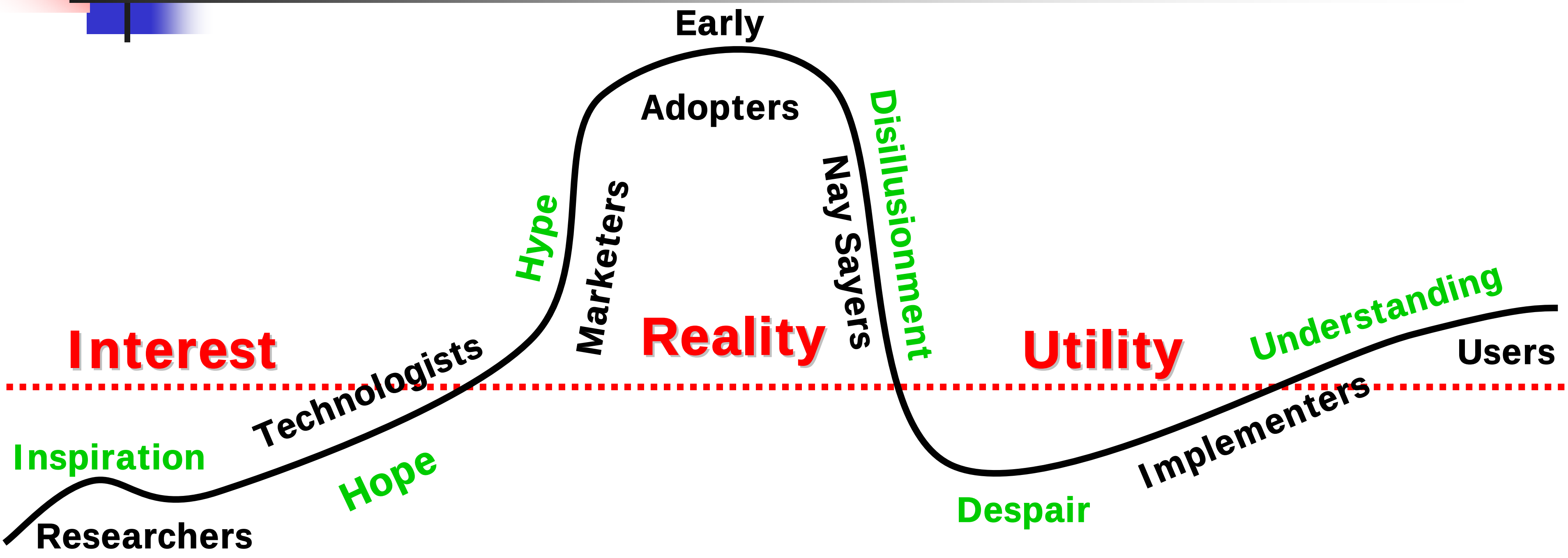
IPv6

Hope, Hype and (Red) Herrings

Doug Montgomery

(dougm@nist.gov)

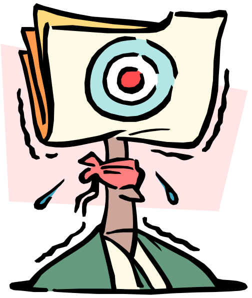
Technology Emotional Life Cycles...



- 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!



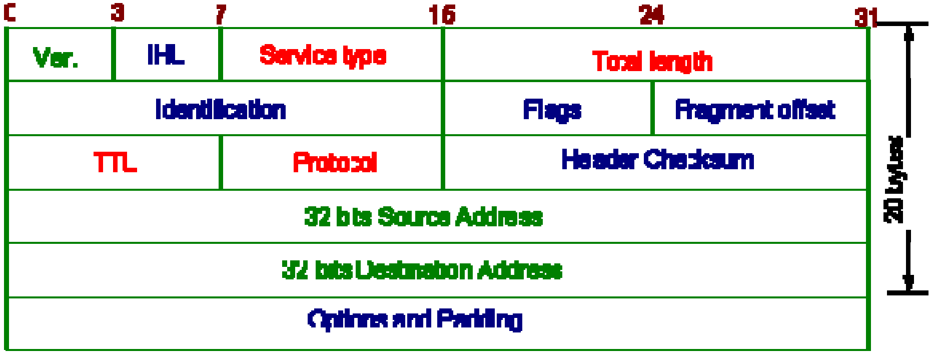
IPv6 in Perspective …

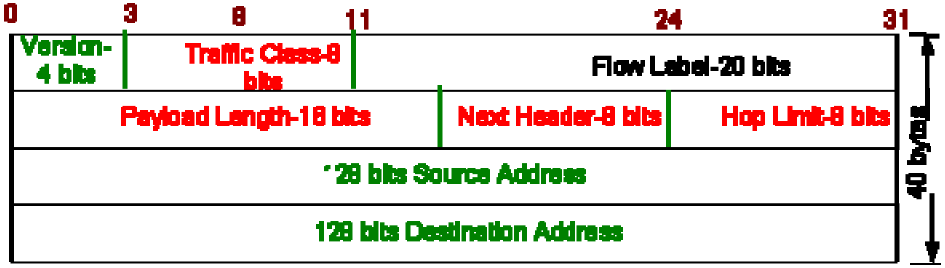
- *Reality does not make interesting sound bites.*
  - The truth about the motivations, capabilities, costs and implications of moving to IPv6 is complex and needs further investigation.
- Gov IPv6 Analysis Activities Underway
  - NTIA / NIST - Interagency task force to focus on competitiveness, security 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

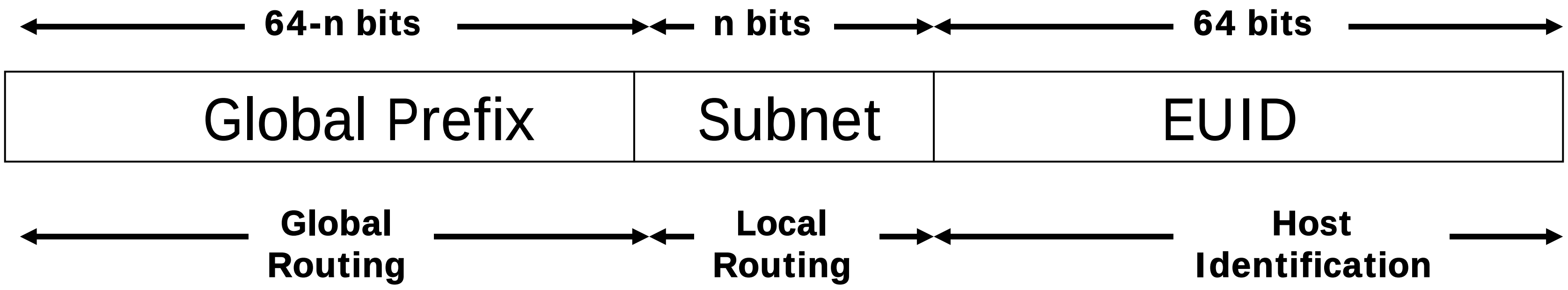




IPv6 Motivations

- *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.



