DOI: http://dx.doi.org/10.26483/ijarcs.v16i4.7307

ISSN No. 0976-5697

Volume 16, No. 4, July-August 2025

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

UNDERSTANDING THE EVOLUTION OF INTERNET PROTOCOLS: AN IN-DEPTH REVIEW OF IPV4 AND IPV6: A COMPARATIVE REVIEW OF TRANSITION CHALLENGES AND SOLUTIONS

Yash Muni
Independent Researcher
USA

***Abstract*—**The exponential growth of internet-connected devices has led to increased pressure on the current Internet Protocol infrastructure, primarily IPv4, which is limited by its 32-bit addressing scheme. This paper compares and contrasts IPv4 with its successor, IPv6, looking closely at their respective technical foundations, structural changes, and performance consequences. The Internet Engineering Task Force (IETF) launched IPv6, which adds a 128-bit address space, reduced headers, better routing efficiency, built-in security methods, and native support for multicast communication, among other improvements. The paper examines the evolution of IP, the limitations of IPv4, and the architectural and functional advancements introduced in IPv6. Furthermore, it compares IPv4 and IPv6 across various parameters, including address notation, configuration methods, header formats, and protocol efficiency. The review highlights the challenges in transitioning from IPv4 to IPv6 and underscores the need for gradual global adoption to support the future scalability, security, and performance of internet communications.**

***Keywords*—**Internet Protocol, IPv4, IPv6, Network Address Translation (NAT), Address Exhaustion, Protocol Comparison.

I. INTRODUCTION

The use of apps on the Internet has been expanding at a fast pace recently. The internet is not only used for everyday living but also for academic study [1]. The expansion of the Internet has had a variety of effects on end users. These days, almost everyone seems to have access, whether it be via their laptop, computer, smart TV, or even their automobile. A distinct Internet Protocol address is required for devices to connect with one another over the Internet [2]. The gadget will encounter a significant issue with the exhaustion of Internet Protocol (IP) addresses as it grows. Nevertheless, although all of these solutions might lessen the issue of IP address scarcity, it also compromise security and resilience [3].

The Protocol for the Internet has been very important in the field of communications in the last several years [4]. The method may have been available for a while, but recent events and incentives have helped it gain popularity among users. One factor might be the evolution of web browsing, and another could be the accessibility of IP and related transport protocols, which make their implementation and use in the classroom a breeze. However, several issues arise with the installation of an IP-based network in a commercial environment [5]. The ongoing IP activity, which includes the creation of systems, applications, methodologies, and prototypes, is really astounding. It is challenging to stay on top of even the notions that are presented in a reasonably limited domain since this implies that the field is always changing. However, to follow any discussion occurring in different forums, one must be aware of the basic protocols, forms and processes [6].

The fundamental communication system that allows devices to connect and share information across the internet and other networks is called the IP. The foundation of internet communication since its conception, IPv4 uses a 32-bit addressing method to facilitate the rapid growth of the digital world [7]. The exponential growth of internet-connected devices has almost depleted IPv4 addresses, highlighting the need for an expandable alternative[8]. This limitation was overcome with the creation of IPv6. Its 128-bit address field provides a virtually infinite range of unique IP addresses. IPv6 provides several improvements beyond address expansion, such as native security capabilities via IPsec, enhanced support for QoS, simpler header formats, and increased routing efficiency [9].

In response to this problem, the IETF created a new IP with the goal of increasing the number of IP addresses and therefore resolving the IP shortage [10]. "Internet Protocol next generation" (IPv6) is another name for this updated version. Expanded address space, enhanced security, robust routing, multicasting, and automatic network setup are some of the new and improved capabilities offered by IPv6. Over time, ISPs are aiming to switch from IPv4 to IPv6 for their physical networks [11]. There are a lot of reasons why the transition from IPv4 to IPv6 can't be done quickly, such as the high cost, the lack of technical assistance, the incompatibility of the two protocols, and the limited availability of online content via IPv6 [12].

A. Structure of the Paper

This paper is structured into six key sections. Section II provides an overview of Internet Protocols (IP), covering key concepts such as IP addressing, routing mechanisms, and the evolution from IPv4 to IPv6. Section III presents a detailed comparison between IPv4 and IPv6, focusing on their differences in header structures, performance, and scalability. Section IV outlines the current challenges and limitations of IP technologies, particularly in scalability, security, and mobile integration. Section V explores the future directions and emerging trends in IP technologies. Section VI provides a brief overview of the paper's findings and their implications for further study and advancement.

II. OVERVIEW OF INTERNET PROTOCOLS (IP)

Among the many protocols that make up the Internet, the most basic and essential is the IP. Its primary function is to transport data packets across network interfaces by addressing, routing, and delivering them [13]. Data packets may be addressed and routed across networks according to a set of rules

called the IP. Data packets are the building blocks of information sent via the Internet [14]. The IP address is a unique identification that routers use to send data packets to their specific locations. Every entity or device that connects to the Internet is assigned an IP address. Data packets are sent to their respective destinations based on their given IP addresses. IP enables all devices on a network to receive messages by assigning them a unique identification called an IP address [15].

A. IP Addressing and Internet Protocol Structures

The explanations of IP addressing concepts (IPv4, IPv6, private/public addressing), network devices like routers, and core data units like packets [16], as well as the accompanying diagrams that illustrate these networking fundamentals.

1) IP Address:

An IP address is a special number that is given to each node in a network that uses the Internet Protocol to send data. Identification, location addressing, and host or network interface are its two main applications [17].

