Transactions on Engineering and Computing Sciences - Vol. 11, No. 5
Publication Date: October 25, 2023
DOI:10.14738/tecs.115.15645.
Mwape, J. C., & Lubobya, C. S. (2023). Performance Evaluation of IPv4 and IPv6 on IPsec/MPLS Enabled Network: A Case of Zambia. Transactions on Engineering and Computing Sciences, 11(5). 88-100.
SERVICES FOR SCIENCE AND EDUCATION

Performance Evaluation of IPv4 and IPv6 on IPsec/MPLS Enabled Network: A Case of Zambia

Jessy Chisenga Mwape
Department of Electrical and Electronics, School of Engineering,
University of Zambia, Lusaka, Zambia

Charles Smart Lubobya
Department of Electrical and Electronics, School of Engineering,
University of Zambia, Lusaka, Zambia

ABSTRACT

This paper explores the performance of IPv4 versus that of IPv6 in an MPLS/IPsec enabled network for real time applications and non-real time applications. Major Internet Service Providers (ISP) in Zambia have implemented MPLS within their core networks in order to provide traffic engineering and Quality of Service and network efficiency, however, MPLS does not encrypt the data as it travels through the network. To mitigate this, customers using the public infrastructure to connect to their remote sites have implemented IPsec. This framework of related protocols protects one or more data flows between network peers; thus, data confidentiality and integrity can be achieved. When MPLS is combined with IPsec both technologies can provide more security for enterprise WAN networks. However, most service providers and ISPs in Zambia and their Enterprise customers have implemented these technologies using Internet Protocol version Four (IPv4). As the number of devices requiring connectivity to the internet and core systems increases exponentially, the limited address space for IPv4 has reached exhaustion. This has prompted the Zambia Information and Communications Technology Authority (ZICTA) which is the statutory body for regulating Information and Communications Technology (ICT) in Zambia to include the development and implementation plan for migration from IPv4 to IPv6 in their 2022 to 2024 strategy. Once implemented, this strategy hopes to increase access and usage of ICT and postal services and increase the internet penetration rate from 60% to 70% by 2025. Based on Google's statistics, the IPv6 adoption rates for Zambia is still at 0%. In order to analyze the penetration rates of IPv4 versus IPv6, a structured questionnaire has been administered on 30 ISP employees and 30 enterprise customer employees to access the use of IPv4 and IPv6 protocols in their MPLS/IPsec networks. The data simulation for Voice over Internet Protocol (VoIP), Video conferencing, and Email was done using Riverbed Modeler simulation software and observe the performance of IPv4 in comparison with IPv6 in terms of jitter, throughput and delay.

Keywords: Multi-Protocol LS, Internet Protocol Security, Internet Protocol version 4 (IPv4) and version 6 (IPv6), Voice over IP, Video Conferencing, throughput, jitter and delay.

INTRODUCTION

As the demand and complexity of network connectivity increases, the need for integrating and securing several services continues to unfold. Critical parts of design and implementation of MPLS enabled enterprise networks include confidentiality and integrity of data. To ensure security of the data traversing the Service Providers, Enterprise customers implement IPsec on their edge devices. The MPLS Protocol became widely adopted because it could work in multiprotocol environments and its ability to support legacy network technologies. There is also was great need for routers to scale more efficiently and improve on speeds to meet the increasing bandwidth demand. In order to meet the growing demand for traffic flow, confidentiality and integrity, IPsec is implemented, and confidentiality is achieved through encryption of the payload before transmission and data integrity is provided by authenticating the packets at the receiving node. IPsec receivers can also detect and reject replayed packets. The sender and the recipient establish a secure IPsec session, negotiate requirements for the secure connection and calculate hash values of checksums to authenticate the exchange data.

The usage of Voice over Internet Protocol (VoIP), end to end encrypted applications and social media services such as Facebook and WhatsApp in Zambia has increased, with 15% of its population using Facebook alone. Owing to the population growth and growing demand for more devices to access the internet secured network services and applications, the need to migrate from Ipv4 to IPv6 becomes more apparent. As the use of broadband internet becomes more prevalent, issues around poor bandwidth has shifted to Network Address Translation (NAT) and performance issues.

