Journal of Theoretical and Applied Information Technology

15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PERFORMANCE AND SCALABILITY OF IPV4/IPV6 TRANSITION MECHANISMS FOR REAL-TIME APPLICATIONS

KHALID EL KHADIRI[1] , NAJIB EL KAMOUN[1], SAMIR EL OUAHAM[1], OUIDAD LABOUIDYA[1], KAWTAR SMAHI[1], RACHID HILAL[1]

[1]STIC Laboratory, Department of physics, Chouaïb Doukkali University, El Jadida, Morocco

E-mail: elkhadiri25@gmail.com, elkamoun.n@ucd.ac.ma, elouaham.s@ucd.ac.ma, labouidya.o@ucd.ac.ma, kawtarsmahi@gmail.com

ABSTRACT

To access the Internet, every device requires an IP address. However, the number of available IPv4 addresses is limited and insufficient to meet the growing demand for new addresses for a multitude of connected devices, including IoT devices and smartphones. In February 2011, the Internet Assigned Numbers Authority (IANA) announced the exhaustion of the /8 blocks of IPv4 addresses allocated to Regional Internet Registries (RIRs). Subsequently, the RIRs themselves exhausted their address reserves. Therefore, it is imperative to deploy the new version of the Internet Protocol, namely IPv6, which offers a significant expansion of the available address space. However, due to the incompatibility between IPv4 and IPv6, given their different headers, the transition from the old version (IPv4) to the new version (IPv6) cannot be achieved in a short period of time, requiring a gradual deployment. To address this challenge, three solutions are possible: a) Equip each device with a dual stack of IP addresses, b) Use tunneling to route IPv6 packets through the existing IPv4 network and c) Implement IP address translation, Among these options, tunneling is generally considered the most viable solution. However, it is worth noting that, like any technology, tunneling is influenced by potential scalability issues that need to be considered and managed to ensure a successful large-scale transition from IPv4 to IPv6. This article presents a comprehensive experimental study of the performance and scalability of IPv4 to IPv6 transition mechanisms. Our research is based on practical implementation in the GNS3 environment, where we increased the number of clients and explored various transition technologies to determine the most scalable solution. To evaluate these mechanisms, we used VoIP traffic generated through the IP SLA (Service Level Agreement) protocol. The evaluation criteria we considered include latency, jitter, the MOS (Mean Opinion Score), and packet loss rate. The results of this research are of great significance for network administrators as well as Internet Service Providers (ISPs). They provide valuable insights for IPv6 migration planning within networks, thereby enabling a more efficient and reliable transition to IPv6.

Keywords: *IPv6, Manual IPv6 tunnel, 6rd, GNS3,IP SLA, VoIP, Scalability*

1. INTRODUCTION

The connection between computing nodes requires a protocol so that each node is recognized, and the source and destination of each packet are known. IPv4, the fourth version of the Internet Protocol (IP), is widely used at present. IPv4 uses 32 bits and can only cover 4.3 billion nodes worldwide [1][2]. However, with the rapid growth of the Internet's size (number of users, Internet of Things, etc.), IPv4 has become limited, and some Internet Service Providers (ISPs) do not have enough IP addresses to meet customer demand. Therefore, it is necessary to deploy the new version of IP (IPv6) to keep up with the development pace of the Internet. IPv6, developed by the Internet Engineering Task Force (IETF), is considered more efficient than IPv4 in terms of scalability, reliability, speed, and security [3][4]. Additionally, the size of the IPv6 address space is larger than that of IPv4 because IPv6 uses 128 bits instead of IPv4's 32 bits. With this addressing capacity, IPv6 can encompass all nodes and services that may require IP, both now and in the future [5][6].

With the exponential growth of the Internet, including the increasing number of users and the expansion of the Internet of Things, IPv4 has proven to be insufficient. Some Internet Service Providers

(ISPs) now face constraints due to the shortage of IPv4 addresses to meet their customers' needs. Therefore, the deployment of the new version of the Internet Protocol, IPv6, has become essential to support the continued development of the Internet [7][8].

IPv6, developed by the Internet Engineering Task Force (IETF), offers numerous advantages over IPv4, including scalability, reliability, speed, and security [9][10]. Furthermore, the size of the IPv6 address space is significantly larger than that of IPv4, as IPv6 uses 128-bit addresses instead of IPv4's 32 bits. This increased addressing capacity enables IPv6 to support all nodes and services requiring an IP address, both currently and for future needs. Thus, IPv6 is not only an immediate solution to the IP address shortage but also a suitable response to the growing connectivity demands in the ever-evolving digital world [11][12]. However, the adoption of IPv6 has been gradually increasing in recent years. Figure 1 below represents the percentage of users who use and connect via IPv6 to Google [13].

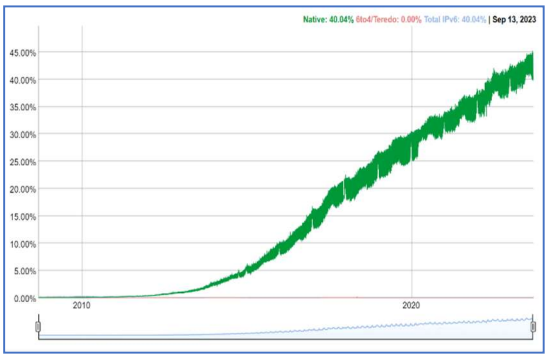


Figure 1: Percentage of users connecting to Google via IPv6

IPv4 and IPv6 are two versions of the Internet Protocol that exhibit a fundamental incompatibility, especially regarding the size and format of IP addresses [14][15]. This incompatibility necessitates a gradual and step-by-step transition from IPv4 to IPv6. To facilitate this transition, the Internet Engineering Task Force (IETF) has established various mechanisms (Dual-Stack, Tunneling, and Translation), each with its own distinctive characteristics.

