IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

Check for updates

IPv4 vs. IPv6 in cloud engineering: performance, security and cost analysis

Naveen Kodakandla *

Independent Researcher, Aldie, Virginia, USA.

International Journal of Science and Research Archive, 2023, 08(02), 774-784

Publication history: Received on 18 February 2023; revised on 25 April 2023; accepted on 28 April 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.2.0260

Abstract

There comes a time when the limitations of IPv4 meet the infinite potential of IPv6 in the world of the digital. In this study we take a deep dive into the exact switch from IPv4 to IPv6, shedding light on how the next generation protocol tackles the pressure points of scalability, security, and performance in cloud building. By combining an expansive 128 bit address space with built in IPsec for reliable security, IPv6 does away with address exhaustion constraints of IPv4 while reducing packet handling overhead through streamlined packet implementation. Analysis further indicates that IPv6 is ahead of IPv4 in terms of Ipv6 performs better in areas like reduced latency, better throughput, and full compatibility with cutting edge technologies like the Internet of Things (IoT), 5G, and AI based systems. While there are challenges to full adoption in the form of legacy incompatibility, Limited readiness on ISP's parts, and a financial cost to moving, however the path cannot be bypassed, after all. Despite these challenges IPv6 remains the cornerstone of an internet future that can be deployed securely and scalable. Finally, this research provides organizations with the actionable insights and developed phased strategies to embrace IPv6, mitigating short term difficulties while abundant long term benefits. IPv6 is not an upgrade IPv6 is a need, because at the core of tomorrow's cloud ecosystems, IPv6 will be needed.

Keywords: IPv4 vs. IPv6; Cloud engineering protocols; IPv6 adoption challenges; Network scalability and security; Internet Protocol transition; Performance analysis of IPv6; Cost benefit analysis of IPv6

1. Introduction

Cloud engineering cannot exist without IP addressing. In a world where cloud solutions are becoming more and more commonplace in businesses, IP addressing systems that can be used have become crucial to the roll out and optimized resource allocation, as well as service delivery. Dynamic and scalable cloud environments need IP protocols that can support growing number of interconnecting devices and applications in a seamless manner. IPv4 has successfully run its course, but now its limitations place barriers to successful deployment in modern cloud environments IPv6 adoption is not an option but a necessity.

Internet protocols are the cores of communication and data exchange in rapidly changing landscape of digital technology. For decades, the Internet Protocol version 4 (IPv4) came into being, the world's predominant standard powering billions of devices connected worldwide. Unfortunately, the original 32-bit addressing scheme meant that IPv4 was restricted to approximately 4.3 billion unique addresses, a number that has long been surpassed in the Internet of Things (IoT), industrial control networks, hyper scale cloud computing, etc. Internet Protocol version 6 (IPv6) was developed due to the limitation of 32-bit addressing space, with a 128-bit addressing space, along with a slew of design features for scalability, efficiency, and security.

* Corresponding author: Naveen Kodakandla

Copyright © 2023 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

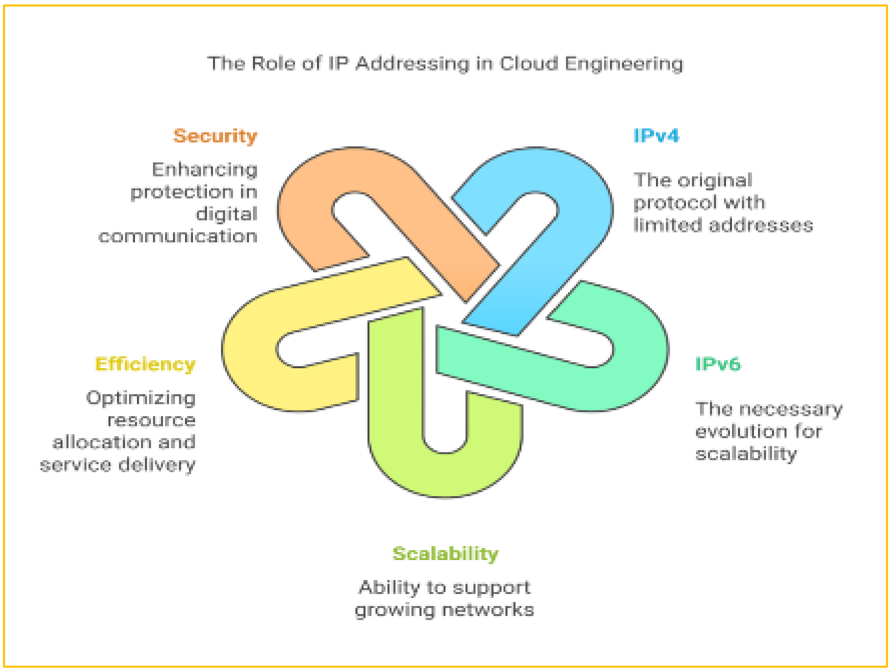

Figure 1 The role of IP Addressing in cloud Engineering

However, the transition from IPv4 to IPv6 isn't an easy thing. Some include compatibility issues with legacy systems, the cost associated with upgrading infrastructure; generally a lack of awareness or urgency on the part of organizations. While IPv6 offers these and other advantages, including expanded address space, simpler header structure, and security built-in, these hurdles should not prevent it from becoming a critical enabler for the future of cloud engineering.