64-n bits	n bits	64 bits
Global Prefix	Subnet	EUID
Global Routing	Local Routing	Host Identification

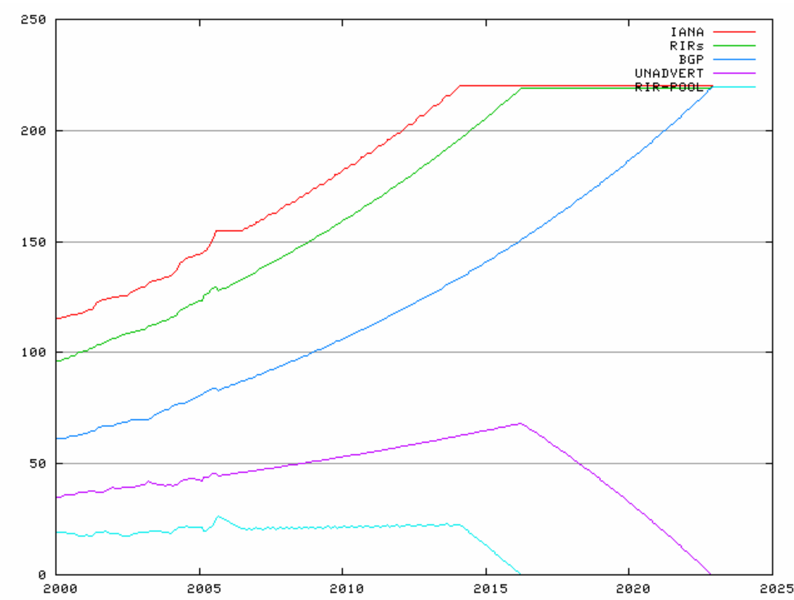
- **Split architecture**
  - Potential for 2^64 hosts in 2^64 locations.
  - Site multi-homing and provider independence remain concerns.
- **RIR allocation policies determine density.**
  - “Treat as an infinite resource”
    - SOHO allocation /48
    - WPAN allocation /56
  - We are figuring out that 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/
  - 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!

IPv4 Usage by Region

Region	Allocated	Announced
Africa	0.49%	0.61%
Americas	63.31%	57.80%
Asia	14.03%	16.29%
Europe	20.74%	23.70%
Oceania	1.41%	1.59%



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, 2nd 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.

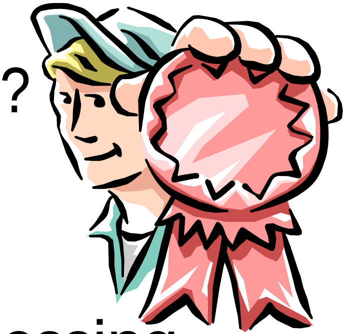
Management and Mobility

- 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.

IPv6 Usage by Region

Region	Allocated	Announced
Africa	0.03%	0.03%
Americas	0.71%	0.41%
Asia	35.52%	18.36%
Europe	51.12%	63.41%
Oceania	12.61%	17.80%

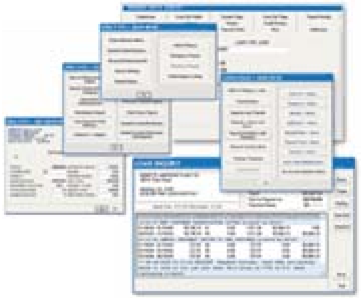
US Vendor Issues

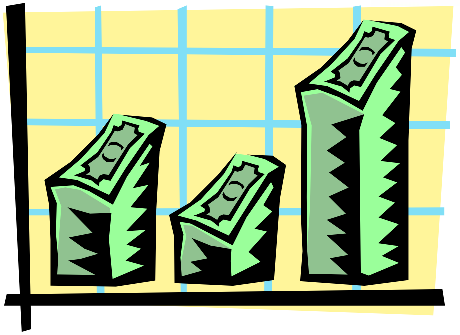
- ***US Vendors will be Disadvantaged!***
- US vendors lead IETF design and standardization efforts.
- Most major US “networking” vendors have some v6 products / capabilities.
  - Additional product development required to cut over to production / default mode, complete product line, address control / 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.



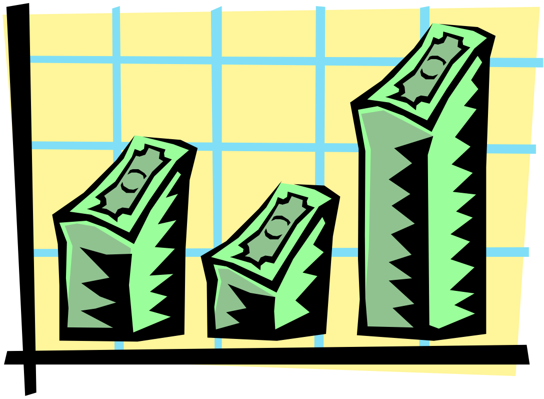


Costs / Risks of (non)Adoption?

- 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 ?

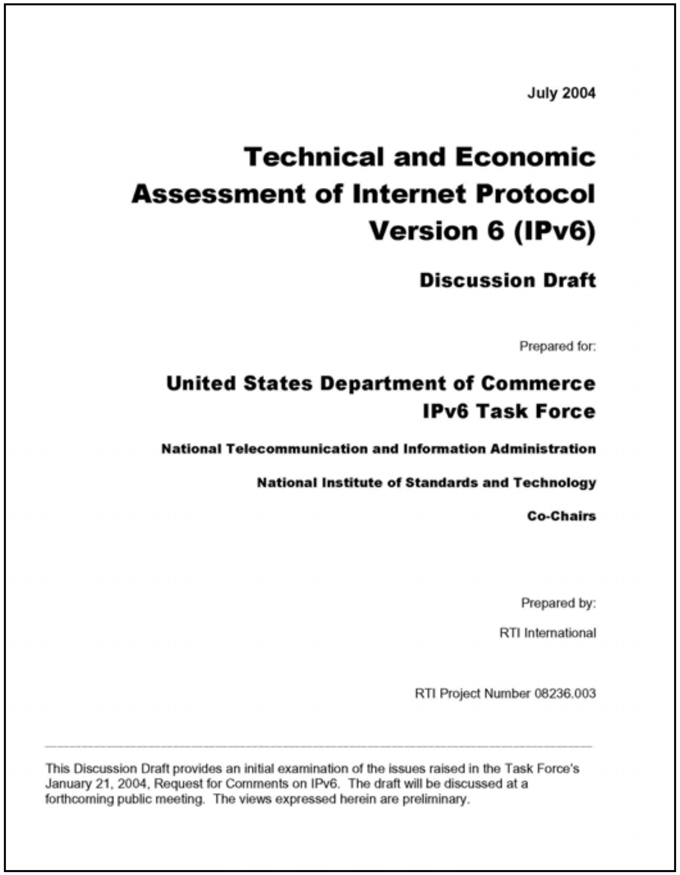
- **Raise IPv6 Awareness / Competence**
  - Technology tutorials, forum participation, vendor / user capabilities and requirements.
  - Pilot deployments, testbed evaluations.
  - Evaluate costs / risks / benefits of adoption vs non.
- **Participate in Ongoing Analysis Efforts**
  - Contribute to community understanding of tradeoffs and techniques.

