IPv6 Update and Challenges For a DoD Enterprise Network

Jeremy Duncan

IPv6 Network Architect

SALIENT FEDERAL SOLUTIONS

IPv6 FORUM CERTIFIED ENGINEER

Agenda

- IPv6 Migration Justifications & Technical Goals
- Secure Implementation Approach
- High-Level Architecture
- Technical Lessons Learned

Our IPv6 Transition Philosophy

- Provide a robust, secure and interoperable future-proof network infrastructure
- Implement IPv6 in order to provide end-to-end application survivability, redundancy and security
- Provide much needed network services for mission systems unknown in IPv4:
  - Restoring secure end-to-end (removing NAT)
  - Better multicasting
  - Provide better IP address summarization and routing

IPv6 Technical Goals

- The use of NAT for both IPv4 and IPv6 will not be authorized (some exceptions)
- IPv6 addressing for hosts will be done with DHCPv6 only
- IPv6 routing must utilize OSPFv3 with authentication
- SNMPv3 management must be done over IPv6
- DPI, Firewalls and IDSs must be able to monitor IPv4 and IPv6 traffic
- Native IPv6 BGP peering with DISA for NIPRNet in FY 2013

Secure Implementation Approach

- Heavy Architecture usage of DoD IPv6 Information Assurance (IA) Guidance called IPv6 Milestone Objective (MO) 1, 2 and 3
  - MO1: One IPv6 internal pilot network without IPv6 externally.
  - MO2: Two IPv6 internal pilot networks, geographically separated, connected over an IPv6 over IPv4 tunnel (IPsec or GRE)
  - MO3: a complete dual-stack (IPv4 and IPv6) network with specific IA controls.

IPv6 Design Process

– Develop a system design for all components in the enterprise including systems and applications (All applicable for Federal 2014 mandate)

- DNS/DNSSEC
- Routing & Switching
- Remote Access & site-to-site VPNs – DMVPNs
- DMZ infrastructure
- Security & Monitoring
- Virtual Desktop
- Network Management
- Multicast
- COOP
- Cloud Management functionality
- WAN & Application Optimization
- IP Address Management (IPAM)
- DHCP/DHCPv6
- Windows Active Directory & Exchange
- Application Servers (Sharepoint, web, etc)

2013 IPv6 Implementation Update

- Implementation done on a newer modernization network that will replace existing production infrastructure
  - In modernization network, servers and applications are built with all functions running IPv4 and IPv6
  - Reduces need to “move” to IPv6
- Transition Plan aimed at successive IPv6 implementations on the following network enterprises:
  - JWICS – Top Secret network – (DIA backbone)
    - Implementation complete; external dependency on DIA
  - NIPRNet (DISN Unclassified) – (DISA backbone)
    - Implementation complete internally; external dependency on DISA
  - SIPRNet (DISN Classified) – (DISA backbone)
    - Implementation nearing completion internally; external dependency on DISA

2013 IPv6 Implementation Update, cont.

- The Defense Information Systems Agency (DISA) IPv6 implementation on the Unclassified Network (NIPRNet/DISN-U)
  - Currently implementing a Community of Interest (COI) backbone that is planned to route all interested IPv6 sites on the NIPRNet/DISN-U
  - The Air Force, DTRA, DTIC and Navy are all trying to gain BGP IPv6 peerings on NIPRNet/DISN-U now
  - DISA may undergo a large IPv6 address re-numbering activity – likelihood is unknown, but very possible
  - DTRA cannot route IPv6 external to its enterprise until DISA is ready to route IPv6 on the NIPRNet/DISN-U

2013 IPv6 Implementation Update, cont.

- Sample technologies impacted by IPv6 implementation:
  - Security devices (firewalls, IPS/IDS)
  - Simplified and secure routing
  - Fabric switching
  - Virtual Desktop Infrastructure (VDI)
  - Windows Server 2008, R2
    - New Forrest and Domain
  - Windows Exchange 2010
  - Cloud Provisioning
    - VMWare Cloud Director
    - Self-service provisioning
  - Windows Direct Access

IPv6 Technical Lessons Learned

- INFOSEC infrastructure
- Routing and Switching
- Client and Server
- Virtual Desktop Infrastructure (VDI)
- Remote Access Solutions
- IP Address Management
- In-House Applications
- Most IPv6 implementation problems occurred because some vendors do not fully support IPv6 functionality in the product (e.g. function in IPv6-only network)

INFOSEC Infrastructure Issues

- Application Firewall cannot do a number of functions over IPv6:
  - SNMPv3, SSH or client admin console
  - Only an Active/Standby HA configuration
  - Most proxy rules aren't supported (only HTTP, SSH and HTTPS have IPv6 capability)
- IDS tools could not properly detect IPv6-based vulnerabilities per NIST IPv6 Secure Deployment and DoD IPv6 MO3 IA Guidance
  - Brought in DPI tools – Assure6 and Cloudshield

INFOSEC Infrastructure Issues, cont.

