IPv6 Deployment at the University of Pennsylvania

Jorj Bauer and Shumon Huque

University of Pennsylvania

Educause Mid-Atlantic Regional Conference, Philadelphia, PA

January 8th, 2009

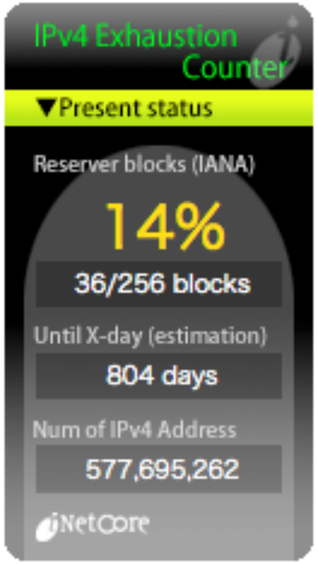
Outline

- Why you should consider IPv6 today
- IPv6 Tutorial
- IPv6 Deployment at Penn
- Future plans/challenges/issues

Why you should consider IPv6

Projected IANA Unallocated Address Pool Exhaustion: 01-Mar-2011

Projected RIR Unallocated Address Pool Exhaustion: 29-Apr-2012



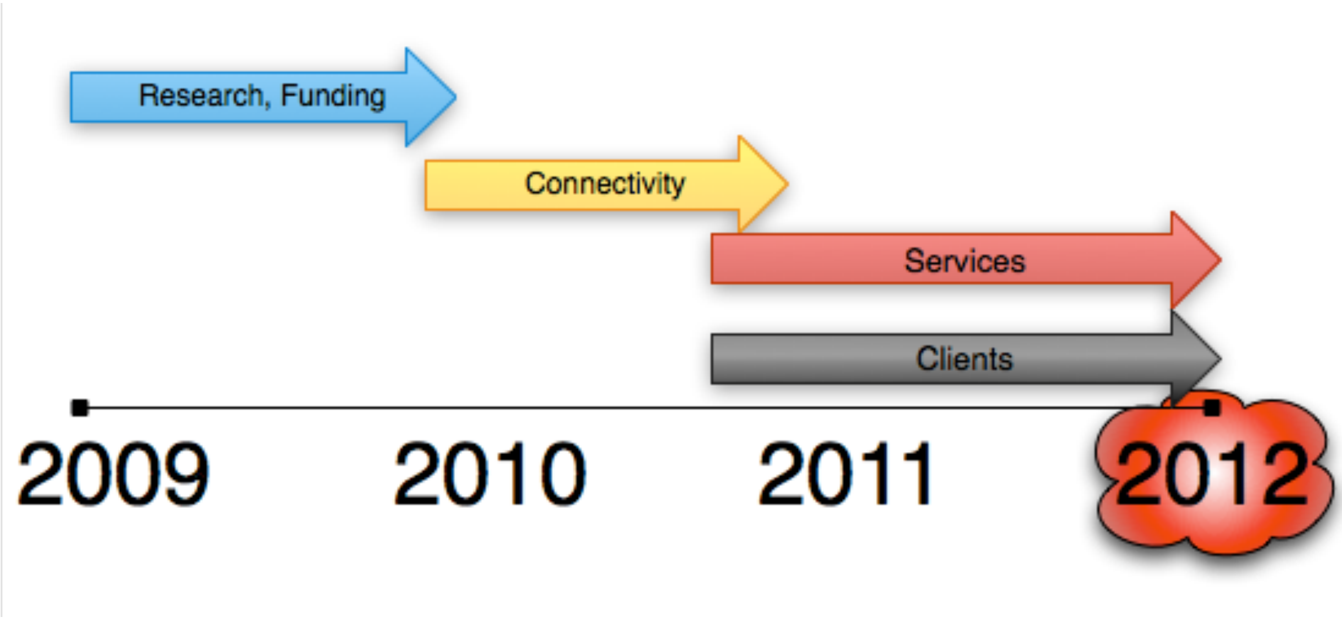
http://ipv4.potaroo.net/

What will happen?

