Full Production IPv6 Deployment An Enterprise View

2011 Fall TXv6TF Conference
14 Sep 2011
Austin, TX

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

Background

- Defense Research and Engineering Network
  - ISP for DoD R&E Organizations
    - High Performance Computing
    - Research and Development
    - Modeling and Simulation
    - Test and Evaluation
- SPAWAR (Navy)
  - Operates network supporting RDT&E
    - wide area, over a dozen campuses
  - large enterprise customer of DREN
  - Internet pioneer

Progress on IPv6 deployment

- ✔ WAN – dual stack everywhere, peering (unicast+multicast)
- ✔ LANs, WLAN – all subnets fully support v6, renumber v4
- ✔ Infrastructure services – recursive DNS, NTP, SMTP, XMPP
- ✔ Support services – RADIUS, LDAP, Kerberos
- ✔ Public facing services – authoritative DNS, MX's, www, NTP
- ✔ "Security stack" – firewall, IDS, IPS, etc.
- ✔ Security services – WSUS, McAfee ePO (aka DoD HBSS)
- ✔ Servers, desktops, laptops – 100% dual stack
- ✔ Storage (NFS, CIFS)
- ✔ Network management

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

Topics today

- The big issues (for us)
- Network Management over IPv6
- World IPv6 Day observations
- Do’s and Don’ts

The major issues for us

- Lack of IPv6/IPv4 feature parity
  - taking too long to get there
- Vendors not eating own dogfood
  - but starting to turn around
- Rogue RAs
  - set router priority to "high" as workaround
- Privacy Addresses (RFC4941)
  - no good solution yet
- MacOSX 10.6
  - but starting to get much better (10.6.8, 10.7)
- Network Management over IPv6

Lack of "feature parity"

- "feature parity" between IPv4 and IPv6 is something we expect in all products.
  - If the device supports a capability in IPv4, we want it to support that same capability in IPv6.
- Nobody delivers feature parity today.
  - Some vendors are working to fix this.
- Until we achieve feature parity...
  - IPv6 is something less than IPv4
  - You may need to re-engineer your network to accommodate missing features.

Privacy Addresses (RFC 4941)

- Incompatible with many Enterprise environments
  - Need address stability for many reasons
    - Logging, Forensics, DNS stability, ACLs, etc.
- Enabled by default in Windows
  - Breaks plug-n-play because we have to visit every Windows machine to disable this feature.
- Just added in Mac OS X "Lion".
- Ubuntu thinking about making it default.
- Need a way for the network to inform systems about proper default on managed enterprise networks
  - new flag in RA prefix information option?

[Privacy addresses] are horrible and I hope nobody really uses them, but they're better than NAT.
… Owen DeLong, Hurricane Electric

If we can't beat 'em, join 'em

- What if the privacy address thing is a losing battle, and we have to live with it?
- We did an Internet-Draft for new RA bits, but it was a hard sell in the IETF.
  - desire for privacy (anonymity) is very strong.
- We've debated the topic in various forums.
- New initiative:
  - created subnet where we allow privacy (temporary, random) addresses, and moved a bunch of machines there (Windows, Mac).
  - disabled the alarms (warning about privacy addresses).
  - modified our NDT scanner and auto-DNS-update tool to keep things updated in DNS (PTR records).
    - some argue that this should not be necessary, but some anti-spam tools will reject email from originating hosts that aren't in DNS.
  - going to generate historical database of MAC address to IPv6 address mapping, for use in IDS and forensics tools.

Vendors not "eating own dogfood"

- We were surprised to find so many IPv6 features in vendor products appear to have never been tested or used.
- We learned that vendors were not using their own IPv6 products and features. They weren't "eating their own dogfood".
- This situation is starting to improve, finally

Brocade (brocade.com)	SUCCESS	SUCCESS	4/4 4/4

  - Others just starting to:

Cisco Systems (cisco.com)	www.ipv6	FAIL	0/2 0/2
Juniper Networks (juniper.net)	ipv6	FAIL (P)	0/3 0/5
Force10 Networks (force10networks.com)	FAIL	FAIL	0/0 0/4

Network Management

- Most products cannot be managed over IPv6
- We've been trying to do ALL network management using IPv6, so we can remove IPv4 from the management networks.
- We think we can succeed by Nov 2011
  - But we've had to remove various vendors' products from our networks

