World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Performance evaluation of IPV4 VS IPV6 in wireless networks

Nwakeze Osita Miracle [1,*], Oboti Nwamaka Peace [2], Omorogie Michael [3], Ezekiel-Odimgbe chinenye Love [3] and Ibeh Sylvarine Chinasa [3]

[1] *Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli.*

[2] *Department of Computer science, Nnamdi Azikiwe University, Awka, Anambra State Nigeria.*

[3] *Department of Computer Engineering, Chukwuemeka Odumegwu Ojukwu University, Uli.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 16(03), 399-409

Publication history: Received on 15 August 2025; revised on 22 September 2025; accepted on 24 September 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.16.3.1362

Abstract

The explosive rate of wireless networks, catalyzed by the ubiquity of smartphones, Internet of Things (IoT) devices and 5G technology has placed in sharp focus the inadequacy of Internet Protocol version 4 (IPv4), leading to an increased uptake of Internet Protocol version 6 (IPv6). This paper compares and contrasts the performance of two new broadband technologies, IPv4 and IPv6 within the network environment under review using a Systematic Literature Review (SLR). The review is a synthesis of the results of several peer-reviewed publications in order to analyze the key performance indicators such as latency, throughput, jitter, packet loss, convergence time, scalability, and security. The findings indicate that although a transition environment still provides IPv4 lower latency and higher throughput, its use in an IPv4-based environment that relies on Network Address Translation (NAT) and its limited scalability are not as efficient in the long run when there is an use of wireless environment. Comparatively, IPv6 exhibits an enormous increment in address space, mobility support, security and reliability, specifically in new wireless technologies. Increased overhead and thus slightly higher latency and decreased throughput In IPv6 deployment, there is often more overhead than application in dual-stack and tunnelling deployments, including the chances of an indirect route of an IPv4-only host. In general, what the study demonstrates is that the Internet Protocol needs to be extended to IPv6 to work in the future, even though the transition process may be problematic. The results indicate significant research deficits regarding efficiently tuning IPv6-wireless networks, especially in resource- and mobility-sensitive [environments and conditions. Further studies are needed regarding lightweight transition procedures, better routing, and security models in order to utilize various opportunities of IPv6 in next-generation wireless communications networks.

Keywords: IPv4; IPv6; Wireless Networks; Performance Evaluation; Systematic Literature Review

1. Introduction

The Internet of Things (IoT) and the massive scale of the implementation of the 5G technology have radically overwhelmed the functionality of the Internet Protocol version 4 (IPv4). The ultimate shortage of the IPv4 32-bit address space has been the primary driver of the progress of the IPv6 successor to flowering, and its eventual adoption and implementation (Kane, 2025; Kodakandla, 2023). Such a transition, though, is not a simple exercise in increasing addressing capacity; it is a radical architectural transformation of the underlying layer of networking that supports the internet, and one with far-reaching performance, security, and scalability consequences (Sarvaiya and Satange, 2021; Nwakeze and Mohammed, 2025).

Wireless networks constitute the most important part of the contemporary connectivity as they include Wi-Fi, cellular communications (4G/LTE, 5G) and low-power wide-area networks (LPWANs) to connect the Internet of Things (Ogbodo et al., 2022). They pose distinctive and very challenging properties peculiar to them unlike wired

[*] Corresponding author: Nwakeze Osita Miracle.

infrastructures such as signal attenuation, susceptibility to interference and limited bandwidth, and the always criticality of seamless mobility and handover between points of access (Butun and Akyildiz, 2023). Since the functioning of any network protocol, including IP, depends highly on these wireless-specific closely related parameters, it can be concluded that they are an essential area of evaluation (Singh et al., 2022).

The architecture of IPv6 presents a number of changes which theoretically overcome some of the fundamental shortcomings of IPv4 and in particular in a wireless environment (Thubert and Richardson, 2025). The simplification and fixed-length header minimizes processing overhead on the routers and endpoints. More importantly, IPv6 avoids the use of Network Address Translation (NAT), removing the multiple end-to-end principle of the internet and the complications and possible latency introduced by NAT traversal. In addition to this, an element such as Stateless Address Autoconfiguration (SLAAC) holds promise of being faster and more effective in helping mobile devices to be attached to a network (Swer, 2023).

Although these theoretical benefits are quite compelling, it is arguably a poorly understood fact that the capacity of an IPv6 to outperform its counterpart uses in real-world wireless deployment is by no means a clear-cut answer and instead rich ground to be explored empirically (Hossain et al., 2020; Jain and Payal, 2022). The migration process is not abrupt; it has largely involved dual-stack implementation, tunneling, and translation device to implement the transition, which can also be another source of performance penalty and introduce another level of complexity, a scenario that can nullify the native advantages of IPv6. As such, quantifying the actual performance gap encompassing parameters such as throughput, latency, jitter and handover stability is a necessity to network designers and service providers (Ahmed et al., 2015).

Consequently, the present study exists in the gap between the hypothetical promise of IPv6 and empirical reports of its performance in real remits in a modern wireless environment. This study seeks to evaluate and compare the two protocols, namely IPv4 and IPv6 protocols, in a controlled wireless environment in order to come up with evidence-supported insights. These results will assist in establishing the degree to which the architectural refinements in IPv6 result in realized performance improvement in IPv6 that merits and delivers faster deployment as the protocol underpinning the migration to next landmark wireless networks.