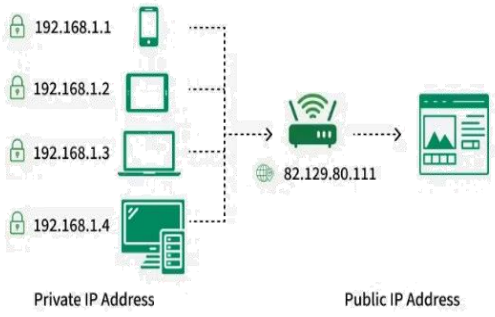

Fig. 1. Private and Public IP Address Mapping via a Router

Figure 1, demonstrates how multiple devices within a local network use private IP addresses to communicate internally. These devices including computers, laptops, and smartphones, connect to a router, which assigns them private Ips [18]. The router uses Network Address Translation (NAT) to translate these private IP addresses into a single public IP address when the user connects to the internet. In addition to enabling effective IP address management, this configuration increases security by concealing internal network information from the public.

2) Packet

Data sent from one location to another via the Internet or another network that uses packet switching is called a packet [19]. A payload and header are the primary components of this part.

3) Router

A router is a piece of network hardware that acts as a go-between for data packets travelling across different networks. Routers are responsible for directing traffic across the Internet [20].

4) IPv4

Virtually all modern Internet connections use the Internet technology version 4 (IPv4), which is a technology that facilitates communication between desktop computers connected to the web [21].

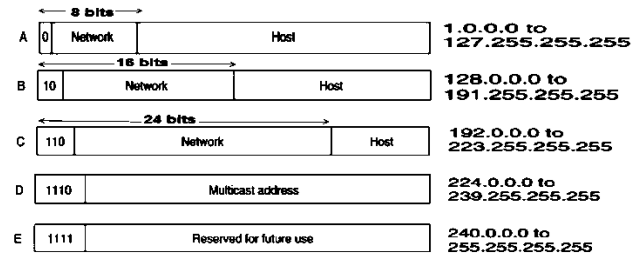

Fig. 2. Classification of IPv4 Address Classes (Class A to E)

Figure 2 presents the five IP address classes in IPv4, showing their structure, bit patterns, and address ranges:

- **Class A:** Begins with 0, uses 8 bits for the network and supports 1.0.0.0 to 127.255.255.255, ideal for large networks.
- **Class B:** Begins with 10, uses 16 bits for the network and covers 128.0.0.0 to 191.255.255.255, suitable for medium networks.
- **Class C:** Begins with 110, uses 24 bits for the network and spans 192.0.0.0 to 223.255.255.255, designed for small networks.
- **Class D:** Begins with 1110, reserved for multicast addresses from 224.0.0.0 to 239.255.255.255.
- **Class E:** Begins with 1111, reserved for experimental use with addresses from 240.0.0.0 to 255.255.255.255.

5) IPv6

The sixth version of the Internet Protocol, known as IPv6, is the last in a line of updates to the protocol that have been implemented for the purpose of identifying, finding, and routing computers so that data exchanged over the Internet may be done correctly [22][23].

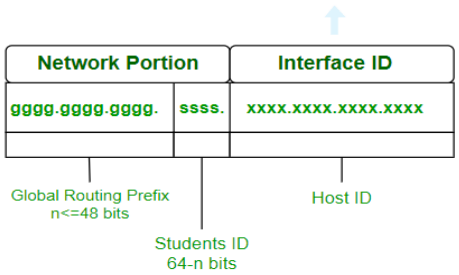

Fig. 3. IPv6 Address Structure with Network and Interface ID Segmentation

There are two primary components to an IPv6 address, as shown in Figure 3, the Network Portion and the Interface ID. Included in the Network Portion are the Subnet ID (student ID, 64-n bits) and the Global Routing Prefix (up to 48 bits). In order to distinguish one host from another on the network, the 64-bit Interface ID is used [24]. This hierarchical structure enables scalable routing and supports subnetting in IPv6 networks.

B. The Evolution and Core Components of the Internet Protocol (IP)

The IP has played a fundamental role in the development of modern networking, acting as the backbone of communication between devices across diverse and interconnected networks. The evolution of IP and its core components reflect how the protocol has grown to accommodate the expanding demands of the internet and ensure seamless data exchange across a vast array of networks [25]. This section delves into the origins, the primary functions, and the ecosystem of protocols that make up the Internet Protocol Suite, which together enable the effective and resilient operation of the modern Internet.

1) Genesis of Connectivity (The Birth of IP)

The need to link disparate systems emerged in the early days of computer networking, which is where IP got its start. The origins of IP may be found in the early phases of computer networking, when the need to link dissimilar systems led to the development of protocols that might make data transmission easier [26]. A standardised protocol was necessary to guarantee smooth communication across diverse settings when networks grew beyond localised domains [27].

2) Foundations of IP

It is part of the IP Suite, which is an all-inclusive framework that includes several protocols that allow for flexible and powerful network communication [28]. IP's principal role is to guarantee the efficient and dependable transmission of information across networks by handling tasks such as data packet addressing, routing, and fragmentation [29].

