A Framework for dynamic and on-demand QoS to Videoconference Session

Christos Bouras
Research Academic Computer Technology Institute and Computer Engineering and Informatics Department, University of Patras
Rion, Greece

Apostolos Gkamas
Research Academic Computer Technology Institute
Rion, Greece

Dimitris Primpas
Research Academic Computer Technology Institute and Computer Engineering and Informatics Department, University of Patras
Rion, Greece

Abstract - *This paper deals with the design and investigation of an approach for dynamic and on demand QoS on videoconference sessions for GRNET's (Greek NREN) network. After the activation of QoS service in GRNET, a new need for automation of mechanisms for QoS in Videoconferencing session arises. The traditional QoS workflow inserts important administrative cost when a connected institute wants to have a videoconference service with specific QoS guaranties. In such case, the network administrator must manual configure the network's edge routers. In order to overcome the above limitation, an "automatic" procedure for providing QoS guaranties to videoconference session was investigated. The result was an automatic solution that provides QoS using the QoS Policy Propagation via BGP mechanism for signaling. This automatic QoS deployment solution was tested successfully on the network and some performance measurement are presented in this paper.*

Keywords: Video conferencing, Real world applications, QoS, IP Premium, BGP signaling

1 Introduction

A very challenging and demanding issue the last years for all the modern networks including National Research and Education Networks (NRENs) and Internet Service Providers (ISPs) is the design and management of Quality of Service (QoS). As today's networks are multi-service packet networks, QoS becomes more crucial. QoS-enabled networks can accommodate simultaneously various differing traffic types, such as data, voice, and video, by handling time-critical traffic appropriately at congestion points.

The whole process to manage such a service with efficient result to the end users is difficult and need specific tools. Many service providers and NRENs try to implement QoS services, using the available techniques. In particular, there are two QoS architectures that has been proposed and standardized by IETF. The first one is called Integrated Services (IntServ) and the second Differentiated Services (DiffServ) [1]. They follow different philosophy as they approach the topic of Quality of Service from different points of view. The IntServ architecture tries to provide absolute guarantees via resource reservations across the paths that the traffic class follows. The main protocol of this architecture is the Reservation Protocol (RSVP) and its operation is quite complicated. On the other hand, DiffServ architecture is more flexible and efficient as it tries to provide QoS via a different approach. It classifies all the network traffic into classes and tries to treat each class differently, according to the level of QoS guarantees that every class needs. DiffServ architecture has proposed 2 different types regarding Per Hop Behaviors (PHB), the Expedited Forwarding (EF) and the Assured Forwarding (AF), where their difference is on the packet forwarding behavior [1][2].

The operation of DiffServ architecture is based on several mechanisms as packet classification, packet marking, metering and shaping. In addition, in order to provide QoS guarantees, it is necessary to configure properly the queue management and time routing/scheduling mechanism. The classification is done via marking the Differentiated Service Code Point (DSCP) field. This field exists both on IPv4 and IPv6 packet header. In particular, in IPv4 it was part of the field Type of Service (ToS) and in IPv6 is part of the field Traffic Class. Next, the queue management mechanism is configured in order to provide the preferentially packet treatment for the appropriate traffic classes. Also, in DiffServ architecture the policing and metering mechanisms are crucial. In addition, the shaping mechanism is used in conjunction with the marking-metering and is actually used when the traffic class contains significant bursts that lead to exceeding the limits defined in the policy profile. Finally, extended capabilities are now available with the emergence of Multi Protocol Label Switching (MPLS) technology [3].

When independently managed networks are interconnected, additional difficulties exist in ensuring interoperability of DiffServ-based QoS across network

boundaries. This involves (a) adopting interoperable conventions about DiffServ traffic classes and the respective PHBs, (b) adopting interoperable dimensioning and provisioning mechanisms and (c) linking together functions of the two domains, such as provisioning, policing and admission control functions.

The last years, several research teams works on this area [5][8][9] and several approaches for QoS services that follow those architectures has been shown. In the general framework of managing such services, a very important point for the Network Operation Centers (NOCs) is the existence of automatic management tool. The last years, only a few networks have such management tools, due to the fact that there are not many open source tools and the commercial ones are very expensive. Besides that, it is very complicated to develop such a tool and also those tools are network and technology oriented.

