IPv6:

POLITICS OF THE NEXT GENERATION INTERNET

by

LAURA E. DENARDIS

Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Science and Technology Studies

Janet Abbate, Ph.D.
(Chair)

Barbara Allen, Ph.D.
Gary Downey, Ph.D.
J. Scott Hauger, Ph.D.
Richard Hirsh, Ph.D.

March 15, 2006

Alexandria, VA

Keywords:
Internet History, Computer Networking, Internet Protocols
Technology Standards, Globalization, Internet Governance

IPv6: Politics of the Next Generation Internet

Laura E. DeNardis

Abstract

IPv6, a new Internet protocol designed to exponentially increase the global availability of Internet addresses, has served as a locus for incendiary international tensions over control of the Internet. Esoteric technical standards such as IPv6, on the surface, appear not socially significant. The technical community selecting IPv6 claimed to have excised sociological considerations from what they considered an objective technical design decision. Far from neutrality, however, the development and adoption of IPv6 intersects with contentious international issues ranging from tensions between the United Nations and the United States, power struggles between international standards authorities, U.S. military objectives, international economic competition, third world development objectives, and the promise of global democratic freedoms. This volume examines IPv6 in three overlapping epochs: the selection of IPv6 within the Internet's standards setting community; the adoption and promotion of IPv6 by various stakeholders; and the history of the administration and distribution of the finite technical resources of Internet addresses. How did IPv6 become the answer to presumed address scarcity? What were the alternatives? Once developed, stakeholders expressed diverse and sometimes contradictory expectations for IPv6. Japan, the European Union, China, India, and Korea declared IPv6 adoption a national priority and an opportunity to become more competitive in an American-dominated Internet economy. IPv6 activists espoused an ideological belief in IPv6, linking the standard with democratization, the eradication of poverty, and other social objectives. The U.S., with ample addresses, adopted a laissez-faire approach to IPv6 with the exception of the Department of Defense, which mandated an upgrade to the new standard to bolster distributed warfare capability. The history of IPv6 includes the history of the distribution of the finite technical resources of "IP addresses," globally unique binary numbers required for devices to exchange information via the Internet. How was influence over IP address allocation and control distributed globally? This history of IPv6 explains what's at stake economically, politically, and technically in the development and adoption of IPv6, suggesting a theoretical nexus between technical standards and politics and arguing that views lauding the Internet standards process for its participatory design approach ascribe unexamined legitimacy to a somewhat closed process.

ACKNOWLEDGEMENTS

Janet Abbate, dissertation advisor and friend, provided invaluable contributions to this work. The genesis of this project was a fall, 2002, research paper written for Janet's *Culture, Politics, and History of the Internet* course. In the following years, countless discussions with Janet crystallized the theoretical and thematic directions of this project. Mentor Scott Hauger provided intellectual guidance, encouragement, and ideas which greatly influenced this project as well as many other endeavors. I am also grateful to Barbara Allen for her significant theoretical influence and ongoing support, and wish to thank Gary Downey and Richard Hirsh for their strong intellectual presence on my committee and their important contributions. A special thanks to Leonard and Gail DeNardis, for their encouragement and for cultivating a zeal for knowledge. Finally, Deborah Smith is the daily inspiration and support steadying the journey.

CONTENTS

LIST OF FIGURES AND TABLES

FIGURES

TABLES

CHAPTER I: INTRODUCTION

FDDC:AC10:8132:BA32:4F12:1070:DD13:6921. Superficially, the preceding hexadecimal representation of an IPv6 address seems neutral and devoid of social significance. Yet various groups have promoted IPv6 as a catalyst for global democratic freedoms, enhanced U.S. military capability, new economic opportunities in the European Union and Asia, and improved Internet security. Some advocates have deemed IPv6 a deontological imperative, citing a societal obligation to embrace IPv6 to improve children's lives and ameliorate a number of social problems.

1.1 Definition of the Problem

IPv6, or Internet Protocol Version 6, is an Internet routing and addressing standard designed to exponentially expand the number of devices able to connect to the Internet. Each device exchanging information over the Internet possesses a unique number (an IP address) identifying its virtual location, somewhat analogous to a unique postal address identifying a home's physical location. The longstanding Internet address standard, IPv4, or Internet Protocol Version 4, originated in the early 1980s and specified a unique 32-bit number such as 01101001001010100101100011111010 for each Internet address.[1] This address length of 32 bits provided 2^{32}, or 4,294,967,296, possible unique Internet addresses.

In 1990, the Internet standards community identified the potential depletion of these 4.3 billion addresses as a crucial design concern. U.S. institutions had received substantial IP address assignments when the Internet was primarily an American endeavor, raising concerns that the remaining address reserve might not meet emerging requirements of rapid international growth and new applications like wireless Internet access and Internet telephony. Against the backdrop of competing international protocols, the Internet standards community selected a new network protocol, IPv6, to expand the Internet address space. Originally designated the Next Generation Internet

[1] Jon Postel, editor, "DOD Standard Internet Protocol," RFC 760, January, 1980, documents the original Internet Protocol specification. See also Jon Postel, "Internet Protocol, DARPA Internet Program Protocol Specification Prepared for the Defense Advanced Research Projects Agency," RFC 791, September, 1981.

Protocol (IPng), the IPv6 standard expanded the address length from 32 to 128 bits for each address, supplying 2^{128}, or 340,232,366,920,938,463,463,374,607,431,768,211,456 (340 undecillion) unique addresses.

IPv6 stakeholders expressed a variety of expectations for the new standard. Governments in Japan, Korea, China, India, and the European Union designated IPv6 as a national priority, both as a solution to projected address shortages and as an economic opportunity to develop new products and expertise in an American dominated Internet industry. IPv6 advocacy groups cited international imbalances in address allocation statistics as indicative of the standard's significance and, with enthusiasm approaching monomania, described IPv6 as a mechanism for spreading democratic freedoms, solving various social problems, and promoting third world development. In contrast to international address scarcity concerns, United States corporations, universities, and government agencies possessed ample IP addresses. Even in 1993, years after the standards community projected international Internet address shortages, Texas-based Halliburton Company received more than 16 million Internet addresses, or 1/256 of the worldwide supply of addresses.[2] The United States, with abundant Internet addresses and a large IPv4 installed base, remained relatively dispassionate about IPv6 until discussions commenced in the area of cybersecurity. Internet security concerns after the September 11, 2001, terrorist attacks prompted the development of a *National Strategy to Secure Cyberspace*, the culmination of a lengthy analysis seeking to reduce U.S. vulnerability to critical information infrastructure attacks. One of the recommendations called for improving the security of several network protocols including the Internet Protocol.[3] The report noted that Japan, the European Union, and China already planned upgrades from IPv4 to IPv6 and cited "improved security features"[4] as an inducement. In 2003, the United States Department of Defense formally established a directive mandating a

[2] Halliburton Company received the Class A address block 034/8 in March, 1993, according to the "Internet Protocol V4 Address Space" record of the Internet Assigned Numbers Authority. (Accessed at www.iana.org/assignments/ipv4-address-space on June 4, 2003). See also Elise Gerich, "Guidelines for Management of IP Address Space," RFC 1466, May, 1993.

[3] The February, 2003, U.S. *National Strategy to Secure Cyberspace* addressed three network protocols: the Domain Name System (DNS), Border Gateway Protocol (BGP), and the Internet Protocol (IP). (Accessed at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf in November, 2003).

[4] Ibid, page 30.

transition to IPv6 by 2008, citing a requirement for greater security and demand for more addresses for military combat applications.[5] Despite the ratification of formal IPv6 specifications and more than a decade of predictions about imminent conversion, IPv6 adoption proceeded lethargically. Many anticipate the two standards (IPv4 and IPv6) coexisting indefinitely, possibly raising intransigent security, management, and administrative challenges.

The history of IPv6 includes the history of Internet address distribution and administration, raising important issues of international resource equitability and control of finite technical resources. Centralized control has historically existed in the area of IP address allocation, in part to maintain the architectural principle of globally unique addresses. Oversight of these finite technical resources originated with a single trusted individual, Jon Postel, but gradually evolved to geographically distributed, international registries such as Réseaux IP Européens-Network Coordination Centre (RIPE-NCC), the Asia Pacific Network Information Centre (APNIC), the Latin America and Caribbean Network Information Centre (LACNIC), and the African Network Information Centre (AfriNIC). Despite this global dispersion of IP addresses and assignment responsibility, definitive control of the entire address reserve, including the allocation of address resources to international registries, remained centralized and eventually became an administrative function under the auspices of the controversial entity ICANN, the Internet Corporation for Assigned Names and Numbers. International concerns have centered on questions about ICANN, a private entity incorporated in California and overseen by the United States Commerce Department, retaining Internet governance authority, including centralized oversight of IPv6 and IPv4 addresses.

This research project has examined what is at stake politically, economically, and technically in the development and adoption of IPv6. The standard**,** on the surface an arcane network protocol invisible to most users, has encompassed intriguing struggles for

[5] United States Department of Defense Memorandum issued by DoD chief information officer, John P. Stenbit for Secretaries of the Military Departments, Subject: "Internet Protocol Version 6 (IPv6)," June 9, 2003. The memorandum stated, "The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities (ref a), depends on effective implementation of IPv6…" (Accessed at http://www.dod.gov/news/Jun2003/d20030609nii.pdf on July 20, 2003).

control of Internet standards development, competitive positioning in Internet markets, and possession and control of finite technical resources.

1.2 Research Questions and Objectives

IPv6 has become the established *de jure* and *de facto* new Internet Protocol designed to replace IPv4. A major research question examined whether there were alternatives to IPv6 in the selection of the so-called Next-Generation Internet Protocol (IPng) and, if so, why these alternatives were rejected. Who decided, and what was at stake in the selection? The project also sought to examine the numerous, often contradictory, expectations for adopting IPv6. What states and institutions had a stake in upgrading or not upgrading to IPv6, and in what political and economic contexts did IPv6 expectations arise? In what ways were IPv6 upgrade decisions and socioeconomic and political order intertwined? A final question addressed the history of Internet address distribution and how address design decisions may have contributed to diminishment of available Internet resources. Were there dissenting voices disputing projections of address scarcity, and in what ways, if any, did the threat of scarcity become aligned with political, economic, and technical objectives? How was (and how is) influence over IP address allocation and control distributed globally, and what was/is at stake?

IPv6 is a surprisingly unexplored area of historical scholarship considering its significance to stakeholders. Some of this inattention could be attributed to the user-transparency or complexity of network protocols or because most IPv6 interest has historically existed outside of the United States. One objective of this work is to elevate the issue of IPv6 and Internet addresses to a broader audience and raise awareness about how centralized Internet institutions ultimately determine the Internet's architectural framework and control the finite Internet address resources required for Internet connectivity. Many Internet scholars extol what they describe as the democratic, participatory Internet standards development process. This project raises critical questions challenging the extent to which Internet standards development is the democratic and participatory process it is often claimed to be. Similarly, IPv6 advocates portray the benefits of IPv6, especially "improved security," as self evident truths. This project raises questions about IPv6 expectations by describing IPv6 implementation tests and dissenting analyses which challenge black and white portrayals of IPv6 as more secure and more manageable than IPv4. Finally, all three areas this project addresses - Internet address distribution, IPv6 selection, and IPv6 adoption – have proceeded outside the realm of market economics, as will be discussed. A theoretical objective is to demonstrate how approaches from the field of Science and Technology Studies enable historical examination and analysis of subject matter related to supply and demand of finite shared resources but not necessarily amenable to classical economic theory.

1.3 Literature Review

No historical accounts of the origin and evolution of the IPv6 standard, as of 2006, existed other than primarily internal accounts of IPv6 technical specifications. An enormous volume of specifications, industry journal articles, and more than forty technical texts address IPv6 technical background, implementation, and management. Notable among these are two books written by individuals directly involved in the selection of IPv6. Christian Huitema, former chair of the Internet Architecture Board (IAB) and Internet Society trustee, published *IPv6: The New Internet Protocol* (1996).[6] Huitema's book technically describes IPv6 but also includes an introduction with a brief first person account of some of the history and controversy behind its selection. Scott Bradner and Allison Mankin, co-directors of the Internet Engineering Task Force (IETF) IPng effort, edited the volume *IPng: Internet Protocol Next Generation* (1996), consolidating the published RFCs[7] leading to the selection of IPv6. Most of the journal articles, such as IEEE and ACM publications, address esoteric IPv6 technical characteristics and transition issues. The narrow technical scope evident in the following journal article titles exemplifies the timbre of the existing body of scholarly technical IPv6 publications: "An IPv4-IPv6 Translation Mechanism for SIP Overlay Network in UMTS All-IP Environment,"[8] and "Implementation of IPv6 Services over a GMPLS-

[6] Christian Huitema, *IPv6: The New Internet Protocol*. Saddle River: Prentice Hall, 1996.

[7] The electronically archived RFCs (Requests for Comments) document the process of Internet standards development since 1969. The "sources" section of Chapter I describes the RFC system.

[8] Whai-En Chen, Yi-Bing Lin, and Ai-Chun Pang, "An IPv4-IPv6 Translation Mechanism for SIP Overlay Network in UMTS All-IP Environment," *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 11, November, 2005.

Based IP/Optical Network."[9] Other self-described technical journals routinely addressing IPv6 issues are actually published by corporations which develop IPv6 products or advocacy groups directly promoting IPv6 adoption. An example of this genre is Cisco Systems' *The Internet Protocol Journal*. Network and computing industry trade magazines (e.g. *Wired*, *LinuxWorld*, *CIO*, *Network World*) have produced more than a decade of IPv6 articles including forecasts of imminent migration to IPv6, forecasts of the demise of IPv6, advocacy articles, and technical and administrative analyses.

Beyond technical texts, the topic of IPv6 intersects with Milton Mueller's interesting theoretical analysis of Internet governance issues, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002).[10] Mueller primarily addresses domain name governance and the circumstances stimulating the formation of ICANN, but includes an insightful description of how both Internet names and addresses are economic and political resources. From the standpoint of Internet governance, Mueller also published (on-line), "Competition in IPv6 Addressing: A Review of the Debate"[11] which contributes an analysis of IPv6 address space management alternatives.

Janet Abbate's Internet history, *Inventing the Internet* (1999) describes the inception of the Internet/ARPANET and includes an account of the development and standardization of the Internet Protocol (IP) in the late 1970s and early 1980s. *Inventing the Internet* describes how Internet protocols reflected a combination of cold war military ideology and the values of early network users and developers. In tracing the history of IP through individual developers, U.S. Department of Defense mandates, and international standards conflicts, Abbate develops the theme of "how standards can be politics by other means."[12] While chronologically concluding prior to the development of IPv6, Abbate's detailed account of the inception of the Internet Protocol and her

[9] Mallik Tatipamula, Francois Le Faucheur, Tomohiro Otani, and Hiroshi Esaki, "Implementation of IPv6 Services over a GMPLS-Based IP/Optical Network," *IEEE Communications Magazine*, May, 2005.

[10] Milton Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002.

[11] Milton Mueller, "Competition in IPv6 Addressing: A Review of the Debate," Concept Paper by the Internet Governance Project, July 5, 2005. (Accessed at http://www.internetgovernance.org on September 14, 2005).

[12] Janet Abbate, *Inventing the Internet.* Cambridge: The MIT Press, 1999, page 179.

themes about networking protocols as political battlegrounds serve as an important catalyst for examining IPv6.

Abbate's research contributed to another relevant historical account of the Internet appearing in *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World* (1998) by Thomas Hughes. Hughes imparts themes about social and political complexity in large technological systems and differentiates ARPANET from earlier projects like SAGE and Atlas by its representation of counterculture ideals such as consensus-based rather than hierarchical management. Hughes also emphasizes the influence of the military in the evolution of technological systems and raises a question salient to the evolution of IPv6, "is government funding needed to maintain the revolutionary development of computing and is government funding needed to generate other technological revolutions in the future?"[13] This theme is pertinent to this research project and intersects with questions about the Commerce Department's role in Internet administration and the repercussions of the DoD's IPv6 adoption mandate.

Katie Hafner and Matthew Lyon provide another historical account of the Internet in *Where Wizards Stay up Late: the Origins of the Internet* (1996).[14] Through extensive personal interviews with Internet pioneers including Jon Postel, Bob Kahn, Len Kleinrock, Paul Baran, Vinton Cerf, et. al., Hafner and Lyon provide a detailed account of the origins of the Internet from the 1960s through the mid-1990s. Though adopting a completely internalist historical approach, this work provides a useful reference of early events leading to the development, standardization, and adoption of the TCP/IP protocols and related Internet technologies.

Several other works directly address economic, political, and social issues underlying network standards and protocols. Urs von Burg, in *The Triumph of Ethernet: Technological Communities and the Battle for the LAN Standard* (2001),[15] presents an economically grounded history of the emergence of the Ethernet local area network

[13] Thomas Hughes, *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World*. New York: Vintage Books, 1998, page 256.

[14] Katie Hafner and Matthew Lyon, *Where Wizards Stay up Late: The Origins of the Internet*. New York: Simon & Schuster, 1996.

[15] Urs von Burg, *The Triumph of Ethernet: Technological Communities and the Battle for the LAN Standard*. Stanford: Stanford University Press, 2001.

standard. Though describing a melee between two competing standards (Ethernet versus Token Ring) rather than an upgrade like IPv6, von Burg's account is pertinent because of its treatment of economic considerations in standardization. A brief analysis of information technology standards, *Scaffolding the New Web: Standards and Standards Policy for the Digital Economy* (2000)[16] by Martin Libicki et al., also adopts an economic analytical approach.

A more political approach to network protocols and standards appears in Alexander Galloway's work, *Protocol: How Control Exists after Decentralization* (2004).[17] Using his background in literary and cultural analysis, Galloway argues that the foundational "code" underlying numerous technical aspects of the Internet reflects not an architecture of freedom, but one of control. This is a related thesis to Stanford scholar Larry Lessig's earlier arguments in *Code and Other Laws of Cyberspace* (1999) and again in *The Future of Ideas: The Fate of the Commons in a Connected World* (2001). However, Lessig believes the Internet's architecture reflects freedom, but that corporate and regulatory threats to liberty (1999) and technical innovation (2001) endanger this architectural value.[18] As addressed later in a discussion of the conceptual framework for this project, Ken Alder's account of the development of the metric standard during the French Revolution, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error That Transformed the World* (1995),[19] serves as an exemplar of how seemingly neutral and objective standards embody historically contingent interests.

This study also thematically intersects with several histories addressing technologies other than Internet protocols, especially computing and radio. For example, both *A History of Modern Computing* (2003)[20] by Paul Ceruzzi and *The Closed World:*

[16] Martin Libicki, et al., *Scaffolding the New Web: Standards and Standards Policy for the Digital Economy*. Santa Monica: Rand, 2000.

[17] Alexander Galloway, *Protocol: How Control Exists after Decentralization*. Cambridge: The MIT Press, 2004.

[18] Lawrence Lessig, *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999; and *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House, 2001.

[19] Ken Alder, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error that Transformed the World*. New York: The Free Press, 2002.

[20] Paul Ceruzzi, *A History of Modern Computing*, Second Edition. Cambridge: The MIT Press, 2003.

Computers and the Politics of Discourse in Cold War America (1996)[21] by Paul Edwards, address the relationship between computing technologies and political contexts, especially the interplay between military and computing goals. Edwards' work, in particular, examines how political positions shape technological design and how technology likewise reinforces politics.

Because IP addresses are common pool resources analogous to electromagnetic spectrum, several radio histories are pertinent methodologically or conceptually, including three works by economist Hugh G. J. Aitken. Aitken's *Technology and Culture* essay, "Allocating the Spectrum: The Origins of Radio Regulation" (1994), raises several important topics. Acknowledging spectrum as an economically valuable, common-pool resource, Aitken addresses what he terms the "elusive" issue of spectrum scarcity and how it has been addressed over time through technical advancements and regulatory machinations. Aitken links early radio regulation policies to extant politics. For example, "In the 1920s, claiming that the spectrum was a public resource owned by all the people, legislators set their face against its alienation to private interests."[22] Aitken contrasts this approach with more modern, property-rights spectrum management, such as spectrum auctions, and raises caveats about market-based approaches. Aitken offers a historical perspective that, in the 1920s, there "were concerns about concentrated economic power, about control over the creation and movement of information, and about equal access to the means of communication by all members of society. Those concerns are still with us, however transformed by new technology."[23] Some of Aitken's themes have parallel issues in IP address distribution, control, and presumed scarcity.

Aitken's first volume on radio history, *Syntony and Spark: The Origins of Radio* (1976)[24] traces the origin of radio from Heinrich Hertz's late 19th century experimental confirmation of James Clerk Maxwell's electromagnetic equations through Oliver Lodge's technical innovations transmitting electromagnetic fields and the work of

[21] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: The MIT Press, 1996.

[22] Hugh G. J. Aitken, "Allocating the Spectrum: The Origins of Radio Regulation," *Technology and Culture*, Volume 35, Issue 4, October, 1994, page 715.

[23] Ibid, page 716.

[24] Hugh G. J. Aitken, *Syntony and Spark: The Origins of Radio*. New York: Wiley & Sons, 1976.

Guglielmo Marconi. An important theme, developed in the context of the discovery and subsequent practical application of the electromagnetic spectrum, addresses knowledge transfer from theoretical science to technological application and the role economics plays in this transfer. Aitken expands this interrelationship between science, technology and economics to include politics in his later volume, *The Continuous Wave: Technology and American Radio, 1900-1932* (1985). Chronologically commencing where *Syntony and Spark* concluded, this later work addresses the progression of radio technology from spark gap approaches to continuous wave technologies like de Forest's vacuum tube. One of Aitken's goals is to develop an explanatory model of technical innovation, and part of his argument recognizes spark technology as a "presumptive anomaly"[25] requiring a technological innovation that would, like IPv6 for the Internet, exponentially expand the number of simultaneous radio transmissions. In explaining the technological upgrade to continuous wave technology, Aitken considers economic exigencies, political contexts, and also the role of individual and institutional "translators"[26] who control the movement of knowledge among various communities.

Susan Douglas' comprehensive portrayal of early radio, *Inventing American Broadcasting: 1899-1922* (1987*)* serves as another model for integrating technical and economic constraints within the context of political climates, societal expectations, and individual and institutional contributions. As Douglas describes it, *Inventing American Broadcasting* "is about the social construction of radio."[27] Although covering many of the same topics as Aitken, this work places additional emphasis on the role of societal expectations on the development of radio. Douglas develops the theme of technology not as a thing but as a process involving the complex interplay between technical constraints and cultural contexts.

A contributive account of radio history addressing regulatory and public policy issues is Hugh Slotten's *Radio and Television Regulation: Broadcast Technology in the*

[25] For a description of presumptive anomaly, see Edward Constant's *The Origins of the Turbojet Revolution*. Baltimore: The Johns Hopkins University Press, 1980, page 15.

[26] Hugh G. J. Aitken, *The Continuous Wave: Technology and American Radio, 1900-1932*. Princeton: Princeton University Press, 1985, page 17.

[27] Susan J. Douglas, *Inventing American Broadcasting: 1899-1922*. Baltimore: The Johns Hopkins University Press, 1987, page xvii.

United States: 1920-1960 (2002).[28] In part, Slotten extends themes from Thomas Hughes (seamless web, heterogeneous engineering, and systems approach) into an appraisal of the interrelationships between engineers and inventors and the social, organizational, and economic contexts in which they exist. Slotten's identification of individuals and institutions influencing the broadcasting industry through standards setting and policy decisions provides an opening for recognizing counterparts in the Internet industry. For one example, Slotten raises issues of private corporate influence on the Wave Length Allocation Committee of the Institute of Radio Engineers (in the 1920s) that seem analogous to issues of private industry influence on the IPv6 working groups of the Internet Engineering Task Force.

The following conceptual framework further elaborates themes from Science and Technology Studies which informed this research project.

1.4 Conceptual Framework

The following conceptual approaches from Science and Technology Studies helped shape the methodological and theoretical framework of this research project.

Technology Standards as Politics

In a discussion of an earlier protocol debate, OSI versus TCP/IP, in *Inventing the Internet* (1999), Janet Abbate notes that technical standards are often construed as neutral and therefore not historically interesting. Perceptions of neutrality derive in part from the especially esoteric and concealed nature of network protocols within the broader realm of information technology. As Abbate demonstrates, "The debate over network protocols illustrates how standards can be politics by other means… Efforts to create formal standards bring system builders' private technical decisions into the public realm; in this way, standards battles can bring to light unspoken assumptions and conflicts of interest. The very passion with which stakeholders contest standards decisions should alert us to the deeper meanings beneath the nuts and bolts."[29] This project reflects Abbate's analytical historical approach toward network protocols and also absorbs elements of

[28] Hugh R. Slotten, *Radio and Television Regulation: Broadcast Technology in the United States, 1920-1960.* Baltimore: The Johns Hopkins University Press, 2000.

[29] Janet Abbate, *Inventing the Internet.* Cambridge: The MIT Press, 1999, page 179.

Paul Edwards' integration of political and technical histories in *The Closed World, Computers and the Politics of Discourse in Cold War America* (1996). Edwards examines how Cold War "politics became embedded in the machines – even, at times, in their technical design – while the machines helped make possible its politics."[30] Larry Lessig, in *Code and Other Laws of Cyberspace* (1999), writes more from a legal perspective but similarly links Internet architecture with politics. Historian of technology Ken Alder's account of the development of the metric standard during the French Revolution, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error That Transformed the World* (1995), served as an especially useful and analogous model for examining how seemingly neutral and objective standards are historically contingent and embody political and economic interests. The theoretical argument of this project is that protocols both embody interests and also are engaged as resources for reinforcing various political and economic objectives.

Yaron Ezrahi's theoretical positions as expounded in *The Descent of Icarus: Science and the Transformation of Contemporary Democracy* (1990) generally informed this project. Ezrahi addresses the connections between science, technology, and politics, suggesting that science and technology are often employed as political resources for mediating the tension in liberal-democratic politics between freedom and order. In addition to this mediation, the political role of science results in "depersonalizing the exercise of political power while preserving the status of agents as responsible actors."[31] Yaron's explanation of the political role of science also addresses the "need to ensure that the actions of public agents are taken 'for the sake' of the citizens and that these agents can be held publicly accountable."[32] As Sheila Jasanoff has suggested as a critique of *The Descent of Icarus*, Ezrahi treats science, technology, and politics as autonomous variables rather than as directly influencing one another.[33] This research project assumes

[30] Paul Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: The MIT Press, 1996, page ix.

[31] Yaron Ezrahi, *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*. Cambridge: Harvard University Press, 1990, page 18.

[32] Ibid.

[33] See Sheila Jasanoff's review of Ezrahi's *The Descent of Icarus: Science and the Transformation of Contemporary Democracy* (1990), in *The American Political Science Review*, Vol. 86, No. 1, March, 1992, pp. 233-234.

that politics also enter the formation of technological standards and follows STS historians who have more specifically developed this theme.

Escobar's Institutional Ethnography

Arturo Escobar's *Encountering Development* (1995) influenced this work both thematically and methodologically. As addressed in later chapters, so-called third world development emerged as a recurrent theme in the inception and promotion of IPv6 and in controversies over IP address control. Methodologically, parts of this project apply Escobar's approach of institutional ethnography to the origins of IPv6, addressing the anticipated problem of Internet address scarcity and the identification of a need for protocol intervention from the perspective of the institution identifying the problem rather than those countries or Internet users who might one day require addresses.[34] This IPv6 analysis follows Escobar in focusing on the institutional apparatus which originally identified the need for a new Internet protocol and by critically examining what these institutional claims about address scarcity, claims about requirements in developing countries, and proposed solutions to these problems contribute to political and economic control of the Internet.

Institutional Economics

This research project introduces the topic of finite technical resources by treating IP addresses as *common pool resources* similar to Hugh Aitken's economic interpretation of broadcast spectrum[35] in "Allocating the Spectrum: The Origins of Radio Regulation" (1994) and Milton Mueller's analytical examination of Internet names using his theory of technologically-induced endowment[36] in *Ruling the Root* (2003). These theoretical approaches draw from institutional economics to address issues of allocative efficiency and help introduce the problem of production, allocation and contestation of technologically-derived resources (IP addresses). Mueller suggests that institutional

[34] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, page 107.

[35] Hugh G. J. Aitken, "Allocating the Spectrum: The Origins of Radio Regulation." *Technology and Culture*, Volume 35, Issue 4, October, 1994, page 690.

[36] Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002, page 105.

economics “is interested in technology insofar as it creates new resources that must be incorporated into legal and institutional regimes, or causes changes in transaction costs or relative prices that lead to a breakdown in a preexisting order.”[37]

Additional Theoretical Influences

Chapter II discusses how the Internet’s standards setting community grappled with fractious ontological and epistemological questions in the process of selecting the next generation Internet protocol. For example, prior to selecting a new protocol, the Internet Activities Board (IAB) believed it must answer the question of *what* is the Internet. The ensuing debate about the existence of universal criteria defining the Internet mirrored the particularistic versus universalistic debate within the philosophy of science about what constitutes a valid scientific theory. In attempting to define the Internet, technologists demarcated between the Internet as a communication system and the Internet as a community of people. The selection process between competing protocol alternatives also directly paralleled questions from the philosophy of science, with many of the selection criteria, notably simplicity, testability, and uniformity seemingly invoking scientific theory choice prescriptions from logical positivism. Because of these parallels, and because this research project assumes a similarity between technological knowledge and scientific knowledge, Chapter II comparatively invokes the theory choice debate in the philosophy of science to describe and critique the ontological and epistemological issues the Internet standards community faced when selecting the next generation Internet protocol. The comparison draws from a variety of theorists including Karl Popper, Sandra Harding, Trevor Pinch and Weibe Bijker.

This project also narrowly adopts Edward Constant’s theory of *presumptive anomaly.* According to Constant, “Presumptive anomaly occurs in technology, not when the conventional system fails in any absolute or objective sense, but when assumptions derived from science indicate that under some future conditions the conventional system will fail (or function badly) or that a radically different system will do a much better

[37] Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002, page 10.

job."[38] This analysis of IPv6 critiques Constant's linear argument that advancements in scientific knowledge drive technological change, seemingly defining technology as applied science. Nevertheless, presumptive anomaly and applications of this concept to technological systems by Walter Vincenti[39] and Hugh Aitken[40] form a starting point for a discussion of the anticipation and articulation of a possible IP address shortage by individuals operating within the institutional framework of the Internet's standards setting community.

This project also generally embraces Thomas Hughes' view of technology as a heterogeneous system involving "technical, social, economic, and political"[41] components and employs some specific Hughes' themes. For example, *conservative technological momentum,*[42] reflecting both institutional and technical inertia, captures the entrenched momentum of the prevailing Internet standard, IPv4, and the development of three widely deployed groups of technologies designed to conserve IP addresses: network address translation, tunneling, and dual stacks.

Finally, many IPv6 policy justifications appear predicated on an unquestioned belief in an "information society" or "network society." This belief espouses a Chandlerian expectation that participation in the global information society presents unprecedented opportunities for economic advancement and productivity improvements.[43] This study follows Nicholas Garnham in critiquing the concept of

[38] Edward Constant, *The Origins of the Turbojet Revolution*. Baltimore: The Johns Hopkins University Press, 1980, page 15.

[39] Walter G. Vincenti, *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History*. Baltimore: The Johns Hopkins University Press, 1990, page 47.

[40] Hugh G. J. Aitken, *The Continuous Wave: Technology and American Radio, 1900-1932*. Princeton: Princeton University Press, 1985, page 6.

[41] Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, *The Social Construction of Technological Systems*. Cambridge: The MIT Press, 1999, page 5.

[42] See Thomas Hughes, *Rescuing Prometheus*: *Four Monumental Projects That Changed the Modern World*. New York: Vintage Books, 1998, page 77; and *American Genesis*, London: Penguin, 1989, p. 71.

[43] In *The Visible Hand: The Managerial Revolution in American Business,* Cambridge: Belknap Press, 1977, Alfred Chandler describes how the "visible hand" of efficiency-driven and technology-enabled managerial practices within modern businesses replaced the invisible hand of market capitalism in controlling systems of production and distribution in the United States. Chandler suggests this economic transformation inaugurated managerial capitalism and positioned large corporations as dominant institutions within the American economy.

‘information society’[44] and examines the role this construct plays in self-evidently presented national mandates about upgrading to IPv6.

1.5 Primary Sources

This project could not have progressed without the enormous historical archive of Internet mailing lists chronicling personal conversations and debates within institutions directly involved in establishing Internet standards. Published documents can conceal the debates preceding conclusions. Mailing lists provide the locus for these debates and are the mechanism for participation in Internet standards setting. Relative to the mailing lists, the RFCs (Requests for Comments) and other published documents provide more of an edited and united front for technical recommendations. The mailing lists include unedited, sometimes heated discussions and strong opinions about controversial issues confronting the standards community.

These first person postings provide a snapshot of what participants expressed *in situ* rather than the more subdued and edited first person retrospective accounts of these debates. Many of these mailing lists existed prior to the development of the World Wide Web, prior to widespread public access to the Internet, and prior to the Internet becoming an economically and socially important public communications medium. Decades later, these conversations are electronically accessible to anyone with Internet access. The forums were open, but conversations preceding widespread public Internet access seemed more private than later mailing list environments self consciously exposed to potentially millions of viewers. The culture of Internet mailing lists addressing technical architecture selection was one of rigorous intellectual debate and candid opinions. For example, an IETF Internet Area Director posted the following opinion reflecting on the next generation Internet protocol selection process, “This whole IPng deal, from its roots in concerns about the IPv4 address space..has been utterly back to front, and so totally and unbelievably amateurish it's incredible. That a standards body with responsibility for a key piece of the world's infrastructure is behaving like this is frightful and infuriating. I

[44] Nicholas Garnham, “Information Society As Theory or Ideology: A Critical Perspective on Technology, Education, and Employment in the Information Age,” *Information, Communication, and Society* 3:2, 2000.

simply cannot find the words to express the depth of my professional contempt for what I've watched happen."[45]

The following mailing list archives were the most contributive to this research because they chronicled dialogs between individuals directly involved in the protocol selection process (and subsequent controversies) and included key participants in standards institutions including the Internet Engineering Task Force (IETF), the Internet Architecture (formerly Activities) Board (IAB), and the Internet Engineering Steering Group (IESG):

❒ info.big-internet

❒ info.ietf

❒ comp.protocols.tcp-ip.

The immense volume of postings in these mailing lists would prohibit thorough scrutiny without the ability to search them via, in the case of this research, the searchable USENET discussion group archives available through Google. This project also accessed the archives for the IETF mailing lists via FTP at the following URL: ftp://ftp.ietf.org/ietf-mailing-archive/ietf.

The Internet RFCs also provided an invaluable source of information. The electronically archived RFCs document the process of Internet standards development since 1969. The thousands of RFCs offer a vivid technical and social history of proposed Internet standards, final Internet standards, and opinions from Internet pioneers. Contained within tens of thousands of RFC pages are a chronicle of the Internet technical community's original development of the Internet Protocol and the technical specifics of IPv4, a historical record of IP address assignments to various institutions, and early opinions about the possibility of IP address depletion. The RFC archives also contain the call for proposals for the next generation Internet Protocol, a store of public requirements documents for the new protocol, published versions of competing protocols, and the original technical specifications for the selected protocol, IPv6. The RFCs also contain an enormous reserve of notes from subsequent IPv6 working groups and document both the Internet's technical and institutional progression. As Chapter II addresses, the

[45] Excerpts from Noel Chiappa posting on the info.big-internet newsgroup, May 14, 1994, Subject "Thoughts on the IPng situation…"

Internet's standards setting community experienced an institutional challenge and procedural retrenching in 1992 and the RFCs depict a variety of institutional perspectives about this era.

As Abbate describes in Inventing the Internet (1999), the Internet RFCs "enabled the NWG to evolve formal standards informally."[46] The NWG, or Network Working Group, was a collection of researchers, primarily graduate students, tasked by ARPANET project manager Lawrence Roberts with creating the host protocols for the ARPANET beginning in the late 1960s. The RFC system served as an informal communications mechanism for the NWG, a group with no formal authoritative structure and no technical blueprint to follow. The late Jon Postel served as collector, editor, and archivist of more than 2500 RFCs for 28 years beginning in 1969.[47] After Postel's death in 1998, his colleague, Joyce Reynolds, assumed these responsibilities, later expanded to a small group of individuals funded by the Internet Society. The RFCs were originally paper documents which Vinton Cerf described as having "an almost 19th Century character to them – letters exchanged in public debating the merits of various design choices for protocols in the ARPANET."[48]

In using RFCs as an archival historical source, this research has carefully noted that not all RFCs represent ratified Internet standards. In the process of becoming standards, RFCs progress through the standards track categories of 'proposed standards,' 'draft standards,' and 'standards.'[49] Additionally, some RFCs are self-described histories, some are informational, and some document technical protocols which never became accepted standards. Several RFCs, often published on April Fools Day, are actually jokes, such as "Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)," a lengthy RFC attributing the consumption of the IPv4 address space to the proliferation of

[46] Janet Abbate, *Inventing the Internet*. Cambridge: The MIT Press, page 74.

[47] RFC Editor, et al., "30 Years of RFCs," RFC 2555, April 7, 1999, page 4.

[48] Ibid, page 6.

[49] For a description of the Internet standards review process, see Harald Alvestrand's best current practices document, "The IESG and RFC Editor Documents: Procedures," RFC 3932, October, 2004.

networked coffee pots and proposing a new control protocol accordingly.[50] The entire RFC series is electronically available via www.rfc-editor.org.

IETF working group documents provided considerable technical information about IPv6. Working groups, teams of individuals which accomplish much of the IETF's technical work before it percolates up to the broader organization, classify into one of several expansive areas: applications, general, Internet, operations and management, routing, security, and transport. IPv6 technical topics and specifications traverse most of these areas. The 'IPv6 Working Group,' formerly the 'IPng Working Group,' provided the most useful technical resource for IPv6 specifications. Electronic working group archives chronicle deliberations, salient issues, and recommendations about the IPv6 specifications and record the events leading to the selection of IPv6 over alternative protocols. For example, archives of meeting minutes from 1994 through the present document the deliberations of the IPng Working Group, the SIPP Working Group (Chapter II explains the significance of this group), the IPv6 Transition Working Group, and the renamed IPv6 Working Group.

IPv6 implementations engage numerous technical specifications depending on requirements, such as operating IPv6 over certain networks (e.g. Ethernet, FDDI, token ring), IPv6 management, and information compression over IPv6. Fortunately, an electronic web archive accessible at http://playground.sun.com/pub/ipng/html/ipng-main.html consolidates more than fifty of the IPv6-related technical specifications, along with working group minutes and a chronicle of IPv6 product implementations within various operating systems and routers.

The IETF web site, www.ietf.org, archives more than 40,000 pages of proceedings from its triennial conferences held since the institution's 1986 inception. The minutes of the monthly IAB meetings also provide a snapshot of debates about IPv6 among leaders in the Internet's technical community. A discussion archive also chronicles the day-to-day discussions of the IPv6 working groups.

Published government IPv6 directives served as a source for official national IPv6 mandates and related policies. The English language translations of meeting

[50] Larry Masinter, "Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)," RFC 2324, April 1, 1998.

deliberations, formal policies, and strategy documents of the Prime Minister of Japan, his Cabinet, and the Japanese IT Strategy Council reflect Japan's IPv6 policies and stated rationales for instituting those policies.[51] Documents describing the Lisbon European Council, the eEurope Action Plan, and IPv6 strategy directives of the Commission of the European Community, are all also publicly available.[52] Korea's Ministry of Information and Communication and India's Minister of Communications and Information Technology similarly have published IPv6 policy documents.[53]

The first U.S. policies addressing IPv6 briefly appear in the *National Strategy to Secure Cyberspace* (2003). A number of Department of Defense briefings, presentations, and policy documents, describe the DoD's IPv6 policies and rationales for upgrading. Other useful publicly available sources of information on U.S. IPv6 policy were the GAO's formal assessment of IPv6, the Commerce Department's lengthy technical and economic IPv6 assessment, transcripts of the public Department of Commerce meeting "Deploying IPv6: Exploring the Issues," the Department of State's Policy on Internet Governance, and the transcripts of the 2005 congressional IPv6 hearing held by the Government Reform Committee.

International IPv6 Technology Summits and associated archival material provided some technical and policy information about IPv6 and presented opportunities to directly interact with international IPv6 scientists and advocates, Department of Defense IPv6 technologists and policy makers, corporate users, IPv6 product vendors, and Internet pioneers. Other research sources included the archives, public comments, and mailing lists of IPv6 advocacy groups such as the IPv6 Forum and the North American IPv6 Task Force. Additionally, the ITU published complete video webcasts, documents, deliberations, and presentations from the two World Summits on the Internet Society (and the preparatory meeting deliberations associated with the Summits), which addressed Internet governance issues including IP address administration. Finally, the web sites of Internet registries APNIC, NCC-RIPE, ARIN, AfriNIC, and LACNIC

[51] (Accessed at http://www.kantei.og-jp/foreign/it-e.html in November, 2002).

[52] (For example, http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm accessed on December 11, 2004).

[53] (For example, www.mic.go.kr and http://www.dotindia.com accessed on October 29, 2005).

provided additional information about IPv4 and IPv6 address allocation statistics, distribution policies, policy discussions, and related Internet governance issues.

1.6 Summary of Chapter Contents

This historical account divides the examination of IPv6 into three overlapping epochs: the origin of the IPv6 standard, the adoption and promotion of IPv6, and the history of the administration and distribution of the finite technical resources of IP addresses.

Chapter II describes the origin and selection of IPv6 within the Internet's standards setting community. It explains how IPv6 became the answer to presumed address scarcity and describes the alternatives to IPv6 and why they were rejected. Methodologically, the analysis employs Escobar's approach of institutional ethnography to examine the selection of the next generation Internet protocol within the Internet's technocracy and theoretically compares issues from the philosophy of science to philosophical questions the IAB invoked during technical standards selection. This chapter suggests that the selection of IPv6 as the next generation Internet protocol reflected friction between the US-based standards institutions and an international standards organization in the context of Internet globalization. A major chapter theme suggests that the issue of protocol selection was also a multifaceted issue of power selection among an entrenched institutional structure of trusted insiders, an internationally expanding sphere of stakeholders, dominant networking vendors, and newer market entrants. Another theme emerging within the account of IPv6 origins addresses the extent to which the standards community, typically held up as a paragon of participatory and open technological development, is participatory and open in practice.

Chapter III addresses efforts to promote and adopt the IPv6 standard, once developed. The chapter describes the state IPv6 policies of Japan, the European Union, Korea, China, and India, all of which, beginning in 2000, declared the standard national priorities and established policies to drive adoption. In contrast, the United States, with a hegemonic Internet industry and ample IP addresses, appeared less eager to embrace a new standard until some in the U.S. Department of Defense began linking IPv6 with improved military capability and enhanced Internet security and, much later, some politicians and IPv6 stakeholders linked IPv6 with various objectives including global democratization, third world development, social melioration, and U.S. economic competitiveness relative to China and India. Drawing from STS historians and theorists like Abbate, Alder, and Ezrahi, the chapter describes how the promise of IPv6 aligned with broader political objectives such as European unification goals and EU economic competitiveness, the promise of thwarting economic stagnation in Japan or unemployment in Korea, or enabling a more secure and orderly war on terrorism for the U.S. DoD. The primary theme of Chapter III is the interconnection between standards and political, economic, and technical objectives.

Chapter IV describes the historical distribution and administration of IP addresses. It explores questions about who first perceived a potential shortage of IP addresses and on what basis, and includes accounts of dissenting arguments challenging predictions of Internet address scarcity. Topics include the allocative method originally determining the distribution of IP addresses, how U.S. based institutions involved in the early Internet and predecessor networks received disproportionately large blocks of addresses, and how IP address administration became internationally distributed but ultimately controlled by a centralized American corporation overseen by the U.S. Commerce Department. The chapter concludes with an account of the international conflict between those advocating United Nations-based Internet governance versus the U.S. position to preserve its role in centralized Internet administration. One theme addresses how antithetical positions in the Internet governance debate share a commonality in citing the needs of developing countries and the promotion of democratic values as validating their respective arguments. The main chapter theme addresses how the historical diaspora of the Internet from a relatively closed community of trusted insiders to an internationally and culturally distinct public medium created intractable Internet governance dilemmas including questions of legitimacy in centrally administering and controlling the globally unique IPv6 (and IPv4) addresses necessary for Internet connectivity.

Chapter V concludes by summarizing the efficacy of an STS approach to historically examining IPv6. The three spheres of IPv6 standards selection, adoption, and technical resource control all reflected tensions over control of an increasingly globalized technological system and all occurred outside of classical market mechanisms of supply and demand of resources. The chapter summarizes five themes pervading this historical account of IPv6: 1) the connection between technical standards and politics, 2) the shift from trusted insider control and use of the Internet and how this shift has transformed the Internet architecturally and administratively, 3) how the Internet standards process is not the democratic, participatory approach scholars often laud it to be, 4) the role portrayals of developing countries play in technology promotion, and 5) the cultural construction of technological inevitability.

CHAPTER II:
ORIGINS OF IPV6

The standards community selecting the new Internet protocol established an *a priori* guideline to appraise competing protocol alternatives based on supposedly objective technical criteria independent of sociological considerations or market factors. Historian of technology, Ken Alder, writing about the political economy of the emerging metric system during the French Revolution, explains, "At the core of 'universal standards' commonly taken to be products of objective science lies the historically contingent, and further, that these seemingly "natural" standards express the specific, if paradoxical, agendas of specific social and economic interests."[54] Alder demonstrates how late 18th Century technical elites crafted a new rational standard, the metric system, which diminished the old regime's political economy in France and facilitated the rise of a market economy. A meter was precisely defined as the distance light traveled in a vacuum for 1/299,792,458 of a second, but its definition and adoption reflected issues of authority, legitimacy, social organization, and political economy. The selected new Internet standard, IPv6, specified 128 bit addresses allowing for a theoretical maximum of 3.4×10^{38} Internet addresses, and its origin and definition also reflected historically contingent issues.

This chapter examines how IPv6 emerged as the universal answer to projected Internet resource constraints and describes the alternatives to IPv6 and why they were rejected. The institutions establishing universal Internet standards wielded considerable influence over the Internet's architectural direction. Internet scholars, such as Stanford's Larry Lessig, extol what they describe as the Internet's traditional participatory and democratic standards development environment. In examining the selection of IPv6, this historical account critically considers the validity of the participatory and open democratic characteristics often attributed to the Internet standards process. Arturo Escobar's approach of institutional ethnography helps address questions of protocol selection from the perspective of those constructing the problem and crafting an intervention rather than from the perspective of those presumably facing a future address

[54] Ken Alder, "A Revolution to Measure: The Political Economy of the Metric System in France," *Values of Precision*, Ed. M. Norton Wise, Princeton: Princeton University Press, 1995, pp. 39-71.

shortfall. Escobar suggests, “The work of institutions is one of the most powerful forces in the creation of the world in which we live. Institutional ethnography is intended to bring to light this sociocultural production.”[55] This chapter describes how the institutional trajectory leading to the IPv6 standard involved a contentious protocol selection process reflecting international geopolitical tensions among an expanding milieu of Internet stakeholders.

2.1 Internationalization

In 1990, the Internet Activities Board (IAB) confronted topics of Internet address scarcity and the need for a new network protocol in the context of increasing Internet internationalization.[56] The IAB wielded considerable power over the Internet’s architectural direction, considering its self-described functions:

1) *Sets Internet standards,*
2) *Manages the RFC publication process,*
3) *Reviews the operation of the IETF and IRTF,*[57]
4) *Performs strategic planning for the Internet, identifying long-range problems and opportunities,*
5) *Acts as an international technical policy liaison and representative for the Internet community, and*
6) *Resolves technical issues which cannot be treated within the IETF or IRTF frameworks.*[58]

[55] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, page 107.

[56] Questions about the possibility of exhausting IP addresses emerged during the April 26, 1990, IAB teleconference attended by IAB members Bob Braden, Hans-Werner Braun, Vint Cerf, Lyman Chapin, David Clark, Phil Gross, Steve Kent, Tony Lauck, Barry Leiner, Dan Lynch, and Jon Postel, according to the minutes of the meeting. (http://www.iab.org/documents/iabmins/IABmins.1990-04-26.html accessed on August 13, 2003). Similar questions and concerns emerged at the next quarterly IAB meeting, on June 28-29, 1990, attended by IAB members Vint Cerf, David Clark, Phil Gross, Steven Kent, Tony Lauck, Barry Leiner, Dan Lynch, and Jon Postel, as well as some participants from the U.S. government and the Internet Engineering Steering Group. (http://www.iab.org/documents/iabmins/IABmins.1990-06-28.html accessed on August 12, 2003).

[57] IRTF: Internet Research Task Force.

Eleven individuals composed the IAB in 1990: all were male, most were American, and most worked for corporations, universities, and research institutions.[59] Members communicated with each other via electronic mailing lists and also held quarterly meetings to assess the overall condition of the Internet and discuss technical and policy issues. This independent group was closed to general public involvement in that the IAB chairman, then Vinton Cerf, appointed members.[60] This small institution establishing Internet standards was open only in the sense that "All decisions of the IAB are made public."[61]

The IAB was formalized as an institution in 1983 but its origins traced to the late 1970s period of the ARPANET project, when researchers involved in protocol development founded an informal committee known as the Internet Configuration Control Board (ICCB). Then DARPA program manager, Cerf, was instrumental in establishing the committee, and David Clark of MIT's Laboratory for Computer Science became the chairman. In 1983, the year TCP/IP became the formal protocol underpinning of the ARPANET, the group renamed the ICCB the Internet Activities Board, or IAB. Vinton Cerf became the IAB's chair in 1989. The organization's primary responsibilities involved oversight of the Internet's protocol architecture and included ultimate responsibility for ratifying protocols.

The IAB established the Internet Engineering Task Force (IETF) in 1986 as a subsidiary task force serving as the primary standards organization developing Internet protocol drafts. In 1990, the IETF had no formal membership, was composed of volunteers, and was a non-incorporated entity with no legal status. The IETF traditionally has held triennial face-to-face plenary meetings. The working climate of these gatherings is informal, with fluid agendas, social gatherings, and a relaxed dress

[58] IAB self-described responsibilities outlined by then-IAB chair, Vinton Cerf, in "The Internet Activities Board," RFC 1120, May 1990, page 2.

[59] The eleven IAB members in 1990 were: Vinton Cerf (CNRI), Chairman; Robert Braden (USC-ISI), Executive Director; David Clark (MIT-LCS), IRTF Chairman; Phillip Gross (CNRI), IETF Chairman; Jon Postel (USC-ISI), RFC Editor; Hans-Werner Braun (Merit), Member; Lyman Chapin (DG), Member; Stephen Kent (BBN), Member; Anthony Lauck (Digital), Member; Barry Leiner (RIACS), Member; and Daniel Lynch (Interop, Inc.), Member. Source: RFC 1160.

[60] Vinton Cerf, "The Internet Activities Board," RFC 1160, May 1990, page 2.

[61] Ibid.

code dominated by “t-shirts, jeans (shorts, if weather permits) and sandals.”[62] IETF working groups conducted the bulk of standards development and communicated primarily through electronic mailing lists to which anyone could subscribe. However, IETF working groups were dominated by Americans, and the extent of participatory and open standards development is contestable because of barriers of access, esoteric complexity, and financial backing, issues addressed later in this chapter. Area Directors (AD) head up the working groups and, these ADs (approximately eight at any time) along with the IETF Chair constitute the Internet Engineering Steering Group (IESG). Standards percolate up from the IETF working groups to the IESG, ultimately responsible for presenting Internet Draft standards to the IAB for ratification as a formal Internet standard.

