QoS issues in the Research and Academic Networks: The case of GRNET

Christos Bouras [1,2]	Anastasios Karaliotas [1,2]	Michael Oikonomakos [1,2]	Michael Paraskevas [1]	Dimitris Primpas [1,2]	Christos Sintoris [1,3]

[1]Research Academic Computer Technology Institute, N.Kazantzaki Str., Patras University 26500 Rion, Patras, Greece &
[2]Department of Computer Engineering and Informatics, University of Patras, 26500 Rion, Patras, Greece &
[3]Department of Electrical Engineering and Computers Technology, University of Patras, 26500 Rion, Patras, Greece

TEL: +30 2610 {960375, 960440, 960351, 960308, 960316}
FAX: +30 2610 960358
E-MAIL: bouras@cti.gr, karaliot@cti.gr, moikonom@cti.gr, mparask@cti.gr, primpas@cti.gr, sintoris@cti.gr

Abstract

This paper describes the design and the implementation of QoS services in a high speed backbone network as well as a management tool for the service. The services were designed taking advantage of features provided by the MPLS technology and also by using the DiffServ architecture. The supported QoS services include the IP Premium that tries to provide zero packet loss as well as minimum delay and jitter and the Less Than Best Effort service. In addition we implemented a management tool for the service. The scope of this tool is to allow the users to manage their QoS requests (make a new one, edit, delete or view a request). Also the tool performs admission control and produces the necessary configuration that must be applied on the network in order to implement every service's request.

1. Introduction

A very challenging and demanding issue the last years for all the modern networks, NRENs and ISPs is the design and management of Quality Of Service. The whole process to manage such a service with efficient result to the end users is difficult and need specific tools. This paper describes the design and implementation of a set of QoS services that aim to be available to end users for their needs. Many service providers and NRENs have implemented QoS services, using the available techniques. In particular, there are 2 architectures for QoS 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 that works with 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 Quality of Service 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. In DiffServ architecture has been proposed 2 different types (Per Hop Behaviours - PHB), the expedited forwarding (EF) and the assured forwarding (AF), where their difference is on the packet forwarding behaviour [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 DSCP (Differentiated Service CodePoint) field. This field exists on IPv4 and on IPv6 packet header too. 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 from the policy profile. Finally, extended capabilities are now available with the emergence of Multi Protocol Label Switching (MPLS) technology [3].

The last years, several research teams works on this area [4][5][7] and several QoS services that follow those architectures has been introduced and tested. In the general framework of managing such services, a very important point for the Network Operation Centers (NOCs) is the existence of an automatic or semi 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.

GRNET which is the Greek Research and Educational network [14] manages a modern backbone network that connects all the universities, research institutes as well as the school networks and many public (governmental) services. In the scope of GRNET's virtual NOC, we designed and applied a Quality of Service solution. The design covered the QoS services IP Premium service as well as the LBE that is presented in this paper. The work includes the design of the service for GRNET's needs, the testing of the necessary configuration evaluating its performance and possible malfunctions with other services. In the meanwhile, a full management tool was designed and implemented. This management tool is part of a bigger one that manages some other services too, like the MBS and L3 MPLS VPNs but its part is quite independent, using only a common database.

The paper is organized as follows; the section 2 describes the GRNET's network and the design of the QoS services. Section 3 gives an overview of network configuration issues and section 4 presents the management tool, focusing on its functionality, the database and the user interface. Finally, section 5 is dedicated for conclusions and future work

2. Quality of Service design

The goal of the DiffServ QoS services is to provide several classes to the end users in order to achieve better performance in specific, delay sensitive, traffic. The QoS services that was designed and implemented in this framework, focused on 3 classes, the IP Premium, the Less Than Best effort (LBE) and the classic best effort. The first one mainly goals to service real time traffic or generally traffic that needs zero packet loss as well as minimum delay and jitter. The LBE service is provided in a network servicing traffic that is not critical and therefore can be dropped first in case of congestion. Otherwise, if the network is un-congested the LBE traffic is served normally.

Before the description of the whole design, it is necessary to describe the GRNET's network that is the case study of the design.

