Management Bandwidth Service on MPLS domain

Christos Bouras[1,2] Vaggelis Kapoulas[1,2] Dimitris Primpas[1,2]

[1]Computer Technology Institute, 61 Riga Feraiou Str., 26221 Patras, Greece
[2]Department of Computer Engineering and Informatics, University of Patras, 26500 Rion, Patras, Greece
TEL: +30-(2)610-{960375, 960355, 996182}
FAX: +30-(2)610-960358
E-MAIL: bouras@cti.gr, kapoulas@cti.gr, primpas@cti.gr

Abstract

This paper describes an efficient way to implement managed bandwidth services. The proposed solution is based on MPLS technology and especially with the creation of virtual private networks. The virtual private networks will be layer 3 VPNs (IP VPNs) and are described all the mechanisms and the MPLS features that are necessary for the MBS service implementation. The paper also describes how the service will interact with the users and finally presents a schema for the interconnection with the MBS service of Geant.

Keywords: Managed Bandwidth Service, MPLS Virtual Private Networks, Quality of Service

1. Introduction

A very common service with high demand the last years is the managed bandwidth service. Its basic idea is the secure bandwidth reservation between the end points that request the MBS connection. The operation of MBS service is planned for the backbone network and the end points will be backbone routers. Many service providers 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 (and software based mechanisms like class based weighted fair queuing) or the use of ATM permanent virtual circuits to guarantee bandwidth. Especially, Geant had implemented it with ATM PVCs on its backbone and provided guaranteed bandwidth connections between European NRENs. Nowadays, with the emergence of Multi Protocol Label Switching (MPLS) technology [3], the service's implementations can also be done with its use. This paper describes the technical details for the implementation of MBS service on MPLS environment and also presents a full schema for the interaction between the users and the service. The rest of the paper is organized as follows; section 2 describes the MPLS technology and the new features that it can provide. Section 3 presents the technical solution for providing the MBS service on an MPLS domain and section 4 a solution to interconnect the service with the appropriate MBS service of Geant where the implementation is a little different. Section 5 describes the design of the interface with the user and finally, section 6 is dedicated for conclusions.

2. MPLS technology

MPLS is a new and powerful technology that can be categorized between layer 2 and layer 3 of ISO/OSI model. Its operation is basically to forward packets using its own rules and providing capabilities for quality of service, multicast and load balancing on a network. It creates its own header (32 bits) and inserts it to the packet header, between data link header and IP header, where it stores the necessary information. The packet forwarding is based on labels that are distributed with the implementation of label switched paths (LSPs). In particular, the LSPs are created for each connection that is needed. In addition, the network must store the necessary information about the LSPs on each router that the LSPs pass. Consequently, when the packets arrive on every router they are checked according to their MPLS header. Routers reads the label, checks its own mechanisms if there is an LSP entry for that label and if they finds it, then they forwards the packet according to LSP. This operation is also presented on Figure 1.

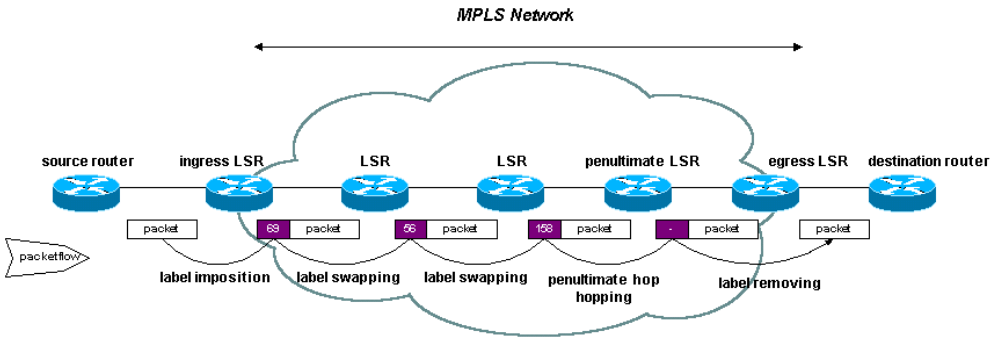

Figure 1 MPLS packet forwarding 7

Generally MPLS' operations are quite complicated and the calculations that the routers must do are many and distributed. MPLS names the edge routers on a network as label edge routers (LER), and their function is very important because the categorize packets and assigns to them labels. Besides, the intermediate routers on a network are called label switched routers and their role is simply to check and forward packets according to the labels. In addition, MPLS uses many mechanisms and protocols for the path calculation and the LSP signaling. In particular, the classic OSPF and IS-IS routing protocols can be used to perform the calculation of routing information. Besides, MPLS can work efficiently with RSVP-TE and CR-LDP that are extensions of well-known mechanisms that provide traffic engineering characteristics and LSP signaling [1]. Finally, the most important feature of MPLS is the ability to create and support virtual private networks. The basic idea of virtual private networks is that they hide packet flows from the whole network with the use of MPLS labels and LSPs. With this solution MPLS can implement networks that are invisible from the other users and can provide security and reliability. The MPLS VRNs can belong to 2 different categories, those that are implemented on layer 2 of ISO/OSI model and those on layer 3. Its operation is based on Costumer edge (CE), provider edge (PE) and provider (P) routers [2] as described on Figure 2 too. Particularly, the CE routers belong to the costumer side and are the routers that connect each site with the backbone network. Next, the PE routers belong to the service providers and are the edge routers at the provider's domain. Finally, the P

