IPv6 at FNAL

(Where We Are; Where We are Going)

Phil DeMar

demar@fnal.gov

NLIT 2013

May 14, 2013

U.S. DEPARTMENT OF ENERGY

Fermilab

Outline

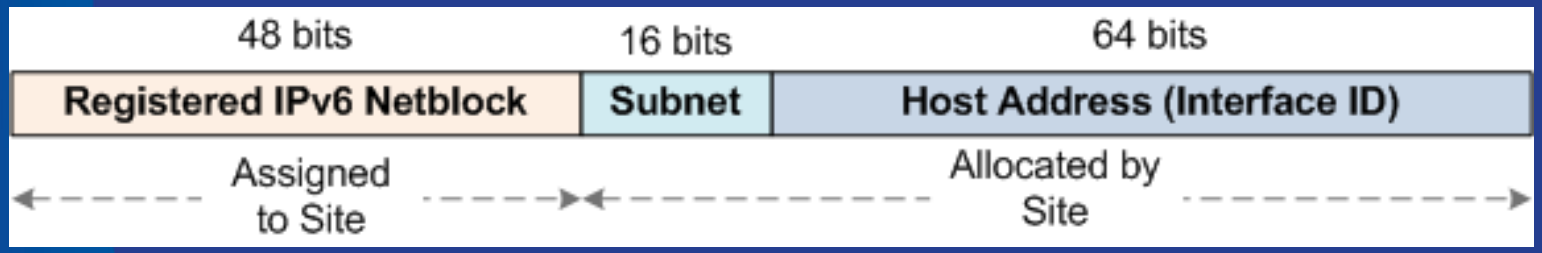
- IPv6 Basics
- Current Status of IPv6 (and IPv4…)
- IPv6 at FNAL Today
- Plans for Moving Forward
- Major Issues to be Addressed

What is IPv6? Why do we want/need it?

- The latest version of the Internet Protocol (IP)
  - Successor to IPv4
- Drafted to alleviate address limitations of IPv4
  - Internet Registry agencies have run out of IPv4 addresses
- 128 bits of address space
  - Versus 32 bits for IPv4
  - Provides 340 undecillion addresses
  - Much more flexible than IPv4 for mobility support
- Designed to be self-configuring
  - Address auto-configuration capabilities
  - Capability to tunnel through IPv4 networks

IPv6 Addressing (I) - IPv6 Address Format

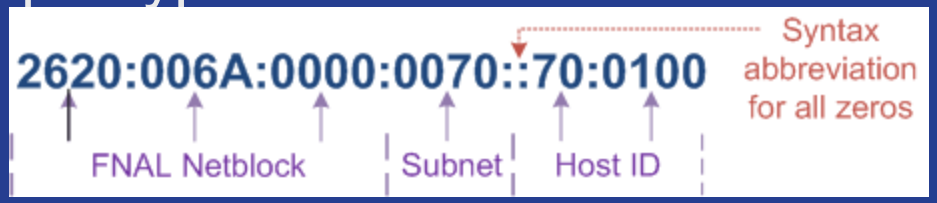
- Default IPv6 address block allocation is /48
  - Host ID is normally left at 64bits
  - Leaving 16 bits for the IPv6 subnet



- No need to be IPv4-like in subnet allocation…
  - Additional address block assignments available as well

IPv6 Addressing (II) - Types of Addresses

- IPv6 interfaces use multiple types of addresses
  - Global addresses:
    - Used for internet communications



  - Link-Local addresses
    - Used for communications within the local subnet

  - Unique local addresses (ULAs):
    - Rough equivalent of IPv4 RFC1918 addresses
  - Privacy address extensions (for SLAAC):
    - Global address that doesn't use MAC address to derive host field
    - Host field component changes regularly
    - Configurable option

IPv6 Addressing (I) - Address Block Types

- Two types of address blocks
  - Provider-Assigned (PA)
    - Service provider issues your IPv6 address block
    - Facilitates more efficient routing from a global perspective
  - Provider-Independent (PI)
    - Obtain your own IPv6 address block from address authority
    - “Needed” for multi-homed sites (multiple ISPs)
    - Minimizes transition difficulties of changing ISPs
- FNAL has two IPv6 /48 address blocks:

ARIN-assigned (PI) block: **2620:006A:0000::/48** **<production network>**

ESnet-assigned (PA) block: **2001:0400:2410::/48** **<used in IPv6 test bed>**

IPv6 Auto-Configuration

- IPv6 addresses can be statically or dynamically configured
- Three dynamic configuration options for global addresses
  - Stateless address auto-configuration (**SLAAC**)
    - End systems configure their own address based on router advertisements (RAs) from neighboring IPv6 router
    - By default, most systems & devices use SLAAC
  - Stateful DHCPv6:
    - Essentially an IPv6 version of DHCP
    - DHCPv6 server implementations emerging; client support varies
  - Stateless DHCPv6 (hybrid):
    - Use SLAAC for global address
    - Use DHCPv6 for additional configuration info (DNS, etc.)
  - Bit fields in RA header determine how clients auto-configure

Dual Stack Operation

- IPv6 and IPv4 address formats are incompatible:
  - An IPv6 system and an IPv4 system can not communicate directly
  - IPv4 systems expected to be around for a long time
- Transition strategy is to run both network stacks on a system (**dual stack**)
- Typical sequence:
  - Dual stack system requests an A (IPv4) record from DNS for a remote system, and also a AAAA (IPv6) record
  - If a AAAA record is returned, the system will normally try IPv6 first:
    - Falling back to trying IPv4 if the IPv6 connection fails
  - Preference of which stack to try first may be configurable, but varies by O/S

