

IPv6 Transition – Industry Best Practices

Jim.Bound@ipv6forum.com

CTO IPv6 Forum www.ipv6forum.org

Chair NAv6tF www.nav6tf.org

HP Fellow



Discussion

- “Basics” Why IPv6 – “Recollection Blues”
- Transition Challenges
- Key Elements of Transition Discussion
- Q & A
- Backup Slides to view on your own
 - Enterprise Network Infrastructure References
 - Enterprise Transition Mechanisms References
 - Background slide on the NAv6TF

What's wrong with IPv4?

Limits Functionality and Restricts Innovation

- Always-on telecommunication, Entertainment and chatting require peer-to-peer and Server-to-client addressability
 - Multi-media messaging, broadcast messaging, Push-to-talk, gaming, VoIP...
 - So does access to Shared Services, to avoid middle boxes.
 - Address space 'extenders' such as NAT prevent reliable service
- Sensors and Machine-2-Machine applications require stateless auto-configuration
- Combat Theatres and First responder networks require ad-hoc capability and roaming mobility
 - Roaming Mobility is facilitated by auto-configuration with adequate addresses for foreign nodes
- All require End-to-End Security



IPv6 technical basics are.....

- Evolved Addressing
 - 128 bit: every grain of sand...
 - Unicast, Multicast, Anycast – but not broadcast
- Streamlined Efficient Headers
 - Fixed Size IPv6 Header with fewer fields
 - 40 bytes vs. 20 bytes for IPv4 header without options
 - Flow Label Added
 - Ordered Extension Headers
 - Extensible to support future payloads
 - Only processed when present
 - 64-bit aligned
- A set of optimizing behaviors
 - Larger MTU, No fragmentation en-route
 - No checksum at the network layer
 - Hop-by-hop options
- A set of new protocols and protocol extensions
 - ICMPv6
 - DHCPv6
 - Mobile IPv6
 - Routing Extensions
 - DNS Extensions
- Automated Configuration
 - Neighbor Discovery
 - ARP + Router Discovery +Router Redirect
 - Autoconfiguration
 - Add 'Stateless' to 'Stateful'
 - Automatic Renumbering for Hosts, Routers
- Secured with IPSec
 - Encryption and Authentication
- Many Transition mechanisms to fit 'every' circumstance



IPv6 Advantages

- Restoration of the end-2-end model for network communications
- Solves Address Shortage, Larger Address Space
- Neighbor Discovery
 - Ad-Hoc /Home networks
 - Network Plug and play
 - Auto Configuration
- Mobile IPv6 Security and Routing Optimizations
- IPsec is MANDATORY for implementation compliance
- Simplicity of management
- IPv4 and IPv6 interoperability
- Faster business and IT alignment

These are just some of the IPv6 advantages over IPv4. IPv6 increases the opportunity for a more secure deployment of Cyber Space for Home Land Defense, Military, Consumers, and Businesses in the U.S., and creates new business opportunity for Internet Service Providers



Transition Challenges

- Technical Analysis
 - Analyze your infrastructure
 - Obtain addresses
 - Your IPv6 Internet Service Provider will delegate a block of address space
 - Pick appropriate deployment scenario / Strategy
- Create a Business Case
- Transition to IPv6 will have multiple choices and that is ok.
- Expect most systems will be software upgradeable
 - Beware of IPv4 implementations in hardware
 - Ask your vendors about their IPv6 plans before buying new hardware
- Transparent for end users
- Network Administrator
 - Quite a lot to learn, but much has a familiar feel

