DISCLOSING THE IPV6 ACCEPTANCE BRIDGE: A COMPREHENSIVE REVIEW

Subrahmanya Ganiga
Dept.Computer Science and Engineering (Alvas Institute of Engineering and Technology)
Alvas Institute of Engineering and Technology*(Student)*
Moodbidri,India
subrahmanyaganigacse@gmail.com

Sudarshan Shetty
Dept.Computer Science and Engineering (Alvas Institute of Engineering and Technology)
Alvas Institute of Engineering and Technology*(Student)*
Moodbidri,India
sudarshanshetty2563@gmail.com

Sriram Prasad M
Dept.Computer Science and Engineering (Alvas Institute of Engineering and Technology)
Alvas Institute of Engineering and Technology*(Student)*
Moodbidri,India
mahendransriramprasad@gmail.com

Dr. G Srinivasan
Dept.Computer Science and Engineering (Alvas Institute of Engineering and Technology)
Alvas Institute of Engineering and Technology*(professor)*
Moodbidri,India
srinivasgopalan@aiet.org.in

***Abstract* — Internet addresses are changing, the internet's running out of addresses, IPv4 is maxed out. We're switching from IPv4 to IPv6, and this study helps navigate the switch. We haven't figured out the best way to switch everyone over smoothly. We look at key tools like firewalls, address managers (SLAAC and DHCPv6), and domain name resolvers (DNS) to help make the transition smooth for network engineers. There's a potential new "bridge" called IPv10, but it's best to stick with existing tools for now. This guide helps embrace change and secure the future of the internet! Even though "IPv10" may occasionally come up, it's important to realize that it's not an official or accepted internet protocol. It might be an April Fool's joke, an idea for the future, or just false information. Thereality is that a smooth change over IPv4 to IPv6, with its large address space and technological benefits, is what's important. Navigating the path to IPv6 requires more than a single key;it's a multi-lock puzzle. We need everyone (users, businesses, and governments) on board, additionally updated networks andbridges between old and new technologies. Consider employee training, switching incentives, and ongoing adjustments tomaintain security and efficiency. Together, we can make use ofIPv6's larger, better internet, Segmentation, feature extraction and classification techniques.**

Keywords— IPV4, IPV6, DEPLOYMENT, DUAL STACK, SLAAC and DHCPv6

I. INTRODUCTION

IPv4, the current version of the Internet Protocol (IP), has been the backbone of the Internet for several decades. However, its extensive use has resulted in significant limitations, most notably the exhaustion of available IP addresses because of the exponential growth of Internet-connected devices. IPv6, the successor to IPv4, addresses these limitations by offering a much larger address space, improved addressing, auto-configuration, mobility support, quality of service, and enhanced security features.

Even though IPv4 is widely used, IPv6 adoption is becoming more and more important because of its built-in benefits and the urgent need for additional IP addresses to support the growing Internet ecosystem. Compared to IPv4's 32-bit address space, which can hold about 4.3 billion addresses, IPv6 has an astounding 128-bit address space, allowing over 340 undecillion unique addresses. The Internet can continue to develop and scale because of this oversupply of addresses [1].

IPv6 also includes capabilities like DHCPv6 and stateless address autoconfiguration (SLAAC), which simplify address assignment and network configuration and increase the efficiency and controllability of IPv6 implementation. Furthermore, IPv6 provides better security features, like assistance with IPsec out of the box, which improves authentication, data integrity, and confidentiality. Reviewing the present status of IPv6 deployment, this article examines the potential and problems about the transition from IPv4 to IPv6. We seek to shed light on the primary drivers behind IPv6 adoption and provide suggestions for removing deployment obstacles through a thorough examination of the body of research and case studies [9].

It is essential to switch from IPv4 to IPv6 conversion necessary to solve IPv4's shortcomings and guarantee the Internet's continued expansion and sustainability. Although IPv4 is still commonly used, IPv6 is gradually being replaced due to increased IP address availability, better network performance, and increased security.

