Alqalam Journal of Medical and Applied Sciences. 2026;9(6):1591-1605
https://doi.org/10.54361/ajmas.269621

Review article

Toward IPv6-only Networking: Deployment Readiness, Enabling Architectures, Operational Challenges, and Future Directions

Munira Ayad[1]*, Nuredin Ahmed[2]

[1]*Department of Electrical and Computer Engineering, Libyan Academy for Postgraduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
Corresponding Email. *munira.b.ayad@gmail.com*

Abstract
IPv6 adoption has expanded significantly across modern Internet infrastructures, leading to increasing interest in the practical realization of IPv6-only networking. While substantial progress has been achieved in protocol deployment, the successful operation of IPv6-only environments depends not only on the availability of transition technologies but also on the readiness of infrastructure platforms, application ecosystems, enterprise environments, and emerging IoT and edge-computing systems. This survey evaluates IPv6-only deployment readiness across key operational domains, including infrastructure, applications, enterprise networks, IoT ecosystems, and global adoption trends. It further reviews the principal architectures enabling IPv6-only networking, including translation-based technologies, IPv4-as-a-Service (IPv4aaS) solutions, and programmable IPv6 frameworks, while examining the operational challenges associated with their deployment. The analysis highlights important issues related to interoperability, service continuity, operational visibility, reliability, enterprise migration, and security management. Unlike previous surveys that primarily focus on transition mechanisms, performance evaluation, or IPv6 adoption trends, this paper integrates deployment readiness assessment, architectural analysis, and operational considerations within a unified IPv6-only networking perspective. Based on the reviewed literature, several research gaps are identified, including a limited understanding of large-scale enterprise IPv6-only deployment, insufficient evaluation of IPv6-only IoT and edge ecosystems, fragmented security assessment, and the lack of long-term operational and performance studies. The findings provide a comprehensive view of the current state of IPv6-only networking and establish a foundation for future research and deployment strategies.
Keywords: IPv6-only Networking, Deployment Readiness, IPv4-as-a-Service (IPv4aaS), IPv6 Adoption.

Introduction

The Internet is undergoing a gradual transformation toward IPv6-only networking as the limitations of IPv4 become increasingly apparent. Originally designed with a 32-bit addressing architecture, IPv4 provides approximately 4.3 billion unique addresses, a capacity that is no longer sufficient to support the continuous growth of cloud computing, mobile communications, hyperscale infrastructures, and Internet of Things (IoT) ecosystems [1], [2], [3]. Although Network Address Translation (NAT) significantly extended the operational lifetime of IPv4, it introduced architectural complexity, reduced end-to-end transparency, and increased dependence on stateful intermediary devices [4], [5], [6].

To overcome these limitations, IPv6 was developed as the long-term successor to IPv4. Through its 128-bit addressing architecture, IPv6 provides an effectively inexhaustible address space while introducing several architectural improvements, including simplified packet processing, Stateless Address Autoconfiguration (SLAAC), improved routing scalability, and enhanced support for modern distributed services [2], [7]. These capabilities make IPv6 a fundamental enabler of future Internet growth and large-scale digital transformation [1], [3].

Table 1. Comparison between ipv4 and ipv6 networking architectures

Feature	IPv4	IPv6
Address Length	32-bit	128-bit
Address Space	~4.3 × 10^9 addresses	~3.4 × 10^{38} addresses
NAT Dependency	High	Minimal NAT requirement
Header Complexity	Variable	Simplified
Broadcast Support	Supported	Replaced by Multicast
End-to-End Connectivity	Limited by NAT	Native Support

The transition toward IPv6-only networking is increasingly influenced not only by technical scalability requirements, but also by governmental policies, cloud operational models, and long-term infrastructure sustainability considerations [1], [8]. For example, the United States Office of Management and Budget (OMB) memorandum M-21-07 established strategic targets encouraging IPv6-only deployment across federal infrastructures by the end of 2025 [1]. In parallel, major cloud service providers have gradually introduced

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

economic disincentives for large-scale public IPv4 utilization, reflecting the growing operational and financial burden associated with scarce IPv4 resources [1], [8].
Recent Internet telemetry measurements indicate continued growth in global IPv6 adoption. According to data from APNIC Labs, worldwide IPv6 capability has exceeded approximately 43%, while the Asia-Pacific region has surpassed the 50% capability milestone [9].

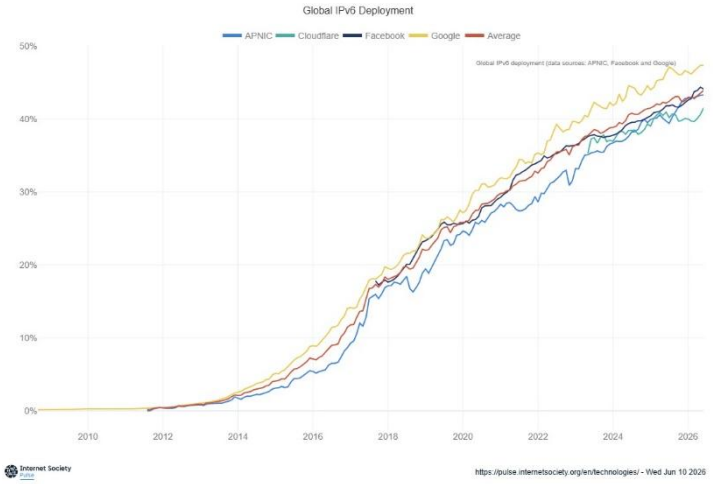

Figure 1. Global IPv6 capability growth and regional adoption trends based on APNIC Labs measurements [9].

Similarly, the Google IPv6 Statistics Platform indicates that native IPv6 traffic accessing Google services has approached nearly half of global Internet connectivity traffic, while several regions have already exceeded 50% deployment levels [10].

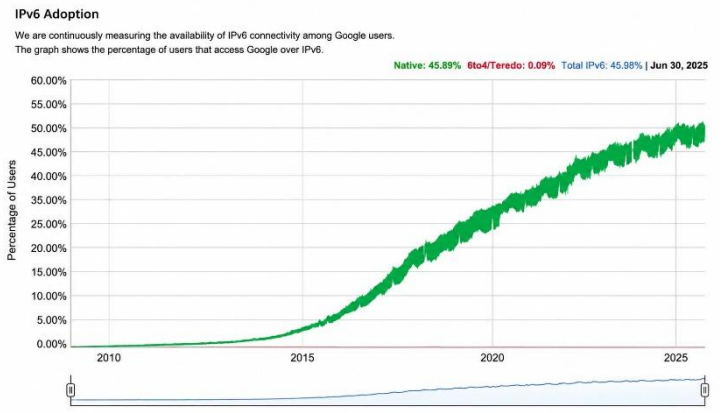

Figure 2. Global IPv6 traffic percentage observed across Google services [10].

Despite this progress, large-scale IPv6-only deployment remains challenging. Since IPv4 and IPv6 are not directly interoperable, organizations must rely on coexistence and interoperability mechanisms to maintain communication with legacy IPv4 services. Consequently, various approaches have been developed, including dual-stack operation, tunneling techniques, translation-based mechanisms, and IPv4-as-a-Service (IPv4aaS) architectures [2], [4], [5], [11].
Although previous studies have extensively investigated individual transition technologies, performance evaluations, and deployment experiences, the literature remains fragmented across isolated technical domains. Existing surveys often focus on specific mechanisms, security issues, or deployment case studies without providing a holistic assessment of IPv6-only deployment readiness across contemporary network ecosystems [3], [4], [5], [12], [13], [14].
Therefore, this survey provides a comprehensive review of the architectures that enable IPv6-only networking and evaluates the readiness of modern infrastructures for sustainable IPv6-only operation. The paper examines deployment readiness across infrastructure platforms, application ecosystems, enterprise environments, IoT and edge-computing systems, and global adoption trends. It further analyzes operational and security challenges, identifies current research gaps, and highlights future research directions that may support the continued evolution toward scalable and sustainable IPv6-only networking.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

Methodology

This survey follows a structured literature review approach. Relevant studies were identified through major digital libraries, including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and RFC repositories. The literature selection focused on publications addressing IPv6-only networking, IPv6 transition technologies, IPv4-as-a-Service (IPv4aaS), deployment readiness, operational challenges, and emerging programmable IPv6 architectures. Priority was given to peer-reviewed journal articles, conference papers, RFC documents, and recent studies published between 2020 and 2026. After screening for relevance and technical contribution, the selected literature was analyzed according to four main dimensions: deployment readiness, enabling architectures, operational challenges, and future research directions.

