IPv6 Security:

Enhancements, New Challenges, and Adoption Barriers

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

IT 315 – Introduction to Networking and Security

November 2, 2025

Instructions:

Pick a topic related to Networking and Security and write a two-page paper on your topic with a references page in APA format.

IPv6 Security: Enhancements, New Challenges, and Adoption Barriers

In late 1998, with a "security in mind" approach, the Internet Engineering Task Force (IETF) developed IPv6 as a successor to IPv4 (FCC, 2016; Internet Society, 2025; Kane, 2025). There were many issues with IPv4; however, the two most concerning problems were IPv4's address space limitations and security vulnerabilities. As a result, engineers improved upon IPv4 with IPv6, which features numerous security enhancements to address IPv4's limitations.

Address Space Expansion

IPv6's 128-bit address space provides approximately 340 undecillion unique addresses, compared to IPv4's 4.3 billion (Panko, 2020). The massive address pool helps mitigate network scanning attacks from hackers and eliminates the need for Network Address Translation (NAT). While NAT provided "security by obscurity" in IPv4 networks, it also compromised end-to-end security connectivity between hosts and devices when addresses changed between private and public statuses. However, with IPv6, hosts and devices are directly addressable from both internal networks and the internet. Unfortunately, due to increased exposure to the world and susceptibility to direct attacks, IPv6 networks require greater attention, care, and stronger firewall configurations (Kane, 2025).

Integrated IPsec

Second, one of the most notable features of IPv6 is IPsec (IP Security) (Weissman, 2022; Kane, 2025). IPsec provides end-to-end encryption between hosts and devices. While IPsec was an optional add-on feature for IPv4, it is a core and seamless security feature for IPv6 (via Extension Headers). As Kane notes, studies have shown IPv6 networks reduce man-in-the-middle attacks by 40% and spoofing incidents by 62% compared to IPv4 (2025).

Protocol Improvements

Third, IPv6 replaces IPv4's Address Resolution Protocol (ARP) with Neighbor Discovery Protocol (NDP). Replacing ARP with NDP mitigates ARP spoofing and man-in-the-middle attacks (Weissman, 2022). Additionally, IPv6 Privacy Extensions allow hosts and devices to periodically rotate their public addresses, making user tracking more difficult. Lastly, Stateless Address Autoconfiguration (SLAAC) enables hosts and devices to automatically configure their own IP addresses without the need for separate DHCP servers. Although IoT devices greatly benefit from SLAAC, the automation introduces other risks and attack vectors, such as rogue Router Advertisement attacks (Frankel et al., 2010).

Adoption Barriers

Despite the numerous benefits of IPv6 over IPv4, organizations remain hesitant to migrate to IPv6 for several reasons. First, IPv4 resilience technologies like NAT and CIDR have effectively extended IPv4's lifespan, removing the incentives and sense of urgency for migrating to IPv6. Second, as Kane states, the average enterprise incurs $2.4 million in transition costs, with hardware upgrades alone costing between $200,000 and $1 million per data center (2025). Third, migration timelines can span 5-7 years for large organizations, forcing engineers to implement dual-stack networks for the duration of the transition, thereby increasing network complexity and potential attack vectors. Lastly, without any immediate business needs for IPv6-only technologies, many organizations view the technological migration as a high-cost/low-reward task with 3-5 year ROI timelines (Kane, 2025).

Conclusion

While IPv6 offers numerous cybersecurity features and improvements over IPv4, its adoption remains challenging due to the significant short-term financial investment and lengthy implementation timelines. However, as IoT, 5G, and smart cities continue to grow, IPv6 will become a necessity rather than a choice. Therefore, it is best to migrate from IPv4 to IPv6 as early as possible to future-ready organizational networks.

References

Cisco. (2025, July 24). *What is IPv6?* Retrieved from https://www.cisco.com/site/us/en/learn/topics/networking/what-is-ipv6.html

FCC (Federal Communications Commission). (2016). *Internet Protocol Version 6 (IPv6) for Consumers*. Retrieved from https://www.fcc.gov/consumers/guides/internet-protocol-version-6-ipv6-consumers

Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). Guidelines for the secure deployment of IPv6 (NIST Special Publication 800-119). National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028 /NIST.SP.800-119

Internet Society. (2025, August 8). *IPv6*. Deploy360. Retrieved from https://www.internetsociety.org/deploy360/ipv6/

Kane, A. (2025). Navigating the Transition: Challenges and Benefits of Shifting from IPv4 to IPv6 in a Rapidly Evolving Internet Landscape. *International Journal of Internet and Distributed Systems*, 7(2), 21-34. https://doi.org/10.4236/ijids.2025.72002

Panko, R. R., & Panko, J. L. (2020, Chapter 2). Business data networks and security (11th ed.). Pearson.

Weissman, J. S. (2022, May 18). *The time is still now for IPv6*. American Registry for Internet Numbers (ARIN). https://www.arin.net/blog/2022/05/18/time-still-now-ipv6/