IPv6
Hope, Hype and (Red) Herrings

Doug Montgomery
(dougm@nist.gov)
Technology Emotional Life Cycles...

- **Inspiration** – “We have a problem.”
- **Hope** – “We can solve the problem.”
- **Hype** – “Easily solves many problems.”
- **Disillusionment** – “Solution not free nor easy”.
- **Despair** – “Not a solution to any problem.”
- **Understanding** – “We know the benefit & cost”.
IPv6: Growing Interest & Questions

- Trade Press “Analysis” … IPv6 Critical to:
  - National Security
    - Mandated Security Mechanisms!
    - Network accountability!
      - NAT as a national security threat!
  - US Economy
    - Asia and Europe are way ahead of US!
  - Future of the Internet
    - Internet is running out of IPv4 addresses!
    - Preservation of the end-to-end principle!
  - New Services
    - Quality of Service, Mobility, Security!
Reality does not make interesting sound bites. The truth about the motivations, capabilities, costs and implications of moving to IPv6 is complex and needs further investigation.

Gov IPv6 Analysis Activities Underway
- NTIA / NIST - Interagency task force to focus on competitiveness, security and user needs.
- DoD – Adoption / transition policy, technology and Interoperability issues.

What are the Motivations / Questions / Issues?
Bits, Bytes and Headers …

- Not that kind of talk, but if we must…..

- What’s in
  - Bigger addresses
  - Flow Label
  - Next header encodings

- What’s out
  - Variable length headers
  - Flags and options
  - Fragmentation
IPv6 Motivations

More Addresses! – the original motivation.
- IPv4 32 bits = $2^{32}$ (~4 billion) addresses
  - but reality of hierarchical administration is ~250 million.
- New users
  - Billions of new users emerging in China, India, SA, Africa
- New classes of devices
  - Large in number, simple in capabilities: cell phones, sensors, appliances, electronic games.
- IPv6 128bits = $2^{128}$ addresses,
  - Practical reality is ~600 billion devices... if it were that easy.

Do we really need that many more addresses?
Is that enough addresses?
IPv6 Addressing.

- **Split architecture**
  - Potential for $2^{64}$ hosts in $2^{64}$ locations.
  - Site multi-homing and provider independence remain concerns.

- **RIR allocation policies determine density.**
  - “Treat as an infinite resource”
    - SOHO allocation /48
    - WPAN allocation /56
  - We are figuring out that infinity isn’t as big as it used to be.
Are we running out of addresses?

- Depends on meaning of “we” and “out”.
  - But in general, if we stick to current growth/use models, yes.
  - Problem varies geographically.
    - US – owns 59% of allocated space, 53% of that is advertised.

- When?
  - Very speculative “science” …
    - [http://bgp.potaroo.net/ipv4/](http://bgp.potaroo.net/ipv4/)
  - Current best guesses are:
    - Exhaustion of IPv4 unallocated pool March 2012
    - Exhaustion of all available IPv4 address space June 2026.
    - Exhaustion of the AS #’s long before we run out of addresses!

<table>
<thead>
<tr>
<th>Region</th>
<th>Allocated</th>
<th>Announced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>0.49%</td>
<td>0.61%</td>
</tr>
<tr>
<td>Americas</td>
<td>63.31%</td>
<td>57.80%</td>
</tr>
<tr>
<td>Asia</td>
<td>14.03%</td>
<td>16.29%</td>
</tr>
<tr>
<td>Europe</td>
<td>20.74%</td>
<td>23.70%</td>
</tr>
<tr>
<td>Oceania</td>
<td>1.41%</td>
<td>1.59%</td>
</tr>
</tbody>
</table>
IPv6 Addressing

- Techniques to Scale IPv4 Addressing
  - Classless Inter Domain Routing (CIDR)
    - Aggregating global routing tables
  - Network Address Translation (NAT)
    - “Hiding” sites with private addresses

- End-to-End Argument – Architectural Purity
  - IPv6 makes it *possible* to uniquely address all devices and communicate directly end-to-end.
    - Avoid complexity / brittleness / obscurity of NAT.
    - Enable peer-to-peer apps.
    - Enable end-to-end security.
  - … but did we want all devices globally reachable?
Network Address Translation

- A lot of confusion about NATs and their implications.
  - A lot of heat, very little light …

- Many people like the (side) effects of IPv4 NAT.
  - Don’t pay for extra addresses
    - Extra IPv4 addresses cost $’s.
  - Provider independent addressing
    - Don’t have to change addresses when you change ISPs.
  - Limited security/obscurity side effects.
    - NAT implements a crude, but effective, firewall behavior.