Background and Evolution Toward IPv6-only Networking

A. Limitations of IPv4 and Address Exhaustion

Internet Protocol version 4 (IPv4) served as the foundational communication protocol of the modern Internet for several decades. Designed during the early stages of Internet development, IPv4 utilizes a 32-bit addressing architecture capable of supporting approximately (4.3×10^9) unique addresses [2]. While this capacity was initially considered sufficient, the rapid expansion of Internet-connected systems significantly accelerated global address consumption.

To mitigate address scarcity, network operators widely adopted Network Address Translation (NAT) technologies, enabling multiple devices to share a limited pool of public IPv4 addresses [15]. Although NAT extended the operational lifetime of IPv4, it also introduced several architectural and operational limitations. These include increased network complexity, dependence on stateful middleboxes and reduced end-to-end transparency. Furthermore, large-scale NAT deployments complicated peer-to-peer communication models and created operational challenges for latency-sensitive and cloud-native applications [5], [6], [7]

These limitations demonstrated that incremental IPv4 extensions alone could not provide a sustainable long-term solution for future Internet growth. Consequently, the Internet Engineering Task Force (IETF) developed IPv6 as the long-term successor to IPv4. By introducing a 128-bit addressing architecture capable of supporting (2^{128}) unique addresses, IPv6 provides a scalable foundation for future Internet expansion while reducing dependence on extensive address translation mechanisms [2], [4].

B. Architectural Advantages of IPv6

In addition to significantly expanding address capacity, IPv6 introduces several architectural improvements designed to support scalability, routing efficiency, and modern distributed network environments [2], [16]. Unlike IPv4, IPv6 utilizes a simplified fixed-length packet header structure that reduces packet-processing complexity within routers and core network devices [2]. The protocol also eliminates several legacy mechanisms that previously increased forwarding overhead in IPv4 environments, including router-based packet fragmentation and header checksum recalculation [2], [4].

IPv6 further supports Stateless Address Autoconfiguration (SLAAC), enabling devices to automatically generate addresses without requiring extensive manual configuration or continuous dependence on Dynamic Host Configuration Protocol (DHCP) infrastructures [16]. This capability improves deployment flexibility and simplifies large-scale network management, particularly in cloud-native and IoT-oriented environments. Another major architectural advantage of IPv6 is its ability to reduce reliance on large-scale Network Address Translation (NAT) deployments [2], [5]. By restoring globally routable addressing models, IPv6 facilitates improved end-to-end communication transparency and simplifies peer-to-peer service deployment.

C. From Dual-Stack to Native IPv6-only Environments

Early IPv6 deployment strategies primarily relied on dual-stack networking models, where IPv4 and IPv6 protocols operated simultaneously within the same infrastructure [2], [4]. Dual-stack deployment was initially considered the most practical migration approach because it allowed gradual IPv6 adoption while maintaining compatibility with existing IPv4 services and applications [17].

However, despite its operational flexibility, long-term dual-stack operation introduced significant complexity for enterprise and carrier-grade environments. Maintaining parallel IPv4 and IPv6 infrastructures increased administrative overhead, routing complexity, security management requirements, and troubleshooting difficulty [3], [5].

As IPv6 deployment matured, network operators and researchers increasingly shifted attention toward IPv6-only operational models combined with selective IPv4 interoperability mechanisms such as NAT64/DNS64, 464XLAT, and IPv4-as-a-Service (IPv4aaS) architectures [5], [11], [18]. This evolution reflects a broader transition away from permanent dual-stack coexistence toward scalable IPv6-centric infrastructures capable of supporting modern cloud-native, hyperscale, and mobile network environments [1], [3], [12].

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

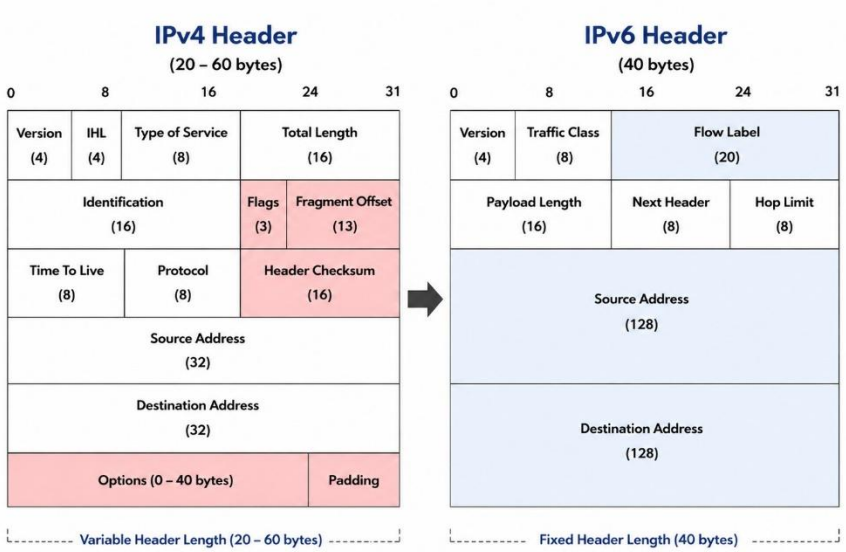

Figure 3. Comparison of IPv4 and IPv6 Header Structures Highlighting Header Simplification and Field Optimization.

D. Emergence of IPv4-as-a-Service (IPv4aaS) Models

As organizations moved toward IPv6-centric networking, several transition models emerged to preserve interoperability with legacy IPv4 services while reducing direct dependence on native IPv4 infrastructure [5], [11]. Among the most significant approaches are IPv4-as-a-Service (IPv4aaS) architectures, which enable IPv4 connectivity to operate as an overlay or translation service across predominantly IPv6 transport networks.

IPv4aaS mechanisms such as Dual-Stack Lite (DS-Lite), Mapping of Address and Port using Translation (MAP-T), and Mapping of Address and Port using Encapsulation (MAP-E) were developed to improve scalability and address conservation within carrier-grade and broadband environments [5], [11], [13]. These mechanisms differ in implementation strategies, including stateful translation, stateless mapping, encapsulation techniques, and traffic forwarding models. In addition to improving address utilization efficiency, IPv4aaS architectures reduce the operational burden associated with maintaining fully native IPv4 infrastructures [5], [11]. Recent studies have also explored the integration of IPv4aaS technologies with programmable networking paradigms, software-defined networking (SDN), and SRv6-based underlay infrastructures to improve scalability and operational flexibility [12], [19].