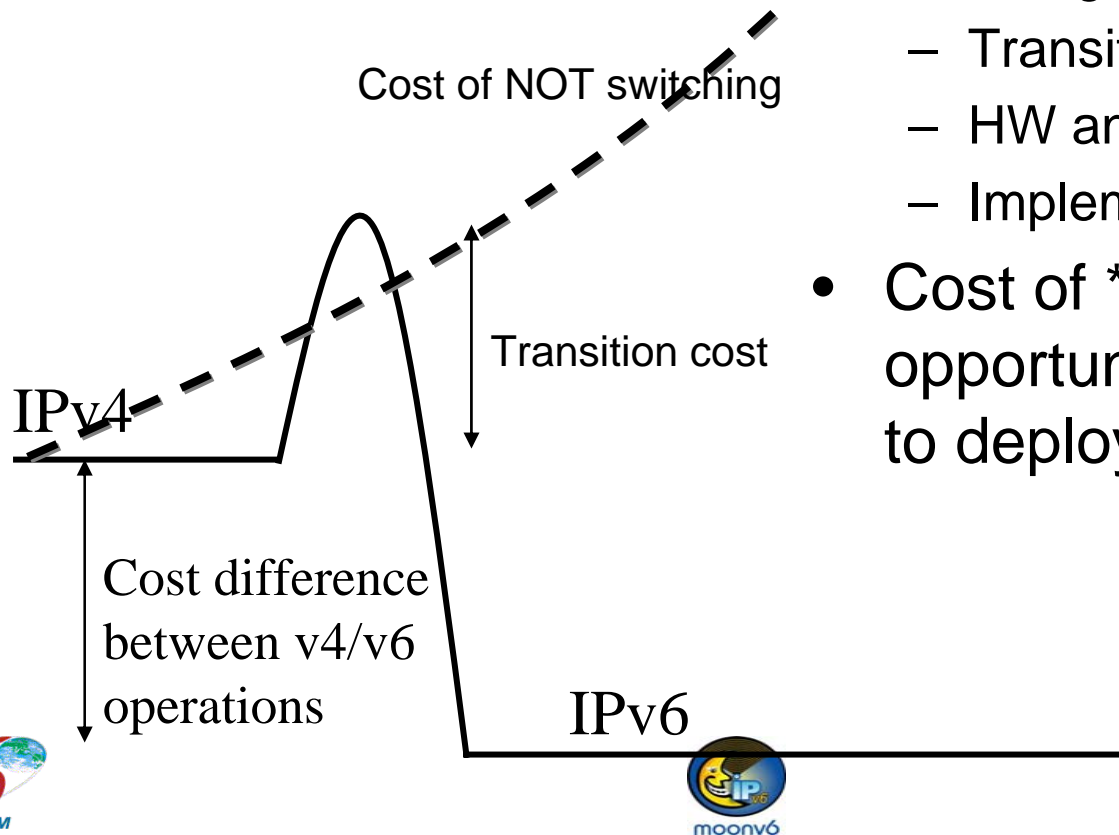
Business Justification Discussion

- IPv6 is a new network plumbing requirement, just like all the updates across the Internet Protocol Reference Model, to stay current.
- Operational Requirements can drive the business case.
- Select the new capabilities from IPv6 which will enhance your operations and make using the network more efficient.
- What is the cost of not doing IPv6?
- What is the cost of Training?
- What is the cost to develop Network Pilots for Testing?



Analyze IPv6 Savings and Costs

- Cost Savings in terms of key IPv6 benefits and Restoration of End-to-End Model
- Costs in terms of hardware, software, staff resources
 - Design
 - Transition
 - HW and SW
 - Implementation
- Cost of *missed* opportunityies of waiting to deploy IPv6



Network Infrastructure Discussion

- How do you want to approach the transition to IPv6 for your intranet/enterprise?
- What network operations do you want to support IPv6?
- How soon do you want to support IPv6 dominant links, sub-networks, and network backbone?
- What network hardware, software, and processes need to be in place to begin the transition on your network backbone?
- What are all the network infrastructure components across your intranet/enterprise that are affected by IPv6?
- What are your external network access requirements for network communications (e.g. Mobility, Partners)?
- What are your requirements to support the principles of Network Centric Operations (connectivity, interoperability, discovery, security, and end-to-end).