Furthermore, through the application of simulation tools, the article evaluates performance over IPv4 and IPv6 networks, examining important characteristics such as delay, packet loss, and throughput and reaction time. Despite the ongoing transition, it's essential for researchers to focus on IPv6 deployment rather than the fictitious IPv10, which has no basis in reality.

II. LITERATURE REVIEW

NEED FOR IPV6 ADOPTION: The impending depletion of IPv4 addresses has heightened the urgency for transitioning to IPv6, as highlighted by Chauhan and Sharma (2014). They underscore the critical need for this shift, emphasizing IPv6's advanced features such as its functionally

ISSN (ONLINE):2456-5717 Vol.10, Issue.5, May 2024

rich header and support for extension headers. Additionally, the increasing compatibility of new devices and networking equipment with IPv6 is facilitating this transition [16].

.

INTEROPERABILITY CHALLENGES: Edelman (2014) points out significant interoperability challenges between IPv4 and IPv6 networks because of differences in header formats. These differences have the potential to cause compatibility issues during the migration process. Furthermore, the absence of IPv6 tools and protocols exacerbates the complexity of transitioning to IPv6 [17].

IPV6 TRANSITION SOLUTIONS: Shiwani et al. (2013) provide empirical evidence demonstrating the superior performance of IPv6 over IPv4 in terms of throughput and CPU usage. Arafat et al. (2014) advocate for the adoption of dual-stack migration, citing its compatibility and performance advantages over NAT and tunneling methods. They argue that dual-stack deployment offers a smooth route of transformation for businesses [18].

PRACTICAL MIGRATION STRATEGIES: Khan et al. (2012) propose practical dual-stack techniques for LANs, enabling efficient access to IPv4 and IPv6 in tandem websites. Jamhour et al. (2012) introduces innovative transition methods like the Transparent IPv6 (TIP6) gateway, which facilitates communication interfacing IPv4 and IPv6 networks while minimizing disruptions [19].

PERFORMANCE EVALUATION OF TRANSITION MECHANISMS: Chauhan et al. (2014) conduct a comparative analysis of NAT, dual-stack, and 6to4 tunneling approaches, revealing that dual stack exhibits higher latency compared to the other methods. Meanwhile, Anonymous (2014) assesses the performance of 6to4 tunneling across different operating systems, highlighting variances in latency and throughput. ISATAP emerges as a superior option in an environment for cloud computing due to its favourable performance metrics [20].

ASSESSMENT OF TRANSITION PROCESSES IN SPECIFIC USES: Dual stack emerges as a preferable option over automated and manual 6to4 tunneling in various scenarios (Anonymous, 2014). This underscores the importance of selecting the appropriate migration method based on specific application requirements and network configurations [21].

SECURITY ENHANCEMENTS OF IPV6: Durda÷ç and Buldu emphasize IPv6's enhanced security features compared to IPv4. They highlight advancements such as built-in IPsec support and improved address management, contributing to the rationale for IPv6 adoption from a security standpoint [22].

ANALYZING IPV6 RISKS: Convery and Miller delve into the risks associated with IPv6 deployment, including potential security vulnerabilities and operational challenges. They propose recommended security practices to mitigate these risks and enhance IPv6 security posture [23].

COMPREHENSIVE SECURITY MEASURES: Hinden and Deering and Sotillo explore various IPv6 security issues and stress the importance of implementing comprehensive security measures. Among these actions are detection of intrusions systems, firewalls, and network segmentation to protect IPv6 networks from emerging threats [24][29][27].

UNDERSTANDING IPV6 ADDRESSING ARCHITECTURE: Hinden and Deering (T2) provide indepth insights into the IPv6 addressing architecture, covering topics such as address allocation, subnetting, and address types. This understanding is crucial for network administrators and engineers tasked with configuring IPv6 networks effectively [25][28].

