Evaluation of tunnel layer impact on VOIP performances (IP – MPLS – MPLS VPN – MPLS VPN IPsec)

Faycal Bensalah[†], Najib El Kamoun[†], and Ayoub BAHNASSE[††]

[†]Lab. STIC, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco
[††]lab. LTI, Faculty of Sciences Ben M'SIK, University Hassan II, Casablanca, 9167 Morocco

Summary
MPLS VPN technology has emerged recently through its various advantages, especially in terms of optimization of performance, quality of service and security. However as each technology, MPLS is influenced by scalability.
In this paper we will first study the following technologies: MPLS, MPLS VPN, MPLS VPN protected by IPsec. Then we will perform an experimental study of scalability under GNS3; by increasing the load and varying technologies, in order to deduce the impact of the tunnel layer on the performance of real-time applications.
For performance measurements we used VOIP traffic generated by IP SLA probes. The evaluation criteria are: (i) jitter, (ii) latency, (iii) MOS score, (iv) loss rate.

Key words:
IP, VPN, MPLS VPN, IPsec MPLS, VOIP, GNS3, IP SLA, Scalability.

1. Introduction

Ensure good quality of communications networks becoming a primary task for modern enterprises. Indeed, most of companies have geographically distributed branch offices, which need as far as possible, have the best quality of network communications. Especially in the case where equipment such as videoconferencing systems are installed. With the multiplication of connections, data protection is a major challenge for companies. Using a virtual private network is one of the key points of an optimized security policy.
Unlike the IP protocol [1]. The MPLS reduces the number of routing searches and eliminates the need to have a particular routing protocol on each router.
Unlike the IP protocol [1]. The MPLS reduces the number of routing searches and eliminates the need to have a particular routing protocol on each router.
By assigning a label [2] to each packet, it is possible to maintain the simplicity of an architecture and also to increase its scalability.

1.1 MPLS

We distinguish two major components in MPLS routing [3]. First, the "Control plane" [4] that controls information and labels exchanged between adjacent devices.
The second is called the "Data plane" [5]. Also known as "forwarding plan", it controls the transmission of information based either on the destination addresses or on the labels.
MPLS technology consists of combining the concepts of Layer 3 (Routing), and the mechanisms of Layer 2 (Switching).
This technology brings the connected mode to the IP protocol which uses the services of level 2 (e.g. ATM [6]).
The main goal of MPLS, was previously, to increase the speed of processing datagrams. However with the appearance of Gigabit routers, operators use it for traffic engineering [7] and tunneling VPN.

1.2 MPLS VPN

In an MPLS VPN, an acronym for VPLS [8], data does not transit via the Internet, but via an MPLS backbone network of the service provider. In other words, unlike the client VPN [9], the data is not processed at source and destination gateways; they are processed at the MPLS of service provider network.
At first, the packets arrive at an LER router acronym of Label Edge Router [10] which assigns them a label according to their origin and transport mode. Once labeled, LER router assigns to the packets a path specifically adapted for each label.
The labeled data packets follow their specific route, marked by LSR (Labeling Switching Routers) [11], which routes them along the correct path.

Manuscript received March 5, 2017
Manuscript revised March 20, 2017

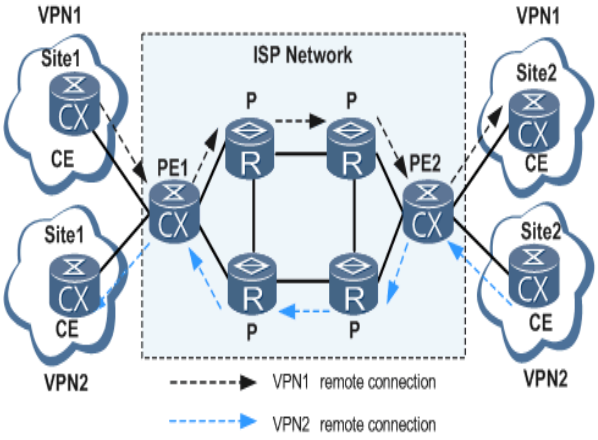

Fig. 1 MPLS VPN

However, two scenarios for securing the MPLS can be performed:

(i) End-to-end security: The client can deploy an additional security layer by IPsec protocol [12] [13] in the CE gateways. This is not advisable if the customer has a service agreement with the ISP, because end-to-end encryption will make the classification process impossible, which represents the preliminary phase of implementing QoS policies.