Emerging discussions within this 1990 institutional structure raised concerns about rapid Internet globalization portending a shortage of IP addresses. At an August, 1990, IETF meeting in Vancouver, participants Frank Solensky, Phill Gross, and Sue Hares projected that the current address assignment rate would deplete much of the Internet address space by March of 1994.[63] IAB members also acknowledged the “rapidly growing concern internationally”[64] that a U.S. centric organization, the Internet Assigned Numbers Authority (IANA) at USC’s Information Science’s Institute (ISI), determined address allocations. The two general assumptions were that the “IP address space is a scarce resource” and that, in the future, a more international, non-military, and non-profit institution might potentially assume responsibility for address allocations.[65] At the fall, 1990, INTEROP trade show, MIT’s Noel Chiappa, the IESG Area Director (AD) for Internet Services, delivered a presentation to the IAB reiterating the looming possibility of IP address space exhaustion.[66]

[62] Gary Malkin, “The Tao of IETF, A Guide for New Attendees of the Internet Engineering Task Force,” RFC 1718, November, 1994.

[63] Scott Bradner and Allison Mankin, “The Recommendation for the IP Next Generation Protocol,” RFC 1752, January, 1995, page 4.

[64] Internet Architecture Board teleconference minutes, April 26, 1990. (Accessed at http://www.iab.org/documents/iabmins/IABmins.1990-04-26.html on August 13, 2003)

[65] Ibid.

[66] Ann Westine, Internet Monthly Report, October, 1990. (Accessed at internet/newsletters/internet.monthly.report/imr9010.txt on August 14, 2003).

After several months of discussions within the IAB, Cerf issued a recommendation to the Federal Networking Council (FNC), then the U.S. government's coordinating body for agencies supporting the Internet, that the responsibility for assigning remaining addresses be delegated to international organizations, albeit with the IANA still retaining centralized control:

> *"With the rapid escalation of the number of networks in the Internet and its concurrent internationalization, it is timely to consider further delegation of assignment and registration authority on an international basis. It is also essential to take into consideration that such identifiers, particularly network identifiers of class A and B type, will become an increasingly scarce commodity whose allocation must be handled with thoughtful care."*[67]

The IAB believed that the internationalization and growth of the Internet warranted a redistribution of remaining addresses to international registries but also recognized that this institutional tactic alone was insufficient for accommodating the globalization and rapid expansion of the Internet.

The IAB held a "soul searching" two-day meeting in January, 1991, at the USC-ISI in Marina del Rey, California, to discuss future directions for the Internet.[68] The issue of Internet internationalization was prominent on the agenda. The IAB pondered whether it could "acquire a better international perspective," by supporting international protocols, increasing international membership in the IAB, and holding some meetings outside of the United States.[69] The topic of Internet internationalization traversed several areas including the controversial issue of export restrictions on encryption products and the divisive issue of "OSI." At the time, interoperability between different vendor's computer networking systems was an intractable problem. The International Standards Organization's (ISO's) Open Systems Interconnection (OSI) protocols were in contention for becoming the interoperability standard for computer networking. OSI was an international standards effort sanctioned by numerous governments, particularly in

[67] Vinton Cerf, "IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status," RFC 1174, August, 1990, page 1.

[68] David Clark, et. al. "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 2.

[69] Internet Activities Board, Meeting Minutes, January 8-9, 1991, Foreward [SIC]. (Accessed at http://www.iab.org/documents/iabmins/IABmins.1991-01-08.html on August 13, 2003).

Western Europe but also throughout the world. The United States government, in 1990, mandated that U.S. government procured products conform to OSI protocol specifications[70] and even the U.S. Department of Defense, an original proponent of TCP/IP, somewhat capitulated to the inevitability of OSI protocols. Despite these OSI endorsements, the competition between TCP/IP and OSI as a dominant vendor-neutral interoperability standard remained unsettled. OSI protocols had limited deployments relative to TCP/IP but had the backing of international governments, the U.S. National Institute of Standards and Technology (NIST), and increasing investment by prominent network computing vendors such as Digital Equipment Corporation (DEC). TCP/IP was the working set of protocols supporting the public Internet, had garnered an increasing presence within private corporate networks, had the backing of the Internet's technical community, and had well documented specifications, productive standards institutions, and working products.

Within IAB deliberations, the issues of OSI and internationalization existed contemporaneously with recognition of Internet address space constraints. These issues surfaced together in the January, 1991, joint meeting between the IAB and the IESG, attended by 23 Internet technical contributors including Vinton Cerf, Bob Braden, Jon Postel, and Robert Hinden.[71] The congregation was later described as "spirited, provocative, and at times controversial, with a lot of soul-searching over questions of relevance and future direction."[72] MIT's Dave Clark commenced the meeting with an introductory presentation attempting to identify and illuminate six[73] problem areas. The first area addressed the multiprotocol question of whether the Internet should support

[70] The United States Federal Information Processing Standards (FIPS) Publication 146-1 endorsed OSI compliant products in 1990. In 1995, FIPS 146-2 retracted this mandate.

[71] The meeting minutes record the following attendees: IAB members Bob Braden, Vint Cerf, Lyman Chapin, David Clark, Phill Gross, Christian Huitema, Steve Kent, Tony Lauck, Barry Leiner, Dan Lynch, and Jon Postel; and IESG members Ross Callon, J. Noel Chiappa, David Crocker, Steve Crocker, Chuck Davin, Phillip Gross, Robert Hagens, Robert Hinden, Russell Hobby, Joyce Reynolds, and Gregory Vaudreuil; and FNC visitor Ira Richer, DARPA. (Meeting minutes accessed at http://www.iab.org/documents/iabmins/IABmins.1991-01-08.html on August 13, 2003).

[72] David Clark et. al, "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 2.

[73] The six problem areas discussed included: The Multi-Protocol Internet, Routing and Addressing, Getting BIG, Dealing with Divestiture, New Services (e.g. video), and Security.

both TCP/IP and OSI protocols, a question Clark phrased as "Making the problem harder for the good of mankind."[74] Clark identified a conflict between an ability to fulfill technical requirements promptly versus taking the time to incorporate OSI protocols within the Internet's architecture. He emphasized that any potential top-down mandates would not be as efficacious as grassroots approaches centered on working code. Other issues included the impact of the Internet's expansion and growing commercialization on routing and addressing architectures. The group generally failed to reach consensus on architectural directions, but the IAB decided to convene again in June for a three day "architecture retreat" to attempt to achieve some consensus on the Internet's technical and policy directions.

The promised June, 1991, Internet architecture retreat included 32 individuals from the IAB, the IESG, and some guests. These individuals represented universities, research institutions, corporations, and the United States government.[75] Five IAB members, including Clark and Cerf,[76] published the outcome of the retreat as an informational RFC in December of 1991. This document, "Towards a future Internet Architecture," outlined a blueprint for the Internet's architectural development for the next 5-10 years and sought discussion and comments from the Internet community. The architecture established guidelines in five areas identified as the most pressing concerns for Internet evolution:

❒ Routing and Addressing

❒ Multiprotocol Architectures

❒ Security Architectures

[74] Internet Activities Board, Summary of Internet Architecture Discussion, January 8-9, 1991, Appendix A, David Clark's presentation. (Accessed at http://www.iab.org/documents/iabmins/IABmins.1991-01-08.arch.html on August 12, 2003).

[75] The 32 individuals participating in the three-day, June, 1991, retreat to attempt to set architectural directions for the Internet included the following: Dave Clark, MIT; Hans-Werner Braun, SDSC; Noel Chiappa, Consultant; Deborah Estrin, USC; Phill Gross, CNRI; Bob Hinden, BBN; Van Jacobson, LBL; Tony Lauck, DEC; Lyman Chapin, BBN; Ross Callon, DEC; Dave Crocker, DEC, Christian Huitema, INRIA; Barry Leiner, Jon Postel, ISI; Vint Cerf, CNRI; Steve Crocker, TIS; Steven Kent, BBN; Paul Mockapetris, DARPA; Robert Braden, ISI; Chuck Davin, MIT; Dave Mills, University of Delaware; Claudio Topolcic, CNRI. Source: RFC 1287, December, 1991.

[76] The other three co-authors were Lyman Chapin (BBN), Robert Braden (ISI), and Russell Hobby (UC Davis).

❒ Traffic Control and State

❒ Advanced Applications.

An uncontested assumption held that the Internet faced an inevitable problem termed *address space exhaustion*, whereby “The Internet will run out of the 32-bit IP address space altogether, as the space is currently subdivided and managed.”[77] Furthermore, the group identified this possibility, along with concerns about the burdens growth would place on the Internet’s routing functionality, as the most urgent technological problem confronting the Internet. Rather than initiate incremental changes to mitigate the presumed address scarcity, the group believed it should embark upon a long term architectural transformation that would replace the current 32-bit global address space.[78]

At the time of the Internet architecture retreat, the prevailing Internet Protocol, IPv4, was ten years old. In 1981, the year IBM introduced its first personal computer, RFC 791 introduced the Internet Protocol (IP) standard. This 1981 IP specification, referred to as both the DoD Standard Internet Protocol and the Internet Protocol, drew from six prior iterations of IP but was its first formal version.[79] Even though there was no official predecessor, it was later named Internet Protocol version 4, or IPv4, because its function bifurcated from the Transmission Control Protocol (TCP), which previously had three versions. The Internet Protocol addresses two key networking functions: fragmentation and addressing. It specifies how to fragment and structure information into small segments, or datagrams (later called packets), for transmission over a network and reassembly at their destination. IP establishes how to append source and destination addresses within these datagrams and uses these addresses to route datagrams to their final destinations. Datagrams contain both content, such as the text of an electronic mail message, and also control information in a “header” sent along with the content. IP specifies certain fields, or spaces, within this header to describe how to fragment and then

[77] David Clark et. al, “Towards the Future Internet Architecture,” RFC 1287, December, 1991, page 4.

[78] Ibid, page 5.

[79] Jon Postel, “Internet Protocol, DARPA Internet Program Protocol Specification Prepared for the Defense Advanced Research Projects Agency,” RFC 791, September, 1981.

reassemble datagrams. The header also contains the source and destination address for the datagram. Routers read a packet's destination IP address and forward the packet to the next appropriate router, which, in turn, makes real time forwarding decisions, and so forth until the information reaches its final destination. The 1981 IP standard, formally implemented in 1983, specified an IP address as a 32-bit code divided into a network prefix and a host prefix. Some of the 32 bits indicated an institution's overall network and the remaining address bits represented an individual host on that network. Only the network prefix is read by the router. This address division into network and host components expedites router performance. Routers store routing tables, enormous quantities of data they reference to make forwarding decisions based on the network addresses they process. Routing tables contain only network prefixes, except for the end routers that directly connect to a local network.

IPv4's fixed length binary address size of 32 bits, or four bytes, is a combination of 32 0s and 1s such as the following address:

00011110000101011100001111011101.

An IP address, such as the above, is included in the header material of a packet before transmission across the network. While computing devices recognize binary sequences, the IP address format more recognizable to Internet users appears in decimal format, such as 30.21.195.221. This conventional short hand notation, called "dotted decimal format," is irrelevant to computing devices but makes 32-bit Internet addresses more comprehensible, numerically condensed, and manageable for humans. Appendix B explains the IPv4 format and describes the mathematical conversion to dotted decimal format.

Mathematically, the 32-bit address length would support more than four billion hosts, calculated as 2^{32}, or 4,294,967,296. The randomly chosen IP address listed above, 30.21.195.221, represents one out of the more than four billion theoretically available addresses. In the early 1980s, prior to the widespread use of personal computers, home Internet access, or even extensive business Internet use, 4.3 billion represented an exorbitant number. Applications like electronic mail continued to grow in popularity, but, as some within the Internet technical community would acknowledge fifteen years later, "Even the most farseeing of the developers of TCP/IP in the early 1980s did not imagine the dilemma of scale that the Internet faces today."[80]

The technologists participating in the 1991 architecture retreat concurred that the supply of more than 4.3 billion Internet addresses under the IPv4 standard would become exhausted at some future time. The retreat included a day-long breakout session for five subgroups to deliberate on the areas identified as most pressing for the Internet's architectural future. MIT's Dave Clark chaired the routing and addressing subgroup.[81] The participants identified some initial possibilities for extending the Internet address space. One alternative would retain the 32-bit address format but eliminate the requirement of global uniqueness for each address. Instead, different Internet regions would require globally unique addresses but each address could be reused in a different region. Gateways would translate addresses as information traversed the boundary between two regions. This concept was theoretically similar to frequency reuse in cellular telephony, whereby electromagnetic spectrum limitations are overcome by reusing frequencies in non-adjacent cells. When a caller moves to an adjacent cell, a hand-off process transfers the call from one frequency to another. Another alternative would expand the Internet address size, such as from 32 to 64 bits.[82]

Predictions of a forthcoming Internet system failure evoke Edward Constant's description of *presumptive anomaly*, a scientifically-derived indication that, under future conditions, a presently working technology will fail and may require a radical redesign. As Constant explains "The old system still works, indeed still may offer substantial development potential, but science suggests that the leading edge of future practice will have a radically different foundation."[83] Constant's primary historical example of a presumptive anomaly addresses late 1920s assumptions in aerodynamic theory leading to

[80] Scott Bradner and Allison Mankin, "The Recommendation for the IP Next Generation Protocol," RFC 1752, January, 1995, page 4.

[81] The other members of the routing and addressing subgroup included Hans-Werner Bruan, SDSC; Noel Chiappa, Consultant; Deborah Estrin, USC; Phill Gross, CNRI; Bob Hinden, BBN; Van Jacobson, LBL; and Tony Lauck, DEC.

[82] David Clark et. al, "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 6.

[83] Edward Constant, "Social Locus of Practice," *The Social Construction of Technological Systems*, Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds. Cambridge: The MIT Press, 1999, page 225.

the development of the turbojet. Scientific speculation assumed that propellers would not suffice at the higher speeds generated by gas turbine technologies and aircraft design advancements. This presumptive anomaly, argues Constant, "led directly to the turbojet revolution."[84]

Constant's definition holds that scientific assumptions portend a future system failure and he describes two harbingers of technological change, both derived from scientific predictions: 1) the current system will fail or 2) a different system will perform better. His example of predictions of propeller failure at high speeds exemplifies the first category. A description of a presumptive anomaly commensurate with Constant's second category appears in Walter Vincenti's *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History* (1990). Vincenti's historical example of the late 1930s development of the laminar-flow airfoil is an example of Constant's second type of presumptive anomaly – that a radically new system might perform better. Vincenti's and Constant's arguments are similar in their attribution of presumptive anomalies to scientifically-derived predictions. Assumptions about potential airfoil design advancements "followed from theoretical estimates of friction drag derived from engineering science,"[85] similar to the turbojet revolution following from theoretical predictions of future failure. Constant and Vincenti argue that advancements in scientific knowledge drive technological change, somewhat defining technology as applied science. Vincenti and Constant also acknowledge the possibility of another driving force behind technological innovations geared towards dramatic performance improvements: "functional failure." Increasing demand for a technology or applications of technologies in new situations portend functional failures.[86] Applying this possibility to the Internet Protocol, demand for more Internet addresses, such as explosive international growth or the proliferation of Internet appliances and wireless applications, was the driving force behind recognition of IPv4 limitations. This analysis departs from Constant's and

[84] Edward Constant, "Social Locus of Practice," *The Social Construction of Technological Systems*, Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds. Cambridge: The MIT Press, 1999, page 226.

[85] Walter G. Vincenti, What *Engineers Know and How They Know It: Analytical Studies from Aeronautical History*. Baltimore: The Johns Hopkins University Press, 1990, page 47.

[86] Ibid.

Vincenti's application of presumptive anomaly by examining the more exogenous political and socioeconomic forces influencing the technologists' identification of presumptive address scarcity and the decision to develop a new protocol accordingly.

2.2 Defining the Internet

Prior to establishing new protocol directions, the IAB believed it must first answer the question of what is the Internet. This topic arose in conjunction with a debate about whether the Internet should offer multiple protocol options, whether it should be technically homogenous, and whether the IAB should mandate certain protocols. In the IAB's "Towards the Future Internet Architecture" (1991) document, international pressure to adopt OSI protocols as a universal computer networking standard loomed large in both the questions asked and in architectural decisions. International institutions endorsed many of the International Standards Organization's OSI protocols. The U.S. government seemed to support OSI through its GOSIP standard. The networking environments within United States corporations were overwhelmingly multi-protocol in 1991, with typical large businesses operating some proprietary protocol networks like IBM's Systems Network Architecture (SNA), DEC's DECNET, some TCP/IP networks, Appletalk protocols to support Macintosh environments, and IPX/SPX protocols associated with Novell Netware LANs. Often, these various network protocol environments were isolated technical islands within large enterprises. An open question was whether TCP/IP or some other family of protocols, especially OSI, would become the universal standard interconnecting these diverse environments.

The technologists tackling questions about what makes the Internet the Internet were based in the United States and had been in control of Internet architectural directions for, in some cases, twenty years. Those involved in the Internet Architecture Retreat acknowledged that:

> *"The priority for solving the problems with the current Internet architecture depends upon one's view of the future relevance of TCP/IP with respect to the OSI protocol suite. One view has been that we should just let the TCP/IP suite strangle in its success, and switch to OSI protocols. However, many of those who have worked hard and successfully on Internet protocols, products, and service are anxious to try to solve the new problems within the existing*

> *framework. Furthermore, some believe that OSI protocols will suffer from versions of many of the same problems."*[87]

They presaged that both the TCP/IP and OSI protocol suites would coexist and acknowledged "powerful political and market forces" behind the introduction of the OSI suite.[88]

Against the backdrop of the TCP/IP versus OSI issue, the IAB tackled the question of *what* is the Internet. The ensuing debate about the existence of universal criteria defining the Internet strikingly resembled the particularistic versus universalistic debate within the philosophy of science about what constitutes a valid scientific theory. The theory choice question in the philosophy of science addresses whether there exist universal criteria for evaluating scientific theories or whether local, particularistic factors influence theory choice. The June, 1991, Internet architecture retreat addressed similar concerns about the Internet, such as whether there existed a universal criterion for what constituted the Internet or whether this definition would depend on local, particularistic environments.

First, the participants in the architecture retreat drew a sharp demarcation between the Internet as a communications system from the Internet as a community of people and institutions. Bounding the Internet with what they termed a sociological description, or "a set of people who believe themselves to be part of the Internet community" was deemed inefficacious.[89] Only its architectural constitution could define the Internet. This *a priori* distinction mirrored positivism and logical empiricism in the philosophy of science, research programs which made *a priori* distinctions between quantitative method and cultural belief. The research programs of logical empiricism and logical positivism normatively prescribed how science should devise and evaluate universal theories capturing the truth of the natural world. [90] Positivists advocated verification as a primary

[87] David Clark et. al, "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 2.

[88] Ibid, page 2.

[89] Ibid, page 9.

[90] For more on the research programs of logical empiricism and positivism, see Carl G. Hempel, *Philosophy of Natural Science*. Foundations of Philosophy Series, Prentice-Hall, 1966; Rudolf Carnap, *An Introduction to the Philosophy of Science*. New York: Dove Publications, 1966; and Karl Popper, *The Logic of Scientific Discovery*. London: Routledge, 1966.

criterion for theory choice, prescribing that statements are meaningful if verified by logic or by observation, with all other statements classifying as metaphysical. Among the heuristic tenets of this program were the principle that the basis of truth is found in observation and experience and the belief in a single empirical methodology for all science. This research program had well established weaknesses because empirical verification as a universal theory evaluation criterion faced the induction problem of how to logically proceed from observational particulars to general statements without facing an infinite regress. In other words, with a finite observation set, deriving theories through induction is probabilistic, a quality challenging verificationism as a universal criterion and suggesting that subjective factors enter the final decision to select one scientific claim over another. The Internet standards community, in its attempt to define the Internet as part of its protocol selection process, believed it could devise technical definitions and assess protocol alternatives on the basis of technology with no consideration of subjective factors like culture or politics.

In contrast to the Internet technical community's belief it could excise what it termed "sociological" factors from technical knowledge, philosophers of science eventually acknowledged the presence of some subjective, or metaphysical, considerations in scientific theory choice. Karl Popper, recognizing problems in the theory evaluation criteria of empirical verification, acknowledged the theory-ladenness of observation and acknowledged metaphysical and particularistic factors in science, suggesting for example, that faith in regularities of nature was a metaphysical belief. Popper prescribed that scientists evaluate theories by subjecting falsifiable theories to severe testing and further appraise theories using criteria of simplicity, universality, spare use of auxiliary hypothesis, and precision. Falsification as a theory choice criterion encountered similar logical problems in that falsifying instances should be as susceptible to theory-ladenness as confirming instances and similarly faced experimenters' regress (how many falsifying instances are necessary?).

Most interestingly, the Internet architecture retreat reached Popperian conclusions. Within the bounds of excising sociological factors and defining the Internet architecturally, the group found a universal description of the Internet that preserved the status quo. The group acknowledged that IP connectivity had historically defined

Internet connectivity. Those using IP were on the Internet and those using another network layer protocol were not. The IAB's description closely resembled theory choice criteria from the philosophy of science:

"This model of the Internet was simple, uniform, and – perhaps most important – testable."[91]

The IAB's analysis appeared to treat the Internet as a natural phenomenon about which it was theorizing. If someone could be PINGed (reached via IP), they were on the Internet. If they could not be PINGed, they were not on the Internet. This historical definition of the Internet emulates Popper's prescription that scientists evaluate theories by subjecting falsifiable theories to testing and perform further evaluation by applying criteria such as uniformity and simplicity. As addressed later, the working group evaluating protocol alternatives to replace IPv4 also cited simplicity and universality among technical evaluation criteria, again following Popper. These criteria reflexively failed to eliminate the subjective factors the IAB sought to exclude. For example, the definition of simplicity as a criterion is itself subjective, making an aesthetic judgment that simplistic protocol structures, or scientific theories, for that matter, are preferable to complex theories. This definition also appears to not descriptively match the historical progression of network protocols, which arguably seemed to become more complex over time, again subjectively depending on one's definition of simple and complex. In short, applying a universal criterion of simplicity made an aesthetic judgment. The ancillary criterion of uniformity similarly made a subjective judgment. Many Internet stakeholders at the time, as the IAB acknowledged, wanted the choice to use either OSI network protocols or TCP/IP for Internet connectivity rather than adopt a homogenous network protocol.

The IAB's prescriptive definition also did not descriptively match the networking circumstances of 1991. Many corporations operated large, private TCP/IP networks disjoint from the public Internet. These networks were based on IP but were autonomous, isolated networks that a public Internet user could not access. Business partners and customers could, if authorized, gain access to these networks, but they were

[91] David Clark et. al, "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 9.

not automatically reachable via IP from the general public Internet. Nevertheless, users of these large, private, corporate IP networks could PING each other, fulfilling the IAB's criteria of "being on the Internet." These private, corporate TCP/IP networks were not connected to the public Internet but would be considered part of the Internet, by the IAB's definition. Additionally, some companies were technically "on the Internet" without using end-to-end IP. Some businesses in 1991 connected email gateways to the Internet, using protocols other than IP for internal corporate communications and only providing an application level gateway to the public Internet for the specific application of electronic mail. These companies accessing the public Internet through gateways would be considered not on the Internet by the IP demarcation criterion. The IAB acknowledged the diversity of network environments and degrees of connectivity to the Internet, and grappled with a definition of the Internet tied to higher level name directories rather than IP addresses. Ultimately though, the 1991 *Future Internet Architecture* document expressed that protocol homogeneity, meaning TCP/IP, is "the magnetic center of the Internet evolution, recognizing that a) homogeneity is still the best way to deal with diversity in an internetwork, and b) IP connectivity is still the best basis model of the Internet (whether or not the actual state of IP ubiquity can be achieved in practice in a global operational Internet.)"[92]

Analysis from an STS perspective helps interrogate the IAB's espousal of architectural objectivity and rejection of the possibility of sociological factors entering the network protocol definition of the Internet. Examinations of science have challenged universally normative frameworks in the evaluation of scientific knowledge and have evaluated how particularistic factors enter the content of scientific knowledge. One way to further investigate the architectural protocol definition is to challenge the possibility of the disembodied objectivity the IAB claims. Philosopher of science, Sandra Harding, argues that, even if neutrality were possible, the proclivity toward neutrality is itself a normalizing value preventing scientists from challenging intellectual traditions and

[92] David Clark et. al. "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 10.

methods. Not only is neutrality infeasible, Harding argues, the cloak of neutrality dampens dissent and preserves power structures.[93]

The preservation of the intellectual traditions, methods, and standards control structures within the IAB and IETF required the preservation of TCP/IP as the Internet's protocol suite. The possibility of an OSI network protocol supplanting IP as the primary network level protocol tying together Internet devices had obvious institutional control repercussions such as the United Nations sponsored International Standards Organization encroaching upon the IAB, IETF, and IESG as the Internet standards setting and policy making authority. OSI was a more internationally endorsed protocol suite. For the Internet Protocol to retain dominance as the homogenous underpinning of the Internet, its "magnetic center," it would have to meet the requirements of rapidly expanding international requirements, particularly more Internet addresses.

The Internet's standards setting establishment appeared to collectively embrace the objective of responding to the projected international requirement for more addresses, but exhibited less unanimity about possible solutions. At the November, 1991, Santa Fe IETF meeting held at Los Alamos National Laboratory, a new working group formed to examine the address depletion and routing table expansion issues and make recommendations.[94] The group, known as the ROAD group, for ROuting and ADdressing, issued specific recommendations for the short term but failed to reach consensus about a long term solution. The IESG synthesized the ROAD Group's recommendations and forwarded an action plan to the IAB for consideration. Part of the IESG's recommendation was to issue a call for proposals for protocols to solve the addressing and routing problems. As the IESG chair summarized, "our biggest problem is having far too many possible solutions rather than too few."[95] Some of the options discussed in 1992 included:

[93] Sandra Harding, *Is Science Multicultural?* Bloomington: Indiana University Press, 1998.

[94] The formation and objectives of the ROAD Group are described in the *Proceedings of the Twenty-Second Internet Engineering Task Force*, Los Alamos National Laboratory, Santa Fe, New Mexico, November 18-22, 1991.

[95] Phillip Gross and Philip Almquist, "IESG Deliberations on Routing and Addressing," RFC 1380, November, 1992.

❒ "Garbage Collecting,"[96] reclaiming some of the many Internet addresses that were assigned but unused

❒ Slowing the assignment rate of address blocks by assigning multiple Class C addresses rather than a single Class B[97]

❒ Aggregating numerous Class C address blocks into a larger size using a technique called Classless Inter-Domain Routing (CIDR)

❒ Segmenting the Internet into either local or large areas connected by gateways, with unique IP addresses within each area but reused in other areas

❒ Enhancing or replacing IP with a new protocol that inherently would provide a larger address space.

Some of these options never gained traction. For example, the prospect of segmenting the Internet into distinct areas separated by protocol converting gateways violated a longstanding architectural philosophy of the standards setting community known as the "end-to-end principle."[98] Historically, Internet users trusted each other to locate important protocol functions (management, data integrity, source and destination addressing) at end nodes. Any intermediate technologies interrupting the end-to-end IP functionality would breach this principle. The possibility of reclaiming unused numbers from institutions, many of which anticipated needing them at some future date for private IP networks or public interconnection to the Internet, was also not a serious consideration, although there would later be examples of organizations voluntarily relinquishing unused address space. Plans for other options proceeded, including CIDR, more conservative assignment policies, and the development of a new Internet protocol.

2.3 The IPv7 "Fiasco" of 1992

The Internet's technical community experienced an institutional controversy within the context of Internet internationalization, discordance about OSI versus TCP/IP, projected address space exhaustion, the growing economic importance of the Internet, and the identified need for a new Internet Protocol. In 1992, The IAB was in the process of

[96] From the minutes of the January 7, 1992 IAB meeting. Section 3 "Policy on Assignment and Usage of IP Network Numbers." Found at http://www.iab.org/documents/iabmins/IABmins.-1992-01-07.html.

[97] Chapter IV addresses the Internet Class System.

[98] Later described by Brian Carpenter in "Architectural Principles of the Internet," RFC 1958, June, 1996.

seeking greater "internationalization of the IAB and its activities."[99] The IAB had met its objective of adding some international members such as Christian Huitema of France. One of Huitema's observations was that the only IETF working groups with any notable non-US participation were those addressing integration with OSI applications.[100] While the IAB was seeking greater internationalization of the Internet standards process, the IETF working groups were still dominated by American participants. At this time, several IETF working groups were developing alternative protocol solutions to address the issues of IP address space exhaustion and routing table growth. The IESG, following the recommendations of the ROAD Group, had already issued a call for proposals.

Also in 1992, a group of Internet technology veterans led by Vinton Cerf established a new Internet governance institution, the Internet Society (ISOC), a non-profit membership oriented institutional home and funding source for the IETF. One impetus for the establishment of this new institutional layer was the emerging issue of liability. Would IETF members face lawsuits by those organizations or institutions which believed Internet standards selection caused them injury? Other drivers included a decline in U.S. government funding of Internet standards activities and an increase in commercialization and internationalization of the Internet. ISOC would consist of fourteen trustees with greater international representation than previous Internet oversight groups[101] and paying corporate and individual members. At the first trustee meeting, held at an INET conference in Kobe, Japan, Lyman Chapin (the new IAB chair and also an ISOC trustee) presented a new IAB charter, "which would accomplish the major goal of bringing the activities of ISOC and the current Internet Activities Board into a

[99] From the minutes of the January 7, 1992 IAB meeting. (Accessed at http://www.iab.org/-documents/iabmins/IABmins.1992-01-07.html on August 12, 2003).

[100] Ibid.

[101] According to the ISOC's Articles of Incorporation, the following individuals served as the first Board of Trustees: Charles N. Brownstein (National Science Foundation), Vinton G. Cerf (CNRI), A. Lyman Chapin (Bolt Beranek & Newman), Ira Fuchs (Princeton University), Frode Greisen (UNI-C, Technical University, Denmark), Geoff Huston (Australian Academic and Research Network), Robert E. Kahn, Tomaz Kalin (RARE Secretariat, Amsterdam, Netherlands), Kenneth M. King (EDUCOM), Lawrence H. Landweber (University of Wisconsin), Kees Neggers (SURFnet, Utrecht, Netherlands), Michael M. Roberts (EDUCOM), Anthony M. Rutkowski (Sprint International).

common organization."[102] The IAB would be renamed the Internet Architecture Board (instead of the Internet Activities Board), and the formal superimposition of this group with the new incorporated, commercially and internationally funded entity would provide more legal status and legitimacy for the group. Additionally, the formation of ISOC formalized Vinton Cerf's ongoing prominence in Internet governance. Cerf's company, CNRI (Corporation for National Research Initiatives) would function as the ISOC Secretariat and also serve as a legal entity supporting ISOC. A resolution passed at the first ISOC meeting also assigned exclusive authority to Cerf, as ISOC president, to appoint members to a trustee nominating committee, a trustee election committee, a new committee on the Internet in developing countries, and a committee on Internet support for disaster relief.

Discussions within the Internet Society mirrored the IAB in highlighting the group's desire for greater international involvement, including a more formal relationship with the International Telecommunications Union (ITU) and the establishment of Internet Society chapters around the world.[103] Many characteristics of this new organization differentiated ISOC from traditional Internet standards activities within the IETF including links to international standards bodies, greater international participation, direct corporate funding, and formal paying membership.

One controversial decision by the new ISOC-related incarnation of the IAB would spark a conflagration that led members of the technical community to solidify the Internet's architectural direction, restructure the Internet's policy making structure, and articulate the IETF's overarching philosophy and values. At the June 18-19, 1992, IAB meeting at the INET conference in Kobe, Japan, the IAB reviewed the findings and recommendations of the ROAD group and the similar report from the IESG on the problem of Internet address space exhaustion and router table expansion. The IAB referred to the problem as "a clear and present danger" to the Internet and felt the short term recommendations of the ROAD Group, while sound, should be accompanied by the IETF endeavoring to "aggressively pursue" a new version of IP which it dubbed "IP

[102] Internet Society, Minutes of Annual General Meeting of the Board of Trustees, June 15, 1992, Kobe Japan. (Accessed at http://www.isoc.org/isoc/general/trustees/mtg01.shtml on August 12, 2003).

[103] Ibid.

Version 7."[104] Rather than referring this standards development goal to IETF working groups, the IAB took an uncustomary top-down step of proposing a specific protocol to replace IPv4. The IAB proposed using CLNP, ConnectionLess Network Protocol, a standard the ISO had specified as part of the OSI protocol suite.

The CLNP-based proposal, "TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing,"[105] would leave higher level TCP/IP protocols (e.g. TCP and UDP) and Internet applications unchanged but would replace IP with CLNP, a protocol specifying a variable length address reaching a maximum of 20 bytes. The CLNP protocol was already a defined specification and existed, often dormant, in many vendors' products.

The IAB's decision met its objective of seeking greater internationalization of the standards process and several of the members were directly involved and invested in OSI integration into the Internet. Ross Callon, an MIT and Stanford graduate, worked at DEC's Littleton, Massachusetts, facility specifically on "issues related to OSI – TCP/IP interoperation and introduction of OSI in the Internet."[106] Callon had previously worked on OSI standards at BBN. The presiding IAB Chairman, Lyman Chapin, worked for BBN in 1992. A Cornell graduate involved in standards development related to OSI, Chapin had noted the irony of formally ratifying OSI international standards but using the TCP/IP-based Internet to communicate these standards. His self-described interest was to "inject as much of the proven TCP/IP technology into OSI as possible, and to introduce OSI into an ever more pervasive and worldwide Internet." [107] IAB member, Christian Huitema, had also participated in OSI developments and Cerf was advocating that, "with the introduction of OSI capability (in the form of CLNP) into important parts of the Internet.. a path has been opened to support the use of multiple protocol suites in

[104] From the Internet Activities Board meeting minutes from the INET conference in Kobe, Japan, June 18-19, 1992. (Accessed at http://www.iab.org/documents/iabmins/IABmins. 1992-06-18.html on August 12, 2003).

[105] See Ross Callon, "TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing," RFC 1347, June, 1992.

[106] According to RFC 1336, "Who's Who in the Internet, Biographies of IAB, IESG and IRSG Members," published in May, 1992.

[107] According to RFC 1336, "Who's Who in the Internet, Biographies of IAB, IESG and IRSG Members," May, 1992.

the Internet."[108] The IAB's CLNP-based proposal for the new Internet Protocol was part of its overall internationalization objectives of integrating internationally preferred protocols into the Internet environment.

Huitema, later recollecting the IAB's CLNP recommendation, explained that he had composed the draft specification on the plane home from the Kobe meeting and that the draft went through eight revisions within the IAB over the following two weeks. Huitema recalled, "We thought that our wording was very careful, and we were prepared to discuss it and try to convince the Internet community. Then, everything accelerated. Some journalists got the news, an announcement was hastily written, and many members of the community felt betrayed. They perceived that we were selling the Internet to the ISO, that headquarters was simply giving the field to an enemy that they had fought for many years and eventually vanquished."[109]

Rank and file participants in the primarily American IETF working groups were outraged about the IAB's suggestion to replace IP with the ISO's CLNP protocol. This dismay surfaced immediately on the Internet mailing lists and at the IETF meeting held the following month. Bearing into consideration that the IETF mailing lists generally contain strong opinions, the reaction to the IAB recommendations was unusually acrimonious and collectively one of "shocked disbelief"[110] and concern that the recommendation "fails on both technical and political grounds."[111] The following abridged excerpts from the publicly available IETF mailing list archives (July 2-7, 1992) reflect the IETF participants' diverse but equally emphatic responses to the IAB recommendation:

> *Do you want to see the political equation? IPv7 = DECNET Phase 5*
>
> *In voluntary systems such as ours, there is a fundamental concept of "the right-to-rule" which is better known as "the consent of the governed." Certainly the original IAB membership had a bona fide right-to-rule when it was composed of senior researchers who designed and implemented a lot of the stuff that was used. Over time, however, the IAB has degenerated under vendor and standardization influences. Now, under ISO(silent)C auspices, the IAB gets to hob-nob around the globe, drinking to the health of*

[108] Ibid.

[109] See Christian Huitema, *IPv6 The New Internet Protocol*. Prentice Hall, 1996, page 2.

[110] Jon Crowcroft (J.Crowcroft@cs.ucl.ac.uk) posting on the IETF mailing list, July 2, 1992.

[111] Marshall Rose (mrose@dbc.mtview.ca.us) posting on the IETF mailing list, July 7, 1992.

Political Correctness, of International networking and poo-poo'ing its US-centric roots. I'm sorry, but I'm just not buying this. The Internet community is far too important to my professional and personal life for me to allow it to be sacrificed in the name of progress.

I view this idea of adopting CLNP as IPv7 as a disastrous idea..
adopting CLNP means buying into the ISO standards process..
as such, we have to face the painful reality that any future changes that the Internet community wishes to see in the network layer will require ISO approval too.

For decisions this big, I'm shocked to see that IAB made the move without holding an open hearing period for opinions from the Internet community.

Procedurally, I am dismayed at the undemocratic and closed nature of the decision making process, and of the haste with which such as major decision was made.

When the IAB tells them that the IAB knows what's best – better than the best minds in this arena know, they are on very dangerous ground.

A proposed change with such extensive impact on the operational aspect of the Internet should have the benefit of considerable open discussion.

The IAB needs to explain why it believes we can adopt CLNP format and still have change control.

IETF participants considered the IAB's proposal controversial for several reasons. The most contentious area concerned standards setting procedures. The IAB's protocol recommendation had circumvented traditions within the standards setting community in which technical standards percolated up from the working groups to the IESG to the IAB, not the converse. Recommendations usually involved a period of public (the IETF public) review and comment. Other IETF participants suggested the IAB no longer had the legitimacy of being comprised of elders and veterans from the ARPANET days and that new IAB members were often not involved in direct coding or standards development. They were suspicious of the recently adopted hierarchical structure which subverted the IAB under a newly formed, private, international legal entity - the Internet Society. Another concern was that vendors, especially DEC, with its heavy investment in OSI, had undue influence in standards selection. Additionally, the new ISOC institutional structure was a departure from previous norms in that network vendors contributed funding to the new organization.

The greatest concerns related directly to the competition between the IETF and the ISO as standards bodies and issues of power and control over standards development and change control. Some IETF participants believed that adoption of an OSI standard meant relinquishing administrative and technical control of protocols to the ISO. Would the IETF still have "change control," as USC's Deborah Estrin questioned? IETF participants feared that protocol development would subsequently be subjected to the ISO's lengthy, top-down, and complex standards development procedures. From a technical and procedural standpoint, some questioned why there was no comparison to the other IPv4 alternatives IETF working groups were already developing. The IESG recommended that the community examine other alternatives for the new Internet protocol rather than uniformly pursuing the TUBA proposal based on the OSI CLNP protocol. The backlash over the IAB's recommendation was multifaceted, involving concerns about CLNP's association with the ISO, questions about whether CLNP was the best alternative, concern about the influence of network equipment and software vendors, and alarm about the IAB's top-down procedural maneuver.

These concerns pervaded deliberations at the twenty-fourth Internet Engineering Task Force meeting convening the following month at the Cambridge, Massachusetts, Hyatt Regency adjacent to the MIT campus.[112] Participating in the more than 80 technical working groups held during the IETF meeting were 687 attendees, a 28% increase over the IETF's previous meeting in San Diego. Technical and procedural challenges associated with Internet growth were the predominant topics of discussion and the culmination of the meeting was a plenary session delivered by MIT's David Clark. Within the IETF community, Clark was respected as a long time contributor to the Internet's architecture, had served as the ICCB's chair beginning in its inaugural year, 1979, and had also previously served as the IAB's chair.

Clark's plenary presentation, "A Cloudy Crystal Ball, Visions of the Future," reflected the angst IETF working group participants felt about the IAB's CLNP recommendation, and ultimately articulated the philosophy that would become the

[112] According to the *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, MIT, Cambridge, Massachusetts, July 13-17, 1992, compiled and edited by Megan Davres, Cynthia Clark, and Debra Legare.

IETF's *de facto* motto. Clark's presentation, to which he assigned the alternative title, "Apocalypse Now," attempted to examine four "forces" shaping the activities of the Internet standards setting community: 1) new Internet services such as real time video; 2) emerging commercial network services such as ATM (Asynchronous Transfer Mode), SMDS (Switched Multimegabit Data Service), and B-ISDN (Broadband Integrated Services Digital Network); 3) cyber-terrorists; and 4) "Us: We have met the enemy and he is…" Clark's last topic, "us," reflected upon the status of the standards community and questioned the optimal model for constructing standards. Clark compared the IAB's current role as "sort of like the House of Lords," advising and consenting to the IESG's proposals, which themselves should percolate up from the IETF working group deliberations. Clark suggested that more checks and balances would be advantageous.

An enduring legacy of Clark's plenary presentation was an articulation of the IETF's core philosophy:

> *"We reject: kings, presidents and voting.*
> *We believe in: rough consensus and running code."*[113]

In particular, the phrase "rough consensus and running code" would become the IETF's operating credo. The standards community, according to Clark, had traditionally succeeded by adopting working, tested code rather than proposing top-down standards and making them work. The message was clear. Reject the IAB's top-down mandate for a new Internet protocol. The IETF's resistance to the IAB's OSI-based TUBA proposal was also evidenced by the conference's presentations and discussions of two competing protocol alternatives, PIP, the "P" Internet Protocol by Bellcore's Paul Tsuchiya, and Bob Hinden's and Dave Crocker's IPAE, IP Address Encapsulation.[114]

The IAB formally withdrew its draft at the IETF conference, which concluded with several outcomes: 1) the IETF would continue pursuing alternative proposals for the next generation Internet protocol rather than exclusively pursuing TUBA; 2) the

[113] From David Clark's plenary presentation, "A Cloudy Crystal Ball, Visions of the Future," at the 24th meeting of the Internet Engineering Task Force, Cambridge, Massachusetts, July, 1992. *Proceedings of the 24th Internet Engineering Task Force*, page 539.

[114] See "A PIP Presentation – The "P" Internet Protocol" by Paul Tsuchiya of Bellcore and "IP Address Encapsulation (IPAE)" by Robert Hinden and Dave Crocker in the *Proceedings of the 24th meeting of the Internet Engineering Task Force*, Cambridge, Massachusetts, July, 1992.

Internet's core philosophy of working code and rough consensus would remain intact; 3) the standards decision process and institutional roles required examination and revamping, and 4) the rank and file IETF participants had asserted a grassroots counter balance to the influence of the self-appointed, closed, and more internationally-oriented IAB, the influence of (some) vendors in the standards process, and the government and vendor influenced momentum of the ISO. One of the specific institutional outcomes of the Kobe affair and subsequent discussion on the IETF boards and at the Cambridge meeting was a consensus decision to determine and instill a procedure for selecting members of the IESG and IAB. Immediately following the IETF meeting, Cerf, still Internet Society president and responsible for the selection of many IAB and IESG members, called for a new working group to examine issues of Internet leader selection, as well as standards processes.[115] Steve Crocker headed the working group, designated the POISED Group, for Process for Organization of Internet Standards Working Group. At that time, Steve Crocker was a Vice President at Internet security firm Trusted Information Systems (TIS) and the IETF's Area Director for Security. Crocker was a long time insider in the Internet standards community and had formerly worked at USC's Information Sciences Institute and served as a research and development program manager at DARPA.[116]

The specific charter of the new working group was to scrutinize Internet standards procedures, IAB responsibilities, and the relationship between the IAB and the IETF/IESG. For example, what should the procedures be for appointing individuals to the IAB? How should the standards community resolve disputes among the IETF, IAB, and IESG? Some of the working group's conclusions[117] included term limits for IAB and IESG members and a selection process by committees and with community input. An

[115] Steve Crocker, "The Process for Organization of Internet Standards Working Group," RFC 1640, June 1994.

[116] From Crocker's biography published in the Proceedings of the Twenty-Fifth Internet Engineering Task Force, Washington, D.C. November 16-20, 1992.

[117] See the following RFCs: Internet Architecture Board and Internet Engineering Steering Group, "The Internet Standards Process – Revision 2," RFC 1602, March, 1994; Christian Huitema, "Charter of the Internet Architecture Board," RFC 1601, March, 1994; Erik Huizer and Dave Crocker, "IETF Working Group Guidelines and Procedures," RFC 1603, March, 1994; and Steve Crocker, "The Process for Organization of Internet Standards Working Group (POISED), RFC 1640, June, 1994.

IETF nomination committee would consist of seven members chosen randomly from a group of IETF volunteers and one non-voting chair selected by the Internet Society.[118] The enunciation of the institutional power relations within the Internet standards community reflexively passed the "working code" philosophy in that the IETF attempted to retain the traditional IETF bottom-up and participatory process it believed had worked well. Borrowing a metaphor from the broader 1990s political discourse, Frank Kastenholz summarized on the IETF mailing list, "the New World Order was brought in when the IAB apparently disregarded our rules and common practices and declared that CLNP should be IP6. They were fried for doing that."[119] In short, the IAB recommendation and subsequent fracas resulted in a revamping of power relations within the standards setting community, an articulation of institutional values, and a demonstration of IETF institutional resistance to adopting any OSI protocols within the Internet's architecture.

2.4 "We Still Need Computer Science Ph.D.s to Run Our Networks"

After the contentious July, 1992, IETF meeting, discussions about a new protocol, referred to as Next Generation IP (IPng), dominated the IETF mailing lists and the following IETF meeting held in Washington, D.C., on November 16-20, 1992. The Monday morning opening session commenced with competing technical presentations on the four proposals, at that time, candidates to become IPng:

❒ TUBA (TCP and UDP with Bigger Addresses)
❒ PIP (The "P" Internet Protocol)
❒ SIP (Simple Internet Protocol)
❒ IPAE (IP Address Encapsulation).

TUBA, the center of the Kobe controversy, remained on the table. This protocol, built upon the OSI-based CLNP, would replace the current Internet Protocol, IPv4, and would provide a 20-byte (160 bit) address exponentially increasing the number of devices the Internet could support. Bellcore's Paul Tsuchiya presented an alternative proposal,

[118] The process is described in RFC 1601, "Charter of the Internet Architecture Board" authored by Christian Huitema, March, 1994.

[119] Frank Kastenholz posting on the IETF.ietf mailing list, March 24, 1995

PIP, which would be a completely new protocol developed within the Internet's standards-setting establishment. PIP would offer a novel approach of specifying IP addresses with an unlimited address length based on dynamic requirements.

Steve Deering of Xerox PARC delivered the presentation on SIP, which he called IP Version 6. SIP would take an incremental approach of retaining the characteristics of the Internet Protocol but extending the address size from 32 bits to 64 bits. Sun Microsystem's Bob Hinden offered a technical presentation of IPAE, which was actually a transition mechanism from IPv4 to a new Internet protocol which was assumed by the IPAE Working Group to be SIP. Part of Hinden's presentation discussed how this proposed protocol differed from TUBA. A selling point of IPAE/SIP was that it would retain existing semantics, formats, terminology, documentation, and procedures and would have "No issues of protocol ownership." The competing Internet proposals, especially SIP and TUBA, were not radically different from a technical standpoint, but the question of *who* would be developmentally responsible for the architectural underpinning of the Internet, the established participants within the Internet's traditional standards setting format or the ISO, continued to be a distinguishing factor and an institutional concern.

At the following IETF gathering (July, 1993) in Amsterdam, the first ever held outside of North America,[120] a Birds of a Feather (BOF) group called the IPng Decision BOF formed. A BOF group is similar to an IETF working group but has no charter, convenes once or twice, and often serves as a preliminary gauge of interest in forming a new IETF working group.[121] The Amsterdam IPng Decision BOF, also called IPDecide, sought to discuss the decision process for the IPng selection. Two hundred people attended the IPDecide BOF and consensus opinion suggested that the IETF needed to take decisive action to select IPng and that any option of letting the market decide was unacceptable. The early 1980s development of the Internet Protocol occurred in a closed technical community outside of market mechanisms so the idea of non-market developed

[120] 46% of the 500 attendees represented countries other than the United States, whereas previously held meetings averaged between 88-92% American attendees, according to the *Proceedings of the Twenty-Seventh Internet Engineering Task Force*, Amsterdam, The Netherlands, July 12-16, 1993.

[121] Defined in George Malkin's "The Tao of the IETF – A Guide for New Attendees of the Internet Engineering Task Force," RFC 1391, January, 1993.

standards was not an aberrant proposition. The IPDecide BOF suggested that the marketplace already had an overabundance of protocol choices, that there were some architectural issues (such as the Domain Name System) which could not contend with multiprotocol environments and required a single protocol, and that:

"The decision was too complicated for a rational market-led solution."[122]

CERN's Brian Carpenter doubted that the general market had any idea that solutions to the problem were being discussed or even that a problem existed. He believed it would take several years for the market to understand the problem and agreed with those who suggested "we still need Computer Science Ph.D.s to run our networks for a while longer."[123]

The IESG created a new *ad hoc* working group to select IPng. The new working group tapped two Internet veterans as co-Area Directors (ADs): Allison Mankin of the Naval Research Laboratory, an IESG member and AD of Internet Transport Services; and Scott Bradner of Harvard University's Office of Information Technology, an IESG member, and AD of Internet Operational Requirements.

In December, 1993, Mankin and Bradner authored a formal requirements solicitation for IPng entitled RFC 1550, "IP: Next Generation (IPng) White Paper Solicitation."[124] The solicitation invited any interested parties to recommend requirements IPng should meet and to suggest evaluation criteria which should determine the ultimate selection of IPng. The white paper solicitation promised that the submitted documents would become publicly available as informational RFCs and that the IPng Working Group would use this input as resource materials during the selection process.

2.5 Proposals First, Requirements Second

This call for public participation and requirements input into the new Internet protocol was, in many ways, the horse behind the cart. The white paper solicitation sought public

[122] From the Minutes of the IPng Decision Process BOF (IPDECIDE) reported by Brian Carpenter (CERN) and Tim Dixon (RARE) with additional text from Phill Gross (ANS), July 1993. (Accessed at http://mirror.switch.ch/ftp/doc/ietf/93jul/ipdecide-minutes-93jul.txt on August 12, 2003).

[123] Brian Carpenter, submission to big-internet mailing list, April 14, 1993.

[124] Scott Bradner and Allison Mankin, "IP: Next Generation (IPng) White Paper Solicitation," RFC 1550, December, 1993.

requirements for IPng which would presumably be incorporated into subsequent proposals. This type of formal process of requirements definition customarily precedes the submission of proposals. In this case, however, requirements criteria, calls for proposals, working groups, proposals, and even some evaluative comparisons of proposals had all already occurred. For example, several sets of requirements for the new protocol were already circulating through the standards community. Working groups already crafted competing protocol alternatives. Most obviously, a formal call for proposals had already been made at the contentious July, 1992, IETF meeting in Cambridge. If IPng working groups were already established and proposals already available, why did the IETF formally conduct an *ex post facto* white paper solicitation seeking requirements and calling for public input?

An informational RFC published in May, 1993, by Tim Dixon already offered a comparison of available IPng proposals. Dixon was the Secretariat of Reseaux Associés pour la Recherche Européenne (RARE), the European Association of Research Networks, which published a series of documents called RARE technical reports sometimes republished as informational RFCs. RFC 1454, "Comparison of Proposals for Next Version of IP," was a republished RARE technical document. The report compared PIP, TUBA, and SIP, and concluded that the three proposals had minimal technical differences and that the protocols were too similar to evaluate on technical merit. The IPDecide BOF also had raised this issue at the Amsterdam IETF meeting, with some suggesting that the proposals lacked significant enough technical distinctions to evaluatively differentiate[125] and, even if there were differences, technical evaluation criteria were too general to argue for any one proposal. Some individuals within the IETF community were displeased with the IPng selection process. Noel Chiappa, former IETF Internet Area Co-Director, member of the TCP/IP Working Group and its successor group since 1977, and formerly at MIT as a student and research staff member,[126] expressed ongoing dismay about this process. Chiappa believed a more effective

[125] From the Minutes of the IPng Decision Process BOF (IPDECIDE) reported by Brian Carpenter (CERN) and Tim Dixon (RARE) with additional text from Phill Gross (ANS), July 1993. (Accessed at http://mirror.switch.ch/ftp/doc/ietf/93jul/ipdecide-minutes-93jul.txt on August 12, 2003).

