Analysis of MPLS and SD-WAN Network Performances Using GNS3

Ivan Grgurevic[1(✉)], Gabriela Barišić[1], and Adam Stančić[2]

[1] Faculty of Transport and Traffic Sciences, Department of Information and Communications Traffic, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia
ivan.grgurevic@fpz.unizg.hr

[2] Karlovac University of Applied Sciences, Ivana Meštrovića 10, 47000 Karlovac, Croatia
adam.stancic@vuka.hr

Abstract. MPLS and SD-WAN are technologies which ensure the quality of service in a different way. MPLS is a network technology which, with its method of routing the network packets, ensures the end-to-end service to users. On the other hand, SD-WAN ensures the global overview of the entire network and central managing thus enabling easy configuration or exchange of the already existing configuration system. The topic of this paper is analysis of these two network technologies by having them configured and simulated in the software tool GNS3. After that the analysis of the traffic network has been carried out. Regarding the ever-increasing development of the network technologies, an overview of the SD-WAN technology has been provided, as the new paradigm and its potential future applications.

Keywords: MPLS · SD-WAN · GNS3 · Software-defined networks · Network performances · Network simulation · Network traffic analysis

1 Introduction

Multi-Protocol Label Switching (MPLS) is a network technology which provides a new method of routing IP packages and it also satisfies the level of service quality at the same time. Since scalability and reliability have become an increasing concern for businesses, especially those with data centres, MPLS has provided the users with setting priorities within the service.

SD-WAN (Software Defined WAN) is a new paradigm which uses the characteristics of software-defined networks in the data centres, but with the application to a wide area network of the company and its affiliates. SD-WAN and SDN virtualize the resources in order to provide better performance, greater availability and automatic network management. At the same time, the costs are significantly reduced, especially compared to the MPLS technology.

By configuration and simulating MPLS and SD-WAN technologies and subsequent comparative analyses of various network parameters such as quality of service,

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 77–90, 2021.
https://doi.org/10.1007/978-3-030-78459-1_6

bandwidth and delay, an analysis of their performances and their application has been made.

The motivation for choosing MPLS and SD-WAN technologies for comparison is their rapid development and expected potential future applications of SD-WAN.

The purpose of the paper is to determine the applicability and manageability of the software-defined WAN as a concept of software-defined networks.

The aim of the paper is to conduct an analysis of MPLS and SD-WAN network performances according to various recognised factors (management, latency, quality of service, etc.). The paper has been divided into eight sections. After the introduction, a brief overview has been given about the existing relevant research of the topic of this paper. Section 3 defines the MPLS technology and the mechanisms of routing MPLS technology that ensure reliable traffic transmission. Section 4, Characteristics of SD-WAN, describes the software-defined networks as the basis of SD-WAN and its characteristics have been defined. Section 5, Case study: Configuration and simulation of MPLS and SD-WAN networks in the GNS3 software tool, a network simulation was made using the GNS3. Section 6, MPLS network performance analysis, an analysis of the MPLS technology network traffic was made using a Wireshark network analyser, which collected data over endpoints in a previously simulated network. In Sect. 7, Analysis of SD-WAN network performances, the functionalities of the Mininet environment were used to define and analyse the network parameters. The last Section, Conclusion, shows the main elements of the work and a conclusion is made based on the conducted research.

2 Related Research

In paper [1], the performance of MPLS and traditional IP routing was measured in order to make a comparative analysis based on delays, missed packets and bandwidth in the OPNET network simulator.

According to research [2], the effectiveness of MPLS was compared with the use of the OpenFlow protocol. The study compared the scalability and interoperability with the emphasis on performance comparison. The test environment was created using routers and Hyper-V technology together with the Mininet environment for the SDN experiments.

According to studies [3] and [4], an overview has been given of the application of the software-defined networks in the WAN technology as well as an overview of the current research on this topic. The advantages of SD-WAN technology implementation as well as the challenges and the future of SD-WAN have been defined. Also, a layered architecture of the software-defined WAN has been defined.

In paper [5], a test environment was created by using *open-source* technology such as OpenvSwitch and OpenDaylight to set up a network monitoring and path selection based on the defined policies. The results have shown new features and benefits for the companies, particularly in resource optimisation.

In paper [6], the authors suggest the so-called *HOMA* approach to SD-WAN topology and routing management, based on the linear programming, and the results show cost reduction and overall efficiency.

In a report by the Frost & Sullivan Company [7], the telecommunication operator AT&T presents their vision of implementing SD-WAN network technology. The emphasis of this work lies on hybrid solutions, i.e. maintaining of the existing Ethernet and MPLS technologies with additional application of SD-WAN solution.

