Qos and authentication experiences in a residential environment within a broadband access framework

Iván Vidal[1], Francisco Valera[1], Jaime García[1], Arturo Azcorra[1]
Vitor Pinto[2], Vitor Ribeiro[2]

[1] Universidad Carlos III de Madrid, Avda. De la Universidad 30
28911 Leganés, Madrid
{ividal, fvalera, jgr, azcorra}@it.uc3m.es
[2] Portugal Telecom Innovaçao, Rua Eng. José Ferreira Pinto Basto
3810-106 Aveiro (Portugal)
{it-v-pinto, vribeiro}@ptinovacao.pt

Abstract. It is sometimes believed that a "broadband access" network, providing ample transmission capacity to residential environments, is enough so as to allow a flawless delivery of advanced services. However, the provisioning of a combination of multiple services with guaranteed quality up to the end-user terminal requires a carefully designed architecture incorporating the appropriated Quality of Service (QoS) concepts throughout the data path. And this path includes the Residential Gateway (RGW) as the last hop towards the home network. This paper describes the different experiences performed with the RGW prototype developed within the framework of the European IST research project MUSE. Special emphasis will be made on the QoS capabilities of the RGW as well as on authentication and auto-configuration features.

Keywords: RGW, triple play, broadband, QoS, 802.1X, trials

1 Introduction

Nowadays, one of the most common trends mentioned in the communication network environment is the one related to 'convergence'. Convergence from services viewpoint allowing video, audio and data to be merged on the so called triple play provisioning and convergence on networks allowing fixed and mobile scenarios (even cellular) to be combined into a single architectural model. And these convergences have been facilitated by means of the provisioning of a large amount of throughput to the final users.

Although it is very common to find that in residential environments, access lines support from 1 Mbps to 20 Mbps (ADSL, ADSL+2, etc.), it is just a question of time that users are capable of filling their access lines with multimedia or peer to peer content and all the applications will be forced to share a limited amount of resources.

In such a common resource restrictive home environment it is remarkable that bandwidth is not at all the only quality of service parameter that must be guaranteed,

since there are many others parameters like latency, jitter, packet loss, etc. that may also be crucial for certain applications to run properly.

This article describes the results of the different experiences, performed with a QoS enabled RGW (RGW) within the framework of a broadband environment such as the one specified by MUSE, which is a large integrated research and development European project on broadband access, whose main objective is the specification and deployment of a future, low cost, multi-service access network.

The RGW is responsible for delivering services to the end-user terminal and so it is responsible for receiving the frames coming from the access network and transferring the quality of service devised for it towards the home network. And it is also responsible for sending the frames towards the access network tagged with the corresponding quality of service so that the network can accordingly process it. The rest of the article is structured as follows.

The second section describes the RGW, first within the MUSE research project and afterwards from a functional and architectural point of view focusing on the two main functionalities that will be trialed: authentication and QoS.

The third section explains the different test and trials performed with this RGW platform and finally the last section summarizes the most important conclusions and provides some guidelines about the possible future work that is being scheduled.

2 A Quality of Service enabled Residential Gateway

2.1 The Residential Gateway in MUSE project

MUSE (MUltiServive access Everywhere, [1]) is a large project on broadband access that belongs to the 6th Framework Programme for R&D of the European Union. MUSE aims at a consensus view of the future access and edge network achieved by the co-operative research of almost all major players in Europe (36 partners, including system and component vendors, telecom operators, SMEs and universities and research institutes). The project integrates studies in the following areas:

- Access and edge network architectures and techno-economical studies.
- First mile solutions (DSL, optical access).
- Internetworking of the access network with RGW and local networks.
- Lab trials.

Figure 1 shows an overview of MUSE general architecture where different scenarios are depicted and the important boxes are remarked. One of the most relevant entities within the whole MUSE architecture is the RGW which is located at the edge of the access network that MUSE is specifying. It means that the RGW must be compliant with all the different functionalities supported by this network in order to be able to make them compatible and to extend them towards the home network. The prototype presented in this article is included in a particular subproject in MUSE focused on a FTTH broadband access scenario (up to 1Gbps). The functionalities of this RGW prototype can be divided in three different groups:

- *Initial autoconfiguration*: the RGW software performs an automatic discovery of the hardware where it is being run, including the number of network interfaces and from them, which one is being used as WAN interface. The RGW authenticates itself towards the network provider and automatically configures the connectivity layers of the WAN and the LAN side (IP addresses, DHCP server, SIP ALG, etc.).
- *Operation*: apart from the traditional NAT and firewall functionalities available on current RGW devices, the prototype is also capable of performing some other actions such as NAT traversal for SIP, based on an application level gateway and for STUN based clients by means of an embedded STUN server, multicast delivery or QoS provisioning (both tagging upstream flows with a 802.1pq header so that the network can properly treat them and providing the corresponding QoS to downstream frames and promoting that QoS into the residential network).
- *Management*: apart from the manual configuration mechanism that is based on a Java servlet guided Web interface and allows a complete configuration of the RGW, other automatic alternatives have also been included like the DSL Forum TR-069 standard [2] mechanism or by means of the SIP signaling protocol (allowing the RGW to be integrated into an IMS/NGN architecture).

All these commented functionalities are structured in the RGW prototype architecture divided in two different layers (see Fig. 2).

The ***data layer*** is responsible for data processing including routing and bridging decisions, shaping/policing functions, flow classification, tagging/untagging of frames with the corresponding VLAN and corresponding p bits, queuing facilities, etc. This data layer (or kernel layer from the implementation point of view) has been implemented using the Click! platform which is a modular software router developed by the MIT, the ICSI and the UCLA for the Linux operating system [3].

The ***configuration/management*** layer is responsible for the management of the services and the management of the network layer, the configuration of the different parameters of the RGW like QoS parameters, NAT/ALG functionality, flow classification, etc.

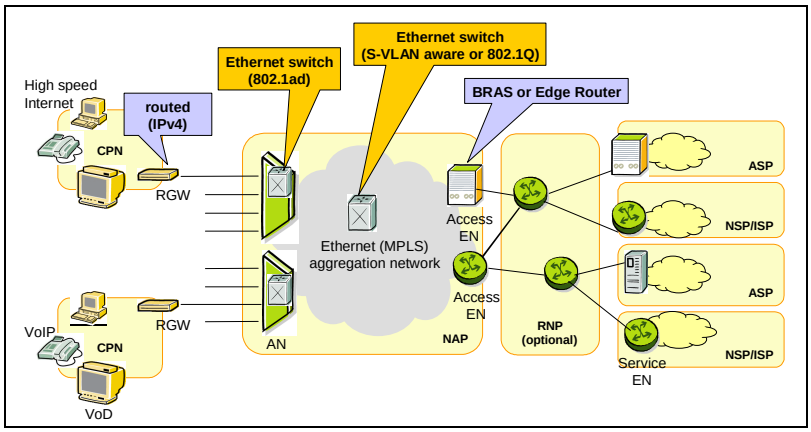

Fig. 1. MUSE overview.

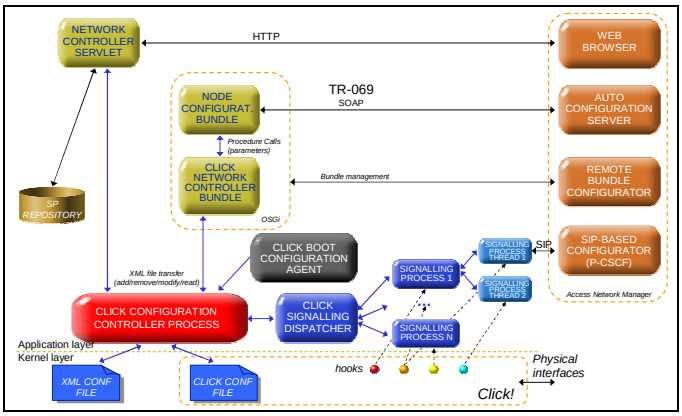

Fig. 2. RGW architecture.

In addition, this layer is also responsible for supporting applications that are capable of interpreting different signaling protocols that in turn, will also configure diverse RGW parameters like SIP, IGMP, RTCP, etc. The configuration/management layer has been implemented using Java (some specific modules have been implemented in C and perl, but almost all of them have been programmed in Java). The main objective of this development decision was to facilitate the implementation of new capabilities for the RGW since developing at the kernel level (Click! level) is not only a difficult task but also a platform dependant task. However, when designing this application layer it was also considered that the time spent in sending the frame from the kernel, layer where it is first received, up to the application layer, to be treated by the corresponding signaling process, and finally down to the kernel layer again to be transmitted, may not be negligible. These details have been analyzed in [4] and [5] for the implemented prototype and demonstrated in [6] and it was concluded that for signaling traffic it is feasible to maintain this hybrid model.

