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

1 Introduction[1]

Over the past decade, the Internet has revolutionized computer and communications activities. First envisioned as a tool for facilitating interaction among government and academic researchers, the Internet now touches almost every aspect of society. It has vastly expanded the individual and societal benefits of personal computers by becoming the primary mechanism for the dissemination, retrieval, and exchange of information between and among millions of computer users worldwide.

The social effects of these developments have been immense. The Internet has enabled consumers to shop more conveniently, choose from a wider selection of products and vendors, and customize their purchases. As a result, according to one estimate, consumers spent $12.8 billion online in the first three months of 2003, up 27 percent from the same period in 2002.[2] Similarly, the growth of online distance

---

[1] This Discussion Draft provides an initial examination of the issues raised in the Task Force's January 21, 2004, Request for Comments on IPv6. The views expressed herein are preliminary. *See* National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA), *Request for Comments on Deployment of Internet Protocol, Version 6*, 69 Fed. Reg. 2890 (2004).

[2] BizRate.com, "Consumers Continue to Buy Online in Q1 2003, Despite War and Iraq" (2003), http://merchant.bizrate.com/oa/general/press/release.xpml?rel=144.

learning classes and medical reference Web sites has given people greater access to educational and medical resources. Government agencies and organizations can more easily process requests from and make information available to citizens, thereby facilitating interaction between citizens and government and reducing the costs to government of providing essential services.[3] The Internet also creates opportunities for individuals to participate or to participate more fully in the marketplace of ideas that is the foundation of American democracy.

The Internet's effects on the economy have been equally profound. Litan and Rivlin assert that a major feature of the Internet revolution "is its potential to make the whole economic system, nationally and internationally, more competitive by rendering many markets closer to economists' textbook model of perfect competition, characterized by large numbers of buyers and sellers bidding in a market with perfect information."[4] Although the Internet has helped increase competitive pressures in many product and service markets, it has also equipped many businesses to thrive in the new market environment. Internet-based electronic mail and business-to-business software applications have enabled companies to reduce transaction costs; increase managerial efficiency; and improve the ways in which they transmit billing, inventory, and other information. That, in turn, has allowed companies to bring better products to the market more quickly and at lower cost.

The United States has played a major role in the development of the networks, standards, and conventions that spawned the Internet, and Americans have become major users of IP-based services. As a result, the United States has been and continues to be a major beneficiary of the Internet revolution. Americans' extensive use of the Internet has contributed to the robust performance of our economy over the last decade, both in absolute terms and relative to other nations. America's central role in the creation and operation of the Internet has also put U.S. companies at the cutting edge of information technology markets, which have been a primary engine of economic growth and job creation domestically in recent years. For these and many other reasons, the

---

[3] *See, e.g.,* Robert Litan and Alice Rivlin, "Projecting the Economic Impact of the Internet," 91 *Am. Econ. Rev.* 313 (2001) (noting studies suggesting the Internet can help government reduce the costs of receiving tax returns and registering for permits and licenses).

[4] *Id.* at 315.

United States has a substantial interest in the future evolution of the Internet and in ensuring that U.S. firms can continue to participate fully in that evolution and its economic spillovers.

1.1 THE INTERNET PROTOCOL AND IPV6

This paper focuses on one of the communications protocols[5] that lie at the heart of the Internet — the Internet Protocol (IP), which enables data and other traffic to traverse the Internet and to arrive at the desired destination. IP not only provides a standardized "envelope" for the information sent, but it also contains "headers" that provide addressing, routing, and message-handling information that enables a message to be directed to its final destination over the various media that comprise the Internet.

The current generation of IP, version 4 (IPv4), has been in use for more than 20 years and has supported the Internet's growth over the last decade. With the transformation of the Internet in the 1990s from a research network to a commercialized network, concerns were raised about the ability of IPv4 to accommodate emerging demand, especially the anticipated demand for unique Internet addresses. As a result, the Internet Engineering Task Force (IETF) began work on the next generation IP, which became IP version 6 (IPv6).[6]

IPv6 offers a number of potential advantages over IPv4, most notably a massive increase in the number of Internet addresses. Demand for such addresses will increase as more and more of the world's population request Internet access. Cisco Systems notes that if the 15 largest countries were to assign unique addresses to only 20 percent of their populations, the resulting demand would easily exhaust the remaining

[5] A communications protocol is "a format or set of rules and conventions that control the format and relative timing of message transmission between two points on a computer network." ComWorld Northwest Telecommunications Glossary, www.members.tripod.com/~commworldnw/Glossary.html.

[6] IPv6 can be defined with reference to the IETF Requests for Comments (RFCs) that contain the relevant standards. The "core" draft standards for IPv6 (*e.g.*, RFCs 2460-2463) were approved in August 1998. Currently, more than 70 RFCs comprise the suite of IETF documents that define IPv6. *See* http://www.ietf.org/html.charters/ipv6-charter.html. The IETF continues its efforts to standardize the new protocol. *See* "WG Action: Recharter: IP Version 6 Working Group (ipv6)," http://www1.ietf.org/mail-archive/web/ietf-announce/current/msg00107.html.

For a brief discussion of the reasons for developing a next generation IP and the IETF's activities in that area, see Geoff Huston, "Waiting for IP version 6," at 1-4, *The ISP Column* (Jan. 2003), http://www.potaroo.net/papers/isoc/2003-01/Waiting.html.

supply of IPv4 addresses.[7] Continued growth in mobile telephone and mobile data terminals (such as personal data assistants [PDAs]) will also expand demand for Internet addresses. The situation may become critical if, as some project, a market emerges for in-home devices (*e.g.*, "smart appliances," entertainment systems) that are accessible from outside the home via the Internet.[8] While there is considerable disagreement about whether, to what extent, and at what pace, such demand will develop, IPv6 would provide the address space to accommodate whatever level of demand does emerge.

Besides affording exponentially expanded address space, IPv6 has been designed to provide other features and capabilities, including improved support for header options and extensions, simplified assignment of addresses and configuration options for communications devices, and additional security features. Development of IPv6, moreover, has resulted in enhancements to IPv4. As useful capabilities have been devised for IPv6, protocol developers and manufacturers have worked to incorporate many of those same capabilities into IPv4.[9] As a result, IPv4 can now support, to varying degrees, many of the capabilities available in IPv6.[10] At the same time, additional mechanisms and tools have been developed to mitigate the IPv4 address exhaustion concerns that in large part prompted development of IPv6.