[126] From RFC 1336, "Who's Who in the Internet: Biographies of IAB, IESG and IRSG Members, May, 1992.

approach would have been to define requirements first, or "what a new internetwork layer ought to do" and then determine how to meet those requirements.[127] Chiappa, as an independent inventor, was one of the IETF members not overtly affiliated with a technology vendor and its products, but had proposed his own alternative project, "Nimrod," not advanced as one of the IPng alternatives. Nevertheless, his criticisms illuminated several characteristics of the selection process including the *ex post facto* requirements definition approach, the conflict between the ISO and the IETF, and the tension between grassroots versus top-down standards procedures. In short, Chiappa wrote, "That a standards body with responsibility for a key piece of the world's infrastructure is behaving like this is frightful and infuriating."[128]

Instead of technically differentiating the proposals, the RARE report suggested a political rational for a formal selection process: "the result of the selection process is not of particular significance, but the process itself is perhaps necessary to repair the social and technical cohesion of the Internet Engineering Process."[129]

Dixon highlighted the ongoing tension about OSI permeating the IPng selection, suggesting that TUBA faced a "spurious 'Not Invented Here' Prejudice"[130] on one hand, and warning that the new protocol ironically faced the danger of what many perceived as the shortcomings of the OSI standards process:

❒ "Slow progress
❒ Factional infighting over trivia
❒ Convergence on the lowest common denominator solution
❒ Lack of consideration for the end-users."[131]

The IETF BOF group raised another rationale for conducting a formal protocol evaluation process, citing the possibility of "potential legal difficulties if the IETF

[127] Excerpts from Noel Chiappa posting on the info.big-internet newsgroup, May 14, 1994, Subject "Thoughts on the IPng situation…"

[128] Excerpts from Noel Chiappa posting on the info.big-internet newsgroup, May 14, 1994, Subject "Thoughts on the IPng situation…"

[129] Tim Dixon, "Comparison of Proposals for Next Version of IP," RFC 1454, May, 1993.

[130] Ibid.

[131] Ibid.

appeared to be eliminating proposals on arbitrary grounds."[132] Within the context of what some considered technically similar proposals, ongoing anxiety about OSI, fear of possible legal repercussions of the protocol selection, and rapid global Internet growth, the IETF issued its white paper solicitation for requirements the next generation Internet protocol should meet. Mankin's and Bradner's brief, six page solicitation invited interested parties to submit documents detailing requirements for IPng that could be used by the IPng Area Working Groups to complete the selection process for the new protocol. Some questions in the solicitation included: what was the required timeframe for IPng; what security features should the protocol include; what configuration and operational parameters are necessary; and what media, mobility, topology, and marketplace requirements should IPng meet? Bradner and Mankin received 21 responses to their white paper solicitation. Three submissions came from companies in industries, at the time, considered poised to become future "information superhighway" providers: the cable television industry, the cellular telephone industry, and the electric power industry.[133] These companies and industries, as potentially new Internet providers, obviously had a vested interest in the standard to which their services would likely comply. Other submissions addressed specific military requirements, corporate user requirements, and security considerations. Several submissions were recapitulations of the actual protocol proposals currently competing for IPng status.

[132] From the Minutes of the IPng Decision Process BOF (IPDECIDE) reported by Brian Carpenter (CERN) and Tim Dixon (RARE) with additional text from Phill Gross (ANS), July 1993. (Accessed at http://mirror.switch.ch/ftp/doc/ietf/93jul/ipdecide-minutes-93jul.txt on August 12, 2003).

[133] See: Ron Skelton, "Electric Power Research Institute Comments on IPng," RFC 1673, August, 1994; Mark Taylor, "A Cellular Industry View of IPng," RFC 1674, August, 1994; and Mario Vecchi, "IPng Requirements: A Cable Television Industry Viewpoint," RFC 1686, August, 1994.

2.6 U.S. Corporate User Perspective

One area of IPng accord within the Internet standards setting community continued to be the espousal of the following philosophy:

> *"the IETF should take active steps toward a technical decision, rather than waiting for the "marketplace" to decide."*[134]

Nevertheless, some of the white paper responses reflected market requirements of large corporate Internet users, which comprised a major marketplace sector of an increasingly commercialized Internet industry.

Large corporate Internet users did not uniformly share the IETF's sanguine belief in the need for a next generation Internet Protocol. Historian of technology, Thomas Hughes, suggests new technology advocates err severely in underestimating the inertia and tenacity of existing technological systems.[135] Once developed and installed, technological systems acquire conservative momentum. This momentum arises from such characteristics as financial investments, political commitments, personal stake, institutional commitments, knowledge base, and installed material conditions. Hughes' examples of conservative momentum primarily address large system developers, describing how technological systems reflect powerful interests with substantially vested capital and human resources that a significant system change might jeopardize.[136] In the case of a new Internet protocol, United States corporate users represented a conservative foundation for IPv4. U.S. corporate Internet users generally had ample IP addresses, a topic Chapter IV addresses, and substantial investment in IPv4 capital and human resources.

Boeing Corporation's response to the white paper solicitation sought to summarize the U.S. corporate user view:

> *"Large corporate users generally view IPng with disfavor."*[137]

Boeing suggested that Fortune 100 corporations, then heavy users of internal TCP/IP networks, viewed the possibility of a new protocol, IPng, as "a threat rather than

[134] Bullet point presented by the IETF chair in a meeting entitled "IPDecide BOF" at the 1993 IETF Amsterdam.

[135] Thomas Hughes, *American Genesis: A History of the American Genius for Invention*. New York: Penguin Books, 1989, page 459.

[136] Ibid, page 460.

[137] Eric Fleischman, "A Large Corporate User's View of IPng," RFC 1687, August, 1994, page 1.

an opportunity."[138] In the early 1990s, large U.S. corporations primarily operated mixed protocol network environments rather than a single network protocol connecting all applications and systems. Corporations wanted a single, interoperable suite of protocols, but it was not yet clear which of several alternatives, if any, would meet this requirement. Correspondingly, the Boeing Corporation's white paper response acknowledged that it used at least sixteen distinct families of protocols within its corporate networks. Typifying large corporate network users in this era, Boeing had an installed base of older network protocol suites like IBM's Systems Network Architecture (SNA) to connect IBM platforms and DECnet for DEC computing platforms, along with AppleTalk for its Macintosh environments, IPX/SPX for its Local Area Networks (LANs) running Novell's Netware, and also private TCP/IP networked environments. Many TCP/IP implementations within large corporate user environments supported internal network computing and did not necessarily provide widespread connectivity to the Internet. Each network environment – SNA, DECnet, Appletalk, IPX/SPX, and TCP/IP - required distinct human skills, equipment, and support infrastructures.

The prevailing trend was to reduce the number of network protocol environments rather than expand them, or, as the Boeing response summarized: "..a basic abhorrence to the possibility of introducing "Yet Another Protocol" (YAP)."[139] TCP/IP implementations relied entirely on the prevailing IPv4 protocol, and Boeing suggested its TCP/IP network was approaching the point of interconnecting 100,000 host computers. Even if the global Internet homogenously adopted a new Internet protocol, Boeing believed it could deploy an application level gateway at the demarcation point between its network and the Internet to convert between IPv4 and the new IPng. The one possible economic rationale for adopting a new protocol would be market introduction of "killer apps" relying solely on IPng. The introduction of greater TCP/IP security would present another opening for the possibility of laboriously converting 100,000 computing devices to a new protocol.

Boeing also acknowledged prevailing tension between OSI and TCP/IP and suggested that any ability of IPng to foster a convergence between the two disjoint

[138] Ibid, page 2.

[139] Eric Fleischman, "A Large Corporate User's View of IPng," RFC 1687, August, 1994, page 6.

protocol suites would make IPng more desirable. It sold products in a global marketplace, often to government customers. Support of a protocol integrated with OSI could prove advantageous in competitive bids for contracts from governments supporting OSI. Additionally, an OSI-based protocol was beginning to replace proprietary network protocols for air-to-ground and ground-to-ground communications, further indicating that any OSI convergence IPng could achieve would make the protocol more economically appealing. Consequently, Boeing suggested that any IPng approach should provide an eventual integration between what it termed Internet standards versus international standards. Even if IPng could achieve an integration with OSI, offer new applications, or add functionality such as improved security, Boeing and other corporate users wanted IPng to coexist with the massive installed base of IPv4 for the foreseeable future.

The one potential rationale for deploying a new protocol not cited by Boeing was the need for more IP addresses. In other words, "Address depletion doesn't resonate with users."[140] According to Internet address distribution records, at the time, Boeing controlled 1.3 million unique addresses.[141] Large American corporate Internet users generally had sufficient, if not superfluous, Internet address reserves and, as Boeing suggested, only a new "killer app" requiring IPng would motivate them to replace their current implementations with a new Internet Protocol. According to Hughes, overcoming the momentum of a large technological system requires a force analogous to that which extinguished the dinosaurs, such as the oil embargo of 1973 or technological catastrophes such as the 1986 Challenger space shuttle disaster or the 1979 Three-Mile Island disaster.[142]

IBM's white paper response reinforced the extent of conservative momentum behind the IPv4 standard, suggesting "IPv4 users won't upgrade to IPng without a

[140] Eric Fleischman, "A Large Corporate User's View of IPng," RFC 1687, August, 1994, page 7.

[141] Boeing held at least twenty distinct Class B address blocks and eighty Class C address blocks. Each Class B address block contains more than 65,000 addresses and each Class C contains 256 addresses, so Boeing controlled at least 1.3 million IP addresses. Source for Address assignment records: Sue Romano, Mary Stahl, Mimi Recker, "Internet Numbers," Network Working Group, RFC 1117, August, 1989.

[142] Thomas Hughes, *American Genesis: A History of the American Genius for Invention*. New York: Penguin Books, 1989, page 462-463.

compelling reason."[143] Similarly, Bolt Beranek and Newman (BBN), the developer of ARPANET's original Interface Message Processors, noted that the IPng effort was "pushing" network technology. The BBN response stressed that marketplace demands should drive the development of IPng and questioned whether IPv4 users would ever have a compelling justification to upgrade to a new protocol.[144]

In contrast, companies without significant investment in IPv4 or positioned to profit from the availability of more addresses or the development of new products and services embraced the idea of a new protocol. This was especially true among industries which were potential new entrants into the Internet Service Provider market. The early 1990s growth and commercialization of the Internet as well as discussions of a multimedia "global information superhighway" or "National Information Infrastructure" within the Clinton administration and in the media, drew attention to the economic potential for non-Internet network service providers to enter the increasingly lucrative Internet services marketplace.

The novel Internet application, the World Wide Web, spurred significant Internet growth in the early 1990s. U.S. based corporations embraced the capabilities of this hyperlinked platform through which they could instantly reach customers and business partners. The Clinton administration established an Internet presence with its own web page and electronic mail addresses for the President, Vice President Al Gore, and First Lady Hillary Clinton. In September of 1993, Gore and Secretary of Commerce Ron Brown formally heralded a National Information Infrastructure (NII) initiative, an expansive economic and social project to promote a national network linking together a variety of network infrastructures and, by 2000, at a minimum "all the classrooms, libraries, hospitals, and clinics in the United States."[145] Also called the "Information Superhighway," the NII initiative did not directly refer to the Internet in its current incarnation, but a more broad amalgamation and convergence of telecommunications

[143] Edward Britton and John Tavs, "IPng Requirements of Large Corporate Networks," RFC 1678, August, 1994.

[144] John Curran, "Market Viability as a IPng Criteria," RFC 1669, August, 1994.

[145] National Information Infrastructure White Paper, "Administration White Paper on Communications Act Reforms." (Accessed at http://ibiblio.org/pub/academic/political-science/internet-related/NII-white-paper on October 8, 2003).

networks, entertainment, and cable systems. The initiative both highlighted possibilities for Internet expansion and intimated that alternative infrastructures, especially cable systems, might provide separate services competing with the Internet in its 1993 embodiment.

In 1993, there was little convergence of different information types over a common medium. Telephone networks and cellular systems supported voice, computer networks supported data, and cable companies transmitted video. The promise of integrating these services over a single, converged, multimedia service represented an enormous opportunity, and several of the white paper responses reflected this interest. Companies in industries not supporting data transmission, and which had never been closely involved in Internet standards development, were interested in a new protocol, IPng, as a way to suddenly compete with existing Internet and data providers like major national telephone companies and new Internet Service Providers.

For example, cable companies envisioned opportunities to become providers of converged services, and one much hyped promise of the "information superhighway" was video-on-demand, the ability to order a movie in real time over a network through a set-top box connected to a television or computer. The emergence of this service outside of cable systems, such as through an ISP, would threaten the cable industry. This interest to expand into the data services market, or at least protect its core market, was reflected in Time Warner Cable's response to the IPng white paper solicitation, "IPng Requirements: A Cable Television Industry Viewpoint."[146] The response touted the potential for cable television networks, because of their ubiquity and broadband capacity, to become the dominant platform for delivery of interactive digital services supporting integrated voice, video, and data information. At the time, only a small percentage of American consumers had home Internet access and there was no interactive network combining video and data transmissions. Time Warner was in the process of building a highly publicized, experimental broadband network in Orlando, Florida, promising to integrate video, voice, and data services. This offering would involve a network based on a then-touted networking technology, Asynchronous Transfer Mode (ATM) connected to a "set-

[146] Mario Vecchi, "IPng Requirements: A Cable Television Industry Viewpoint," RFC 1686, August, 1994.

top" box linked to a consumer's television. The purpose of the Time Warner Cable white paper response was to position itself, and the cable industry generally, as dominant future providers of converged "information superhighway" services and to embrace IPng as a potential protocol supporting broadband interactive cable service. IP, as a network protocol for addressing and routing, actually would have no relationship or ability to facilitate convergence of voice, video, and data, but was nevertheless embraced as a way to provide more addresses, therefore reaching more consumers, and perhaps as a late entrant opportunity to enter the Internet marketplace and become involved in the Internet standards process.

The cellular industry was another sector not involved in Internet services but hoping to become competitive through the potential of converged voice and data services. Mark Taylor, the director of system development for McCaw Cellular Communications, Inc., responded on behalf of the Cellular Digital Packet Data (CDPD) consortium of cellular providers. The primary requirements of the digital cellular consortium were mobility, the ability to "operate anywhere anytime" and scalability, meaning "IPng should support at least tens or hundreds of billions of addresses."[147]

The Electric Power Research Institute (EPRI) also submitted an interesting response to the IPng white paper solicitation on behalf of the electric power industry. The EPRI, a non-profit research and development institution representing seven hundred utility companies, specifically linked the future of IP to the National Information Infrastructure and compared its importance to standards for railroads, highways, and electric utilities. The EPRI response suggested that, while the electric power industry currently used TCP/IP protocols, it was pursuing a long term strategy of employing OSI protocols. In short, the requirements of the electric power industry "are met more effectively by the current suite of OSI protocols and international standards under development."[148] One of the reasons EPRI stated that it preferred OSI standards was that it believed the NII should have an international perspective. Another reason for endorsing OSI protocols was that the EPRI had already, according to its white paper

[147] Mark Taylor, "A Cellular Industry View of IPng," RFC 1674, August, 1994.

[148] Ron Skelton, "Electric Power Research Institute Comments on IPng," RFC 1673, August, 1994.

submission, developed and invested in industry specific communications standards and services based on OSI.

2.7 The Selection: ISO Standard v. IETF Standard

Upon completion of the white paper solicitation process, who would ultimately decide which protocol proposal would become IPng? Bradner and Mankin, as the IPng Area Directors, would make the final recommendation to the IESG for approval. Additionally, the IESG also established an "IPng Directorate" to function as a review body for the proposed alternatives which already existed prior to the white paper solicitation process calling for public IPng input. The IPng Directorate, over the course of the selection process, included the following individuals:[149] J. Allard, Microsoft; Steve Bellovin, AT&T; Jim Bound, Digital; Ross Callon, Wellfleet; Brian Carpenter, CERN; Dave Clark, MIT; John Curran, NEARNET; Steve Deering, Xerox PARC; Dino Farinacci, Cisco; Paul Francis, NTT; Eric Fleischmann, Boeing; Robert Hinden, Sun Microsystems; Mark Knopper, Ameritech; Greg Minshall, Novell; Yakov Rekhter, IBM; Rob Ullmann, Lotus; and Lixia Zhang, Xerox.

Bradner and Mankin later indicated these individuals were selected for diversity of technical knowledge and equitable representation of those involved in each IPng proposal working group.[150] The group represented numerous technical areas spanning routing, security, and protocol architectures, but only exhibited diversity in this sense. The majority (88%) of IPng Directorate members represented software vendors (Microsoft, Novell, Lotus, Sun Microsystems), hardware vendors (Digital, Wellfleet, Cisco, IBM) or their research arms (Xerox PARC), or service providers (AT&T, NEARNET, NTT, Ameritech). These corporations would presumably incorporate the new standard, once selected, into their products and therefore had an economic stake in the outcome. Most of the corporations represented on the IPng Directorate were based in the United States. The only academician on the IPng Directorate was MIT Professor David Clark, again a respected long time denizen of the Internet's technical community.

[149] Scott Bradner and Allison Mankin, "The Recommendation for the IP Next Generation Protocol," RFC 1752, January, 1995.

[150] Ibid.

Only one member, Lixia Zhang, was female. Only one member represented Internet users, and only corporate Internet users: Boeing's Eric Fleischmann, author of "A Large Corporate User's View of IPng," the white paper response indicating that corporate users viewed the idea of IPng circumspectly.

There was no direct representation on the IPng Directorate of the United States government or other government. There were no individual end users and only one large corporate end user. Many participants in the 1990s standards setting community had corporate organizational affiliations so the IPng Directorate composition was not surprising. Nevertheless, the IPng Directorate was relatively homogenous. One "rule at start" for the IPng directorate was that no IESG or IAB members would participate, although directorate members Brian Carpenter and Lixia Zhang were both also IAB members. Bradner and Mankin emphasized that the IAB would implicitly not participate in the ultimate approval process, a ground rule emphasizing the IAB's diminished standards setting credibility after the Kobe affair.[151]

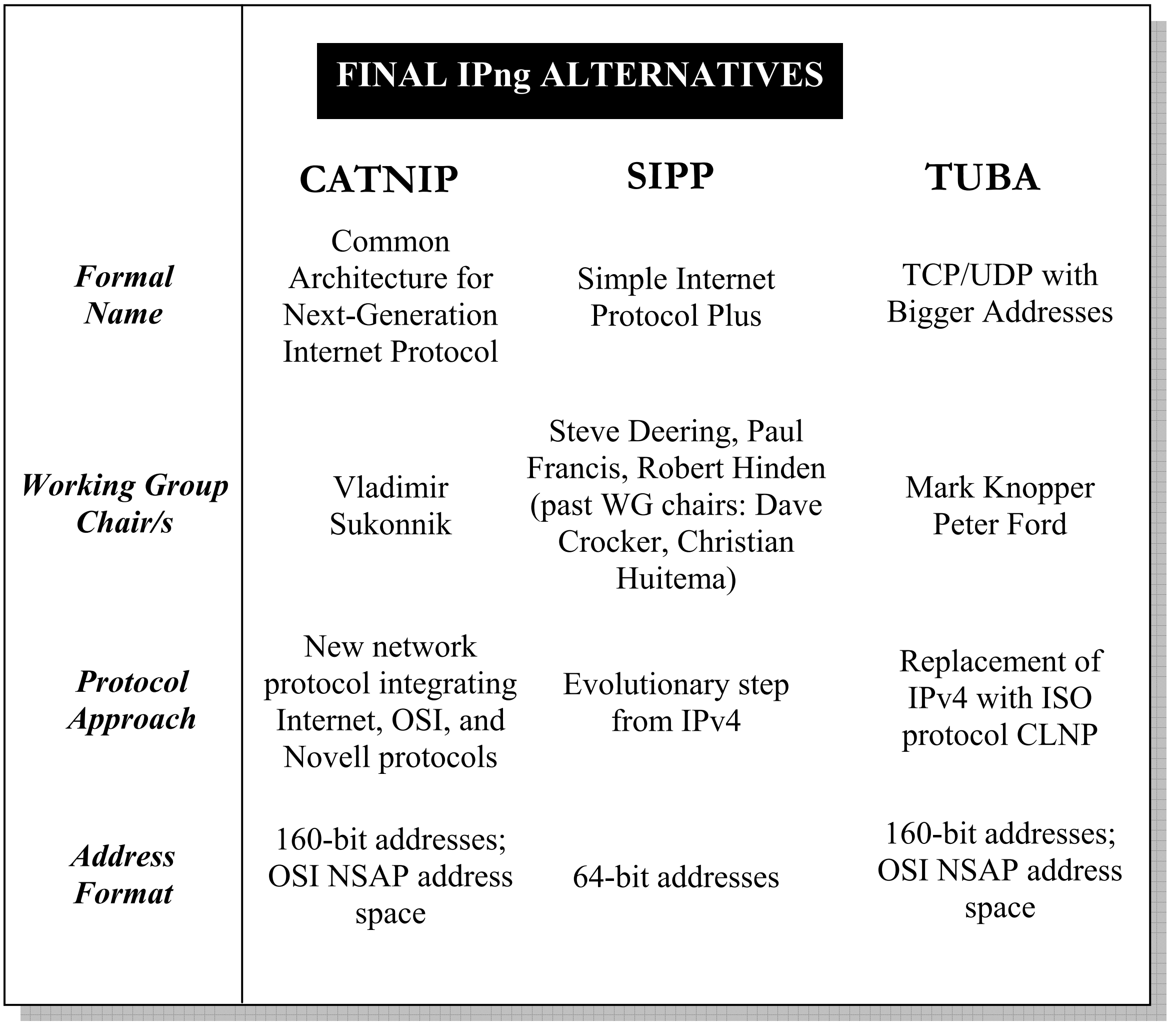
By the final IPng evaluation process, three proposals contended to become the next generation Internet Protocol: SIPP (Simple Internet Protocol Plus), CATNIP (Common Architecture for the Internet), and TUBA (TCP and UDP with Bigger Addresses). The proposed protocols shared two major functional approaches: all would provide larger address fields allowing for substantially more addresses; and all would become a universal protocol. Although the proposals had technical differences, two distinguishing characteristics were *who* was behind the development of the standard and *whether* it would preserve IP or discard it. Protocol ownership and control continued to remain a significant concern. Internet scholar Larry Lessig has said: "the architecture of cyberspace *is* power in this sense; how it is could be different. Politics is about how we decide. Politics is how that power is exercised, and by whom."[152] Abbate elaborates that "technical standards are generally assumed to be socially neutral.. but have far-reaching

[151] Scott Bradner and Allison Mankin, "IPng Area Status Report," 29th IETF Conference, Seattle, Washington, March 28, 1994.

[152] Larry Lessig, *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999, page 59.

economic and social consequences, altering the balance of power between competing businesses or nations and constraining the freedom of users."[153]

TABLE 1: FINAL IPng ALTERNATIVES



FINAL IPng ALTERNATIVES

	CATNIP	SIPP	TUBA
Formal Name	Common Architecture for Next-Generation Internet Protocol	Simple Internet Protocol Plus	TCP/UDP with Bigger Addresses
Working Group Chair/s	Vladimir Sukonnik	Steve Deering, Paul Francis, Robert Hinden (past WG chairs: Dave Crocker, Christian Huitema)	Mark Knopper Peter Ford
Protocol Approach	New network protocol integrating Internet, OSI, and Novell protocols	Evolutionary step from IPv4	Replacement of IPv4 with ISO protocol CLNP
Address Format	160-bit addresses; OSI NSAP address space	64-bit addresses	160-bit addresses; OSI NSAP address space

The SIPP proposal was a collaborative merging of previous proposals, IPAE, SIP, and PIP, and championed by longstanding IETF insiders Steve Deering of Xerox PARC and Bob Hinden of Sun Microsystems. Sun Microsystems was closely associated with TCP/IP environments and obviously had a vested interest in maintaining IP as the dominant network level protocol. SIPP was the only proposal preserving IP and part of the technical specification called for expanding the address size from 32 bits to 64 bits. CATNIP would be a completely new protocol with the objective of providing a

[153] Janet Abbate, *Inventing the Internet*. Cambridge: The MIT Press, 1999, page 179.

convergence between the Internet, ISO protocols, and Novell products. In other words, it would integrate three specific protocols: CLNP (ISO protocol), IP (Internet protocol), and IPX (Novell protocol). CATNIP would actually use the ISO developed OSI Network Service Access Point (NSAP) format for addresses. The CATNIP proposal, authored by Robert Ullman of Lotus Development Corporation and Michael McGovern of Sunspot Graphics, was explicit in its endorsement of ISO standards and its belief that convergence with ISO protocols was an essential requirement for the new protocol. The TUBA proposal was an even greater endorsement of the ISO as a standards body because it specified the ISO developed protocol, CLNP. TUBA would completely displace IP, would provide a 20-byte (160 bit) address, and, like CATNIP, would use the ISO specified NSAP address space. The IPng Directorate considered CATNIP not adequately specified and the deliberations on the Internet mailing lists indicated a binary choice between TUBA and SIPP. The decision for a new protocol was a decision between an extension of the prevailing IETF Internet Protocol (SIPP) and an ISO developed protocol.

There appeared to be a certain degree of inevitability that the selected protocol would be an extension of IPv4. The presumption that IP would triumph permeated several aspects of the selection's lexicon and process. First, an asymmetrical aspect of the selection process was the name of the future protocol – IPng, IP next generation. The nomenclature referring to the new protocol specification reflected the initial assumption that the new protocol would be an extension of the existing Internet Protocol, IP. Second, the IAB's 1991 "Towards the Future Internet Architecture" document (RFC 1287) had concluded that IP was the one defining architectural component of the Internet, with those using IP considered on the Internet and those using another network layer protocol not on the Internet. Selecting a different network layer protocol would make the Internet not the Internet. Finally, the presumption that the new protocol would be an extension and modification of IP was present, though concealed, in the evaluation criteria for IPng, as the following chronology suggests. Bradner and Mankin stated that Craig Partridge of BBN and Frank Kastenholz of FTP Software submitted the "clear and concise set of technical requirements and decision criteria for IPng"[154] in their document "Technical

[154] Scott Bradner and Allison Mankin, "The Recommendation for the IP Next Generation Protocol," RFC 1752, January, 1995, page 8.

Criteria for Choosing IP the Next Generation (IPng)." The authors explained that their derivation of criteria emanated from several sources including discussions on the Internet mailing lists, IETF meetings, and from IPng working group meetings.[155] The 1995 "Recommendation for IPng," RFC 1752, contained a lengthy summary of nineteen selection criteria Partridge and Kastenholz had defined earlier in RFC 1726.[156] Comparing their original selection criteria with those listed in the IPng Recommendation reveals an omission. The IPng Recommendation excluded the following criterion: "One Protocol to Bind Them All. One of the most important aspects of the Internet is that it provides global IP-layer connectivity. The IP layer provides the point of commonality among all nodes on the Internet. In effect, the main goal of the Internet is to provide an IP Connectivity Service to all who wish it."[157]

This requirement for global IP connectivity was the only evaluation criteria not conveyed from the definitive "Technical Criteria for Choosing IP the Next Generation" document into the explanation, in "Recommendation for IPng," for how the proposals were evaluated. Carrying forth this technical criterion would have conveyed an unmistakable SIPP predisposition. The CATNIP and TUBA alternatives obviously did not meet this IP connectivity requirement so, if retained as an evaluation criterion, a proclivity toward SIPP would have been apparent. The nineteen officially sanctioned technical evaluation criteria for the new protocol, omitting the requirement for global IP connectivity, included the following (paraphrased):

❒ Completeness: Be a complete specification.
❒ Simplicity: Exhibit architectural simplicity.
❒ Scale: Accommodate at least 10^9 networks.
❒ Topological flexibility: Support a diversity of network topologies.
❒ Performance: Enable high speed routing.
❒ Robust Service: Must provide robust service.
❒ Transition: Include a straightforward transition from IPv4.
❒ Media Independence: Operate over a range of media using a range of speeds.
❒ Datagram Service: Accommodate unreliable delivery of datagrams.
❒ Configuration Ease: Enable automatic configuration of routers and Internet hosts.
❒ Security: Provide a secure network layer.

[155] Craig Partridge and Frank Kastenholz, "Technical Criteria for Choosing IP the Next Generation (IPng)," RFC 1726, December, 1994.

[156] Ibid.

[157] Ibid.

❐ Unique names: Assign globally unique identifiers to each network device.
❐ Access to Standards: Provide freely available and distributable standards with no fees.
❐ Multicast Support: Support both unicast and multicast transmissions.
❐ Extensibility: Able to evolve to meet future Internet needs.
❐ Service Classes: Provide service according to classes assigned to packets.
❐ Mobility: Support mobile hosts and networks.
❐ Control Protocol: Include management capabilities like testing and debugging.
❐ Tunneling Support: Allow for private IP and non-IP networks to traverse network.

The overall selection process and even the specific technical evaluation criteria reflected a tension between what the participants considered evaluating the proposals technically versus evaluating proposals politically. Bradner and Mankin recognized and acknowledged the politics involved in the decision, characterizing it as pressure for convergence with the ISO versus pressure to resist ISO standards and retain protocol control within the IETF. As they described in their IPng Area Status Report at the IETF meeting in Seattle on March 28, 1994, the pressure for convergence with the ISO is something the Working Group has to understand but must "dismiss as not a technical requirement."[158]

The selection process exhibited a general asymmetry about what was considered political, with positions advocating technical convergence with the ISO standard deemed political but positions against convergence with the ISO standard (i.e. preserving IP) considered technical. The 1991 Internet architecture document had acknowledged "powerful political and market forces"[159] behind the introduction of the OSI suite and this sentiment appeared to persist years later during the IPng selection process with Bradner and Mankin considering "convergence" not a technical issue but a political issue. Additionally, many of the evaluation criteria were arguably not objective technical criterion but subjective choices. For example, the technical criteria of "simplicity" makes an aesthetic judgment that simple protocols are preferable to complex protocols. This criteria also appears somewhat contradictory to other technical criteria such as supporting a diversity of network topologies, operating over a range of media and supporting a

[158] From Scott Bradner and Allison Mankin, IPng Area Status Report given at IETF 29, Seattle, WA, March 28, 1994. (Accessed at http://www.sobco.com/ipng/presentations/ietf.3.94/report.txt on August 20, 2003).

[159] David Clark et. al, "Towards the Future Internet Architecture," RFC 1287, December, 1991, page 2.

variety of transmission speeds. The process appeared to asymmetrically define the ISO preference for protocol convergence as a political bias and define preferences that privilege a non-ISO protocol as technical criteria.

The political factor the IPng Directorate acknowledged related to control over the standard. The IETF wanted protocol ownership (i.e. change control), even if they selected the ISO-based protocol, TUBA. This issue represented an area of discord even within the TUBA Working Group, with some arguing that only the ISO should control the standard and others believing the IETF should have authority to modify the standard. This battle for control over the new standard permeated deliberations within the working groups and the IPng Directorate, was reflected in the mailing list forums, and even in draft proposals competing groups issued. For example, the proposed CATNIP alternative included the following statement: "The argument that the IETF need not (or should not) follow existing ISO standards will not hold. The ISO is the legal standards organization for the planet. Every other industry develops and follows ISO standards.. ISO convergence is both necessary and sufficient to gain international acceptance and deployment of IPng."[160]

Many expressed the opposite sentiment and the angst over the possibility of relinquishing protocol control to the ISO was especially prevalent on the big-Internet mailing list, the forum used to discuss the proposals and the site where Mankin and Bradner posed questions to the IETF standards community. For example, one IETF participant declared that "the decisions of ISO are pretty irrelavent <sic> to the real world which is dominated by IETF and proprietary protocols."[161] A significant factor in the evaluation process appeared to be whether the IETF would retain control of the protocol or whether the ISO would assume change control.

2.8 IPv6

At the opening session of the 30th meeting of the IETF in Toronto, Ontario, Canada, Bradner and Mankin presented their recommendation that SIPP, with some

[160] Michael McGovern and Robert Ullman, "CATNIP: Common Architecture for the Internet," RFC 1707, October, 1994.

[161] Donald Eastlake, posting on big-internet mailing list, September 14, 1993.

modifications, become the basis for IPng. More than 700 people attended, with the high attendance rate attributable to excitement about the protocol announcement and an increase in press representation.[162] The IANA formally assigned the version number "6" to IPng so the new protocol would be named IPv6. IPv4 was the prevailing version of IP and number 5 was already allocated to an experimental protocol. The next version number available was 6. (The nomenclature "IPv7" for the Kobe protocol had erroneously skipped over 6.)

Mankin and Bradner recounted how the IPng Directorate had identified major technical flaws in each proposal. The Directorate had dismissed CATNIP as an insufficiently developed protocol. The general technical assessment of TUBA and SIPP suggested "both SIPP and TUBA would work in the Internet context"[163] despite technical weaknesses in each approach. Yet the assessment of TUBA was also "deeply divided."[164] The Directorate identified some technical weaknesses in the CLNP protocol, the centerpiece of the TUBA proposal, but division also remained about IETF ownership of the protocol. Two of the IPng Directorate comments Mankin and Bradner cited in their presentation reflected this division: 'TUBA is good because of CLNP. If not CLNP, it is a new proposal' and 'If TUBA becomes the IPng, then the IETF must own TUBA.'

If the IETF modified CLNP, some believed this would negate the advantage of CLNP's installed base and would diminish the possibility for a meaningful convergence between ISO and IETF standards. If IETF could not modify CLNP, it would lose control of the Internet. Christian Huitema, an IAB member involved in the SIPP Working Group, later summarized his assessment of the reason TUBA was not selected, "In the end, this proposal failed because its proponents tried to remain rigidly compatible with the original CLNP specification."[165]

[162] According to the Director's Message, *Proceedings of the thirtieth IETF*, Toronto, Ontario, Canada, July 25-29, 1994.

[163] Scott Bradner and Allison Mankin, "The Recommendation for the IP Next Generation Protocol," RFC 1752, January, 1995.

[164] From the text version of the IPng presentation Scott Bradner and Allison Mankin made at the IETF meeting in Toronto on July 25, 1994. (Accessed at http://www.sobco.com/ipng/presentations/ietf.toronto/ipng.toronto.txt on September 6, 2003).

[165] Christian Huitema, *IPv6: The New Internet Protocol.* Prentice Hall, 1996, page 5.

TABLE 2: PROTOCOL SELECTION CRITERIA

Proposals Evaluated against Technical Requirements

(from RFC 1752: The Recommendation for IPng)

	CATNIP	SIPP	TUBA
Complete spec.	no	yes	mostly
Simplicity	no	no	no
Scale	yes	yes	yes
Topological flex	yes	yes	yes
Performance	mixed	mixed	mixed
Robust service	mixed	mixed	yes
Transition	mixed	no	mixed
Media indepdnt	yes	yes	yes
Datagram	yes	yes	yes
Config. ease	unknown	mixed	mixed
Security	unknown	mixed	mixed
Unique names	mixed	mixed	mixed
Access to stds	yes	yes	mixed
Multicast	unknown	yes	mixed
Extensibility	unknown	mixed	mixed
Service classes	unknown	yes	yes
Mobility	unknown	mixed	mixed
Control proto	unknown	yes	mixed
Tunneling	unknown	yes	mixed

With CATNIP and TUBA eliminated, SIPP became IPng, now renamed IPv6. Members of the IPng Directorate identified numerous technical issues with SIPP, including considerable operational problems with IPAE (the IPv4 to IPng transition mechanism), inadequate address size, and insufficient support for autoconfiguration, mobility, and security. A significant modification to SIPP was that the new SIPP-based protocol, IPv6, would have 128-bit addresses rather than 64-bit addresses. A new working group, the "IPng Working Group," would form to work on the new IPv6 specifications and resolve open or unfinished issues. Steve Deering, the primary SIPP architect, and Ross Callon, who had been a proponent of TUBA, became co-chairs of the new working group, illustrating a conciliatory attempt to unify the TUBA and SIPP bases. The IESG approved the IPv6 recommendation, which became a "proposed standard," in accordance with the IETF's conventional nomenclature, on November 17, 1994.

The most significant difference between IPv4 and IPv6 was the expansion of the Internet address length from 32 bits to 128 bits, increasing the number of available addresses from approximately 4.3 billion to 3.4×10^{38} addresses. This address length expansion represented only one technical change in the protocol. Another modification was a significant simplification of the header format.[166] Headers contain the control information preceding content transmitted over a network, analogous to the function of an envelope for mailing a letter. Header content includes information such as source address, destination address, and the length of the transmission (payload length). The IPv6 header specification eliminated some information to keep the header size as compact as possible, especially considering its larger address size. To illustrate the header simplification IPv6 provided, IPv6 addresses are four times longer than IPv4 addresses but the IPv6 header is only two times longer than the IPv4 header. Another distinction between the newly selected IPv6 protocol and IPv4 included support for autoconfiguration, an attempt to simplify the process of adding IPv6 nodes into a "plug and play" scenario whereby users could plug in a computer and have it connected via IPv6 without extensive intervention. The specification also included a format extension designed to encourage encryption use. As the IPv6 specification stated, "Support for this (security) extension will be strongly encouraged in all implementations."[167] Interestingly, these two features – autoconfiguration and support for encryption – seem somewhat contradictory because implementing encryption requires user intervention while the functional requirement of autoconfiguration sought to minimize user intervention.

Although characteristics of the IPv6 specifications were yet to be developed, the 1994 decision to proceed with a SIPP-based IPv6 concluded two years of deliberations about selecting a new protocol. The selection retained IP, though modified, as the dominant network layer protocol for the Internet and settled the issue of who would control the next generation Internet protocol. The final rejection of the OSI-based protocol, CLNP, solidified the position of the IETF as the standards body responsible for the Internet's architectural direction.

[166] Appendix B describes the IPv4 and IPv6 header formats.

[167] Scott Bradner and Allison Mankin, "The Recommendation for the IP Next Generation Protocol," RFC 1752, January, 1995, page 21.

Bradner and Mankin closed their IETF plenary presentation recommending IPv6 with the following two quotes and a concluding sentiment:

> In anything at all, perfection is finally attained not
> when there is no longer anything to add, but when
> there is no longer anything to take away.
>
> Antoine de Saint-Exupery

> Everything should be made as simple as possible, but not simpler.
>
> A. Einstein

[IETF work is trying to find the right understanding of the balance between these two goals. We think we have done that in IPng.][168]

2.9 Chapter Conclusion

The issue of protocol selection was also an issue of power selection. The next generation Internet Protocol selection was not exclusively technical but reflected an international and institutional tension between the entrenched position of the dominant Internet establishment versus later Internet entrants poised to change the balance of power and control over the Internet's architecture. Arturo Escobar suggests, "The deconstruction of planning leads us to conclude that only by problematizing these hidden practices-that is, by exposing the arbitrariness of policies, habits, and data interpretation and by suggesting other possible readings and outcomes – can the play of power be made explicit in the allegedly neutral deployment of development."[169]

Examining IPv6 against its discarded and historically overlooked alternatives demonstrated a complicated admixture of tension among dominant vendors like DEC versus newer entrants like Sun Microsystems, the Internet's grassroots rank and file establishment versus newer institutional formations like the Internet Society, trusted and familiar insiders versus newer participants, and the U.S.-centric IETF versus the ISO. The ISO alternative had the political backing of most western European governments, the

[168] From the text version of the IPng presentation Scott Bradner and Allison Mankin made at the IETF meeting in Toronto on July 25, 1994. (Accessed at http://www.sobco.com/ipng/presentations/ietf.toronto/ipng.toronto.txt on September 6, 2003).

[169] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, page 123.

United Nations, influential vendors and user organizations invested in OSI protocols, and was even congruent with United States OSI directives. The selection of IPv6, an expansion of the prevailing IPv4 protocol over such a politically sanctioned OSI alternative solidified and extended the position of the Internet's traditional standards setting establishment to control the Internet rather than relinquish standards control to a more international standards institution. The selection of IPv6 occurred outside of the realm of market economics, with the Internet's cognoscenti describing the protocol selection as too complex for markets and suggesting that corporate users, many with ample IP addresses were not even aware of the presumptive international problem of Internet address space exhaustion.

The IPv6 selection process contained an inherent contradiction. The technical community was adamant about excising sociological considerations from what they considered a purely technical protocol decision. The IAB had drawn a positivistic demarcation between the Internet as a communications system and the Internet as a community of people. Only its architectural constitution could define the Internet. Yet the outcome of the IPng selection process appeared to define the Internet, in part, as the community of *people* who would either retain or gain control of its architecture. Almost following the logical contradictions of positivism, a consideration in making architectural decisions related to the next generation Internet Protocol seems to have been the retention of the IAB, IESG, IETF institutional structure/people as controlling the Internet's direction rather than relinquishing control to a more international standards body.

Academic exegesis of the Internet often lauds its user-driven, democratized development environment and confers legitimacy to the standards setting apparatus because of this participatory approach. The Internet's democratized content and general public accessibility to the medium help fuel perceptions of the medium as an egalitarian technological system. User engagement with content and applications convey a misleading sense of control when content and applications are only the surface of a malleable technical architecture concealed to users. Many scholars view the standards setting process determining this technical architecture as a paragon of democratized technological design. For example, a belief in the Internet's participatory and open design process is the foundation of Larry Lessig primary theses. In *Code and Other Laws* *of Cyberspace* (1999) and *The Future of Ideas* (2001), Lessig describes how control over the Internet's architecture has shifted from a collaborative and democratic technical community which designed principles of personal and technical freedom into the Internet to hegemonic corporate entities formerly threatened by the Internet but now the "invisible hand, through commerce .. constructing an architecture that perfects control."[170] Dominant corporations, according to Lessig, have supplanted the collaborative and open efforts of the Internet user community, and dictate architectural directions in a manner that threatens innovation and the foundational freedoms and values of the Internet. This account of IPv6 development has suggested that Lessig bases his analysis on a romanticized assumption about the historical extent to which this participatory and democratized standards development ever was really participatory and democratic.

For example, the work of the IAB in 1990 was patently not an open process. Participation required an appointment by the IAB chair. Many IAB members were trusted colleagues familiar with each other organizationally, educationally, and through a shared history of protocol development beginning with the ARPANET. IETF working group involvement was ostensibly open in that anyone could participate, but involvement required access, often corporate affiliation and financial backing, and technical expertise in esoteric protocol matters. Additionally, the IPng Working Group solicited formal public requirements, but this process occurred after proposed alternatives were already developed and against a backdrop of a certain degree of inevitability that the IP-based SIPP alternative would become the next generation Internet Protocol. More generally, even though IETF working groups are open to public participation and an example of collective action in the technical sphere, the extent to which this work is an exemplar of democratized technological design is debatable. The esoteric knowledge and technological expertise required to participate meaningfully in the working groups create obvious inherent barriers to involvement. Similarly, many participants in the standards setting institutions worked for private corporate entities with an obvious stake in the architectural outcome of standards work. This interleaving of private industry and standards institutions in the 1980s and 1990s was, if anything, commensurate with Lessig's caveats about what he considers the new phenomenon of twenty first Century

[170] Lawrence Lessig, *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999, page 6.

corporate hegemony. Considering possible barriers of access, esoteric complexity, and financial backing, the degree of openness in standards work is not explicit and if anything, academic and public perceptions of democratized technological design actually have bolstered the legitimacy of a somewhat closed process.

CHAPTER III:
IPV6 POLITICAL ECONOMY

This chapter shifts attention from IPv6 development within the Internet's technocracy to nascent global IPv6 adoption. The IETF completed the core IPv6 specifications in 1998 and 1999.[171] Beginning in 2000, governments in China, Japan, the European Union, Korea, and India considered IPv6 a national priority and inaugurated policies to rapidly drive deployment. The United States, with a dominant Internet industry and ample addresses, remained dispassionate about IPv6 until the Department of Defense, in 2003, endorsed the protocol as a potential apparatus in the post September 11 war on terrorism. IPv6 advocates also extolled the standard as a mechanism for global democratic reform, third world development, and the eradication of poverty. Others warned that U.S. inaction on IPv6 threatened American competitiveness and jobs relative to countries like China and India with aggressive IPv6 strategies. Political theorist Yaron Ezrahi has suggested, "As a cultural enterprise, science, like religion or art, .. while differentiated from politics, can be deployed and adapted as elements of particular political worlds."[172] This chapter describes the historical progression of national IPv6 policies and IPv6 advocacy within the context of prevailing political and economic milieux, exploring possible intersections between IPv6 decisions and socioeconomic and political order and examining the repercussions of upgrading, or not upgrading, to IPv6.

3.1 The Lost Decade and the E-Japan Strategy

In 2000, the new Japanese Prime Minister, Yoshiro Mori, introduced an "e-Japan Program" establishing a 2005 deadline for upgrading every Japanese business and public sector computing device to IPv6. Mori had commissioned his administration the "Cabinet for the Rebirth of Japan,"[173] prioritizing economic recovery in the wake of long

[171] For the formal IPv6 draft standard document, see Steven Deering and Robert Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December, 1998.

[172] Yaron Ezrahi, *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*. Cambridge: Harvard University Press, 1990, page 1.

[173] Yoshiro Mori, "Policy Speech by Prime Minister Yoshiro Mori the 147th Session of the Diet," April 7, 2000, (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2000/0407policy.html on April 16, 2003).

term stagnation often designated “Japan’s lost decade.”[174] Rising stock and land prices had dominated the late 1980s, with capital gains on these assets exceeding Japan’s Gross Domestic Product (GDP) by 40%.[175] The government sought to contain speculative investment through a series of interest rate increases and real estate lending ceilings, resulting eventually in real estate and stock market declines including a 61% drop in the Nikkei 225 average between January, 1990, and January, 1999.[176] Although the Japanese economy had begun to rebound[177] when Prime Minister Mori assumed office, Japan had recently weathered a decade-long recession characterized by economic stagnation and high unemployment. The Japanese people were also anticipating the advent of the new millennium, which they celebrated on January 1, 2001. In contrast to Japan’s arduous economic circumstances throughout the 1990s, the Prime Minister believed the Internet had created positive structural changes in other countries, had engendered productivity improvements, and had inaugurated entirely new industries, especially in the United States.

Within this context, the Prime Minister delivered his first Session of the Diet, a constitutionally mandated address to elected representatives in Japan’s legislative parliament.[178] Mori selected the promotion of science and technology as his administration’s policy cornerstone and envisioned “economic development that capitalizes on the explosive force of the IT Revolution.”[179] The Prime Minister introduced a structural program for the “Rebirth of Japan” containing five pillars: the rebirth of the economy, the rebirth of social security, the rebirth of education, the rebirth

[174] Yoshiro Mori, “Shaping Japan, Shaping a Global Future – A Special Message from Yoshiro Mori,” (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2001/0127davos_e.html on April 16, 2003).

[175] *The Economist Intelligence Unit*, “Country Profile Japan 2000-Economic Performance,” March 14, 2000.

[176] The Nikkei index closed at 37,189 on January 31, 1990, and closed at 14,499.25 on January 29, 1999, a decline of 61%.

[177] Robert M. Uriu, “Japan in 1999: Ending the Century on an Uncertain Note,” *A Survey of Asia in 1999* Vol. 40, No. 1, January-February, 2000, page 143.

[178] *The Constitution of Japan*, Article 52, November 3, 1946.

[179] “Policy Speech by Prime Minister Yoshiro Mori the 147th Session of the Diet,” April 7, 2000. (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2000/0407policy.html on April 15, 2003).

of government, and the rebirth of foreign policy.[180] The Prime Minister suggested that economic resurgence was a foremost priority and believed information technology represented a critical ingredient in reaching all his pillar priorities. Information technology would represent the "major key to ensuring the prosperity of Japan in the 21st Century."[181] Mori announced the establishment of an Office of Information Technology within the Cabinet Secretariat and established a deadline of five years within which Japan would become a leader in information and communications technologies.[182]

Mori also established an IT Strategy Headquarters within the Japanese cabinet, tasked with transforming Japan into a global information technology leader and comprising senior administration officials including the Minister of Justice, the Minister of Finance, and the Minister of Foreign Affairs.[183] The Cabinet directive establishing the IT Strategy headquarters also installed an "IT Strategy Council" of industry and academic experts to serve in an advisory capacity. The majority of Strategy Council members represented large Japanese technology corporations. Nobuyuki Idei, Chairman and CEO of Sony Corporation, chaired the Council, which also included presidents and CEOs from major Japanese corporations such as NEC Corporation, Fujitsu Research Institute, Nippon Telegraph and Telephone (NTT) Corporation, and professors from several of Japan's universities.[184]

The IT Strategy Council and its corporate membership would play a central role in establishing Japan's technical policy directions. Four months after its inception, the

[180] Yoshiro Mori, "Policy Speech by Prime Minister Yoshiro to the 149th Session of the Diet," July 28, 2000. (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2000/0728policy.html on April 15, 2003).

[181] Yoshiro Mori, "Statement by Prime Minister Yoshiro Mori at the Eleventh Joint Meeting of the Advanced Information and Telecommunications Society Promotion Headquarters and Their Advisory Council." May 19, 2000. (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2000/0519statement-it-html on April 15, 2003).

[182] Yoshiro Mori, "Policy Speech by Prime Minister Yoshiro to the 149th Session of the Diet," July 28, 2000. (Accessed at http://www.kantei.go.jp/foreign/souri/mori/2000/0728policy.html on April 15, 2003).

[183] Japanese Cabinet Directive, "Establishment of the IT Strategy Headquarters," July 7, 2000. (Accessed at http://www.kantei.go.jp/foreign/it/council/establishment_it.html on April 17, 2003).

[184] The complete member list of Japan's IT Strategy Council is included in the Japanese Government's IT Strategy Council announcement. (Accessed at http://www.kantei.go/jp/foreign/it/council/council_it.html on April 15, 2003).

Council published its basic IT strategy recommendations for Japan. The Council's strategy contained some blanket assumptions about the significance of information technology in society, the position of Japan in the world IT market, and the causes of Japan's shortcomings. The Council asserted that a worldwide IT revolution was "beginning to bring about a historic transformation of society, much like the Industrial Revolution did from the 18th century in the United Kingdom" but that Japan's "backwardness" was precluding Japan from embracing this revolution.[185] By backwardness, the Council suggested Japan trailed the United States, Europe, and other Asia-Pacific countries in information technology usage in business and government and that this sluggishness might create an irreparable competitive disadvantage. The Council's causative attribution of this backwardness ignored Japan's decade-long economic stagnation, the historical circumstances of Internet technologies emanating originally from the United States, or cultural conditions within Japan. Instead, the Council attributed Japan's competitive disadvantage to a single circumstance. Excessive government regulations, telecommunications fees, and restrictions on the technology industry were responsible for Japan's predicament. The solution to Japan's economic indolence in information technology was the implementation of institutional reforms enabling "free and fair competition."[186] The first of four policy priorities the Council recommended was the promotion of a high-speed[187] network infrastructure accompanied by a shift from regulations-oriented to competition-promoting government attitudes toward the telecommunications industry. As part of achieving its top priority of a high-speed network infrastructure and accompanying policies, the Council recommended the IPv6 standard. IPv6 was the only standard or technology mentioned by name in the recommendations and the Council cited the need for more Internet addresses, enhanced security, and requirements to connect wireless devices and home appliances to the

[185] Japan IT Strategy Council, "Basic IT Strategy," November 27, 2000, (Accessed at http://www.kantei.go.jp/foreign/it/council/basic_it.html on April 15, 2003).

[186] Ibid.

[187] The Japanese IT Strategy Council's definition of high-speed in 2000 was 30-100 Mbps (Megabits per second).

Internet as justifications for implementing IPv6.[188] The IT Strategy Council's recommendations were contradictory in that they denounced competition-stifling governmental dictates as the causative factor in economic stagnation but, conversely, recommended a governmental dictate for industry-wide adoption of a single technology, IPv6.