USG and IPv6

- 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.



July 2004

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)

Discussion Draft

Prepared for:

United States Department of Commerce IPv6 Task Force

National Telecommunication and Information Administration

National Institute of Standards and Technology

Co-Chairs

Prepared by:

RTI International

RTI Project Number 08236.003

This Discussion Draft provides an initial examination of the issues raised in the Task Force's January 21, 2004, Request for Comments on IPv6. The draft will be discussed at a forthcoming public meeting. The views expressed herein are preliminary.

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:**
  - IETF – http://www.ietf.org/
    - ipv6 - IP Version 6 Working Group
    - mip6 - Mobility for IPv6
    - multi6 - Site Multihoming in IPv6
    - v6ops - IPv6 Operations
  - IPv6 Forum – http://www.ipv6forum.com/
  - North American IPv6 Task Force - http://www.nav6tf.org/
  - North American Network Operators Group – http://www.nanog.org/
    - IPv6 tutorials, deployment status, transition issues.
- **US Government Activities:**
  - **DoC IPv6 Task Force**
    - http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/
  - **DoD / DISA IPv6 Office**
    - http://ipv6.disa.mil/

Discussion / Questions?

Thank you for you attention and participation.

Additional Information Not Presented.

What do we mean by "IPv6"?

- "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 ...

RFC number or Internet draft	Title
1752	The Recommendation for the IP Next Generation Protocol
1886	DNS Extensions to Support IP version 6
1981	Path MTU Discovery for IP version 6
2185	Routing Aspects of IPv6 Transition
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header
2403	The Use of HMAC-MD5-1-96 within ESP and AH (implemented for AH only)
2404	The Use of HMAC-SHA-1-96 within ESP and AH (implemented for AH only)
2406	IP Encapsulating Security Payload (ESP)
2428	FTP Extensions for IPv6 and NATs
2460	Internet Protocol, Version 6 (IPv6) Specification
2461	Neighbor Discovery for IP Version 6 (IPv6)
2462	IPv6 Stateless Address Autoconfiguration
2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
2464	Transmission of IPv6 Packets over Ethernet Networks
2467	Transmission of IPv6 Packets over FDDI Networks
2472	IP version 6 over PPP
2473	Generic Packet Tunneling in IPv6 Specification
2526	Reserved IPv6 Subnet Anycast Addresses
2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
2710	Multicast Listener Discovery (MLD) for IPv6
2711	IPv6 Router Alert Option (implemented for host only)
2732	Format for Literal IPv6 Addresses in URLs
2893	Transition Mechanisms for IPv6 Hosts and Routers
3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
3056	Connection of IPv6 Domains via IPv4 Clouds
3484	Default Address Selection for IPv6
3493	Basic Socket Interface Extensions for IPv6
3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
3587	IPv6 Global Unicast Address Format
3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
3596	DNS Extensions to Support IP Version 6
Converting	IP Version 6 Scoped Address Architecture
Internet draft	An Extension of Format for IPv6 Scoped Addresses
Internet draft	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
Internet draft	Routing of Scoped Addresses in the Internet Protocol Version 6 (IPv6)
Internet draft	Site Prefixes in Neighbor Discovery
Internet draft	The UDP Lite Protocol
Internet draft	Default Router Preferences and More-Specific Routes

Source: http://msdn.microsoft.com/library/en-us/wcemain4/html/cmpssIPv6RFCsInternetDrafts.asp

Maybe we mean ……

IETF Specs:

- An Architecture for IPv6 Unicast Address Allocation (RFC 1887)
- DNS Extensions to support IP version 6 (RFC 1886)
- Path MTU Discovery for IP version 6 (RFC 1981)
- IPv6 Multicast Address Assignments (RFC 2375)
- Neighbor Discovery for IP Version 6 (IPv6) (RFC 2461)
- IPv6 Stateless Address Autoconfiguration (RFC 2462)
- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (RFC 2463)
- Transmission of IPv6 Packets over Ethernet Networks (RFC 2464)
- Internet Protocol, Version 6 (IPv6) Specification (RFC 2460)
- Management Information Base for IP Version 6: Textual Conventions and General Group (RFC 2465)
- Management Information Base for IP Version 6: ICMPv6 Group (RFC 2466)
- Proposed TLA and NLA Assignment Rules (RFC 2450)
- Transmission of IPv6 Packets over FDDI Networks (RFC 2467)
- Transmission of IPv6 Packets over Token Ring Networks (RFC 2470)
- IP Version 6 over PPP (RFC 2472)
- Generic Packet Tunneling in IPv6 Specification (RFC 2473)
- Transmission of IPv6 Packets over ARCnet Networks (RFC 2497)
- IP Header Compression (RFC 2507)
- Reserved IPv6 Subnet Anycast Addresses (RFC 2526)
- Transmission of IPv6 over IPv4 Domains without Explicit Tunnels (RFC 2529)
- IPv6 Jumbograms (RFC 2675)
- Multicast Listener Discovery (MLD) for IPv6 (RFC 2710)
- IPv6 Router Alert Option (RFC 2711)
- DNS Extensions to Support IPv6 Address Aggregation and Renumbering (RFC 2874)
- Router Renumbering for IPv6 (RFC 2894)
- Initial IPv6 Sub-TLA ID Assignments (RFC 2928)
- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 3041)
- IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol (RFC 3019)
- Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification (RFC 3122)
- IPv6 multihoming support at site exit routers (RFC 3178)
- Transmission of IPv6 Packets over IEEE 1394 Networks (RFC 3146)
- Unicast-Prefix-based IPv6 Multicast Addresses (RFC 3306)
- Recommendations for IPv6 in 3GPP Standards (RFC 3314)
- Default Address Selection for Internet Protocol version 6 (IPv6) (RFC 3484)
- Basic Socket Interface Extensions for IPv6 (RFC 3493)
- IP Version 6 Addressing Architecture (RFC 3513)
- A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block (RFC 3531)
- IPv6 for Some Second and Third Generation Cellular Hosts (RFC 3316)
- Advanced Sockets Application Program Interface (API) for IPv6 (RFC 3542)
- IPv6 Global Unicast Address Format (RFC 3587)
- IPv6 Flow Label Specification (RFC 3697)
- Requirements for IPv6 prefix delegation (RFC 3769)
- Deprecating Site Local Addresses (RFC 3879)
- Management Information Base for the Transmission Control Protocol (TCP) (RFC 4022)
- IPv6 Scoped Address Architecture (RFC 4007)
- IP Tunnel MIB (RFC 4087)