Furthermore, a hybrid solution of SD-WAN and MPLS has been proposed with a combination of OpenFlow routers on the edges of the network whereas the core network consists of MPLS routers. The results of the research showed that the hybrid architecture in network engineering has better efficiency compared to traditionally implemented MPLS networks [8].

3 MPLS Features

Multi-Protocol Label Switching (MPLS) is an IETF standard based on Cisco tag switching and allows interoperability with other network equipment manufacturers [9].

MPLS allows packet forwarding through the network so that the information in the packet header is analysed only once, and further forwarding is based on label checking, [10, 11]. Labels represent packet identification tags, and they are of fixed length. An MPLS tag is a 32-bit field with a specific structure [12]. An MPLS domain consists of one or several MPLS Label Switch Routers (LSRs) that scan and replace MPLS packet labels in order to forward them through the network [13].

The LSR that is on the edge of an MPLS domain and forwards the traffic inside and outside the MPLS domain is called a Label Edge Router (LER). The Label Switched Path (LSP) is a series of LSRs that switch the labelled packets through an MPLS network or a part of a MPLS network. That is, the LSP is the path through the MPLS network. The first LSR for a LSP is the input LSR and the last LSR for this LSP is the output LSR. LSP is a one-way communication. LSP is established for the first time by using the Label Distribution Protocol (LDP) [14].

The Forwarding Equivalence Class (FEC) is a group or flow of the packets that are forwarded the same way and treated equally in terms of forwarding. All the packets that belong to the same FEC have the same label. However, not all packets that have the same label do necessarily belong to the same FEC, since their forwarding treatment may differ [15].

For the packets to be transmitted via LSP through the MPLS network, the LDP is run on the LSR. When LSRs have labels for each FEC, the packets can be forwarded to the LSP. Label operations (addition, replacement and removal) are known to each LSR according to the LFIB table. The Label Forwarding Information Base (LFIB) is a table for forwarding labelled packets, and it consists of input and output labels for LSP [16–18].

4 SD-WAN Features

SD-WAN is a specific application of the software-defined networks technology on the WAN connections such as the broadband Internet or Long Term Evolution (LTE). It connects the corporate networks, including branches and datacentres, over long geographical distances [19].

SDN is a new network paradigm that is an example of software networks whose basic idea is to separate the control plane from the data plane. The control plane is all the logic which decides what needs to be done and gives instructions to the data plane on how to implement the decision. The control plane contains the control and routing behaviour such as topological change tracking, forwarding rule installation, route calculation, etc. The data plane forwards the traffic based on the rule specified by the control plane. The centralized control part is called the controller and it manages all the data planes and is software-installed in the hardware [20].

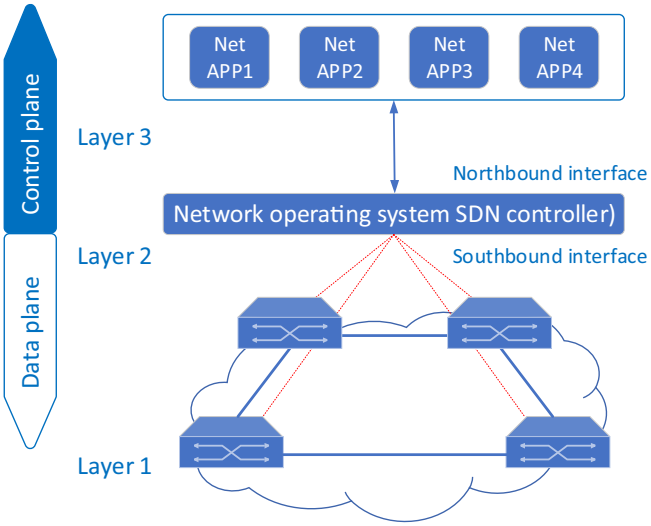

Fig. 1. Layered architecture of SDN network

Figure 1 shows the SDN network architecture. The first layer is the infrastructure layer that is called data plane, and it consists of network forwarding elements. The responsibilities of this layer are data forwarding, local information following and statistics collection. The layer above is the control plane. It is responsible for programming and management of the forwarding layer. OpenFlow, which is one of the most frequently used southbound interface consists mostly of switches, where some other SDN solutions use also routers [21].

The last layer is the application plane which contains network applications. They can introduce new network features such as security and management, forwarding schemes or help in the control part of the network configuration. The interface between the application plane and the control plane is called the northbound interface [21].

