



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



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



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



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
27-Sep-2011



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



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