2.2 Authentication and auto-configuration

MUSE project encourages the support of a dynamic, nomadic multi-service environment requiring the dynamic change of network resources that a given costumer is allowed to use at a given time, as well as the recognition of a given device and/or person on the different network access points. Therefore, is essential, to the different providers, the regular execution of authentication routines towards devices and/or persons. Given the strategic role that the RGW plays in this scenario, it is fundamental its authentication towards one or even more providers and since a RGW is usually contractually bounded to a given costumer, performing RGW authentication is an implicit way of performing costumer authentication. Considering these requirements, the prototype has the ability to authenticate itself towards one or more authenticating entities that reside in the network. For this purpose a combination of IEEE 802.1X [7] protocol with Extensible Authentication Protocol was chosen (EAP [8]). The flexibility of 802.1X protocol and its intrinsic support for transport of EAP messages over IEEE 802.3/Ethernet based networks were determinant to this choice.

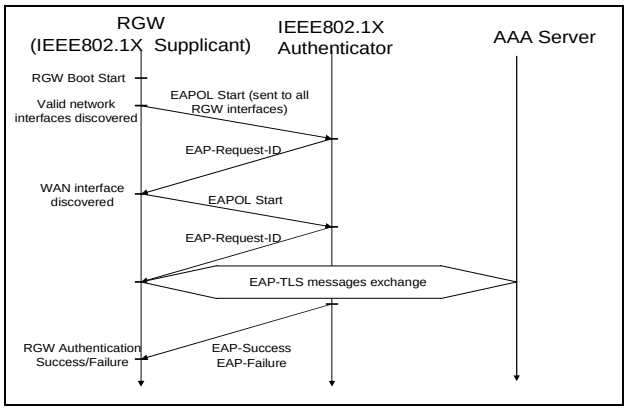

Fig. 3. RGW interface discovery and authentication.

Although EAP-TLS [9] based authentication was used, other authentication methods are also possible (e.g. EAP-AKA, EAP-MD5, EAP-SIM, etc.). The distribution of the different authentication related entities in the MUSE network is as follows: the 802.1X supplicant is located in the RGW, the 802.1X authenticator is located in the access node and the authentication server in the aggregation network (see Figure 1).

Besides authentication, some mechanisms for auto-configuration were also added. These deal essentially with RGW network interfaces discovery and WAN interface identification, allowing the portability of the RGW software to hardware platforms that can differ on the number of network interfaces. The following paragraphs describe the boot up sequence of the RGW.

The first task performed when the RGW is powered up, is the detection of all network interfaces present in the hardware platform. Considering the discovered interfaces, several variables (e.g. physical connectivity) are taken into account to select only valid interfaces, through which the RGW can try to authenticate itself.

The next process, uses this set of valid interfaces and determines which one is the WAN interface. To achieve this, an 802.1X “EAPOL-Start” message is broadcasted through every valid RGW interfaces. The 802.1X Authenticator present in the access network, answers with an “EAP-Request-ID” message containing the string “muse.net” (in “EAP-Message” field) used to identify the WAN interface.

The next step is then to launch an EAP-TLS authentication process through the RGW WAN interface. A failed authentication process will result in re-authentication attempts and finally in the halt of the boot up process, while a successful authentication process results in the achievement of the boot up process (see Fig. 3).

2.3 QoS

One of the most important points to be considered when delivering services not only to business users but also to residential users is the capacity to assure a certain quality on this provisioning. This quality does not only mean a considerable amount of bandwidth, as it is usually advertised in the commercials, and should not be provided only until the access node. End to end QoS has already reached the terminals in the

mobile (cellular) world with the IP Multimedia Subsystem (IMS) and is also being promoted to the fixed networks by some entities like the ETSI TISPAN. However, no QoS schema had been specified for a device such as the RGW at the moment. The proposal in this MUSE prototype is to enable the RGW to assure QoS to transit data, and to integrate residential network resources within the whole QoS schema, since nowadays we do not have anymore the single-PC residential context and it tends to be more a set of devices connected in a LAN.

The RGW must be able to understand QoS marked packets (802.1pq tagging in MUSE) so as to prioritize their processing and to propagate that marking to the home network (mapping the QoS tagging schema used in the access network to the schemas used in home networks like the 802.11e specification, IP DSCP bits, etc.). It also means that for upstream traffic the RGW should to map the QoS that packets are bringing from the terminals or in case this action is forbidden for the terminals, mark packets by itself based on configured information.

