# After 2012

## Internal Enterprise IPv6 Transition Best Practices

Jeremy Duncan

Senior IPv6 Network Architect

SALIENT
FEDERAL SOLUTIONS

IPv6 FORUM
CERTIFIED ENGINEER

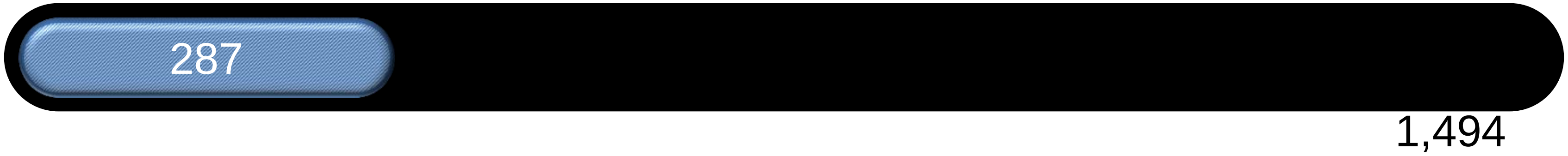
# Agenda

- Quick 2012 US Government Mandate Distillation
- The Real 2014 Expectations
- What an enterprise needs to plan on for 2014
- Technical Roadblocks

# BLUF

- IPv6 transition on your internal enterprise is possible right now
- Enterprise buy-in and process willingness is key
- It won’t be perfect – but I can help provide some technical workarounds

# October 2012 – US Government IPv6 Aftermath

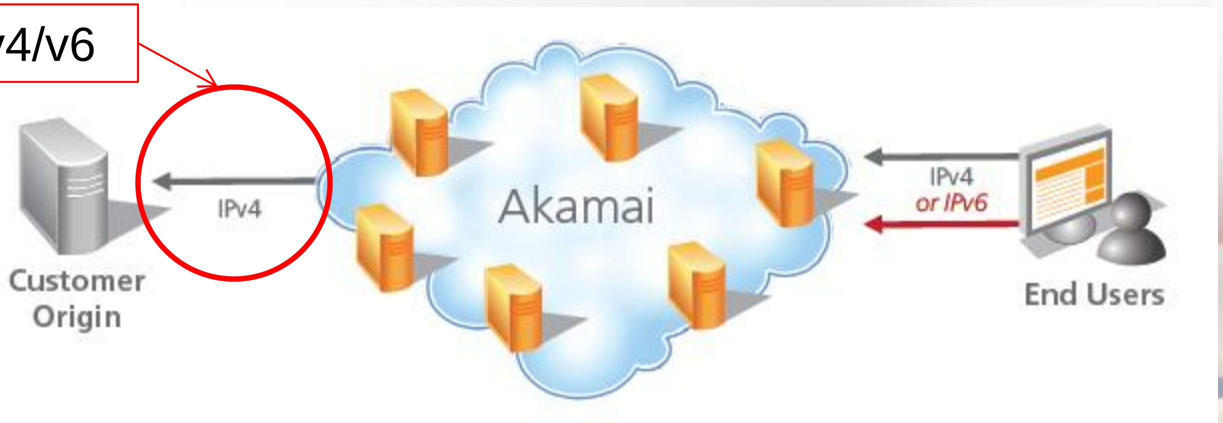


- Of all of the domains NIST monitored 1,494 only 287 had IPv6 on their public-facing websites
- Huge hurdle with email filtering/SPAM gateways
- Of the 20% a large majority are highly reliant on CDNs like Akamai.
- Without full end-to-end IPv6 on public infrastructure, public sector could be setting up for 2014 failure

# October 2012 – Picking Up with 2014

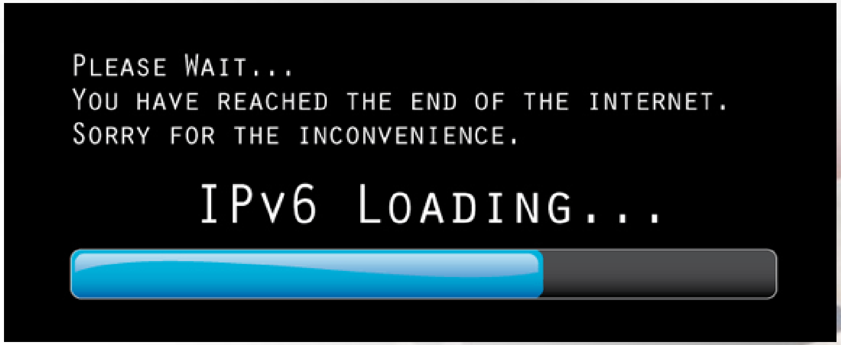
- Of the public sector network transitioned using CDNs this is what work will need to be done above and beyond an internal IPv6 transition:
  - IPv6 enable public DNS service
    - Must work with CDN to provide end-to-end DNS over IPv6 transport
  - IPv6 enable public web and DMZ services
    - Must work with CDN to provide end-to-end service proxying over IPv6 transport
  - IPv6 enable SPAM gateways and load balancers

