Enterprise IPv6 Deployment
Lessons, Observations

2012 North American IPv6 Summit
10 Apr, 2012
Denver, CO

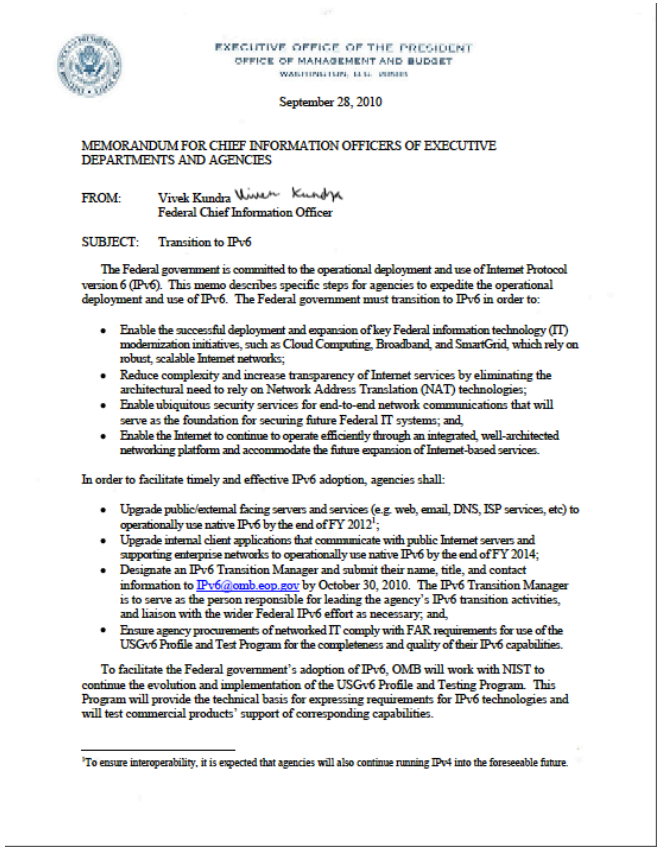
Ron Broersma
DREN Chief Engineer
SPAWAR Network Security Manager
Federal IPv6 Task Force
ron@spawar.navy.mil

Looking from multiple perspectives

- Internet Service Provider
  - Defense Research and Engineering Network
  - 10+ years IPv6-enabled
- Enterprise Network
  - SPAWAR (Navy)
  - 10+ years IPv6-enabled
- Federal Agencies
  - Trying to roll out IPv6 now to meet new Federal Mandates

Defense Research and Engineering Network (dren.net)	SUCCESS	SUCCESS	0/0 3/3	Stratum 1	SUCCESS
SPAWAR (spawar.navy.mil)	SUCCESS	SUCCESS	0/0 3/3	Stratum 1	SUCCESS

Source: http://www.mrp.net/IPv6_Survey.html



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 28, 2010

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Vivek Kundra
Federal Chief Information Officer

SUBJECT: Transition to IPv6

The Federal government is committed to the operational deployment and use of Internet Protocol version 6 (IPv6). This memo describes specific steps for agencies to expedite the operational deployment and use of IPv6. The Federal government must transition to IPv6 in order to:

- Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
- Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;
- Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and,
- Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.

In order to facilitate timely and effective IPv6 adoption, agencies shall:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012[1];
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
- Designate an IPv6 Transition Manager and submit their name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

To facilitate the Federal government's adoption of IPv6, OMB will work with NIST to continue the evolution and implementation of the USGv6 Profile and Testing Program. This Program will provide the technical basis for expressing requirements for IPv6 technologies and will test commercial products' support of corresponding capabilities.

[1] To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.

Bottom Line Up Front

- While not fully matured in all areas, IPv6 is ready for prime time.
- Security and Performance of IPv6 is equivalent to IPv4
- IPv6 deployment does not have to be costly
  - If you start early and use an incremental approach, and use tech refresh, there is almost no cost to deployment.
  - If you procrastinate, it will be costly.
  - If you haven't started, you may be too late.

Bottom Line

- Some service providers and product vendors have limited IPv6 support today.
  - You may need to switch providers or products.
  - But the mainstream router/switch products, and the major operating systems all have very good support. Some of the major carriers do not, and most residential (DSL, cable) networks do not.
- The "business case" for IPv6 deployment is business survival.
- The "killer app" for IPv6 is the Internet itself.

Better than 2 years ago

- Mac OS X issues addressed in 10.6.8 and 10.7
  - and it now supports DHCPv6 too
- Windows 2000 is gone
- VMWARE supports IPv6 since ESX 4.x
- NetApp now works over IPv6
- Much better story for doing network management over IPv6

Benefits of IPv6 today (examples)

- Addressing
  - can better map subnets to reality
  - can align with security topology, simplifying ACLs
  - sparse addressing (harder to scan/map)
  - never have to worry about "growing" a subnet to hold new machines
  - auto-configuration, plug-n-play
  - universal subnet size, no surprises, no operator confusion, no bitmath
  - shorter addresses in some cases
  - at home: multiple subnets rather than single IP that you have to NAT
- Multicast is simpler
  - embedded RP
  - no MSDP

Some Lessons Learned

- Gain operational IPv6 experience before putting too much effort into enterprise-wide planning
- Addressing Plans
  - everyone makes the same mistakes because they are coming from an IPv4 mindset.
- Go native (dual stack, no tunnels, no translators)
- Start from outside, and work in
  - focus now on public facing services
- There will be challenges (surprises) along the way
- You can automate the DNS updates
- It doesn't require significant resources, if you start early and leverage tech refresh