The RGW has to consider that traffic in the home network is consuming resources that are not usually taken into account (i.e. upstream traffic and downstream traffic may be transmitted over a shared medium together with local traffic, etc.).

Some of the functionalities implemented in the RGW to allow this QoS support include scheduling and policing, traffic shaping, call admission control, per flow classification or frame tagging. These possibilities are typically included in other network nodes, but here it is proposed their inclusion in the RGW because otherwise the home network would be left out of the overall QoS schema. These functionalities combined with the flexibility offered by the Session Initialization Protocol (SIP) so as to automatically set up services, will allow the development during the second phase of MUSE project of an IMS/NGN compatible RGW and would also faclitate new QoS enabled scenarios that may involve the RGW into P2P overlay networks, community networks, mobility, roaming, etc.

4. RGW TRIALS

4.1 Authentication trials

The trials were divided in three phases, each one intended to test a specific part of the RGW boot up process.

- **Discovery of the number of Ethernet interfaces on the RGW**: the objective of this trial was to check if all Ethernet compliant interfaces currently available on the RGW were correctly detected, considering as invalid interfaces with no physical connectivity. Tests were performed for different sets of interfaces with different physical connectivity availability (all available, none available, some available).
- **Discovery of the WAN interface**: the purpose of the test was to verify that among all valid interfaces, the WAN interface was correctly identified. Trials were performed for the following test cases:
  - Changing the interface of the RGW that is connected to the access network.

  - Changing “EAP-Message” field of the “EAP-Request-ID” message issued by the authenticator to other string than “muse.net”.
- **Authentication process**: the goal of this trial was to check the correct operation of the 802.1X supplicant implemented on the RGW. For this purpose both 802.1X supplicant and AAA Server (RADIUS server) were configured to perform an EAP-TLS authentication. Trials were performed for the below test cases:
  - Credentials sent by the supplicant contain an invalid certificate because the Certification Authority who issued the certificate is not known to the authentication server (the RGW should receive an “EAP-Failure” message).
  - In the same conditions than the previous point, check that after a failed authentication, re-authentication is tried again after 120 seconds.
  - Credentials sent by the supplicant are correct (the RGW should receive an “EAP-Success” message).

4.2 Operation trials

A triple play scenario with applications like voice over IP, video streaming and bulk data transfer, is defined to test the Queue and Scheduling Functional Blocks inside the RGW, since these are the principal blocks to be tested in order to assure a complete end to end QoS. The main RGW operation characteristics to be tested in these trials are the following:

- **Queues functionality**: the RGW implements four queues (one per CoS) per interface. This functionality will be tested in several scenarios where different upstream/downstream flows (associated with video streaming, data bulk traffic and VoIP applications) will be processed at the corresponding queue.
- **Signaling functionality**: how the RGW processes the signaling flows, the overhead of the special treatment of these predefined signaling flows and their marking with a specific CoS different from the data flows.

The selection of applications used for the trials covers the four CoS defined in MUSE project (low latency, real time, elastic and best effort) and is based on the premise of providing a “full service” testing with a limited number of applications:

- **Voice over IP** as an example of the low latency CoS application for signaling flows and real time for data flows with a strict delay requirements. The main requirements for this application are the very low delay and jitter.
- **Video streaming** as an example of real time CoS application and a possible killer application for broadband networks. In addition, this application might generate a considerable amount of traffic and we have divided the tests in two cases, low quality video and high quality video. Within these RGW trials we will test video quality for both unicast and multicast traffic. The bandwidth and packet-loss are the main parameters that can affect the quality of this application. The results of the tests with the video streaming application can be classified in qualitative (subjective) and quantitative ones (objective).
- **Bulk data** as an example of elastic or best effort CoS application. It is related with Internet browsing or peer to peer communication and will be simulated with the Iperf application [10]. They can be considered commodity applications and can be provided with guaranteed QoS or with the lowest quality.