- Uncertain at this point
- Orderly dual-stack transition (probably not)
- Mad rush/panic for remaining IPv4 space
- More and more layers of NAT
- Balkanization of Internet
  - Pockets of IPv4-only, IPv6-only, and dual stack
  - IPv4-only hosts may not be able to communicate with new IPv6-only services/hosts coming online

Why you should consider IPv6

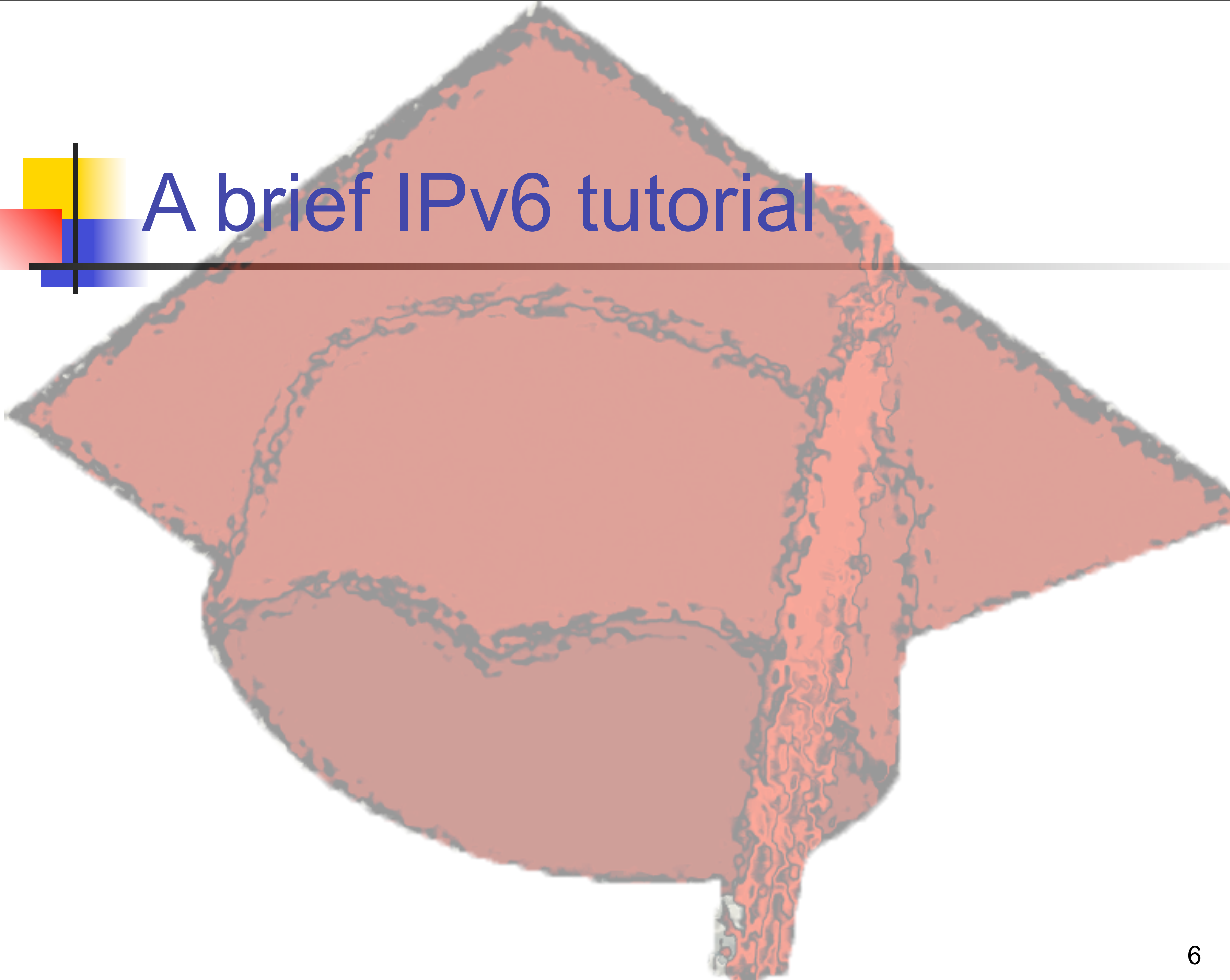
- How long will it take you to deploy IPv6?
- When do you need to start planning?