Needs to be v4/v6



# The 2014 Expectations

- Government enterprises will need to IPv6-enable everything
  - Not just a network/transport issue
  - If you can’t shut off IPv4 --- You’re not done yet
- Equipment vendors have to step up now
  - If your product can’t work in only IPv6 -- You’re not done



PLEASE WAIT...
YOU HAVE REACHED THE END OF THE INTERNET.
SORRY FOR THE INCONVENIENCE.

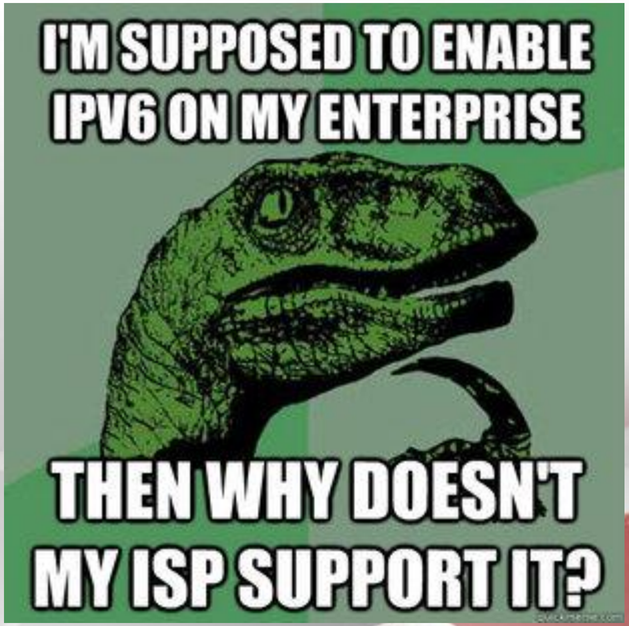
IPv6 LOADING...

