

# Performance comparison between virtual MPLS IP network and real IP network without MPLS

Case Study

**Ivan Nedyalkov**

South – West University “Neofit Rilski”

Faculty of Engineering, Department of Communication and Computer Engineering,

Ivan Mihailov str. 66, Blagoevgrad, Bulgaria

i.nedqikov@gmail.com

**Abstract** – In this paper an IP based network consisting of two separate IP networks - a virtual one, running MPLS and an experimental IP network, connected to the virtual one, have been studied. VoIP traffic is exchanged between the two networks. Both networks are connected to the Internet and exchange traffic with it. The virtual network is created by using GNS3. The purpose of this paper is to show a comparison in the performance between the two IP networks. In addition, mathematical distributions and approximations have been made to be used to further evaluate the performance of the two networks. The used methodology in the present work can be applied in the study of different IP networks through which different types of real-time traffic passes.

**Keywords** – GNS 3, IP networks, Monitoring VoIP traffic, Wireshark

## 1. INTRODUCTION

The IP networks are constantly expanding - becoming larger and more complex. Subscribers of these networks are also growing. As a result, these networks must continually provide new and new services to subscribers. In addition, more and more devices are gaining access to these networks. This leads to an increase in the number of network devices in such a network. All of this causes network congestion and slows down the network. Reducing the speed of the IP network leads to a deterioration in the quality of services offered, which in turn leads to consumer dissatisfaction [1]. In order to avoid delays in the network MPLS (Multiprotocol Label Switching) is introduced [2, 3, 4, 5, 6, 7]. In order to find out if the use of MPLS will lead to a significant improvement in the speed of data exchange in a particular network with a particular type of traffic, research needs to be done. Setting up such an experimental network is expensive and not every institution would allow such an experiment. It is therefore appropriate to use programming environments for modeling of IP networks [8, 9, 10, 11, 12, 13].

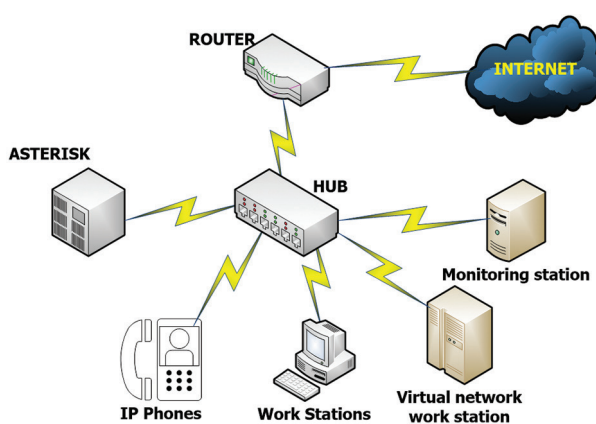
The purpose of the present work is to study and compare the performance between a virtual network using MPLS and a real IP network not using MPLS. The two IP networks are interconnected and exchange traffic between each other and the Internet. What the two networks have in common are the subscribers of the IP telephone exchange, which is located in the real network. The real network does not use the MPLS technology but the virtual IP network does. Therefore, it is

possible to monitor the voice traffic that is exchanged between the two networks and make a comparison of the performance between the two networks (study of the time delay between the individual packets).

## 2. TOPOLOGY OF THE NETWORK

### 2.1. TOPOLOGY OF THE EXPERIMENTAL NETWORK

Figure 1 shows the topology of the experimental network, which is part of the bigger real network – the IP network of university campus building.



**Fig. 1.** Topology of the real network

Due to the lack of a layer 2 switch with a “mirror port”, a hub is used to monitor the traffic in the experimental network. Figure 1 shows an idea of what the part of the

real network that will be studied looks like. Therefore, the topology has the shape of a star and the hub is at its center. The experimental real network is composed of several IP phones connected to the IP telephony exchange Asterisk, a router that provides Internet connectivity, several workstations, and a hub that forwards all the traffic in the experimental network to the monitoring station. At the monitoring station specialized software for traffic monitoring - Wireshark is installed. The workstation where the virtual network is running is also connected to the hub.

## 2.2 TOPOLOGY OF THE VIRTUAL NETWORK

Figure 2 shows the topology of the virtual network. The GNS 3 platform is used for the modeling [14, 15]. The platform enables integration with specialized network monitoring programs and connection to real IP networks and emulating real network devices. Device emulation is the imitation (emulation) of a device's hardware. This allows the users to start and work with real images of working network devices.

The network is configured to work with the dynamic routing protocol OSPF. The network uses MPLS. R1 to R4 are the routers. These are disk image emulations of real routers. S1 to S2 are switches, more precisely, these are simulations of switches. Router\_Firewall is a module that connects the virtual network to real networks. Test\_PC\_1 and Test\_PC\_2 are virtual machines that are used to generate network traffic. Test\_PC\_1 has a software phone installed on it. It is used to generate VoIP calls to the IP phones on the real network. Additionally, an Internet browser is used to generate Internet traffic – the browser is used for opening Internet pages of any kind (forums, pages with multimedia content, news sites, etc.). Test\_PC\_2 is used only to generate traffic from the Internet. This will simulate the most common business network traffic - IP telephony and Internet access.