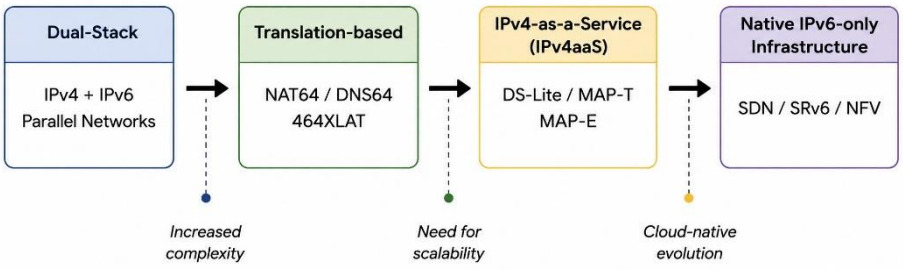

Figure 4. Evolution from dual-stack to native IPv6-only environments.

Despite their advantages, IPv4aaS deployments introduce several technical and operational challenges, including interoperability limitations, translation overhead, troubleshooting complexity, and additional security considerations [11], [14]. Consequently, understanding the strengths and limitations of these architectures remains essential for evaluating real-world IPv6-only deployment readiness.

IPv6-only Deployment Readiness Assessment

The successful adoption of IPv6-only networking depends not only on protocol availability but also on the readiness of the surrounding ecosystem. While significant progress has been achieved in IPv6 deployment, readiness remains uneven across infrastructure platforms, applications, enterprise environments, and IoT ecosystems. Consequently, evaluating deployment readiness has become a critical component of long-term

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

IPv6-only planning. To provide a holistic perspective, this section examines IPv6-only readiness across five key domains: infrastructure modernization, application and service ecosystems, enterprise environments, IoT and edge computing, and global deployment trends.

A. Infrastructure Modernization

Infrastructure modernization is one of the strongest indicators of IPv6-only readiness. Over the past decade, Internet service providers (ISPs), mobile operators, cloud providers, and research networks have significantly expanded native IPv6 support across routing infrastructures, data centers, and service delivery platforms [1], [3], [8]. As a result, IPv6 capability is now a standard feature in most modern networking environments. However, readiness remains uneven. While hyperscale cloud providers and large telecommunications operators have largely modernized their infrastructures, many organizations continue to rely on legacy hardware, software platforms, and management systems originally designed for IPv4 environments [3], [8]. These dependencies often require coexistence mechanisms that increase operational complexity and slow the transition toward fully native IPv6-only operation.

Real-world deployment experiences illustrate both the progress achieved and the challenges that remain. Robinson et al. [20] documented the successful deployment of an IPv6-enabled network supporting the SC23 conference environment, demonstrating that heterogeneous infrastructures can effectively support large-scale IPv6 operation when supported by careful planning, validation, and operational testing. Their findings suggest that technical barriers have decreased substantially, while organizational readiness and migration planning increasingly determine deployment success. Overall, the literature indicates that infrastructure modernization has reached a relatively mature stage in many sectors. Nevertheless, sustainable IPv6-only deployment continues to depend on the gradual replacement of legacy components, improved operational integration, and long-term modernization strategies.

B. Application and Service Ecosystems

The readiness of application and service ecosystems is a critical requirement for IPv6-only operation. Modern operating systems, cloud platforms, web services, and content delivery infrastructures increasingly support IPv6 natively, while interoperability mechanisms such as NAT64 and DNS64 allow IPv6-only clients to maintain connectivity with legacy IPv4 services [18]. Despite this progress, application compatibility remains a challenge. Several studies report that some applications continue to depend on embedded IPv4 literals, legacy APIs, and IPv4-specific assumptions that may only become apparent after migration to IPv6-only environments [21], [22], [23]. Such hidden dependencies can increase migration complexity and introduce operational risk.

Service reliability is also influenced by DNS behavior and network configuration practices. Yamamoto et al. [22] identified issues related to DNS resolution failures, Path MTU Discovery (PMTUD), and inappropriate ICMPv6 filtering, demonstrating that application performance may be affected by factors extending beyond basic connectivity. Similarly, Dekinder et al. [24] observed that many web ecosystems continue to operate in mixed IPv4/IPv6 environments, indicating that protocol dependencies remain embedded within modern content delivery and service infrastructures. These observations suggest that application readiness extends beyond protocol support and requires comprehensive ecosystem-wide validation of services, dependencies, and operational workflows.

C. Enterprise and Operational Environments

Enterprise networks remain among the most challenging domains for IPv6-only deployment. Although modern routing, switching, firewall, and management platforms generally support IPv6, organizations frequently operate heterogeneous environments containing legacy applications, business systems, authentication platforms, and third-party integrations [3], [25], [26].

In many cases, operational processes present greater obstacles than technology itself. Monitoring procedures, security policies, troubleshooting methodologies, and address-management frameworks have often evolved over decades of IPv4 operation [25], [26]. Consequently, IPv6-only deployment frequently requires process modernization, staff training, and governance adaptation in addition to infrastructure upgrades.

Operational evidence from real-world deployments reinforces this observation. Costello et al. [27] described the implementation of an IPv6-only testbed supporting legacy connectivity through NAT64, DNS64, RFC8925, and related translation mechanisms. Their experience showed that successful deployment depended not only on technical IPv6 support but also on effective troubleshooting procedures, user awareness, operational guidance, and management of application and VPN dependencies. These findings highlight the importance of organizational preparedness and end-user support in reducing deployment barriers.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

The literature therefore suggests that enterprise readiness should be evaluated as a combination of technical capability, operational maturity, and organizational commitment. While technological barriers have decreased substantially, operational transformation remains essential for sustainable IPv6-only adoption.

D. IoT and Edge Environments

IoT and edge-computing ecosystems are widely regarded as major drivers of IPv6 adoption because of their requirement to support massive numbers of interconnected devices. IPv6 provides virtually unlimited address capacity, enabling scalable connectivity without the constraints associated with IPv4 address exhaustion [1], [28].

Recent studies indicate increasing IPv6 adoption across smart-home systems, industrial sensors, consumer devices, and edge-computing infrastructures [28], [29]. Nevertheless, readiness remains inconsistent across device categories, manufacturers, and deployment scenarios. Hu et al. [28] demonstrated that IPv6 utilization varies significantly among IoT devices, with some platforms providing full support while others retain partial dependence on IPv4-based services.

Recent Internet-scale measurements further highlight the complexity of IPv6 deployment within IoT ecosystems. Dahlmanns et al. [29] identified thousands of IPv6-reachable IoT deployments across the global Internet and observed that many devices remained exposed through publicly accessible IPv6 services. Their findings suggest that, although IPv6 adoption is expanding within IoT environments, challenges related to device management, deployment visibility, and operational security remain significant. These observations reinforce the need for improved understanding of large-scale IPv6-enabled IoT ecosystems beyond controlled smart-home environments. Additional challenges arise from device lifecycle management, limited firmware updates, heterogeneous implementations, and resource-constrained operating environments [28], [29], [30]. These factors complicate interoperability, operational consistency, and large-scale deployment governance. Consequently, achieving sustainable IPv6-only operation in IoT ecosystems requires improved implementation consistency and stronger lifecycle management practices.

E. Global Adoption and Deployment Readiness

Global IPv6 readiness has improved substantially in recent years, but deployment remains highly uneven across countries, regions, and service providers. Recent Google measurements show that IPv6 traffic to Google services has reached approximately the 50% global milestone, while APNIC measurements report lower global IPv6 capability, around the low-40% range, demonstrating that adoption levels vary depending on the measurement methodology and data source [9], [10].