In this paper, we present an approach for providing on demand QoS services on video-conference sessions. Today, the video-conference has become a powerful tool for communication but as it consists of voice and video, suffers from network congestion or delay. For this purpose, we designed an approach for GRNET (the Greek National Research and Education Network) that uses the already deployed QoS framework and provides on demand QoS on all scheduled videoconference sessions without the need for additional signaling or marking.

The paper is organized as follows; the section 2 describes the GRNET's network, the design of the QoS services and which was the problem. Section 3 presents in detail the implemented approach and its components. Section 4 presents some performance evaluation results of the implemented approach. Finally, section 5 is dedicated for conclusions and future work.

2 The GRNET network

The Greek National Research and Educational Network - GRNET, interconnects approximately 90 universities and research institutes. The core network consists of twelve nodes interconnected with STM-16 lambdas (2.5Gbps), while the subscriber access links vary from 1 Gbps down to 2 Mbps. It is also interconnected with Geant [14] through 2 connections (a primary and a backup one) at 10Gbps using Ethernet technology. Finally, GRNET hosts the AIX (Athens Internet Exchange) that connects GRNET and all Greek ISPs, in order to exchange traffic.

The GRNET backbone consists of network nodes in 8 major Greek cities, which are, Athens (with 3 Points of Presence - PoPs), Thessaloniki, Patras, Ioannina, Xanthi, Heraklion, Larisa and Syros. All nodes are collocated in the Greek Telecommunications Organization's (OTE company – Greek PPT) facilities under a leasing agreement.

2.1 QoS Services

GRNET has deployed many network services, one of them is a full QoS framework [5][6][10]. GRNET uses Differentiated Services (DiffServ) in order to support different service guarantees to portions of traffic. The following three classes of service -in descending order of quality- are identified and deployed for IPv4 traffic:

- Premium IP (PIP), based on Expedited Forwarding PHB (EF-PHB), gives absolute priority over any other class and provides low delay/jitter plus negligible packet loss guarantees. It is suitable for real-time applications.

- Best Effort (BE) does not offer any qualified guarantees to traffic and is served by default FCFS (First Come First Served) queuing.

- Less than Best Effort (LBE) exploits network resources without (negative) impact other traffic classes. It is suited for specific scavenger applications.

Premium IP class is further divided into three sub-classes; PIP Virtual Wire, PIP VoIP (Voice over IP) and PIP Transparent. PIP Virtual Wire is used for traffic exchanged between two well identified access interfaces and emulates a virtual circuit. GRNET supports both unidirectional and bidirectional traffic in this class. Premium IP VoIP is used for voice traffic generated in a known source network but heading to an unidentified destination. PIP Transparent is used for high priority traffic routed towards GÉANT which is downgraded to BE in the domain borders.

Premium IP traffic is always serviced by output priority queues in network's routers. In worst case (all institutes sends the maximum allowed PIP traffic), the PIP traffic can occupy up to 25% of a core link's capacity in order to minimize inter-packet delay variation (jitter). LBE traffic can potentially occupy all the available network resources and, in periods of high congestion, is granted 1% of the link capacity, which ensures that established connections do not brake. PIP traffic is marked with DSCP values 46, 47 and 40 while LBE traffic is marked with DSCP value 8.

GRNET has implemented a semi-automatic provisioning tool that is used for performing the admission control and generating the appropriate router configuration. Provisioning of QoS service is accomplished by means of a web-based tool developed, which we call the Advanced Network Services (ANS) tool [12]. The ANS tool is accessible by the administrators of all subscriber networks, and performs various provisioning functions besides QoS,

such as MPLS VPN provisioning. The tool is based on a topology database which models the Layer-2 and Layer 3 network topology and stores subscriber link bandwidth.

Through simple submission forms, the administrator of a subscriber network can request any of the available service types, its endpoints, the start and end date of the request, validity period and access control lists. Using the dimensioning algorithm, ANS tool checks in real time if there is sufficient resources for the request in both the source and the destination subscriber links and core network. If so, the tool automatically grants the request and provides the necessary QoS configuration that the administrators applies on the network. Besides the above, the tool performs many more administrative tasks, such as parsing the actual QoS configuration on the routers, comparing the provisional and the actual configurations, reporting on inconsistencies and providing notifications and configuration commands for automated decommissioning of expired requests.

