which just use SDP to configure the whole network will not be able to do it properly. TISPAN proposes the "address latching" concept where the BGF detects the real IP address and ports to forward the packets. All these solutions have a high price for the network, so in this article it is proposed to do the NAPT functionality also in the RGW with an ALG functionality to avoid other problems.

In this paper proposal, the RGW has the same functional elements than in the access network to be as TISPAN compliant as possible. This will be done using a previous architecture defined in the MUSE Research and Development project [5] that belongs to the 6th Framework Program of the European Union, where a prototype was implemented using a hybrid model (see [6] and [7]). In this hybrid model, the data layer is implemented in the kernel while the control is done at the application layer (developed in Java). This model allows to extend the RGW functionalities faster and in a high level language. For example, the RGW (the kernel) could be configured to extract all SIP frames and sent it to the application level to manage them.

We propose two complementary mechanisms to achieve the NAT traversal functionality: the first one is to create an Application Level Gateway to configure the NAT box (implemented in the kernel). The second one is to introduce a STUN server in the own RGW to simplify the end user device configuration. Figure 3 shows the proposed extension to the architecture, where three new applications are introduced to handle and configure the NAT box (already available in the previous architecture):

– SXC (Signalling Cross Connector): this block handles all signalling frames. Although SIP is the main signalling protocol, this block could be extended to treat other signalling protocols. At the startup, this block configures the kernel level to extract all signalling available protocols (that can be handled by itself). When a signalling frame arrives to the SXC, it has to process it to detect if it is already NAT friendly or, in other words, if the end user device is using a STUN client. In that case, the frame has public IP addresses so it is easy to detect. In other case, the SXC must get the operation intention

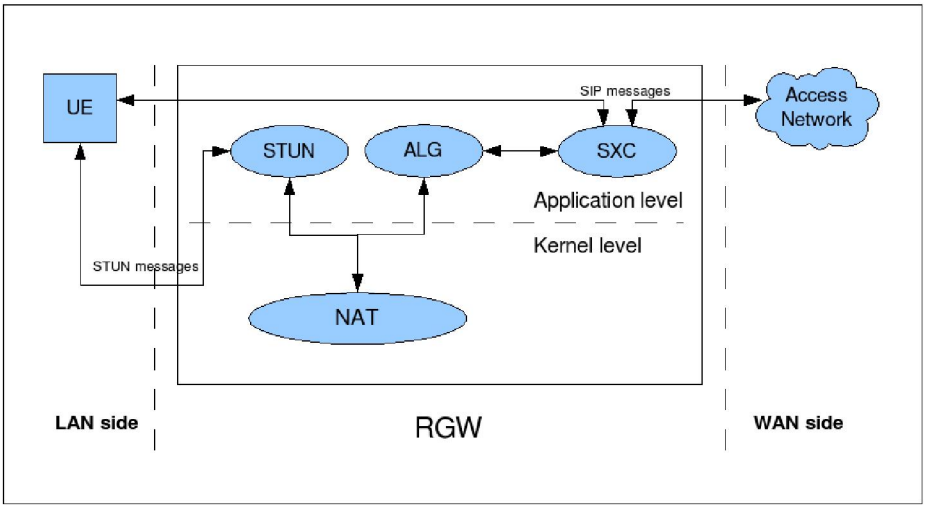

Fig. 3. ALG block in a NGN RGW

of the SIP message. When a *"connection start"* (INVITE or OK in SIP) or *"connection end"* (BYE in SIP) is detected, the SXC must contact the ALG to get to the corresponding mapping. After the processing is done, the SXC re-injects the frame in the flow in the appropriate direction.
- ALG (Application Level Gateway): this block is in charge of changing the frame payload after the corresponding NAT mapping. The ALG can configure the NAT box using its own information. For example, the ALG has a list of the already used ports (and the associated transport protocol) in the WAN side so, whenever a RTP session is requested, the ALG changes the port (in the SDP load, for example) with the opened one (the own ALG will open that port in the NAT). To perform these functionalities, the ALG has access to read and write the RGW configuration, not directly but through other blocks in the application level.
- STUN server: this block gets STUN requests to assign public ports to the requested connections. As the ALG block, the STUN server block creates new mappings in the NAT box at the kernel level (see Figure 3) generating the proper STUN response. With this block, we can modify the dynamic behaviour of the NAT box (which performs a symmetric mechanism) allowing the proper functioning of the STUN clients implemented in the end user devices. Unlike external STUN or ICE, this deployment is not fully independent from network configurations (a concatenation of NATs may still cause problems if no further solutions are provided). However, it definitively makes the client independent from the network (it is the client that chooses between ALG or STUN) and in case the network is applying an additional NAT mechanism it is the operator responsibility to provided the require solutions so as to allow NAT traversal for signalling messages.