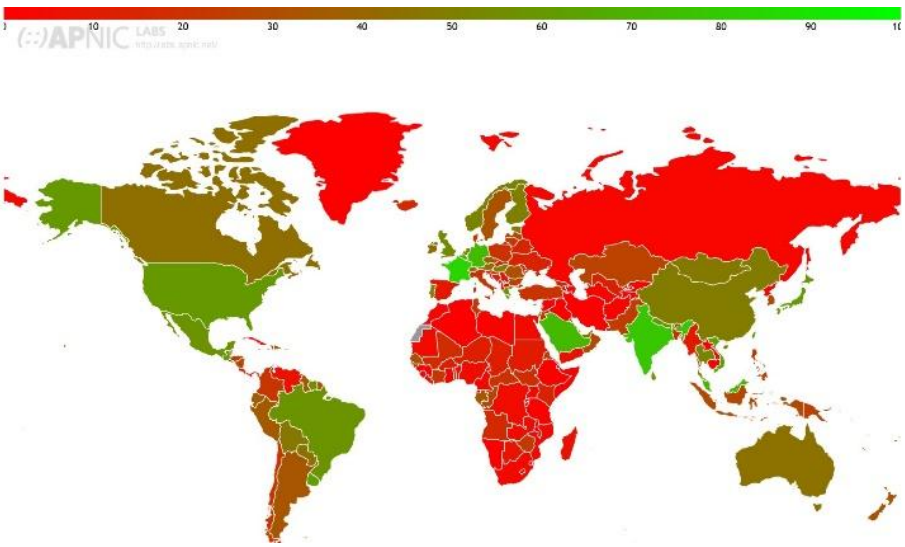

Figure 5. IPv6 Capable Rate by country (%) [9]

The disparity becomes clearer at the country and regional levels. APNIC Labs reports that several economies and regions have exceeded 50% IPv6 capability, while others remain far below this level, and some are still below 10% capability [9]. Internet Society Pulse similarly shows regional differences: IPv6 support among top websites is about 49% in the Americas, 48% in Asia, 35% in Europe, 37% in Oceania, and only 6% in Africa [9]. These figures show that IPv6 readiness is not globally uniform.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

Table 2. Regional Differences APNIC Labs [9].

Region	IPv6 Capable[1]	IPv6 Preferred[1]
World	43.17%	41.56%
Africa	5.86%	5.71%
Americas	49.68%	48.99%
Asia	50.02%	47.61%
Europe	36.13%	35.54%
Oceania	39.89%	37.38%
Unclassified	14.00%	13.71%

[1] *June 2026.*

This uneven deployment creates practical challenges for IPv6-only transition. Organizations operating across multiple regions may find that some networks, providers, or application ecosystems are highly IPv6-capable, while others still require IPv4 connectivity. As a result, even organizations with strong internal IPv6 readiness may need to maintain dual-stack or translation-based mechanisms to preserve global reachability. Several factors explain this variation, including differences in infrastructure maturity, national policy support, economic priorities, vendor readiness, workforce expertise, and operational incentives. Mobile operators and large cloud providers have generally advanced faster because they face stronger scalability pressure, while many enterprise and regional networks continue to operate stable IPv4-based infrastructures with limited short-term motivation to migrate [1], [8]. Overall, global IPv6 adoption statistics demonstrate positive momentum, but they also reveal a major readiness gap. The existence of regions above 50% adoption alongside regions below 10% indicates that IPv6-only deployment is becoming practical in some environments while remaining difficult in others. Therefore, global IPv6-only readiness should be understood as uneven and multidimensional rather than complete or universally achieved.

Table 3. IPv6-only Deployment Readiness Assessment.

Domain	Current Readiness	Major Challenges
Infrastructure	High	Legacy systems and integration
Applications	Medium–High	Hidden IPv4 dependencies
Enterprise Networks	Medium	Operational transformation
IoT & Edge	Medium	Heterogeneous implementations
Cloud Platforms	High	Service integration
Security Operations	Medium	Visibility and monitoring challenges

Enabling Architectures and Operational Challenges for IPv6-only Networking

The evolution toward IPv6-only networking has been supported by a diverse set of architectural approaches designed to maintain interoperability with legacy IPv4 systems while reducing long-term dependence on native IPv4 infrastructures. These mechanisms differ in their operational principles, scalability characteristics, deployment complexity, and suitability for IPv6-only environments. This section reviews the principal architectural approaches that enable IPv6-only operation and examines their advantages, limitations, and contemporary relevance.

A. Dual-Stack Architectures

Dual-stack networking represents one of the earliest IPv6 deployment strategies, allowing IPv4 and IPv6 to operate simultaneously within the same infrastructure [2], [4]. Its primary advantage lies in maintaining compatibility with legacy IPv4 systems while enabling incremental IPv6 adoption. This flexibility contributed significantly to the early expansion of IPv6 across enterprise, ISP, and cloud environments [17].

Despite these benefits, long-term dual-stack operation introduces considerable operational complexity, organizations must maintain parallel routing policies, security controls, monitoring frameworks, and address-management systems for both protocols. In addition, persistent IPv4 fallback behavior often slows the transition toward fully native IPv6 operation and prolongs dependence on legacy infrastructures [3], [8]. Security management also becomes more challenging because administrators must secure and monitor two independent protocol environments simultaneously, increasing the overall attack surface [6], [7], [14].

Consequently, contemporary research increasingly views dual-stack networking as an effective transitional mechanism rather than a sustainable long-term architecture. Modern deployment strategies are progressively shifting toward IPv6-only operation supported by selective interoperability mechanisms for legacy IPv4 communication [5].

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

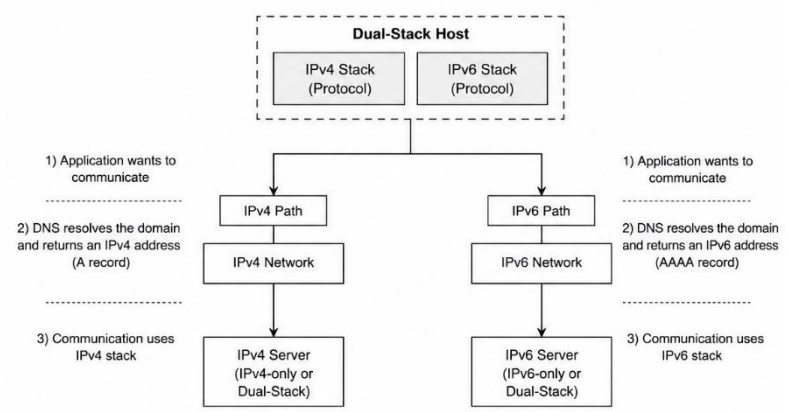

Figure 6. Conceptual operation of a dual-stack architecture.

B. Tunneling-Based Transition Mechanisms

Tunneling mechanisms were developed to facilitate IPv6 communication across IPv4 infrastructures during the early stages of IPv6 deployment. These approaches encapsulate IPv6 packets within IPv4 headers, allowing IPv6 traffic to traverse networks that lack native IPv6 support [2], [4]. Representative mechanisms include 6to4, ISATAP, and Teredo, each designed to address specific deployment scenarios such as inter-site connectivity, enterprise integration, and NAT traversal [2].

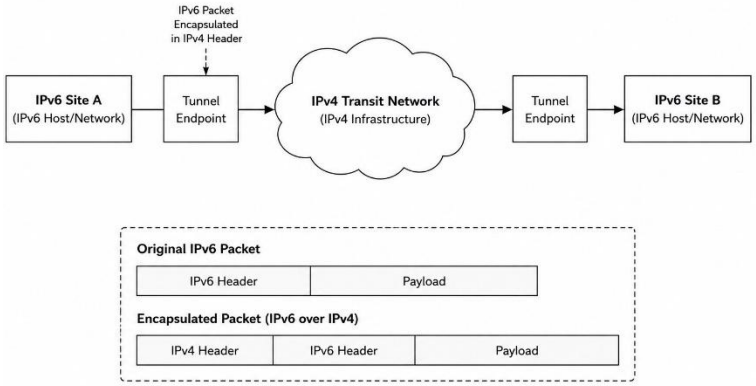

Figure 7. Conceptual operation of an IPv6-over-IPv4 tunneling mechanism.