(ii) Security between CE and PE: This is the most deployed solution because the data passes without encryption.

1.3 MPLS VPN IPsec

IPsec, is a tunneling protocol based on two protocols ESP [14] and AH [15]. The ESP protocol guarantees confidentiality, integrity and authentication, while the AH protocol only provides data integrity and authentication.

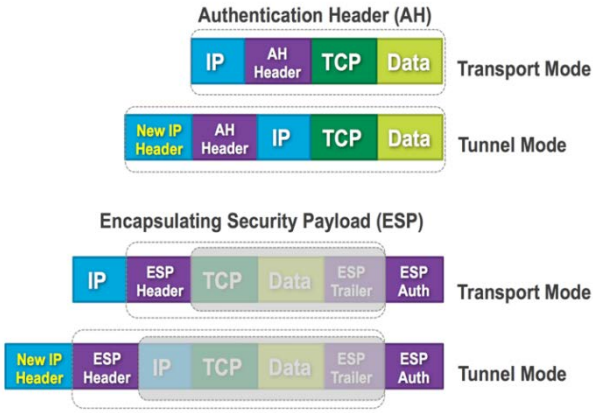

Fig. 2 methods for implementing the encapsulation of IPsec header

IPsec operates in two modes: tunnel mode and transport mode. The transport mode is interposed between the network layer and the transport layer of the OSI model.
The tunnel mode adds a new public IP header and encrypts the entire payload. (Fig. 2).
IPsec relies on several protocols for its proper functioning; Namely the ISAKMP protocol [16] for managing security associations and the IKE protocol [17] to negotiate policies and establish IPsec tunnels.

1.4 IP SLA

IP SLA [18] is a Cisco method that allows to generate test traffic between different network devices, such as routers or switches, to measure the quality of the link and applications. The advantage of this method is that it is not necessary to install additional equipment and does not require the development of new software or protocols.
In an enterprise network, quality from one end to the other must be able to be qualified according to precise criteria. This is called SLA (Service Level Agreement).
The quality of a network is measured by several indicators:

- Latency time
- Jitter time
- Percentage of packets lost (packet loss)
- Server response time

The paper is organized as follows, we will first present the related works. We will describe the simulation environment in the third section. The results obtained will be discussed in the fourth section, and we will conclude in the fifth section.

2. Related works

Performance evaluation is an active research area, as most decisions related to deployment, engineering, or design are based on results and recommendations of the evaluation.
Concerning our problem, we will try to answer on a certain number of problems:

- Measure the impact of packet load.
- Measure the quality induced by MPLS compared to IP.
- Measure the impact of the tunnel layer on VOIP performances.

Several research studies have been carried out comparing the performances of the IP and MPLS networks [19-20-21]. All these studies have resulted in the efficiency of the MPLS protocol compared to IP. The work was carried out by varying the architecture or applications. The obtained results seem very normal and expected given the nature of the MPLS protocol which offers better results, independently of the transport network or transported applications.
The work [22-23-24] performed a comparative study including traffic engineering (TE). The authors have demonstrated that the integration of TE offers a much

higher efficiency. However, this work did not take into account the increase in traffic load, which may change at some point the degree of preference of different technologies.
Previous work has been carried out under simulators such as OPNET Modeler. Papers [25-26] performed measurements in a GNS3 environment; overall, the results obtained have retained the same degree of preference.
MPLS VPN technology has been widely discussed, article [27] deals with various MPLS VPN technologies. Several works compared its effectiveness compared to IP tunneling. According to our research, all the work showed the efficiency of the MPLS VPN compared to other tunneling technologies [28-29-30]. None of these works addressed the IPsec protocol issue in MPLS VPN, its deployment, and its impact on network performance and transported applications.
Taking into account our remarks on previous work, we will propose a study that includes (i) MPLS, (ii) MPLS IPsec VPN, (iii) MPLS TE and (iv) IP. These studies will be carried out by increasing the load of the packets, taking into account the smooth configurations of the network.