REVIEW OF IPSEC OVER MPLS, IPV4 AND IPV6

IPsec Over MPLS

MPLS is a protocol independent transport technique which uses label switching to direct traffic from one node to another on the network. Instead of developing long complex IP routing tables, MPLS uses labels. MPLS is not bound to any specific underlying technology and can be implemented across various networking protocols. It functions similarly to bookmarks as MPLS-enabled routers are informed about the location of specific prefixes in the routing table through the MPLS protocol. MPLS VPN standards are defined in RFC4364.The document specifies the Service Provider method to provide VPN for its customers through their backbone network. The RFC4364 obsoletes RFC2547 which defined the use of MPLS VPN to forward packets while using Border Gateway Protocol (BGP) to distribute routes over the backbone. [1] IPsec ensures the confidentiality and authentication of application data exchanged between two end notes. It protects the data from replay (man-in-the-middle) attacks by verifying the integrity of sent packets and allowing the recipient to authenticate the source of the data. It is worth noting that IPsec can secure more than one data flow. Data confidentiality is achieved through encryption of the payload before transmission and data integrity is provided by authenticating the packets at the receiving node. [2] The standards of IPsec were initially defined in RFCs 1825-1829 and the protocol is commonly implemented in IPv4 networks. However, the standards were updated in RFC 2401-2412. This framework provides integrity, confidentiality and authentication of data. In 2005, the new IPsec superset standards of these preceding ones were defined in RFCs 4301-4309 which saw the abbreviation ***IPsec*** changed to ***IPsec***. The "standard provides network encryption (confidentiality), digital certification

(integrity), and device authentication (authentication)." [3] In an enterprise network IPsec can be used to provide router security for data that transverse the public network. The exhaustion of IPv4 addresses means that the Internet Assigned Numbers Authority (IANA) has no more IPv4 addresses available in the central pool of addresses to hand down to the different Regional Internet registry (RIR).

Numerous research studies have been conducted on MPLS networks and IPsec operations. Ongoing advancements in these technologies provide opportunities for further research. Previous research works have attempted to investigate various aspects of MPLS networks including traffic engineering, performance analysis and security aspects. The studies also cover different aspects of IPsec implementation using Ipv4, security enhancements, key management and performance evaluation.

The study by C. K. Simatimbe and C. S. Lubobya concluded that even though IPsec over MPLS increases the size of the data packets and bandwidth usage, the acceptable operating levels of the network are maintained. Additionally, the use IPsec on an MPLS network significantly improves security of the data and the network. [4]

The study by Johnson et al focuses on the scalability and performance analysis of MPLS networks with IPsec. The study analyses the impact of IPsec on MPLS network performance, particularly in large-scale deployments. The study investigated the overhead introduced by IPsec encryption and authentication processes and proposes optimization techniques to mitigate these overheads. The study provides valuable insights into the trade-offs between security and performance in MPLS networks with IPsec. [5]

In a study by Abid Shahzad and Mureed Hussain, the authors explore the benefits of deploying MPLS VPNs in order to enhance quality of service (QoS) and security of the network. This study shows the detailed analysis of the existing and future models and techniques used for implementing, optimizing and securing MPLS VPN technology. The results of this study demonstrate the effectiveness of the combined approach in providing enhanced security without compromising network performance. [6]

Internet Protocol Version 4

While implementing of MPLS/IPsec enabled networks continues to increase among service provides and enterprise customers, the migration from IPv4 to IPv6 has not made much progress. In Zambia, Internet Protocol version 4 (IPv4) is widely used in implementing small to medium and enterprise networks. Additionally, Mobile Network Operators (MNO) use IPv4 when providing subscribers with data services. Currently, there are 1,694,720 IP addresses allocated to Zambia. [7][1] With the digital transformation journey that the Government of Zambia has embarked on, the number of IPv4 addresses available will not carter for the entire population of 20 million Zambians. Therefore, it becomes more apparent now that the country should implement the proposed migration strategy from IPv4 to IPv6.

IPv4 is a one of the core protocols of internetworking methods for packet switched networks and the internet. Majority of MPLS/IPsec enabled networks use IPv4 because it is supported by most Virtual Private Networks (VPNs). The protocol is easy to deploy by most operators

because they find it familiar and widely supported by most network infrastructure including the ones with Pv6 capabilities. While IPv4 is widely deployed and supported on current internet infrastructure, it has several limitations. The study conducted by Daniel Abad Camarero indicated that due to the use of broadcast IP addresses in IPv4, routing scalability is significantly affected. Additionally, since the size of the IP address is limited to 32 bits which gives 2^{32} (4,294,967,296) addresses to be allocated globally which have since been depleted. [1]

In a related study by Emre Durdagi and Ali Buldu, indicated that the limited addresses in IPv4 do not meet the excellarated growth of the internet. Other common and frequent security threats on IPv4 networks include rogue devices, flooding attacks and Man in The Middle (MiTM) attacks. [8]

Internet Protocol Version 6

As seen below, the utilization of IPv6 in Zambia currently stands at a mere 0.02%. This figure encompasses traffic generated by key entities such as Liquid Intelligent Networks, AIRTEL, MTN, ZAMTEL and ZAMREN and other operators. However, the usage of IPv6 remains low in several African countries. According to statistics from APNIC, the usage of IPv6 in the mentioned African nations is as follows:

Table 1: IPv6 Usage Rates in Africa

Country	IPv6 Usage Rate (%)
Botswana	0.03
Kenya	7.51
Malawi	0.11
Rwanda	18.58
South Africa	4.94
Tanzania	0.46
Zambia	0.02
Zimbabwe	9.24

In contrast, within the African continent, Rwanda boasts the highest IPv6 usage rate at 18.58%. Nevertheless, compared to other regions, countries like the China exhibit a considerably higher adoption rate at 30.30%, while India leads globally with the highest adoption rate at 78.81%. [9] The slow rate of IPv6 adoption in Zambia is owing to the belief that IPv4 depletion is not an African problem yet. The results obtained from the survey conducted also showed that Enterprises and ISPs do not see the immediate need to migrate to IPv4. Other factors include the cost implication, lack of adequate training and policy direction for IPv4 to IPv6 migration and the lack of support for technical staff by key decision makers.

