Automatic Provisioning of End-to-End QoS into the Home

Lukasz Brewka, *Student Member,* IEEE, Pontus Sköldström, Jelle Nelis, *Member,* IEEE, Henrik Wessing, *Member*, IEEE, and Chris Develder, *Member*, IEEE

Abstract — *Due to a growing number of high bandwidth applications today (such as HDTV), and an increasing amount of network and cloud based applications, service providers need to pay attention to QoS in their networks. We believe there is a need for an end-to-end approach reaching into the home as well. The Home Gateway (HG) as a key component of the home network is crucial for enabling the end-to-end solutions. UPnP-QoS has been proposed as an in-home solution for resource reservations. In this paper we assess a solution for automatic QoS reservations, on behalf of non-UPnP-QoS aware applications. Additionally we focus on an integrated end-to-end solution, combining GMPLS-based reservations in e.g., access/metro and UPnP-QoS based reservation in the home network*[1].

Index Terms — Automation of QoS, inter-domain QoS, GMPLS, UPnP-QoS

I. INTRODUCTION

The importance of Quality of Service (QoS) provisioning cannot be overemphasized. With triple and quadruple play being offered by many service providers, and constant service upgrades exhausting the capacity of the networks, QoS assurance is a must in order to provide a proper user experience. This brings the attention of Internet Service Providers (ISPs) when their access networks are considered, but we believe the QoS aspects should also be addressed in home networks. Modern home networks comprise a mix of different devices starting with white and brown goods, through alarm systems and phones, to video storage servers and HD displays. This heterogeneous environment inside a home is calling for QoS assurance but also for user-friendly ways to manage the network, especially since network devices could join and leave home networks relatively often (either because they are physically moving, or they are turned on/off). To cope with this dynamic environment in a user-friendly way, we will consider UPnP-QoS and propose an extension that should allow more automated QoS establishment between end devices and a Home Gateway (HG). Aside from the establishment of QoS within the home we are also concerned about the interaction of HG with the outside world (i.e., usually with the access network) in order to extend the QoS provisioning as close as possible to service provider hosts. As an access network technology we consider an Active Optical Network (AON) based on Ethernet. A couple of approaches towards QoS can be discussed when access networks are considered, all falling into two general categories (or their mix) i.e., Differentiated Service (DiffServ) or Integrated Services (IntServ). While DiffServ gives fairly good results, only IntServ is able to give hard QoS guarantees. For this reason in the scope of AON networks we are particularly interested in the Generalized MPLS (GMPLS) protocol suite integrating OSPF-TE as routing and RSVP-TE as resource reservation protocols. Though MPLS and GMPLS are usually seen as core network technology, during recent years they have been moving towards the end customers (so called *MPLS access*). GMLPS's support for traffic engineering and multi-technology data planes (e.g., high capacity optical networks) together with the future need for bandwidth in this part of the network makes GMPLS a valid candidate for a future control plane.

Addressing the issues of non-UPnP-QoS compliant devices which normally can compromise QoS in the UPnP-QoS managed network, and proposing a control and management plane interface between the UPnP-QoS and GMPLS networks is an important step towards building automated integrated QoS. This paper contributes firstly with a proposal of automatic classification of traffic flows for resource reservation, and assessment of required level of classification accuracy. Secondly, we show interworking of GMPLS and UPnP-QoS to realize end-to-end resource reservation across access/metro into the home network. This is a true end-to-end approach for QoS provisioning, not only from the HG but from the end device in a user's home up to an (access) server.

The remainder of this paper is organized as follows. Section II describes related work. In Section III the basics of UPnP-QoS and GMPLS are presented. This is followed by a description of flow classification and UPnP-QoS extensions in Section IV. Next the proposal of mapping between UPnP-QoS and GMPLS parameters is presented in Section V. Section VI describes the modeling, implementations and simulations with their results. Finally the conclusions are given in Section VII.

II. RELATED WORK

The automation of QoS establishment was previously

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7) under project 212 352 ALPHA, and from the Flemish Government through the IBBT ICON project OMUS. C. Develder is supported in part as a post-doctoral fellow of the Research Foundation – Flanders (FWO).

L. Brewka and H. Wessing are with the Technical University of Denmark, Department of Photonics Engineering (e-mail: ljbr@fotonik.dtu.dk, hewe@fotonik.dtu.dk)

P. Sköldström is with Acreo AB, Sweden (e-mail: ponsko@acreo.se)

Jelle Nelis and Chris Develder are with Ghent University - IBBT, Belgium, (e-mail: jelle.nelis@intec.ugent.be, chris.develder@intec.ugent.be)

addressed in the context of traffic classification and gateway design. Automatic traffic classification for QoS provisioning was presented e.g., in [1], where a traffic signature based approach is proposed for Class-of-Service (CoS) marking. In [2] the authors stress the importance of scalability and trade-offs between precision and computational complexity comparing different approaches to automated classification. The scalability is also being addressed by authors of [3], who consider classification in the ISP network, though problems like asymmetric routing and real-time matching vs. ISP network size arise.

Some early work in the field of QoS home gateways is presented in [4], where authors use a QRG (QoS-aware Residential Gateway) for bandwidth management; but it is limited to Differentiated Services Code Point (DSCP) remarking and Class Based Queuing (CBQ) properties adjustment. Also the authors of [5] point out the need for exchange of QoS information between home and access networks. They propose to outsource the traffic classification to the access network (similar to [3]). They correctly claim that use of RSVP requires that applications are specially re-written, per flow reservations raise the scalability issues, and typical consumer equipment potentially lacks the resources for RSVP support. They propose a scheme that requires a copy of user's traffic to be sent to a centralized classifier.

The authors of [6] propose a design of IMS-based set-top boxes providing network performance feedback, and allowing the priority increase in the operator's network, similar like [4] the solution is based on DSCP.