- Management Information Base for the User Datagram Protocol (UDP) (RFC 4113)
- Unique Local IPv6 Unicast Addresses (RFC 4193)
- Default Router Preferences and More-Specific Routes (RFC 4191)
- IPv6 Host-to-Router Load Sharing (RFC 4311)
- IPv6 Node Information Queries (30637 bytes)
- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (50112 bytes)
- A Method for Generating Link Scoped IPv6 Multicast Addresses (14435 bytes)
- IPv6 Node Requirements (37342 bytes)
- IP Forwarding Table MIB (82941 bytes)
- Management Information Base for the Internet Protocol (IP) (275436 bytes)
- IP Version 6 Addressing Architecture (52281 bytes)
- IPv6 Stateless Address Autoconfiguration (79909 bytes)
- Optimistic Duplicate Address Detection for IPv6 (32804 bytes)
- IP Version 6 over PPP (36839 bytes)
- Neighbor Discovery for IP version 6 (IPv6) (231673 bytes)
- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (63394 bytes)
- Considerations on M and O Flags of IPv6 Router Advertisement (27850 bytes)
- Neighbor Discovery Proxies (ND Proxy) (36922 bytes)
- Transition Scenarios for 3GPP Networks (RFC 3574) (0 bytes)
- Unmanaged Networks IPv6 Transition Scenarios (RFC 3750) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Sub-IP Area Standards (RFC 3793) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Operations & Management Area Standards (RFC 3796) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Application Area Standards (RFC 3795) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Transport Area Standards (RFC 3794) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Security Area Standards (RFC 3792) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Routing Area Standards (RFC 3791) (0 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Internet Area Standards (RFC 3790) (0 bytes)
- Introduction to the Survey of IPv4 Addresses in Currently Deployed IETF Standards (RFC 3789) (0 bytes)
- Evaluation of Transition Mechanisms for Unmanaged Networks (RFC 3904) (0 bytes)
- Security Considerations for 6to4 (RFC 3964) (0 bytes)
- Application Aspects of IPv6 Transition (RFC 4038) (0 bytes)
- Scenarios and Analysis for Introducing IPv6 into ISP Networks (RFC 4029) (0 bytes)
- IPv6 Enterprise Network Scenarios (RFC 4057) (0 bytes)
- Procedures for Renumbering an IPv6 Network without a Flag Day (RFC 4192) (0 bytes)
- Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks (RFC 4215) (0 bytes)
- Basic Transition Mechanisms for IPv6 Hosts and Routers (RFC 4213) (0 bytes)
- IPv6 Neighbor Discovery On-Link Assumption Considered Harmful (19120 bytes)
- IPv6 Enterprise Network Analysis (78474 bytes)
- Reasons to Move NAT-PT to Experimental (62143 bytes)
- ISP IPv6 Deployment Scenarios in Broadband Access Networks (193470 bytes)
- IPv6 Network Architecture Protection (94900 bytes)
- IPv6 Transition/Co-existence Security Considerations (89221 bytes)
- Using IPsec to Secure IPv6-in-IPv4 Tunnels (44155 bytes)
- Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks (24720 bytes)
- Best Current Practice for Filtering ICMPv6 Messages in Firewalls (64389 bytes)
- Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents (RFC 3776) (0 bytes)
- Mobility Support in IPv6 (RFC 3775) (0 bytes)
- Mobile Node Identifier Option for Mobile IPv6 (MIPv6) (RFC 4283) (0 bytes)

... and, or ......

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 MIP6 (37034 bytes)
- IP Address Location Privacy and Mobile IPv6: Problem Statement (17884 bytes)
- Dual Stack Mobile IPv6 (DSMIPv6) for Hosts and Routers (53869 bytes)
- MIP6-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.

Prefixes	ASnum	AS Description
69	AS1221	ASN-TELSTRA Telstra Pty Ltd
21	AS30071	ASN-TBONE - TowardEX Technologies Network
12	AS4621	UNSPECIFIED UNINET-TH
7	AS18062	GRANGENET-AS-AP GRid And Next GEneration NETwork
6	AS12008	ULTRADNS - Centergate Research, LLC.
5	AS3557	ISC-CALIFORNIA Internet Systems Consortium, Inc.
5	AS9270	APAN-KR-AS Asia Pacific AdvNetwork Korea(APAN-KR) Consortium
5	AS7660	APAN-JP Asia Pacific Advanced Network - Japan
5	AS8175	CETLINK - Computer Enhancement Technologies, Inc.
4	AS2518	JPNIC-ASBLOCK-AP JPNIC
4	AS4555	EP0-BLK-ASNBLOCK-5 - Exchange Point Blocks
4	AS6175	SPRINTLINK9 - Sprint
4	AS8472	VIAG-INTERKOM BT (Germany)
4	AS9316	DACOM-PUBNETPLUS-AS-KR DACOM PUBNETPLUS
4	AS16838	VERISIGN-CORP - VeriSign Infrastructure & Operations
4	AS20495	WEDARE We Dare BV Autonomous System
3	AS109	CISCO-EU-109 Cisco Systems Global ASN - ARIN Assigned
3	AS284	UUNET-AS - UUNET Technologies, Inc.
3	AS1200	AMS-IX1 Amsterdam Internet Exchange (AMS-IX) Peering AS
3	AS1273	CW Cable & Wireless