- IPv6 Network Architecture Protection
  - Attempts to provide similar network obscurity features in IPv6, but without using NAT.

- Many people hate the engineering implications.
  - Adds additional state in the network, complex to engineer peer-to-peer applications, etc.
NAT Love / Hate Relationships

- NATs are Evil!
  - NATs break peer-to-peer applications.
    - Running “servers” behind NATs requires effort/impossible.
  - NATs impact robustness of network.
  - NAT engineering adding complexity to design / deployment.

- Some Users (Think They) Love NAT!
  - Do desirable side effects (previous slide) require NAT?
    - IPv6 cheap, globally unique, provider independent addressing.
    - Privacy / address hiding is a double edged sword.
    - Stateful firewalls just as easy to do without NAT.

- Will IPv6 users deploy NAT anyway?
IPv6 and Security

IPv6 is more secure!

- IPv6 mandates support for IPsec.
  - Is IPsec availability an issue?

- E-to-E argument enables direct IPsec to every device!
  - Not clear this is a desirable / viable granularity at which to administer security policies.

- Defining trust models / boundaries that are implementable, deployable, and scalable is the real issue.
  - Need to deploy missing pieces of security infrastructure (e.g., PKI, key distribution, policy management).
IPv6 Implicit Security Issues

- There are security issues ... not discussed in usual sound bites.
  - Must be careful to avoid backward steps in Enterprise security as a result of deploying a new, 2\textsuperscript{nd} protocol suite.

- Addressing
  - Privacy / Obscurity - No more scanning – for evil or good!
  - Semantics - Anycast, multicast.

- New Protocol Functions.
  - Neighbor discovery, router discovery, auto-configuration, MTU discovery

- Security in Transition
  - Numerous transition mechanisms – DSTM, SIT, ISATAP, Teredo, NAT-PT, TRT, IPsec NAT-T

- IPv6 Security Planning
  - Vital whether you decide to deploy IPv6 or not.
  - Failure to do so could compromise any and all networked IT resources.

- Evolving Security Architectures
  - From: Network / perimeter based.
  - To: Host / end-to-end based.
Management and Mobility

- **IPv6 Auto Configuration & Renumbering**
  - Stateful and Stateless address auto-configuration is integral to IPv6.
    - Enables completely self-configuring devices and networks.
    - Possible (in theory) to easily renumber networks (including routers) when your IP addresses change.

- **IPv6 Mobility**
  - IPv6 routing headers enable more flexible and efficient routing and handoff of mobile hosts.
More Motivations …

IPv6 Provides QoS!
- Architecturally, IPv6 does nothing new for QoS
  - IPv4 QoS products already ship.
- Real question is who needs QoS and for what?
  - Mostly used for single link bandwidth management

IPv6 Improves Routing Scalability?
- Potential exists for better aggregation of addressing
  - But serious IPv6 addressing issues remain: multi-homing, provider independence, etc
- Potential exists for the problem to become much worse!
  - In theory, IPv6 routing table could be 140B x larger than IPv4.
Competitiveness Motivations

A Little Technology Lifecycle Perspective:
- The transition to IPv6 is a marathon. We are not out of sight of the starting line yet, but if we want to start looking at who is in the lead...

The US is falling behind ASIA / Europe!
- Reality depends upon what you examine.
  - Europe & Asia have more official IPv6 address allocations and announced (routed) addresses.
  - What is driving early adopters?
    - Real business trends?
    - Foreign Government economic incentives for IPv6?
- What about North American ISPs?
  - NA ISP economics not favorable to “field of dreams” approach at the moment.

Key Technical / Economic Indicators
- Very little useful data / analysis here. Need to monitor commercial services driven by business needs.

