A MPLS Simulation for Use in Design Networking for Multi Site Businesses

Petac Eugen
"Ovidius" University of Constanța, Faculty of Mathematics and Computer Science
epetac@univ-ovidius.ro

Abstract

The ease of administration and its reduced costs make the MPLS (Multiprotocol Label Switching) technology attractive to those who want to deploy a performant, reliable and scalable private network. Connecting enterprises to remote locations, customers, and vendors via the MPLS is a very flexible solution that is being taken into account by many communication providers. VPN (Virtual Private Networks) is one of the most demanding services for the MPLS technology. The service providing of MPLS Differentiated Services (MPLS DiffServ) allows the customization of each client's traffic. This paper briefly outlines the theoretical aspects of the MPLS technology. The theoretical analysis is summed up in a case study called MPLS_DiffServ, developed with the OPNET Modeler simulator. This simulator allowed us to create a network model and configure the network equipment to provide MPLS DiffServ services. The results that are obtained from the simulation run are suggestive for networking education and a good starting point for the networking research area, as services for new business environment.

Key words: MPLS, QoS, Differentiated Services, Network Simulation.
J.E.L. Classification: L8, M1, M3

1. Introduction

In a dynamic business environment, characterized by innovations and technological advances, MPLS (Multi-Protocol Label Switching) allows the connectivity of data centers to branch offices, or branches to each other, based on major advantages such as: any-to-any connectivity, built-in support for Quality of Service (QoS), Service-Level Agreements (SLAs) with delivery guarantees, outsourced routing, lower cost, scalability (MegaPath, 2010). The MPLS network has become a platform for new communications and cloud-computing services, which enables voice and data to be transported together on wide area networks (WANs), with possibility to integrate VPN (Virtual Private Networks) connections for added encryption and security (AT&T, 2015).

Network simulation is a technique for modeling the behavior of a network, either by computing the interaction between different network entities (end devices, intermediate devices, links, packets, etc.) by using laborious mathematical methods, or by observing the behavior of a functional network. OPNET Modeler, NS2, NS3, GNS3, Packet Tracer, OMNeT++ (Wehrle, Günes and Gross, 2010) are some of the dedicated software solutions, being known as network simulators. They implement network simulation techniques, enabling the development of simulation models within this field.

The case study presented in this paper is developed in OPNET Modeler (Sethi and Hnatyshin, 2013). Choosing this software solution has the following main arguments: object-oriented modeling and graphical interface; the ability to analyze through graphs; the possibility of hierarchical network viewing; the running and then the choice of comparing multiple scenarios; the possibility of importing traffic patterns within the scenarios; the possibility of fully simulating heterogeneous networks with various protocols; the option of modifying the network parameters and being able to observe the immediate effects. Being given the costs associated with the construction and the functioning of a network, OPNET Modeler represents a viable solution within the decision-making processes of planning, modifying and analyzing the network performance. It

can be used as a tool for research or to design and analyze modern networks. The workflow of this simulator is based on the following steps: create network models, specify statistics and data collection, run simulations, view and analyze results. These are the steps that have been followed in this paper, in our MPLS_DiffServ network modelling.

2. MPLS Overview

Multi-Protocol Label Switching (MPLS) is a packet-forwarding technology which uses labels in order to make data forwarding decisions and aims to simplify core IP routing. The MPLS architecture (De Ghein, 2016) was designed to provide a unified data service for many traffic types, such as IP packets, ATMs, SDH frames, or Ethernet. MPLS uses a solution that integrates both IP routing control (Layer 3 of the OSI model) and data link switching (Layer 2 of the OSI model) (IETF, 2010). The MPLS architecture separates the control and data planes. Control plane is responsible for exchanging Layer 3 routing information and labels. Data plane (forwarding plane) is responsible to forward packet based on labels and IP header. MPLS defines a mechanism based on CEF (Cisco Express Forwarding) for forwarding the packets to network routers (Sayeed and Morrow, 2006).

In an MPLS network, input streams are classified into equivalence classes. These are treated equally by the nodes of the network. An equivalent class corresponds to a set of fixed length labels. They will be switched to the nodes of the network, until they reach the destination. Input nodes will classify the streams, whereas the intermediate nodes have less to process because it is enough to switch labels. Label swapping allows to change the label value in the MPLS header during MPLS routing, in an independent way of the Layer 3 routing protocol.

