Evolving the Core: Deployment Challenges and the Internet

J. Scott Marcus
Senior Advisor for Internet Technology
Office of Strategic Planning and Policy Analysis, FCC

The opinions expressed are my own, and do not necessarily reflect the views of the FCC or any of its commissioners

… and don't worry.
Nobody is looking to "regulate the Internet".

A Glacial Pace of Deployment?

- Enhancements to DNS security
- Operational and protocol enhancements to the BGP-4 exterior routing system
- IPv6 (tangentially relevant to security)

See *The National Strategy to Secure Cyberspace* (DRAFT), February, 2003

- Differentiated services (across multiple providers)
- Multicast
- … and more. But whether all of these capabilities are *desirable* is debatable.
- Why are these capabilities problematic, but others not?

Thought Questions

- Might common factors be at work here?
- Are market incentives alone sufficient to ensure that societally vital enhancements to Internet infrastructure (including security enhancements) will be deployed?
- If not, is it possible to *correctly* identify and prioritize those features that are unlikely to be deployed without “help”?

More Thought Questions

- What public policy measures are available to foster deployment of those features?
- What are the costs and benefits of those measures?
- What are the prospects that they will be effective?

Public Goods

"Things that can be consumed by everybody in a society, or nobody at all. They have three characteristics. They are:

- non-rival – one person consuming them does not stop another person consuming them;
- non-excludable – if one person can consume them, it is impossible to stop another person consuming them;
- non-rejectable – people cannot choose not to consume them even if they want to.

Examples include clean air, a national defence system and the judiciary. The combination of non-rivalry and non-excludability means that it can be hard to get people to pay to consume them, so they might not be provided at all if left to market forces ..."

From economist.com.

Three Views of the Role of Government

- NTIA Discussion Draft, “Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)” (July 2004), at: http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/
- NIAC, “Best Practices for Government to Enhance the Security of National Critical Infrastructures” (April 2004), at: http://www.dhs.gov/dhspublic/display?theme=9&content=3445
- Marcus, “Evolving Core Capabilities of the Internet”, to appear in the *Journal on Telecommunications and High Technology Law* (October 2004).

Market Forces

- Economic incentives
  - Sufficiency
  - Alignment - Who pays? Who benefits?
  - Quantifiability
  - Time frame over which benefits are generated
- The economics of network externalities
- Transaction costs and the end-to-end principle

Economic Incentives

- Who pays?
  - The service provider?
  - Ultimately, the customer?
  - The Government?
- Who benefits?
  - The service provider?
  - Society at large?
  - How can the benefits be quantified?
- In what time frame?
  - Financial markets have short horizons.
  - Difficult to insure against a “30 year flood”.
  - “Après moi, le déluge!”

The Business Case

"Scott, you don't have to wait a year or two to find out whether we are having problems getting this stuff deployed. We already know the answer. There is nothing new in these reports. All of this has been known for years. If we were able to craft business cases for our management, all of this would have been done long ago."

- Participant, ISP Working Group, CIPB

More on Economic Incentives

" … Underinvestment occurs because conditions exist that prevent firms from fully realizing or appropriating the benefits created by their investments, causing firms to view prospective investments as having expected rates of return below the firm's minimum acceptable rate of return (hurdle rate). … research to support development of interoperability solutions, conformance testing, and ... standards are all paradigmatic examples of cases where private returns to investment can be less than both social returns and private hurdle rates."

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), NTIA, 2004

Network Externalities

- Some capabilities are worth more as more consumers adopt them. Nothing succeeds like success.
- The societally optimal value is not necessarily where the market would settle without “help”.
- The initial adoption hump:
  - telephone - Universal Service
  - VCRs - widespread deployment for time shifting antedated the emergence of a rental industry.
  - CD players - vertical integration with recording studios
  - black and white TV - industry / gov’t standards

Cf. Rohlffs, *Bandwagon Effects in High-Technology Industries*, 2001.

More on Network Externalities

"Sufficient levels of investment are needed to minimize interoperability problems and to realize the positive network externalities generated by IPv6. Because network externalities are difficult for the private sector to appropriate, the public sector frequently supports investment in infratechnologies, such as conformance testing mechanisms and certification protocols."

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), NTIA, 2004

The End-to-End Principle

- A guiding principle of Internet architecture.
- Certain features are best implemented, not in the network, but in the end systems that implement the application. It is counterproductive for the network to also provide those same features.
- It is easy to incorporate new innovations at the Application Layer (e.g. the WorldWide Web).
- It is also easy to incorporate new innovations at the Data Link and Physical Layers (e.g. cable modem, DSL, Wi-Fi).