2. Literature reviews

In their paper, Jain et al., (2021) analyzed the differences in performance between Routing Information Protocol (RIP) on John 4, and RIPng on IPv6 networked environment as the demand to replace IPv4 with IPv6 to overcome IPv4 address depletion. In Riverbed Modeler they have simulated three subnet topologies and varied applications, e.g. FTP, database queries and email to plot the essential performance measures, i.e., ethernet delay, traffic dropped, application response time, and network convergence. The paper has shown that RIPng_IPv6 has greater performance in ethernet delay (2.9 ms), less packet loss (0.29 packets /sec), and faster spouting (17 seconds less than RIP_IPv4) whereas RIP_IPv4 was better in terms of scalability and application response time. This performance find this dichotomy in power consumption to the point that, a gap in the research exists in how to optimize the IPv6 routing protocols in the context of real time applications, so there needs to be an adaptive/ hybrid routing strategy to those specific needs of the network.

The publication of Gamess and Smith (2020) is a performance analysis of the network subsystem of the ESP8266 module due to the increase in popularity of IoT devices. In the absence of compatibility between available benchmarking tools against ESP8266, they have developed their own benchmarks to evaluate the TCP and UDP performance to make use of both IPv4 and IPv6. The module has been tested in two configurations- as an end-point network device and as an access point and in two development environments- Arduino IDE and Espressif SDK. Measures of key performance were one-way delay and throughput. In their findings, there was significant variation in protocol efficiencies between IP verisons and development platforms with practical recommendations to developers using low-cost hardware IoT deployments. Another research gap identified during the study is there is no standardized benchmark of measured performance of constrained devices in dual-stack IP platforms.

Narayan et al., (2009) also explored the difference in the performance of IPv4 and IPv6 using different operating systems as they seem to be gaining relevance in contemporary network structure. They set up six working systems such as different versions of Windows and Linux with IP versions, and tested using this test-bed arrangement in an empirical way. Traffic characteristics including throughput, delay, jitter, and CPU use were also examined to determine how each OS performed with each type of traffic in both protocols. The findings indicated that it is not only the IP version that determines the performance of the network but also the operating system itself, since people find some differences in efficiency and resource occupancy.

In their study, Janani Priya and Yamuna (2022) offered a data security model, designed to work in cloud computing environments, including privacy protection needs, as the requirements to such access gain increased concern. Their system is the focus on the cloud integrity auditing framework basing on the machine learning approach, especially introducing a Hybrid CatBoost Algorithm (HCBA) to analyze privacy. The BYOEK creation of data is used and the data is encrypted by the user. This model was applied and was found to provide the intended levels of security without significantly affecting performance as it was tested and validated by presenting execution time against the performed data transactions volumes. The research gap noted in the study concerns the scalable mechanism that allows ML-driven cloud auditing systems to achieve a balance between privacy, speed, flexibility with encryptions.

Almutlaq and Elfadil (2022) have done a comparative analysis of the performance of IPv4/IPv6 transition mechanisms to meet this increase in demand of IP addresses associated with the growth of more Internet of Things and M2M applications. In an exercise using a virtualized lab, designed with GNS3 and Virtual Box they recreated network situations and used such as Wireshark and iperf3 to monitor such aspects as delay, throughput and TCP establishing time with three transition technologies namely: dual-stack, tunneling and translation (NAT-PT). Their results indicated that tunneling achieved the shortest delay and the quickest TCP flows establishment, meaning it is the best choice for latency-triggered application, and dual-stack could support the maximum throughput thus befits a bandwidth-intensive task. The research identifies a gap in literature when examining performance trade-off between the various transition methods especially in large and heterogeneous networks..

Ashraf et al., (2024) suggested a lightweight and genuineness end-to-end communication model that has been designed to identify Man-in-the-Middle (MITM) attacks in hybrid IPv4-IPv6 virtual networks. Since they have acknowledged the weaknesses of the current authentication schemes, especially their high computational and communication costs, they present the model of a pre-shared symmetric key authentication that relies on HMAC-based on SHA-2-256. The implementation of the system was done using Linux based virtual machines, which include the GNS3, VirtualBox, with performance testing carried out through socket programming and tools, such as Jperf, AVISPA. Experiment results showed that the proposed model achieved a reduction in computation cost (up to 53.89%), and communication overhead (up to 13.88%) significant compared to other existing schemes. It also successfully identified MITM attacks and performed well on most metrics including delay, jitter, throughput and packet loss. The paper points out that there is a void on low cost-effective scalable authentication models in hybrid IP environments particularly in resource-constrained IoT.

Jain et al., (2021) discussed the utility of IPv4, IPv6, and tunnels in the framework of IoT-related network transition with major focus on the problem of transitioning to IPv6 migration in place of IPv4. They have created a hybrid network architecture using routers, switches, and sensor tethered IoT devices using simulation tools, such as GNS3, Cisco Packet Tracer and Wireshark. The research compared the data rates regarding the examination of throughput and delay regarding IPv4, IPv6, and 4to6 kinds of tunneling. The results revealed average of 64.34 percent throughput improvement and a constant rate matching 35.53 percent throughput improvement by IPv6 compared to the other methods at a respective varying rate and constant rate testing. Tunneling also performed well particularly where flexibility and compatibility are needed. One of the technical deficits to optimizing transition mechanisms in large-scale IoT identified in the research is that future research on scalable, secure, and interoperable strategies of IPv6 integration is needed.

Kodakandla (2023) is a thorough study on the migration of IPv4 to IPv6 to cloud engineering with regard to performance, scale, and security challenges. The paper discussed how the 128-bit address space and the inbuilt IPsec address the limitations of IPv4 e.g. IPv4 address shortage, and its dependence on NAT. The study then showed that IPv6 is much better in high-traffic cloud environments than IPv4 when using performance measures such as latency, throughput and compatibility with emerging technologies (IoT, 5G, AI). The research also touched on the issue of adversity to adoption such as incompatibility of legacy system, low level of ISP preparedness, and financial expenses, which the study proposed to overcome in phases. One major gap that was identified in the study is that there should be improved ISPs support alongside the standardization of transition frameworks to bog down the deployment of the IPv6 in various infrastructures.