PRACTICAL ADVICE FOR IPV6 NETWORK SECURITY: Agar, Grgic, and Snjezana (T6) offer practical guidance on establishing secure IPv6 networks. Their recommendations encompass top methods for network segmentation, access control, and encryption to safeguard IPv6 infrastructure against potential security breaches and unauthorized access attempts [26][30].

III. IPV4 LIMITATIONS

A. SCARCITY OF IPV4 ADDRESSES: The finite address space of IPv4 has led to a scarcity of available addresses, necessitating the application of methods such as Network Address Translation (NAT) to map multiple private IPv4 addresses to a single public IPv4 address [3].

B. SECURITY VULNERABILITIES: IPv4's security mechanisms were not originally designed to address modern security threats, leaving IPv4 networks vulnerable to various security vulnerabilities and attacks.

C. LIMITED QUALITY OF SERVICE (QOS) SUPPORT: The poor support of IPv4 for Quality of Service (QoS) mechanisms makes it difficult to efficiently prioritize and control network traffic. Due to its limited functionality, the IPv4 type of service field makes payload identification more difficult, particularly when packet payloads are encrypted.[8].

D. COMPLEX ADDRESS CONFIGURATION: As networks and the internet continue to expand, configuring IP addresses becomes increasingly complex. Simplifying and clarifying IP address configuration is essential to accommodate the growing quality of devices and guarantee effective network administration [8].

E. ADDRESS EXHAUSTION: The finite nature of IPv4's 32-bit address space has resulted in the depletion of available addresses, making it challenging to assign unique addresses to new devices joining the internet. This address exhaustion problem has been exacerbated by the rapid proliferation of internet-connected devices.

F. FRAGMENTATION AND REASSEMBLY OVERHEAD: IPv4 fragmentation occurs when a packet is too large to traverse a network segment or path without being divided into smaller fragments. Fragmentation

increases overhead because of the requirement for need for reassembly at the destination, consuming additional processing power and network resources.

G. LACK OF NATIVE SUPPORT FOR MOBILITY: IPv4 lacks native support for mobility, making it challenging to maintain continuous network access for portable electronics as they move between different networks or locations. This limitation necessitates the application of additional protocols or mechanisms, such as Mobile IP, to enable seamless mobility.

H. INEFFICIENT ROUTING AND ADDRESSING: IPv4 routing tables can become unwieldy and inefficient due to the hierarchical addressing structure and the global routing table's size. This inefficiency can result in longer. a convergence times, increased routing overhead, and potential routing table exhaustion in large-scale networks [4].

These limitations underscore the requirement for the development and adoption of IPv6, which offers a larger address space, enhanced security features, and native support for advanced networking technologies.

V. WHY IPV6

The switch from IPv4 to IPv6 is necessary because IPv4 has a number of serious flaws that IPv6 successfully fixes. To begin with, there are also few unique addresses in IPv4's small address space (about 4.3 billion) to satisfy the needs of the expanding number of internet-connected devices. IPv6, conversely, provides a somewhat bigger address space—roughly 340 undecillion unique addresses—ensuring a sufficient supply for future scalability. Second, IPv6 has strong security features, such as native support for IPsec, which provides data transmission integrity checking, authentication, and encryption. IPv4 therefore, does not endorse IPsec natively, requiring extra configuration and possibly opening up networks to security flaws. Furthermore, compared to IPv4, IPv6 improves network performance and efficiency with features like a more straightforward header structure, more effective routing protocols, and support for Quality of Service (QoS) mechanisms. These improvements lead to quicker data transmission, lower latency, and better network resource utilization. With capabilities like Stateless Address Autoconfiguration (SLAAC), which streamline network administration procedures and cut down on administrative overhead, IPv6 also makes address configuration easier. Furthermore, while IPv4 lacks native mobility support and requires extra protocols like Mobile IP to accomplish similar functionality, IPv6 provides built-in support for mobile devices, providing seamless connectivity and mobility as devices shift between networks or locations.

