Using IPv6 – Drink Responsibly

Santosh Pandit, London, 2 May 2025

Important disclaimer: The views expressed in this article are solely my own and do not necessarily reflect those of my employer. Any errors are my responsibility.

The Hacking Problem

Sophisticated cybercriminals are exploiting IPv6 features, such as Stateless Address Autoconfiguration (SLAAC)[1] to hack Android phones[2]. Researchers have identified SLAAC-spoofing[3] as one of the techniques used in these attacks.

The Incompatible Guidance Problem

The NSA's IPv6 Security Guidance[4] provides valuable insights but advises against using Network Address Translation (NAT) for IPv6. My business use case relies on NAT66, so following the NSA's recommendation without adjustment isn't practical.

Some guidance suggests disabling IPv6 entirely. I consider this an oversimplified approach and disagree with it. Instead, I support DigiCert's view that "IPv6 is still the future"[5] and the secure implementation recommendations from Dutch authorities.[6]

My Multi Layered Solution

With attacks on mobile devices increasing[7] and cybercriminals' tactics evolving, it's critical to build a robust and sustainable technology stack. Here's my approach:

Upstream:

- Enable both IPv4 and IPv6.
- Ensure Resource Public Key Infrastructure (RPKI) route origin authorisation is in place and valid for the server's prefixes.
- Confirm the use of DHCPv6-shield at Layer 2 to block rogue DHCPv6 servers.

Server:

- Use statically assigned IPv4 and IPv6 addresses.
- Implement "RA-guard" as per RFC 7113 or disable Router Advertisements (RA) to prevent SLAAC-spoofing.

[1] Attribution: (Ravi Lakshmanan / HackerNews): https://thehackernews.com/2025/04/chinese-hackers-abuse-ipv6-slaac-for.html

[2] Other devices could be vulnerable too and I have included references so that you can carry out your own research.

[3] Attribution (Facundo Munoz / ESET research): https://www.welivesecurity.com/en/eset-research/thewizards-apt-group-slaac-spoofing-adversary-in-the-middle-attacks/

[4] Attribution (NSA): https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/1/CSI_IPv6_security_guidance_.PDF

[5] Attribution (DNS Made Easy / Digicert): https://dnsmadeeasy.com/resources/the-state-of-ipv6-adoption-in-2025-progress-pitfalls-and-pathways-forward

[6] Attribution (SIDN.nl / internet.nl): https://www.sidn.nl/en/modern-internet-standards/ipv6

[7] Attribution (Kaspersky): https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023

- Ensure all DNS resolution is handled by the server’s own recursive DNS resolver, supporting both IPv4 and IPv6, with strict DNSSEC validation.
- Implement NAT66 by forwarding traffic from the external interface (e.g., ens3) to the internal interface (e.g., wg0) and masquerading both IPv4 and IPv6 traffic.

Client:

- I find iOS devices easier to manage and prefer them over Android for security reasons.
- Allocate random internal IPv6 addresses to each client to improve privacy.
- Ideally, use a kill switch for the VPN and ensure DNS resolution is managed within the VPN.
- If VPN use isn’t possible (or if split tunnelling is enabled), ensure DNS resolution is handled by a trusted resolver, preferably using DNS over HTTPS (DoH) or DNS over TLS (DoT).

I’m confident this approach enables secure IPv6 usage and addresses recently identified sophisticated threats. I’d welcome any alternative solutions or suggestions you might have.

I would like to end with a personal note. My mother is 81 year old and I am worried. Not because of her age but as she uses an android phone. 😊 Do you think, I should buy her an iPhone for her next birthday?

Love to my readers.

Santosh Pandit