Classification of IPv6 Transition Mechanisms using Multiple-Criteria Decision-Making

Mouataz Hamdou
Research Laboratory of Informatics, Data Sciences and Artificial Intelligence, School of Information Sciences, Rabat, Morocco
mouataz.hamdou@esi.ac.ma (corresponding author)

M'barek El Haloui
Research Laboratory of Informatics, Data Sciences and Artificial Intelligence, School of Information Sciences, Rabat, Morocco
melhaloui@esi.ac.ma

Ali El Ksimi
Research Laboratory of Informatics, Data Sciences and Artificial Intelligence, School of Information Sciences, Rabat, Morocco
ael-ksimi@esi.ac.ma

Badia Ettaki
Research Laboratory of Informatics, Data Sciences and Artificial Intelligence, School of Information Sciences, Rabat, Morocco
bettaki@esi.ac.ma

Received: 13 January 2025 | Revised: 10 February 2025 | Accepted: 21 February 2025

 DOI: https://doi.org/10.48084/etasr.10222

ABSTRACT

IPv4-to-IPv6 transition is critical for dealing with the depletion of IPv4 addresses and ensuring the future scalability of the internet. This paper presents a systematic evaluation and ranking of 13 widely utilized IPv4-to-IPv6 transition mechanisms through a Multi-Criteria Decision-Making (MCDM) process. Initially, a methodology inspired from Bradford's Law was applied to prioritize mechanisms in terms of how frequently they appear in the literature. Then, using the Weighted Sum Model (WSM), the current work assessed each mechanism on the basis of four key criteria: Performance, security, deployment, and routing efficiency. Mechanisms, such as Dual-stack, MAP-T, and NAT64, emerged as the top performers, offering sustainable scalability, high security, and deployment ease. However, mechanisms, like Teredo and 6to4, ranked lower due to significant security vulnerabilities, limited scalability, and performance bottlenecks. The performed analysis underscores the importance of selecting transition mechanisms that balance performance and security, particularly in large-scale networks and mobile environments. Potential areas for improvement, especially in tunneling mechanisms, are also identified and future research directions are proposed, focusing on lightweight and hybrid solutions to optimize IPv6 transition strategies.

Keywords-network migration; IPv4; IPv6; dual-stack; tunneling; translation; weighted sum model

I. INTRODUCTION

The Internet Protocol (IP) is central to internet communication, facilitating data transfer across networks by assigning unique addresses, segmenting data into packets, and routing them to their destinations [1]. IPv4, introduced in 1981, uses 32-bit addressing, supporting approximately 4.3 billion unique addresses. However, rapid device proliferation and inefficient allocation practices led to address exhaustion by 2011, despite the implementation of temporary measures, like Network Address Translation (NAT), and advancements, like Classless Inter-Domain Routing (CIDR) [1-3]. These limitations prompted the development of IPv6 in 1998, which uses 128-bit addressing to vastly expand the address space. IPv6 introduces features, such as IPsec for security, Neighbor Discovery Protocol (NDP), Stateless Address Auto-Configuration (SLAAC) for simplified configuration, streamlined headers for routing efficiency, and advanced Quality of Service (QoS) support [1, 4-6]. Despite its advantages, IPv6 adoption has been gradual, with many networks employing dual-stack environments to maintain compatibility [7]. As the demand for scalable, secure, and

efficient networks grows, IPv6 is expected to become the dominant protocol, constituting the next generation of internet connectivity [8]. IPv4-to-IPv6 transition is complex due to their incompatibility, necessitating mechanisms, such as dual-stack approaches, tunneling, and translation, to facilitate coexistence and migration [9]. This study aims to classify IPv6 transition mechanisms using an MCDM approach, namely WSM. It evaluates mechanisms based on performance, security, routing efficiency, deployment ease, and alignment with industry recommendations.

II. BACKGROUND

Choosing the right IPv4-to-IPv6 transition mechanism involves evaluating the network environment, interoperability needs, application compatibility, security requirements, and overall transition strategy [10]. There has been considerable research on comparing and classifying IPv4-to-IPv6 transition mechanisms [7, 11-13]. These studies often evaluate the mechanisms based on performance, security, complexity, and suitability for different network environments. Thus, they provide valuable insights into the strengths and limitations of each method, helping stakeholders make informed decisions based on their network requirements and transition goals.

A. IPv4-to-IPv6 Transition Mechanism Overview

1) Dual-stack

Dual-stack is the most widely adopted IPv4-to-IPv6 transition mechanism, enabling devices and networks to operate both protocols simultaneously. It allows systems to communicate over IPv4 and IPv6 networks, ensuring interoperability during the transition phase. Devices and routers in a dual-stack environment manage traffic from both protocols based on network requirements and IPv6 availability. Despite its effectiveness, maintaining dual-stack networks is resource-intensive, requiring robust configurations for routing and security to support both protocols [14].

2) Tunneling

Tunneling facilitates communication between IPv4 and IPv6 by encapsulating one protocol within the other, addressing interoperability challenges. Mechanisms for IPv6-to-IPv4 include 6in4, which relies on manual configuration of tunnel endpoints, and 6to4, which automates tunneling using a special IPv6 prefix. However, the decline of public relays has reduced 6to4's utility. ISP-managed solutions, like 6rd, bypass public relays for improved reliability. Other mechanisms, such as Teredo and ISATAP, address specific challenges, like NAT traversal and IPv6 deployment, within IPv4 networks [1, 7, 9, 10]. IPv4-to-IPv6 solutions enable IPv4 traffic to traverse IPv6 networks. 4in6 employs dynamic tunneling to reduce configuration complexity, while DS-Lite uses IPv6 infrastructure with Carrier-Grade NAT (CGN) for IPv4 address sharing. Advanced tunneling mechanisms, such as 6PE, 6VPE, and MAP-E, enhance capabilities by integrating MPLS backbones, secure VPN services, and stateless encapsulation for scalability. Additional protocols, like Tunnel Broker, GRE, and Softwire, address flexible encapsulation and dynamic tunnel configuration needs [7, 9-11]. Experimental mechanisms, including MPT, SA46T, and AYIYA, have explored redundancy, load balancing, and NAT traversal but are no longer actively developed [1, 7].