Applications Discussion

- Any application that sends packets over an IPv4 network to support IPv6 will require porting that application.
- Identify what applications are a 3rd Party and those that are 'in house' developed applications.
- Applications can be ported to be IP layer agnostic so they support IPv4 or IPv6 out of the box, and the binaries. Unless the source code is lost.
- Applications that will remain IPv4 can be treated as legacy, and tunneled over IPv6 or IPv4 to the legacy application network location.
- Applications need to be considered within your design center of the Network Infrastructure for the transition.



Information Security Discussion

- Any security application you have for IPv4, that you want for IPv6 needs to be ported to IPv6.
- Any security edge software or devices that are used to protect your network with IPv4 need to be upgraded to support IPv6. (e.g. Firewalls, Network Management)
- Any tunnels used for IPv6 Transition must be secured, and any security infrastructure supporting IPv4 entering or exiting VPNs needs to be upgraded to support IPv6.
- IPv6 with IPsec affords the move to end-to-end security model, but that implies that there is a trusted Public Key Infrastructure in place for IPsec.
- Do not turn IPv6 on by default in your network unless all of the above security analysis and upgrades have been done.

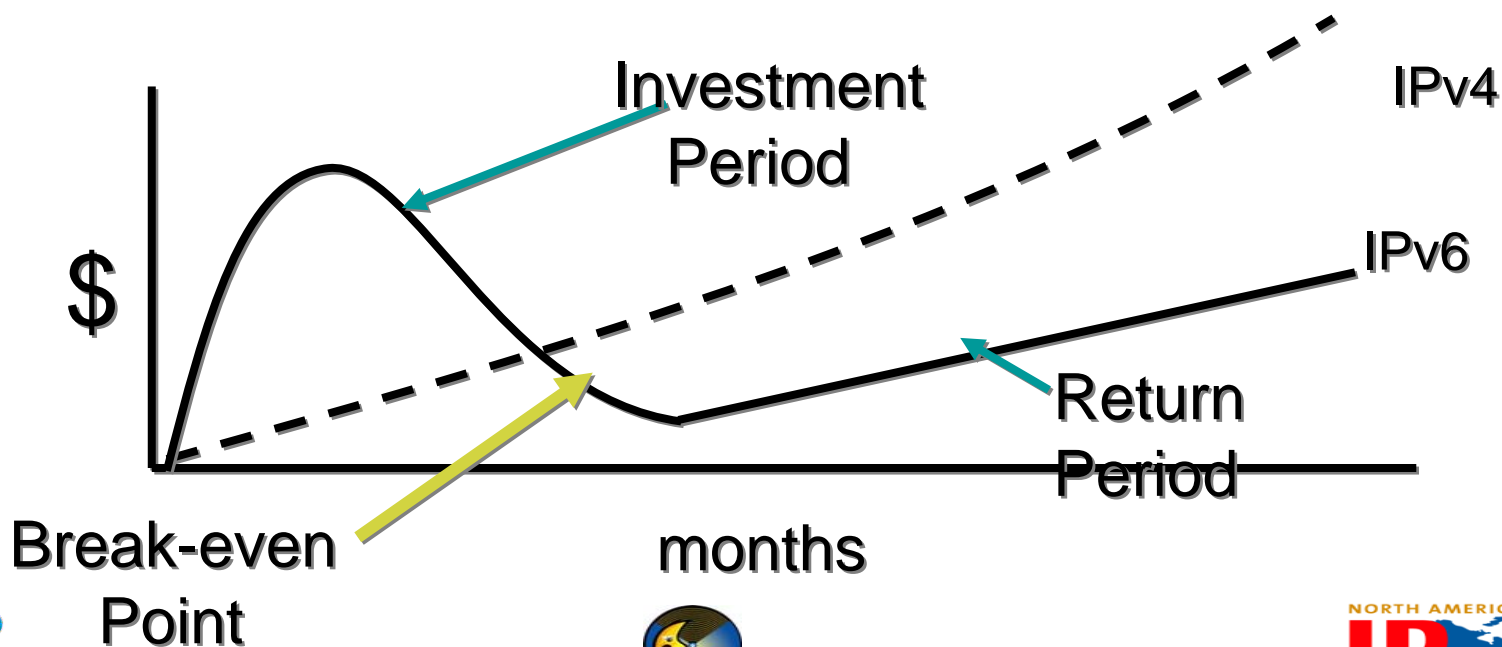


Transition Mechanisms Discussions

- One specific Transition Mechanism cannot solve all possible Enterprise deployment scenarios.
- Multiple Transition Mechanisms can be used by an Enterprise.
- Dual Stack specifications and methods.
- Tunneling specifications and methods.
- Translation specifications and methods.
- Security analysis is imperative for Transition Mechanisms, before deployment.
- Must run Network Pilots and Testing before moving to a production network implementation.

Things to Think about

- Timeline of Vendors
- Market / Customer Demand
- IPv6 Capabilities of Network Equipment
- IPv6 Capabilities in ISP
- Concrete new Business Models for IPv6



Questions?



Enterprise Network Infrastructure References

- IETF RFC 4057 IPv6 Enterprise Scenarios (<ftp://ftp.rfc-editor.org/in-notes/rfc4057.txt>) document. This document defines the Enterprise Networking scenarios and infrastructure components and can be used as example to identify Networking Infrastructure components within an Enterprise.
- IETF RFC 4029 Scenarios and Analysis for Introducing IPv6 into ISP Networks (<ftp://ftp.rfc-editor.org/in-notes/rfc4029.txt>).