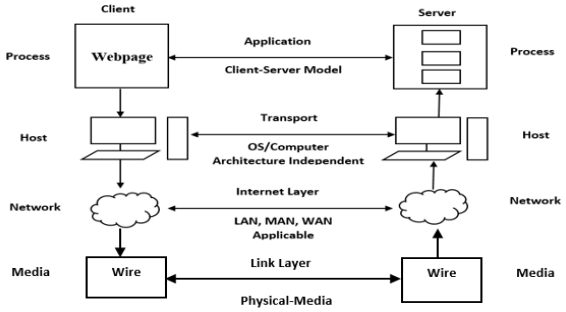

Fig. 4. Client-Server Model and the TCP/IP Protocol Suite

A communication flow is depicted through the different layers of the TCP/IP model displayed in Figure 4:

- **Application Layer:** This is where the client and server applications directly interact, using protocols specific to the application (HTTP for web pages). The diagram explicitly labels this interaction as following the "Client-Server Model".
- **Transport Layer:** This layer ensures reliable or unreliable data transfer between the client and server processes. The diagram notes that this layer is "OS/Computer Architecture Independent," highlighting its role in abstracting away the underlying system differences.
- **Internet Layer:** Appointed to handle the addressing and routing of packets across many networks. The diagram indicates that this layer is applicable across various network types: "LAN, MAN, WAN Applicable."
- **Link Layer:** Handles the physical transmission of data over a specific medium. In this illustration, "Wire" is shown as the "Media," and the communication at this level is governed by the "Link Layer" protocols. The physical connection is labeled as "Physical-Media" [30].

3) Connectionless Paradigm

Packet switching enables this connectionless paradigm, which permits dynamic routing and effective use of network resources. Additionally, it gives IP an innate resilience that allows it to easily adjust to network disturbances and variations.

4) Addressing and Routing

Internet Protocol addresses, whether in IPv4 or IPv6, are like virtual coordinates that routers use to send data packets to their correct locations. An essential component in the development of the Internet, IPv4 is defined by its 32-bit addressing system [31].

5) Protocol Ecosystem

"An extensive network of protocols and services enhances the usefulness and dependability of IP. The Internet Protocol Suite is comprised of several protocols that have a significant impact on the development of digital communication. For example, ICMP allows for the reporting and diagnostics of errors, while TCP and UDP govern the transport layer" [32].

III. Comprehensive Comparison of IPv4 And IPv6: Technical Aspects, Header Structure, and Performance Analysis

This section presents a holistic evaluation of IPv4 and IPv6 by examining their key differences across three major dimensions: technical aspects, header structure, and performance [33]. It explores how each protocol handles addressing, configuration, routing, and security shown in table I. The comparison of header structures highlights the simplified and more efficient design of IPv6. Performance analysis focuses on latency, Round Trip Time (RTT), and payload overhead in TCP/UDP transmissions. Through detailed tables and figures, this section provides insights into the functional evolution from IPv4 to IPv6, emphasizing IPv6's advantages in scalability, efficiency, and security in modern networking environments [34].

TABLE I. KEY DIFFERENCES BETWEEN IPV4 AND IPV6 IN TERMS OF THEIR TECHNICAL ASPECTS, PERFORMANCE, AND FEATURES.

Aspect	IPv4	IPv6
Address Length	32-bit (4.3 billion addresses)	128-bit (340 undecillion addresses)
Address Notation	Dotted decimal (e.g., 192.168.1.1)	Hexadecimal with colons (e.g., 2001:0db8::1)
Header Complexity	Complex header (12 fields)	Simplified header (8 fields)
Address Configuration	Manual or via DHCP	Auto configuration via Stateless Address Autoconfiguration (SLAAC)
NAT (Network Address Translation)	Required for address conservation	No NAT required due to larger address space
Security	Optional (IPsec support)	Mandatory (IPsec support for encryption and authentication)
Routing	More complex, can lead to routing table bloat	Simplified routing with hierarchical addressing
Broadcasting	Supports broadcasting	Does not support broadcasting, uses multicast
Packet Size	20-60 bytes	Minimum size 40 bytes, but more efficient in handling large packets

Fragmentation	Performed by both sender and router	Performed only by sender (routers don't fragment packets)
Address Availability	Limited (Exhaustion of IPv4 addresses)	Vastly more available (virtually unlimited)
Performance (Latency/Throughput)	May be slower due to NAT and routing complexities	Generally faster, especially with reduced NAT and streamlined routing
Transition Mechanisms	Dual stack, NAT64, tunneling (e.g., 6to4)	Dual stack, tunneling, IPv4/IPv6 intercommunication
Header Fields	12 fields (Source IP, Destination IP, TTL, etc.)	8 fields (Source IP, Destination IP, Hop Limit, etc.)
Security Features	Optional IPsec	Mandatory IPsec for end-to-end encryption
QoS (Quality of Service)	Supported via Type of Service (ToS)[35]	Supported via Traffic Class field
Compatibility	Backward compatible with older technologies	Not directly compatible with IPv4 (requires transition mechanisms)[36]
Ease of Deployment	Easier to implement and widespread	Requires upgrades to infrastructure and software
Number of Routers Supported	Limited by IPv4 address space	Can handle far more routers due to the larger address space

A. Comparison Transition of IPv4 Header vs IPv6 Header

The two primary header formats used by IPv6 are the Main IPv6 Header and the more recent IPv6 Extension Headers [37]. The primary IPv6 header is functionally identical to its IPv4 counterpart, with the exception of a few fields that have been optimised for IPv6. Both headings are compared in Figure 5 [38].