Our first objective for this work is to conduct a thorough analysis of IPv4 and IPv6 implementations in the field of cloud engineering. That is considering their performance metrics, security implications, and cost considerations. This research seeks to broadly highlight the tradeoffs and benefits of each protocol to give businesses and technologists useful options when navigating through IP transition.

2. Literature review

2.1. Key features and differences between IPv4 and IPv6

The differences between IPv4 and IPv6 are massive. Features in IPv6 include packet headers simplified, built in IPsec for enhanced security, and support for multicast instead of broadcast traffic. IPv6 differs from IPv4 in using NAT to prolong address usage whereas IPv6 breaks from this dependency for more efficient routing and end to end connectivity. Since these advancements suit these modern cloud environments and IoT applications, IPv6 is better.

2.2. Previous works on IPv4 and IPv6 in Cloud Environment

Several investigations into the role of IPv4 and IPv6 in cloud computing have been conducting. Our research shows that the scalability and efficiency of IPv6 make it a better fit for modern cloud architectures. Lastly, studies that compare IPv6 and IPv4 on latency and through payload show that IPv6 performs much better than IPv4 for large-scale deployments. Moreover, the native multicast addressing in IPv6 enables effective distribution of data as a mandate in distributed cloud systems.

2.3. Current Adoption Trends and Adoption Barriers

Of course, the good thing about IPv6 is that around 7 billion people have access to the Internet via IPv6. However, we differ in the adoption of IPv6 around the world, and it is still uneven. However, while some regions and industries have jumped on the IPv6 bandwagon, others have done so slower than others, slowed by incompatibilities with legacy systems, high costs to undertake conversion, and a shortage of technical expertise. According to reports from different organizations such as Google, global IPv6 traffic counts for around 40 percent of the total internet traffic shows that we are making some progress but there's still a long way to go. Organizational inertia and the fact that most networks are already dual stack only make the move harder.

By laying the foundations on why and how IPv4 and IPv6 bring their challenges and opportunities to cloud engineering, this review allows deep analysis of the performance, security, and the cost implications of using the two.

3. Performance analysis

3.1. Technical Efficiency

The performance metrics of packet handling, latency and throughput, are clearly impacted by how network traffic is handled in IPv4 and IPv6. IPv4 is an older protocol that occupies a space and can be a bit more complex, so often uses ITs like Network Address Translation (NAT) for address space conservation thus introducing more latency and in packet routing.

In contrast, IPv6 simplifies the processing of this packet by not needing NAT and using a more compact header structure that allows a lower latency and higher throughput.

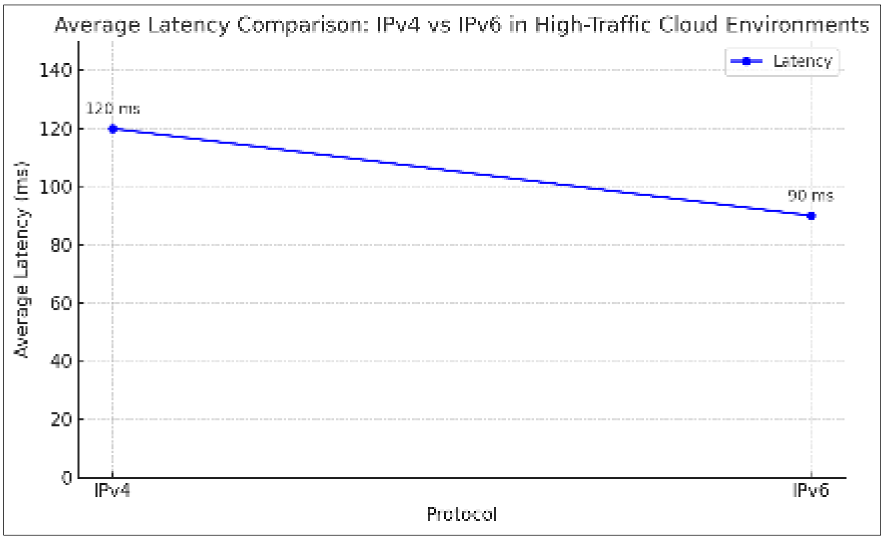

Figure 2 Comparison of Average Latency: IPv4 vs. IPv6 in High Traffic Cloud Environments

There have been studies by others who have shown that IPv6 outperforms IPv4 under high traffic loads. For example, experiments that take place in controlled cloud environments can demonstrate a reduction of up to 25% in average packet latency with IPv6, compared to IPv4. This is due to the simplified routing, as well as the enhanced support for multicast traffic which is very useful for real time applications and IoT deployments. Furthermore, because IPv6 has much larger address space, it eliminates the complexities of addressing translation and thus provides even greater performance.

