Novel Software-Defined Network Approach of Flexible Network Adaptive for VPN MPLS Traffic Engineering

Faycal Bensalah[1], Najib El Kamoun[2]
Lab STIC, FS El Jadida, University Chouaib Doukkali,El Jadida, Morocco

***Abstract*—Multi-Protocol Label Switching VPN (MPLS-VPN) is a technology for connecting multiple remote sites across the operator's private infrastructure. MPLS VPN offers advantages that traditional solutions cannot guarantee, in terms of security and quality of service. However, this technology is becoming more prevalent among businesses, banks or even public institutions. With this strong trend, the management of the paths on which these tunnels can be deployed has become a necessity is a priority need for Internet access providers (ISPs). Through the principle of controller orchestration, ISPs can overcome this difficulty. Software-defined network is a paradigm allowing through the principle of orchestration to manage the entire network infrastructure. In this paper, we propose a new approach called FNA-TE "Flexible Network Adaptive - Traffic Engineering", this approach allows to manage MPLS VPN tunnels to meet the QoS requirements of those with the highest priority.**

Keywords—SDN; QoS; VPN; MPLS; Adaptive network

I. Introduction

Multi-Protocol Label Switching "MPLS" is a transfer protocol that uses tags for routing data [1][2]. This technology brings more flexibility, speed, and security compared to the Internet Protocol "IP". The MPLS technology provides advantageous applications, among them we quote virtual private network "VPN" [3][4][5], quality of service "QoS"[6][7], security[8], all transport on MPLS "AToM".

Among the strengths of the MPLS technology, traffic engineering (TE) is used to optimize the use of network resources to avoid congestion. It is the consideration of the bandwidth avail-able on a link during routing decisions that makes this optimization possible. MPLS-TE allows the establishment of MPLS tunnels routed explicitly according to the constraints of the trans-ported traffic (bandwidth, delay ...) and the resources available in the network. MPLS-TE creates a connected mode in IP net-works, optimizing the use of resources and maximizing the traffic load that can flow over the network while preserving the quality of service.

In order to overcome the complexities of implementing traffic engineering policies across multiple routers, software-defined network (SDN) [9][10][11] technology can be used. SDN de-couples the data plane from the control plane by centralizing it on a device called a controller. SDN can be used to solve a variety of problems related to the complexity and the high number of equipment. SDN is mainly based on three logical layers: the given layer, the control layer, and the application layer. The application layer provides the set of services and applications used by the end user. The given layer contains the physical equipment responsible for conveying the information. The control layer contains all the operations and instructions that man-age the entire network.

The rest of the paper is organized as follows: in Section 2 we will discuss the strengths of our contributions. In Section 3 we will detail the architecture of our solution. Section 4 will focus on performance evaluation. And we will conclude in Section 5.

II. Flexible Network Adaptive – Traffic Engineering

To understand the motivation behind our approach, we will briefly describe the existing issues in MPLS VPN technology:

- A customer may have one or more VPNs with the same or different destinations.
- These VPN tunnels can have different priorities.
- Multiple MPLS VPNs can follow the same path.
- Paths can have asymmetric performance, in terms of effective bandwidth and unused bandwidth.

A. Strengths

1) Detect VPN tunnels in the establishment phase or already established.

2) Draw the architecture of the intermediate network.

3) Detect for each tunnel the associated LSP.

4) Classify tunnels by priority.

5) Decide on the shortest LSP to assign to the VPN.

6) Check that the remaining bandwidth meets the QoS requirements of the tunnel.

7) Treat tunnels fairly; that is to say, not necessarily to route the tunnel with the highest priority by the short path having sufficient bandwidth, to the detriment of the lowest priority tunnels. A higher priority tunnel can be routed through the second or nth best path if this degrades the performance of the lower priority tunnels already deployed.

B. Proof

- Let G be a graph (V, E) with V are the vertex routers and E are links. E (u, v) are the ends of a link.
- Let w be a neighbor vertex.

- Let Ba be the available bandwidth.
- The bandwidth of the first link to the source:

$$B_a^S = Min\,|\bar{B}_{au} - \bar{B}_{av}\,|$$

The bandwidth beyond the neighbor:

$$B_a^w = Min\,|\bar{B}_{a\,u+1} - \bar{B}_{a\,v+1}\,|$$

U + 1 and v + 1 to avoid a closed path.

The most optimal segment S is therefore defined by the following function:

$$S_i = Max\,\left|B_a^{si} - B_a^{wi}\right|\,;\ \forall\ i\ \in V(G)$$

Since the segments are determined; they must be sorted by available bandwidth from the highest (h) to the lowest (l).