- Internal firewall had many bugs in a recent code release v. 9
  - OSPFv3 bugs caused failover to break
  - OSPFv2 intermittent bugs
  - Required to roll-back to a previous version that has no OSPFv3 support
  - Current status is “Release Pending”

INFOSEC Infrastructure Issues, cont.

- Cannot use IPv6 Secure Neighbor Discovery (SeND) because Cisco ASRs and Microsoft Windows 7 do not support it
  - Cisco ISR routers with at least 12.4(24)T (and M) have support
  - Some 3rd party client applications
  - Using 802.1x to mitigate this issue

IPv6 Routing & Switching

- Core routers now fully support most needed IPv6 features
  - HSRPv2 still uses the IPv6 Link-Local standby – VMware ESX can only use a Global Unicast Address as an IPv6 gateway
  - Using IPv6 General Prefixing to ease re-numbering issues
- Using IPv6 Router Advertisement (RA) Guard on host facing switch interfaces
- Internal server access switches break IPv6 at layer-2 unless “ip igmp snooping optimised-multicast-flood” is disabled

IPv6 Client & Server Issues

- When running Windows Server 2008, R2:
  - Disable all tunneling interfaces – DisabledComponents=0x1
    - Except on the Direct Access server – all tunnel interfaces required
  - Do <u>not</u> turn on “advertising” – causes a huge DoS
    - `netsh int ipv6 set int “Local Area Connection” adv=d`
- Active Directory, IIS, CA server, NPS, etc all work with IPv6 out of the box with very few issues
- The DHCP client service is the same for both IPv4 and IPv6
- Turn off and disable the IP Helper service

IPv6 and Unified Messaging

- Microsoft Lync 2013 has IPv6 issues
- Cisco CUCM and Jabber can use IPv6 without issue
- Microsoft Lync 2013 and Cisco CUCM Integration challenges:
  - CUCMC or CUCM Lync cannot run on an IPv6-enabled Microsoft Windows 7 workstation
  - DoD pending certification for Non-Assured Services PBX:
    - Use of Microsoft Lync for non-assured services voice and presence
    - Cisco CUCM used for assure-services voice and presence (e.g. heavy use of network-based MLPP)

IPv6 & Mail Servers

- Implementing Microsoft Exchange 2010
  - IPv6 must be disabled on Server 2008 R2 platform when doing the Exchange application install – can be enabled later
  - Database Availability Group (DAG) network must have IPv6 disabled – not supported
  - For all other functions IPv6 works just fine – RPC, MAPI, SMTP, etc – after IPv6 is re-enabled

IPv6 & Virtual Desktop

- Citrix application and desktop streaming/hosting platform considerations
  - Citrix Netscaler is fully functional over IPv6
  - Citrix XenDesktop and XenApp may have full IPv6 support now - untested
    - This means IPv6 transport from Citrix Receiver to XenApp or XenDesktop server
  - Hosted operating systems will function just fine with IPv6 now

IPv6 & Remote Access Solutions

- Current VPN remote access platform issues
  - There is no IPv6 capability at all today or anytime in the future
  - Will be implementing Microsoft's DirectAccess
    - Fully IPv6 enabled
    - IPsec over IPv6 over SSL

IPv6 & IPAM

- IP Address Management encompasses the way in which IPv6 addresses will be allocated/assigned, and the tools used for management
- IP address distribution model:
  - DHCPv6 instead of Stateless Address Autoconfiguration (SLAAC)
    - Better control/management
  - SLAAC is used on printer VLANs as majority do not have DHCPv6 clients
    - Using Unique Local Address (ULA) scope for printers

IPv6 & IPAM, cont

- IP Address Management (IPAM) tool is an application that is used to help plan, manage and reconcile IP addresses – our criteria:
  - Must have easily hardened platform
  - Must have capability to reconcile, discover and scan for IPv4 and IPv6 addresses
    - Must use SNMPv3 with AES-128 over IPv6
  - Must be able to manage Windows DHCP and DHCPv6 servers – <u>all IPAM tools do not support Windows DHCPv6 server management/discovery yet</u>

IPv6 & Home-Grown Applications

- With every network application built you must test it in an IPv6-only environment
- Microsoft's sample code for development: Simple.C
- Use of a code scanning tool can help identify possible socket issues:
  - PortToIPv6: http://porttoipv6.sourceforge.net (for C+ applications – non-Microsoft)
  - Microsoft's Checkv4 utility: http://msdn.microsoft.com/en-us/library/windows/desktop/ms740624%28v=vs.85%29.aspx (part of Windows SDK)

Summary

- IPv4 will still be around for a very long time – go dual-stack
  - Stay away from NAT64/DNS64, NPT, or CGN unless there's no other way
- DISA will likely renumber all IPv6 allocations and routing access will be limited – DMZ Extension traffic only
- Include IPv6 as part of modernization programs
- There was C-Level buy-in because IPv6 affected future mission success
- Implementing IPv6 in an enterprise is not easy – deliberate planning and focused architecture is required
- COTS vendors technical capabilities do not always match their marketing language – ask the tough and technical questions or it will be your mistake
  - Most security device vendors fall into this category

Questions?