3) Translation

Translation mechanisms enable communication between IPv4-only and IPv6-only devices by converting packets between the two protocols. Widely utilized solutions include DNS64, which synthesizes IPv6 (AAAA) records from IPv4 (A) records, and NAT64, which performs bidirectional translation while managing session states to support multiple IPv6 clients sharing a single IPv4 address. Stateless translation approaches, such as SIIT and IVI, offer scalability for large networks. SIIT translates IP and ICMP packets without maintaining state, whereas IVI uses IPv4-embedded IPv6 addresses to ensure interoperability. SIIT-DC extends these capabilities for data center environments, facilitating traffic translation between IPv4 clients and IPv6-only services [7, 9, 15]. Experimental solutions, like SA46T-AT, address specific scenarios, such as data center scalability, but have limited adoption [7]. In large-scale and mobile network deployments, mechanisms, such as 464XLAT and MAP-T, are prominent. 464XLAT combines stateless (CLAT) and stateful (PLAT) translation to enable IPv4 application support in IPv6-only environments. MAP-T integrates address translation and port mapping to achieve scalability in extensive deployments. Host-based approaches, such as BIH, intercept DNS queries to facilitate IPv4 applications to interact with IPv6 servers on dual-stack hosts, superseding earlier methods, like BIS and BIA [7, 9, 12, 15, 16]. Experimental methods, including 4rd and dIVI, focus on preserving IPv4 services during IPv6 transitions. Additionally, 4rd supports public IPv4 address usage through layered translations, while dIVI emphasizes dual stateless translation, influencing mechanisms, like MAP-T [7].

B. Evaluating Criteria

IPv6 transition mechanisms require a multi-criteria evaluation to determine their suitability for various network environments. Key criteria include performance metrics, security considerations, and deployment measures, each contributing to the overall effectiveness and practicality of transition solutions.

1) Performance and Routing Metrics

Performance metrics are essential for assessing the efficiency and reliability of network systems. Throughput, RTT, and CPU utilization provide insights into data transfer rates, responsiveness, and resource demands [16-20]. Metrics, such as packet loss, latency, jitter, and delay are critical for real-time and time-sensitive applications, while network convergence ensures stability after topology changes [21-24]. Scalability and routing efficiency, including optimized discovery and node traversal, enhance the adaptability and responsiveness of transition mechanisms in dynamic and large-scale networks [10-11].

2) Security Considerations

Security is a crucial aspect of IPv4-to-IPv6 transition due to vulnerabilities introduced during their coexistence [25, 26]. Key risks include address spoofing, packet tampering, and DNS attacks, like hijacking and cache poisoning [27, 28].

Mitigation strategies involve encryption, robust DNS configurations, and the use of secure protocols, such as IPsec [11, 13]. Tunneling mechanisms face additional threats, including Denial-of-Service (DoS) attacks [27] and session-level vulnerabilities [29, 30], emphasizing the need for security-enhanced designs to safeguard transitional communications.

3) Deployment Measures

Successful deployment of transition mechanisms hinges on simplicity, compatibility, and flexibility. Simplicity reduces complexity and potential errors during configuration and management [10]. Compatibility ensures seamless integration with existing IPv4 infrastructure, preserving operational continuity and minimizing costs [31]. Flexibility enables adaptation to diverse network topologies and scalability demands, supporting the long-term adoption and sustainability of IPv6 [32].

C. Multiple-Criteria Decision-Making

MCDM provides a structured approach to decision-making, balancing multiple, often conflicting criteria, and is widely applied across various fields [33]. Key components of MCDM include alternatives (e.g., transition protocols, like 6to4, DS-Lite, NAT64) and criteria (e.g., performance, security). Two types of MCDM problems exist: Multiple-Attribute Decision-Making (MADM) and Multiple-Objective Decision-Making (MODM). MADM, which evaluates a finite set of alternatives against criteria, is the most suitable approach for this study. It deploys techniques, such as the Analytic Hierarchy Process (AHP) and WSM [34]. The present study employs MADM with WSM, an extensively utilized and straightforward technique. WSM assigns weights to criteria based on their importance, summing the weighted scores for each alternative to identify the optimal choice. This approach ensures a systematic and quantitative evaluation of IPv6 transition mechanisms.

III. COMPARATIVE STUDY

To provide a comprehensive understanding of IPv4-to-IPv6 transition strategies, this study conducted a comparative analysis of research articles published between 2011 and August 2024. The articles were selected based on stringent criteria, including a focus on evaluating multiple transition mechanisms and their performance, security, and routing efficiency. Although efforts were made to include all relevant literature, search engine limitations and access issues may have led to the omission of some contributions. Of the 37 studies reviewed, 28 focused on performance, 11 on security, and 6 on routing efficiency, reflecting the emphasis on network performance during the transition. The tunneling approach emerged as the most examined transition mechanism, featuring in 33 studies, while 12 papers discussed translation methods, and only 10 addressed dual-stack techniques. Table I summarizes key insights from the reviewed studies, shedding light on various aspects of these mechanisms. For example, the scalability and performance comparisons of 464XLAT and MAP-T in [17, 18] show MAP-T's superior scalability when managing CPU cores and concurrent user sessions. Studies, such as [16, 35], further highlight performance variations, identifying BIH's faster convergence and ISATAP's superior throughput and jitter performance, even though additional exploration of payload size impacts is proposed. Security vulnerabilities in IPv6 transition mechanisms were a recurring theme. Authors in [27, 36] identified risks, such as DNS hijacking and Man-in-the-Middle (MitM) attacks in ISATAP and Teredo, proposing discontinuation of legacy mechanisms and improved cryptographic routing authentication. Similarly, authors in [13, 29] highlighted vulnerabilities, like address spoofing and routing loops, emphasizing the importance of enhanced protocols, such as IPsec. Although security remains underexplored relative to performance, proposals for mitigation strategies, including IPsec adoption, underline its critical role despite the associated overhead. Deployment strategies have received limited focus. For instance, authors in [12] compared IPv4aaS mechanisms, noting the simplicity of 464XLAT deployment while favoring MAP-T and DS-Lite for scalability in large-scale environments. Similarly, authors in [21] advocated for dual-stack deployment in small networks and tunneling mechanisms for larger networks, aligning with performance considerations. Although the literature offers extensive performance analyses—focusing on metrics, like throughput, delay, and jitter—security and deployment aspects are comparatively underrepresented. For example, authors in [37, 38] highlighted performance variations under diverse conditions, but these studies lacked detailed security insights. Similarly, authors in [39, 40] analyzed performance metrics without addressing deployment concerns. In summary, while IPv6 transition mechanisms have been extensively evaluated regarding their performance, security, and deployment considerations remain secondary in most studies. Future research should adopt a more integrated approach, combining comprehensive performance evaluation with in-depth security and deployment analyses to guide the development of robust, scalable, and secure IPv6 transition strategies.