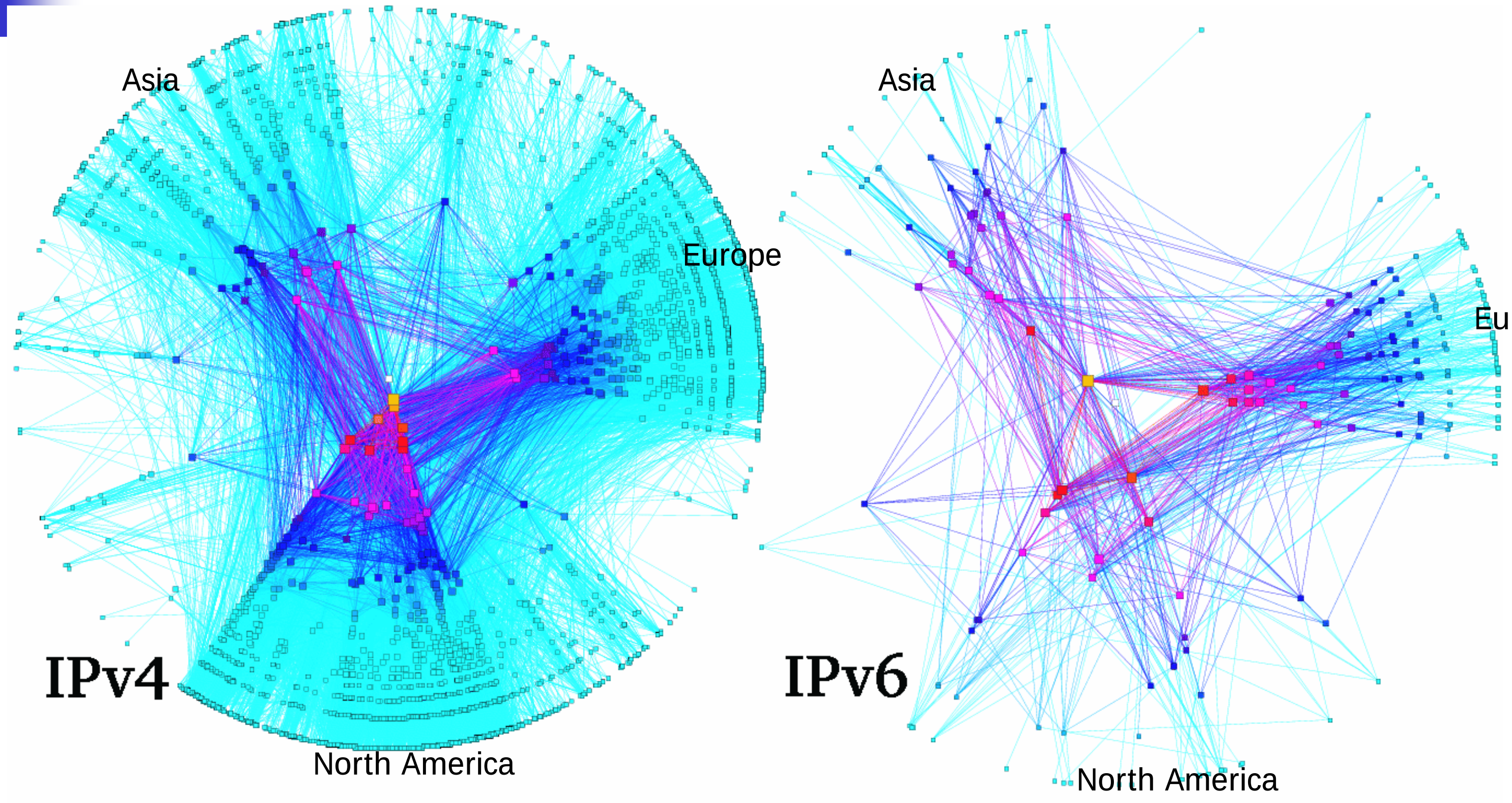
Current IPv4 Global Routing Tables (2005-12-15)

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.

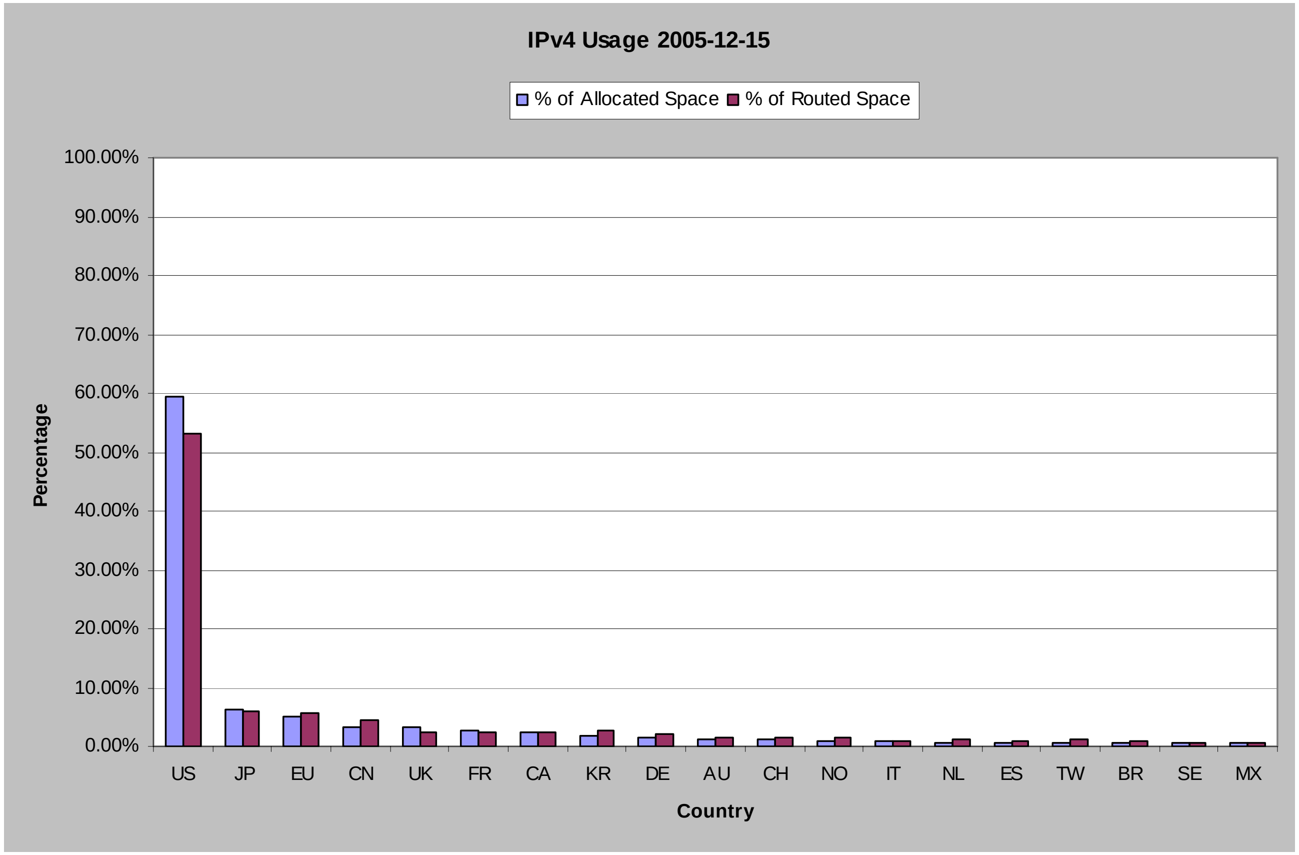
Prefixes	ASnum	AS Description
1447	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
1185	AS4323	TWTC - Time Warner Telecom
1057	AS174	COGENT Cogent/PSI
1050	AS721	DLA-ASNBLOCK-AS - DoD Network Information Center
1006	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street
970	AS701	ALTERNET-AS - UUNET Technologies, Inc.
969	AS6197	BATI-ATL - BellSouth Network Solutions, Inc
916	AS2386	INS-AS - AT&T Data Communications Services
883	AS18566	COVAD - Covad Communications
839	AS9583	SIFY-AS-IN Sify Limited
838	AS1239	SPRINTLINK - Sprint
662	AS1221	ASN-TELSTRA Telstra Pty Ltd
660	AS20115	CHARTER-NET-HKY-NC - Charter Communications
657	AS209	ASN-QWEST - Qwest
632	AS11492	CABLEONE - CABLE ONE
615	AS4766	KIXS-AS-KR Korea Telecom
609	AS4755	VSNL-AS Videsh Sanchar Nigam Ltd. Autonomous System
596	AS702	AS702 MCI EMEA - Commercial IP service in Europe
592	AS22773	CCINET-2 - Cox Communications Inc.
572	AS852	ASN852 - Telus Advanced Communications