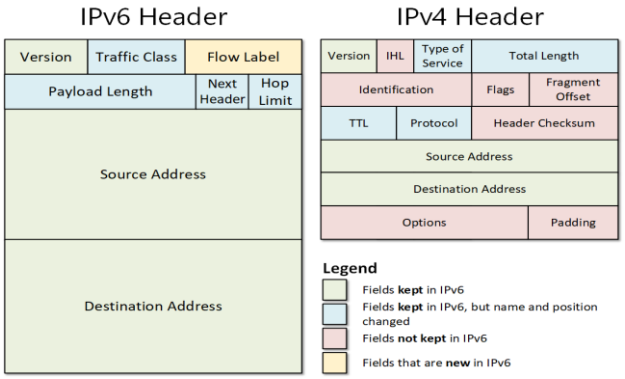

Fig. 5. Comparison of IPv6 and IPv4 Header Formats

The header formats of IPv6 and IPv4, highlighting the evolutionary changes in the Internet Protocol. The IPv6 header, designed for greater efficiency and scalability, streamlines the structure by including fields like Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, and the significantly larger 128-bit Source and Destination Addresses. In contrast, the IPv4 header contains fields such as Version, IHL, Type of Service, Total Length, Identification, Flags, Fragment Offset, Time to Live (TTL), Protocol, Header Checksum, 1 32-bit Source and Destination Addresses, Options, and Padding [39]. The color-coded legend further clarifies which fields are retained (green), renamed/repositioned (light blue), removed (pink), or newly introduced (yellow) in the transition from IPv4 to IPv6.

B. Comparative Performance Analysis of IPv4 and IPv6

This section analyzes the performance differences between IPv4 and IPv6 using Round Trip Time (RTT) under varying latency conditions and examines the payload overhead associated with TCP and UDP transmissions between the two protocols.

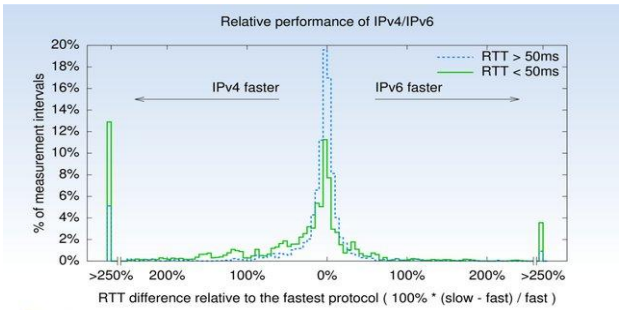

Fig. 6. IPv4 vs. IPv6 Performance Analysis by Latency

Figure 6, compares IPv4 and IPv6 performance (based on RTT difference) for high-latency (>50ms, dotted blue) and low-latency (<50ms, solid green) connections [40]. The x-axis shows the percentage difference relative to the faster protocol, with negative values favouring IPv6 and positive favouring IPv4. The y-axis indicates the percentage of measurements within each difference range. The analysis reveals how latency influences the relative speeds of the two protocols [41].

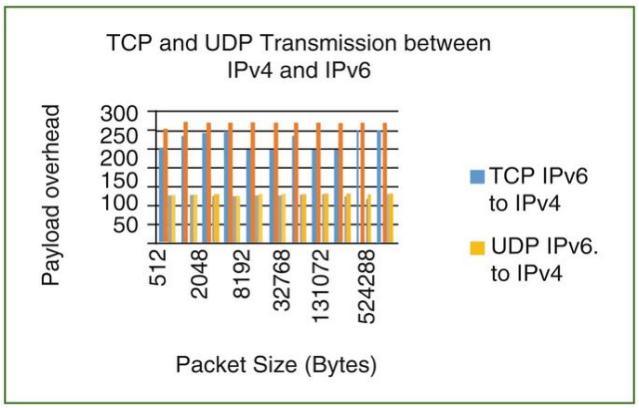

Fig. 7. TCP and UDP Transmission Overhead between IPv6 and IPv4 Networks

Figure 7, shows the consistent payload overhead for TCP (around 280 bytes) and UDP (around 140 bytes) when transmitting from IPv6 to IPv4 across various packet sizes. TCP's connection-oriented nature and IPv6-to-IPv4 translation contribute to its higher overhead compared to UDP's connectionless approach, with the overhead remaining fixed regardless of packet size.

IV. Transitioning From IPv4 To IPv6: Challenges And Best Practices

An important step in the growth of the Internet is the move from IPv4 to IPv6. Although IPv6 improves upon IPv4 in many ways, including scalability, security, and performance, there are still obstacles to its widespread adoption [42]. This section outlines the major technical, organizational, and security barriers encountered during the transition and presents proven strategies and best practices to overcome them [43].

A. Technical and Infrastructure Challenges

One of the most significant hurdles is the technical complexity of migrating global internet infrastructure to IPv6. Some key challenges include:

- **Dual Stack Implementation:** Operating IPv4 and IPv6 simultaneously requires additional configuration and maintenance. Managing two stacks increases the network's complexity and operational cost.
- **Backward Compatibility Issues:** IPv6 is not inherently backward compatible with IPv4. This necessitates the use of transitional technologies, such as tunnelling or protocol translation, to ensure interoperability [44].
- **Hardware and Software Readiness:** Many legacy network devices and systems may not support IPv6, requiring costly upgrades or replacements to enable IPv6 functionality [45].

B. Organizational and Policy Barriers

Transitioning to IPv6 involves more than just technical changes it also requires organizational alignment and policy-level support:

- **Cost of Migration:** Upgrading infrastructure, training personnel, and testing interoperability all incur significant costs, particularly for large enterprises and developing countries [46].
- **Training and Awareness:** Many IT professionals are more familiar with IPv4. A lack of awareness or understanding of IPv6 often leads to resistance in adoption [47].
- **Compliance and Standardization:** Different regions and organizations may follow varying standards and compliance regulations, making global coordination difficult [48].