The subscribers with different access lines can be grouped MPLS without changing their current environment, as MPLS is independent of the access technologies. The integration of the MPLS components, including Level 2 VPN, Level 3 VPN, Traffic Engineering, QoS, GMPLS, or IPv6, enables the development of secure and highly efficient networks that guarantee SLA (Service Level Agreements) ((De Ghein, 2016). MPLS offers IP point to point services with a high degree of scalability and differentiation, with very simple configuration and management for both the vendors and the subscribers. This solution is supported by a very wide range of platforms, which is essential not only to service providers but also to private networks. MPLS uses IPv4 and IPv6 addresses to identify network terminals or the intermediary switches and routers. This makes MPLS networks IP-compatible and easy to integrate with the traditional IP networks (Goralski, 2009). Unlike the traditional IP networks, MPLS flows are connection-oriented and packets are routed on pre-configured paths, called LSP (Label Switched Paths).

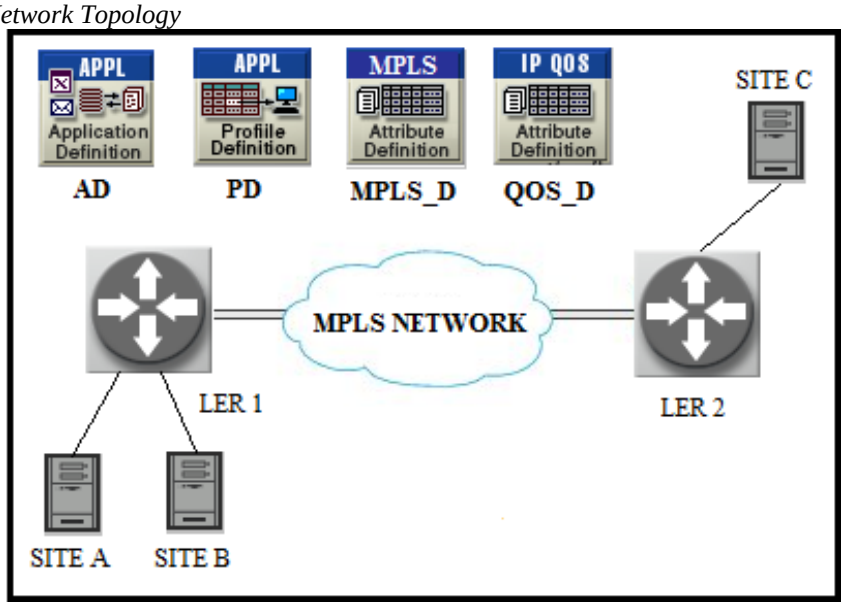
3. Modeling the MPLS_DiffServ Network

Using the OPNET Modeler simulator, we build a network that uses MPLS QoS Differentiated Services (DiffServ) for forwarding the packets within the MPLS domain. Assured Forwarding (AF) defines different services of forwarding assurances through a DiffServ domain. The MPLS DiffServ mechanism highlights the differentiated treatment of two traffic flows in the context of service quality (Srecko, Krile and Perakovic, 2009). The our objective is to analyze the way two different customers transmit the same type of traffic (for example, FTP-File Transfer Protocol) over a common path, called the Label Switched Path (LSP), but with different priorities. MPLS LSPs carry two data streams and use DiffServ codes to assign different QoS levels for each of them. The chosen network model will be configured to secure two LSPs associated with the two client input ports. The streams sent to these ports include packets for FTP applications but have different tutorial behaviors: AF3x, for High priority FTP (SITE A), and AF1x for Low priority FTP (SITE B), x=1,2,3. For the analysis of the results, it will be highlighted the differential treatment of packages from different Forwarding Equivalence Classes (FEC) (De Ghein, 2016) and the effects of these treatments under normal and congestion conditions in the network.

3.1. Network Development

The OPNET Modeler simulator offers a wide variety of equipment and solutions to create the elements of a network. In order to create the MPLS_DiffServ domain within OPNET Modeler, it is important to determine which are the required network nodes and attributes that need to be configured. Adding nodes to the project is done using the Object Palette' simulator. This contains the available nodes, broken down by network type, manufacturer, component type, etc. The network corresponding to the case study is shown in figure 1.