Projected IANA Unallocated Address Pool Exhaustion: 01-Mar-2011

Projected RIR Unallocated Address Pool Exhaustion: 29-Apr-2012

A brief IPv6 tutorial



IPv6 History

- Development started in 1993, RFC 1550 “IP: Next Generation (IPng) White Paper Solicitation”

IPv6: What happened to IPv5?

- RFC 1190, 1819: The Internet Streaming Protocol v2 (SPv2)
  - Experimental protocol for voice/video transmission
  - Not called IPv5, but used version number 5 in its IP headers

IPv6 Addresses

- IPv4 address: 192.168.7.13
- IPv6 address: 2001:DB8:1902:7B2::905B:FE01
  - Leading zeroes may be dropped, and intermediate zeroes may be abbreviated
    - 2001:***<u>0</u>***DB8:1902:***<u>0</u>***7B2:***<u>0000:0000</u>***:905B:FE01

IPv6: Client Addressing

- IPv4 hosts typically have two addresses
- IPv4 either uses static assignment or dynamic DHCP/BOOTP assignment
  - Requires intelligent configuration of the workstation, or you’re at the mercy of the OS vendor’s default configuration

IPv6: Client Addressing

- IPv6 hosts may have many addresses
- IPv6 has SLAAC (**S**tate**L**ess **A**ddress **A**uto **C**onfiguration)
  - The link-local address is used to find the local router
  - An address is automatically generated from the router's advertised *prefix* and the *interface ID*

IPv6: Client Addressing

- IPv6 also has a DHCPv6 protocol
  - Fairly young; devised in mid-2003
  - This allows *stateless* and *stateful* configs
    - *Stateful* is similar to current DHCP
    - *Stateless* negotiates configuration information (e.g. DNS) but not IP addresses (uses SLAAC)
- Of course, static addressing is also possible (recommended for servers)

IPv6 infrastructure: DNS

- With 128-bit addressing, IPv6 is heavily reliant on DNS
  - IPv4 address records are "*A*" records
  - IPv6 address records are "*AAAA*" ("*Quad-A*") records

IPv6: Application Support

- IPv6 is programmatically different than IPv4
  - This means IPv4 applications/services have to be ported to IPv6 manually and may require application-specific configuration

IPv6: Application Support

- For example: Firefox supports IPv6, but FF2 disabled it by default
- To check yours, go to **about:config**
  - Set **network.dns.disableIPv6** to **false**

IPv6 Deployment at Penn

GigaPoP deployment

- Penn operates an Internet2 GigaPoP called MAGPI – http://www.magpi.net/
- Suitable place for trial IPv6 deployment
- Started around 2002

GigaPoP deployment

- Obtained address space (Internet2)
- Developed addressing plan
- Routing: IS-IS, BGP4
- Addr Assignment: stateless autoconfig
- Services:
  - DNS, NTP, SSH, Web
  - Multicast (work in progress)

University Deployment

- Production deployment began 2005
- IPv6 ready network gear
- Address Space (delegated by MAGPI)
- Development of Addressing Plan
  - http://www.huque.com/~shuque/doc/penn-ipv6-plan.html
  - Good for now, new plan will evolve

University Deployment

- Routing protocols: IS-IS, BGP4
- Infrastructure deployment status:
  - Border routers, core routers, a few distributed routers
  - Several end-user & server subnets
  - Not entire campus yet (but planning)
  - Engineering School – all client subnets (roughly 18% of clients are capable)

