Implementation issues of Managed Bandwidth Service: The case of GRNET

Christos Bouras Dimitris Primpas
Research Academic Computer Technology Institute, 61 Riga Feraiou Str., 26221 Patras, Greece &
Department of Computer Engineering and Informatics, University of Patras, 26500 Rion, Patras, Greece
TEL: +30 2610 {960375, 960316}
FAX: +30 2610 960358
E-MAIL: bouras@cti.gr, primpas@cti.gr

Abstract

This paper describes the design and the implementation of the Managed Bandwidth Service (MBS) in a high speed backbone network as well as a management tool for the service. The service was designed taking advantage of features provided by the MPLS technology and also using the DiffServ architecture. So, it uses L2 MPLS VPNs to provide point to point connection and also marks the traffic in order to pass from certain priority queues (to provide guaranteed bandwidth). It also enables traffic engineering characteristics in order to provide load balancing on the network as well as fast rerouting in case of link failure. In addition we implemented a management tool for the service. The scope of this tool is to allow the users to manage their MBS 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. This service was designed and implemented on GRNET's network.

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 such a service, called managed bandwidth service, where its basic idea is to provide secure bandwidth connections between end points. Many service providers and NRENs have implemented MBS and provide it to their customers, using each one different implementation solutions. In particular the most common solutions are the use of DiffServ architecture or the use of ATM permanent virtual circuits to guarantee bandwidth. Nowadays, with the emergence of Multi Protocol Label Switching (MPLS) technology [1] the service implementations can also be done with its use. In addition, a very important point, especially for the network operation centers (NOCs) is an automatic or semi automatic mechanism for the management of such services. The last years, only a few networks have such management tools, due to the fact that there are not many free tools, the commercial are very expensive, they are very complicated to develop them and finally they are network and technology oriented.

GRNET which is the Greek Research and Educational network [16] manages a 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 IP Premium service as well as the MBS that is presented in this paper. The work includes the design of the MBS 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 for the MBS service was designed and implemented. This management tool is part of a bigger one that manages some other services too using a common database.

The paper is organized as follows; the section 2 describes the GRNET's network and the design of the MBS service. 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. MBS Service's design

The goal of the service is to provide point to point connections of different clients with guaranteed bandwidth. Before the description of the whole design, it is necessary to describe the GRNET's network that is the case study of the design.

2.1.GRNET's Network

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 [13] 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 [15] through a POS link (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.MBS technical details

The network follows the DiffServ architecture and will provide the IP Premium and the MBS service [12]. According to this architecture, the traffic is classified and marked into classes. Also, various queues are enabled on each router and are configured to enqueue packets from certain classes.

In GRNET, we initially activated 2 queues in each link. The first one provides the classic best effort service and the second one is configured as high priority queue that is going to be used for IP premium and MBS service. The choice to use the same high priority queue for both IP Premium and MBS service was done due to the fact that the network's throughput is still low and therefore it will work efficiently. There are already plans (and design) for the activation of a third queue with given capacity that will enqueue all the MBS traffic and will leave the high priority queue only for IP Premium. In addition, the whole network has been studied and dimensioned in such a way that each connected member has a given portion of its access link's capacity for QoS (IP Premium and MBS traffic). This portion is secured in every case, even if there is a backbone link failure.

The GRNET's network uses CISCO platforms and for the queue management it uses the MDRR mechanism (Modified Deficit Round Robin) [8][13]. We designed the relevant configuration that was applied on the network and made it QoS enabled. 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.