An investigation of end-to-end QoS establishment and some work on integration of reservations is presented in [7] where the authors use SIP information to discover the domains to request QoS in. The authors however do not explain how specific QoS parameters (bandwidth, delay, etc.) are signaled in different domains.

In [8] the multi-residential gateway is treated and the Hierarchical Token Bucket (HTB) with FIFO queues is proposed for providing link sharing with real-time services. The authors point out that locally managed solutions (like [8] and [4]) are more suitable for QoS support comparing to those that rely on control protocols.

The authors of [9] present the idea of Automatic QoS Control in UPnP networks by defining a special component i.e., Automatic Control Point (ACP). ACP should detect the flow in its initial phase and request QoS from the QosManager service (QM). The authors in their paper however focus just on the classification part, not considering specifics of interactions between UPnP-QoS services nor showing how the presence of a classifier influences the QoS level in the network. We will address some unresolved issues and propose modifications that allow integration of non-UPnP-QoS devices in the UPnP-QoS Architecture.

In this paper we propose moving the classification functionality as close to its source as possible. Thus, we treat traffic auto-classification as a supplement to the functionality performed by a UPnP-QoS Control Point (CP). This also addresses a scalability issue as this excludes the requirement for redirecting a copy of all customer traffic to a centralized classifier in the access network as in [3]. On the other hand our solution requires only a few modifications to the standard Layer 2 or 3 (L2/L3) UPnP-QoS-enabled network component's behavior, however while we do not make modifications to the UPnP-QoS services themselves (see details in Section IV).

When interaction with the access network is considered in order to provide hard guarantees, we consider traffic marking and shaping alone as insufficient and we combine it with signaling protocols. We propose using RSVP for resource reservation and the reservation itself is HTB reconfiguration (details are presented in Section VI).

When scalability in the access network is considered, in our scenario only a few quality sensitive applications need translation of UPnP-QoS parameters to access reservations and scalability is not of a great concern as global end-to-end reservations are segmented into reservations limited to smaller domains. Additionally, we do not necessarily have a 1:1 relationship between application flows and network reservations i.e., application flows can be merged into a single reservation thus reducing the amount of signaling state.

III. UPnP-QoS and GMPLS basics

A. UPnP-QoS Architecture

The UPnP-QoS Architecture is the extension of the UPnP protocol suite that defines additional services and entities that are interacting with each other to manage QoS in the home network. There are four entities that are involved in QoS establishment:

- *QosPolicyHolder (QPH)* [10] – service that provided a Traffic Descriptor returns policies for this traffic.
- *QosDevice (QD)* [11] – service running on any device that is involved in handling traffic, it can be a source, destination or intermediate node for the traffic that QoS is requested for, it has to be able to control its own resources.
- *QosManager (QM)* [12] – service that establishes QoS between traffic source and destination through interaction with QPH and QDs.
- *Control Point (CP)* – is not a service itself, it is an entity that requests QoS; this request is based on prior knowledge of Traffic Specification, and traffic source and destination.

Fig. 1 presents the interaction between the entities of the UPnP-QoS Architecture during QoS setup. The QoS establishment of one flow can cause preemption of another flow of lower importance. The horizontal dashed line in the figure splits the scenarios with preemption disabled (above the line) and enabled (above and below). The importance of the flow can be signaled on two levels, one is purely on the control level and is referred to as User Importance Number (UIN) the second is on the data traffic level and is called Traffic Importance Number (TIN). UPnP-QoS supports three types of QoS, *prioritized* QoS, which is simply prioritizing packets of certain flows, *parameterized* QoS which reserves

resources between the source and destination of the flow, and *hybrid* QoS which uses parameterized QoS on segments that support it and falls back to prioritized QoS.

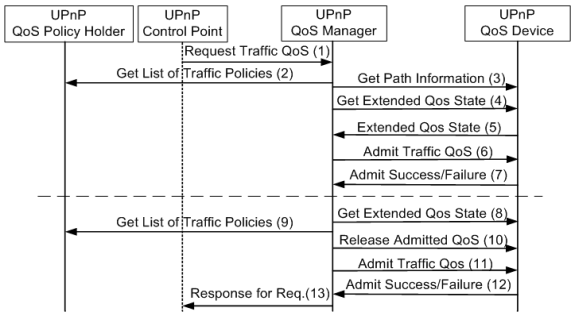

Fig. 1. Interaction diagram for Traffic QoS request.

In a fully UPnP-QoS controlled network all the sources of the traffic in the network (i.e., all the applications, devices) are starting the traffic transmission after requesting QoS from the QM. As long as all the sources are requesting resources before transmission and do not proceed with the transmission in case the resources are not granted there should be no problems with the level of QoS due to network congestion. On the contrary, the level of QoS may be degraded when in the network there are also some non-UPnP-QoS devices[2]. That is especially true for prioritized QoS setup, as it might be that a non-compliant device is flooding the network with packets marked with high priority causing the prioritization scheme to fail. For parameterized setup the traffic coming from non-compliant devices can be treated in a number of ways. This traffic could be simply discarded, which might be considered as an extreme approach. The other approach is to treat this traffic as best-effort traffic despite the application's requirement. The third option is to perform traffic classification and have an entity acting as CP and requesting the proper QoS for the application. In sections III and V we have a look at this last approach, its potential and validity.

B. *In access QoS - GMPLS/RSVP*

Generalized MPLS (GMPLS) is a suite of protocols developed by the IETF for reserving resources, setting up circuits and performing traffic engineering in multi-technology networks for example combinations of MPLS, SDH, and OTN. Reservations are made through the signaling protocol RSVP-TE [13] which transmits reservation requests that contains a traffic specification. The request messages are transmitted from ingress to egress nodes in a hop-by-hop fashion and accumulate information about the state of the nodes as it passes. In case the nodes have the capacity to meet the traffic specification, the procedure is finalized by the egress node sending a confirmation message to the ingress using the reverse path. The reservation procedure is interrupted if one of the intermediate nodes is lacking resources. The GMPLS suite contains other protocols (OSPF-TE, LMP, etc.) as well as entities separate from the network nodes themselves e.g., a Path Computation Engine that calculates a path suitable for a particular reservation or a Service Management System that is responsible for initiating reservations.