4.1 Definition of SD-WAN

SD-WAN is a part of a wider SDN technology which was described in the previous section. Both are software-defined technologies, but SD-WAN uses similar software-defined concepts of separating the control and the data plane on WAN network. Gartner defines SD-WAN with four characteristics:

1. Supports various types of connections like MPLS, Internet, LTE, etc.;
2. Has the ability to dynamically select the route, i.e. load sharing on WAN connections;
3. Provides a simple network management interface;
4. VPNs as well as other third-party service should be supported, [22].

Another important feature of SD-WAN technology is Zero touch provisioning (ZTP). This is a characteristic of the switch that allows automatic configuration. That is, when the switch is turned on, it sends a DHCP request in order to get the location of the centrally stored image and configuration, which it then downloads and runs [23].

4.2 SD-WAN and Network Virtualization

Network Functions Virtualization (NFV) is a technology that enables the separation of network functions from their assigned hardware devices and the implementation of these functions as software components into fully virtualized network infrastructures. NFV avoids manufacturer exclusivity and provides resource flexibility of upper layers (L4–L7) [24].

NFVs are Virtual Network Functions (VNFs) that manage the specific network functions. Individual VNFs can be connected or merged as building blocks to create a fully virtualized environment. VNFs run on Virtual Machines (VM) on the network infrastructure hardware [25].

The controller maintains the global network overview and programs the edges that can be custom or generic (VNF) hardware deployed to remote locations. The edges learn the routes, which enables central decision-making with remote execution by the edge. This architecture ensures the availability if the controller or the gateway is unavailable, and the edge device can make a local decision based on the latest instructions [26].

5 Case Study: Configuration and Simulation of MPLS and SD-WAN Networks in the GNS3

Graphical Network Simulator-3 (GNS3) is a network software emulator that allows the combination of virtual and real devices in order to simulate a complex network. GNS3 is used by many organizations and telecommunication networks specialists for their studies and the greatest advantage of GNS3 is the ability to collaborate with real networks. The configuration requires the Cisco Operating System (IOS) images on network devices, and in order to accomplish this, GNS3 uses Dynamips emulation software [27]. Version 2.2.9 of the GNS3 was used in the simulation, and the Cisco C3725 router with the image *c3725-adventerprisek9-mz.124–15.T14* was used for the MPLS network topology. Further in the text the following is described: the configuration and simulation of the MPLS core network (5.1), the configuration of user locations and VRF (5.2), and the configuration and simulation of the SD-WAN network (5.3).

5.1 MPLS Core Network Configuration and Simulation

The first part of the MPLS network simulation is the core network configuration consisting of three Cisco C3725 routers. The routers are assigned loopback addresses and

interface IP addresses. An OSPF routing protocol is started on each router and LDP is enabled. Between the edge routers, a Multi Protocol BGP session is started with the vpnv4 configuration. Figure 2 shows the topology of the core network.

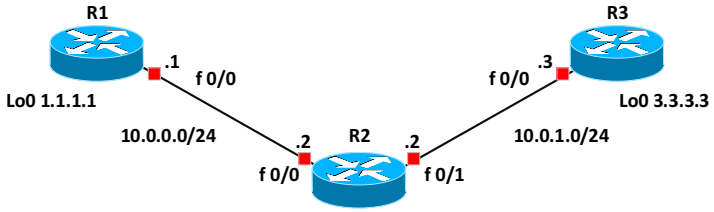

Fig. 2. MPLS core network topology

First, the IP address is configured for a loopback interface that is always running (state *up*); so the OSPF protocol will recognize it as a Router ID, and OSPF is started with the last line of the code and it is assigned process 1, and the area is 0 for the MPLS core network.

MPLS LDP is enabled under the OSPF process, and MP-BGP is configured on all Provider Edges (PEs).

5.2 Configuration of User Locations and VRF

It is necessary to configure two user locations that will also run the OSPF protocol, and Virtual Routing and Forwarding (VRF) will be configured on the PE routers. Figure 3 shows the selected MPLS network topology.

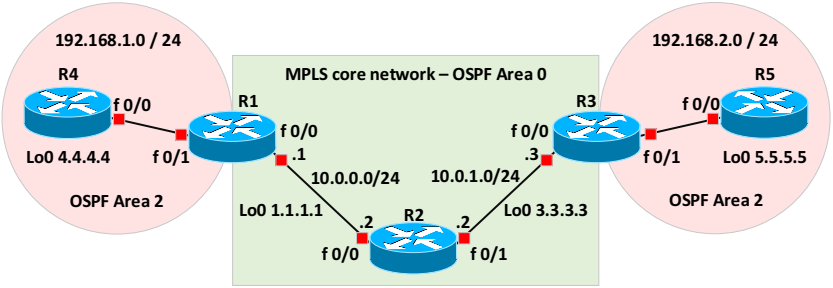

Fig. 3. MPLS network topology

The f0/1 interface with IP address 192.168.1.1/24 is configured on R1. After this step, the VRF needs to be configured. VRF is a technology included in the IP routers that allows multiple instances of routing tables within a router and their simultaneous operation. The VRF provides automatic traffic segregation which is applicable in creating separate virtual private networks (VPN) for the users. Hence, PE routers are able to store routes and to forward packets even if the users use identical addressing [28].