There is a debate within industry about the magnitude of the benefits associated with adopting IPv6 and the timing of their realization. That debate is influenced heavily by the massive embedded base of IPv4 equipment and applications that currently comprise the Internet. Most observers agree that, other things being equal, IPv6-based networks would be superior to IPv4-based networks. Further, as noted above, IPv6 would adequately accommodate increased demand for IP addresses in the event that a proliferation of end-user devices or the emergence of a "killer application" outstrips the existing supply of IPv4 addresses. As important, IPv6 has been designed to afford IPv4 users a migration path to evolve gradually to IPv6-based networks. A central

---

[7] Comments of Cisco Systems, Inc. (Cisco) in response to Request for Comments, Docket No. 040107006-4006-01, at 1. Unless otherwise noted, all subsequent citations to Comments refer to comments filed in response to the January 21, 2004 Request for Comments (RFC). For the text of the RFC, see note 1 *supra*. Copies of those comments are available at http://www.ntia.doc.gov/ntiahome/ntiageneral/pv6/index.html. *See* also Tony Hain (Hain) Comments at 6.

[8] *See*, *e.g.*, Cisco Comments at 1; MCI Comments at 3.

[9] *See, e.g.* Alcatel Comments at 3-4.

[10] *See* Cisco Comments at 6.

policy question concerning IPv6 deployment in the United States is whether the incremental benefits of adopting IPv6 justify the costs of converting the large embedded IPv4 base to IPv6 on an accelerated basis.[11]

Because of those conversion costs, most observers believe that there will be a considerable transition period during which IPv4 and IPv6-based networks will coexist.[12] During that transition, firms will incur costs to ensure interoperability among equipment, applications, and networks, both domestically and internationally. Simultaneous operation of IPv4- and IPv6 may also require additional effort to ensure communications security and to protect networks from attack. These transition costs, in addition to the more obvious direct costs of converting to IPv6, should be considered when assessing the potential benefits of IPv6. Enterprises must determine whether the net present value of the cumulative benefits of deploying IPv6 will exceed the costs of migrating from IPv4 to IPv6.

1.2 CURRENT MARKET ACTIVITIES WITH RESPECT TO IPV6

1.2.1 Domestic Market Activities

Amid the debate over the benefits and costs of deploying IPv6, many domestic and foreign companies have incorporated or are steadily incorporating IPv6 capabilities into their hardware and software products. The two major manufacturers of Internet routers, Cisco and Juniper, have included IPv6 capability in their equipment for several years.[13] Linux operating systems are generally capable of handling IPv6 traffic ("IPv6-capable"),[14] and Microsoft has moved aggressively to make its operating systems IPv6-capable.[15] Indeed, Cisco estimates that about

[11] As used in this document, the term "accelerated" refers to a firm's decision to acquire hardware and software networking components for the purpose of obtaining IPv6 capabilities in advance of the firm's normal replacement cycle.

[12] *See* GSA Federal Technology Service (GSA) Comments at 3; Network Conceptions LLC (Network Conceptions) Comments at 9; VeriSign, Inc. (VeriSign) Comments at 6.

[13] Cisco Comments at 20; Juniper Networks, Inc. (Juniper) Comments at 5.

[14] *See* NTT/Verio Comments at 27. For purposes of this discussion, a network, a piece of equipment, or an application is considered "IPv6-capable" if it can recognize IPv6 addresses and process IPv6 messages once it has been "enabled" or "turned on."

[15] Microsoft Corp. (Microsoft) Comments at 7-8.

one-third of desktop computers currently deployed in the United States are IPv6-capable.[16]

Microsoft is also working to make more of its Windows applications capable of handling the larger IPv6 addresses.[17] Additionally, consumers can download a limited selection of e-mail programs, multimedia software, remote access software, games, and Java applications that can operate in an IPv6 environment. Similarly, network administrators can use access software, domain name system (DNS) servers, firewalls, and World Wide Web servers that can interact with both IPv4 and IPv6 applications.[18]

Despite the availability of IPv6 products in the marketplace, a significant portion of the installed base of equipment in the United States appears to be capable of handling only IPv4 transmissions.[19] Furthermore, IPv6 has not been "turned on" in much of the already installed IPv6-capable equipment and software. In June 2003, the United States Department of Defense (DoD) announced that all hardware and software "being developed, procured, or acquired" for its Global Information Grid (GIG) would have to be IPv6-capable by October 1, 2003.[20] However, DoD apparently does not plan for the GIG to handle significant quantities of IPv6 traffic for several years.[21] The bulk of the IPv6 traffic in the United States appears to be carried by government and university research networks, such as the Abilene backbone network.[22] NTT/Verio is apparently the only commercial provider of IPv6-based Internet access service in the United States.[23] The company estimates that less than

---

[16] Cisco Comments at 20.

[17] Microsoft Comments at 8.

[18] *See* NTT/Verio Comments at 32-37 for a list of IPv6-capable hardware, operating systems, and software applications.

[19] *See* Cisco Comments at 20 (citing wired and wireless end user devices, cable and digital subscriber line (DSL) modems, printers and other peripheral equipment).

[20] *See* John Stenbit, "Internet Protocol Version 6 (IPv6)" (U.S. Department of Defense memorandum of intent June 9, 2003). All IPv6 equipment must also be able to support IPv4. *See also* D.S. Onley, "Defense picks consultant for IPv6 transition," *Government Computer News*, at 5 (May 24, 2004).

[21] *See* Stenbit, note 20 *supra* (indicating that no DoD networks carrying operational data will be converted to IPv6 in the near term); Roswell Dixon, "IPv6 in the Department of Defense," at 9, Presentation at the North American IPv6 Task Force Summit, San Diego, CA, (June 25, 2003), http://www.usipv6.com/ppt/IPv6SummitPresentationFinalCaptDixon.pdf (DoD IPv6 adoption plan contemplates a 5-year transition period with a trial period of approximately 3 years in which IPv6 and IPv4 will be operated simultaneously).

[22] *See* Internet2 Comments at 9 (Abilene network has supported native IPv6 since summer of 2002); Juniper Comments at 5.

[23] NTT/Verio Comments at 29. *See also* Cisco Comments at 20 (noting some private reports that other companies will provide IPv6 service if pressed).