3. Experimental Scenario

3.1 Simulation Environment

This project addresses voice performance and evaluates the performance of MPLS, MPLS VPN, MPLS IPsec VPNs and IP networks.
Studies were performed under Graphical Network Simulator GNS3 [31]. As background traffic, we used VOIP traffic. For the generation of traffic, we used IP SLA. Network Testbed is shown in Fig. 3:

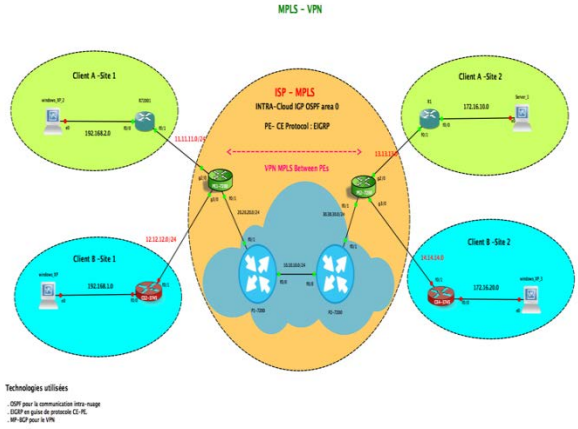

Fig. 3 Network Testbed

From this Testbed, 64 scenarios was created based on IP, MPLS, MPLS VPN and MPLS IPsec VPN technologies, for each technology we increased the packet load by 2^2, from 64 to 475000.

3.2 Simulation Parameters

Table 1 shows the VOIP application settings.

Table 1: VOIP Parameters

Traffic	VOIP
Codec	G.711 with silence suppression
Packet interval	20 ms
Number of packets	1000

Table 2 illustrates the evaluation criteria:

Table 2: Evaluation Criteria

Jitter	Jitter is the variation of latency over time. Specifically, jitter is the difference in end-to-end transmission delay between selected packets in the same packet stream, without taking into account eventually lost packets (RFC 3393)
Latency	Refers to the time required for a data packet to pass from the source to the destination through a network.Latency = network_delay + encoding_delay + decoding_delay + compression_delay + decompression_delay
MOS	Mean Opinion Score stands for MOS is a note given to an audio codec to characterize the quality of the reproduction of speech. The score can range from 0 (very bad) to 5 (excellent, comparable to the original version). It is defined by the ITU-T in the standard « P.800 : Méthodes d'évaluation subjective de la qualité de transmission ».
Loss rate	Percentage of Packet Loss

Table 3 illustrates the configuration of the equipment used in the simulation:

Table 3: Routers and links used in simulation

P	c7200-advipservicesk9-mz.152-4.S5.image
PE	c7200-advipservicesk9-mz.152-4.S5.image
CE	c3745-advipservicesk9-mz.124-25d.image
Link CE-PE	FastEthernet 10MB
Link PE-P	GigaEthernet 1000MB
Link P-P	GigaEthernet 1000MB

Table 4 illustrates routing protocols used in the simulation:

Table 4: Routing protocols of experimentation

intra-cloud routing	OSPF
Between CE and PE	EIGRP
VPN Tunnel Routing	MP-BGP

Table 5 shows the IPsec parameters used in the IPsec MPLS VPN scenario:

Table 5: IPsec Parameters

Authentication	PSK
Integrity	SHA

Encryption	AES
Group	5
Lifetime	86400

4. Obtained results and discussion

4.1 Jitter

Figure 4 illustrates the jitter value in the various scenarios: IP (a), MPLS (b), MPLS VPN (c), and MPLS VPN IPsec (d).