The path with the highest available bandwidth is defined by the following equation:

$$\rho^h = \sum_{u\,\in V(G)} S_i^h\ ;\ \forall\, S_i > B_{requested}$$

Consider MPLS VPN tunnels already established on an S-segment: either Vc the number of VPN tunnels and Vp the priority of a tunnel.

Suppose that the available bandwidth of the shortest path is not sufficient, our algorithm can move to the next path:

$\rho^{h-1}, \rho^{h-2}, \dots, \rho^{h-n}$, where n is the variance.

The variance is relative to the priority. A non-priority VPN can traverse the longest path with restricted bandwidth.

$$\rho^h\left(\sum_{i=1}^{Vc} V_{pi}\right) > V_{p\,req}\ ;\ \rho = \rho^{h-1}$$

Until this phase we were able to determine the shortest path having the available bandwidth meeting the QoS requirements of the source. But, is it necessary to move the other tunnels to another path in favor of the tunnel with the highest priority? In some cases we can find the nth best way for the tunnel with the highest priority:

Case 1: It is possible that several lower priority tunnels coexist in ρ.

Case 2: Moving several non-priority tunnels to another ρ can jeopardize their quality of service.

Case 3: Sometimes routing the highest priority VPN by the nth best path does not degrade the quality of its exchanges as this path meets the customer's QoS requirements.

The following formula is used to define the closest path $\rho^{h-i}$to the best ρ^h , meeting the Breq requirements.

$$\sum_{i=1}^{Vc} V_{pi} < V_{p\,req}\ ;\ \forall\, Vc\ \in\ [2, +\infty[$$

III. FNA-TE Architecture

The proposed approach is based on three layers: application, control and data. Fig. 1 illustrates the proposed architecture.

The application layer is responsible for defining VPN tunnels and their priorities. Fig. 2 illustrates an example of the GUI interface for customizing tunnels.

The control layer can act on the path on which to deploy MPLS VPN tunnels based on the available bandwidth and the shortest route. This layer consists of five modules:

A. Network Discover

This module is responsible for detecting the network topology, V-vertex and E-links. In a hybrid network where routers do not support the OpenFlow protocol, additional protocols can be used as CDP for Cisco devices and LLDP for non-Cisco equipment. The controller verifies the network topology based on these protocols. For SDN devices, OFDP messages can be used for topology detection. In the case of the Moroccan university, specifically Chouaïb Doukkali University, the routers set up do not support SDN. The topology detected automatically by our controller is shown in Fig. 3.

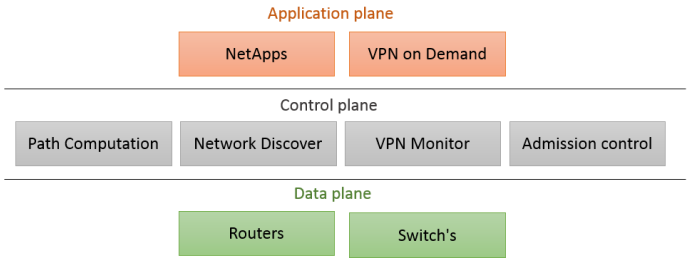


Fig. 1. The Architecture of the Proposed Approach.

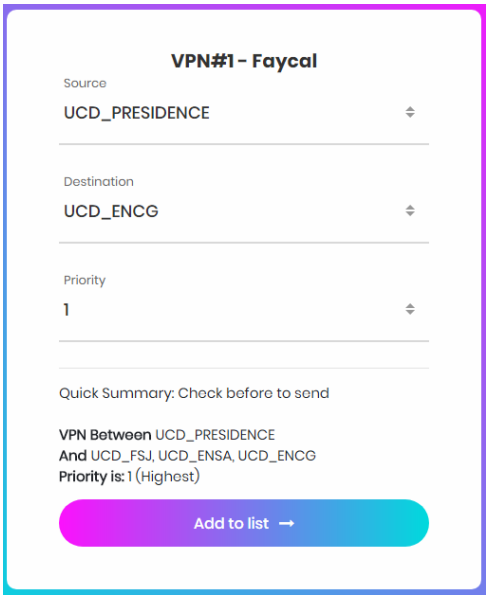


Fig. 2. The GUI Interface of the Application Layer.