routers are the core routers at the provider‘s domain and simple forward packets according to LSPs’ information.
The establishment of an MPLS VPN is based on the implementation of LSP tunnel. At the edge of the VPN, the VPN flows are classified by adding the appropriate MPLS label on the packet header. All the labels that are used must be advertised to the entire MPLS domain and the advertisement can become by many protocols such as CR-LDP (Constraint routing label distribution protocol) or RSVP-TE (Reservation Protocol – Traffic Engineering). Besides, important point on VPN establishment is the LSP calculation, which can be done by many mechanisms. The most frequently used are the OSPF (Open shortest path first), BGP (Border gateway protocol) or IS-IS.

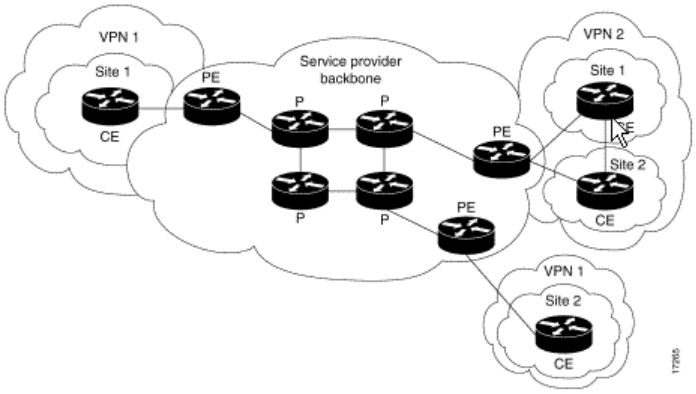

Figure 2 MPLS VPN architecture 7

3. The technical solution for providing MBS service

Our proposal is an efficient way to provide management bandwidth service on an MPLS domain, as it described above. The main idea is to create a layer 3 VPN per each MBS connection that is requested. In that VPN, there will be only 2 sites, the 2 positions that want the MBS connection. This approach makes the VPN establishment easy and more secure. Particularly, the costumer edge routers will be the access routers of the clients who want the connection. Accordingly, the provider edge routers will be the edge routers of the provider’s domain, which are connected directly with the CE routers. All the other routers in the path that the VPN use will be the provider routers.
The path that each VPN follows will be calculated with the mechanism OSPF. There are many other mechanisms too, which can calculate the path, but we decided to use the OSPF because it suites our needs better. By default the OSPF finds the best path between 2 routers, with only criterion the number of hops. On the MBS service, this isn’t always correct, because some other parameters must be taken into account too. The OSPF must check if the requested bandwidth for an MBS connection can be reserved on the path. Besides, our objective is to use fairly all the network resources, so some times it is possible the MBS connection to use a “longer” path but with less congestion in order to succeed load balancing. The OSPF mechanism creates on every router a database called OSPF database and keeps there many parameters for the network topology. On the implementation of the MBS service it is necessary to extend that database with more information, to satisfy all the above requirements. Especially on the OSPF database must be kept too the following parameters, the maximum

bandwidth of the link, the maximum possible reserved bandwidth on the link by the MBS service, the current reserved bandwidth by the MBS service and finally the current utilization of bandwidth. All the extended information on the database can be created by the definition of Opaque LSAs, which are a new LSA class [5].
So the OSPF mechanism can calculates the best path based only on the number of hops or either using a cost for each single link [3]. If OSPF is configured to use a cost metric then it is used a metric according to link's bandwidth (this is the default option) or it is forced to use a user-configured parameter. In this case, the new MBS service is proposed to use the second solution, to calculate the path using a cost for each link. This cost can be produced by the information in the OSPF database and particularly it must depend on the free bandwidth of the link that can be used by the MBS service. This approach leads to more fairly treatment of network resources. Generally, the OSPF mechanism must calculate the best path with the above criteria and check if the requested bandwidth can be reserved on that path. Finally, the output is the most appropriate path, which the requested MBS connection must follow.