# The 2014 Probable Realities

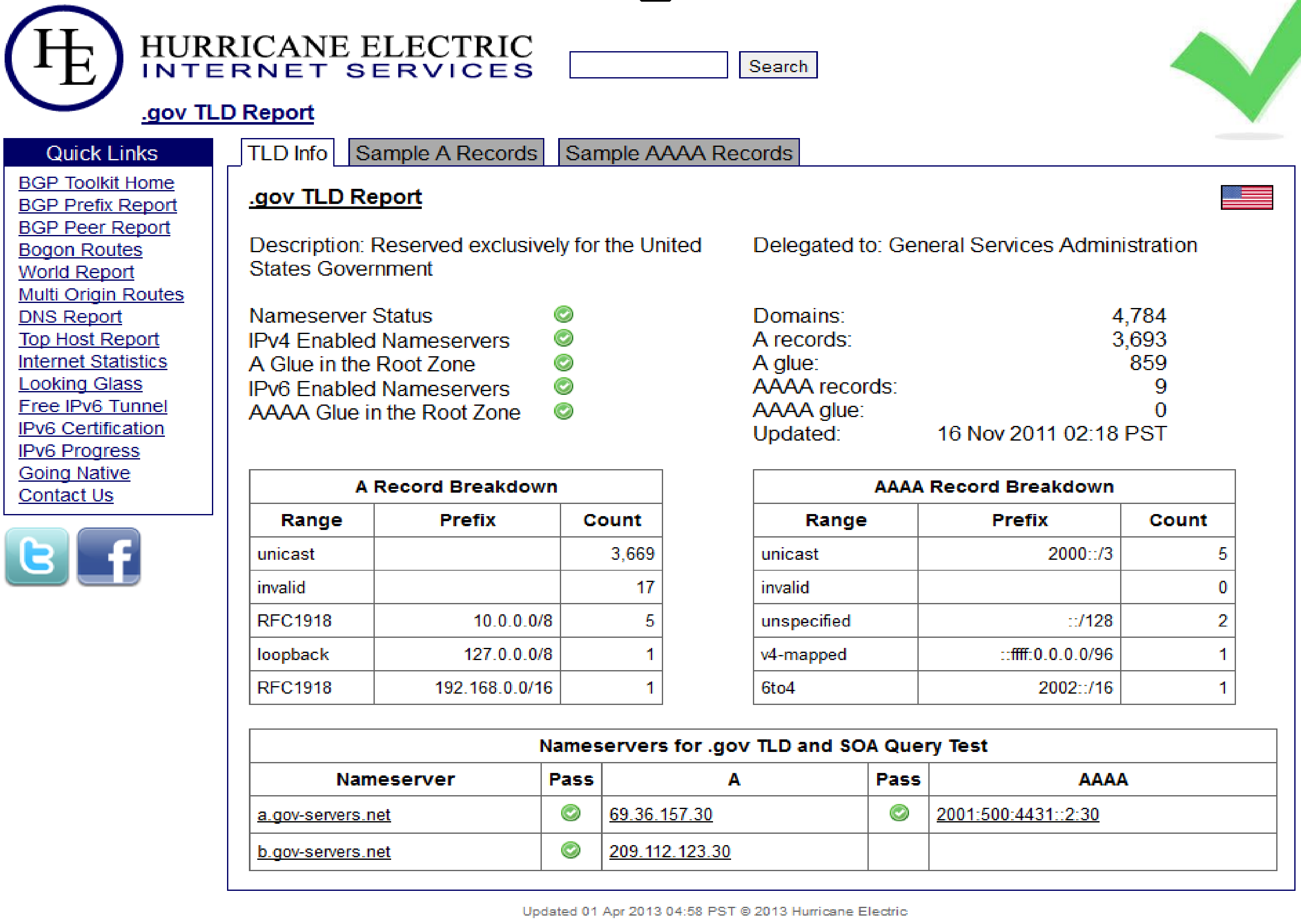
- Government enterprises will need to IPv6-enable most parts of their internal networks
  - Standard outbound services must be available over IPv6 like DNS, mail, HTTP/HTTPS
  - Network management will likely be acceptable over IPv4
  - Most inbound services must be available over IPv6 with exception of email (re: SPAM gateway issues)
- Internal network MUST have IPv6 working flawlessly
  - Windows will only use IPv6 if it has it

# ISP/Hosting Provider/CDN?

- Ask them the tough questions
- Hold their feet to the fire
  - Make IPv6-enablement part of an SLA
- Does your web/Internet provider support IPv6 now?


I'M SUPPOSED TO ENABLE IPV6 ON MY ENTERPRISE
THEN WHY DOESN'T MY ISP SUPPORT IT?

# DNS IPv6 Glue - .gov



## .gov TLD Report

Description: Reserved exclusively for the United States Government

Delegated to: General Services Administration

| | |
|---|---|
| Nameserver Status | ✓ |
| IPv4 Enabled Nameservers | ✓ |
| A Glue in the Root Zone | ✓ |
| IPv6 Enabled Nameservers | ✓ |
| AAAA Glue in the Root Zone | ✓ |

| | |
|---|---|
| Domains: | 4,784 |
| A records: | 3,693 |
| A glue: | 859 |
| AAAA records: | 9 |
| AAAA glue: | 0 |
| Updated: | 16 Nov 2011 02:18 PST |

**A Record Breakdown**

| Range | Prefix | Count |
|---|---|---|
| unicast | | 3,669 |
| invalid | | 17 |
| RFC1918 | 10.0.0.0/8 | 5 |
| loopback | 127.0.0.0/8 | 1 |
| RFC1918 | 192.168.0.0/16 | 1 |