Tunneling technologies played an important role in accelerating early IPv6 adoption by providing interoperability without requiring immediate infrastructure replacement. However, their operational relevance has gradually declined as native IPv6 deployment has become more widespread [2], [5].

Several limitations have reduced the long-term attractiveness of tunneling-based approaches. Packet encapsulation introduces additional processing overhead and may negatively affect latency, throughput, and troubleshooting efficiency [2], [5]. Furthermore, tunnel management becomes increasingly complex in large-scale operational environments, particularly when multiple transition mechanisms coexist.

Security considerations represent another significant challenge. Encapsulated traffic can complicate firewall inspection, intrusion detection, and network monitoring because IPv6 payloads are transported indirectly through IPv4 infrastructures [7], [14]. In some cases, tunneling mechanisms may also bypass traditional security controls, increasing operational risk [6]. Consequently, contemporary IPv6 deployment strategies rarely rely on tunneling as a primary long-term solution. Instead, modern environments increasingly favor translation-based mechanisms, IPv4-as-a-Service (IPv4aaS) architectures, and programmable IPv6 infrastructures that provide greater scalability, operational simplicity, and support for sustainable IPv6-only operation [5], [12], [19].

C. Translation-Based Transition Mechanisms

Translation-based mechanisms have become fundamental components of contemporary IPv6-only deployments. Unlike tunneling approaches, which encapsulate traffic across heterogeneous infrastructures, translation mechanisms directly convert packets between IPv4 and IPv6, enabling communication between hosts operating on different protocol versions [2], [5].

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

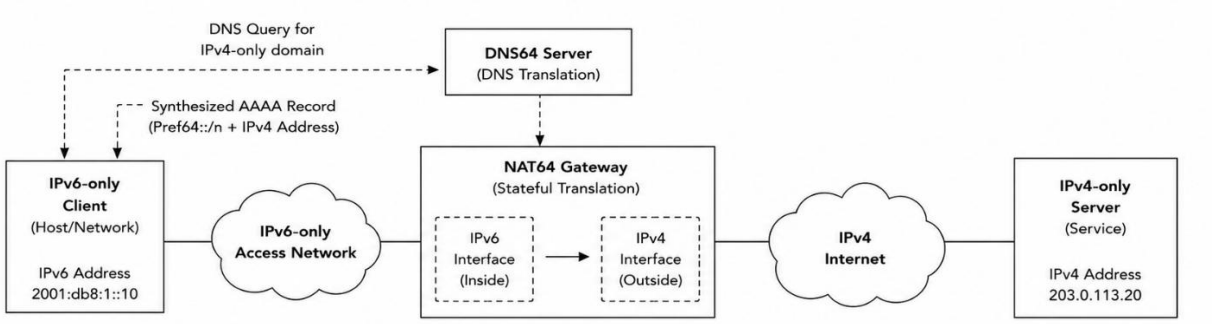

Figure 8. Conceptual operation of translation-based mechanisms (NAT64/DNS64) in an IPv6-only environment.

These architectures are particularly valuable in environments where IPv6-only clients must continue to access legacy IPv4 services. Consequently, translation technologies are widely deployed in mobile networks, cloud platforms, enterprise environments, and broadband infrastructures, pursuing IPv6-centric operational models [5], [18]. One of the most widely adopted solutions is the NAT64/DNS64 architecture. DNS64 synthesizes IPv6 records for IPv4-only destinations, while NAT64 gateways translate traffic between IPv6 and IPv4 domains [18]. This approach enables IPv6-only devices to access legacy IPv4 resources without requiring native IPv4 connectivity. As a result, NAT64/DNS64 has become a key enabler of large-scale IPv6-only deployments. Another important mechanism is 464XLAT, which combines customer-side and provider-side translation functions to improve compatibility with applications that continue to rely on IPv4 communication models [31]. Owing to its ability to support legacy applications while preserving IPv6-centric transport networks, 464XLAT has been widely adopted by mobile operators transitioning toward IPv6-only operation.

Despite their advantages, translation-based architectures introduce several operational considerations. Dynamic protocol translation may increase processing overhead, complicate troubleshooting, and create interoperability challenges for applications that embed IPv4 literals or depend on protocol-specific behaviors [4], [18]. Furthermore, maintaining consistent security visibility and policy enforcement across translated traffic flows remains an ongoing operational challenge. Nevertheless, translation-based mechanisms are increasingly regarded as practical interoperability layers that enable organizations to reduce native IPv4 dependence while maintaining service continuity. Compared with traditional coexistence and tunneling approaches, they offer a more scalable pathway toward sustainable IPv6-only operation.

D. IPv4-as-a-Service (IPv4aaS) Architectures

As network operators increasingly adopt IPv6-centric infrastructures, IPv4-as-a-Service (IPv4aaS) architectures have emerged as scalable approaches for delivering legacy IPv4 connectivity across predominantly IPv6 transport networks. Unlike traditional dual-stack deployments, IPv4aaS models treat IPv4 connectivity as a service operating over an IPv6 underlay, thereby reducing dependence on native IPv4 infrastructures [11].

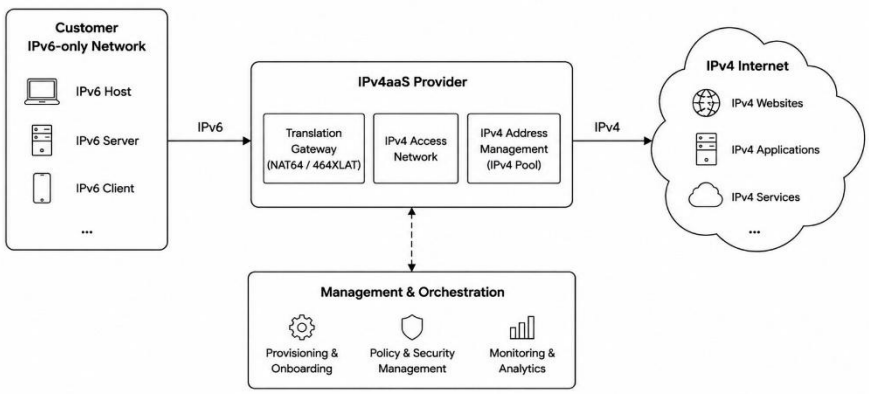

Figure 9. Conceptual operation of IPv4-as-a-Service (IPv4aaS) Architectures.

Several IPv4aaS mechanisms have been developed to support this objective, including Dual-Stack Lite (DS-Lite), Mapping of Address and Port using Translation (MAP-T), and Mapping of Address and Port using Encapsulation (MAP-E) [5], [13]. Although these architectures differ in forwarding methods, translation models, and state management strategies, they share a common goal: preserving compatibility with IPv4-dependent services while accelerating the transition toward IPv6-centric operation.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

DS-Lite encapsulates IPv4 traffic within IPv6 packets and relies on centralized Carrier-Grade NAT (CGN) infrastructures to provide IPv4 connectivity. In contrast, MAP-T and MAP-E employ stateless mapping techniques that reduce dependence on centralized stateful translation systems and improve scalability in large-scale broadband environments [11], [13].

Recent research has explored the integration of IPv4aaS mechanisms with Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Segment Routing over IPv6 (SRv6) to improve service automation, traffic engineering, and operational flexibility [12], [19]. These developments reflect a broader shift toward programmable and cloud-oriented networking architectures.

Despite their scalability advantages, IPv4aaS deployments introduce several operational challenges. Carrier-grade translation systems may reduce traffic visibility, complicate troubleshooting, and create interoperability issues for specific applications and protocols [11], [14]. In addition, maintaining consistent security policies across hybrid IPv4/IPv6 environments remains an important operational concern [6], [14]. Nevertheless, IPv4aaS architectures are increasingly regarded as one of the most practical pathways toward sustainable IPv6-only networking. By minimizing direct reliance on native IPv4 infrastructures while preserving compatibility with legacy services, they enable gradual modernization without disrupting existing operational ecosystems.