IPv6 is made up of 128bits allowing for 2^{128} addresses to be allocated globally. With this increase IP size, it is realistic to conclude that more devices now and in the foreseeable future can be allocated an IP address without the threat of depletion. It is worth noting that IPv6 has no broadcast addresses and uses unicast, anycast and multicast addresses. The unicast address is used to identify single interfaces which can be used for local use, anycase addresses identifies a set of interfaces. Packets sent to anycast addresses are delivered to the nearest interface

assigned one of these addresses. Multicast addresses are used to identify a group of interfaces. [10]

Several study topics concerning how essential security is in the deployment of IPv6, however, IPsec is not automatically deployed in IPv6 networks. IPv6 was made with security in mind when authentication and privacy support was built in the protocol. The simplified header format provides for more efficient routing and better multicast routing. In the same study of Daniel Abad Camarero, these advantages of IPv6 are highlighted. [11] Additionally, when IPsec is deployed with IPv6 this provides more enhanced features for the security of IP networks. The downside to IPv6 is that the majority of VPNs currently do not support it. Hence deployment is scarcely done.

Although IPv6 is not widely deployed globally, it is slowly being accepted. IPv6 has several advantages over IPv4. It provides better Quality of Service (QoS) support for real time traffic such as VoIP and Video conferencing. This also includes labeled flows which routers can use to recognize the end-to-end flow of packets being transmitted. [12] In Zambia, the rollout of the ZICTA 2022 to 2024 strategy which includes the migration plan of IPv4 to IPv6 will impact greatly on the success of increased access and usage of ICT throughout the country. The implementation of this strategy will require paying particular focus on addressing challenges relating to costs, increased access and awareness and training on the benefits of migrating for IPv4 to IPv6. [13]

METHODOLOGY

The study has used qualitative and quantitative methods. A structured questionnaire with precise, simple and easy to follow questions has been used to get results concerning factors affecting the security and performance of IPsec on Multiprotocol Label Switching (MPLS) enterprise enabled networks, deployment of IPv4 on such networks and the challenges of migrating to IPv6 in Zambia. In order to analyze the performance of IPv4 and IPv6, the study used OPNET modeler version 14.5 educational model to simulate a network configured with IPsec over MPLS.

Multiprotocol Label Switching (MPLS)

MPLS is an encapsulation mechanism most commonly implemented in Service Provider networks. In an enterprise environment, it can provide multi tenancy and segmentation. Ideally, the MPLS network architecture consists of the Provider (P), Provider Edge (PE) and Customer Edge (CE) routers. In order to conduct this study, the network set up uses the peer-to-peer VPN model in which the customer data is carried over the public network through the MPLS routers belonging to the ISP. MPLS packets can carry a set of labels in a stack. An MPLS packet undergoes label operations such as push, swap and pop. When a new label is added to the IP packet before forwarding it on the Label Switched Path (LSP), this operation is called push and is performed by the Ingress router. The transit router swaps the labels with new labels for transiting MPLS traffic. The Egress router strips off (pop) the label from packets leaving the MPLS environment to destination network. In this study, PE routers play both roles of Ingress and Egress depending on the source of the traffic. [14]

Using OPNET Modeler 14.5 the MPLS network shown in Figure 1 above was designed for a distance of 20 kilometers (20Km) between CE1 and CE2. CE1 connects to PE1 using the fiber cable and the distance between the two devices is five kilometers (5Km). The P, PE1 and PE2 are configured to run MPLS protocol. PE1, PE2, CE1 and CE2 are using static IP routing to peer with each other. In this configuration the routers Provider 1 and 2, PE1, PE2 which are running MPLS protocol. The configuration shows full mesh of label switched paths (LSP).