Tunneling mechanisms play a crucial role in the transition phase from IPv4 to IPv6. During this period of coexistence of both protocols, tunneling mechanisms enable seamless connections between IPv4 and IPv6 networks. They facilitate the transition by encapsulating IPv6 packets within IPv4 packets to traverse existing network infrastructures based on IPv4. This approach allows organizations to migrate gradually to IPv6 without disrupting their existing IPv4 connectivity [16][17].

However, the scalability of tunneling mechanisms is a major concern as more and more nodes and networks adopt IPv6. The higher the number of IPv6 clients and applications, the heavier the load on tunneling mechanisms becomes. This increased load can lead to management, performance, and security issues. Many studies have been conducted in this context to propose and evaluate the performance of various tunneling mechanisms, aiming to select the optimal solution. However, few studies have delved into the impact of scalability on the performance of these mechanisms. It becomes crucial, therefore, to undertake a thorough analysis of the scalability of these mechanisms. Such a study will help understand how these mechanisms respond to an increase in IPv6 traffic, identify their limits and constraints in terms of scalability, and determine how to optimize them to ensure a smooth and efficient transition to IPv6, even with the ongoing growth in the number of IPv6 clients and applications.

This article presents an experimental study under GNS3 of the performance and scalability of two tunneling mechanisms, namely manual IPv6 tunnel and automatic 6rd tunnel. This study will be conducted within a test network infrastructure configured in the GNS3 environment. Our approach involves increasing voice traffic by adding more clients engaging in VoIP communication, while exploring various technologies to identify the optimal solution. Performance indicators used in this study include latency, jitter, MOS score, and packet loss rate.

The rest of the document is structured as follows: In Section 2, we conduct a non-exhaustive literature review in this field. Section 3 provides an overview of IPv4/IPv6 transition techniques and categorizes them into relevant categories. The experimental study scenarios are detailed in Section 4. Section 5 is dedicated to presenting the results and making a comparative analysis of the examined technologies, along with a discussion of their scalability. Finally, the conclusions and future perspectives are outlined in the final section of this document.

2. LITERATURE REVIEW

The problem of transitioning to IPv6 is a major challenge in the field of computer networks. This challenge primarily arises from the impending exhaustion of available IPv4 addresses, which have become insufficient to accommodate the exponential growth of connected devices and the need to

transition to the new protocol version, IPv6, which offers a significantly larger address space [18] [19].

Many research studies have proposed various techniques, but the efficiency and performance of these methods remain a major challenge. Another study examines several IPv6 transition mechanisms within the Multiprotocol Label Switching (MPLS) network to evaluate and compare their performance. According to simulation results, ISATAP is the best choice due to its high performance in terms of high throughput and low packet jitter during data transmission [20]. The 6to4 and manual tunneling mechanisms were configured simultaneously with the RIPng (Routing Information Protocol next generation) and OSPFv3 (Open Shortest Path First version 3) routing protocols using Riverbed Modeler Academic Edition 17.5 in [21]. Performance was compared using real-time applications such as FTP and Email for different criteria including queue delay, throughput for incoming and outgoing traffic, packet loss, network convergence time, and sent traffic. The results obtained indicate that the 6to4 tunneling technique outperforms the manual tunneling technique. In the majority of observed cases, the OSPF 6to4 network performs better than other scenarios. Additionally, the studies [22] and [23] provide a performance evaluation of three IPv4/IPv6 transition mechanisms (dual-stack, manual tunnel, and automatic 6to4 tunnel). These performances were assessed using two real-time applications, namely VoIP and video conferencing, taking into account five simulation parameters: delay, delay variation, jitter, MOS (Mean Opinion Score), and packet loss. The results obtained showed that the dual-stack technique performed better compared to tunneling mechanisms. In 2022, Al-Azzawi and Lencse set up a test environment to explore two IPv6 transition technologies: Lightweight 4over6 and Dual Stack Lite. The implementation of each transition technology was facilitated by using four virtual machines. This testbed was created to establish benchmark measurements, enabling a performance comparison between two IP tunnel-based transition technologies: Dual Stack Lite, as a stateful mechanism, and Lightweight 4over6, as a stateless mechanism [24].

While IPv6 incorporates security improvements over IPv4, it can still be vulnerable to certain attacks, particularly Distributed Denial of Service (DDoS) attacks carried out through ICMPv6 messages. In [25], AIghuraibawi and colleagues proposed a method for detecting ICMPv6 DDoS attacks using a modified Flower Pollination Algorithm (MFPA). The results obtained show that the proposed method (MFPA) achieved higher accuracy. In 2022, Al-Azzawi and Lencse aimed to build a testbed for one of the most important IPv6 transition technologies (464XLAT) and examined its security analysis. The setup of the testbed was explained in detail, and its operation was illustrated through an example Denial of Service (DoS) attack scenario implemented using the hping3 command. Additionally, adjustments were made to the testbed to highlight vulnerabilities in the 464XLAT technology. As a result, the presented testbed proved to be an effective and convenient tool for the security analysis of the IPv6 transition technology 464XLAT, demonstrating highly promising performance by simulating the actual packet path through the double translation mechanism. Therefore, the main conclusion that can be drawn from this testbed is that it could also be applied to other technologies (not just 464XLAT) [26]. Subsequently, in 2023, the same researchers conducted a security risk analysis for the IPv6 transition technology DS-Lite (Dual-Stack Lite), based on the STRIDE method, which encompasses aspects of Spoofing, Tampering, Repudiation, Information Disclosure, and Elevation of Privilege. To achieve this, a test environment was developed for the DS-Lite topology using multiple virtual machines based on CentOS Linux images. This testing framework was used to carry out various forms of attacks against the DS-Lite infrastructure, with particular attention to the B4 (Basic Bridging Broadband) and AFTR (Address Family Transition Router) components, demonstrating that it is possible to deplete the source port pool in just 14 seconds. The conclusions of this study demonstrate that, in the DS-Lite topology, the IPv4 client does not require a public IPv4 address to establish communication with an IPv4 server. However, each component of this DS-Lite topology is vulnerable to various types of attacks, including denial of service attacks, tampering, and spoofing. Therefore, it is imperative to conduct further analysis and address these vulnerabilities to ensure the successful implementation of IPv6 transition technologies using tunneling [27].