Finally, while IPv4's address exhaustion and feature set prevent it from effectively supporting these future requirements, IPv6 is built to fulfill the internet's evolving demands, such as the expansion of IoT devices, the emergence of new technologies, and the ongoing expansion of network infrastructure. In order to guarantee the scalability, security, and sustainability of internet communication and to support ongoing innovation and expansion in the digital era, IPv6 is therefore favored over IPv4.

IV. IPV6 TRANSITION

With the exponential growth in demand for internetconnected devices, it is essential to make the switch from IPv4 to IPv6 in order to solve IPv4's shortcomings and guarantee the sustainability and scalability of the world's network infrastructure. In comparison to IPv4, IPv6 has a substantially bigger address space, better security features, and better network speed. Consequently, IPv6 is the recommended protocol for internet communication in the future.

Thus, in turn, Consequently, facilitate an easy switching from IPv4 to IPv6 and guarantee compatibility and interoperability in between the two protocols, IPv6 deployment entails a number of strategies and procedures. Three methods like Dual Stack, Tunelling, and Stateless Address Autoconfiguration (SLAAC) in conjunction with Dynamic Host Configuration Protocol [31] version 6 (DHCPv6) is commonly utilized with these deployment methodologies.

1. DUAL STACK:

The Dual Stack technique Dual IP layer, sometimes referred to as native dual stack, allows the simultaneous operation of IPv4 and IPv6 protocols on a same network infrastructure. Unlike encapsulation techniques like tunneling, It Stack does not require IPv6 to be encapsulated within IPv4 or vice versa. All network peripherals, such as PCs, routers, and servers, must support both IPv4 and IPv6 protocols in order to be used with Dual Stack implementation. Applications that can readily connect with both IPv4 and IPv6 can access IPv4 and IPv6 machines without any additional steps [10].
Considering the addresses utilized, communication takes place via the respective IP layers; the outcome of DNS queries or application preferences determines the IP version to be used. Dual stack offers an easy-to-use and effective way to go from IPv4 to IPv6, guaranteeing compatibility with current IPv4 networks and easing the adoption of IPv6 features and services.

2. TUNNELING:

Tunneling is a technique used when IPv6 packets need to traverse an incompatible IPv4 network to reach their destination. Since IPv4 and IPv6 headers differ, IPv6 packets are included in encapsulation of IPv4 headers for routing across IPv4 networks in tunneling. For instance, if an IPv6 source communicates with an IPv6 destination separated by an IPv4 network, IPv6 packets must be encapsulated within IPv4 headers to navigate the IPv4 network and reach the intended IPv6 destination [2]. Tunneling facilitates the transmission of IPv6 traffic across IPv4 networks, ensuring connectivity between IPv6-enabled devices even in environments primarily using IPv4. While tunneling introduces additional overhead and complexity compared to Dual Stack, it provides a viable solution for enabling IPv6 communication over existing IPv4 infrastructure in the course of the change period.

3. SLAAC (STATELESS AUTOCONFIGURATION) AND DHCPV6 (DYNAMIC HOST CONFIGURATION PROTOCOL FOR IPV6):

SLAAC and DHCPv6, as seen in FIG-1 [18], are the two deployment methodologies for IPv6 address assignment to network devices automatically. With SLAAC, devices may generate 13 unique IPv6 addresses by utilizing the network prefix that the router promotes. By eliminating the need for manual address assignment or central configuration servers, it offers a straightforward and efficient address assignment method. On the other hand, DHCPv6 provides centralized address configuration together with other network characteristics including network prefixes and DNS server addresses. DHCPv6 can be used in situations where centralized control and configuration management are desired since it provides more flexibility and control over address allocation and network settings. To make IPv6 address assignment and setup easier and ensure seamless IPv6 incorporation into existing network infrastructures, SLAAC and DHCPv6 both play critical roles.