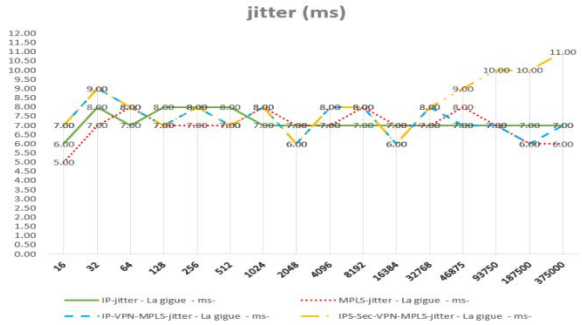

Fig. 4 Jitter

The obtained results show that in the first three scenarios the values are almost identical. However, with the introduction of the encryption layer the jitter increases, from the scenarios of 46875 bytes of load.

4.2 Loss Rate

Figure 5 illustrates loss rate results, as shown, all IP Based scenarios bypass recommended loss rate values. IP pass to 5% from the scenario of 2048 byte, while IPsec MPLS VPN resists to the load up to the scenario of 46875 byte. However MPLS Based technologies offer a loss rate less than 1%.

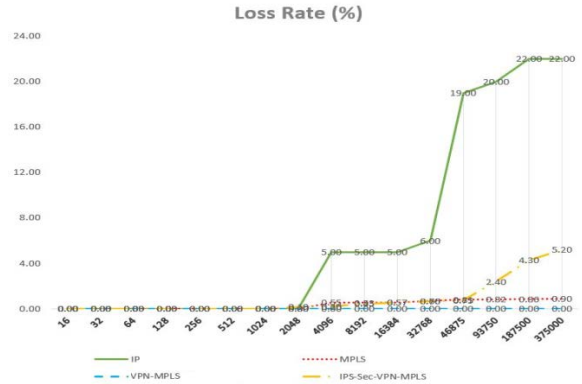

Fig. 5 Loss Rate

4.3 Latency

Figure 6 illustrates the latency results. Taking into account the results of the loss rate, it can be seen that the IP protocol is not scalable even if it proposes a lower latency compared to the other scenarios.

The MPLS protocol offers good results, the same results are shown from MPLS VPN. The difference between them is justified by the process of routing in the tunnel and the dual labeling process performed in MPLS VPN.

IPsec, as in the IP network, adds an additional delay, making VOIP unusable from scenario of 46875 bytes.

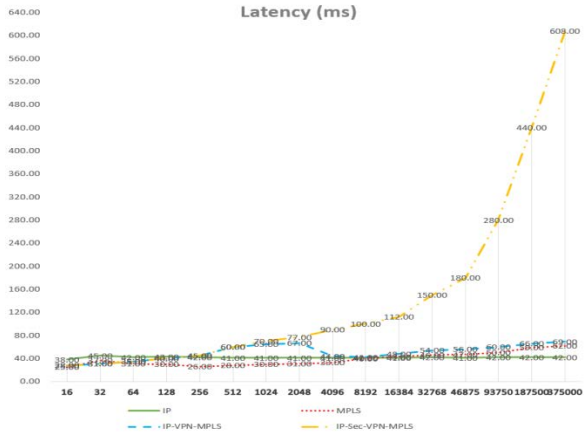

Fig. 6 Latency

4.4 MOS

Figure 7 shows the MOS score. MPLS offers the most suitable score, while IP and IPsec based scenarios offer the worst quality of speech. MPLS VPN offers an acceptable score.