IV. METHODOLOGY

A. Mechanism Selection

Regarding IPv4-to-IPv6 transition mechanism selection, the current study aimed to balance recency and robustness while ensuring that the chosen mechanisms were representative of the broader research landscape. Bradford's Law [52], a bibliometric principle, guided the proposed methodology. The law describes the distribution of literature across core and peripheral sources, where a small number of sources contain the majority of information, and progressively larger source numbers contribute limited insights [53]. This principle was adapted to classify transition mechanisms based on their occurrence in the literature, which allowed identifying the most studied and relevant mechanisms for further analysis. This approach is particularly suitable for the present study as it provides a structured and unbiased method for selecting transition mechanisms. By leveraging Bradford's Law, it is certified that frequently analyzed mechanisms are prioritized while also considering emerging mechanisms that, though less studied, may offer valuable insights. This systematic selection process helps avoid arbitrary choices and enhances the transparency, reliability, and representativeness of this study's evaluation compared to selections based on individual

perspectives. Data on transition mechanisms were collected from research articles, and were organized according to their appearance frequency. Highly cited mechanisms, like 6to4 and ISATAP, appeared 26 and 17 times, respectively, stressing their prominence in the field. Table II details these occurrences, which helped identify the most frequently discussed mechanisms and prioritize them for analysis. To emphasize recent developments while maintaining historical context, a Research Interest Score (RIS) was calculated for each mechanism. This score integrated the recency of studies using:

$$RIS(Mechanism) = \sum_{t=1}^{3} O_t(Mechanism) \cdot W_t \quad (1)$$

where O_t represents occurrences within a given time period t, and W_t is the weight assigned to each period. Papers from 2020 onward received the highest weight ($W_1 = 3$), those from 2016–2019 a moderate weight ($W_2 = 2$), and older papers (< 2016) the lowest weight ($W_3 = 1$). For instance, the RIS for 6to4 was calculated as $(2 \times 3) + (12 \times 2) + (12 \times 1) = 42$. This method prioritized mechanisms with recent surges in research, such as NAT64 and 464XLAT, even if their overall frequency was lower.

TABLE I. SUMMARY OF IPV4-TO-IPV6 TRANSITION STUDIES

Mechanism family	Mechanisms evaluated	Performance	Routing efficiency	Security aspects	Deployment findings	References
Dual-Stack	Dual-Stack	High performance in most scenarios. Outperforms tunneling and translation for small-scale networks, but increased latency in some cases.	Efficient for gradual IPv6 adoption or for coexisting IPv4 and IPv6 traffic. Better for small networks.	Doubles the attack surface with vulnerabilities across both IPv4 and IPv6. Spoofing and security configuration challenges persist.	Ideal for networks in the initial stages of IPv6 adoption. Dual-stack is easy to deploy and maintain in small networks. Security requires enhanced IPv6 firewalling.	[19, 21, 30, 32, 36, 38, 41-44]
Tunneling	6to4, ISATAP, GRE, DS-Lite, 6in4, MAP-E, 6rd, Teredo, Tunnel-Broker	Performance varies across tunneling methods. ISATAP and GRE generally perform better for specific traffic profiles. Static tunneling (e.g., 6in4) excels in specific scenarios.	Routing efficiency depends on tunnel placement. ISATAP performs best in intranet settings, while GRE is optimal for inter-network traffic. RIPng and OSPFv3 are common protocols used for routing.	Tunneling mechanisms are prone to injection, spoofing, and DoS attacks. Security measures, like IPsec and ACLs, enhance protection but increase complexity and latency.	Tunnels are suitable for large distributed networks or where dual-stack deployment is infeasible. Mechanisms, like DS-Lite, provide interoperability. ISATAP is cost-effective and stable for internal traffic. Some methods (e.g., Teredo) introduce vulnerabilities when bypassing firewalls.	[7, 10-13, 19-24, 27, 29-32, 35-51]
Translation	464XLAT, MAP-T, NAT64, DNS64, BIH, BIS, BIA, SA46T	MAP-T and NAT64 offer better scalability. 464XLAT is efficient but less scalable. Stateless translations, like BIH, offer more reliability.	Translation mechanisms, like NAT64, provide routing simplification by translating IPv4 traffic to IPv6. DNS64 adds routing resolution but risks cache poisoning.	Stateless translations have smaller attack surfaces, but mechanisms, like DNS64, are vulnerable to poisoning, tampering, and DoS attacks. Stateful NAT64 can exhaust resource pools and increase session hijacking risks.	MAP-T and DNS64 are widely adopted due to their scalability. DNS64 requires regular updates to avoid vulnerabilities. Stateless options, like BIH, offer better performance in high-traffic scenarios. 464XLAT is efficient for dual-stack environments, but faces scalability challenges in large-scale deployments.	[7, 12, 16-19, 23, 28, 32, 36, 41, 48]

Following Bradford's Law, the mechanisms were categorized into three zones based on their cumulative occurrences. The total occurrences (T) of all mechanisms were divided equally among the zones, as represented in (2):

$$N_z = \frac{T}{3}, z \in \{1,2,3\} \quad (2)$$

where N_z is the target number of occurrences per zone.