Figure no. 1. Network Topology



Source: Made by Author

The mandatory network nodes are:

- SITE A, SITE B - are responsible for generating traffic within the network;
- SITE C - is used in client-server applications; connect to a data exchange workstation (SITE A, SITE B);
- LER (Label Edge Router) routers - represent the input or output nodes of a LSP, ingress (LER 1) and egress (LER 2); there are nodes to which workstations and servers are connected; have the role of classifying and associating traffic to the used in guidance classes, and perform label disposition or removal (POP) and forwards IP packet to destination.
- LSR (Label Switch Router) routers - represent intermediate nodes, present in the MPLS NETWORK cloud; they change labels along the LSPs; depending on its location in MPLS domain, this router performs label disposition (removal, POP), label imposition (addition, PUSH) or label swapping (replacing the top label in a stack with a new outgoing label value).
- Application Definition (AD) - defines the types of applications that can be used to simulate the network traffic;
- Profile Definition (PD) - creates one or more profiles that select the applications that will be used by the workstations when they start transmitting data;
- MPLS Attribute Definition (MPLS_D) - is responsible for configuring the FEC (Forward Equivalence Class) and Traffic Trunk [4] associated with different flows;
- QOS Attribute Definition (QOS_D) – allows the configuration of the QoS parameters.

The configurable attributes are:

- FEC (Forwarding Equivalence Class) specifications - states the equivalent classes that may be forwarded the same way; these can be specified by: one or more combinations of the ToS (Type of Service) field, the protocol used (TCP, UDP, OSPF, ICMP, etc), the source or destination IP address, the source or destination port;

- Profile Traffic Trunk - specifies different traffic profiles with different maximum traffic rates, averages, traffic bursts, action for packages that are out of profile. Each Traffic Trunk is associated with a DiffServ class;
- MPLS parameters - MPLS parameters used and that need to be configured in each LER and LSR;
- TE (Traffic Engineering) configurations – are done in each LER. These are used to perform traffic associations: different FEC classes and Traffic Trunk profiles are linked to different interfaces and can be assigned to different LSPs.

The Label Switch Path (LSP) used in this scenario is static, having specified all the nodes through which it passes. The links used between the routers within the MPLS domain are DS0 with a 64Kbps capacity, having the purpose to demonstrate how to prioritize the packets associated with each traffic profile under congestion conditions within the network.

The stations we are going to monitor in this scenario are SITE A and SITE B, in the posture of customers, who will perform FTP data traffic to SITE C, the server.

3.2. Network Configuration

- The Application Definition (AD) node is a traffic management type that may exist within the MPLS_DiffServ domain. For this scenario, a File Transfer Protocol (FTP) application was used.
- Profile Definition (PD) - The second step in the network setup is to create a profile that will be assigned to customers. This is done in the PD node, choosing the three types of traffic listed above.
- MPLS Attribute Definition (MPLS_D) is the node defining the FEC types used by the LSR nodes within the network, the correspondences between the EXP (Experimental bits) field and the PHB (Per-Hop Behavior) behavior or, as the case may be, between the EXP field and the drop precedence field as well as the traffic profiles. Because the LSP used for packet forwarding is of E-LSP type, the packet treatment in each node will be determined by the EXP field and standard mail will be used. The two network clients, on which we observe the MPLS DiffServ mechanism, have demanded different package-handling priorities, so they have different traffic profiles. SITE B will have a higher priority on packet transmission than SITE A. This is possible thanks to the MPLS DiffServ mechanism that allows customization of each client's traffic. The higher priority client will be associated with an AF3x behavior, and the one with the lower priority with AF1x, x=1,2,3. No action will be taken on cases where packages are out-of-profile. Packages are mapped to the lowest AFx1 drop-down precedence (AF11, AF31).
- Workstations Configuration - The SITE A and SITE B workstations, simulated clients, are configured with the same MPLS DiffServ profile to benefit from the data traffic set in PD. Both stations will transmit the packets at the same pace, at the same rate, the same size, and will be equal at the time of the transmission.
- Label Edge Router Configuration (LER) - The packages arrive at the LER router where they are checked to see if they fit into the client's traffic profile. To do this, first need to be configured how traffic from customers is delimited. In the configuration of the LER 1 input node, the traffic profiles are mapped to the client interface: 64Kbps AF1x on interface 1, low priority (SITE A), and 64Kbps AF3x on interface 2 for the higher priority client (SITE B), x=1,2,3. The egress node LER 2 uses the PHP (Penultimate Hop Popping) function (De Ghein, 2016).
- Label Switch Router (LSR) - There is no other packet classification in the LSR nodes. LSR nodes are designed to switch the labels and to respect the package handling according to the deduced PHB in the EXP field of the package. This is done by configuring the LSR nodes, present in the MPLS NETWORK cloud.

