

Notes from a Large Enterprise on IPv6 Adoption

June 2019

The Why

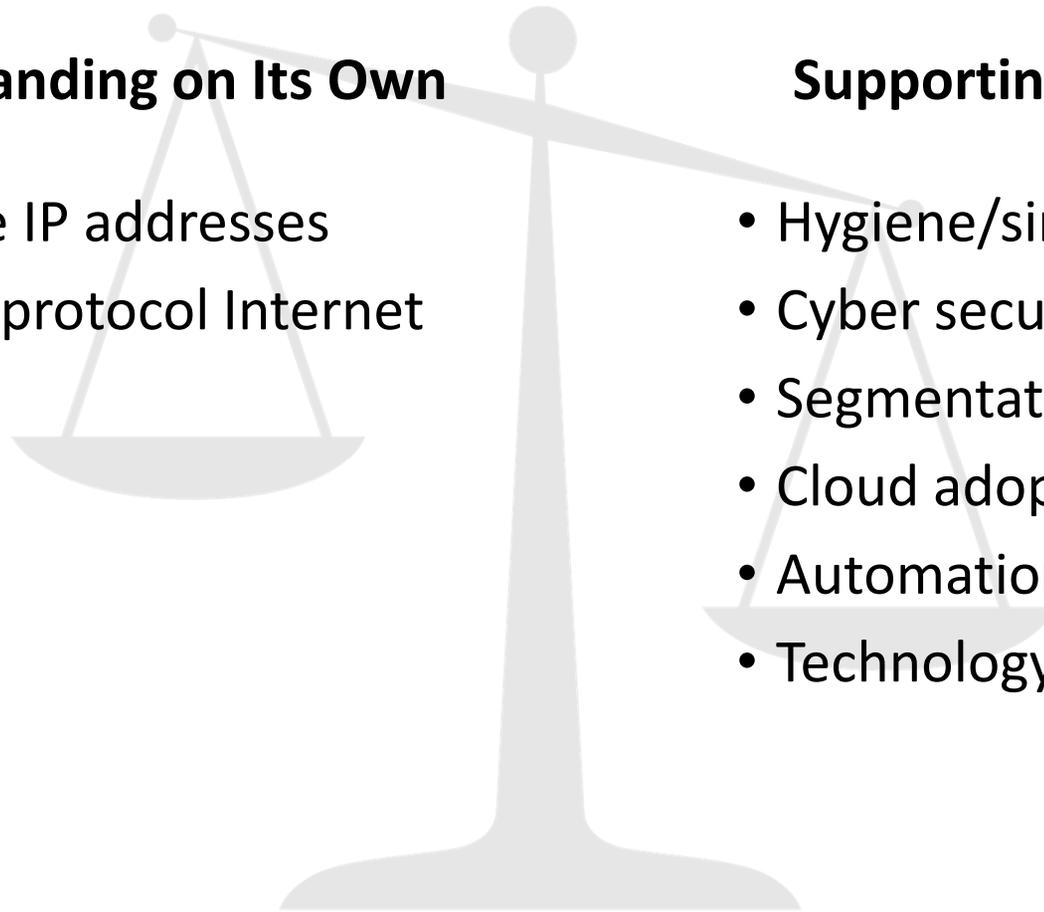
IPv6 is not just about addresses

Standing on Its Own

- More IP addresses
- Dual protocol Internet

Supporting Other Efforts

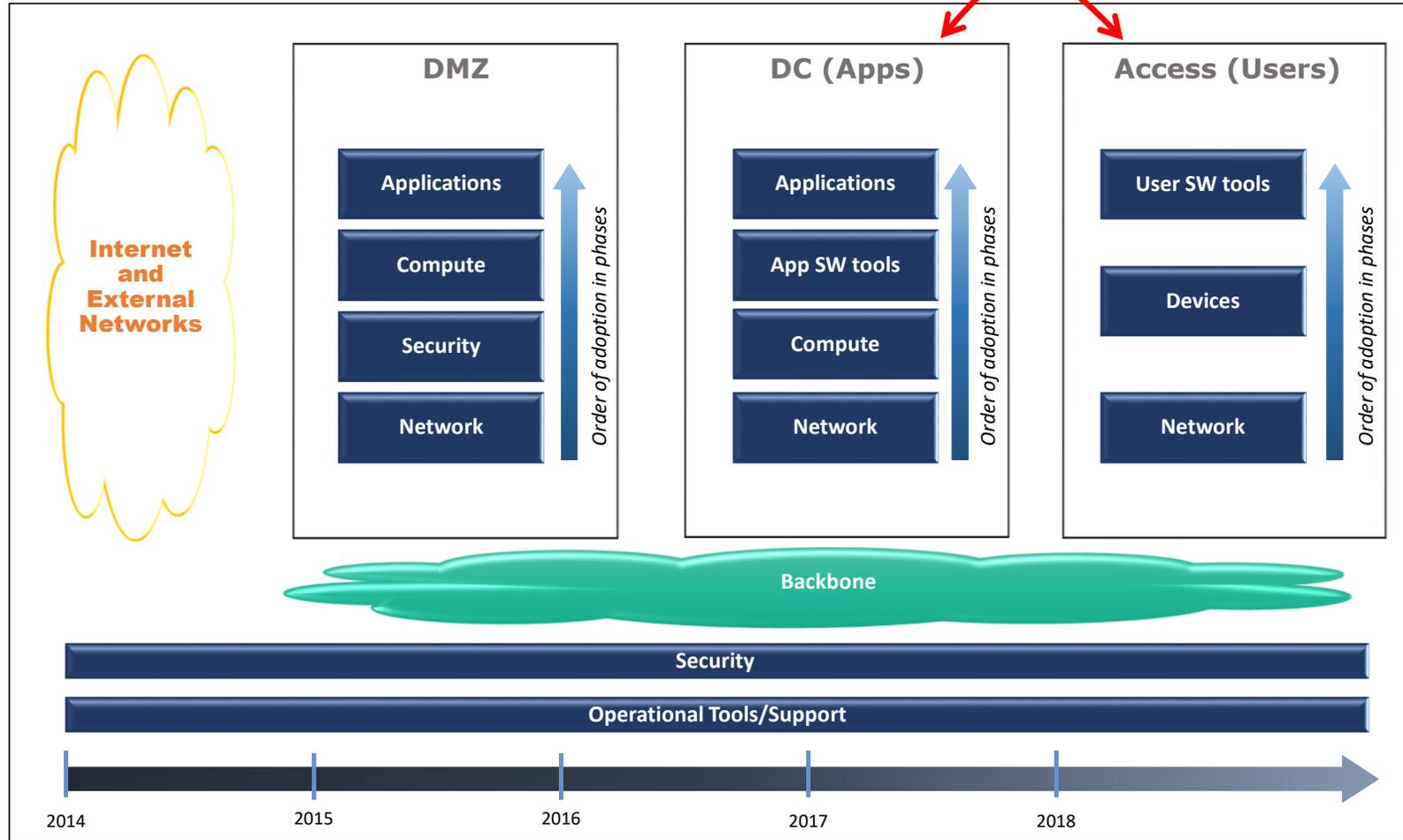
- Hygiene/simplification
- Cyber security
- Segmentation
- Cloud adoption
- Automation
- Technology Currency



The How

A sample v6 roadmap – your mileage may vary

Lots of debate on the order of these



Some things were *almost* painless

- ✓ General IPv6 routing has been rock solid
- ✓ Standard load balancing (including 6to6 and 6to4)
- ✓ Firewalling (although getting parity in policies can be challenging)
- ✓ DNSv6 is solid (DDNS is a different story...)
- ✓ Dual stack outbound web proxy
- ✓ Packet capture/decode and flow monitoring tools
- ✓ V6 support in tool libraries (e.g. python, Java, etc.)
- ✓ Training was widely available and went smoothly, after some tweaks to content (do we really need to still discuss ISATAP and 6over4?)

The Bad

Lots of product and feature gaps with IPv6

- ☹️ Missing network security features (RA-guard, ND-inspection, OSPFv3 MD5 auth, 802.1X DACLs, etc.)
- ☹️ Host security agents
- ☹️ Remote access VPN products (surprisingly late to the game)
- ☹️ Peer-to-peer content distribution