RFC 2474 DSCP bits						DEC	Description
1	0	1	1	1	0	46	IP Premium (IPP)
1	0	1	0	0	0	40	IP Premium Transparent
1	0	1	1	1	1	47	IP Premium (IPP) for VoIP
0	0	1	0	0	0	8	Less than Best Effort (LBE)
0	0	0	1	1	0	6	Downgraded Premium-Discard Eligible (DP/DE)
0	0	0	0	0	0	0	Best Effort (BE)
All others							Best Effort (BE)

Table 1: The valid DSCP values

2.1.GRNET case

The GRNET backbone consists of network nodes in 8 major Greek cities, which are, Athens (3 PoPs), Thessaloniki, Patras, Ioannina, Xanthi, Heraklion, Larisa and Syros. The hardware equipment of all nodes has been recently updated to CISCO platforms [12] series 12000 (GSRs). Also, the backbone links have been upgraded to POS (Packet over Sonet) links at 2.5Gbps. The routers have many access interfaces to connect all the universities, research institutes, the school network and other. The access interfaces are using Gigabit Ethernet technology with 1Gbps capacity. In addition, some of the old GRNET's equipment (Cisco routers series 7500) still exists in GRNET's PoPs and is now connected to GSRs. The usage of the old equipment is to offer backup connections to some institutes and universities or to connect some that have not upgraded their internal network and their access link to GRNET to Gigabit Ethernet technology.

The GRNET has almost 70 access links on its backbone routers. It is also interconnected with Geant [13] through 2 POS links (2.5Gbps) and a backup link on 1Gbps (Gigabit Ethernet). Finally, GRNET hosts the AIX (Athens Internet Exchange) that connects GRNET and all Greek ISPs, in order to exchange traffic.

2.2.Design of IP Premium service

The IP Premium service aims to provide absolute guarantees to a portion of traffic. This service in order to be provided correctly, several parameters should be taken into account. For GRNET's network we decided to provide 2 kinds of IP Premium services, the first one provides guarantees to traffic between given end points and the other to traffic that has given only the source and the destination could be anywhere in the network. The declaration of the traffic that belongs to each class is done at the edge of the network, where the traffic is marked with the appropriate DSCP value (see Table 1). The valid values are DSCP=46 and DSCP=47, where the former is for IP Premium traffic declared with given source – destination and the latter for IP Premium traffic with given source.

The packet marking is based on DSCP values but also on MPLS Experimental field, as the network is an MPLS domain. According to the MPLS implementation in the network, every time a packet inserts to the MPLS domain, the 3 most significant bits of DSCP are rewritten to the MPLS exp. In the core routers, the packet classification to the appropriate queue is also based on DSCP and MPLS EXP, due to the penultimate hop popping of MPLS [10][8].

Access link speed	Portion of IP Premium traffic
>=1 Gbps	1%
500Mbps - 1Gigps	1,5%
100Mbps - 500Mbps	2%
30Mbps- 100 Mbps	5%
10Mbps-30 Mbps	10%
2Mbps-10Mbps (DSL users)	15%
>= 2 Mbps	20%

Table 2: The dimensioning values of access links

The whole network has been dimensioned in such a way that each access link has declared a given percentage of its capacity that can be used by IP Premium traffic (Table 2). This portion is secure in any case and can provide the IP Premium's guarantees even if all access links in GRNET's topology are full and there is a link failure.

The packet marking is done at the edge of the network, either by GRNET or by the source itself. Each request for usage of the IP Premium service is described by an extended ACL that is provided by the access network that requested it. This choice gives a flexible way for traffic classification as it can be done by IP addresses, protocols, ports etc. Next, the request also declares the traffic profile of this request that is used by GRNET. In particular, at the access interface of the network, we classify the packets according to the ACL and police the traffic with rate equal to the requested. Policing is done using the Token Bucket algorithm, which has been configured to police the traffic with CIR (Committed Information Rate) equal to the requested and with depth equal to 2 network's MTU. As the access interfaces are Gigabit Ethernet, the depth is equal to 3000 (the MTU is 1500). This policing profile has been initially tested and in case of UDP traffic provides ideal policing. In case of TCP traffic the result is good but it depends on other parameters too, as the TCP window of the application that produces the traffic etc. All the exceeded traffic is either dropped or remarked to DSCP value 6 and treated as best effort. The decision regarding the treatment of the exceeded traffic is taken by the end users at the submission of their request and then GRNET implements it.