University Deployment

- Address Assignment/Management:
  - Servers: static addreses
  - Other endstations:
    - Stateless Autoconfig (mainly)
    - DHCPv6 (planning)

University Deployment

- Campus wide Services done:
  - DNS, NTP, SSH
  - Jabber
  - DNS Management system (homegrown)
- Services posing problems:
  - Web (impediment: Akamai)
  - E-mail (impediment: Message Labs/ Postini)

Future Plans

- Enable more services:
  - Web, Email, Kerberos, LDAP
- Portable Address Space from ARIN
- Turn on IPv6 routing everywhere
- IPv6 Multicast Routing

Future Plans

- Track New Developments in IPv6
  - SHIM6
  - Various Locator-ID split schemes
  - Transition mechanisms:
    - NAT64, DNS64

The Darker Side of IPv6

The Darker Side of IPv6

- You should think about IPv6 today, whether you deploy it or not
  - Migration technologies may be preinstalled and activated on your clients without your knowledge…

Food for Thought: Tunneling

- Clients that don't have direct IPv6 connectivity can still use IPv6 via tunnels
  - 6to4 requires the client to have a public IP address (no NAT)
  - Teredo allows IPv6 tunneling over IPv4 UDP, even through NAT

Food for Thought: Tunneling

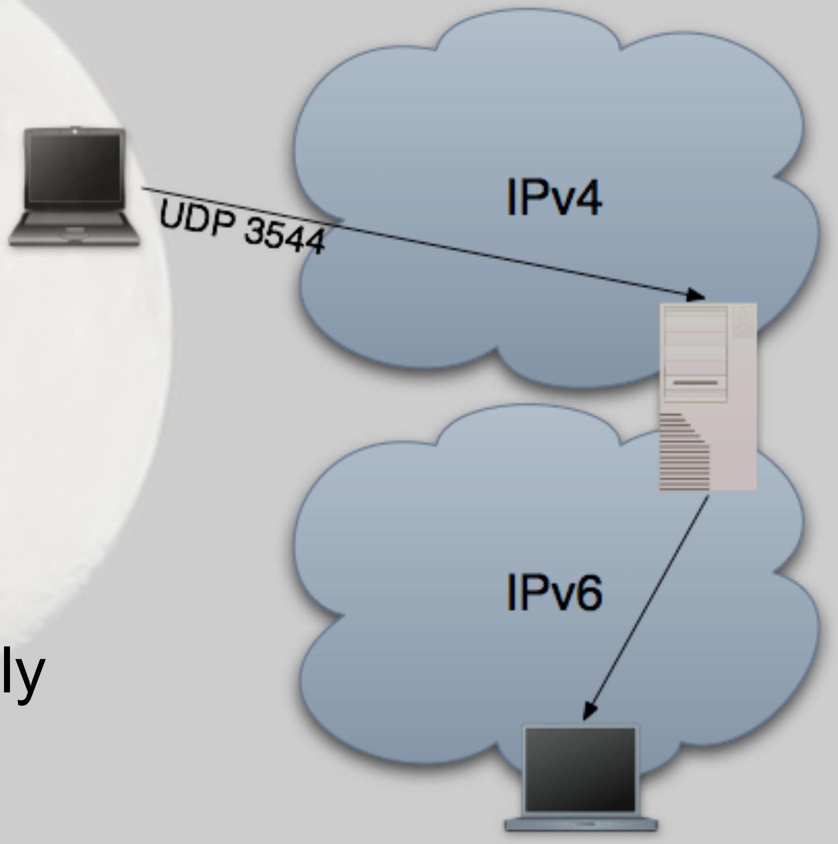
- Teredo was invented by Microsoft: RFC 4380
- Designed as a transitional mechanism for clients that were unable to use 6to4
- Teredo IP addresses use the global prefix 2001:0000::/32