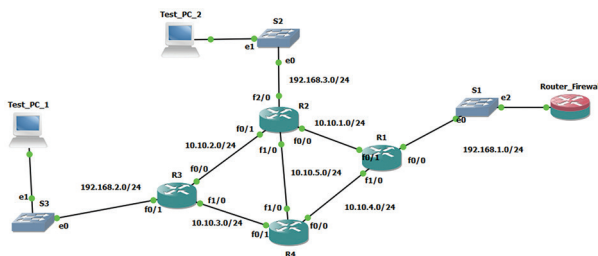


Fig. 2. Topology of the virtual network

## 3. METHODOLOGY FOR CONDUCTING THE MEASUREMENTS

As mentioned above, in the real network, a hub is used to forward all the generated traffic to the monitoring station [16, 17, 18]. The software used for monitoring is Wireshark [19, 20, 21]. In the virtual part of the network, due to the functionality of GNS 3, Wireshark will monitor the traffic in all the links between the routers.

One of the Wireshark functionalities for IP telephony analysis, in particular, RTP streams analysis, will be used to evaluate the two networks. The parameters to be monitored are:

- Delta: this is the difference in the receipt of one packet from the previous packet. As the devices in one RTP session are not synchronized, each device and the network itself cause additional delay. The receiving party must cope with this delay and synchronize with the transmitting party. To be able to do the synchronization, the receiving party uses the timestamp information of the RTP packet. The Delta parameter shows exactly this difference in the timestamps of the captured RTP packets. This parameter is characteristic of the network layer and reflects the arrival of the capture interface packet (where timestamp is placed);
- Jitter: this is the difference in packet delay. Also known as spurious phase modulation. In IP networks the jitter is used to measure the time difference between packet arrivals. It is expressed as the displacement of packets in time. This is not a particular problem with data transmission, but with voice transmission, jitter is important.

## 4. RESULTS

### 4.1 RESULTS OBTAINED IN THE VIRTUAL NETWORK

Based on the monitoring of the traffic in the virtual network, it was found out that the traffic generated by Test\_PC\_1 passes through R3, R4, R1, Router\_Firewall and vice versa. The traffic from Test\_PC\_2 flows through R2, R4, R1, Router\_Firewall and vice versa. No additional configurations for QoS or route prioritization have been made in the virtual network. Therefore, the traffic passes through these nodes. Based on the dynamic routing protocol used, OSPF, and the configured MPLS, the routers themselves chosen these routes to traverse the data flows. On the other links only service information is exchanged, such as: OSPF Hello packets, LDP packets, and other service packets.

During the study of the virtual network, all links between the routers are monitored, but the presented results are for only one of the monitored links, because the obtained results from this connection provide sufficient information to evaluate the performance of the virtual network. The monitored link in the virtual network is the link between R1 and R4. Firstly, this link is chosen because the whole traffic in the virtual network passes through it and so it is more deeply studied. Secondly, the obtained data from the measurement can be used as a representative sample for the whole network. From the analysis of the results obtained by Wireshark for all links between the routers of the virtual network, for the values of the jitter and the delta parameter in the various links, there is a con-

tinuous increase of their values, approaching the Router\_Firewall. This is due to the fact that each subsequent router begins to process more and more data streams, and eventually Router\_Firewall processes all the traffic from the virtual network to the real one. As a result, there is an increase in the delay after each subsequent router. For this reason, in the present work, it was decided to present the results only from the link between R1 and R4. Presenting the results of all links would be unnecessary because they will not provide any different information.

Figure 3 shows summary results for a single stream (forward – reverse direction) of a VoIP call. The device with the IP 192.168.2.2 is the software phone on the virtual machine - Test\_PC\_1 and the device with the address 192.168.31.50 is the Asterisk IP telephony exchange. According to Cisco [22], the average one-way jitter should be less than 30 ms. As it can be seen, the mean jitter value is well below the 30 ms limit for both directions. The summary results obtained by Wireshark also contain other data such as: packet loss. The results show that there are no losses in the forward stream – to the Asterisk, but in the reverse direction there are 146 lost packages or about 0.13%. Information is also given about the total number of RTP packets for each of the streams. Information about the duration of the call is also available - 2326 seconds. Figure 3 also shows the sampling frequency - 8000 Hz (as can be seen, there is a deviation from this frequency for both directions), as well as the deviation from the clock frequency. From this data, it is also possible to get an idea of the delay between the packets, by following the values of Delta and Skew. Delta shows the time difference between the receipt of the previous packet from the stream and the packet that is now received. Skew shows how long the current packet is ahead of or behind the entire call, relative to the nominal speed of the packet. In the presented case, it is noticed that the packet lags behind the whole conversation.