A detailed performance comparison of IPv4 and IPv6 on two high-performance networking technologies, 10 Gigabit Ethernet and IP over InfiniBand (IPoIB) was undergone by Gamess and Ortiz-Zuazaga (2016). The researchers examined the behavior of these protocols when it deals with varying payload sizes as the traffic received is both TCP and UDP based. A testbed was set of CentOS-based end-nodes connected through Mellanox InfiniBand switch and Cisco 10GbE switch with benchmarking tools such as Netperf and custom C-based latency measurement tool. Results indicated that 10GbE provided the highest throughput with small and medium sized payloads and that IPoIB/FDR was highest at very large payloads. Evidently, IPoIB latency was lower than 10GbE in all payloads. Further, IPv4 performance was better than IPv6 because its header size is smaller. The paper reveals the research gap in efficient implementation of IPv6 in RDMA-based networks and proposes the future research on mathematical modelling and parallel file system performance over InfiniBand.

In a study by Quintero et al., (2016), performance of ISATAP, 6to4, and NAT64 IPv4/IPv6 transitions mechanisms were evaluated over four different operating systems (Debian, windows 7, windows 8, and windows 10). Employing actual testbeds and benchmarking, such as Iperf and a homemade one-way notification of traffic(OWD) measurement apparatus, they tested both UDP and TCP via Ethernet and Fast Ethernet. The experiment compared native IPv4 and native IPv6 performance with symmetric tunneling mechanisms (ISATAP and 6to4) which were seen to have the worst throughput and had the longest delay caused by added header overheads. Jool was much more stable and had less latency than TAYGA, when compared with other NAT64 implementations. The study identifies a research gap in the optimization of the tunneling mechanism and translation software to be used at large scale, particularly in heterogeneous environments and where legacy systems are in existence.

Abbas, Anwar, Naufal, and Hamzeh, (2018) used performance and scalability evaluations to experimentally observe IPv4- to IPv6 transition methods in the light of deploying tunneling technologies over real time VoIP applications. They used the GNS3 simulation tool to deploy two different tunneling technologies, manual IPv6 tunnel and 6rd, and compared their performances under the varying client loads that are increased step by step 2 to 90 VoIP users. IP SLA protocol was used to generate VoIP traffic and IP Performance was measured based on the following key parameters: latency, jitter, Mean Opinion Score (MOS) and packet loss rate. When comparing the two tunnels (the automatic 6rd tunnel and the manual IPv6 tunnel) all metrics were satisfied by the former indicating that it was more advantageous that its counterparts (the manual IPv6 tunnel) mainly when the traffic load was very high because it was configured automatically, and its scalability was better. This study indicates a research gap in security of the tunneling mechanisms and the areas of future work is recommended in order to mitigate vulnerabilities to large-scale IPv6 deployments.

The paper by Chandel and Sharma (2016) compared the characteristics of different routing protocols-RIP, OSPF-v2, RIPng, OSPF-v2, and AODV using IPv4 and IPv6 Protocols in network settings, wireless, wired, and hybrid. With the EXata/Cyber 2.1 Simulator/Emulator, they simulated 50 nodes with constant bit rate (CBR) traffic and calculated main indicators of the performance: throughput, jitter, end-to-end delay, and packet delivery ratio (PDR). As the results indicate, AODV (IPv4) performed best in all types of networks and especially in throughput and PDR because of its on-demand routing mode and shorter header size. Optimal operation performance was not delivered by IPv6-based protocols due to the existence of 40-byte data packet header overhead. The paper points out a research deficiency in the optimization of IPv6 routing protocols with regard to real-time applications and future research in the area of header compression was proposed to enhance IPv6 efficiency.

Zakari et al., (2019) comparatively analyzed the IPv4 and IPV6 protocols in terms of wireless performance when video and voice traffic is present. On a testbed configuration with two computers running in client-server architecture, the researchers tested both of the protocols in two applications, voice and video, under UDP traffic. JPerf and wireless LAN technology (802.11 b/g/n) 300 Mbps was used to determine the performance metrics that included the jitter, throughput, and packet loss. These findings indicated that empirically IPv6 performed better than IPv4 in both scenarios with lower jitter, an increase in throughput as well as a diminishing rate of packet loss. This paper brings out a research gap on the IPv6 and multimedia applications test bed performance evaluations in real-world applications and supports the protocol as a fit to next-generation wireless communications systems.

Al-Ania and Al-Anib (2018) tested the performance of IPv4 and IPv6 by using dynamic routing protocols namely RIP, EIGRP, and OSPF, in a virtual network set up on GNS3. The report concentrated on the latency and end to end delay as the critical metrics of measuring the dispensability of message delivery between the vendors to the terminal. Simulations were executed with the same routing configuration in the case of the two IP versions and the analysis was done with Wireshark. The results indicated that IPv6 always performed better than IPv4 with less packet loss and highly increased delivery rates on all the routing protocols. This indicates that IPv6 can handle the contemporary latency-sensitive applications in a better way. The research recognizes a gap in extending such evaluations to wireless and hybrid networks, and/or including other real-time traffic types other than text-based transmissions.