Next, the main idea for every MBS connection is to create a layer 2 MPLS Virtual Private Network (VPN) with advanced characteristics in QoS and traffic engineering [6][7]. This approach gives the required point to point connectivity and allows the traffic management, taking advantage of the MPLS technology. The VPN has only 2 sites, the 2 end points that want the MBS connection, as CE (customer edge) routers. This approach makes the VPN establishment easy and more secure. The technology that allows the L2 MPLS VPN establishment is known with the name AToM (Any Transport over MPLS) for Cisco routers and follows specific internet drafts [2][3][10]. According to this technology, the L2 frames that came in the VPN are "encapsulated" to MPLS frames adding a VC-id and the classic MPLS label that will allow the routing in the network. The AToM technology supports the following L2 protocols: Ethernet, ATM and Frame Relay and therefore it is suitable for GRNET's case.

The next most important issue is the proper marking and policing of the traffic. For this purpose, the incoming traffic in the PE router (GRNET's edge router) is policed to the requested - admitted rate using a token bucket mechanism and the exceeded traffic is dropped. On the other hand, all the conformed packets are properly marked. The marking is done on the MPLS experimental field of MPLS label on the configured L2 MPLS VPN and remains unchangeable across the network's path. Therefore, the packet marking leads the packets in the priority queue in every network router and consequently secures the zero packet loss (guaranteed bandwidth as the policing is very tight to the admitted transmission rate).

The next step in the design of the service is the design of the traffic engineering characteristics [6][11]. For this purpose, we have studied the operation of MPLS traffic engineering tunnels that can be used in conjunction with L2 MPLS VPNs (AToM). The traffic engineering tunnels are established by the usage of certain protocols that advertise and configure the LSP (MPLS label switched path). There are 2 widely known protocols, the CR-LDP (Constraint routing label distribution protocol) and the RSVP-TE (Reservation Protocol – Traffic Engineering) and for GRNET's network we have selected the RSVP-TE.

The traffic engineering tunnel that is configured for every MBS connection has certain capabilities. In particular, all the backbone interfaces will be configured as RSVP enabled and specific bandwidth will be declared for usage from MBS tunnels. This bandwidth will be the result of the network's dimensioning and the RSVP uses this information to perform admission control on every new LSP. It can also be used to perform load balancing, by calculating all alternative LSPs for a tunnel and next to select that LSP that has the minimum reservations. In addition, the traffic engineering tunnel provides capabilities to declare explicit path that the traffic will follow (by selecting the chain of the routers), but in GRNET's case we selected the dynamic routing of the LSPs. Finally, a very important issue that has been designed for the MBS' traffic engineering tunnels is the fast-reroute feature that reroutes the traffic from a tunnel when the initial tunnel is down due to a link failure or other reason. This is done through a mechanism that is called shared explicit. It establishes a new LSP, maybe using different path, without waste of resources, as in the common links, the reservation for the new LSP is not added to the summary of the reservations but it is considered as backup of another one.

Consequently, the design of the MBS service contains the creation of a L2 MPLS VPN for every requested connection. This VPN is created by "connecting" 2 sub interfaces and transmitting all traffic from one sub-interface to the other with out any external impact and securely. For GRNET's network, the sub-interfaces will be Gigabit Ethernet sub-interfaces (VLANs). Next, the incoming traffic to the PE router will be policed and marked to value 5 in MPLS EXP. The marking is done in the first mpls label that is added by the AToM technology in the L2 frames that comes from the sub-interfaces [1][10]. Next, the traffic is declared to follow a traffic engineering tunnel that has been configured with all the above characteristics (Figure 1 presents a typical MBS connection). The insertion of the traffic in the tunnel is done by adding a new MPLS label on the "MBS mpls frames" [11], and in this case the marking of the MPLS EXP in the previous label is copied to the label added by the tunnel. The later is necessary in order to have the packets marked in all nodes (as only the outer mpls label is always examined) and therefore use the priority queues.