Next, the valid IP Premium traffic inserts the GRNET's domain and is delivered to the destination with high priority. The GRNET's network uses CISCO platforms and for the queue management it uses the MDRR mechanism (Modified Deficit Round Robin) [8][9][12]. We designed the IP Premium by introducing a high priority queue on all network's routers using the MDRR. In particular, on every output interface (backbone or access) 2 queues were activated and they configured to enqueue packets with specific values (the priority queue should enqueue packets with DSCP 46 or 47 or MPLS EXP 5 and the other queue the "best effort" packets). Also, on every input interface, a specific configuration was applied in order to prevent the network from unauthorized traffic that can be enqueued in high priority queue (authorized marked traffic).

Applying this design to the network, there is an operational service for the end users. The IP Premium traffic with both ends (source – destination) declared used the DSCP marking 46. On the other hand, the IP Premium traffic with only the source declared was introduced for usage by VoIP calls, for which is not efficient to declare each time its destination. In this case, the packets were marked with DSCP 47.

Every time a new request was applied, an admission control was applied, taken into account the profile of the request. In particular, the IP Premium allocation on the access interfaces of the 2 ends (or the source only in case of VoIP calls) was examined whether with the addition of the new request it remains below the maximum allocation or not. In case of violation of the maximum allocation, the request was initially rejected, otherwise the request is accepted automatically. Some rejected requests could also be accepted under several conditions as the routing between the 2 end points and the congestion in the backbone links

2.3.Less Than Best effort

Also, GRNET provides the Less Than Best Effort service (LBE) to its users. This services aims to sere non critical traffic with the condition that there are network resources available. In case of congestion, this traffic is dropped first, in order to protect the best effort. The LBE traffic is marked by the end users with DSCP value 8 and is unprovisioned in backbone network. This means that there is not any kind of requests or admissions, but simply the end users sends marked traffic. The LBE traffic in the backbone is served by a separate queue on each output interface. This queue has allocated a very small portion of network resources (actually the 1%), in order to prevent it from complete struggling. This queue actually sends a few packets (due to 1% allocation) and drops all the other if the network is congested.

3. Network Implementation issues

After the design phase of the QoS services, as described in the above paragraph, we proceeded to the implementation phase. This phase contained several steps that aimed to configure and evaluate all the above mechanisms. The first one was the configuration of all routers in order to become QoS-enabled, by configuring 3 queues on every output interface (physical or logical interfaces as Ethernet VLANs). The above steps made the network operational and we started configuring and evaluating all the other mechanisms. The next step was the evaluation of the QoS (policing, marking and queue management mechanisms). These features was configured on network's testbed and remained operational in order to investigate possible performance aspects. The tests done by using 2 traffic generators (Smartbits 600) that tried to overload some access links with background traffic and also send a small portion of "IP Premium marked" traffic. The tests contained the investigation of the policing, marking and queue management mechanisms and were totally successful.

At this point we should mention that in GRNET's domain, the valid marked traffic is policed strictly and on the other hand the marked packets (with invalid values for GRNET) are simply treated as best effort.

Simultaneously, the design of QoS service also contains the design of possible interconnection to the relevant Geant's service [5][13]. In particular, Geant is the pan-European network that interconnects all the NRENs and has connections with Internet2 and Asia. Geant implements the QoS services (IP Premium and LBE) by enabling high and low priority queues respectively in Juniper equipment that Geant has. The marking that Geant uses is the same that GRNET adopted, so their services are totally compliant. The only point that should be taken into account is the profile of the aggregated IP Premium traffic that GRNET and GEANT exchange. In order to avoid possible problems in this point, GRNET polices aggregately all the incoming IP Premium traffic from GEANT in CIR rate equal to the sum of the requests' rate. Finally, a new QoS class, which is supported by GEANT, was introduced in GRNET. Actually this class is marked with DSCP 40 and serves traffic that is targeted to an end point of GEANT. This traffic is treated as IP Premium in GRNET but when it inserts the GEANT's domain, it is served as best effort. This class is already implemented in GEANT and was introduced in GRNET's network for compatibility reasons.