- IETF RFC 4215 Third Generation Partnership Project (3GPP) Networks (<ftp://ftp.rfc-editor.org/in-notes/rfc4215.txt>).



Transition Mechanisms References

- Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000
- Nordmark, E., Gilligan, R. "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005
- Nordmark, E., "Stateless IP/ICMP Translator (SIIT)", RFC 2765, February 2000.
- Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
- F. Baker et al., IETF RFC 4192 "Procedures for Renumbering an IPv6 Network Without a Flag Day" September 2005
- F. Templin, T. Gleeson, M. Talwar, D. Thaler, RFC 4214 "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" October 2005.
- A. Durand, P. Fasano, I. Guardini, D. Lento, RFC 3053 "IPv6 Tunnel Broker", 2001
- RFC 3056, Connection of IPv6 Domains via IPv4 Clouds
- Savola, P., Patel, C., "Security Considerations for 6to4", IETF draft <draft-ietf-v6ops-6to4-security-02.txt, March 9 2004>
- Bound, J. Internet draft "Dual Stack Transition Mechanism" IETF draft <draft-bound-dstm-exp-03.txt> June 2005
- DSTM <http://www.ipv6.rennes.enst-bretagne.fr/dstm>
- Bound, J (Editor), Pouffary Y., Chown, T. Green, D, and Klynsma, S. "IPv6 Enterprise Network Analysis" IETF draft <draft-ietf-v6ops-ent-analysis-03.txt>
- Huitema, C "Teredo: Tunneling IPv6 over UDP through NATs" IETF draft <draft-huitema-v6ops-teredo-05.txt>



North American IPv6 Task Force (NAv6TF)

www.nav6tf.org

- Support the deployment of IPv6 across North America
 - As a non-profit vendor neutral volunteer body Sub-Chapter of the IPv6 Forum www.ipv6forum.com
- Provide business, promotional, educational, and technical center of expertise for IPv6 in North America
- Provide technology and transition input to support North American deployment efforts for both Industry and Government.
- Continue to lead the Moonv6 IPv6 Network Pilot www.moonv6.org
- Continue to lead and further develop the MetroNet6 project and prototype First Responder Mobile Ad Hoc Network <http://www.cav6tf.org/html/metronet6.html>
- Develop technology partner relationships with other Consortia's, Industry, Government, and Standards Development Organizations.
- Participate in North American Industry and Government trade show events, seminars, and technology briefings.
- Develop IPv6 deployment technology usage guides as required.
- Support North America Sub-Chapter Task Forces:
 - California IPv6 Task Force www.cav6tf.org
 - Mid Atlantic IPv6 Task Force <http://mav6tf.stealth.net/>