<table>
<thead>
<tr>
<th>IPv6 Usage by Region</th>
<th>Allocated</th>
<th>Announced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>0.03%</td>
<td>0.03%</td>
</tr>
<tr>
<td>Americas</td>
<td>0.71%</td>
<td>0.41%</td>
</tr>
<tr>
<td>Asia</td>
<td>35.52%</td>
<td>18.36%</td>
</tr>
<tr>
<td>Europe</td>
<td>51.12%</td>
<td>63.41%</td>
</tr>
<tr>
<td>Oceania</td>
<td>12.61%</td>
<td>17.80%</td>
</tr>
</tbody>
</table>
US Vendor Issues

- **US Vendors will be Disadvantaged!**
- US vendors lead IETF design and standardization efforts.
- Most major US “networking” vendors have some v6 products / capabilities.
  - Additional product development required to cut over to production / default mode, complete product line, address control / management functions, etc.
  - Most are waiting for customer demand.
    - Current lists of “tested” products are pretty sparse.
  - Customers will need to upgrade software / hardware, train / staff operations, etc. There will be additional CapEx and OpEx.
- IS there a problem here?

To name just a few ....
Vendor Issues

- Other Vital (non-core-networking) Systems?
  - Host OSs, routers and switches may be the easy part.
    - Majority of enterprise investments in networked IT systems maybe elsewhere.
  - Significant effort/expense required to modify, test and redeploy all applications to make them v6 and/or dual-stack capable.
    - Must open the hood on home grown applications.
  - Provisioning/management/monitoring systems, IDSs/firewalls, databases, middleware, load-balancers, etc.
Costs / Risks of (non)Adoption?

- Highly dependent upon the deployment / use scenarios:
  - New/Existing, Public/Private, Pure IPv6 or dual stacks/apps?
  - New, private networks (“isolated green fields”) are an easier target. Bounded scope and no legacy issues.
  - Existing private networks bound the scope on interoperability and legacy issues.
  - Existing public networks (i.e., things “on the Internet”) are going to be the hardest.
- A technology insertion / adoption like no other to date.
  - IPv4 technologies are already in pervasive use in all aspects of life.
  - A whole raft of transition issues / technologies are emerging.
    - Numerous approaches defined: dual stack, mutual tunneling, protocol translations.
    - Increases network complexity / vulnerability / management.
  - “Transition period” could last for decades…or forever.
    - Need to carefully evaluate transition mechanisms and their implications to cost, security, performance, robustness.
Understanding the Tradeoffs

- **Users**
  - Want services / reduced cost and could not care less what the bits on the wire look like.
  - Will bear the significant costs of either decision.

- **Vendors**
  - Want to sell new hardware / software and reduce support costs.

- **Service Providers**
  - Want to sell new services to customers.
  - Will deploy v6 if customers demand / pay for it.
  - Will bear costs of either decision also.
What Can You Do?

- **Raise IPv6 Awareness / Competence**
  - Technology tutorials, forum participation, vendor / user capabilities and requirements.
  - Pilot deployments, testbed evaluations.
  - Evaluate costs / risks / benefits of adoption vs non.

- **Participate in Ongoing Analysis Efforts**
  - Contribute to community understanding of tradeoffs and techniques.
Government Activities Related to IPv6...

- Research and Development
  - Various labs / agencies involved in IPv6 since the beginning.
- 2003 National Strategy to Secure Cyberspace
  - Directs DoC to “examine the issues related to IPv6”, including: security in transition, trade and economics, costs and benefits, and appropriate role for Government.
- DoD announces policy to migrate to IPv6 by 2008.
- DoC forms IPv6 study task force.
DoC IPv6 Task Force Efforts

- **Activities**
  - Public Request for Comments.
    - 25 corporate responses
  - 7/2004 Summary Discussion Document
    - 7/2004 Public Meeting
  - RTI – Interviews with 36 Industry stakeholders.

- **Outputs**
  - Development of Technical and Economic Assessment.
  - Development of Draft Recommendations.
IPv6 Research & Development

- **Security in Transition**
  - Evaluate the threats / vulnerabilities associated with near IPv6 transition mechanisms and develop appropriate mitigation techniques.