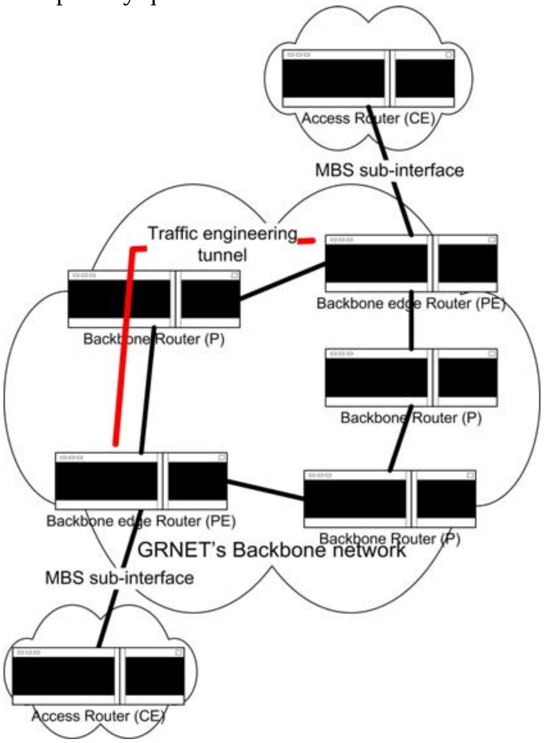


Figure 1: A typical MBS connection

3. Network Implementation issues

After the design phase of the MBS service, 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 2 queues on every output interface. Next, the same backbone interfaces was declared to use RSVP and the appropriate bandwidth that is available for reservation was declared.

The above steps made the network operational and we started configuring and evaluating all the other mechanisms. Firstly, the creation of L2 MPLS VPN tested successfully, as this feature is widely known. This test in the network infrastructure noticed 2 main restrictions, where the first one is the necessity for the 2 Ethernet sub-interfaces to have the same vlan id. This restriction is important but it must be considered as temporary as the routers' vendor (CISCO) has already developed a technique for this that will be available in newer software release. The second restriction is the fact that it is not possible to connect 2 sub-interfaces (vlans) that exist on the same router. This one is proportional related to the first restriction and is due to AToM's implementation that distinguish the destination by the loopback IP address of the router and the vlan id.

The next step was the evaluation of the QoS (policing, marking and queue management mechanisms) as well as the traffic engineering, over the L2 MPLS VPNs. These features was configured on network's testbed and remained operational in order to investigate possible performance aspects. Finally, from the configuration and evaluation of the mechanisms, a fully operational MBS connection, with all the above features, was enabled on the backbone network. In addition, the configuration template for each MBS connection's end device (PE router) was finalized

Table 1: Configuration template for MBS service

```
policy-map pm_mbs[id]
class class-default
police cir (requested bandwidth) bc 3000 conform-action set-mpls-exp-imposition-transmit 5 exceed-action drop
exit

policy-map pm_parent_mbs_out[id]
class class-default
shape average percent 100 0 ms
service-policy pm_mbs_out[id]
exit

policy-map pm_mbs_out[id]
class class-default
bandwidth (requested bandwidth)
exit

interface Tunnel_mbs_[id]
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination (loopback of destination router)
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth (requested bandwidth)
tunnel mpls traffic-eng path-option 10 dynamic

pseudowire-class mbs[id]
encapsulation mpls
preferred-path interface Tunnel_mbs_[id]

interface GigabitEthernet0/0.(vlan id)
encapsulation dot1Q (vlan id)
no ip directed-broadcast
no cdp enable
xconnect (loopback of destination router) (vlan id) pw-class mbs[id]
service-policy input pm_mbs[id]
service-policy output pm_parent_ mbs_out[id]
```