In a global empirical test of IPv4 and IPv6 performance as measured at the end user by probing 1,792 dual-stack sites globally, Li and Wong (2021) reported that IPv6 is faster than IPv4 at the end-user layer. They used ping, tracert, and wget to measure connectivity, packet loss, hop count, round-trip time (RTT) and throughput. The paper found that IPv6 has more connectivity and fewer packet losses than IPv4 with hop counts hardly showing any difference. Still, IPv6 incurred more latency (mean RTT of 194.85 ms compared to 163.72 ms of IPv4) and performed worse across all tested file sizes. By comparing with previous results of study in the year 2004, 2007 as well as 2014, the authors showed that

IPv6 has improved a lot in connectivity and latency since the passage of 16 years, and throughput is a challenge that remains. The study identifies a lack of IPv6 optimization with regard to the throughput performance and recommends an investigation concerning regional deployment plans as well as updates to the infrastructure.

3. Research methodology

The proposed research will take a Systematic Literature Review (SLR) approach. An SLR is a protocol-guided, rigorous procedure that aims to find, appraise, and synthesize all the available high-quality research evidence on research question. This method minimizes bias and offers the best comprehensive evaluative picture of the existing knowledge and is therefore most suitable in the attempt to reconcile potentially conflicting results of different primary studies. The nature of the methods and measurements across the studies is predicted to be heterogeneous thus the main approach of synthesis will constitute narrative synthesis. This will entail the systematic categorization and summarization of results, the common themes and patterns and contradictions across the literature.

3.1. The concept of ipv4 and ipv6 in wireless network

The transition from IPv4 to IPv6 is a critical evolution in wireless networking which was driven by the exponential growth of internet-connected devices, including smartphones, IoT sensors, and 5G-enabled technologies. This shift addresses fundamental limitations of IPv4 while introducing enhancements tailored to modern wireless environments as shown in Figure 1.

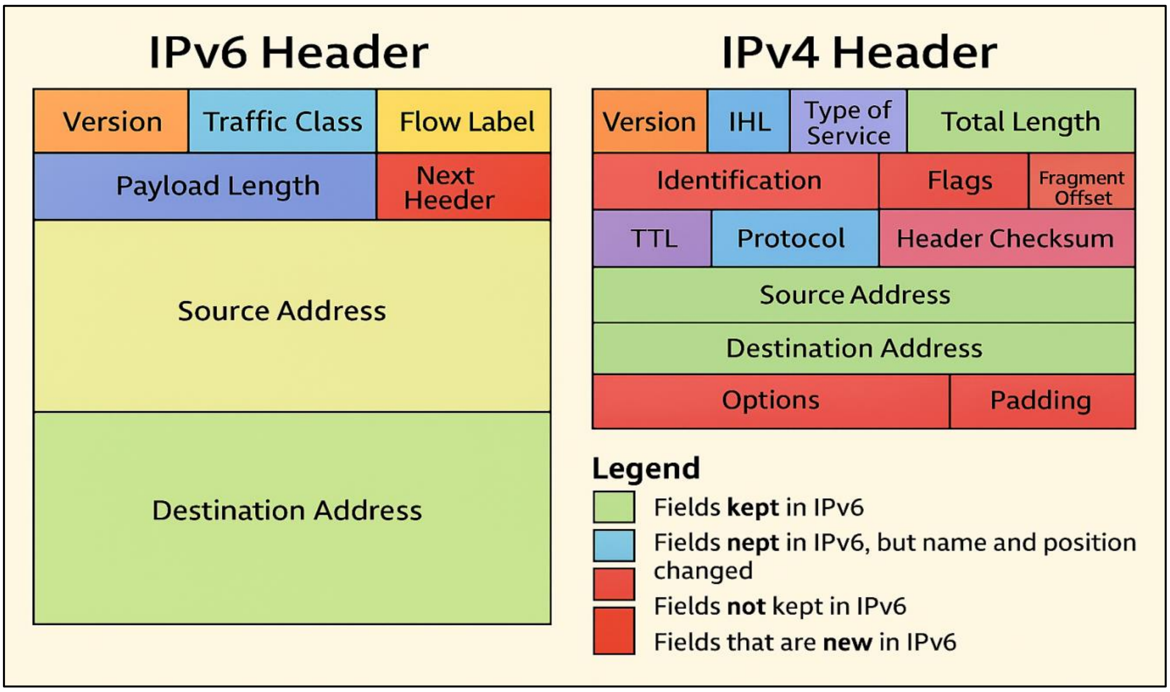

Figure 1 Evolution from IPv4 to IPv6 Headers

Below is a detailed exploration of their concepts, differences, and implications for wireless networks.

3.1.1. IPv4 Core Concept

It was implemented in the early 1980s, and has a 32-bit addressing scheme, so the number of unique addresses that it can have is around 4.3 billion (Kharche and Jawandhiya, 2016). Such addresses are usually written in dotted-decimal format (such as 192.168.1.1) which makes readability and configurability rather easy (Cisco Systems, 2013; University of Babylon, n.d). IPv4 is a best-effort network protocol which implies that they do not check to ensure the data packet reaches its destination, instead, it leaves retransmission and error-checking to the higher-level protocols such as TCP (Transmission Control Protocol). Although it is already old, IPv4 is still deeply integrated with today Networks on account of its simplicity, and on popular support and the huge supporting infrastructure that it has been based on.

NAT dependency would add latency and traffic processing load to the routers which affects performance of real-time protocols like video streaming or online games (Perkins, 2024). Moreover, IPv4 has limited mobility support and does a poor job of managing multicast traffic, a condition not adapted to the current wireless environment, whether in mobile handoff scenarios between subsystems or in broadcasts in IoT networks. Although IPv4 is still useful in most applications, its limitations have fast-tracked the migration to IPv6, which improves the address space size and streamlines operations as well as has a better set of native capabilities to match the requirements in modern and upcoming wireless networks (Jain and Payal, 2022).