- **Scalable End-to-End Security Models**
  - Technologies to support evolution from network-centric to host-centric security infrastructure.

- **Viable QoS Mechanisms**
  - Technologies to enable deployment of multi-domain QoS controls in commercial Internet environments.

- **Scalable Routing**
  - Technologies to support multi-homing, provider independence, and nomadicity in large scale inter-networks.

- **Self Organizing Networks**
  - Technologies to enable ubiquitous mobility and self organization of heterogeneous network technologies.

- **Resilient Networks**
  - Technologies to enable continuous operation in the face of successful cyber/physical attacks and failures.
IPv6 Adoption in .Gov?

- What technical underpinnings are required to support .Gov plans?
  - What does “IPv6” mean in .Gov?
  - Does the plan need Gov profiles / standards?
  - Does the plan need compliance testing?

- Testbed Infrastructures
  - Large scale, persistent testbed infrastructures to leverage agency testing requirements.

- Performance / Behavior Analysis
  - Test and measurement infrastructure to evaluate operational impact of IPv6 in large scale environments.

- Technical and Policy Guidance
  - Gov wide information clearing house for results from aggressive test and measurement activities.
  - Development of additional technical guidance specifications (e.g., NIST-800 Series) to ensure safe and efficient adoption.
For more information . . .

IPv6 Technologies / Issues:
  - [ipv6](http://www.ietf.org/IPV6/) - 1P Version 6 Working Group
  - [mip6](http://www.ietf.org/MIP6/) - Mobility for IPv6
  - [multi6](http://www.ietf.org/MULTI6/) - Site Multihoming in IPv6
  - [v6ops](http://www.ietf.org/V6OPS/) - IPv6 Operations


  - IPv6 tutorials, deployment status, transition issues.

US Government Activities:
- DoC IPv6 Task Force

- DoD / DISA IPv6 Office
Thank you for your attention and participation.
Additional Information
Not Presented.
“IPv6” is not a monolithic technology and thus can not be used meaningfully as a singular description.

The common reference to “IPv6” includes a vast span of affected technologies, including new protocols, optional features, modifications to existing technologies etc.

The technical specification of these technologies and their deployment guidance is comprised of dozens of protocols and technical specifications.

The level of maturity of these specifications vary from soon-to-be full standards, to informal drafts.

Example: Windows CE supports ...
Maybe we mean ……
IETF Specs:

- Mobile IPv6 Management Information Base (221251 bytes)
- Extension to Sockets API for Mobile IPv6 (58339 bytes)
- Securing Mobile IPv6 Route Optimization Using a Static Shared Key (15797 bytes)
- Mobile IP version 6 Route Optimization Security Design Background (100038 bytes)
- Authentication Protocol for Mobile IPv6 (40552 bytes)
- Problem Statement for bootstrapping Mobile IPv6 (54818 bytes)
- Mobile IPv6 and Firewalls: Problem statement (34411 bytes)
- Mobile IPv6 Operation with IKEv2 and the revised IPSec (54446 bytes)
- Using IPSec between Mobile and Correspondent IPv6 Nodes (16332 bytes)
- Mobile IPv6 bootstrapping in split scenario (77648 bytes)
- Mobility management for Dual stack mobile nodes A Problem Statement (15861 bytes)
- Why Authentication Data suboption is needed for Mobile IPv6 (37034 bytes)
- IP Address Location Privacy and Mobile IPv6: Problem Statement (17884 bytes)
- Dual Stack Mobile IPv6 (DSMIPv6) for Hosts and Routers (53869 bytes)
- MobileIPv6-bootstrapping via DHCPv6 for the Integrated Scenario (39003 bytes)
- Fast Handovers for Mobile IPv6 (RFC 4068) (0 bytes)
- Hierarchical Mobile IPv6 mobility management (HMIPv6) (RFC 4140) (0 bytes)
- Mobile IPv6 Fast Handovers for 802.11 Networks (37497 bytes)
- Network Mobility (NEMO) Basic Support Protocol (RFC 3963) (0 bytes)
- Network Mobility Support Goals and Requirements (32729 bytes)
- Network Mobility Support Terminology (41475 bytes)
- NEMO Home Network models (43575 bytes)
- Analysis of Multihoming in Network Mobility Support (93826 bytes)
- NEMO Management Information Base (63048 bytes)
- Network Mobility Route Optimization Problem Statement (51874 bytes)
- DHCPv6 Prefix Delegation for NEMO (14735 bytes)
- Mobile Network Prefix Delegation (48421 bytes)
- Network Mobility Route Optimization Solution Space Analysis (94620 bytes)