E. Programmable IPv6 Architectures

The emergence of cloud-native services, hyperscale data centers, and software-defined infrastructures has accelerated interest in programmable IPv6 architectures. Unlike traditional transition mechanisms that focus primarily on interoperability between IPv4 and IPv6, these approaches emphasize automation, service orchestration, traffic engineering, and long-term operational scalability within IPv6-centric environments [12], [19].

One of the most significant developments in this area is Segment Routing over IPv6 (SRv6), which extends native IPv6 forwarding by embedding routing and service instructions directly into packet headers. This capability enables flexible traffic engineering, service chaining, and improved network programmability without requiring complex overlay infrastructures [19]. Recent studies suggest that SRv6 can simplify network operations and enhance scalability in large-scale distributed environments [12], [32].

Programmable IPv6 infrastructures are also increasingly integrated with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). SDN enables centralized traffic management and automated policy enforcement, while NFV allows transition functions such as NAT64, DNS64, and carrier-grade translation services to operate as virtualized network functions rather than dedicated hardware appliances [32]. Together, these technologies improve deployment flexibility and facilitate dynamic resource scaling in cloud and service-provider environments. Despite their advantages, programmable architectures introduce new operational challenges. Organizations may face implementation complexity, interoperability concerns, and increased dependence on orchestration platforms and control systems [19], [32]. Nevertheless, programmable IPv6 architectures represent a significant evolution beyond traditional migration models. Rather than treating IPv6 adoption solely as a compatibility problem, these approaches position IPv6-only networking as a foundation for automated, scalable, and service-oriented Internet infrastructures. Consequently, SRv6, SDN, and NFV are increasingly viewed as strategic enablers of future IPv6-only ecosystems.

Table 4. Comparative Evaluation of IPv6-only Enabling Architectures.

Architecture	Scalability	Operational Complexity	Security Considerations	IPv6-only Suitability	Typical Deployment
Dual Stack	Medium	High	Medium	Low	Enterprise Networks, ISP Migration Environments
Tunneling (6to4, ISATAP, Teredo)	Low	High	Medium	Low	Legacy IPv4 Networks, Temporary Transition Scenarios
NAT64/DNS64	High	Medium	Medium	High	Mobile Networks, Cloud Platforms, IPv6-only Data Centers
464XLAT	High	Medium	Medium	Very High	Mobile Operator Networks, Smartphone Ecosystems
DS-Lite	High	Medium	Medium	Medium	Broadband ISPs, Residential Internet Services

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

MAP-T / MAP-E	Very High	Medium	High	High	Carrier Networks, Large-Scale Broadband Deployment
SRv6 / SDN / NFV	Very High	Medium	High	Very High	Cloud-Native Infrastructures, Data Centers, Service Provider Networks

Research Gaps and Future Research Directions

A. Synthesis of Major Findings

The literature reviewed in this survey demonstrates that the transition toward IPv6-only networking has progressed significantly over the past decade. Early transition approaches such as dual-stack deployment and tunneling mechanisms played a critical role in enabling IPv6 adoption during the initial migration stages. However, recent studies increasingly indicate that these mechanisms are best viewed as transitional solutions rather than sustainable long-term deployment models [2], [5], [11].

The review further reveals that translation-based technologies, including NAT64/DNS64 and 464XLAT, have become key enablers of contemporary IPv6-only deployments. These mechanisms allow IPv6-only networks to maintain interoperability with legacy IPv4 services while reducing dependence on scarce IPv4 address resources [11], [18]. Similarly, IPv4-as-a-Service (IPv4aaS) architectures such as DS-Lite, MAP-T, and MAP-E provide scalable alternatives for supporting IPv4 connectivity over IPv6 infrastructures [5], [11], [13].

From a deployment perspective, the findings indicate that infrastructure readiness has improved considerably across mobile networks, cloud environments, and modern service-provider infrastructures [1], [8], [20]. Application ecosystems have also demonstrated increasing levels of IPv6 support, although hidden IPv4 dependencies and compatibility limitations continue to affect some deployment scenarios [21], [22], [24]. Enterprise environments remain more heterogeneous, with operational processes, organizational priorities, workforce preparedness, and legacy systems often influencing migration decisions as much as technical considerations [25], [26], [27].

The review also highlights the growing importance of IoT and edge-computing ecosystems in driving IPv6 adoption. The scalability requirements associated with billions of connected devices reinforce the need for IPv6-based architectures capable of supporting sustainable long-term growth. At the same time, recent studies reveal significant challenges related to deployment visibility, device lifecycle management, interoperability, and operational governance within large-scale IPv6-enabled IoT environments [28], [29].

Security remains a critical consideration throughout the transition toward IPv6-only networking. Existing studies emphasize that future security strategies must extend beyond protocol-level vulnerabilities and address broader issues, including operational visibility, policy consistency, threat detection, monitoring, and governance across increasingly distributed environments [16], [30], [33]. Another important observation concerns the uneven nature of global IPv6 adoption. Although several countries and network operators have achieved high levels of IPv6 capability and traffic utilization, significant disparities remain across regions and deployment sectors [8], [9], [10]. These differences suggest that IPv6-only readiness is influenced not only by technological availability but also by economic conditions, organizational priorities, workforce expertise, and broader ecosystem maturity. Overall, the literature suggests that IPv6-only networking is increasingly achievable from a technical perspective. Nevertheless, successful deployment continues to depend on balancing interoperability requirements, operational readiness, security considerations, and long-term migration strategies. These observations provide the foundation for the research gaps and future directions identified in this survey.

B. Research Gaps

Despite substantial progress in IPv6 deployment and the growing maturity of IPv6-only networking architectures, several important research challenges remain insufficiently addressed in the current literature. Existing studies provide valuable insights into individual transition mechanisms, deployment experiences, and performance evaluations; however, many investigations remain fragmented across isolated technical domains. Based on the reviewed literature, four major research gaps can be identified.

Table 5. Summary of Identified Research Gaps in IPv6-only Deployment Research

Research Gap	Key Supporting Literature	What Existing Studies Cover	Remaining Gap / Research Need
Limited Understanding of Large-Scale Enterprise IPv6-only Deployment	[20], [26], [27]	Existing studies provide deployment experiences, enterprise deployment	There is still a limited understanding of how large enterprises manage governance adaptation,

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

		guidelines, and IPv6-only testbed evaluations.	workforce development, operational transformation, risk management, and business continuity during long-term IPv6-only migration. Additional longitudinal enterprise-scale studies are needed.
Insufficient Evaluation of IPv6-only IoT and Edge Ecosystems	[28], [29]	Current research investigates IPv6 usage in smart-home environments and Internet-scale discovery of IPv6-enabled IoT deployments.	Comprehensive evaluation of industrial IoT, edge-computing platforms, heterogeneous device ecosystems, lifecycle management, and large-scale operational governance remains limited. More ecosystem-level studies are required.
Fragmented Security Assessment Across IPv6-only Environments	[6], [16], [30], [33]	Existing work examines IPv4aaS security, NAT-centric security assumptions, IPv6 scanning behavior, and protocol-specific vulnerabilities.	Security research remains fragmented across isolated domains. Future work should develop integrated security frameworks addressing monitoring, threat detection, incident response, operational visibility, and policy enforcement in IPv6-only environments.
Lack of Long-Term Operational and Performance Studies	[20], [21], [22], [23], [27]	These studies discuss IPv6-only networking experiences, deployment case studies, DNS-related operational issues, and IPv6-only testbed implementations.	Most available evidence is based on short-term deployments, experiments, or migration-focused evaluations. Longitudinal studies examining reliability, performance, operational overhead, and service continuity in mature IPv6-only environments remain scarce.