C. Security Concerns

Although IPv6 was designed with integrated security features, its deployment brings new challenges:

- **Differences in Security Handling:** IPv6 changes how some traditional security mechanisms (like NAT) are implemented, requiring updates to security policies and tools [49].
- **Misconfiguration and Transition Vulnerabilities:** Poor implementation of dual-stack environments or tunnelling mechanisms can introduce vulnerabilities, such as exposure to IPv6-based attacks while defences are still configured for IPv4 [50].

D. Solutions and Best Practices

Despite these challenges, numerous strategies and technologies have emerged to ease the transition process:

- **Dual Stack and Tunnelling Techniques:** Running both protocols concurrently (dual stack) allows gradual migration. Tunnelling mechanisms like 6to4, Teredo, and ISATAP encapsulate IPv6 packets within IPv4 to traverse legacy networks.
- **Translation Mechanisms:** Tools such as NAT64 and DNS64 allow IPv6-only clients to communicate with IPv4 servers, acting as a bridge during the transition period.
- **Vendor and ISP Support Strategies:** Collaboration with hardware vendors and internet service providers is crucial for ensuring that IPv6-capable products and services are available and reliable [51].
- **Government and Institutional Role:** National governments and regulatory bodies play a pivotal role by mandating or incentivizing IPv6 adoption through policies, public-sector leadership, and funding support [52].
- **Roadmaps and Implementation Guidelines:** Structured transition plans and adherence to international best practices help ensure smooth migration with minimal service disruption [53].

V. Literature of Review

In this section, provides the previous research on Internet Protocol an In-depth Review of IPv4 and IPv6 and their Comparative analysis shown in Table II.

Pongrac and Kasunic (2022) comparing will help us understand how IPv6 works in a real-world setting with actual users. They tested 3,000 of the most popular IPv4 and IPv6 enabled (dual stack) domains in a real-world end-user setting in Croatia. Results showed that IPv4 and IPv6 traffic were comparable in terms of reachability, packet loss, RTT-based latency, hop counts, and throughput. The global adoption rate is currently over 36%, up from around 20% five years ago. There has to be testing and analysis of end-user IPv6 performance compared to IPv4 performance since the number of devices that can utilise IPv6 is growing [54].

Fahmi et al. (2021) compares and contrasts two protocols, IPv6 and IPv4, based on their respective features, services, and performance. These days, ISPs are busy planning for IPv6 migrations as IPv4 reaches its limits. There are more IP addresses in IPv6 than in IPv4. Different from IPv4, which utilises 32 bits, IPv6 uses 128 bits. Compared to IPv6, IPv4 is not inherently safer. The effectiveness of IPv6 and IPv4 is tested by simulating a communication network, checking the response time of the target server and clients, and analysing the routing protocol and packet size intervals. The performance of both IPv4 and IPv6 is evaluated at the same time using all of these factors [55].

Bala and Bansal (2022) evaluate IPv6 and IPv4 capabilities in the context of VANET routing. In this case, it uses two routing protocols, AODV and GPSR, to examine performance under various conditions. Two metrics are taken into account to evaluate and contrast IPv6 and IPv4 performance. Known as Internet Protocol Version 6, or IPv6, is the most recent update to the original protocol. This protocol will eventually supersede IPv4. Not only does it meet the growing need for IP addresses, but it also has other characteristics that contribute to the overall health of the Internet. Improvements in throughput and reliability should be seen with IPv6 [56].

Meijers (2023) presents the findings of an evaluation of IPv4 and IPv6 forwarding performance, including metrics like packet loss rate, delay, and throughput. Assessing IPv6 readiness requires measuring IPv6 performance in both physical and virtual routers. Since IPv4 is well-established in both physical and virtual environments, it provides a solid foundation for

future comparisons. There is a critical shortage of IPv4 addresses, making the transition to IPv6 an urgent matter of discussion and investigation [57].

Bhuiyan et al. (2023) delves into the evolution of IPv4 and IPv6 addresses, exploring the popular transition methods and assessing the current state of IPv6 implementation globally and in the context of Bangladesh. The comparative analysis of recent data, they have identified challenges and offered possible solutions for a seamless transition toward IPv6. As the demand for IP addresses surges and the exhaustion of IPv4 resources becomes imminent, embracing the potential of IPv6 holds the key to sustaining a connected and innovative digital world. The insights gleaned from this research may guide businesses and stakeholders in navigating the path to IPv6 integration [58].

Davies and Pagani (2022) compare and contrast IPv4 and IPv6 in detail, looking at how each protocol meets the needs and has the characteristics of high-performance blockchains. In terms of scalability, privacy, and security, IPv6 is better suited to these types of networks. Networks that use blockchain technology often use the IPv4 and IPv6 protocols, since they are built on top of the TCP/IP stack. They conclude that IPv6 offers better privacy, security, and scalability for these types of networks. Additionally, they detail how IPv6 provides enhanced functionality compared to IPv4 via the use of various P2P payment methods and enhanced identity management through the use of cryptographically generated addresses [59].