The final step for complete connectivity over the MPLS core is the redistribution of OSPF routes to R1 and R3 in MP-BGP and MP-BGP in OSPF. After configuration of the routers the MPLS core network is built which runs the OSPF with loopback addresses. R1 and R3 have peering with MP-BGP. LDP is enabled on all internal interfaces, and the external interfaces of the MPLS core network are set in VRF under the name RED which is also joined by local routers. The final step for complete connectivity via MPLS core is the redistribution of OSPF routes to R1 and R3 in MP-BGP and MP-BGP in OSPF.

5.3 Configuration and Simulation of SD-WAN Network

To begin with, the configuration of the physical part of the SD-WAN network was made, and it consists of four Cisco c3725 routers between which there is the OpenvSwitch, as presented in Fig. 4. As seen in Fig. 4, according to the network topology, two routers each form separate networks that are interconnected by OpenvSwitch.

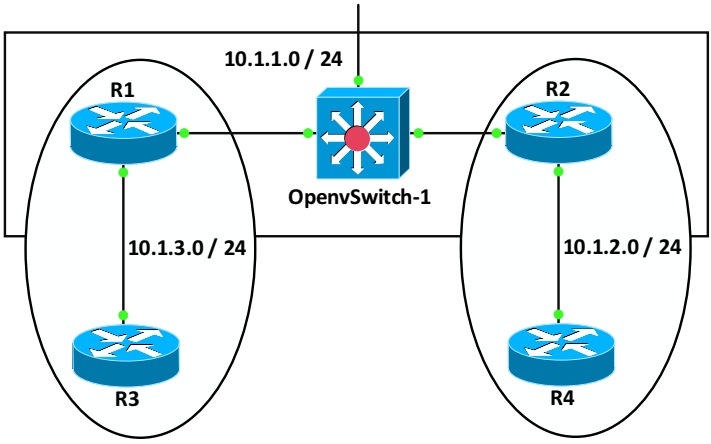

Fig. 4. Topology of physical routers connected by OpenvSwitch in SD-WAN network

The routers are interconnected by RIP routing protocol and end-to-end communication is achieved, and no additional configuration on OpenvSwitch was required, which shows the simplicity of the SD-WAN network configuration itself.

The next step in configuring the software-defined networks is to add a Mininet controller to the network topology, as shown in Fig. 5. After having configured the OpenvSwitch, the communication of the Mininet controller with the physical part of the network is established. With this, the centralised management of the entire simulation has been achieved, which will be also evident from the network traffic analysis.

The next part of the paper describes the simulation of SD-WAN network. A GNS3 simulator has been used as the basic simulation program, in which the physical Cisco c3725 router, OpenvSwitch and Mininet controller were run.

OpenvSwitch is a virtual switch designed for the network automation through program extensions, while still providing standard interfaces and protocols. It's a multilayer software switch and it's suited for virtual environment to function as virtual switch, [29]. Furthermore, the Mininet virtual environment enables the management of software-defined networks and supports the OpenFlow protocol [30].

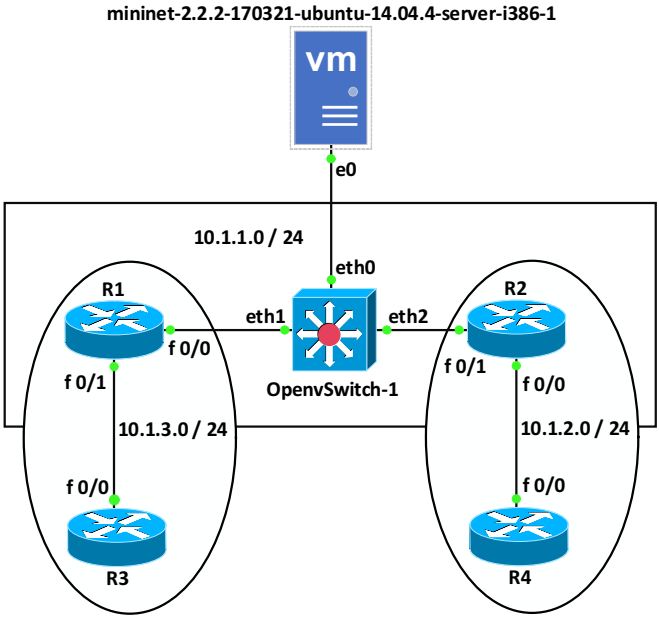

Fig. 5. Simulation of SD-WAN technology by adding Mininet as network controller

Mininet is a free network emulator hosting standard Linux network software with flexible custom routing and support of Software Defined Networking, [30]. The following sections will present an analysis of the traffic and the SD-WAN network parameters and their comparison with the MPLS.

