IPv6 investigation within Informatics

George Ross
gdmr@inf.ed.ac.uk
Overview

- We enabled IPv6 on some of our subnets
- It basically just worked
- The End
- ... a bit more to it than that, of course
- Going to assume that you already know the IPv6 basics
- “Investigation” involving quite a lot of implementation
Why might we have wanted to implement IPv6?

- Make ourselves visible to IPv6-only ISPs
- In particular: web, ssh, OpenVPN
- Allow our users to speak to IPv6-only services elsewhere
- Machines are increasingly IPv6-enabled, and if we want to set some policy we have to have the support in the network.
Development project overview

- Project started in June 2015
- … much reading, preliminary testing, internal routing, core and edge switch configuration
- Global routing enabled in February 2016
- More testing, roll-out carefully staged
- All managed staff/PG and server subnets enabled by October 2016
- 10 weeks actual effort, spread over 16 elapsed months

Network

• We manage our own network (routing, switches, etc.), which made things a lot easier.
• Core uses ProCurve (now Aruba) 54xx and 3800 switches
• OSPFv3 on selected subnets
• BIRD on Linux routers
• Router Advertisement
• RA-guard on all untrusted network ports
• Biggest problem: old switches, which were missing some features or implemented some SNMP OIDs differently.
Addressing

- Everything already has a link-local address
- Most machines acquire a MAC-based SLAAC-style global IPv6 address
- We already have MAC addresses in lcfg, so it’s easy to generate DNS entries for these
- (IPv6-enabled) Client subnets: always generate both forward and reverse entries for everything which has an IPv4 address on the subnet
- Server subnets: only reverse entries by default, but managers can easily add forward entries as required
- Mechanism in place to give machines specific addresses, and add these to DNS
- 4866 A RRs, 601 AAAA RRs (excluding dhcp-*)
- (extractBySubnet and makeDNSv6 in the latest makeDNS package in lcfg svn)
- Some machines prefer to use privacy addresses (RFC4941)
Address use auditing

- We use arpwatch for IPv4
- Decided on addrwatch for IPv6
- Doesn’t send emails (so we’re actually now using both for IPv4)
- Logs all ARP and ND, rather than trying to keep a “current mapping”
- Logs are copious, so we consolidate them nightly
- Address-search tools enhanced to use both
iptables

- lcfg-iptables already had IPv6 support
- Some rule fragment-files were IPv4-only
- Rule-generating scripts needed to be told how to handle IPv6
- We now automatically handle edge-holes where a DNS name has an AAAA RR, just as we do for IPv4 A RRs
- At last count we had 5379 IPv4 rules and 545 IPv6 rules
Linux summary

- Surprisingly few problems
- Most things just worked
- IPv6 is preferred over IPv4 where possible (RFC6724)
- We didn’t have to make any gai.conf changes for IPv6
- ssh and svn need the -4 flag to force IPv4 for a few cases
- No user feedback at all, so presumably it hasn’t broken anything for them
Windows and Macs

- We didn’t really try these in earnest
- Initial tests with the Windows 7 managed desktop showed some IPv4 DHCP oddities when IPv6 was enabled on the subnet
- Might be fixed with Windows 10, but we haven’t tried that
- Meantime, we have all of our Windows managed desktops on their own non-IPv6 subnets
- Macs appear to just work
OpenVPN

• Our test, DR and AT service endpoints are handing out IPv6 tunnel addresses alongside IPv4
• Won’t be routed through unless client-end configuration has it enabled
• … but works perfectly in tests
• IPv6 endpoint addresses work too
• Unfortunately, dual-stack endpoints don’t appear to work, even on SL7
Access control

- **BEWARE!**
- Some systems (e.g. ProCurve / Aruba switches) allow free access from IPv6 addresses unless an IPv6 access control list is explicitly provided.
- Others default to closed unless IPv6 access is explicitly enabled (much more sensible!)
- If you advertise an IPv6 address, machines out there will expect to be able to use it just as they would your IPv4 address.
- Moral of the story: check what your applications really do.
- (That’s why we don’t automatically add forward IPv6 DNS entries for server subnets)
Other issues

• Address-based authentication to some sites (e.g. IEEExplore) broke until IS got the University’s IPv6 block added to the necessary lists

• Our central-firewall settings disappeared after an upgrade (IPv6 is now on the checklist)
Where next?

- Will enable IPv6 for the student labs after we return to Appleton Tower (400+ more machines)
- Need to look at DHCPv6
- Edge-switch upgrade for the Forum, which will enable RA-guard throughout
- Roll out to self-managed subnets
Summary

• For managed Linux machines within Informatics, IPv6 is now as well supported as IPv4

• You may already be using it, even if you don’t mean to (so turn on RA-guard everywhere, just in case)

• When buying, make sure you specify “proper” IPv6 support now, even if you don’t intend using it immediately. Old models may have issues.

• Check your access control lists!