Limited Understanding of Large-Scale Enterprise IPv6-only Deployment

While numerous studies have evaluated IPv6 technologies and transition mechanisms, relatively few have examined long-term IPv6-only deployment within large enterprise environments. Most published work focuses on technical feasibility, protocol interoperability, or experimental testbeds rather than organizational deployment outcomes [20], [26], [27]. As a result, there remains limited understanding of how large organizations manage operational transformation, governance adaptation, workforce development, and business continuity during IPv6-only migration. Additional longitudinal studies are needed to evaluate enterprise-scale deployment experiences and identify best practices for sustainable adoption.

Insufficient Evaluation of IPv6-only IoT and Edge Ecosystems

IoT and edge-computing environments are frequently identified as major drivers of IPv6 adoption; however, empirical studies examining large-scale IPv6-only operation in these ecosystems remain limited. Existing research often focuses on protocol implementation, device behavior, or specific deployment scenarios rather than comprehensive ecosystem-level evaluation [28], [29].

Consequently, important questions related to interoperability, lifecycle management, operational

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

governance, and long-term scalability remain insufficiently explored. Future research should investigate how heterogeneous IoT ecosystems can be effectively managed within fully IPv6-only environments.

Fragmented Security Assessment Across IPv6-only Environments

Security research related to IPv6 remains fragmented across multiple domains, including protocol vulnerabilities, transition mechanisms, scanning behavior, and deployment-specific analyses [6], [16], [30], [33]. Although these studies provide valuable insights, there is a lack of integrated security frameworks capable of addressing the broader operational realities of IPv6-only networking.

Future work should focus on developing holistic security models that combine governance, monitoring, threat detection, policy enforcement, and operational visibility within large-scale IPv6-only environments.

Lack of Long-Term Operational and Performance Studies

Many existing evaluations are based on laboratory experiments, short-term deployments, or isolated case studies [20], [21], [22], [23], [27]. While such investigations provide important technical insights, they do not fully capture the operational challenges that emerge during sustained IPv6-only operation.

Longitudinal studies examining performance, reliability, operational overhead, and service continuity over extended periods are still relatively rare. Additional real-world deployment evidence is required to improve understanding of long-term IPv6-only sustainability.

C. Future Research Directions

The literature suggests that IPv6 research is gradually shifting from transition-oriented investigations toward understanding the operation of mature IPv6-only environments. While previous studies primarily focused on coexistence mechanisms and migration strategies, increasing deployment maturity indicates a growing need for research addressing long-term operational sustainability, service reliability, deployment governance, and post-migration management practices [22], [23], [27].

Future deployment environments are expected to be strongly influenced by the continued expansion of cloud-native infrastructures, IoT ecosystems, and edge-computing platforms. As these environments become increasingly distributed and interconnected, greater attention will be required to understand scalability, interoperability, lifecycle management, and operational governance challenges beyond traditional enterprise and service-provider networks [28], [29]. Emerging networking paradigms such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Segment Routing over IPv6 (SRv6) represent promising directions for future IPv6 research. These technologies provide new opportunities for network automation, traffic engineering, service orchestration, and operational flexibility within large-scale IPv6-only infrastructures [12], [19], [32]. Recent studies have also begun exploring the integration of artificial intelligence and machine-learning techniques with programmable IPv6 architectures to support intelligent traffic engineering, adaptive routing, and automated network optimization [32], [34]. However, their deployment implications, scalability characteristics, and operational readiness remain insufficiently explored.

Finally, security and operational visibility are expected to remain central research priorities as IPv6 adoption continues to expand. Recent studies demonstrate that challenges associated with monitoring, policy enforcement, threat detection, large-scale scanning behavior, and operational governance persist across IPv6-enabled environments [6], [30]–[33]. Consequently, future research should focus on integrated security frameworks that combine deployment management, operational visibility, continuous monitoring, and governance within sustainable IPv6-only operational ecosystems.

Conclusion

This survey demonstrated that the realization of IPv6-only networking depends on a combination of technological maturity, deployment readiness, and operational preparedness. Although IPv6 adoption has progressed substantially across modern Internet infrastructures, the transition toward sustainable IPv6-only operation remains influenced by application compatibility, enterprise readiness, interoperability requirements, and ecosystem-wide deployment conditions. The analysis showed that infrastructure platforms, cloud environments, and service-provider networks have achieved considerable progress in IPv6 deployment, whereas enterprise environments and large-scale IoT ecosystems continue to face operational and organizational challenges. Furthermore, global adoption trends reveal significant regional disparities, indicating that IPv6-only readiness remains uneven across different deployment contexts. The survey further reviewed the principal architectures enabling IPv6-only networking, including dual-stack, tunneling, translation-based approaches, IPv4-as-a-Service (IPv4aaS) solutions, and programmable IPv6 frameworks. While early transition mechanisms were instrumental in accelerating IPv6 adoption, contemporary deployment strategies increasingly favor IPv6-first operational models supported by selective interoperability mechanisms capable of maintaining communication with legacy IPv4 services.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

Several important research gaps were identified, including limited understanding of large-scale enterprise IPv6-only deployment, insufficient evaluation of IPv6-only IoT and edge ecosystems, fragmented security assessment across IPv6-only environments, and the lack of long-term operational and performance studies. Addressing these challenges will be essential for improving deployment confidence and supporting sustainable large-scale adoption.

Overall, the reviewed literature indicates that IPv6-only networking is becoming increasingly achievable from both technical and operational perspectives. Continued progress will depend on effective deployment governance, operational modernization, security visibility, interoperability management, and ecosystem-wide readiness capable of supporting sustainable IPv6-only operation at Internet scale.