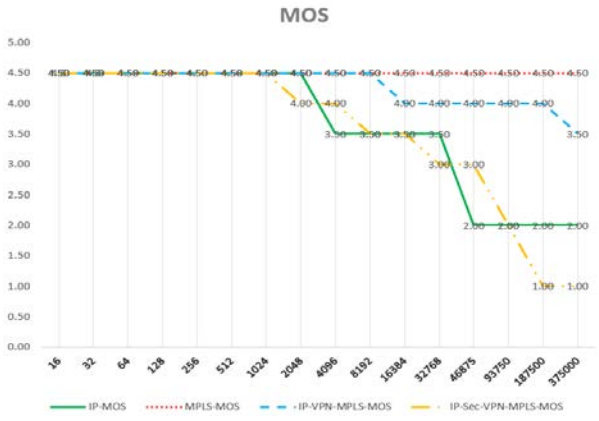

Fig. 7 MOS Score

5. Conclusion

In this study we evaluated the scalability of architectures: (i) IP, (ii) MPLS, (iii) MPLS VPN, and (iv) MPLS IPsec VPN. Measurements were made by increasing the packet load. The results obtained showed that the IP network is affected by a high latency and a bad MOS score. In contrast, MPLS technology is a faster transfer technique than IP transmission even when the loads rise.

MPLS VPN offers acceptable results close to MPLS technology alone in terms of latency, jitter and MOS score. Its additional values can be justified by dual labeling and routing on the tunnel.

IPsec in MPLS VPN leads to a degradation of performance with the rising loads.

References

[1] FALL, Kevin R. et STEVENS, W. Richard. TCP/IP illustrated, volume 1: The protocols. addison-Wesley, 2011.

[2] DECRAENE, Bruno, LE ROUX, J. L., et MINEI, I. LDP extension for inter-area label switched paths (LSPs). 2008.

[3] LE ROUX, Jean-Louis. MPLS: applications à l'ingénierie de trafic et à la sécurisation. Techniques de l'ingénieur. Télécoms, 2006, no TE7577.

[4] DAS, Saurav, SHARAFAT, Ali Reza, PARULKAR, Guru, et al. MPLS with a simple OPEN control plane. In : Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference. IEEE, 2011. p. 1-3.

[5] MOISAND, Jerome P., AGGARWAL, Rahul, WADHWA, Sanjay, et al. Layer two (L2) network access node having data plane MPLS. U.S. Patent No 8,121,126, 21 févr. 2012.

[6] PHAM, C. D. et FDIDA, S. Evaluation de Performance des Reseaux ATM: Etude et Perspectives en Utilisant la Simulation Distribu ee. In : Actes du Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'96). 1996. p. 17-31.

[7] BEKER, Sergio. Techniques d'optimisation pour le dimensionnement et la reconfiguration des réseaux MPLS. 2004. Thèse de doctorat. Paris, ENST.

[8] SUN, Ming-Song et WU, Wen-Hao. Engineering analysis and research of MPLS VPN. In : Strategic Technology (IFOST), 2012 7th International Forum on. IEEE, 2012. p. 1-5.

[9] DORASWAMY, Naganand et HARKINS, Dan. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.

[10] HAMA, Daisuke. Network and edge router. U.S. Patent No 7,072,346, 4 juill. 2006.

[11] GUICHARD, Jim, ROSEN, Eric, et RAZA, Syed Kamran. Selective label retention in a label switching network. U.S. Patent No 8,891,553, 18 nov. 2014.

[12] ZHANG, Mu et TAO, ZhongPing. Application research of MPLS VPN all-in-one campus card network based on IPSec. In : Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on. IEEE, 2012. p. 872-875.

[13] REN, Rong, FENG, Deng-Guo, et MA, Ke. A detailed implement and analysis of MPLS VPN based on IPSec. In : Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on. IEEE, 2004. p. 2779-2783.

[14] JOKELA, Petri, MELEN, Jan, et MOSKOWITZ, Robert. Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP). 2015.

[15] RAZA, Shahid, DUQUENNOY, Simon, et SELANDER, Göran. Compression of ipsec ah and esp headers for constrained environments. 2013.