Service Providers …



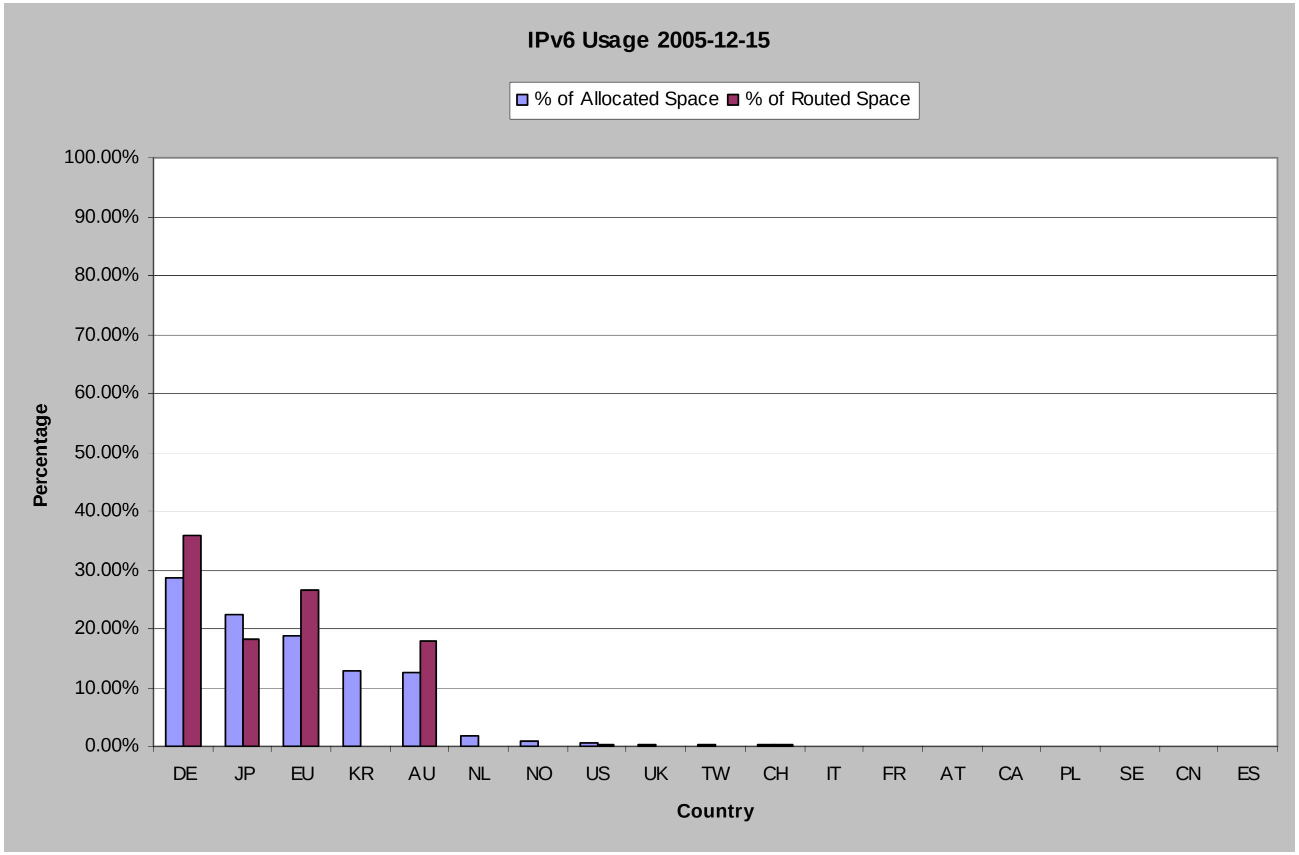
Source: http://www.caida.org/analysis/topology/as_core_network/ipv6.xml

Who Has the IPv4 Addresses?



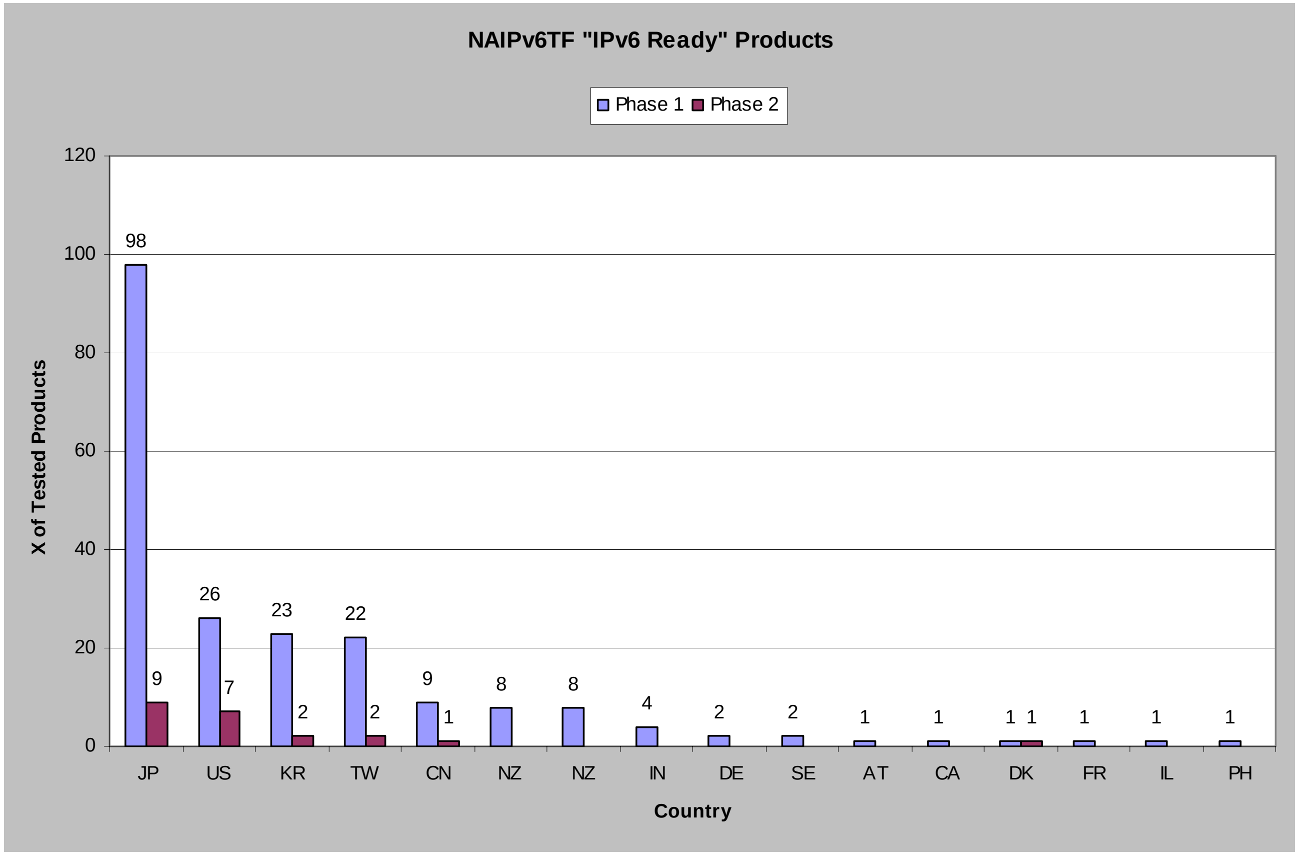
Source: http://www.potaroo.net/tools/ipv4/