Mgmt LAN over IPv6

- Goal – Management LAN IPv6-only (see previous talks)
- Status:
  - Switches: removed all IPv4 configuration from all (over 500) switches at one campus.
    - other campuses in process of doing same
  - Routers: using only IPv6 for most functions, but awaiting fixes or features
  - monitoring: went with Gigamon instead of Anue
  - sensors: all IPv6, including the DRAC ports
  - UPSs: replaced with new APC hardware, all managed over IPv6
  - management/admin tools (apps): still dual stack to accommodate remaining few IPv4-only devices.
  - replacing some old hardware that will never get IPv6 support
- Upcoming milestone:
  - remove all remaining IPv4 configurations (no more lifeline).
  - Oct 2011?
- Remaining issues
  - Lack of unified IP MIB support (RFC 4293) in some products

Management over IPv6 in some mainstream products

	SSH HTTPS	DNS	Syslog	SNMP	NTP	RADIUS	Unified MIB RFC4293	Flow export	TFTP FTP	CDP LLDP
Cisco[6]										
Brocade				1				2	3	4
Juniper										
ALU	5							7		

1. Lack IPv6 ACL support
2. can't specify router-ID as IPv6 in MLX
3. firmware bug in FastIron products
4. not in MLX
5. ssh over IPv6 not supported until 2012(Q1)
6. 12.2(58)SE1
7. R10.4 July 2012

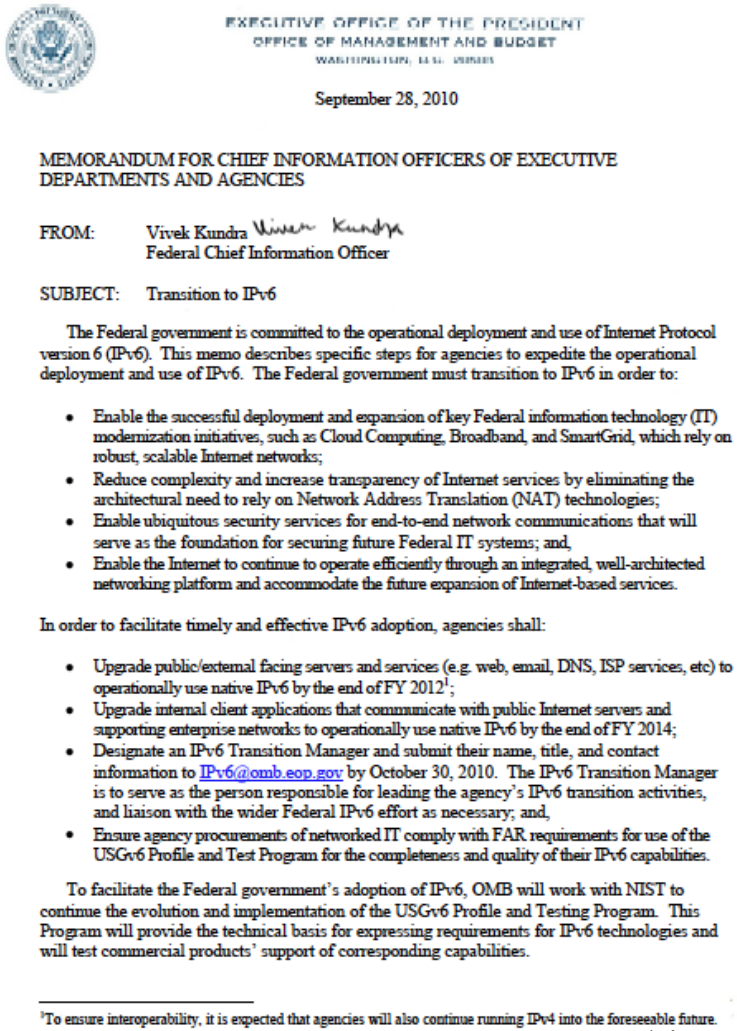
Many other enterprises have not started their IPv6 deployment

- Reasons:
  - Lack of incentives and resources
  - Other higher priorities (improving security)
  - It all seems overwhelming, and don't know where to start.
  - No “business case”
- My answer:
  - If you haven't started, you're late and at risk
  - It doesn't take additional resources if you do it right.
  - For U.S. Federal agencies, there is a new mandate.
  - Don't waste time on developing a business case.
    - Its a matter of business continuity.
  - “Don't be afraid to break some glass”

New U.S. Federal Mandate

- Sept 28, 2010
- IPv6-enable all public services by 2012
- Everything else by 2014
- All agencies deliver transition plans by April 2011

Status Monitor:
http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov



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.