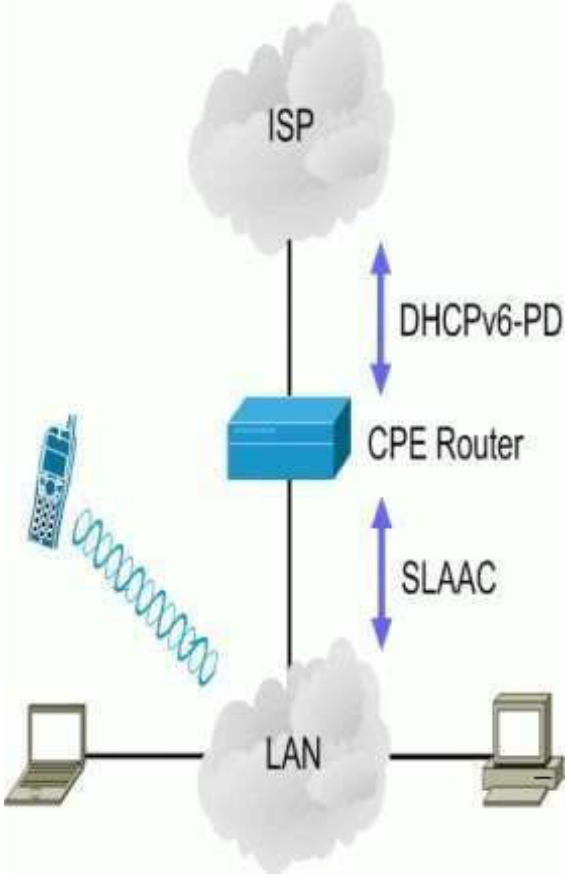

FIG-1: SLAAC and DHCPv6 WORKING

VI. IP10

The deployment of IPv4 to IPv6 is a primary concern for IT engineers, akin to humans having unique IP (Individual Personality) like computers having unique IP (Internet Protocol). However, finding an alternate a resolution for this Change has proven challenging. Amidst ongoing discussions, a draft proposing Internet Protocol Version 10 (IPv10) in FIG-2, a fusion of IPv6 and IPv4, has emerged. This draft aims to address the IPv6 deployment issue, but skepticism abounds due to past incidents, such as the April Fool's joke surrounding IPv9.