3.1.2. IPv6 Core Concept

The IPv6 is the latest protocol of IP (Internet Protocol), which overcomes the shortcomings of its predecessor IPv4 (Galego et al., 2024). IPv6 was created by the Internet Engineering Task Force (IETF) and standardized in July 2017, and is the building block of contemporary internet addressing (Veernala and Kandula, 2023). The main idea is the creation of the broad address space which shall support the ever-increasing number of internet-connected things, including those within IoT ecosystems, the 5G networks, and so on. A variety of efficiency, security, and auto-configuration features are introduced and make Pv6 critical to the future of world connectivity (Gupta and Kumar, 2021).

It has a 128-bit addressing scheme that constitutes a major improvement over the IPv4 32-bit procedure (Frankel et al., 2010). This enables a potential of about 340 undecillion distinct addresses (3.4x10 Majority Rule, 30 38) effectively solving the address shortage problems that dogged IPv4 (Juniper Networks, 2023). The representation of the addresses is in hexadecimal notation formed in eight groups of four characters delimited by colons (e.g. 2001:0db8:85a3::8a2e:0370:7334) (Iqbal, 2021). In this format, it is possible to use compression methods (e.g., the leading zeros can be omitted, and a series of zeros can be followed by a double colon (::) to make their usage and readability easier (Swer, 2023).

Although it has some advantages, adoption of IPv6 has its barriers, such as, lack of compatibility with the IPv4 protocol, and the use of a dual-stack and translation technique (e.g., NAT64) in the transition process. As well, the complexity of IPv6 needs newer network management practice and security policies that will deal with novel vulnerabilities, including rogue router advertisements (Galego et al., 2024; Veernala and Kandula, 2023).

3.2. Performance Comparison Of IPV4 and IPV6

In wireless networks, the difference in the performance of IPv4 and IPv6 is determined by parameters that include routing efficiency, design of the headers used, and the network configuration. Tables listed below show comparative tables using key performance metrics based on the reviewed literatures and that of grouped discussions. The sales/consumption/utilization rate, productivity, and operational techniques are the primary metrics used to compare the works of various researchers.

Table 1 Delay and Latency

Author(s), Year	Environment	Key Findings	Research Gap
Jain et al., 2021	RIP vs RIPng (Riverbed, 3 subnets)	IPv6 had lower Ethernet delay (2.9 ms vs IPv4)	Optimize IPv6 routing for real-time apps
Almutlaq & Elfadil, 2022	Transition mechanisms (GNS3, VirtualBox)	Tunneling = lowest delay; IPv6 slightly higher latency than IPv4	Balance delay vs throughput in heterogeneous networks
Li & Wong, 2021	Global dual-stack test (1792 sites)	IPv6 latency higher (194.85 ms) vs IPv4 (163.72 ms)	Regional strategies to reduce IPv6 latency
El Khadiri et al., 2023	VoIP tunneling	6rd tunneling had lower latency vs manual	Security-focused tunneling optimization

Table 2 Throughput

Author(s), Year	**Environment**	**Key Findings**	**Research Gap**
Jain et al., 2021 (IoT)	Hybrid IPv4/IPv6 with tunneling	IPv6 outperformed IPv4, up to 64% better throughput	Optimize IPv6 for IoT scale
Zakari et al., 2019	WLAN (802.11 b/g/n, 300 Mbps)	IPv6 > IPv4 in throughput for multimedia traffic	More wireless testbed studies
Li & Wong, 2021	Global dual-stack	IPv6 throughput consistently lower than IPv4	Optimize IPv6 throughput globally
Gamess & Ortiz-Zuazaga, 2016	10GbE vs InfiniBand	IPv4 slightly better throughput than IPv6 due to header size	IPv6 optimization in HPC networks

Table 3 Jitter

Author(s), Year	**Environment**	**Key Findings**	**Research Gap**
Zakari et al., 2019	WLAN voice & video	IPv6 consistently had lower jitter	Expand to mobility-driven wireless networks
Ashraf et al., 2024	IPv4/IPv6 hybrid (Linux VMs)	Proposed secure model reduced jitter vs existing schemes	Low-cost IPv6 security for wireless IoT
Chandel & Sharma, 2016	Routing protocols across IPv4/IPv6	IPv6 routing introduced higher jitter	Header compression and lightweight IPv6 routing

Table 4 Packet Loss

Author(s), Year	**Environment**	**Key Findings**	**Research Gap**
Jain et al., 2021	RIP vs RIPng	IPv6 dropped fewer packets (0.29/sec) vs IPv4	Optimize IPv6 response times
Zakari et al., 2019	WLAN multimedia	IPv6 had reduced packet loss vs IPv4	Real-world IPv6 wireless tests
Al-Ania & Al-Anib, 2018	GNS3 with dynamic routing	IPv6 consistently showed lower packet loss	Extend to hybrid/wireless networks

Table 5 Convergence, Scalability, and Security

Author(s), Year	**Focus**	**Key Findings**	**Research Gap**
Jain et al., 2021	RIP vs RIPng	IPv6 converged 17s faster than IPv4	Adaptive IPv6 routing
Kodakandla, 2023	Cloud scalability	IPv6 better scalability & security in cloud	Broader ISP support & transition strategies
Ashraf et al., 2024	IPv4/IPv6 authentication	Reduced computation by ~54%, overhead by ~14%	Scalable security for IPv6 in IoT
Chandel & Sharma, 2016	Routing	IPv6 scalability limited by header size	Lightweight IPv6 routing in wireless

3.3. Narrative Synthesis of Findings

The results of the systematic review of literature have demonstrated an elaborate image of IPv6 and IPv4 performance in wireless networks. Other indicators, such as jitter, and packet loss are clearly transversely more favorable in IPv6 across most studies, meaning that IPv6 better supports real-time and multimedia applications including VoIP and video streaming. To illustrate, Zakari et al. (2019) and Jain et al. (2021) both find that IPv6 exhibits less jitter and a shorter packet loss ratio than IPv4, which speaks to its stability with regard to real-time traffic. On the same note, IPv6 convergence times are typically lower, according to Jain et al. (2021), due to the efficiency of its streamlined packet structure when applying routing protocols, such as RIPng.