Incentives

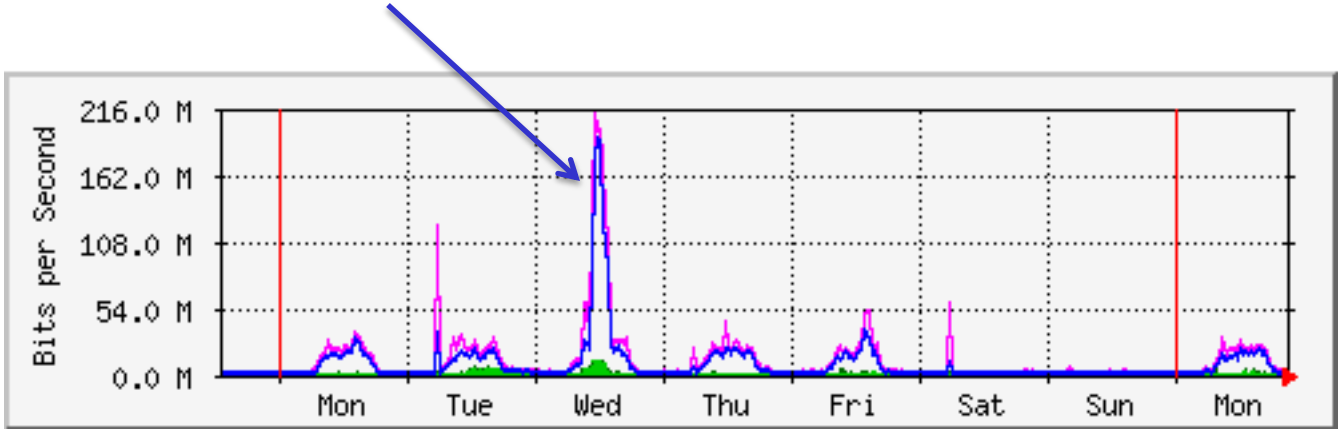
- DREN3 RFP (Jan 2011)
  - "DREN is identified as an IPv6 network with IPv4 legacy support"
  - "Additionally, all network management shall be enabled using IPv6"

World IPv6 day

- For DREN and SPAWAR, nothing new to turn on for the day
  - every day is IPv6 day for us
- What does it look like from an enterprise perspective, where ALL clients (users) are dual-stack?
  - well, 99% actually

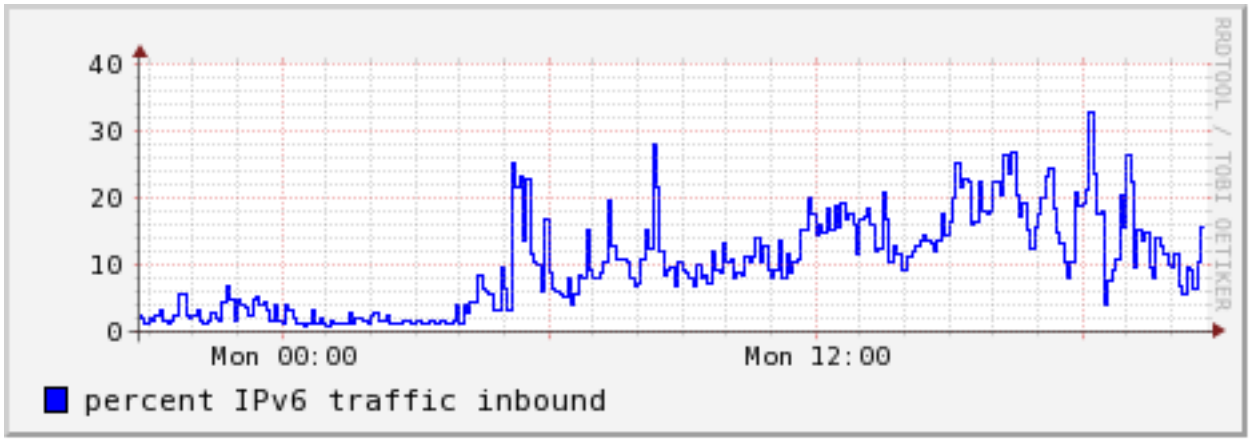
Percentage of Internet traffic over IPv6