Ifconfig on IPv6-enabled Laptop (WinXP)

Wireless Interface

Hardwire Interface

Command Prompt

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : dhcp.fnal.gov
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : 8C-70-5A-87-A4-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d46d:5958:345b:2a06%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 131.225.173.28(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : Thursday, November 01, 2012 10:53:31 AM
   Lease Expires . . . . . . . . . . : Thursday, November 01, 2012 5:23:30 PM
   Default Gateway . . . . . . . . . : 131.225.172.1
   DHCP Server . . . . . . . . . . . : 1.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 529297498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-17-AB-15-44-24-B6-FD-FA-A8-B4

   DNS Servers . . . . . . . . . . . : 131.225.0.254
   Primary WINS Server . . . . . . . : 131.225.9.1
   Secondary WINS Server . . . . . . : 131.225.110.15
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : D0-DF-9A-40-DB-44
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dhcp.fnal.gov
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connecti
on
   Physical Address. . . . . . . . . : 24-B6-FD-FA-A8-B4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2620:6a:0:87:71b5:7aba:7a5f:b7e5(Preferre
d)
   Temporary IPv6 Address. . . . . . : 2620:6a:0:87:68fc:c6c:2783:d537(Preferred
)
   Link-local IPv6 Address . . . . . : fe80::71b5:7aba:7a5f:b7e5%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 131.225.82.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Lease Obtained. . . . . . . . . . : Monday, October 22, 2012 8:50:52 AM
   Lease Expires . . . . . . . . . . : Friday, November 02, 2012 12:18:26 PM
   Default Gateway . . . . . . . . . : fe80::20b:45ff:feb0:7c80%12
                                       131.225.87.200
   DHCP Server . . . . . . . . . . . : 131.225.8.120
   DNS Servers . . . . . . . . . . . : 131.225.0.254
   Primary WINS Server . . . . . . . : 131.225.9.1
   Secondary WINS Server . . . . . . : 131.225.110.15
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Link-Local IPv6 Address

Global IPv6 Addresses

IPv6 Default Gateway

Tunnels

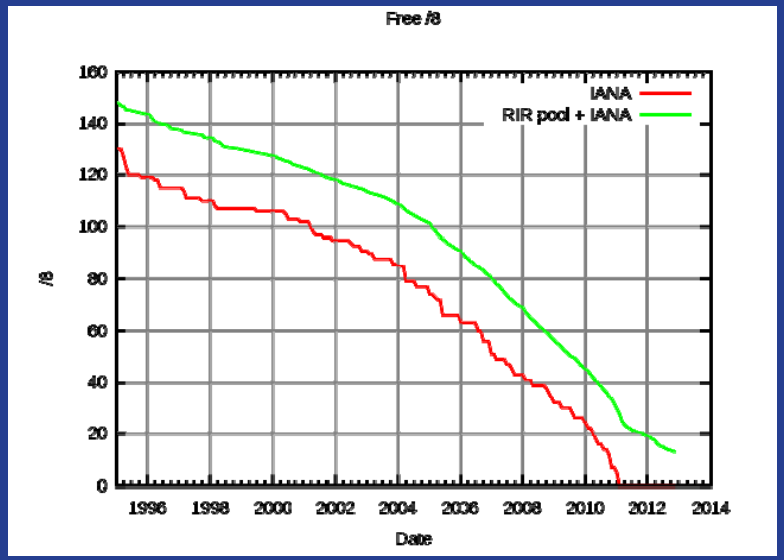
- IPv6 has native tunneling capabilities to work across IPv4-only networks
- Regarded as a transition tool to assist islands of IPv6
- Intended to work automatically & transparently
- IPv6 tunnels come in many flavors:
  - Router-to-Router
  - Host-to-Router
  - Router-to-Host
  - Host-to-Host

Outline

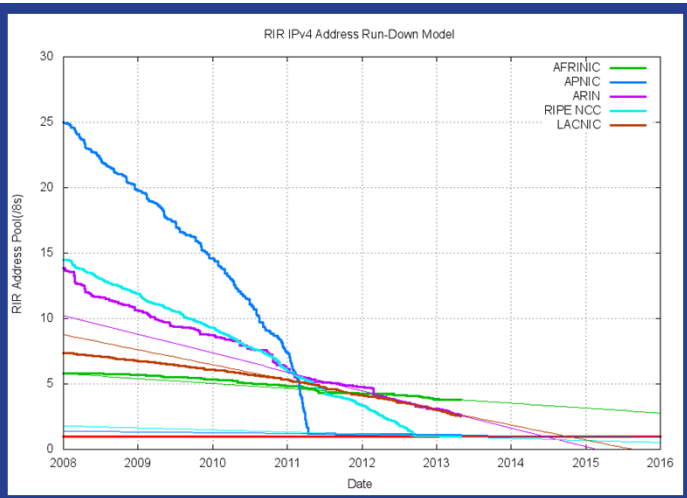
- IPv6 Basics
- Current Status of IPv6 (and IPv4…) ←
- IPv6 at FNAL Today
- Plans for Moving Forward
- Major Issues to be Addressed