**AAAA Record Breakdown**

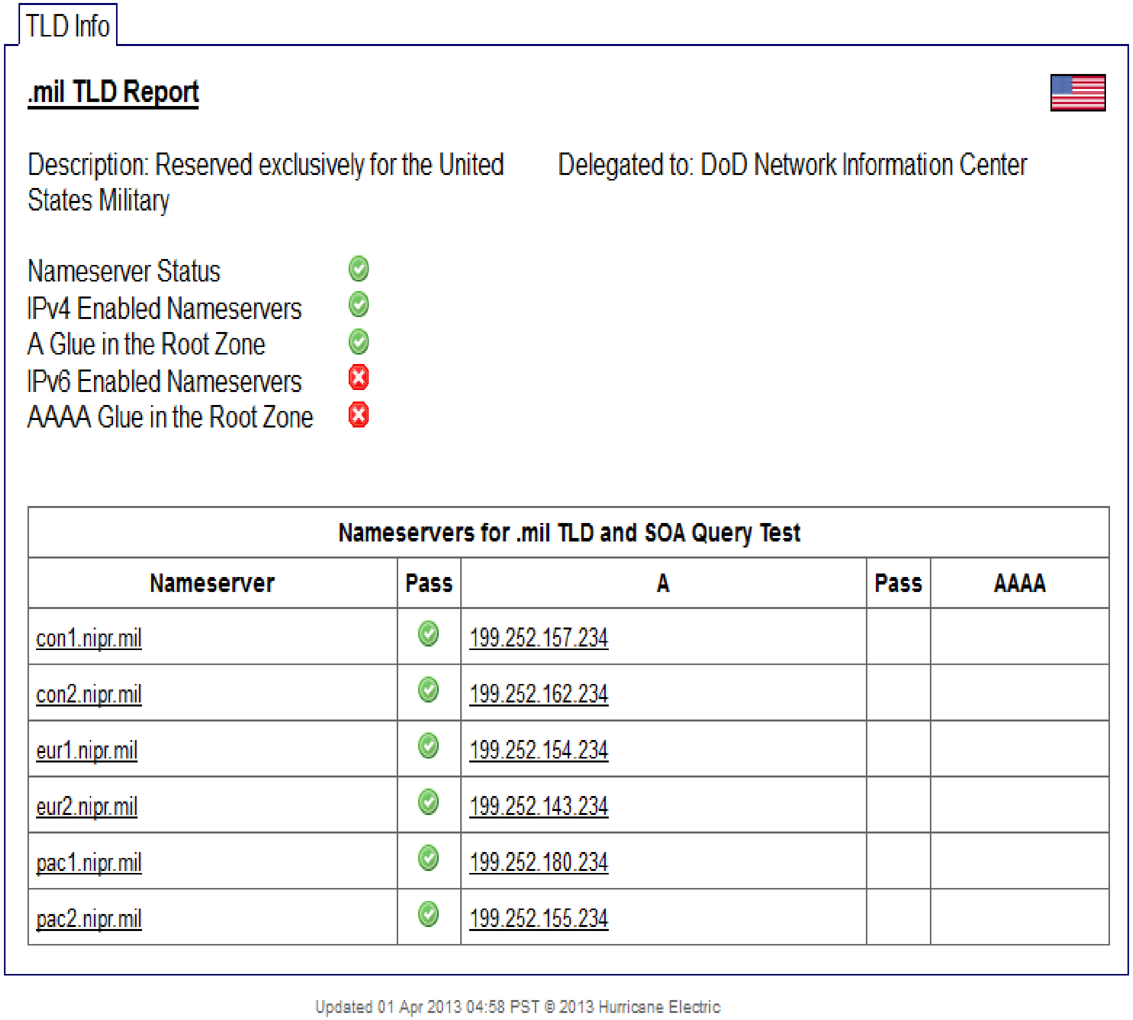
| Range | Prefix | Count |
|---|---|---|
| unicast | 2000::/3 | 5 |
| invalid | | 0 |
| unspecified | ::/128 | 2 |
| v4-mapped | ::ffff:0.0.0.0/96 | 1 |
| 6to4 | 2002::/16 | 1 |

**Nameservers for .gov TLD and SOA Query Test**

| Nameserver | Pass | A | Pass | AAAA |
|---|---|---|---|---|
| a.gov-servers.net | ✓ | 69.36.157.30 | ✓ | 2001:500:4431::2:30 |
| b.gov-servers.net | ✓ | 209.112.123.30 | | |

Updated 01 Apr 2013 04:58 PST © 2013 Hurricane Electric

# DNS IPv6 Glue - .mil



TLD Info

**.mil TLD Report**

Description: Reserved exclusively for the United States Military

Delegated to: DoD Network Information Center

| | |
|---|---|
| Nameserver Status | ✓ |
| IPv4 Enabled Nameservers | ✓ |
| A Glue in the Root Zone | ✓ |
| IPv6 Enabled Nameservers | ✗ |
| AAAA Glue in the Root Zone | ✗ |