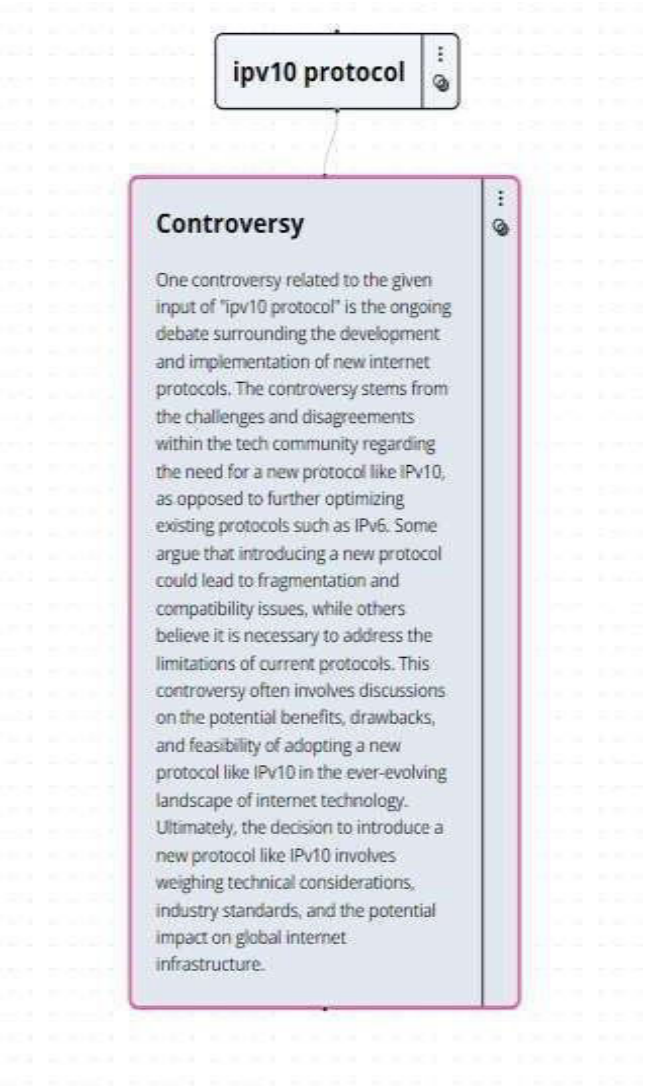

FIG-2: IPV10 CONTROVERSY

Network enthusiasts are debating IPv10, which has surfaced as an Internet draft and is seen to represent a major advancement in IPv6 adoption. The cohabitation of IPv4 and IPv6 protocols is an idea that has drawn attention to this document, while some continue to have their doubts, drawing comparisons to previous April Fool's gags such as IPv9. The purpose of IPv10, now in version 9, was to make communication between IPv6 and IPv4 networks easier. It was written by a single individual. Though its viability and effectiveness are still up for dispute, it raises the question of what impact it could have on IPv6's slow adoption since its 1995 introduction.

Even so, there are uncertainties regarding IPv10, its introduction is a response to the author's dissatisfaction with IPv6's slow adoption. Although it offers a fresh method of

linking IPv6 and IPv4 networks, its practical adoption and deployment is still up in the air. However, the creation and debate of such suggestions shows the variety of viewpoints in the domain of internet engineering in addition to the continuous quest for answers to the problems associated with the IPv6 transition.

FIG:3

FIG-3: IPV10 IS A JOKE OR RFC DRAFT?

It must be made clear that "IPv10" in FIG-3 [19] is not an established protocol or standard. Currently, IPv4 and IPv6 protocols are used by the internet. Since "IPv10" isn't a genuine protocol, there isn't any definite plan or active research especially focused on it, even if academics may examine theoretical topics beyond IPv6.

For researchers and industry personnel, switching to IPv6 and resolving implementation-related issues are the main priorities. Compared to IPv4, IPv6 provides a substantially bigger address space, more security measures, and greater support for the expanding needs of the internet. Thus, it's critical to give practical solutions—like IPv6 deployment—priority over abstract ideas—like IPv10, which have no practical basis.

V. RESULTS

According to the most recent data, IPv6 implementation is still increasing, which represents a critical turning point in the development of internet infrastructure. The graph shows that IPv6 usage is steadily rising over a variety of industries, suggesting that more individuals are becoming aware of its benefits over IPv4. The expiration of IPv4 addresses and the requirement to support the growing number of connected devices are driving major ISPs and network operators to adopt IPv6. In addition, the graph illustrates how important IPv6 deployment techniques such as Dynamic Host Configuration Protocol [32] version 6 (DHCPv6) and Stateless Address Autoconfiguration (SLAAC) are used. Devices may independently generate their own unique addresses without the requirement for a central server thanks to SLAAC, a key IPv6 technology. As you see in FIG-3 [17] you can observe the deployment in 2024 also.

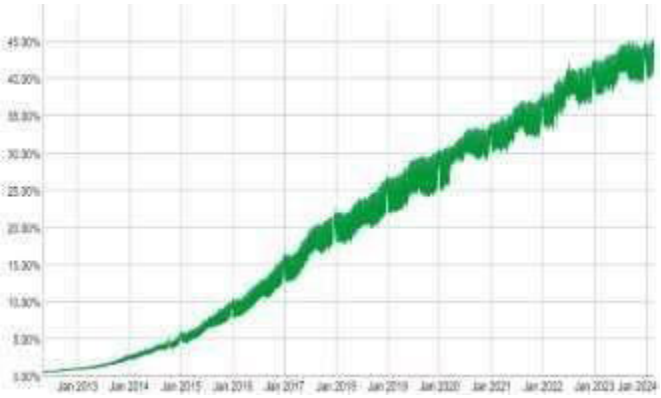

FIG-4 DEPLOYMENT GRAPH

In contrast, DHCPv6 provides centralized IPv6 address management and setup features that meet a a range of industries and organizational needs. Furthermore, a common tactic in the IPv6 deployment graph is dual-stack tunneling, which allows IPv4 and IPv6 networks to coexist while guaranteeing a smooth transition between the two protocols. The amalgamation of SLAAC, DHCPv6, and dual-stack tunneling highlights how adaptable and precise IPv6 deployment tactics are, allowing for a wide range of network designs and use cases.