TABLE II. RESEARCH ON ANALYSIS OF IPV4 AND IPV6: PERFORMANCE METRICS, TRANSITION CHALLENGES, AND APPLICATION INSIGHTS

Author(s)	Year	Focus Area	Comparison Criteria	Key Findings
Kasunić and Pongrac	2022	IPv4 vs IPv6 behavior in end-user environment (Croatia)	Reachability, Packet Loss, RTT Delay, Hop Counts, Throughput	IPv6 adoption rising (~36%); tests show performance metrics for IPv6 vs IPv4 in dual stack; emphasizes importance of measuring IPv6 performance in real-world conditions.
Fahmi et al.	2021	IPv4 vs IPv6 technical comparison and network simulation	Response time, Routing Protocols, Packet Size, Communication Delay	IPv6 uses 128-bit addressing vs 32-bit in IPv4; IPv6 provides more efficient and secure communication; comparative simulation shows protocol behavior under load.
Bala and Bansal	2022	IPv4 and IPv6 performance in VANET (Vehicular Ad Hoc Networks) using AODV and GPSR	Routing Performance, Speed, QoS	IPv6 expected to enhance speed and service quality; essential for IP address demand in VANETs; tested using routing protocols under different scenarios.
Meijers	2023	Performance analysis of IPv4 and IPv6 forwarding in hardware and virtual routers	Throughput, Latency, Packet Loss	IPv6 readiness assessed through hardware and virtualized tests; IPv4 serves as baseline; key insight into IPv6 performance on modern networking devices.
Bhuiyan et al.	2023	Global and regional (Bangladesh) IPv6 transition methods and implementation challenges	Transition Methods, Challenges, Readiness	Presents a transition roadmap; IPv6 necessary to overcome IPv4 exhaustion; offers solutions to mitigate transition barriers and help businesses integrate IPv6.
Davies and Pagani	2022	IPv4 vs IPv6 in blockchain networks	Privacy, Security, Scalability	IPv6 is more favorable for blockchain due to features like cryptographically generated addresses and scalability; better suited for P2P networks and future blockchain use.

VI. CONCLUSION AND FUTURE SCOPE

An important step in the evolution of internet communication protocols is the move from IPv4 to IPv6. IPv4's limitations, most notably the exhaustion of address space, are making it more unsustainable, despite its long history as the Internet's backbone. IPv6 provides a solid answer to the problems of network scalability and connection in the future due to its enhanced efficiency, built-in security measures, and significantly increased address capacity. IPv6 addresses the major limitations of IPv4 and provides a limitless supply of addresses as well as a more secure process for future growth on the internet. While there are clear benefits for implementing IPv6, there are also considerable obstacles such as large implementation costs, no backward compatibility, and a lack of awareness from service providers. However, as it continues to develop new applications and devices that need a unique IP address, the migration to IPv6 is not optional. Organizations must also understand both protocols well enough to make a knowledgeable IP decision while also keeping their networks efficient, resilient, and secure.

The future of IP networking will depend on broad adoption of IPv6-driven momentum further facilitated by worldwide policy and readiness of the infrastructure. With the continued advancements of IoT, cloud computing, and 5G, this will only require more IPv6 support for device overload. Its expansive address space and enhanced features make it ideal for supporting the growth of the IoT, 5G networks, and cloud-native infrastructures. IPv6 enables seamless connectivity, better scalability, and improved security, which are critical for advanced systems like edge and fog computing. It also supports AI/ML applications for intelligent network management and

cybersecurity, and facilitates secure peer-to-peer communication in blockchain and decentralized networks. Overall, IPv6 will be a foundational enabler for next-generation digital transformation.

REFERENCES

[1] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum Internet protocol stack: A comprehensive survey," Comput. Networks, vol. 213, p. 109092, Aug. 2022, doi: 10.1016/j.comnet.2022.109092.

[2] S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems," Int. J. Innov. Res. Creat. Technol., vol. 8, no. 2, pp. 1–8, 2022.

[3] L. Kamiński, M. Kozłowski, D. Sporysz, K. Wolska, P. Zaniewski, and R. Roszczyk, "Comparative Review of Selected Internet Communication Protocols," Found. Comput. Decis. Sci., vol. 48, no. 1, pp. 39–56, Mar. 2023, doi: 10.2478/fcds-2023-0003.

[4] V. Pillai, "System And Method For Intelligent Detection And Notification Of Anomalies In Financial And Insurance Data Using Machine Learning," Pat. Off. J., 2025.

[5] V. Prajapati, "Exploring the Role of Digital Twin Technologies in Transforming Modern Supply Chain Management," Int. J. Sci. Res. Arch., vol. 14, no. 03, pp. 1387–1395, 2025.

[6] Y. Wang, P. Chang, H. Wang, Y. Ding, and R. Sun, "MAE-CAD: An IP-Based Core Network Asset Discovery Technology Based on Multiple Autoencoders," Secur. Commun. Networks, 2022, doi: 10.1155/2022/6854344.

[7] S. Thombre, R. Ul Islam, K. Andersson, and M. S. Hossain, "Performance analysis of an IP based protocol stack for WSNs," in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, Apr. 2016, pp. 360–365. doi: 10.1109/INFCOMW.2016.7562102.

[8] A. Gogineni, "Observability Driven Incident Management for Cloud-native Application Reliability," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 9, no. 2, pp. 1–10, 2021.

[9] V. Prajapati, "Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 3, pp. 1011–1020, Mar. 2025, doi: 10.38124/ijisrt/25mar1062.

[10] A. Gogineni, "Multi-Cloud Deployment with Kubernetes: Challenges, Strategies, and Performance Optimization," Int. Sci. J. Eng. Manag., vol. 04, no. 01, pp. 1–6, Jan. 2025, doi: 10.55041/ISJEM00036.

[11] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection for Secure Edge-Based Iot," J. Crit. Rev., vol. 6, no. 7, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[12] D. G. Chandra, M. Kathing, and D. P. Kumar, "A Comparative Study between IPv4 and IPv6," ANP J. Soc. Sci. Humanit., vol. 2, no. 1, pp. 68–72, Feb. 2021, doi: 10.53797/anpjssh.v2i1.9.2021.