Food for Thought: Tunneling

- In Windows Vista, Teredo is enabled by default
  - Microsoft uses this as part of *Remote Assistance*
  - This means that all Vista machines have a globally-addressable IPv6 tunnel

Food for Thought: Tunneling

How Teredo Works:



Teredo can bidirectionally circumvent your firewall

Food for Thought: Tunneling

- Microsoft band-aided this situation with local firewalling and access control
  - The IPv6 stack, and Teredo driver, are still reachable from the internet (even if the packets are dropped)
  - Outbound IPv6 traffic still flows
    - For example, you can *ping6* from a Vista workstation

Food for Thought: Tunneling

- All IPv6 traffic running through Teredo is passing through proxy servers that are out of your control, bypassing your firewall bidirectionally
  - Traffic from a Vista Teredo/6to4 client at Penn destined for another Penn machine over IPv6, travels from Penn to Microsoft and back

Food for Thought: Tunneling

- Symantec picked up on this and published a whitepaper on the security implications of Teredo
- This progressed to an IETF draft on tunneling protocol security implications
  - http://snipurl.com/teredo

Food for Thought: Tunneling

- Teredo and 6to4 are both disabled if the client has a native IPv6 address
  - Enabling IPv6 natively in the School of Engineering means that all of the Vista clients there use native IPv6, which can be monitored and controlled, rather than Teredo

And What If You Deploy?

- Tunnels are a useful and valid transition strategy
- Some other thoughts…

Food for Thought: Middleboxes

- Middleboxes
  - Firewalls, IDS, VPNs, Server Load Balancers …
  - Make sure these support IPv6 if necessary (and implement it properly!)

Food for Thought: Hardware

- Router support
  - Support for IPv6
  - Packet forwarding in hardware
- Switches
  - MLD snooping (for multicast)

Food for Thought: v6 addresses

- Hosts typically can have many addresses of many types:
  - Global, ULA, privacy, cryptographic, etc
- Port scanning
  - For attackers or defensive scanning
  - Blindly scanning entire range infeasible
  - See RFC 5157
    - http://www.ietf.org/rfc/rfc5157.txt

Food for Thought: Connectivity

- Some low end routers/NATs not dealing with IPv6
- Some broken DNS servers
- Apps not falling back to IPv4 if IPv6 doesn't work
- Apps attempting IPv6 connections but not having global IPv6 connectivity
- Improper address selection algorithms (see RFC 3484 and I-Ds on this topic)
- Poorer performance due to tunnelling and suboptimal routing
- Situation getting much better

Food for Thought: at Penn

- Rate limiting/bandwidth management
  - Penn does rate limiting by IP address for bandwidth management in its residential networks
  - Router configured to rate limit every /32 in a specified prefix to configured rate/burst
  - This scheme probably won’t work with IPv6

Feedback

- Questions, comments?
- Your experiences, successes, lessons?
- Also your non-experiences: why haven't you deployed or planned to deploy yet?

Contact Info:

jorj@isc.upenn.edu

shuque@isc.upenn.edu

IPv6 Resources

- IPv4 depletion and migration to IPv6:
  - http://www.internet2.edu/presentations/spring08/20080423-ipv4depletion-curran.pdf
- ARIN IPv6 Resolution
  - http://www.arin.net/v6/v6-resolution.html
- ARIN update
  - http://www.internet2.edu/presentations/jt2008jul/20080721-jimmerson.pdf

IPv6 Resources

- RFC 2460: Internet Protocol Version 6 Specification
  - http://www.ietf.org/rfc/rfc2460.txt
- RFC 4291: IP Version 6 Addressing Architecture
  - http://www.ietf.org/rfc/rfc4291.txt
- RFC 4861: Neighbor Discovery for IPv6
  - http://www.ietf.org/rfc/rfc4861.txt
- RFC 4862: IPv6 Stateless Address Autoconfiguration
  - http://www.ietf.org/rfc/rfc4862.txt