[2] non-UPnP-QoS device refers to a device non-compliant with UPnP-QoS i.e. not implementing a QosDevice Service.

IV. AUTOMATION OF UPNP-QOS

In this section we describe the problem of auto-classification of the traffic from non-UPnP-QoS devices present in the UPnP-QoS enabled network. Such scenario is depicted in Fig. 2 where green lines indicate reservations performed by UPnP enabled devices, while the red line is an example of a flow without a reservation. The idea we present is to place a traffic classifier in the intermediate nodes that would perform the classification and request QoS from the QM. In following sections we analyze the capability of traffic auto-classification and present how it fits in UPnP-QoS architecture.

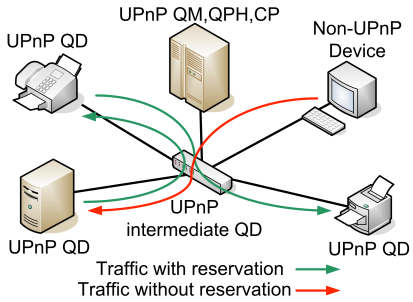

Fig. 2. UPnP-QoS home network model.

A. *Flow classification*

This section presents an overview of challenges in traffic classification and a short description of a promising application using automated QoS provisioning. Performing accurate traffic classification is not an easy task. When the establishment of QoS is considered, an additional requirement for such a classifier is its speed (understood as how much time it requires to perform the classification after the flow was initiated). Simple methods for traffic classification that are based on well-known ports, have been proven insufficient [14]. The difficulty in classifying traffic is caused by the fact that network traffic nowadays comes from applications that use dynamic port negotiation, avoid well known ports, and large amounts of traffic is sent as HTTP [15]. Presence of aforementioned applications has lead to development of more advanced methods for more advanced traffic classification. The methods differ as their purpose is different ranging from long term network planning, security enforcing and finally QoS provisioning.

In this paper we are not focusing on particular classification methods, we relate to the work showing performance of techniques proposed to date. For the QoS provisioning problem described in this paper we will consider the use of the Appmon application [16]. Appmon uses a three-layer classification. On the first layer packet inspection is used, the payload is inspected to identify characteristic application messages. The second layer depends on protocol decoding and uses publicly documented application level protocols. Finally,

the third layer is based on header inspection. The sequence of the classification layers aims at the lowest misclassification possible [16].

As stated earlier the amount of time consumed by the classifier is important as far as QoS provisioning is considered (i.e., the classifier should be able to detect the need for QoS and reserve it accordingly, quickly enough not to hamper user experience). Fortunately, after capturing the protocol control messages typically sent at the beginning of a flow, Appmon can usually perform positive classification after only 100 bytes of packet payload. This low latency together with around 90% accuracy is a good base for flow categorization methods that can be used for network supported UPnP-QoS provisioning. Though packet inspection may pose a high computational load, based on Appmon's CPU usage [16], we believe this type of classification method can be used in foreseeable future in a home or office environment.

B. UPnP-QoS with Automatic Flow Detection – NBCP

Here the changes to the standard behavior of some devices within a UPnP-QoS network are described. It is important to mention that our goal is to achieve auto classification in UPnP-QoS with minimal changes to its components.

To define the required modifications we consider a home network environment with full UPnP-QoS functionality and non-UPnP-QoS devices (as in Fig. 2). We also make the assumption that the home network infrastructure in the network considered is built from UPnP-QoS compliant devices with QD services. Assuming intermediate nodes e.g., switches, gateways are compatible with UPnP-QoS is crucial for supporting QoS in this home environment. The non-compliant devices, for which our proposed extensions enable interworking with the UPnP-QoS architecture, are assumed to be end devices.

An intermediate QosDevice service, which we will refer to also as Home Gateway (HG), interconnects UPnP-QoS services (QM and QPH) and four devices. Three of those devices are UPnP-QoS compliant and one is a non-compliant device that simply starts packet transmission without prior signaling. In a case where some non-UPnP-QoS devices start transmission, there are a couple of approaches, as described before, to treat their traffic. We will focus on the solution where traffic classification is attempted, and for successful classification QoS is requested. Since our focus is parameterized QoS as the only way to provide strict guarantees on QoS, and since this QoS setup already demands at least some level of packet inspection (verification of source/destination ports, addresses), we think that auto-classification provides most additional functionality for reasonably low additional inspection effort.

Part of the normal interaction between the QM and the CP as depicted in Fig. 1 is the QM reporting an outcome of a resource reservation attempt. If the QM reports a failure the CP (that usually would be a UPnP aware application) should back-off and try to request resources at a later time. When we are dealing with a centralized Automatic CP (ACP) like in [9], even in a case of very fast flow classification, where the ACP requests QoS and receives a failure notification, there is no mechanism that can stop the source device from transmitting the traffic and compromising the QoS.

In such circumstances the only way to stop the traffic is to discard it on the first intermediate device so it does not waste the network resources or, what is worse, cause congestion. An alternative to this approach is granting fewer resources than asked for. However, this may cause an unacceptable degradation and hence unusable application, which leads to the assigned resources being wasted.