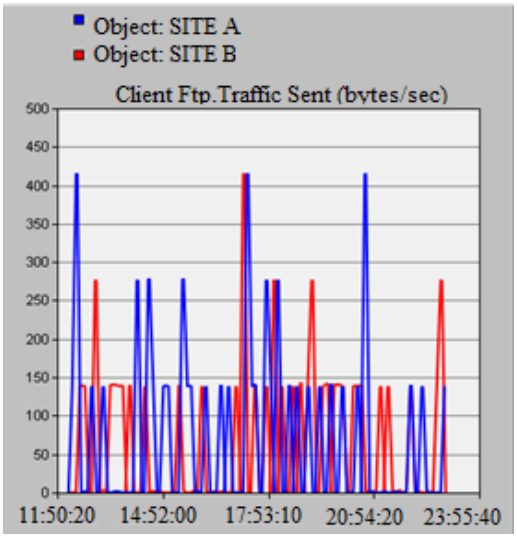
4. Statistics and Results

We will now analyze the results obtained only under congestion on the network conditions. These conditions provide data on which to draw relevant conclusions. In the scenario we created and run as discrete event simulation (DES) (Sethi and Hnatyshin, 2013), tracking then the parameters: the amount of traffic transmitted, the upload time, the delay from the queues, the use of queue buffers. Based on these we will further analyze the performances of the MPLS-DiffServ model.

- **The amount of traffic transmitted**

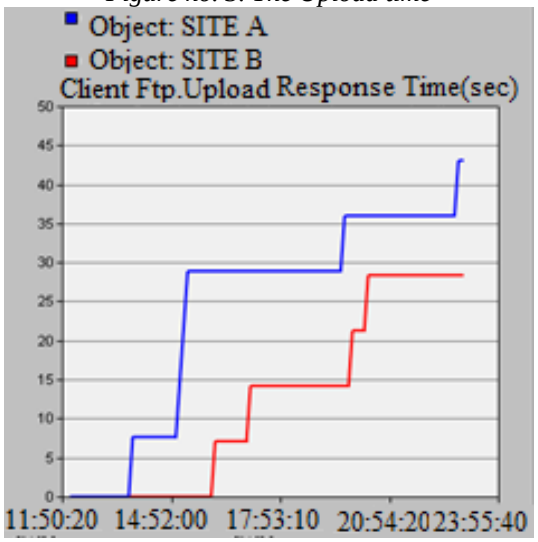
Following the simulation run, it can be seen that there is an equal amount of traffic transmitted by both clients (Fig. 2). This is important because we can make future comparisons in nearly ideal conditions and we can clearly see the differences.

Figure no. 2. The amount of traffic transmitted over the network



Source: Made by Author

Figure no. 3. The Upload time



Source: Made by Author

- **Upload time**

The upload time is the time elapsed between the start of the packet transmission and the receipt of the confirmation packet. This also includes the signaling time for connection setup and connection timeout. Figure 3 clearly shows that the upload time for SITE B is significantly lower than SITE A. This statistic shows that for a client with higher priority traffic, its packets arrive at the server faster than the client with lower priority. This is due to the MPLS DiffServ classification that allows the traffic to receive preferential treatment in the LSP nodes in favor of certain streams, respectively in the detriment of others.

- **Queuing delay**

As mentioned above, each flow receives individual treatment according to the classification that is made in the ingress node. The better the classification results in the better the treatment.

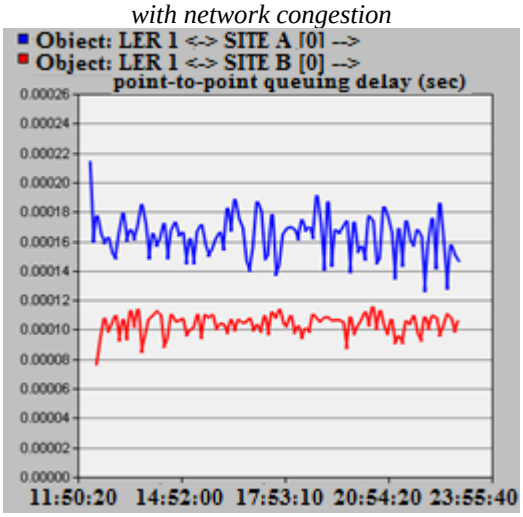
Within the ingress node, after the measurement, conditioning and traffic classification has been done, the flux is distributed in waiting queues, which according to the serving mechanism will be sent to the next hop. In this scenario, the LSR routers use the Weighted Fair Queue (WFQ) technique (Sayeed and Morrow, 2006) for the queue routine. The charts represented in figure 4 show the packet delays when waiting to be delivered to the next hop in the LER 1 ingress. We notice that there are two waiting queues LER 1 - SITE A and LER 1 - SITE B. In LER 1 - SITE B the waiting time is much smaller than in LER 1 - SITE A, as proof of the MPLS DiffServ mechanism. A better prioritization of a stream has made the waiting time in the queues across the LSP much shorter, resulting in a much better response times for customers as desired by their requirements.