2.2 RTS Services

GRNET operates the national level gatekeeper that offers its connected partners connectivity of VoIP and Videoconference services (over the H.323 protocol). The installed gatekeeper infrastructure provides to the end-users the ability to place VoIP calls to any GRNET party and VideNet connected organizations, either through their office telephone, or their PCs. At the same time, multi-point video conferencing services are offered over H.323, after reservation of resources at the centrally managed MCUs and H.320 gateway of GRNET. Such reservations are handled by a web-based environment through which the connected institutes can request videoconference services.

2.3 Which was the problem

The RTS service of GRNET provides point-to-point and multipoint videoconferences (based on H323 protocol) among the connected institutes of GRNET. Initially, the videoconference traffic was handled as best effort traffic.

When a connected institute wants to have a videoconference service with specific QoS guaranties, the institute should make a request on ANS provisioning tool and the GRNET administrators must manual configure the GRNET edge routers in order to provide QoS guaranties to the videoconference service. Alternatively, an institute can make a permanent request for videoconferencing sessions, reserving permanently some resources (see Figure 1). In this request the connected institute must declare the IP addresses of the stations which participate to the RTS sessions and the QoS parameters that are needed (bandwidth, time period). In case the participated IP stations changes, updated requests must be submitted.

Generally, this procedure requires the following steps to take place:

- Request submission to the ANStool ([12]) provisioning system by the participated institutes
- Check by the ANStool if the requesting can be granted based on the GRNET QoS dimensioning and policy.
- Configuration of the edge GRNET's router connected with the edge router of the connected institute. More particularly, the configuration must allow the IP addresses of stations (with destination the IP address of the MCU) (which participate to the RTS sessions from the connected institute) to receive QoS based on GRNET QoS policy.
- Configuration of the edge GRNET router connected with the MCU. More particularly the configuration must allow the IP addresses of stations (as destination with source IP address the MCU IP address) (which participate to the RTS sessions from the connected institute) to receive QoS based on GRNET QoS policy

This normal procedure has many limitations if it is going to be used on frequent videoconferences due to the fact that manual configuration of router is needed every time an institute requests QoS guaranties. In addition, if permanent reservations are used, there is waste of resources. In order to overcome the above limitation an "automatic" procedure for providing QoS guaranties to videoconference session was investigated.

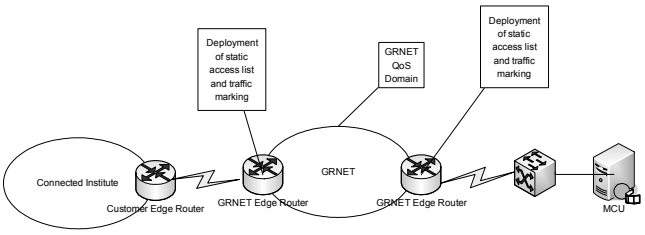

Figure 1: The normal procedure scenario

3 Automated QoS approach

In order to overcome the above mentioned limitations, we decided to use the QoS Policy Propagation via BGP (QPPB) [13] approach for the propagation of QoS parameters over BGP routing protocol. The basic difference with the normal procedure is the fact that the network can autonomously find the stations which participate to the RTS session and can receive QoS guaranties and propagate this information to all the routers. This investigation of the participants in a videoconference is done by a new software module which communicates with the MCU and stores the IP addresses of the connected stations to a database. This software stores to the database only the IP addresses of the stations which have the appropriate authority to receive QoS guaranties.

Next, a modified version of the Quagga software router [11] that has eBGP (external BGP) peers with all the router of the network is used. The modified version of the Quagga software router reads the IP addresses stored in the database and advertise them through BGP to all the routers of the GRNET network with the appropriate BGP community which indicates the IP addresses that must receive QoS guaranties.