- 1% (2009, before Google whitelisting)
- 2.5% (Google whitelisted)
- 10% (late Jan 2010, Youtube added)
- World IPv6 day… (peak at 68%)



After IPv6 day

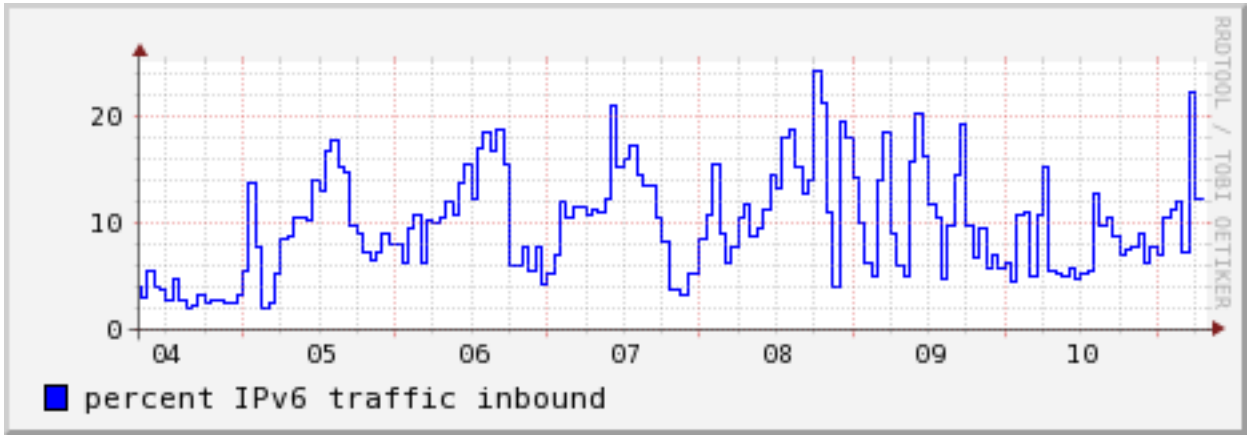
- Percentages across a day (5 min averages):



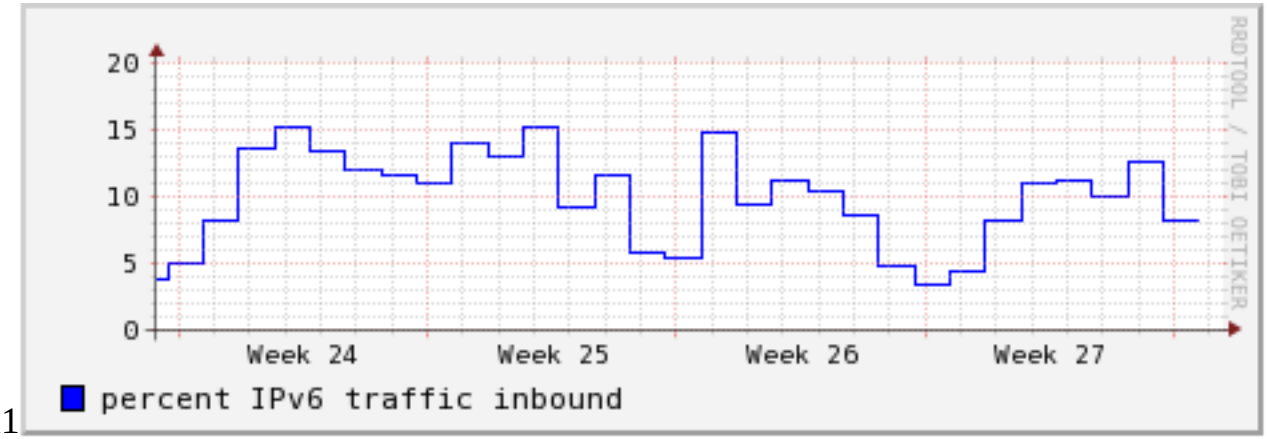
- Why higher during the work day?

