Final Thoughts I

How to get started

- Work from outside in, then bottom-up
  - WAN/ISP, border, DMZ, firewall, enclave
  - LAN interfaces, desktops, servers, apps
- Focus first on your public facing services
  - www, DNS, MX
- Establish a corporate culture to include IPv6 in all IT plans and activities
  - from CIO down to all technical staff
- Take the long view
  - get there via normal tech refresh, not forklift upgrade during crisis
- Don’t be afraid to try new things, take calculated risks

Final Thoughts II

How Hard is it?

- Easy parts of the IPv6 transition:
  - Dual-stacking the networks (WANs, LANs)
  - Enabling IPv6 functionality in modern operating systems
  - Establishing basic IPv6 services (DNS, SMTP, NTP)
  - Enabling IPv6 in some commodity services (HTTP)
- A little more challenging:
  - Getting the address plan right
  - Operating and debugging a dual stack environment
  - Multicast (though easier than in IPv4)
- Hard parts:
  - Creating and maintaining a security infrastructure
    - firewalls, IDS, proxys, IDP/IPS, VPNs, ACLs
  - Working around missing or broken functionality
  - DHCPv6 (in conjunction with IPv4, rather than in isolation)
  - Creating incentives to upgrade and try IPv6
  - Getting the vendors to fix bugs or incorporate missing features
    - Not enough market pressure, so other activities take priority

Final Thoughts III

On-going Challenges

- Keeping security policies consistent across dual stacks.
  - ACLs, Firewall policies, et cetera.
- Adversaries now have a new entry vector.
  - Don't allow IPv6 path to become a new weakest link.
- Diagnosing network problems.
  - Especially where the routing topology isn't congruent across protocols.
  - Confusion over which protocol is broken, and what protocol is being tested using diagnostic tools.
- Trying to outlaw NAT.
  - Some still believe that it brings important features (i.e. "security" rather than "obscurity").

Final Thoughts IV

- These are necessary but not sufficient to show functional equivalence:
  - Standards activities (IETF, DISR), theoretical analysis of standards (NSA), test equipment (Agilent, Ixia, Spirent), JITC generic test plans and approved product lists, and test beds (DRENv6, MoonV6).
- These are sufficient but not conclusive to show equivalence:
  - Extended use in real networks to expose and fix remaining errors (Internet2, DREN IPv6 pilot, still more would be nice).
- To really determine IPv6 support for your needs, query the vendor for specific features that matter to you. Be careful in evaluating their response. Try not to let your expectations dictate the results you find, or you will overlook/misinterpret results that contradict those expectations.

*It is **crucial** that IPv6 products have **functional parity** with IPv4 products!*