



---

# Government Enterprise IPv6 Deployment Experiences

gogoNET LIVE! 2

2 Nov 2011

San Jose, CA

Ron Broersma

DREN Chief Engineer

SPAWAR Network Security Manager

Federal IPv6 Task Force

[ron@spawar.navy.mil](mailto:ron@spawar.navy.mil)



# Quick Status



- DoD
  - Research and Engineering nets IPv6-enabled for over a decade
  - Operational nets recently approved for IPv6, but nothing running yet.

- US Federal Agencies

- mandate to IPv6-enable public facing services by Sept 2012
- transition managers assigned in each agency

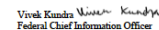
2-Nov-2011



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

September 28, 2010

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Vivek Kundra   
Federal Chief Information Officer

SUBJECT: Transition to IPv6

The Federal government is committed to the operational deployment and use of Internet Protocol version 6 (IPv6). This memo describes specific steps for agencies to expedite the operational deployment and use of IPv6. The Federal government must transition to IPv6 in order to:

- Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
- Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;
- Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and
- Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.

In order to facilitate timely and effective IPv6 adoption, agencies shall:

- Upgrade public/federal facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012<sup>1</sup>;
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
- Designate an IPv6 Transition Manager and submit their name, title, and contact information to [IPv6@omb.eop.gov](mailto:IPv6@omb.eop.gov) by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

To facilitate the Federal government's adoption of IPv6, OMB will work with NIST to continue the evolution and implementation of the USGv6 Profile and Testing Program. This Program will provide the technical basis for expressing requirements for IPv6 technologies and will test commercial products' support of corresponding capabilities.

<sup>1</sup>To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.



# Status, continued



- US Federal Agencies...
  - Lots of planning, with no operational experience
    - partially wasted effort?
  - Addressing plans have serious problems
  - Almost no progress on actually IPv6-enabling anything
  - GSA Networx contract ISPs aren't ready!
    - even though they claim otherwise in public
  - World IPv6 Day – some cheated
  - Confusion over the term "native IPv6"
    - It means "not tunneled", but many think it means "IPv6-only" (IPv4 disabled).