References

1. Ladid L. 2026 Call for Final Action: Move to Native IPv6-Only. IEEE Netw. 2026 Mar;40(2):7-15. doi: 10.1109/MNET.2026.3654618.
2. Wu P, Cui Y, Wu J, Liu J, Metz C. Transition from IPv4 to IPv6: A State-of-the-Art Survey. IEEE Commun Surv Tutorials. 2013;15(3):1407-24. doi: 10.1109/SURV.2012.110112.00200.
3. Blancaflor E, Unciano CD, Arcigal EM, Contreras IJ, Abisado M. Towards the Increasing Usage of IPv6 & Its Implication: A Literature Review. In: Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence. New York (NY): ACM; 2024 Apr. p. 373-8. doi: 10.1145/3669754.3669811.
4. Al-hamadani ATH, Lencse G. Survey on the performance analysis of IPv6 transition technologies. Acta Tech Jaurinensis. 2021 May;14(2):186-211. doi: 10.14513/actatechjaur.00577.
5. D'yab O. A Comprehensive Survey on the Most Important IPv4aaS IPv6 Transition Technologies, their Implementations and Performance Analysis. Infocommun J. 2022;14(3):35-44. doi: 10.36244/ICJ.2022.3.5.
6. Olson K, Wampler J, Keller E. Doomed to Repeat with IPv6? Characterization of NAT-centric Security in SOHO Routers. ACM Comput Surv. 2023 Dec;55(14s):1-37. doi: 10.1145/3586007.
7. Fujimura S, Okumura M. IPv6 and Network Security Deployment Use Cases. In: Proceedings of the 2023 ACM SIGUCCS Annual Conference. New York (NY): ACM; 2023 Mar. p. 53-7. doi: 10.1145/3539811.3579580.
8. Thottungal Valapu S, Heidemann J. Towards a Non-Binary View of IPv6 Adoption. In: Proceedings of the 2025 ACM Internet Measurement Conference. New York (NY): ACM; 2025 Oct. p. 727-45. doi: 10.1145/3730567.3764467.
9. APNIC Labs. IPv6 Measurement Maps. APNIC Regional Data [Internet]. 2026 May 28 [cited 2026 Jun 15]. Available from: https://stats.labs.apnic.net/ipv6/
10. Google LLC. Google IPv6 Adoption Statistics Platform. Global Connectivity Telemetry Data [Internet]. 2026 May 28 [cited 2026 Jun 15]. Available from: https://www.google.com/intl/en/ipv6/statistics.html
11. Lencse G, Martinez JP, Howard L, Patterson R, Farrer I. Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS). RFC Editor; 2022 Oct. doi: 10.17487/RFC9313.
12. Ghumman S, Swain B, Sanjesh R, Venkateswara Reddy H, Venkadeshwaran K, Singh D. Scalable IPv6 Transition Mechanism for Future Internet Architecture. J Internet Serv Inf Secur. 2025 Aug;15(3):344-61. doi: 10.58346/JISIS.2025.I3.024.
13. Hamdou M, El Haloui M, El Ksimi A, Ettaki B. Classification of IPv6 Transition Mechanisms using Multiple-Criteria Decision-Making. Eng Technol Appl Sci Res. 2025 Jun;15(3):22960-8. doi: 10.48084/etasr.10222.
14. Al-Azzawi A, Lencse G. Methodology for the security analysis of IPv4-as-a-Service IPv6 transition technologies. Comput J. 2025 Oct;68(10):1450-62. doi: 10.1093/comjnl/bxaf048.
15. Abudaber T, Ahmed N. Implementation and Analysis of NAT and PAT Techniques in Cisco-Based Networks for Efficient IPv4. AlQalam J Med Appl Sci. 2026 Jan;:58. doi: 10.54361/ajmas.269111.
16. Sun C, et al. Efficient IPv6 address scanning based on hostname correlation in IPv6-only network. Sci Rep. 2026 Feb;16(1):8799. doi: 10.1038/s41598-026-39577-2.
17. ALgzite H, Ahmed N. IPv6 Addressing and Configuration: Building a Dual-Stack Network with OSPFv3. AlQalam J Med Appl Sci. 2025 Dec;:2974. doi: 10.54361/ajmas.2584129.
18. Wang T, Zhang S, Jiang J. Research on the application of DNS64/NAT64 technology in IPv6 environment in national network security. In: Proceedings of the 2025 International Conference on Big Data, Communication Technology and Computer Applications. New York (NY): ACM; 2025 Feb. p. 117-21. doi: 10.1145/3727505.3727526.
19. Parwitayasa W, Akbar SR, Basuki A. IPv4 Routing over IPv6 Routing Data Plane Using SRv6. In: Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology. New York (NY): ACM; 2023 Oct. p. 266-72. doi: 10.1145/3626641.3626934.
20. Robinson K, Zurawski J, Costello T. Designing, Constructing, and Operating an IPv6 Network at SC23: A case study in implementing the IPv6 protocol on a heterogenous network that supports the SC23 conference. In: Practice and Experience in Advanced Research Computing 2024: Human Powered Computing. New York (NY): ACM; 2024 Jul. p. 1-8. doi: 10.1145/3626203.3670531.
21. Arkko J, Keränen A. Experiences from an IPv6-Only Network. RFC Editor; 2012 Apr. doi: 10.17487/RFC6586.
22. Yamamoto M, Nakazato J, Tsukada M, Esaki H. Iterative Resolution with IPv6 Packets Failing. In: 2023 32nd International Conference on Computer Communications and Networks (ICCCN). IEEE; 2023 Jul. p. 1-2. doi: 10.1109/ICCCN58024.2023.10230170.
23. Fiebig T, Feldmann A. 'How I learned to stop worrying and love IPv6': Measuring the Internet's Readiness for DNS over IPv6. In: Proceedings of the 2025 ACM Internet Measurement Conference. New York (NY): ACM; 2025 Oct. p. 359-80. doi: 10.1145/3730567.3764439.

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*

24. Dekinder F, Vyncke E, Donnet B. Evaluating Dual-Stack Content Delivery Within Websites. In: Proceedings of the 20th International Conference on Emerging Networking Experiments and Technologies. New York (NY): ACM; 2024 Dec. p. 25-6. doi: 10.1145/3680121.3699886.
25. Fujimura S, Okumura M. Elevating Network Performance - Part II from IPv6 and Network Security Deployments. In: Proceedings of the 2025 ACM SIGUCCS Annual Conference. New York (NY): ACM; 2025 Apr. p. 5-8. doi: 10.1145/3675229.3712525.
26. Chittimaneni KK, Chown T, Howard L, Kuarsingh V, Pouffary Y, Vyncke É. Enterprise IPv6 Deployment Guidelines. RFC Editor; 2014 Oct. doi: 10.17487/RFC7381.
27. Costello T, Buraglio N, Fleming A, Tasker B, Siegel B. Improving transition to IPv6-only via RFC8925 and IPv4 DNS Interventions: A case study in implementing an IPv6-only testbed which informs IPv4-only clients why internet access is unavailable. In: SC24-W: Workshops of the International Conference for High Performance Computing, Networking, Storage and Analysis. IEEE; 2024 Nov. p. 785-92. doi: 10.1109/SCW63240.2024.00112.
28. Hu T, Dubois DJ, Choffnes D. IoT Bricks Over v6: Understanding IPv6 Usage in Smart Homes. In: Proceedings of the 2024 ACM on Internet Measurement Conference. New York, NY, USA: ACM; 2024. p. 595–611. doi:10.1145/3646547.3688457
29. Dahlmanns M, Heidenreich F, Lohmöller J, Pennekamp J, Wehrle K, Henze M. Unconsidered Installations: Discovering IoT Deployments in the IPv6 Internet. In: NOMS 2024-2024 IEEE Network Operations and Management Symposium. IEEE; 2024. p. 1–8. doi:10.1109/NOMS59830.2024.10574963
30. Zilberman A, Dvir A, Stulman A. IPv6 Routing Protocol for Low-Power and Lossy Networks Security Vulnerabilities and Mitigation Techniques: A Survey. ACM Comput Surv. 2025 Nov 30;57(11):1–77. doi:10.1145/3732776
31. Lencse G, Bazsó Á. Benchmarking methodology for IPv4aaS technologies: Comparison of the scalability of the Jool implementation of 464XLAT and MAP-T. Comput Commun. 2024 Apr;219:243–58. doi:10.1016/j.comcom.2024.03.007
32. Leiter Á, Böősy P, Bokor L. Enhancing Scalability in SRv6 Networks: A Novel Approach. IEEE Access. 2025;13:217176–85. doi:10.1109/ACCESS.2025.3645322
33. Tanveer H Bin, Chan E, Mok RKP, Kappes S, Richter P, Gasser O, et al. Unveiling IPv6 Scanning Dynamics: A Longitudinal Study Using Large Scale Proactive and Passive IPv6 Telescopes. Proceedings of the ACM on Networking. 2025 Sep 3;3(CoNEXT3):1–24. doi:10.1145/3749221
34. Wang P, Hu Y, Cui P, Bai L, Wang Y, Dong Y. SRv6-PPO Network Nodes Deployment Method. In: Proceedings of the 3rd International Conference on Signal Processing, Computer Networks and Communications. New York, NY, USA: ACM; 2024. p. 542–8. doi:10.1145/3712335.3712429

Copyright *Author (s) 2026. Distributed under Creative Commons CC-BY 4.0*
Received*: 10-04-2026 -* ***Accepted****: 09-06-2026 -* ***Published****: 15-06-2026*