Forward		Reverse	
192.168.2.2:8000 → 192.168.31.50:15968		192.168.31.50:15968 → 192.168.2.2:8000	
SSRC	0x0d8caaea	SSRC	0x66531d9e
Max Delta	173.02 ms @ 583606	Max Delta	512.56 ms @ 597773
Max Jitter	17.91 ms	Max Jitter	51.93 ms
Mean Jitter	1.81 ms	Mean Jitter	3.42 ms
Max Skew	-1175.93 ms	Max Skew	-572.50 ms
RTP Packets	116227	RTP Packets	116191
Expected	116227	Expected	116337
Lost	0 (0.00 %)	Lost	146 (0.13 %)
Seq Errs	0	Seq Errs	141
Start at	2079.460558 s @ 313834	Start at	2079.489061 s @ 313840
Duration	2325.53 s	Duration	2326.81 s
Clock Drift	-1224 ms	Clock Drift	-398 ms
Freq Drift	7996 Hz (-0.05 %)	Freq Drift	7999 Hz (-0.02 %)

Fig. 3. Summary results from Wireshark

Figure 4 shows the jitter distribution throughout the whole session in the direction from the virtual machine to the Asterisk (forward direction), and figure 5 shows the jitter distribution in the opposite direction. X is for the whole duration of the conversation, and Y stands for the values of the jitter at each moment of the conver-

sation. From figure 4 it is noticed that during the whole conversation the jitter in the forward direction, for every moment of the conversation, does not exceed the limit of 30 ms. As a result, there is a lack of packet loss.

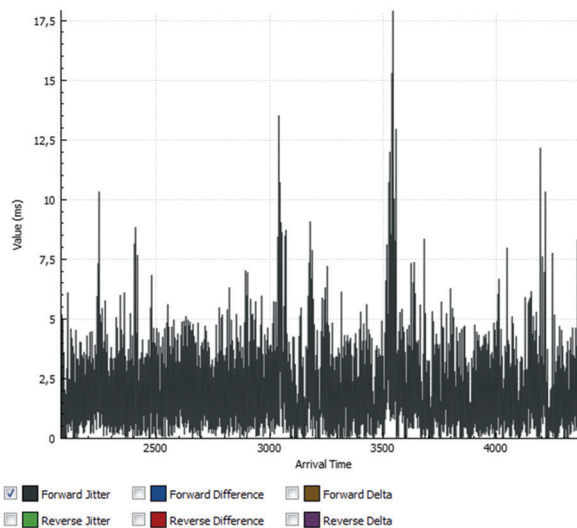


Fig. 4. Forward jitter for the whole stream

The results in figure 5 are quite different. It is noticed that the jitter repeatedly exceeds the limit of 30 ms. - reaches values of 50 ms, which is unacceptable. As a result, there is a loss of packets in the reversed direction, also evident from figure 3. This increase in the values in the reversed direction is due to the accumulation of delay in the real network.

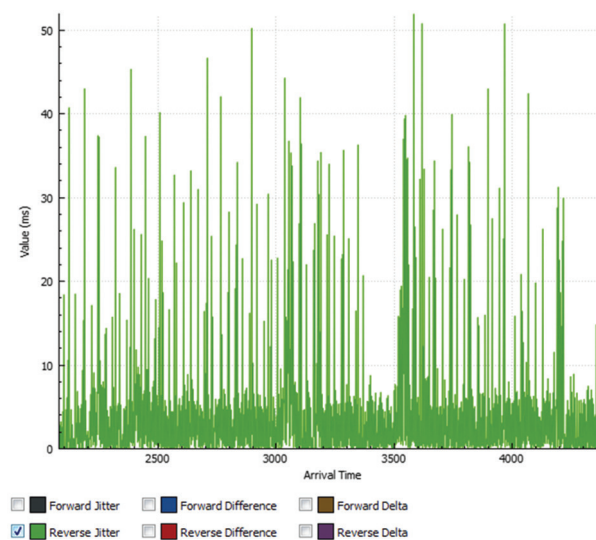


Fig. 5. Reversed jitter for the whole stream

Figures 6 and 7 show the delta values for each second of the call in both directions. Again X stands for the whole duration of the conversation, and Y stands for the values of the delta at each moment of the conversation. As explained above, this parameter indicates the arrival time between two packets or known as a



time delay. By default, it almost always coincides with packetization time - 20ms. Due to the presence of jitter on the network, its value can increase and lead to packet loss. The one-way transmit delay should not exceed 150 ms. (G.114 recommendation) [23] and the maximum round-trip delay should not exceed 300ms. As can be seen from figure 6, the delta in the forward direction exceeds the 150 ms limit only two times. The results in the reversed direction are getting worse because of the high value of the jitter.