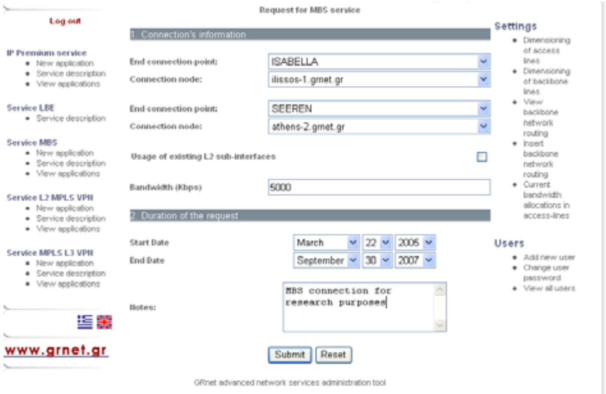
Simultaneously, the design of MBS service also contains the design of possible interconnection to the relevant Geant's service [15]. In particular, Geant is the pan-European network that interconnects all the NRENs and has connections with Internet2 and Asia. Geant implements the MBS service using L2 MPLS VPNs based on circuit cross connect (CCC) [4] method of Juniper equipment that Geant has [14]. But, the CCC method is not automatic interoperable with Cisco's AToM, as they are based on different internet standards and therefore a special handling is necessary. The basic idea is to establish an MBS connection in GRNET and terminate it at Geant's router (CE). Next, Geant will implement an MBS connection in its domain. The packets that arrive from GRNET's MBS connections should be forwarded into the new MBS connection in Geant. The interconnection of the 2 MBS connections, therefore the 2 MPLS VPNs, will be done using the MPLS stitching [14]; it is a feature of Juniper equipment that allows the interconnection of 2 different L2 MPLS VPNs at layer 2.

4. Management Tool functionalities for MBS service

Likewise, another very important issue of the proposed MBS service 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 members that are connected on the network and therefore can request an MBS connection. 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.



Request for MBS service

1. Connection's information

End connection point: ISABELLA

Connection node: ilissos-1.grnet.gr

End connection point: SEEREN

Connection node: athens-2.grnet.gr

Usage of existing L2 sub-interfaces ☐

Bandwidth (Kbps) 5000

2. Duration of the request

Start Date March 22 2006

End Date September 30 2007

Notes: MBS connection for research purposes

GRnet advanced network services administration tool

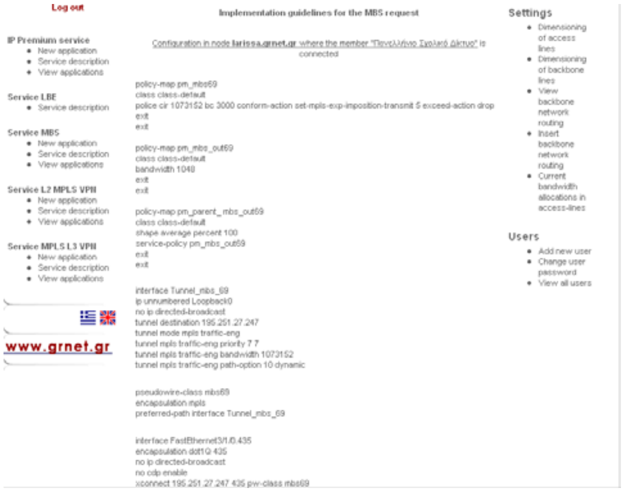
Figure 2: The management tool (form for new MBS connection)

A user of the management tool has a personalized access to a web interface and a number of capabilities as well. In particular, the user can fill in a form requesting a new MBS connection (Figure 2 shows this interface). The form is fully operational and represents the network status, routers, interfaces etc. Through this wizard the user can also choose if he wants to use existing interfaces (vlans) for the MBS, as it can upgrade an existing L2 MPLS VPN to an MBS connection. Also, the user specifies the requested bandwidth as well as the time period that he wants the connection. Next, the system checks all the input information and informs the user for possible errors. In case that everything is right, then 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, then the request goes to confirmation pending status, where the other end of the requested MBS connection is informed via email and should acknowledge or reject the request. In case the other end acknowledges it, then 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 MBS requests (active, pending or rejected). On these requests, 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 MBS 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 an MBS connection (Figure 3 shows the produced configuration for an MBS connection). 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 tool whenever using the producing configuration changes the request's status. 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.