The decision distinguishing IPv6 as a specific technological direction for Japan directly corresponded with technical strategies of the corporations represented on the IT Strategy Council. Some of the Council's participants manufactured consumer electronic devices, lucrative gaming products, or home appliances, and were pursuing a strategy of network-enabling these products through embedding IPv6 addresses. These manufacturers, by 2000, had adopted strategies of producing nothing without an embedded network interface. For example, Sony Corporation envisioned a "broadband network society" in which unique IPv6 addresses would be assigned to every television, computing device, telephone, appliance, and gaming product, including its profitable Playstation 2.[189]

Japan's IT Strategy Council also included representatives of network service providers and network equipment vendors, corporations with their own IPv6 strategies. In 2000, Japan's market leaders in networking products and services introduced a flurry of new IPv6 product and service offerings. Japanese network service provider, NTT Communications, had already announced the availability of its first IPv6 based Internet service and had trial customers.[190] Nokia announced the availability of an IPv6 service as part of its GPRS (General Packet Radio Service) network. Nokia's rationale for introducing IPv6 services included what it considered constraints on available IPv4 addresses and perceptions of greater security and quality of service in IPv6.[191] Another major IPv6 product announcement was Hitachi's expansion of IPv6 support to its entire

[188] Japan IT Strategy Council, "Basic IT Strategy," November 27, 2000. (Accessed at http://www.kantei.go.jp/foreign/it/council/basic_it.html on April 15, 2003).

[189] Sony Annual Report 2001, Year Ended March 31, 2001.

[190] NTT Press Release, "NTT Multimedia Communications Laboratories Announces First Commercially Available IPv6 IX," March 13, 2000.

[191] Nokia Press Release, "Nokia announces the world's first IPv6 enabled GPRS network," November 21, 2000.

line of Gigabit speed routers, the GR2000 product family.[192] Hitachi had already included some IPv6 support in its router products dating back to 1997 and believed IPv4 addresses would be depleted by the year 2001.[193] Japan's NEC and Fujitsu similarly offered new router products incorporating IPv6. In the preceding year, U.S. based router manufacturer, Cisco Systems, dominated the router market with an estimated 77% market share.[194] Nortel Networks and 3Com were the number two and three router vendors, with roughly 8% and 3% of the worldwide router market. Japanese router vendors, whose market share barely registered relative to these other equipment suppliers, were seeking ways to competitively differentiate, or at least competitively maintain, their product lines and considered IPv6 support one possibility.

Many Japanese corporations associated with the IT Strategy Council also had a history of IPv6 development and testing through participation in WIDE Project, a Japanese Internet research consortium. WIDE Project, short for Widely Integrated Distributed Environment, formed an IPv6 Working Group in 1995 to address the prospect of IP address space exhaustion and examine the possibility of transitioning to the new protocol. In 1996, WIDE's IPv6 testbed, 6Bone, forwarded its first IPv6 packets. This experimentation preceded the IETF's formalization of the core IPv6 specifications. In 1998, WIDE Project members launched KAME Project, a research effort designed to combine numerous IPv6 software implementations into a single IPv6 software stack integrated into the BSD operating system.[195] In other words, project members worked to develop free IPv6 software code for variants of BSD. Participants in KAME, (the Japanese word for "turtle") funded their involvement, and most of the core project researchers worked for Japanese technology companies including Fujitsu, Hitachi, Toshiba, Internet Initiative Japan, and NET Corporation.[196] The corporate members of the IT Strategy Council establishing Japan's IT policies were already involved in IPv6

[192] Hitachi News Release, "Hitachi GR2000 Router Supports IPv6," November 29, 2000.

[193] Ibid.

[194] According to *InternetWeek's* By the Numbers Archive, "Worldwide Router Market Share," citing Dataquest statistics, June 23, 1999.

[195] Jun-ichiro itojun Hagino, "Implementing IPv6: Experiences at KAME Project," *Applications and the Internet Workshop*, Symposium Proceedings, January, 2003, page 218.

[196] From KAME Project overview. (Accessed at http://www.kame.net on November 4, 2005).

development, had expressed concern about possible IPv4 addresses shortages, and had an economic stake in IPv6 through the prospect of becoming more competitive with dominant Internet vendors and service providers.

Two months prior to the Council's official publication of Japan's IT strategy, the Prime Minister delivered a policy speech in which he discussed social issues like educational reform, social security, and foreign policy, but first addressed a topic he called "The IT Revolution as a National Movement."[197] Reflecting the Council's strategic recommendations, IPv6 was the only specific technology the Prime Minister mentioned in his address to Japan's joint legislative body. The Prime Minister promised, "We shall also aim to provide a telling international contribution to the development of the Internet through research and development of state-of-the-art Internet technologies and active participation in resolving global Internet issues in such areas as IP version 6."[198] The mention of such an esoteric network protocol standard by a Prime Minister seemed anomalous, as was his rhetorical grouping of IPv6 with such issues as foreign policy and educational reform.

Following the Prime Minister's mandate for Japan to pursue IPv6 as part of a national strategy, the IT Strategy Headquarters formally issued its *e-Japan Strategy* (January, 2001). The *e-Japan Strategy* reiterated verbatim the IT Strategy Council's recommendations with the addition of specified deadlines for achieving priorities. The e-Japan Strategy's overall objective was to elevate Japan to a global IT leader within five years. Achieving this objective would require Japan transitioning to an IPv6 Internet environment by 2005.[199] The government's comprehensive mandate included myriad strategies to drive adoption: spending 8 billion Yen on IPv6 research and development in 2001, offering tax incentive programs to IPv6 developers and providers, and instituting

[197] Yoshiro Mori, "Policy Speech by Prime Minister Yoshiro Mori to the 150th Session of the Diet," September 21, 2000. (Accessed at http://www.kantei.go.jp/foreign/sourimori/2000/0921policy.html on November 11, 2002).

[198] Ibid.

[199] Specified in the e-Japan Priority Policy program, Policy 2, March 20, 2001. (Accessed at http://www.kantei.go.jp/foreign/it/network/priority/slike4.html on April 15, 2003).

educational campaigns to encourage migration.[200] The Japanese government also launched an IPv6 advocacy group called the IPv6 Promotion Council of Japan.

The e-Japan strategy and especially the Prime Minister's personal endorsement of IPv6 raised awareness of IPv6 among the Japanese people, but not everyone agreed that a top-down mandate to drive IPv6 adoption was prudent or necessary. Nobuo Ikeda, a senior fellow at the Research Institute of Economy, Trade, and Industry (REITI) and Professor Hajime Yamada issued a technical bulletin challenging many of the Japanese government's assumptions about IPv6.[201] They challenged the notion that IPv4 addresses were critically scarce and disputed the e-Japan program's assertion that IPv6 provided novel functionality such as improved security or privacy. For example, they noted the IP security standard, IPsec, could be used with either IPv4 or IPv6, although it was often cited as a reason for upgrading to IPv6. Ikeda and Yamada especially challenged the merits of Japanese government mandates versus a public, national debate, suggesting that "debate on these fundamental issues concerning IPv6 has been neglected in Japan, and instead the nationalistic argument that the U.S. enjoyed an exclusive victory with IPv4, so Japan should strike back with IPv6 is being raised."[202] The authors suggested the top-down mandate from the Japanese government reversed the historical trajectory under which the Internet had progressed and also raised the question of whether the rest of the world would even transition to IPv6.

3.2 European Union IPv6 Mandates

Contemporaneous to Japan's sweeping mandate, the European Union announced a pan-European IPv6 upgrade. This emphasis on homogenization of technology standards accompanied the integration of monetary standards under the Euro, and reflected general European unification objectives. In March, 2000, European Union leaders convened in Lisbon, Portugal, to formally inaugurate a litany of national and pan-European reforms.

[200] According to the presentation by the Co-Chair of the IPv6 Promotion Council of Japan and board member of the IPv6 Forum, Takashi Arano, at the Shangai ICANN meeting, October 28, 2002.

[201] Nobuo Ikeda and Hajime Yamada, "Is IPv6 Necessary?" Technology Bulletin: Series #2, *GLOCOM Platform from Japan*, February 27, 2002

[202] Ibid.

This meeting of the European Council in Lisbon established a sweeping objective for the European Union to overtake U.S. IT market dominance and "become the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion."[203] The Council cited concerns about Europe's unemployment rate and identified telecommunications and the Internet as an underdeveloped sector poised to strengthen the region economically. The Council posited that increased understanding and diffusion of Internet technologies would increase European employment rates and enable the E.U. to "catch up with its competitors" in these areas.[204] One outcome of the Lisbon summit was a call for an "eEurope Action Plan."

The European Council and the Commission of the European Communities later issued a 2000 eEurope Action Plan identifying areas in which cross-European action might advance the Lisbon objectives of developing a "new" network-enabled knowledge-based economic structure capable of improving European global competitiveness. "Rapid deployment and use of IPv6"[205] ranked among specific action items for achieving this vision.

The E.U.'s 2000 IPv6 announcement cited "the need for vastly increased Internet IP addresses"[206] as a justification for a comprehensive IPv6 conversion. An unquestioned assumption asserted that the IPv4 address space would become "critically scarce by 2005."[207] A significant consideration in the European Union's decision to advance IPv6 included the planned deployment of Third Generation (3G) wireless networking, itself a

[203] Lisbon European Council, *Presidency Conclusions*, March 23-24, 2000. (Accessed at http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm on November 11, 2002).

[204] Ibid.

[205] eEurope Action Plan prepared by the Council of the European Union and the European Commission for the Feira European Council, Brussels, Belgium, June 14, 2000, page 6. (Accessed at http://europa.eu.int/information_society/eeurope_en.pdf on November 11, 2002).

[206] Ibid.

[207] Commission of the European Communities, Communication from the Commission to the Council and the European Parliament, "Next Generation Internet-Priorities for Action in Migrating to the new Internet Protocol IPv6," Brussels, Belgium, February 21, 2002. (Accessed at http://www.ec.ipv6tf.org/PublicDocuments/com2002_0096en01.pdf on November 20, 2002).

technology standardization effort enmeshed in a complex array of economic and political circumstances. At the onset of the 21st century, more than 60% of Europeans used mobile telephones primarily through GSM (Global System for Mobile Telecommunications) service subscriptions, also called 2G, or second generation wireless.[208] GSM service offered a digital upgrade from what would retrospectively be called "first generation" analog mobile technology. The European Union, trailing the U.S. in Internet software and hardware markets, recognized the anticipated convergence between Internet applications and mobile telephony and believed it could leverage its mobile phone diffusion and expertise to globally dominate markets for high-speed mobile Internet services. Consequently, the E.U. decided to adopt the ITU's recommended family of high-speed, digital, wireless standards known as 3G. The European Parliament established legislation dictating how member states would grant licenses for the 3G frequency spectrum.[209] By March of 2001, purchases of 3G licenses, primarily through spectrum auctions, amounted to more than 130 billion Euros.[210] Telecommunications operators intending to eventually sell 3G services incurred these spectrum costs, which excluded the enormous expenditures of deploying completely new wireless communications infrastructures. The auctions only sold rights to the invisible resource of airwaves. Telecommunications operators raised massive capital through financial markets and debt instruments to acquire spectrum. The European Commission recognized the great risks inherent in massive radio spectrum expenditures, including delays in availability of 3G handsets, without which 3G services would be useless, and

[208] Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward," Brussels, Belgium, March 20, 2001, page 4. (Accessed at http://europa.eu.int/ISPO/infosoc/telecompolicy/en/com2001-141en.pdf on November 20, 2002).

[209] Directive No 13/1997/EC of the European Parliament and of the Council, April 10, 1997. (Accessed at http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52001DC0141:EN:HTML on November 21, 2002).

[210] Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward," Brussels, Belgium, March 20, 2001, page 6. (Accessed at http://europa.eu.int/ISPO/infosoc/telecompolicy/en/com2001-141en.pdf on November 20, 2002).

delays in 3G network equipment components.[211] The European Commission also linked the estimated success of 3G systems to another invisible resource, IP addresses. Providing Internet connectivity via a 3G wireless platform would require an IP address, which the European Union considered in scarce supply. A 2001 European Commission Report on the introduction of 3G mobile communications warned:

> *"The current implementation of the Internet Protocol (version 4, IPv4) is considered to limit the full deployment of 3G services in the long run. The proposed new IP version (IPv6) would overcome this addressing shortage and enable additional features, such as guaranteed quality of service and security…Any delay in the transition to all-IPv6 networks, which will require several years of effort, risks hindering the deployment of these advanced 3G service features at a later state."*[212]

European Commission policies linked IPv6 expertise and deployment with economic opportunities in 3G services and emerging Internet technologies, with achieving its objective of the European Union becoming a competitive knowledge-based economy, and with reducing unemployment.

In 2002, both European and Asian leaders, sometimes working in consort, elevated the need for IPv6 with such issues as weapons of mass destruction disarmament and eradicating poverty. The 2002 annual Japan-European Union Summit, held in Tokyo, addressed a number of joint political objectives. The first objective addressed promotion of peace and security, including weapons disarmament and reconstruction assistance to Afghanistan. The second objective addressed broad prescriptions about fighting poverty, strengthening the international monetary system, and regulatory reform, but also contained one esoteric prescription: a call for "Expert meetings on the fourth <sic> generation mobile telecommunications system and IPv6."[213] The joint statement emanated from the Prime Minister of Japan and the Prime Minister of Denmark in his

[211] Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward," Brussels, Belgium, March 20, 2001, page 6. (Accessed at http://europa.eu.int/ISPO/infosoc/telecompolicy/en/com2001-141en.pdf on November 20, 2002).

[212] Ibid, page 8.

[213] 11th Summit between Japan and the European Union. Joint Press Statement of Junichiro Koizumi, Prime Minister of Japan, Anders Fogh Rasmussen, Prime Minister of Denmark, and Romano Prodi, President of the European Commission, Tokyo, Japan, July 8, 2002.

capacity as President of the European Council, yet another example of European leaders singling out IPv6 over numerous other technologies and aligning expectations of IPv6 with specific political objectives.

3.3 IPv6 Momentum in Asia

The Korean government similarly announced an objective of rapidly developing IPv6 networks and products in February of 2001, when Korea's Ministry of Information and Communication issued a strategic blueprint termed the IT839 Strategy. Between 2000 and 2001, information technology exports, particularly semiconductor products, experienced a precipitous decline of 21%.[214] Emphasizing that information technology products comprised 30% of Korean exports, the IT Strategy's objective was to "open the era of $20,000 GDP per capita."[215] The nomenclature 8-3-9 indicated that Korea would promote eight new services (e.g. radio frequency identification sensor technologies), three infrastructures, and nine new growth engines (e.g. next generation mobile communications). Korea's strategy cited the economic potential of serving emerging technology markets like wireless broadband and Internet telephony (VoIP) and itemized three necessary infrastructural developments to achieve its goals: broadband convergence networks providing high-speed multimedia access, ubiquitous sensor networks to improve the management and distribution of food and products, and IPv6.

The Korean strategy embraced the assumption that IPv4 addresses would become depleted by 2006 but emphasized the overall objective of becoming "an Internet powerhouse by promoting IPv6."[216] The Ministry of Information and Communication initially committed $150 million dollars for pilot projects and funding of Korean manufactured routers supporting IPv6. The Ministry also established an IPv6 Strategic Council to promote collaboration between industry, government, academics, and research institutions. The Korean government expected significant returns on its IPv6 investment:

[214] From the statistics of Korea's Ministry of Information and Communication. (Accessed at http://eng.mic.go.kr on January 29, 2006).

[215] Ministry of Information and Communication, Republic of Korea, "The Road to $20,000 GDP/capita, IT839 Strategy." (Accessed at www.mic.go.kr on January 28, 2006).

[216] Ibid.

"The successful promotion of IPv6 will create 8.6 trillion *won* in production and 53,000 new jobs." Considering that IPv6 was a networking standard for routing and addressing and not an actual application sold to end users, South Korea expected it would sell IPv6 equipment. Relative to the worldwide router market in 2001, the estimate of selling 8.6 trillion *won* (approximately 8 billion dollars) worth of IPv6 products appeared extremely optimistic.

Japan, the European Union, and Korea were frontrunners in the early promotion of IPv6 products, services, and adoption. India and China, the two countries with the largest potential Internet services user markets, later issued similar sweeping mandates. In 2004, India's Minister of Communications and Information Technology included the goal of national migration to IPv6 by 2006 in his "Ten Point Agenda" for promoting economic development in information technology in India.[217] The Indian government established 2006 as the target for all of India's Internet Service Providers (ISPs) to upgrade to IPv6. China began testing IPv6 in 1998 by developing the China Education and Research Network (CERNET) IPv6 testbed. Established with federal government funding and Chinese Ministry of Education oversight, CERNET would eventually interconnect twenty five universities in twenty cities.[218] In 2002, China entered into a joint initiative with Japan to undertake an IPv6 testbed called the sino-Japan IPv6 trial network, IPv6-CJ. Also in 2002, the Chinese government established a "National 863 Program, Comprehensive Experimental Environment for New Generation Internet Technology" and an objective of the Chinese IPv6 strategy was to earmark significant funding to support domestic router development.[219] The government sought to encourage China's router manufacturers to develop IPv6 enabled routers for use in domestic networks and to potentially gain market share in the global router market dominated by American router manufacturers such as Cisco Systems and Juniper Networks. In 2003,

[217] Thiru Dayanidhi Maran, "Ten Point Agenda Declared by Hon'ble Minister of Communications and Information Technology," May 26, 2004. (Accessed at http://www.dotindia.com on June 12, 2005).

[218] Chinese Ministry of Education, "Chronicle of CERNET, 1999-2003." (Accessed at http://www.edu.cn/20041125/3122220.shtml on December 20, 2005).

[219] Hua Ning, Chief Engineer, Beijing Internet Institute, "IPv6 Test-bed Networks and R&D in China," *Proceedings of the 2004 International Symposium on Applications and the Internet Workshops*, IEEE Computer Society, 2004.

China formally announced its national IPv6 strategy to develop a nationwide IPv6 backbone, the China Next Generation Internet (CNGI).[220] All five of China's national service providers – China Telecom, Unicom, Netcom, China Mobile, and China Railcom, along with CERNET, would participate in the national CNGI IPv6 network.

3.4 Network Society Assumptions

The IPv6 strategies of Asian and European Union governments shared several commonalities. First, IPv6 mandates emanated directly from national government leaders: the Japanese Prime Minister, Korea's Ministry of Information and Communication, India's Ministry of Communications and Information Technology, the Chinese government, and the European Commission. These governments chose to mandate IPv6, rejecting the possibility of allowing free markets to embrace IPv6 products and services. Additionally, each IPv6 promotion strategy consistently cited a twofold rationale: a recognition that each country faced a potential exhaustion of the limited resources of IPv4 addresses and an objective of becoming more economically competitive in information technology markets relative to the United States, either directly through IPv6 products, services, and expertise, or through services enabled by more addresses. Additionally, governments backed national IPv6 directives with funding, tax incentives, and other direct economic inducements for service providers and equipment manufacturers. This direct governmental intervention in specific standards adoption and sweeping mandates again countervailed the IETF's philosophy of working code percolating up through grassroots adoption rather than authoritative decrees. Recall that the IETF philosophy had espoused, "Top down mandates are useless."[221]

The IPv6 policy discussions also espoused a conceptual belief in an "information society" or "network society" structured upon global information networks and unprecedented economic opportunities for productivity improvements and job creation. National policies touted an information society predicated upon availability and control

[220] Jie An and Jianping Wu, of CERNET/Tsinghua University, "CNGI and CERNET2 Updates," November 2, 2005. (Accessed at http://cans2005.cstnet.cn/down/1102/A/morning/200501101- wjp-aj-CERNET2_1A.pdf on December 20, 2005).

[221] Quote from Dave Clark, MIT, documented in David D. Clark et al., "Towards the Future Internet Architecture," RFC 1287, December, 1991.

of IP resources and sufficient IPv6 expertise and products, as a requirement for international economic competitiveness. The information society represented something new, something unquestioned, and a necessary prerequisite for global economic advancement. Japan, through its e-Japan strategy, sought to contribute to a global, advanced information society. Europe's Lisbon objective called for Europe to become "the most competitive and dynamic knowledge-based economy in the world,"[222] and policy makers developed expectations of IPv6 as a mechanism for achieving this objective. As promised in the strategies related to IPv6 as an enabler of national and international information networks, IPv6 would enable a new societal order affecting economic structures, labor composition, food distribution, and other social concerns like weapons disarmament and poverty.

These expectations resembled the theoretical musings of sociologist Manuel Castells, who claims the Internet created a social structure called the "network society" which, in turn, inaugurated a new economic order. Castell's somewhat technologically deterministic theories argue, "Core economic, social, political, and cultural activities throughout the planet are being structured by and around the Internet…"[223] Castells identifies a "new economy" enabled by the Internet's unprecedented capacity for productivity growth. Reminiscent of themes from Alfred Chandler's *The Visible Hand: The Managerial Revolution in American Business* (1977), he believes the driving force of rational change is the quest for efficiency, whether reducing costs, gaining economies of scale, or improving productivity. As Castells summarizes, "If, as I shall argue, the new economy is based on unprecedented potential for productivity growth as a result of the uses of the Internet by all kinds of business in all kinds of operations, then we are entering, probably, a new business world."[224] The European and Asian governments' IPv6 preferments exalted the standard as a lever for productivity improvements and global competitiveness, an extrapolation of Castells' contention that "The proper uses of the Internet have become a key source of productivity and competitiveness for all kinds

[222] Lisbon European Council, "Presidency Conclusions," March 23-24, 2000. (Accessed at http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm.on May 3, 2003).

[223] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2001, page 3.

[224] Ibid, page 5.

of business."[225] Commensurate with IPv6 expectations, Castells emphasizes labor, job creation, and expertise as the basis of competitiveness, innovation, and productivity.

Nicholas Garnham of the University of Westminster has criticized this information society construct, particularly the European formulation, and has correspondingly impugned Castells' network society theory. Garnham argues that policy strategy using the information society concept can only be understood ideologically:

> *"information or knowledge society .. the term has become largely meaningless and the vision bears very little, if any relation, to any concretely graspable reality. It therefore operates not as a useful concept for theoretical analysis but as an ideology. Rather than serving to enhance our understanding of the world in which we live, it is used to elicit uncritical assent to whatever dubious proposition is being put forward beneath its protective umbrella."* [226]

Following Garnham, governmental policies espousing IPv6 as a precursor to information society ascent presented an unquestioned worldview leaving scant room for critical examination. Furthermore, IPv6 mandates as a precursor to achieving an information society economy competitive with the United States appeared to achieve political purposes: a sense of the Japanese government 'doing something' in the wake of economic stagnation or the European Union outwardly reflecting political unification objectives and globalization concerns through standardized monetary and technological infrastructure. Garnham underscores the dramatic shift in European Union policy from: 1) a model promoting free market competition, liberalization of regulatory structures, and neutrality on specific technologies; to 2) a model of rigid state intervention legislating specific technologies through mandates, tax relief, and funding. [227] Correspondingly, state IPv6 interventions bypassed the possibility of free market IPv6 development and instead adopted government intervention, mandates, and subsidization. Garnham believes information society assumptions mask the failed EU information technology

[225] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2001, page 64.

[226] Nicholas Garnham, "Information Society As Theory or Ideology: A Critical Perspective on Technology, Education, and Employment in the Information Age," *Information, Communication, and Society* 3:2 2000, page 140.

[227] Nicholas Garnham, "Contradiction, Confusion and Hubris: A Critical Review of European Information Society," *European Network for Communication and Information Perspectives*. (Accessed at htt://www.encip.org/garnham_2.php on July 30, 2005).

policies of the recent past and the enormous expenditures associated with them. Garnham is not advocating "letting the market rip" versus state intervention but is calling for critical examination of the relationship between a global capitalist economy and information and communication technologies rather than blindly subscribing to unexamined assumptions.

3.5 A Taciturn United States

While the Prime Minister of Japan touted IPv6 as part of a national economic strategy in 2000, few U.S. institutions appeared interested in immediate IPv6 adoption. The U.S. already enjoyed a hegemonic IT industry and had recently weathered the Y2K transition. The market capitalizations of Internet companies, "dot-coms," and network equipment manufacturers like Cisco and Lucent reached record valuations. Venture capital poured into companies poised to profit from web growth and Internet infrastructure expansion. The Nasdaq composite index soared more than 400% between 1994 and 2000.

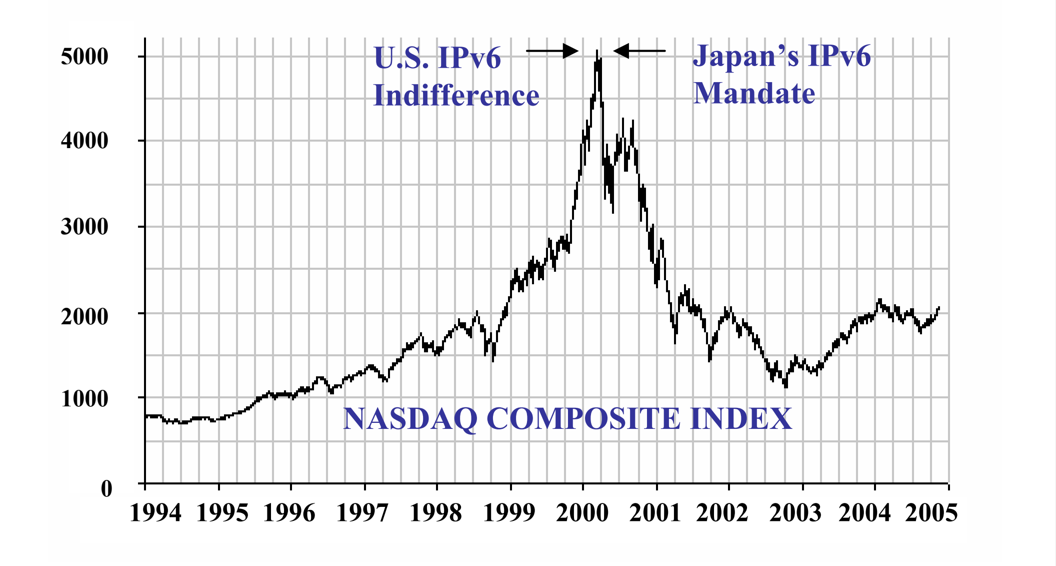


Figure 1: IPv6 Interest Relative to NASDAQ Composite Index

New companies such as Amazon, eBay, Google, and Yahoo! helped solidify America's dominance in Internet applications. In this context of entrepreneurship, stock market growth, and associated affluence, the prospect of the U.S. government promoting a potentially disruptive software upgrade seemed implausible.

U.S. corporate Internet users similarly had little incentive to immediately adopt IPv6 because they generally possessed ample IP addresses and an installed base of IPv4 compliant applications, network devices, and IPv4 expertise and administrative capital. Those who did face address shortages had the option of implementing Network Address Translation (NAT).[228] Transitioning to IPv6 would require significant software updates and address reconfiguration and necessitate new training and technical skills. The need to concurrently support both IPv4 and IPv6, expected to coexist, presented a greater impediment to businesses implementing IPv6. Institutions wanting to support coexisting IPv4/IPv6 protocols faced three alternatives: dual stack, tunneling, and translation.

The dual stack options involved installing separate suites of IPv4 and IPv6 software on routers and hosts. Applications could employ either IPv4 or IPv6 based on IP address or a preprogrammed preference. An alternative technique, tunneling, would encapsulate packets of IPv6 information within IPv4 packets for transmission over an IPv4 network or, inversely, encapsulate IPv4 packets within IPv6 packets before traversing an IPv6 network. The third approach, translation, enabled devices only supporting IPv4 to communicate with devices only supporting IPv6 by translating IPv4 packets entirely into IPv6 packets or vice versa. Each approach would present challenges, require administrative and processing resources, and possibly complicate network security. The process of translation would also affect network performance because of the additional step of translating packets between the two protocol formats.

With such disincentives and ample addresses, U.S. businesses and the federal government were not significant IPv6 drivers relative to European and Asian policies in 2000. International IPv6 advocates expressed frustration about relative U.S. indifference. Latif Ladid, a visible European IPv6 advocate and President and founder of an advocacy group called the IPv6 Forum, criticized perceived U.S. inaction:

> *"As soon as IPv6 picks up in Europe, the U.S. will not want to miss the opportunity and will catch up. But it is an unusual situation for a country*

[228] Network Address Translation (NAT) allows a network device, such as a router, to employ limited public IP addresses to mediate between a private network with many unregistered (fabricated) IP addresses and the public Internet. Chapter IV addresses this in greater detail.

> *that takes leadership in practically anything; the U.S. seems to not be ready for it."* [229]

Advocates such as Ladid focused efforts on IPv6 evangelism to the North American Internet community. For example, the IPv6 Technology Deployment summit held in conjunction with INET 2002 in Washington D.C. was partially intended "to alert the North American technology, business and political community about the importance of America's role in making worldwide deployment of IPv6 a reality."[230]

3.6 IPv6, U.S. Cybersecurity, and Distributed Warfare

One of the first U.S. policy areas to even tangentially address IPv6 was Internet security. While Japan and the European Union were announcing national IPv6 strategies, one concern in the United States was the possibility of "cyberterrorism," the intentional disruption or destruction of the Internet or its supporting telecommunications and power infrastructures. An increasing national dependence on networks meant that a major outage could impact critical systems like financial networks, water, power, or transportation and have significant economic and social repercussions. In 2001, several destructive Internet worms, especially Code Red and Nimbda, resulted in disruptive and costly Internet outages.

Within the context of increasingly virulent computer worms and economic and social dependence on networks, the September 11, 2001, terrorist attacks on the United States crystallized an already mounting concern about the vulnerability of economically and operationally vital information networks to possible cyberterrorism. One governmental response to this concern was the development of the *National Strategy to Secure Cyberspace*, the culmination of a lengthy analysis seeking a reduction in U.S. vulnerability to attacks on critical information infrastructures. One of the Strategy's recommendations included improving the security of several network protocols,[231]

[229] Reported in "The numbers Game" by Reed Hellman on the IPv6 Forum web site. (Accessed on www.ipv6forum.org on October 1, 2002).

[230] General information about IPv6 Deployment Summit at INET 2002 found at http://www.ipv6summit.com/.

[231] The network protocols addressed in the *National Strategy to Secure Cyberspace* (February, 2003) included the Domain Name System (DNS), Border Gateway Protocol (BGP), and the Internet Protocol (IP), page 30.

including the Internet Protocol. The Strategy noted that Japan, the European Union, and China were already upgrading from IPv4 to IPv6 and cited "improved security features,"[232] as one of the benefits of IPv6, although Richard Clarke, the top counter terrorism official at the time of the September 11 attack and later the "cybersecurity czar," noted that "a world of mixed IPv4 and IPv6 implementations actually increases the security threat."[233] IPv6 received only a cursory mention in the Strategy, but the document asserted as a fact that IPv6 was more secure than IPv4. One of the document's concrete recommendations called for the U.S. Department of Commerce to launch a task force examining issues related to IPv6.[234]

A significant momentum shift also occurred on June 9, 2003, when the United States Department of Defense mandated it would transition to IPv6 by 2008. John Stenbit, then Assistant Secretary of Defense for Networks and Information Integration and DoD Chief Information Officer, issued a memorandum establishing the directive. The memorandum stated, "The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities (ref a), depends on effective implementation of IPv6…"[235]

The DoD's rationale for upgrading was not consistently expressed. For example, the formal memorandum announcing the IPv6 mandate cited the requirement for end-to-end security and management and more addresses for military combat applications[236] but

[232] *National Strategy to Secure Cyberspace*, February, 2003, page 30. (Accessed at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf on May 1, 2003).

[233] Reported in *Converge Network Digest* (Accessed at http://www.convergedigest.com/packetsystems.html, 2002 on November 13, 2002).

[234] *National Strategy to Secure Cyberspace* recommendation A/R 2-3: "The Department of Commerce will form a task force to examine the issues related to IPv6, including the appropriate role of government, international interoperability, security in transition, and costs and benefits. The task force will solicit input from potentially impacted industry segments." February, 2003, page 56.

[235] United States Department of Defense Memorandum issued by DoD chief information officer, John P. Stenbit for Secretaries of the Military Departments, Subject: Internet Protocol Version 6 (IPv6), June 9, 2003. "ref a" refers to DoD 8100.1 Global Information Grid Overarching Policy, September 19, 2002. (Accessed at http://www.dod.gov/news/Jun2003/d20030609nii.pdf on July 20, 2003).

[236] Ibid.

Stenbit's press briefing[237] contradicted this. Stenbit described how IPv4 had three major shortcomings: end-to-end security, quality of service, and address shortages. Furthermore, only two of these were important to the DoD. The one he described as not salient to the DoD was IP address shortages, although Stenbit acknowledged this was important to Europe. The shortcomings of concern to the DoD were end-to-end security and quality of service. Consistent with the U.S. *Strategy to Secure Cyberspace* and the promise of IPv6 in the EU and some Asian countries, the DoD IPv6 strategy cited enhanced security as one rationale for transitioning to IPv6. Defense Department discussions about IPv6 emphasized its ability to keep military personal safe and secure in a new, fluid, and distributed battleground.

The DoD's IPv6 strategy announcement raised numerous issues. One implication of the DoD's mandate was that net-centric military communications would traverse public Internet infrastructure, using universal protocols and a global IPv6 address space, and would be concerned with quality of service relative to other Internet users. Were classified military communications really best served through transmission over the public Internet? If the communications were not over the public Internet, the DoD could use private addresses over dedicated mobile or fixed links, rendering IPv6 quality of service and expanded address space features irrelevant.

The DoD's mandate also reflected general confusion about *who's in charge* of standards development and who should lead in IPv6 adoption. One questioner asked the DoD's CIO, "How defined is this standard? Is there a world body that defines it somewhere? And if so, who is on it? And does DoD play a role? How does this work?" Stenbit answered that some organization defined standards but he was not certain who, reinforcing the concealed quality of Internet standards development and how hidden standards organizations are tacitly accepted as authorities wielding considerable influence over the Internet's architectural and social directions. Furthermore, an assumption underlying the briefing was that U.S. commercial IPv6 adoption would precede DoD IPv6 adoption. U.S. commercial adoption of IPv6 seemed distant in 2003. Open

[237] See "Briefing on New Defense Department Internet Protocol," John Stenbit, Presenter, Friday, June 13, 2003. (Accessed at http://www.dod.mil/transcripts/2003/tr20030613-0274 on July 20, 2003).

questions included how a potential U.S. commercial rejection of IPv6 or a delay or rejection by the rest of the federal government would impact DoD plans. A related issue was to what extent, if any, the DoD's decision would influence IPv6 adoption in the United States considering the historical relationship between the Defense Department and Internet technologies. In the case of IPv6, military requirements did not drive the IPv6 specifications, but could potentially influence IPv6 adoption. Another open issue was the definition of "IPv6 Capable." The new DoD policy specified that, beginning in October, 2003, all information technology products procured or developed must be "IPv6 capable." In 2003, many software and hardware products contained native IPv6 capability as well as IPv4. Purchasing these products did not equate to implementing IPv6. "IPv6 capable" seemed malleable, ranging from procuring routers and operating systems already including dormant IPv6 support, versus implementing IPv6 as the network layer protocol along with IPv4 through complicated dual stack IPv6 and IPv4 software implementations or protocol tunneling.

Despite any open issues, the IPv6 advocacy community ardently commended the DoD for mandating IPv6 by 2008. IPv6 Forum president, Latif Ladid, issued the following statement, "The IPv6 community and stakeholders applaud the U.S. Department of Defense for leadership in IPv6 and for taking the Internet where it should go. This massive call to action is unprecedented in the history of the Internet as IPv6 will restore the fundamental end to end model of the Internet, the prime enabling technology piece for growth and innovation for everyone and everything to be on the Net where it makes sense."[238]

The DoD IPv6 decision, like the publication of the *Strategy to Secure Cyberspace*, occurred contextually in the wake of the September 11, 2001, terrorist attacks on the United States. John Osterholz, Director of Architecture and Interoperability for the DoD, in spoken public remarks about IPv6, attributed the origins of the requirement for netcentric warfare, in part, directly on the attack on the Pentagon:

> *"When the airplane hit the Pentagon on September 11, a number of things changed. Things are no longer black and white. We're not in*

[238] Quote from Latif Ladid, President of the IPv6 Forum, Chair of the European Union IPv6 Task Force and Internet Society Trustee. (Accessed at www.usipv6.com on November 3, 2003).

> *the cold war anymore – replaced with a million shades of gray. As a department, we were not prepared. Now we've put computers between people and victory. We lost some data in the destruction at the Pentagon. We got a shot to the kneecap. The fire raged for many days. We realized we needed to be more networked, that centralized everything doesn't make sense. The future is broad places of access. This gave birth to a set of things you now hear about as net-centric warfare and operations. It all started on September 11."*[239]

The IPv6 decision appeared interleaved with a broader conversation about the war on terrorism, framed as a new type of war requiring distributed rather than centralized information flows, mobile versus static command and control, and a ubiquitous versus defined front. The new type of war required a new strategy, the Global Information Grid (GIG), which required a new standard, IPv6. The DoD incorporated the GIG/IPv6 strategy within its Joint Transformation Roadmap (January, 2004) designed to transform the military into a force geared toward supporting the DoD's top priorities. These priorities included improving intelligence gathering, surveillance, and strike capabilities in fighting the global war on terrorism, and empowering 'warfighters in the distributed battlespace of the future.'[240] The Department of Defense presented its GIG architecture vision as a groundbreaking approach to a new type of warfare, but many of the objectives seemed familiar. Consider the following vision: "I see an army built into and around an integrated area control system that exploits the advanced technology of communications, sensors, fire direction, and the required automatic data processing – a system that is sensitive to the dynamics of the ever-changing battlefield – a system that materially assists the tactical commander in making sound and timely decisions."[241] Although consistent with the 2003 GIG Architecture objectives, General William Westmoreland, former Commander-in Chief of U.S. Forces in Vietnam espoused this vision in 1969, as historian Paul Edwards notes in *The Closed World: Computers and the Politics of Discourse in Cold War America* (1996).

[239] Public remarks by John L. Osterholz during his presentation "Building the Foundation for Transformation: Net-Centric Operations and IPv6" at the U.S IPv6 Summit in Arlington, Virginia, on December 9, 2003.

[240] U.S. Department of Defense Joint Transformation Roadmap, January 21, 2004. (Accessed at http://www.ndu.edu/library/docs/jt-transf-roadmap2004.pdf on April 4, 2004).

[241] Paul Edwards citing General William Westmoreland, former Commander-in-Chief of U.S. Forces in Vietnam, in *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: The MIT Press, 1996, page 72.

Edwards argues that military planners, often encouraged by civilians, enrolled computers to support a cold war political discourse of centralized command and control capability that fit in with overall Cold War objectives. Analogously, the promise of IPv6 appeared to fit in with the political objectives for a distributed, decentralized, vision of fighting a ubiquitous war on terrorism. Although the cold war network infrastructure approach focused on centralized command and control and the post-September 11 GIG architecture emphasized distributed command and control, the overall vision of General Westmoreland's cold war electronic battlefield and the electronic battlefield of the war on terrorism seemed similar. The connection between digital computers and the cold war and the connection between IPv6 and the war on terrorism are linkages between what Edwards describes as the politics of material change and the politics of representation. Both promised instantaneous information, bloodless remote controlled battlefields, decisive certainty, an impression of technological protection in the face of public fear, and as Edwards describes, "a chaotic and dangerous space rendered orderly and controllable by the powers of rationality and technology."[242] The GIG architecture, enabled by IPv6, seemed retrospective, a recapitulation of cold war communications objectives directed at a ubiquitous enemy rather than the well defined adversary of the Soviet Union.

3.7 U.S. Economic Competitiveness

Despite the DoD's 2003 IPv6 announcement, U.S. government views about the extent of federal IPv6 involvement varied by agency. For example, the Commerce Department's stance on IPv6 seemed cautious relative to the DoD's position. One of the directives in President Bush's *National Strategy to Secure Cyberspace* had called for a formal examination of IPv6 issues. The Commerce Department convened a task force assessing the appropriate role of the United States government in IPv6 deployment and evaluating possible economic opportunities. The National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) co-chaired the task force and solicited public input about U.S. IPv6 opportunities, the

[242] Paul Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War Americ*a. Cambridge: The MIT Press, 1996, page 72.

state of international and domestic IPv6 deployments, technical and economic IPv6 issues, and the merits of U.S. federal government involvement in IPv6.[243] The Commerce Department task force received twenty one public responses, many from American software, hardware, and IT services vendors including Bell South, Sprint Corporation, Microsoft Corporation, Qwest Communications, VeriSign, WorldCom, and Motorola. The task force also received public responses from a few individuals in the Internet standards and IP address registry communities and several advocacy institutions including the Electronic Privacy Information Center (EPIC), the North American IPv6 Task Force (NAv6TF), and the Internet Security Alliance (ISA).

The Commerce Department's task force published a draft discussion report, "Technical and Economic Assessment of Internet Protocol Version, 6 (IPv6),"[244] generally concluding that market mechanisms, not the federal government, should drive IPv6 adoption. The task force acknowledged that, by 2003, most major software and hardware products, like the Linux operating system, some Microsoft products, and Cisco and Juniper routers, already embedded IPv6 capability, but that these features were generally dormant and not activated by users. NTT/Verio was the only service provider already offering IPv6-based Internet access service. The United States had an enormous installed base of IPv4-based communications, and the Commerce Department report estimated that less than one percent of U.S. Internet users employed IPv6 services.

Considering the enormous installed base of IPv4 and the transition costs for upgrading from IPv4 to IPv6, a major policy question addressed whether the benefits of IPv6 outweighed the expense of an accelerated, government influenced or government funded conversion to IPv6. ISPs would incur the highest transition costs, related to upgrading hardware and software and the cost of acquiring IPv6 expertise, while envisioning scant demand in the U.S. and therefore no return on investment. The

[243] United States Department of Commerce, "Commerce Department Task Force Requests Comments on Benefits and Costs of Transition to New Internet Protocol, Appropriate Role of Government in IPv6 Deployment to be Addressed," Washington, D.C., January 15, 2004. (Accessed at http://www.ntia.doc.gov/ntiahome/press/2004/IPv6_01152004.htm on May 1, 2004).

[244] United States Department of Commerce, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)," Washington, D.C., July, 2004. (Accessed at http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf on September 17, 2004).

Commerce Department analysis concluded that many of the touted benefits of IPv6 were already available in IPv4:

> *"IPv4 can now support, to varying degrees, many of the capabilities available in IPv6."*[245]

For example, IPv6 advocates touted improved security as a benefit because the IPv6 standard called for the support of an encryption protocol, IPsec. In contrast, the Commerce Department task force noted that, while "IPsec support is mandatory in IPv6. IPsec *use* is not"[246] and that IPv4 networks can also use IPsec encryption. Furthermore, IPv6 might actually be less secure than IPv4. The analysis summarized the security issue as follows:

> *"it is likely that in the short term (i.e., the next 3 to 5 years) the user community will at best see no better security than what can be realized in IPv4-only networks today. During this period, more security holes will probably be found in IPv6 than IPv4."*[247]

In addition to dismissing improved security as an incentive for upgrading, the report also concluded that many existing mechanisms already mitigated address depletion problems.

Another concern was whether the United States would somehow become disadvantaged economically because of more rapid IPv6 dissemination internationally through governmental promotion and incentives in Asia and Europe. On one hand, the Commerce Department argued that major U.S. software and hardware vendors already supported both IPv4 and IPv6 and sold IPv6 products in international markets. Lethargic U.S. IPv6 adoption would not alter the opportunity for American technology companies to compete in these global markets. On the other hand, concerns about the shift of intellectual resources to Asia in well-funded IPv6 research and development fit into broader Commerce Department and social concerns about the outsourcing of IT jobs to India, China, and other nations. Despite overall outsourcing concerns, the Commerce Department's draft report concluded that, while the U.S. government could "stimulate

[245] United States Department of Commerce, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)," Washington, D.C., July, 2004, Introduction, page 2. (Accessed at http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf on September 17, 2004).

[246] Ibid, chapter 2, page 6.

[247] Ibid.

adoption" as an IPv6 customer, ultimately private sector decisions should drive the market.

The Commerce department's *laissez-faire* conclusions faced ardent criticism from U.S. IPv6 advocates. Alex Lightman, a prominent IPv6 advocate and Chairman of IPv6 Summits Inc., questioned the prospects of future U.S. economic competitiveness in light of rapid international IPv6 deployment. Lightman criticized the Commerce Department recommendation to allow markets to determine IPv6 deployment and questioned where the United States would be economically without a history of IT investment in such areas as telegraph lines, digital computers, satellites, radar, and early Internet innovations such as packet switching and the original ARPANET research project. Some of Lightman's arguments about IPv6 echoed those of governments in Asia and Europe, especially the linking of IPv6 to jobs and economic competitiveness. In 2004, after George W. Bush defeated John Kerry for the presidency, Lightman alluded to Kerry's campaign warning, "America cannot afford a President who's the first to lose jobs since Herbert Hoover in the Great Depression" and suggested that IPv6 investment could stave off unemployment and create 10 million new jobs.[248] Achieving this, he argued, would require $10 billion in government investment over four years and a federal mandate that all its systems transition to IPv6. This type of a mandate would be more contained than national policies in China, Korea, and Japan mandating that all systems, not just federal IT systems, deploy IPv6.

What was at stake if the U.S. failed to upgrade to IPv6 while other parts of the world, especially China, India, Korea, Japan, and the EU upgraded to IPv6? Lightman argued that U.S. exports of Internet products were at risk to such an extent that the U.S. would one day retrospectively ask "Who lost the Internet?"[249] The Commerce Department report noted that U.S. software and hardware vendors generally supported both IPv4 and IPv6, primarily because they served global markets, not just U.S. markets. Yet Lightman suggested the IPv6 issue should have a Sputnik-like urgency for the federal government.

[248] Alex Lightman, "10 Million New Jobs from IPv6: The Case for U.S. Government Investment," *6Sense Newsletter*, November, 2004.

[249] Alex Lightman, "Lead, Follow, or Lose the Great Game: Why We Must Choose a U.S. IPv6 Leader," *6Sense Newsletter*, April, 2005.

An assumption underlying IPv6 advocacy was that IPv6 ranked among "major information technology advances."[250] Whether IPv6 represented a major IT advance was a debatable question dependent upon one's perspective. The IETF designed IPv6 expressly *not* as a novel innovation but an incremental upgrade from IPv4 transparent to users. IPv6 was a network layer protocol technically consistent with IPv4 but allowing for some new features and exponentially more addresses. The availability of more addresses represented an advance relative to international address distribution inequities and emerging applications in wireless and Internet telephony potentially requiring many more IP addresses. But Lightman and others compared IPv6 to new applications like the telegraph, the computer, and radar. Once implemented, IPv6 operates at a technological level invisible to most users. To an individual accessing the web via a browser such as Firefox over an IPv6 based network, a web site or commerce application would usually appear identical as it would to an individual using Firefox over an IPv4 infrastructure.

Nevertheless, a recurrent theme in IPv6 advocacy has cast IPv6 as a Kuhnian paradigm shift. Karen Evans, administrator for electronic government and information technology in the U.S. Office of Management and Budget (OMB), referred to IPv6 as a new communications paradigm and suggested, "the paradigm shift has already started in the Federal government because IPv6 capable software and hardware already exist in Federal government networks (and elsewhere)."[251] Similarly, Dr. Chuck Lynch, Chief of the DoD IPv6 Transition Office, viewed IPv6 as a paradigm shift. While no entirely new applications have emerged which take advantage of the enormous pool of unique identifiers available in the IPv6 address space, Lynch suggested IPv6 held out the potential for new applications. In other words, "complete paradigm shifts are necessary for new capabilities to be brought forth."[252] Sheer numbers of addresses would enable the assignment of unique identifiers to every imaginable communicating device, resulting in new applications. Rather than IPv6 acting as a new capability in itself, it would act as

[250] Alex Lightman, "Twenty Myths and Truths About IPv6 and the U.S. IPv6 Transition (Such as it is)," *6Sense Newsletter*, June, 2005.

[251] From the Statement of the Honorable Karen Evans, Administrator for Electronic Government and Information Technology, Office of Management and Budget, before the Committee on Government Reform, United States House of Representatives, June 29, 2005.

[252] Chuck Lynch, "Newton vs. Einstein," *6Sense Newsletter*, August, 2005.

a potential catalyst for new applications. To emphasize what he viewed as the importance of IPv6 and the differentiation between IPv6 and IPv4, he compared the two to Newton's laws of physics versus Einstein's special relativity.[253]

Those advocating IPv6 and frustrated by their perceptions of slow IPv6 deployment within the United States, and the federal government particularly, appropriated Kuhnian terminology to justify or bolster arguments advocating U.S. government intervention into IPv6. The standards setting community, as discussed in the previous chapter, developed IPv6 as an incremental upgrade to IPv4 operating at the user-transparent network level rather than the application level. The description of IPv6 as a revolutionary paradigm shift among those outside of the standards development process touting IPv6 contradicted this incremental and conservative design philosophy that sought to transparently preserve the basic approach of the Internet Protocol.

3.8 IPv6 Hearing on the Hill

Concerns about IPv6 and American IT competitiveness and outsourcing threats escalated to the United States Congress in June of 2005, exactly five years after Japanese Prime Minister Yoshiro Mori announced his country's E-Japan program establishing the goal of a nationwide IPv6 upgrade. Virginia Representative Tom Davis (R), Chairman of the Government Reform Committee, convened a congressional committee hearing on the Internet and IPv6.[254] The hearing, "To Lead or Follow: the Next Generation Internet and the Transition to IPv6," examined questions about economic opportunities and risks to the United States and about the possibility of a mandate to upgrade the federal government to IPv6.

Representative Davis opened the congressional hearing with remarks about the relationship between the geographical area he represents and the Internet. Davis asserted that 25% of the world's Internet Services Providers (ISPs) were within an hour's drive of Fairfax County, Virginia and that 25% of Internet traffic passed through a hub in Northern Virginia. The Representative further stated that "the current Internet, and the

[253] Chuck Lynch, "Newton vs. Einstein," *6Sense Newsletter*, August, 2005.

[254] The full committee hearing convened on June 29, 2005, at 2:00 p.m. in the Rayburn House Office Building.

protocols and networks that underpin it, may have reached its limits."[255] The hearing generally assumed that the Internet required upgrading and Davis wished to understand the economic implications of Asia's lead, particularly China's lead, in investing hundreds of millions of dollars in aggressive IPv6 deployment. In addition to concerns about United States Internet competitiveness, Davis mentioned homeland security and U.S. defense capability as possible drivers for examining IPv6. Seven individuals offered testimony in the IPv6 hearing, but notably missing were any individuals speaking on behalf of U.S. Internet users, whether corporate, institutional, or individual. Also missing were individuals involved in standards development, with the exception of John Curran testifying for Internet registrar ARIN, but who had served on the IPng Directorate responsible for selecting IPv6 from competing alternatives. Also testifying were representatives of the DoD, GAO, OMB, Microsoft, Verio, and IPv6 Summit, Inc.

The prospect of the United States trialing Asia in Internet innovation, jobs, and economic stature thematically dominated the hearing. Alex Lightman's testimony contained the most emphatic caveats about the economic and political stakes of IPv6. According to Lightman, federal leadership in IPv6, particularly a mandate to transition federal systems to IPv6, might create 10 million American jobs, generate trillions of dollars in revenue, and add products vital to national defense, homeland security, and network security.[256] Conversely, government inaction would result in lost jobs and market share. Lightman estimated that U.S. funding of $50 million in the early Internet resulted in approximately $500 billion annually in federal revenue as well as adding more than a trillion in business wealth through Internet companies. In contrast, he underscored the imbalance between U.S. versus international IPv6 expenditures, suggesting that China, Japan, Korea, and the EU, had invested $800 million versus the U.S. committing $8 million.