4. Management Tool for QoS service

Additionally, another very important issue of the proposed QoS framework - services is its interface with the users. In particular, we designed and implemented a management tool with a number of capabilities. Users of the tool will be all the NOCs of the organizations that are connected on the network and therefore can request a QoS service. This tool interacts with GRNET's database and models the network's topology and connections. This database was initially maintained by GRNET and has been extended for the scope of this management tool. It stores much information as:

- The connected organizations, the contact persons and other related information
- The PoPs, routers and switches of the network with all related information (topology etc).
- The network interfaces (physical interfaces, layer 2 and layer 3 interfaces) and their relationships with all the related information.
- The users of the management tool and their rights.
- Various other tables with information about the daily management of the network (troubleshooting tickets) or information about other network services.

Generally, the database has all the necessary information and monitors the network, providing the ability to use it in order to develop advanced network services. The scope of the management tool is to provide 3 different roles: the users, the router's administrators and the system (service) administrators.

A user of the management tool has a personalized access to a web interface that provides a number of capabilities. In particular, the user can fill in a form (Figure 1) requesting a new QoS service (IP Premium). The form is fully operational and represents the network status, routers, interfaces etc. Through this

wizard the user choose the type of the IP Premium service that he needs, the ends of the flow (source - destination or source only), as well as the time frame that he needs it. Additionally, the user declares the profile of the traffic (requested bandwidth) and finally describes the traffic class. This description of traffic class is done by inserting an extended access list (ACL) through an operational ACL wizard that we implemented (Figure 2).

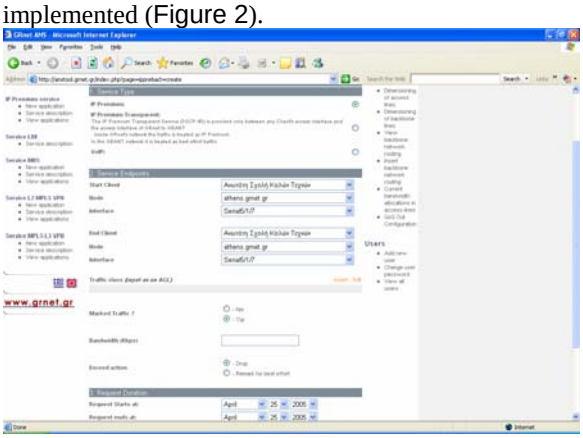

Figure 1: The QoS request's submission form

Next, the system checks all the input information and informs the user for possible errors. In case that everything is right, the system runs the admission control algorithm, as mentioned in the design of the service, which is based on network's dimensioning. This module finally decides if the request is accepted or rejected. In case of accepted request, the request goes to confirmation pending status, where the other end of the request is informed via email and should acknowledge or reject this request. In case the other end acknowledges it, the request is in implementation pending status and the routers' administrators should implement it on its start date. The users have also the capabilities to view all the related QoS requests (active, pending or rejected). On these requests, the users have the privileges to edit or even delete them. Finally, the users can view all the access interfaces that their organization has on GRNET's network and see the current and the maximum allowed bandwidth reservations.

The second role in the management tool provides special capabilities to the routers' management team. They have access to the tool and can view all the submitted requests and their status. Also, the management tool checks daily for new requests that should be active in the next 3 days or for requests that should be decommissioned in the next 3 days and informs the team via email. Finally, the team has access to view the details of each request according to its status and can see the configuration details. The details provide all the configuration commands that should be applied in the network's routers in order to implement or decommission a QoS request (Figure 3). The routers' management team makes a final check on the produced configuration and then applies it on the routers. Also, this team has the responsibility to update the request's status whenever they change its status using the produced configuration. At this point, we should notice that the produced configuration follows the configuration template that was created at the design and implementation phase. We could have configured the management tool to apply the configuration to the network routers automatically, but finally we decided to remain in the status where the routers' management team checks and applies it. The automatic configuration will be enabled in later stage where the development of the network will have been finalized. Finally, the routers' management team has the capability to view through the management tool all the interfaces on the routers with the maximum and current bandwidth reservations.