1 percent of the Internet access users in the United States have IPv6 service.[24]

1.2.2 International Market Activities

Commercialization of IPv6 technology appears to be somewhat more advanced in other parts of the world, although market statistics are not readily available, presumably for proprietary reasons. NTT Communications began offering commercial IPv6-based Internet access service in Japan in March 2000. An NTT competitor, Internet Initiative Japan (IIJ), followed suit in September 2000.[25] NTT/Verio reports that Telecom Italia Laboratory was the first company to provide commercial IPv6 service in Europe in July 2001.[26] Juniper indicates that several other companies are conducting commercial pilots in other parts of Europe.[27]

Foreign governments, particularly those in Asia, have taken various steps to promote deployment of IPv6. Japan's support for IPv6 dates back to September 2000, when Prime Minister Mori emphasized the importance of IPv6 research.[28] In 2002–2003, the Japanese government created a tax credit program that exempted the purchase of IPv6-capable routers from corporate and property taxes.[29] Commenters noted, moreover, that in furtherance of the Japanese government's e-Japan initiative, the Ministry of Public Management, Home Affairs, Post and Telecommunications has sponsored an "IPv6 promotion council," which, among other things, has established and promoted an IPv6 Ready Logo program and allocated the equivalent of $70 million for IPv6 research and development.[30] In 2001, the South Korean Ministry of Information and Communication announced its intention to implement IPv6 within the country. In September 2003, the Ministry adopted an IPv6 Promotion Plan that commits $150 million through 2007 for funding

---

[24] NTT/Verio Comments at 29.

[25] *Id.* at 25; Juniper Comments at 6. In April 2001, NTT/Verio launched the first commercial global IPv6 backbone network connecting Japan, Europe, and the United States. NTT/Verio Comments at 25.

[26] NTT/Verio Comments at 25.

[27] Juniper Comments at 6.

[28] *See* http://www.kantei.go.jp/foreign/souri/mori/0921policy.html.

[29] *See* Juniper Comments at 6; NTT/Verio Comments at 30.

[30] *See* NTT/Verio Comments at 30-31; Juniper Comments at 5-6. For further information on the e-Japan initiative, see http://www.kantei.go.jp/foreign/it/network/0122full_e.html. *See also* http://www.v6pc.jp/en/council/detail/index.html.

IPv6 routers, digital home services, applications, and other activities.[31] In December 2003, the Chinese government issued licenses and allocated $170 million for the construction of the China Next Generation Internet (CGNI). The goal is to have that network fully operational by the end of 2005.[32] For its part, the European Commission (EC) in 2001 funded a joint program between two major Internet projects—6NET and Euro6IX—to foster IPv6 deployment in Europe. The Commission committed to contribute up to 17 million euros over 3 years to enable the partners to conduct interoperability testing, interconnect both networks, and deploy advanced network services.[33] The EC has also allocated 180 million euros to support some 40 IPv6 research projects on the continent.[34]

1.3 DEPARTMENT OF COMMERCE IPV6 TASK FORCE

Much of the IPv6 market activity internationally, particularly that in Asia, seems attributable to perceived shortages of IPv4 addresses.[35] However, some have said that foreign governments also see a swift transition to IPv6 as a way to gain a competitive advantage in the equipment and applications markets.[36] This, in turn, has raised concerns about the pace of IPv6 deployment within the United States and whether a "lag" in U.S. deployment could jeopardize the competitiveness of domestic firms in cutting-edge information technology markets.

To address these and other concerns about deployment of IPv6 in the United States, the President's *National Strategy to Secure Cyberspace* directed the Secretary of Commerce to "form a task force to examine the issues related to IPv6, including the appropriate role of government,

---

[31] *See* Sangjin Jeong, "IPv6 Deployment and its Testing Activities in Korea," at 9 (Sep. 22, 2003), http://www.ipv6event.be/v6kim.pdf.

[32] *See* Cisco Comments at 22; Juniper Comments at 6. It has been reported that 50 percent of the CNGI project will go to local vendors. *See* Cisco Comments at 22.

[33] *See* "Europe Drives Next Generation Internet Deployment" (Dec. 4, 2001), http://www.euro6ix.org/press/Joint_Press_Release_v12.pdf .

[34] *See* Juniper Comments at 6; Jordi Palet, "IPv6 in Europe: From R&D to Deployment," http://usipv6.com/6sense/2004/june002.htm.

[35] *See, e.g.*, NTT/Verio Comments at 25.

[36] *See, e.g.*, Nobuo Ikeda and Hajime Yamada, "Is IPv6 Necessary?", Glocom Tech Bulletin #2, at 2, 12 (Feb. 27, 2002), http://www.glocom.org/tech_reviews/tech_bulle/20020227_bulle_s2.html; Motorola, Inc. (Motorola) Comments at 5; Michael Dillon (Dillon) Comments at 1. *See also* Cisco Comments at 22 (Chinese carriers may feel political pressure to showcase China as a technology leader).

international interoperability, security in transition, and costs and benefits."[37]

Formed in October 2003, the Task Force is co-chaired by the Administrator of the National Telecommunications and Information Administration (NTIA) and the Director of the National Institute of Standards and Technology (NIST) and consists of staff from those two agencies, with the assistance of a consultant, RTI International (RTI). In January 2004, the Task Force published a Request for Comments (RFC) on various IPv6-related issues in the *Federal Register*.[38] This draft provides a preliminary discussion of the questions presented by the ongoing deployment of IPv6 both domestically and internationally, including those issues identified in the *National Strategy*. This discussion is informed by the comments submitted in response to the RFC and by extensive contacts with private- and public-sector stakeholders by RTI and Task Force staff.

Section 2 of the discussion draft provides an analysis of the potential benefits of IPv6, as compared to IPv4. It also outlines the principal direct and indirect costs that entities will likely incur to deploy IPv6. We anticipate that this general cost/benefit analysis will be supplemented by a more detailed economic study conducted by RTI, to be released at a later date. Section 3 evaluates the competitiveness concerns that may stem from differences between nations in the timing and pace of IPv6 deployment. It also considers issues related to the interoperability of IPv4 and IPv6 equipment and networks across national borders. Finally, Section 4 examines possible rationales for U.S. government action to influence domestic IPv6 deployment and discusses several potential areas for such action. The Task Force will discuss this draft paper at a public meeting to be held in July 2004.

---

[37] *The National Strategy to Secure Cyberspace*, A/R 2-3, at 30 (Feb. 2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf .

[38] *See* note 1 *supra*.

2 Benefits and Costs of Adopting IPv6

Industry stakeholders and Internet experts generally agree that IPv6-based networks would be superior to IPv4-based networks. The increased address space available under IPv6 could stimulate development and deployment of new communications devices and new applications, and could enable network restructuring to occur more easily. The redesigned header structure in IPv6 and the enhanced capabilities of the new protocol could provide significant benefits to Internet users, network administrators, and applications developers. IPv6 could also simplify the activation, configuration, and operation of certain mobile networks and services.