- Architectural Commentary on Site Multi-homing using a Level 3 Shim (36106 bytes)
- Shim6 Application Referral Issues (25701 bytes)
- Multihoming L3 Shim Approach (69481 bytes)
- Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming (62797 bytes)
- Shim6 Applicability Statement (10603 bytes)
- Hash Based Addresses (HBA) (52444 bytes)
- Shim6 Reachability Detection (20329 bytes)
- Functional decomposition of the multihoming protocol (33313 bytes)
- Level 3 multihoming shim protocol (166447 bytes)
- Goals for IPv6 Site-Multihoming Architectures (RFC 3582) (0 bytes)
- IPv4 Multihoming Practices and Limitations (RFC 4116) (0 bytes)
- Architectural Approaches to Multi-Homing for IPv6 (RFC 4177) (0 bytes)
- Threats relating to IPv6 Multihoming Solutions (RFC 4218) (0 bytes)
- Things Multihoming in IPv6 (MULTI6) Developers Should Think About (RFC 4219) (0 bytes)

- To name a few from the IETF
  - Internet Area
  - Operations and Management Area

- There are more in the IETF
  - Routing Area
  - Security Area
  - Transport Area
  - Applications Area
Who Are the Service Providers?

Current IPv6 Global Routing Tables (2005-12-15)

- 838 Number of announced prefixes (755 CIDR blocks)
- 595 Number of ASes in routing system
- 474 Number of ASes announcing only one prefix
- 69 Largest number of prefixes announced by an AS

AS/ISPs Originating the most routes.

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>ASnum</th>
<th>AS Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>69</td>
<td>AS1221</td>
<td>ASN-TELSTRA Telstra Pty Ltd</td>
</tr>
<tr>
<td>21</td>
<td>AS30071</td>
<td>ASN-TBONE - TowardEX Technologies Network</td>
</tr>
<tr>
<td>12</td>
<td>AS4621</td>
<td>UNSPECIFIED UNINET-TH</td>
</tr>
<tr>
<td>7</td>
<td>AS18062</td>
<td>GRAGENET-AS-AP Grid And Next Generation Network</td>
</tr>
<tr>
<td>6</td>
<td>AS12008</td>
<td>ULTRADNS - Centergate Research, LLC.</td>
</tr>
<tr>
<td>5</td>
<td>AS3557</td>
<td>ISC-CALIFORNIA Internet Systems Consortium, Inc.</td>
</tr>
<tr>
<td>5</td>
<td>AS7660</td>
<td>APAN-JP Asia Pacific Advanced Network - Japan</td>
</tr>
<tr>
<td>5</td>
<td>AS8175</td>
<td>CETLINK - Computer Enhancement Technologies, Inc.</td>
</tr>
<tr>
<td>4</td>
<td>AS2518</td>
<td>JPNIC-C-ASBLOCK-AP JPNIC</td>
</tr>
<tr>
<td>4</td>
<td>AS4555</td>
<td>EPO-BLU-ASNBLOCK-5 - Exchange Point Blocks</td>
</tr>
<tr>
<td>4</td>
<td>AS6175</td>
<td>SPRINTLINK9 - Sprint</td>
</tr>
<tr>
<td>4</td>
<td>AS4872</td>
<td>VIAG-INTERKOM BT (Germany)</td>
</tr>
<tr>
<td>4</td>
<td>AS9316</td>
<td>DACOM-PUBNETPLUS-AS-KR DACOM PUBNETPLUS</td>
</tr>
<tr>
<td>4</td>
<td>AS16838</td>
<td>VERISIGN-CORP - VeriSign Infrastructure &amp; Operations</td>
</tr>
<tr>
<td>4</td>
<td>AS20495</td>
<td>WEDARE We Dare BV Autonomous System</td>
</tr>
<tr>
<td>3</td>
<td>AS109</td>
<td>CISCO-EU-109 Cisco Systems Global ASN - ARIN Assigned</td>
</tr>
<tr>
<td>3</td>
<td>AS284</td>
<td>UUNET-AS - UUNET Technologies, Inc.</td>
</tr>
<tr>
<td>3</td>
<td>AS1200</td>
<td>AMS-I-IX Amsterdam Internet Exchange (AMS-I-IX) Peering AS</td>
</tr>
<tr>
<td>3</td>
<td>AS1273</td>
<td>CW Cable &amp; Wireless</td>
</tr>
</tbody>
</table>