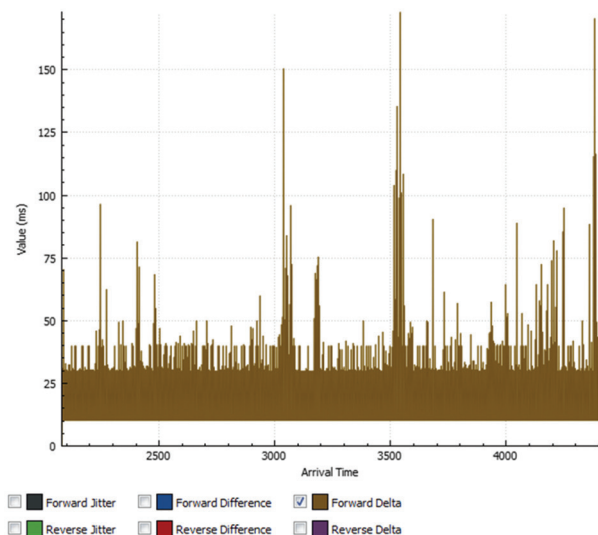


Fig. 6. Forward delta for the whole stream

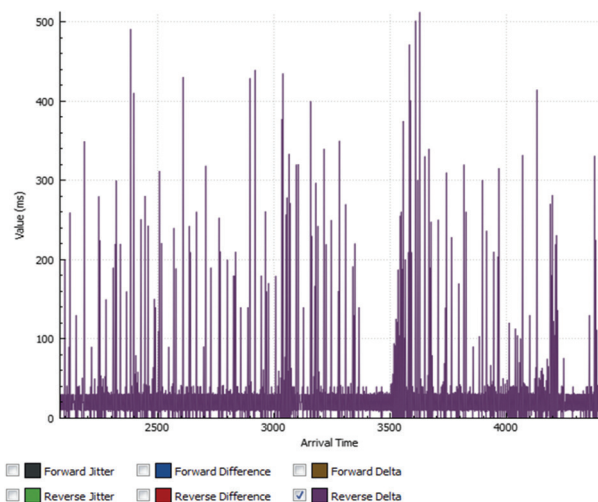


Fig. 7. Reversed delta for the whole stream

In the virtual network, the values of the delta in the reverse direction decrease after each node passed. This is due to the presence of the MPLS. Figures 8 and 9 and 10 show these dependences. As can be seen from the summarized results for the reverse flow for the link between R3 and R4 (Figure 8), the values of Delta and max jitter decreases. The graph for Delta for the whole conversation period (figure 9), for the link R3 - R4, compared to the result of figure 7 shows a significant improvement in the instantaneous values of the parameter.

Forward		Reverse	
192.168.2.2:8000 → 192.168.31.50:15968		192.168.31.50:15968 → 192.168.2.2:8000	
SSRC	0x0d8caaea	SSRC	0x66531d9e
Max Delta	271.03 ms @ 554197	Max Delta	501.56 ms @ 567725
Max Jitter	36.27 ms	Max Jitter	37.54 ms
Mean Jitter	0.83 ms	Mean Jitter	3.60 ms
Max Skew	-1161.29 ms	Max Skew	-1785.42 ms
RTP Packets	116227	RTP Packets	116175
Expected	116227	Expected	116337
Lost	0 (0.00 %)	Lost	162 (0.14 %)
Seq Errs	0	Seq Errs	148
Start at	2041.299212 s @ 301343	Start at	2041.396725 s @ 301361
Duration	2325.52 s	Duration	2327.04 s
Clock Drift	-925 ms	Clock Drift	31 ms
Freq Drift	7997 Hz (-0.04 %)	Freq Drift	8000 Hz (0.00 %)

Fig. 8. Summary results from Wireshark

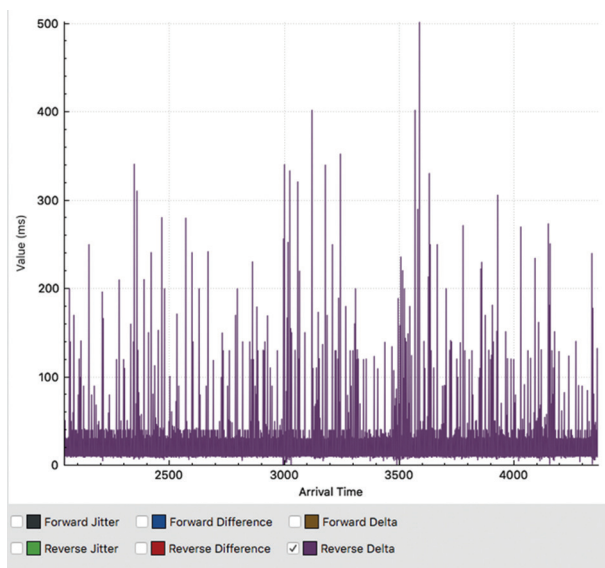


Fig. 9. Reversed delta for the whole stream

Figure 10 presents the graph for the reversed jitter for the whole conversation period for the link R3 - R4, compared to the result of figure 5 shows a significant improvement in the instantaneous values of the parameter.