Widespread adoption of IPv6 would likely entail substantial transition costs, because the Internet today is comprised almost entirely of IPv4-based hardware and software. Furthermore, as noted above, many of IPV6's enhanced capabilities have also been made available in IPv4. As a result, producers and consumers may continue to use IPv4 for some period of time (perhaps with further augmentation) to avoid or to defer the costs of upgrading to IPv6. Many of the prospective benefits of IPv6, moreover, appear to be predicated on the removal or modification of Network Address Translation (NAT) devices (*see* Section 2.1.1), and modification of firewalls and other "middleboxes" that affect direct communications between end-user devices via the Internet. It remains to be seen whether or when such devices will be either phased out or made transparent to end-to-end (E2E) Internet communications and applications.

In this section, we discuss the benefits and costs of adopting IPv6. After first evaluating the potential benefits of deploying IPv6, we discuss the nature and relative magnitude of the costs that enterprises and individuals may incur to deploy IPv6. To make this general discussion more concrete, we also provide a case study that illustrates potential transition costs for a small or medium-sized business. Finally, we discuss transition issues and costs that are of particular importance in assessing the net economic impact of adopting IPv6. We intend to supplement this general benefit-cost analysis with a more detailed assessment to be conducted in the next stage of our work.

2.1 Relative Benefits of IPv6 vs. IPv4

There appears to be a general consensus about the types of benefits that could follow from widespread adoption of IPv6. There is, however, disagreement about the size of those benefits and whether the incremental benefits of IPv6 (versus IPv4) for some or all users would outweigh the costs of an accelerated transition from IPv4 to IPv6.[39] This section discusses the potential net benefits of adopting IPv6, as identified by RFC commenters, RTI interviews, and the available literature.

2.1.1 Increased Address Space

The principal by-product of deploying IPv6 would be a large increase in the number of available IP addresses. The 32-bit address field in the IPv4 packet header provides about 4 billion ($4x10^9$) unique Internet addresses.[40] The 128-bit address header in IPv6, in contrast, provides approximately $3.4x10^{38}$ addresses, enough to assign literally trillions of addresses to each person now on earth or even to every square inch of the earth's surface.[41]

The vast pool of addresses available under IPv6 would, at a minimum, "future proof" the Internet against potential address shortages resulting from the emergence of new services or applications that require large quantities of globally routable Internet addresses.[42] In this regard, there are reasons to believe that demand for IP addresses could expand considerably in future years. The very success of the Internet will likely increase pressures on existing IPv4 address resources, as more and more people around the globe seek IP addresses to enjoy the benefits of Internet access.[43] The burgeoning demand for "always-on" broadband services (*e.g.*, DSL and cable modem services) and the expected proliferation of wireless phones and wireless data devices (*e.g.*, personal data assistants [PDAs]) may further deplete the available IPv4 address

---

[39] The timing of the transition from IPv4 to IPv6 for any particular adopter could dramatically affect the costs incurred and the benefits realized.

[40] *See* Microsoft Comments at 3 (4.3 billion addresses); Sprint Corporation (Sprint) Comments at 3 (same).

[41] *See* Sprint Comments at 3 ($1x10^{30}$ addresses for every person); Joe St. Sauver, "What's IPv6 . . . and Why Is It Gaining Ground?", http://cc.uoregon.edu/cnews/spring2001/whatsipv6.html ($3.7x10^{21}$ addresses per square inch).

[42] *See*, *e.g.*, NTT/Verio Comments at 10-11 (future applications that could benefit from expanded IPv6 address space).

[43] *See* North American IPv6 Task Force (NAv6TF) Comments at 4.

space.[44] If consumers are drawn to devices (*e.g.*, smart appliances, in-home cameras and entertainment systems, automobile components or subsystems) that can be remotely accessed and controlled via the Internet and that require fixed, globally accessible Internet addresses, the demand for IP addresses may overwhelm the remaining pool of IPv4 addresses.[45] Although it is difficult to predict whether or when these developments may threaten the existing supply of IP addresses, the availability of virtually unlimited IPv6 addresses would enable Regional Internet Registries (RIRs)[46] and Internet service providers (ISPs) to accommodate any sharp spike in demand.

At the same time, adoption of IPv6 could provide an opportunity to reform and rationalize the current system for allocating Internet addresses, because IPv6 would create a vast new and unpopulated address space. The historical allocation of IPv4 addresses has provided organizations in North America, Europe, and Australia with the majority of currently assigned IPv4 address blocks. A large portion of those addresses remain unused. Although, as discussed below, current allocation policies have improved, no incentives have been created to prevent "warehousing" of IP addresses[47] or to encourage the return of unused IP addresses. As a result, many organizations still have very large address blocks that have never been fully used and may never be reclaimed in the absence of concerted action by governments or by Internet registries.[48] Deployment of IPv6 creates an opportunity to use the lessons learned from the past to develop more efficient allocation policies for IPv6 addresses.

---

[44] *See* Cisco Comments at 1; MCI Comments at 3; Motorola Comments at 4; NTT/Verio Comments at 5, 10. In contrast, one commenter questions w hether each new mobile device will need its own IP address. *See* Network Conceptions Comments at 7.

[45] *See* Cisco Comments at 2; Dillon Comments at 1; GSA Comments at 2, 6; NTT/Verio Comments at 10.