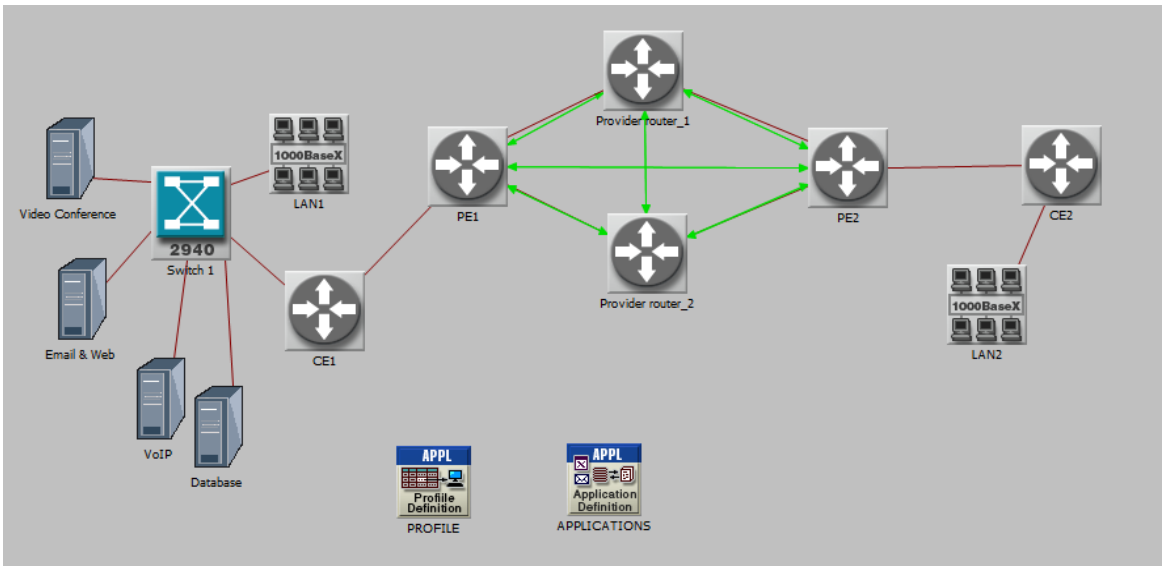


Figure 1: IPsec over MPLS network Architecture

Internet Protocol Security (IPsec)

IPsec ensures the confidentiality and authentication of application data exchanged between two end notes. It protects the data from replay (man-in-the-middle) attacks by verifying the integrity of sent packets and allowing the recipient to authenticate the source of the data. [13] It is worth noting that IPsec can secure more than one data flow. Data confidentiality is achieved through encryption of the payload before transmission and data integrity is provided by authenticating the packets at the receiving node. IPsec receivers can also detect and reject replayed packets. The sender and the recipient establish a secure IPsec session, negotiate requirements for the secure connection and calculate hash values of checksums to authenticate the exchange data. IPsec provides security during transmission of sensitive data over the service provider MPLS network. It acts as network layer protection by authenticating and protecting IP packets between IPsec nodes. The IPsec is configured in tunnel mode between CE1 and CE2. The configuration for this study is as shown in Figure 2 below.

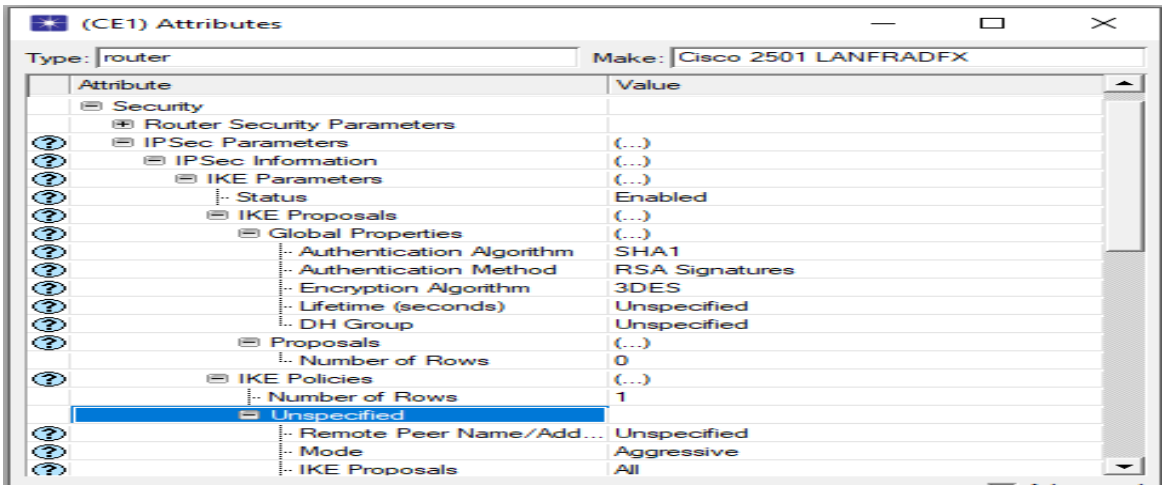


Figure 2: IPsec Parameters on CE1 and CE2

In this study, IPsec employs the authentication algorithm Secure Hash Algorithm (SHA1), the authentication method Rivest, Shamir and Adelman (RSA) and the encryption algorithm Triple Data Encryption Standard (3DES). These Internet Key Exchange (IKE) parameters are enabled to ensure authentication and encryption of data packets as they are transmitted between CE1 and CE2 through the MPLS network. The standards are supported on most vendor equipment like Cisco Systems which is used in this study.