6 Analysis of MPLS Network Performances

In order to analyse the end-to-end MPLS network performances in the software tool GNS3, a large quantity (<10,000) of ping packets between the end devices has been generated.

Figure 6 shows the MPLS network performance statistics when analysing the collected packets at the destination device. From graph in Fig. 7, one can see the average, maximal and minimal response times to ICMP packets.

As can be seen from Graph 7, the average response time of a ping packet is stable all the time and the maximal value is 0.66 ms.

Statistics

Measurement	Captured	Displayed
Packets	13098	11474 (87.6%)
Time span, s	5762.292	5743.598
Average pps	2.3	2.0
Average packet size, B	97	98
Bytes	1268754	1124452 (88.6%)
Average bytes/s	220	195
Average bits/s	1761	1566

Fig. 6. Statistics of MPLS network performances

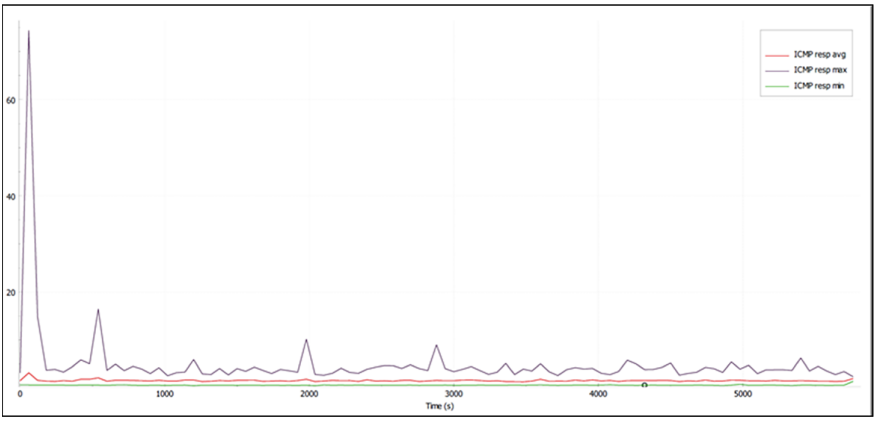

Fig. 7. Graph of response times to ICMP packets

Furthermore, the next packet collection was done between core and edge MPLS router, and according to Fig. 8, by using the network analyser *Wireshark,* the exchange of messages between these two routers is visible [17].

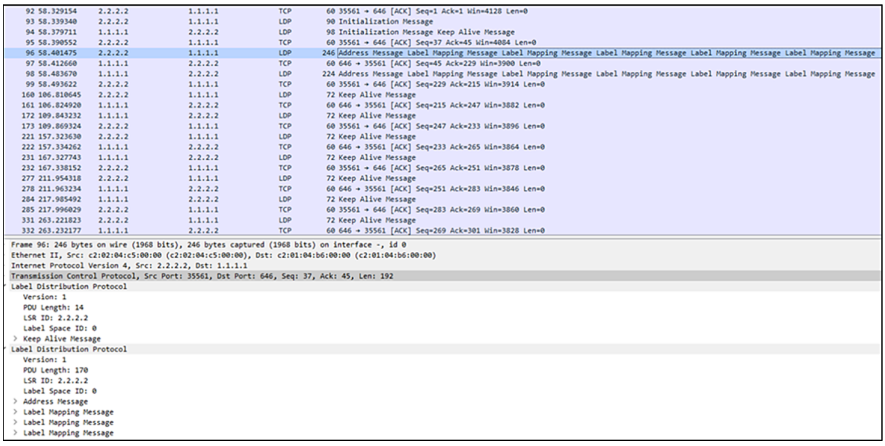

Fig. 8. Packets of LDP MPLS protocol between two routers

Figure 8 shows the communication of the LDP protocol which is responsible for the distribution of labels in the network. After the hello messages have been successfully sent in the network, and TCP connection between the core and the edge router has been established, the exchange of messages between these two routers began. Through LDP messages it is visible that the ID of the router is the loopback address that we had configured on the router. The LDP messages exchange information on the routes, labels and address families. The second filtering is the filtering of the BGP protocol which shows the label replacement mechanism, as shown in Fig. 9.