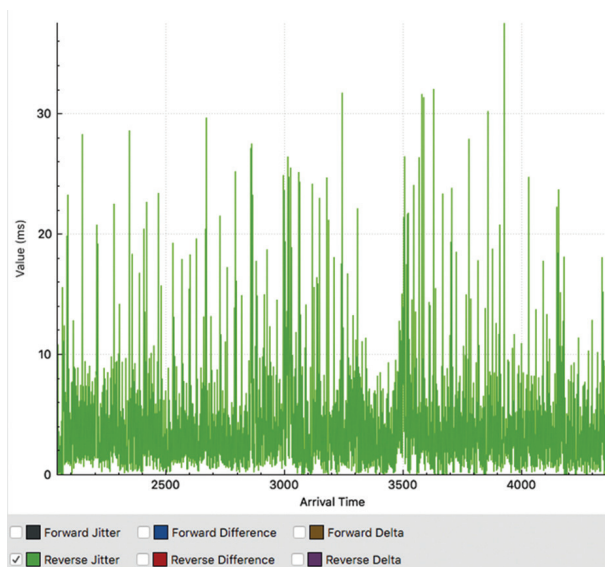


Fig. 10. Reversed jitter for the whole stream

Another method for assessing the performance of an IP network is by using mathematical distributions and approximations for distribution of the intervals between the arrival times of packets (time delays between individual packets) [24, 25, 26]. Such mathematical distribution is made for the link between R1 and R4. The distribution is made as the captured packets from Wireshark are further processed by a specialized program on the parameter intervals between the moments of arrival of the packets. Figure 11 shows the mathematical distribution of the captured packets from the link between R1 and R4. On "x" are the times of arrival of the individual packets – the whole conversation stream and "y" indicates the delay of the received packet compared to the previous packet. As it can be seen from the distribution, it can be argued that the time delay is almost constant after a short period of oscillation due to the network establishment time. The Wakeby approximation further confirms the constant time delay between the packets. The use of this approximation makes it easier to read the obtained results of the mathematical distribution. The constant time delay is due to the use of the MPLS technology in the virtual network.

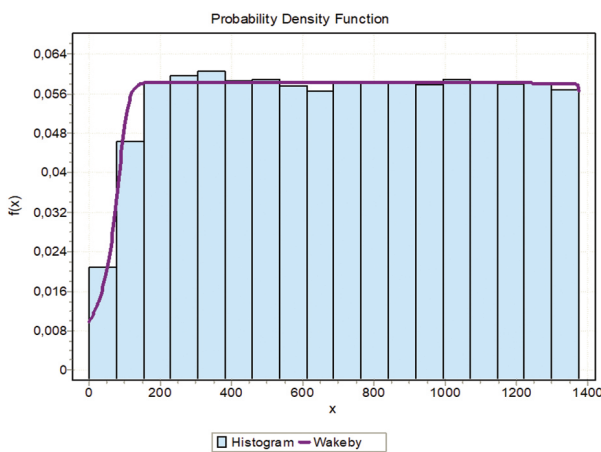


Fig. 11. Mathematical distribution for the R1–R4 link

## 4.2 RESULTS FROM THE EXPERIMENTAL NETWORK

Figure 12 shows the summarized results for the same VoIP call stream discussed in 4.1 (forward – reverse direction). As the results show, in the forward direction from the virtual network (192.168.31.67 exit/entry interface of the virtual network) to the Asterisk (192.168.31.50) the mean jitter value is much higher than that of the virtual network, but is still smaller than the limit of 30 ms. As the voice flow in the reverse direction (from Asterisk to Test\_PC1) starts from this network, the first lost packets in this direction are noticed - 28 (0.02%).

Figure 13 shows the jitter distribution for every second of the call in the forward direction. The graph shows that the jitter significantly exceeds the 30 ms limit. As a result, a large percentage of lost packets is observed - 0.3%, compared to the same flow in the virtual network where there is no packet loss.

Figure 14 presents the jitter distribution for the entire duration of the call in reverse direction. From the graph, it can be argued that the results obtained are almost identical to those of figure 5, except that the lost packets are much smaller here.

Forward		Reverse	
192.168.31.67:33970 → 192.168.31.50:15968		192.168.31.50:15968 → 192.168.31.67:33970	
SSRC	0x0d8caaea	SSRC	0x66531d9e
Max Delta	394.95 ms @ 1088690	Max Delta	509.65 ms @ 1789675
Max Jitter	39.33 ms	Max Jitter	53.46 ms
Mean Jitter	5.76 ms	Mean Jitter	1.76 ms
Max Skew	-2744.92 ms	Max Skew	-567.46 ms
RTP Packets	115884	RTP Packets	116309
Expected	116227	Expected	116337
Lost	343 (0.30 %)	Lost	28 (0.02 %)
Seq Errs	228	Seq Errs	27
Start at	2168.778674 s @ 951198	Start at	2168.783591 s @ 951201
Duration	2325.52 s	Duration	2326.82 s
Clock Drift	-870 ms	Clock Drift	-420 ms
Freq Drift	7997 Hz (-0.04 %)	Freq Drift	7999 Hz (-0.02 %)