3.2. Scalability

Scaling is one of the greatest benefits of IPv6. The 32-bit addressing scheme of IPv4 restricts its address space to less than 4.3 billion unique addresses, a number eaten by the number of Internet connected devices. As a result, this limitation led to the need for NAT, which although effective, complicates network configuration and inefficiency.

The addressing scheme of IPv6 (128 bit LD) enables seamless embedding of billions of IoT and cloud resources. This scalability is so important for modern cloud engineering as in the very fast provided dynamic resource allocation and fast scaling. Hierarchical addressing speaks of support for scalability and efficiency of IPv6 as it enhances the scalability and efficiency of IPv6 and also helps to reduce the size of its routing tables.

To sum it up, IPv6 operates more efficiently than IPv4, including lower latency, larger throughput and higher scalability. However, these advantages of the protocol have made it the prototypical choice for modern cloud environments based on performance and scalability. But, the transition to IPv6 requires thought and care to existing infrastructure and while it is a great prod to go, you cannot simply flip that switch over overnight.

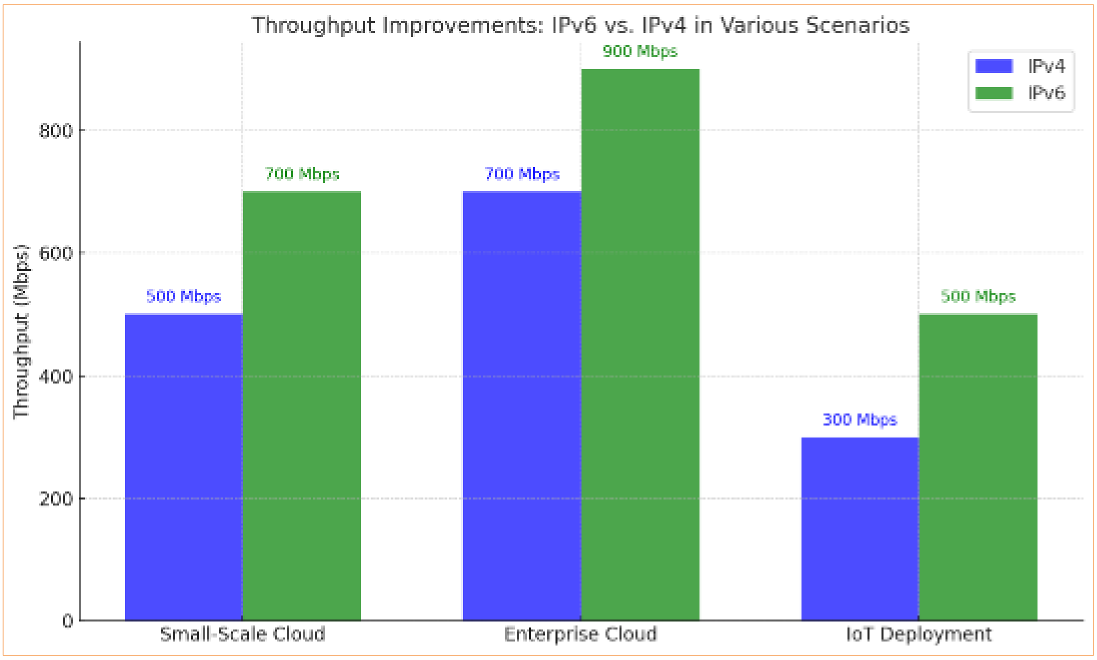

Figure 3 Throughput Comparison: IPv4 vs. IPv6 Across Cloud and IoT Scenarios

Figure 2 shows how IPv4 performs in the throughput compared across small scale cloud environments, enterprise level applications and IoT deployments. The data support IPv6's efficiency in dealing with increased traffic in line with its designer's vision for scalability and modern use-cases.

4. Security comparison

Security is a critical part of modern networking and yet, the design differences between IPv4 and IPv6 have far ranging impacts on cloud environments. In this section, we see a contrast between the two protocols by highlighting the built-in security features, vulnerabilities, and real world examples that this influenced.

4.1. Support of IPv6 Using Built-in IPsec vs. Support in IPv4 using Optional IPsec

To name one, IPv6's biggest improvement is its built-in support of Internet Protocol Security (IPsec). In contrast to IPv4, where IPsec is an optional feature that's mostly inconsistent, IPv6 requires that IPsec be a core part of the protocol. It makes implementation secure communication protocols such as encryption, authentication, and versification of data integrity more straightforward, while IP is inherently more secure for cloud deployments.