Two scenarios were developed namely: Scenario 1: Internet Protocol version 4 (IPv4) and Scenario 2: Internet Protocol version 6 (IPv6). Both scenarios had four servers deployed, twenty-four VPN users. Two profiles are configured in both scenarios namely: IPsec over MPLS IPv4 and IPsec over MPLS IPv6. The four servers were configured to use either profile for each scenario with Email, VoIP, Web browsing (HTTP), Database and video conferencing services. Twenty VPN users were configured with all the five services on Local Area Network 1(LAN1) and LAN2 in both scenarios. The users in both LAN1 and LAN2 are configured to use Giga Ethernet (1000BaseX) to connect to the customer Edge routers. In scenario 1, all devices are automatically assigned IPv4 addresses while in scenario 2 the devices are assigned IPv6 addresses. In scenario 1, IPv6 is disabled on all interfaces while in scenario 2, all interfaces are enabled to use IPv6.

Figure 3 below shows the configuration of profiles and application services attached to the servers and users on the network.

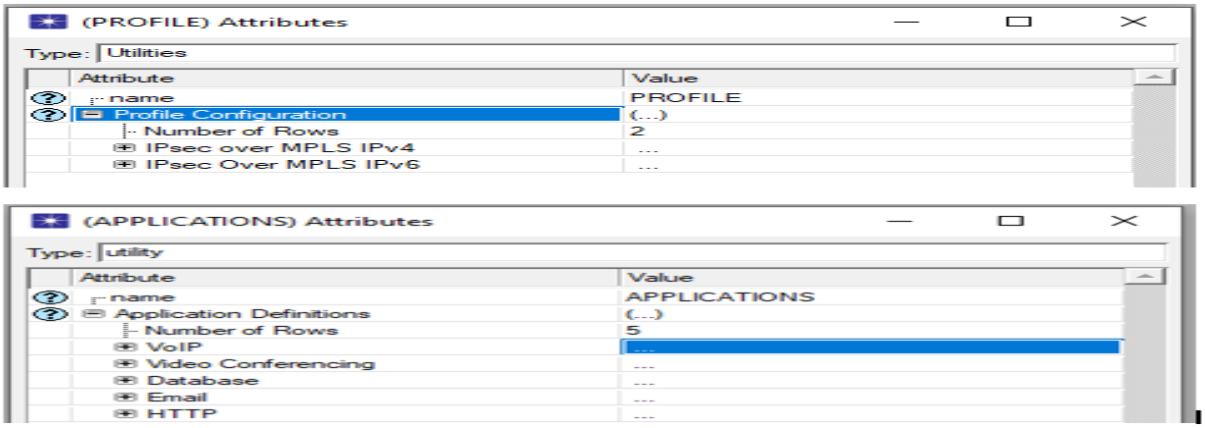


Figure 3: Profiles and Application Configuration

RESULTS AND DISCUSSION

Ipv4 Versus Ipv6 Survey

The results obtained from the 60 respondents from different MPLS/IPsec Enterprise customers and service providers showed that 85% of respondents are using IPsec over MPLS networks. These networks have been implemented using IPv4 protocol. Only 37% of respondents had some roadmap or plan on implementing the migration from IPv4 to IPv6 in the next 10years. 50% of respondents felt that the migration to IPv6 would still be lower than 10% in Zambia due to low demand for services. Additionally, these respondents felt that there is need for regulatory bodies to push for IPv4 to IPv6 migration by providing policy direction, perform readiness assessment and get the government support. The creation of a regulatory framework to mandate or incentivize IPv6 adoption in order to accelerate the deployment.27% of respondents indicated that companies need to prioritize the IPv6 migration and adoption through budgetary allocations for infrastructure, training and sensitization of the benefits of IPv6.

Figure 1 below shows the responses on how IPv6 deployment and usage will look like in the next 10 years. Interestingly, 12% said that the deployment and usage of IPv6 in the next 10 years will still be at 0.02%, 48% believe that will be lower than 10% and 40% said it will be higher than 10%. These responses give a general idea of the notions around IPv6 deployment and usage in Small to Medium Enterprises, Government agencies and department, Banks and Commercial Enterprises, Public and Private Hospitals, Internet Service Providers and Mobile Network Operators.

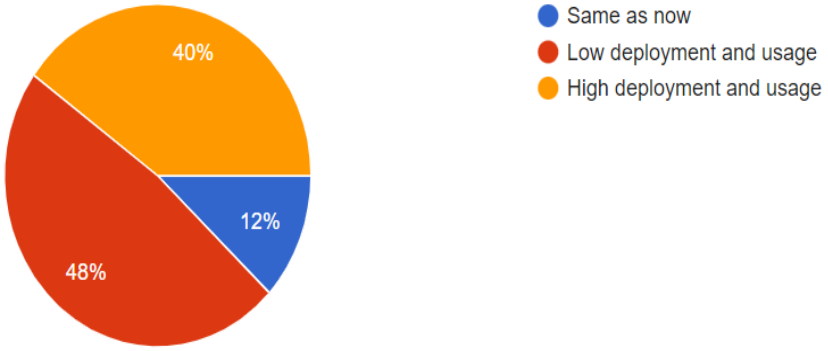


Figure 4: IPv6 in the next 10years in Zambia

Throughput

Real Time Applications:

The real time applications configured are VoIP and video conferencing. The utilization for the Enterprise network for the real time applications shows that IPv6 performs better than IPv4. Figure 2 below shows that IPv6 had twice as much utilization of the point to link in the network than IPv4. The throughput for IPv6 ranged from 200bps to 640Kbps while IPv4 ranged from 90bps to 430bps. This shows a 32% increase in point-to-point throughput on IPv6 network. This increase in utilization can be eluded to the extended header feature in IPv6 which reduces the overhead of header bandwidth and packet processing thereby making the connection much faster.

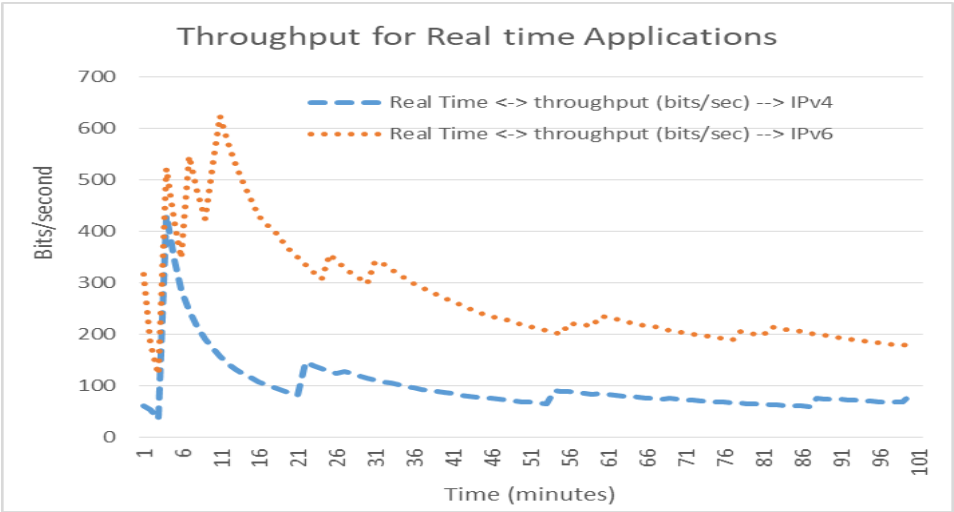


Figure 5: Point to Point Utilization for VoIP and Video Conferencing

Database:

The throughput results obtained for Database application shows that IPv6 performed better on traffic sent and received by the database server on the network. As shown in Figure 3 below, IPv4 was lower than IPv6 with the average throughput of 0.2 packets per second. This shows a record of 50% increase in throughput for IPv6 than IPv4 network.

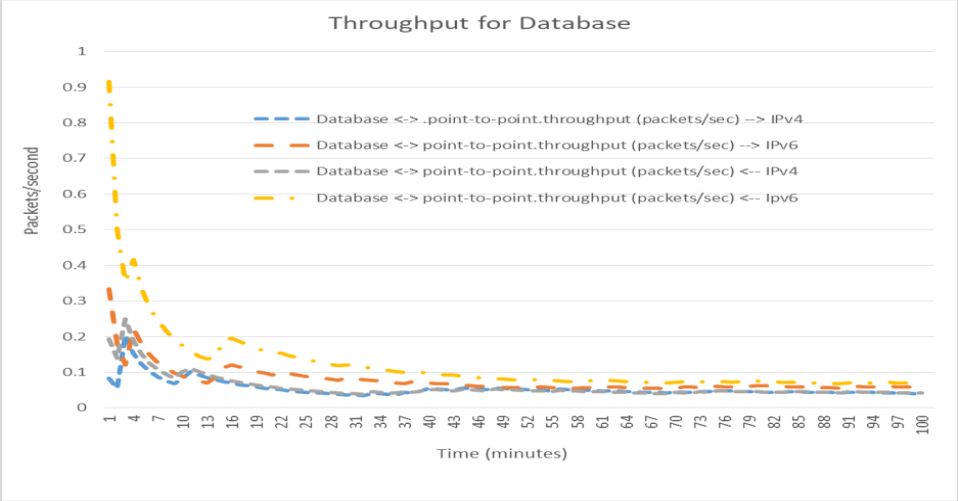


Figure 6: Throughput for Database

End to End Delay - Real Time Applications

The maximum end to end delay obtained for IPv6 is between 0.29ms and 0.33ms, however IPv4 experienced higher end to end delay of 0.45ms which dropped to a constant 0.43ms after 17 minutes of the results simulation. IPv4 relies on Network Address Translation (NAT) and Port Address Translations (PAT) when routing traffic from the MPLS network to the customer routers. This is due to the IPv4 address exhaustion, as a result these techniques introduce jitter and latency on the IPv4 network. End to end delay is also closely linked to the quality of service on the network. Hence the lower the values of delay, the better the quality of service provided by the enterprise network. Figure 3 below in which IPv4 experienced higher end to end delay than IPv6.