[13] N. Malali, "The Impact of Digital Transformation on Annuities: Personalization, Investment Strategies, and Regulatory Challenges," J. Glob. Res. Math. Arch., vol. 11, no. 12, pp. 01–07, 2024, doi: 10.5281/zenodo.15279540.

[14] W. Buchanan, "Transmission Control Protocol (TCP) and Internet Protocol (IP)," in Advanced Data Communications and Networks, London: CRC Press, 2023, pp. 231–248. doi: 10.1201/9781003420415-16.

[15] P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," J. Intell. Syst. Internet Things, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[16] N. Malali, "Predictive AI for Identifying Lapse Risk in Life Insurance Policies: Using Machine Learning to Foresee and Mitigate Policyholder Attrition," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 5, pp. 1–11, 2025.

[17] P. Sokol, L. Rózenfeldová, K. Lučivjanská, and J. Harašta, "IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic," Forensic Sci. Int. Digit. Investig., vol. 32, Apr. 2020, doi: 10.1016/j.fsidi.2020.300918.

[18] M. Menghnani, "Advancing PWA Accessibility : The Impact of Modern Frameworks and Development Tools," TIJER – Int. Res. J., vol. 12, no. 3, pp. 465–471, 2025.

[19] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," ESP J. Eng. Technol. Adv., vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

[20] V. Gadelha, A. Sumper, E. Bullich-Massague, and M. Aragues-Penalba, "Electrical Grids Based on Power Routers: Definition, Architecture and Modeling," IEEE Access, vol. 11, pp. 10004–10017, 2023, doi: 10.1109/ACCESS.2023.3240243.

[21] A. K. Babar, Z. Ali, N. Nawaz, S. Qureshi, and S. Han, "Assessment of IPv4 and IPv6 Networks with Different Modified Tunneling Techniques using OPNET," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 9, 2019, doi: 10.14569/IJACSA.2019.0100963.

[22] P. Chatterjee, "Smart Contracts and Machine Learning: Exploring Blockchain and AI in Fintech," Indian J. Sci. Technol., vol. 18, no. 2, pp. 113–124, Jan. 2025, doi: 10.17485/IJST/v18i2.3838.

[23] P. Venkata, P. Reddy, K. Mohammed, I. Ali, B. Sandeep, and T. Ravi, "Importance and Benefits of IPV6 over IPV4: A Study," Int. J. Sci. Res. Publ., 2012.

[24] V. Rajavel, "Optimizing Semiconductor Testing: Leveraging Stuck-At Fault Models for Efficient Fault Coverage," Int. J. Latest Eng. Manag. Res., vol. 10, no. 2, pp. 69–76, Mar. 2025, doi: 10.56581/IJLEMR.10.02.69-76.

[25] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[26] M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.

[27] D. Syamsuar, P. Dell, D. Witarsyah, and A. Luthfi, "Organizational Resistance to Technology Diffusion: The

Case of IPv6," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 12, no. 6, pp. 2462–2468, Nov. 2022, doi: 10.18517/ijaseit.12.6.16073.

[28] B. Chaudhari and S. C. G. Verma, "Synergizing Generative AI and Machine Learning for Financial Credit Risk Forecasting and Code Auditing," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 11, no. 2, pp. 2882–2893, Apr. 2025, doi: 10.32628/CSEIT25112761.

[29] A. Annu and A. Dudy, "Review of the OSI Model and TCP/IP Protocol Suite on Modern Network Communication," Int. J. Curr. Sci. Res. Rev., vol. 07, no. 02, pp. 1230–1239, Feb. 2024, doi: 10.47191/ijcsrr/V7-i2-41.

[30] B. Ramanujam, "A review on collateral management and Risk-Weighted Assets (RWA) strategies : Challenges and solutions for financial institutions," vol. 14, no. 03, pp. 1750–1760, 2025.

[31] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," J. Adv. Dev. Res., vol. 11, no. 1, pp. 1–9, 2020.

[32] M. K. Tiwari et al., "The Comprehensive Review: Internet Protocol (IP) Address a Primer for Digital Connectivity," Asian J. Res. Comput. Sci., vol. 17, no. 8, pp. 34–45, Jul. 2024, doi: 10.9734/ajrcos/2024/v17i7488.

[33] M. Menghnani, "Modern Full Stack Development Practices for Scalable and Maintainable Cloud-Native Applications," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 2, pp. 1–11, 2025, doi: https://doi.org/10.5281/zenodo.14959407.

[34] S. R. Thota, S. Arora, and S. Gupta, "Hybrid Machine Learning Models for Predictive Maintenance in Cloud-Based Infrastructure for SaaS Applications," 2nd IEEE Int. Conf. Data Sci. Netw. Secur. ICDSNS 2024, no. July, pp. 1–6, 2024, doi: 10.1109/ICDSNS62112.2024.10691295.

[35] H. Mistry, K. Shukla, and N. Patel, "Securing The Cloud: Strategies and Innovations in Network Security for Modern Computing Environments," Int. Res. J. Eng. Technol., vol. 11, no. 04, pp. 1786–1796, 2024.

[36] V. Panchal, "Energy-Efficient Core Design for Mobile Processors : Balancing Power and Performance," Int. Res. J. Eng. Technol., vol. 11, no. 12, pp. 191–201, 2024.

[37] S. Murri, S. Chinta, S. Jain, and T. Adimulam, "Advancing Cloud Data Architectures: A Deep Dive into Scalability, Security, and Intelligent Data Management for Next-Generation Applications," Well Test. J., vol. 33, no. S2, pp. 619–644, 2024.