The key issue is that the software router advertises IPs differently than the usual BGP peering. Usually, a router advertises through BGP a sub-network that it routes. In our case, the Quagga router advertises a set of IP addresses that belongs to other Autonomous Systems. This choice was done in order to minimize the overall administrative effort and aiming at having a fully automated service. Therefore, the Quagga needs an additional module (the pathfinder module) that is able to recognize and set the correct next hop for each IP address that is connected in RTS service. The next hop in this case should be the appropriate exit interface from GRNET's backbone to the institute that the IP belongs to. Generally, this module is quite demanding as it should takes into account several parameters like multihoming, multisiting etc. In our case, this module benefits from MPLS deployment in the network and operates in two steps. Initially, it finds through MPLS labeling pool, the end GRNET's routers that the institute is connected. Next, it queries this router (for the next hop for the IP address) and it responds with the actual exit interface from GRNET's network. With this concept, the IP addresses that participate in a videoconference session are advertised separately (through a private BGP community) in the network through the modified Quagga that actually works as a "route injector". Next, using QPPB technique we can assign to this community special attributes and QoS characteristics.

In details, the implemented approach operates as follows:

- The implemented admission control software monitors the MCU and periodically updates (adds and removes) the database with the IP addresses of the connected stations which have the appropriate authority to receive QoS guaranties.

- The modified Quagga software router monitors the database periodically for addition or removal of IP addresses. In the case that a new IP address has been added to the database, the modified Quagga software router determines the appropriate next hop by the pathfinding module and advertises that IP address within the appropriate private BGP community to all BGP peers. In the case that an IP address has been removed by the database, the modified Quagga software router stops to advertise that IP address to all BGP peers.

- The edge GRNET's router marks the traffic based on the predefined BGP community in order to provide QoS guaranties to the traffic from the connected institutes to the MCU. The whole operation is done in 2 steps. Initially, through QPPB signaling (source based), the router makes a local scope (in the router only) marking, using the qos-group feature [13]. Next all marked packets in every incoming interface (from an institute that are destined to MCU system) are classified and policed into a separate class. This class has been created for RTS traffic only and the policing profile that is applied, has been decided with the connected institute (usually, the connected institute asks for a specific profile that is also compliant with GRNET's QoS dimensioning). All the conformed packets are marked as IP Premium traffic (with DSCP 46) and transmitted in the network. The exceeded packets are dropped. The 2 step operation is necessary due to the fact that the QPPB signaling operated is source only or destination only aware and in our case we need source and destination aware

- The edge GRNET router connected with the MCU works on the opposite direction and marks the traffic based on the predefined BGP community in order to provide QoS guaranties to the traffic from the MCU to the connected institutes. The marking is done through QPPB signaling on destination based mode.

In the core GRNET's network, there is no need for any changes as the QoS framework has been initially deployed (there are activated queues in all output interfaces). Additionally, the edge policing and marking (the separate RTS class per interface) has also been once and there in no need for changes, unless an institute asks to change the traffic profile (the bandwidth that it wants to use for videoconference services).

Consequently, the integration of all the modules and the correct initial QoS configuration of the network provide a fully dynamic framework that recognizes the connected stations on RTS services and using the QPPB and QoS setup, provides the appropriate QoS guarantees across the network.

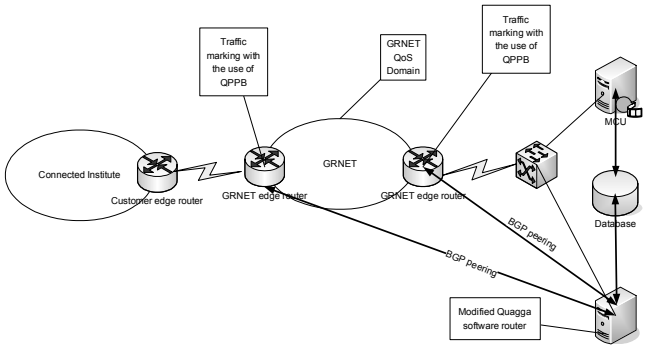

Figure 2: The Automated QoS approach

4 Evaluation of the concept

In order to evaluate the approach, we deployed the concept on GRNET's backbone. In particular, the modified Quagga router obtained BGP peers with all the routers of the network (9 routers) and the QoS setup on network's perimeter was set (see Figure 5).

```
Class-map: cm_rts_qos (match-all) (10645969/7)
    391873 packets, 253275711 bytes
    Match: qos-group 1 (13756610)
    Match: access-group 199 (15174802)
    police: 1024000 bps, 9000 limit, 9000 extended limit
conformed 391873 packets, 253275711 bytes actions: set-
dscp-transmit ef, exceeded 0 packets, 0 bytes; actions: set-
dscp-transmit default
```