The study of IPv6 routing is essential for a successful transition to IPv6. Indeed, IPv6 routing was examined in [28]. The dynamic IPv6 routing protocols were studied, presenting the principles of operation, routing algorithms, and deployment limitations for each of them in [29]. The performance of IS-ISv6 routing was evaluated through two real-time applications: voice and video in [30]. The results showed that the IS-ISv6 routing protocol improves the throughput of video applications in the IPv6 network. However, average performance was

achieved for the voice application, with reduced end-to-end delay and packet delay variations. Furthermore, an analysis of the impact of routing protocols (RIPv2/RIPng, OSPFv2/OSPFv3, and IS-IS) on the performance of IPv4/IPv6 transition mechanisms (dual-stack, manual tunneling, and automatic 6to4 tunneling) was conducted for a real-time video conferencing application in [31]. This analysis was carried out on three essential measurement parameters: delay, delay variation, and packet loss. The results showed that the performance of these mechanisms was significantly better when associated with the IS-IS routing protocol compared to the other routing protocols examined.

According to the above study, it has been observed that many researchers have focused on security in IPv4/IPv6 transition environments. Concurrently, research has been conducted on IPv6 routing, shedding light on various IPv6 routing protocols and their impact on the performance of certain transition techniques.

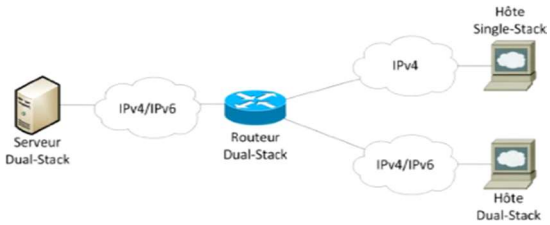
Furthermore, the performance evaluation of various tunneling mechanisms has been at the core of numerous studies, providing a better understanding of their effectiveness and limitations in real-world scenarios. These evaluations have covered various performance parameters. However, the aspect of scalability of tunneling mechanisms has not been addressed in these studies. We note that an analysis of the scalability of these mechanisms is of great importance as it helps determine to what extent a tunneling mechanism can withstand an increase in load (number of IPv6 clients or applications) on the network. This article presents a study of performance and scalability of tunneling mechanisms by increasing the number of VoIP clients and varying different technologies to determine the optimal solution. We will measure performance using VoIP traffic generated by IP SLA. Evaluation parameters include latency, latency variation, MOS (Mean Opinion Score), and packet loss rate.

3. IPV4/IPV6 TRANSITION MECHANISMS

IPv4/IPv6 transition mechanisms are of crucial importance in the evolution of computer networks. They represent a set of techniques and strategic approaches aimed at enabling a gradual transition from IPv4 to IPv6 while preserving connectivity between these two fundamental Internet protocols. These mechanisms are carefully classified into three main families, with each family having its own distinctive implementation method [32][33] :

3.1 Dual-Stack

Within this family, the strategy involves simultaneously enabling IPv4 and IPv6 on devices, networks, and applications in a way that they operate side by side, as illustrated in Figure 2 below. This

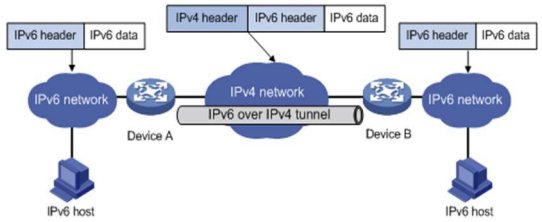


creates a harmonious coexistence of both protocols, allowing users to gradually transition to IPv6 while maintaining their existing IPv4 connectivity intact. Dual-Stack mechanisms are an essential means to ensure a smooth transition [34][35].

Figure 2: Dual-Stack

3.2 Tunneling

This technique is implemented when two hosts or sites use the same version of the IP protocol but are separated by an intermediate network using a different IP version [36][37]. Tunneling encapsulates IPv6 packets within IPv4 packets to transmit them over an existing IPv4 network, as illustrated in figure 3 below. This allows IPv6 networks to traverse IPv4 segments. Tunneling techniques are generally categorized into two distinct categories: automatic tunnels and manual tunnels. Manual tunnels involve manual configuration, with predefined tunnel endpoints. In contrast, automatic tunneling does not require manual configuration or endpoint specification [38][39]. Here are some examples of tunneling



techniques that can be implemented to carry IPv6 traffic over IPv4 networks:

Figure 3: Tunneling

3.2.1 Manual IPv6 tunnel

A manual IPv6 tunnel is a tunnel configuration where the tunnel parameters and endpoints need to be manually defined by a network administrator. Unlike automatic tunnels, which can be configured dynamically without human intervention, manual tunnels require direct intervention to specify tunnel details [40][41].

In a manual tunnel, the administrator must determine the IP addresses of the tunnel endpoints, the tunneling protocols to use, as well as other tunnel-related parameters, such as security options and routing mechanisms [42].

3.2.2 6rd (IPv6 Rapid Deployment)

6rd is a transition technique adopted by some service providers to facilitate a quick implementation of IPv6 for their customers who want to use IPv6 on an infrastructure already established in IPv4. 6rd is designed to simplify the transition from IPv4 to IPv6 by leveraging existing IPv4 addressing and automating the tunnel configuration process [43][44].

