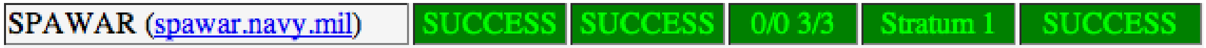
IPv6 at SPAWAR
Implementation on RDT&E Net

Progress on major components

- ✓ LANs, WLAN – all subnets fully support v6, renumber v4
- ✓ Infrastructure services – recursive DNS, NTP, SMTP, XMPP
- ✓ Support services – RADIUS, LDAP, Kerberos
- ✓ Public facing services – authoritative DNS, MX's, www, NTP
- ✓ "Security stack" – firewall, IDS, IPS, etc.
- ✓ Security services – WSUS, McAfee ePO (aka DoD HBSS)
- ✓ Servers, desktops, laptops – 100% dual stack
- ✓ Storage (NFS, CIFS)
- ✓ Network management



SPAWAR (spawar.navy.mil)	SUCCESS	SUCCESS	0/0 3/3	Stratum 1	SUCCESS

Source: http://www.mrp.net/IPv6_Survey.html

The major issues for us

- Lack of IPv6/IPv4 feature parity
  - taking too long to get there
- Vendors not eating own dogfood
  - but starting to turn around
- Privacy Addresses (RFC4941)
  - no good solution yet
- MacOSX 10.6
  - but starting to get much better (10.6.8, 10.7)
- Network Management over IPv6

Privacy Addresses (RFC 4941)

- Incompatible with many Enterprise environments
  - Need address stability for many reasons
    - Logging, Forensics, DNS stability, ACLs, etc.
- Enabled by default in Windows
  - Breaks plug-n-play because we have to visit every Windows machine to disable this feature.
- Just added in Mac OS X “Lion”.
- Ubuntu thinking about making it default.
- Need a way for the network to inform systems about proper default on managed enterprise networks
  - new flag in RA prefix information option?

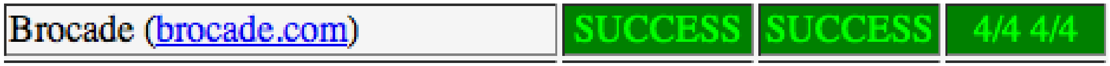
[Privacy addresses] are horrible and I hope nobody really uses them, but they're better than NAT.
… Owen DeLong, Hurricane Electric

If we can’t beat ‘em, join ‘em

- What if the privacy address thing is a losing battle, and we have to live with it?
- We did an Internet-Draft for new RA bits, but it was a hard sell in the IETF.
  - desire for privacy (anonymity) is very strong.
- We’ve debated the topic in various forums.
- New initiative:
  - created subnet where we allow privacy (temporary, random) addresses, and moved a bunch of machines there (Windows, Mac).
  - disabled the alarms (warning about privacy addresses).
  - modified our NDT scanner and auto-DNS-update tool to keep things updated in DNS (PTR records).
    - some argue that this should not be necessary, but some anti-spam tools will reject email from originating hosts that aren’t in DNS.
  - going to generate historical database of MAC address to IPv6 address mapping, for use in IDS and forensics tools.

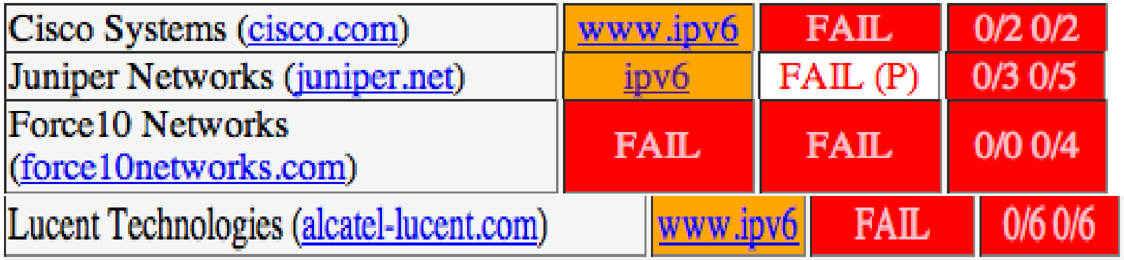
Vendors not “eating own dogfood”

- We were surprised to find so many IPv6 features in vendor products appear to have never been tested or used.
- We learned that vendors were not using their own IPv6 products and features. They weren't “eating their own dogfood”.
- This situation is starting to improve, finally



Brocade (brocade.com)	SUCCESS	SUCCESS	4/4 4/4

  - Others just starting to:



Cisco Systems (cisco.com)	www.ipv6	FAIL	0/2 0/2
Juniper Networks (juniper.net)	ipv6	FAIL (P)	0/3 0/5
Force10 Networks (force10networks.com)	FAIL	FAIL	0/0 0/4
Lucent Technologies (alcatel-lucent.com)	www.ipv6	FAIL	0/6 0/6