For the proposed dataset of 169 occurrences, this resulted in approximately 56 occurrences per zone. Zone 1 (core) included mechanisms that accounted for the first 56 occurrences. Summing from the most frequent mechanisms, it was found that 6to4 (26 occurrences) and ISATAP (17 occurrences) alone contributed 43 occurrences. Including 6in4 (14 occurrences) brought the cumulative total to 57, slightly exceeding 56. Thus, Zone 1 consisted of these three mechanisms. Zone 2 was defined by the next 56 occurrences, extending to the 11th-ranked mechanism. Zone 3 contained the remaining mechanisms, which were less frequently mentioned. The geometric progression of mechanism representation is expressed as:

$$Zone\ 2\ size = r \cdot q_1, \ \ Zone\ 3\ size = r \cdot {q_2}^2 \quad (3)$$

where r is the core size and q_1 and q_2 are progression factors.

Calculating:

$$q_1 = \frac{mechanisms\ in\ Zone\ 2}{r} \ ; \quad q_2 = \sqrt{\frac{mechanisms\ in\ Zone\ 3}{r}}$$

an average progression factor q of approximately 4.1 was obtained. Using this, the zone sizes were recomputed as $r \cdot q \approx 8$ for Zone 2, and $r \cdot q^2 \approx 35$ for Zone 3.

The performed analysis focused on the mechanisms in Zones 1 and 2, representing the top 10 mechanisms. These included 6to4, ISATAP, Dual-stack, and 464XLAT, which

provided substantial research data for comparison. Additionally, emerging mechanisms, like NAT64, MAP-E, and Lw4o6, though outside the top 10, were included due to their increasing significance in recent studies. This systematic approach, inspired from Bradford's Law, ensured a balanced selection of transition mechanisms that prioritized relevance, research backing, and emerging trends. By combining historical significance with recent advancements, the specific mechanisms' selection provides a comprehensive foundation for analyzing IPv4-to-IPv6 transition strategies.

TABLE II. OCCURRENCES OF TRANSITION MECHANISMS IN THE STUDIED PAPERS

Mechanism	Occurrences	Accumulated occurrences	Research interest (score)
6to4	26	26	42
ISATAP	17	43	29
6in4	14	57	25
Dual-stack	10	67	18
Teredo	8	75	13
DS-Lite	7	82	12
6rd	7	89	10
464XLAT	6	95	14
MAP-T	6	101	14
GRE	6	107	11
NAT64	5	112	10
MAP-E	5	117	9
Lw4o6	4	121	8
6over4	4	125	7
4over6	4	129	6
BIS	2	131	5
BIA	2	133	5
BIH	2	135	5
DNS64	2	137	4
NAT-PT	2	139	4
SIIT-DC	2	141	4
IVI	2	143	4
dIVI	2	145	4
SA46T-AT	2	147	4
Softwire	2	149	4
4to6	2	151	3
Tunnel-Broker	2	153	3
6PE	2	155	3
4rd	2	157	3
6VPE	1	158	2
6to4-PMT	1	159	2
4in6	1	160	2
SA46T	1	161	2
TSP	1	162	2
AYIYA	1	163	2
MPT	1	164	2
NAT46	1	165	2
DNS46	1	166	2
NAPT-PT	1	167	2
SIIT	1	168	2
TRT	1	169	2

B. Mechanism Classification

To rank the 13 selected IPv4-to-IPv6 transition mechanisms, WSM, an MCDM technique, was deployed. This approach evaluates each mechanism based on predefined criteria and their corresponding weights, ensuring a systematic and transparent ranking process. The evaluation focused on four key criteria: performance, security, deployment, and routing efficiency.

Security was assigned the highest weight ($w_{Sec} = 0.5$) due to its critical role in mitigating risks, such as spoofing, packet tampering, and DoS attacks. During the IPv4-to-IPv6 transition, new mechanisms can introduce vulnerabilities that threaten network stability. As mentioned above, these risks can have serious implications, rendering security a decisive factor in network planning and implementation. A mechanism's ability to safeguard against such threats is crucial, and therefore, a higher weight is assigned to ensure that more secure mechanisms are prioritized.

Performance was assigned a weight of 0.3 ($w_P = 0.3$). This criterion assesses how well the mechanism handles network conditions, including throughput, latency, jitter, and scalability. While performance is essential for maintaining efficient network operations, it is secondary to security. Even the best-performing mechanism can be inadequate if it has significant security flaws. Thus, performance is weighted to reflect its importance in network quality and data transfer speeds, but it is considered less critical than security.

Deployment was given a lower weight ($w_D = 0.1$). This factor evaluates the ease of implementing a mechanism, including its configuration complexity, operational costs, and resource requirements. Although deployment considerations are important, they are typically a one-time concern compared to the ongoing issues of security and performance. With sufficient resources, most mechanisms can be deployed relatively easily. Therefore, deployment is given a lower weight as it does not affect daily network operations as significantly as security and performance.

Routing efficiency also received a weight of 0.1, as it pertains to convergence time and routing overhead. However, detailed studies on routing efficiency are less common, and its effects often overlap with performance metrics. Given its lower direct impact compared to security and performance, it was assigned the minimum weight.

The weight distribution satisfies the normalization condition as shown in:

$$\sum_{j=1}^{m} w_j = 1 \quad (4)$$

Each mechanism (A_i) was scored on a scale of 0 to 10 for each criterion (C_j), based on insights from the comparative study. These scores (s_{ij}) were used to compute the total weighted score (S_i) for each mechanism using:

$$S_i = \sum_{j=1}^{m} w_j \cdot s_{ij} \quad (5)$$

where m is the total number of criteria, w_j represents the weight for criterion C_j, and s_{ij} is the score of mechanism A_i for criterion C_j.