The 6rd mechanism has adopted the operational principles of the 6to4 protocol, but it has made improvements by addressing the shortcomings of the latter. Unlike 6to4, which uses a single prefix (2002::/16), 6rd assigns a distinct prefix to each Internet Service Provider (ISP). Additionally, 6rd replaces 6to4 routers with 6rd routers, and the relay router with a Border Relay (BR) router accessible via the anycast IPv4 address 10.1.1.1[45]. Various tunneling methods can be employed, including 6to4 [46], Teredo [47], Broker [48], and others.

3.3 Translation

This method is used to establish connections between hosts or sites using different versions of the IP protocol. It involves the use of a device located at the border between an IPv4 network and an IPv6 network, enabling communication between IPv4 nodes in an IPv4 network and IPv6 nodes in an IPv6 network. This device performs header translation (IPv4 to IPv6 and vice versa) based on source and destination addresses, as illustrated in Figure 4 below. It allows IPv6 networks to communicate with IPv4 networks without requiring dual-stack on all devices [49][50]. Translation mechanisms include:

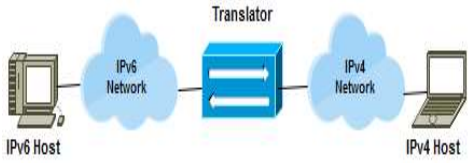


Figure 4: IPv4/IPv6 Translator

3.3.1 NAT-PT (Network Address Translation-Protocol Translation)

NAT-PT is another translation mechanism that facilitates communication between IPv6 and IPv4 nodes. NAT-PT maintains a global pool of routable IPv4 addresses and assigns IPv4 addresses to IPv6 nodes, and vice versa. This works similarly to traditional IPv4 NAT (Network Address Translation). NAT-PT can also be used in conjunction with DNS-PT, which enables automatic resolution of IPv4 names to IPv6 and vice versa [51][52].

NAT-PT can be complemented by DNS-PT (DNS Protocol Translation). DNS-PT plays a crucial role in enabling automatic resolution of domain names between IPv4 and IPv6 formats. In other words, it automatically converts IPv4 domain names to IPv6 addresses and vice versa, thus facilitating seamless communication between nodes of both protocols [53][54].

3.3.2 TRT (Transport Relay Translator)

The TRT mechanism provides a solution operating at the transport layer in the TCP/IP model. Its primary purpose is to facilitate the exchange of TCP traffic between IPv6 hosts and IPv4 hosts by performing protocol conversion from IPv6 TCP to IPv4 TCP, and vice versa. Similarly, TRT also manages UDP traffic in the same manner. This mechanism can be deployed on hosts with dual-stack IPv4/IPv6 or on routers [55][56].

When an IPv6 host wants to communicate with an IPv4 host (or vice versa), the TRT mechanism steps in to ensure seamless translation of traffic between the two protocols. This translation operation at the transport layer enables applications and services to work smoothly without being concerned about the differences in underlying protocols [57]. A range of translation methods is available, including NAT64/DNS64[58], SIIT[59], BIS[60], and others.

4. EXPERIMENTAL FRAMEWORK

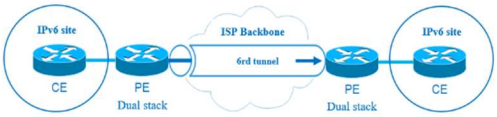
4.1 Network Testbed

In this section, we will examine the scalability of two tunneling mechanisms: manual IPv6 tunneling and 6rd. To conduct this study, we used the GNS3 (Graphical Network Simulator) [61] tool to create a network testbed project. Using the same network testbed, we configured two scenarios for each of the technologies: manual IPv6 tunneling and 6rd, as illustrated in Figures 5 and 6 below. As background traffic, we chose VoIP traffic. To generate this traffic and assess the link and application quality, we used IP SLA [62], a Cisco method for generating test traffic between various network devices, such as routers or switches. This method has the advantage of not requiring the installation of additional equipment or the development of new software or protocols. The objective of this study is to enable the two IPv6 sites to communicate with each other through the IPv4 backbone using both tunneling

technologies while measuring their scalability by increasing the load in terms of the number of clients communicating via VoIP.

Figure 5: Network testbed – Manual IPv6 tunnel
Figure 6 : Network testbed –6rd tunnel

From this project, we generated 68 distinct scenarios. For each technology (manual IPv6 tunnel



and 6rd), we gradually increased the number of clients participating in VoIP communications, ranging from 2 to 90 clients. In the provider's infrastructure, we used GigabitEthernet technology (1000MB) for the core network, while the

Scenarios	ISP Backbone	PE & CE connections	ISP Backbone connections
Manual IPv6 tunnel	IPv4	FastEthernet (10MB)	GigabitEthernet (1000MB)
6rd	IPv4	FastEthernet (10MB)	GigabitEthernet (1000MB)

connection between client sites and the provider's borders was established using FastEthernet technology (10MB). Configuration details are provided in Tables 1, 2, 3, and 4 below.

Table 1: Characteristics of the connection technologies used for each scenario

Table 2: Addressing used for each scenario

Addressing		
Scenarios	ISP Backbone	IPv6 Sites
Manual IPv6 tunnel	Addressing IPv4	Addressing IPv6
6rd	Addressing IPv4	Addressing IPv6

Table 3: Routing used for each scenario

Routing		
Scenarios	ISP Backbone	IPv6 Sites
Manual IPv6 tunnel	RIPv2	RIPng
6rd	RIPv2	RIPng

4.2 Traffic and Measurement Parameters

The following table, Table IV, represents the

Traffic criteria	
Used traffic	VoIP
Used codec	G729
Number of packets	1000 packets
Interval between packets	20 milliseconds

criteria for VoIP traffic generated by the IP SLA tool.