Current IPv4 Global Routing Tables (2005-12-15)

- 175381 Number of announced prefixes (115858 CIDR blocks)
- 21071 Number of ASes in routing system
- 8745 Number of ASes announcing only one prefix
- 1447 Largest number of prefixes announced by an AS

AS/ISPs Originating the most routes.

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>ASnum</th>
<th>AS Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1447</td>
<td>AS7018</td>
<td>ATT-INTERNET4 - AT&amp;T WorldNet Services</td>
</tr>
<tr>
<td>1185</td>
<td>AS4323</td>
<td>TWTC - Time Warner Telecom</td>
</tr>
<tr>
<td>1057</td>
<td>AS174</td>
<td>COGENT Cogent/PSI</td>
</tr>
<tr>
<td>1050</td>
<td>AS721</td>
<td>DLA-ASNBLOCK-AS - DoD Network Information Center</td>
</tr>
<tr>
<td>1006</td>
<td>AS4134</td>
<td>CHIANET-BACKBONE No.31,j in-rong Street</td>
</tr>
<tr>
<td>970</td>
<td>AS701</td>
<td>ALTERNET-AS - UUNET Technologies, Inc.</td>
</tr>
<tr>
<td>969</td>
<td>AS6197</td>
<td>BATT-ATL - BellSouth Network Solutions, Inc</td>
</tr>
<tr>
<td>916</td>
<td>AS2386</td>
<td>INS-AS - AT&amp;T Data Communications Services</td>
</tr>
<tr>
<td>883</td>
<td>AS18566</td>
<td>COVAD - Covad Communications</td>
</tr>
<tr>
<td>839</td>
<td>AS9583</td>
<td>SI-Y-AS-IN Sify Limited</td>
</tr>
<tr>
<td>838</td>
<td>AS1239</td>
<td>SPRINTLINK - Sprint</td>
</tr>
<tr>
<td>662</td>
<td>AS1221</td>
<td>ASN-TELSTRA Telstra Pty Ltd</td>
</tr>
<tr>
<td>660</td>
<td>AS20115</td>
<td>CHARTER-NET-HKY-NC - Charter Communications</td>
</tr>
<tr>
<td>657</td>
<td>AS209</td>
<td>ASN-OWEST - Qwest</td>
</tr>
<tr>
<td>632</td>
<td>AS1492</td>
<td>CABLEONE - CABLE ONE</td>
</tr>
<tr>
<td>615</td>
<td>AS4766</td>
<td>KXS-AS-KR Korea Telecom</td>
</tr>
<tr>
<td>609</td>
<td>AS4755</td>
<td>VSINL-AS Videsh Sanchal Nigam Ltd. Autonomous System</td>
</tr>
<tr>
<td>596</td>
<td>AS702</td>
<td>AS702 MCI EME - Commercial IP service in Europe</td>
</tr>
<tr>
<td>592</td>
<td>AS22773</td>
<td>CCI-NET-2 - Cox Communications Inc.</td>
</tr>
<tr>
<td>572</td>
<td>AS852</td>
<td>ASN852 - Telus Advanced Communications</td>
</tr>
</tbody>
</table>

2/28/2006
Service Providers …

Source: http://www.caida.org/analysis/topology/as_core_network/ipv6.xml
Who Has the IPv4 Addresses?