V. RESULTS

The evaluation ranks IPv4-to-IPv6 transition mechanisms based on performance, security, deployment, and routing efficiency. Dual-Stack emerged as the top mechanism, offering high performance (9/10) and ease of deployment (7/10), though

its dual-protocol nature increases the attack surface (security: 6/10), making it susceptible to spoofing, DoS attacks, and neighbor discovery replay attacks [32, 36]. MAP-T and NAT64 also performed well, scoring 8/10 in performance, demonstrating robust scalability and throughput. However, NAT64 remains vulnerable to DNS cache poisoning, session hijacking, and resource exhaustion [28]. Mechanisms, like MAP-E, DS-Lite, and 464XLAT, delivered balanced performance, excelling in mobile networks and large-scale transitions, but scored lower in security and routing efficiency (5–6/10). MAP-E and DS-Lite are prone to packet injection and DoS attacks, particularly when misconfigured [10]. 6in4 provided strong performance (8/10) but suffered from security vulnerabilities (4/10), including address spoofing and injection attacks, requiring manual security configurations to mitigate risks [29]. Lower-ranked mechanisms, including 6rd, 6to4, GRE, and Teredo, exhibited significant security and deployment limitations. 6to4 and Teredo, in particular, are highly vulnerable to spoofing, traffic manipulation, and relay abuse, making them less suitable for modern networks [13, 27]. GRE suffers from encapsulation bypass attacks, leading to potential DoS threats [36]. Additionally, automatic tunneling mechanisms, like ISATAP and 6to4, lack built-in security, making them prone to MitM and traffic injection attacks [13]. Overall, the present study underscores the suitability of mechanisms, like Dual-Stack, MAP-T, and NAT64, for robust and secure IPv4-to-IPv6 transitions, while highlighting the inefficiencies and security weaknesses of legacy tunneling solutions. The impact of security vulnerabilities on rankings demonstrates the importance of integrating native security features (e.g., IPsec, traffic filtering, and ingress/egress controls) to mitigate attacks and enhance transition reliability. The detailed scores for all mechanisms are provided in Table III. These scores are further visualized in Figure 1, where individual criteria are plotted as bar charts, and the weighted sum curve provides the aggregated ranking.

TABLE III. MCDM (WSM) DECISION MATRIX

Mech.	Performance (0.3)	Routing efficiency (0.1)	Security (0.5)	Deployment (0.1)	Overall score
Dual-stack	9	6	6	7	7
MAP-T	8	5	6	6	6.5
NAT64	8	6	5	6	6.1
MAP-E	7	5	5	6	5.7
DS-Lite	6	5	5	7	5.5
464XLAT	6	5	5	7	5.5
6in4	8	7	4	4	5.5
Lw4o6	7	5	4	5	5.1
ISATAP	7	6	4	4	5.1
6rd	6	5	4	4	4.7
6to4	6	5	3	4	4.2
GRE	5	4	3	3	3.7
Teredo	4	4	3	3	3.4

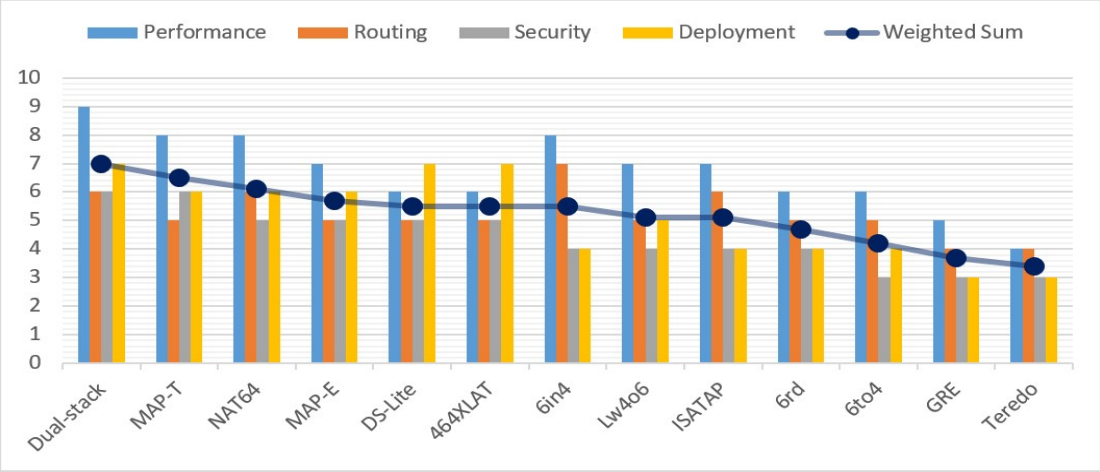

Fig. 1. Comparative analysis of IPv6 transition mechanisms based on performance, routing, security, and deployment criteria. The bar chart illustrates individual scores for each criterion, while the line with markers highlights the weighted sum (overall score) of the mechanisms.

VI. DISCUSSION

The evaluation of IPv6 transition mechanisms has traditionally lacked a structured selection and ranking methodology, often leading to comparison inconsistencies. The present study addresses these limitations by integrating Bradford's Law for systematic selection and WSM for structured multi-criteria ranking, ensuring a transparent, adaptable, and reproducible decision-making process. While many prior studies rely on experimental performance, security comparisons, or qualitative descriptions, the proposed method certifies a balanced evaluation across performance, security, deployment complexity, and routing efficiency. By applying Bradford's Law, bias toward either extensively studied legacy mechanisms or underexplored newer mechanisms are avoided, ensuring a representative selection that reflects the broader research landscape. Meanwhile, WSM allows for adaptable ranking based on network-specific requirements, bridging the gap between theoretical evaluation and real-world implementation. These advancements make IPv6 transition planning more systematic, reducing reliance on isolated experimental comparisons and enabling consistent and practical decision-making for network engineers and policymakers. Tunneling solutions, like Teredo, 6to4, and

GRE, rank lower due to security vulnerabilities, performance limitations, and dependency on relay infrastructure. Enhancing these mechanisms requires integrating stronger security features (e.g., IPsec, TLS) and optimizing encapsulation overhead to improve efficiency. Adaptive tunneling techniques could also optimize performance by dynamically adjusting to traffic and security demands. Stateless mechanisms, like MAP-T and NAT64, excel in scalability and security, particularly in large-scale transition environments, but they require further optimization for multi-tenant networks and high-concurrency scenarios. Hybrid solutions that combine stateless scalability with stateful security may offer balanced performance for complex networks. Lightweight mechanisms, such as Lw4o6 and MAP-E, are efficient and scalable, but they require enhanced security measures and adaptive routing to improve their usability in dynamic networking environments. Dual-Stack remains widely used due to its flexibility and high performance, but it presents resource and security challenges owing to its dual-protocol nature. Security frameworks and resource optimization techniques, such as virtualization and load balancing, are crucial to maintaining its viability. However, its reliance on IPv4 reinforces the urgency for full IPv6 adoption.