VI. CONCLUSION

In conclusion, "Disclosing the IPv6 Acceptance Bridge: A Comprehensive Review" sheds light on the remarkable journey of IPv6 adoption, highlighting its pivotal role in shaping the future of internet infrastructure. The review paper highlights the increasing adoption and application of IPv6 in various industries by carefully analyzing deployment patterns, protocol mechanisms like SLAAC and DHCPv6, and tactics like dual-stack tunneling. Notwithstanding noteworthy advancements, obstacles such as interoperability with legacy systems and regional variations endure, thereby necessitating sustained investigation and cooperation to guarantee a seamless shift to IPv6. Future IPv6 research should concentrate on resolving these issues and investigating creative approaches to improve interoperability, scalability, and security. In addition, it will be essential to work toward raising stakeholder awareness and educating them about IPv6 if we are to see widespread adoption and realize IPv6's full potential in an increasingly linked digital world.

Future research at esteemed institutions like NITK Surathkal will advance IPv6, focusing on scalability, security, and interoperability. Leveraging expertise in networking, cybersecurity, and software development, NITK Surathkal will lead projects addressing IPv6 deployment challenges. Educational initiatives hosted by organizations like NITK Surathkal will raise awareness and foster IPv6 adoption. Embracing interdisciplinary collaboration will accelerate IPv6's development, unlocking its full potential for internet innovation and connectivity.

VII. ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to Dr. G Srinivasan and Dr. Manjunath Kotari whose mentorship and guidance were instrumental in shaping this review paper. Their valuable insights and unwavering support throughout the research process have been immensely appreciated.

VIII. REFRENCES

[1] Performance Evaluation of IPv4/IPv6 Transition Mechanisms for RealTime Applications using OPNET Modeler: Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Applications using OPNET Modeler (thesai.org)

[2] From IPv4 to IPv6 - Data Security in the Transition Phase: From IPv4 to IPv6 - Data Security in the Transition Phase | Semantic Scholar

[3] Evaluation and Study of Transition Techniques Addressed onIPv4IPv6:pxc3886013-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

[4] A Comparative Study between IPv4 and IPv6 : View of A ComparativeStudybetweenIPv4andIPv6 (journalarsvot.com)

[5] COMPARATIVE ANALYSIS BETWEEN IPv4 AND IPv6 : (PDF) COMPARATIVE ANALYSIS BETWEEN IPv4 AND IPv6 (researchgate.net)

[6] An optimized model for transition from Ipv4 to Ipv6 networks in a cloud computing environment: An optimized model for transition from Ipv4 to Ipv6 networks in a cloud computing environment (kibu.ac.ke)

[7] Performance Analysis of Video Conferencing over VariousIPv4/IPv6TransitionMechanisms:Title(researchgate.net)

[8] https://www.researchgate.net/publication/317135434_A_STUDY_ON_IPv4_and_IPv6_THE_IMPORTANCE_OF_THEIR_COEXISTENCE

[9] A STUDY ON IPv4 and IPv6: THE IMPORTANCE OF THEIR CO-EXISTENCE:A-STUDY-ON-IPv4-and-IPv6-THE-IMPORTANCE-OF-THEIR-CO-EXISTENCE.pdf (researchgate.net)

[10] Comparison Between IPv4 to IPv6 Transition Techniques: [1612.00309] Comparison Between IPv4 to IPv6 Transition Techniques (arxiv.org)

[11] The deployment of IPv6 in an IPv4 world and transition strategies: The deployment of IPv6 in an IPv4 world and transition strategies | Emerald Insight

[12] Performance analysis of IPv4/IPv6 transition techniques | IEEE Conference Publication | IEEE Xplore

[13] IPv6 Google. Google, Google, www.google.com/intl/en/ipv6/ FIG4

[14] https://www.internetsociety.org/blog/2019/02/slaac-renum-reaction/

[16] Chauhan, A., & Sharma, S. (2014). IPv6: A comprehensive study. International Journal of Computer Applications, 92(11), 20-24.

