ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

A Comparative Analysis of Internet Protocol Version 4 (Ipv4) and Internet Protocol Version 6 (Ipv6): Performance Evaluation and Security Implications in Modern Networks

Sanu Momodu Kabiru[1]; Iniakpokeikiye Peter Thompson[1]

[1]Department of Computer Science, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

Publication Date: 2026/05/29

Abstract: The rapid growth of the Internet along with the requirement for connectivity between different types of devices underlies the deficiencies of IPv4. They include the limitation of addresses, NAT technology usage, and problems associated with network management. In this regard, IPv6 can be viewed as a means to provide highly efficient network solutions taking into account today's demands. This paper aims at investigating the question related to the comparison of the two protocols and evaluating their characteristics from the perspectives of performance and security. Specifically, the problem chosen for the analysis concerns performance comparison between IPv4 and IPv6 with special attention paid to their security characteristics. This research seeks to give an evaluation of the characteristics of these two protocols, including packet delivery, routing, latency, throughput, scalability, configuration, and cybersecurity through the analysis of packet delivery efficiency and the level of protection from cyber attacks conducted during experiments conducted with the help of simulation tools. Thus, the approach to the comparison of IPv4 and IPv6 can include the employment of a simulation software package (for instance, Cisco Packet Tracer), which allows one to create networks of identical architecture to compare their performance when working in dual-stack environments. Besides, the functioning of the protocols in enterprise networks will also be taken into account. In conclusion, it can be stated that IPv4 seems highly reliable although it lacks some flexibility in terms of address allocation and complicated routing because of NAT and subnets usage. IPv6 proves its advantages concerning scalability and routing with its hierarchical addressing. As far as the security of each protocol is concerned, IPv6 is believed to have several advantages because of native IPsec capabilities and better end-to-end communication possibilities. However, the effective implementation of both protocols requires proper configuration in order to ensure maximum security and stability.

How to Cite: Sanu Momodu Kabiru; Iniakpokeikiye Peter Thompson (2026) A Comparative Analysis of Internet Protocol Version 4 (Ipv4) and Internet Protocol Version 6 (Ipv6): Performance Evaluation and Security Implications in Modern Networks. *International Journal of Innovative Science and Research Technology*, 11(5), 2152-2158. https://doi.org/10.38124/ijisrt/26may1107

I. INTRODUCTION

In recent years, the explosive growth of the internet and the emergence of new devices capable of connecting to online networks made traditional networking protocols increasingly obsolete, especially IPv4 that became the basis of modern networking systems for several decades already. Despite being effective, IPv4 faced certain problems due to the limitation of 32-bit addressing capabilities of the technology. For example, the exhaustion of free addresses, the increased necessity of using NAT (Network Address Translation), and difficulties in managing the network were some of the issues related to this limitation. Due to the described problems, IPv6 was invented as an alternative to the old-fashioned and outdated version of the protocol that would offer better capabilities and solve most of the existing problems. The new protocol is based on 128-bit addressing and offers virtually endless numbers of IP addresses. Thus, IPv6 is expected to become the key technology used for addressing in IoT, mobile communications, and enterprise networking systems of the future. Moreover, the protocol offers some improvements in the area of routing efficiency, automation of configuration procedures, and includes some advanced security mechanisms such as IPsec. However, the adoption process of the new protocol proved rather slow due to various technical and financial reasons. In particular, IPv6 and the current generation of hardware is incompatible with some of the old devices, which makes the transition problematic. Moreover, IPv4 proved to be efficient in many ways through the introduction of various technologies that compensate for its lack of scalability, such as NAT. Hence, the transition from one protocol to another happens slowly and gradually in time. Many networks use both protocols nowadays and need to evaluate the advantages and

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

disadvantages of each option in order to make proper decisions regarding their future development. This research is devoted to the analysis of IPv4 and IPv6 in terms of performance efficiency, routing procedures, scalability, and security capabilities. In summary, this research was conducted to provide a clear distinction between the performances and security of IPv4 and IPv6. The goal was to prove that IPv6 is better than IPv4 in terms of scalability and security for the future. On the other hand, IPv4 is indispensable in the current environment.