Table 4: VOIP traffic criteria

Performance measurement criteria	
Latency	Latency: This term refers to the time it takes for a packet, from its creation at the source, to travel through the network to its final reception at the destination, thus measuring the entire end-to-end transmission duration.
Jitter	Jitter: It is defined as the variation in end-to-end transmission delays between packets within the same data stream, regardless of potential packet loss. This parameter is of great importance for voice applications, as variations in transmission delay during a VoIP conversation can lead to a deterioration in audio quality. An ideal jitter approaches as close to zero as possible.
MOS Score	MOS Score: Abbreviation for Mean Opinion Score. This indicator is of great importance in evaluating the quality of a voice application. It is on a scale from 0 to 5, where 5 represents excellent quality and 1 indicates poor quality. The MOS score depends on the codec used; for example, in the case of the G.729 codec (our example), the MOS score reaches 4.06 (under ideal conditions).
Packet Loss Rate	Packet Loss Rate: This parameter is expressed as a percentage and represents the number of packets lost compared to the total number of packets sent. It is a crucial measure for evaluating the reliability of a network or communication. In other words, it indicates what proportion of the packets sent did not reach their intended destination.

The performance evaluation criteria considered in this study include:

Table 5. Performance measurement criteria

5. RESULTS AND DISCUSSION

5.1 Results Analysis

5.1.1 Latency

The results displayed in the figure 7 below provide latency measurements, expressed in milliseconds,

for each of the evaluated technologies: Manual IPv6 Tunnel and 6rd. These latency values are crucial for assessing the performance and efficiency of these communication mechanisms.

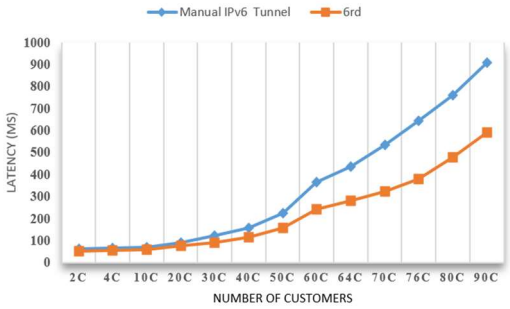


Figure 7: Latency

5.1.2 Jitter

Figure 8 below represents the results related to jitter. Upon initial analysis, it is noticeable that the jitter variation follows a similar trend to that of latency but with different values. Indeed, as the VoIP load increases (meaning the number of clients communicating via VoIP), the results highlight that the automatic tunnel 6rd outperforms the manual IPv6 tunnel, recording lower jitter values compared to the latter.

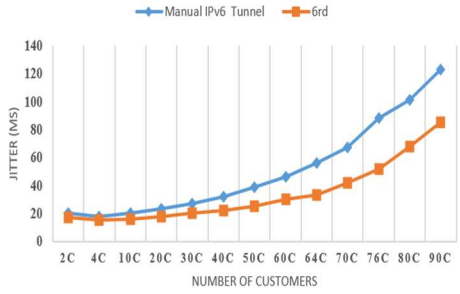


Figure 8: Jitter

5.1.3 Packet loss rate

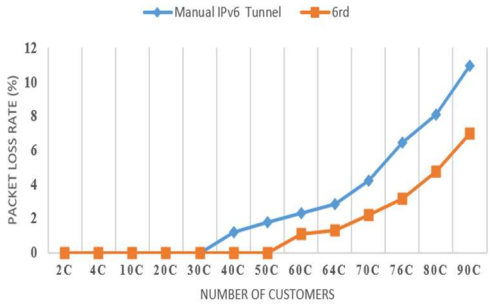


Figure 9: Packet loss rate

The Figure 9 presented above shows the results regarding packet loss rate. According to this representation, it is possible to observe that as the VoIP load increases, the results indicate that the packet loss rate of the automatic 6rd tunnel is lower than that of the manual IPv6 tunnel because 6rd has better packet management as the load increases, resulting in a lower packet loss rate compared to the manual IPv6 tunnel. Furthermore, the capacity of the 6rd tunnel is substantial. The 6rd tunnel could be designed to effectively handle a large number of packets under high load, minimizing losses.

5.1.4 MOS score

The results shown in Figure 10 below illustrate the Mean Opinion Score (MOS) associated with the examined technologies. A higher MOS score indicates better voice quality performance. The results revealed by this figure suggest that the automatic 6rd tunnel offers superior voice quality compared to the manual IPv6 tunnel.

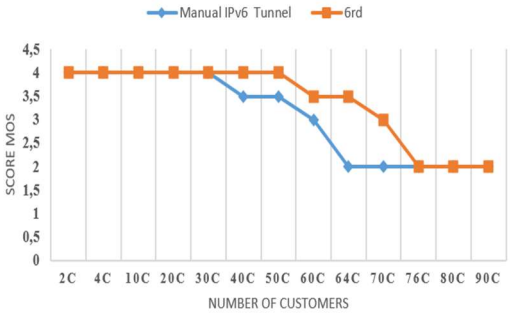


Figure 10: MOS score

5.2 Scalability discussion

During this study conducted using the GNS3 tool, we examined the scalability of two tunneling technologies, namely the manual IPv6 tunnel and the automatic 6rd tunnel. Each of these technologies was subjected to 68 distinct scenarios, with an increase in the number of VoIP clients communicating from 2 to 90 clients. To evaluate performance, we used VoIP traffic generated by IP SLA, focusing on four essential measurement parameters: latency, jitter, MOS score, and packet loss rate.