Who Has the IPv6 Addresses?



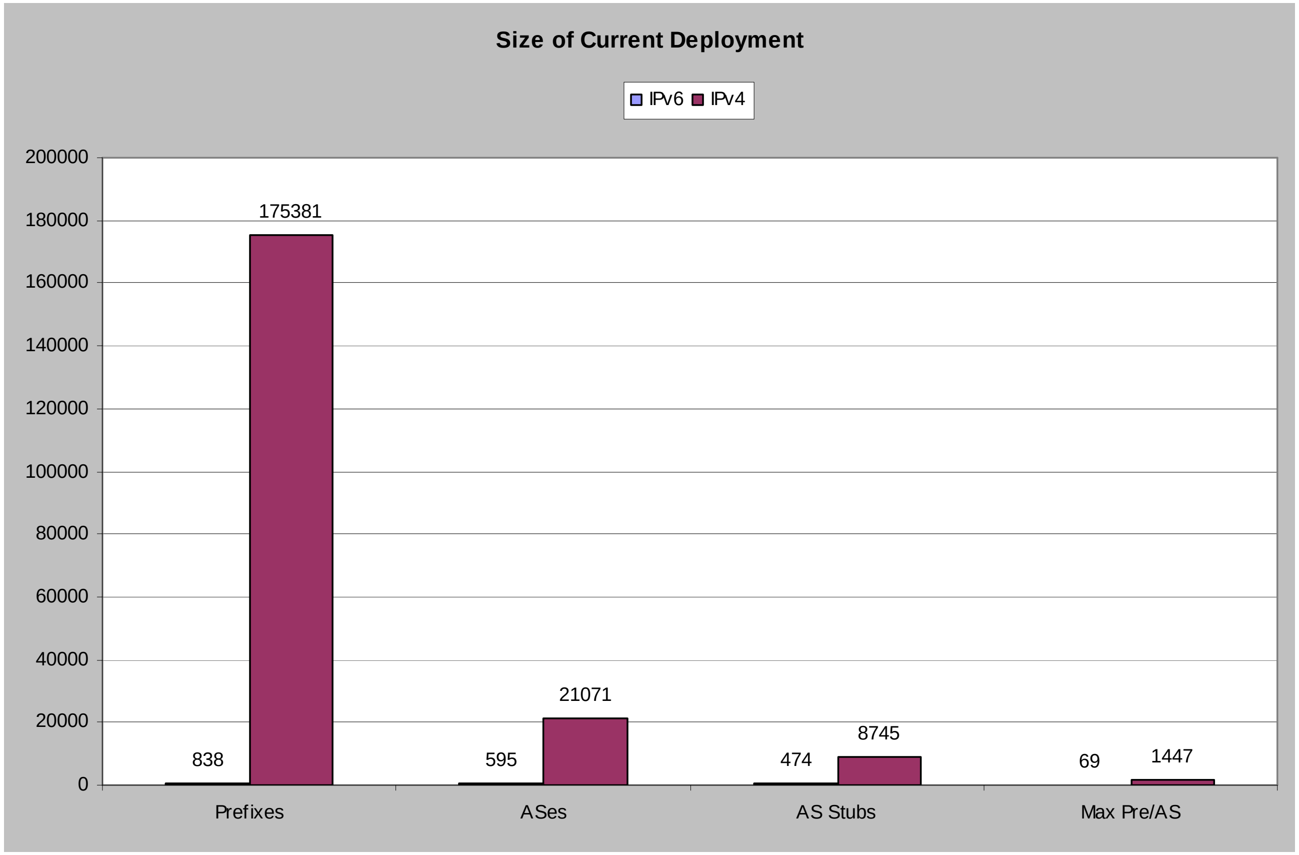
Source: http://www.potaroo.net/tools/ipv6/

Who Has the IPv6 Products?