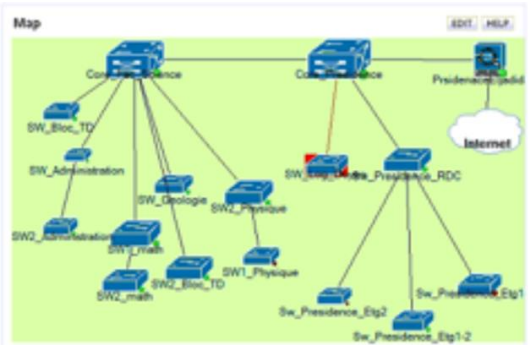


Fig. 3. The Network Architecture Detected Automatically.

Algorithm 1: Path Computation

```
Load Ba : Available bandwidth;
Load Breq : Requested bandwidth;
Load ρ^h : Most optimal path;
Load Vc : Number of tunnels on a path ;
if (Ba < Breq & Vc > 2 & Vp > Vreq) then
    ρ = ρ(h − 1) ;
end
for each ρ = ρ(h − n) ; n<2 do
    if (Ba < Breq & Vc > 2 & Vp < Vreq) then
        ρ = ρ(h − n) ;
    end
end
```

Fig. 4. The Operating Algorithm of the Path Computation Module.

B. Path Computation

As soon as the topology is discovered, this module makes it possible to calculate the most optimal path on which to deploy / route the MPLS VPN tunnel. The processing performed by this module is described in the previous section. However, the algorithm 1 illustrated in Fig. 4 describes the main operating phases of this module.

C. VPN Monitor

This module is used to check the MPLS VPN already deployed on a router. The controller can verify the VPN instances already open on a device by querying the SNMP MIB object: 1.3.6.1.4.1.9.9.711 or launch the "Show ip vrf" or "display ip vpn instance" commands for routers such as Cisco, Juniper, and HP. Recall that the priority of a tunnel can be detected at the base of the initial declaration by the administrator during the first phase (please refer to Fig. 2).

D. Admission Control

This module allows authorizing or not:

1) The establishment of a tunnel.
2) Routing a higher priority VPN.
3) Destruction of a lower priority VPN if all paths are overloaded.
4) The data plan contains all routers of the network architecture consisting of P, PE and CE equipment.

In the next section we will evaluate the performance of our approach.

IV. Performance Evaluation

A. Network Testbed

In order to evaluate the performances of our approach, we set up a network testbed consists of several routers and tens of clients (Fig. 5). Used applications for the evaluation are Voice over IP [12][13][14], Video streaming, and Database traffic. Evaluation criteria are:

1) VoIP latency: Delay it takes for one endpoint to send a packet to another.
2) VoIP jitter: Delay between submission of two packets.
3) VoIP MOS: Quality imperceptible of the call.
4) VoIP loss rate: Quantity of VoIP non-received traffic.
5) Video loss rate: Amount of non-received video traffic.
6) Delay of database query.

B. Obtained Results

Fig. 6 illustrates the overall results obtained. Fig. 6(a) illustrates the VoIP loss rate obtained by our FNA approach compared to the RSVP-TE protocol. The results obtained showed the effectiveness of our approach compared to FNA-TE, we find that both models offered an acceptable rate up to the scenario of 80 clients, however, from the scenario of 90 clients we found that RSVP-TE exceeded the tolerable threshold of 3%, our model has shown its effectiveness even in the scenario of 200 customers. The VoIP latency results (Fig. 6(b)) thus showed the efficiency of our approach, a latency not exceeding 50 milliseconds was measured by FNA-TE against 150 RSVP-TE. Fig. 6(c) illustrates the VoIP jitter, the results obtained showed that the delay variation of our approach is the smallest not exceeding a value of 19 milliseconds against 50 of RSVP-TE. The same results are observed for Video Traffic Fig. 6(f) and Fig. 6(g).