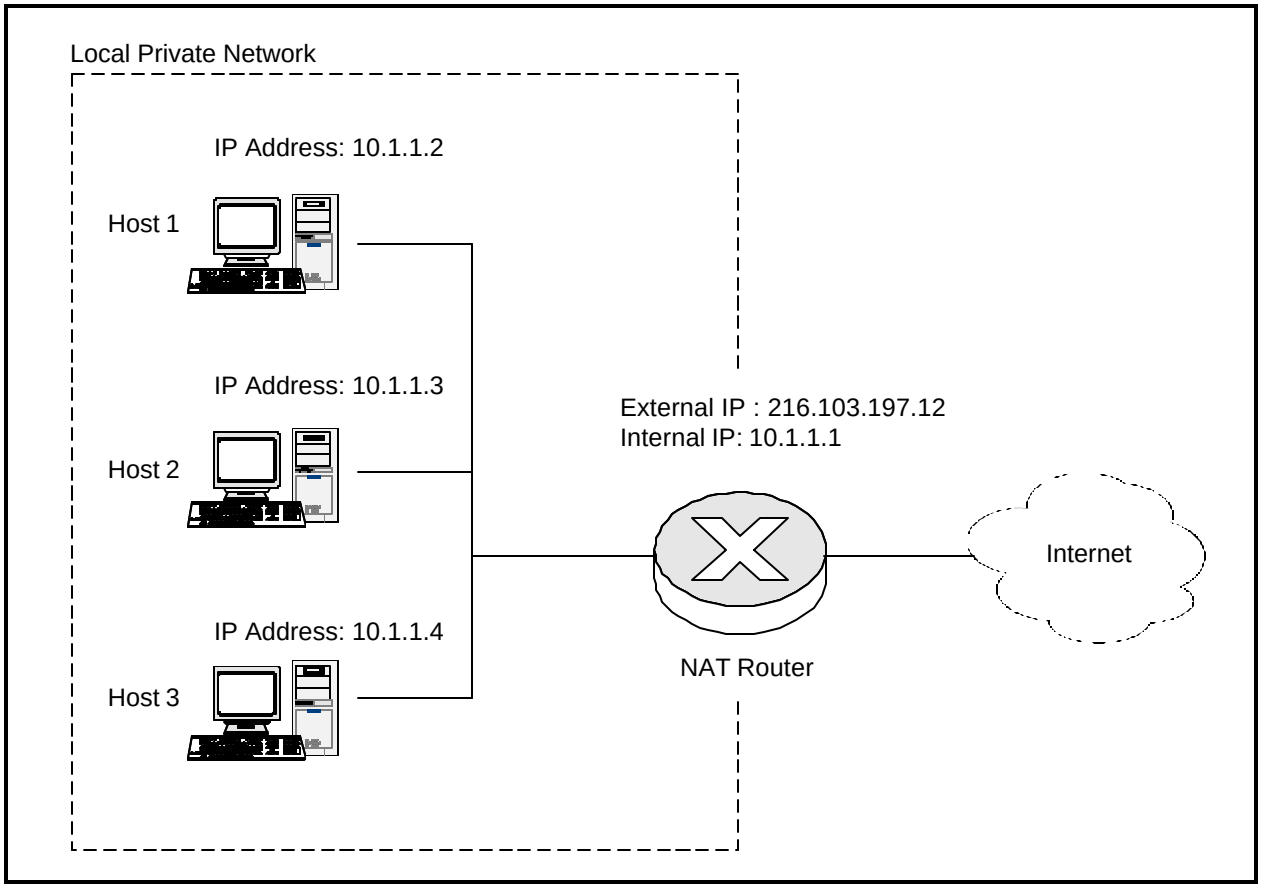
[46] RIRs are responsible for allocating IP address space to organizations (and in some cases individuals) in their respective regions. The American Registry of Internet Numbers (ARIN) is the RIR for the United States.

[47] *See* VeriSign Comments at 2. Some reclamation has occurred. Stanford University, which was originally allocated nearly 17 million IP addresses, restructured its network in 2000 and gave back a Class A address block equal to approximately 16 million IP addresses. *See* Carolyn Marsan, "Stanford Move Rekindles 'Net Address Debate,'" NetworkWorldFusion (Jan. 24, 2000), http://www.nwfusion.com/news/2000/0124ipv4.html.

[48] Current Regional Internet Registry (RIR) policies state that unused address space should be returned to the RIR that allocated the addresses. There is limited enforcement of this policy. Consequently, few IP addresses have been reclaimed. *See* the American Registry for Internet Numbers (ARIN) Web site, www.arin.org, for the specific policies.

Finally, the massive increase in IP addresses made available by IPv6 deployment could reduce the need for NATs. A NAT is a hardware device often placed between a private network and the Internet to allow a large number of hosts on the private network to share a smaller number of globally routable, "public" IP addresses for communications over the Internet.[49] For internal communication, each host is assigned a locally-unique private IP address (see Figure 2-1). As the term implies, a NAT converts the private source address in outgoing communications to a

Figure 2-1. NAT Operating between a Private Network and the Internet



globally routable IP address. In many implementations, an external address is assigned only for the duration of a communications session originated by an internal host, and the internal host cannot receive communications originated from the outside. Because NATs are an

[49] Because NATs use port address translation (PAT), NAT/PAT could be used where NAT is referenced in this discussion.

effective way for many hosts to share a single or a small group of public IPv4 addresses, they have proven to be a popular way to slow the consumption of IPv4 addresses. Because adoption of IPv6 would eliminate concerns about address conservation, NATs would not be needed for that purpose in an IPv6 environment.[50]

Although NATs provide benefits for end users, as discussed below, they also complicate the use and development of new E2E networking applications.[51] Without NATs, applications such as Voice-over IP (VoIP) and real-time videoconferencing could be implemented much more simply, because a direct connection (*i.e.*, IP address to IP address) could be initiated to any host, without the need to establish additional protocols and procedures to traverse one or more NAT devices. Some commenters assert that without NATs, various features of IPv6 (such as connectivity via a wider range of media and delivery mechanisms, the ability to maintain several simultaneous access paths for multiple parties without manual intervention, improved speed, and quality of connections) could spur the deployment of new E2E applications.[52]

Indeed, advocates contend that widespread deployment of IPv6 (and removal of NATs) would permit a return to the original "open scheme" of the Internet, based on E2E connectivity.[53] One commenter suggests that the existing IPv4 infrastructure can be compared to the code of a large software application—after years of adding work-arounds and patches, it is sometimes simpler to replace the application and develop a streamlined program with which to move forward, rather than to continue patching.[54] Representatives of Nortel Networks have stated that designing the next generation of Internet applications will be simplified when using IPv6 because it avoids the more than 20 years of work-arounds embedded in IPv4, in part, to support E2E applications.[55]

Supporters of IPv6 also believe that, to the extent that use of IPv6 obviates the need for NATs, adoption of IPv6 would stimulate the development and deployment of innovative E2E applications. This would occur, they claim, because applications designers would be able to

---

[50] *See* Hain Comments at 3.

[51] *See id.* at 2.

[52] *See* Cisco Comments at 2; Internet2 Comments at 2-3; Microsoft Comments at 5; NAv6TF Comments at 6.

[53] *See*, *e.g.*, Internet2 Comments at 1-2.

[54] *See* Hain Comments at 11.

[55] This information was gained in interviews with representatives of Nortel Networks.

