Infoblox
CONTROL YOUR NETWORK

IPv6 deployment for Enterprise/Sysadmins

Paul Ebersman
pebersman@infoblox.com, @paul_ipv6

NAv6 Summit 2013, Denver, 17-19 Apr 2013

The only constant is change

‘Cause the IETF likes change…

- SLAAC vs DHCP
- Identifying users/machines
- Interface “magic”
- Org/political challenges

‘Cause the IETF likes change…

- App changes (esp. browsers)
- Policy changes (PTR)
- Security and “broadcast domain” changes
- IPSEC
- Continually evolving ecosystem

McDUID

DUID > Mac address

- **Mac address as ID is flawed:**
  - Not always unique
  - Can be altered
  - Multi-interface hosts confuse things
- **But it's works for a huge percentage of the internet**
- **DUID (DHCP Unique Identifier) is the replacement in IPv6**

What DUIDs do right

- One DUID per DHCP server or client
- One Identity Association (IA) per network interface on a host
- A host can DHCP for all interfaces via DUID/IA as unique key

Where DUIDs don’t work…

- Anyone using mac address for identification or filtering
- Anyone trying to correlate IPv4 and IPv6 to the same machine/user
- Persistent storage of DUID may cause surprises

But I do dual stack…

- How to correlate all addrs to same client:
  - draft in ietf: draft-ietf-dhc-dhcpv6-client-link-layer-addr-opt (headed to IESG)
  - circuit-id/remote-id work as with DHCPv4

Happy Eyeballs

IPv6. Yes. Have some.

- **Original plan: Always use IPv6/AAAA if available**
- **Result: poor user experience (long timeouts, use of slower links, etc.)**

Err… We meant Happy…

- Next attempt was to specify draft/RFC
- “But that doubles DNS traffic”…
- And OS and browser folks both dived on it

Hence “Hampering Eyeballs”

- **Testing by Geoff Huston (**https://labs.ripe.net/Members/emileaben/hampered-eyeballs**)**
- **Problems with browsers**
- ***Lots*** **of problems with OS X**
- **Windows trying to fix at network layer…**

How do it know?

Source/Destination Address

- Multiple interfaces w/ multiple addrs
- Multiple prefixes
- Dual stack…
- How to choose…
- RFC 6724 (formerly RFC 3484)

RFC 6724 (was 3484)

- Types of addrs:
  - IPv6: GUA, ULA, Link Local, privacy
  - IPv4: public, APIPA, 1918
- Some better than others
  - Consider scope, type, prefix length
  - Avoid deprecated
- Allow local policy overrides

Debugging will be fun

- Decisions time/context sensitive
- How to train staff and users
- Local tools to dump all info
- Packet sniffers?

Who owns what

Turf wars

- Who assigns IP addrs
- Who owns DHCP servers
- Who owns DNS
- Who owns routers/Ras
- Who supports OS/apps

Apps

We'll make up our own darned minds

- OS makes decisions on DNS lookups and using v4 vs v6
- Browsers and other apps do own DNS lookups and picking of v4 vs v6
- How to debug…

Reverse/PTR goo

How did we do it IPv4

- By hand (ow)
- Scripts
- $GENERATE
- IPAM

How would that work for IPv6

- A single subnet is a /64
- A /64 has 18 quintillion (4 bil x 4 bil) addrs
- A PTR record has 34 labels in IPv6
- Anyone got a computer with enough disk or RAM to hold one /64 zone file?

So what are we left with?

- Admit that PTRs are pointless
- Pre-populate (assuming FTL travel…)
- Pre-populate statics for routers & big servers
- As above plus DHCP server adding clients
- Lie on the fly (if not doing DNSSEC)

Security

The Myth

IPSEC in IPv6 is better than IPv4 because it was designed in and mandated.

And the reality

- RFCs said “MUST” support IPSEC (but softening to “SHOULD”…)
- Didn’t define “support”, let vendors do it
- Vendors shipped, didn’t enable
- No PKI…

ICMPv6

- **Required for:**
  - **DAD**
  - **Finding routers (RA/SLAAC)**
  - **Finding servers (DHCP)**
  - **PMTUD**
  - **Connectivity (echo request/response)**
  - **Network errors**

ICMPv6 Filtering

- **Filter it all and you don’t have a useful network**
- **ICMPv6 much more detailed/precise in types and functions**
- **RFC 4890 has excellent filtering practices**

And what don't we know yet

Default route

- Multiple default routes from RAs
- No more HSRP/VRRP! Maybe…
- But does this actually work?
- Not all OSs did the right thing (Fedora, ???)

What else will we find…

- AIX makes multiple AAAA/ip6.arpa queries with no working IPv6 stack
- Changing A/O/M bits… Interesting… (see draft-liu-bonica-dhcpv6-slaac-problem)
- And there will be more…

Questions?

Thank you!