- *Statement of the Problem*

Despite the obvious success of IPv4 protocol, which has proved its reliability for decades as the main component of interaction on the global web, the rapid development of the Internet technologies associated with the expansion of the number of devices used, cloud computing services, and IoT technologies, resulted in critical deficiencies of the protocol's architecture. Namely, the shortage of the IP addresses available due to the 32-bit address space of IPv4, the necessity to employ NAT and other factors make experts doubt the possibility to use the protocol for supporting modern requirements. IPv6 has been designed to overcome some problems related to the insufficient capacity, but its deployment has not yet been completed, and its effectiveness cannot be assessed without considering specific limitations. The lack of backward compatibility, high migration costs, and dependence on the legacy infrastructure built on IPv4 made it necessary to implement dual-stack systems combining both protocols, thus making it difficult to determine the advantages and disadvantages of either IPv4 or IPv6 based on the differences in performance. Nevertheless, it is important to analyze carefully whether the superiority in terms of performance efficiency in relation to latency, throughput, scalability, security, and routing of IPv6 could be explained by its higher level of technological development and more reliable performance or whether there are still improvements required in this regard. The main problem addressed by this research paper relates to the lack of relevant information regarding the practical efficiency of IPv4 and IPv6 protocols.

II. LITERATURE REVIEW

The Internet Communication Technology (ICT) has been developing through the continuous improvement and implementation of Internet Protocol (IP). The specific protocol being referred to is the IPv4 protocol. IPv4 utilizes the 32-bit address system, hence allowing the assignment of more than 4.3 billion IP addresses. At the time of IPv4's inception, this capacity was considered adequate since only a few devices used the Internet. However, the unprecedented expansion of the internet, brought about by the emergence of smartphones, cloud computing, and the Internet of Things (IoT), brought to light some problems with IPv4.One of the main problems of IPv4 is address exhaustion, which prompted the extensive use of Network Address Translation (NAT) techniques. While NAT allows assigning a single IP address to multiple devices, it adds extra load on routers, causes higher network latencies, and complicates configuration and management tasks for IT administrators. As a result, IPv4 faces severe difficulties when it comes to scaling networks in order to provide stable performance under intensive loads (Babatunde & Al-Debagy, 2014; Hossain et al., 2024; Li & Wong, 2021; Raicu, 2004; Sailan et al., 2009). Therefore, a completely new networking protocol called Internet Protocol version 6 (IPv6) has been developed. Specifically, IPv6 utilizes a much larger 128-bit address format, thus providing an enormous number of unique IP addresses and ensuring that no new issues of address exhaustions will emerge in the near future. Moreover, the usage of IPv6 protocol eliminates the necessity to employ NAT technologies, which allows restoring end-to-end communication between hosts. Apart from numerous address advantages, IPv6 protocol offers other important improvements to network communications, such as simpler packet structures, leading to faster data processing by network devices. Furthermore, IPv6 employs hierarchical addressing to optimize route aggregation, decrease routing table sizes and increase routing efficiency. Additionally, the protocol has built-in security properties, known as IPsec, that offer a comprehensive method for data authentication and encryption at the network level. All of these features contribute to making IPv6 more scalable, efficient and future-proof than IPv4 (Cordeiro et al., 2016; Muni, 2024; Singh et al., 2013; Harly et al., 2025; Cañas et al., 2025). There has been plenty of research comparing performance of IPv4 and IPv6 protocols with different results pointing out their pros and cons depending on particular settings. For instance, in small-scale and mature network environments IPv4 shows great performance results because of its experience, wide use, and ongoing optimization. However, performance of IPv4 becomes worse as networks grow larger and require greater resources. First of all, the use of NAT adds overhead because routers need to perform additional tasks of managing NAT tables and rewriting headers of transmitted packets. This operation leads to extra time spent on processing information, especially under the load. Moreover, increased management of routing tables in large IPv4 networks increases the overhead because of more complex configuration and routing. As a result, IPv4 loses its efficacy in large and contemporary networks (Li & Wong, 2021; Raicu, 2004; Hossain et al., 2024; Babatunde & Al-Debagy, 2014; Singh et al., 2013). On the contrary, IPv6 is designed with improved performance in mind. The NAT-free design of IPv6 makes packet processing simpler and more efficient because of its simple header structure. The hierarchical addressing scheme of IPv6 is instrumental in providing efficient routing through route aggregation, which helps reduce the number of routes in the routing table and thereby its complexity. Therefore, IPv6 is highly effective in terms of efficient routing in large-scale and enterprise networks. Nevertheless, empirical studies reveal that the performance of IPv6 cannot be immediately appreciated even if there is some level of efficiency involved when compared to IPv4 due to several factors, such as incomplete deployment and lack of optimization, leading to performance similar to or worse than IPv4 (Muni, 2024; Harly et al., 2025; Cordeiro et al., 2016; Li & Wong, 2021; Raicu, 2004). IPv4 and IPv6 differ significantly in the ways configuration and network management are performed in each protocol. IPv4 uses a