Through the LDP messages the router ID is the loopback address that we had configured on the router. The LDP messages exchange information on the routes, labels and address families. The second filtering is the BGP protocol filtering which shows the mechanism of label replacement, shown in Fig. 9.

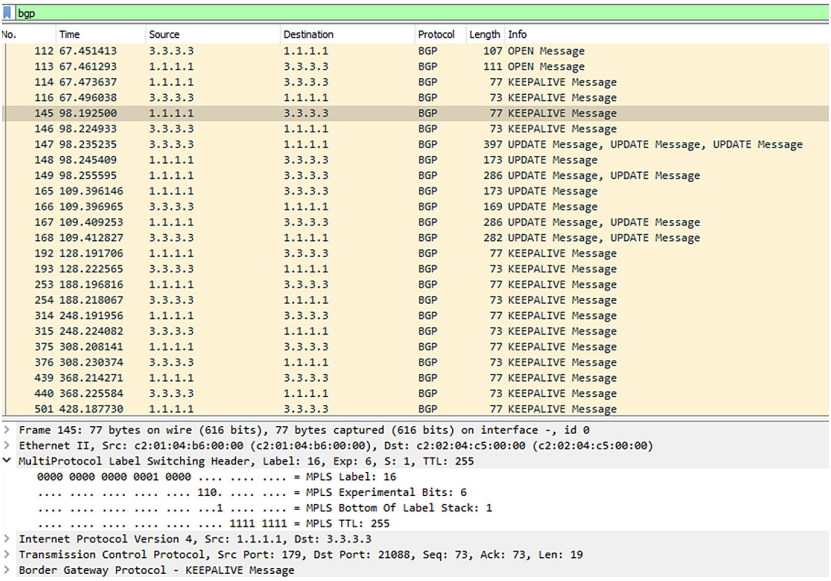

Fig. 9. MPLS label replacement presented in *Wireshark*

It can be seen from Fig. 9 that MPLS label 16 was used, and that the experimental bit used to determine the class of service is set to the binary value 110 which marks the high importance of the packet (network control). Also, label 16 is the last label in the stack, which is seen from the value of MPLS Bottom of Label Stack with the value 0 except if the label is the last one in the stack [31, 32].

7 Analysis of SD-WAN Network Performances

In this part of analysing the network performances, an analysis of the SD-WAN network technology has been made. The SD-WAN network technology and its performances can

be analysed directly on the network controller, and the analysis has been made on the previously used Mininet controller.

For the analysis of network performances, the performances are used with which the quality of service in the networks is measured, and these are: availability, throughput capacity, delay and loss of packet.

Mininet enables checking the availability among all the hosts by simple command *pingall* by which for every host ping packets are sent to all hosts in the network. Figure 10 shows that there are no losses in the network and that the reachability is 100%.

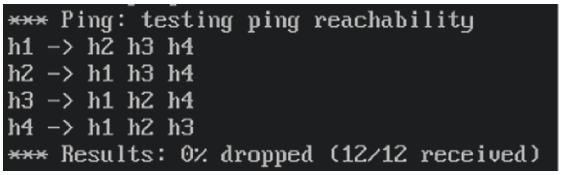

Fig. 10. Checking reachability of all hosts in the network

With this check it is in fact clear how much the checking of mutual reachability of hosts is simplified. In traditional network, such checking would require connecting with each host individually and generating ping packets towards every host in the network.

Furthermore, Fig. 11 shows how it is possible with the command *iperf* to analyse the TCP network bandwidth and network capacity on the link between *h1* and *h2*. Such an analysis in traditional networks would require an analysis of the traffic generated in a tool like *Wireshark* in order to calculate the average link bandwidth.

Fig. 11. Analysis of network bandwidth and throughput capacity on the link

Figure 12 shows the delays that are caused by delay of 10 ms on three links between two hosts resulting in the average Round Trip Times (RTTs) of 60 ms.

The loss of packet is one of the most important parameters of the quality of service in real-time applications where it is important that the loss of packets is as low as possible.

Figure 13 shows that by defining the loss of packet of 15% on every link, out of twenty ping packets between hosts *h1* and *h2* the loss is as much as 70% of packets.