IPv4 Address Exhaustion is Happening…

- IANA = global IP address body
  - Issued remaining address blocks in Feb' 2011



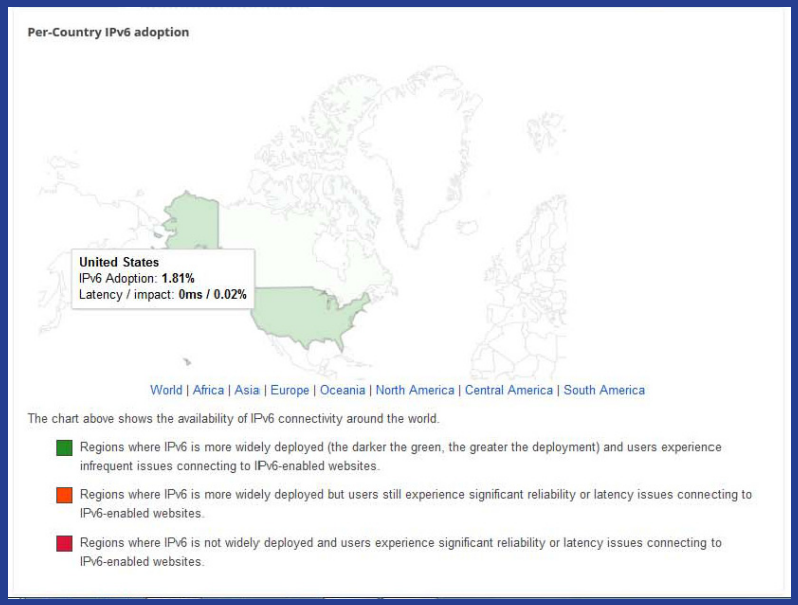
- RIRs = regional address bodies:
  - APNIC = Asia
  - RIPE = Europe
  - ARIN = North America
  - LACNIC = Latin/South America
  - AFRINIC = Africa



Fermilab

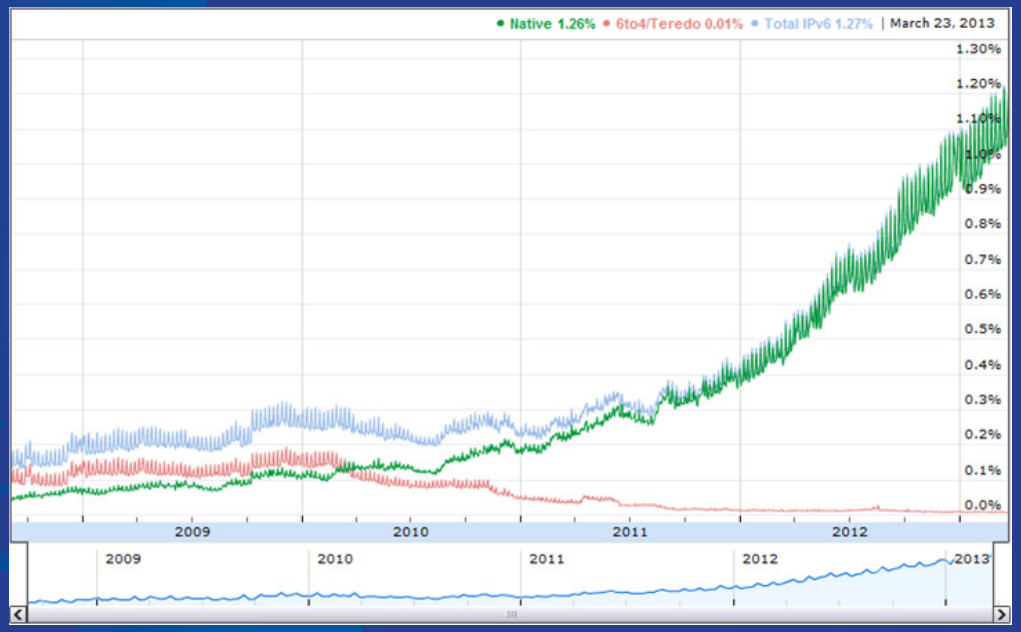
Current status of IPv6 deployment

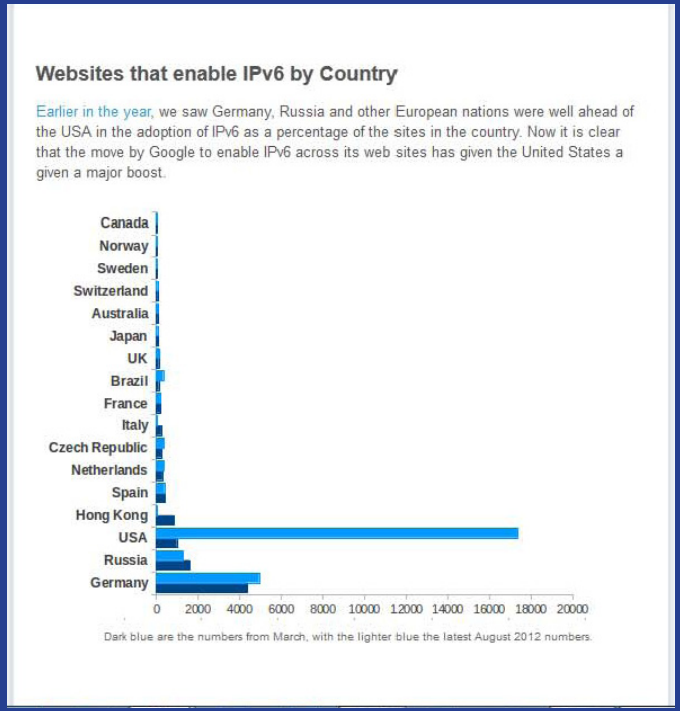
- World-wide IPv6 deployment has been slow
  - Difficult to overcome “IPv4 works; why change?” issue
  - A few countries have established strategic government policies
    - US joined that list
    - European countries looking to emulate US policies