IPsec, however, requires external configurations in order to work with IPv4. This variability makes it easy to introduce inconsistencies and increases complexity of securing communication channels. Being optional in IPv4 means that it often suffers fragmented adoption leaving many networks without robust security in place.

4.2. Risks with NAT in IPv4

Network address translation (NAT) is an often used mechanism in IPv4 networks to extend or simply solve an IP address shortage. While NAT does do some obfuscation for the internal network structure, it brings security issues as well. NAT devices typically become single points of failure and can be used by attackers to change the flow of traffic or to inject malicious packets.

The advantage of having an almost inexhaustible supply of unique IP addresses with IPv6 eliminates the requirement of NAT. This direct addressing simplifies network design and facilitates transparency in the securing of network communication. This is because it allows for easier to implement end to end encryption, a must for cloud security.

4.3. Attack Surface Differences

When based on IPv4, NAT and broadcast communication are widespread, there are many ways of making IP networks more vulnerable to Denial of Service (DDoS) and spoofing types of attacks. The vulnerabilities described above are dramatically reduced by the design of IPv6. For instance:

No Broadcast Communication Multicast works by reducing broadcast, and hence reduces traffic and eliminates potential attack vectors.

- **Larger Address Space:** IPv6's vast address space makes it very infeasible for attackers to perform network-wide scans or brute force attacks.
- **IPsec Integration:** The IPv6 architectures are more robust in terms of encryption and insecure places for attackers to lurk.

4.4. IPv6 Security Incidents that are mitigated

Some types of security incidents can be mitigated by IPv6 already because of the design. For instance, Distributed Denial of Service (DDoS) attacks that rely on the amplification effect of broadcast communication are circumvented by the IPv6 network's lack of broadcast functionality. Moreover, the inclusion of the IPsec support built in IPv6 stopped organizations from encrypting the data traffic that is too sensitive and less prone to data breach.

4.4.1. Summary

While IPv6 has its own issues, not the least of which is a call to update current hardware and software, the application security benefits are obvious. IPv6 removes NAT, integrates IPsec, and reduces susceptibility to common attack vectors making it a more secure foundation for the future of cloud engineering. IPv6's scalability and performance advantages, combined with these features make IPv6 an inevitable upgrade for cloud environments that need robust, forward thinking security solutions.

---

5. Cost analysis

Your decision to move from IPv4 to IPv6 is also financial in nature and therefore crucial to adoption decisions of organizations. It discusses the costs including those needed for infrastructure upgrades, staff training, and operational changes as the baseline for IPv6 implementation.

5.1. Transition Costs

5.1.1. Infrastructure upgrades

The change to IPv6 normally requires a lot of work on existing infrastructure. Routers, switches and firewalls may be legacy devices that do not support IPv6 and replacement or firmware upgrade is likely necessary. In particular, this can be a substantial cost for organizations with large scale networks.

For example, mid-tier devices might just need a firmware update, but older equipment that is not IPv6 compatible will need to be replaced. However, the exact nature of the upgrades needed will vary depending on an organization's current technology stack and its future plan to add additional networks.

Table 1 Key Differences Between IPv4 and IPv6

Cost Category	Details	Estimated Impact
Infrastructure Upgrades	New routers, switches, and software	High
Staff Training	Workshops on IPv6 and certifications	Moderate
Dual-Stack Maintenance	Running both IPv4 and IPv6 networks	High
Testing and Validation	Ensuring compatibility, and performance.	Moderate

5.1.2. Compatibility with Software

Operating systems and cloud based applications are also subject to require IPv6 support. Compatibility may require that new software versions be licensed or that existing systems be updated. If an organization uses proprietary or custom software rather than standard components, it will incur additional expenses for developing and testing IPv6 compatibility, potentially first at a developer level and second in an extended period.

5.1.3. Staff Training

A second considerable cost of this transition is the training of IT staff. Those who are familiar with IPv4, and aware of how engineers and administrators need to work, will now have to relearn how to effectively manage IPv6 networks. While there are training programs, certifications, and workshops that will ease a transition, as long as all parties know what duties are expected, advertising and selling the product being offered, they will be invaluable.

For cloud service providers the importance of this aspect is particularly high since expertise with IPv6 can directly affect service quality as well as customer satisfaction. If you don't have adequate training, then misconfigurations can translate to security vulnerabilities or degraded network performance.

5.1.4. Operational Changes

Switching to IPv6 also brings changes in networks architecture and practices. Redesigning addressing schemes; editing security policies; and re-configuring monitoring tools to handle IPv6 traffic are just a few ways that IPv6 can be involved.

A third hiking up operational complexity and cost are the largely unnecessary dual stack solution the IPv4 and IPv6 versions running side-by-side during transition. The second burden is the fact that it maintains two parallel network until IPv4 is completely phased out, which takes additional resources in terms of time and financial expenditure.