According to our results, the automatic 6rd tunnel outperforms the manual IPv6 tunnel for all evaluated measurement parameters when increasing VoIP load in terms of the number of VoIP clients communicating. This can be attributed to the strategy adopted by the 6rd tunnel. In general, the automatic 6rd tunnel significantly automates the process, simplifying configuration and management compared to the manual IPv6 tunnel. Thus, 6rd reduces administrative overhead by allowing for a more global and automated configuration, avoiding the tedious individual configuration associated with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the manual IPv6 tunnel as the number of clients increases. Additionally, 6rd exhibits intrinsic scalability, designed to expand easily as the number of IPv6 clients grows.

To assess the scalability or scaling capability of the technologies studied, it is now necessary to simultaneously consider acceptable thresholds for latency (400 ms), jitter (50 ms), and packet loss rate (3%) to determine which technology will withstand the increase in load in terms of the number of VoIP clients communicating.

We observe that:

- The manual IPv6 tunnel, although it maintains an acceptable packet loss rate of 2.82% in the scenario with 64 clients, experiences a delay of 436 ms in the same scenario. Therefore, it appears that the manual IPv6 tunnel cannot effectively route VoIP traffic from this scenario.
- The automatic 6rd tunnel maintains an acceptable delay until the scenario with 76 clients, with approximately 379 ms. However, in the same scenario, the packet loss rate reaches 3.14%, making VoIP unusable from that point onwards.

To summarize, Figure 11 below provides a comprehensive assessment of the scalability of the examined technologies, namely the manual IPv6 tunnel and the automatic 6rd tunnel, based on the number of clients communicating via VoIP, considering three crucial parameters: latency, jitter, and packet loss. This overall analysis allows us to better understand how these technologies perform under increasing load, evaluating their ability to maintain acceptable performance while accounting for these critical quality of service factors. Based on these results, it is clear that the automatic 6rd tunnel offers superior scalability compared to the manual IPv6 tunnel.

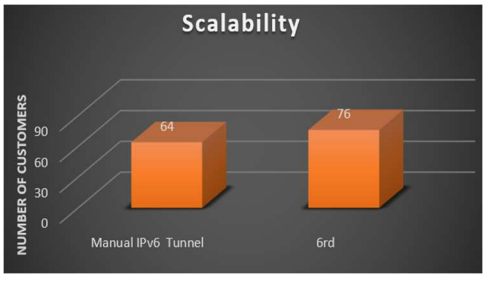


Figure 11. Scalability

6. CONCLUSION AND FUTURE WORK

In this article, we have studied and measured the performance and scalability of tunneling mechanisms, namely the manual IPv6 tunnel and the automatic 6rd tunnel, by increasing the voice load in terms of the number of clients communicating via VoIP. The study was conducted using GNS3 based on four measurement parameters: latency, jitter, MOS score, and packet loss rate. The results have shown that the automatic 6rd tunnel is more scalable than the manual tunneling mechanism. Consequently, it outperformed the manual tunneling mechanism in all measurement parameters.

The main objective was to test which tunneling technique performs better in terms of performance and scalability as the load increases on the network in terms of the number of clients communicating via VoIP. The future research perspectives could encompass the security aspect of these tunneling techniques to identify their vulnerabilities and address them. This work could be beneficial for network administrators, policymakers, and researchers aiming to enhance the security of their networks and prevent attacks.

REFERENCES:

[1] Kalita, A., & Khatua, M. (2022). 6tisch–ipv6 enabled open stack iot network formation: A review. ACM Transactions on Internet of Things, 3(3), 1-36.

[2] Aguilar, S., Vidal, R., & Gomez, C. (2023). IPv6 over Cross-Technology Communication with Wake-up Radio. Internet of Things, 22, 100804.

[3] Abdullah, S. A., & Al Ashoor, A. A. (2022). IPv6 Security Issues: A Systematic Review Following PRISMA Guidelines. Baghdad Science Journal, 19(6 (Suppl.)), 1430-1430.

[4] Zhang, C., & Xie, G. (2022). Using XorOffsetTrie for high-performance IPv6 lookup in the backbone network. Computer Communications, 181, 438-445.

[5] Hussain, I., & Bashir, J. (2022). Dynamic MTU: A smaller path MTU size technique to reduce packet drops in IPv6. Journal of King Saud University-Computer and Information Sciences, 34(9), 7070-7088.

[6] M. R. A. Ahmed et S. S. A. Shaikhedris, « Network migration and performance analysis of IPv4 and IPv6 », in 2020 International Conference on Computer, Control, Electrical,

and Electronics Engineering (ICCCEEE), IEEE, 2021, p. 1-6.

[7] Nikolina, K. (2022, May). Overview of the progress of IPv6 adoption in Croatia. In 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 405-408). IEEE.

[8] L. Mamushiane, T. Shozi, et L. MANQELE, « IPv6 Adoption in South Africa: Barriers, Benefits and Government Intervention », in 2021 IST-Africa Conference (IST-Africa), IEEE, 2021, p. 1-10.

[9] Kim, C. M., Lim, S. K., Jeong, J. D., Choi, Y., & Koh, S. J. (2022). 6LoWPAN over optical wireless communications for IPv6 transport in Internet of Things networks. IEEE Wireless Communications Letters, 11(6), 1142-1145.

[10] M. A. Khan, K. Mahmood, et A. M. Shah, « Analysis of IPv4 vs IPv6 Traffic in US », International Journal of Advanced Computer Science and Applications, vol. 7, no 12, 2016.

[11] Hou, B., Cai, Z., Wu, K., Yang, T., & Zhou, T. (2023). 6Scan: A High-Efficiency Dynamic Internet-Wide IPv6 Scanner With Regional Encoding. IEEE/ACM Transactions on Networking.

[12] Hong, Q., Jie, Y., Yingjiao, Z., Yang, S., & Guihua, Z. (2020, July). IPv6 Based Intelligent Monitoring System for industrial instruments. In 2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS) (pp. 691-695). IEEE.