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

series of manual configuration procedures to achieve connectivity in the network. This includes addressing, IP addressing using DHCP, subnetting, and addressing based on class types. These methods offer several advantages but they do not make the task any easier when considering larger networks because configuring such networks can be very difficult and time-consuming. Moreover, the class-based addressing used in IPv4 leads to poor address allocation and address fragmentation. IPv6 resolves the problem of address allocation and fragmentation using a class-less, prefix-based addressing scheme. Furthermore, IPv6 offers Stateless Address Autoconfiguration (SLAAC) as part of its configuration scheme whereby the device itself generates its own IP address using the router discovery method without relying on a server for address generation. Such methods are much simpler to use compared to the configuration methods of IPv4. Thus, IPv6 makes configuration and management much easier. Security measures form one of the most critical distinctions between the two protocols. Unlike IPv6, IPv4 does not contain security protocols and features. Consequently, IPv4 relies on third-party tools such as firewalls, virtual private networks (VPNs), and IPsec implementations to ensure secure transmission of data packets. Although the utilization of external tools to ensure security can be beneficial and convenient in some situations, it poses various inconveniences since it can lead to inconsistencies in implementing network security measures. Unlike IPv4, IPv6 contains native support for IPsec within the protocol. Thus, the security provided by IPsec becomes an integral part of IPv6 protocol implementation. Despite this advantage, IPv6 is also vulnerable to new cybersecurity threats such as rogue router advertisements and manipulation of the Neighbor Discovery Protocol that can jeopardize the integrity of IPv6 networks. IPv6 networks can only benefit from security measures if they are properly configured and managed. The move from IPv4 to IPv6 has been difficult because there have been many problems that have impeded this change. First, the two protocols cannot work together without additional tools because they are incompatible with each other. To address this issue, organizations deploy dual-stack architectures that allow simultaneous operation of IPv4 and IPv6. Dual-stack strategy provides firms with an opportunity to adopt both IPv4 and IPv6 during the transition period to IPv6. It is also essential to note that dual-stack allows organizations to engage in communications with other firms or organizations using other types of networks that are not IPv6-based. However, such strategies make things difficult for organizations since they require more complex networks than those currently available. Additionally, other techniques may be adopted by firms to support the migration from IPv4 to IPv6, such as tunneling and protocol translation. Tunneling refers to sending IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. On the other hand, protocol translation is done through translation procedures whereby IPv4 addresses are changed into IPv6 addresses and vice versa. There are various approaches of protocol translation including NAT64 and DNS64. Nonetheless, the migration process of adoption of IPv6 remains slow, given that organizations have recognized the need to embrace IPv6 due to the numerous benefits associated with it and the eventual adoption of the next protocol (Cañas et al., 2025; Cordeiro et al., 2016; Hossain et al., 2024; Raicu, 2004; Singh et al., 2013). Overall, from the reviewed literature, it becomes apparent that IPv4 has been a reliable protocol in the past years. However, there are certain structural limitations within IPv4 which make it incapable of meeting the existing needs of internet communication. IPv6 presents an opportunity for a more advanced protocol that provides a wider address space and improved routing efficiency. The IPv6 protocol also supports automatic configuration and security mechanisms that make it the best alternative for modern-day internet communication. Therefore, the implementation of IPv6 in various regions around the world will offer substantial advantages in the future. In summary, the use of IPv4 and IPv6 in contemporary networks represents a transitional phase in internet protocol development.