All blocks are already implemented in our RGW prototype and successfully tested. Four different tests (for all four possible combinations) were performed with hardware (IP Zyxel Prestige 2000) and software (Kapanga) SIP phones activating and deactivating the STUN client and all connections could be established.

5.3 VoD in the RGW

There are several improvements that can be done in the VoD scenario when a next generation RGW is used. Regarding the problems commented before, these are the extensions proposed to the RGW architecture:

- RTSP snooping: a new application could be developed to process RTSP frames. In this case, the frames do not have to be extracted from the flow but just copied to this application. The RTSP application will generate a SIP message to inform the access network when necessary. For example, if the end user PAUSEs the video reception, the RTSP applicatio could generate a message to release resources from the network or simply decrease the bandwidth associated to the video/audio flows.

- RTCP snooping: it is also a new application receiving RTCP frames (just the copies) and processing them. At the initiation phase, the network commits some resources for the data flows as requested by the end terminals but, following the RTCP messages, the requirements could change in the middle of a session. The RTCP application could generate a SIP message modifying (if possible) the available resources for those flows.
- P2P communities: with this new application, the end users could distribute a previously received video itself to other users. If the Service Provider allows this service (configuring the RGW device), the P2P application will receive all video frames (a copy generated at the kernel level in fact) storing them in the RGW hard disk (this is also useful for time scheduled downloads). Whenever requested by the Service Provider, the P2P application will transmit the video to another user. Although this solution is adequate to replicate the videos as closer as possible to the end users but not in a specific server in their surroundings, it has some drawbacks that are outside of this work, but mentioned here for completeness:
  - Security: the users could access the videos stored in their RGW.
  - Bandwidth waste: the user could experiment bandwidth degradation when acting as a server for other users.
  - Disk space: normally a RGW is a low cost device with limited hard disk capacity so, depending on the video/audio quality, a film may not fit in the RGW.

5.4 IPTV in the RGW

Besides the solutions given in the VoD section, IPTV can benefit from other ideas for the multicast protocol. The following are proposals to extend the previous RGW architecture:

- IGMP snooping: in case the access network supports multicast signalling, the RGW could detect the IGMP frames and later inform about them to the IMS Core in order to reserve resources in the network. This could be performed by a new application. With this solution, the RGW could request a minimum QoS degree and then, using the RTCP application these parameters could be changed to provide the best parameters for that connection as the application does not request any QoS.
- Creation of IPv4 tunnels in IGMP application for multicast frames when the access network does not allow this protocol.

6 Conclusions

A key functionality in Next Generation Networks so as to be able to promote them and to achieve a faster penetration is to allow the operation of legacy applications without modifications. As these networks are specifically designed to carry multimedia services, it seems reasonable that technologies like IPTV or

VoD are finally deployed in NGN. Since these and other technologies use other underlying protocols to transport data like RTP, and as SIP is the signalling protocol used in the TISPAN NGN, the NAT problem with SIP must be taken into consideration.

In this article the different problems to move several broadcasting applications to the NGN and solutions used today in the Internet have been presented. ETSI TISPAN proposes some answers to overcome these difficulties, but all of them are focused on the access or core networks. These solutions have scalability issues that must be studied in depth. The new proposal detailed in this article explains how to solve these issues not in network but in the user RGW. The idea is to extend a previously validated RGW architecture introducing several application level blocks to handle all these signalling protocols in order to avoid modifying the applications and, more important, using the QoS benefits of Next Generation Networks.

Acknowledgements

This article has been partially granted by the European Commission through the MUSE project.

References

1. 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)
2. 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)
3. Srisuresh, P., Egevang, K.: Traditional IP Network Address Translator (Traditional NAT). RFC 3022 (Informational) (2001)
4. 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.
5. MUSE: Multi Service Access Everywhere. Internet (2006) http://www.ist-muse.org/.
6. 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).
7. Valera, F., Garcia, J., Guerrero, C., Ribeiro, V.M., Pinto, V.: Demo of Triple Play Services with QoS in a Broadband Access Residential Gateway. In: IEEE Infocom. (2006) Barcelona, Spain.