In order to develop functionality required for automation of QoS setup, we need some modification on the intermediate devices. Below we present a list of UPnP-QoS network components and services and modifications that we propose in order to allow UPnP-QoS to efficiently accommodate non-UPnP-QoS devices. As described earlier, our intention is to minimize these modifications.

a) QosPolicyHolder service requires no modifications, remains stateless, identical with standard UPnP implementation.

b) QosManager service requires no modifications, remains stateless and identical with standard UPnP implementation.

c) QosDevice service itself does not require any modification, the only minimal modification that is required is referring to the device as a whole[3] and requires packet marking - all the packets should be marked to indicate packets from UPnP-QoS compliant device. This is an optional modification in order to lower the load on the traffic classifier. *QosDevice* service for intermediate devices also stays unmodified, but additionally the intermediate devices should be equipped with a Network Based Control Point (NBCP). The NBCP is a component that based on the flows classification, requests QoS from the QM. The packets belonging to flows that were successfully classified and admitted on the path, should be marked as compliant, lowering the load on other classifiers that could reside in the other network components. What makes our approach different from ACP, is that in our architecture the functionality of the CP together with the detector should be placed in all intermediate QDs that interconnect the end devices, as in this way network flooding by a non-compliant traffic can be avoided. Additionally, we propose packet marking in order to lower the processing power required for the classifiers (we think that at least some traffic will be generated by the UPnP-QoS aware applications and this traffic does not require in-depth inspection). Described service should maintain soft state of classified flows, reset after flow's activity discontinues. To tackle scalability issues, each intermediate device only classifies flows originating from directly connected end devices. As for maintaining the state of all ongoing reservations passing through certain network devices scalability is not of a big concern in the home network due to a limited number of flows. The NBCP together with QD functionality would create a new type of device. There might

[3] Note the difference between the QosDevice service and the implementation of the traffic management functionality.

be some issues with placing the classifier in all the intermediate nodes of the network, but we would like to notice that it is not a must. For cases where some simple network nodes are not capable of performing traffic classification the architecture as proposed still can improve QoS management. However, lack of auto-classification in some intermediate devices, implies possible QoS degradation in network segments "behind" these devices and more load for classifiers in remaining part of the network.

V. MAPPING QOS BETWEEN HOME AND ACCESS NETWORK

In this section first we present prioritized and parameterized QoS in both UPnP-QoS and GMPLS. This creates the base for presentation of the proposed mapping scheme between QoS parameters in home and access networks.

A. Prioritized QoS in UPnP-QoS

The main advantage of prioritized setup is its simplicity and scalability, but it does not provide any end-to-end guarantees. In prioritized QoS setup in UPnP-QoS after the CP requests QoS the QM determines which QDs should take part in the traffic forwarding, by invoking the *GetPathInformation* action, and it verifies the state of these devices via the *GetExtendedQosState* action. Next, the QM obtains the TIN for this particular traffic flow from the QPH and attempts the establishment of the QoS on the QDs using the *AdmitTrafficQoS* action, passing the Traffic Descriptor with proper TIN as this action's argument. If no errors occur throughout the above procedure and the configuration of the QDs, then the specific traffic flow should be admitted and the QM sends to the CP an UpdatedTrafficDescriptor which contains up-to-date information about the traffic specification.

The TIN, along with the TrafficId (used for unique identification of packets belonging to particular stream), is the only mandatory part of the Traffic Descriptor when setting up prioritized QoS.

B. Parameterized QoS in UPnP

Parameterized QoS guarantees that admitted traffic will be treated in the desired manner. Parameterized QoS setup is performed similarly as in the prioritized case (with additional parameters described below).

The key parameters for parameterized QoS (similarly like for prioritized) are in the Traffic Descriptor structure passed during the *AdmitTrafficQoS* action. The most relevant parameter for parameterized QoS setup is the *AvaialbleOrderedTspecList*, which contains a list of Traffic Specifications (Tspec). Tspec is composed of a number of traffic parameters listed below together with their units, the only mandatory parameter is marked in bold.

1. **DataRate,** bytes per second
2. RequestedQosType, prioritized, parameterized or hybrid
3. TimeUnit, smallest time interval in µs
4. PeakDataRate, bytes per second
5. MinServiceRate, bytes per second
6. ReservedServiceRate, bytes per second
7. MaxBurstSize, bytes
8. MaxPacketSize, bytes
9. E2EMaxDelayHigh, upper bound for the E2EDelay, in µs
10. E2EMaxDelayLow, lower bound for the E2EDelay, in µs
11. E2EMaxJitter, µs
12. QosSegmentSpecificParameters, Interface ID, QoSSegment ID and Segment specific delay and jitter values

C. Prioritized QoS in GMPLS

Prioritized QoS in GMPLS network is based on the Differentiated Services (DiffServ) where the Per Hop Behavior (PHB) defines the processing of packet-flows associated with particular label. This information is carried in the RSVP-TE DiffServ Object [17]. RSVP can signal DiffServ in two ways:

a) for packet oriented networks an E-LSP approach can be used. E-LSPs support multiple Ordered Aggregates (OAs) and the priority indicate the packets' PHB (traffic that belongs to single OA it is assigned the same Per Hop Behavior Scheduling Class (PSC) and drop precedence),

b) for cases where priority is determined by the label, L-LSPs are used. L-LSP is used to carry the single OA traffic, it supports single PSC signaled during the LSP setup procedure (the priority bits can indicate the drop precedence).

D. Parameterized QoS in GMPLS

In parameterized QoS setup usually referred to as Integrated Services (IntServ), two types of services are available: Controlled Load (CL) [18] and Guaranteed Services (GS) [19]. CL should provision QoS to provide the forwarding characteristics a flow would receive in unloaded network, CL parameter are listed below (1 - 5). GS provides more strict QoS that guarantees no packet drops and strict delay boundaries, GS uses parameters 1 to 7.

1. Token Bucket Rate (r)
2. Token Bucket Size (b)
3. Peak Data Rate (p)
4. Minimum Policed Unit (m)
5. Maximum Packet Size (M)
6. Rate (R) - increases the token bucket rate (r) to reduce queuing delays such that - r=<R=<p
7. Slack Term (s) - defines the difference between the desired delay and the delay obtained using the rate R

The QoS parameters are signaled during the reservation procedure through Path and Resv messages that pass the traffic flow information to the LSRs (Label Switching Routers) on the path.