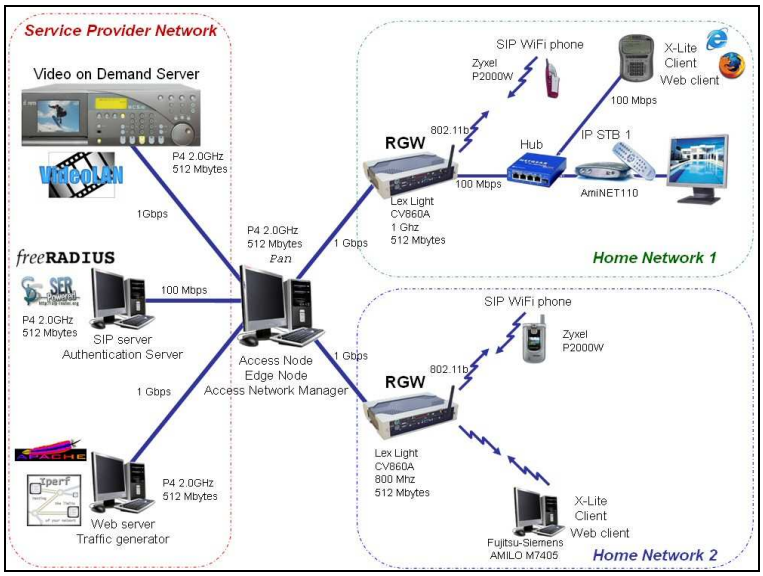

Fig. 4. Network trial testbed

An association between these applications and end to end network requirements (throughput, delay, packet loss and jitter) has to be defined in the trials. The results of the trials with respect to QoS will consider how to score and measure the perceived QoS at each application and/or scenario: objective measurements, subjective measurements and the mapping from network quality to perceived quality.

In order to test all the different concepts and characteristics previously described the considered scenario will be the one depicted in Figure 4. This scenario shows the residential environment on the right part of the picture with two different home networks connected to the Network Access Provider network through different RGWs, that may be connected to the same or different access nodes.

The access node will be 802.1pq aware (like the 802.1ad Ethernet switch in Figure 1) so that it will understand the VLAN encapsulation coming from the RGW with the corresponding p-bits and it will also be able to reformat the frame according to the VLAN schema used within the Network Access Provider network. At the other end (left hand side in the picture), the traffic will be received by the different servers that will provide the requested demand.

Since the development done by our working team in MUSE is focused on the RGW itself, the rest of the network is out of the scope of our workpackage. However, in order to properly test the RGW it was mandatory to emulate the whole network so that the RGW could in fact be involved into a real triple play scenario with real autoconfiguration on startup performed towards the Access Network, real authentication phase towards the Access Network, real signaling messages exchanged towards the corresponding counter part in the network and real services received from the service provider domain.

The triple play services will be provided to two different residential environments that will also interact between them (through a VoIP scenario based on SIP). All this

traffic interchange will be performed within a certain QoS framework that will guarantee the proper treatment of the different flows in the different QoS aware entities so that clients will receive the service without degradation.

4.2.1 Qualitative trials

For these trials, three different kinds of flows were used to test the triple play scenario where video and audio applications are present in the video streaming (using the VLC application [11] for both server and client sides) and VoIP (using SER as the SIP server [12] and X-Lite as user clients [13]). To simulate constant user data (intensive Web browsing, FTP or peer to peer data for example) Iperf is used to generate raw frames in the Server Provider side and collect statistics in the client side.

Although video and data applications were configured using different rates, VoIP was tested using just one codec generating traffic at 120 kbps (high quality audio). To test the video scenario, two different sources were used with different video and audio codecs: low quality where both video and audio are transmitted at 2 Mbps (DivX for video and MP3 for audio) and high quality using 5.2 Mbps (MPEG2 for video and AC3 for audio).

It is important to notice that all experiments were executed during 30 seconds reinstalling all the devices at the beginning and gathering the results at the end. Due to this fact, the relevance of the queue sizes (10000 frames for each queue) is not so important because for a very long experiment the results could differ for a given value. The aim of these tests is to probe the feasibility and performance of the QoS system standardized in MUSE and developed for this prototype and not to obtain the best values for the queues length for a given performance.

Iperf was executed from different servers depending on the required QoS. It is always invoked to generate 100 Mbps.

In the first and simpler test, two different types of flows were generated: the SIP signaling, treated as low latency (the best quality) and the RTP media transfer (the voice) treated as real time. The registration process of both the SIP phone and the X-Lite SIP software is always almost instantaneous and the delay could be considered negligible. In the data (voice) transmission, no packets were dropped in the RGWs and no delay was appreciated.