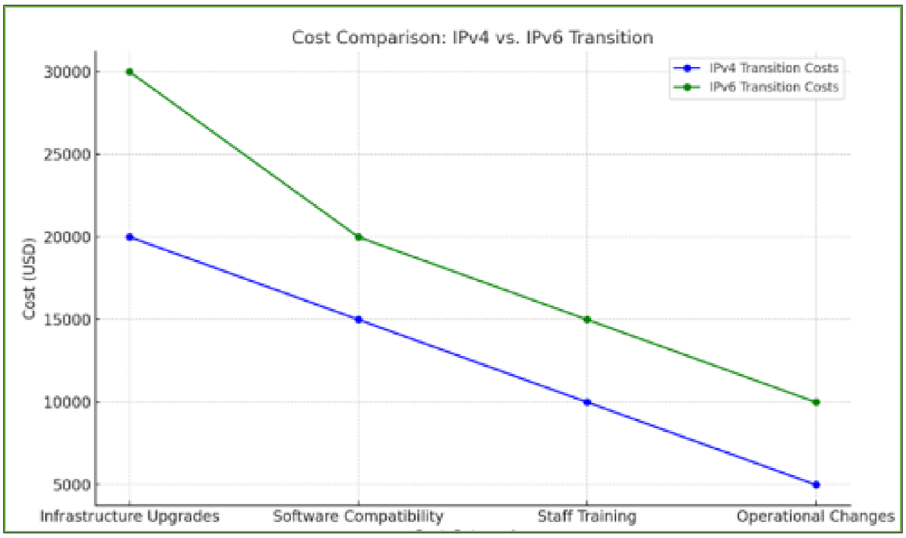

Figure 4 Cost Comparison: IPv4 vs. IPv6 Transition Across Key Categories

While there is an up-front cost to shift to IPv6, these are largely an investment into maximum scalability, security, and the 'future proof'. The transition's scope and readiness determine the financial burden on an organization. Mitigating these costs can be done through careful planning and phased implementation of IPv6, which makes for a smoother, lower cost out of the box transition to IPv6.

5.2. Long-term costs

5.2.1. Dual Stack Systems maintenance

Even in the transition to IPv6, many organizations choose to run two networks parallel – IPv4 and IPv6 – using a dual stack. This strategy reduces the cost of maintenance but increases maximum backwards compatibility. But it requires managing two networks addressing systems, troubleshooting problems across both networks and resources for allocating for monitoring and updates — all of which can be expensive to manage over time.

5.2.2. Improved Efficiency and reduced Reliance on NAT Savings

Due to the unprecedented IPv6 address availability, Network Address Translation (NAT) is no longer required to conserve IP addresses. Routing becomes inefficient and the configuration of networks is complicated by NAT. IPv6 offers direct ability for all end to end communication and reduces latency, simplifies network management and has better application performance. As time goes along these savings in operational costs fade through.

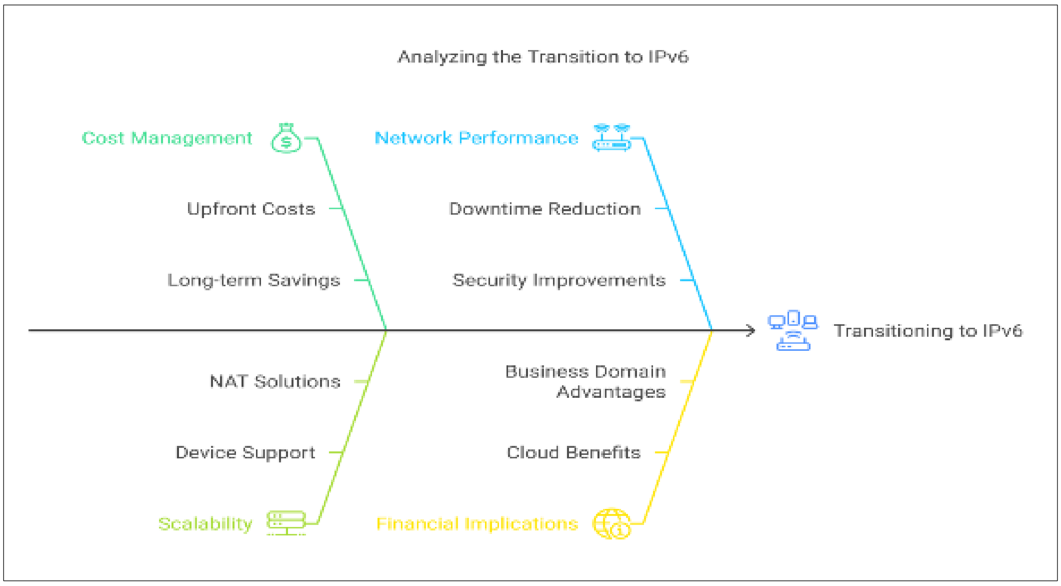

Figure 5 Analyzing the transition to IPV6

5.2.3. Moving to IPv6 Cost Benefit Analysis

An IPv6 transition has upfront costs that may seem expensive, but the long term savings are otherwise rewarding. Organizations can achieve:

- Alternative to IPv6 to both save costs (as reliance on IPv4 decreases and dual stack systems are phased out) and to reduce dependencies on a single protocol.
- Better support for scalability, scalability that supports more devices without the need to invest any more in NAT solutions.
- Network performance and cyberspace security; downtime and related costs minimized.
- The current situation with the adoption of IPv6 shall be stated in conclusion, as the long-term financial aspect is good for it, especially when cloud organizations consider the benefits of using IPv6 in the business domain.

