



DREN IPv6 Implementation Update

Internet2 Joint Techs, Summer 2010

13 July, 2010
Columbus, Ohio

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



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)



Progress to date

- ✓ 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 – 97.4% dual stack



WAN infrastructure

- Moving all traffic to a new IPv6 IPSEC mesh
 - currently operates over an IPv4 IPSEC mesh
 - test mesh is built and undergoing acceptance
- Deployed a new backbone addressing plan
- IPv6 uRPF enabled on all customer interfaces
- Upgraded to JunOS 9.3R4.4 to fix:
 - IPv6 Path MTU discovery bug
 - Router crash when receiving “ICMP packet too big” message



WAN infrastructure

- Upgrading to 9.3S9 (next 2 weeks) to fix:
 - IPv4 traceroute over IPv6 IPSEC tunnel returns erroneous information
 - non-deterministic route selection v4 and v6 when using CsC.
- No unresolved IPv6 bugs at this time 😊
 - 9.3S9 looks like a solid release
- Continuing to bring up more IPv6 external peering
- Converted UUNET peering to native
 - previously could only do GRE tunnels ☹️



SPAWAR mgmt LAN update

- Goal:
 - migrate management LAN to IPv6 where possible
 - all devices get IPv6 address
 - all management services use IPv6 transport
 - eventually turn off IPv4, where possible
- Triage
 - ignore devices that were eventually going away anyway (ATM switches, dialup modems, ...)
 - use tech refresh to get IPv6 support on various devices
 - all NS-200's replaced with SSG-5's, and other firewall upgrades
 - replaced many Foundry (Brocade) switches
 - Pushed vendors for firmware updates on others



mgmt LAN

- Foundry (Brocade) enhancements requested and delivered
 - snmp (v3) over IPv6 transport
 - DNS over IPv6 transport
 - sflow records over IPv6 transport
 - sflow agent-ID set to IPv6 address
 - RADIUS over IPv6
 - Full IPv6 support in FDP and LLDP
 - Unified IP MIB support
 - set router priority in RAs
 - ... and many bug fixes along the way
- Not yet delivered
 - RA Guard
- Can't disable IPv4 just yet
 - TCP over IPv6 bug unresolved
 - some end-of-support switches still need to be replaced (\$\$\$)



mgmt LAN

- Other devices with IPv6 mgmt support (some only partial support)
 - Spectracom NTP servers
 - Symmetricom NTP servers
 - Netscreen devices (ScreenOS)
 - TippingPoint IPS
 - new APC UPS units ***
- No support
 - Google Search Appliance
 - Aruba WLAN controller and APs
 - Cisco 3000-series VPN servers



Managing the UPSs

- None of the manageable UPS devices supported IPv6
- APC Network Management 2 card now has IPv6 support
 - IPv6-ready Phase-2/Gold Logo
- We're upgrading all APC UPS devices



NetApp Storage Appliance

- We've been waiting a long time for IPv6 support
- Delivered in 7.3.1 (Jan '09) but very buggy
- 7.3.1_P2 (Jul '09) was supposed to work, and be more reliable, but every time we enabled IPv6, all mounts started failing.
- 7.3.3 (May '10) now works, and is enabled
 - All NFS now over IPv6 (Linux clients, Solaris 10 clients)
 - not supported in Solaris 8
 - CIFS now over IPv6 from modern Windows systems
 - IPv6 file sharing not supported in Windows XP
- Possible latent bug – interface flap loses v6 route permanently until interface reset



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
 - 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



Final points...