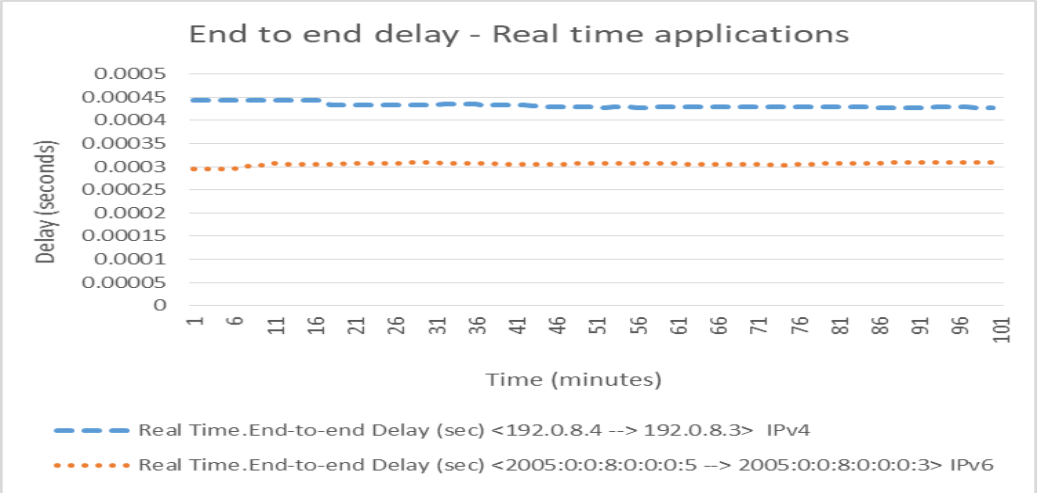


Figure 7: End to end Delay for real time applications

Load -Email and WEB

The performance of IPv6 was equally better for email and web browsing. The configuration in study is heavy browsing for HTTP and heavy load for email. As shown in Figure 5 below, IPv6

had 62% more email and Web load at the beginning of transmission. The hourly analysis still shows that IPv6 consistently had more traffic sent than IPv4 network.

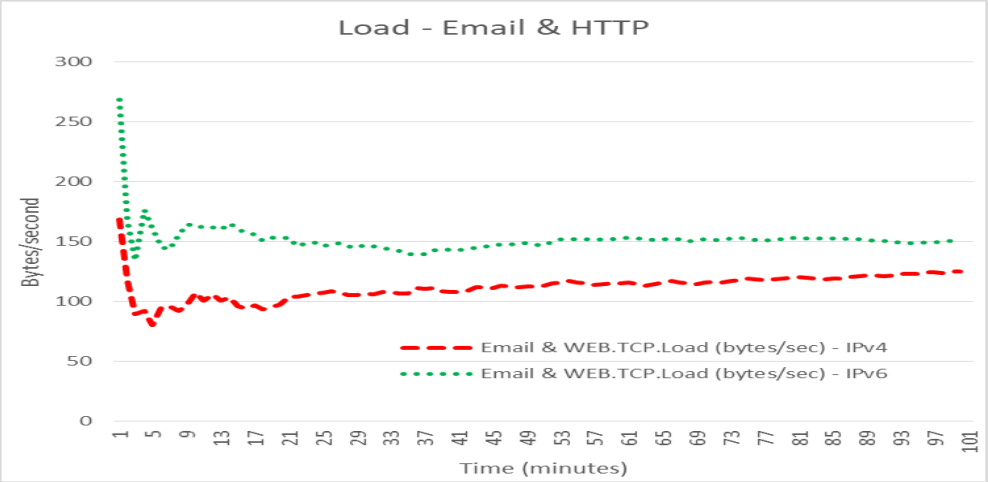


Figure 8: Email and Web traffic on Enterprise network

Response Time - Email

Comparing the email upload and download response time for IPv4 and IPv6, it can be seen from Figure 5 above that IPv6 had a higher download response time than IPv4. Interestingly, IPv4 had a higher upload response time in the first twenty-five (25) minutes than IPv6. Email services response time determines the quality of service and experience given to users of the services. When the response time is high, it means the users have a better experience when using the email service.