Network Management

- Most products cannot be managed over IPv6
- We've been trying to do ALL network management using IPv6, so we can remove IPv4 from the management networks.
- We think we can succeed by Oct 2011
  - But we've had to remove various vendors' products from our networks

Mgmt LAN over IPv6

- Goal – Management LAN IPv6-only (see previous talks)
- Status:
  - Switches: removed all IPv4 configuration from all (over 500) switches at one campus.
    - other campuses in process of doing same
  - Routers: using only IPv6 for most functions, but awaiting fixes or features
  - monitoring: went with Gigamon instead of Anue
  - sensors: all IPv6, including the DRAC ports
  - UPSs: replaced with new APC hardware, all managed over IPv6
  - management/admin tools (apps): still dual stack to accommodate remaining few IPv4-only devices.
  - replacing some old hardware that will never get IPv6 support
- Upcoming milestone:
  - remove all remaining IPv4 configurations (no more lifeline).
  - Oct 2011?
- Remaining issues
  - Lack of unified IP MIB support (RFC 4293) in some products

Management over IPv6 in some mainstream products

	SSH HTTPS	DNS	Syslog	SNMP	NTP	RADIUS	Unified MIB RFC4293	Flow export	TFTP FTP	CDP LLDP
Cisco[6]	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩
Brocade	🟩	🟩	🟩	🟨 1	🟩	🟩	🟩	🟨 2	🟨 3	🟨 4
Juniper	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟥
ALU	🟨 5	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	

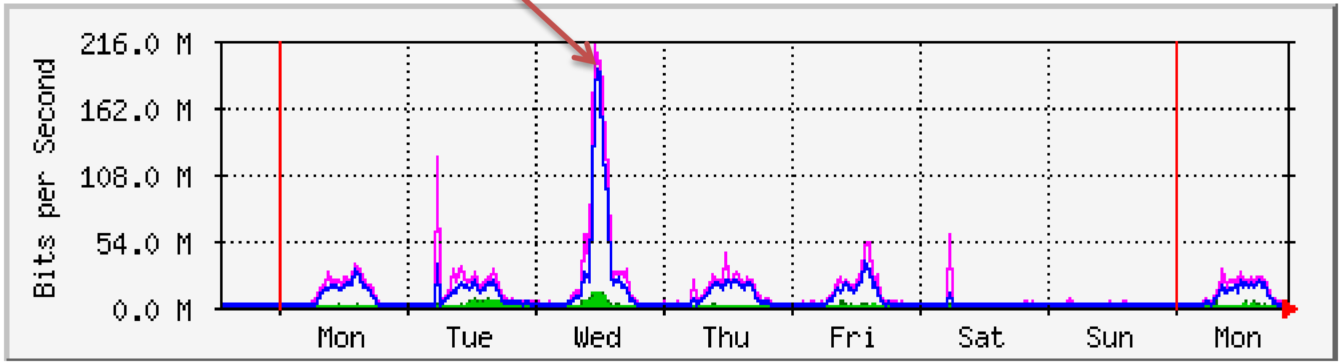
1. Lack IPv6 ACL support
2. can't specify router-ID as IPv6 in MLX
3. firmware bug in FastIron products
4. not in MLX
5. ssh over IPv6 not supported until 2012(Q1)
6. 12.2(58)SE1

World IPv6 day

- For SPAWAR, nothing new to turn on for the day
  - every day is IPv6 day for us
- What does it look like from an enterprise perspective, where ALL clients (users) are dual-stack?
  - well, 99% actually

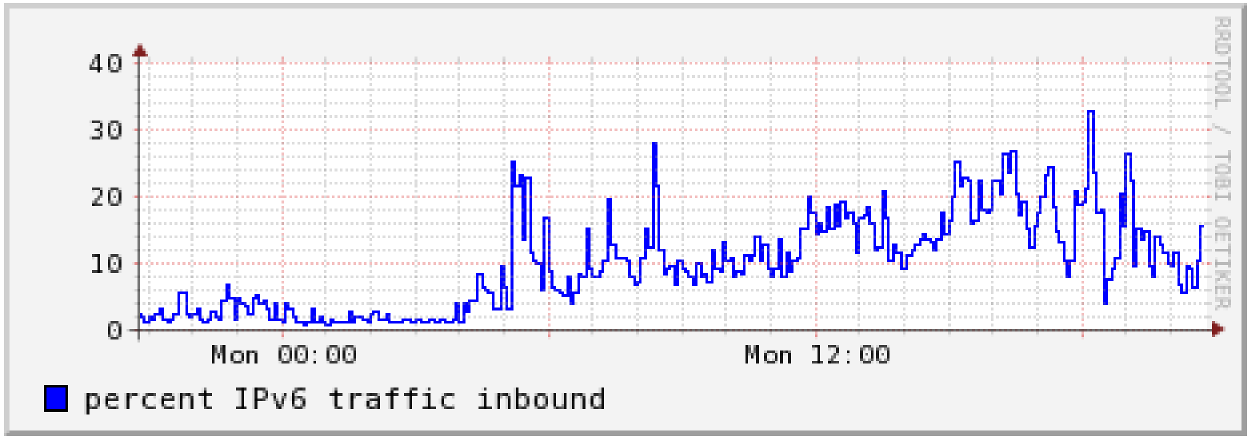
Percentage of Internet traffic over IPv6