The absence of corporate, institutional, or individual Internet users in the congressional hearings accentuated a disconnect between advocacy about upgrading to

[255] From the opening statement of Chairman Tom Davis, "To Lead or To Follow: The Next Generation Internet and the Transition to IPv6," Committee on Government Reform, Washington, D.C., June 29, 2005.

[256] Alex Lightman, Testimony submitted to the Committee on Government Reform Hearing, "To Lead or Follow: The Next Generation Internet and the Transition to IPv6," Washington D.C., June 28, 2005.

IPv6 in the U.S. and the reality of what the IT professionals responsible for network protocol upgrades were actually doing. For example, a 2005 survey[257] of government and private sector IT managers about IPv6 plans revealed two circumstances: 1) among both private and public IT personnel, there were "low levels of interest in IPv6," and 2) despite the DoD IPv6 mandate, federal government IT professionals demonstrated a lower level of IPv6 awareness than even dispassionate corporate IT professionals. The survey further underscored a lack of consensus about the meaning of "IPv6-ready," ranging from IPv6 software in all applications, network devices, and infrastructural components comparable to IPv4 features, to the belief, expressed by 37% of respondents, that IPv6-ready meant the product should be upgradeable to IPv6 at some future time. The surveyed IT professionals overwhelmingly doubted IPv6 would help them achieve their organization's IT objectives and failed to see a compelling functional or budgetary reason to upgrade. Those that did see a compelling reason cited what they perceived as improved security of IPv6.[258]

3.9 The Apotheosis of IPv6

Early strategies for IPv6 adoption reflected a variety of political, economic, and technical interests, but IPv6 advocates have also situated the standard in a more explicitly moral space. Passionate and utopian views of IPv6 have linked the standard with promises of democratization, freedom, social justice, massive job creation and third world development. Many of these claims emanated from advocacy institutions established to promote and advance global IPv6 adoption. A small IPv6 advocacy group, the Sacramento Association of IPv6 Adopters (SAIA) indirectly linked the evolution from IPv4 to IPv6 with the possibility of curing cancer. The following abridged statement appeared on the organization's web site as part of its educational campaign about the benefits of IPv6:

[257] O'Keefee and Company, on behalf of Juniper Networks, surveyed 349 private and government sector IT representatives in April, 2005.

[258] Source: Juniper Networks 2005 Federal IPv6 IQ Study. (Accessed at http://209.183.221.252/Juniper_Networks_2005_Federal_IPv6_IQStudy.pdf on December 19, 2005).

> ***"Can you imagine…***
>
> *What the world would be like without cancer? What it would be like if every young child could access the power of the Internet without knowing how to use a keyboard, or owning a monitor, or without even knowing how to read or write for that matter..even young women living in the poorest, most remote parts of Sub-Saharan Africa? The world is on the cusp of this progress….and, many other countless possibilities…*
>
> *If you are wondering what the economic implications would be for the successful deployment of IPv6 on a global basis, ask yourself this:*
>
> *What percentage of your net worth would you be willing to part with to know the exact time and location of the first cancer cell existing in your body? This is the kind of information that can eventually be uncovered in the future with the Internet running on IPv6."*[259]

This linkage between IPv6 and curing cancer was anomalous in its optimism, but other advocates have claimed that the IPv6 routing and addressing standard could help impoverished children in Africa, eradicate social inequities, and spread democratic freedoms. IPv6 proponents have described the standard as "for the people," an instrument of democratization, freedom, and egalitarianism. Alder describes how, two hundred years earlier, French Revolutionary scientists viewed the metric system as "for all people, for all time," a utopian democratic vision of equal access to information contra powerful entities wishing to protect their interests. Expectations about the social benefit of the expansion of the Internet address space under IPv6 have also mirrored descriptions of the expansion of "ether" (electromagnetic spectrum) in radio broadcasting a century earlier. Both radio spectrum and the IP address space are invisible and intangible finite resources mediating access and linking individuals over a communal medium. In *Inventing American Broadcasting* (1987), Susan J. Douglas discusses the "democratic rhetoric that described the air as being free and the property of the people."[260] Hugh R. Slotten, in *Radio and Television Regulation in Broadcast Technology in the United States, 1920-1960*, explores the utopian rhetoric surrounding technological advancements in radio broadcasting. Engineers and policy makers, as well as some public participants, viewed broadcasting innovations as precursors to social progress and as imperatives for

[259] From the web site of the Sacramento Association of IPv6 Adopters (SAIA). (Accessed at http://www.sacramentoipv6.com/imagine.html on November 17, 2004).

[260] Susan J. Douglas *Inventing American Broadcasting: 1899-1922*. Baltimore: The Johns Hopkins University Press, 1987, page 214.

solving social problems.[261] Utopian claims about IPv6 as a solution to common pool resource scarcity followed an identical trajectory in linking the standard with solving social problems and world conflicts. Jim Bound, a Hewlett Packard fellow who served as the Chair of the IPv6 Forum Technical Directorate, Chair of the North American IPv6 Task Force,[262] and who had previously served within the IETF on the IPng Directorate, posted the following (abridged) fall, 2002, statement on the opening web page of the North American IPv6 Task Force:

> *"IPv6 is about Freedom. I agree. . Today, the cost of freedom is great. IPv6 reduces that cost I believe greatly, thus IPv6 is also about peace. And peace is good for business. So from a business perspective the cost of not doing IPv6 is great. This should be part of our business view. We need that peace as soon as possible and our world economies will benefit; thus the people will benefit. And all people will benefit not just the rich, the famous, the strong, and the elite but the child in a ghetto of an inner city, the handicapped trying to survive, and many other cases. Because peace is good for business and one vehicle to achieve peace is with communications. IPv6 will permit worldwide global peer to peer communications and in a secure manner. This expands markets for individual creativity to flow and for businesses to achieve growth. Clearly a metaphysical logic with an innate premise that the effort is beyond ones own self interest, but logic none the less."*[263]

Bound was responding, in part, to an earlier statement at an IPv6 Global Summit in Ottawa, Ontario, Canada, by Joost Van-Gestel of Nokia, who publicly suggested that IPv6 is about "freedom"[264] in the context of his presentation on Nokia's wireless IPv6 strategy.[265] As Chairman of the North American IPv6 Task Force and long time participant in the IPng/IPv6 standards development process, Bound consistently articulated both technical and social visions for IPv6. Bound joined those hoping IPv6 would restore the end-to-end architectural philosophy of the Internet and serve as a catalyst for innovation and therefore, free enterprise, which would enable world wide connectivity via the Internet. Bound, consistent with the overall vision of the North

[261] Hugh R. Slotten, *Radio and Television Regulation: Broadcast Technology in the United States, 1920-1960*. Baltimore: The Johns Hopkins University Press, 2000, page 237.

[262] A subchapter of the IPv6 Forum.

[263] Jim Bound, posting on North American IPv6 Task Force web site. (Accessed at www.nav6tf.org accessed in October, 2002).

[264] Posting on IPv6forum mailing list on behalf of Jim Bound, May 18, 2001.

[265] Joost Van Gestel's presentation at the IPv6 Global Summit, "Nokia Vision on IPv6" Ottawa, Ontario, Canada, May 16, 2001.

American IPv6 Task Force, ascribed to the doctrine that ubiquitous interconnectivity via the Internet would promote human dialog and that this "dialogue will enable us to come up with new and innovative ways to live in peace and prosperity, to better understand our environment, and to coexist with nature and each other."[266]

The NAv6TF's mission and IPv6 vision reflected the objectives of its parent organization, the IPv6 Forum. Latif Ladid founded the IPv6 Forum in May of 1999, shortly after the formal ratification of the IPv6 specifications, to promote worldwide deployment of IPv6. In frequent presentations about IPv6, Ladid has often suggested that participants promote IPv6 to generally serve society. He has argued that IPv6 could help alleviate the digital divide and suggested that those interested in IPv6 "do something for yourself, your community, your society, your country, your world. Be a pioneer in IPv6."[267]

Exemplifying the linkage between IPv6 and global democratization, Lightman has described the potential for "IPv6 as an Instrument of Freedom Amplification," advocating a U.S. foreign policy of distributing IPv6-based communication devices to contribute to President Bush's general objective of "spreading freedom." Shortly after President Bush's second inaugural address, Lightman suggested that the U.S. spend $20 billion annually to provision one billion IPv6-enabled devices around the world. These devices would allow users to send instant messages, place telephone calls, and access the web, functional equivalents of devices like Blackberries or multimedia cell phones. Lightman estimated each device would cost $20. Even if this strategy were feasible, it omitted from the $20 billion annual expenditure the monthly cost of providing service for each user. Disregarding this and other legal, cultural, technical, financial, linguistic, and access impediments, the thesis of Lightman's article is the direct linkage between IPv6 and freedom. Distributing IPv6 communicators or, by extension, their functional equivalent of Blackberries or multimedia cell phones, would "support the growth of democratic movements and institutions in every nation and culture" and enable users to

[266] Jim Bound, "NAv6TF Mission/Deployment/Vision Status," January, 2004. (Accessed at http://www.ec.ipv6tf.org/PublicDocuments/NAv6TF_Mission.pdf on December 14, 2005).

[267] Latif Ladid speaking at the United States IPv6 Summit, Arlington, VA, December 10, 2003.

"end tyranny in their own countries, without the U.S. needing to fire a shot."[268] Many of these assumptions mirrored themes in Bush's inauguration speech: only the force of human freedom could end hatred and expose tyranny; it is in the best interest of the United States to promote democratic freedom around the world; and that this promotion of freedom represents the policy of the United States. Lightman argued that IPv6 communicators "would be the single greatest achievement in the history of freedom,"[269] an assertion responding to the last sentence in President Bush's inaugural address, "we are ready for the greatest achievements in the history of freedom."[270]

IPv6 advocates have worked directly with governmental agencies around the world, including some U.S. entities including the Department of Defense and members of Congress. From its 2001 inception as a North American outgrowth of the IPv6 Forum, the NAv6TF worked with U.S. government entities (the Cybersecurity Office and the Department of Defense) to promote IPv6, assess possible roles of IPv6 in the federal government, and address technology deployment issues. As part of this liaison, the institution participated in "Moonv6," a collaborative IPv6 test pilot launched in 2003 with the InterOperability Laboratory at the University of New Hampshire, the U.S. Department of Defense Joint Interoperability Testing Command, and industry vendors.[271] The founding mission of the collaboration sought to develop a testbed network demonstrating interoperability between diverse IPv6 products. Moonv6 project leaders reflected a mixture of IPv6 perspectives and included: NAv6TF Chair and IETF contributor Jim Bound; Major Roswell Dixon, IPv6 Action Officer within the DoD's

[268] Alex Lightman, "IPv6 as an Instrument of Freedom Amplification," 6Sense Newsletter, February, 2005.

[269] Ibid.

[270] Transcript of President George W. Bush's Second Inaugural Address, January, 2005. (Accessed at http://www.whitehouse.gov/news/releases/2005/01/20050120-1.html on December 2, 2005).

[271] Participating service providers and laboratories in the Phase I Moonv6 tests included: Chunghwa Telecom, France Telecom, Internet2, NTT R&D, Root Server Test Bed, Sprint, UNH-IOL, and the U.S. Department of Defense Vendors included: 6 Wind, Agilent Technologies Check Point Communications, Cisco Systems, Elmic Systems, EMC, Extreme Networks, Foundry Networks, Fujitsu, Ixia, Hewlett Packard, Hitachi, Hexago, IBM, IP Infusion, Juniper Networks, Navtel Communications, NEC, Nokia, Procket Networks, Microsoft, S-Net Systems, Spirent Communications, Sun Microsystems, and Windriver, according to the Moonv6 list of Phase I vendors listed on the testbed website. (Accessed at www.moonv6.org on October 15, 2004).

Joint Interoperability Test Command; and Yasuyuki Matsuoka of NTT in Tokyo, Japan. The testbed's nomenclature "Moonv6" symbolically represented the importance participants placed on IPv6. In a meeting discussing the seriousness with which the United States should consider IPv6, someone questioned whether the United States should view IPv6 with the same urgency is viewed reaching the moon in 1969.[272] The IPv6 testbed leaders selected the name "Moonv6" accordingly.

A variety of optimistic expectations for IPv6 similarly converged at a one day public IPv6 meeting in July, 2004, entitled, "Deploying IPv6: Exploring the Issues." The United States Commerce Department sponsored the meeting, which included Vinton Cerf, Mark Rotenberg of the Electronic Privacy Information Center (EPIC), various representatives from industry, academics, and government, and IPv6 advocates Latif Ladid and Jim Bound.[273] Jim Bound posed the following provocative question to the morning session panelists: "how that can help in your mind the social aspects that we face in our own inner city ghettos, for security defense networks. In 9/11, police, port authority, and firemen were unable to communicate. That cost lives. That's a social problem, too. And how can IPv6 maybe help it so that the kids that I work with in my private life from the inner city ghettos have equal opportunity to learn about communications, learn about the Internet and evolve? Thank you."[274] Bound's question during the IPv6 public forum invoked September 11, 2001, as others had in previous forums and his question presupposed an association between IPv6 and a broad range of

[272] According to the moonv6 web site. (Accessed at www.moonv6.org on October 15, 2004).

[273] The meeting took place at the Herbert C. Hoover Building, Room 4830, of the United States Department of Commerce, in Washington D.C. on Wednesday, July 28, 2004. The meeting was webcast live on the Internet and included the following participants: Mr. Michael D. Gallagher, Department of Commerce; Dr. Vinton Cerf, MCI; Dr. Michael Gallaher, RTI; Mr. Dan Caprio, Department of Commerce; Dr. Mark Skall, NIST; Mr. Joseph Watson, NTIA; Mr. Stan Barber, Verio; Mr. Mark Desautels, CTIA; Dr. Paul Francis, Cornell University; Mr. Tony Hain, Cisco; Mr. Henry Kafka, Bell South; Dr. Latif Ladid, IPv6 Forum; Dr. Paul Liao, Panasonic; Mr. Mark Rotenberg, EPIC; Mr. Jim Bound, North American Task Force; Ms. Marilyn Kraus, DoD; Mr. Preston Marshall, DARPA; Dr. Douglas Maughan, Department of Homeland Security; Mr. Gene Sokolowski, GSA; Dr. Rick Summerhill, Internet2; Mr. Ted Tanner, Microsoft; and Mr. Rick White, TechNet.

[274] Transcript of the Department of Commerce public meeting, "Deploying IPv6: Exploring the Issues," Washington, D.C., July 28, 2004. (Accessed at http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/IPv6Transcript_part1.htm on November 2, 2004).

social concerns: poverty, national defense, homeland security, first responder capability, and education.

Not everyone embraced expectations about the broad social benefits of IPv6. Dr. Paul Francis of Cornell University characterized the linkage between social inequity, ghettos, and IPv6 as tenuous[275] and Mark Rotenberg of EPIC summarized "it's a bit of a stretch to think that we solve problems of social inequality through IPv6 deployment."[276] In contrast, Bound's colleague, Latif Ladid, accentuated the social possibilities of IPv6 and portrayed implementing the standard as a moral obligation:

> *"I think we have a moral obligation and a unique opportunity to do something special, not only to look at the profits and look at the stock market and so on and so forth. I think we've got to go beyond this and do something that's going to give some kind of hope and vision for the entire world...most probably the kids in Detroit and the Bronx so on and so forth, they have exactly the same digital chasm that we have in Africa."*[277]

Ladid's choice of the term "moral obligation" toward the next generation of children and Bound's references to inner city ghettos certainly appear distant objectives from the DoD's distributed warfare strategy or the economic objectives of Japan and the European Union. Nevertheless, themes of IPv6 improving children's lives and ameliorating social problems accompanied various IPv6 rationales. Even the Director of Architecture and Interoperability for the United States Department of Defense, in public remarks, had suggested that IPv6 "is really important to the lives of kids."[278] His statement mirrored the IPv6 advocacy rhetoric of Bound and Ladid in indicating that IPv6 would improve children's lives. These rationales alluded to IPv6 as a moral intervention aimed at a teleological goal of Internet globalization. The Internet Society, with the motto "Internet For Everyone," similarly viewed the upgrade to IPv6 as a necessary precursor to the objective of Internet ubiquity. Several assumptions

[275] Dr. Francis responded, "Just to answer Jim's question it seems to me it's a pretty long distance between IPv6 and talking about social inequity and ghettos and things."

[276] Mark Rotenberg statement from the transcript of the Department of Commerce public meeting, "Deploying IPv6: Exploring the Issues," Washington, D.C., July 28, 2004.

[277] Latif Ladid statement from the transcript of the Department of Commerce public meeting, "Deploying IPv6: Exploring the Issues," Washington, D.C., July 28, 2004.

[278] John L. Osterholz, Director of Architecture and Interoperability, United States Department of Defense, Keynote Address at United States IPv6 Summit, Arlington, Virginia, Tuesday, December 9, 2003.

underpinned both the teleological notion of Internet globalization and the mechanism, IPv6, for achieving this goal. This project assumes a problem requiring fixing, namely a digital divide, whether Africa, as Ladid mentioned, or inner city ghettos in the United States, as Bound referenced, and assumes that modernization and Internet ubiquity are self-evident imperatives. As Escobar describes, "An entire politics of needs interpretation, mediated by expert discourses, is at stake… Experts become brokers of sorts mediating the relations between communities, the state, and- in some cases-social movements."[279]

3.10 The IPv6 Security Question

One commonality among IPv6 advocacy was the espousal of "increased security" as a considerable advantage of IPv6 over IPv4. The 2003 Defense Department memorandum mandating IPv6 lauded end-to-end security as one rationale for upgrading. The U.S. *Strategy to Secure Cyberspace* tersely described IPv6 as providing greater security than IPv4. Japan's IT Strategy Council argued that a benefit of IPv6 was its enhanced security features. The IPv6 Forums, with their self described objective of advocating worldwide IPv6 deployment, touted security features in conjunction with address space expansion as justification for upgrading. IPv6 advocates have incessantly reproduced the argument and the technical media has unquestioningly depicted "enhanced security" features of IPv6. Exemplifying this advocacy, the networking industry journal, Network World, argued, "IPv6 promises a dramatically larger addressing scheme as well as enhanced security and easier administration."[280] Technical engineers for vendors economically invested in IPv6 have also touted security as an inherent IPv6 feature, referring to the standard as "IPv6, An Enhanced Security Network Protocol."[281]

In contrast, some groups within the United States government challenged the extent to which IPv6 provided greater security than IPv4. A 2005 Government Accountability Office (GAO) analysis of IPv6 identified security risks as a significant

[279] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, page 110.

[280] Carolyn Duffy Marsan, "IPv6 Expert Sees Adoption Growing… Slowly," *Network World*, September 27, 2004.

[281] Chuck Sellers, Senior Product Engineer, Verio Network Services, "IPv6, An Enhanced Security Network Protocol," *6Sense Newsletter*, December, 2004.

transition consideration for federal agencies. The U.S. House of Representatives Committee on Government Reform requested that the GAO perform an analysis auditing the progress the DoD and any other government agencies have made in transitioning to IPv6 and identifying considerations for agencies upgrading or planning to upgrade. The GAO methodology employed government auditing standards and issued its findings in a May, 2005, report entitled, "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks."[282]

The GAO noted the dormant IPv6 capability in the software and hardware products many federal agencies already routinely procured. Most routers already incorporated features, by 2005, allowing users to configure networks for IPv6 traffic. Similarly, leading operating systems such as Linux, Solaris, Cisco IOS, Microsoft Windows, and Apple OS X supported IPv6. The GAO report stressed that this dormant IPv6 capability actually exacerbated security risks rather than mitigating risks. For example, an employee enabling IPv6 capability might create an inadvertent security problem because an institution's security system configuration might not detect breaches exploiting IPv6 features. The GAO audit specifically investigated two IPv6 characteristics, automatic configuration and tunneling, for security vulnerabilities. The audit confirmed already widely understood security vulnerabilities of these features and determined "they could present serious risks to federal agencies."[283] Protocol designers included automatic configuration as an IPv6 featured intended to simplify network administration of IP addresses. This autoconfiguration feature might permit an unauthorized router connected to an agency network to reconfigure neighboring system addresses and routers, exposing them to vulnerabilities because resulting IPv6 activity could circumvent existing intrusion detection systems (IDS). The GAO audit similarly assessed security vulnerabilities associated with tunneling, the technique of transmitting IPv6 packets over an IPv4 network. The embedding of IPv6 formatted information within IPv4 packets allowed potentially unauthorized activity to occur undetected by firewalls.

[282] United States Government Accountability Office, Report to Congressional Requesters, "Internet Protocol Version 6, Federal Agencies Need to Plan for Transition and Manage Security Risks," GAO-05-471, May, 2005.

[283] Ibid, page 22.

The U.S. Computer Emergency Readiness Team (US-CERT) also identified numerous IPv6 security vulnerabilities. CERT, originally an acronym for Computer Emergency Response Team, formed in the aftermath of the 1988 computer worm which disrupted thousands of Internet-connected computers. The worm, launched by Cornell graduate student Robert Morris, raised awareness about network security vulnerabilities and led to DARPA establishing a new DoD-funded organization at Carnegie Mellon University called the Computer Emergency Response Team to respond to security incidents and educate users.[284] Years later, in September of 2003, the U.S. Department of Homeland Security created a new CERT, the U.S.-CERT, which would supercede but coordinate with the Carnegie Mellon operated CERT and numerous other CERT organizations throughout the world. The formation of U.S.-CERT reflected homeland security concerns about cyberterrorism in the wake of the September 11 attacks and awareness of increasing economic and political value of the Internet as a critical national infrastructure. As part of its activities, U.S.-CERT identified vulnerabilities in products, systems, and protocols and identified a number of inherent security vulnerabilities in the IPv6 protocol. The following includes some abridged CERT vulnerability notes addressing a range of IPv6 related security weaknesses.

SELECTED EXCERPTS
FROM CERT VULNERABILITY NOTES
RELATED TO IPv6

Vulnerability Note VU#930892

Cisco IOS vulnerable to DoS or arbitrary code execution via specially crafted IPv6 packet

Cisco Internetwork Operating System (IOS) IPv6 packet handling is vulnerable to a denial-of-service attack and may potentially be vulnerable to a flaw that allows arbitrary code execution.

[284] DARPA press release, DARPA Establishes Computer Emergency Response Team," December 6, 1988.

A remote, unauthenticated attacker on the local network segment that can craft and send an arbitrary IPv6 packet may be able to crash or take control of the device running IOS.[285]

Vulnerability Note VU#472582

Cisco IOS IPv6 denial-of-service vulnerability

A vulnerability in the way Cisco IOS handles IPv6 packets could result in a remotely exploitable denial of service.

A remote attacker may be able to cause an affected device to reload, thereby creating a denial of service condition.[286]

Vulnerability Note VU#658859

Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 memory leak

The Juniper JUNOS Packet Forwarding Engine (PFE) leaks memory when certain IPv6 packets are submitted for processing. If an attacker submits multiple packets to a vulnerable router running IPv6-enabled PFE, the router can be repeatedly rebooted, essentially creating a denial of service for the router.[287]

Vulnerability Note VU#658859

Solaris systems may crash in response to certain IPv6 packets

Solaris 8 systems that accept IPv6 traffic may be subject to denial of service attacks from arbitrary remote attackers.[288]

Vulnerability Note VU#370060

[285] US-CERT Vulnerability Note VU#930892, “Cisco IOS vulnerable to DoS or arbitrary code execution via specially crafted IPv6 packet,” Date Public, July 27, 2005.

[286] US-CERT Vulnerability Note VU#472582, “Cisco IOS IPv6 denial-of-service vulnerability,” Date Public, January 26, 2005.

[287] US-CERT Vulnerability Note VU#658859, “Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 memory leak,” First Public, June 29, 2004.

[288] US-CERT Vulnerability Note VU#370060, “Solaris systems may crash in response to certain IPv6 packets,” First Public, July 21, 2003.

Each vulnerability pronouncement necessitated that users install vendor issued software patches and upgrades. In some cases, users were not even cognizant of the dormant IPv6 features inherent in products, a phenomenon the GAO's IPv6 assessment emphasized. Many users assumed IPv6 security advisories were not applicable unless they had activated IPv6 features so would assume vulnerability announcements did not pertain to their systems.

3.11 Latent National IPv6 Implementations

Considering the history of optimistic IPv6 expectations and aggressive adoption plans, how did strategic plans progress? Japan's IT strategy ranked among the most aggressive for implementing IPv6. Recall that, in 2000, Japanese Prime Minister Yoshiro Mori established a 2005 deadline for upgrading every Japanese business and public sector computing device to IPv6. The e-Japan Strategy sought to elevate Japan to a global IT leader by 2005, an objective requiring a complete national transition to IPv6.[289] By 2005, this ubiquitous transition had simply not occurred. According to the official description of Japan's IPv6 Promotion Council, in 2005, "The spread of IPv6 has just begun.." and: "There are still a number of barriers to the deployment of IPv6 and promotion measures to solve this problem and remove the barriers are needed for some time. As we pull through this stage, IPv6 will propagate on its own."[290]

For the introduction period of IPv6, the Council noted that they could not expect to achieve "things only IPv6 can do,"[291] seemingly acknowledging that IPv6 is not an application but a transparent network addressing and routing protocol. It also acknowledged that IPv4 and IPv6 would coexist and that IPv6 security issues were complex. Korea's IPv6 deployment status in 2005 also primarily involved trial networks. In 2005, Korea's IPv6 strategy modified to continue research and development test networks and expand commercial services toward a goal of full national IPv6 deployment

[289] Specified in the e-Japan Priority Policy program, Policy 2, March 20, 2001. (Accessed at http://www.kantei.go.jp/foreign/it/network/priority/slike4.html on April 15, 2003).

[290] IPv6 Promotion Council of Japan, "2005 Version IPv6 Deployment Guideline: About the IPv6 Deployment Guideline," March, 2005. (Accessed at http://www.v6pc.jp/pdf/en-01-IPv6_Deployment_Guideline.pdf on December 4, 2005).

[291] Ibid.

by 2010.[292] European Union, Chinese, and Indian IPv6 deployments were similarly inchoate. The overall worldwide status of IPv6 deployment, while steadily progressing, still primarily involved measured network pilots. Limited production networks were beginning to become available but, as Internet technologist and IPv6 advocate Jim Bound described, not with "the required management, application, middleware, or security infrastructure required for most production networks."[293]

3.12 Chapter Conclusion

Historian of technology, Ken Alder, argued: "if standards are a matter of political will as much as of economic or technical readiness, then reaching an agreement on standards depends as much on myths as on science, especially on myths *about* science."[294] IPv6 is a routing and addressing specification, not a specific application, but advocates have espoused buoyant expectations about IPv6 curing cancer, spreading democratic freedoms, fighting poverty, adding thousands of new jobs, and bolstering the U.S. war on terrorism. Even manifest claims of IPv6 as self-evidently more secure than IPv4 (and therefore an apologia for upgrading) appeared somewhat contestable. The DoD, IPv6 advocacy groups, national government technology councils, the technical media, and networking vendors promoted IPv6 as self-evidently more secure than IPv4, but in practice, protocol vulnerability reports from CERT, GAO technical assessments, and security experts seem to cast doubt on these claims. As usual, implementation realities are more nuanced than paper specifications. IPv6, commensurate with most evolving protocols, has had a history of intrinsic security vulnerabilities. Even institutions or individuals choosing not to enable the IPv6 capability available in many products were still susceptible to these vulnerabilities. Assertions that IPv6 provided enhanced security emanated from the written specification, IPv6, which mandated inclusion of the network encryption protocol IPsec. Although IPv6 - as a standard - does mandate support of encryption protocol

[292] "IPv6 Development Status in Korea," Doc no: Telwg31/IPv6/05; APEC telecommunications and Information Working Group 31st Meeting, Bangkok, Thailand, April, 2005.

[293] Jim Bound, "IPv6 Deployment State 2005," in *Upgrade: The European Journal for Informatics Professionals*, Vol.VI, Issue No. 2, April, 2005.

[294] Ken Alder, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error That Transformed the World*, New York: Free Press, 2002, page 327.

IPsec, IPv6 – as actually implemented – does not require IPsec. IPsec encryption requires user action. Additionally, network administrators can choose to implement IPsec with IPv4 or IPv6 so using IPsec support as a significant security demarcation between the two protocols is somewhat of a mischaracterization. Former "cybersecurity czar" Richard Clark further forecasted that mixed IPv4/IPv6 environments might actually provide less security than either a homogenous IPv4 or homogeneous IPv6 environment. Most importantly, IPsec, even if implemented in IPv4 or IPv6, only achieves encryption and does not directly address other security concerns such as authenticating users, detecting worms or viruses, combating spyware, or defending against denial of service attacks. Categorical statements such as the DoD's claim about IPv6 being more secure than IPv4 are oversimplifications of complex Internet security realities.

Any magnified IPv6 claims have not diminished historical concerns about inherent resource constraints, distribution inequities, or projected address requirements of emerging applications. On the surface, these concerns are classical questions about allocation of finite technical resources, but they prove not to be conducive to scrutiny using conventional economic theory. Chapter II described how those establishing standards rejected the possibility of market mechanisms determining standards selection. The following chapter will address the distribution of IP addresses and how addresses have never been exchanged in any markets. This chapter described how those driving IPv6 adoption have abrogated *laissez faire* approaches, instead delivering top-down mandates such as Japan's national IPv6 directive or the DoD's IPv6 pronouncement. With the exception of the U.S. Commerce department's positions, state interventions have selected the technology, IPv6 products, vendors must develop rather than promoting competitive market development of Internet products.

Nascent IPv6 adoption proceeded by political fiat, reinforcing the argument that standards are a political phenomenon. Rather than oversimplifying the role of state interventions, the history of early IPv6 mandates has also revealed the influence of IPv6 activists, and especially large corporations, in the formulation of national IPv6 strategies. Economic interests directly infused IPv6 decision making, not only nationalistic macroeconomic objectives but the interests of corporations poised to benefit from massive IPv6 adoption, state funding interventions, or accompanying regulatory liberalization.

Incipient IPv6 adoption strategies reflected competitive struggles for control of Internet resources and economic dominance in the Internet industry. The profusion of IPv6 resources seemed to solve the impending resource constraints of late entrants into a U.S. dominated Internet industry, while those with ample addresses postponed consideration of IPv6. Distinct from resource requirements, international governments also selected IPv6 as a new arena in which market hegemony was not yet established. Conversely, the conservative position of maintaining the status quo by deflecting federal standards involvement onto market mechanisms sought to maintain the dominance of those with ample addresses, resource control, or market leadership in Internet products. The promise of IPv6 aligned with a variety of political objectives: a homogenizing specification advancing European unification and economic competitiveness; governmental promises of IPv6 thwarting economic stagnation in Japan or unemployment in Korea; the DoD promise of IPv6 for an orderly, secure, intelligent, and decisive war on terrorism; or the potential for the U.S. to subvert economic threats from India and China. In most cases, the issue of address space exhaustion existed as a tangential rationale. In general, political and technical objectives were mutually cast as unquestioned certainties, with the concealed complexity of the IPv6 specification all but precluding public ability to question the efficacy of the standard to achieve promised objectives. In a complex admixture of economics, politics, and technology, early IPv6 adoption aligned with political objectives and also reflected tensions between competing campaigns for Internet ascendancy.

CHAPTER IV:
THE INTERNET ADDRESS SPACE

The presumption of Internet address space exhaustion contributed to the complex rationales for IPv6 development and adoption. Convictions about the Internet providing insufficient addresses to accommodate international growth and emerging applications have prevailed among a mélange of interests spanning the Internet's technical community, factions within the United States Department of Defense, and heads of state like former Japanese Prime Minister Yoshiro Mori. One commonly reproduced narrative has cited statistics about American universities controlling more Internet addresses than entire countries. A cursory Google search for "Stanford and China and Internet address" returned thousands of stories spanning a decade and replicating the "statistical fact" that Stanford possessed more IP addresses than the People's Republic of China. One account in ChinaDaily.Com asked, "What do China, Stanford University, MIT, and Princeton University have in common?"[295] The article rejoined that they possessed approximately the same number of Internet Protocol (IP) addresses and that upgrading the Internet to the new IPv6 protocol would ameliorate this disproportion. Momentarily suspending examination into the validity of this claim, the possibility of geographical, political, or socioeconomic disparities in IP address allocation raises questions about equitable control, distribution, and possession of technologically generated resources within a system that transcends international boundaries.

Once again, notions of the Internet as an egalitarian platform with no central control are erroneous in that some underlying administrative functions entail central coordination. Chapter II discussed centralized standards coordination. A centralized authority has also controlled and allocated addresses to maintain global uniqueness of every assigned IP address. This raises several questions. On what basis has any authority had legitimacy to allocate finite resources? What allocative method originally determined the distribution of IP addresses - market based approaches, government intervention, or community based distribution - and did this contribute to real or

[295] See "IP Address Supply Facing Crunch," by Liu Baijia, China Daily, April 20, 2005. Accessed at http://www.chinadaily.com.cn/english/doc/2005-04/20/content_435822.htm on July 17, 2005).

perceived IP address shortages? Most public controversies about Internet resource control have centered on domain names, the human readable text strings (e.g. www.dartmouth.edu or www.yahoo.com) associated with IP addresses. IP addresses have not historically received proportionate attention, partly because users do not directly engage Internet addresses and because addresses do not involve the same controversial issues involving free speech, privacy, antitrust issues, intellectual property, and cultural standards of decency which have plagued Internet governance of domain names. This chapter seeks to elevate the issue of IP address space origination, allocation, and control. It historically traces the progression of the Internet address space from its 1960s inception, to the development of the IPv4 address space, to anticipation of potential Internet address space exhaustion by the Internet's technical cognoscenti in 1990, to the IPv6 address structure. The chapter includes accounts of dissenting arguments challenging predictions of Internet address scarcity and also describes intractable governance dilemmas involving international struggles for control of Internet addresses.

4.1 Internet Address Space Circa 1969

New technologies create new, technologically-derived resources. Radio systems engendered the technologically-derived resource of the electromagnetic spectrum's radio frequency band. Internet connectivity requires the technologically-derived resource of unique binary addresses. As discussed, all devices transmitting or receiving information over the Internet use a unique numerical designation similar to a unique postal address. Unlike electromagnetic spectrum (which includes harmful ultraviolet, x-ray, and gamma-ray bands), no natural demarcation constricts the number of theoretically possible Internet addresses. The Internet standards community established specifications dictating the size of binary Internet addresses and therefore the number of devices able to interconnect.

The topic of network addresses appeared in the premiere Request For Comment, RFC 1, "Host Software." UCLA's Stephen Crocker authored RFC 1 in April of 1969, several months before the UCLA ARPANET node, the first of four original ARPANET nodes, became operational and prior to any definitive decisions about the applications the network would eventually support. RFC 1 enumerated tentative specifications for the Interface Message Processor (IMP) software, and host-to-host connections. ARPANET researchers decided to allocate 5 bits to information headers as a destination code for the IMPs.[296] The allocation of 5 bits as a destination address would have theoretically provided 2^5, or 32, unique destination codes:

00000 00001 00010 00011

00100 00101 00110 00111

01000 01001 01010 01011

01100 01101 01110 01111

10000 10001 10010 10011

10100 10101 10110 10111

11000 11001 11010 11011

11100 11101 11110 11111

Expanding the total number of addresses above 32 would require expanding the size of the binary code. Each additional bit would double the number of available addresses. For example, increasing the binary code to 6 bits would provision 2^6, or 64 addresses; increasing the binary code to 7 bits would expand the number of unique addresses to 2^7, or 128; and increasing the code to 8 bits would provide 2^8, or 256 unique addresses, and so forth.

The researchers gradually augmented the number of addresses as they anticipated requirements for connecting more devices. In 1972, the Network Working Group extended the address size to 8 bits, increasing the number of possible device connections to 2^8, or 256. In 1976, seven years after the 1969 operational installation of IMP No. 1 at UCLA, the ARPANET interconnected 63 hosts.[297] The 256 available destination codes more than sufficed to connect these devices. A gradual ARPANET expansion occurred within a mid-seventies computing context dominated by mainframe computers, with a modest minicomputer industry, but prior to widespread availability of personal computers. In this experimental environment in which expensive mainframe computers predominated, widespread growth or even success of the ARPANET was hardly inexorable. Even if successful, as Katie Hafner and Matthew Lyon posited in *Where Wizards Stay up Late: The Origins of the Internet* (1996), "Who but a few government bureaucrats or computer scientists would ever use a computer network?"[298]

[296] Steve Crocker, "Host Software," RFC 1, April 7, 1969, page 2.

[297] Peter H. Salus. "One Byte at a Time: Internet Addressing." *The Internet Protocol Journal*, Volume 2, Issue 4, December, 1999.

[298] Hafner, Katie and Matthew Lyon. *Where Wizards Stay up Late: The Origins of the Internet*. New York: Simon & Schuster, 1996, page 104.

As Abbate explains, a phenomenon unforeseen by ARPANET developers was the emergence of electronic mail in the 1970s as the network's most widespread and expansive application. Prior to the network's development, ARPANET Project Manager Larry Roberts downplayed electronic messaging as a possible application, focusing instead on resource sharing and file transfer.[299] But rather than primarily interconnecting computing resources as anticipated, ARPANET users developed and embraced programs and protocols for real-time messaging which supported collaborative work and served as a forum for the growing ARPANET community. The unanticipated application of electronic mail continued to interest users. On March 26, 1976, Great Britain's Queen Elizabeth II became one of the first heads of state to send an electronic mail message, issued during a visit to the Royal Signals and Radar Establishment in Malvern, Worcestershire.[300]

Electronic mailing lists became both a driver of increased network usage and also a reflection of the ARPANET's growing role as a communications platform for a rapidly expanding electronic community. Rather than providing communications between two computers, mailing lists enabled large groups of people with common interests and identities to communicate in a shared, open forum. Mailing lists contributed to the unexpected growth in the size of the network, played an important role in facilitating communications among Internet standards and technology communities, and reflected shared values of open communications and collaborative development within the Internet user/developer culture.

RFC 791 (1981) introduced the Internet Protocol standard, later called IPv4, expanding the size of each IP address to a 32-bit code divided into a network prefix and a host prefix. Mathematically, this binary address size of 32 bits would support more than four billion hosts, calculated as 2^{32}, or 4,294,967,296. Each of the more than four billion unique addresses under the IPv4 standard was simply a combination of 32 0s and 1s such as: 00011110000101011100001111011101, or 30.21.195.221 in conventional dotted

[299] Janet Abbate, *Inventing the Internet*. The MIT Press, 1999, pp. 106-110.

[300] The original text of Queen Elizabeth's 1976 email message is found on the British Monarchy web site. (Accessed at http://www.royal.gov.uk/output/page1119.asp on July 19, 2005).

decimal notation. Four billion addresses seemed immense, but still required centralized coordination and distribution to guarantee global uniqueness for each address.

4.2 Distributing Limited Resources

If each device connected to the Internet required a globally unique address from the pool of almost 4.3 billion IPv4 addresses, some mechanism would have to provide central administration, tracking, and distribution of addresses. For years and years, a single individual, Jon Postel, performed this function. As casually noted in the RFCs documenting assigned Internet numbers in the 1970s and into the early 1980s, "The assignment of numbers is also handled by Jon."[301]

Number assignment in the context of the 1970s and 1980s was hardly controversial work. Postel worked at the University of Southern California's (USC) Information Sciences Institute (ISI), then a United States Department of Defense funded institution. Postel's activities were DARPA-sanctioned, providing some legitimacy for him to act as a central authority distributing addresses to what were then primarily American institutions. The Internet's institutional standards community made many technical and policy decisions, and within this structure, Postel had considerable stature as a respected insider and early ARPANET contributor. In addition to technical stature, experience, and DARPA-sanctioned legitimacy, Postel also had direct personal ties with others prominently involved in ARPANET development. For example, Postel and Vinton Cerf attended Van Nuys High School together in California's San Fernando Valley and were both UCLA graduate students working for Leonard Kleinrock on the ARPANET project beginning in the late 1960s. Cerf later memorialized Postel as the Internet's "North Star,"[302] and recalled, "Someone had to keep track of all the protocols, the identifiers, networks and addresses and ultimately the names of all the things in the networked universe. And someone had to keep track of all the information that erupted with volcanic force from the intensity of the debates and discussions and endless

[301] Jon Postel, "Assigned Numbers," RFC 739, November, 1977.

[302] Vinton Cerf quoted in Internet Society Press Release, "Internet Society Statement on the Death of Jon Postel," Reston, Virginia, October, 1948.

invention that has continued unabated for 30 years."[303] Postel's familiar and respected status as a technical luminary within the Internet's institutional framework, along with DoD backing, endowed him with legitimacy within his community to administer finite Internet resources.

ALLOCATING THE ADDRESSES
Jon Postel (1943-1998)

"Our Internet Assigned Numbers Authority"

Internet's "North Star"

"leader" "rock" "icon"

"Steadfast service for decades, moving when others seemed paralyzed, always finding the right course in a complex minefield of technical and sometimes political obstacles."

Quotes from Vinton Cerf (RFC 2468) 1998

Joyce Reynolds, also at USC's Information Sciences Institute, also a major contributor to the Internet RFC process and author of numerous RFCs, assumed additional day-to-day address assignment responsibility in 1983.[304] Cerf described Reynolds and Postel as functioning "in unison like a matched pair of superconducting electrons – and superconductors they were of the RFC series. For all practical purposes, it was impossible to tell which of the two had edited any particular RFC."[305] From 1983 through 1987, the network assignment RFCs instructed those wanting network numbers to "please contact Joyce to receive a number assignment."[306] The functions performed by Postel and Reynolds at the USC-ISI were called the "Internet Assigned Numbers Authority." Institutions freely obtained addresses on an as-requested basis. The primary purpose of central address distribution was to ensure the global uniqueness of each address. In the 1970s and 1980s, there were ample addresses and the possibility of exhausting the Internet address space seemed almost inconceivable.

[303] Vinton Cerf, "I remember IANA," RFC 2468, October, 1998.

[304] Joyce Reynolds and Jon Postel, "Assigned Numbers," RFC 870, October, 1983.

[305] From Vinton Cerf's entry in "30 Years of RFCs," RFC 2555, April, 1999.

[306] See RFC 870 (1983), RFC 900 (1984), RFC 923 (1984), RFC 943 (1985), RFC 960 (1985), RFC 990 (1986), and RFC 1010 (1987).

As Internet growth exponentially expanded in the late 1980s, number assignment responsibility institutionally shifted to a more formal government funded structure, the Defense Data Network-Network Information Center (DDN—NIC), sponsored by the U.S. Defense Communications Agency[307] and operated at Stanford Research Institute (SRI). Milton Mueller suggests that this shifting of assignment authority followed a Defense Department pattern. As technological systems transfer from experimental to operational, authority shifts from researchers to a military agency.[308] Mueller is correct in that the DDN-NIC distributed addresses, but, as Cerf described in RFC 1174, the IANA, meaning primarily Postel, retained responsibility and had "the discretionary authority to delegate portions of this responsibility."[309] In other words, the DDN-NIC would handle requests and provide address (and name) registration services but Postel still controlled the allocation of addresses to the NIC for further allocation or assignment. The easiest way to understand this is to differentiate between allocation and assignment. Although the terms are routinely used interchangeably, to *allocate* address space is to delegate a block of addresses to an entity for subsequent distribution to another entity. To *assign* address space is to distribute it to a single entity, such as a corporation, for actual use. The centralized entity of IANA allocated large address blocks to registry organizations like the DDN-NIC to either assign directly to end users or to allocate to ISPs for assignment to end users. This distinction between responsibility for delegating allotments of addresses to registries and the actual assignment of addresses would endure indefinitely as the DDN-NIC later transformed into the less military oriented InterNIC which transformed into the American Registry for Internet Numbers (ARIN) and various international Internet Registries. A variety of entities performed address assignment, but, more than anyone else, Jon Postel controlled address allocations. A colleague later

[307] Sue Romano, Mary Stahl, Mimi Recker, "Internet Numbers," RFC 1020, November, 1987.

[308] Milton Mueller, *Ruling the Root Internet: Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002, page 82.

[309] Vinton Cerf, "IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status," RFC 1174, August, 1990.

eulogizing Jon Postel said, "I find it funny to read in the papers that Jon was the director of IANA. Jon was IANA."[310]

Address distribution occurred outside of traditional market mechanisms of supply and demand. Milton Mueller enumerates five possible methods of distributing resources, including the resources of Internet names and numbers:

❒ First-Come/First-Served

❒ Administrative Fees

❒ Market Pricing

❒ Administrative Rules

❒ Merit Distribution.[311]

First-come/first-served describes early entrants acquiring whatever resources they request or claim, such as a parking space. The administrative fees approach, often in conjunction with first-come/first-served, imposes a price on resources to prevent massive hoarding of finite resources. Allocation based on market pricing allows price to reflect demand, the economic value of the resource, and the extent to which the resource is scarce. Using this method, those wanting IP addresses would purchase the quantity they required at market price. Allocative approaches could also impose administrative rules to ration resources, such as imposing a maximum allowable per user allocation or requiring organizations to demonstrate need prior to allocation. Finally, merit distribution, somewhat of a subset of the administrative rules approach, would allocate resources based on highly subjective merit assessments.

In the case of IP addresses, the IETF/IAB standards community determined how addresses should be packaged for distribution and who should receive how many of these technical resources. In the initial two decades of address distribution, addresses were received on a first-come/first-served basis. Administrative decisions determined several additional address distribution characteristics which would ultimately impact the issue of address space exhaustion: addresses would be allocated in large blocks; once distributed, these resources would become the irrevocable property of the recipient organization; the

[310] Danny Cohen, "Working with Jon, Tribute delivered at UCLA, October 30, 1998," RFC 2441, November, 1998.

[311] Milton Mueller, *Ruling the Root Internet: Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002, pp. 24-25.

resources would be virtually free (until 1997 when U.S. subsidization of the assignment function ceased); and large American research institutions and corporate entities requesting addresses would receive an asymmetrically large quantity of addresses relative to demand for Internet connectivity. The following sections describe how emerging IP address constraints were not purely a mathematical limitation relative to demand but an administratively imposed limitation influenced by institutional decisions about an Internet "class system" and based on massive, irrevocable, allocations of addresses to those American institutions involved as early users and developers.

4.3 Initial Internet Address Constraints

Mathematically, IPv4 provided almost 4.3 billion addresses, but several administrative and technical decisions about the composition and distribution of addresses constrained the actual number of available addresses and therefore the number of devices able to connect to the Internet.

The Internet Class System

The IPv4 specification defined a 32-bit address as consisting of two distinct domains, a network prefix and a host number.[312] Recall that the first address segment, the network prefix, would represent the network to which a destination computing devices was attached. The second part, a host number, would identify a specific computing device, called a "host" in 1980s network parlance. For example, the first 16 bits of an Internet address could designate a specific network, and the final 16 bits represent various hosts on that network. The IANA would provide a unique network number to an Internet user institution, which would then discretionarily assign the host numbers associated with that network number to devices on the network. This hierarchical concept did not significantly differ from the conventionally layered approach of postal addresses. For example, a typical street address contains a six layer hierarchy: country, zip code, state, city, street, and house number. This hierarchical structure simplifies the routing process. Intermediate postal centers need only scan a zip code to determine how to route a letter. Analogously, an Internet router need only scan the network prefix to make routing

[312] Jon Postel, Editor, "DoD Standard Internet Protocol," RFC 760, January, 1980, page 7.

decisions. Only when a postal letter or Internet packet reaches the zip code or network destination is it necessary to process local information such as street address or host IP address. Routers rely on routing tables to decide where to forward packets, and the hierarchical network/host address structures eliminated the requirement for routing tables to include every address component, conserving storage and processing resources.

This IPv4 address division into network prefix and host number underpinned the Internet class system and set constraints on how many host addresses a single institution could receive. Rather than an individual organization requesting an *ad hoc* number of addresses, the network/host address division necessitated that an institution receive a network prefix address accompanied by the fixed number of host addresses associated with that prefix. The Network Working Group anticipated that some organizations would require large blocks of host addresses while some might only require a small number of addresses. Accordingly, they divided IPv4 address blocks into 5 categories: Class A, B, C, D, and E. Class D and E addresses were reserved for multicast[313] applications and experimental uses, rendering those address blocks unavailable for general user assignment.

Rather than requesting a specific number of addresses, institutions would receive a block of addresses according to whether the assignment was designated Class A, B, or C. Recalling that each IPv4 address contained a total of 32 bits, a Class A designation divided addresses into a 7-bit network prefix ((within the first octet, the highest order (i.e. leftmost) bit was set to 0)) and a 24-bit local, host address. This address structure would allow for a theoretical total of 128 blocks of Class A networks (2^7), with each network supporting approximately 16 million (2^{24}) computers.[314] In other words, only 128 organizations could receive large Class A blocks of IP addresses. Another class, called Class B address blocks, would include a 14-bit network number and a 16-bit local address, with the first two bits set to 1-0. This allowed for 16,384 (2^{14}) Class B address blocks, each supporting approximately 65,000 (2^{16}) computers.[315] Finally, organizations could also receive a Class C address assignment, which set the first three address bits to

[313] Multicast is the ability to transmit to all IP-addressed computers on a network or subnetwork, usually for autoconfiguration.

[314] 2^{24}=16,777,216.

[315] 2^{16}=65,536.

1-1-0 and allocated a 21-bit network number and an 8-bit local address. This would theoretically allow for 2,097,152 Class C networks (2^{21}), each providing only 256 addresses (2^{8}).

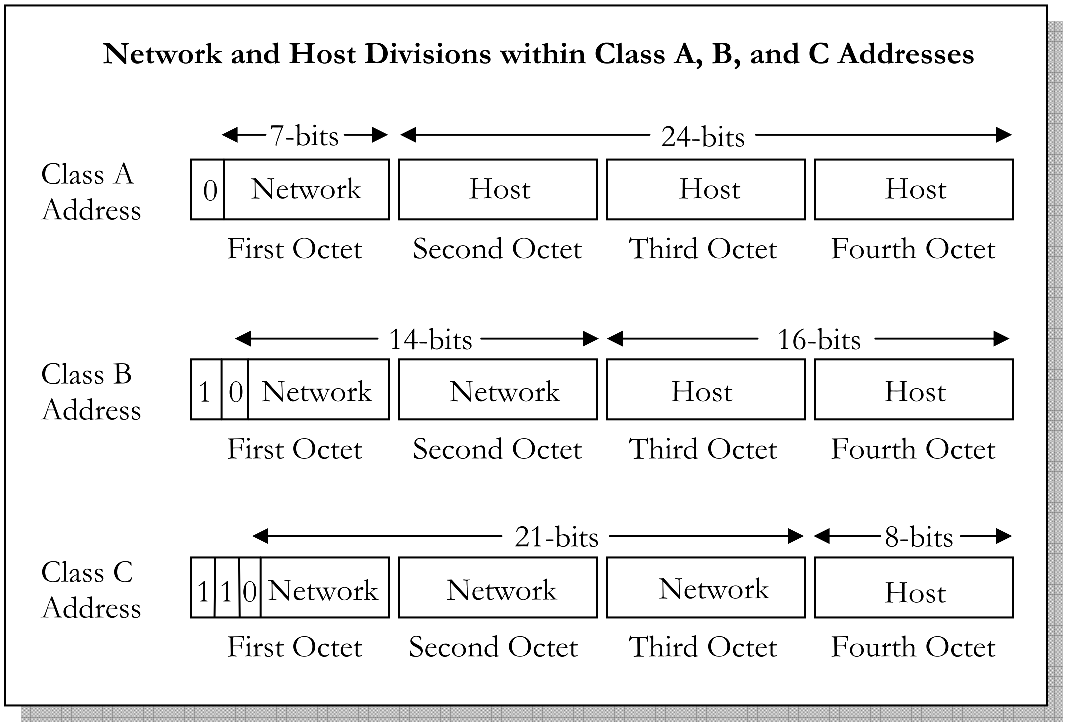


FIGURE 2: NETWORK AND HOST ADDRESS DIVISIONS

The diagram above depicts the network and host division of a Class A, B, and C address. The rationale behind this class system assumed that few organizations would require more addresses than a Class C address block provided. In the 1980s context, it was not readily conceivable that many organizations would require as many as 256 addresses, so the more than two million available Class C networks seemed sufficient. RFC 1117, "Internet Numbers," documents a snapshot of the assigned Class A, B, and C Internet address assignments in the 1980s and describes the binary structure of the address classes.[316] The following table summarizes the number of available Class A, B, and C address blocks and the number of local, or host, addresses supported by each block:

[316] Sue Romano et. al., "Internet Numbers," RFC 1117, August, 1989.