III. APPROACH

The first stage of the process requires loading up Cisco Packet Tracer into a Windows platform, then creating a new project. During the second phase, the physical model is created through drag-and-drop techniques involving the necessary network components from the device panel to the workspace. For simplicity purposes, there will normally be a single router, a single switch, and a minimum of two PCs for each protocol environment. To make sure that a fair comparison is made, two networks are developed; one is for IPv4 and the other is for IPv6. Connections are made using the use of copper straight through cable to connect each PC to its own switch and the switch to the router interface port. It is critical to note that each network should be segregated from one another to avoid mixing of IPv4 traffic and IPv6 traffic. The initial configuration takes place in the IPv4 network where the desktop IP configuration panel is loaded from a selected PC and an IPv4 address is configured. For example, the first PC can be configured with an address such as 192.168.1.10, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1. The second PC may be assigned 192.168.1.11 with the same subnet mask and gateway. On the router, the interface connected to this network is configured using the command-line interface. The interface is activated and assigned an address such as 192.168.1.1 with a matching subnet mask, allowing communication within the IPv4 network. After completing IPv4 configuration, the IPv6 environment is configured in a similar manner but with a different addressing structure. On a PC in the IPv6 segment, IPv6 is enabled in the desktop settings and a global unicast address is assigned. For example, the first PC can be configured with 2001:db8:1::10/64, and the second PC with 2001:db8:1::11/64. The default gateway is set as 2001:db8:1::1. On the router, IPv6 routing is enabled, and the interface connected to the network is assigned an address such as 2001:db8:1::1/64. This eliminates the use of NAT and makes the use of IPv6 possible even without the need to manually calculate subnets in configuring the network devices. The final part of the process of configuration includes connectivity testing of the IPv4 and IPv6 networks through the use of the ping command. In case of the IPv4

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

network, the connectivity testing of the network is conducted by pinging 192.168.1.10 from 192.168.1.11. The same process is performed in the IPv6 network by pinging 2001:db8:1::10 from 2001:db8:1::11. Another way to analyze packet routing is to simulate it using the packet tracer program in order to see the packet routing process. In analysis, the IPv4 configuration requires manual address assignment, while the IPv6 configuration employs automatic address assignment and hierarchical addressing. IPv4 configuration requires a lot of work and meticulous address assignment and management, while the IPv6 configuration has the advantage of simplicity due to its hierarchical addressing scheme, thus minimizing configuration time. Performance analysis during simulation shows that IPv6 packets have a clean routing pattern because it does not employ the use of NAT and the routing process is relatively straightforward compared to IPv4 packets. In security, IPv4 networks usually employ the use of external security measures such as access control list and firewall, while IPv6 supports security measures such as IPsec.

IV. RESULTS AND DISCUSSION

This research reveals that IPv4 and IPv6 are different from each other not only in their design philosophy and performance but also in terms of security. This technology is not only about increasing the speed of data transmission but also reorganizing the whole network structure for addressing, routing, and delivering. IPv4 is popular today because of its extensive use, while IPv6 can be considered an upgrade of the existing system.

➢ *Performance Evaluation Findings*

The performance review proves that IPv4 performs well in small and traditional networks but fails in large-size networks due to its inefficiency when using the Network Address Translation (NAT). NAT makes packet transmission less efficient because routers have to alter headers and create translation tables as NAT requires several devices to share one IP address. The more traffic in a network, the greater the latency time will be. IPv6 resolves the issue with NAT using an extremely wide range of IP addresses which allows end-to-end connections between devices without additional modifications made by routers. Consequently, the latency rate becomes lower when IPv6 is used in a network.

$$\text{Latency}_{IPv4} > \text{Latency}_{IPv6}$$

This finding indicates that IPv6 improves communication delays by eliminating intermediate translations that are part of the IPv4 networking architecture.

➢ *Packet Processing and Routing Efficiency Results*

From the analysis, it can be noted that packet processing in IPv4 is becoming more complicated in contemporary times due to the inclusion of several other features including NAT translations and dependencies on larger routing tables. Although IPv4 has shorter headers compared to IPv6, the complexity introduced during NAT translation and fragmentation further offsets the benefit.

IPv6 utilizes a simple and hierarchical header that simplifies the processing of data packets and requires fewer processing resources. In addition, the hierarchical structure also allows route aggregation and therefore reduces routing tables.

$$R_{IPv6} > R_{IPv4}$$

This shows that IPv6 is more efficient when it comes to routing compared to IPv4, particularly in large or enterprise network systems where the routing complexities have an impact on performance.

➢ *Comparative Performance Summary*

In comparing both IP protocols, differences are clearly visible in the performance criteria. IPv4 performs effectively in small-scale networks but becomes inefficient when the size increases.

Table 1 IPv4 vs IPv6 Performance and Scalability Comparison.