"focus on core products and services, rather than network logistics."[56] More specifically, designers could avoid the time and effort needed to develop work-arounds that enable specific E2E applications to operate in a NATed environment. IPv6 supporters contend that those work-arounds may not scale well in all environments,[57] may reduce the performance and robustness of the associated applications, and may increase the cost and complexity of network management.[58] In their view, if designers are not distracted by the need for NAT work-arounds, new services and applications could be brought to market quicker and at a lower cost.

Although deployment of IPv6 promises significant benefits from the concomitant increase in address space, several factors may limit full realization of those benefits, at least in the near term. For example, although concerns about IPv4 address exhaustion drove development of IPv6,[59] steps have been taken to conserve addresses and to improve the efficiency of address allocation.[60] As a result, many observers believe that the United States, Western Europe, and Australia may not experience address space concerns for some time.[61] Even in those areas of the world that are most concerned about potential exhaustion of IPv4 addresses (*e.g.*, India and the Pacific Rim countries), some observers still question whether the problem is so severe as to warrant accelerated adoption of IPv6.[62]

Additionally, in response to concerns about the perceived shortage of IPv4 addresses stemming from historical address allocation policies,[63] the Regional Internet Registries (RIRs) have reorganized themselves in

---

[56] Hain Comments at 2. *See also* Cisco Comments at 8 (unfettered E2E will allow for more rapid prototyping of new services, which is critical to developing those services). Alcatel Comments at 3; MCI Comments at 3.

[57] *See* Cisco Comments at 5-6 (work-arounds scale well in most consumer markets, less well for enterprises and service providers).

[58] *See* Internet2 Comments at 4. The task of creating work-arounds typically must be repeated for each new application and frequently for differing types of NATs.

[59] *See*, *e.g.*, Network Conceptions Comments at 1; Sprint Comments at 1.

[60] *See* Alcatel Comments at 2 (*e.g.,* deployment of NATs, implementation of Classless Inter-Domain Routing [CIDR], use of Dynamic Host Configuration Protocol [DHCP]).

[61] *See*, *e.g.*, Cisco Comments at 1.

[62] *See* John Lui, "Exec: No Shortage of Net Addresses," CNET News.Com (June 23, 2003), http://news.com.com/2100-1028_3-1020653.html (interview with Paul Wilson, director general of the Asia-Pacific Information Centre [APNIC]); Nobuo Ikeda and Hajime Yamada, note 36 *supra*. Indeed, there are widely different estimates as to when the existing supply of IPv4 addresses may finally run out. *See, e.g.,* Lui, *supra* (estimate of Paul Wilson); Geoff Huston Comments *passim*; NTT/Verio Comments at 2-10.

[63] *See* notes 47 and 48, *supra*, and accompanying text.

recent years to ensure that, prospectively, all regions are allocated IP addresses through a fair, transparent, and efficient process.[64] IPv4 address blocks are currently allocated to the RIRs from a common global pool, using agreed upon criteria and methodology.[65] When a region requests more addresses, they are allocated to the RIR on a need-justified basis.[66] As a result of these changes, the regional distribution of remaining IPv4 addresses now mirrors the global distribution of IP networks themselves. Consequently, the allocation scheme should no longer be the cause of any perceived regional shortages of IPv4 addresses.[67]

To capture fully the address benefits of IPv6, stakeholders will need to take early steps to create mechanisms that allocate IPv6 addresses fairly and efficiently. The North American IPv6 Task Force (NAv6TF) indicates that some organizations have had trouble getting IPv6 addresses recently and suggests that allocation procedures may need to be changed so that IPv6 addresses can be obtained more easily. Otherwise, NAv6TF avers, widespread IPv6 adoption (and the potential associated benefits) might be stalled or precluded.[68] At the same time, VeriSign emphasizes the need for allocation policies that discourage "warehousing" of IPv6 addresses to prevent inefficient consumption of those addresses.[69]

More importantly, adoption of IPv6 may not prompt a return to the "open architecture" originally envisioned by the designers of the Internet. In fact, as the commercialization of the Internet has proceeded, the network has diverged considerably from the original end-to-end design, and there is little evidence that a substantial number of stakeholders want to return

---

64 *See, e.g.,* Ripe NCC, "Global Distribution of IP-Addresses," http://www.ripe.net/ripencc/faq/general/qa2.html.

65 Andrew McLaughlin, "Bad Journalism, IPv6 and the BBC," *Circle ID* (Nov. 7, 2003), http://www.circleid.com/article/369_0_1_0_C/.

66 Lui, note 62 *supra*.

67 Steps taken to improve the allocation of IP addresses on a going-forward basis will not correct imbalances in past allocations. The relevant authorities may need to enact measures to reclaim previously allocated but unused addresses or address blocks.

68 NAv6TF Comments at 34. ARIN's procedures currently dictate that only ISPs can apply for and receive IPv6 addresses, although a proposed rule could change that policy. ARIN, "IPv6 Address Allocation an Assignment Policy, June 26, 2002," http://www.arin.net/policy/ipv6_policy.html. ARIN is considering a proposal to change its allocation policy. ARIN, "Public Policy Proposal 2004-3: Global Addresses for Private Network Inter-Connectivity," http://www.arin.net/policy/2004_3.html.

69 VeriSign Comments at 2, 8.

to that design.[70] Although NATs may frustrate application designers and service providers, users and network administrators often realize economic and security-related benefits from using NATs in their networks. By reducing the number of "public" Internet addresses that an organization may need, use of NATs can reduce that organization's payments to Internet service providers (ISPs) for address space. Moreover, although it was not their original purpose, NATs are often used to provide anonymity for a network and its hosts. In effect, NATs provide a form of "security through obscurity," thereby enabling network operators to block externally initiated contacts and to hide internal hosts.[71] Networks that adopt IPv6 may therefore be reluctant to dispose of their NATs, even if address conservation is no longer a concern.

Additionally, concerns about security in the rambunctious Internet environment have prompted organizations to deploy a range of "middleboxes" (*e.g.*, firewalls, intrusion detection and prevention systems) that, like NATs, break or purposely inhibit E2E communications. Indeed, those devices have become essential elements of most current enterprise networks and are commonly used to enforce network security policies that have emerged since the Internet was first developed.[72] Few, if any, network operators will be likely to remove those devices should they decide to implement IPv6. In short, the ability to exploit the virtually unlimited IPv6 address space to support a growing number of networked devices or to stimulate development of innovative E2E Internet applications and services will likely be offset by several relevant factors—a continuing supply of IPv4 addresses, any perceived difficulties with obtaining IPv6 addresses, a possible reluctance to eliminate NATs and other middleboxes that affect E2E applications, and an absence of compelling applications that require E2E connectivity.