Security remains the most critical factor across all mechanisms, with tunneling solutions being particularly vulnerable. Future strategies should integrate native security features and automate configurations to reduce complexity and human error. AI-driven network management tools could further enhance traffic optimization and dynamic security adjustments, making transition mechanisms more efficient and resilient. Finally, the lack of standardized deployment practices remains a challenge. Establishing clear guidelines through organizations, like the IETF, would guarantee uniform benchmarks for performance, security, and scalability across different network environments. These advancements will be crucial in certifying a secure and efficient IPv6 transition tailored to modern network demands.

VII. CONCLUSIONS

The transition from IPv4-to-IPv6 requires a structured evaluation of existing transition mechanisms. This study integrates Bradford's Law to ensure a balanced selection of mechanisms, avoiding bias toward older, extensively studied technologies. Unlike prior studies that focus on descriptive analyses, Security assessments, or experimental performance comparisons, the proposed approach synthesizes multiple research insights using the Weighted Sum Model (WSM) for a structured, multi-criteria evaluation. The findings rank Dual-Stack, MAP-T, and NAT64 as the most effective mechanisms due to their superior performance, scalability, and security, while older mechanisms, like Teredo and 6to4, exhibit security vulnerabilities and performance limitations. Security emerged as the most critical factor, with stateless mechanisms outperforming others in large-scale deployments. Tunneling mechanisms, such as 6in4 and Lw4o6, remain relevant in controlled environments, but require improved security measures.

This study provides a structured, adaptable, and reproducible methodology for IPv6 transition, bridging the gap between theoretical evaluation and practical decision-making to assist network engineers in selecting the most suitable mechanism.

REFERENCES

[1] G. K. Ordabayeva, M. Othman, B. Kirgizbayeva, Z. D. Iztaev, and A. Bayegizova, "A systematic review of transition from IPV4 to IPV6," in *6th International Conference on Engineering and MIS*, Almaty, Kazakhstan, Sep. 2020, pp. 1–15, https://doi.org/10.1145/3410352.3410735.

[2] L. Prehn, F. Lichtblau, and A. Feldmann, "When wells run dry: the 2020 IPv4 address market," in *16th International Conference on emerging Networking EXperiments and Technologies*, Barcelona, Spain, Dec. 2020, pp. 46–54, https://doi.org/10.1145/3386367.3431301.

[3] J. Beeharry and B. Nowbutsing, "Forecasting IPv4 exhaustion and IPv6 migration," in *International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Balaclava, Mauritius, Aug. 2016, pp. 336–340, https://doi.org/10.1109/EmergiTech.2016.7737362.

[4] F. Abusafat, T. Pereira, and H. Santos, "Roadmap of Security threats between IPv4/IPv6," in *International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Toronto, ON, Canada, Apr. 2021, pp. 1–6, https://doi.org/10.1109/IEMTRONICS52119.2021.9422653.

[5] A. El Ksimi and C. Leghris, "Contribution to Optimization and Evaluation of IPv6 Signals Based Constrained Devices Networks," *Wireless Personal Communications*, vol. 117, no. 3, pp. 2311–2325, Apr. 2021, https://doi.org/10.1007/s11277-020-07974-z.

[6] M. Piraux *et al.*, "The multiple roles that IPv6 addresses can play in today's internet," *SIGCOMM Comput. Commun. Rev.*, vol. 52, no. 3, pp. 10–18, Jun. 2022, https://doi.org/10.1145/3561954.3561957.

[7] G. Lencse and Y. Kadobayashi, "Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis," *IEICE Transactions on Communications*, vol. E102-B, no. 10, pp. 2021–2035, Oct. 2019, https://doi.org/10.1587/transcom.2018EBR0002.

[8] K.-H. Li and K.-Y. Wong, "Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites," *Information*, vol. 12, no. 6, Jun. 2021, Art. no. 246, https://doi.org/10.3390/info12060246.

[9] A. T. H. Al-hamadani and G. Lencse, "A survey on the performance analysis of IPv6 transition technologies," *Acta Technica Jaurinensis*, vol. 14, no. 2, pp. 186–211, May 2021, https://doi.org/10.14513/actatechjaur.00577.

[10] W. Mi, "The Applicability and Security Analysis of IPv6 Tunnel Transition Mechanisms," in *International Conference on Algorithms and Architectures for Parallel Processing*, Dalian, China, Aug. 2014, pp. 560–570, https://doi.org/10.1007/978-3-319-11194-0_49.

[11] Z. Ashraf, A. Sohail, S. Latif, A. Hameed, and M. Yousaf, "Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network," *The International Arab Journal of Information Technology*, vol. 20, no. 1, pp. 78–91, 2023, https://doi.org/10.34028/iajit/20/1/9.

[12] O. D'Yab, "A Comprehensive Survey on the Most Important IPv4aaS IPv6 Transition Technologies, their Implementations and Performance Analysis," *Infocommunications Journal*, vol. XIV, no. 3, pp. 35–44, Nov. 2022, https://doi.org/10.36244/ICJ.2022.3.5.

[13] S. A. Abdulla, "Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms," *International Journal of Security and Networks*, vol. 12, no. 2, pp. 83–102, Jan. 2017, https://doi.org/10.1504/IJSN.2017.083830.

[14] Y. Zhang, Y. Fu, and Q. Wang, "IPv4 to IPv6 Transition Strategy Based on Dual Stack Protocol," in *Intelligent Computing Technology and Automation*, Amsterdam, Netherlands: IOS Press, 2024, pp. 428–435.