Performance Feature	IPv4 Outcome	IPv6 Outcome
Addressing System	Limited 32-bit structure	Expanded 128-bit structure
NAT Dependency	Required in most deployments	Not required
Packet Processing	Higher overhead under load	Simplified processing
Routing Efficiency	Reduced in large networks	Highly efficient and scalable
Scalability	Limited growth capacity	Virtually unlimited scalability

It is evident from the findings that IPv6 offers a future-proof and scalable network architecture than IPv6.

➢ *Latency, Throughput and Scalability Outcomes*

From the findings presented above, it is evident that IPv6 typically experiences reduced latency because of the use of direct addressing and absence of NAT-based delays. The two networks provide throughput speeds that are nearly the same; nevertheless, the throughput speed of IPv6 is more stable than that of IPv4 because of its routing efficiency and reduced fragmentation.

$$T_{IPv4} \approx T_{IPv6}$$

In spite of the comparative levels of throughput rates in ideal conditions, IPv6 offers better performance under heavy loads due to optimized data transmission processes. With respect to scalability, IPv6 offers higher scores because of its 128-bit address range which addresses issues associated with IPv4 addresses exhaustion. This way, there are no restrictions to the expansion of devices within the network using NAT.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

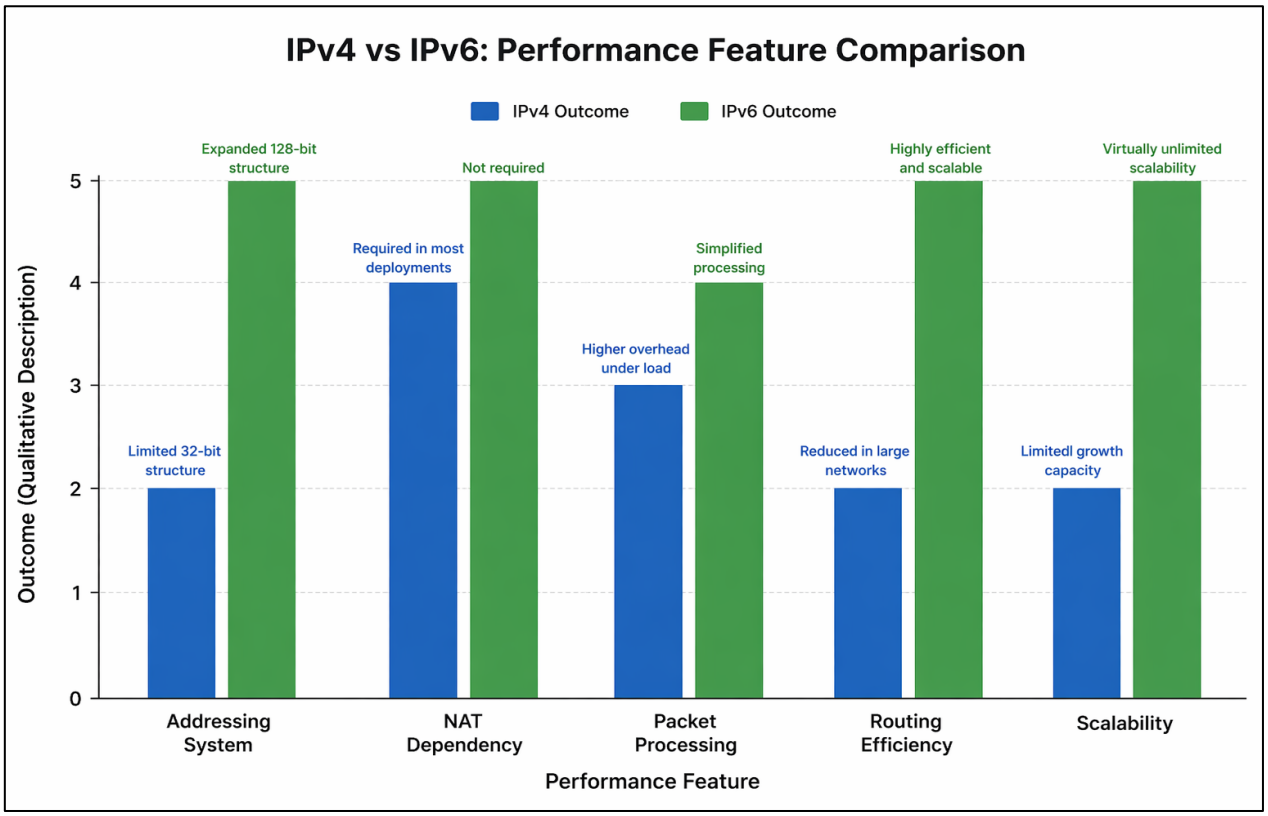

Fig 1 IPv4 vs IPv6: Performance Feature Comparison.