2.1.2 Increased Security

A number of commenters contend that IPv6 will provide a greater level of security than is available under IPv4. NTT/Verio states that because IPv6 was "designed with security in mind," it is inherently more secure

---

[70] *See* BellSouth Comments at 4-5. *See also* Interview with John Streck, Centaur Labs (Mar. 2004) (likelihood of the world, or even United States alone, moving completely back to the "open architecture" Internet model is not very high).

[71] *See* Alcatel Comments at 4; NTT/Verio Comments at 13-14.

[72] *See* Cisco Comments at 5.

than IPv4, which does not have integrated security fields.[73] Other commenters note that support for Internet Protocol Security Architecture (IPsec) is "mandatory" in IPv6, but only "optional" in IPv4, which should lead to more extensive use of IPsec in IPv6 networks and applications.[74] BellSouth suggests that incorporating IPsec into the IPv6 protocol stack may reduce incompatibility between different vendors' implementations of IPsec.[75]

Widespread deployment of IPv6 may indeed produce security benefits in the long term. The near-term benefits are less clear, however. Although IPsec *support* is mandatory in IPv6, IPsec *use* is not. In fact, many current IPv6 implementations do not include IPsec.[76] On the other hand, though optional, IPsec is being widely deployed in IPv4.[77] Several commenters state that there are no significant functional differences in the performance of IPsec in IPv6 and IPv4 networks.[78] Any differences in performance are attributable to the presence of NATs in most IPv4

---

[73] NTT/Verio Comments at 13. *See also* Microsoft Comments at 11 (IPv6 is a "new, more secure protocol" that could help make North America a "Safe Cyber Zone").

[74] *See*, *e.g.*, Cisco Comments at 3; GSA Comments at 6; MCI Comments at 4. IPsec is a set of protocols developed by the IETF to support the secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec consists of 2 optional security headers: Encapsulating Security Payload (ESP), which can provide both encryption and integrity-protection, and Authentication Header (AH), which provides only integrity-protection. The ESP header is more widely used. Both headers support two modes -- transport and tunnel. In transport mode using ESP, IPsec protects only the data portion (payload) of each packet but leaves the header untouched. In tunnel mode with ESP, IPsec protects both the payload and the inner header (that of the ultimate recipient), but leaves the outer header untouched. On the receiving side, an IPsec-compliant device decrypts and authenticates each packet. For IPsec to work, the sending and receiving devices must agree on secret (symmetric) keys, which are used to provide encryption and integrity-protection. This is accomplished through a protocol known as Internet Key Exchange (IKE), which also allows the peers to mutually authenticate using digital certificates or other methods, and which negotiates the IPsec protections to be provided and the cryptographic algorithms to be used.

[75] BellSouth Comments at 3. The massive increase in addresses made possible via IPv6 may enhance security by making it difficult for "hackers " to identify and to attack IP addresses by performing exhaustive address and port sweeps. *See* Cisco Comments at 3.

[76] *See*, *e.g.*, Alcatel Comments at 4; BellSouth Comments at 3; Cisco Comments at 3, 17; Internet2 Comments at 3; VeriSign Comments at 9. Although most parties believe that increased use of IPsec will improve security, other commenters are less certain. Motorola asserts that IPsec, in its current form, cannot defend against denial of service attacks. Motorola Comments at 4. BellSouth questions whether IPsec can strictly eliminate "spoofing." BellSouth Comments at 4. More broadly, VeriSign suggests that IPsec may have been rendered irrelevant by the rise of attacks and security threats for which IPsec-based solutions are either unhelpful or counterproductive. VeriSign Comments at 2. Other commenters note that IPsec provides only network-level security and, as a result, may need to be supplemented by other measures. *See* Alcatel Comments at 3 (need to secure critical subsystems such as neighbor discovery, routing, DBC); Electronic Privacy Information Center (EPIC) Comments at 2 (need to secure applications).

[77] *See* Qwest Communications International Inc. (Qwest) Comments at 4; VeriSign Comments at 2.

[78] *See* BellSouth Comments at 3; Cisco Comments at 3; Internet2 Comments at 3.

networks, which interfere with E2E communications using IPsec.[79] Thus, to the extent that NATs persist in IPv6 networks, they may reduce the security benefits available via the new protocol.[80]

The principal impediment to widespread use of IPsec appears to be the absence of a public key infrastructure (PKI) and associated trust models, which are necessary to effectively manage widespread IPsec operations.[81] In this regard, the social and business aspects of establishing identities and trust relationships (*e.g.*, privacy concerns and legal considerations) will likely be more difficult to resolve than the technical issues.[82] Until these issues are resolved and the required security infrastructure is created, IPv6 is not likely to stimulate any more use of IPsec than IPv4 does today.[83]

Furthermore, experts generally agree that implementing any new protocol, such as IPv6, will be followed by an initial period of increased security vulnerability and that additional network staff will be necessary to address new threats posed by a dual network environment.[84] IPv4 currently benefits from 20 years of identifying and addressing security issues. As IPv6 becomes more prevalent, many security issues will likely arise as attackers give it more attention. On the other hand, the experience gained from running IPv4 networks will help bring security levels in IPv6 networks up to the level of current IPv4 networks fairly rapidly.[85]

The implications of IPv6 and IPsec deployment for law enforcement are similarly ambiguous. Widespread use of IPsec to encrypt communications may reduce law enforcement agencies' ability to monitor criminal activities over the Internet, particularly when IPsec is used in conjunction with IPv6 mobility.[86] To the extent that deployment

---

[79] *See* Internet2 Comments at 3; MCI Comments at 5. Cisco asserts that work-arounds are becoming available that will permit E2E IPsec even across NATs. Cisco Comments at 3.

[80] Some commenters suggest that the removal of NATs to implement IPsec fully may reduce security for some users. *See, e.g.,* Motorola Comments at 3.

[81] *See* BellSouth Comments at 3; Cisco Comments at 3; Hain Comments at 4; NAv6TF Comments at 9; NTT/Verio Comments at 15.

[82] *See* BellSouth Comments at 4.

[83] *See id.* at 3-4.

[84] *See id.* at 7; Cisco Comments at 14; Network Conceptions Comments at 9.

[85] *See* Internet Security Alliance (ISA) Comments at 2.