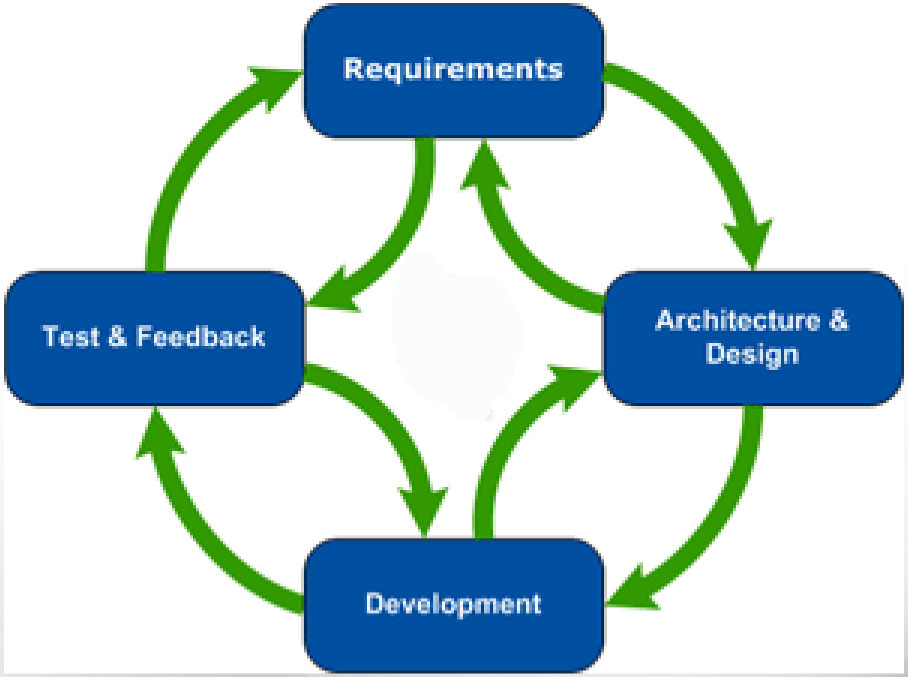
**Nameservers for .mil TLD and SOA Query Test**

| Nameserver | Pass | A | Pass | AAAA |
|---|---|---|---|---|
| con1.nipr.mil | ✓ | 199.252.157.234 | | |
| con2.nipr.mil | ✓ | 199.252.162.234 | | |
| eur1.nipr.mil | ✓ | 199.252.154.234 | | |
| eur2.nipr.mil | ✓ | 199.252.143.234 | | |
| pac1.nipr.mil | ✓ | 199.252.180.234 | | |
| pac2.nipr.mil | ✓ | 199.252.155.234 | | |

Updated 01 Apr 2013 04:58 PST © 2013 Hurricane Electric

# Internal IPv6 Deployment Lessons

- Conduct a deep research phase to ensure all server and network components have **IPv6-parity** to IPv4
  - Think "agile"
  - Requirements, Architect, Develop, Test, and back again



# Internal IPv6 Deployment Lessons

1. Training is paramount – Everyone needs it
2. IPv6 security – must be planned, documented and implemented
3. Enforce your IPv6 addressing plan when implementation is underway
   - Re-design if it doesn't work – implement if it does
4. Have detailed IPv6 design, implementation, and "As Built" documentation upon competition

# What does IPv6 touch on an Enterprise?

- DNS
- DHCP
- Active Directory
- Email
- Host-based security
- Firewalls
- Routers
- Switches
- Chat (re: Lync/Jabber)
- Remote Access/VPN
- Site-to-Site VPN
- VoIP
- QoS policies
- Custom applications
- Mobile devices
- Workstations
- IPS/IDS
- Virtual Desktops
- Cloud provisioning
- Fabric switching
- IPAM
- Multicast
- AAA

# IPv6 Deployment Best Practices, Technical Issues and Workarounds

- Virtual Server Issues/Windows Server Issues
- Routing/Switching
- BGP Peering
- Firewalls
- Virtual Desktops
- DHCPv6 vs. SLAAC vs. Static
- IPAMs
- Custom Applications

# Virtual Server / Windows Server Issues

- When cloning a Windows Server (re: Server 2008 R2) you must remember to delete the values of the GUID and IAID in the registry or you'll have a huge IPv6 address conflict problem
  - DUID & UUID is used for DHCPv6 leasing

Delete value (not key) in:

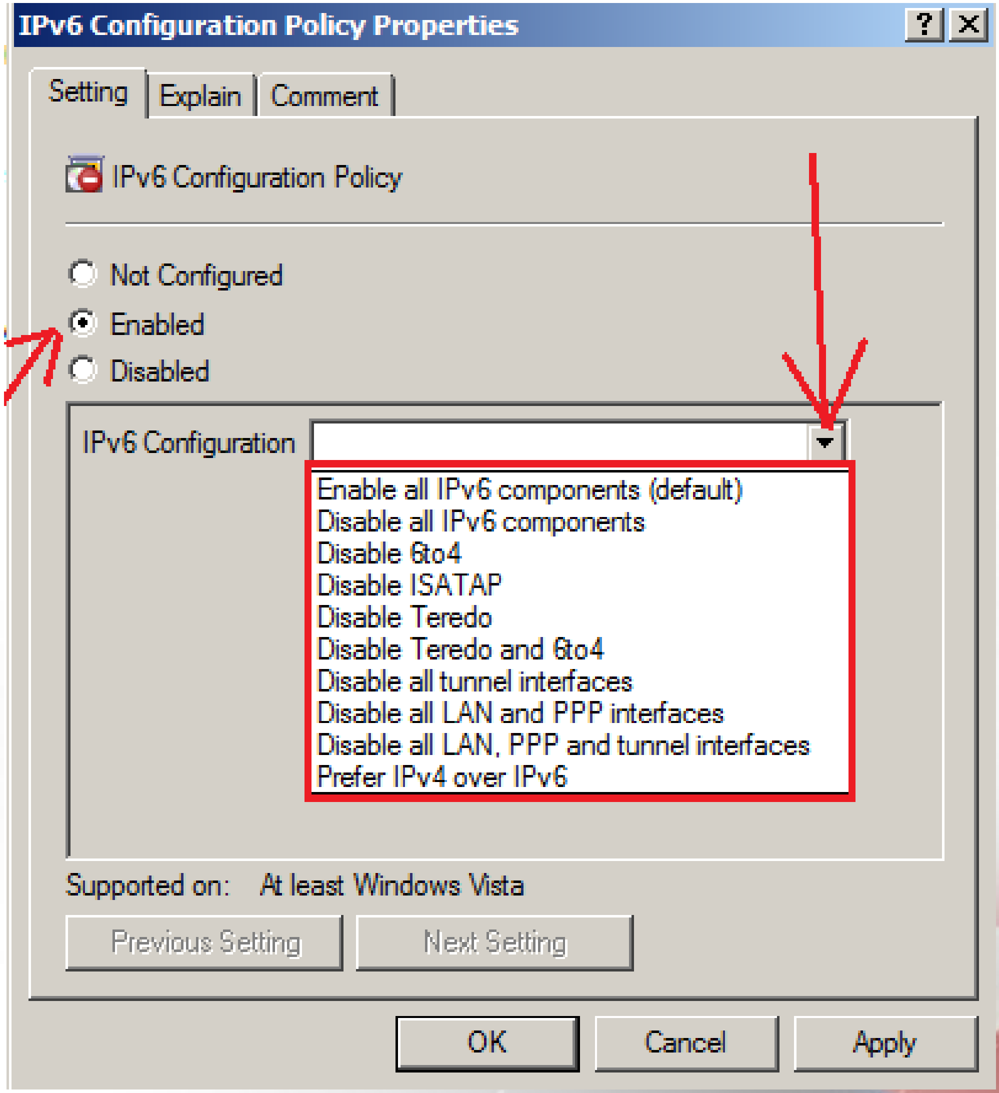
- **`HKLM>CurrentControlSet>services>TCPIP6>Parameters>Dhcpv6DUID`**
- **`HKLM>CurrentControlSet>services>TCPIP6>Parameters>Interfaces>{INT}>Dhcpv6Iaid`**

# Virtual Server / Windows Server Issues, cont

- If disabling IPv6 (but be warned): **HKLM>CurrentControlSet>services>TCPIP6 >Parameters>DisabledComponents=0xFF**
  - Disabling could cause IPv4 LDAP problems (see Microsoft KB 816103)
- If using IPv6 enable it without tunneling: **HKLM>CurrentControlSet>services>TCPIP6 >Parameters>DisabledComponents=0x1**
  - Except on the Direct Access server – **all tunnel interfaces required**
- If you need to prefer IPv4 over IPv6: **HKLM>CurrentControlSet>services>TCPIP6 >Parameters>DisabledComponents=0x20**