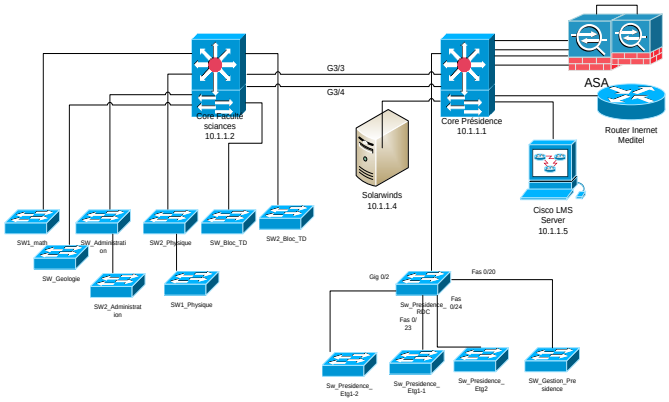
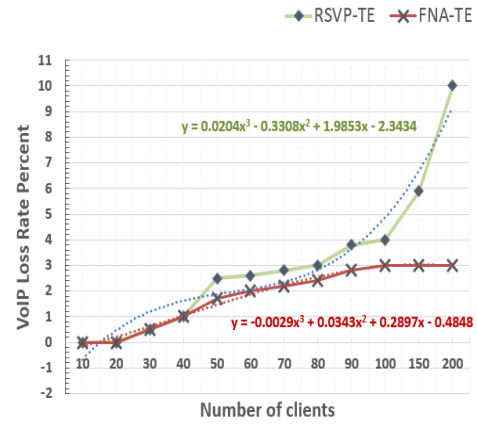
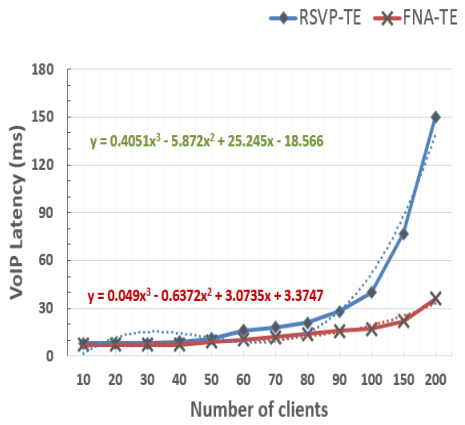


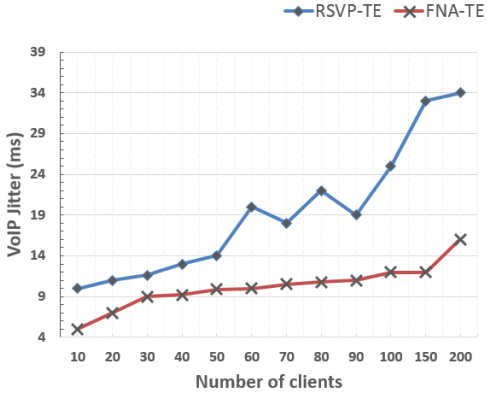
Fig. 5. The Operating Algorithm of the Path Computation Module.



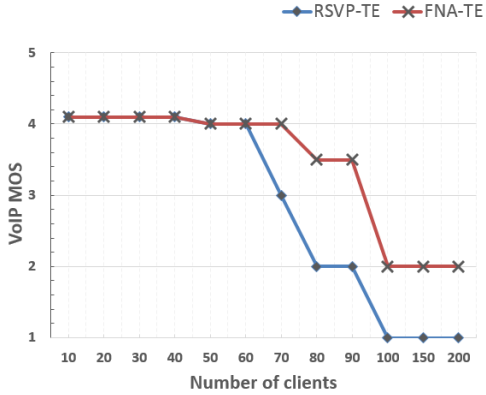
(a) VoIP Loss Rate.



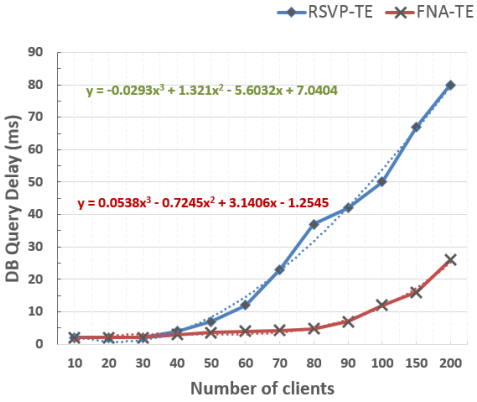
(b) VoIP latency.



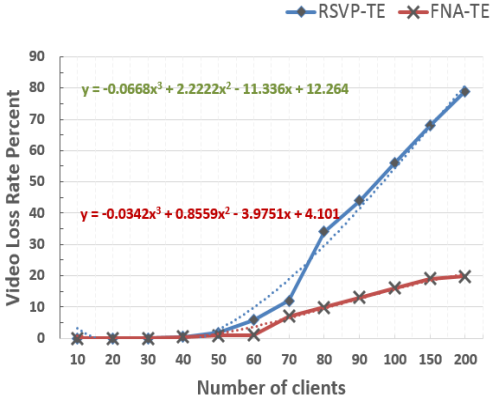
(c) VoIP Jitter.