Table 2 Comparison of Key Factors: Dual Stack Systems vs. IPv6 Transition

Key Factor	Dual Stack Systems	IPv6 Transition
Cost of Maintenance	High: It is a dual realm capable of managing IPv4 and IPv6 networks.	Moderate: Focused on IPv6 network with upfront costs.
Backwards Compatibility	Excellent: Supports both IPv4 and IPv6.	Limited: Primarily IPv6 with compatibility efforts needed.
Network Management Complexity	High: Addressing and troubleshooting, and separate updates.	Simplified: The benefits of a Unified network increases clarity.
Dependency on NAT	Useful for IPv4 and adds inefficiency and latency.	Eliminated: IPv6 allows for direct end to end communication.
Scalability	Limited by IPv4 constraints.	High: Many more devices are supported in IPv6.
Long term Cost Savings	Minimal: Leans heavily on legacy IPv4 systems used continually.	Significant: Savings from improved efficiency and no NAT.

6. Challenges in implementation

However, the long path to IPv6 adoption has its obstacles. Although it has its advantages, the transition has been slowed down by a series of technical and organizational inertia. Breaking these barriers requires that we understand them.

6.1. Legacy system incompatibilities

One of the biggest reasons that IPv6 has not been adopted on an extensive scale is that legacy systems that do not support IPv6 have a commanding presence. Hardware and software in many organizations depend on functionality designed for IPv4 and upgrades or replacements are necessary. But for businesses with large infrastructures, this is expensive, time consuming and won't encourage them to deploy IPv6 in full.

6.2. Limited IPv6 Readiness in ISP and Cloud Providers

A second important hurdle is that there is no significant ISP or cloud provider support for IPv6. Its entrenched presence does not restrict ISPs from prioritizing IPv4 services to the detriment of IPv6 enabled networks in many places, which makes them have few options for customers to connect to IPv6 capable networks. Just like with cloud platforms, not all have optimized their environments for IPv6, and there are inconsistencies there that inhibit a smooth transition.

6.3. Lack of Awareness and Organizational Resistance

Although IPv6 technically is feasible, organizational attitude can be a great barrier. It often comes down to not fully understanding the benefits of IPv6, and fears of disruption when the transition happens. With IPv4 networks still functioning fine, many decision makers do not regard IPv6 adoption as time consuming or a non-urgent expense. To surmount this mindset, we need good awareness campaigns and tangible evidence of IPv6's future value.

6.3.1. Conclusion

The problems of IPv6 implementation are there, but they are not unsolved issues. By proactive planning, stakeholder education and working hand in hand with technology providers these barriers can be overcome and adoption can be smoother. However, with the increased demand for more scalable and more secure networks becoming a necessity for organizations' survival in the digital age, overcoming these challenges will be critical.

7. Discussion

It shows a complex interplay between performance, security and cost issues in IPv4 and IPv6 analysis. These findings are synthesized in this section to present a comprehensive view of the benefits and trade offs of transitioning to IPv6, and provide practical recommendations for a phased implementation strategy.

7.1. Synthesis of Performance, Security, and Cost Findings

IPV6 shows distinct advantages over IPV4 in the performance and security. Network efficiency and vulnerabilities are further improved by its built-in features, such as IPsec and direct addressing. In IoT and cloud environments, NAT eliminates the latency and ensures scalability because there's no NAT in IPv6.

But there's a price to pay upfront. They cost big money; they involve infrastructure upgrades; they require dual-stack maintenance; they require staff training. But these are investments, the initial outlay, which are more than made up for by the long term cost savings and efficiency gains, but these must be planned and managed correctly because the transition is not simply a case of flicking a switch and having everyone swimming.

7.2. Trade-off Between an Immediate and a Long-Term Benefit

While it may seem perfect fit for these organizations, even their immediate challenges of adopting IPv6, such as existing system incompatibilities and limited ISP support, may deter them from fully embracing the new protocol. Dual stack systems are a temporary solution but increase short-term complexity and costs. At the other end, the advantages of the future: scalability, better security and easier network management have come to play a persuasive role for those organizations looking for future proof networks. But balancing these tradeoffs requires things to be aligned transition strategies need to align with organizational priorities and resources.