Figure 3: CLI statistics in direction 'user to MCU'

Also, the admission control software was enabled and the concept was used experimentally in several videoconferences (with 2 hours duration). During those tests, the stability and the proper setup were measured using the CLI (Command Line Interface) counters (see Figure 3 and Figure 4) and BGP monitoring. The automatic QoS concept showed excellent result, as the QoS policy was propagated to all network's elements and the videoconferencing traffic was classified as IP Premium. The next set of tests aimed at measuring the QoS performance in the network for videoconferencing traffic, using this approach. Also, a comparison with the classic best effort is done.

```
Class-map: ip_premium_out (match-any) (3447969/1)
      659862 packets, 323954552 bytes
      Match: ip dscp 46  (1941986)
      Match: ip dscp 47  (1941730)
      Match: ip dscp 40  (1939426)
      Match: mpls experimental  5  (392754)
      Priority
      police: cir 20%, burst 250 ms, extended burst 250 ms
200000000 bps, 6250000 limit, 6250000 extended limit
conformed 659862 packets, 323954552 bytes; actions:
transmit, exceeded 0 packets, 0 bytes; actions:          drop
conformed 0 bps, exceed 0 bps
```

Figure 4: CLI statistics in direction 'MCU to user'

Therefore, a videoconference was set up between several parties, using the central MCU. In this case, we measured the received performance by an end point. During the videoconference session we measure the following parameters which are important for videoconference sessions:

- Bandwidth/Throughput: During the experiment, we measure the video and audio payload (without the headers overhead) of the used RTP streams. Due to the fact that audio and video are transmitted in different RTP streams we perform different measurements for audio and video data.

- Packet loss: During the experiment, we measure packet lost to both audio and video RTP streams. Packet loss is an import QoS parameter for videoconference session and a small value of packet loss can influence important the videoconference quality.

- Delta: During the experiment, we measure delta parameter to both audio and video RTP streams. Delta parameter is the difference in one way delay of two sequentially packets transmitted in a RTP stream and is used in the jitter calculation according to [15]. The delta parameter is an indication of the variations in delay during the transmission of the multimedia data.

- Jitter: During the experiment, we measure delay jitter parameter to both audio and video RTP streams. Delay jitter is an import QoS parameter for videoconference session and affects (among other characteristics) the interactivity of a videoconference session.

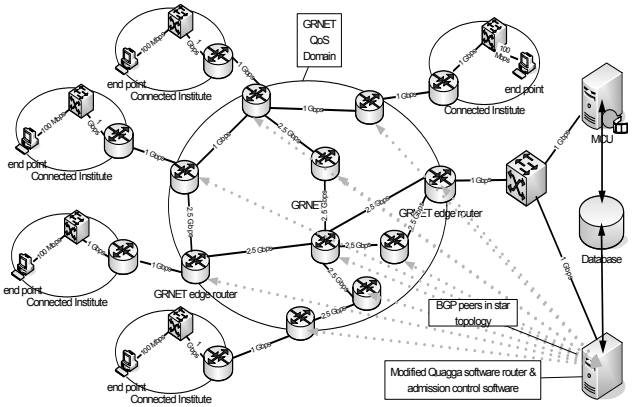

Figure 5: Network's setup in GRNET

We measure the above parameters both in the direction from end point to MCU and the opposite direction (from MCU to end point). The following figures show indicative diagrams that compares a best effort videoconference session and a QoS-enabled videoconference session. We present the jitter, delta and throughput diagrams during the video transmission from one participant to the MCU as indicative diagrams. We also present an indicative one regarding the audio delay jitter form the MCU to one participant). The other diagrams (video from MCU and audio from/to MCU) show the same results.