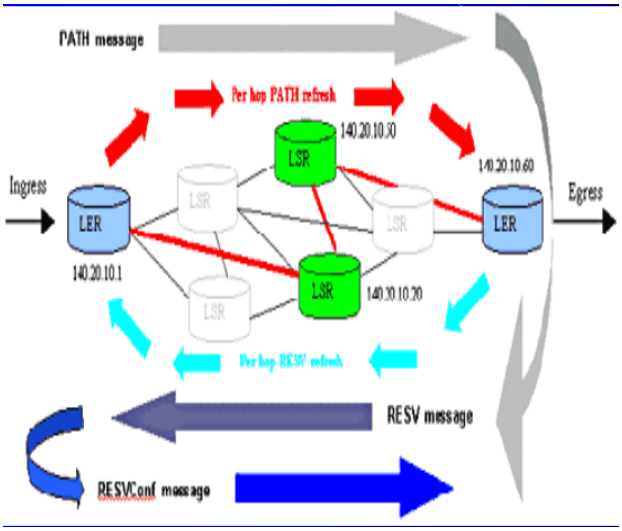

Figure 3 RSVP-TE operation for LSP establishment

After that procedure, it is necessary the use of a signaling protocol, which must advertise the labels and at the same time reserve the requested bandwidth on each link. This protocol must use as input the calculated path from the OSPF mechanism and the requested bandwidth. The available solutions are the use of RSVP or CR-LDP protocol. Our proposal is to be used the RSVP protocol with the traffic engineering extensions for the MPLS architecture. Its operation is quite simple and known; it sends a path message from the source to the destination and the destination answer with a RESV message if all the routers along the path can satisfy the request (its operation is also described on Figure 3). After that procedure, all the routers know the MPLS labels and have done the appropriate bandwidth reservation on each link. It is necessary, the RSVP protocol to take as input the calculated path and only using the explicit path feature can do it. The explicit path describes the path that the LSP will use and force the RSVP to follow that. Besides, a very important characteristic in RSVP protocol is that it has an efficient mechanism for rerouting. It is useful for the cases where there is a link failure. This mechanism is called shared explicit and calculates with an efficient way a new LSP, maybe using different path, without waste of resources. In particular, it calculates new paths that are treated as replacements of

earlier paths, in order to avoid adding the reserved bandwidth on the common links to the total reserved.
Consequently, the main idea of the proposed Management Bandwidth Service is to be implemented with MPLS VPNs. Each MBS connection will be implemented with a new layer 3 VPN and the CE routers will be the access routers of each organization, who requested the connection. The OSPF mechanism with the appropriate extensions will calculate the best path between the PE routers for the VPN. Next, the RSVP protocol will take as input the whole calculated path and the requested bandwidth and will run across the path so to make the appropriate bandwidth reservations.
The whole implementation of the VPNs and the appropriate settings on each mechanism can be done quickly using efficient tools such us CISCOWORKS. CISCOWORKS is a web-based environment, which provides access to all the routers and gives the opportunity to the administrator to configure them and also evaluate the performance of every service.
Focusing on some technical issues, it is necessary to notice some critical mechanisms for the VPN implementations. In particular, CISCO uses a schema called VRF (Virtual routing forwarding) that uses the CEF (CISCO Express Forwarding) mechanism and an IP routing table. The VRF instances determine the sites of a VPN at costumer edge that are connected to PE routers. Generally, VRF and CEF must be configured properly on each router in order to connect safely the end sites. Similarly, Juniper and all the other manufactures dispose analogous schemas. In addition, the implementation of a VPN can be separated on several independent steps. The first one is the configuration of the interface and the IGP on the PE routers. Secondly it is the declaration of a VPN with the creation of the routing tables on every router and the creation of the VRF instances. The third step is the configuration of routing between PE routers and the fourth the configuration of routing between PE and CE routers. Finally, the last steps are the configuration of P and CE routers, where it must agree with the respective configuration settings of PE routers.
Finally, it must noticed that the proposed solution, as presented above, is designed and will be implemented on the GRNET [8] backbone where it uses CISCO infrastructure [6].

4. The interconnection with Geant

Simultaneously, in this paper is proposed a way to interconnect this service with the corresponding on Geant's domain, as presented on Figure 4 [4]. Geant implement the Management Bandwidth service using MPLS VPNs at layer 2 which are not directly interoperable with layer 3 VPNs. Besides, Geant use Juniper equipment and the method circuit cross connect to implement the VPNs [7]. The basic idea for the interconnection is the network to treat each request to Geant's domain as a request to his edge router connected with Geant. The client's access router and the network's edge router will be the CE routers of the new VPN. That VPN will be implemented as described above. At the edge router, with the connection with Geant, the packet will arrive using the MBS connection and all the labels will be removed. Next, Geant will create a Layer 2 VPN across its domain where PE router will be his edge router and CE router the network's edge router, which is directly connected with the PE router. The packets then will be forwarded to the new VPN and arrive to the destination. The connection between CE and PE router is implemented using POS technology. The circuit cross connect method requires the encapsulation method at the 2 sites to be the

same and the POS interfaces that are supported are CISCO-HDLC, PPP and Frame Relay. So, at the VPN's CE-PE connection must be used one of the above interfaces and the decision must be taken according to the interfaces supported to the destination. Generally, the main direction, according to our opinion, will be the use of Frame Relay.