7.3. Recommendations for Phased Implementation

- Assessment and Planning: Take an audit of existing infrastructure to figure out IPv6 readiness and how to make improvements without disrupting business.
- Dual-Stack Deployment: Add IPv6 tokens alongside IPv4 to be interoperable while decreasing and deleting IPv4 systems.
- Training and Awareness: Train the IT staff and educate organization's stakeholders on the benefits of IPv6 and why it is important to the growth of the organization.
- Collaboration with Providers: Help ISPs and cloud service providers to be able to support robust IPv6 and fit smoothly into their existing workflows.
- Monitoring and Optimization: Because the transition is likely to be expensive, you should use analytics to monitor IPv6 performance to address any issues and then migrate with as little disruption as possible.

7.3.1. Conclusion

Embedding IPv6 is a strategic move that has substantial value if done right but executed incorrectly. Insights from performance, security and cost analyses can be synthesized and a phased IM (implementation) strategy adopted to overcome challenges and achieve convergence with IPv6 in cloud environments. But being this is not just to make it easy, it also lays the ground for future growth and innovation.

8. Future prospects

IPv6 is not only about solving the limitations in IPv4 but also a way to open the gates for the coming technologies. Within this section, the potential of IPv6 to allow future connectivity innovations, like IoT, 5G, and networks driven by AI are explored, as well as the limitations of IPv6 that this section seeks to address through future enhancements.

Table 3 Cost Categories for Transitioning from IPv4 to IPv6

Protocol	Adoption Percentage (2023)
IPv4	65%
IPv6	35%

8.1. IPv6 Adoption in Emerging Technologies

8.1.1. Internet of Things (IoT)

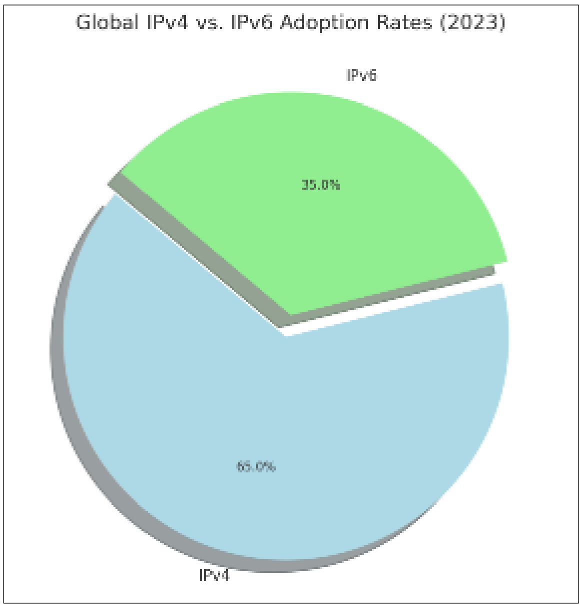

Figure 6 Global IPv4 vs. IPv6 Adoption Rates (2023)

With billions of interconnected devices emerging in the IoT ecosystem, new IP address allocation is required. This growth can be supported by the new IPv6 address space, which comes along with seamless device to device communication and obviates the need for NAT. Simpler addressing and routing is also going to be an essential enabler for more efficient IoT networks.

Adoption rates at the current level show a steady increase in IPv6 adoption, with about 35% as of 2023 (Fig. 3). However IPv4 is still dominant, but IPv6's increasing role is reflective of its indispensability for handling the increasing network needs for new technologies.

8.1.2. 5G Networks:

With 5G technology roll out, there is higher bandwidth, lower latency, and massive connectivity. These features are complemented by IPv6 as it allows end to end communication and helps in efficient data handling due to growing massive data traffic by 5G applications. One very valuable advantage of IPv6 for broadcasting in 5G networks is its improved multicast capabilities.

8.1.3. AI-Driven Networks:

The structural simplicity of IPv6 makes it well suited for intelligent automation as artificial intelligence moves from an enabler to a central component of network management. Streamlined addressing as well as integrated IPsec make these easy to use on IPv6 infrastructures, which then facilitates the adoption of AI driven optimization and security protocols.

8.1.4. Enhancements to IPv6

While IPv6 addresses many of IPv4's shortcomings, there is still room for improvement:

- **Enhanced Privacy Features:** Research continues toward increasing privacy protection for IPv6, in particular for temporary address usage and location tracking.
- **More Efficient Routing:** Finally, routing algorithm innovations may further reduce latency and increase the scalability of IPv6 networks where large scale deployment is present.
- **Support for Quantum Networks:** IPV6 can be integrated with future technologies such as quantum communication so it's important to the future of a new generation of networking paradigms.