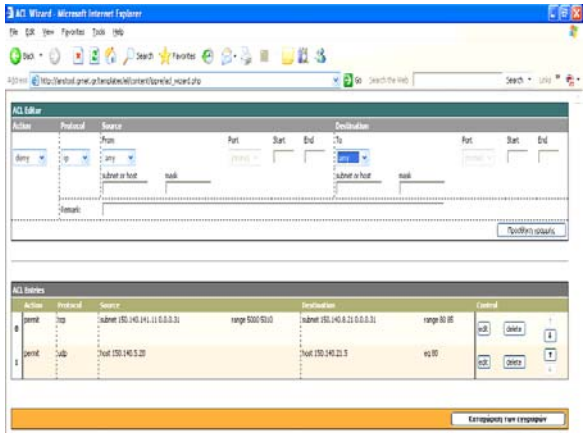

Figure 2: The ACL wizard

The third role is the administrator of the management tool. The capabilities that he has, contains the ability to create a new request, edit or view an existing one. In addition, the administrator can view and change the network dimensioning as well as view and change the QoS configuration template that is used to produce the exact configuration for every request. The later is very important as small changes in the configuration may be necessary while new software releases (IOS) for the routers will be available. Finally, the administrator has the responsibility for the user management (creation of new user accounts etc).

This management tool was designed and implemented in parallel with the design and implementation of the QoS service itself and now the implementation phase has finished. The management tool has passed successfully from a testing phase and now has been fully integrated into GRNET's network and is operational.

Figure 3: An example of the produced configuration per request

5. Conclusions – Future Work

This paper described the design and implementation of QoS services in a WAN network as GRNET's. The implemented QoS services include the IP Premium; an EF PHP based service, as well as the Less Than Best Effort. Also, we have designed and implemented a management tool for the services that takes advantage of the database that keeps updated information for network's condition. The services and the management tool has already been finalized, tested and deployed in GRNET's network and are fully operational.

In addition, we already have plans for future work in this area. These plans are divided into 2 categories, the service's enhancements and the management's tool upgrades. The first category contains the better dimensioning of the network in order to support the IP Premium service offering more resources (increasing the maximum allocation in the access links).

On the other hand, we plan some upgrades in the management tool, where the first one is the fully automation of the network's configuration (via SNMP or COPS), where the management tool will connect to the routers and will apply the relevant configuration. Secondly, we plan to investigate a method for providing real time statistics. The later is very important as it can be used as metric for future service's SLAs [6].

Additionally, we already work on monitoring of the implemented requests. GRNET implemented a configuration parser and stores the applied QoS configuration on every router in its database. Taken advantage from this implementation, we are implementing a monitoring – diagnostic module that checks daily the active (according to the management tool) and the implemented requests (searching the database) for possible errors. Such errors can be caused either at the process of enabling the configuration or by routine changes on a router.

6. Acknowledgments

This work is partially funded by the project GRNET/ VNOC-2 [14]. 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, the NOC of National Technical University of Athens (NTUA) and the NOC of University of Crete (UoC).

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] "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

[5] "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

[6] "SLA definition for the provision of an EF-based service" C. Bouras, M. Campanella, A. Sevasth, 16th International Workshop on Communications Quality & Reliability (CQR 2002), Okinawa, Japan, May 14-16 2002, pp. 17-21

[7] D. Verma, M. Beigi and R. Jennings, "Policy Based SLA Management in Enterprise Networks", Policy Workshop 2001

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

[9] Understanding and Configuring MDRR and WRED on the Cisco 12000 Series Internet Router, Cisco Systems

[10] "Deploying Guaranteed Bandwidth Service with MPLS", Cisco White Paper

[11] SEQUIN: 'Service Quality across Independently Managed Networks', IST Project IST-1999-20841, (http://www.dante.net/sequin/)

[12] http://www.cisco.com

[13] http://www.geant.net

[14] http://www.grnet.gr