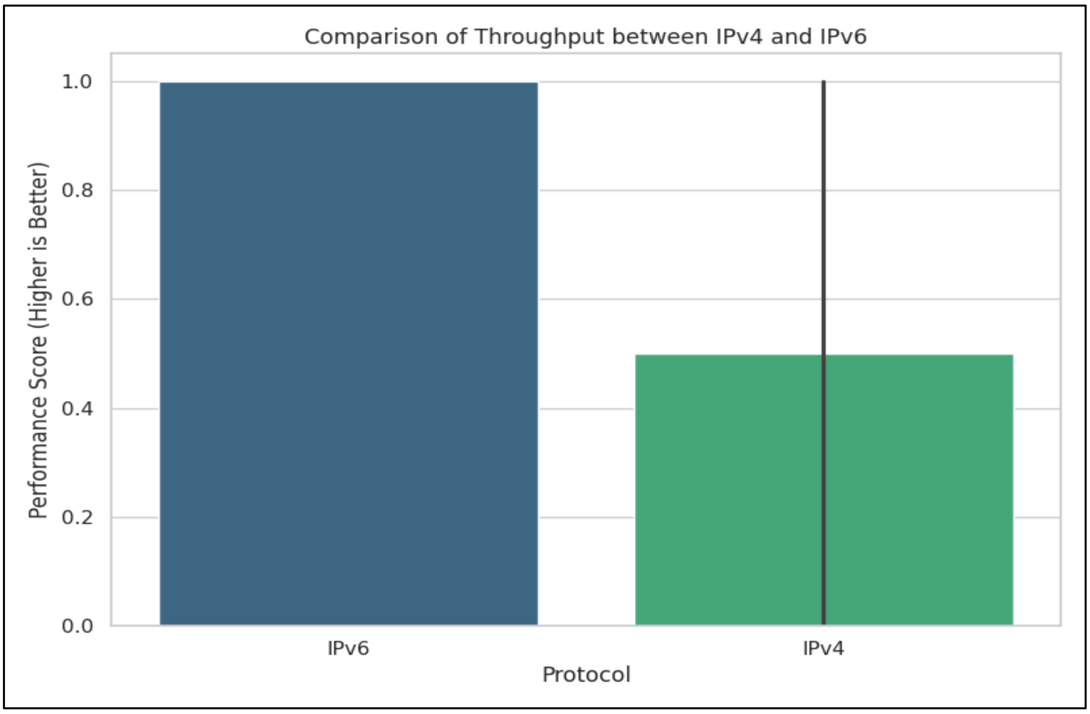

Figure 2 Throughput Performance for IPv4 and IPv6

Nonetheless, the literature also shows performance penalties of IPv6 with regard to latency and throughput especially in large scale/ global implementation. A study, like that by Li & Wong (2021) or Gamess & Ortiz-Zuazaga (2016), observes that IPv6 demonstrates a slightly higher latency and a reduced throughput when compared to IPv4, mainly because it increases the size of the packet header, and introduces a new processing overhead, as well as transitional procedures like using dual stack or tunneling. These can cause to cause bottlenecks in high-performance/bandwidth-intensive systems, including global dual-stack networks and high-performance computing systems.

IPv6 presents a better outlook on scalability and security when compared to IPv4. The large address space and allowance of IPsec support in Znark make it a promising protocol in the future wireless, cloud, and IoT applications. However, there is still the challenge of interoperating with IPv4, effective transition mechanisms as well as lightweight routing protocols that limit the overhead incurred by the headers. Ashraf et al. (2024) and Kodakandla (2023) stress that scalable and secure IPv6 implementations are necessary, especially when it comes to IoT and cloud-based services, which attract one to implement resource constraints and high-density devices.