The End-to-End Principle

- Innovations that impact the global system may be harder.
  - Requirements for interoperability and upward compatibility.
  - Limited value until ubiquitously (or at least widely) available.
  - Many participants -> high transaction costs.

Domain Name System Vulnerabilities

- No authentication of the domain name server.
- No assured integrity of the DNS response.
- No assurance that the information in the DNS server has not been maliciously altered.
- Exposure to Denial of Service (DoS) attacks.

DNS Security Mechanisms

- Secret Key Transaction Authentication for DNS (TSIG)
  - MD5 cryptographic hash/checksum.
  - Authenticates sending system and transmission integrity.
  - Does not authenticate underlying data.
  - Lack of a key distribution mechanism limits applicability.
- Domain Name System Security Extensions (DNSSEC)
  - Public key cryptography facilitates key distribution.
  - Chain of trust proceeds from the DNS root to the leaves.
  - Provides authentication, integrity and object security.
  - Unambiguously deals with lack of existence of a DNS name.

Deployment Considerations: TSIG

- A point solution rather than a general solution.
- Computational and operational cost are modest.
- Can be implemented by a pair of DNS servers, e.g. for zone transfers.
- Transaction costs are low.
- Deployable today.

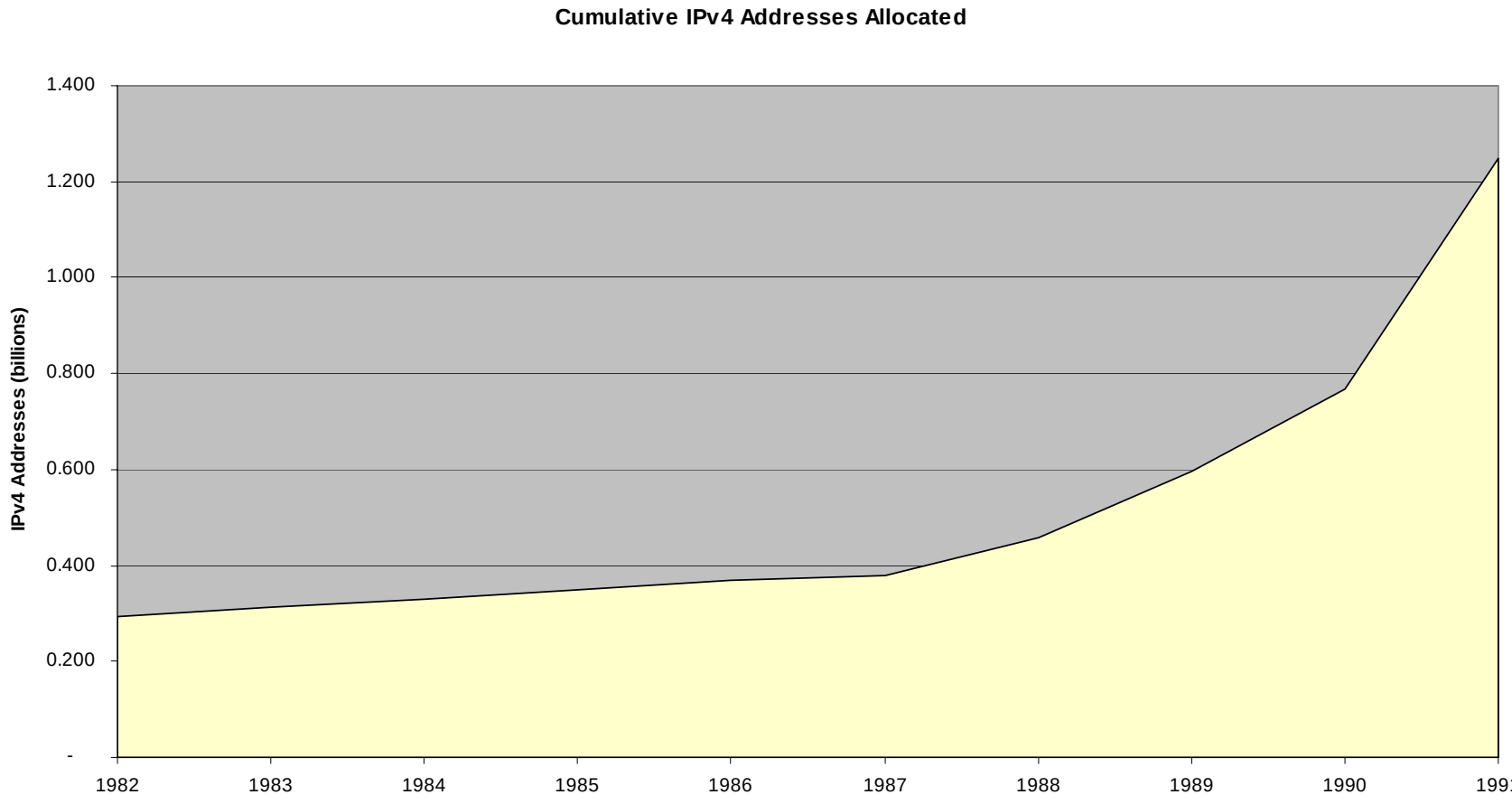
Deployment Considerations: DNSSEC

- An elegant, general solution.
- Computational and operational complexity is high.
- Solution ideally involves a great many components, from DNS root servers to TLDs to SLDs … and finally to DNS clients in end user systems.
- Transaction costs for global deployment are considerable.
- DNSSEC has often been viewed as difficult and immature.

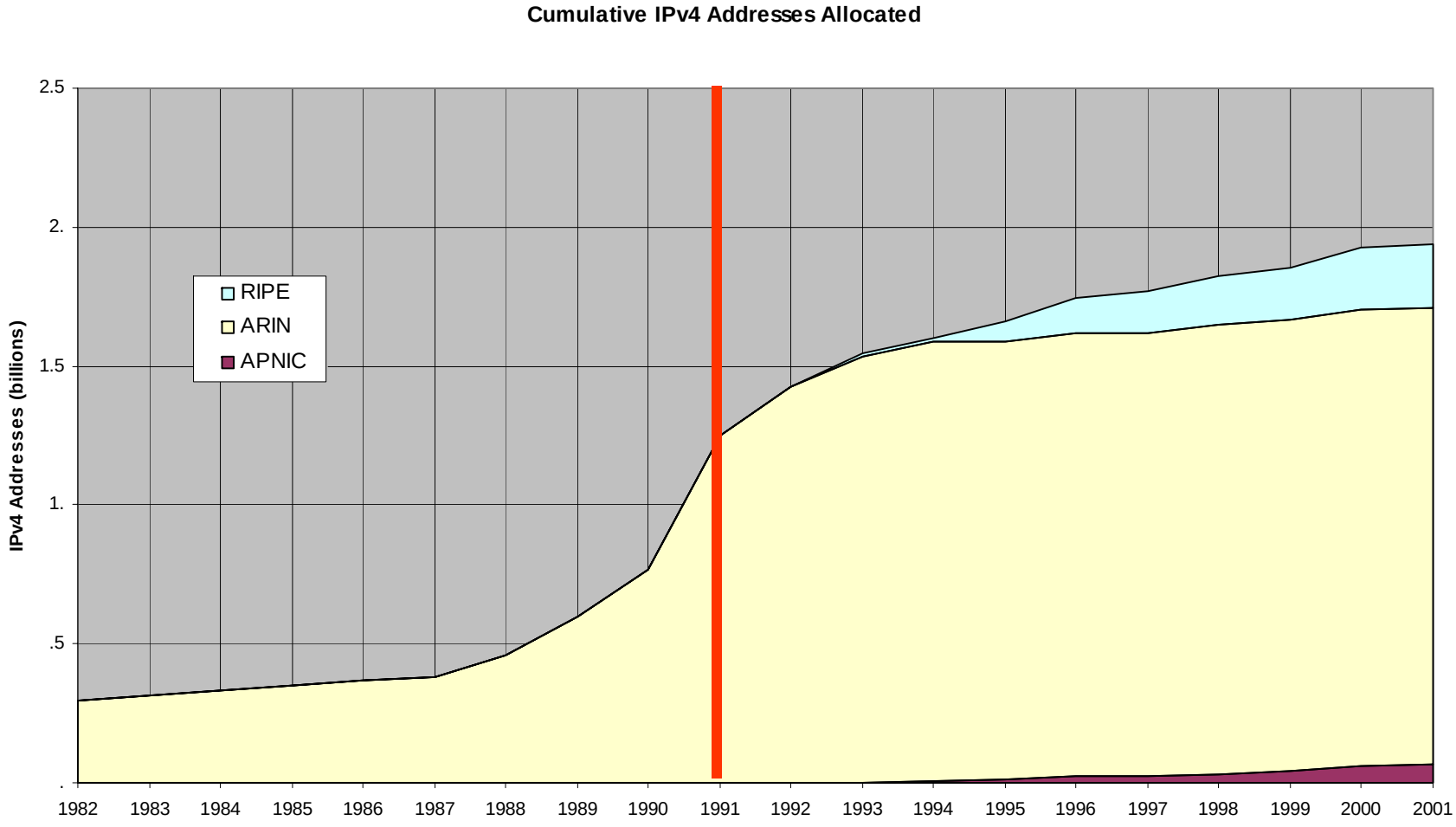
Internet Protocol version 6 (IPv6)