To collect the information about the capabilities and resources available on a path the Path message contains an *Adspec* object that is updated by the traversed nodes. Once the Path message reaches the destination the *Adspec* reflects the end-to-end state of the path. The *Adspec* object is composed of a default fragment for both Control Load and Guaranteed Services; and from service specific fragments.

The *Flowspec* object is part of the RESV message and contains the *ReceiverTSpec* that describes the traffic flow and an *Rspec* which defines the desired service parameters

required for the service to be invoked.

E. Inter-domain control and management for QoS

The study of the QoS mechanisms and methodologies used in UPnP-QoS and GMPLS shows a good match between the UPnP-QoS TrafficDescriptor and RSVP-TE parameters. The following subsections will present the mapping for prioritized and parameterized QoS setups.

1) Inter-domain mapping for Prioritized QoS

For prioritized QoS the mapping is straightforward. The only parameter that is used in UPnP-QoS is the TIN which should be mapped into the PHB in the GMPLS domain. For the simplest case, eight TINs could be mapped into the eight different values of the EXP bits. In more general case where the TIN matching has to be done with the L-LSP, the Label Edge Router (LER) connected to the home link has to be aware of the level of QoS support in a particular LSP.

However, the situation becomes complex when there is a mismatch in a number of available classes in the home and access. The need for class merging or splitting could be addressed in a couple of ways:

a) merging based on the requirements; merging all control traffic in one group, all real-time traffic in the other, etc; or

b) one can consider remote management of the HG using TR-069 [20] – the number of TINs returned by the QPH for flows that will be directed to the access network could be limited, achieving a one-to-one mapping.

2) Inter-domain mapping for Parameterized QoS

In order to perform mapping for parameterized QoS setup matching RSVP *SendersTSPEC* parameters with the UPnP-QoS Traffic Descriptor is most significant. The part of the Traffic Descriptor that contains the information required for parameterized QoS has to be mapped into the CL or GS parameters. Table I presents the proposed mapping between the UPnP-QoS parameters and GMPLS/RSVP-TE parameters. Explanation for unmapped parameters and clarification of chosen mappings is described below.

The MinServiceRate parameter is defined as the minimal bitrate that is acceptable for the requesting application, it is not mapped as there is no equivalent parameter in the GMPLS domain. This is not an issue, as the reservation is performed to provision the proper QoS for the service in question and the Data Rate parameter is sufficient for that purpose.

There is no parameter defined in UPnP-QoS that could indicate the Minimum Policed Unit (m) which indicates the minimum size of the processed packets in order to estimate the worst case overhead for bandwidth calculation [21]. Translation of this information is not mandatory though its lack might cause miscalculation of available bandwidth.

TABLE I
MAPPING BETWEEN UPNP-QOS PARAMETERS AND GMPLS-RSVP

UPnP-QoS parameter	GMPLS/RSVP-TE parameter
RequestedQosType	DiffServ/IntServ
Data Rate	Bucket Rate (r)
Time Unit	1000000
Peak Data	Peak Data Rate (p)
MaxBurstSize	Token Bucket Size (b)
MinServiceRate	–
ReservedServiceRate	Rspec (R) - FLOWSPEC
MaxPacketSize	Maximum Packet Size (M)
–	Minimum Policed Unit (m)
E2EMaxDelayHigh	based on Ctot, Dtot
E2EMaxJitter	based on Min and Max Latency
E2EMaxDelayLow	Minimum Path Latency
–	Slack Term
ServiceType	0 (CL) or 1 (GS)

Rate R (reserved service rate reflecting the actual rate reserved); and Slack Term [19] - are not ordinarily mapped between UPnP-QoS and GMPLS but instead should be returned to the CP to update the TrafficDescriptor.

The most critical delay related parameter is E2EMaxDelayHigh. As the LSR does not have any knowledge about the committed delay in the home network it cannot be sure that the LSP total delay meets the requirement of the requesting application. In order to save resources we propose a LER behavior where the LSP is released or an error is signaled once the LSP delay is higher than the requested E2EMaxDelayHigh. Additionally, the interface between home and access network should include the possibility of reporting the LSP's MaxCommittedDelay parameter allowing the QM to send the E2EMaxCommittedDelayHigh in the Updated-TrafficDescriptor to the CP. The UpdatedTrafficDescriptor received by a CP would include the delay calculated until the end of the LSP in the access network, which allows the CP to verify if this delay value is within acceptable bounds.

The maximum delay for LSP can be calculated based on the token bucket parameters, C_{tot}, and D_{tot} values according to (1) [21]. The resulting parameter should be mapped to MaxCommitedDelayHigh and reported to the QM.

$$E2Edelay = b/R + C_{tot}/R + D_{tot} \tag{1}$$

where b is the token bucket depth, R is the reserved rate, C_{tot} and D_{tot} are the described earlier error rates.

For reporting MaxCommitedJitter (where MaxJitter is the upper bound on the end-to-end jitter defines as a difference between maximum of End-to-End Delay and the minimum of End-to-End Delay) we propose the maximum LSP jitter to be calculated based on the Minimum Path Latency (part of the default *Adspec* [21]) assuming that (2) holds.

$$MaxCommitedJitter = \max(Jitter_1, Jitter_2, \ldots) \leq b/R + C_{tot}/R + D_{tot} - MinimumPathLatency \tag{2}$$

where $Jitter_n$ is a jitter value based on a number of consequential packet delay measurements.

This value should be reported to the QM which composes

E2EMaxCommitedJitter value to be sent to the CP in the UpdatedTrafficDescriptor.

VI. Implementation and Results

In this section we present the implementations used to verify our proposals and the results of this verification. First we present results of simulations of in-home traffic auto-classification for the purpose of QoS provisioning in order to assess if traffic auto-classification brings improvement of the QoS level, and to determine the classification accuracy that allows for obtaining satisfactory results. Next, we detail the mapping functionality, we describe the implementation of the interface and home and access networks, and later we show some results of cross-domain QoS setup.

