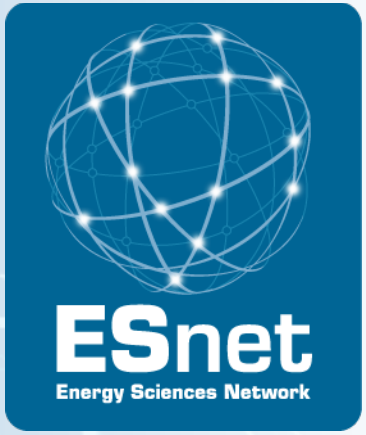


State of R&E IPv6 Deployment: Successes and Setbacks

Michael Sinatra, Network Engineer

ESnet Network Engineering Group

ARIN 29

Vancouver, BC

April 23, 2012

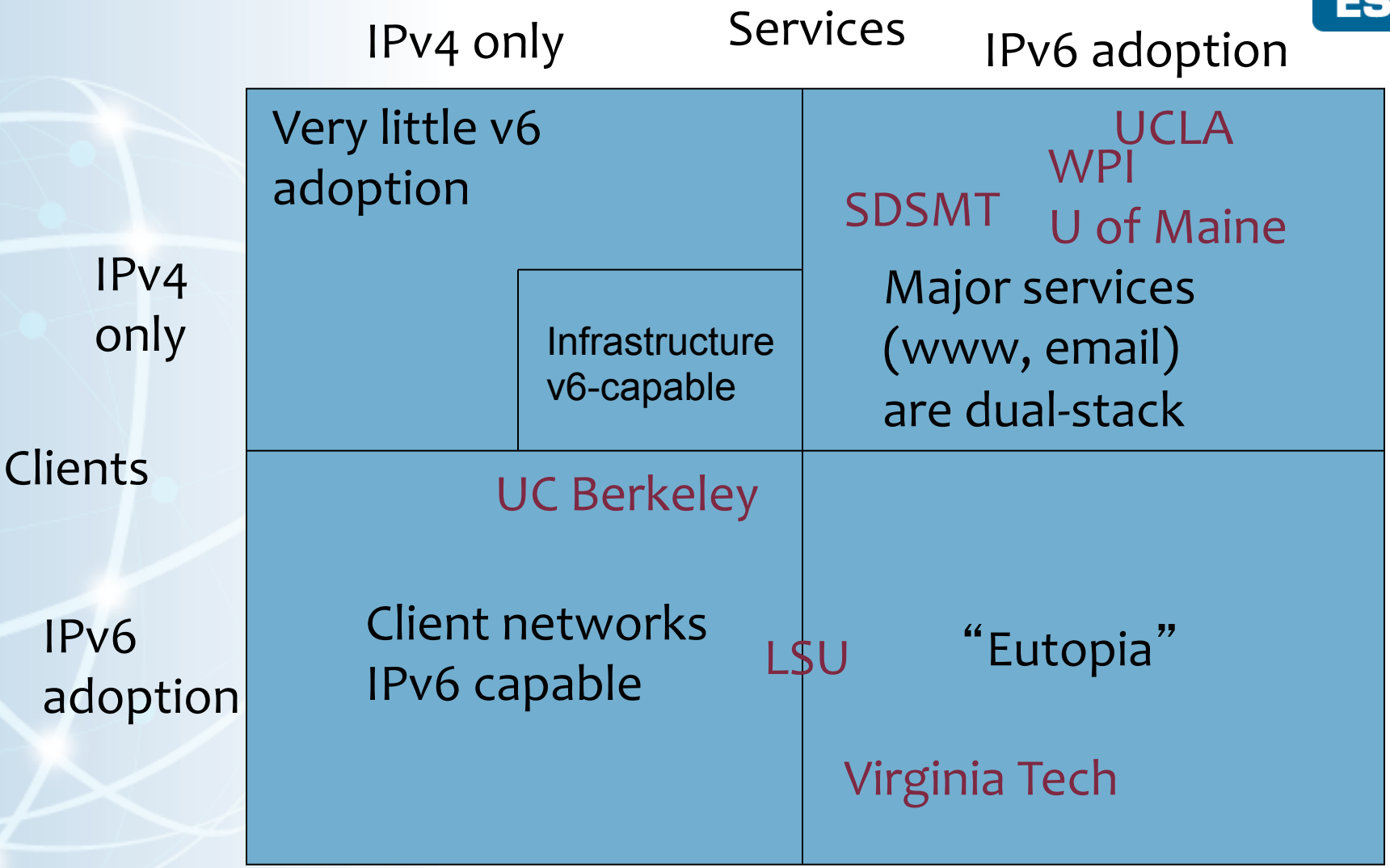
Overview

- Background
- What's right with IPv6 adoption in EDU and GOV?
- What's wrong with IPv6 adoption in EDU and GOV?
- Why is this happening?
- What am I doing to fix it?

Background: Different Models

- EDUs have different models for network support.
  - Model I: Centralized network (and security) management. Possibly border firewalls and security policy.
  - Model II: (Mostly) centralized network management, security generally decentralized (departmental firewalls or virtual contexts).
  - Model III: Completely decentralized. Central network group is backbone ISP for the rest of the enterprise.
- GOV models (mainly national labs)
  - Model I: Open network, very little (if any) classified info.
  - Model II: Different layers of security between classified and non-classified networks and visitor nets. (Red/Yellow/Green)
- In both cases, Model II (ironically) can be the best for v6 uptake.