Use of IPv6 Starting To Get Traction

- Google tracks its IPv6 versus IPv4 accesses
  - Worldwide use is at ~1.25%
    - Interpret trend as you wish….
  - Use in US is ~2.4%





Fermilab

Vendors & Service Providers Move to IPv6

- Network OEMs provide full IPv6 support now
  - In US, all federal network procurements must be IPv6 compliant
  - CPE vendors now supporting IPv6 on home routers as well
  - Implementations now in ASICs
- Operating systems:
  - Windows 7 & MacOS 10.6 enable IPv6 **by default**
  - Linux has IPv6 support for 5+ years (but not enabled by default)
- Tablets & smart phones have IPv6 support
- Internet service providers:
  - Comcast targeting 100% IPv6 availability to homes
  - AT&T, Verizon, Time-Warner, & others are also deploying
- Content service providers:
  - Google, Facebook, Yahoo, Youtube, Wikipedia support IPv6

OMB IPv6 “Mandates” for 2012 & 2014

- End of FY12: Public-facing servers to support native IPv6
  - For DOE, this means e-mail, DNS, & web services
  - “Public-facing” interpreted as “intended for the general public”
- End of FY14: Internal client systems to support IPv6
  - Essentially, this means all desktops
- Labs are not included in DOE IPv6 compliance reporting
  - Current DOE interpretation: Labs aren’t bound to OMB mandate
- “Mandate” lacks enforcement element
  - NIST dashboard for agency compliance:

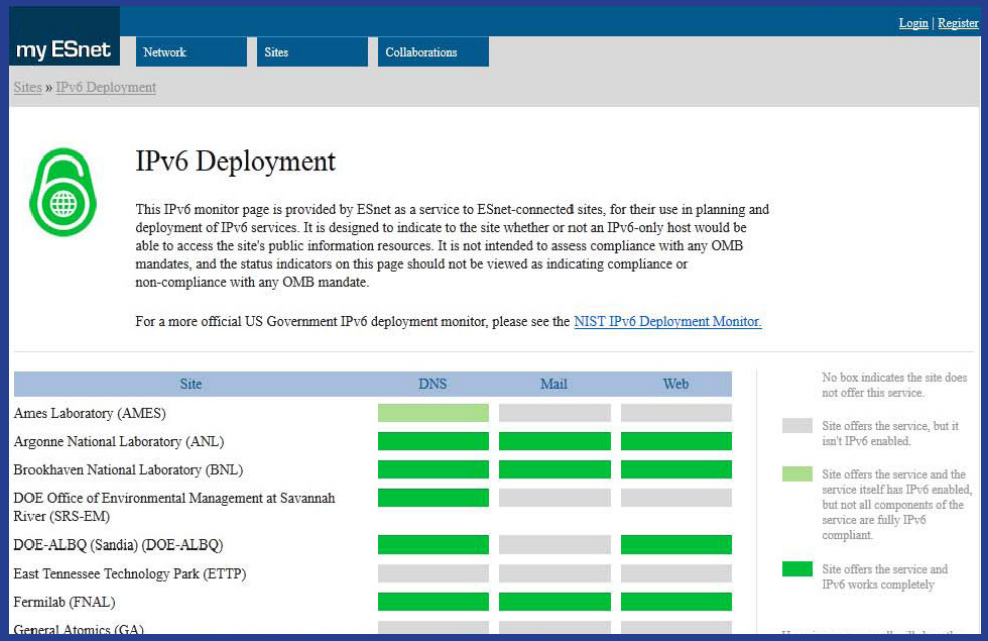
http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov

Outline

- IPv6 Basics
- Current Status of IPv6 (and IPv4…)
- IPv6 at FNAL Today ←
- Plans for Moving Forward
- Major Issues to be Addressed

FNAL & the OMB 2012 IPv6 Milestones

- We're done:
  - DNS in March '12
  - Email in Aug. '12
  - Central web in Oct. '12