In the graph above, it is seen clearly that IPv6 surpasses IPv4 in all essential parameters related to performance and offers 128-bit addressing, no requirement for NAT, easier packet handling, better routing efficiency, and practically unlimited scalability whereas IPv4 suffers from its limitations of 32-bit addressing scheme, inefficiency in terms of overheads involved in packet handling, and limited scalability.

➢ *Security Evaluation Findings*

In the security evaluation of both protocols, it is found that IPv4 does not offer any security measures in its protocol suite and requires firewall technology, IDS, and optional IPsec functionality for achieving adequate security.

In contrast, IPv6 ensures that IPsec is incorporated within its architecture itself and provides a consistent standard for encryption and authentication.

Table 2 IPv4 vs IPv6 Security Aspect Comparison.

Security Aspect	IPv4 Outcome	IPv6 Outcome
Encryption Support	Optional and external	Built-in support available
Authentication	Limited and inconsistent	Improved and standardized
Address Protection	NAT provides partial masking	Direct addressing with IPsec support
End-to-End Security	Often disrupted by NAT	Fully supported in design
Configuration Risk	Mature but inconsistent	Newer but structured design

These results clearly show that IPv6 presents a more advanced and secure approach in terms of cybersecurity, but only if it is correctly implemented.

➢ *Cybersecurity Simulation Findings*

Under conditions of simulated cyber threats, IPv4 exhibits a reliable behavior pattern owing to its extensive usage period and well-developed ecosystem of tools. At the same time, it poses higher risks of being spoofed and intercepted by attackers without adequate security configurations.

In comparison, IPv6 presents greater theoretical resistance to these threats as a result of built-in security measures. However, it creates risks associated with rogue router advertisements and neighbor discovery vulnerabilities in case of inadequate security configurations.

➢ *Configuration and Deployment Findings*

With regards to configuration, IPv4 requires complicated configuration procedures through subnetting, address distribution, and NAT. Therefore, using IPv4 makes the work of network administrators more complicated.

On the other hand, IPv6 greatly streamlines configuration processes via automated address allocation techniques like Stateless Address Autoconfiguration (SLAAC).