Top Challenges

- Lack of IPv6/IPv4 feature parity
  - taking too long to get there
- Vendors not eating own dogfood
  - but starting to turn around
- Rogue RAs due to Windows ICS
  - set router priority to "high" as workaround
- Privacy Addresses (RFC4941) break address stability
  - no easy way to centrally disable
- Lack of DHCPv6 client support in older OS's
- Network Management over IPv6 not quite there
- Operational Complexity with dual-stack
- Bad planning in some organizations due to no operational experience with IPv6
  - serious mistakes in developing addressing plans

Management over IPv6 in some products

Previously (June '2011):

	SSH HTTPS	DNS	Syslog	SNMP	NTP	RADIUS	Unified MIB RFC4293	Flow export	TFTP FTP	CDP LLDP
Cisco										
Brocade										
Juniper										

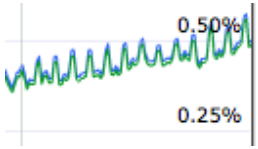
Now:

	SSH HTTPS	DNS	Syslog	SNMP	NTP	RADIUS	Unified MIB RFC4293	Flow export	TFTP FTP	CDP LLDP	IPv6 MTU	No v4
Cisco[3]								6				
Brocade											9	1
Juniper								5				
ALU	2							4				
A10							8	7				

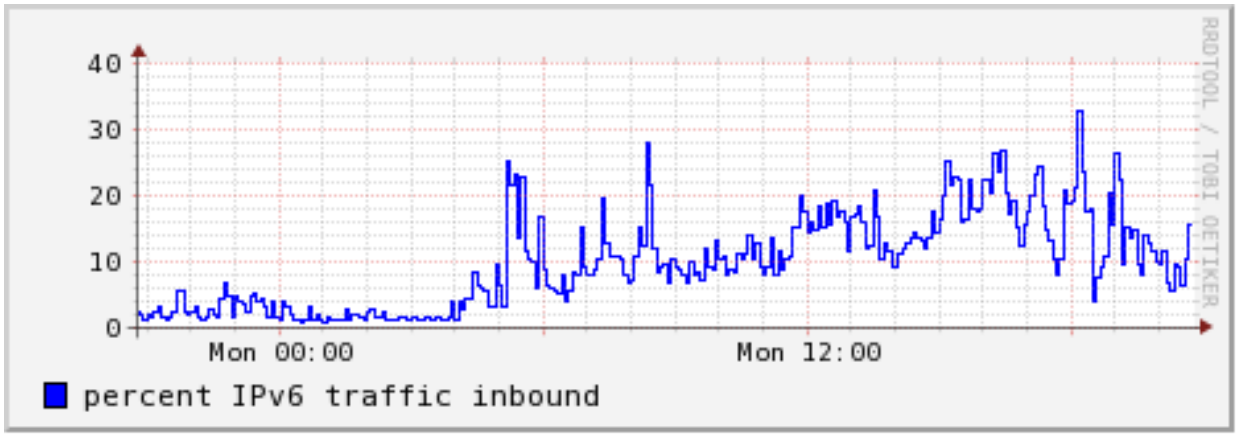
1. In FESX devices with v4 disabled, still does v4
2. ssh over IPv6 not supported until 10.0R1 (March 2012)
3. 15.2(2)TR
4. R10.4 July 2012
5. 12.3R1 Nov 2012 (beta in August)
6. ASR1K:3.7S (July 2012)
7. 3.0 release, 2012Q4
8. No plans
9. fixed in 7.3.0c (May 2012)

IPv6 traffic percentage

- From a server perspective, what percentage of the Internet will try to reach you over IPv6 today?
  - 0.5%



- From a client perspective, what percentage of Internet traffic is IPv6, where everything at your site is IPv6-enabled:



U.S. Government Status

- Federal IPv6 Task Force
  - Roadmap (new version soon)
  - Mandates (2012, 2014)
  - Transition Managers in each Federal Agency
  - Facilitation and Encouragement to meet mandates, and participate in World IPv6 Events

U.S. Government Status

- Progress
  - Awareness, interest, and activity is accelerating
  - Progress monitoring (NIST monitor)
  - Some agencies might meet 2012 mandate, but much work still required
- Issues
  - Carrier(s) lacking IPv6 support
  - TIC, MTIPS
  - Existing security products lack IPv6 support
  - Transition planning without IPv6 operational experience.
    - impacts things like addressing plans

Addressing Plans

- Common mistakes
  - Doing other than /64 for subnets
    - Didn't read RFC 4291 nor 5375
  - Thinking that the addressing plan has to be perfect the first time
    - because you can't afford to re-address
  - Choosing allocations for sites based on size of site
    - because /48 for all sites is too wasteful
  - Justification "upwards", instead of pre-allocation "downwards"
  - Host-centric allocation instead of subnet-centric

Addressing Plans

- Without sufficient operational experience with IPv6 deployment, you WILL get it wrong at first.
  - usually takes the 3rd time to get it right
- Planners are hindered by IPv4-thinking
  - being conservative with address space
  - thinking "hosts" instead of "subnets"

Making the paradigm shift

- You may be un-qualified to develop an IPv6 addressing plan if you think:
  - /64 for subnets is wasteful
  - /64 for point-to-point links is wasteful
  - /48 for small sites is wasteful