Fig. 12. Summary results from Wireshark

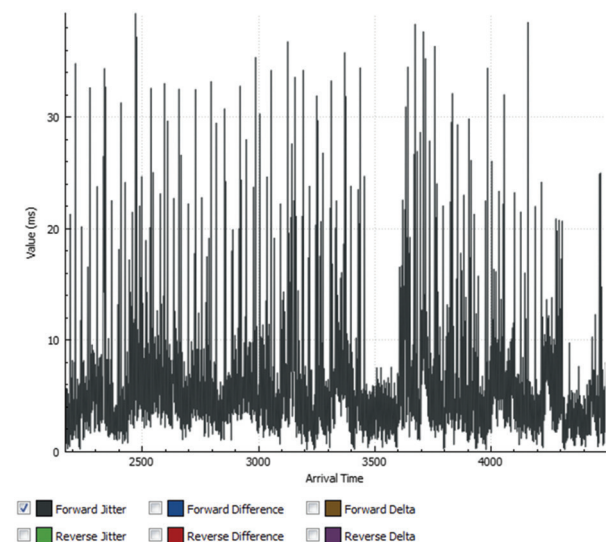


Fig. 13. Forward jitter for the whole stream

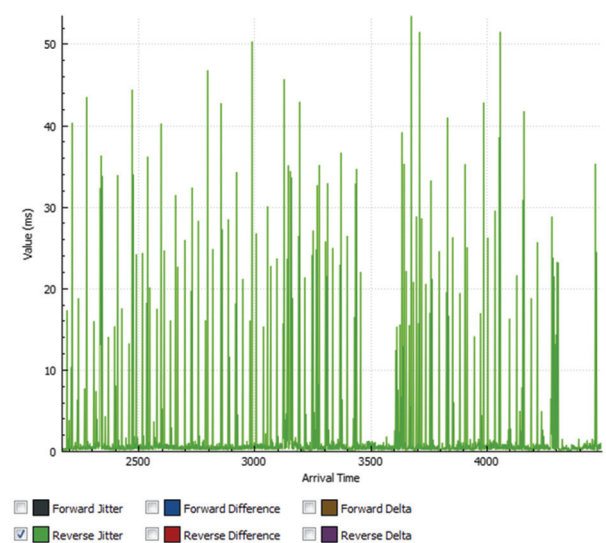


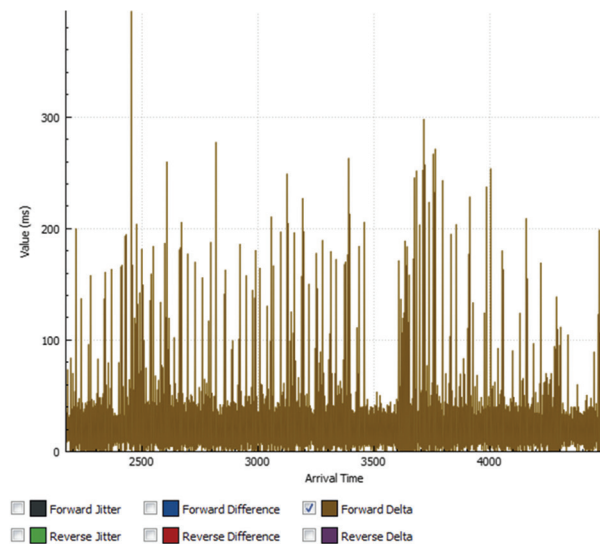
Fig. 14. Reversed jitter for the whole stream

The better jitter values in the forward direction on the virtual network are due to the fact that MPLS is used in the virtual network, which accelerates the network operation while it is not used in the real network. As it can be seen, the deterioration of the parameters of the stream in the reverse direction in the virtual network starts in the experimental network and in the virtual network they are getting worse.

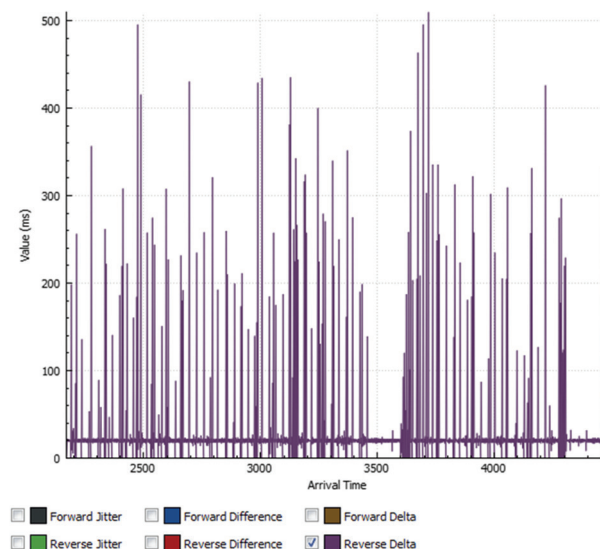
Figure 15 shows the results for the delta in the forward direction. There is a significant deterioration in the values of this parameter - many times it is exceeding the 150 ms limit.