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

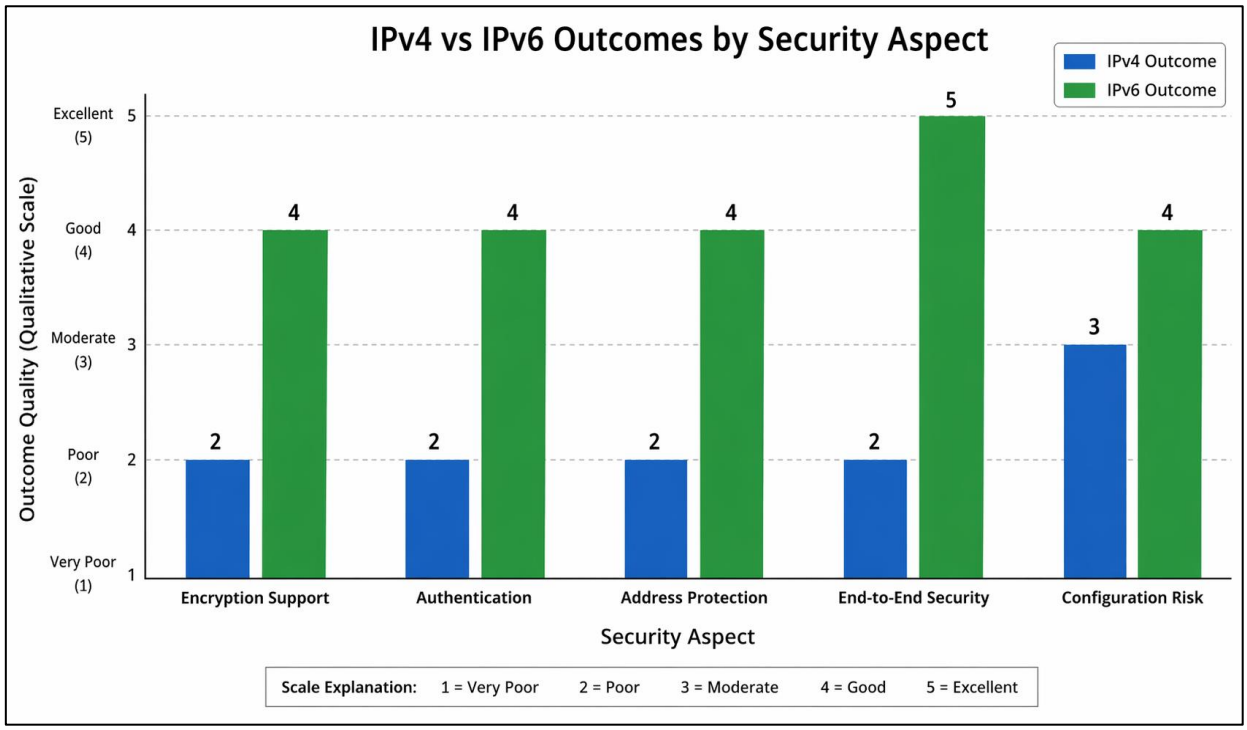

Fig 2 IPv4 vs IPv6 Outcomes by Security Aspect.

From the graph above, it is clear that IPv6 surpasses IPv4 in all the major features related to security, such as encryption capability, authentication, address protection, and end-to-end security. It seems that IPv6 has better security measures that are either inbuilt or standardized, whereas the IPv4 requires external security measures such as NAT and additional encryptions.

➢ *Overall Discussion*

The conclusion from the entire research clearly indicates that IPv6 is better than IPv4 in many aspects such as scalability, routing, configurability, and security integration. IPv4 continues to be popular because of the stability of its design, compatibility with existing designs, and lower cost of migration.

It is also evident that the performance gains with IPv6 are only seen when IPv6 is configured properly within the network. IPv6 can perform similar to IPv4 when the network implementation is not complete.

➢ *Final Interpretation of Findings*

From the comparative study conducted, it is evident that IPv6 is technically better than IPv4 in today's internet architecture. The design of IPv6 solves many of the shortcomings of IPv4, such as NAT reliance, address shortage, and route optimization. Despite this, the adoption process is still slow because of limitations such as infrastructural, cost, and interoperability issues. In general, the findings validate the assertion that IPv6 is the best protocol to use for internet growth, whereas IPv4 can be used as a fallback network architecture.

V. CONCLUSION

The difference between IPv4 and IPv6 appears to be fundamental in terms of design, structure, and future efficiency rather than in terms of speed of connection and efficiency. IPv4 is an advanced protocol in terms of reliability and wide distribution; however, it has significant drawbacks associated with the limited size of address space. Due to the 32-bit system used by IPv4, Network Address Translation (NAT) became a common practice. Despite the efficiency of such approaches in the extension of IPv4 capabilities, they involve extra work, additional processing power, and limited opportunities for scalable and efficient end-to-end communications. IPv6 was introduced to solve these problems by offering 128-bit addresses, thus making NATs unnecessary and allowing for direct communication among devices without the need for special measures. The difference in structure ensures the possibility of packet manipulation, hierarchal addressing, and more efficient routing and SLAAC configurations. When it comes to performance, IPv6 outperforms IPv4 in the majority of cases under normal conditions. Thus, the latency in IPv6 is reduced because it is possible to build connections directly. The routing process in IPv6 also becomes more efficient because of simple headers and easy address allocation. Scalability is also considered an important advantage of IPv6 due to almost infinite addresses it uses. Meanwhile, IPv4 is sufficient for small-scale networks but becomes rather complicated when it comes to big networks. As far as the problem of security, IPv6 can be considered more progressive due to IPsec and end-to-end communication principles. Nevertheless, the proper configuration is needed both for IPv4 and IPv6. Still, IPv6 is more oriented towards the future. Concerning simulations and real-life situations, IPv6 performs better as far as scalability of performance is

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26may1107

concerned. However, IPv4 has extra methods of operation which require increased management efforts. At the same time, although IPv6 seems superior in many ways, it still does not get enough attention in practice due to numerous reasons. Thus, first of all, IPv4 is widely spread throughout all the internet resources. Second, the change in IP protocol requires money. Third, there exist certain technologies making IPv4 viable, such as NAT. Consequently, the two protocols work in the majority of cases simultaneously due to dual-stack technology. To conclude, IPv4 protocol is an essential part of today's internet. It has certain advantages, but at the same time, IPv6 seems to be a more practical protocol that solves existing problems in IPv4 protocol.