[16] IACOB, Nicoleta Magdalena. Security for Virtual Private Networks. Knowledge Horizons. Economics, 2015, vol. 7, no 3, p. 176.

[17] NIR, Yoav. ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec. 2015.

[18] TEARE, Diane, VACHON, Bob, et GRAZIANI, Rick. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide:(CCNP ROUTE 300-101). Cisco Press, 2014.

[19] Naoum, R. S., & Maswady, M. (2012). Performance Evaluation for VOIP over IP and MPLS. World of Computer Science and Information Technology Journal (WCSIT), 2(3), 110-114.

[20] Porwal, M. K., Yadav, A., & Charhate, S. V. (2008, July). Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS. In Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on (pp. 187-192). IEEE.

[21] Akinsipe, O., Goodarzi, F., & Li, M. (2012). Comparison of IP, MPLS and MPLS RSVP-TE Networks using OPNET. International Journal of Computer Applications, 58(2).

[22] Gous, A., Afrakhteh, A., & Evans, J. (2016). A Comparison of Approaches for Traffic Engineering in IP and MPLS Networks. arXiv preprint arXiv:1608.03770.

[23] Yousif, A. A. O., Sharif, S. M., & Ali, H. A. (2015). Comparison Between Ngn Core Networks Protocol (Mpls) And Traditional Networks Core Protocols (Rip & Ospf) Using Opnet. Sudan Engineering Society Journal, September 2014, Volume 60; No.2.

[24] B. Boudani, B. Cousin, C. Jawhar, and M. Doughan, "Multicast routing simulator over MPLS networks", Proceedings of the 36th Annual Simulation Symposium (ANSS'03), Orlando, Florida, March 2003, pp. 327–334.

[25] Kathiresan, S. (2015). Performance Analysis of MPLS over IP networks using CISCO IP SLAs (Doctoral dissertation, SIMON FRASER UNIVERSITY).

[26] Bhandure, M., Deshmukh, G., & Varshapriya, J. N. Comparative Analysis of Mpls and Non-Mpls Network. International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, Jul-Aug 2013, pp. 71-76

[27] Shahzad, A., & Hussain, M. (2013). IP Backbone Security: MPLS VPN Technology. International Journal of Future Generation Communication and Networking, 6(5), 81-96.

[28] Xia, J. B., Li, M. H., & Wan, L. J. (2008, December). Research on MPLS VPN networking application based on OPNET. In Information Science and Engineering, 2008. ISISE'08. International Symposium on (Vol. 1, pp. 404-408). IEEE.

[29] Georgakakos, K.Implementation and performance evaluation of WAN services over MPLS Layer-3 VPN. Master Dissertation (2014)

[30] Arora, N., & Kaur, S. (2015). Performance Evaluation and Fault Repair Mechanism for Resilience of MPLS RSVP-TE

Network with different application Traffic load balancing across Label Switched Path. Performance Evaluation. International Journal of Engineering Technology Science and Research. Volume 2, Issue 11. November 2015

[31] Neumann, J. C. (2015). The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More. No Starch Press.

Faycal Bensalah received the Master degrees, Network and telecommunication, from Faculty of sciences El Jadida in 2014. Network administrator at Chouaib Doukkali University, Actually a Ph.D Student on STIC Laboratory on Faculty Of sciences El Jadida, Network and Telecommunications team. His research interest are : NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications

Najib Elkamoun Ph.D, professor higher education degree at Faculty of sciences El Jadida.in the dept. of physics. Researcher member on STIC laboratory, header of Network and Telecommunications team. His research interest includes, NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Ayoub BAHNASSE Ph.D on Networks and telecommunication received the master degrees, in 2013 and 2017 respectively. Actually a researcher associate on LTI laboratory Ben M'sik faculty of sciences. Reviewer on ELSEVIER journals. His research fields are: Security of networks, mobile learning, Wireless Sensor networks, QoS of networks, MPLS, IMS and NGN.