Considering conducted analysis of MPLS and SD-WAN network traffic, it's visible that without real network traffic, there isn't many QoS parameters to be gathered from MPLS network traffic in GNS3 simulation. Using Wireshark, analysis of MPLS network traffic showed no packet loss and low response time to ping requests. As opposed to MPLS, utilizing Mininet in SD-WAN simulation, it's possible to manipulate and analyse network parameters from centralized point which simplifies real-life troubleshooting.

```
mininet> h1 ping -c10 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=134 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=64.5 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=63.7 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=64.3 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=62.2 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=62.8 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=64.1 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=64.4 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=62.9 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=64.4 ms

--- 10.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 62.252/70.843/134.618/21.273 ms
```

Fig. 12. Checking of RTT between two hosts

```
mininet> h1 ping -c20 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=1 Destination Host Unreachable
From 10.0.0.1 icmp_seq=2 Destination Host Unreachable
From 10.0.0.1 icmp_seq=3 Destination Host Unreachable
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=63.4 ms
64 bytes from 10.0.0.1: icmp_seq=9 ttl=64 time=64.4 ms
64 bytes from 10.0.0.1: icmp_seq=10 ttl=64 time=65.2 ms
64 bytes from 10.0.0.1: icmp_seq=16 ttl=64 time=64.0 ms
64 bytes from 10.0.0.1: icmp_seq=17 ttl=64 time=63.0 ms
64 bytes from 10.0.0.1: icmp_seq=20 ttl=64 time=66.1 ms

--- 10.0.0.2 ping statistics ---
20 packets transmitted, 6 received, +3 errors, 70% packet loss, time 19058ms
rtt min/avg/max/mdev = 63.002/64.402/66.111/1.073 ms, pipe 4
```

Fig. 13. Test of packet losses through ping packets

8 Conclusion

The MPLS network technology was created as Cisco response to provide the users with an end-to-end service ensuring the quality of service. However, with the development of advanced technologies such as cloud computing, the applications no longer need to run on local servers, but can be accessed anywhere and anytime. The MPLS does not have a technical solution for the ever-increasing presence of cloud services.

On the other hand, a software-defined network is a newly created technological solution that offers simplified management of complex network systems by separating the control and the data parts. This enables a global overview of the entire system and centralized management of all network elements. SD-WAN is an extension of SDN technology where the application of SDN solutions to WAN is defined, and where the service providers and their transformation from traditional technologies into software networks play a major role.

The conducted configuration and simulation of network technologies in the software tool GNS3 has shown the complexity and depth of the necessary knowledge required to configure the MPLS networks. It can be therefore concluded that in the large systems the process of implementing the MPLS technology can take time. Furthermore, in order to analyse the network traffic in the MPLS network, it was necessary to generate a certain traffic and to analyse it using the *Wireshark* network analyser.

Unlike the MPLS, the configuration and simulation of SD-WAN technology is simpler and the configuration itself of all the network elements is possible centrally by using the Mininet controller from which later a complete traffic analysis was made. By comparing the ease of performing the traffic analysis, the software-defined technologies provide a much simpler solution where different parameters of the quality of service (e.g. delay, bandwidth, packet loss, etc.) can be defined and checked with a single command. In contrast, the analysis of the traffic and performances of the MPLS network required the collection of data and their detailed analysis in order to verify the success of the simulation.

The SD-WAN network technology allows adjustment of network parameters in real time, which can be extremely useful during large video conferences, etc., where the performances on the links are adapted to the current traffic flows without too much expense for the user. Such approach to network engineering and flexible adaptation to user requirements can transform the way the network service is understood as opposed to the traditional approach.

It is evident from the conducted research that both technologies have their benefits and drawbacks. Since many users already have implemented technologies such as MPLS, the future research should be based on achieving the interoperability of the traditional routing technologies with an SD-WAN solution. Furthermore, by using the analyses and the application of the artificial intelligence in the field of network engineering, the models of optimisation and prediction of network traffic will be made, and this will lead to an overall improvement of the level of the quality of service.