The results of figure 16 for the reverse delta are almost identical to those of Figure 7.

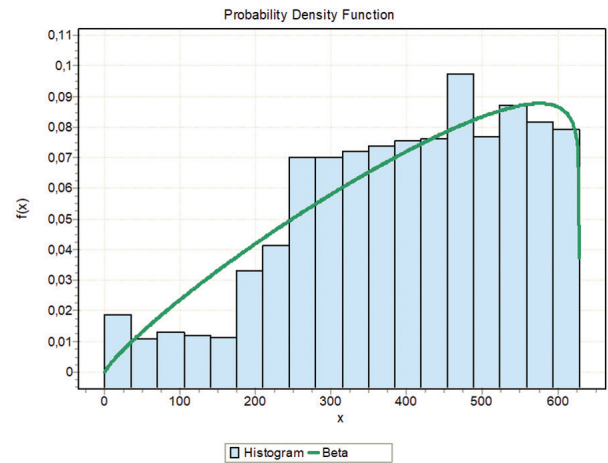
Again, to further evaluate the performance of the real network, a mathematical distribution of the intervals between the moments of packet arrival is made. Figure 17 shows the resulting distribution for the time delay between the packets.



**Fig. 15.** Forward delta for the whole stream



**Fig. 16.** Reversed delta for the whole stream



**Fig. 17.** Mathematical distribution for the real network

As it can be seen from the distribution for the experimental network, the delay between packets varies and it can be claimed to be constant at times, but not as it is on the virtual network, where MPLS is configured. This statement is further supported by the Beta approximation. It shows that the time delay is constantly increasing. Again, the use of the approximation makes it easier to read and understand the results of the distribution.

## 5. CONCLUSIONS

A virtual IP - based network has been created and it is configured to work with MPLS. A real experimental IP based network is also created. There is connectivity between the two networks. Both networks are connected to the Internet.

Monitoring programs for IP – based networks and mathematical distribution have been used to evaluate the performance of the two networks. Based on the results from the monitoring of the two networks, the following results were obtained: the mean and maximum values of the jitter in the virtual network in the forward direction are much smaller than the one in the experimental network.

The delta parameter in the virtual network in the forward direction is the lowest. In the reverse direction a significant improvement in the instantaneous values of the parameter are noted compared to the values of the parameter in the real network.

The instantaneous values of the jitter in the reversed direction are drastically improved too, compared to the values from the real network.

The deterioration of the flow parameters caused by the experimental network is partially compensated in the virtual network. This is due to the configured MPLS in the virtual network.

The mathematical distributions also confirm the results of the monitoring. The time delay on the network using MPLS is constant, unlike the experimental real



network. This statement is further confirmed by the two used approximations - Wekaby and Beta.

The obtained results from the monitoring and the mathematical distributions confirm that, in an IP - based network that uses MPLS, the performance (in terms of packet time delays) is much better than without using MPLS. The use of the MPLS technology in an IP - based network, in which real time traffic (VoIP traffic) will be transmitted, significantly improves network performance - the time delay between packets is constant. It is therefore advisable to use this technology in IP networks where the transmitted traffic is in real time.

The used methodology in this work - the use of monitoring programs and mathematical distributions, can be applied to evaluate the performance of other IP-based networks through which other types of real-time traffic is transmitted as video.