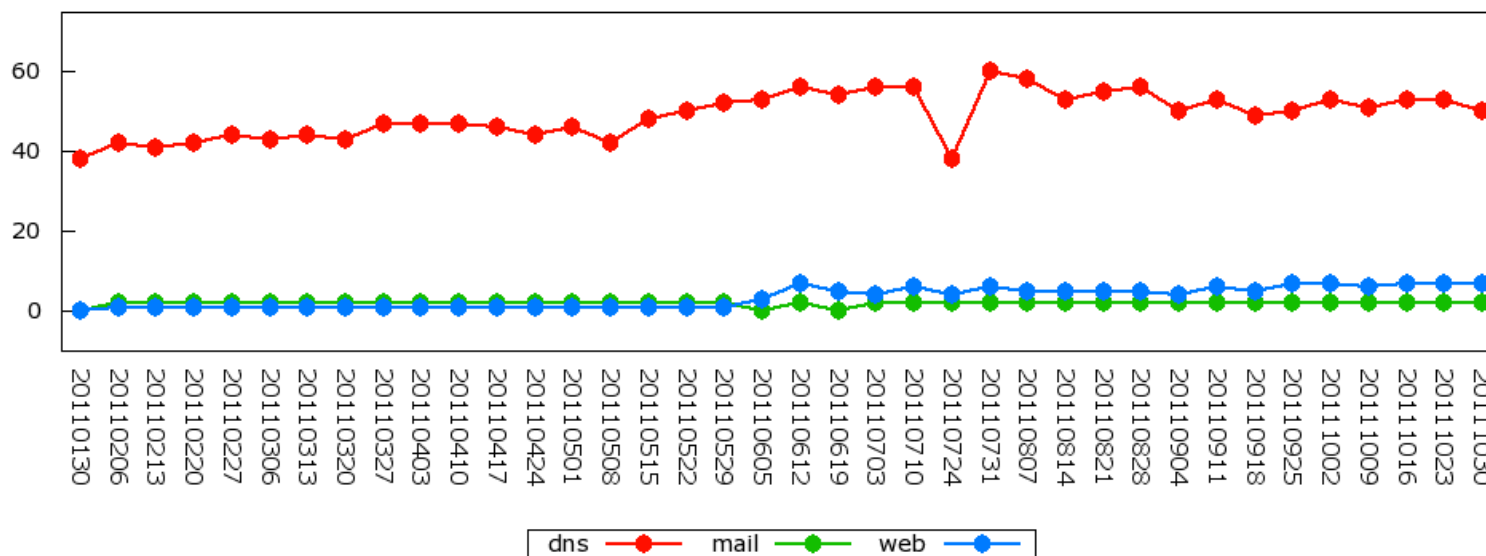
# USG Deployment Status



<http://usgv6-deploymon.antd.nist.gov>

(or just search for "USG IPv6 Status")

USG Unique IPv6 Operational Service Interfaces Over Time





## Many enterprises have not started their IPv6 deployment

---



- Reasons:
  - Lack of incentives and resources
  - Other higher priorities (improving security)
  - It all seems overwhelming, and don't know where to start.
  - No “business case”
- My answer:
  - If you haven't started, you're late and at risk
  - It doesn't take additional resources if you do it right.
  - For U.S. Federal agencies, there is a new mandate.
  - Don't waste time on developing a business case.
    - Its a matter of business continuity.
  - “Don't be afraid to break some glass”



# Some Lessons Learned

---



- Addressing Plans
  - everyone makes the same mistakes
- Go native (dual stack)
- Start from outside, and work in
  - focus now on public facing services
- There will be challenges (surprises) along the way
- You can automate the DNS updates
- It doesn't require significant resources, if you start early and leverage tech refresh



# Addressing plans



- Without sufficient operational experience with IPv6 deployment, you WILL get it wrong at first.
  - usually takes the 3<sup>rd</sup> time to get it right
- Planners are hindered by IPv4-thinking
  - being conservative with address space
  - thinking “hosts” instead of “subnets”
- Typical mistakes:
  - suggesting other than /64 for standard subnet size
    - Didn't read RFC 4291 nor 5375
  - thinking a /48 is wasteful for some small sites
  - thinking a /64 is wasteful for point-to-point links
  - request-up instead of pre-allocate-down



# Addressing plans



- After operational experience, you realize:
  - you never have to “grow” subnets, so you don’t need to accommodate that situation
  - if you don’t use /64’s for subnets, you can’t do SLAAC, DHCPv6, Multicast with Embedded-RP, etc.
  - huge opportunity to align addressing with security topology, to simplify ACLs
  - can better align subnetting and aggregation with existing topology
  - bad idea to embed IPv4 addresses in IPv6
  - every interface has multiple IPv6 addresses
  - internal aggregation is not as important as you initially thought
  - you can do a lot of pre-allocation



# Go native



- 
- “native IPv6” means “don’t use tunnels”.
    - some confuse this term to mean IPv6-only, but that is not the case.
  - Access to Legacy IPv4 networks and systems will be necessary for years to come.
    - we need both IPv4 and IPv6 at the same time.
    - IPv4 and IPv6 are not directly interoperable
  - Use “dual stack” as the IPv6 transition mechanism
    - can use translators in the interim, but NOT long term.



# Start outside, work inwards



- Common mistake
  - Start IPv6 deployment on internal enclave
    - more secure because you are protected with firewall that blocks all IPv6 access to the outside.
    - maybe your WAN connection doesn't even support IPv6
    - MO1 comes first
  - Configure subnet and hosts with IPv6-enabled
  - One of these IPv6-enabled desktops tries to browse to an Internet website that is IPv6-enabled
  - gets both AAAA and A record from DNS
  - tries IPv6 first (since he has IPv6 connectivity, and has AAAA record, and obeys RFC 3484)
  - 21 second delay before it fails over to IPv4
- Solution:
  - don't enable IPv6 internally without access to IPv6 Internet
  - start with WAN, DMZ, public-facing services