TABLE 3: CLASS A, B, AND C INTERNET ADDRESSES

Type of Address Block	Number of Available Blocks	Number of Assignable Host Addresses Per Block
Class A	128	16,777,216
Class B	16,384	65,536
Class C	2,097,152	256

The hierarchical structure and class system of Internet addresses immediately decreased the theoretical maximum number of available addresses. Communications protocol developer, Christian Huitema,[317] was among those within the Internet standards community who analyzed issues of maximum theoretical address availability.[318] Most obviously, the mathematical maximum of 4.3 billion decreased because Class D addresses were reserved for multicast applications and Class E addresses were reserved for experimental uses. The number of reserved Class D and E addresses totaled 536,870,912. Eliminating these addresses from the theoretical maximum reduced the number of available addresses from roughly 4.3 billion to just under 3.8 billion. Two entire Class A address blocks, 0 (null network) and 127 (loopback) were made unavailable for general allocation, eliminating 33,554,432 additional addresses from allocation availability. Decisions about allocating class resources created this diminishment of available addresses, but the real impact of the class system was that it ensured the allocation of often unnecessarily enormous blocks of addresses to some institutions. As discussed subsequently, many of these institutions did not require or use the majority of addresses allocated to them. In other words, these allocated addresses were unused yet rendered unavailable for eventual distribution to others.

[317] Huitema has worked at CNET (Centre National d'Etudes des Telecommunications), INRIA (Institut National De Rechereche En Informatique Et En Automatique), Bellcore, and Microsoft and has been an active member of the Internet Architecture Board and Internet Society. (Information found on http://www.huitema.net/bio.asp on October 21, 2005).

[318] Christian Huitema, "The H Ratio for Address Assignment Efficiency," RFC 1715, November, 1994.

Address Assignment Inefficiency

Address assignment inefficiency and asymmetry significantly constricted the available IP address space. The class system allowed for assigning more than 2,000,000 organizations Class C address blocks with 256 addresses each. By the late 1980s, many institutions did not yet require 256 addresses but anticipated they would at some future time. A tendency among organizations was to request Class B address blocks providing 65,536 IP addresses rather than a small Class C address block of 256 IP addresses. Although the term "hoarding" is probably excessive, this planning for future growth resulted in organizations using a relatively small number of their Class B addresses and leaving the rest unused, yet unavailable for other users. If an organization with a Class B assignment actively used 1000 Internet addresses, 64,536 addresses would remain dormant and unavailable. A much greater allocative inefficiency ensued among institutions with Class A allocations. Even a large corporation connecting a then-exorbitant 10,000 devices to the Internet would result in 16,767,216 addresses unused and unavailable. Rather than requesting an *ad hoc* number of addresses supporting current requirements and anticipating future growth, such as 30,000 addresses, organizations would have to request a paltry 256, a large block of more than 65,000, or a massive block of more than 16 million addresses. The primary rationale for the Internet class system was consideration of router table sizes, but built into the structural characteristics of the Internet class system was the potential for allocative inefficiency and stockpiling of superfluous addresses.

The historical relationship between the number of addresses distributed and the number of addresses actually used demonstrates this inefficiency. In 1981, according Stanford Research Institute's statistics immortalized in the RFC system, the Internet supported 213 hosts. The following table[319] provides a snapshot of the Internet's scope during the 1980s:

[319] Statistics on the number of Internet hosts from "Internet Growth (1981-1991)," RFC 1296, January, 1992.

TABLE 4: INTERNET HOST STATISTICS, 1981-1989

Year	**Number of Hosts on Internet**
1981	213
1982	235
1983	562
1984	1,024
1985	1,961
1986	5,089
1987	28,174
1988	56,000
1989	159,000

The majority of hosts used a single IP address (though some had multiple IP addresses), so the table provides an approximate, though somewhat underestimated, indication of the demand for IP addresses during the 1980s. What was the relationship between the number of hosts connected by the Internet and the number of addresses already assigned? At the time, SRI's NIC maintained statistics about both the number of Internet hosts and the number of assigned addresses.

If the Internet connected 159,000 hosts in 1989, as reported, and if most of these hosts required a single unique IP address, then at least 159,000 addresses should have been allocated at that time. According to 1989 NIC records,[320] large universities, defense agencies, and corporations already held 33 Class A address blocks, 1500 Class B address blocks, and numerous Class C addresses. The assigned Class A address assignments alone expended more than 500 million IP addresses. The Class B assignments exhausted a pool of more than 100 million.

In other words, in 1989, there were approximately 159,000 computers connected to the Internet and more than 600 million addresses assigned, or a ratio of almost 4,000 addresses assigned per Internet host. A substantial reason for this titanic address to host ratio, as mentioned, was the structural design of the Class A, B, and C address blocks, intended to save router processing requirements but mathematically exhausting enormous, unused blocks of IP addresses.

An ancillary explanation for some of this high address to host ratio was that, in the late 1980s, many corporations operated private TCP/IP networks disjoint from the

[320] Sue Romano, Mary Stahl, Mimi Recker, "Internet Numbers," RFC 1117, August, 1989.

broader public Internet. These networks required IP addresses. Institutions operating private TCP/IP networks could have implemented any IP numbering scheme, as long as the numbers were unique within each private network environment, but corporations frequently sought globally unique IANA assignments, presaging a future interconnection of their private TCP/IP networks to a public network or to other private TCP/IP networks operated by business partners, customers, or suppliers. Using these globally unique, assigned addresses would allow corporations later connecting to the public Internet to avoid the cumbersome task of renumbering networks.

Initial Allocation to U.S. Institutions

Additionally, the principal recipients of the technologically-derived resource of IP addresses in the 1970s and 1980s were American institutions: universities, government agencies, corporations, and military networks. The RFCs divided address recipients into four categories: research, government agency, commercial, and military. Many holders of large Class A address blocks were organizations involved in the early development and use of ARPANET technologies, such as BBN, UCLA, Stanford, and a variety of defense agencies. By the late 1980s, the large address holders expanded to include then-dominant technology corporations like IBM, DEC, HP, and Xerox; prominent universities; and a variety of defense and governmental agencies and commercial networks.

TABLE 5: SELECTED CLASS A ADDRESS HOLDERS (1989)

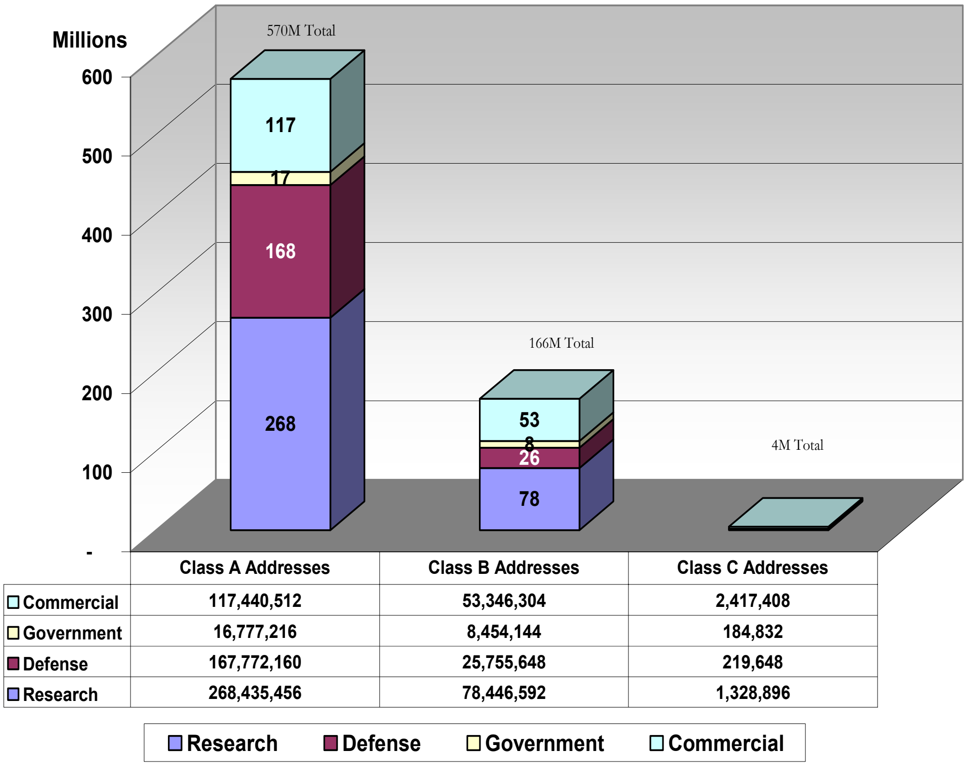
1989
SELECTED* INSTITUTIONS WITH
16+ MILLION INTERNET ADDRESSES

❑ AT&T Bell Labs
❑ Bolt Beranek and Newman
❑ DoD Intel Information Systems
❑ Defense Data Network
❑ General Electric Company
❑ Hewlett-Packard Company
❑ International Business Machines
❑ MILNET
❑ Massachusetts Institute of Technology
❑ SRI International
❑ Stanford University
❑ University of California Los Angeles
❑ Xerox Corporation
❑ Yuma Proving Grounds

* Appendix B Documents the Complete List of Allocations

A few non-American institutions from Great Britain, Canada, and Japan held Class A address blocks by the late 1980s, but the vast majority of address holders were American. Of the addresses already distributed by 1990, approximately 80% were held by government, military, and research institutions and roughly 20% were held by American corporations.[321] The following diagram, derived from raw numbers published in RFC 1166 (July, 1990), offers an address distribution snapshot by address class and institution type.

1990 Internet Address Distribution



	Class A Addresses	Class B Addresses	Class C Addresses
Commercial	117,440,512	53,346,304	2,417,408
Government	16,777,216	8,454,144	184,832
Defense	167,772,160	25,755,648	219,648
Research	268,435,456	78,446,592	1,328,896

FIGURE 3: INTERNET ADDRESS DISTRIBUTION BY CLASS AND INSTITUTION TYPE (1990)

The chart illustrates several characteristics of relatively early IP address distribution. First, the majority of assigned addresses were part of large, Class A address blocks, many distributed in the 1970s and 1980s to institutions involved in early Internet use and development. Second, research institutions, government agencies, and military

[321] Percentages calculated from the address allocation data published in RFC 1166: Sue Kirkpatrick, et al., “Internet Numbers,” RFC 1166, July, 1990.

networks received the bulk of address allocations. Corporations controlled only 23% of address assignments, and many of these were for private TCP/IP networks rather than public Internet connectivity.

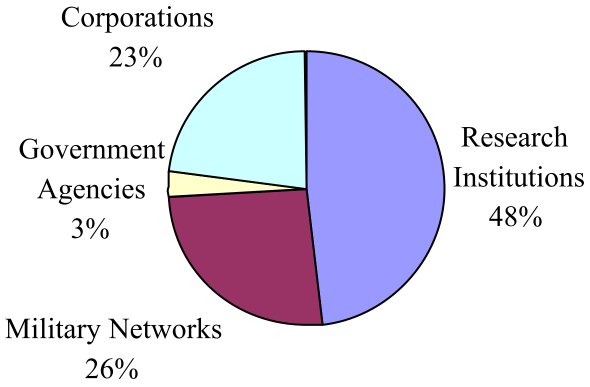


FIGURE 4: ADDRESS DISTRIBUTION BY INSTITUTION TYPE (1990)

Finally, the numerical data prefigured a problem which would later surface: a paucity of unassigned Class A and B address blocks. Comparing the 1990 data from RFC 1166 with the theoretical maximum number of Class A, B, and C addresses, in 1990, fewer than 1% of Class C addresses were distributed but 27% of Class A addresses and 15% of Class B addresses were already assigned. The Internet had experienced rapid growth by the close of the 1980s, but clearly supported relatively few hosts relative to the number of Internet addresses already assigned. Despite the relatively small number of hosts, institutions held more than 600 million addresses - all prior to the World Wide Web, rapid international growth, home Internet access, or widespread corporate connectivity to the public Internet.

4.4 The Debate over Address Scarcity

IPv6 promoters have consistently invoked IP address space exhaustion and historical address allocation inequities between United States institutions and other countries as underlying rationales for upgrading. One highly reproduced description of address inequity has noted that Stanford University controls more IP addresses than the Peoples Republic of China. Stanford University was one of the institutions apportioned a Class A block of more than 16 million Internet addresses prior to 1980.[322] In addition to its Class A assignment, Stanford also controlled four Class B networks, providing approximately 250,000 addresses. In the late 1990s, however, the University voluntarily relinquished its 16 million plus Class A addresses to the IANA and completed a renumbering of its network addresses[323] by mid 2000. This renumbering process required a laborious conversion of more than 50,000 network devices from numbers within its Class A allocation to numbers from its four class B network address blocks. Prior to 2000, China held the equivalent of a Class A address block, or 16,777,214 addresses, indeed fewer than Stanford controlled before its decision to voluntarily relinquish addresses. China steadily requested and received additional addresses, increasing to a number equivalent to more than four Class A blocks, or roughly 67 million addresses, by 2004. By mid 2000, therefore, the address comparison between Stanford University and the People's Republic of China was no longer current.

Despite this, years after Stanford relinquished its Class A address block and China received additional address allocations, a prolific IPv6 justification in government policy documents, at conferences, and in articles, remained the "statistical fact" that Stanford University controlled more IP addresses than China. Literally hundreds upon hundreds of articles reproduced this assertion. Mainstream technical journals such as *IEEE Computer* have erroneously referenced the outdated comparison.[324] *Business Communications Review* suggested that "Stanford University is assigned more IPv4 addresses than the entire nation of China."[325] Silicon.com argued, in 2003, that "The whole of China has for instance been allocated just nine million global IP addresses – Stanford University alone has twice that…"[326] Politicians have likewise commandeered

[322] Jon Postel, "Assigned Numbers," RFC 770, September, 1980, page 1.

[323] Stanford University's announcement "IP Address Changes at Stanford," relinquishing its Class A address block and renumbering it network to its four Class B networks. (From announcement on the University web site accessed at http://www.stanford.edu/group/networking/NetConsult/ipchange/index on August 1, 2005).

[324] See citation in George Lawton's "Is IPv6 Finally Gaining Ground," *IEEE Computer*, August, 2001, page 12.

[325] Eric Knapf, "Whatever Happened to IPv6," *Business Communications Review*, April, 2001, pp. 14-16.

[326] Simon Marshall, "Convergence: IPv6 migration–a necessary pain?" *Silicon.com*, June 5, 2003.

this allegory to accentuate their arguments. The Stanford and China address comparison even appeared in the 2002 Commission of the European Communities' IPv6 strategy document to the European Parliament as proof of Internet address scarcity and as further justification for immediately upgrading to IPv6. The enduring mythos of the Stanford versus China address comparison illustrates how statistical "facts" cited by technology advocates, the media, and government institutions can simply be incorrect or, in this case, outdated, and supports Escobar's analysis of "how certain representations become dominant and shape indelibly the ways in which reality is imagined and acted upon."[327]

Nevertheless, Stanford's decision to relinquish addresses was not indicative of IP address redistribution trends and did not diminish historical circumstances of United States institutions controlling disproportionate percentages of IPv4 addresses. IPv6 discussions have often focused on perpetuated myths while overlooking more enduring international address asymmetry as reflected in address distribution statistics. Years after the IETF expressed concern about potential address space exhaustion, after the IETF began developing the IPv6 specifications, and concurrent to the IANA distribution of address blocks to global registries like Europe's RIPE-NCC (Réseaux IP Européens-Network Coordination Centre) and Asia's APNIC (Asia Pacific Network Information Centre), U.S. institutions continued receiving enormous blocks of unassigned addresses. Texas based Halliburton Company received a previously unallocated Class A address block in March of 1993.[328] In other words, Halliburton controlled, beginning in 1993, 1/256 of all available Internet addresses in the world. Drug manufacturer Eli Lily and Company similarly received a Class A allocation in June of 1994.[329] Prudential

[327] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, page 5.

[328] Halliburton Company received the Class A address block 034/8 in March of 1993, according to the "Internet Protocol V4 Address Space" Record on the web site of the Internet Assigned Numbers Authority. (Accessed at www.iana.org/assignments/ipv4-address-space on June 4, 2003). RFC 1466 also documents this assignment.

[329] Eli Lilly and Company received the Class A address Block 040/8 in June of 1994, according to the "Internet Protocol V4 Address Space" Record on the web site of the Internet Assigned Numbers Authority. (Accessed at www.iana.org/assignments/ipv4-address-space on June 4, 2003). RFC 1466 also documents this assignment.

Securities received its allocation of more than 16 million addresses in May of 1995.[330] Internet Service Provider, Performance Systems International (PSI), received a Class A block in September of 1994 and has subsequently retained its addresses even after declaring bankruptcy.[331] The involvement of U.S. institutions in the early days of the Internet's predecessor networks explains the initial distribution of enormous IP address blocks, but the pattern of copious resource distribution to U.S. institutions clearly continued well into the 1990s.

The same year Halliburton received more than 16 million addresses, the IANA delegated some IPv4 addresses to internationally distributed Regional Internet Registries (RIRs) such as Asia's newly formed APNIC and Europe's RIPE-NCC. The transition to a more distributed Internet registry system (though still under IANA with overall centralized address delegation responsibility) originated with the Internet Activities Board in 1990.[332] The initial IAB recommendation for a more international distribution of assignment functions arose from several circumstances – an ever growing volume of assignments, a prevailing circumstance of the U.S. government funding administrative activities supporting non-U.S. entities, and, as addressed in Chapter II, a concern for retaining architectural control of the Internet by maintaining IP and IP addresses (versus ISO standards) as a unifying architecture. Additionally, the separation of IP address distribution from the domain name registration function accompanying this administrative change would potentially keep the IP address space clear of the contentious issues confronting domain name registration. Prior to the advent of internationally distributed RIRs, the IANA at the USC Information Sciences Institute had delegated the day-to-day assignment responsibility to the then-NSF funded NIC at SRI International. In 1993, the U.S. government separated this assignment function from the defense department and shifted responsibility for address assignment (as well as domain

[330] Prudential Securities received the Class A address Block 048/8 in May of 1995, according to the "Internet Protocol V4 Address Space" Record on the web site of the Internet Assigned Numbers Authority. (Accessed at www.iana.org/assignments/ipv4-address-space on June 4, 2003). RFC 1466 also documents this assignment.

[331] The IANA IPv4 address space list published on January 27, 2005, listed Performance Systems International as still retaining the 038/8 Class A address block.

[332] Vinton Cerf, "IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet 'Connected' Status," RFC 1174, August, 1990.

name registration) to a private company, Network Solutions (NSI), whose function was called the InterNIC. As the assignment function shifted to globally distributed registries, assignment in North America eventually moved to a membership oriented, non-profit corporation called ARIN (American Registry for Internet Numbers), the Regional Internet Registry for much of the western hemisphere. With the advent of the international registry system, the centralized IANA allocated addresses to RIRs, who in turn would reallocate address space to Local Internet Registries (LIRs), National Internet Registries (NIRs), ISPs, or end user institutions. RIPE-NCC became the first international registry. Headquartered in Amsterdam, RIPE-NCC became fully operational in 1992 and received funding from membership organizations. The Asia Pacific Network Interface Centre (APNIC), based originally in Tokyo but later relocated to Brisbane, Australia, assumed responsibility for allocating addresses to approximately 50 nations in the Asia Pacific region including Japan, China, Indonesia, and Australia. According to an IPv4 address space audit the RIRs jointly conducted in 2002, APNIC controlled nine /8 address blocks (IP addresses with a fixed 8 bit prefix; providing 16,777,216 addresses). Ignoring that APNIC allocated some of these addresses for exchange points and for experimental uses, the total allocated number of IPv4 addresses for all of the Asia Pacific region in 2002 totaled approximately 151 million, or roughly 3.5% of the IPv4 address space.

China received a portion of this approximately 3.5% of IPv4 address space allocated to APNIC, as well as some other address allocations. Rather than operating Local Internet Registries (LIRs), China operated, beginning in 1997, a state NIR called China Internet Network Information Center (CNNIC), run by the Ministry of Information Industry and operated by the Chinese Academy of Sciences (CAS). From a statistical perspective, the entire Asia Pacific region controlled a number of IP addresses roughly equal to one tenth of the population of China, seemingly foreshadowing an impending shortage. In contrast, some institutional insiders suggested IP address shortage claims about China were exaggerated. Geoff Huston, APNIC's Internet Research Scientist, has debated the imminence of Internet address space depletion and has consistently suggested the IPv4 address space would last until roughly 2023.[333]

[333] Geoff Huston, "IPv4: How Long Have We Got?" *The ISP Column*, August, 2003.

"there is no imminent exhaustion or shortage of IPv4 address space"

- Geoff Huston, APNIC Internet Research Scientist, March, 2005

One of the statistical considerations Huston emphasized was that roughly 35% of the IPv4 address space was still unassigned. The IPv4 allocation record archives of the IANA support Huston's contention. Prior to June, 2005, 79 class A address blocks remained categorized as "IANA – reserved."[334] This block of reserved addresses represented 31% of the entire pool of IPv4 addresses.

Other APNIC sources have specifically suggested that claims of address scarcity in mainland China were inflated and nothing more than rumors. Nations do not receive preallocations of IP addresses based on population, Internet statistics, or any other metric, but must issue specific address requests. APNIC, in 2004, noted that China received IP addresses at a greater allocation rate than any other economy and that APNIC has not declined any address request made by China.[335] However, one explanation for China receiving all its requested allocations for IPv4 addresses, despite the obvious statistical asymmetry between the enormous population of China and the number of APNIC controlled addresses may be IPv6 itself. China has focused its development efforts on IPv6 and has been more concerned with IPv6 addresses than IPv4 addresses.

Both IPv6 and IPv4 addresses had to be globally unique. Postel had derived credibility to centrally oversee these resources from his trusted insider status and U.S. government funding. The RIR system was obviously too expansive to garner legitimacy through personal networks of trust. Most of the newly formed RIRs were also non-governmental organizations funded, generally, by membership rather than governments. Those involved in the RIR system believed "it maintains its legitimacy and relevance by firmly adhering to open, transparent, participatory decision-making processes."[336]

[334] Internet Protocol v4 Address Space records available at www.iana.org, updated June 30, 2005.

[335] Paul Wilson and Chris Buckridge, "IP Addressing in China," appearing in Issue 12 of *Apster*, APNIC's quarterly newsletter, December, 2004.

[336] Daniel Karrenberg (RIPE-NCC), Gerald Ross (APNIC), Paul Wilson (APNIC), and Leslie Nobile (ARIN), "Development of the Regional Internet Registry System," *The Internet Protocol Journal* (undated).

Similar to the standards development process, these claims of participatory decision making and transparency seem disputable because of the potential influence of the RIR's paying corporate members and because of technical knowledge barriers to participation. Openness claims appear similarly contestable because many public Internet users are not even aware the RIR system exists.

An event which drew attention to questions about legitimately controlling the finite resources of the Internet was the formation of ICANN, the Internet Corporation for Assigned Names and Numbers, and the folding of the IANA function under this umbrella. In 1998, the Clinton administration issued a white paper calling for the creation of a private, non-profit corporation to administer the Internet's domain name system (DNS), a hierarchical, distributed database translating between domain names and IP addresses. As this project addresses, Internet device connections under the IPv4 standard have a 32-bit IP routing address (e.g. 151.196.19.22). They may also have a human readable alphanumeric address (e.g. cnn.com). Like addresses, names must be globally unique to avoid collisions or Internet fragmentation and a central tracking authority maintains this uniformity. ICANN, consistent with Postel's original responsibilities, would provide the following functions:

1) Set policy for and direct allocation of IP number blocks to regional Internet number registries;
2) Oversee operation of the authoritative Internet root server system;
3) Oversee policy for determining when new TLDs are added to the root system; and
4) Coordinate Internet technical parameter assignment to maintain universal connectivity.[337]

Centralized control of the IP address space (both IPv4 and IPv6) fell squarely under the purview of ICANN. Milton Mueller provides a detailed analysis of the institutional formation and ongoing controversy over ICANN in *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002). Mueller describes the instrumental role Jon Postel and his close associates played in ICANN's formation, how the ICANN structure was built around the existing IANA, and how informal networks, in many ways, trumped the objective of participatory oversight. The technical coordination functions

[337] United States Department of Commerce, National Telecommunications and Information Agency, *Management of Internet Names and Addresses*, June 5, 1998. (Accessed at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm on August 12, 2003).

assigned to ICANN, especially pertaining to domain names, had significant policy repercussions in areas like intellectual property and privacy, effectively rendering ICANN a policy setting organization. For example, is www.microsoftsucks.com constitutionally protected speech? Who should own www.united.com, United Van Lines or United Airlines or another entity? Which domain names should be censored as pornographic given internationally disparate cultural norms? Critics, including those inside ICANN, have noted that, as a private entity, ICANN lacked the requisite legitimacy to make these decisions. Professor Hans Klein of the Georgia Institute of Technology divided these policy issues into four categories: intellectual property, free speech, privacy, and competition policy/antitrust.[338] Reform efforts have advocated bolstering ICANN's legitimacy by making it a representative entity with formal accountability to the Internet community through international government participation. To emphasize the degree of dissatisfaction about ICANN's inability to satisfactorily manage the Internet's domain name system, the most compelling indictments emanated from ICANN insiders like former chair Esther Dyson, who submitted a Wall Street Journal op-ed piece pronouncing that "ICANN is weak and powerless" and "suffers from a flawed decision-making structure."[339] Departing president and reform advocate, Stuart Lynn, described ICANN's trajectory in 2002 "a bleak picture"[340] and concluded that any private entity attempt to incorporate consensus was intractable.

Regardless, centralized control of the IP address space fell under the jurisdiction of ICANN employees such as Doug Barton, appointed General Manager of IANA in 2003.[341] Barton was formerly a Yahoo! employee and had been active in the IETF protocol process. Consistent with the history of Internet insiders straddling multiple governance and technical institutions and retaining direct authority over the Internet's technical and policy directions, some of ICANN's directors were also directly involved in

[338] Professor Klein, George Institute of Technology, presented these policy issues at the *Public Voice in Internet Policy Making Symposium*, Washington, D.C., June 22, 2002.

[339] Esther Dyson, Op-Ed Appearing in the Wall Street Journal, June 17, 2002.

[340] Stuart Lynn, ICANN, *President's Report: ICANN – The Case for Reform*, February 24, 2002. (Accessed at www.icann.org/general/lynn-reform-proposal-24feb02.htm on July 1, 2002).

[341] "ICANN Announces Appointment of General Manager, IANA," November 10, 2003. (Accessed at http://www.icann.org/announcements/announcement-10nov03.htm on December 15, 2005.)

the development, selection, and promotion of IPv6. For example, Vinton Cerf served as ICANN's chairman of the board as well as the founding president of the Internet Society, IAB member, and honorary chairman of the IPv6 Forum dedicated to the promotion and adoption of IPv6 throughout the world. Steve Crocker served as Chair of ICANN's Security and Stability Committee. Former IAB chair, Lyman Chapin, also served on the ICANN board, as did Steve Deering, the developer of the SIPP protocol selected as the new IPv6 standard.

Most Internet governance controversies have historically addressed domain names, a more visible and comprehensible resource than IP addresses. Numerical IP addresses circumvent the obvious privacy, free speech, and antitrust policy questions concerning domain names. The user transparency of IP addresses also contrasts direct user engagement with domain names. However, there exists an infinite number of possible domain names and a finite number of IP addresses (under both IPv4 and IPv6). The history of IP address space constraints as a common rationale for upgrading to IPv6, involved not only scarcity claims but also unresolved questions of power and legitimacy for various entities to control finite Internet resources. Years before the formation and controversy over ICANN, the IAB identified a need for greater internationalization of Internet resources. Even after the formation of the international registry systems, legitimacy issues remained unresolved, including the primacy of ICANN, viewed primarily as an American institution because of U.S. Commerce Department oversight, to retain centralized global control of the address space, and the legitimacy of RIRs, funded by interest-driven membership, to regionally distribute addresses.

4.5 Address Conservation Controversies

Another question in the history of IP addresses involved the urgency of address depletion concerns given the availability and widespread implementation of a technical measure, Network Address Translation (NAT), designed to conserve addresses and the deployment of Classless Inter-Domain Routing (CIDR) beginning in 1994 and 1995. The Internet Class System for IPv4 addresses assigned addresses in Class A, B, or C increments of roughly 16,000,00 addresses, 65,000 addresses, or 256 addresses, respectively. As discussed earlier, this hierarchical system, designed in part to minimize router processing overhead, resulted in highly inefficient address distribution patterns such as a single corporation possessing 16,000,000 addresses but only using 20,000. The IETF engineered CIDR[342] to make address assignments less wasteful and to promote routing efficiency. As the IETF RFC describing the rational for CIDR explained:

> *"The IP address space is a scarce shared resource that must be managed for the good of the community. The managers of this resource are acting as its custodians. They have a responsibility to the community to manage it for the common good."*[343]

In short, CIDR eliminated the Class A, B, and C address distinctions to promote more flexible and efficient allocations of IPv4 addresses. Additionally, CIDR offered route aggregation whereby a single router table entry could represent thousands of address routes. This type of aggregation reduced the number of decisions for each router, in turn reducing processing time and router table size. Each packet of information to be routed would contain a prefix-length, often referred to as a *bit mask*, notifying the router of the length of the network prefix it should read. This CIDR approach enabled routers to read all bit sizes of network addresses rather than the fixed 8-bit, 16-bit, or 24-bit network numbers under the Internet class system.

In addition to CIDR, and in addition to recommending a distribution of available IP addresses to international Internet registries, the IETF introduced address translation in the early 1990s[344] to stave off potential resource depletion. NAT techniques allowed a network device, such as a router, to employ limited public IP addresses to mediate between a private network with many unregistered (fabricated) IP addresses and the public Internet. As an oversimplified example, a single publicly unique address could serve a local area network of twenty computers. When a computer on a private network accesses the public Internet, the NAT device dynamically allocates a globally unique, temporary IP address the computer uses for transmission. When the same computer transmits to devices within the private network, it uses a private, non-globally unique address. In this regard, network address translation conserves addresses by allowing numerous devices to share public IP addresses. The technique has also enabled some

[342] RFCs 1517, 1518, and 1519 document the Classless Inter-Domain Routing approaches.

[343] Yakov Rekhter and Tony Li, "An Architecture for IP Address Allocation with CIDR," RFC 1518, September, 1993.

[344] Kjeld Egevang and Paul Francis, "The IP Network Address Translator," RFC 1631, May, 1994.

institutions with a large installed base of private IP addresses to connect to the Internet without laboriously converting entire networks from private (not IANA assigned) addresses to public IP addresses.

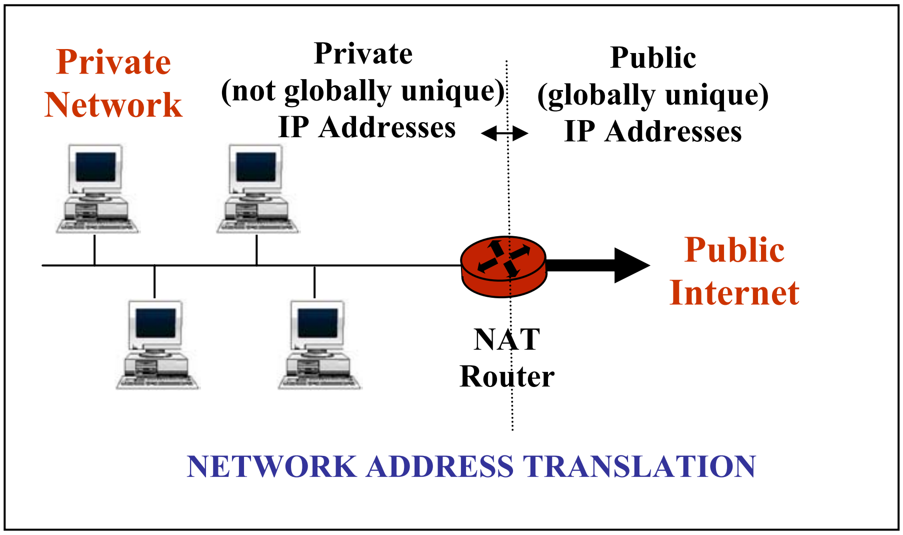

Private Network
Private (not globally unique) IP Addresses
Public (globally unique) IP Addresses
Public Internet
NAT Router
NETWORK ADDRESS TRANSLATION

FIGURE 5: NETWORK ADDRESS TRANSLATION

Despite its origination in the IETF, many in the Internet's standards setting community ardently criticized increased NAT usage because it violated the architectural philosophy, the "end-to-end" principle, which had underpinned the Internet (and precursor networks) since its inception. Internet engineers first articulated the end-to-end philosophy in the mid-1980s.[345] The architectural principle responded to a design question about where to place intelligent functions within a communications network. Some of these functions included congestion control, error detection and correction, encryption, and delivery confirmation. Internet engineers in the 1980s decided these functions should reside at network endpoints rather than *in medias res*. Under this design philosophy, network routers would only transmit packets as expeditiously as possible to their destinations, with all other functionality performed in the fringes, for example in applications. The IAB, in 1996, attempted to summarize Internet architectural principles and devised three general philosophies: the objective of the Internet is global

[345] An articulation of the end-to-end architectural philosophy appears in two mid-1980s papers: John Saltzer et. al, "End-to-End Arguments in System Design," ACM TOCS, Volume 2, Number 4, November, 1984, pp. 277-288; and Dave Clark, "The Design Philosophy of the DARPA Internet Protocols," Proceedings of SIGCOMM 88, ACM COR Volume 18, Number 4, August, 1988, pp. 106-114.

connectivity; the means for network level connectivity is the Internet Protocol; and intelligent functions should reside at end points rather than within networks.[346] This design philosophy significantly contrasted prevailing network approaches which established temporary fixed paths, or virtual circuits, between end points that remained fixed for the duration of a transmission. Part of the rationale for the end-to-end design was to allow applications to continue working in the event of a partial network failure.

Acknowledging that "Internet standards have increasingly become an arena for conflict," the IAB expressed reservations about translation intermediaries like NAT.[347] Intermediary devices reduced the need for a single network protocol, IP, and would "dilute its significance as the single necessary feature of all communications sessions. Instead of concentrating diversity and function at the end systems, they spread diversity and function throughout the network."[348] The standards community feared that translation techniques would challenge older, dominant protocols and would create myriad network protocol choices for users. Ironically, the original rationale for the end-to-end philosophy has evolved among some IETF quarters to include concern about "preserving the properties of user choice."[349] This argument that the end-to-end philosophy preserved user choice directly contradicted the same institution's contention that translation techniques diminished protocol homogeneity and allowed imprudent multiprotocol complexity.

As noted earlier, many IETF participants had become involved in Internet standards development when the network connected a relatively homogeneous group of trusted insiders. The philosophical climate in this environment was antithetical to later Internet environments of widespread public and global access, identity theft, worms, denial of service attacks, and other security challenges. Institutional and individual Internet users, in practice, repudiated the prevailing values of the standards community, instead routinely embracing intelligent intermediaries violating the end-to-end

[346] Brian Carpenter, Editor, "Architectural Principles of the Internet," RFC 1958, June, 1996.

[347] James Kempf and Rob Austein, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture," RFC, 3724, March, 2004.

[348] Brian Carpenter, "Middleboxes: Taxonomy and Issue," RFC 3234, February, 2002, page 2.

[349] James Kempf and Rob Austein, eds., "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture," RFC, 3724, March, 2004.

architectural principle. By 2000, network intermediaries, or "middleboxes," like security firewalls and translation devices became fairly widespread among U.S. businesses and individual Internet users. [350] IETF participants have expressed divergent and fervent opinions about the efficacy and prudence of using network address translation and other intermediaries. Some IETF participants argued that the interruption of protocol formats within networks would actually reduce the ability of users to implement security techniques, like encryption, which are specifically applied at end points. Others proclaimed NAT as the obvious remedy for address exhaustion and a potential workaround for forestalling IPv6. In contrast once again, the policy proclamations and documents mandating IPv6 usage in Asia and the EU altogether ignored the prospect of network address translation as an interim address conservation approach, instead leapfrogging to IPv6. Within the Internet standards setting community, as Microsoft's Tony Hain described in 2000, NAT discussions "frequently take on religious tones," with proponents arguing NAT staves off IPv4 address depletion and dissenters referring to it as "a malicious technology, a weed which is destined to choke out continued Internet development."[351] The phenomenon of standards as a locus of conflict is certainly supported in the history of network address translation. Some in the standards community viewed IPv6 as an avenue to minimize intermediary network technologies which disrupted the end-to-end architectural principle.

4.6 IPv6 Addresses as Grains of Sand

The history of expectations about the adequacy of the IPv6 address space has mirrored the history of expectations about the adequacy of the IPv4 address space twenty years earlier. The maximum number of Internet addresses under the IPv4 standard, approximately 4.3 billion, appeared wildly profligate in the era in which the IPv4 standard emerged but, retrospectively, seemed parsimonious because it provided less than one Internet address per human on earth. In contrast, the IPv6 standard, by specifying 128 bit addresses, theoretically provided 2^{128} unique addresses. One way to describe this enormous number is with scientific notation: the standard allows for a theoretical

[350] Tony Hain, "Architectural Implications of NAT," RFC 2993, November, 2000, page 1.

[351] Ibid.

maximum of 3.4 x 10^{38} unique addresses. Another way to describe the number uses the multiplier undecillion: the standard allows for a theoretical maximum of 340 undecillion addresses. In the American system, an undecillion is mathematically equivalent 10^{36}. To capture the number's enormity, the highly contestable Internet encyclopedia, Wikipedia, described the address size as allowing "an average of about 430 quintillion (4.3 x 10^{20}) unique addresses per square inch, or 670 quadrillion (6.7 x 10^{17}) per square millimeter, of the Earth's surface."[352] One irony in Wikepedia's entry is that it stated the address size in both the metric system and the English system, leaving one to contemplate the analogous possibility of a long term coexistence of IPv4 and IPv6 standards.

Even descriptions of the size of the IPv6 address space are contestable because of the lack of universal standards for mathematical multiplier terminology. For example, a quintillion in the American system equals 10^{18}. A quintillion in the British system equals 10^{30}. IPv6 discussions among different cultures require translation. What most cultures have agreed upon is an analogy to describe the size of the IPv6 address space. Similar to the replicated story comparing Stanford University's address pool to China's address allocation, a universal description has equated the number of IPv6 addresses with the number of grains of sand – depending on the source – on the Earth, on 300 million planets the size of the earth, or in the Sahara desert. For example, the European Commission's 2002 IPv6 strategy announcements included a reference to the size of the IPv6 address space as supporting, "more locations in cyberspace than there are grains of sand on the world's beaches."[353] The technical media has consistently used the "grains of sand" analogy to describe the IPv6 address space. Many technology vendors selling IPv6 have used this analogy. The IPv6 Forums and other IPv6 advocacy groups have routinely invoked this analogy. This description, despite the implausibility of calculating the number of grains of sand on the earth, has become one of the IPv6 justificatory stories portrayed as fact.

The "grains of sand" message from the IPv6 advocacy groups, from governments promoting IPv6, and from technology vendors selling IPv6 products conveys that IPv6

[352] Wikipedia entry.(Accessed at http://en.wikipedia.org/wiki/Ipv6 on September 12, 2005).

[353] European Commission Press Release, "Commission Takes Step Towards the Next Generation Internet," Reference IP/02/284, Brussels, Belgium, February, 2002. (Accessed at http://europa.eu.int on April 2, 2004).

provides more than a sufficient number of addresses for Internet requirements for the conceivable future. Interestingly, the Latin word for sand is *arena*, a locus of conflict and competition. But those exhorting the colossal store of IPv6 addresses have assumed the new standard would circumvent competitive tensions existing over the IPv4 address space. The argument for deploying the IPv6 standard has rested on a premise that the supply of IPv6 addresses is sufficient indefinitely. Circa 1981, no one envisioned a possible dearth of IPv4 addresses. Two decades later, IPv6 proponents appeared to not conceive of possible future constraints on the IPv6 address space.

This assumption that the Internet will never face address constraints clearly overlooks the history of the Internet itself. Scientist Leonard Kleinrock was one of the original contributors to the development of the ARPANET beginning in the late 1960s, and has a long term, insider perspective on the evolution of increasing demands on the IPv4 address space. Twenty five years after his initial ARPANET involvement, Kleinrock raised questions about the adequacy of the IPv6 address reserve. Kleinrock asked, "Why does IPv6 only have 128 bits?" He suggested that, although it seemed adequate at the time, it might "run into trouble two decades from now."[354]

The development of the RIR system sought to avoid a geographically asymmetrical distribution of addresses as historically unfolded in IPv4 address assignments. The RIRs serve large geographical areas, managing the address space allocated to them by the IANA, under ICANN, and assigning addresses within their jurisdicational regions. Recall that in registry parlance, to allocate means to disperse address space from IANA to registries for subsequent distribution. To assign indicates to delegate addresses to ISPs and/or end users for actual use by them. Two additional registries joined ARIN, RIPE NCC, and APNIC. ICANN formally recognized The Latin America and Caribbean Network Information Centre (LACNIC) as the fourth regional internet registry (RIR) in October of 2002.[355] The authority to accredit the LACNIC organization lay exclusively with the ICANN Board of Directors and Vinton Cerf, who

[354] Leonard Kleinrock, public remarks during final panel discussion at the United States IPv6 Summit, Arlington, Virginia, December, 2004.

[355] "Final Approval of LACNIC" in the Preliminary Report of the ICANN Board of Directors Meeting in Shanghai, October 21, 2002. (Accessed at http://www.icann.org/minutes/prelim-report-31oct02.htm#FinalApprovalofLACNIC on September 14, 2004).

chaired ICANN at that time. The ICANN board formally accredited a fifth RIR, the African Network Information Centre (AfriNIC) in 2005 to distribute addresses within the African and Indian Ocean regions.

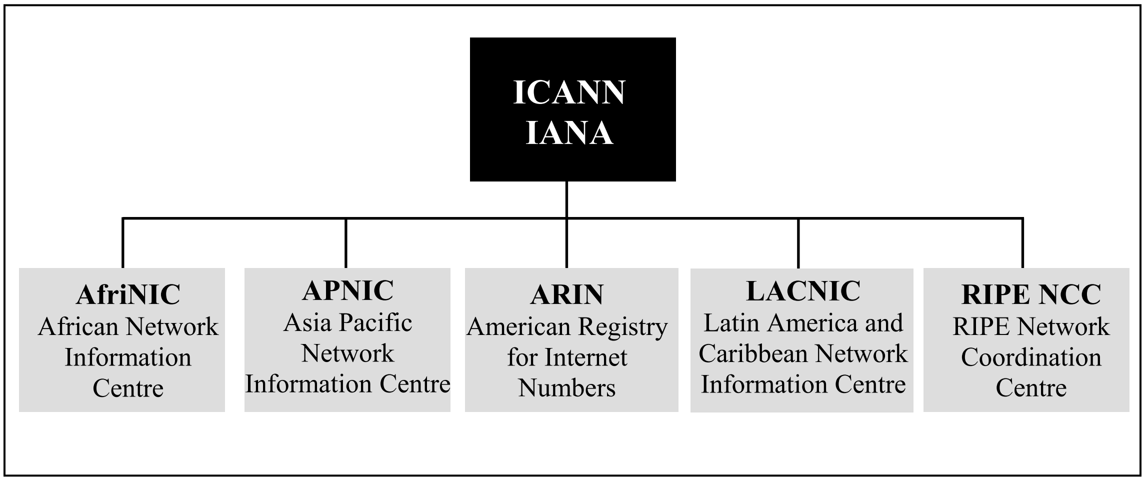

ICANN
IANA
AfriNIC
African Network Information Centre
APNIC
Asia Pacific Network Information Centre
ARIN
American Registry for Internet Numbers
LACNIC
Latin America and Caribbean Network Information Centre
RIPE NCC
RIPE Network Coordination Centre

FIGURE 6: REGIONAL INTERNET REGISTRIES CIRCA 2005

These five RIRs subsequently developed joint address registry policies establishing procedures for IPv6 address assignment.[356] The RIRs' joint registry procedures established "conservation" as one policy objective, calling for avoidance of wasteful practices and address stockpiling and requiring appropriate documentation to support all address requests.

One agreed upon RIR IPv6 principle directly contrasting earlier IPv4 practices stated "Address space not to be considered property."[357] Once an organization received IPv4 address assignments, those addresses remained, in practice, the irrevocable property of that organization, even if unused. To avoid the possibility of hoarding or languishing of unused addresses, the RIR's jointly concurred that it "is not in the interests of the Internet community as a whole for address space to be considered freehold property."[358] IPv6 addresses would be licensed rather than owned. RIRs would renew these address licenses on a periodic basis and retain the right to revoke addresses. This policy

[356] APNIC, ARIN, and RIPE NCC, "IPv6 Address Allocation and Assignment Policy," Document ID: RIPE-267, January 22, 2003.

[357] APNIC, ARIN, and RIPE NCC, "IPv6 Address Allocation and Assignment Policy," Document ID: RIPE-267, January 22, 2003, Section 4.1.

[358] Ibid, Section 4.1.

originated in the mid 1990s with the Internet Architecture Board and the Internet Engineering Steering Group, which issued recommendations for the IANA about managing IPv6 address allocations.[359] The IAB/IESG position emphasized that a central authority (IANA) responsible for allocations was a necessary precursor of "good management" of the IPv6 address space. Additionally, allocations of address space by the IANA were not irrevocable and there should continue to be no charges for addresses beyond fees to cover the administrative costs. The IAB/IESG IPv6 address management positions served not only to address how to manage the IPv6 address space but to fortify the authority and philosophies of the IAB/IESG/IETF/IAB structure. First, the IANA, under the advice of the IAB and IESG, would retain exclusive centralized control of the address space, by delegation to registries. Second, even after delegating addresses to registries, the IANA retained control because it could revoke allocations, if, in its own judgment, it believed an entity has "seriously mishandled the address space delegated to it."[360] The IAB also renewed its commitment to the "Internet is for Everyone" philosophy by fortifying a system whereby IP addresses could never be bought and sold in open markets. Everyone would have a chance for Internet resources, not just the highest bidder. The belief that IP addresses were common pool resources in the public domain served as a philosophical underpinning for positions against exchanging IP addresses in open markets. Many in the standards and registry communities believed "you cannot sell what you do not own."[361] This position preserved the power of the registries and of the centralized IANA to control the allocation and assignment of IP addresses.

4.7 Addresses Not For Sale. Price: $36,000

Despite the philosophical view of addresses as public resources which should never be exchanged in markets, IP addresses had ceased being completely free resources in the

[359] See IAB and IESG, "IPv6 Address Allocation Management," RFC 1881, December, 1995.

[360] IAB and IESG, "IPv6 Address Allocation Management," RFC 1881, December, 1995.

[361] Quote from ARIN Counsel Dennis Molloy documented in the minutes from the ARIN Members Meeting, October 16, 1998, section "Solicitations for the Purchase of Address Space." (Accessed at http://www.arin.net/meetings/minutes/ARIN_II/index.html on September 16, 2004).

mid-nineties. When ARIN was formally decoupled from the government funded Network Solutions InterNIC in late 1997, it announced it would commence charging for IP addresses, though only enough to cover the costs of its small assignment operation located in Chantilly, Virginia. ISPs accounted for a great number of IP address requests made to registries, and ARIN announced that new IP address requests would cost between $2,500 and $20,000 per year, depending on the assignment size. The registry would not charge institutions holding existing IP addresses. Corporations (or individuals) requesting new IP addresses would pay a one time fee between $2,500 and $20,000, depending on assignment size.

RIR policies have consistently and adamantly affirmed that they do not charge for IP addresses:

"IP addresses are a shared public resource and are not for sale."[362] *– RIPE-NCC*

Despite this shared public position, the RIRs have consistently charged initial allocation fees and maintenance fees for IP address allocations and assignments. The IP address fees have not varied significantly by RIR. For illustrative purposes, the following uses a snapshot of LACNIC's pricing structure to describe the initial allocation cost and the annual renewal fees for Internet Service Providers to hold various size blocks of IP addresses. Recall that after the IETF developed Classless Inter-Domain Routing (CIDR), address blocks were no longer allocated in Class A, B, and C increments but in more flexibly sized network address increments. In post-CIDR terminology, a "/20" (pronounced "slash twenty") referred to an address block with a 20-bit network number followed by 12 bits of host numbers, or a total number of IP addresses of 2^{12}, or 4,096 addresses. A "/16" referred to an address block with a 16-bit network number followed by 16 bits of host address numbers, or 65,536 addresses. The following chart describes the pricing structure of one RIR – LACNIC – to illustrate IP address charges.[363]

[362] See RIPE-NCC allocation and assignment policies available on the RIR's web site. (Accessed at http://www.ripencc.net/info/faq/rs/general.html#1 on December 22, 2005).

[363] This chart reflects LACNIC's fee schedule as of January 1, 2006.

Table 6: Sample IPv4 Address Registration Prices

LACNIC IPv4 REGISTRATION PRICE LIST

Category	Size	Initial Amount USD	Renewal Amount USD
Small/Micro	< /20	$1,000	$1,000
Small	>= /20 y <= /19	$2,000	$2,000
Medium	> /19 y <= /16	$5,000	$5,000
Large	> /16 y <= /14	$10,500	$10,500
Extra Large	> /14 y <= /11	$22,000	$22,000
Major	> /11	$33,000	$33,000

The RIRs charged these IP address registration fees to large ISPs and Local Internet Registries which would, in turn, assign addresses to end users. The cost for end users directly purchasing from RIRs (some offer end user assignments) was considerably less than prices charged to ISPs. For example, LACNIC charged an annual maintenance fee of $400 to end users. ARIN charged the same initial registration fee for ISPs and end users but would not charge the large annual maintenance fee to users. In reality, ISPs passed on registration fees to end users, so the efficacy of the RIR pricing differentiation between end users and ISPs seems debatable.

An interesting RIR fee schedule differentiation also existed between IPv4 addresses and IPv6 addresses. In 2004, AfriNIC announced that "to encourage and promote IPv6 usage and allocation in the Region, organizations which qualify to receive IPv6 allocation will have the first year's fees waived."[364] Similarly, the ARIN Board of Trustees announced it would waive IPv6 fees between January 1, 2005 and December 31, 2006. The RIR's IPv6 address policies sought both to promote IPv6 and to maintain the long term viability of the IPv6 address space through conservation strategies. Some of these conservation policies underscored the ongoing power these entities, as well as lower level registries like LIRs and NIRs would have over addresses, and raised some

[364] Adiel Akplogan, AfriNIC Fees Schedule (2004-2005), May 10, 2004. (Accessed at http://www.afrinic.net/docs/billing/afadm-fee200405.htm on December 22, 2005).

potential concerns. One concern was the possibility of address reclamation abuse such as an NIR closely aligned with a national government reclaiming (i.e. seizing) an organization's addresses to retaliate for statements critical of the government. Similarly, a user organization requesting addresses from a local Internet registry must provide justification for the request. The generality of such a policy leaves the door open for denials of address requests for almost any reason. Finally, the complete rejection of the prospect of exchanging some addresses in free markets (while charging for them) eliminates the possibility of even opening up a dialog about whether this type of exchange might serve to promote conservation rather than diminish conservation as the RIRs argued.