- In the early Nineties, the then-current version of the Internet Protocol (IPv4) was running out of addresses.
- Technical specifications for a new version, IPv6, were completed in present form in 1998.
  - Expands address field from 32 bits to 128 bits.
  - Support for IPSEC security protocol.
  - Support for Quality of Service (QoS).
  - Some enhancements for configuration and mobility.
- What happened?

IPv4 Usage Trends



IPv4 Usage Trends



What Happened?

- IPv4 addresses were not exhausted.
  - The Regional Internet Registries (RIRs) implemented an effective system of "rationing".
  - The system nonetheless imposes subtle societal costs.
  - IPv4 addresses will eventually be exhausted, but probably not for many years.
- The economic case is not compelling today.

What Happened?

- IPSEC is available in both IPv4 and IPv6.
- QoS/ToS is not much used, and is available in both IPv4 and IPv6.
- IPv6 may offer mobility and configuration advantages over IPv4.
- The economic case is not compelling today.

Who would have to act to deploy IPv6?

- Routers and networking equipment
  - Manufacturers
  - ISPs
- End systems
  - PC operating systems, notably Windows
  - Applications
- DNS
- IP address administration (RIRs and NSO)
- … and more …

Who would have to act to deploy IPv6?

- Long value chain –> transaction costs are high.
- Benefits of migration are limited until large numbers of end users have migrated.

Public Policy Considerations

- **Balance**
  - What are the risks of action?
  - What are the risks of inaction?
- **Minimalism**
  - What is the least intrusive intervention that will achieve the desired public policy objective?
  - "That government is best which governs least."

    - Thoreau

Public Policy Implications

- Alternative forms of intervention
- NTIA's consultation on IPv6
- NIAC's report on Best Practices for Government
- Case studies

Public Policy Alternatives

- Help industry to coalesce consensus.
- Collect relevant data and statistics.
- Provide “seed money” for research and for interoperability testing.
- Support desired services through government’s own purchasing preferences.
- Provide remedies (e.g. under tort law) where firms fail to achieve a recognized standard of care.*
- Fund the deployment of desired services.
- Mandate the use of desired services.

* - *Critical Information Infrastructure Protection and the Law*, National Academies, 2003

Helping to Coalesce Industry Consensus

- Government can use the “bully pulpit” to advance public policy goals.
- Support sharing of information on best practices, while protecting sensitive information.
- Mitigate antitrust concerns when competitors discuss joint actions that are not anticompetitive.
- Stimulate standards bodies to focus on relevant issues.

Helping to Coalesce Industry Consensus

- NTIA's public consultation on IPv6
- FCC's NRIC
- DHS's NIAC

Impediments to Data Collection and Information Sharing

- Antitrust concerns
- Obligations to make data publicly available
  - FOIA concerns
    - Need for predictability and certainty
    - Perception versus reality
    - DHS enabling legislation
  - State sunshine laws

Cf. *Critical Information Infrastructure Protection and the Law*, National Academies, 2003

A Role for Government in IPv6?

- "Although the deployment of IPv6 has occurred more slowly than was anticipated when the IETF began work on IPv6, there is no evidence of a market failure warranting government intervention."
- Government support for R&D
  - Research funding
  - Human resources
  - Testbeds and interoperability
- Government as consumer
- Information dissemination

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), NTIA, 2004

A Role for Government in IPv6?

"… government could take one or more of the following courses:

- play a major role in coordinating the development of IPv6 standards, protocols, and conformance;
- be an active participant in identifying and facilitating solution of technology and interoperability issues; and
- stimulate adoption as a major consumer of IPv6 products and services when in the best interest of individual government agencies.

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), NTIA, 2004

A Role for Government in IPv6?