A. Network Based Control Point

1) Model details

The model used for verification of usability of NBCP consists of the elements presented in Fig. 2 interconnected by be full-duplex 70 Mbps links. Each of the presented UPnP QDs is equipped with: a) a module managing and reporting the state of its resources, b) a source that generates traffic, and c) a sink used for obtaining statistics. The flows are generated on the CP's request with tunable exponentially distributed rate. The priority of each flow is assigned uniformly between 0 and 7. The resources assigned to flows range between 5 and 30 percent of sub-queue capacity. The pair of source and destination is randomly selected.

The non-UPnP-QoS device generates traffic in eight classes towards random destinations. The average traffic generated by the non-UPnP-QoS device is equal to 50Mbps. The intermediate UPnP QD has the same UPnP-QoS functionality as the network end-devices with the difference that it is neither a source nor a destination of any other than the management traffic. It performs switching of packets between the source and destination, and on the outbound interface it queues the packets according to their class. The outbound interface is UPnP-QoS managed (i.e., the device verifies if it is possible to accommodate this reservation upon resource request arrival).

The traffic detection is simulated with out-of-band communication between the centralized CP and the non-UPnP Device. In this way any detection accuracy can be simulated. Flows with auto detected QoS are described with the lowest UIN. We consider eight classes on the TIN level - Class 0 for the lowest priority and Class 7 for the highest. The end devices use FIFO queue for outbound traffic. The intermediate device is using Weighted Round Robin, providing highest bandwidth to classes 7 and 6 (4 x minimum bandwidth unit) and lowest to classes 0 and 1 (1 x minimum bandwidth unit). The holding time for each of the flows is set to 120 seconds and the QoS request rate changes between 0.3 and 2 requests per second.

2) Simulations and Result

The analysis of efficient traffic classification and its influence on the QoS level in the UPnP-QoS network are based on a number of test scenarios described in this section. We chose to present the QoS level by delay characteristics as in our model delay is the most important influenced parameter by the injection of the traffic from non-complaint devices. We first consider a network fully controlled by UPnP-QoS. Then, we show the influence of placing a non-UPnP-QoS device in the modeled network. Finally, we present improvement of the QoS level after deployment of proposed UPnP-QoS extensions for different traffic classification accuracies. Chosen reservation rate range allows assessment of the network under loaded and unloaded conditions.

Fig. 3 presents the results for a fully controlled UPnP-QoS network. It is clearly visible that the delay values are very limited (close to transmission delay: 2×512B/70Mbps = 0.12ms). On the contrary the delay values in Fig. 4 are extremely high and this is caused by presence of the non-UPnP device generating a number of flows assigned to different L2/L3 priority groups, accounting for 50 Mbps.

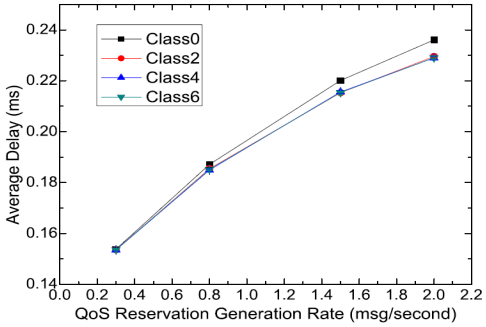

Fig. 3. Average end-to-end delay for different packet generation rates for full UPnP-QoS control.

Fig. 5 and Fig. 6 show the results obtained for different classification accuracy (Clf) and different traffic priorities. Fig. 5 shows the delay for low priority traffic for five different classification accuracy levels. It is clearly depicted that low classification accuracy causes delay growth with increase of reservation generation rate and traffic load. Same stays true for 50% accuracy. Visible improvement in delay characteristic can be seen for average (70%) and high (90-95%) accuracy, showing that auto classification based QoS provisioning can be used for limiting the degradation caused by non-UPnP devices. Fig. 6 presents the results for class 6, which show similar trends. The reduction of delay with growing classification accuracy is very clear. (Note that for high priority traffic, Fig. 6, the decrease in delay with growing reservation rate – esp. for 0.3-0.8 reservations/s – for low classifications accuracies is caused by the growing share of traffic originating from UPnP-QoS compliant devices compared to the total traffic volume[4].) Considering all priority classes we can conclude that low efficiency of traffic classification can be insufficient to increase the QoS level for compliant traffic, but combined with the proper UPnP-QoS policing (i.e., using UIN in a way ensuring higher preemption probability for non-UPnP flows) it can be still useful to improve overall QoS. High accuracy classifiers for all the

[4] Since the average delay is calculated for traffic originating both from UPnP-QoS and non-UPnP-QoS devices, and the non-UPnP-QoS traffic rate is fixed, the growth of the UPnP-QoS traffic can cause a small decrease of the average delay values.

cases bring significant improvement to the delay characteristics.

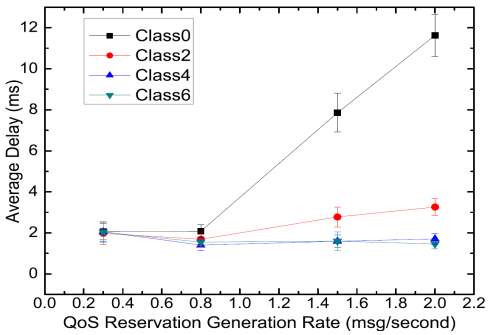

Fig. 4. Average end-to-end delay for different packet generation rates with UPnP-QoS non-compliant devices in the network.