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 can view and change the MBS configuration template. 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. Also he has the authorization to declare, through a special wizard, certain network paths that the traffic engineering tunnels between 2 routers should follow. Finally, the administrator has the responsibility for the user management (creation of new user accounts etc).

Additionally, we are working on monitoring of the implemented requests. GRNET implemented a parser and stores the applied MBS configuration on every router in its database. Taken advantage from this implementation, we are implementing a 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 during routine changes on a router.



Implementation guidelines for the MBS request

Configuration in node **larissa.grnet.gr** where the member "Πανελλήνιο Σχολικό Δίκτυο" is connected

```
policy-map pm_mbs69
class class-default
police cir 1073152 bc 3000 conform-action set-mpls-exp-imposition-transmit 5 exceed-action drop
exit
exit

policy-map pm_mbs_out69
class class-default
bandwidth 1048
exit
exit

policy-map pm_parent_ mbs_out69
class class-default
shape average percent 100
service-policy pm_mbs_out69
exit
exit

interface Tunnel_mbs_69
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 195.251.27.247
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 1073152
tunnel mpls traffic-eng path-option 10 dynamic

pseudowire-class mbs69
encapsulation mpls
preferred-path interface Tunnel_mbs_69

interface FastEthernet3/1/0.435
encapsulation dot1Q 435
no ip directed-broadcast
no cdp enable
xconnect 195.251.27.247 435 pw-class mbs69
```

Figure 3: The configuration commands

Generally, this management tool was designed and implemented in parallel with the design and implementation of the MBS 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.

5. Conclusions – Future Work

This paper described the design and implementation of Managed Bandwidth Service in a WAN network as GRNET's. The MBS service is an advanced service that provides point to point connections with guaranteed bandwidth. The service, as it is designed, is an interconnection of the L2 MPLS VPNs with QoS and traffic engineering features. Also, we have designed and implemented a management tool for the service that takes advantage of the database that keeps updated information for network's condition. The service 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 solving of the restrictions that we mentioned above and also an effort to extend it in multipoint connections with the use of CISCO VPLS technology [9]. 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, 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. In addition, future work will be based on enhancements that the service's users will demand. Finally, when the upgrade of Geant's network, through GN2 project, will be finished and its new services and management tools will be available, we plan to connect our management tool with those.

6. Acknowledgments

This work is partially funded by the project GRNET/ VNOC-2 [16]. 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 thank the GRNET, the NOC of National Technical University of Athens (NTUA) and the NOC of University of Crete (UoC).

7. References

[1] 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

[2] "Transport of Layer 2 Frames Over MPLS", draft-martini-l2circuit-trans-mpls-16.txt, Martini et al., February 2005

[3] "Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks", draft-martini-l2circuit-encap-mpls-09.txt, Martini et al., February 2005

[4] "Layer 2 VPNs Over Tunnels", draft-kompella-ppvpn-l2vpn-03.txt, Kompella et al, April 2003

[5] "Management Bandwidth Sevice on MPLS domain" C. Bouras, V. Kapoulas, D. Primpas, 17th IEEE International Workshop on Communications Quality & Reliability – CQR 2003, Kiawah Island, South Karolina, USA, April 7 – 10 2003

[6] "Traffic engineering with MPLS in the Internet" X. Xiao, A. Hannan, B. Bailey, and L. Ni, IEEE Network Magazine, pages 28–33, March 2000.

[7] "An Analysis of Virtual Private Network Solutions" Gustav Rosenbaum, William Lau, Sanjay Jha, 28th Annual IEEE International Conference on Local Computer Networks, October 20 - 24, 2003

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

[9] "VPNs: A Case for VPLS" , Cisco Systems

[10] "MPLS AToM - Configuring", Cisco Systems

[11] "MPLS Traffic Engineering LSP Attributes", Cisco Systems

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

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

[14] http://www.juniper.net

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

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