"[I]ndustry should continue to take the lead in developing the IPv6 standards architecture, with coordination support and participation from government. Similarly, industry consortia and academic institutions should take the lead in conformance testing and development of interoperability solutions to support implementation, with support and participation from government. Finally, government has an important role to play as a major consumer of IPv6 products and services, but it should not mandate adoption by industry or government agencies in the United States. Private sector decisions to purchase IPv6 products and services should be market driven, without influence from federal government mandates."

Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), NTIA, 2004

NIAC: A Role for Government?

"… where market forces are free to operate, they will be the most efficient and efficacious vehicle to enhance the security posture of critical infrastructures. However, some suggest that the pace of change may be too slow and the response may be incomplete. If market forces prove unable to operate efficiently and quickly, government should consider timely intervention, but only when there is a good characterization of the potential harm that could occur from an attack, and a better understanding of the role that market forces play in promoting an improved security posture …"

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC Framework

"1. Deep understanding of sector dynamics is needed for effective intervention.

2. Organizations are responding through competition and cooperation, to address threats.

3. Government action may be required in some sectors.

4. A common framework may be used to discuss the role of market intervention.

5. Identified best practices should be considered when intervention is planned."

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC's Common Framework

1. Are there network interdependencies in the sector?
2. Do security concerns drive customers to switch?
3. Is voluntary sector activity already occurring?
4. Can the sector exert peer pressure?
5. Do attacks occur frequently?
6. Could the attack cause catastrophic injury or major economic damage?
7. Is the industry profitability high enough to invest in security?
8. Is there sufficient expertise to execute a plan?

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC: Identified Best Practices

1. Develop plans in concert with industry.
2. Mandate outcomes rather than specific actions.
3. Ensure alignment between federal, state, and local regulations.
4. Evaluate all new and existing rules through a "security filter".
5. Incorporate flexibility or sunset provisions.
6. Funding may be necessary to fulfill government mandates.
7. Implement interventions in phases.

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC: Intervention in the Internet?

- "… [R]egulation of the Internet is unwise, and market innovation will continue to drive adoption and innovation.
- [There is a risk of] providing a roadmap of vulnerabilities to nefarious parties intent on causing damage.
- [There is a risk of government making] unsophisticated decisions yielding less, rather than more security.
- The political process … could result in an inefficient program that could yield a false sense of security.
- Government regulation of technology may blunt innovation resulting in less consumer choice, economy and security."

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC: Alternative Approaches to Intervention

- "Policy makers could consider incentives like tax credits, R&D subsidies, procurement leverage, and enforcement of existing criminal laws.
- [T]he federal government could demand strict security best practices for technology purchased by all its departments and agencies.
- [T]he government could work with the private sector to develop security standards, test products and publish results…"

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

NIAC: Alternative Approaches to Intervention

- "The government could also fund more security research to better understand the cyber threats and ways the IT sector can defend against them.
- [A] program of insurance, liability, and tax incentives is more likely to yield an effective, comprehensive, and ongoing program of cyber-security consistent with the evolving and international nature of technology and threats."

Best Practices for Government to Enhance the Security of National Critical Infrastructures, NIAC, April 2004

New NIAC Recommendation

- "Sponsor research on adoption of security Best Current Practices. Focus on:
  - Surveys or other techniques to determine adoption and deployment rates of cyber security best practices within the critical infrastructure sectors;
  - Investigation into the best-practice adoption and deployment decision process, including perceived costs, benefits, risks, rewards, competitive advantages, externalities, and other factors affecting decsions…"

Hardening the Internet, NIAC, October 2004

Promising Case Studies

- Government funding and sponsorship of the ARPAnet.
- Government funding of the University of California at Berkeley to incorporate TCP/IP protocols into Berkeley UNIX.
- These and other related initiatives created necessary network externalities and played an indispensable role in the ultimate success of the Internet.

Sobering Case Studies

- Government OSI Protocol (GOSIP) - the purchasing power of the U.S. Government and of governments worldwide was insufficient to drive global adoption of OSI protocols. TCP/IP won out, largely due to network externality advantages.
- Metric conversion - A similar story. The U.S. Government has been officially committed to metric since the Seventies, and most measures short of an outright mandate have been attempted. Progress has nonetheless been glacial.

Public Policy Considerations

- **Balance**
  - What are the risks of action?
  - What are the risks of inaction?
- **Minimalism**
  - What is the least intrusive intervention that will achieve the desired public policy objective?
  - "That government is best which governs least."

    - Thoreau