- **Using queue buffers**

The more a package waits in a queue, the longer the queue is occupied. In the graphs of figure 5, we can observe this, corresponding to the above queues. If there is no network congestion, both

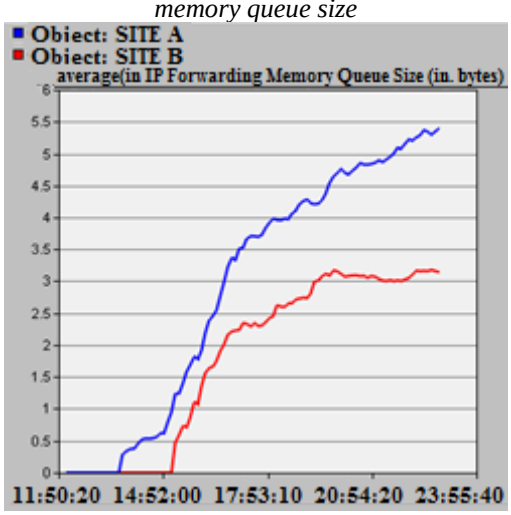
queuing time and buffers are very low. In these situations of using low packet rollout priorities, the QoS mechanism is not clearly highlighted.

Figure no. 4. The delay caused by queues with network congestion



Source: Made by Author

Figure no. 5. The average forwarding memory queue size



Source: Made by Author

5. Conclusions

The simulation results show that two similar streams to the same destination, but with different traffic profiles, behave differently at the network transit. The higher the MPLS DiffServ code stream has lower upload time, less delay and lower buffer usage. The ranking in the first node, LER 1, was designed to prioritize the traffic flow from SITE B reported to the traffic flow from SITE A.

Such classifications can be performed for each client, based on the SLA (Service Level Agreements), on the destination, traffic types, or other parameters. The MPLS DiffServ mechanism is ideal because it provides the quality that customers need, and MPLS support is best to achieve this because it benefits service providers. The granularity of MPLS DiffServ services is best absorbed by the speed of label switching and with a very good service quality. The use of differentiated services allows for the creation of new, customized quality levels according to customer requirements, while MPLS allows switching from traditional IP networks to guaranteed QoS networks, adapting at minimal cost to any physical environment.

5. References

- AT&T, 2015. *Why you still need an MPLS VPN*, [online] Available at
- < https://www.business.att.com/content/whitepaper/mpls-vpn.pdf> [Accessed 25 April 2017].
- De Ghein, L., 2016. *MPLS fundamentals*, Indianapolis: Cisco Press.
- Goralski, W., 2009. *How TCP/IP Works in a Modern Network*, Elsevier Inc.: New York.
- IETF, 2010. *A Framework for MPLS in Transport Networks, Request for Comments: 5921*, [online] Available at <https://tools.ietf.org/html/rfc5921> [Accessed 25 April 2017].
- MegaPath, 2010. *MPLS Networks for Small and Mid-Size Business*, [online] Available at
- < http://www.etimes.com/Files/WP-MPLS-Networks-for-SMB.pdf > [Accessed 25 April 2017].
- Sayeed, A., and Morrow, M. J., 2006. *MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization*, Indianapolis: Cisco Press.
- Sethi, A. S., and Hnatyshin, V. Y., 2013. *The Practical OPNET® User Guide for Computer Network Simulation*, Boca Raton, FL.:CRC Press.
- Srecko, Krile.S. and Perakovic, D., 2009. *Load Control for Overloaded MPLS/DiffServ Networks during SLA Negotiation*, [online] Available at <http://file.scirp.org/pdf/IJCNS20090500013_27257381.pdf > [Accessed 25 April 2017].
- Wehrle, K., Günes, M., and Gross, J. (Eds.), 2010. *Modeling and Tools for Network Simulation*, New York: Springer Science & Business Media.