# challenges, bugs



- Examples of problems we encountered
  - Lack of IPv6 support in Net::LDAP perl module
  - Perl Socket.pm module was IPv4-only
    - improved in Perl 5.14
  - Linux < 2.6.20 iptables dropped IPv6 frags, breaking some DNSSEC functions
  - NetApp storage appliance – problems with IPv6 support - fixed
  - java defaults to IPv4 instead of IPv6
    - fixable, but not on a Mac
  - Using ISATAP to solve VPN issues
    - but Mac doesn't support ISATAP
  - Wrong tunnel metrics in Windows, chooses wrong interface
  - Lack of DHCPv6 support (XP, Mac)
    - fixed in Windows 7, Mac OSX "Lion"
  - Broken Path MTU discovery in Juniper routers – fixed
  - many VPN products don't support IPv6
    - only IPv4 goes through the tunnel, IPv6 gets blocked by firewall



# more challenges...

- Versions of MS Outlook prior to 2007 won't do IPv6
- Printers
  - Most lack IPv6 support.
  - We've started to upgrade the Jet Direct cards in our HP printers.
- Large groups of systems are under "configuration control", and can't be modified.
- Systems administrators are too busy with other priorities to enable IPv6.
- Rogue 6to4 relays sending RAs
  - Windows systems with ICS enabled.
- Symantec Endpoint Protection (SEP) breaks IPv6 – being fixed
- Vmware ESX 3.x systems – need upgrade to 4.x
- Blackberry Enterprise Services (BES) on IPv6-enabled Windows server will crash.



# Keeping DNS updated



- Need to get all PTRs and some AAAA's in DNS for all devices doing IPv6
- Manual editing of zone files?
  - Much more painful than IPv4
  - How do you know when some device starts doing IPv6 and gets a SLAAC address?
- DHCPv6?
  - Use DHCPv6 to provide addresses, and use dynamic DNS update
  - Problem: too many clients do not yet support DHCPv6 (Windows XP, MAC OSX, others)



# DNS auto-update



- Basic scheme
  - Use SNMP to poll the routers
    - Grab the ARP cache and the ND table
  - For all MAC addresses in the ND table with global unicast addresses matching the site IPv6 prefix:
    - Find the corresponding IPv4 address from the ARP cache
    - Find the FQDN for the IPv4 address in DNS (PTR lookup)
    - Build a PTR record for the IPv6 address, using FQDN from IPv4 address
    - Push to DNS dynamically
  - Works very well
  - Yes, there are some additional complexities, and optimizations required, like garbage collection of temporary and privacy addresses.
- Lingering problems with IPv6 objects in the IP-MIB and IPV6-MIB
  - We really need all routers supporting RFC 4293 (version independent IP-MIB)



## It doesn't have to be costly



- When you purchase anything IT related, make sure it fully supports IPv6
- Any major initiative should include IPv6 support
  - including tech refresh of network infrastructure, or operating systems
- With that, if you start early enough, you will naturally acquire infrastructure, services, and apps that support IPv6
- Gradually enable IPv6 over time
- Not hard, not expensive
- To meet 2012 deadlines, you should have started a few years ago.
  - This was mandated in 2003



My world...



- 
- Defense Research and Engineering Network
    - ISP for DoD R&E Organizations
      - High Performance Computing
      - Research and Development
      - Modeling and Simulation
      - Test and Evaluation
  - SPAWAR (Navy)
    - Operates network supporting RDT&E
      - wide area, over a dozen campuses
    - large enterprise customer of DREN
    - Internet pioneer



# DREN/SPAWAR Progress



- ✓ WAN – dual stack everywhere, peering (unicast+multicast)
- ✓ 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

Defense Research and Engineering Network ( <a href="http://dren.net">dren.net</a> )	SUCCESS	SUCCESS	0/0 3/3	Stratum 1	SUCCESS
SPAWAR ( <a href="http://spawar.navy.mil">spawar.navy.mil</a> )	SUCCESS	SUCCESS	0/0 3/3	Stratum 1	SUCCESS



# 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
- Rogue RAs
  - set router priority to “high” as workaround
- 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



# Lack of "feature parity"



- "feature parity" between IPv4 and IPv6 is something we expect in all products.
  - If the device supports a capability in IPv4, we want it to support that same capability in IPv6.
- Nobody delivers feature parity today.
  - Some vendors are working to fix this.
- Until we achieve feature parity...
  - IPv6 is something less than IPv4
  - You may need to re-engineer your network to accommodate missing features.