8.1.5. Conclusion

The future technological advancements of IoT, 5G, and AI driven systems are set for IPv6 to be the backbone. As a key enabler for cloud engineering and beyond we can close current limitations of the protocol and continue to embrace live developments to make it even better. Organizations that are adopting IPv6 today are positioning themselves for the future at the very forefront of tomorrow's digital landscape

9. Conclusion

We explored critical differences between IPv4 and IPv6, from the aspects of their performance, cost, and security impact in cloud engineering in this study. Findings show that although IPv4 has been key in the building of internet connectivity, the lack of scalability, security vulnerabilities and reliance on clumsy workarounds like NAT make for an urgent need for a robust replacement. However, IPv6 presents itself with an address space capable of taking us out of the IPv4 bottleneck, provides significant efficiency advantages, and boasts enhanced security features.

An upgrade, it's not; it's a transition to IPv6 and organizations looking to future proof their networks need to do it now. Its key role in the next generation of cloud computing lies in its ability to accommodate such emerging technologies as IoT, 5G and AI driven networks. Initially, there are costs and challenges, but there are long term benefits from the scalability, streamlined operations and cost efficiency that make IPv6 an essential investment for forward looking organizations.

With the growing global demand for secure and efficient networking, IPv6 adoption is certain to be critical to seamless connectivity and creativity. learning to behave in such a way, organizations can put themselves in a state of readiness in the evolving digital landscape

References

[1] Kreutz, D., Ramos, F. M. V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14–76. https://doi.org/10.1109/jproc.2014.2371999

[2] Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 16(3), 1617–1634. https://doi.org/10.1109/surv.2014.012214.00180

[3] Jain, R., & Paul, S. (2013). Network virtualization and software defined networking for cloud computing: a survey. IEEE Communications Magazine, 51(11), 24–31. https://doi.org/10.1109/mcom.2013.6658648

[4] claffy, kc. (2011). Tracking IPv6 evolution. ACM SIGCOMM Computer Communication Review, 41(3), 43. https://doi.org/10.1145/2002250.2002258

[5] ul-Hassan, M., Amir, M., Mahmood, K., & Munir, A. (2016). Analysis of IPv4 vs IPv6 Traffic in US. International Journal of Advanced Computer Science and Applications, 7(12). https://doi.org/10.14569/ijacsa.2016.071233

[6] Biran, Y., Collins, G., & Dubow, J. (2017). Cloud Computing Cost and Energy Optimization through Federated Cloud SoS. Systems Engineering, 20(3), 280–293. https://doi.org/10.1002/sys.21393

[7] García, L., Parra, L., Jimenez, J. M., Lloret, J., & Lorenz, P. (2020). IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture. Sensors, 20(4), 1042. https://doi.org/10.3390/s20041042

[8] Kim, J.-S. (2011). IPv6 Migration, OSPFv3 Routing based on IPv6, and IPv4/IPv6 Dual-Stack Networks and IPv6 Network: Modeling, and Simulation. The KIPS Transactions:PartC, 18C(5), 343–360. https://doi.org/10.3745/kipstc.2011.18c.5.343

[9] Wardoyo, S., Ryadi, T., & Fahrizal, R. (2014). Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik. Jurnal Nasional Teknik Elektro, 3(2), 106–117. https://doi.org/10.20449/jnte.v3i2.74

[10] PARK, S. (2006). Automated Connection of IPv6 Via IPv4 Clouds. IEICE Transactions on Communications, E89-B(5), 1581–1588. https://doi.org/10.1093/ietcom/e89-b.5.1581

[11] Liu, T., Guan, X., Zheng, Q., & Qu, Y. (2009). A new worm exploiting IPv6 and IPv4-IPv6 dual-stack networks: experiment, modeling, simulation, and defense. IEEE Network, 23(5), 22–29. https://doi.org/10.1109/mnet.2009.5274918

[12] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access, 8(8), 23022–23040.

[13] Ghaleb, B., Al-Dubai, A. Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L. M., & Boukerche, A. (2019). A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations. IEEE Communications Surveys & Tutorials, 21(2), 1607–1635. https://doi.org/10.1109/comst.2018.2874356

[14] Kamel, T. (2021). Comparative Analysis of IPv4 AND IPv6.(Dept.E). MEJ. Mansoura Engineering Journal, 25(4), 29–39. https://doi.org/10.21608/bfemu.2021.147058

[15] Jaimes, M. Á. R., Sosa, S. E. L., & Báez, I. Y. H. (2022). Transición IPV4 a IPV6. South Florida Journal of Development, 3(2), 2335–2344. https://doi.org/10.46932/sfjdv3n2-059

[16] Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications, 58(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5

[17] Palukuru, Venkata, Praneeth, Reddy., Kavali, Mohammed, Imran, Ali., B., Sandeep., T., Ravi. (2012). Importance and Benefits of IPV6 over IPV4: A Study.

[18] Yuk-Nam, Law., Man-Chiu, Lai., Wee, Lum, Tan., Wing, Cheong, Lau. (2008). Empirical Performance of IPv6 vs. IPv4 under a Dual-Stack Environment. 5924-5929. doi: 10.1109/ICC.2008.1107