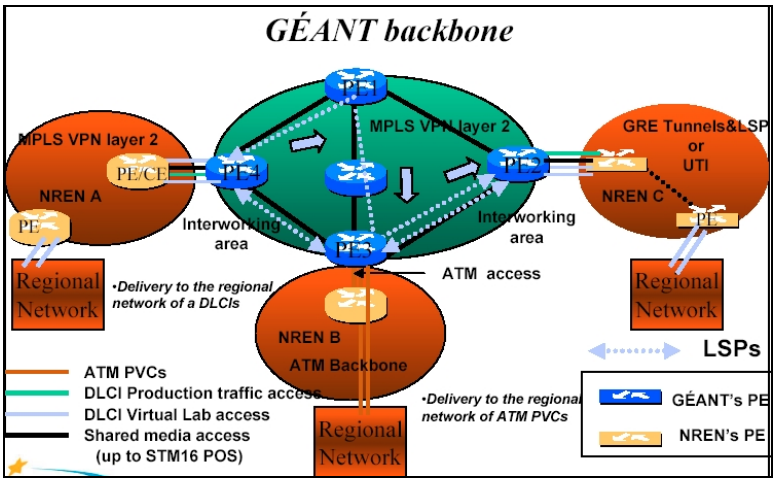

Figure 4 Geant's design for MBS service 7

5. The interface with the users

Likewise, another very important section of the proposed Management Bandwidth Service is its interface with the users. Particularly, our proposal is the implementation of a new web site, which will inform the users and interact with them. The users will have limited access to the web site (username and passwords will have been assigned to them). Every time they want to connect to the web site, they will be asked for their information. Next, they will have authorized to access specific procedures in the site; they will be able to request a new MBS connection or to take more information about the service. In addition, the web site will be supported by a database, which will store all the exchanged information.

Consequently, the users will have the ability to request an MBS connection by filling out a specific form. That form will be stored to the database and will be announced to the service administrator. The service administrator is proposed to be responsible for the administration of the web site too and he will have access to more procedures than a user. In particular, there will be a mechanism that will inform him for the new requests so to take action about them. In this case, he will implement the new connections, he will create the appropriate VPNs and next it is necessary to store the corresponding information to the base. The last can be done by filling out a new form with the VPN characteristics, the reserved bandwidth, the VPN id, the expiration time etc. Also is proposed to be available a procedure that will inform the administrator for the expired connection so to delete them. Then, he must configure the routers to delete the corresponding VPNs and next he must also delete the connections' entries to the database too. Finally, it is useful the administrator to have access to procedures that will allow him to change the VPN characteristics for existing connections.

Likewise, in the case of a connection with Geant, a very important point is the way of making the request to Geant to implement the VPN in its domain. When the

administrator receive a request which crosses the Geant domain, must check if the connection in local network is possible and simultaneously make a request to Geant. That request must contain the end point of the requested connection and the requested bandwidth. If the answers from Geant and local network are positive, that is the MBS connection can be supported, then the VPNs on the two domains must be implemented. Otherwise the user that made the request must be informed for the reasons that lead the service to reject his request.

6. Future Work

As a conclusion, the paper describes a new efficient technique to provide Management Bandwidth Service on MPLS domain. This method is based on Virtual Private Networks and provides connections with guaranteed bandwidth. The proposed service is very efficient and scalable and could be extended in the future to provide more Quality of Service characteristics inside each VPN. In addition, it is interoperable with other implementation solution of MBS service in order to extend the service. However, there are several issues that is necessary to be investigated in the future. First of all, an issue that must be noticed is the ability of creating MPLS stacks on each link with total bandwidth reservation. The most important point that must be investigated is if it can support the LSPs to have each one guaranteed bandwidth. Besides, the future work must be focused on the implementation of the above solutions and the evaluation of its performance.

7. References

[1] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999

[2] E. Rosen, Y.Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999

[3] "Advanced MPLS Design and Implementation", Vivek Alwin, CISCO PRESS, ISBN 158705020X

[4] Deliverable D9.5 "Proposal and implementation plan of the migration of current MBS", Geant's Report, Work Package 8

[5] "Traffic Engineering Extensions to OSPF", Dave katz, Derek Yeung, internet draft (draft-katz-yeung-ospf-traffic-00.txt) 1999

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

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

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