[15] S. Manimozhi and J. G. Jayanthi, "A Literature Survey on Transition Mechanisms in IPv4 and IPv6 Networks," in *4th International Conference on Intelligent Computing and Control Systems*, Madurai, India, Dec. 2020, pp. 12–18, https://doi.org/10.1109/ICICCS48265.2020.9121047.

[16] A. Hamarsheh *et al.*, "Comparative Evaluation of Host-Based Translator Mechanisms for IPv4-IPv6 Communication Performance Analysis With Different Routing Protocols," *International Journal of Cloud Applications and Computing*, vol. 13, no. 1, pp. 1–26, Jan. 2023, https://doi.org/10.4018/IJCAC.332765.

[17] G. G. Lencse and A. Bazso, "Benchmarking methodology for IPv4aaS technologies: Comparison of the scalability of the Jool implementation of 464XLAT and MAP-T," *Computer Communications*, vol. 219, pp. 243–258, Apr. 2024, https://doi.org/10.1016/j.comcom.2024.03.007.

[18] G. Lencse and N. Nagy, "Towards the scalability comparison of the Jool implementation of the 464XLAT and of the MAP-T IPv4aaS technologies," *International Journal of Communication Systems*, vol. 35, no. 18, 2022, Art. no. e5354, https://doi.org/10.1002/dac.5354.

[19] S. Singalar and R. M. Banakar, "Performance Analysis of IPv4 to IPv6 Transition Mechanisms," in *Fourth International Conference on Computing Communication Control and Automation*, Pune, India, Aug. 2018, pp. 1–6, https://doi.org/10.1109/ICCUBEA.2018.8697539.

[20] T. Saraj, A. Hanan, M. S. Akbar, M. Yousaf, A. Qayyum, and M. Tufail, "IPv6 tunneling protocols: Mathematical and testbed setup performance analysis," in *Conference on Information Assurance and Cyber Security*, Rawalpindi, Pakistan, Dec. 2015, pp. 62–68, https://doi.org/10.1109/CIACS.2015.7395568.

[21] K. El Khadiri, O. Labouidya, N. Elkamoun, and R. Hilal, "Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Applications using OPNET Modeler," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 4, pp. 387–392, May 2018, https://doi.org/10.14569/IJACSA.2018.090454.

[22] Z. Ashraf and M. Yousaf, "Optimized Convergence of OSPFv3 in Large Scale Hybrid IPv4-IPv6 Network," in *14th International Conference on Emerging Technologies*, Islamabad, Pakistan, Nov. 2018, pp. 1–6, https://doi.org/10.1109/ICET.2018.8603633.

[23] A. Quintero, F. Sans, and E. Gamess, "Performance Evaluation of IPv4/IPv6 Transition Mechanisms," *International Journal of Computer Network and Information Security*, vol. 8, no. 2, pp. 1–14, 2016, https://doi.org/10.5815/ijcnis.2016.02.01.

[24] P. Amr and N. Abdelbaki, "Convergence study of IPv6 tunneling techniques," in *10th International Conference on Communications*, Bucharest, Romania, Dec. 2014, pp. 1–6, https://doi.org/10.1109/ICComm.2014.6866678.

[25] O. Aslan, S. S. Aktug, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, Jan. 2023, Art. no. 1333, https://doi.org/10.3390/electronics12061333.

[26] J. Kumar and G. Ranganathan, "Malware Attack Detection in Large Scale Networks using the Ensemble Deep Restricted Boltzmann Machine," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11773–11778, Oct. 2023, https://doi.org/10.48084/etasr.6204.

[27] J. Kristoff, M. Ghasemisharif, C. Kanich, and J. Polakis, "Plight at the end of the tunnel: Legacy ipv6 transition mechanisms in the wild," in *International Conference on Passive and Active Network Measurement*, Cottbus, Germany, Mar. 2021, pp. 390–405, https://doi.org/10.1007/978-3-030-72582-2_23.

[28] G. Lencse and Y. Kadobayashi, "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64," *Computers & Security*, vol. 77, pp. 397–411, Aug. 2018, https://doi.org/10.1016/j.cose.2018.04.012.

[29] K. Gu, L. Zhang, Z. Wang, and Y. Kong, "Comparative studies of IPv6 tunnel security," in *13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery*, Guilin, China, Jul. 2017, pp. 2799–2804, https://doi.org/10.1109/FSKD.2017.8393224.

[30] W. Alzaid and B. Issac, "Analysis of IPv6 through Implementation of Transition Technologies and Security Attacks," *International Journal of Business Data Communications and Networking*, vol. 12, no. 1, pp. 36–62, Jan. 2016, https://doi.org/10.4018/IJBDCN.2016010103.

[31] N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong, R. Elz, and P. Pongpaibool, "Performance evaluation of IPv4/IPv6 transition mechanisms: IPv4-in-IPv6 tunneling techniques," in *The International Conference on Information Networking*, Phuket, Thailand, Feb. 2014, pp. 238–243, https://doi.org/10.1109/ICOIN.2014.6799698.

[32] A. S. Ahmed, R. Hassan, and N. E. Othman, "Security threats for IPv6 transition strategies: A review," in *4th International Conference on Engineering Technology and Technopreneuship*, Kuala Lumpur, Malaysia, Aug. 2014, pp. 83–88, https://doi.org/10.1109/ICE2T.2014.7006224.

[33] P. A. Alvarez, A. Ishizaka, and L. Martínez, "Multiple-criteria decision-making sorting methods: A survey," *Expert Systems with Applications*, vol. 183, Nov. 2021, Art. no. 115368, https://doi.org/10.1016/j.eswa.2021.115368.

[34] A. Singh, "Major MCDM Techniques and their application-A Review," *IOSR Journal of Engineering*, vol. 4, no. 5, pp. 15–25, May 2014, https://doi.org/10.9790/3021-04521525.