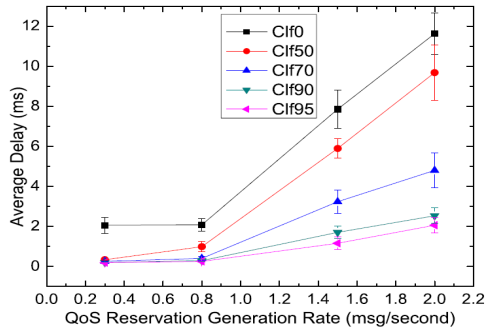

Fig. 5. Average end-to-end delay for different packet generation rates and detection accuracy for traffic priority 0.

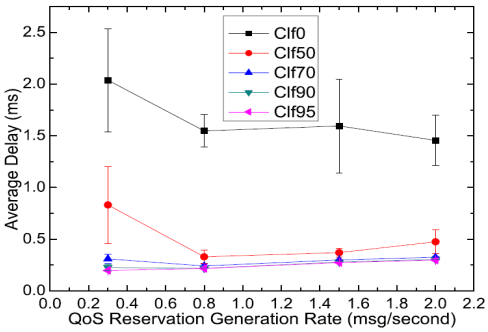

Fig. 6. Average end-to-end delay for different packet generation rates and detection accuracy for traffic priority 6.

B. UPnP-QoS/GMPLS adapter

In order to verify the usability of the proposed QoS parameter mapping between home and access networks we have developed software for performing the gateway mapping functionality called the *UPnP-QoS/GMPLS Adapter*. The Adapter runs in the HG/LER depicted in Fig. 7. The implemented interface uses the OSGi framework and acts as an proxy between the home and access networks. Upon receiving a UPnP-QoS request the module converts the UPnP-QoS Traffic Descriptor into parameters expected by the GMPLS access network. The access network used is emulated by a number of virtual machines running a GMPLS control plane that is managing a user-space implementation of a IEEE 802.1{Q, ad, ah} data plane [22]. The Adapter connects to the GMPLS control plane and based on the Traffic Descriptor determines which nodes are the end-points of the LSP (their IP addresses are used fro LSP establishment). Later the Adapter processes the Traffic Specification and priority parameters and passes this information to be used in LSP creation through the use of the RSVP-TE protocol message exchange between involved LSRs along the LSP.

Aside from the LSP establishment a couple of additional issues needed to be addressed. Namely, the routing of the traffic to proper LSPs and installation of Traffic Control (TC) rules on the testbed nodes. For that purpose two scripts were developed.

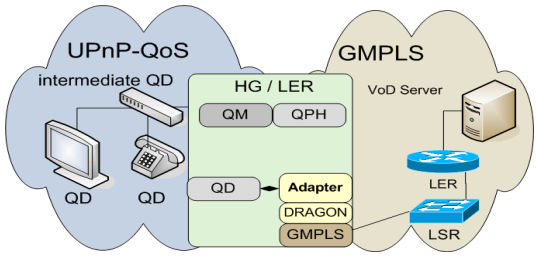

Fig. 7. Test-bed setup – placement of the Adapter.

The first script, which maps client and server traffic into the correct LSP, runs on the LERs. The Adapter triggers it by passing the upstream and downstream label to the LERs, which causes the script to create an interface and add routing and ARP table entries required for routing of the newly admitted traffic into the LSP. The second script installs the QoS rules on the user-space Ethernet switches. The Traffic Specification is used to create rules and filters for the Linux Hierarchical Token Bucket (HTB) Queuing Discipline (qdisc) which matches and shapes the admitted traffic flow.

1) Test Scenario

The assessment of QoS was based on a measurement of data flow parameters in the presence of background traffic. Measurements using IPerf and evaluation of perceptional quality for video streaming were used. Both methods verified proper establishment of forwarding rules and QoS handling of traffic flows through the home and access edge. In the virtual environment used in the testbed the setup time through all the components along the path (including LSRs and script execution) was around 5 seconds. In Fig. 8 we show the video frame[5] before (on the left) and after (on the right) the QoS establishment.

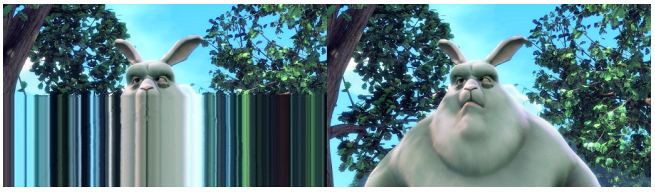

Fig. 8. Video frame before and after QoS establishment.

VII. CONCLUSIONS

In this paper we have presented extensions to UPnP-QoS that allows both the coexistence of UPnP-QoS and non-UPnP-QoS devices in a single UPnP-QoS based network, and enable end-to-end set-up of QoS reaching up to the user's end device, based on UPnP-QoS in the home and GMPLS in the provider's (access/metro) network. With the introduction of

[5] copyright 2008, Blender Foundation

automatic traffic classifiers in the home network devices interconnecting the QoS unaware end devices, a high level of QoS can be preserved without requiring adaptations to pre-existing (non-UPnP-QoS-aware) applications. We have also presented a simulation model and verified the performance improvement of our proposal, enabling us to determine what accuracy of the classifiers is required to obtain satisfactory improvements. The results presented clearly show that for average and high ratio (above 70%) of properly classified flows coming from non-UPnP-QoS devices, the QoS level can be raised to that of a fully UPnP-QoS enabled case. In fact, state-of-the-art classifiers reach even 90-95% accuracy (e.g., Appmon [14]), hence incorporating such approaches into our proposed automatic QoS framework seems viable.

The in-home QoS setup achieved by UPnP-QoS is extended beyond the home gateway by introduction of an Adapter performing QoS parameter translation between home and access domains. We demonstrated feasibility of this approach in a proof-of-concept test-bed set-up. Our first test results indicate that setup time might be an issue in the use-case for user initiated resource allocation (pre-established LSPs vs. ad hoc LSP setup); but once improved, it would allow an automatic (gateway initiated) QoS setup meeting user experience requirements.