[13] Google's IPv6 Statistics, https://www.google.com/intl/en/ipv6/statistics.html. Consulted on 13/09/2923.

[14] S. Dasgupta, P. J. Roy, N. Sharma, et D. D. Misra, « Application of IPv4, IPv6 and dual stack interface over 802.11 ac, 802.11 n and 802.11 g wireless standards », in 2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC), IEEE, 2020, p. 1-6.

[15] Liu, R., Weng, Z., Hao, S., Chang, D., Bao, C., & Li, X. (2020). Addressless: enhancing IoT server security using IPv6. IEEE Access, 8, 90294-90315.

[16] S. Dasgupta, P. J. Roy, N. Sharma, et D. D. Misra, « Application of IPv4, IPv6 and dual stack interface over 802.11 ac, 802.11 n and 802.11 g wireless standards », in 2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC), IEEE, 2020, p. 1-6.

[17] Khan, H. U., Hussain, A., Nazir, S., Ali, F., Khan, M. Z., & Ullah, I. (2023). A Service-Efficient Proxy Mobile IPv6 Extension for IoT Domain. Information, 14(8), 459.

[18] Han, Y., Zhang, L., Wang, Y., Deng, X., Gu, Z., & Zhang, X. (2023). Research on the Security of IPv6 Communication Based on Petri Net under IoT. Sensors, 23(11), 5192.

[19] M. R. Uddin, N. A. Evan, M. R. Alam, et M. T. Arefin, « Analysis of Generic Routing Encapsulation (GRE) over IP Security (IPSec) VPN Tunneling in IPv6 Network », in Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings, Springer, 2021, p. 3-15.

[20] J. Kristoff, M. Ghasemisharif, C. Kanich, et J. Polakis, « Plight at the End of the Tunnel: Legacy IPv6 Transition Mechanisms in the Wild », in Passive and Active Measurement: 22nd International Conference, PAM 2021, Virtual Event, March 29–April 1, 2021, Proceedings 22, Springer, 2021, p. 390-405.

[21] M. M. Alhassoun et S. R. Alghunaim, « A Survey of IPv6 Deployment », International Journal of Advanced Computer Science and Applications, vol. 7, no 9, 2016.

[22] A. K. Babar, Z. A. Zardari, S. H. Sirajuddin Qureshi, et N. N. Hussaini, « Assessment of IPv4 and IPv6 networks with different modified tunneling techniques using OPNET », International Journal of Advanced Computer Science and Applications (IJACSA), vol. 10, no 9, 2019.

[23] N. Jain et A. Payal, « Performance Comparison Between Different Tunneling Techniques Using Different Routing Protocols », Wireless Personal Communications, vol. 123, no 2, p. 1395-1441, 2022.

[24] K. El Khadiri, O. Labouidya, N. Elkamoun, et R. Hilal, « Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler », International Journal of Advanced Computer Science and Applications, vol. 9, no 4, 2018.

[25] K. El Khadiri, O. Labouidya, N. Elkamoun, et R. Hilal, « Performance analysis of video conferencing over various IPv4/IPv6 transition mechanisms », IJCSNS, vol. 18, no 7, p. 83-88, 2018.

[26] O. D'yab et G. Lencse, « Testbed for the Comparative Analysis of DS-Lite and Lightweight 4over6 IPv6 Transition

Technologies », in 2022 45th International Conference on Telecommunications and Signal Processing (TSP), IEEE, 2022, p. 371-376.

[27] A. H. B. AIghuraibawi, S. Manickam, R. Abdullah, Z. A. A. Alyasseri, H. M. Jasim, et N. S. Sani, « Modified Flower Pollination Algorithm for ICMPv6-Based DDoS Attacks Anomaly Detection », Procedia Computer Science, vol. 220, p. 776-781, 2023.

[28] A. Al-Azzawi et G. Lencse, « Testbed for the Security Analysis of the 464XLAT IPv6 Transition Technology in a Virtual Environment », in 2021 44th International Conference on Telecommunications and Signal Processing (TSP), IEEE, 2021, p. 5-9.

[29] A. Al-Azzawi et G. Lencse, « Analysis of the Security Challenges Facing the DS-Lite IPv6 Transition Technology », Electronics, vol. 12, no 10, p. 2335, 2023.

[30] M. A. Sadat, « Lab Implementation of IPv6 in Enterprise NetworkUsing Cisco Packet Tracer », Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no 10, p. 6564-6580, 2021.

[31] K. EL KHADIRI, O. Labouidya, N. Elkamoun, et R. Hilal, « Comparative Study Between Dynamic IPv6 Routing Protocols of Distance Vectors and Link States », in 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, 2018, p. 1-6.

[32] N. Jain et A. Payal, « Performance evaluation of IPv6 network for real-time applications using IS-ISv6 routing protocol on Riverbed Modeler », Procedia Computer Science, vol. 173, p. 46-55, 2020.

[33] Sisinni, E., Fernandes Carvalho, D., Depari, A., Bellagente, P., Flammini, A., Pasetti, M., ... & Ferrari, P. (2023). Assessing a Methodology for Evaluating the Latency of IPv6 with SCHC Compression in LoRaWAN Deployments. Sensors, 23(5), 2407.

[34] K. El Khadiri, O. Labouidya, N. E. Kamoun, et R. Hilal, « Study of the impact of routing on the performance of IPv4/IPv6 transition mechanisms », in Smart Data and Computational Intelligence: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-18) Held on October 17–18, 2018 in Mohammedia 3, Springer, 2019, p. 43-51.

[35] Sun, Z., Ruan, H., Cao, Y., Chen, Y., & Wang, X. (2022). Analysis and Prediction of the IPv6 Traffic over Campus Networks in Shanghai. Future Internet, 14(12), 353.