# Virtual Server / Windows Server Issues, cont

[http://social.technet.microsoft.com/wiki/contents/articles/5927.how-to-disable-ipv6-through-group-policy.aspx](http://social.technet.microsoft.com/wiki/contents/articles/5927.how-to-disable-ipv6-through-group-policy.aspx)



IPv6 Configuration Policy

○ Not Configured
● Enabled
○ Disabled

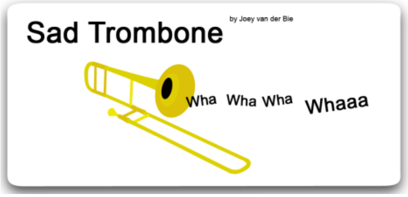
IPv6 Configuration:
- Enable all IPv6 components (default)
- Disable all IPv6 components
- Disable 6to4
- Disable ISATAP
- Disable Teredo
- Disable Teredo and 6to4
- Disable all tunnel interfaces
- Disable all LAN and PPP interfaces
- Disable all LAN, PPP and tunnel interfaces
- Prefer IPv4 over IPv6

Supported on: At least Windows Vista

# Windows Client & Server Issues

- When running Windows Server 2008, R2:
  - 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 Interoperability



- 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)

# Microsoft Exchange 2010 Issues

- 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

# VMWare IPv6 Default Gateway

- VMWare IP pools want a Global Unicast Address when configuring an IPv6 pool
  - Errors out when adding link-local address**
- VMWare management does not allow for a configured IPv6 link-local**

**Active VMware bug

# IPv6 Routing & Switching

- Host interface example:

```
interface GigabitEthernetX/X
standby version 2
standby 100 ipv6 FE80::1
standby 100 preempt
ipv6 address FE80::2 link-local
ipv6 address GENERAL::2:0:0:0:1/64
ipv6 nd prefix 2001:db8:1:2:: /64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 nd router-preference high
ipv6 nd ra interval 4 3
ipv6 dhcp relay destination 2001:db8:1:2:3:4:5:6
ipv6 mld limit 100
```

HSRPv2 w/ Link-Local

IPv6 General-Prefix

Disable SLAAC

DHCPv6 configs

Mitigate Rogue RAs

# IPv6 Routing & Switching, cont

- Be very intentional about point-to-point interfaces:

```
interface GigabitEthernetX/X
ipv6 address FE80:::1 link-local
ipv6 address GENERAL ::1:0:0:0:1/64
ipv6 enable
ipv6 nd ra suppress
no ipv6 redirects
no ipv6 unreachables
ipv6 dhcp relay destination 2001:db8:1:2:3:4:5:6
```

**Suppress RA for PtP links**

**Do not do IPv6 Redirect on PtP links**

**Do not do IPv6 Unreachables on PtP links**

**Must provide relays**

# IPv6 Routing & Switching, cont.

- ASR 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
- Use IPv6 Router Advertisement (RA) Guard on host facing switch interfaces:
  - **`ipv6 nd raguard`**

# Cisco OSPFv3 and Address Families

- With the later 15.x code on ISR and ASR routers OSPFv3 added new features:
  - OSPFv3 on VRF instances
  - Add IPv4 routes on the OSPFv3 process – can eliminate need for 2 routing protocols**
    - router ospfv3 1
      - address-family ipv4 unicast vrf XXX
        - » redistribute ospf 1
  - OSPFv3 authentication supports authentication and authentication + encryption
    - ospfv3 encryption ipsec spi 512 esp aes-cbc 256

# Cisco Nexus Switching

- When doing simple Layer-2 on Nexus switch interfaces with Fabric 2 modules you must disable Optimized Multicast Snooping or **ALL** IPv6 is blocked
  - `no ip igmp snooping optimised-multicast-flood`

# IPv6 BGP Peering Best Practice

- IPBCOP provided some great recommendations
  - http://www.ipbcop.org/drafts/bcop-ipv6-peering-and-transit/

1. Establish new IPv6-only peerings
2. Route filtering – follow your IPv4 practices here
3. Use tools:
   - Internet Routing Registry (IRR)
   - Register with a Peering DB
   - Use an IPAM
4. Use RPKI

# IPv6-only BGP Peerings

Forces transport over IPv6

```
router bgp 9999
     bgp log-neighbor-changes
     no bgp default ipv4-unicast
     neighbor 2001:db8::1 remote-as 1000
     neighbor 2001:db8::1 description IPv6
eBGP peer ISP
     neighbor 2001:db8::1 password 7 xxxx
     neighbor 2001:db8::1 update-source
Loopback0
```