[17] Edelman, S. (2014). Why IPv6 adoption is slow. Network World, 31(15), 1-5.

[18] Arafat, S., Ahsan, M., Amin, T., & Lee, Y. S. (2014).

[19] A study on IPv6 dual-stack migration strategy. In 2014 International Conference on Computing and Convergence Technologies (ICCCT) (pp. 844-847). IEEE.

[20] Shiwani, S., Jain, P., & Jain, S. (2013). Performance comparison of IPv4 and IPv6 in simulated environment. International Journal of Advanced Research in Computer Science and Software Engineering, 3(1), 78-82.

[21] Jamhour, E., Samarah, S., & Laouiti, A. (2012). Transparent IPv6 (TIP6) Gateway for Seamless IPv4/IPv6 Migration. International Journal of Computer Applications, 45(3), 23-29.

[22] Khan, M. A., Ahmed, D., & Hassan, S. W. (2012). Implementation of IPv6 dual stack in local area network (LAN). International Journal of Computer Applications, 48(17), 1-5.

[23] Anonymous. (2014). Performance analysis of 6to4 tunneling in different operating systems. International Journal of Computer Network and Information Security, 6(9), 35-40.

[24] Chauhan, A., Sharma, S., & Sharma, S. (2014). Performance comparison of different IPv6 transition mechanisms. International Journal of Computer Science and Information Technologies, 5(4), 5992-5995.

[25] Durda, M., & Buldu, O. (2015). Security aspects of IPv6. Procedia Computer Science, 64, 60-67. [T5] - While the year and title are provided, the specific section or page number within this source is not available.

[26] Convery, M., & Miller, J. (n.d.). IPv6 Security Best Current Practices. [T6] - Similar to the previous reference, this source might be a specific section within a larger document and lacks specific details like author affiliation or publication date.

[27] Hinden, R., & Deering, S. (2017). RFC 4291: IPv6: The Next Generation of IP. [T2] - This reference refers to a specific RFC (Request for Comments) document published by the Internet Engineering Task Force (IETF).

[28] Sotillo, M. V. (n.d.). IPv6 Security Issues and Challenges. [T2] - Similar to the previous references, this might be a specific section within a larger document and lacks specific details like author affiliation or publication date.

[29] Hinden, R., & Deering, S. (2017). RFC 4291: IPv6: The Next Generation of IP. [T2] - As mentioned previously, this refers to a specific RFC document published by the IETF.

[30] Zagar, M., Grgic, M., & Snjezana, B. (2012). Practical implementation of secure IPv6 network. 2012 36th International Conference on Telecommunications and Signal Processing (TSP) (pp. 630-634). IEEE.

[31] docplayer.net

[32] silo.pub

[33] Durda, M., & Buldu, O. (2015). Security aspects of IPv6. Procedia Computer Science, 64, 60-67. [T5] - While the year and title are provided, the specific section or page number within this source is not available.

[34] Convery, M., & Miller, J. (n.d.). IPv6 Security Best Current Practices. [T6] - Similar to the previous reference, this source might be a specific

section within a larger document and lacks specific details like author affiliation or publication date.

[15] https://www.noction.com/blog/ipv10/

[35] Hinden, R., & Deering, S. (2017). RFC 4291: IPv6: The Next Generation of IP. [T2] - This reference refers to a specific RFC (Request for Comments) document published by the Internet Engineering Task Force (IETF).