- ☹️ Some endpoints support “split stack” (IPv4 OR IPv6, not both)
- ☹️ The storage world is definitely lagging in v6 support
- ☹️ Cloud stacks (public and private) have generally limited or non-existent v6 support

Many niche products for enterprises lacked not only IPv6 support, but any credible roadmap to get there

The Ugly

Some problems are worse than others...

- 💣 RFC5952 text representation is not well understood/adopted (and IPv6 regexes are challenging)
- 💣 Active Directory and DHCP integration can be rocky even in IPv4, and IPv6 exacerbates the issues
- 💣 Discovery/scanning tools are very challenged (brute force sweeps and dual-stack address affinities in particular)
- 💣 Troubleshooting dual stack complicates familiar techniques
- 💣 Native IPv6 only, which is the real goal, remains significantly out of reach

What would help?

- More validation of v6 only solutions, so that we can actually move beyond the limitations of v4
- Better support for features which remediate deficiencies in IPv4 (i.e. ND-inspection, SEND, SAVI)
- Guidance on how to break our decades-old addiction to IP addresses as objects/labels
- More exposure of v6 capabilities that improve on v4 (e.g. ext headers for native segment routing, multi-addressed interfaces, address authenticity)
- Validation of IPv6 as the *next generation* protocol, not just TCP Using Bigger Addresses