References

1. Nousyba, E., Elrasoul, H., Algasim, A., Babiker, A., Mustafa, A.N.: MPLS Vs IP Routing and its Impact on QoS Parameters. Int. J. Eng. Tech. Res. **11**, 179–180 (2014)
2. Terefenko, D.: A Comparison of Multiprotocol Label Switching (MPLS) and OpenFlow Communication Protocols. Institute of Technology Tallaghtno, Dublin, Ireland (2018)
3. Mine, G., Hai, J., Jin, L., Huiying, Z.: A design of SD-WAN-oriented wide area network access. In: International Conference on Computer Communication Networking Security, pp. 174–177 (2020). https://doi.org/10.1109/ccns50731.2020.00046
4. Yang, Z., Cui, Y., Li, B., Liu, Y., Xu, Y.: Software-defined wide area network (SD-WAN): architecture, advances and opportunities. In: Proceedings of International Conference Computer Communiacation Networks, ICCCN, vol. 2019-July (2019). https://doi.org/10.1109/ICCCN.2019.8847124
5. Troia, S., Zorello, L.M.M., Maralit, A.J., Maier, G.: SD-WAN: an open-source implementation for enterprise networking services. In: International Conference on Transparent Optics Networks, vol. 2020-July, pp. 1–4 (2020). https://doi.org/10.1109/ICTON51198.2020.9203058
6. Zad Tootaghaj, D., Ahmed, F., Sharma, P., Yannakakis, M.: Homa: an efficient topology and route management approach in SD-WAN overlays. In: Proceedings IEEE INFOCOM, vol. 2020-July, pp. 2351–2360 (2020). https://doi.org/10.1109/INFOCOM41043.2020.9155503
7. Hoonachari, R.: The Critical Role of Hybrid Networks in SD-WAN Deployments. Frost & Sullivan, USA (2018)
8. Tajiki, M. M., Akbari, B., Mokari, N., Chiaraviglio, L.: SDN-based resource allocation in MPLS networks: A hybrid approach. In: Concurrency and Computation Practice and Experience, pp. 1–11 (2018)

9. Cisco Community. https://community.cisco.com/t5/networking-documents/how-to-Configure-tag-switching-and-mpls/ta-p/3128570, Accessed 16 Aug 2020
10. Ferdous, J.: The Basic Concept of Multiprotocol Label Switching (MPLS). Daffodil International University Dhaka, Bangladesh (2019)
11. Ridwan, M.A., Radzi, N.A.M., Wan Ahmad, W.S.H.M., Abdullah, F., Jamaludin, M.Z., Zakaria, M.N.: Recent trends in MPLS networks: technologies, applications and challenges. IET Commun. **14**(2), 177-185 (2020). https://doi.org/10.1049/iet-com.2018.6129
12. Cisco certified expert. https://www.ccexpert.us/mpls-network/mpls-and-the-osi-reference-model.html, Accessed 16 Aug 2020
13. Nadeau, T.D.: MPLS Network Management, Label-Switching Router. https://www.sciencedirect.com/topics/computer-science/label-switching-router, Accessed 16 Aug 2020
14. Nadeau, T.D.: MPLS Network Management, Label Switched Path. https://www.sciencedirect.com/topics/computer-science/label-switched-path, Accessed 17 Aug 2020
15. De Ghein, L.: MPLS Fundamentals. Cisco, Indianapolis, USA (2007)
16. Semantic Scholar – LIB. https://www.semanticscholar.org/topic/Label-Information-Base/2763152, Accessed 24 Aug 2020
17. Yasin, W., Ibrahim, H.: Improving triple play services using multi protocol label switching technology label switching technology. J. Comput. Sci. (2010)
18. MPLS Fundamentals: Forwarding Labeled Packets. http://www.ciscopress.com/articles/article.asp?p=680824&seqNum=2, Accessed 25 Aug 2020
19. SDxCentral. https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/, Accessed 27 Aug 2020
20. Ranjan, P., Pande, P., Oswal, R., Qurani, Z.: A survey of past, present and future of software defined networking. Inst. Electric. Electron. Eng. **7782**, 238–248 (2014)
21. Braun, W., Menth, M.: Software-defined networking using openflow: protocols, applications and architectural design choices. Futur. Internet **6**(2), 302–336 (2014)
22. Network World. https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html, Accessed 13 Sept 2020
23. Juniper, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/zero-touch-provision.html, Accessed 16 Sept 2020
24. Prashanth, M., Manthena, V., Lucent, A.: Network-as-a-service architecture with SDN and NFV: a proposed evolutionary approach for service provider networks network-as-a-service architecture with SDN and NFV, Netherlands (2016)
25. SDxCentral. https://www.sdxcentral.com/networking/nfv/definitions/virtual-network-function, Accessed 16 Sept 2020
26. VeloCloud, Guide to SDN, SD-WAN, NFV, and VNF, VeloCloud (2016)
27. GNS3. https://docs.gns3.com/docs/, Accessed 17 Sept 2020
28. Plixer VRF. https://www.plixer.com/blog/what-is-vrf-virtual-routing-and-forwarding, Accessed 20 Sept 2020
29. Openvswitch. http://www.openvswitch.org, Accessed 17 Sept 2020
30. Mininet. http://www.mininet.org, 17 Sept 2020
31. Cisco MPLS QOS classification overview. https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/classification_oview.html, Accessed 17 Sept 2020
32. IETF MPLS label stack encoding. https://tools.ietf.org/html/rfc3032, Accessed 18 Sept 2020