4.8 The ITU Seeks Greater Involvement

In October of 2004, the director of the ITU's Telecommunication Standards Sector, Houlin Zhao, formally suggested a change in IPv6 address assignment procedures. Rather than RIRs acting as regional monopolies distributing addresses, Zhao proposed that blocks of IPv6 addresses be allocated to individual countries. Then, governments would choose how to distribute addresses.[365] Entities seeking addresses could approach either the RIR or the government, producing some competition and choice in the IP address allocation system. The ITU was not proposing that ICANN/IANA directly allocate IPv6 addresses to nations. Instead, the ITU would allocate blocks of IPv6 addresses to nations, giving the ITU significant IP address responsibilities. The ITU stressed its "unique position as an intergovernmental organization.." under the United Nations[366] and the need for a legitimate governance organization responsible for resources and for establishing public policy. The ITU had traditionally established telecommunications standards and had handled such issues as radio spectrum disputes. In making his case for ITU influence on Internet governance issues, Zhao described the Internet as part of a broader existing public telecommunications infrastructure he called

[365] Houlin Zhao, ITU and Internet Governance, draft input to the 7th meeting of the ITU Council Working Group on WSIS, December, 2004. (Accessed at http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf on November 18, 2005).

[366] Ibid.

the “Next Generation Network (NGN).”[367] This subsumption of the Internet under a broader telecommunications infrastructure, rather than the inverse, would serve to bring Internet governance issues closer to ITU jurisdiction, with a constitution that described its mission “to maintain and extend international cooperation among all its Member States for the improvement and rational use of telecommunications of all kinds.”[368] The IETF had led the development of the core routing and transport protocols for the Internet, but Zhao wished to contest the notion that the ITU had historically minimal involvement in the development of Internet standards or in Internet governance and administration. Zhao argued “Some think that the ITU has no role in Internet standardization. But this is not correct.”[369] He argued that the ITU had been a “major contributor” to the Internet and Internet standards, making references to the ITU’s involvement in access standards such as ADSL (Asymmetric Digital Subscriber Line) and cable modems, and standards directly related to specific applications of Internet voice transmission such as VoIP (Voice over IP). Zhao claimed: “ITU activities have directly or indirectly, supported the technical development of Internet from the very beginning.”[370] The ITU offered another rationale for its proposed Internet oversight role. The ITU-T’s director argued that the ITU could uniquely protect and represent the interests of developing countries relative to Internet governance because the ITU had traditionally defended the interests of developing countries relative to other countries. Zhao ultimately argued that the Internet’s national importance necessitated management in each country by its national government. Furthermore, governments should play a role at the international level, an assumption presumably setting up an argument for United Nations (ITU) governance of the Internet.

[367] Houlin Zhao, ITU and Internet Governance, draft input to the 7th meeting of the ITU Council Working Group on WSIS, December, 2004. (Accessed at http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf on November 18, 2005).

[368] Mission statement from International Telecommunications Union web site. (Accessed at www.itu.int on November 17, 2005).

[369] Houlin Zhao, ITU and Internet Governance, draft input to the 7th meeting of the ITU Council Working Group on WSIS, December, 2004. (Accessed at http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf on November 18, 2005).

[370] Ibid, Section 3.3.

4.9 Enter the United Nations

A controversy over control of Internet addresses and, especially names, erupted in the summer of 2005 when Koffi Annan, Secretary-General of the United Nations announced the findings of a U.N. subgroup report proposing several Internet governance alternatives which would, in effect, place Internet governance responsibilities under the United Nations. The United Nations "Working Group on Internet Governance," or WGIG, issued the recommendations. Koffi Annan had established the WGIG in response to recommendations he received from the December, 2003 World Summit on the Information Society.[371] The group's mission was to define Internet governance, identify major policy areas, and issue recommendations for Internet governance responsibilities in these areas.

The WGIG included 40 participants representing governments, the private sector, and individuals from what the United Nations called "civil society." Many of these participants held high level governmental technology policy positions, such as Saudi Arabia's Deputy Governor of Technical Affairs for the Communications and Information Technology Commission of Saudi Arabia and Cuba's Coordinator of the Commission of Electronic Commerce.[372] The following is a partial list of the countries with governmental representatives participating in the working group deliberations:

❒ Barbados
❒ Belgium
❒ Brazil
❒ China
❒ Cuba
❒ Egypt
❒ Iran
❒ Japan
❒ Luxembourg
❒ Pakistan
❒ Russia
❒ Saudi Arabia
❒ South Africa.

United Nations Secretary-General Koffi Annan had the final authority in selecting the forty WGIG participants. The United States chose not to contribute a government

[371] The first phase of the World Summit on the Information Society was held in Geneva, Switzerland on December 10-12, 2003.

[372] The complete list of participants appears in the Annex of the WGIG's Report of the Working Group on Internet Governance, Chateau de Bossey, June, 2005. Also see the United Nations Press Release, "United Nations Establishes Working Group on Internet Governance," PI/1620, November 11, 2004. (Accessed at http://www.un.org/News/Press/docs/2004/pi1620.doc.htm on November 11, 2004).

representative to participate in the WGIG.[373] Governments with patently undemocratic and oppressive Internet governance policies were prominently involved in establishing Internet governance recommendations. Additionally, countries with notoriously undemocratic Internet governance policies, such as Iran, China, Cuba, Saudi Arabia, and Egypt, were overrepresented in this working group. Other participants were affiliated with a variety of commercial entities, a few academics, ICANN, the World Bank, and the ITU. No WGIG participants represented the U.S. Government, any U.S. corporation, any organization involved in establishing standards for the Internet's routing and addressing protocols or domain name system, or any leading private sector vendors (U.S. or otherwise) involved in developing the products which incorporate Internet standards and policies. In other words, the United Nations group appeared to not adequately include the input of Internet users, Internet vendor, or anyone technically involved in the systems underlying the policy areas the group addressed.

One of the charges of the WGIG was to define "Internet governance." After a lengthy exercise, the group settled on the following definition:

> *"Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."*[374]

On the surface, the WGIG's definition of Internet governance seemed so broad as to be dismissed as a non-definition. However, the definition conveyed some distinct Internet governance positions. The definition assigned an Internet governance role to "governments," setting up potentially greater involvement of nations in taking over Internet governance. Second, the definition assumed the existence of shared principles and norms in Internet policies. This assumption was not reflective of the political approaches to Internet governance among nations represented on the WGIG. The

[373] Ambassador David Gross, U.S. Coordinator for International Communications and Information Policy in the Bureau of Economic and Business Affairs, explained that the United States Government did not participate in the WGIG because of "serious legal issues (under U.S. law) that such participation could have raised," in a State Department live Internet chat answering questions about the forthcoming WSIS summit in Tunis, November 2, 2005.

[374] Report of the Working Group on Internet Governance, Chateuau de Bossey, June, 2005. (Accessed at http://www.wgig.org/docs/WGIGREPORT.pdf on August 8, 2005).

Internet governance principles and norms in Egypt, Cuba, China, Saudi Arabia, Pakistan, and Tunisia, hardly resembled those of France, Brazil, and Switzerland in areas such as censorship, freedom of expression, privacy, surveillance, intellectual property, and Internet trade taxation. Finally, the WGIG definition of Internet governance itemized three entities – government, the private sector, and civil society – as responsible for Internet governance. The definition did not specifically categorize technical and academic communities, historically influential in Internet governance roles such as standards setting. The presumed, tacit, grouping of organizations such as the Internet Engineering Task Force in the broad "civil society" category, listed less prominently than "governments," seemed to intimate a diminished role for technical communities.

The WGIG identified the following Internet governance policy issues: management of Internet resources (including IP addresses); network security; intellectual property and international trade; and Internet deployment in developing countries. Within these policy priorities, the highest priority for the WGIG was to address "unilateral control by the United States Government" in administering the root zone files of the Domain Name System. The WGIG also identified IP address allocation equitability by geographic area as a concern.

After developing its definition of Internet governance and identifying some specific Internet governance policy areas, the WGIG attempted to address who should assume responsibility in various areas. An overall WGIG conclusion asserted that there currently existed a "vacuum within the context of existing structures, since there is no global multi-stakeholder forum to address Internet-related public policy issues."[375] The group determined that, in the forum that would fill this vacuum, no single government would have the ability to unilaterally act. The U.N. WGIG's emphasis on diminishing the dominance of the United States and eliminating unilateralism seemed reflective of contemporaneous U.N. criticisms of what it described as United States unilateral action in the U.S. led war in Iraq. The alternatives of multilateral Internet governance the WGIG explored involved, among other things, wresting the control of IP addresses from the

[375] Report of the Working Group on Internet Governance, Chateuau de Bossey, June, 2005, Section V.A.1.40. (Accessed at http://www.wgig.org/docs/WGIGREPORT.pdf on August 8, 2005).

ICANN/IANA structures then overseen by the U.S. Department of Commerce. The group also emphasized that "gender balance," or equal representation of men and women within any forum for discussions of Internet governance, should "be considered a fundamental principle," a recommendation which lacked reflexive credibility considering the overwhelming preponderance of men on the United Nations Working Group discussing Internet governance, and the oppressed condition of women in several WGIG countries.

The United Nations also alluded to a new approach for establishing Internet standards. The WGIG included standards development in a lengthy list of international government responsibilities.[376] Without elaboration, the working group's recommendation insinuated moving Internet standards development to an international, inter-governmental organization, presumably shifting standards development from the IETF to the United Nation's standards setting body, the ITU. Furthermore, the recommended list of responsibilities for "civil society" and the private sector did not include standards development, excluding citizens, users, and vendors from governmentally constituted Internet standards development. Establishing top-down, inter-governmental, presumably United Nations-based control of Internet standards setting would depart from the traditional standards development process.

The United Nations working group also recommended four alternative models for multilateral Internet policy oversight. The first model would establish a Global Internet Council, anchored in the United Nations and comprised of governmental representatives to establish names and address policies such as how to internationally allocate IPv6 addresses. Some of the recommendations included the following: completely eliminate the authority of the United States Commerce Department in Internet oversight of the technical and operational functions of the Internet such as management of Internet addresses and the domain name system; either place ICANN under the United Nations or replace ICANN's role with a reformed internationalized organization, possibly given the name WICANN, (pronounced Y-CAN, not wiccan) for World Internet Corporation for

[376] Report of the Working Group on Internet Governance, Chateuau de Bossey, June, 2005, Section V.A.1.40. (Accessed at http://www.wgig.org/docs/WGIGREPORT.pdf on August 8, 2005).

Assigned Names and Numbers; and anchor any overarching international Internet governance council or forum in the United Nations.

The primary objective of the United Nations recommendations was to replace U.S control with United Nations control, in other words to expunge the control of U.S. agencies like the Commerce Department or the authority of historically U.S. based organizations such as ICANN, the IETF, the IAB, and IANA. The United Nations did not provide any technical or economic rationale for changing oversight of the centralized IP address allocation administration. If anything, the European Union and nations like China and Korea were touting IPv6 because of its abundance of addresses rather than any economic scarcity or inequity.

The recommendations raised questions about what role the private sector, Internet users, and Internet developers would have if a United Nations council led by governmental representatives made Internet policy decisions. Another question was the possible architectural ramifications to the Internet if technical standards oversight related to addressing, routing, and the DNS moved from those historically involved in technical specifications to inter-governmental oversight. Most importantly, what impact would the involvement of countries with repressive Internet policies have on Internet governance policies? The Number Resource Organization[377] (NRO), a collaborative venture of the Regional Internet Registries, acknowledged that the United Nations emphasis on multistakeholder models was important, but suggested that the WGIG did not adequately present alternatives for existing organizations (like the registries the NRO represents) to incorporate multistakeholder principles.[378] The NRO also accentuated the importance of retaining a role for academic and technical communities in Internet governance. The organization agreed that United States monopoly oversight of ICANN and its IANA function must end, but cautioned that any increase in government oversight might stunt innovation and increase bureaucracy.

[377] The Regional Internet Registries founded the Number Resource Organization (NRO) on October 24, 2003. The four RIRs extant at that time included: APNIC, ARIN, LACNIC and RIPE-NCC.

[378] Number Resource Organization Document NR026, “Number Resource Organization (NRO) Comments on the WGIG Report,” July, 2005. (Accessed at http://www.nro.net/documents/nro26.html on August 14, 2005).

4.10 The U.N.'s Development Rationale

A dominant and recurrent theme underlying the United Nations' proposed appropriation of Internet governance functions, including IPv6 address administration, involved the need for the Internet in the developing world. The U.N.'s articulated rationales for recommending a diminishment of U.S. power never mentioned the economic and political requirements of economically more advanced countries (represented on the WGIG) to gain more say over Internet governance including control of Internet resources like IPv6 addresses. Instead, the WGIG agreed upon only two overarching requirements for Internet governance legitimacy, both related to developing countries:

> *"The WGIG agreed that there are two overarching prerequisites to enhance the legitimacy of Internet governance processes:*
> *-The effective and meaningful participation of all stakeholders, especially from developing countries.*
> *-The building of sufficient capacity in developing countries, in terms of knowledge and of human, financial and technical resources."*[379]

Sociologist Manuel Castells claims that "the Internet is a fundamental instrument for development in the Third World." [380] The United Nations emphasized the priority of Internet "capacity-building" as a mechanism for helping developing countries and as a rationale for more multilateral control of Internet governance including management of the IP address space. The Internet Society has similarly espoused a vision of extending what it considers to be the benefits of the Internet to all people. Its institutional mission codifies this objective, "To assure the open development, evolution and use of the Internet for the benefit of all people throughout the world."[381] ISOC has singled out "developing countries" as recipients of Internet globalization efforts. Developing countries in this context appear to be "technologically emerging nations"[382] defined by what is absent. They lack Internet access, technical expertise, Internet governance

[379] Report of the Working Group on Internet Governance, Chateuau de Bossey, June, 2005, Section V.B.74. (Accessed at http://www.wgig.org/docs/WGIGREPORT.pdf on August 8, 2005).

[380] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2001, page 5.

[381] Internet Society Mission Statement. (Accessed at http://www.isoc.org/isoc/mission on July 21, 2003).

[382] Internet Society Programs. (Accessed at http://www.isoc.org/isoc/mission/goals on July 21, 2003).

representation, IP addresses, and interconnectivity to a global communications system and are thus disenfranchised from the global information economy.

Escobar stresses that "understanding the discursive and institutional construction of client categories requires that attention be shifted to the institutional apparatus that is doing the 'developing.'"[383] The Internet Society and the United Nations portrayed developing countries as targets for intervention. Both institutions also prescribed themselves as solutions to the Internet needs of these targets for intervention. A mission statement of ISOC programs described "assisting technologically developing countries, areas, and peoples in implementing and evolving their infrastructure and use…"[384] Analogously, the United Nations framed the appropriation of Internet governance functions from the United States as a necessary precursor to legitimate third world representation and resource distribution.

At the time of the U.N. Working Group's proposals and accompanying rationale that a more equitable resource and governance structure was necessary for developing countries, how geographically imbalanced was the global distribution of IPv4 and IPv6 addresses? By the summer of 2005, address allocation statistics appeared geographically more egalitarian than in earlier years. IPv4 addresses were geographically distributed equally among the Asia-Pacific region, North America, and Europe, with small allocations to Latin America and Africa. Europe and the Asia Pacific region controlled the majority of IPv6 address allocations. The following charts illustrate the IPv4 and IPv6 address allocation statistics from 2005. According to the address distribution statistics, Africa and Latin America controlled only 4% of IPv4 addresses and 4% of IPv6 addresses.

[383] Arturo Escobar, *Encountering Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995, p. 107.

[384] Internet Society Mission Statement Goals (Accessed at http://www.isoc.org/isoc/mission/goals on July 21, 2003).

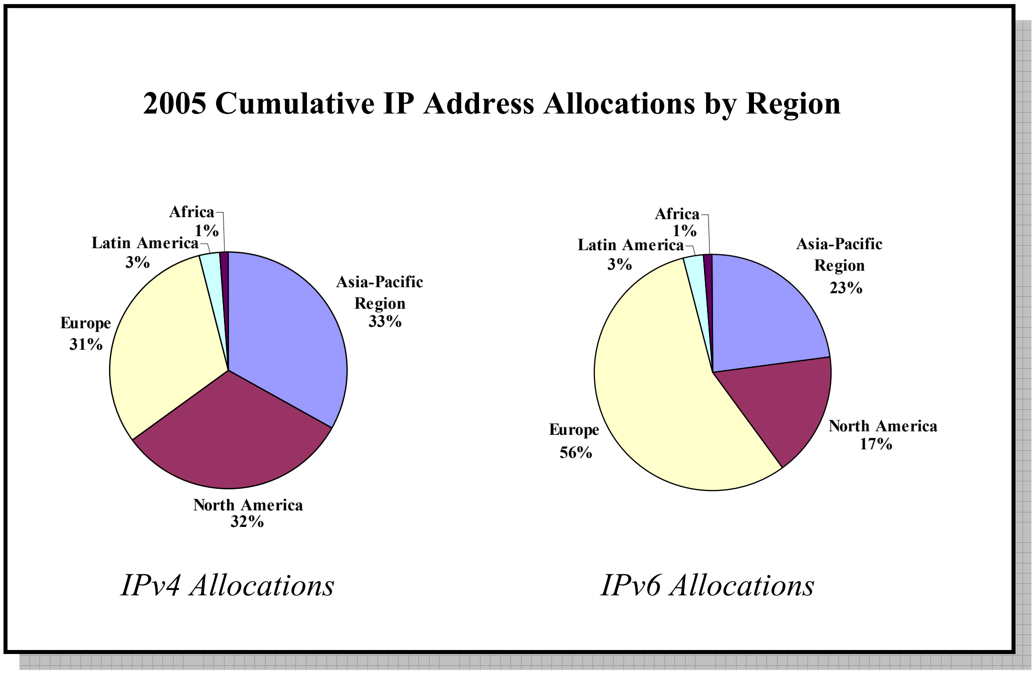


FIGURE 7: REGIONAL IP ADDRESS ALLOCATION (2005)

4.11 The U.S. Retrenches

Two weeks before the United Nations released its Internet governance report advocating U.S. relinquishment of unilateral Internet names and addresses oversight, the U.S. Commerce Department, on behalf of the Bush administration, issued a terse articulation of core principles for the Internet's addressing and domain name systems. The "U.S. Principles on the Internet's Domain Name and Addressing System"[385] asserted that the United States government would retain its historical responsibility and oversight of ICANN. ICANN's primary responsibilities included central administration of Internet addresses through its IANA function, the operation of the Internet's root name server system, and administering domain names. The message was clear in the Commerce Department's articulation of Internet principles: United States unilateral oversight of addresses and DNS administration would continue, cutting off the possibility of internationalizing this function by relinquishing any responsibilities to the United Nations. The U.S. argument for maintaining the status quo rested on the notion that the

[385] "U.S. Principles on the Internet's Domain Name and Addressing System." (Accessed at http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm on December 8, 2005).

current Internet system was working and any changes might disrupt the security, stability, and efficient operation of the Internet.

The Bush administration's statement of principles conveyed an impression of durability and firmness because it would serve as a guiding foundation for establishing all federal government policies related to Internet names and addresses "in the coming years."[386] The new principles also emerged as one part of a broader administration technology framework. Michael Gallagher, J.D. directed the policy review effort leading to the formation of the U.S. principles. President Bush appointed Gallagher on July 1, 2004 to the post of Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration (NTIA). Assistant Secretary Gallagher announced the new U.S. policy principles during his presentation at the Wireless Communications Association (WCA) annual conference in Washington, D.C. on June 30, 2005.[387]

President Bush was a central presence in Gallagher's short presentation, which included twenty five references to the President or his Administration, five direct quotes attributed to President Bush, and three pictures of the President. Gallagher stated that "Thanks to the President's policies, American's economy is strong," and presented comparative economic statistics (GDP, job growth, and unemployment rate) suggesting a superior performance of America's economy over the EU, Japan, and Canada. The presentation emphasized three areas critical to continued U.S. economic success: broadband, spectrum policies, and the Internet. Gallagher linked the administration's policies of business tax relief and regulatory reductions with economic growth in broadband. He also identified spectrum management reform geared toward freeing up scarce resources of radio frequencies as a precursor to promoting the growth of wireless broadband technologies and increasing imports of these products to vast markets like China and India. Finally, Gallagher stated that the Department of Commerce would

[386] According to the web site of the National Telecommunications and Information Agency. (Accessed at http://www.ntia.doc.gov/ntiahome/ntiageneral/bios/mdgbio.htm on December 4, 2005).

[387] The NTIA web site published Assistant Gallagher's presentation. (Accessed at http://www.ntia.doc.gov/ntiahome/speeches/2005/wca_06302005_files/frame.htm on December 20, 2005).

retain its role in Internet name and address system oversight to preserve the Internet's economic stability, economic opportunities, and security.

The Bush administration's position embraced the status quo, but was also a reversal of previously established policy directives. Beginning with the Commerce Department's 1998 "white paper"[388] calling for the creation of a private, non-profit corporation to administer the Internet's domain name and addressing functions, U.S. government policy included transition agreements with ICANN anticipating an eventual phasing out of a federal government role in Internet address and name system oversight. The plans for a transition from federal government control originated during the Clinton Administration and had two primary objectives: a more privatized approach and more internationalized oversight. The U.S. Department of Commerce anticipated that U.S. government policy oversight of the new private corporation would end within two years:

> *"the U.S. Government would continue to participate in policy oversight until such time as the new corporation was established and stable, phasing out as soon as possible, but in no event later than September 30, 2000."*[389]

The Commerce Department's original policy objective established that the functions related to administering the names and number systems would be private, non-profit, and "managed by a globally and functionally representative Board of Directors."[390]

The policy anticipating a phasing out of federal government oversight required ICANN to meet certain conditions and went through several years of evaluations followed by extensions of federal government oversight. For example, in 2003, the policy agreements between the U.S. Department of Commerce and ICANN anticipated an eventual phasing out (by 2006) of U.S. governmental funding and oversight of the new entity.[391] The new Commerce Department declaration of Internet principles reversed this. Against the backdrop of the United Nations proposing an eradication of unilateral U.S. Department of Commerce oversight, the U.S. formally reversed its transition

[388] United States Department of Commerce, National Telecommunications and Information Agency, Docket Number 980212036-8146-02, *Management of Internet Names and Addresses*, June 5, 1998.

[389] Ibid.

[390] Ibid.

[391] See the "Memorandum of Understanding between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers, Amendment 6," September, 2003, http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6_09162003.htm.

objective and unilaterally drew an unambiguous demarcation preserving indefinitely its oversight role.

In addition to preserving boundaries, the U.S. Declaration of Principles appeared to also anticipate and rebuff the possibility of the United Nations assuming any Internet governance role. The statement of principles stated that no single organization could adequately "address the subject in its entirety." The notion of a variety of organizations rather than a single forum as appropriate for Internet governance preempted the U.N.'s impending report seeking Internet governance power. Finally, the U.S. Principles appeared to prioritize the possible role of market-based approaches and the private sector, promising "the United States will continue to support market-based approaches and private sector leadership in Internet development broadly." Market-based approaches were not historically pertinent to the Internet names and numbers management function, but this principle served to diminish the prospect for greater governmental (or inter-governmental) involvement while maintaining overall U.S. oversight of Internet resources.

The timing of the announcement preempted the U.N.'s WGIG report by two weeks and assumed an antithetical position to the one the U.N. would present calling for U.S. relinquishment of its unilateral oversight of the ICANN function. The announcement also ensconced a firmer position from which the U.S. could negotiate during an upcoming U.N. sponsored conference discussing Internet governance issues. Michael Froomkin, law professor and founder of advocacy group ICANNWatch, described the announcement's timing "Bolton-eseque,"[392] [sic] a reference to U.S. Ambassador to the United Nations, John Bolton, whose nomination faced a lengthy filibuster and eventually proceeded through a congressional recess appointment by President Bush. Bolton's March, 2005, recess appointment was controversial because he was an outspoken critic of the U.N. and had, in 1994, remarked, "There is no such thing as the United Nations. There is an international community that occasionally can be led

[392] A. Michael Froomkin, "US Drops ICANN/DNS Bombshell (on WSIS?)." (Accessed from Froomkin's personal blog www.discourse.net on January 3, 2006).

by the only real power left in the world, and that's the United States, when it suits our interest and when we can get others to go along."[393]

The “Internet Governance Project” (IGP), a small consortium of academics from Syracuse University and Georgia Institute of Technology researching Internet and Information and Communication Technology (ICT) policies, criticized the Bush administration’s announcement. The IGP called Assistant Secretary Gallagher a “newcomer to the debate” who didn’t realize that what he called the U.S. government’s historic involvement was less than seven years old. This criticism was misleading because, while ICANN was only seven years old, the U.S. government had historically maintained oversight and funding of the responsibilities it later repositioned under ICANN. Nevertheless, the IGP’s position suggested that oversight, albeit limited oversight, of the ICANN functions, must be internationalized and that “No single government can be trusted to eliminate all considerations of national self-interest from its oversight role.”[394] ICANN’s legitimacy emanated from increasing international representation and the expectation that U.S. unilateral oversight would eventually wane. A continuation of U.S. unilateralism would detract from ICANN’s already tenuous legitimacy and create conditions whereby the Internet might fragment into national segments independent of U.S. participation. In short, “If nothing changes, the US role will continue to inflame political criticism of Internet governance for years to come.”[395] The U.S. announcement did appear to incite some political criticism. In one graphic example, British technology weekly, The Register, framed the U.S. announcement in an overall cultural zeitgeist of the Bush administration’s world philosophy: “that the U.S. will continue to run the Internet and everyone will just have to lump it – is very in keeping with how the U.S. government is currently run!”[396]

Once Koffi Annan formally released the U.N.’s WGIG report, the United States Department of State released official “Comments of the United States of America on

[393] As cited in a transcript from *The NewsHour with Jim Lehrer*. (Accessed at http://www.pbs.org/newshour/bb/fedagencies/jan-june05/bolton_3-8.html on January 3, 2006).

[394] Internet Governance Project Concept Paper, “The Future US Role in Internet Governance: 7 Points in Response to the U.S. Commerce Dept.’s ‘Statement of Principles,’” July 28, 2005. (Accessed at www.internetgovernance.org on December 22, 2005).

[395] Ibid.

[396] Kieren McCarthy, “Bush Administration Annexes Internet,” *The Register*, July 1, 2005.

Internet Governance"[397] responding to the findings and recommendations. Without specifically stating that the United States Department of Commerce planned to retain its ICANN oversight role, the State Department echoed the sentiments expressed in the U.S. principles on Internet governance. The State Department suggested an implausibility of one single entity completely addressing the spectrum of Internet governance issues and wove references to global Internet governance entities (like the World Intellectual Property Organization (WIPO) and the London Action Plan on spam) into its response. The State Department also disputed the notion that Internet governance related to address and name administration was completely centralized or unilaterally administered. Internationalization and administrative distribution of the Internet was evident in the creation of RIRs, the efforts to allocate IP addresses in a more geographically equitable pattern, and because the "vast majority" of the 103 root servers (and mirror root servers) were located outside of the U.S. The State Department's formal comments were diplomatically phrased in not specifically denouncing (or even mentioning) the possibility of U.N. Internet oversight but nevertheless presented arguments that would countervail this governance change. For example, the document reiterated U.S. commitment to freedom of expression, presumably an argument against Internet governance participation by undemocratic regimes like China and Cuba through U.N. conduits. Additionally, the State Department acknowledged the need for governmental representation but highlighted the importance of civil sector and private sector involvement in Internet governance, using as an example the private sector led ICANN with government input provided through ICANN's Global Advisory Committee (GAC) in contrast to U.N. oversight which could limit civic involvement and could impede private investment, competition, and associated innovation.

4.12 International Impasse

The United Nations and the United States espoused seemingly irreconcilable differences about Internet governance, including, among many functions, the IP address oversight

[397] U.S. Department of State, Bureau of Economic and Business Affairs, "Comments of the United States of America on Internet Governance," August 15, 2005. (Accessed at http://www.state.gov/e/eb/rls/othr/2005/51063.htm on November 11, 2005).

role. The United States declared it would continue its ICANN oversight function and the United Nations declared U.S. unilateral oversight must cease. The international debate over who should oversee Internet addresses and the domain name system continued in "PrepCom3," the third preparatory committee meeting prior to the World Summit on the Information Society (WSIS) scheduled for November 16-18, 2005 in Tunis, Tunisia. PrepCom3, held in September in Geneva, Switzerland, was a politically charged, two week session of debates about Internet governance and other Internet issues.[398] Almost 2000 individuals representing governments, NGOs, and businesses participated in the sessions,[399] including a U.S. delegation with David Gross, U.S. Coordinator, International Communications and Information Policy in the Department of State. The preparatory conference ended with a polarizing impasse over the Internet governance issue of management of Internet addresses and the domain name system, reflecting prevailing tensions between United States and United Nations policies.

The U.S. and U.N. positions shared one common denominator in invoking democratic ideals as justifications for each argument. This linkage between Internet architectural oversight and democratic freedoms resembled prevailing associations, among IPv6 advocates, between the IPv6 standard and the promotion of worldwide freedom and democracy throughout the world. Multilateral oversight by a United Nations-based entity was the true democratic approach, according to those espousing the diminishment of United States oversight. Others argued that handing over Internet oversight to an organization – the United Nations - with no democratic preconditions for membership could compromise the democratic and libertarian underpinnings of the Internet.

Some in the United States Congress supported the Bush administration's position on Internet governance by formally denouncing the prospect of U.N. intervention. Senator Norm Coleman (R-MN) entered a statement into the Congressional Record censuring the recommendation in the U.N.'s WGIG report calling for an end to U.S.

[398] The ITU published video webcasts of PrepCom-3 on its web site. (Accessed at http://www.itu.int/wsis/preparatory2/pc3/#pc3 on November 31, 2005).

[399] According to the final list of participants, PrepCom-3 for World Summit on the Information Society, Geneva, Switzerland, September, 2005. (Accessed at http://www.itu.int/wsis/docs2/pc3/participants-list-final.pdf on December 1, 2005).

oversight of ICANN functions. Coleman, with Senator Dick Lugar (R-IN), had recently introduced U.N. reform legislation, the Coleman-Lugar U.N. Reform Bill, which addressed a "culture of corruption" at the U.N. centered around the Oil for Food scandal. Coleman described U.N. management as "at best, incompetent, and at worst corrupt" and denounced the possibility of U.N. control over the Internet.[400] Besides the negative heuristics of mismanagement and corruption, Senator Coleman argued that the move would allow countries like China and Cuba, with no commitments to democratic freedoms or the free flow of information, to gain unwarranted influence over the Internet.

Three members of the House of Representatives, California Republican John Doolittle, Virginia Republican Bob Goodlatte, and Virginia Democrat Rick Boucher, issued a similar resolution[401] offering more political backing for the Bush Administration's position opposing United Nations involvement in ICANN oversight. The House resolution concurred with previously issued U.S. principles on Internet governance and stated that that any interest in moving the name and addressing system under U.N. control was "on political grounds unrelated to any technical need." Additionally, the resolution argued that U.S. oversight of names and numbers should continue for the following reasons: historical roots of Internet found in U.S. government funding; retention of private sector leadership and public involvement as essential for continued Internet evolution; maintenance of Internet's security and stability, and preservation of freedom of expression and free flow of information.[402] The general political position of the Bush administration and some in Congress argued that ICANN, while imperfect, allowed for significant private sector involvement and international representation and any transfer of ICANN functions to the United Nations would threaten democratic freedoms of the Internet, private sector involvement, and the stable ongoing operations of the infrastructure.

[400] From "Coleman Denounces Report Calling for UN Global Internet Control: Coleman opposed to any proposal to hand control of Internet governance over to the United Nations," published on Senator Coleman's web site on July 29, 2005. (Accessed at http://coleman.senate.gov/ on December 2, 2005).

[401] HCON 268 IH, 109th Congress, House Congressional Resolution 268, "Expressing the sense of the Congress regarding oversight of the Internet Corporation for Assigned Names and Numbers," October 18, 2005.

[402] Ibid.

After lengthy preparatory meetings, working group deliberations, and great controversy, the result of the ITU-organized World Summit on the Information Society (November, 2005) as it pertained to address oversight, was retention of the status quo. The summit's consensus statement, "the Tunis Agenda for the Information Society"[403] made no specific mention of ICANN or the United States but preserved the status quo by leaving Internet resource control in the existing governance forums, meaning ICANN with U.S. government oversight. The summit rejected the WGIG recommendation to create a new U.N.-based governance body, primarily because changes could not proceed without the agreement of the United States, which would not acquiesce to any structural changes. On the final day of the Summit, John Marburger, Presidential Science and Technology Advisor, firmly reiterated the U.S. position to retain the existing oversight structure which was "working so well." The U.S. State Department described the rejection of a new U.N.-based governance body as a victory that would "keep the Internet free of bureaucracy."[404] Not surprisingly, ICANN welcomed the WSIS Tunis Declaration, and suggested the WSIS recognition of ICANN's multi-stakeholder model (i.e. its Governmental Advisory Committee) would ensure the ongoing stability and integrity of the Internet's name and addressing system. The WSIS statement also included a compromise many nations described as a victory for multilateralism, the formation of an Internet Governance Forum (IGF). The IGF would continue the dialog about Internet governance issues but would have no authority or formal responsibility. As a joint statement of the Internet Governance Project summarized, "Almost all of the Internet governance issues raised by the summit remain open and unresolved."[405]

4.13 Chapter Conclusion

Explaining the sudden value of electromagnetic spectrum during the 19th century expansion of radio technologies, economist Hugh Aitken argued, "Here we have new

[403] Final WSIS documents, conference statements, and videocasts published on the ITU web site. (Accessed at http://www.itu.int/wsis on December 11, 2005).

[404] "World Summit Agrees on Status Quo for Internet Governance." (Accessed on U.S. State Department web site http://usinfo.state.gov/eur/Archive/2005/Nov/16-493027.html on December 12, 2005).

[405] Internet Governance Project statement, "An Inconclusive Summit." (Accessed at http://www.internetgovernance.org on December 9, 2005).

resources – invisible resources, to be sure… These resources, furthermore, when their economic and military uses came to be appreciated, were to become the object of competitive struggles for exclusive possession and occupancy, just like the colonial empires carved out by European powers in North America in the seventeenth century or in Africa in the nineteenth."[406] Like radio spectrum, Internet addresses came to be seen as invisible, but valuable, scarce resources.

The original ARPANET destination codes were only 5 bits long, providing a total of 32 unique addresses. Researchers gradually augmented the number of addresses as they anticipated requirements for connecting additional devices. IPv4 specified a 32-bit code providing more than four billion unique addresses. Original administrative and technical decisions such as the Internet Class System, assignment inefficiencies, and an asymmetrical allocation to U.S. institutions contributed, along with rapid global Internet growth, to concerns about an impending IPv4 address shortage. However, CIDR, NAT, conservation techniques, and the distribution of large blocks of the IPv4 address space to international registries, helped mitigate some concerns about address depletion and inequity. Additionally, governments in Asia and the European Union described IPv6 and the abundance of available IPv6 addresses throughout the globe as the solution to any conceivable address depletion concerns. In many ways, the issue of address scarcity appears to not be the significant factor in this struggle for resource control. The same international institutions extolling the enormity and global availability of the IPv6 address space have contradicted their own claims by arguing that developing countries are at risk of having insufficient Internet resources unless U.S. oversight of the centralized address allocation function is further internationalized.

Analogous to the question of who would be responsible for Internet standards that had shaped the selection of SIPP over the ISO-based alternative, the issue of who would ultimately control IP addresses shaped decisions about the address distribution succession. Tensions between those involved in the Internet since the early days of ARPANET versus newer participants, and politically reflective tensions between an American-controlled structure and greater multilateral control, once again fueled

[406] Hugh G. J. Aitken, *Syntony and Spark: The Origins of Radio*. New York: Wiley & Sons, 1976, page 32.

controversies over institutional administrative structures. A single trusted insider originally distributed addresses. As this responsibility shifted to more formal institutional structures, Postel and his colleagues remained central figures in structural decisions regarding resource distribution. The ongoing institutional decision to oppose the possibility of exchanging IP addresses in free markets served to support the technical community's philosophy that Internet resources be available to everyone but also fortified the centralized institutional control of resource distribution. The Internet's transformation from a relatively closed and trusted community to a culturally heterogeneous medium created multifaceted and intractable Internet governance dilemmas involving authority to control the globally unique IPv6 and IPv4 addresses necessary for Internet connectivity.

CHAPTER V:
CONCLUSION

The IPv6 standard has served as a locus for incendiary international tensions over control of the Internet. As the Internet's development environment transformed from a small community of trusted insiders to a diffuse international collaboration, the selection of IPv6 solidified the authority of the traditionally American-dominated IETF over the international ISO to establish Internet standards. Various government IPv6 adoption strategies aligned with the international objective of dismantling American Internet industry hegemony or, alternately, preserving the status quo. Centralized control of the finite technical resources of IP addresses similarly developed into a political impasse between retaining U.S. unilateral oversight and pursuing greater multilateralism. In addition to these conflicts, IPv6 directly intersected with a heterogeneous mixture of geopolitical issues including third word development objectives, U.S. military strategies, and the promise of global democratic freedoms.

These three spheres of development (Chapter II), adoption (Chapter III), and technical resource distribution (Chapter IV) also share a common analytical denominator in that they occurred outside of classical market mechanisms. The Internet standards community selecting IPv6 circumvented market considerations and disregarded contrarian views of some large corporate U.S. Internet users, who, with enormous IPv4 installed bases, were disinclined to embrace the new standard. The historical distribution of IP addresses, on the surface a straightforward problem of supply and demand of common pool resources, followed a similar trajectory. IP addresses were never exchanged in free markets and were originally generously allocated on a first come first serve basis to American organizations involved in early Internet development. Regarding IPv6 adoption, national governments eschewed *laisse faire* possibilities for IPv6 market adoption, instead issuing top-down, national IPv6 mandates, with the exception of the U.S. position to "let the market decide." State interventions rejected the potential sufficiency of competitive market mechanisms in both development and deployment of IPv6 products, instead federalizing technology selection for citizens and institutions. This historical account of IPv6 has demonstrated the explanatory power of STS theoretical approaches and has elevated the following historical themes and theoretical implications.

5.1 Network Protocols as Politics

The history of IPv6 suggests a theoretical nexus between politics and standards. Network protocols coerce adherence to rigid architectures, excising difference by enforcing technical specificity. What eliminates other possibilities is not solely technical rationalization but political negotiation between stakeholders. The history of IPv6 indicates that standards are political in several respects. First, they are historically specific conventions politically negotiated by those with the power, access, and knowledge to influence outcomes. Once developed, standards appear outwardly an objective technological approach but embody the interests of these negotiators in a Habersmasian sense of technocratic consciousness. Economically, the selection process pitted then-dominant vendors like Digital Equipment Corporation against newer entrants like Sun Microsystems. More generally, the choice of the next generation Internet protocol was an issue of selecting who would have authority to establish the Internet's architectural directions. While the assessment process adamantly emphasized that *only technical considerations* would influence protocol selection, a salient question in selecting the new standard appeared to involve *who* would retain or gain architectural control. The ISO-based alternative had considerable momentum: backing of the United Nations, endorsement by most western European governments, patronage by prominent American vendors, and limited U.S. government acquiescence because of its endorsement of the GOSIP architecture. The stakeholder interests of the Internet's growing corporate user base were also reflected in expressing resistance to the possibility of investing in any new protocol order. If the IETF had selected the ISO-developed protocol, CLNP, it would have raised complicated questions about which standards organization would have protocol change control in the future. In other words, the ISO would suddenly control the Internet's architecture. The selection of SIPP, an IETF insider developed extension of the prevailing IPv4 standard, entrenched the existing power of the Internet's standards setting establishment and rejected the possibility of relinquishing architectural authority to the U.N. backed ISO. A decade after this decision, discord between U.N. backed standards organizations and the Internet's traditional standards body, the IETF, remained as pronounced as ever, with the ITU proposing it take the reins of Internet standards setting from the IETF and the U.N.'s Working Group on Internet governance suggesting standards should be the purview of governments. These conflicts over standards setting corroborate how standards selection is power selection.

Additionally, governments have associated IPv6 standards adoption or IPv6 product development with the achievement of specific objectives of economic competitiveness, military capability, reduction in unemployment, and information access. The Japanese government, encouraged by Japanese corporations with a direct interest in IPv6 adoption, suggested its IPv6 mandate and corresponding industry product innovations would contribute to economic recovery and Internet industry competitiveness in the wake of long term stagnation. European Union policy linked IPv6 adoption with its Lisbon objectives of becoming the world's most competitive knowledge based economy. The Korean government followed Japan in arguing that IPv6 expertise could make the country an "Internet powerhouse" and experience a corresponding reduction in unemployment and rise in GDP. The U.S. Department of Defense linked IPv6 with achieving its specific Global Information Grid military objectives. These linkages between the IPv6 standard and government policies were political in the straightforward instrumental rationality sense of achieving specific objectives. But the linkages also seemed political in the broader sense that talk about a future upgrade to IPv6 and what it might achieve supported positions such as reinforcing EU unification, spreading democracy, supporting economic reform, or bolstering perceptions of enhanced capabilities in homeland security or military engagements. The history of IPv6 demonstrates how various groups with contradictory objectives can make use of the same technology as a political resource.

The history of IPv6 points to a related subtheme of how communications standards create new, finite resources and how, once the value of these resources is understood, control of these finite resources and control of the standards defining these resources become struggles among those seeking greater possession, tenure, and economic positioning within the communications medium. The T-3 telecommunications standard carves out a finite number of 672 transmission channels. Radio transmission standards specify a finite number of usable frequency bands. Cellular towers allow a finite number of concurrent cell phone conversations. IPv4 and IPv6 standards specify a finite number of Internet addresses. In the case of the Internet, the initial distribution of technical resources involved allocation to those organizations involved in the early development and adoption of Internet predecessor networks. The technical insiders within the Internet standards setting community first identified the Internet address space as a potentially scarce resource and proposed expanding the number of available addresses through a new standard, as well as allocation of addresses to more geographically distributed registries. Once later entrants recognized the value of Internet connectivity and the finite resources that enable this connectivity, they embraced the standard that would provide a larger address space. The resource control question of who should centrally administer the allocation of unique, finite resources became a source of controversy centered on issues of international fairness, legitimacy, security, and stability, as reflected in the conflict between U.S. oversight of the IANA function under ICANN versus the possibility of turning that control over to a U.N.-based organization. The impasse seemed to arise from issues of political conflict rather than resource scarcity because the IPv6 address space, central in the impasse over address space centralized administration, is so large.

5.2 The Dissolution of Trust

In the early days of the Internet and its predecessor networks, Internet participants were both users and developers. These user-developers shared educational and experiential commonalities and primarily participated within American academic, research and military contexts. They were trusted insiders with familiarity, demographic correspondence, and communicative relationships with other trusted insiders. Relative to later Internet contexts, access was limited, materializing in an era devoid of home access, business Internet use, or even personal computers. Enormous amounts of money were not at stake and there was no obvious linkage between corporate profits and standards development. No outsiders participated. In this collegial, relatively closed environment, standards consensus was uncomplicated and security was not a significant concern. The commercialization and international expansion of the Internet into businesses, across the globe and into homes heightened economic stakes, cultural complexity, and security concerns and transformed the prevailing trusted insider development environment into a more diffuse collaboration among strangers, including involvement of those not directly contributive to technical standards and those with pronounced corporate or political stakes in architectural outcomes.

This historical account of IPv6 demonstrates how the breakdown in trusted insider status transformed the Internet architecturally and administratively. First, the 1992 "Kobe Affair" reflected anxiety about non-trusted technical outsiders influencing architectural decisions and inaugurated a solidification of Internet standards governance approaches. In the context of increasing Internet internationalization, expansion, and commercialization, the IAB responded to concerns about Internet address space exhaustion by taking an uncustomary step of proposing a specific protocol, the ISO-developed CLNP, to replace IPv4. The IAB had recently superimposed with a new umbrella organization, the Internet Society, which exhibited several characteristics breaking historical traditions in Internet standards development. ISOC cultivated links with competing international standards bodies, received direct corporate funding, promoted formal membership, and responded to the emerging threat of lawsuits related to standards development. IETF participants expressed alarm over the IAB's CLNP recommendation for several reasons. The IAB seemed to be relinquishing responsibility for Internet standards development and change control to the competing international ISO standards process. The decision disseminated from a top-down, closed, and hastily issued mandate without benefit of open hearings and public review and in contrast to the IETF's prevailing bottom-up decision making process. Some also believed the recommended standard to replace IPv4 was untested, expressed concern about undue corporate influence and believed the IAB lacked the legitimacy it once garnered because participants were no longer veteran ARPANET veterans or those directly involved in development and coding. IETF participants no longer viewed the IAB as trustworthy insiders concerned with preserving standards setting continuity and traditions. This breakdown in trust resulted in a solidification and articulation of the standards community's operating philosophy of bottom-up, consensus-based, and open standards development and a rejection of top-down mandates.

Another manifestation of the dissolution of trust was the patent rejection by the standards setting community of market mechanisms in selecting between competing standards. When Internet users were mutually familiar with each other and were also Internet developers, user technical development and standards selection was the norm. Users were also standards selectors. Users eventually became a more amorphous "market," severing the connection between users and standards selections. This fracture between users and standards development was not only a manifestation of the lack of insider familiarity but also an assertion that general Internet users were unqualified to make decisions about the next generation Internet protocol. As Brian Carpenter summarized, the decision was "too complicated for a rational market-led solution"[407] and "we still need Computer Science Ph.D.s to run our networks for a while longer."[408] The user-developer Internet phenomenon was acceptable when users were Ph.D. computer scientists but not when users became a more generalized, corporate, and public market.

An interesting sphere of incongruity enveloped the concepts of 1) bottom-up standards selection versus top-down mandates and 2) market mechanisms. National governments and the standards community both rejected market mechanisms. The standards community rejected top-down mandates while national governments instituted top-down IPv6 mandates. From the multifarious perspectives of stakeholders, either the new breed of users comprising *the market* could not be relied upon to decide, or the *IETF* was not internationally representative enough to decide, or *IAB participants* were not sufficiently involved in coding and insider standards involvement, or the *U.N.* could not be trusted with Internet governance, or *U.S.* unilateral control provided inadequate stewardship.

Architecturally, the breakdown in trust also resulted in a complete reversal of the end-to-end technical philosophy of the early Internet. Even while the IETF continued to espouse the end-to-end principle, implementation realities, especially among corporate

[407] From the Minutes of the IPng Decision Process BOF (IPDECIDE) reported by Brian Carpenter (CERN) and Tim Dixon (RARE) with additional text from Phill Gross (ANS), July 1993.

[408] Brian Carpenter, submission to big-internet mailing list, April 14, 1993.

Internet users, obliterated this architecture. The end-to-end principle, espoused originally in the mid-1980s[409] and formalized in the IAB's 1996 Architectural Principles of the Internet manifesto,[410] responded to questions about where to locate protocol functions such as congestion control, error control, addressing, encryption, and data integrity. The end-to-end principle asserted the Internet engineers' decision to design these network functions at end points, with routers relegated only to expeditiously forwarding packets to their destinations, technically enabling applications to continue working in the event of a partial network failure. It would also preserve protocol homogeneity and therefore preserve the ability to control protocol standards. Despite the continued declaration of this guiding architectural principle, the realities of security challenges like worms, viruses, denial of service attacks, spyware, spam, identity theft, and intrusion led businesses to insert intelligent intermediaries like firewalls and intrusion detection systems in such a way that patently violated this end-to-end protocol framework. Debates within the IETF about these intermediaries took on "religious tones" but the breakdown in trust among users in a global, public medium, created a technical reality of firewalls and intrusion detection intermediaries as the new architectural norm.

This collapse in trust resulted in an architectural retrofitting of security into protocols designed in a time when security was not a salient concern. The Internet transformed from a network of 'that which is not expressly prohibited is permitted' to a network of 'that which is not expressly permitted is prohibited.' Preserving the privacy of information traversing the Internet would require encryption and this issue resulted in the procedural interjection of an existing security protocol, IPsec, into the IPv6 standards context. The IPv6 standard mandated IPsec inclusion, a decision IPv6 advocates would later embrace to tout IPv6 as more secure than IPv4. Advocates ranging from the United States Department of Defense, Japan's IT Strategy Council, and the IPv6 Forums cited "enhanced security" capabilities as one rationale for upgrading to IPv6. This claim technically originates in the mandate of the IPsec encryption protocol within the IPv6

[409] An articulation of the end-to-end architectural philosophy appears in two mid 1980s papers: John Saltzer et. al, "End-to-End Arguments in System Design," ACM TOCS, Volume 2, Number 4, November, 1984, pp. 277-288; and Dave Clark, "The Design Philosophy of the DARPA Internet Protocols," Proceedings of SIGCOMM 88, ACM COR Volume 18, Number 4, August, 1988, pp. 106-114.

[410] Brian Carpenter, Editor, "Architectural Principles of the Internet," RFC 1958, June, 1996.

standard. However, the black and white portrayal of IPv6 as more secure than IPv4 is contestable for five reasons. First, mandating IPsec in the IPv6 standard is a 'paper' specification network implementers may choose to ignore. Mandating IPsec within the IPv6 standard does not automatically translate into real world implementations. Second, IPsec encryption can operate in conjunction with the IPv4 protocol, similar to the IPv6 protocol. The exclusive linking of IPsec encryption with IPv6 in rationales for upgrading is not entirely accurate because IPsec can also accompany IPv4. Third, as discussed in Chapter III, mixed IPv4 and IPv6 network environments are less secure, especially when interoperable through translation gateways or protocol tunneling techniques. Additionally, the proliferation of products with built in IPv6 capability, even if dormant, provides some security challenges. For example, a business using products with unactivated IPv6 might be vulnerable to security exploitation of IPv6 but might not configure security products to detect IPv6-related security breaches. Finally, and consistent with most evolving protocols, various Computer Emergency Response Teams, both in the U.S. and around the world have identified numerous, intrinsic security vulnerabilities in IPv6 products. While not atypical, the spate of IPv6 security weaknesses appears to complicate the self-evidently presented arguments that IPv6 is intrinsically more secure than IPv4.

A similar response to the breakdown in trust involved the diffusion of IP addresses to internationally distributed Internet registries such as RIPE-NCC, APNIC, LACNIC, and AfriNIC. Address assignment stewardship shifted from a single individual to an American institutional framework to an internationalized structure more trusted to distribute limited resources by geographical region. But controversies over ongoing centralized control of international address allocations reflected the lack of trust by international stakeholders in a California-based corporation overseen by the U.S. Commerce Department to make decisions in the best interest of the world rather than in the best interest of the United States.

This historical pattern suggests that the dissolution of trust between Internet stakeholders will continue to create tensions in deliberations and decision making about who should control centralized address administration, root zone file changes, root name server management, and the ongoing development and change control of the Internet's core addressing and routing standards.

5.3 Internet Democratization Caveats

Many IPv6 advocates have viewed the standard, and the Internet generally, as inherently democratic platforms. Views of the Internet as a democratic medium usually have addressed the Internet's application layer: an electronic public space for democratic activity, a medium providing a diversity of political information sources; a forum for voices extraneous to dominant social forces; an auxiliary platform for governments to interact with citizens; a participatory tool for facilitating grassroots organizing, rapid information exchange, electronic petitions, and galvanization of local political action. Additionally, direct user contributions to application content – developing web sites, publishing blogs, sharing MP3 files – convey the sense of a democratic development environment. This direct user engagement with content development and applications imparts an outward sense of technical control. However, much of the Internet's technical architecture lies concealed beneath the application layer users directly engage. Views of the Internet as a democratic medium also extend beneath the application layer to overall Internet standards development and administration of the Internet's technical architecture, with some extolling the standards process as a paragon of grassroots democratic decision making and some perhaps unaware that centralized standards establishment and resource administration occurs.