# 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*



# Living with Privacy addresses



- 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 ( <a href="http://brocade.com">brocade.com</a> )	SUCCESS	SUCCESS	4/4 4/4
--	---------	---------	---------

– Others just starting to:

Cisco Systems ( <a href="http://cisco.com">cisco.com</a> )	<a href="http://www.ipv6">www.ipv6</a>	FAIL	0/2 0/2
Juniper Networks ( <a href="http://juniper.net">juniper.net</a> )	<a href="http://ipv6">ipv6</a>	FAIL (P)	0/3 0/5
Force10 Networks ( <a href="http://force10networks.com">force10networks.com</a> )		FAIL	0/0 0/4



# Rogue Router Advertisements

## See RFC 6104



- Router Advertisements (RAs) inform hosts of the default router/gateway
- Windows systems with Internet Connection Sharing (ICS) enabled, and IPv6 enabled, will announce itself as the default router using RAs ("Rogue RAs").
  - VERY common problem
- Hosts then start sending all their default traffic to the Windows system
- Workaround: set router preference to "high" (RFC 4191)
  - Doesn't work on JunOS
- Long term: "RA Guard" (RFC 6105) or SeND (RFC 3971)



# Network Management

---



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



# Mgmt LAN over IPv6



- Goal – Management LAN IPv6-only
- 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).
  - Dec 2011?
- Remaining issues
  - Lack of unified IP MIB support (RFC 4293) in many products



# Management over IPv6 in some products



	SSH HTTPS	DNS	Syslog	SNMP	NTP	RADIUS	Unified MIB RFC4293	Flow export	TFTP FTP	CDP LLDP
Cisco <sup>6</sup>										
Brocade				1				2	3	4
Juniper										
ALU	5							7		

1. Lack IPv6 ACL support
2. can't specify router-ID as IPv6 in MLX
3. firmware bug in FGS and FESX products
4. not in MLX
5. ssh over IPv6 not supported until 2012(Q1)
6. 12.2(58)SE1
7. R10.4 July 2012



# World IPv6 day



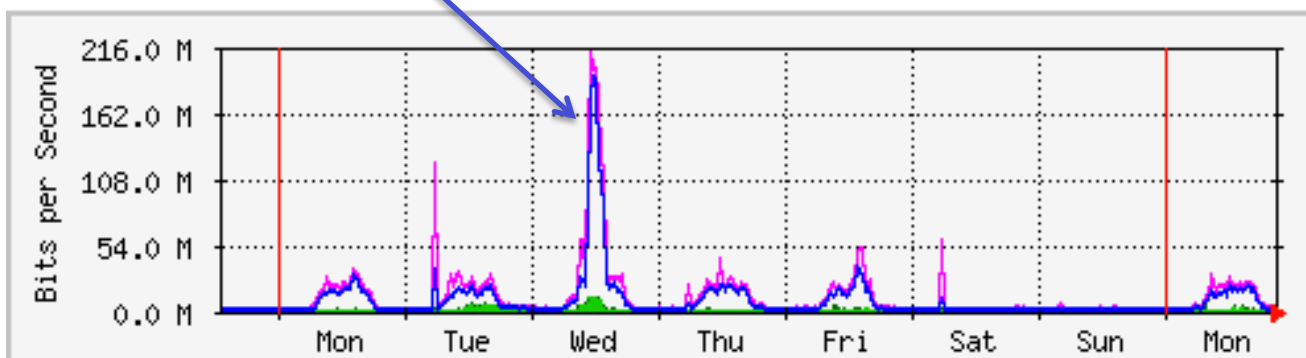
- 
- For DREN and SPAWAR, nothing new to turn on for the day
    - every day is IPv6 day for us
  - What does it look like from an enterprise perspective, where ALL clients (users) are dual-stack?