- 1% (2009, before Google whitelisting)
- 2.5% (Google whitelisted)
- 10% (late Jan 2010, Youtube added)
- World IPv6 day… (peak at 68%)



After IPv6 day

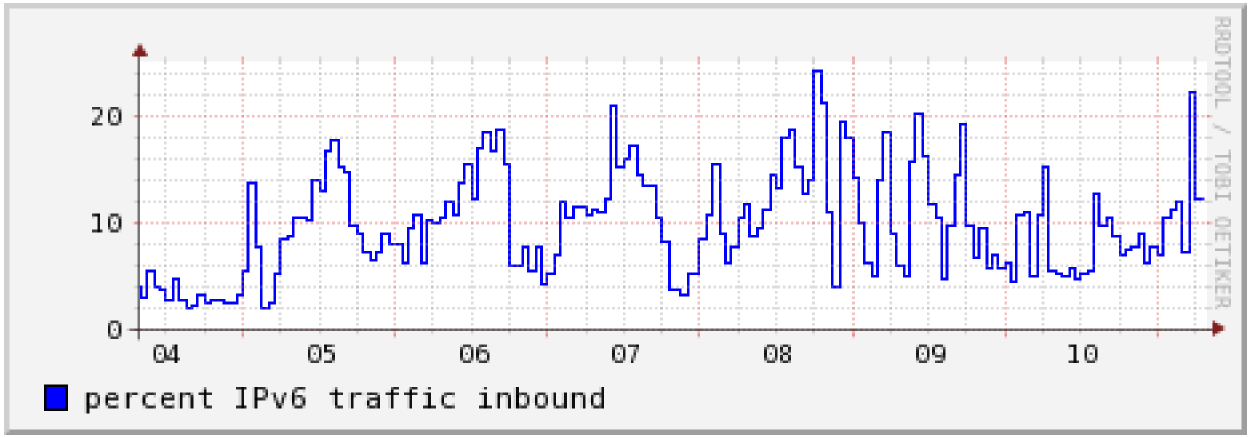
- Percentages across a day (5 min averages):



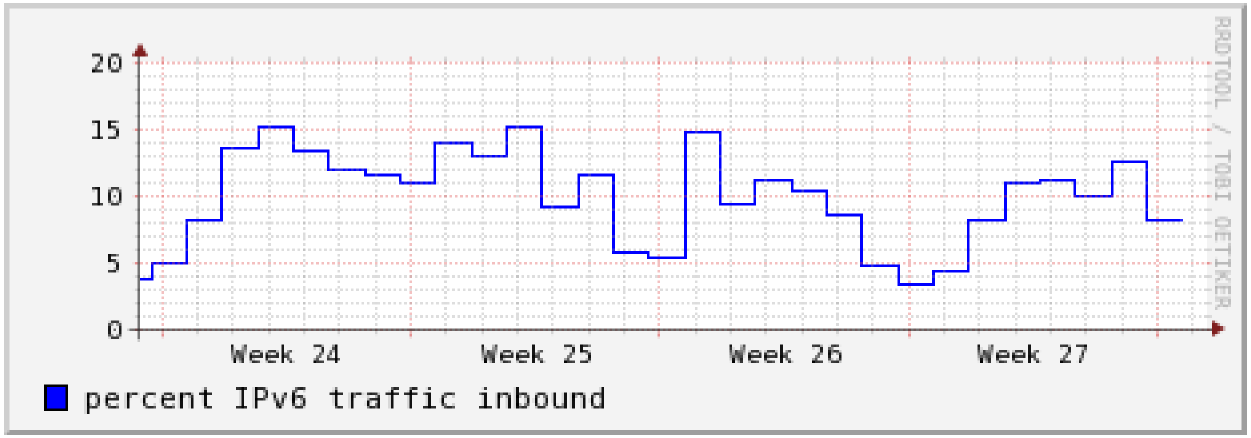
- Why higher during the work day?

After IPv6 day

- Past week (hourly averages):



- Month (daily averages):


Week 24
Week 25
Week 26
Week 27
🟦 percent IPv6 traffic inbound
RRDTOOL / TOBI OETIKER