# IPv6-only BGP Peerings

Network to advertise

Route-Map filters

```
 address-family ipv6
     network 2001:db8::/48
     neighbor 2001:db8::1 activate
     neighbor 2001:db8::1 next-hop-self
     neighbor 2001:db8::1 route-map AS-1000-Incoming in
   neighbor 2001:db8::1 route-map AS-1000-Outgoing out
     exit-address-family
```

# BGP and RPKI

- Think DNSSEC/PKI for BGP
- Consists of standard PKI for routing table updates
- Keeps you from killing the internet (re: Pakistan Telecom (AS 17557) adverting part of YouTube)
- If RPKI is not supported on your edge routers use BGP Origin Authentication
  - Cisco supports both

# BGP and RPKI – How to**

```
router bgp 9999
     bgp rpki server tcp 192.168.2.2 port 1029 refresh 600
     bgp rpki server tcp FEC0::1002 port 32002 refresh 600
     neighbor 2001:db8::1 send-community extended
     neighbor 2001:db8::1 announce rpki state
```

****Source: Cisco BGP—Origin AS Validation**

# BGP and RPKI – How to**

```
router bgp 1000
     address-family ipv4 unicast
     neighbor 10.0.102.1 route-map rtmap-PEX1-3 in
     bgp bestpath prefix-validate allow-invalid


route-map rtmap-PEX1-3 permit 10
     match rpki invalid
     set local-preference 50
```

****Source: Cisco BGP—Origin AS Validation**

# BGP and RPKI – How to**

```
route-map rtmap-PEX1-3 permit 20
     match rpki not-found
     set local-preference 100

route-map rtmap-PEX1-3 permit 30
     match rpki valid
     set local-preference 200

route-map rtmap-PEX1-3 permit 40
```

****Source: Cisco BGP—Origin AS Validation**

# INFOSEC Infrastructure Issues

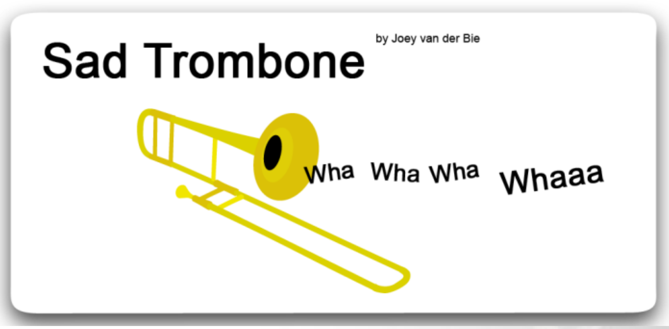
- McAfee Application Firewalls (v. 8.3.0) cannot do a number of functions over IPv6:
  - SNMPv3, SSH or client admin console
  - Only an Active/Standby HA configuration
  - Most proxy rules aren't supported (only HTTP, SSH and HTTPS have IPv6 capability)
- Most IDS/IPS tools cannot properly detect IPv6-based vulnerabilities per NIST IPv6 Secure Deployment and DoD IPv6 MO3 IA Guidance
  - Exception – Assure6 and CloudShield

# INFOSEC Infrastructure Issues, cont.

- Cisco ASA has many IPv6-related bugs in a recent code release v. 9
  - – OSPFv3 bugs caused failover to break
  - – OSPFv2 intermittent bugs
  - – Roll-back to a previous version that has no OSPFv3 support
    - 8.4.1
  - – Fixed release is “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
  - Use 802.1x to mitigate this issue



# 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
  - Juniper SA-6000 has no IPv6 capability at all today or anytime in the future
  - Cisco ASA and remote-access VPN solution works with IPv6 transport and provides DHCPv6 relay and RA support.
  - Microsoft’s DirectAccess
    - Fully IPv6 enabled – mostly native
    - Location and DNS must be reachable on IPv6
    - 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)
    - More secure and better control/management
  - SLAAC is used on printer VLANs as majority do not have DHCPv6 clients
    - Use 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 – my criteria:
  - Must have easily hardened platform (e.g. virtual or physical appliance)
  - 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 – all IPAM tools do not support Windows DHCPv6 server management/discovery yet

# IPv6 & Home-Grown Applications

- With every network application built you must test it in an IPv6-only environment – see IPv6 test & evaluation
- 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

- There was moderate success on US Gov't meeting 2012
  - 20%
- Meeting 2014 is going to require more work if you only used a CDN to translate
- 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?