This history of IPv6 should dispel the mischaracterization that "no one controls the Internet." Recall that the CIO of the U.S. Department of Defense, during a question and answer session about IPv6, was unaware of who was in charge of the complex technical standards on which the DoD's future architecture would rely, again reinforcing both the concealed quality of standards development and the tacitly accepted authority ascribed to organizations wielding the ability to establish the Internet's architectural and cultural directions. Those who are aware of underlying network protocols and the existence of a corresponding standards setting process might not be concerned with the process because of the ongoing pragmatic success of these standards in achieving interoperability and interconnectivity or assumptions that objective technical decisions determine standards.

An inherent contradiction underlies the standards setting formulation as characterized by the IETF and extolled by outsiders. The IETF specified that only technical considerations would factor into the IPv6 selection process. The IETF process also embraces a one voice, one vote democratic process. The belief in technical neutrality denies the role of a political process in standards setting. The inherent contradiction is that the process can not be apolitical, on one hand, and a democratic political structure, on the other. Addressing questions about democratic standards setting requires deciding whether the process is political. This research has demonstrated that standards decisions are not unadulterated technical formulations but reflective of political and economic exigencies, warranting critical examination of the standards setting process.

The Internet standards process does exhibit properties of informational and participatory openness, pragmatism, grassroots involvement, and consensus decision making. The history of IPv6 development has nevertheless raised some questions about the extent to which IPv6 development, adoption, and resource governance are necessarily democratic processes. Chapter II described how the IPng Working Group solicited formal public requirements after the proposed alternatives were already developed. The group also appeared to have requirements defined prior to the process of selecting the next generation Internet protocol. The solicitation of public input appeared more of a formality further ascribing legitimacy onto a process in which a proposed alternative seemed inevitable. Additionally, barriers to participation obviously exist. In addition to the specific instances of quasi-democratic standards selection, general barriers to democratic participation include the four horsemen of money, access, culture, and knowledge. Because involvement in developing standards like IPv6 is uncompensated activity, participants usually have the financial backing of salaries from corporate employers supporting their participation. Within the IETF, individuals have “one voice” from which to participate but the individuals also represents interests of the institutions funding their involvement. Most communications occur over the Internet, requiring access, and those participating appear to have clear cultural commonalities, including speaking exclusively in English and subscribing to the procedures, norms and values the IETF espouses. Participation in network standards work also requires technical understanding of abstract and esoteric network protocol issues, an obvious barrier to general public participation. At one point, technocracy and democracy in standards setting were equivalent. As the constituency expanded beyond the technocracy's network of familiar insiders, technocracy and democracy diverged. This account has also shown that some individuals organizationally traverse what, on the surface, appear to be distinct organizations: the IAB, the IETF, the IPng Decide, ISOC, and ICANN. The implication is that what appear like distinct episodic power struggles actually preserves the status and influence of the same core individuals. The same questions apply to the Internet registry system. The RIRs themselves claim their legitimacy is based on openness, transparency, participatory decision making. There is no general public involvement in the registry system, other than paid corporate participation. The geographical dispersion of IPv4 and IPv6 addresses to international registries like LACNIC, AfriNIC, RIPE-NCC, and APNIC has resulted in a more geographically equitable (though imperfect) distribution of Internet resources relative to the early allocation asymmetry. At a minimum, the power of registries to assign addresses and potentially reclaim addresses should rise to the level of general public awareness.

This issue of democracy and expertise relative to establishing standards for the Internet's underlying routing and addressing protocols follows the broader question about the relationship between democracy and scientific expertise. Steven Epstein thoroughly addressed this issue in *Impure Science: AIDS, Activism, and the Politics of Knowledge* (1996). Through discussing the role of public expertise in AIDS treatment research, Epstein recognized "the extraordinary difficulty of eradicating hierarchies founded on knowledge-possession," the issue of how science practice presupposes specialization.[411] Democratic involvement in network standards faces a further difficulty. Those contributing lay expertise to AIDS research were primarily HIV positive and epidemiologically motivated. Many end users do not interact directly with the Internet's underlying routing and addressing standards and might not be aware of their existence.

[411] Steven Epstein, *Impure Science: AIDS, Activism, and the Politics of Knowledge*. University of California Press, 1996, page 350.

Standards like IPv6 are obviously not as visible as the applications, operating systems, and programming languages that users directly engage. Those involved in Internet protocol work are able to do so because of their employment and technical involvement in corporations like Sun Microsystems, Microsoft Corporation, and Cisco Systems. This again raises the question of how corporate interests enter and financial and knowledge barriers impede what outwardly appears to be a democratic, open, and participatory public process. As Shapin and Schaffer described, "A form of knowledge that is the most open in principle has become the most closed in practice. To entertain these doubts about our science is to question the constitution of our society."[412]

Raising questions about the extent of participatory democracy underlying the Internet standards development process evokes Winston Churchill's proclamation about democracy as the worst form of Government except all others. Despite barriers, the standards process does provide the option of private and public participation, is roughly consensus based, has a great deal of transparency in making documents and deliberations publicly available, emphasizes grassroots involvement and resists top-down mandates. But Internet democratization caveats are an important counterweight to the romanticized views of participatory design which ascribe unexamined legitimacy to a somewhat closed process.

5.4 Developing Countries as a Theme in Technology Ascent

Hyperbolic expectations for the IPv6 standard have traversed a spectrum of often antithetical areas ranging from promoting peace and social justice to eradicating poverty in Africa to improving military capabilities. One recurrent thread throughout the history of IPv6 development, adoption, and resource administration was the identification of IPv6 as a precursor for third world economic development. In most cases, attention and concern about development emanated not from institutions or countries "being developed" but by those in the position to do the developing. Outsiders articulated the needs and technical categories of developing countries relative to the IPv6 standard, IPv6 deployment, and IPv6 resources. The IAB's and IETF's 1990 identification of the need

[412] Steven Shapin and Simon Schaffer, *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton: Princeton University Press, 1985, page 343

for a new standard to expand the address space centered on the identification of Internet internationalization and an eventual expansion into developing countries. At this time, IAB and IETF participants were predominantly American and working for companies with ample addresses. They were externally identifying a requirement for more addresses they believed other countries would someday need, but none of them represented a developing country. Similarly, the institutional structure of the IAB, IANA, and IETF proposed the distribution of IP addresses to international registries supporting developing countries. Likewise, those advocating adoption of IPv6, especially individuals within IPv6 advocacy institutions like the IPv6 Forum and NAv6TF, portrayed IPv6 adoption as an intervention aimed at a teleological goal of Internet globalization. The United Nations WGIG recommendations cited the needs of the developing world to bolster their positions. In recommending a diminishment of American power over IP address administration and other governance functions, the WGIG never articulated as a rationale the economic and political benefits for countries participating in the WGIG if they gained greater power over Internet governance. Rather, the WGIG report unambiguously argued that enhancing Internet governance legitimacy required participation of developing countries and development, within these countries, of associated knowledge and technical resources associated with Internet governance. The countries arguing for a diminishment of U.S. influence never stated "we want greater power," instead making a ventriloquist argument that "developing countries need greater power."

Aiming IPv6 as an intervention into a moral space of developing world social and economic needs follows a larger framework portraying the Internet as uniquely positioned to enable third world development. From sociologist Manuel Castells to the United Nations to the Internet Society, this prioritization of the Internet as a lever for third world economic development and social progress is a consistent theme centered around external identification of what is absent elsewhere and what is necessary as an intervention to fill this absence. In addition to prescribing a technical change like IPv6, these institutions also appear to prescribe themselves as solutions. IPv6 selection solidified the role of the IETF in establishing standards, and fifteen years later, the United

Nations prescribed itself as a solution to ensuring developing country representation in Internet governance functions like IP address administration.

5.5 Constructing Technical Inevitability

This historical account also demonstrates the social construction of notions of technical inevitability and technical resistance. Promises of imminent migration to the IPv6 standard have permeated the history of this routing and addressing standard yet implementation realities have been far more abstemious. The Japanese Government mandated nationwide IPv6 migration by 2005. In 2005, the status of IPv6 deployment in Japan had progressed, but was more aptly described as "in trials" rather than in full nationwide production. The European Union prognosticated that IPv4 addresses would be "critically scarce" by 2005, again a timeframe elapsing without any catastrophic Internet collapse and a date in which approximately 35% of the IPv4 address space was still unassigned. In the United States, no significant IPv6 deployments had occurred by 2005, despite Department of Defense IPv6 momentum. If the history of IPv6 thus far is any indication, the two standards, IPv4 and IPv6, could coexist for the foreseeable future.

Some governments have mandated IPv6 adoption while others, particularly the United States, have espoused *laisse faire* approaches of letting the market decide whether to upgrade from IPv4 to IPv6. U.S. IPv6 policies, in part, mirror U.S. government policy on the metric system a century and a half earlier. One incompatibility in comparing the IPv6 standard to the metric system is obviously user transparency. The public would notice a sudden conversion of distance markers on American highway from miles to kilometers, but embedding IPv6 enabled software within newly purchased wireless devices or an associated expansion of an ISP's network to IPv6 support could remain undetected by most computer users. Nevertheless, the centuries-long American rejection of the metric system reinforces how standards are social conventions, portends that upgrading to a new standard in the face of international inertia is not preordained, and also foreshadows the risks of coexisting standards. Historian Ken Alder explained the role of coexisting but distinct standards in the loss of the 1999 NASA satellite, the Mars Climate Orbiter. One group of engineers had used the metric system while another team had used the traditional American system. This disunion resulted in a 6-mile trajectory error and loss of an expensive satellite. The possibility of the long term contemporaneous existence of IPv4 and IPv6 presents its own complications. First, many of the promises of the new standard have assumed homogeneity. In encouraging IPv6 deployment, Vinton Cerf suggested, “The value of IPv6 can be realized only if the deployment effort is broadly based on a global scale.”[413] For example, adequately implementing the IPsec (or any other) encryption protocol as part of IPv6 implementations requires end-to-end protocol homogeneity so it is possible that mixed protocol environments could make networks less secure. The implication is a potential diminishment of individual and institutional privacy because of the possibility of unauthorized surveillance, interception, or modification of unencrypted information. Organizations, individuals, or service providers supporting both IPv6 and IPv4 face additional challenges such as network administration complexities and greater resource requirements (both computers and intellectual resources). It is also possible that some parts of the Internet could, in effect, bifurcate into “IPv6 sections” and “IPv4 sections,” adding technical complexity and network translation burdens, but also potentially establishing an information class system that changes the ubiquitous and free flow of information over the Internet. Both the history of IPv6 and the history of the metric system challenge depictions of IPv6 as a preordained inevitability. IPv6 may never completely replace IPv4. More speculatively, the history of unexpected Internet developments points to the possibility of a radically different development that replaces, obsoletes, or renders irrelevant both standards.

In addition to challenging the presumed inevitability of IPv6, the history of Internet routing and addressing protocols suggests questioning its sufficiency. IPv6 advocacy groups, governments mandating IPv6, and technology companies incorporating IPv6 addresses into appliances and communication devices promote the standard as not only adequate but as self-evidently profuse in providing more addresses than “grains of sand” on the earth. The historical recidivism touting address space superabundance should raise questions about the numerical solvency of the new standard. The expectations of the IPv6 address space follow expectations of the IPv4 standard as a

[413] Vinton Cerf. Quoted on opening web page of European IPv6 Task Force. (Accessed at http://www.eu.ipv6tf.org/in/i-index.php on February 16, 2005).

safety against future address constraints. The 1981 IPv4 standard allowing for approximately 4.3 billion IP addresses seemed profligate in its time and was considered a guarantee against future address depletion. The IPv6 standard, when developed, seemed equally extravagant as a solution to address space exhaustion. The IPv6 address space is orders of magnitude larger than the IPv4 address space and the Internet registries have instituted some conservation policies. IPv6 address assignments are not irrevocable, staving off the IPv4 circumstance of massive address allocations assigned but unused. Nevertheless, at least three historical patterns in network protocols challenge unexamined presumptions of address superabundance: the parallels between assumptions about the address space sufficiency of IPv6 and the decades earlier claims about IPv4; the historical impact of unanticipated applications such as email on Internet address consumption; and statements by Internet pioneers like Leonard Kleinrock questioning the long term adequacy of 128 bits.[414] Questions about IPv6 inevitability and address space adequacy should at least accompany prevailing and unchallenged IPv6 presumptions.

Rather than addressing IPv6 from an exclusively technical standpoint, this analysis has sought to interrogate the political and economic complexities and power struggles behind IPv6 standards development, adoption, and resource administration. This historical examination has hopefully raised some critical questions about prevailing IPv6 technical assumptions and social expectations, identified the finite technical resources of IP addresses as a locus for struggle over control of the Internet, and described a multifaceted connection between politics and technical standards. Decisions about what standard would become IPv6 and about the administrative structure controlling addresses could be reduced, in part, to who would be in control. Despite the Internet standards community's avowed strategy of excising sociological considerations from its architectural decisions, the history of IPv6 indicates that the definition of the Internet, ultimately, is people.

[414] Leonard Kleinrock, public remarks during final panel discussion at the United States IPv6 Summit, Arlington, Virginia, December, 2004.

APPENDIX A:
LIST OF ABBREVIATIONS

3G	Third Generation Wireless
AD	Area Director (within IETF)
ADSL	Asymmetric Digital Subscriber Line
AfriNIC	African Network Information Centre
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ATM	Asynchronous Transfer Mode
BBN	Bolt Beranek and Newman
B-ISDN	Broadband Integrated Services Digital Network
BIT	Binary Digit
BOF	Birds of a Feather Group (within IETF)
BSD	Berkeley Software Distribution
CATNIP	Common Architecture for the Internet
CERNET	China Education and Research Network
CIDR	Classless Inter-Domain Routing
CLNP	ConnectionLess Network Protocol
CNGI	China Next Generation Internet
CNRI	Corporation for National Research Initiatives
DARPA	Defense Advanced Research Projects Agency
DDN-NIC	Defense Data Network-Network Information Center
DNS	Domain Name System
DoD	Department of Defense
EPIC	Electronic Privacy Information Center
FNC	Federal Networking Council
FTP	File Transfer Protocol
GAO	Government Accountability Office
GIG	Global Information Grid
GOSIP	Government Open Systems Interconnection Protocol
GSM	Global System for Mobile Telecommunications
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board or Internet Activities Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies

IDS	Intrusion Detection System
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IMP	Interface Message Processor
IOS	Internetwork Operating System
IP	Internet Protocol
IPAE	Internet Protocol Address Encapsulation
IPng	Internet Protocol Next Generation
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRTF	Internet Research Task Force
ISO	International Standards Organization
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
LACNIC	Latin America and Caribbean Network Information Centre
LAN	Local Area Network
LIR	Local Internet Registries
NAT	Network Address Translation
NAv6TF	North American IPv6 Task Force
NII	National Information Infrastructure
NIR	National Internet Registries
NIST	National Institute of Standards and Technology
NRO	Number Resource Organization
NSAP	Network Service Access Point
NTIA	National Telecommunications and Information Administration
NWG	Network Working Group
OMB	U.S. Office of Management and Budget
OSI	Open Systems Interconnection
PIP	“P” Internet Protocol
POISED	Process for Organization of Internet Standards Working Group
RARE	Reseaux Associés pour la Recherche Européenne
RFC	Request for Comments
RIPE-NCC	Réseaux IP Européens-Network Coordination Centre
RIR	Regional Internet Registry
ROAD	ROuting and ADdressing Group
SIP	Simple Internet Protocol
SIPP	Simple Internet Protocol Plus
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol
SRI NIC	Stanford Research Institute’s Network Information Center

STS	Science and Technology Studies
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domain
TUBA	TCP and UDP with Bigger Addresses
UN	United Nations
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USC-ISI	University of Southern California Information Sciences Institute
VoIP	Voice over Internet Protocol
WCA	Wireless Communication Association
WGIG	Working Group on Internet Governance
WIDE	Widely Integrated Distributed Environment
WSIS	World Summit on the Information Society
XML	eXtensible Markup Language
YAP	Yet Another Protocol

APPENDIX B:
TECHNICAL BACKGROUND - THE INTERNET PROTOCOL

Network Protocols. Computing devices are able to exchange information only if they adhere to a common system of formatting and addressing rules known as protocols. Protocols govern any exchange of information between humans and are so pervasive they are almost transparent. For example, writing a letter requires adherence to protocological conventions: grouping alphanumeric characters into words, separating words into sentences using punctuation, and placing the letter in an envelope bearing the recipient's unique postal address in a predetermined format. The social conventions for writing a letter are analogous to the protocological conventions enabling information exchange between digital computing devices but, rather than providing order to the alphabet, these protocols provide order to another code, binary.

Binary, a code (analogous to the alphabet) which assumes only two values symbolized by a 0 or a 1, represents all information digitally exchanged over a communications network. Binary corresponds well to the on or off states of switches within microprocessors, and unlike a code with more than two values, the two states are easy to distinguish from each other. Various combinations of 0s and 1s are sufficient to encode text, image, video, sound, and any other type of information. Obviously, 0s and 1s are not literally transmitted over a network. What is physically transmitted is either the presence or absence of light over fiber optic cable, voltage variations over copper wire, or frequency variations through free space. It's easier for humans to discuss these transmitted binary signals as long streams of "0s" and "1s" rather than pulses of light.

How do computing and communications devices generate and interpret streams of 0s and 1s?Where does a message begin and end? Which bits represent a message's destination address? Protocols are the standards providing order to information exchange over a communications network. They specify exactly how to represent information in binary code, how to break binary information into manageable units (sometimes termed "packets" or 'frames") prior to transmission, how to append a source and destination address to the bits in a standardized format, and how to apply error detection and correction methods (e.g. adding a "parity bit").

An example of a simple standard that helps organize bits into meaningful information is ASCII (American Standard Code for Information Interchange). When an individual types characters on a keyboard, ASCII automatically specifies the conversion of each letter into an 8-bit binary code. For example, the letter "e" translates into the 8-bit code 01100101. Other common protocols include Ethernet (a LAN or Local Area Network standard); HTTP (HyperText Transfer Protocol) for communications between web servers and browsers; and SONET (Synchronous Optical Network) specifying formats for transmitting information over fiber optic cable. A single instance of information sharing across a network relies on numerous protocols, each performing a distinct function.

Protocol Suites. A network industry convention takes a taxonomic approach of grouping protocols into families, called "network protocol suites." Protocols are hierarchical in that any given protocol depends on those already applied. This hierarchical quality makes protocols conducive to additional schisming of protocol families into "layers," not unlike a Linnaean classificatory approach. Each layer defines a specific function, such as the task of breaking a message into smaller units. "Suites" and "layers" are only *conceptual* categories that help organize protocols and these theoretical layers could be divided in any number of ways. The networking industry has chosen to adopt a conceptual framework called the OSI (Open Systems Interconnection) Model. The OSI Model is a theoretical model for understanding how various protocols contribute to information exchange between computing devices and divides protocol functions into seven groupings (layers), with each subsequent layer building on the previous layer. For example, layer 1 is the "physical layer" defining electrical rules (such as voltage levels and circuit impedances) for transferring data onto a network. An example of a physical layer protocol is the RS-232 serial interface specification. Subsequent layers perform functions such as error control, formatting, and addressing. The OSI Model is a useful framework for thinking about the functions of various protocols but does not always correspond to the layers of working protocol suites, including TCP/IP, which functionally uses four layers. Nevertheless, the networking industry has retained the OSI model as a theoretical framework, even when not at all applicable.

TCP/IP. TCP/IP is the standard language for information exchange via the Internet. To communicate over the Internet, a computing device must "speak" TCP/IP, a system of rules defining how to structure, transmit, and receive information (e.g. information originating from a computer application). By strict definition, TCP/IP is only two protocols - TCP (Transmission Control Protocol) and IP (Internet Protocol) – each performing a distinct function. However, the term "TCP/IP" customarily describes an entire family of protocols known as the TCP/IP protocol suite. For example, it specifies protocols for performing tasks such as file transfer (FTP or File Transfer Protocol), electronic mail (SMTP or Simple Mail Transport Protocol), and remote access to a computer (telnet). The nomenclature "TCP/IP" encompasses more than just TCP and IP and is also a misnomer because some communications over the Internet don't even use TCP. The alternative protocol to TCP, UDP (User Datagram Protocol), is customarily considered part of the TCP/IP suite. TCP/IP, by convention, is the group of protocols that work together to facilitate information sharing over the Internet.

The TCP/IP protocol suite defines a hierarchy of four protocol layers, with each layer specifying a different function and dependent on a preceding layer. The four layers usually associated with the TCP/IP suite are: 1) the network interface layer; 2) the Internet Layer; 3) the transport layer; and 4) the application layer. Assuming information originates from a software application on a computer, a series of protocols adds information (e.g. extra bits sometimes called "headers") to the original data. To attempt a physical analogy, the end result is similar to nested boxes, with a smaller box inside a bigger box inside an even bigger box, etc. The functionality and level of detail defined in each of TCP/IP's four layers is complex but can be summarized as follows. Within a computer, data passes from a software application (like electronic mail) to another piece of software (like TCP) which divides data into manageable pieces and applies formats and routines that make sure data will arrive correctly at a destination. The next step, using the Internet Protocol (IP), applies information to logically address and route the data. Then, a network interface protocol may append a physical address such as a 48-bit address hardwired onto a piece of networking hardware within a computer (a network interface card or NIC). The network interface protocol also transforms the data into an appropriate format for a stream of bits to pass physically from a computer onto a network.

Discussing “Layers” rather than specific protocols helps define the purpose of each protocol but also has the obvious drawback of further abstracting an already abstract subject. Remember that “layers” are only conceptual tools; the “protocol standards” are specifications or rules; and software products loaded onto computers and communications devices (often called “protocol stacks”) are how the standards actually translate into practice. Also, TCP/IP is not necessarily synonymous with the Internet. The TCP/IP protocols are standards for formatting, addressing, fragmenting, delivering, reassembling and checking transmitted information. Any computer network, even a physically isolated one having no connection to the Internet can use TCP/IP protocols. However, many consider the public Internet synonymous with these protocols because it is a global TCP/IP network. The Internet, among other things, is an enormous TCP/IP network.

The Internet Protocol (IP). The Internet Protocol (IP) is part of the TCP/IP family of protocols and implements two functions: addressing and fragmentation. The Internet Protocol appends a header to each packet of information. The header contains routing information such as the destination address and the source address, and the total length of the packet to be transmitted. The function of IP is to deliver (or route) blocks of information from a source to a destination over a complex network. IP is the one TCP/IP protocol needed in almost every instance of information sharing over the Internet. The IP standard specifies a hierarchical addressing scheme assigning a hardware-independent (logical) address to every “device” connected to the Internet. Each device must have a unique address, known as an IP address, to communicate with other devices over the Internet.

IP addresses. IPv4 specifies a unique 32-bit address. In other words, an IPv4 address is a combination of 32 “0s” and “1s” such as the following:

01011110000101001100001111011100.

The above IP address, containing 32 bits, is comprehensible to a computer but awkward for humans to discuss and administer. Therefore, humans rarely write or discuss an IP address in its binary form. Instead, industry convention dictates a shorthand method (termed "dotted decimal format") for discussing and managing IP addresses. An example of dotted decimal format for an IP address is 94.20.195.220 – a format Internet users recognize. This shorthand convention involves a conversion from the binary numbering system (using two digits) computers understand to the decimal numbering system (using ten digits) to which humans are more accustomed.

The mathematical conversion between the computer-readable 32-bit address and the human-readable dotted decimal format address includes three steps: dividing the 32-bit address into four octets (groups of 8 bits), converting each octet into its decimal equivalent, and placing "dots" between each of the four derived decimal numbers. The following is an example of this conversion:

Computer readable IP address: 00011110000101011100001111011101

Divide the IP address into four octets (groups of 8 bits)

00011110
00010101
11000011
11011101

Convert each binary octet into its equivalent decimal number

00011110	= 16+8+4+2 = 30
00010101	= 16+4+1 = 21
11000011	= 128+64+2+1 =195
11011101	= 128+64+16+8+4+1 = 221

Write out the decimal values separated by dots

Human readable IP address: 30.21.195.221

Mathematically, the 32-bit address length would support more than four billion hosts, calculated as 2^{32}, or 4,294,967,296. The randomly chosen IP address listed above, 30.21.195.221, represents one out of the more than four billion addresses.

This "dotted decimal format" is much easier for humans to comprehend, discuss, track, and manage, but not useful to networking equipment. Routers are intelligent computing devices distributed throughout the Internet to read the logical (i.e. hardware independent) destination IP address on each packet and, using "routing tables," direct the packet in the most efficient way towards its destination.

Shorthand notation is even more important for 128-bit IPv6 addresses.[415] The following is an IPv6 address:

011101001001110110000110101011101111010001100100110010010010011101001001
11011000011010101110111101000110010011001001001010111000."

Just like "dotted decimal format" is used as shorthand for an IPv4 address, IPv6 has its own shorthand representation:

X:X:X:X:X:X:X:X,

Where each X is equal to the hexadecimal representation of 16 bits. The convention for IPv6 notation is to use the hexadecimal numbering system. The following is a random example of an IPv6 address in shorthand notation:

FDDC:AC10:8132:BA32:4F12:1070:DD13:6921.

Note that the above shorthand representation of an IPv6 address consists of eight groups of four hexadecimal numbers separated by colons. Each hexadecimal number represents four binary numbers as follows:

Hexadecimal Numeral	Binary Equivalent
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Therefore, the above shorthand representation of an IPv6 address can be translated as follows:

[415] The conventions for IPv6 Notation appear in Robert Hinden and Steve Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture," RFC 3513, April, 2003.

FDDC	= 1111110111011100
AC10	= 1010110000010000
8132	= 1000000100110010
BA32	= 1011101000110010
4F12	= 0100111100010010
1070	= 0001000001110000
DD13	= 1101110100010011
6921	= 0110100100100001

Putting it all together, the “human readable” address

FDDC:AC10:8132:BA32:4F12:1070:DD13:6921

is equivalent to the actual “machine readable” IPv6 address

1111 1101 1101 1100 1010 1100 0001 0000 1000 0001 0011 0010 1011 1010 0011 0010 0100 1111 0001 0010 0001 0000 0111 0000 1101 1101 0001 0011 011 01001 0010 0001.

As cumbersome as the hexadecimal version appears, it’s obviously an improvement over writing out the entire 128-bit string of 0s and 1s as above.

Compressing the Address Further   X:X::X:X

Many IPv6 addresses contain long strings of 0s, and notation conventions can further compress these addresses. For example, the hexadecimal representation:

ADFD:0000:0000:0000:0000:0000:1357:3A11

Is customarily shortened to:

ADFD:0:0:0:0:0:1357:3A11

by dropping the “leading zeros” in each group.

To compress this even further, the symbol “::” customarily indicates one or more groups of 16 bits of zeros.

ADFD::1357:3A11

Sometimes an older IPv4 address is incorporated into an IPv6 address. The framework for this notation is: X:X:X:X:X:X:d.d.d.d,

where the Xs are hexadecimal representations of 16-bit groups and the ds represent standard dotted decimal format. An example of this notation is the following:

0:0:0:0:0:FFFF:15.129.55.9

Header Frame Formats. Each packet of information traversing the Internet contains not only information (payload) but a header providing administrative and routing information about the packet. The header contains the source and destination address, for example. The following two pages depict the header formats for IPv4 and IPv6. Note that the IPv6 header format is significantly simplified relative to the IPv4 header format.

IPv4 Header Format[416]

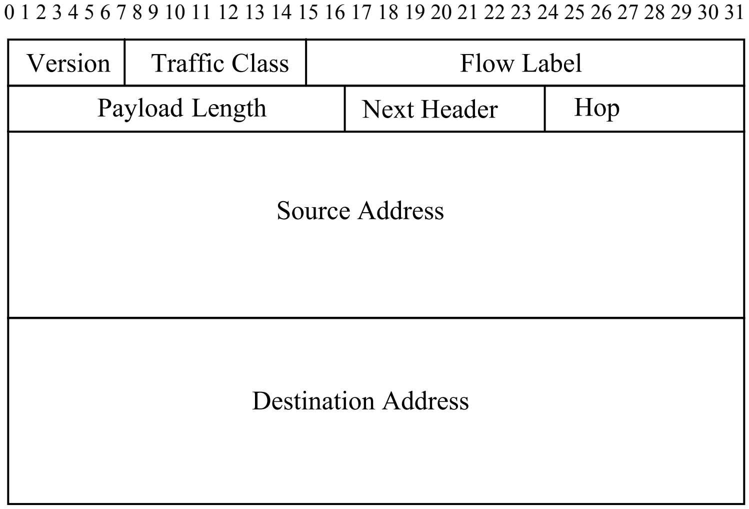
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

<table>
<tr><td>Ver</td><td>IH</td><td>Type of service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="3">Header</td></tr>
<tr><td colspan="6">Source</td></tr>
<tr><td colspan="6">Destination</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Version:	4-bit Internet Protocol version number = 4.
IHL:	4-bit Internet header length.
Type of Service:	8 bits specifying precedence of information.
Total Length:	16 bits, total length of datagram in octets.
Identification:	A sender assigned value to aid fragment assembling.
Flags:	3-bit control flag such as "last fragment."
Fragment Offset:	13 bits indicating where fragment belongs in datagram.
TTL:	8-bit time to live.
Protocol:	8-bit identification of next level protocol.
Header Checksum:	16-bit error detection procedure.
Source Address:	32-bit source Internet address.
Destination Address:	32-bit destination Internet address.
Options:	Variable length field for optional information.
Padding:	Variable length superfluous bits ensuring header ends on 32-bit boundary.

[416] John Postel, editor. "Internet Protocol: DARPA Internet Program Protocol Specification," RFC 791, September, 1981.

IPv6 Header Format[417]



Version: 4-bit Internet Protocol version number = 6.

Traffic Class: 8-bit traffic class field.

Flow Label: 20-bit flow label.

Payload Length: 16-bit assigned integer specifying IPv6 payload length.

Next Header: 8-bit selector identifying type of header following IPv6 Header.

Hop Limit: 8-bit integer decremented by 1 for each node forwarding the packet. Packet is discarded if hop limit is decremented to zero.

Source Address: 128-bit address of packet originator.

Destination Address: 128-bit address of intended packet recipient.

[417] Steven Deering and Robert Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, December, 1998.

APPENDIX C:
SELECTED CLASS A ADDRESS ASSIGNMENT RECORD

IPv4 CLASS A INTERNET ADDRESS
ASSIGNMENTS: 1989 VERSUS 2005
(Each address block contains 16,777,214 addresses)

	1989[418]	**2005**[419]
Internet Address Block	Owner	Owner
000/8	Reserved	IANA - Reserved
001/8	Unassigned	IANA - Reserved
002/8	Unassigned	IANA - Reserved
003/8	General Electric	General Electric
004/8	Atlantic Satellite Network	BBN
005/8	Unassigned	IANA - Reserved
006/8	Yuma Proving Grounds	Army Information Systems Center
007/8	DCEC EDN	IANA - Reserved
008/8	BBN Net	BBN
009/8	IBM	IBM
010/8	ARPANET	IANA-Private Use
011/8	DoD Intel Info. Sys.	DoD Intel Info. Sys.
012/8	AT&T Bell Labs	AT&T Bell Labs
013/8	Xerox Corporation	Xerox Corporation
014/8	Public Data Net	IANA-Public Data Network
015/8	Hewlett-Packard	Hewlett Packard
016/8	Unassigned	Digital Equipment Corporation
017/8	Unassigned	Apple Computer
018/8	MIT	MIT
019/8	Unassigned	Ford Motor Company
020/8	Unassigned	Computer Sciences Corporation
021/8	DDN	DDN
022/8	DISNET	Defense Information Systems Agency
023/8	DDN-TestCell-Net	IANA Reserved
024/8	Unassigned	ARIN
025/8	Royal Signals and Radar	Royal Signals and Radar Establishment
026/8	MILNET	Defense Information Systems Agency
027/8	NOSC/LCCN	IANA Reserved
028/8	Wide Band Sat Net	DSI-North
029/8	MILNET X.25 Temp.	DISA

[418] Sue Romano, Mary Stahl, Mimi Recker, “Internet Numbers,” RFC 1117, August, 1989.

[419] IANA, Internet Protocol V4 Address Space, Updated January 27, 2005. http://www.iana.org/assignments/ipv4-address-space.

030/8	ARPA X.25 Temp	DISA
031/8	UCLA-CATALOG-NET	IANA - Reserved
032/8	Unassigned	Norsk Informasjonsteknology
033/8	Unassigned	DLA Systems Automation
034/8	Unassigned	Halliburton Company
035/8	MERIT Computer Network	MERIT Computer Network
036/8	Stanford University	IANA Reserved
037/8	Unassigned	IANA Reserved
038/8	Unassigned	PSI
039/8	SRI Local Net	IANA Reserved
040/8	Unassigned	Eli Lily and Company
041/8	BBN-GATE-TEST-A	IANA Reserved
042/8	Canadian Rsch Net	IANA Reserved
043/8	Japan Inet	Japan Inet
044/8	Amateur Rad. Exp. Net.	Amateur Radio Digital Comm.
045/8	Trade Show Net	Interop Show Network
046/8	BBN Corp Net	Bolt Beranek and Newman Inc.
047/8	BNR Corp Net	Bell-Northern Research
048/8	Unassigned	Prudential Securities (Dec 1995)
049/8	Unassigned	Joint Technical Command (May 1994)
050/8	Unassigned	Joint Technical Command
051/8	Unassigned	Department of Social Security of UK
052/8	Unassigned	E.I. duPont de Nemours and Co., Inc.
053/8	Unassigned	Cap Debis CCS
054/8	Unassigned	Merck and Co., Inc.
055/8	Unassigned	Boeing Computer Services
056/8	Unassigned	U.S. Postal Service
057/8	Unassigned	SITA
058/8	Unassigned	APNIC
059/8	Unassigned	APNIC
060/8	Unassigned	APNIC
061/8	Unassigned	APNIC
062/8	Unassigned	RIPE NCC
063/8	Unassigned	ARIN
064/8	Unassigned	ARIN
065/8	Unassigned	ARIN
066/8	Unassigned	ARIN
067/8	Unassigned	ARIN
068/8	Unassigned	ARIN
069/8	Unassigned	ARIN
070/8	Unassigned	ARIN
071/8	Unassigned	ARIN
072/8	Unassigned	ARIN
073/8	Unassigned	IANA - Reserved
074/8	Unassigned	IANA - Reserved
075/8	Unassigned	IANA - Reserved
076/8	Unassigned	IANA - Reserved

077/8	Unassigned	IANA - Reserved
078/8	Unassigned	IANA - Reserved
079/8	Unassigned	IANA - Reserved
080/8	Unassigned	RIPE NCC
081/8	Unassigned	RIPE NCC
082/8	Unassigned	RIPE NCC
083/8	Unassigned	RIPE NCC
084/8	Unassigned	RIPE NCC
085/8	Unassigned	RIPE NCC
086/8	Unassigned	RIPE NCC
087/8	Unassigned	RIPE NCC
088/8	Unassigned	RIPE NCC
089/8	Unassigned	IANA - Reserved
090/8	Unassigned	IANA - Reserved
091/8	Unassigned	IANA - Reserved
092/8	Unassigned	IANA - Reserved
093/8	Unassigned	IANA - Reserved
094/8	Unassigned	IANA - Reserved
095/8	Unassigned	IANA - Reserved
096/8	Unassigned	IANA - Reserved
097/8	Unassigned	IANA - Reserved
098/8	Unassigned	IANA - Reserved
099/8	Unassigned	IANA - Reserved
100/8	Unassigned	IANA - Reserved
101/8	Unassigned	IANA - Reserved
102/8	Unassigned	IANA - Reserved
103/8	Unassigned	IANA - Reserved
104/8	Unassigned	IANA - Reserved
105/8	Unassigned	IANA - Reserved
106/8	Unassigned	IANA – Reserved
107/8	Unassigned	IANA - Reserved
108/8	Unassigned	IANA - Reserved
109/8	Unassigned	IANA - Reserved
110/8	Unassigned	IANA - Reserved
111/8	Unassigned	IANA - Reserved
112/8	Unassigned	IANA - Reserved
113/8	Unassigned	IANA - Reserved
114/8	Unassigned	IANA - Reserved
115/8	Unassigned	IANA - Reserved
116/8	Unassigned	IANA - Reserved
117/8	Unassigned	IANA - Reserved
118/8	Unassigned	IANA - Reserved
119/8	Unassigned	IANA - Reserved
120/8	Unassigned	IANA - Reserved
121/8	Unassigned	IANA - Reserved
122/8	Unassigned	IANA - Reserved
123/8	Unassigned	IANA - Reserved
124/8	Unassigned	APNIC

125/8	Unassigned	APNIC
126/8	Unassigned	APNIC
127/8	Unassigned	IANA - Reserved

BIBLIOGRAPHY

Abbate, Janet. *Inventing the Internet*. Cambridge: The MIT Press, 1999.

Aitken, Hugh G. J. "Allocating the Spectrum: The Origins of Radio Regulation," *Technology and Culture*, Volume 35, Issue 4. October, 1994, pp. 686-716.

Aitken, Hugh G. J. *Syntony and Spark: The Origins of Radio*. New York: Wiley & Sons, 1976.

Aitken, Hugh G. J. *The Continuous Wave: Technology and American Radio, 1900-1932*. Princeton: Princeton University Press, 1985.

Alder, Ken. *The Measure of All Things: The Seven-Year Odyssey and Hidden Error that Transformed the World.* New York: The Free Press, 2002.

Alder, Ken. "A Revolution to Measure: The Political Economy of the Metric System in France." In *Values of Precision*, Ed. M. Norton Wise. Princeton: Princeton University Press, 1995, pp. 39-71.

Bijker, Wiebe. *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge: The MIT Press, 1995.

Bijker, Wiebe E., Thomas P. Hughes, and Trevor Pinch. *The Social Construction of Technological Systems*. Cambridge: The MIT Press, 1999.

Berners-Lee, Tim with Mark Fischetti. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. HarperCollins, 1999.

Blumenthal, Marjory S. and David D. Clark. "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," *Communications Policy in Transition: The Internet and Beyond*, Benjamin M. Compaine and Shane Greenstein, eds. Cambridge: The MIT Press, 2001.

Bradner, Scott and Allison Mankin, Editors. *IPng: Internet Protocol Next Generation*. Addison-Wesley, 1996.

Bradner, Scott and Allison Mankin. "IP: Next Generation (IPng) White Paper Solicitation." RFC 1550, Internet Engineering Task Force, Network Working Group. December, 1993.

Bradner, Scott and Allison Mankin. "The Recommendation for the IP Next Generation Protocol." RFC 1752. January, 1995.

Britton, Edward and John Tavs. "IPng Requirements of Large Corporate Networks." RFC 1678, August, 1994.

Bush, Randy and David Meyer. “Some Internet Architectural Guidelines and Philosophy.” RFC 3439. December, 2002.

Callon, Ross. “TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing.” RFC 1347, June, 1992.

Carlson, Richard and Domenic Ficarella. “Six Virtual Inches to the Left: The Problem with IPng.” RFC 1705, October, 1994.

Carpenter, Brian. “Architectural Principles of the Internet,” RFC 1958, June, 1996.

Carpenter, Brian. “Middleboxes: Taxonomy and Issue.” RFC 3234, February, 2002.

Carpenter, Brian. “IPng White Paper on Transition and Other Considerations.” RFC 1671, August, 1994.

Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2001.

Cerf, Vinton. “I Remember IANA.” RFC 2468, October, 1998.

Cerf, Vinton. “IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet “Connected Status,” RFC 1174, August, 1990.

Cerf, Vinton. “The Internet Activities Board.” RFC 1160, May, 1990.

Ceruzzi, Paul. *A History of Modern Computing*. Second Edition. Cambridge: MIT Press, 2003.

Clark, David. “The Design Philosophy of the DARPA Internet Protocols.” Proceedings of SIGCOMM 88, ACM COR Volume 18, Number 4, August, 1988, pp. 106-114.

Clark, David, et. al. “Towards the Future Internet Architecture.” RFC 1287, December, 1991.

Cohen, Danny. “Working with Jon, Tribute delivered at UCLA, October 30, 1998.” RFC 2441, November, 1998.

Commission of the European Communities. *Next Generation Internet – Priorities for Action in Migrating to the New Internet Protocol IPv6*. February 21, 2002. Brussels.

Constant, Edward. *The Origins of the Turbojet Revolution*. Baltimore: The Johns Hopkins University Press, 1980.

Constant, Edward. “Social Locus of Practice.” In *The Social Construction of Technological Systems*, Bijker, Hughes, and Pinch, eds. Cambridge: The MIT Press, 1999.

Crocker, Steve. “Host Software.” RFC 1, April 7, 1969.

Crocker, Steve. “The Process for Organization of Internet Standards Working Group.” RFC 1640, June, 1994.

Curran, John. “Market Viability as an IPng Criteria.” RFC 1669, August, 1994.

David, Paul A., and Partha Dasgupta. *Toward a New Economics of Science*. Research Policy 23, 1994, pp. 487-521.

Deering, Stephen and Robert Hinden. *Internet Protocol, Version 6 Specification*. RFC 1883, (Replaced by RFC 2460) Internet Engineering Task Force, Network Working Group. December, 1995.

Deering, Stephen and Robert Hinden. *Internet Protocol, Version 6 Specification*. RFC 2460, (Replaces RFC 1883) Internet Engineering Task Force, Network Working Group. December, 1998.

Deering, Stephen and Robert Hinden. *Internet Protocol, Version 6 (IPv6) Architecture*. RFC 2401, Internet Engineering Task Force, Network Working Group. December, 1998.

Dixon, Tim. “Comparison of Proposals for Next Version of IP.” RFC 1454, May, 1993.

Douglas, Susan J. *Inventing American Broadcasting: 1899-1922*. Baltimore: The Johns Hopkins University Press, 1987.

Edwards, Paul N. The *Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: The MIT Press, 1996.

Egevang, Kjeld and Paul Francis. “The IP Network Address Translator.” RFC 1631, May, 1994.

Epstein, Steven. *Impure Science: AIDS, Activism, and the Politics of Knowledge*. University of California Press, 1996.

Escobar, Arturo. Encountering *Development, The Making and Unmaking of the Third World*. Princeton: Princeton University Press, 1995.

Ezrahi, Yaron. *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*. Cambridge: Harvard University Press, 1990.

Eric Fleischman, “A Large Corporate User’s View of IPng.” RFC 1687, August, 1994.

Fuller, Vince et. al. “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy.” RFC 1519, September, 1993.

Galloway, Alexander. *Protocol: How Control Exists after Decentralization*. Cambridge: The MIT Press, 2004.

Garnham, Nicholas, "Information Society as Theory or Ideology: A Critical Perspective on Technology, Education, and Employment in the Information Age," *Information, Communication, and Society* 3:2 2000.

Gieryn, Thomas. "Boundary-Work and the Demarcation of Science from non-Science: Strains and Interests in Professional Ideologies of Scientists." *American Sociological Review* 48:781-795, 1983.

Gross, Phill. "A Direction for IPng." RFC 1719. December, 1994.

Gross, Phill and Philip Almquist. "IESG Deliberations on Routing and Addressing." RFC 1380, November, 1992.

Hafner, Katie and Matthew Lyon. *Where Wizards Stay up Late: The Origins of the Internet*. New York: Simon & Schuster, 1996.

Hain, Tony. "Architectural Implications of NAT." RFC 2993, November, 2000.

Harding, Sandra. *Whose Science? Whose Knowledge? Thinking from Women's Lives*. Ithaca, NY: Cornell University Press, 1991.

Hinden, Robert, M. "Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)." RFC 1517. September, 1993.

Hinden, Robert, M. *IP Next Generation.* Communications of the ACM. June, 1996, Vol. 39, No. 6, pp. 61-71.

Hinden, Robert, M. "Simple Protocol Plus White Paper." RFC 1710. October, 1994.

Hirsh, Richard F. *Power Loss: The Origins of Deregulation and Restructuring in the American Electric Utility System*. Cambridge: The MIT Press, 1999.

Hirsh, Richard F. *Technology and Transformation in the American Electric Utility Industry*. Cambridge: Cambridge University Press, 1989.

Huang, Nen-Fu, Han-Chieh Chao, Reen-Cheng Wang, Whai-En Chen, and Tzu-Fang Sheu. "The IPv6 Deployment and Projects in Taiwan." Proceedings of the 2003 Symposium on Applications and the Internet Workshops, IEEE Computer Society, 2003.

Hughes, Thomas. *American Genesi*s. London: Penguin, 1989.

Hughes, Thomas. *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World*. New York: Vintage Books, 1998.

Huitema, Christian. *IPv6: The New Internet Protocol*. Upper Saddle River, New Jersey: Prentice Hall, 1996.

Huitema, Christian. "The H Ratio for Address Assignment Efficiency," RFC 1715, October, 1994.

Huitema, Christian. “Charter of the Internet Architecture Board.” RFC 1601, March, 1994.

Ikeda, Nobuo and Hajime Yamada. “Is IPv6 Necessary?” *Technology Bulletin*: Series #2, GLOCOM, Japan, February, 2003.

Kahin, Brian and Janet Abbate (eds.). *Standards Policy for Information Infrastructure*. Cambridge: The MIT Press, 1995.

Kempf, James and Rob Austein. “The Rise of the Middle and the Future of End to End: Reflections on the Evolution of the Internet Architecture.” Internet Draft, draft-iab-e2e-futures-03.txt, April, 2003 and later RFC 3724, March, 2004.

Knapf, Eric. “Whatever Happened to IPv6? *Business Communications Review*, April, 2001, pp. 14-16.

Kruse, Hans, William Yurcik, and Lawrence Lessig, “The InterNAT: Policy Implications of the Internet Architecture Debate,” *Communications Policy in Transition: The Internet and Beyond*, Benjamin M. Compaine and Shane Greenstein, eds. The MIT Press, 2001.

Lawton, George. “Is IPv6 Finally Gaining Ground?” *IEEE Computer*, August, 2001.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Lessig, Lawrence. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House, 2001.

Libicki, Martin, et al. *Scaffolding the New Web: Standards and Standards Policy for the Digital Economy*. Santa Monica: Rand, 2000.

Lightman, Alex. “Twenty Myths and Truths about IPv6 and the U.S. IPv6 Transition (Such As It Is), *6Sense Newsletter*, June, 2005.

Lightman, Alex. “10 Million New Jobs from IPv6: The Case for U.S. Government Investment,” *6Sense Newsletter*, November, 2004.

Lightman, Alex. “Lead, Follow, or Lose the Great Game: Why We Must Choose a U.S. IPv6 Leader,” *6Sense Newsletter*, April, 2005.

Lightman, Alex. “IPv6 as an Instrument of Freedom Amplification,” *6Sense Newsletter*, April, 2005.

Malkin, Gary. “The Tao of IETF, A Guide for New Attendees of the Internet Engineering Task Force.” RFC 1718. November, 1994.

Mann, Catherine L., Sue E. Eckert, and Sarah Cleeland Knight. *Global Electronic Commerce: A Policy Primer*. Washington, DC: Institute for International Economics, 2000.

McGovern, Michael and Robert Ullman. "CATNIP: Common Architecture for the Internet." RFC 1707, October, 1994.

Mueller, Milton L. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: The MIT Press, 2002.

Mueller, Milton L. *The "Governance" Debacle: How the Ideal of Internetworking Got Buried by Politics*. Proceedings of the Internet Society's INET '98 Conference, Geneva, Switzerland. The Internet Society, 1998, www.isoc.org/inet98/proceedings/5a/5a_1.htm.

Mueller, Milton L. "Competition in IPv6 Addressing: A Review of the Debate," Concept Paper by the Internet Governance Project, July 5, 2005, accessed at http://www.internetgovernance.org.

National Research Council, Computer Science and Telecommunications Board. *Global Networks and Local Values*. Washington, DC: National Academy Press, 2001.

Neuman, Russell W., Lee McKnight, and Richard Jay Solomon. *The Gordian Knot: Political Gridlock on the Information Highway*. Cambridge: The MIT Press, 1998.

Ning, Hua. "IPv6 Test-bed Networks and R&D in China." Proceedings of the 2004 International Symposium on Applications and the Internet Workshops, IEEE Computer Society, 2004.

Partridge, Craig and Frank Kastenholz. "Technical Criteria for Choosing IP the Next Generation (IPng)." RFC 1726, December, 1994.

Popper, Karl. 1963. *Conjectures and Refutations*. New York: Harper and Row.

Popper, Karl. 1966. *The Logic of Scientific Discovery*. London: Routledge.

Postel, John, "DoD Standard Internet Protocol," RFC 760, January, 1980.

Postel, John. "Assigned Numbers," RFC 739, November, 1977.

Postel, John, editor. "Internet Protocol: DARPA Internet Program Protocol Specification." RFC 791, September, 1981.

Rekhter, Yakov. "An Architecture for IP Address Allocation with CIDR." RFC 1518, September, 1993.

Reynolds, Joyce and John Postel. "Assigned Numbers." RFC 870, October, 1983.

Reynolds, Joyce and John Postel. "Assigned Numbers." RFC 900, June, 1984.

Reynolds, Joyce and John Postel. "Assigned Numbers." RFC 923, October, 1984.

Reynolds, Joyce and John Postel. "Assigned Numbers." RFC 943, April, 1985.

Reynolds, Joyce and John Postel. “Assigned Numbers.” RFC 960, December, 1985.

Reynolds, Joyce and John Postel. “Assigned Numbers.” RFC 990, November 1986.

Reynolds, Joyce and John Postel. “Assigned Numbers.” RFC 1010, May 1, 1987

RFC Editor, et. al. “30 Years of RFCs,” RFC 2555, April 7, 1999.

Romano, Sue, et. al. “Internet Numbers.” RFC 1117, August, 1989.

Saltzer, J., D. P. Reed, and D. D. Clark. “End-to-End Arguments in System Design.” ACM Transactions on Computer Systems, Vol.2, No. 4, November, 1984, pages 277-288.

Salus, Peter H. “One Byte at a Time: Internet Addressing.” *The Internet Protocol Journal*, Volume 2, Issue 4, December, 1999.

Shapin, Steven and Simon Schaffer. *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton University Press, 1985.

Skelton, Ron. “Electric Power Research Institute Comments on IPng.” RFC 1673, August, 1994.

Slotten, Hugh R. Radio and Television Regulation: Broadcast Technology in the United States, 1920-1960. Baltimore: The Johns Hopkins University Press, 2000.

Solensky, Frank. *Minutes of the Address Lifetime Expectations Working Group (ALE)*, July, 1994. Documented at ftp://ftp.ietf.cnri.reston.va.us/ietf-onlineproceedings/94jul/ area and.wg.reports/ipng/ale/ale-minutes-94jul.txt.

Staudenmaier, John M. *Technology's Storytellers: Reweaving the Human Fabric*. Cambridge: MIT Press, 1985.

Taylor, Mark. “A Cellular Industry View of IPng.” RFC 1674, August, 1994.

US-CERT Vulnerability Note VU#930892, “Cisco IOS vulnerable to DoS or arbitrary code execution via specially crafted IPv6 packet,” Date Public, July 27, 2005.

US-CERT Vulnerability Note VU#472582, “Cisco IOS IPv6 denial-of-service vulnerability,” Date Public, January 26, 2005.

US-CERT Vulnerability Note VU#658859, “Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 memory leak,” First Public, June 29, 2004.

US-CERT Vulnerability Note VU#370060, “Solaris systems may crash in response to certain IPv6 packets,” First Public, July 21, 2003.

Vecchi, Mario. “IPng Requirements: A Cable Television Industry Viewpoint.” RFC 1686, August, 1994.

Vincenti, Walter G. What *Engineers Know and How They Know It: Analytical Studies from Aeronautical History*. Baltimore: The Johns Hopkins University Press, 1990.

von Burg, Urs. *The Triumph of Ethernet: Technological Communities and the Battle for the LAN Standard*. Stanford: Stanford University Press, 2001.

Weiser, Mark. *Whatever Happened to the Next-Generation Internet?* Communications of the ACM. September, 2001, Vol. 44, No. 9, pp. 61-68.

Wilson, Paul and Chris Buckridge. "IP Addressing in China." *APSTER*, the Quarterly Newsletter of APNIC, Issue 12, December, 2004.