IPv6 Cybersecurity Enhancements

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity

September 28, 2025

Instructions:

Internet Protocol Version 6 (IPv6) was designed to address the limitations of Version 4 (IPv4).

- What cybersecurity-related enhancements have been incorporated into IPv6?
- The adoption of IPv6 has been pretty slow across both the public and private sectors.
    - What reasons can you attribute to this?

Cite resources and references that support your assertions.

IPv6 Cybersecurity Enhancements

IPv6 was developed by the Internet Engineering Task Force (IETF) in December 1998 to replace IPv4 because of the growing number of internet users and connected devices. With a "security in mind" approach, they implemented many improvements in IPv6 to addresses the insufficiencies of IPv4 (Cisco, 2025; Internet Society, 2025). The most notable addition is IPsec support. IPsec is important because it provides end-to-end security using authentication, integrity protection, and confidentiality to IP packets. For IPv6, IPsec is a native, integrated, and built-in feature; however, for IPv4, users had to manually install and configure it for their networks as an extra feature on top of other layered security protocols.

A second significant improvement is the larger address space for internet users and connecting devices (Weissman, 2022; GeeksforGeeks, 2025). IPv4's address space cannot meet global IP demands due to its 32-bit address length (allowing approximately 4.3 billion unique addresses); however, IPv6 addresses are greater in length (128-bit long) and written in hexadecimal notation, offering plenty of room for growth to meet the demand of growing devices connecting to the internet. The additional address scope in IPv6 also makes it much harder for attackers to exploit network discovery operations, such as port scans. The Neighbor Discovery Protocol (NDP) replaces IPv4's Address Resolution Protocol (ARP), thereby mitigating ARP spoofing attacks and man-in-the-middle attacks on networks. Lastly, IPv6 offers multiple privacy extensions to periodically rotate a device's address, making it more challenging to track a user over extended periods.

Lastly, Stateless Address Autoconfiguration (SLAAC) is an important feature of IPv6 because it enables devices to automatically configure and assign their own IP addresses without requiring a DHCP server or other third-party assistance. It is a significant step forward for network

management, particularly for large-scale networks that utilize IoT devices in conjunction with Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs). With IPv6's simplified header formats and improved routing efficiencies, IT administrators can better manage industrial networks and machine control devices (i.e., reviewing log histories and promptly pushing firmware updates instead of waiting months or years) from remote regions of the world without the need for direct access to those remote devices.

Reasons for Slow Adoption

Despite the numerous benefits of adopting and upgrading to IPv6, organizations remain hesitant and slow to do so, for several reasons (Federal Communications Commission, 2016; Weissman, 2022; GeeksforGeeks, 2025).

1. **IPv4 Resilience:** Technologies (i.e., Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR)) continue to support IPv4, compensating for some of IPv4's inefficiencies and security weaknesses. Such technologies have turned into "crutches" for many organizations, staving off the looming IPv6 migration.
2. **Cost and Complexity:** The shift would be expensive because it requires huge investments in upgrading hardware, migrating software, and training personnel to use the new technologies.
3. **Backward Compatibility:** IPv4 and IPv6 are not inherently interchangeable or compatible, forcing organizations to "dual stack" (run both protocols in parallel). The additional processing may create more burdens for IT teams and network management, as new security vulnerabilities, attack vectors, and costs may emerge for organizations.

4. **No Urgency:** Many organizations and end-users do not perceive the urgency to migrate from IPv4 to IPv6, as IPv4 continues to function sufficiently for their current individual and operational needs. A proverbial "kicking the can down the road" situation.

References

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

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

GeeksforGeeks. (2025, August 11). Differences between IPv4 and IPv6. https://www.geeksforgeeks.org/computer-networks/differences-between-ipv4-and-ipv6/

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

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/