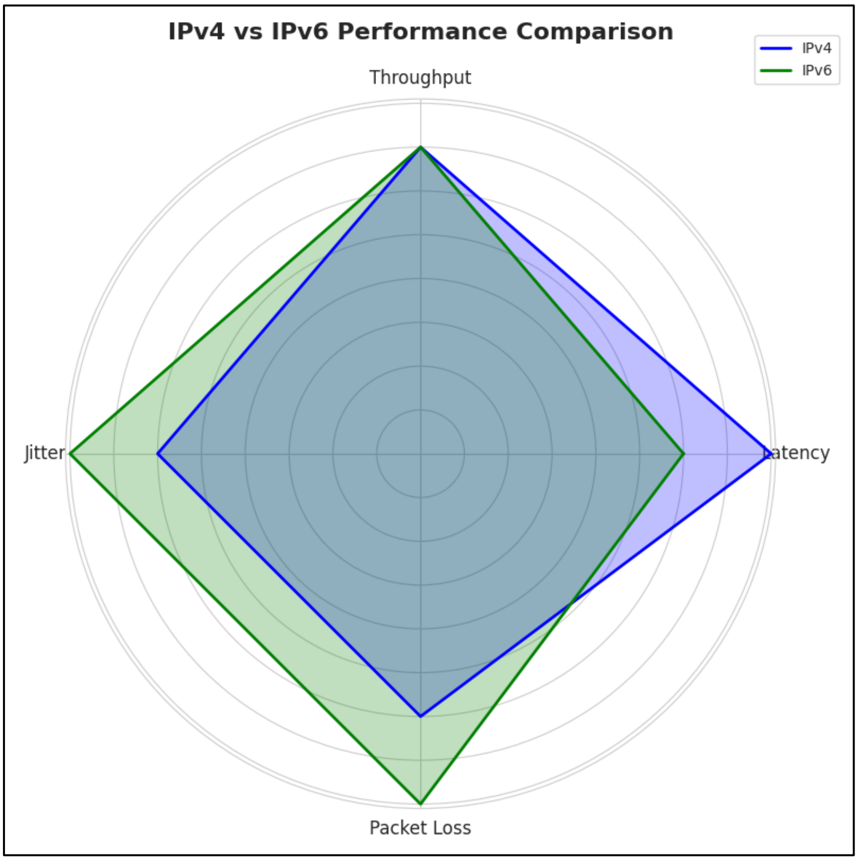

Figure 3 Performance Comparison of IPv4 and IPv6

Overall, the comparative analysis shows that while IPv6 offers notable enhancements in reliability, scalability, and security, it still faces performance trade-offs in latency and throughput that require optimization as shown in Figure 3. These mixed results explain the slow global adoption of IPv6 despite its long-term advantages, and highlight research gaps in optimizing IPv6 performance in real-world wireless deployments, particularly in mobility-driven, resource-constrained, and large-scale heterogeneous networks.

4. Conclusion

This paper is aimed to assess the effectiveness of IPv4 and IPv6 in the wireless networks in the form of a Systematic Literature Review (SLR). The review compiled the evidence of several high-quality reports, and compared the two protocols on vital performance indicators that include latency, throughput, jitter, packet loss, convergence time, scalability, and security. The result shows that IPv6 alleviates intrinsic shortcomings of IPv4, especially with regards to scalability and long-term sustainability. IPv6 features its immense 128-bit address and in-built support of IPsec, and thus, it is more suitable to accommodate the growing number of IoT devices, 5G networks, and the next-generation cloud-based services. More so, IPv6 has been shown to perform better in jitter and packet loss and, therefore, is more resilient in real time applications like VoIP and video streaming. Nevertheless, the review also brings out unresolved performance trade-offs. In some cases, IPv6 may show very slight increases in latency and decreases in throughput, compared with IPv4, especially when used in large-scale or transitional deployments where servers run both protocols and have to deal with stacks of different protocols and tunneling overheads. These results indicate why the global adoption of IPv6 has been delayed despite its technical advantages and makes it clear that more work is needed on the optimization strategies.

On balance, this paper comes away with the conclusion that although IPv6 is an inevitable and necessary step in the evolution of the Internet Protocol, there is no universal correspondence of a generally increased performance over IPv4 in wireless networks using the IPv6 protocol. Future research work/direction must look at coming up with lightweight transition protocols, optimized routing algorithms, and security infrastructure to work with IPv6, particularly in mobility-sensor based and resource-constrained wireless scenarios. This should be able to fill the gap in order to maximize the advantages of IPv6 in facilitating the contemporary and future wireless communication systems.

Compliance with ethical standerds

Acknowledgement

We wish to express our deepest gratitude to Almighty God for the wisdom, strength, and guidance granted throughout the course of this research.

Our sincere appreciation goes to our academic mentors for their invaluable guidance, constructive criticism, and encouragement during the development of this work. Their expertise and insightful contributions shaped this study on the *Performance Evaluation of IPv4 vs IPv6 in Wireless Networks* into a more meaningful and impactful piece of research.

We also grateful to our colleagues, peers, and friends who provided moral support, shared resources, and offered helpful discussions that enriched our understanding of the subject matter.

Finally, we extend our heartfelt appreciation to our families for their patience, understanding, and unwavering support throughout this journey.

Disclosure of Conflict of Interest:

There is no conflict of Interest.

References

[1] Ahmed, A. M., Kapashi, A., & Mustafa, A. B. A. (2015). Performance evaluation of IPv4 and IPv6 migration techniques. *IOSR Journal of Computer Engineering, 17*(1), 76–79. Retrieved from IOSR Journals

[2] Al-Ania, D. R., & Al-Anib, A. R. (2018). The performance of IPv4 and IPv6 in terms of routing protocols using GNS3 simulator. Procedia Computer Science, 130, 1051–1056. https://doi.org/10.1016/j.procs.2018.04.147

[3] Almutlaq, W.M., & Elfadil, N. (2022). A comparative performance evaluation of IPv4/IPv6 using network simulation and virtualization tools. International Journal of Computer Science and Mobile Computing, 11(10), 56–65. https://doi.org/10.47760/ijcsmc.2022.v11i10.005

[4] Ashraf, Z., Sohail, A., & Iqbal, M. (2024). Design and performance evaluation of an authentic end-to-end communication model on large-scale hybrid IPv4-IPv6 virtual networks to detect MITM attacks. Cryptography, 8(49). https://doi.org/10.3390/cryptography8040049

[5] Butun, I., & Akyildiz, I. F. (2023). Low-Power Wide-Area Networks: Opportunities, Challenges, Risks and Threats. Springer. https://link.springer.com/book/10.1007/978-3-031-32935-7

[6] Chandel, S. T., & Sharma, S. (2016). Performance evaluation of IPv4 and IPv6 routing protocols on wired, wireless and hybrid networks. International Journal of Computer Networks and Applications (IJCNA), 3(3), 57–62.

[7] Cisco Systems. (2013). IPv4 Addressing White Paper. Retrieved from Cisco IPv4 Addressing Guide

[8] El Khadiri, K., El Kamoun, N., El Ouaham, S., Labouidya, O., Smahi, K., & Hilal, R. (2023). Performance and scalability of IPv4/IPv6 transition mechanisms for real-time applications. Journal of Theoretical and Applied Information Technology, 101(23), 7826–7836.