As someone can see in the following diagrams (Figure 6, Figure 7 and Figure 8 regarding video transmission) there is a significant reduction of delay jitter during the QoS-enabled videoconference session comparing with best effort videoconference. This assumption reflects also to the mean value of jitter (QoS-

enabled videoconference: 0,87ms and best effort videoconference: 1,51ms) and the maximum value of jitter (QoS-enabled videoconference: 6,91ms and best effort videoconference: 38,55ms).

Regarding the parameter delta, QoS-enable videoconference session and best effort videoconference session have similar performance with the QoS-enable videoconference session to have less picks as someone can see in Figure 8. This reflects also to the mean (QoS-enabled videoconference: 33,96ms and best effort videoconference: 34,78ms) value of the parameter detla. Regarding the throughput, the QoS-enabled videoconference has better performance than the best effort videoconference but the difference, as the above diagrams show, is not so big like the delay jitter.

Similarly the average throughput is better for QoS-enabled videoconference (QoS-enabled videoconference: 145kbps and best effort videoconference: 130kbps). Moreover, both QoS-enabled videoconference and best effort videoconference had no packet losses during the experiments.

As someone can see in Figure 9 (audio jitter from MCU to a participant), QoS-enable videoconference session and best effort videoconference session have similar performance with the QoS-enable videoconference session to have fewer fluctuations

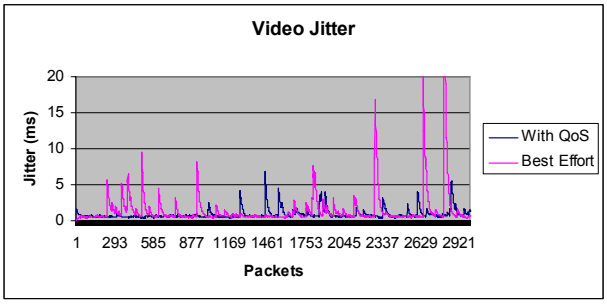

Figure 6: Video Jitter

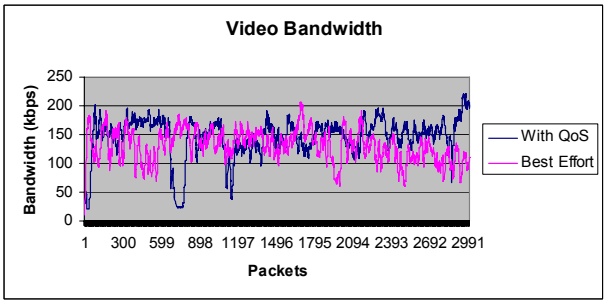

Figure 7: Video Bandwidth

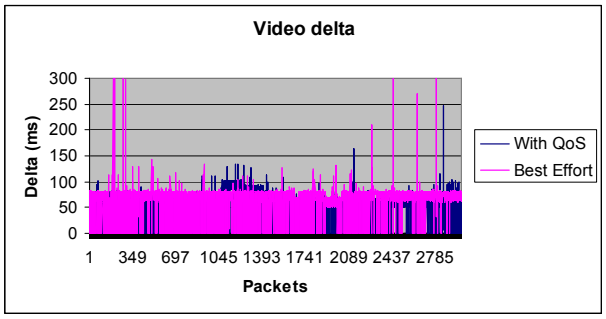

Figure 8: Video Delta

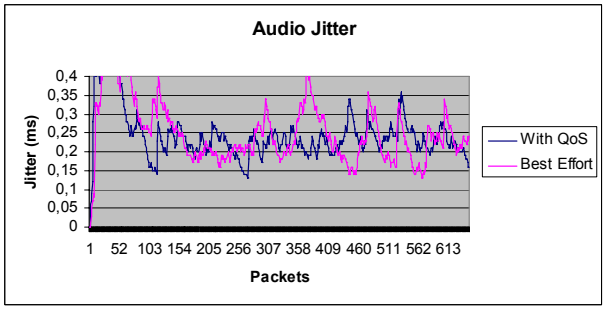

Figure 9: Audio Jitter

Consequently, there is an improved performance for the videoconference sessions with the implemented automatic QoS mechanism. Especially the improved delay jitter during the QoS-enabled videoconference is important due to the fact that delay jitter affects significantly the videoconference quality. In terms of throughput the improvement is quite small but this is explained due to the fact that the backbone and the access network (in the testbed) is high speed and uncongested (in worst case, the network's resources utilization is 50%). Therefore, we did not expected differences in terms of packet loss. Finally, we expected and measured better results in terms of jitter due to the fact that the videoconferencing traffic is served by high priority queues.