EDU IPv6 deployment matrix



Background: GOV mandates

- September 30, 2012: All public facing services must be natively dual-stack (no tunnels but proxies are okay). Some agencies are interpreting this to mean “email and www,” but it really refers to *all* public-facing sites.
- September 30, 2014: All backed systems in support of all public services must be natively dual-stack (no more proxies!).

GOV success stories

- Veterans Administration has been very aggressive in deploying *and* evangelizing IPv6 and is actively assisting other agencies.
- DREN has been a big success. Now bills itself as an "IPv6 network with legacy IPv4 support."
- IRS (the *IRS??*) has a comprehensive lessons-learned site and even came up with a (sort of) witty acronym: GEEKV6.
- National Labs: Plugging forward with the mandates; some doing better than others.

EDU Success Stories

- Virginia Tech: Eyeball success
- UCLA: Public-facing service success (for a Model III)
- UC Berkeley: Wireless eyeballs
- SDSMT, WPI, Maine

So what's the problem?

- GOV and EDU CIOs very concerned about security.
  - Generally paramount on their radar.
  - They hear that IPv6 creates more security problems (wrong).
  - They hear that their IDSes and Firewalls don't support IPv6 (or don't do it as well as IPv4). (Probably right.)
  - GOV CIOs being pushed by mandates; EDU CIOs not.
- GOV and EDU CIOs also enamored with the Cloud.
  - Need to reduce costs; looking to outsource.
  - Seem to understand that the network is very important for network-based services, but seem to take it for granted.
  - Network is a substrate that just works. It's mature and basically complete. Now we need to worry about "services above the network."

So what's the problem?

- Results: While EDUs were initially on the forefront of IPv6 deployment, things have stagnated somewhat.
- Internet2 announced with great fanfare a "cloud" agreement with Box (formerly box.net). No IPv6 support.
- → This is an organization that has been giving IPv6 workshops for more than 10 years! (I attended my first in February 2002.)
- Cool new SSH replacement/overlay called mosh. Works on bad, high-latency connections! Automatically reconnects! Doesn't support IPv6! (But they are working on it…)
- IPv6 still an afterthought in many cases.
- Not much movement on my matrix slide or on Mark Prior's IPv6 Survey website.

Dang, there's still a lot of red in here!

EDU Organization

- Central networking group is the ISP for both the students/faculty and the Enterprise.
- IPv6 is a “network problem.” Systems and (especially applications people don’t need to pay attention.
- Network often funded differently than central systems and applications. No incentive for IPv6 beyond the network.
- Complacency: “Wow! I'm at NYU so I think we have a block of ipv4 addresses big enough to last till about 202012.” –user johnmcdonnell on reddit thread as to why mosh doesn’t yet support IPv6 (yet another example of complacency!). **Note! This user appears to be a grad student and does not represent the views of the central IT department.** But he does appear to be a tech-savvy user.

EDU organization

- In other words, outside of the central networking group, there is little interest in IPv6.
- And moreover, you can't trust those network engineers! Besides, they're mean and they don't like us. They all hang out together and laugh at us systems people as we walk by.
- CIOs not focused on fixing a "substrate" they don't see as broken.
- See more risks to deploying IPv6 than to not deploying IPv6.

Technical issues

- Before it was support for IPv6 at all. Now it's lack of feature parity, and that's still biting us!
  - Load balancers that throw away IPv6 MTU messages.
  - Firewalls and IDSes.
  - Management tools (or lack thereof).
  - We're getting close, but there are a few final pieces that need to go into place.
- What about our own tools?

Technical issues

- Don't you hate seeing this?
- if ($_=~ /(\d+)\.(\d+)\.(\d+)\.(\d+)/) {
- I go through and spray all of our scripts with "IPv4 assumption bug repellent spray."
- There are libraries that do this for you and they work with IPv4 AND IPv6!!
  - perl: Net::IP and NetAddr::IP
  - python: IPy
  - Note that Postgresql has a data type 'inet' that magically handles both IPv4 and IPv6 addresses. No fuss, no muss!
- The tools are there, but we need to change the way we think!

So what am I doing?

- Educate CIOs and managers. Since they are motivated by risk, explain the risks of *not* deploying IPv6 to balance the risks they already know about.
  - Security (yes, security): Unknown tunnels, NAT obfuscation, etc.
  - Eyeball networks needing access to IPv6-only resources. (Scientific instruments in Asia, etc.)
  - Access to your information networks. (Wealthy donors in Asia, students in developing countries, etc.)
  - Even if you think you have a lot of address space, your probably don't. (Mobile/wireless growth, HPCCs, more and more networked devices.)

So what am I doing?

- Train users and sysadmins:
  - Putting something on the network means dual-stacking it *from day one.*
  - Dev and QA nets must be IPv6 as well as production.
  - New services must be developed with IPv6 *from day one.*
  - IPv6 cannot be an afterthought.
  - → Provide examples of pain and additional costs of grafting IPv6 onto a service that didn't have it from the beginning. Unfortunately, I have many in my bag of tricks.

References

- http://www.mrp.net/IPv6_Survey.html
- http://www.reddit.com/r/programming/comments/s2hpx/mosh_ssh_for_2012/
  - Another good quote from the above: “It's hardly for 2012 when it doesn't support IPv6 yet.”