- Seven SC Labs are "all green" today

ESnet IPv6 Dashboard:
https://my.es.net/sites/ipv6

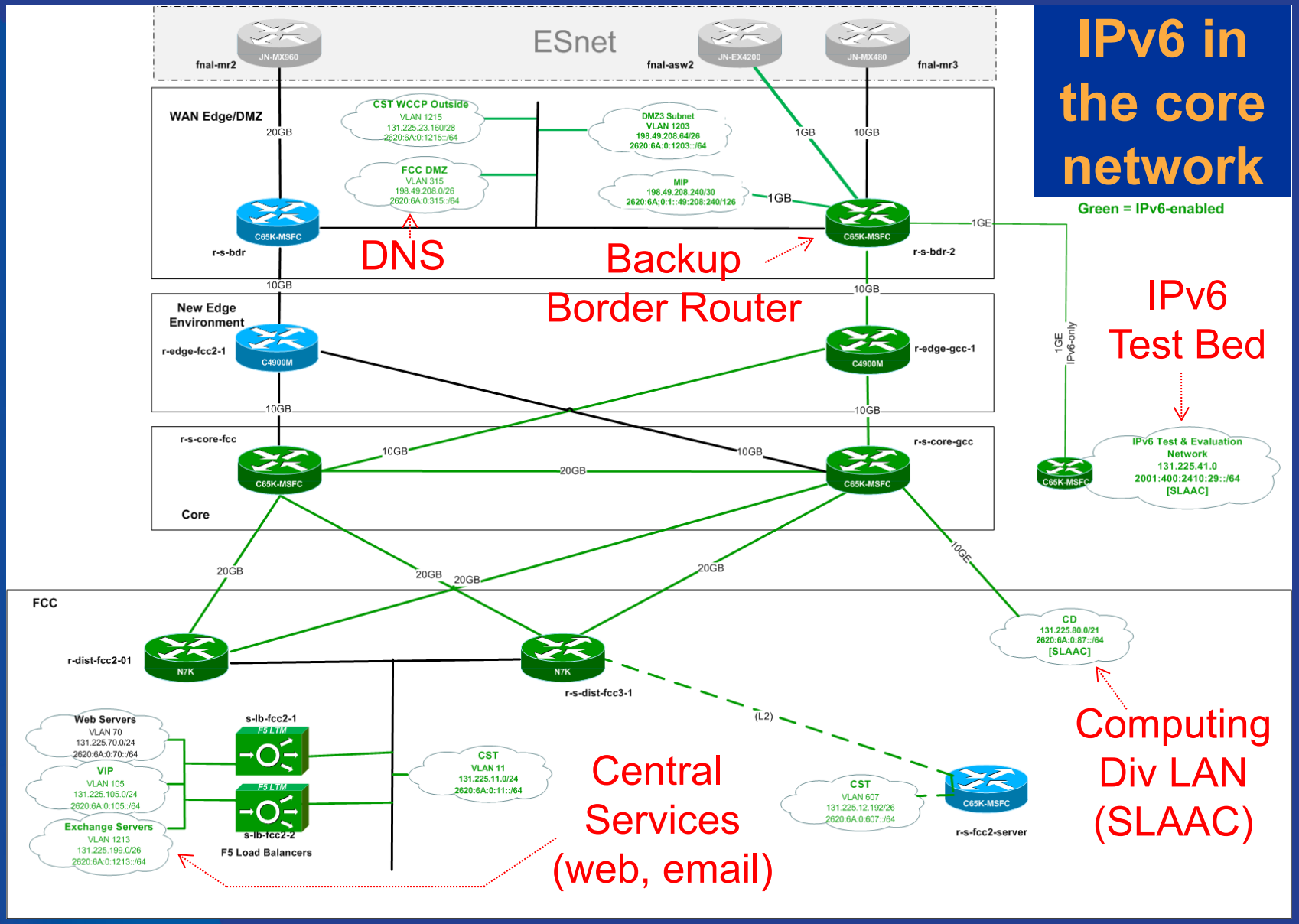
Fermilab

Accomplishments in Conjunction with OMB 2012 Milestones

- Provider-Independent (PI) address space procured
- Addressing model adopted & plan written
  - Will overlay IPv4 addressing that's in place
- Test bed environment deployed
- IPv6 Routing in place within core network
- Flow data collection adapted for IPv6 (NetFlow v9)
- Quasi-production IPv6 evaluation with real users
  - Computing Division staff ( )
  - In place since ~2007

Will become the "foundation" of our future IPv6 efforts

IPv6 in the core network



Fermilab

IPv6 Address Plan – Subnet Allocation Model

- Map to current IPv4 subnet assignments
- /64s for all non point-to-point subnets
  - Point-to-point subnets = /126, not /64
- Based on VLAN assignment
- Decimal equivalents (ie., not in hex)
  - Vlan 87 = IPv6 subnet 87, not 57[hex]

IPv6 Address Assignments - Static

- IPv6 assignment based on IPv4 assignment – last two bytes
  - Again, using decimal equivalents (ie., not in hex)
  - IPv6-only systems – same model; last byte higher than 256
- Examples:

vLAN 70; IPv4 subnet 131.225.70.0/24:

IPv4 addr **131.225.70.100** → IPv6 addr **2620:006A:0000:0070::70.0100**

vLAN 87; IPv4 subnet 131.225.80.0/21:

IPv4 addr **131.225.80.100** → IPv6 addr **2620:006A:0000:0087::80:0100**

IPv4 addr **131.225.87.100** → IPv6 addr **2620:006A:0000:0087::87:0100**

Routing Model & Issues

- Routing Protocols:
  - EGP = BGP4 (just extension to MBGP)
  - IGP = OSPFv3 (ships in the night with IPv4 OSPFv2)
  - Router ID = existing IPv4 loopback address
- Routing Model:
  - Map to the existing IPv4 routing configuration
- OSPFv3 Routing Authentication:
  - Requires complex configuration of IPsec tunnel today
    - Not doing authentication right now
  - Cisco scheduled to implement simple CLI command for IPsec ESP authentication tunnel later this year

IPv6 Tools in Use

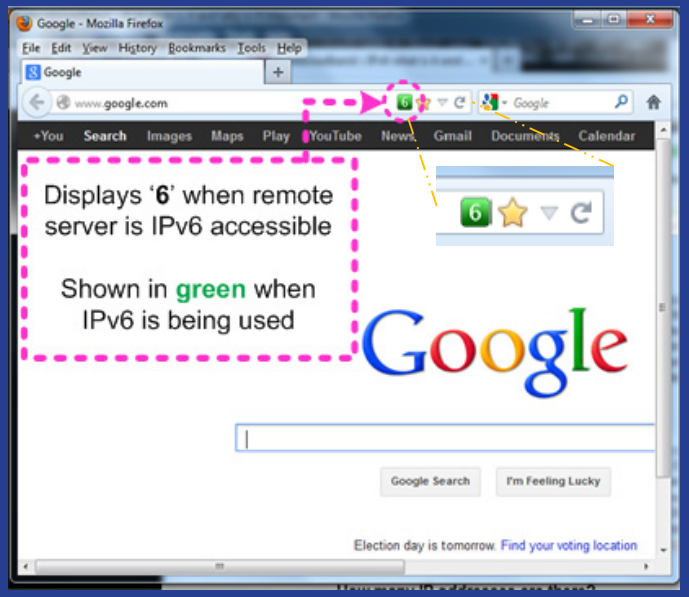
- Ping & Traceroute:

O/S	Ping	Traceroute
Windows XP	**Ping6**	**Tracert6**
Windows 7	**Ping** *<-4;-6 >*	**Tracert** *<-4;-6>*
MacOS	**Ping6**	**Traceroute6**
Linux	**Ping6**	**Traceroute6**

```
Terminal — bash — 138×37
cd-117052m:~ vyto$ traceroute6 -I www.isc.org
traceroute6 to www.isc.org (2001:4f8:0:2::d) from 2620:6a::87:c62c:3ff:fe3c:9a4f,
 1  r-s-fapl-ge2-5.fnal.gov  0.934 ms  0.513 ms  0.466 ms
 2  vlan371.r-s-bdr-2.fnal.gov  0.680 ms  0.517 ms  0.502 ms
 3  2001:400:2402:8::1  0.531 ms  0.472 ms  0.458 ms
 4  chicsdn2-ip-fnalmr3.es.net  1.907 ms  1.967 ms  1.956 ms
 5  eqxchirt1-10g-chicsdn2.es.net  2.078 ms  2.074 ms  2.233 ms
 6  chi-ibx.r1.ord1.isc.org  3.292 ms  3.881 ms  3.248 ms
 7  int-0-0-1-8.r1.pao1.isc.org  53.760 ms  53.833 ms  53.544 ms
 8  www.isc.org  53.028 ms  53.194 ms  53.323 ms
cd-117052m:~ vyto$ ping6 www.isc.org
PING6(56=40+8+8 bytes) 2620:6a::87:c62c:3ff:fe3c:9a4f --> 2001:4f8:0:2::d
16 bytes from 2001:4f8:0:2::d, icmp_seq=0 hlim=53 time=53.708 ms
16 bytes from 2001:4f8:0:2::d, icmp_seq=1 hlim=53 time=53.490 ms
16 bytes from 2001:4f8:0:2::d, icmp_seq=2 hlim=53 time=53.539 ms
16 bytes from 2001:4f8:0:2::d, icmp_seq=3 hlim=53 time=53.425 ms
16 bytes from 2001:4f8:0:2::d, icmp_seq=4 hlim=53 time=53.616 ms
^C
--- www.isc.org ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 53.425/53.556/53.708/0.098 ms

cd-117052m:~ vyto$
```

- Firefox **Sixornot**: add-on that indicates IPv6 accessibility/use:
  - **IPvFoo** (Google Chrome) & **IPvFox** (Firefox) are very similar
  - Haven't found counterpart for IE…

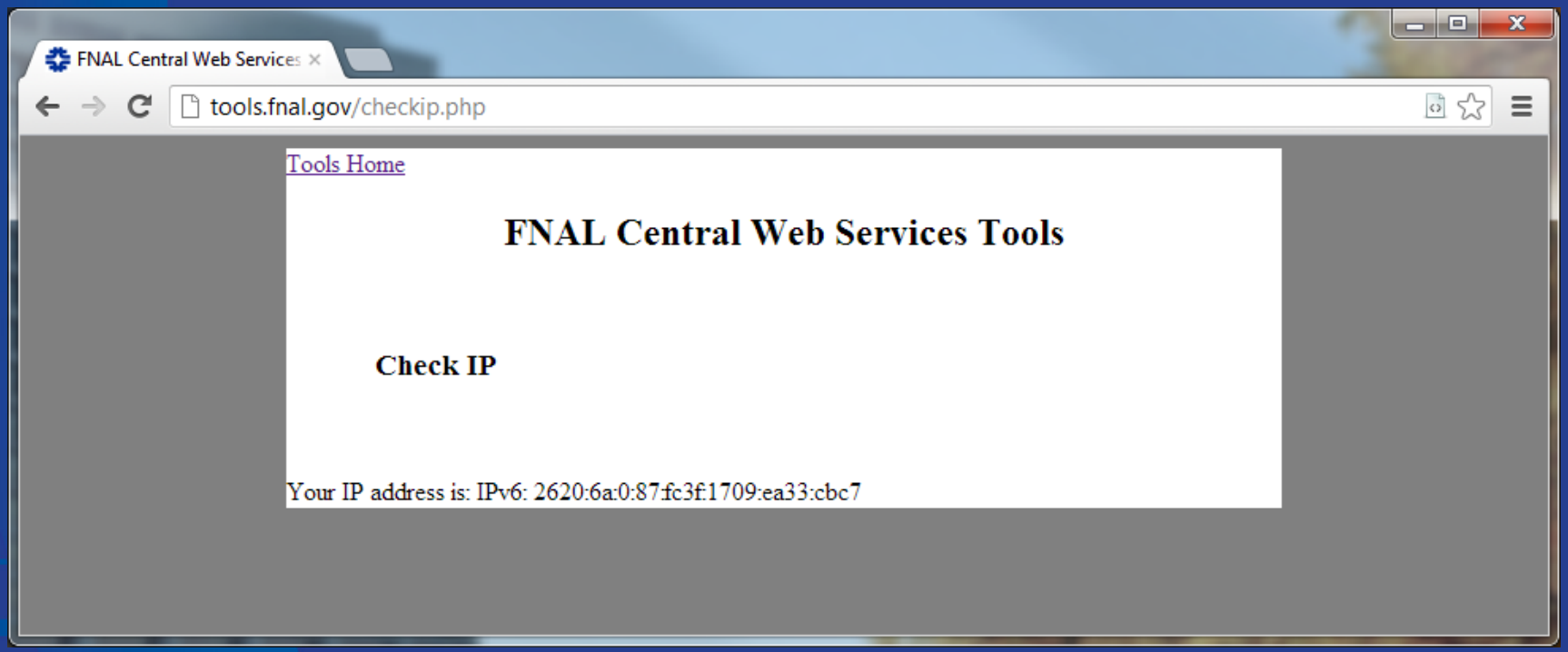


Fermilab

IPv6 Address Verification Service

IPv6 or IPv4 verification is located at:

http://tools.fnal.gov/checkip.php



Fermilab

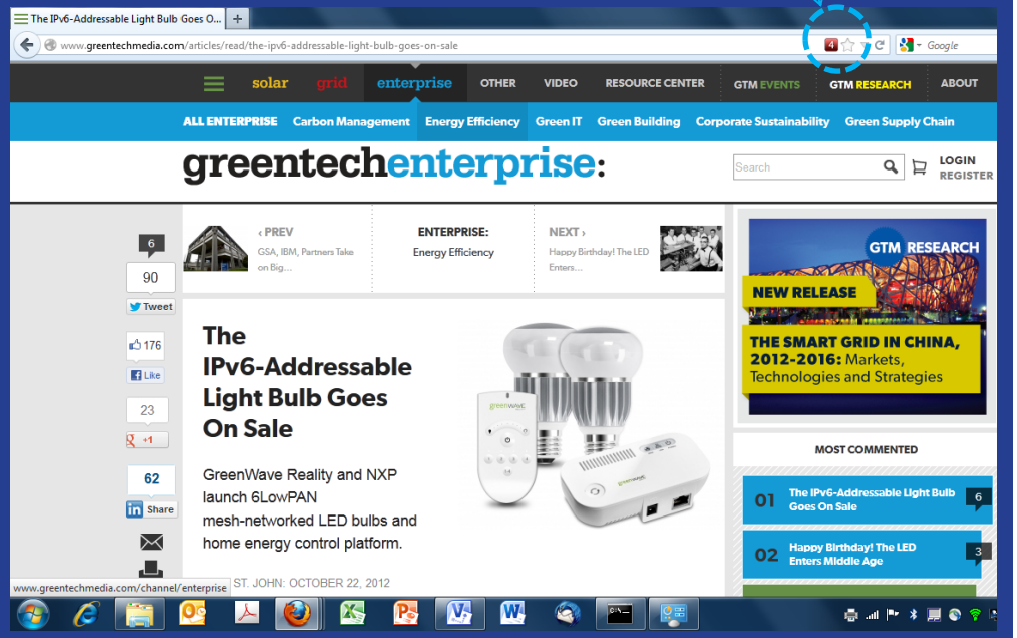
Outline

- IPv6 Basics
- Current Status of IPv6 (and IPv4…)
- IPv6 at FNAL Today
- Plans for Moving Forward ←
- Major Issues to be Addressed

Trying to Think Strategically; Not Tactically

A little irony here…

- IPv6-addressable light bulb (LED)
  - Uses 6LoWPAN over IEEE 802.15.4
  - $200 for the kit
  - $30/light bulb
  - Why we might need an undecillion addresses…