# 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%)

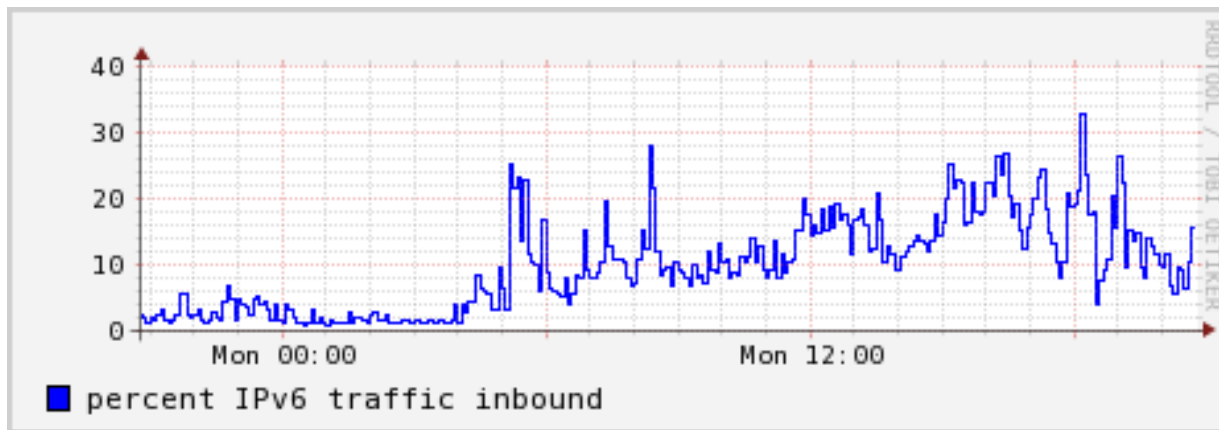




# After IPv6 day

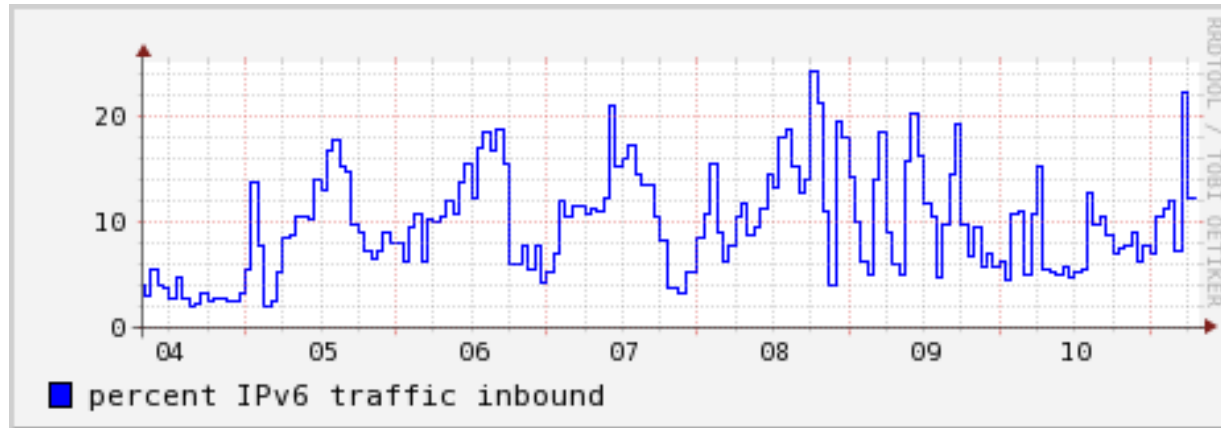


- Percentages across a day (5 min averages):