[36] G. Lencse et Y. Kadobayashi, « Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis », IEICE Transactions on Communications, vol. 102, no 10, p. 2021-2035, 2019.

[37] Wang, M., & Yang, D. (2021, March). IPv6 Address Assignment and Management Mechanism for Heterogeneous Industrial Networks. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 2116-2121). IEEE.

[38] Mansour, M., Agomati, M., Alsaid, M., & Alasem, R. (2022). Performance Analysis and Functionality Comparison of First Hop Redundancy Protocol IPV6. Procedia Computer Science, 210, 19-27.

[39] Deac, D., Teshome, E., Van Glabbeek, R., Dobrota, V., Braeken, A., & Steenhaut, K. (2022). Traffic Aware Scheduler for Time-Slotted Channel-Hopping-Based IPv6 Wireless Sensor Networks. Sensors, 22(17), 6397.

[40] S. Kalwar, N. Bohra, et A. A. Memon, « A survey of transition mechanisms from IPv4 to IPv6—Simulated test bed and analysis », in 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC), IEEE, 2015, p. 30-34.

[41] Liu, Z., Fu, L., Pan, M., & Zhao, Z. (2022). Lightweight Path Recovery in IPv6 Internet-of-Things Systems. Electronics, 11(8), 1220.

[42] Wang, Z., & Cui, B. (2020, July). An Enhanced System for Smart Home in IPv6-Based Wireless Home Network. In 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 119-122). IEEE.

[43] A. Jain, M. Singh, et P. Bhambri, « Performance evaluation of IPv4-IPv6 tunneling procedure using IoT », in Journal of Physics: Conference Series, IOP Publishing, 2021, p. 012010.

[44] Li, K. H., & Wong, K. Y. (2021). Empirical analysis of IPv4 and IPv6 networks through dual-stack sites. Information, 12(6), 246.

[45] Wang, K., Tong, M., Yang, D., & Liu, Y. (2020). A web-based honeypot in IPv6 to enhance security. Information, 11(9), 440.

[46] N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong, R. Elz, et P. Pongpaibool, « Performance evaluation of IPv4/IPv6 transition

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mechanisms: IPv4-in-IPv6 tunneling techniques », in The International Conference on Information Networking 2014 (ICOIN2014), IEEE, 2014, p. 238-243.

[47] Z. A. Zardari, M. Ali, R. A. Shah, et L. H. Zardari, « A hybrid technique for tunneling mechanism of IPv6 using Teredo and 6RD to enhance the network performance », International Journal of Advanced Computer Science and Applications, vol. 9, no 11, p. 100-105, 2018.

[48] Khalaf, O. I., & Abdulsahib, G. M. (2021). Design and Performance Analysis of Wireless IPv6 for Data Exchange. Journal of Information Science & Engineering, 37(6).

[49] K. EL KHADIRI et O. LABOUIDYA, « Etude comparative des mécanismes de transition de l'IPv4 à l'IPv6 », Revue Méditerranéenne des Télécommunications, vol. 7, no 1, 2017.

[50] Lucas, T., Ferreira, M., Plachta, R., Ferreira, G., & Costa, K. (2020). Non-Fragmented Network Flow Design Analysis: Comparison IPv4 with IPv6 Using Path MTU Discovery. Computers, 9(2), 54.

[51] R. Munadi, D. D. Sanjoyo, D. Perdana, et F. Adjie, « Performance analysis of tunnel broker through open virtual private network », TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no 3, p. 1185-1192, 2019.

[52] Ordabayeva, G. K., Othman, M., Kirgizbayeva, B., Iztaev, Z. D., & Bayegizova, A. (2020, September). A systematic review of transition from IPV4 To IPV6. In Proceedings of the 6th International Conference on Engineering & MIS 2020 (pp. 1-15).

[53] R. Tadayoni et A. Henten, « From IPv4 to IPv6: lost in translation? », Telematics and Informatics, vol. 33, no 2, p. 650-659, 2016.

[54] Ibhaze, A. E., Okoyeigbo, O., Samson, U. A., Obba, P., & Okakwu, I. K. (2020). Performance evaluation of IPv6 and IPv4 for future technologies. In Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 1 (pp. 15-22). Springer International Publishing.

[55] Jain, A., Singh, M., & Bhambri, P. (2021, August). Performance evaluation of IPv4-IPv6 tunneling procedure using IoT. In Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012010). IOP Publishing.

[56] A. A. Khudher, A. Munther, et S. Praptodiyono, « Efficient IPv4-IPv6 translation mechanism for IMS using SIP proxy », International Journal of Internet Protocol Technology, vol. 15, no 1, p. 41-52, 2022.

[57] M. Hunek et Z. Pliva, « DNSSEC in the networks with a NAT64/DNS64 », in 2018 International Conference on Applied Electronics (AE), IEEE, 2018, p. 1-4.

[58] Tomar, S. S., Rawat, A., Vyavahare, P. D., & Tokekar, S. (2020). Conceptual model for comparison of IPv6 ISPs based on IPv4 traffic profiles. International Journal of Information Technology, 12, 1171-1182.

[59] G. Lencse et K. Shima, « Performance analysis of SIIT implementations: Testing and improving the methodology », Computer Communications, vol. 156, p. 54-67, 2020.

[60] K. Tsuchiya, H. Higuchi, et Y. Atarashi, « Dual stack hosts using the" bump-in-the-stack" technique (BIS) », 2000.

[61] J. C. Neumann, The book of GNS3: build virtual network labs using Cisco, Juniper, and more. No Starch Press, 2015.

[62] D. Teare, B. Vachon, et R. Graziani, Implementing Cisco IP routing (ROUTE) foundation learning guide:(CCNP ROUTE 300-101). Cisco Press, 2014.