[35] A. K. Babar, Z. A. Zardari, S. Qureshi, S. Han, and N. N. Hussaini, "Assessment of IPv4 and IPv6 Networks with Different Modified Tunneling Techniques using OPNET," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 9, pp. 476–482, Jan. 2019, https://doi.org/10.14569/IJACSA.2019.0100926.

[36] M. Georgescu, H. Hazeyama, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "The STRIDE Towards IPv6: A Comprehensive Threat Model for IPv6 Transition Technologies:," in *2nd International Conference on Information Systems Security and Privacy*, Rome, Italy, Feb. 2016, pp. 243–254, https://doi.org/10.5220/0005652402430254.

[37] S. Narayan, S. Ishrar, A. Kumar, R. Gupta, and Z. Khan, "Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols," in *Thirteenth International Conference on Wireless and Optical Communications Networks*, Hyderabad, India, Jul. 2016, pp. 1–7, https://doi.org/10.1109/WOCN.2016.7759027.

[38] J. L. Shah and J. Parvez, "An examination of next generation IP migration techniques: Constraints and evaluation," in *International Conference on Control, Instrumentation, Communication and Computational Technologies*, Kanyakumari, India, Jul. 2014, pp. 776–781, https://doi.org/10.1109/ICCICCT.2014.6993064.

[39] D. Hadiya, R. Save, and G. Geetu, "Network Performance Evaluation of 6to4 and Configured Tunnel Transition Mechanisms: An Empirical Test-Bed Analysis," in *6th International Conference on Emerging Trends in Engineering and Technology*, Nagpur, India, Dec. 2013, pp. 56–60, https://doi.org/10.1109/ICETET.2013.14.

[40] M. Aazam, A. M. Syed, S. A. H. Shah, I. Khan, and M. Alam, "Evaluation of 6to4 and ISATAP on a test LAN," in *IEEE Symposium on Computers & Informatics*, Kuala Lumpur, Malaysia, Mar. 2011, pp. 46–50, https://doi.org/10.1109/ISCI.2011.5958881.

[41] L. Smith, M. Jacobi, and S. Al-Khayatt, "Evaluation of IPv6 transition mechanisms using QoS service policies," in *11th International Symposium on Communication Systems, Networks & Digital Signal Processing*, Budapest, Hungary, Jul. 2018, pp. 1–5, https://doi.org/10.1109/CSNDSP.2018.8471772.

[42] T. T. Lu, C. Y. Wu, W. Y. Lin, H. P. Chen, and K. P. Hsueh, "Comparison of IPv4-over-IPv6 (4over6) and Dual Stack Technologies in Dynamic Configuration for IPv4/IPv6 Address," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, J.-S. Pan, P.-W. Tsai, and H.-C. Huang, Eds. New York, NY, USA: Springer, 2017, pp. 259–269.

[43] Y. Sookun and V. Bassoo, "Performance analysis of IPv4/IPv6 transition techniques," in *IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Balaclava, Mauritius, Aug. 2016, pp. 188–193, https://doi.org/10.1109/EmergiTech.2016.7737336.

[44] G. Altangerel, E. Tsogbaatar, and D. Yamkhin, "Performance analysis on IPv6 transition technologies and transition method," in *11th International Forum on Strategic Technology*, Novosibirsk, Russia, Jun. 2016, pp. 465–469, https://doi.org/10.1109/IFOST.2016.7884155.

[45] J. S. Sansa-Otim and A. Mile, "IPv4 to IPv6 Transition Strategies for Enterprise Networks in Developing Countries," in *International Conference on e-Infrastructure and e-Services for Developing Countries*, Blantyre, Malawi, Nov. 2013, pp. 94–104, https://doi.org/10.1007/978-3-642-41178-6_10.

[46] S. Narayan, R. Gupta, A. Kumar, S. Ishrar, and Z. Khan, "Cyber security attacks on network with transition mechanisms," in *International Conference on Computing and Network Communications*, Trivandrum, India, Dec. 2015, pp. 163–169, https://doi.org/10.1109/CoCoNet.2015.7411182.

[47] Komal, "Performance Evaluation of Tunneling Mechanisms in IPv6 Transition: A Detailed Review," in *Second International Conference on Advances in Computing and Communication Engineering*, Dehradun, India, Dec. 2015, pp. 144–149, https://doi.org/10.1109/ICACCE.2015.95.

[48] M. Georgescu, H. Hazeyama, Y. Kadobayashi, and S. Yamaguchi, "Empirical analysis of IPv6 transition technologies using the IPv6 Network Evaluation Testbed," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 2, no. 2, Feb. 2015, Art. no. e1, https://doi.org/10.4108/inis.2.2.e1.

[49] M. Aazam and E.-N. Huh, "Impact of ipv4-ipv6 coexistence in cloud virtualization environment," *annals of telecommunications - annales des telecommunications*, vol. 69, no. 9, pp. 485–496, Oct. 2014, https://doi.org/10.1007/s12243-013-0391-6.

[50] A. S. Wahid, M. Othman, O. Sembiyev, and M. H. Selamat, "Performance of cpu utilization for IPv6 tunneling mechanisms on linux based testbed," *Eurasian Journal of Mathematical and Computer Applications*, vol. 2, no. 3, pp. 30–42, 2014.

[51] F. Sans and E. Gamess, "Analytical performance evaluation of native IPv6 and several tunneling technics using benchmarking tools," in *XXXIX Latin American Computing Conference*, Caracas, Venezuela, Oct. 2013, pp. 1–9, https://doi.org/10.1109/CLEI.2013.6670610.

[52] B. C. Brookes, "Bradford's Law and the Bibliography of Science," *Nature*, vol. 224, no. 5223, pp. 953–956, Dec. 1969, https://doi.org/10.1038/224953a0.

[53] D. J. Borgohain, Verma ,Manoj Kumar, Nazim ,Mohammad, and M. and Sarkar, "Application of Bradford's law of scattering and Leimkuhler model to information science literature," *COLLNET Journal of Scientometrics and Information Management*, vol. 15, no. 1, pp. 197–212, Jan. 2021, https://doi.org/10.1080/09737766.2021.1943041.