IPv6 Resources

- Internet2 IPv6 Working Group
  - http://ipv6.internet2.edu/
- Mid-Atlantic IPv6 Task Force
  - http://www.midatlanticv6tf.org/
- General IPv6 Information Website
  - http://www.ipv6.org/

IPv6 Resources

- RFC 3513: DHCPv6
  - http://www.ietf.org/rfc/rfc3513.txt
- RFC 3736: Stateless DHCPv6
  - http://www.ietf.org/rfc/rfc3736.txt
- RFC 3056: 6to4 tunnelling
  - http://www.ietf.org/rfc/rfc3056.txt
- RFC 4380: Teredo: tunnelling IPv6 over UDP through NATs
  - http://www.ietf.org/rfc/rfc4380.txt

IPv6 Resources

- Multihoming and scalable routing in IPv6
  - SHIM6
    - http://www.ietf.org/html.charters/shim6-charter.html
  - Routing Research Group
    - http://www.irtf.org/charter?gtype=rg&group=rrg

IPv6 Resources

- IPv6/IPv4 Transition and Co-existence mechanisms

IPv6 Resources

- RFC 5211: An Internet Transition Plan
  - http://www.ietf.org/rfc/rfc5211.txt
- Native IPv6 ISPs:
  - http://www.sixxs.net/faq/connectivity/?faq=native

Bonus Slides

Studies of IPv6 usage

- Many studies, by Google, Arbor, RIPE, and others …
- Google:
  - http://www.ietf.org/proceedings/08nov/slides/v6ops-4.pdf

Google study results

- Goal: how much usable IPv6 is available to ordinary users?
- Randomly picked out sample of google users
- 0.238% of sample have working IPv6 (and prefer it), 0.09% have broken IPv6
- Steadily increasing over time
- Type: 6to4 (68%), Native (29%), Teredo/other (3%)

Disaster Recovery

- If you have offsite DR plans, does your DR site support IPv6?
  - Penn uses SunGard; no immediate IPv6 plans that we know of, so this will affect us soon...

Comparative Deployment

- Mark Prior’s survey:
  - http://www.mrp.net/IPv6_Survey.html

Research and Education Network Members

Organisation (domain)	Web	Mail	DNS	NTP	XMPP
3ROX (Three Rivers Optical Exchange) (3rox.net)	SUCCESS	PARTIAL	0/1/3		
CENIC (Corporation for Education Network Initiatives in California) (cenic.org)	FAIL	FAIL	0/0/3	FAIL	
Florida LambdaRail, LLC (FLR) (flrnet.org)	FAIL	FAIL	0/0/2		
GPN (Great Plains Network) (greatplains.net)	FAIL	FAIL	0/0/4		
Indiana GigaPoP (indiana.gigapop.net)	SUCCESS	FAIL	0/2/3	FAIL	
KanREN (Kansas Research and Education Network) (kanren.net)	SUCCESS	SUCCESS	2/2/2	SUCCESS	SUCCESS
LEARN (Lonestar Education and Research Network) (tx-learn.net)	FAIL	FAIL	0/0/2		
LONI (Louisiana Optical Network Initiative) (loni.org)	FAIL	FAIL	0/0/4		
MAGPI (magpi.net)	SUCCESS	FAIL	2/2/2	SUCCESS	SUCCESS

Excerpt of Universities section (web, mail, dns, ntp, xmpp)

University of California, Berkeley (berkeley.edu)	PARTIAL	FAIL	4/5/6	SUCCESS	
University of California, Davis (ucdavis.edu)	FAIL	FAIL	0/0/2	FAIL	
University of California, Irvine (uci.edu)	FAIL	FAIL	0/0/3		FAIL
University of California, Los Angeles (ucla.edu)	SUCCESS	SUCCESS	2/2/3	SUCCESS	SUCCESS
University of Oregon (uoregon.edu)	FAIL	FAIL	3/3/4	FAIL	
University of Pennsylvania (upenn.edu)	FAIL	FAIL	1/1/4	SUCCESS	SUCCESS