## 6. ACKNOWLEDGMENT

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science

## 7. REFERENCES:

- [1] F. Sapundzhi, M. Popstoilov, "C # implementation of the maximum flow problem", Proceedings of the 27<sup>th</sup> National Conference with International Participation TELECOM, Sofia, Bulgaria, 30-31 October 2019, pp. 62-65.
- [2] M. Taruk, E. Budiman, M. Wati, Haviluddin, "OSPF Wireless Mesh with MPLS Traffic Engineering", Proceedings of the International Conference on Electrical, Electronics and Information Engineering, Denpasar, Bali, Indonesia, 3-4 October 2019, pp. 119-122.
- [3] M. A. Ridwan, N. A. M. Radzi, W. S. H. M. Wan Ahmad, F. Abdullah, M. Z. Jamaludin, M. N. Zakaria, "Recent trends in MPLS networks: technologies, applications and challenges," IET Communications, Vol. 14, No. 2, 2020, pp. 177-185.
- [4] O. Lemeshko, O. Yeremenko, "Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection", Proceedings of the 14<sup>th</sup> International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, Lviv-Slavske, Ukraine, 20-24 February 2018, pp. 1009-1013.
- [5] T. Chang, Y. Tang, Y. Chen, W. Hsu, M. Tsai, "Maximum Concurrent Flow Problem in MPLS-Based Software Defined Networks", Proceedings of the IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9-13 December 2018, pp. 1-7.
- [6] E. N. Lallas, A. Xenakis, G. Stamoulis, J. Korinthios, "QoS and MPLS design issues in NoCs", Proceedings of the South-Eastern European Design Automation, Computer Engineering, Computer Networks and Society Media Conference, Kastoria, Greece, 22-24 September 2018, pp. 1-4.
- [7] O. Nevzorova, O. Lemeshko, A. Mersni, A. M. Hailan, A. S. Ali, S. Harkusha, "Improved Two-Level Method of Multicast Routing in MPLS-TE Network", Proceedings of the 2<sup>nd</sup> Ukraine Conference on Electrical and Computer Engineering, Lviv, Ukraine, 2-6 July 2019, pp. 846-850.
- [8] S. T. Mirtchev, "Investigation of Pareto/M/1/k Teletraffic System by Simulation", Proceedings of the 27<sup>th</sup> National Conference with International Participation TELECOM, Sofia, Bulgaria, 2019, 30-31 October 2019 pp. 70-73.
- [9] M. Imran, M. A. Khan, M. Abdul Qadeer, "Design and Simulation of Traffic Engineering using MPLS in GNS3 Environment", Proceedings of the 2<sup>nd</sup> International Conference on Computing Methodologies and Communication, Erode, India, 15-16 February 2018, pp. 1026-1030.
- [10] N. I. Sarkar, S. Gul, B. Anderton, "Gigabit Ethernet with Wireless Extension: OPNET Modelling and Performance Study", Proceedings of the International Conference on Information Networking, Kuala Lumpur, Malaysia, 9-11 January 2019, pp. 216-221.
- [11] Cherneva G., H. Spiridonova, "Determination of the Impulse Response of a Communication Channel in the Process of Information Transmissions", Journal of the Technical University of Gabrovo, Vol.57, 2018, pp.103-106.
- [12] S. T. Mirtchev, "Packet-Level Link Capacity Evaluation for IP Networks", Cybernetics and Information Technologies, Vol. 18, No. 1, 2018, pp. 30-40.
- [13] F. I. Sapundzhi, M. S. Popstoilov, "Optimization Algorithms for Finding the Shortest Paths", Bulgaria

- ian Chemical Communications, Vol. 50, No. Special Issue B, 2018, pp. 115-120.
- [14] B. Korniyenko, L. Galata, L. Ladieva, "Research of Information Protection System of Corporate Network Based on GNS3", Proceedings of the International Conference on Advanced Trends in Information Theory, Kyiv, Ukraine, 18-20 December 2019, pp. 244-248.
- [15] M. A. Barry, J. K. Tamgno, C. Lishou, M. B. Cissé, "QoS impact on multimedia traffic load (IPTV, RoIP, VoIP) in best effort mode", Proceedings of the 20<sup>th</sup> International Conference on Advanced Communication Technology, Chuncheon, South Korea, 11-14 February 2018, pp. 694-700.
- [16] R. K. CV, H. Goyal, "IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark", Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking, Vellore, India, 30-31 March 2019, pp. 1-6.
- [17] A. Siswanto, A. Syukur, E. A. Kadir, Suratin, "Network Traffic Monitoring and Analysis Using Packet Sniffer", Proceedings of the International Conference on Advanced Communication Technologies and Networking, Rabat, Morocco, 12-14 April 2019, pp. 1-4.
- [18] K. Sinchana, C. Sinchana, H. L. Gururaj, B. R. Sunil Kumar, "Performance Evaluation and Analysis of various Network Security tools", Proceedings of the International Conference on Communication and Electronics Systems, Coimbatore, India, 17-19 July 2019, pp. 644-650.
- [19] P. Goyal, A. Goyal, "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark", Proceedings of the 9<sup>th</sup> International Conference on Computational Intelligence and Communication Networks, Girne, Northern Cyprus, 16-17 September 2017, pp. 77-81.
- [20] R. Das, G. Tuna, "Packet tracing and analysis of network cameras with Wireshark", Proceedings of the 5<sup>th</sup> International Symposium on Digital Forensic and Security, Tirgu Mures, Romania, 26-28 April 2017, pp. 1-6.
- [21] P. Navabud, C. Chen, "Analyzing the Web Mail Using Wireshark", Proceedings of the 14<sup>th</sup> International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Huangshan, China, 28-30 July 2018, pp. 1237-1239.
- [22] T. Sziget, C. Hattingh, "End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs", Cisco Press. Part of the Networking Technology series, 2004
- [23] Cisco - Understanding Delay in Packet Voice Networks, white paper, <https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html> (accessed: 2021)
- [24] M. M. Alani, "Mathematical Approximation of Delay in Voice over IP", International Journal of Computer and Information Technology, Vol. 3, No. 1, 2014, pp. 78-82.
- [25] K. Hammad, A. Moubayed, A. Shami, S. Primak, "Analytical Approximation of Packet Delay Jitter in Simple Queues", IEEE Wireless Communications Letters, Vol. 5, No. 6, pp. 564-567, 2016.
- [26] R. Dehghan, M. Keyanpour, "A numerical approximation for delay fractional optimal control problems based on the method of moments", IMA Journal of Mathematical Control and Information, Vol. 34, No. 1, 2017, pp. 77-92.