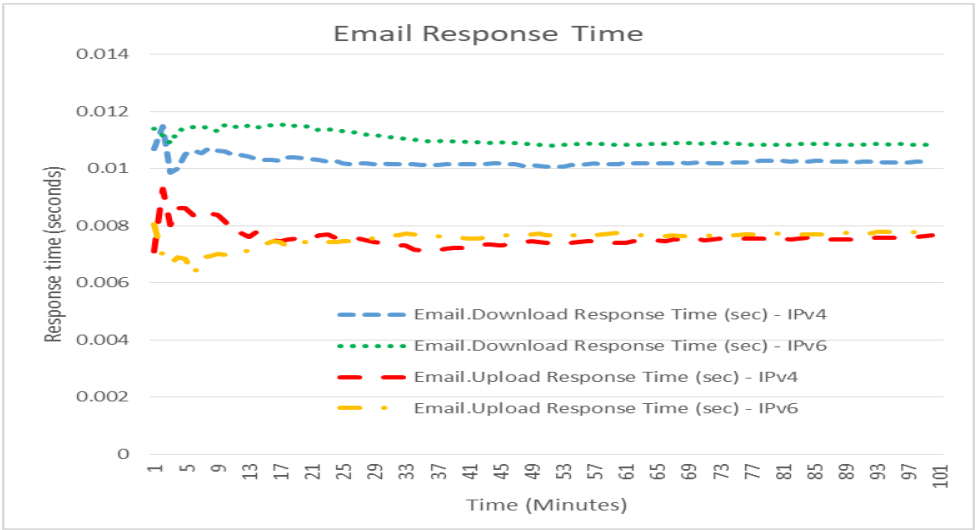


Figure 9: Response time - Email

CONCLUSION

Through the survey conducted in this study, issues surrounding the IPv6 deployment in Zambia have been identified. Respondents felt that the demand for IPv6 services, the will power, roadmap and support from relevant Authorities and stakeholders is required in order to

expedite the migration from IPv4 to IPv6. This may include providing policy direction, IPv6 readiness assessment, guidelines and regulatory framework by government and ICT regulator. This study has also obtained the survey results indicating that most respondents are have deployed IPsec over MPLS on their networks using IPv4. From the simulation done using OPNET modeler, it can be seen that IPv6 can be deployed on these underlying protocols on the network. IPsec over MPLS networks is supported by both IPv4 and IPv6. IPv6 provides improved performance and response times for emails, more throughput for real time and database applications. This provides enhanced quality of service and experience for users. It can be concluded that due to its dependency on NAT and PAT, IPv4 experiences higher end to end delay and proving less efficient than IPv6. Additionally, IPv6 offers more security capabilities which would improve the overall security of the network.

In future, the study of IPsec could be extended software defined and cloud-based networks. With the current shift to cloud-based solutions, there is need to study the performance of IPsec and IPv6 on such networks.

References

[1] T. I. Society, "RFC4364 -BGP/MPLS IP Virtual Private Networks (VPNs)," February 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4364. [Accessed 20 April 2023].

[2] C. S. Inc., IPsec Configuration Guide, Cisco IOS XE 16 (Cisco ASR 920 Series), San Jose: Cisco Systems, 2020.

[3] G. S. E. C. (GSEC), "IPsec and MPLS (Even better together)," SANS Institute, Rockville Pike, 2023.

[4] C. K. Simatimbe and Smart Charles Lubobya, "Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network," Journal of Computer and Communications, vol. 8, pp. 100-108, 2020.

[5] Johnson, R., Williams and Thompson, G, "Scalability and Performance Analysis of MPLS Networks with IPsec.," in International Conference on Communications and Networking.

[6] A. Shahzad and Mureed Hussain, "IP Backbone Security: MPLS VPN Technology," International Journal of Future Generation Communication and Networking, vol. 6, no. 5, pp. 81-96, 2013.

[7] Fetus, " IP addresses allocated to Zambia," 2023. [Online]. Available: https://ipv4.fetus.jp/zm?_lang=en-US. [Accessed 24 August 2023].

[8] Emre Durdagi and Ali Buldu, "IPV4/IPV6 security and threat comparisons," Procedia Social and Behavioral Sciences, vol. 2, no. 2, pp. 5285-5291, 2010.

[9] A. P. N. I. Centre, Writer, IPv6 Capable Rate by country (%). [Performance]. APNIC, 2023.

[10] O. Systems, "IPv6 Addressing - System Administrator Guide," 2023. [Online]. Available: https://docs.oracle.com/cd/E19455-01/806-0916/6ja8539be/index.html#:~:text=IPv6%20has%20no%20broadcast%20addresses,of%20the%20IPv4%20address%20space... [Accessed 29 August 2023].

[11] D. A. CAMARERO, "Performance analysis of IPv4 / IPv6 protocols over the third-generation mobile network," Stockholm, Sweden, 2014.

[12] Mohd.Khairil Sailan, Rosilah Hassan and Ahmed Patel, "A Comparative Review of IPv4 and IPv6 for Research Test Bed," in International Conference on Electrical Engineering and Informatics, Selangor, Malaysia, 2009.

[13] Z. I. a. C. T. A. (ZICTA), "Corporate Strategy Plan 2022-2024," Lusaka, 2022.

[14] A. A. Mian and Sardar Usman Khalid, "Multi-Protocol Label Switching Traffic Engi-neering with QoS," Blekinge Institute of Technology, Sweden, 2010.