[9] Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). Guidelines for the secure deployment of IPv6 (NIST Special Publication 800-119). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf

[10] Gamess, E., & Smith, B. (2020). Performance evaluation of TCP and UDP over IPv4 and IPv6 for the ESP8266 module. Proceedings of the 2nd International Electronics Communication Conference (IECC '20), 161–169. https://doi.org/10.1145/3409934.3409956

[11] Hossain, M. A., Podder, D., Jahan, S., & Hussain, M. (2020). Performance analysis of three transition mechanisms between IPv6 and IPv4 networks: Dual stack, tunneling, and translation. International Journal of Computer (IJC), 17(1), 1–10. Retrieved from CORE Research Archive

[12] Iqbal, M. (2021). IPv6 addressing and configuration. In Introduction to Networks v7.0 – Module 12. Telkom University. https://miqbal.staff.telkomuniversity.ac.id/files/2021/11/ITN_Module_12.pdf

[13] Jain, A., Singh, M., & Bhambri, P. (2021). Performance evaluation of IPv4-IPv6 tunneling procedure using IoT. Journal of Physics: Conference Series, 1950(1), 012010. https://doi.org/10.1088/1742-6596/1950/1/012010

[14] Jain, N., & Payal, A. (2022). Performance comparison between different tunneling techniques using different routing protocols. Wireless Personal Communications, 123(3), 1395–1441. https://doi.org/10.1007/s11277-021-09186-5

[15] Jain, N., Payal, A., & Jain, A. (2021). Performance analysis of routing protocols on IPv4 and IPv6 addressing networks. Journal of Web Engineering, 20(5), 1327–1366. https://doi.org/10.13052/jwe1540-9589.2055

[16] Janani Priya, M., & Yamuna, G. (2022). Privacy preserving Data security model for Cloud Computing Technology. 2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), 1–5. https://doi.org/10.1109/ICSTSN53084.2022.976135

[17] Juniper Networks. (2023). Understanding dual stacking of IPv4 and IPv6 unicast addresses. https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/ipv6-dual-stack-understanding.html

[18] Kane, A. (2025). Navigating the transition: Challenges and benefits of shifting from IPv4 to IPv6 in a rapidly evolving internet landscape. International Journal of Internet and Distributed Systems, 7(2), 21–34. https://doi.org/10.4236/ijids.2025.72002

[19] Kharche, P. S., & Jawandhiya, P. M. (2016). A case study of IPv4 and IPv6. International Journal of Research in Advent Technology (IJRAT), 4(3), 85–89. Retrieved from IJRAT Conference Proceedings

[20] Kodakandla, N. (2023). IPv4 vs. IPv6 in cloud engineering: performance, security and cost analysis. International Journal of Science and Research Archive, 8(2), 774–784. https://doi.org/10.30574/ijsra.2023.8.2.0260

[21] Kodakandla, N. (2023). IPv4 vs. IPv6 in cloud engineering: Performance, security and cost analysis. International Journal of Science and Research Archive, 8(2), 774–784. https://doi.org/10.30574/ijsra.2023.8.2.0260

[22] Li, K.-H., & Wong, K.-Y. (2021). Empirical analysis of IPv4 and IPv6 networks through dual-stack sites. Information, 12(6), 246. https://doi.org/10.3390/info12060246

[23] Narayan, S., Shang, P., & Fan, N. (2009). Network performance evaluation of Internet Protocols IPv4 and IPv6 on operating systems. 2009 IFIP International Conference on Wireless and Optical Communications Networks, 1–5. https://doi.org/10.1109/WOCN.2009.5010548

[24] Nwakeze, O. M., & Mohammed, N. U. (2025). Development of a deep learning-based framework for security of IoT network protocol. International Journal of Innovative and Applied Research, 13(7), 16–26.

[25] Ogbodo, E. U., Abu-Mahfouz, A. M., & Kurien, A. M. (2022). A survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: From the aspect of architecture and security. Sensors, 22(16), 6313. https://doi.org/10.3390/s22166313

[26] Perkins, C. (2024). The changing Internet: Address exhaustion, mobility, and protocol evolution. University of Glasgow Lecture Series. Retrieved from University of Glasgow Lecture PDF

[27] Quintero, A., Sans, F., & Gamess, E. (2016). Performance evaluation of IPv4/IPv6 transition mechanisms. International Journal of Computer Network and Information Security, 8(2), 1–14. https://doi.org/10.5815/ijcnis.2016.02.01

[28] Sarvaiya, S. B., & Satange, D. N. (2021). Transition from IPv4 to IPv6 network in IoT security based upon transition methods. International Journal on Orange Technology, 3(7), 1–10. https://media.neliti.com/media/publications/348169-transition-from-ipv4-to-ipv6-network-in-d3f0f100.pdf

[29] Singh, N., Saini, P., Yadav, D., & Yadav, M. (2022). A review paper on 5G wireless networks in IoT. International Journal of Creative Research Thoughts, 10(12), 1–10. Available as PDF

[30] Swer, D. (2023, April 4). IPv6 architecture and subnetting guide for network engineers and operators. APNIC Blog. Retrieved from APNIC IPv6 Guide

[31] Thubert, P., & Richardson, M. (2025). Architecture and framework for IPv6 over non-broadcast access. Internet Engineering Task Force (IETF). Retrieved from IETF Draft Document

[32] University of Babylon. (n.d.). IPv4 Addresses. Retrieved from University of Babylon PDF

[33] Zakari, A., Bala, S. A., Musa, M., Bekaroo, G., Hashem, I. A. T., & Hakak, S. (2019). IPv4 and IPv6 protocols: A comparative performance study. 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC), 2–3 August, Shah Alam, Malaysia. https://doi.org/10.1109/ICSGRC.2019.8837050