[38] A. Haggag, "Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet of Things Networks over IEEE 802.15.4," Wirel. Pers. Commun., vol. 130, no. 2, pp. 1449–1477, May 2023, doi: 10.1007/s11277-023-10340-4.

[39] S. Chatterjee, "Mitigating Supply Chain Malware Risks in Operational Technology : Challenges and Solutions for the Oil and Gas Industry," J. Adv. Dev. Res., vol. 12, no. 2, pp. 1–12, 2021.

[40] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[41] M. I. Haji, S. E. S. G. . Purwantoro, and S. P. Arifin, "Analysis Tunneling IPv4 and IPv6 on VoIP Network," Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control, pp. 337–344, Oct. 2018, doi: 10.22219/kinetik.v3i4.708.

[42] R. Tarafdar, "AI-Powered Cybersecurity Threat Detection in Cloud Environments," Int. J. Comput. Eng. Technol., vol. 16, no. 1, pp. 3858–3869, Feb. 2025, doi: 10.34218/IJCET_16_01_266.

[43] M. I. Khan, A. Arif, A. R. A. Khan, N. Anjum, and H. Arif, "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges," Int. J. Innov. Res. Comput. Sci. Technol., vol. 13, no. 1, pp. 62–67, Jan. 2025, doi: 10.55524/ijircst.2025.13.1.9.

[44] L. Lukman and W. A. Pratomo, "Implementasi Jaringan Ipv6 Pada Infrastruktur Jaringan Ipv4 Dengan Menggunakan Tunnel Broker," J. Teknol. Inf., vol. 15, no. 1, pp. 1–11, Mar. 2020, doi: 10.35842/jtir.v15i1.324.

[45] V. Kolluri, "Cybersecurity Challenges in Telehealth Services : Addressing the security vulnerabilities and solutions in the expanding field of telehealth," Int. J. Adv. Res. Interdiscip. Sci. Endeav., vol. 1, no. 1, pp. 23–33, 2024, doi: doi.org/10.61359/11.2206-2403.

[46] K. Rajchandar, M. Ramesh, A. Tyagi, S. Prabhu, D. S. Babu, and A. Roniboss, "Edge Computing in Network-based Systems: Enhancing Latency-Sensitive Applications," in 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, Sep. 2024, pp. 462–467. doi: 10.1109/IC3I61595.2024.10828607.

[47] A. S. González, A. E. Díaz, and H. V. González, "Technological transition from IPv4 to IPv6 at SNR," Ing. Solidar., vol. 17, no. 2, pp. 1–28, May 2021, doi: 10.16925/2357-6014.2021.02.12.

[48] T. K. Kota and S. Rongala, "Implementing AI-Driven Secure Cloud Data Pipelines in Azure with Databricks," Nanotechnol. Perceptions, vol. 20, no. 15, pp. 3063–3075, 2024, doi: https://doi.org/10.62441/nano-ntp.vi.4439.

[49] S. Pandya, "Integrating Smart IoT and AI-Enhanced Systems for Predictive Diagnostics Disease in Healthcare," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 10, no. 6, pp. 2093–2105, Dec. 2024, doi: 10.32628/CSEIT2410612406.

[50] D. G. Chandra, M. Kathing, and D. P. Kumar, "A Comparative Study on IPv4 and IPv6," in 2013 International Conference on Communication Systems and Network Technologies, IEEE, Apr. 2013, pp. 286–289. doi: 10.1109/CSNT.2013.67.

[51] N. Kodakandla, "IPv4 vs. IPv6 in cloud engineering: performance, security and cost analysis," Int. J. Sci. Res. Arch., vol. 8, no. 2, pp. 774–784, Apr. 2023, doi: 10.30574/ijsra.2023.8.2.0260.

[52] V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," Tech. Int. J. Eng. Res., vol. 11, no. 12, pp. 74–82, 2024.

[53] A. Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," Int. J. Res. Anal. Rev., vol. 8, no. 4, pp. 396–402, 2021.

[54] D. Pongrac and N. Kasunic, "Empirical analysis of IPv4 and IPv6 protocols in end user environment in Croatia," Polytech. Des., vol. 10, no. 2, pp. 147–152, 2022,

doi: 10.19279/TVZ.PD.2022-10-2-19.

[55] Fahmi, Muladi, M. Ashar, A. P. Wibawa, and Purnawansyah, "IPv6 vs IPv4 Performance Simulation and Analysis using Dynamic Routing OSPF," in 2021 4th International Conference of Computer and Informatics Engineering (IC2IE), IEEE, Sep. 2021, pp. 452–456. doi: 10.1109/IC2IE53219.2021.9649228.

[56] R. Bala and M. Bansal, "Performance Analysis of IPv4 and IPv6 in VANET Routing," in 2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE, Nov. 2022, pp. 1–5. doi: 10.1109/ICICT55121.2022.10064554.

[57] I. Meijers, "Comparison of IPv4 and IPv6 Forwarding Performance in Virtual and Hardware Routers," in 2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), IEEE, Oct. 2023, pp. 1–4. doi: 10.1109/ITMS59786.2023.10317747.

[58] Z. A. Bhuiyan, A. B. M. A. Ullah, M. M. H. Khan, S. Morshed, and M. M. Islam, "An Empirical Research Towards the State of Transition from IPv4 to IPv6," in 2023 5th International Conference on Sustainable Technologies for Industry 5.0 (STI), IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/STI59863.2023.10464716.

[59] J. Davies and A. Pagani, "IPv4 and IPv6 for Blockchain Networks: a Comparative Analysis," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), IEEE, Nov. 2022, pp. 1–6. doi: 10.1109/iGETblockchain56591.2022.10087175.