**IPv4 Usage 2005-12-15**

<table>
<thead>
<tr>
<th>Country</th>
<th>% of Allocated Space</th>
<th>% of Routed Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MX</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** http://www.potaroo.net/tools/ipv4/
Who Has the IPv6 Addresses?

IPv6 Usage 2005-12-15

Source: http://www.potaroo.net/tools/ipv6/
Who Has the IPv6 Products?

Source: http://www.ipv6ready.org/
Let’s Keep a Little Technology Lifecycle Perspective!

- IPv6 deployment is in its infancy – trend significance?
IPv4 Consumption Models.

Source: http://www.potaroo.net/tools/ipv4/
NIST Efforts in Internet Infrastructure Protection

DNSSEC, BGP, IPv6

Scott Rose, Steve Quirolgico, Okhee Kim, Kevin Mills, Kotikalapudi Sriram, Darrin Santay
M.K. Shin, Oliver Borchert, Rick Kuhn (CSD), Ramaswamy Chandramouli (CSD), Sheila Frankel (CSD)
Tim Grance (CSD) Doug Montgomery (dougm@nist.gov)

“Improving Trust and Confidence in IT”
NI ST and IPv6

- **NI ST/ ITL involved in the genesis of IPng**
  - Actively involved in early IETF IPng designs, specifications, prototypes, and tests.
  - Developed 1st test tools for IPv6 testbeds (NIST 6Bone Monitor / LibpcapV6).

- **Internet Infrastructure Protection & Resilient / Agile Nets.**
  - 1995 – shifted focus to concentrate on core security technologies and robustness for both IPv4 and IPv6.
    - Internet Infrastructure Protection – fostering new technologies to improve the robustness and reliability of key components of the nations information infrastructure.

- **Evaluation IPv6 Transition Mechanisms**
  - New project to study the behavioral, performance and security implications of the IPv6 transition mechanisms.
Evaluating IPv6 Transition

- **“Transition Period”** – the rest of our careers / lives.
  - Estimated at 20+ years (i.e., age of current Internet).
  - Growing concerns about the complexity / security issues associated with operating 2+ network infrastructures.

- **NIST/ITL goals to address key questions/ concerns**
  - Performance, functional and security implications of IPv6 transition mechanisms?
  - Implications of concurrent proposed techniques for site multi-homing and provider independent addresses?
  - Impact on security management technologies (e.g., IDS systems, firewalls)?
  - What operational guidance can be provided to ensure that transition and deployment mechanisms do not compromise the security and stability of vital Internet systems?
Current Customers & Collaborators:

- **DNS** - IETF, DHS, SPARTA, NTIA, Shinkuro, USC/ISI, Verisign, Nominum.
- **BGP** - IETF, DHS, Cisco, DETER/EMIST {UCDavis, SPARTA, PSU}.
- **IPv6** - IETF, NTIA, ETRI.

Example Recent Contributions:

**IETF Standards:**

**Publications:**

**Tools for Industry:**
- **SZIT** - Secure Zone Integrity Checker - [http://www-x.antd.nist.gov/dnssec/](http://www-x.antd.nist.gov/dnssec/)
- **DNS Zone File Anonymizer** - [http://www-x.antd.nist.gov/dnssec/](http://www-x.antd.nist.gov/dnssec/)
NIST Efforts in Internet Infrastructure Protection and Resilient, Agile Networking

- Advanced Networks - http://www.antd.nist.gov/
About the Speaker

Doug Montgomery is the manager of the Internetworking Technologies Research Group in NIST’s Information Technology Laboratory. In that role he provides technical leadership and direction to research and standardization projects in areas that currently include: IPv6, Internet infrastructure protection (domain name system security, routing security, IP security and key management), web services and grid technologies, Internet telephony technologies, self managing systems, networking for pervasive computing, advanced network metrology, and quantum information networks.

Prior to joining NIST in 1986, Doug received his MS degree in Computer Science from the University of Delaware and a BS in Mathematics from Towson State University. He is a member of the IEEE and participant in the IETF and NANOG communities. Doug can be reached at dougm@nist.gov.