In the second test, the goal is to observe the performance of the VoIP communication in a high load scenario when both signaling and data voice are marked with the highest priority. The results of this test were clear: both registration and data (voice) transmissions are performed with no delay even when the high load traffic was marked with the best quality of service. Only when there is a continuous audio stream being transmitted it can be appreciated that very small cuts appear and that the sound is perceived with a metallic tune. These effects are not appreciated in a normal VoIP conversation.

The third test tries to represent a complete triple-play scenario (with voice, low quality video and Iperf) where voice is marked with the highest priority, video uses the next one and Iperf simulates a high load traffic using variable priority (the lowest one in the first scenario, the same one than the video in the second scenario and the highest in the last one). With these three different scenarios the behavior of both the voice and the video transmission depending on the high load priority traffic is compared. The results confirm that the voice has too a low rate to be affected (even

although a high rate codec was selected precisely because of this reason) by other traffic and video with low quality is unaffected too due to this fact.

The final scenario repeats the last tests using a high quality video. This time, when the high load is marked as low latency, the video reception is too bad (neither the video nor the audio are received during the high load transmission). As soon as the Iperf transmission ends, the video restarts its reception in the client side (it needs 2 or 3 seconds to resynchronize).

4.2.2 Quantitative trials

The purpose of these final tests is to determine the real quality of the different flows focusing on the bandwidth and the jitter, so that the subjective results obtained in previous tests can be measured.

In the first scenario, three different Iperf flows are sent towards the same end user device in order to test the efficiency of the QoS procedure implemented in the RGW. Table 1 gathers the information about the test parameters including the bandwidth and the instant when the Iperf flows are started and stopped and the results are presented in Figure 5. As it can be seen, during the first ten seconds, the first flow shows the input rate at the output due to the RGW LAN interface whose performance is just 95 Mbps due to hardware limitations. As soon as the medium priority flow starts, the low one decreases its rate while the former is totally served. In the 20-40 seconds range, the three flows share the LAN interface but, as the RGW prioritizes the frames following the marks, the low priority flow is not served any more and its frames are lost because the queues have just capacity for 1000 frames. When the high priority flow ends, the low priority one gets some bandwidth and is totally served again when the medium priority ends. Regarding the jitter, the most important area is the range between 20-40 seconds where there are huge jitter variations for the medium priority frames and high jitter variations for the low priority one. The reason for this is that almost all low priority frames go lost so there are no frames to estimate the jitter. The jitter for high priority frames is almost inappreciable.

The aim of the second test is to show how low priority applications always use the available bandwidth if there is any. The results are as expected: between 20-40 seconds, the three flows share the medium with the two highest priority flows completely served and the best effort one using the available bandwidth. High priority frames do not suffer any jitter (or it is not perceptible), medium priority ones have less jitter than in the previous test because this time all frames are served but, as the higher priority are served first, there exists some jitter. Best effort frames are also served but after higher ones so a big jitter is introduced.

Table 1. Flow parameters for the first, second and third tests.

Priority	**Rate[Mbps]**			**Start [s]**			**End [s]**		
	1st	2nd	3rd	1st	2nd	3rd	1st	2nd	3rd
Best Effort (Low)	100	100	40	0	0	0	60	60	40
Real Time (Medium)	30	20	40	10	10	0	50	50	40
Low Latency (High)	80	60	60	20	20	10	40	40	30