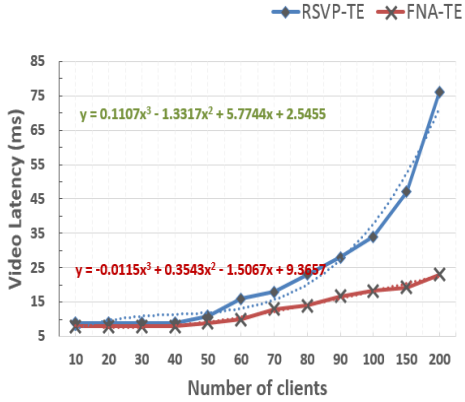
(d) VoIP MOS.



(e) Oracle Query Delay.



(f) Video Loss Rate.



(g) Video Latency.

Fig. 6. Obtained Results from Performances Evaluation: (a) VoIP Loss Rate (b) VoIP Latency (c) VoIP Jitter (d) VoIP MOS (e)Oracle Query Delay (f) Video Loss Rate (g) Video Latency.

V. Conclusion

In this paper we dealt with a problem of traffic engineering in MPLS-VPN tunnels. Our FNA-TE contribution is to guarantee MPLS-VPN tunnels the least short path guaranteeing the bandwidth necessary for a good level of the quality of service of the transported traffic. Our contribution allows through fair treatment not to compromise the lowest priority tunnels. Our approach was tested in a network consistent with that of Chouaïb Doukkali University, in which we evaluated the performance of real-time, streaming and transactional traffic by increasing the load and the number of users. The results obtained showed the effectiveness of our approach compared to the protocol commonly used RSVP-TE.

Acknowledgment

The authors would like to thank editor and referee for providing valuable comments to improve our manuscript.

References

[1] Bensalah, F., El Hamzaoui, M., & Bahnasse, A. (2018). Behavior study of SIP on IP multimedia subsystem architecture MPLS as transport layer. International Journal of Information Technology, 10(2), 113-121.

[2] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec). International Journal of Computer Science and Network Security (IJCSNS), 17(3), 87.

[3] Khiat, A., Bahnasse, A., Bakkoury, J., & El Khaili, M. (2017). Study, evaluation and measurement of IEEE 802.16 e secured by dynamic and multipoint VPN IPsec. International Journal of Computer Science and Information Security, 15(1), 276.

[4] Bahnasse, A., Louhab, F. E., Talea, M., Oulahyane, H. A., Harbi, A., & Khiat, A. (2017, November). Towards a new approach for adaptive security management in new generation virtual private networks. In 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE.

[5] Bahnasse, A., & El Kamoun, N. (2016). A policy based management of a smart adaptive QoS for the dynamic and multipoint virtual private network. International Journal of Control and Automation, 9(5), 185-198.

[6] Bahnasse, A., Badri, A., Talea, M., Louhab, F. E., & Khiat, A. (2018). Towards a New approach for automating the simulation of QoS mechanisms in a smart digital environment. Procedia computer science, 134, 227-234.

[7] Khiat, A., Bahnasse, A., El Khaili, M., & Bakkoury, J. (2017). SAQ-2HN: A Novel SDN-Based Architecture for the Management of Quality of Service in Homogeneous and Heterogeneous Wireless Networks. International Journal of Computer Science and Network Security (IJCSNS), 17(3), 55.

[8] Alouneh, S., Al-Hawari, F., Hababeh, I., & Ghinea, G. (2018). An Effective Classification Approach for Big Data Security Based on GMPLS/MPLS Networks. Security and Communication Networks, 2018.

[9] Bahnasse, A., Louhab, F. E., Oulahyane, H. A., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS Traffic Engineering-DiffServ Aware management. Future Generation Computer Systems, 87, 115-126.

[10] Bahnasse, A., Louhab, F. E., Oulahyane, H. A., Talea, M., & Bakali, A. (2018). Smart bandwidth allocation for next generation networks adopting software-defined network approach. Data in brief, 20, 840-845.

[11] Alharbi, A., Bahnasse, A., Talea, M., Oulahyane, H. A., & Louhab, F. E. (2017, October). Smart SDN Policy Management Based VPN Multipoint. In First International Conference on Real Time Intelligent Systems (pp. 250-263). Springer, Cham.

[12] BAHNASSE, A., BADRI, A., LOUHAB, F. E., TALEA, M., KHIAT, A., & PANDEY, B. (2018). Behavior analysis of VoIP performances in next-generation networks. International Journal of Engineering & Technology, 7(3.15), 353-359.

[13] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP. IJCNS International Journal of Computer Science and Network Security, 17(4), 361-369.

[14] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Scalability evaluation of VOIP over various MPLS tunneling under OPNET modeler. Indian Journal of Science and Technology, 10(29), 1-8.