- IPv6 autoconfiguration & address space is enabling technology…

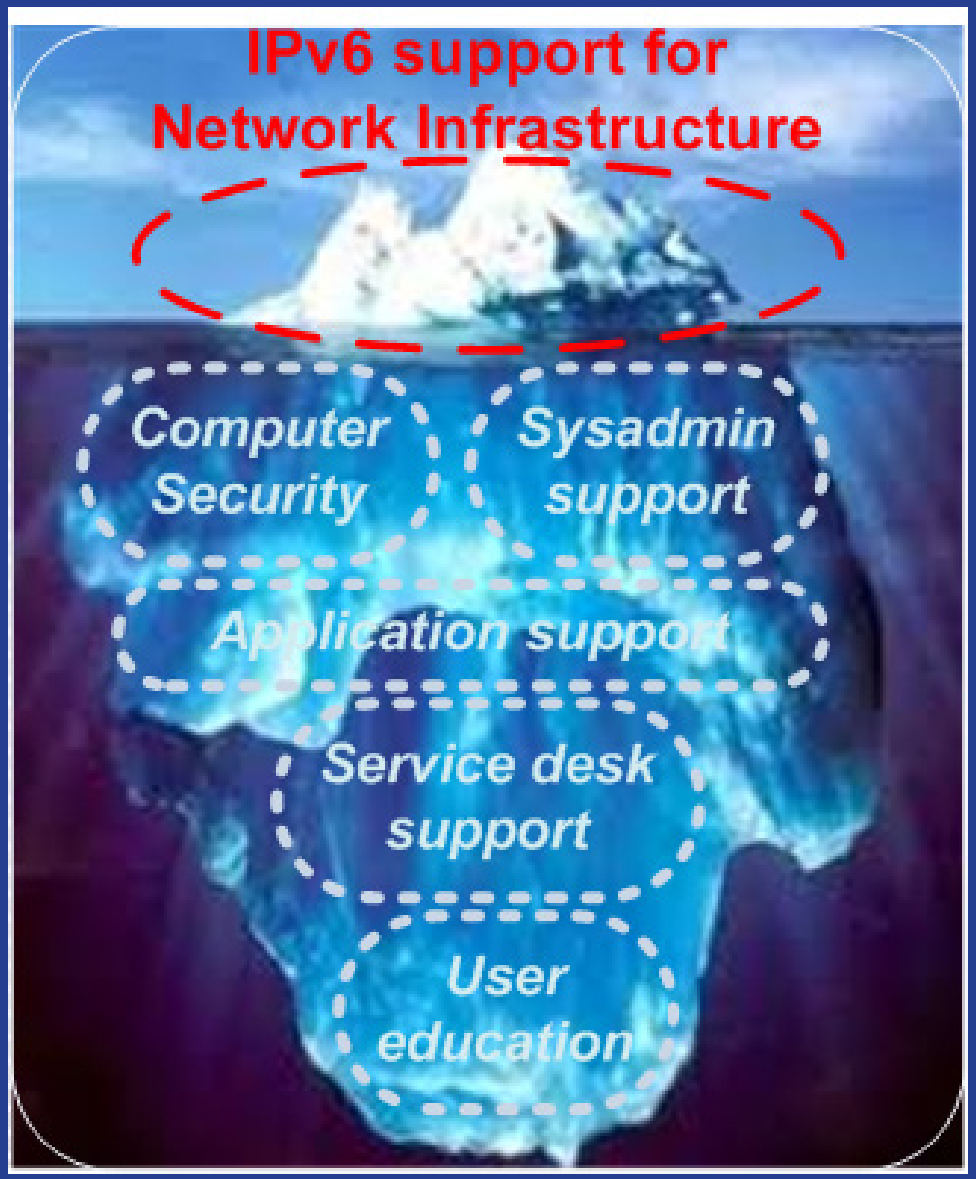
Fermilab

IPv6 Planning Scope: Taking a Broad View

What you see shouldn't sink your ship

What you don't see might…

Fermilab


IPv6 support for
Network Infrastructure
Computer Security
Sysadmin support
Application support
Service desk support
User education

FNAL IPv6 Directions (I)

- Planned direction:

  Implement limited deployment of **production-quality** IPv6 user support, consistent with OMB directives

  - Based on Computing Div. wired LAN and volunteer wireless

- Specifically, what does this translate to?
  - Develop:
    - Appropriate addressing configuration mechanisms
    - IP address management (IPAM) support comparable to IPv4
    - IPv6 configuration guidance for common platforms
    - IPv6-based monitoring capabilities
  - Adapt existing networking & computer security tools and utilities to support IPv6 addresses

- Not looking to expand current level of deployment

FNAL IPv6 Directions (II)

- Current planning structure:
  - Small group analyzing key IPv6 deployment issues:
    - Address configuration mechanisms (SLAAC)
    - Router configurations & controls
    - Tunnel controls
    - Dual stack considerations
    - Privacy address considerations
  - Also meeting individually with other support groups on IPv6
- Short term road map:
  - Recommendations on key IPv6 technical issues by August
  - Engage other groups to develop FY14 IPv6 support effort plan
- High-level objective:
  - Meet OMB 2014 milestones within limited IPv6 deployment
  - Position ourselves for wider IPv6 deployment with low effort

What About IPv6 for Scientific Computing?

- Current FNAL IPv6 demands:
  - No known requests from FNAL experiments or collaborations
  - Scientific computing services not in scope of OMB directive
    - Not clear whether this was deliberate or oversight
- Test bed facility for scientific computing R&D includes IPv6
- HEPix IPv6 work group has ongoing testing effort:
  - Focusing on HEP applications/middleware

CERN perturbing HEP IPv6 landscape

- CERN expecting to run out of IPv4 addresses in 2014:
  - VMs blamed as major factor
  - Options under consideration:
    - Private IPv4 address space (NAT)
    - IPv6-only VMs (ie., not dual stack…)
- IPv6 is their preferred solution:
  - Native IPv6 seen as more viable than tunneling options
- Moving forward with plans to provide IPv6 service in 2013
  - Dual stack while IPv4 addresses hold out
- Will push LHC community to adopt IPv6

Outline

- IPv6 Basics
- Current Status of IPv6 (and IPv4…)
- IPv6 at FNAL Today
- Plans for Moving Forward
- Major Issues to be Addressed ←

StateLess Address Auto-Configuration Support (SLAAC)

- It's simple and it works for all clients
  - Privacy address extensions supported
  - May be necessary in the long run for large-scale addressing
    - Think light bulbs…
- But can cause apoplexy among security types…
  - Absence of access control that DHCP currently provides
- Currently grappling with whether & where to use SLAAC
  - We'd like to know & understand managing SLAAC
  - Leaning toward deployment in Guest environment(s)
  - Developing polling-of-router-adjacencies capability considered desirable with or without SLAAC

Shadow IPv6 Networks

- Shadow IPv6 Networks:

  networks that have IPv6 traffic floating around, but not in a controlled or managed manner

- Auto-configuration capabilities enable IPv6 to just “work”
  - Even without SLAAC, IPv6 hosts auto-configure link local address
    - Tunneling capabilities may work automatically too…
    - Potential for someone to send out router advertisements is real
- Question is how to control IPv6 where its not supported
  - Investigating feasibility of implementing wide-scale RA-guard
  - Risk analysis of this type of vulnerability is needed

Tunnel Control

- IPv6 has a myriad of tunneling options:
  - Windows XP & later have 6-to-4 and Teredo tunneling by default
  - Other O/S vary in default tunneling capabilities
- Observed significant IPv6 tunneling flow records through our perimeter.
- Implemented blocking:
  - 6-to-4 anycast address
  - Teredo UDP port
  - IPv6 tunneling protocol port (41)
- Investigating developing captive IPv6 tunnel capabilities
- Expect this to be an ongoing whack-a-mole problem

?

Questions

Fermilab