After IPv6 day

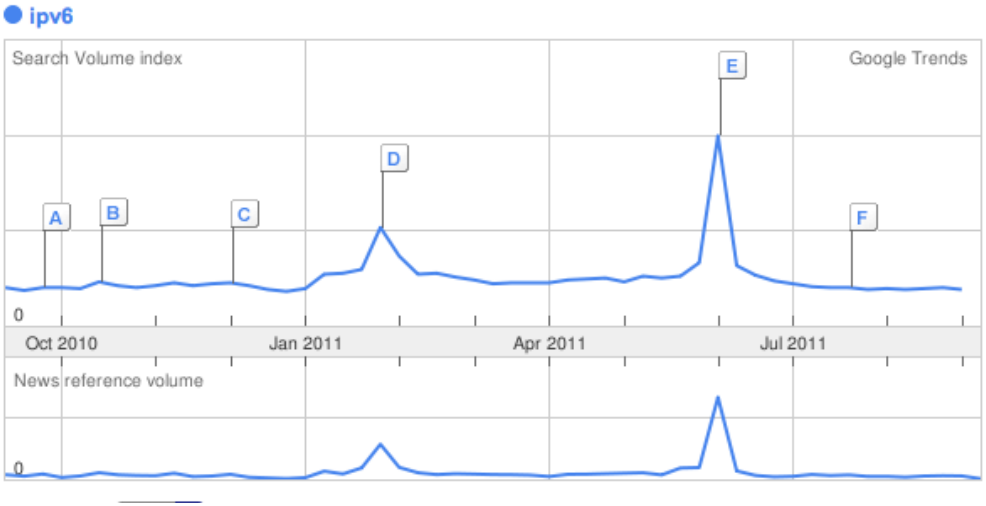
- Past week (hourly averages):



- Month (daily averages):



From Google Trends



A [Too Little, Too Late: The Feds call for IPv6](#)
ZDNet - Sep 29 2010

B [Blue Coat Chief Scientist to Discuss Internet Security and IPv6 at Australian IPv6 Summit](#)
MarketWatch - Oct 18 2010

C [Verizon Launches IPv6 Transition Services](#)
PC World - Dec 8 2010

D [Net powers: IPv4 is over. All hail IPv6!](#)
CNET - Feb 3 2011

E [Happy World IPv6 Day!](#)
CANOE - Jun 8 2011

F [Yahoo, Facebook, Google to IETF: Where Are the IPv6 Users?](#)
PCWorld - Jul 27 2011

Other observations

- DoD
- NIST
- Proxy/Translators
  - how do we make sure they are only temporary?
- What's next?
  - World IPv6 week (early 2012?)
  - entire Public Internet (1/1/2013?)

Some Do’s and Don’ts

Do

- Get buy-in from corporate leadership, especially CIO
- Develop a corporate culture for IPv6
  - involve all parts of organization, not just the network guys
  - have a local champion
  - include IPv6 in every IT initiative
- Take baby steps
  - go for the low hanging fruit
  - get experience along the way
- Leverage tech-refresh rather than spend $$$ on fork-lift upgrades out-of-cycle.
  - it doesn't have to be very expensive
- Start now
  - if you haven't, you are already quite late to the game
- Start by IPv6-enabling your public facing services
  - work from outside in, and from bottom up
- Go native
  - avoid translators, tunnels, and other transition schemes
- Only choose suppliers that have a good IPv6 story

Don't

- waste time developing a complete transition plan with no operational experience
- base your addressing plan on conservative IPv4 practices
- waste time on a comprehensive addressing plan without operational experience
  - consider the first one a throw-away
- waste time trying to develop a business case (ROI) for deploying IPv6.
  - it is a matter of business survival
- be afraid to break some glass
  - world ipv6 day validated that

Benefits of IPv6 today (examples)

- Addressing
  - can better map subnets to reality
  - can align with security topology, simplifying ACLs
  - never have to worry about "growing" a subnet to hold new machines
  - 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

Is there a killer app for IPv6?

- The killer app is the Internet itself.
- The Internet cannot grow and evolve without more addresses, and IPv6 fixes that.
- Within a couple years, the IPv4 Internet will have an increasing number of performance and availability problems, and the IPv6 Internet will be superior.

Final Thoughts

- Enabling IPv6 throughout your environment needs to be a cultural thing.
  - Get everyone involved and on-board
  - Include it as part of technology refresh.
  - Don’t be afraid to break some glass
- Very important that we focus on making our public facing services dual-stack as soon as possible.
  - otherwise we’ll be in translator-hell, breaking various applications
  - eventually some clients won’t be able to reach you
- IPv6 is an “unfunded mandate”, and everyone needs to do their part.
- Need v4/v6 feature parity in products
- Avoid vendors that don’t have a good IPv6 story