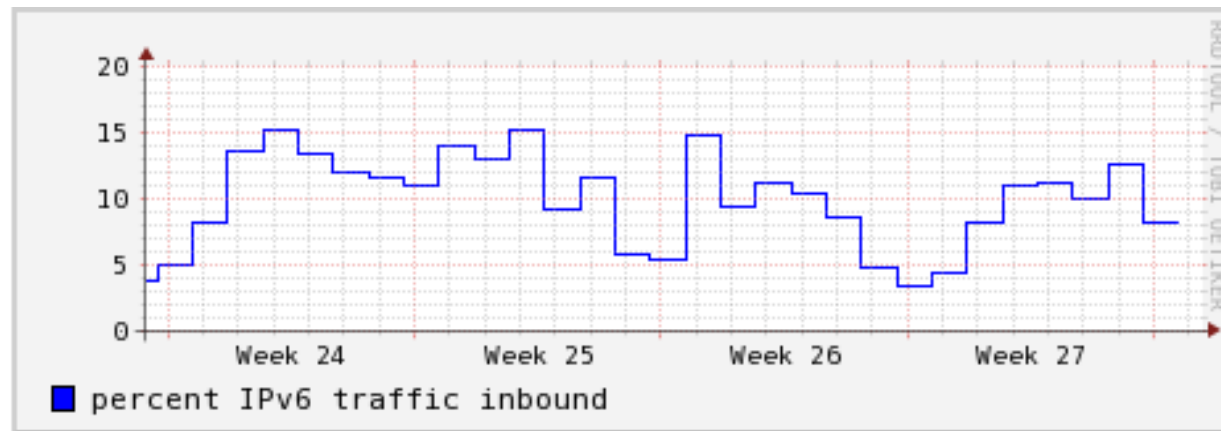


- Why higher during the work day?

- Past week (hourly averages):



- Month (daily averages):





# Other observations



- DoD
- NIST
- Proxy/Translators
  - how do we make sure they are only temporary?
- What's next?
  - World IPv6 day/week (June 2012?)
  - entire Public Internet (1/1/2013?)



---

# Some Do's and Don'ts



- 
- Get buy-in from corporate leadership, especially CIO
  - Develop a corporate culture for IPv6
    - involve all parts of organization, not just the network guys
    - have a local champion
    - include IPv6 in every IT initiative
  - Take baby steps
    - go for the low hanging fruit
    - get experience along the way
  - Leverage tech-refresh rather than spend \$\$\$ on fork-lift upgrades out-of-cycle.
    - it doesn't have to be very expensive
  - Start now
    - if you haven't, you are already quite late to the game
  - Start by IPv6-enabling your public facing services
    - work from outside in, and from bottom up
  - Go native
    - avoid translators, tunnels, and other transition schemes
  - Only choose suppliers that have a good IPv6 story



- 
- waste time developing a complete transition plan with no operational experience
  - base your addressing plan on conservative IPv4 practices
  - waste time on a comprehensive addressing plan without operational experience
    - consider the first one a throw-away
  - waste time trying to develop a business case (ROI) for deploying IPv6.
    - it is a matter of business survival
  - be afraid to break some glass
    - world ipv6 day validated that



# Benefits of IPv6 today (examples)

---



- Addressing
  - can better map subnets to reality
  - can align with security topology, simplifying ACLs
  - never have to worry about “growing” a subnet to hold new machines
  - auto-configuration, plug-n-play
  - universal subnet size, no surprises, no operator confusion, no bitmath
  - shorter addresses in some cases
  - at home: multiple subnets rather than single IP that you have to NAT
- Multicast is simpler
  - embedded RP
  - no MSDP



## Is there a killer app for IPv6?



- 
- The killer app is the Internet itself.
  - The Internet cannot grow and evolve without more addresses, and IPv6 fixes that.
  - Within a couple years, the IPv4 Internet will have an increasing number of performance and availability problems, and the IPv6 Internet will be superior.



# Final Thoughts



- Enabling IPv6 throughout your environment needs to be a cultural thing.
  - Get everyone involved and on-board
  - Include it as part of technology refresh.
  - Don't be afraid to break some glass
- Very important that we focus on making our public facing services dual-stack as soon as possible.
  - otherwise we'll be in translator-hell, breaking various applications
  - eventually some clients won't be able to reach you
- IPv6 is an "unfunded mandate", and everyone needs to do their part.
- Need v4/v6 feature parity in products
- Avoid vendors that don't have a good IPv6 story