



DREN IPv6 Implementation Update

Internet2 Joint Techs, Winter 2011

1 Feb, 2011
Clemson, SC

Ron Broersma
DREN Chief Engineer
ron@spawar.navy.mil



The DREN IPv6 Initiative

- Aggressive deployment of IPv6 to DoD's R&E WAN (**DREN**) and to all campuses of one major customer (**SPAWAR**)
- These are production networks with 10's of thousands of users and systems.
 - i.e., not just a testbed
- Goals
 - See what works and what's broken
 - See what's missing
 - Share lessons learned



IPv6 deployment progress

- ✓ 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



Previously discussed...

- Reported at Salt Lake City meeting:
 - New approach to training, and bootstrapping sites, and BCPs
 - All DREN on Google-IPv6, very successfully
 - Some customer sites see 10% of traffic now over IPv6
 - Too hard right now: Windows 2000, older printers
 - Auto-sync for DNS tool
 - Rogue RAs – mostly from Windows with ICS – fix with router-priority
 - Semantec Endpoint Protection (SEP) breaks IPv6
 - vmware ESX 3.x
 - Blackberry Enterprise Services (BES) on IPv6-enabled Windows server will crash
 - WSUS (windows patching) all over IPv6 successfully
 - Serious problems with randomized identifiers in Windows (RFC 4941)
 - Problems with Mac OSX 10.6 (Snow Leopard)
 - DNS (mDNSresponder bug), java can't be made to use IPv6, talking to IPv6 printers
 - IPv6 support in FreeRadius (how to)
 - Goal: ALL servers, desktops, laptops running dual stack (at SPAWAR)



Previously discussed...

- Reported at Columbia meeting:
 - Continued additional support for network management over IPv6
 - DREN-wide updates to resolve JunOS bugs
 - Remaining issues with IPv6 on management LAN
 - managing UPSs over IPv6
 - NFS (via NetApp) over IPv6



Mgmt LAN over IPv6 - update

- Goal – Management LAN IPv6-only (see previous talks)
 - replaced remaining old Foundry switches that had lingering IPv6 issues
 - Brocade TCP bug fixed (had been a showstopper)
 - APC units all replaced by manufacturer
 - first version had flaws, was unstable
- Success:
 - removed IPv4 from switch mgmt LAN at one campus (supporting over 500 switches)
 - removed lingering IPv4 config lines from all switches
- Problem:
 - Server ops group uses Zenoss, and lost all visibility to switches
 - too bad, they should not have purchased it if it didn't support IPv6
 - Recently added ping6 support, so some visibility restored



Mgmt LAN over IPv6 - update

- Remaining issues
 - Lack of unified IP MIB support (RFC 4293) in most products
 - A few devices still need upgrade or replacement in our infrastructure
 - Aruba WLAN controller
 - Cisco 3000 series VPN
 - ServerIrons
 - Bluecoat Proxy
- DREN3 RFP (Jan 2011)
 - “DREN is identified as an IPv6 network with IPv4 legacy support”
 - “Additionally, all network management will be enabled using IPv6”



Other updates

- Symantec Endpoint Protection (SEP)
 - broke IPv6, so outlawed on our net
 - workaround (config change) identified
 - Symantec now committed to full IPv6 support in all products
- MacOSX 10.6
 - broke address selection (didn't prefer AAAA)
 - caused Internet brokenness (6to4 preferred over native v4 if on private address space)
 - 10.6.5 starts to fix these issues
 - but see <http://arstechnica.com/apple/news/2010/11/apple-fixes-broken-ipv6-by-breaking-it-some-more.ars?comments=1&p=21007430#comment-21007430>
- Much NFS and CIFS still using IPv4
 - no client support in XP, RedHat up through RHEL5, Solaris 8.
- Juniper SRX testing
 - lacking many IPv6 features (management, tunnels, IPSEC, etc.)



Other updates

- Privacy Addresses (RFC 4941) – we still hate it
 - Default enabled in Windows
 - Incompatible with many Enterprise environments
 - Ubuntu thinking about making it default
 - PLEASE DON'T!!!
 - Work underway on I-D to address this issue
 - new flag in RA prefix information option.

- Some vendors eating own dogfood, 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	0/0 0/4



New OMB mandate

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



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 *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 2012¹;
- 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.

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



New OMB Mandate

- Federal IPv6 Task Force coordinating efforts
- All agencies made initial presentations
 - situation is not good
- Major issues for most Agencies
 - TIC doesn't support IPv6 yet
 - Carriers on Networx contract don't seem to support IPv6 yet
 - Akamai
 - Load Balancers
- Agencies have done very little real work
 - some have generated lots of paper
 - almost no evidence of actually passing any IPv6 traffic



New guidance

- Updated FAQ coming soon
 - clarifying things like “public facing services”
- Checklists and Transition Plan templates
- Do something NOW, don’t wait until 2012
 - “don’t be afraid to break some glass”
 - identify primary agency web site and IPv6-enable it within next 4 months
 - establish internal tiger-team, will full support and authorization by management.
 - Participate in World IPv6 day
 - will help gain much needed operational experience
 - will create demand signal for suppliers
- Will define milestones and measures of success
 - status reported weekly to Federal CIO



Soapbox

- Enabling IPv6 throughout your environment needs to be a cultural thing.
 - Get everyone involved and on-board
 - Include it as part of tech refresh.
- It may seem overwhelming in the beginning, but its really not that hard to get started.
- 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