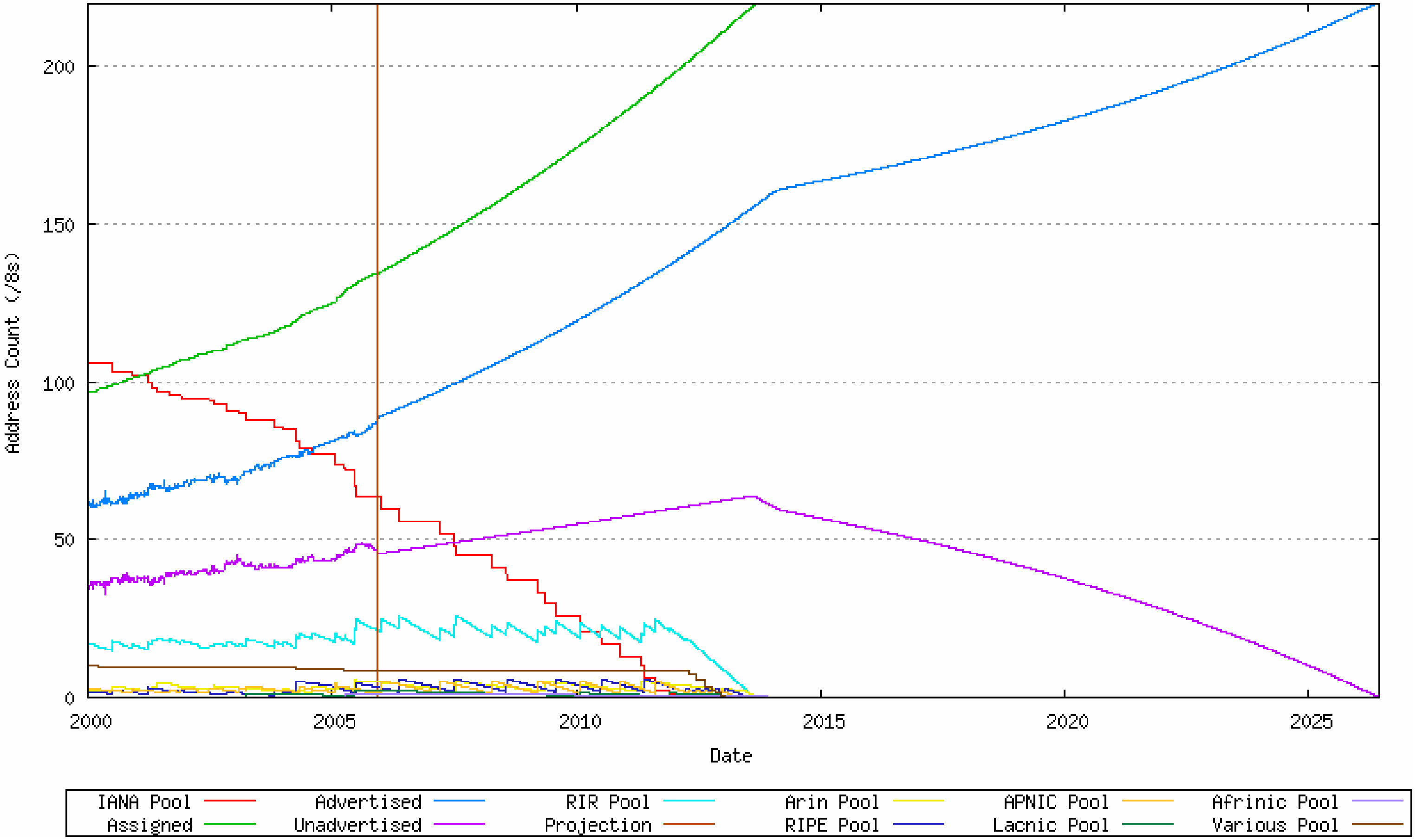
Source: http://www.ipv6ready.org/

Let’s Keep a Little Technology Lifecycle Perspective!



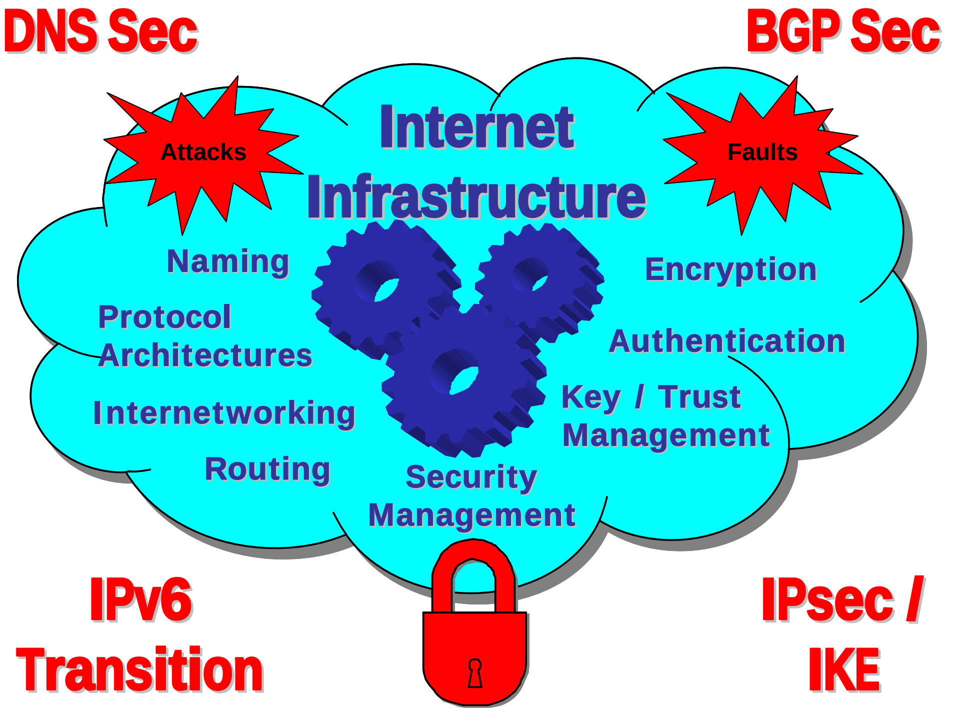
- IPv6 deployment is in its infancy – trend significance?

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"

NIST and IPv6

- **NIST/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 Security Technologies: IPsec/IKE, IETF specifications, reference implementations, interoperability test systems, AES/SHA underlying technologies, PKI specifications.
    - 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?

Internet Infrastructure Protection

Currnet 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:

- S. Rose, et al, **DNS Security Introduction and Requirements** , <draft-ietf-dnsext-dnssec-intro-13.txt>, Oct 2004
- S. Rose, et al, **Resource Records for DNS Security Extensions** , <draft-ietf-dnsext-dnssec-records-11.txt>, Oct 2004
- S. Rose, et al, **Protocol Modifications for the DNS Security Extensions** , <draft-ietf-dnsext-dnssec-protocol-09.txt>, Oct 2004
- S. Rose, et al., **Limiting the Scope of the KEY Resource Record** (RR), <RFC 3445> Standards Track.
- M.K. Shin, et al., **Link Scoped IPv6 Multicast Addresses**,<draft-ietf-ipv6-link-scoped-mcast-05.txt>, Sep 2004.
- M.K. Shin, et al., **IPv4 Prefix Options for DHCPv6**,<draft-shin-dhc-dhcpv6-opt-ipv4-prefix-00.txt>, Sept 2004.
- M.K. Shin, et al., **Application Aspects of IPv6 Transition**,<draft-ietf-v6ops-application-transition-03.txt>, Sept 2004

Publications:

- O. Kim and D. Montgomery, "**Behavioral and Performance Characteristics of IPsec/IKE in Large-Scale VPNs**," Proc. of the IASTED International, Conference on Communication, Network, and Information Security, Dec., 2003.

Tools for Industry:

- **SZIT** - Secure Zone Integrity Checker – http://www-x.antd.nist.gov/dnssec/
- **DNS Zone File Anonymizer** – http://www-x.antd.nist.gov/dnssec/
- **NIIST -** NIST IKE(v1/v2)/IPsec Simulation Tool - http://www.antd.nist.gov/niist/
- **IPsec-WIT:** Web based IPsec/IKE interoperability test system - http://ipsec-wit.antd.nist.gov/
- **Cerberus/PlutoPlus: -** IPsec/IKE reference implementation – http://www.antd.nist.gov/cerberus/

For more information ….

- NIST Efforts in Internet Infrastructure Protection and Resilient, Agile Networking
  - Advanced Networks - http://www.antd.nist.gov/
  - Computer Security - http://csrc.nist.gov/

NIST
National Institute of Standards and Technology
. . .working with industry to develop and apply technology, measurements and standards

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.