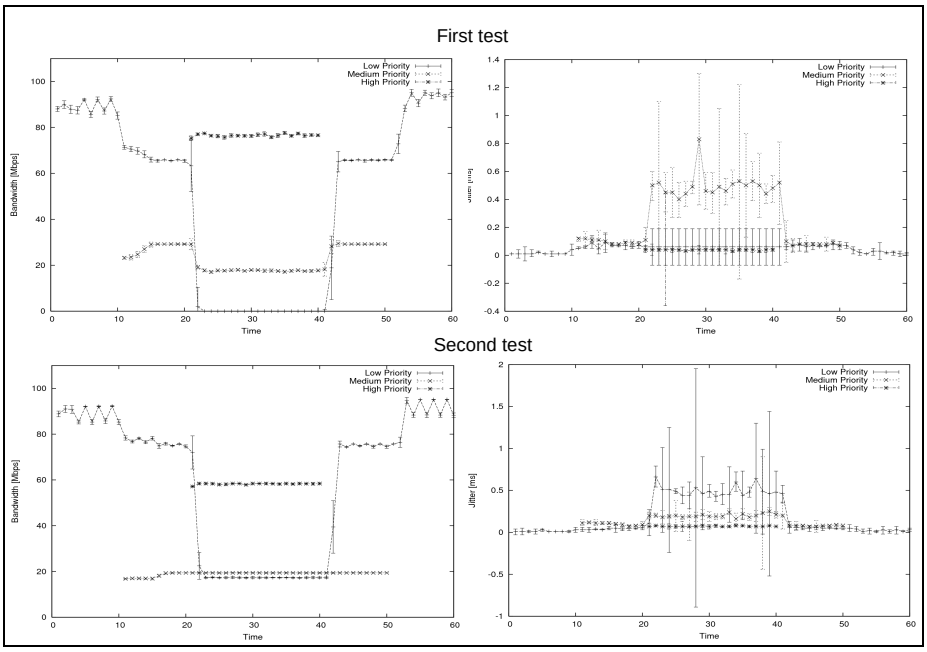

Fig. 5. Bandwidth and jitter value for the first and the second test

In the last test it is intended to see how two flows with the same priority share the remaining bandwidth in a Round Robin fashion. The result is the expected one: in the 10-30 seconds range, the highest priority flow gets the best service, while the two other flows reduce the output to 20 Mbps.

5. Conclusions

This article has presented the RGW prototype that has been developed and trialed within the framework of an Ethernet access network in a FTTH broadband scenario such as the one specified in the MUSE project.

The RGW prototype is prepared so as to be integrated in a QoS environment like the one specified by the MUSE project and the most important characteristics included in the prototype, are the following ones:

- The RGW prototype is capable of autoconfiguring itself independently of the hardware and of the network environment where it is deployed.
- The authentication procedure based on IEEE 802.1X is very flexible and allows many specific authentication methods to be applied.
- The RGW offers a very flexible configuration/management API making it possible to access it by means of a Web based interface, through the DSL Forum TR-069 standard, or through SIP (these are the implemented possibilities although any other could be integrated).

- The QoS capabilities included in the RGW allows it to expand the IEEE 802.1pq tagging schema used in MUSE access network towards the home network and it is also capable of treating the different flows accordingly to their marked QoS.
- The RGW is also capable of marking the different flows in the upstream direction with the required QoS.
- The RGW prototype incorporates an ALG in order to overcome NAT traversal problems caused by the SIP signaling messages.

These characteristics have been trialed and the different results have been shown in this article both from a qualitative and from a quantitative viewpoint.

For the second phase of the project (MUSE will finish at the end of 2007), different enhancements are being studied: integration of prototype into a TISPAN-NGN scenario, users and service roaming, fixed mobile convergence scenarios, value added services provided within the RGW (video server) or managed by the RGW (e-care), etc.

Acknowledgements
This article has been partially granted by the European Commission through the MUSE (IST-026442) project.

References

1. MUSE. Multimedia Access Everywhere. European Union 6th Framework Programme for Research and Technological Development. http://www.ist-muse.org
2. DSL Forum TR-069: CPE WAN Management Protocol, May 2004
3. The Click! modular router project. http://www.read.cs.ucla.edu/click/
4. QoS Management in Fixed Broadband RGWs. C. Guerrero, J. Garcia, F. Valera, and A. Azcorra. IFIP/IEEE International Conference on Management of Multimedia Networks and Services. MMNS 2005 (Oct 2005), Barcelona (Spain)
5. Designing a broadband RGW using Click! modular router. H. Gascón, D. Díez, J. García, F. Valera, C. Guerrero and A. Azcorra. IFIP EUNICE (Networked applications) 2005 (Jul 2005), Madrid (Spain).
6. Demo of Triple Play Services with QoS in a Broadband Access RGW. F. Valera, J. García, C. Guerrero, V. Pinto, V. Ribeiro. IEEE Infocom 2006. Barcelona (Spain)
7. IEEE Std 802.1X™- 2004, 802.1 IEEE Standard for Local and metropolitan area networks
8. IETF RFC 3748, June 2004. Extensible Authentication Protocol (EAP)
9. IETF RFC 2716, October 1999. PPP EAP-TLS Authentication Protocol
10. Iperf: The TCP/UDP Bandwidth Measurement Tool. http://dast.nlanr.net/Projects/Iperf/
11. VLC: VideoLAN Client. http://www.videolan.org/vlc/
12. SER: SIP Express Router. http://www.iptel.org/ser/
13. X-Lite. SIP Software Phone. http://www.xten.com