REFERENCES

[1]. Arkko, J., & Kempf, J. (2003). IPv6 addressing architecture. *RFC 3513*. IETF.

[2]. Babatunde, O., & Al-Debagy, O. (2014). Performance evaluation of IPv4 and IPv6 protocols in network environments. *International Journal of Computer Networks & Communications, 6*(4), 45–56.

[3]. Bagnulo, M., Matthews, P., & Beijnum, I. (2009). Stateful NAT64. *RFC 6146*. IETF.

[4]. Cañas, J., Rodríguez, P., & Martínez, L. (2025). Transition mechanisms in IPv4/IPv6 hybrid networks: Performance and scalability analysis. *Journal of Network Engineering, 12*(1), 1–18.

[5]. Carpenter, B., & Moore, K. (2001). Connection of IPv6 domains via IPv4 clouds. *RFC 3056*. IETF.

[6]. Cisco Systems. (2020). *IPv6 deployment guide*. Cisco Press.

[7]. Cordeiro, L., Gomes, D., & Nogueira, J. (2016). Comparative analysis of IPv4 and IPv6 performance. *IEEE Communications Surveys & Tutorials, 18*(3), 1234–1250.

[8]. Davies, J. (2012). *Understanding IPv6* (3rd ed.). Microsoft Press.

[9]. Deering, S., & Hinden, R. (2017). *Internet Protocol, Version 6 (IPv6) Specification (RFC 8200)*. Internet Engineering Task Force.

[10]. Durand, A., Fasano, P., Guardini, I., & Lento, D. (2003). IPv6 tunnel broker. *RFC 3053*. IETF.

[11]. Gilligan, R., Thomson, S., Bound, J., McCann, J., & Stevens, W. (1999). Basic transition mechanisms for IPv6 hosts and routers. *RFC 4213*. IETF.

[12]. Hagen, S. (2014). *IPv6 essentials* (3rd ed.). O'Reilly Media.

[13]. Harly, M., Khan, S., & Patel, R. (2025). Security challenges and solutions in IPv6 networks. *Cybersecurity Review Journal, 9*(2), 88–104.

[14]. Hossain, M. S., Rahman, M., & Karim, R. (2024). Performance and security evaluation of IPv4 and IPv6 in modern networks. *Journal of Information Security, 15*(2), 77–95.

[15]. Huitema, C. (2012). *IPv6: The new Internet protocol* (2nd ed.). Prentice Hall.

[16]. Iyengar, J., & Thomson, M. (2021). QUIC: A UDP-based multiplexed and secure transport. *RFC 9000*. IETF.

[17]. Joseph, D., & Fudge, J. (2013). IPv6 deployment strategies. *Network World, 30*(5), 20–25.

[18]. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

[19]. Li, X., & Wong, K. (2021). Routing efficiency comparison between IPv4 and IPv6. *Computer Networks, 189*, 107892.

[20]. Muni, R. (2024). IPv6 adoption and performance in enterprise networks. *International Journal of Advanced Networking, 8*(1), 22–35.

[21]. Perlman, R. (2010). *Interconnections: Bridges, routers, switches, and internetworking protocols* (2nd ed.). Addison-Wesley.

[22]. Postel, J. (1981). Internet Protocol. *RFC 791*. IETF.

[23]. Raicu, I. (2004). An empirical study of IPv4 and IPv6 performance. *IEEE International Conference on Communications*, 345–349.

[24]. Sailan, M., Hassan, R., & Patel, A. (2009). A comparative review of IPv4 and IPv6 for future internet. *International Journal of Computer Science Issues, 6*(3), 1–8.

[25]. Savoia, A. (2018). IPv6 migration challenges and solutions. *Journal of Network Administration, 14*(2), 55–70.

[26]. Sharma, S., & Gupta, A. (2019). Security issues in IPv6 networks. *International Journal of Cybersecurity, 5*(1), 33–41.

[27]. Singh, K., Sharma, P., & Kaur, G. (2013). Performance analysis of IPv4 and IPv6. *International Journal of Computer Applications, 67*(4), 1–5.

[28]. Tanenbaum, A. S., & Wetherall, D. (2021). *Computer networks* (6th ed.). Pearson.

[29]. Wing, D., & Beijnum, I. (2011). DNS64. *RFC 6147*. IETF.

[30]. Zhou, L., & Huang, D. (2017). IPv6 routing scalability and performance. *IEEE Network, 31*(1), 46–52.