5 CONCLUSION – FUTURE WORK

This paper described the design aspects of a framework for dynamic and on demand QoS services on Videoconference sessions. After the deployment of QoS service in GRNET's network, a new need for automation of mechanisms for QoS in Videoconferencing session arise. Following the traditional workflow, when a connected institute wants to have a videoconference service with specific QoS guaranties the GRNET's administrators must manual configure the GRNET's routers in order to provide QoS guaranties to the videoconference service. In order to overcome the above limitation an "automatic" procedure for providing QoS guaranties to videoconference session was investigated. The result was a proposed solution that makes use of QoS Policy Propagation via BGP (QPPB) signaling mechanism and some newly developed modules that automatically

investigate and advertise the IP addresses that participate on RTS sessions and have the privileges to use QoS service. It is worth noting that this solution can be extended in order to provide a scalable and dynamic mechanism for QoS propagation in federated networks.

The overall solution has been deployed and tested on GRNET's backbone with very positive results. The next steps have been already discussed and consist of full service deployment in order to introduce this service in GRNET's production service portfolio. Additionally, we plan to investigate a monitoring schema for real time statistics of service's usage. Finally, more automated and advanced techniques for admission control (that identify the privilege of an IP address that participate to an RTS session to use the QoS service) will be investigated and implemented.

6 ACKNOWLEDGMENTS

This work is partially funded by the project GRNET/ VNOC-2 [10]. The authors would like to thank the GRNET and the partners of project for their valuable cooperation and contribution to the design and implementation of the service. In particular, we would like to especially thank the GRNET and the NOC of National Technical University of Athens (NTUA).

7 References

[1] RFC 2475, "An Architecture for Differentiated Services", S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, December 1998

[2] RFC 2598, "An Expedited Forwarding PHB", V. Jacobson, K. Nichols, K.Poduri, June 1999

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

[4] 'IP Quality of Service: the complete resource for understanding and deploying IP quality of service for Cisco networks', S. Vegesna, Cisco Press, 2001

[5] "Techniques for DiffServ - based QoS in Hierarchically Federated MAN Networks - the GRNET Case" A. Varvitsiotis, V. Siris, D. Primpas, G. Fotiadis, A. Liakopoulos, C. Bouras, The 14th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN 2005), Chania. Island of Crete, Greece, September 18 - 21 2005

[6] "QoS issues in the Research and Academic Networks: The case of GRnet" C. Bouras, A. Karaliotas, M. Oikonomakos, M. Paraskevas, D. Primpas, C. Sintoris, Industrial Conference on Multi-Provider QoS/SLA Internetworking (MPQSI 2005), Tahiti, French Polynesia, October 23 - 28 2005

[7] "BGP Design and Implementation", Micah Bartell, Randy Zhang, Cisco Press, ISBN: 1587051095, 2004

[8] "A Management and Control Architecture for Providing IP Differentiated Services in MPLS-based Networks", P. Trimintzios, I. Andrikopoulos, G. Pavlou, P. Flegkas, D. Griffin, P. Georgatsos, D. Goderis, Y. T'Joens, L. Georgiadis, C. Jacquenet, R. Egan, IEEE Communications, special issue in IP-Oriented Operations and Management, Vol. 39, No. 5, pp. 80-88, IEEE, May 2001

[9] "Providing and verifying advanced IP services in hierarchical DiffServ networks - the case of GEANT" A. Liakopoulos, B. Maglaris, C. Bouras, A. Sevasti, International Journal of Communication Systems, Wiley InterScience, 2004, pp. 321 - 336

[10] GRNET's website http://www.grnet.gr

[11] Quagga software http://www.quagga.net

[12] GRNET's ANS provisioning tool http://anstool.grnet.gr

[13] CISCO Systems website http://www.cisco.com

[14] GEANT2 Network http://www.geant2.net/

[15] RFC 3550, RTP: A Transport Protocol for Real-Time Applications, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, July 2003