REFERENCES

[1] M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, "Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification," in *Proc. 4th ACM SIGCOMM Conf. Internet measurement*, Taormina, Italy, Oct. 2004, pp. 135-148.

[2] M. Dusi, F. Gringoli, and L. Salgarelli, "IP traffic classification for QoS guarantees: The independence of packets," in *Proc. 17th Int. Conf. Computer Communications and Networks,* Virgin Islands, USA, Aug. 2006, pp. 1-8.

[3] J. Park, H.-R. Tyan, and C.-C. Kuo, "GA-based internet traffic classification technique for QoS provisioning," in *Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal,* Los Alamitos, USA, Dec. 2006, pp. 251-254.

[4] W.-S. Hwang and P.-C. Tseng, "A QoS-aware residential gateway with bandwidth management," *IEEE Trans. Consumer Electron.,* vol. 51, no. 3, pp. 840-848, Aug. 2005.

[5] J. But, G. Armitage, and L. Stewart, "Outsourcing automated QoS control of home routers for a better online game experience," *IEEE Commun. Mag.* vol. 46, no. 12, pp. 64-70, Dec. 2008.

[6] M. Siddiqui, S. Amin, and C. S. Hong, "A set-top box for end-to-end QoS management and home network gateway in IMS," *IEEE Trans. Consumer Electron.*, vol. 55, no. 2, pp. 527-534, May 2009.

[7] R. Good and N. Ventura, "End-to-end session based bearer control for IP multimedia subsystems," *Proc. IFIP/IEEE Int. Symp. Integrated Network Management,* Long Island, USA, Jun. 2009, pp. 497-504.

[8] S. Arrizabalaga, P. Cabezas, J. Legarda, and A. Salterain, "A novel QoS architecture for multi-service provisioning in multi-residential gateways," *IEEE Trans. Consumer Electron.*, vol. 55, no. 2, pp. 477-485, May 2009.

[9] J.-P. Laulajainen and M. Hirvonen, "Automatic QoS control in UPnP home networks," in *Proc. 14th IEEE Symp. Computers and Communication*, Souse, Tunisia, Jul. 2009, pp. 455-460.

[10] *UPnP QosPolicyHolder:3 Service Template Version 1.01* UPnP Forum, November 2008.

[11] *UPnP-QoSDevice:3 Service Template Version 1.01*, UPnP Forum, November 2008.

[12] *UPnP-QoSManager:3 Service Template Version 1.01 For UPnP Version 1.0*, UPnP Forum, November 2008.

[13] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification," RFC 2205, IETF, September 1997.

[14] A. W. Moore and K. Papagiannaki, "Toward the accurate identification of network applications," *Proc. 6th Passive and Active Measurement Workshop*, Boston, USA, Mar. 2005, pp. 41-54.

[15] A. W. Moore and D. Zuev, "Internet traffic classification using bayesian analysis techniques," *Proc. ACM SIGMETRICS Int. Conf. Measurement and modeling of computer systems*, Banff, Canada, Jun. 2005, pp. 50-60.

[16] D. Antoniades, M. Polychronakis, S. Antonatos, E. Markatos, and S. Ubik, "Appmon: An application for accurate per application network traffic characterization," in *BroadBand Europe,* Geneva, Switzerland, Dec. 2006.

[17] L. Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," RFC 3270, IETF, May 2002.

[18] J. Wroclawski, "Specification of the Controlled-Load Network Element Service," RFC 2211, IETF, Sep. 1997.

[19] S. Shenker, C. Partridge, and R. Guerin, "Specification of guaranteed quality of service," RFC 2212, IETF, Sep. 1997.

[20] *TR-069 CPE WAN Management Protocol v1.1*, The Broadband Forum, Dec. 2007.

[21] J. Wroclawski, "The use of RSVP with IETF integrated services," RFC 2210, IETF, Sep. 1997.

[22] V. Nordell, A. Gavler and P. Sköldström, "GMPLS controlled multi-layer ethernet," *Proc. SPIE 7989, 79890G*, Shanghai, China, Dec. 2010.

BIOGRAPHIES

Lukasz Brewka received his Master's of Science degree in 2008 from Technical University of Denmark, Department of Photonics Engineering. Currently he is pursuing his Ph.D. in the same department. His main research topics are inter-domain QoS provisioning, home and access networks.

Pontus Sköldström received M.Sc. degree in 2008 from the KTH Royal Institute of Technology of Sweden. Currently he is at the research institute Acreo while pursuing a Ph.D. at the Telecommunication Systems Laboratory at KTH. His focus is software defined networking and network virtualization.

Jelle Nelis received M.Sc. in Computer Sciences at Ghent University in 2006. Shortly after, he joined IBCN-IBBT, a networking research group at Ghent University. His main research topics are home networks, with focus on Quality of Service and interoperable service provisioning**.**

Henrik Wessing received the Master degree in 2001 and his Ph.D. degree in 2006 both at DTU Fotonik, Technical University of Denmark. Henrik Wessing has participated in several Danish national and European projects among others IST-DAVID, IST-MUPBED and in ICT-ALPHA he coordinated the DTU activities in the project as well as leading the activities towards integrated cross domain control and management architectures.

Chris Develder received the M.Sc. degree in computer science engineering and a Ph.D. in electrical engineering from Ghent University, in 1999 and 2003 respectively. From 1999 to 2003, he has been working in the Dept. of Information Technology, at the same university, as a Researcher for the Research Foundation – Flanders. In 2005, after working for OPNET, he re-joined INTEC as a post-doctoral researcher, and as a post-doctoral fellow of the FWO since 2006. In Oct. 2007 he obtained associate professorship at Ghent University. He was and is involved in national and European research projects (IST David, IST Phosphorus, IST E-Photon One, BONE, IST Alpha, IST Geysers, etc.). His research interests include dimensioning, modeling and optimizing optical (Grid) networks and their control and management, smart grids, as well as multimedia and home network software and technologies.