[86] *See* NTT/Verio Comments at 16. This tension mirrors that experienced by users and network administrators. Although implementation of IPsec allows users to protect the secrecy of their communications traffic, IPsec encryption can reduce security for network administrators by denying them the ability to monitor the content of each

of IPv6 enables the assignment of static IP addresses to most or all end-user devices, adoption of IPv6 could enhance the traceability of illegal or harmful communications back to their source.[87] Users could still employ NATs to give themselves some anonymity, even in IPv6 networks, and thus limit traceability of their communications.[88] Furthermore, IPv6 has a "privacy extension" option in its autoconfiguration feature that enables users to randomize their IPv6 addresses or to generate temporary addresses that are independent of the identification label embedded in user devices.[89] Such addresses are traceable to the ISP or customer demarcation point but are more difficult to trace beyond those points. As a result, it may be challenging for law enforcement authorities to trace a specific node or device as it moves between attachment points or over extended periods of time.[90] Authorities will have to develop new tools and procedures to address these potential problems.[91]

In summary, 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 in IPv4, and IPv4 networks will continue to have at least the same level of security issues as they do currently. In the long term, however, security may well increase as a result of increased use of IPsec.

2.1.3 Simplified Mobility[92]

Various commenters anticipate a rapid growth in the potential number of mobile or portable devices that may connect to the Internet. NTT/Verio notes that the use of mobile phones for email and database browsing in Japan has been growing rapidly.[93] Sprint suggests that the emergence of mobile data services such as wireless data, picture mail, and text messaging could drive the adoption of IPv6.[94] Motorola argues further that IPv6 offers exciting opportunities for wireless sensor networks and

---

packet stream for hostile content. *See* Hain Comments at 4. IPsec-based packet encryption may also defeat network security screening activities by firewalls and intruder detection systems.

[87] *See* Cisco Comments at 3. At the same time, enhanced traceability could make it more difficult to engage in anonymous online conduct. *See* EPIC Comments at 2-3.

[88] *See* NTT/Verio Comments at 13-14.

[89] *See* EPIC Comments at 3.

[90] *See* Cisco Comments at 4.

[91] *See* NTT/Verio Comments at 16.

[92] For the IETF working document that describes how mobility support can be provided in IPv6, see http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-24.txt.

[93] NTT/Verio Comments at 10.

[94] Sprint Comments at 11.

for machine-to-machine communications, potentially leading to a large proliferation of devices that will connect to the Internet.[95]

Many experts believe that, whether used in a mobile or a portable environment, IPv6 can better support such devices than currently available options under IPv4.[96] According to Microsoft, "IPv6 better handles mobile applications and services."[97] NAv6TF suggests that IPv6 allows devices to attach to networks at different points more easily than is currently achievable using IPv4 alternatives, principally through the use of stateless address autoconfiguration and neighbor discovery capabilities.[98] Sprint suggests that IPv6 will permit more optimal routing of mobile traffic because IPv6 mobility specifications are being designed to eliminate "triangular routing."[99] The simplification of mobile networking in IPv6 could enable Internet users to remain seamlessly connected and easily reachable when portable or mobile devices move from their home networks to other unaffiliated networks.[100] The possibility of continuous Internet connectivity for laptops, mobile phones, PDAs, sensors, and other mobile or portable devices, in turn, could spur development of myriad new applications in both the public and private sectors.

---

[95] Thus, devices commonly found in the home (such as lights, dishwashers, refrigerators, cameras, home computers, and other home appliances) can be assigned IP addresses, linked together on home networks, and connected to the Internet, allowing home owners to control such devices remotely. *See* Motorola Comments at 4; interview with John Streck, Centaur Labs (Mar. 2004).

[96] Cisco suggests that IPv4 networks can also handle any mobile applications that exist today. Cisco believes, however, that a large scale deployment of mobile IP "will be done more easily through Mobile IPv6 and its feature set." Cisco Comments at 6.

[97] Microsoft Comments at 5.

[98] NAv6TF Comments at 12-13. The autoconfiguration and neighbor discovery mechanisms of IPv6, which are used for node discovery, also eliminate the need for DHCP or foreign agents currently used to route mobile traffic. *See* Wolfgang Fritsche and Florian Heissenhuber, "Mobile IPv6: Mobility Support for the Next Generation Internet," at 18 (2000), http://www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf.

[99] Sprint Comments at 6. The mobility protocols within IPv6 are designed to avoid routing packets from a correspondent node to the mobile node via the home agent. This route optimization mechanism will reduce transport delay and save network capacity. Route optimization is designed to be an integral part of Mobile IPv6 and is also available as an added functionality for Mobile IPv4. *See* Fritsche and Heissenhuber, note 98, *supra*, at 18.

[100] For example, a laptop linked to the Internet at home could be carried to work and then connected to the Internet there. Alternatively, a mobile phone user, who is browsing the Web, could remain seamlessly connected to the Internet while traveling from Boston to New York by linking to networks along the way. In both cases users can be reached by simply querying their home IP addresses.

2.1.4 Improved Quality of Service (QoS)

Internet transmission currently is a "best effort" scheme—users cannot expect that "high priority" traffic will be handled any differently from other traffic.[101] For business IP-based services to flourish, service providers will likely need to provide quality of service (QoS) support for those customers. This would require, among other things, the ability to identify different classes of traffic and to provide sufficient instructions to the connecting networks so that messages are delivered with acceptable performance characteristics (*e.g.*, error rates, delay).[102]

The evidence suggests that, as presently implemented, IPv6 provides no better QoS support than does IPv4.[103] However, the IPv6 packet header contains a field—the "flow label"—that is not found in IPv4 and that is intended to assist with QoS. The flow label allows a user or provider to identify, with greater specificity (or "granularity") than is available under IPv4, those traffic flows for which the provider requests special handling by network routers.[104] The IETF has not yet finalized the standards needed to enable developers and service providers to use IPv6's expanded QoS capabilities. According to IETF RFC 2460, "There is no requirement that all, or even most, packets belong to flows, i.e., carry non-zero flow labels [such as QoS] . . . [and] protocol designers and implementers [should] not assume otherwise."[105] One expert has indicated, however, that "without the flow label and hop-by-hop option processing of IPv6, [optimal QoS operations] would not be possible."[106] Accordingly, more work, particularly more standardization work, is needed before any potential QoS benefits of IPv6 can be realized.[107]

Another constraint on the widescale implementation of QoS, either in IPv6 or IPv4, would be the lack of QoS support in any network segment

---

[101] *See Wikipedia: The Free Encyclopedia*, "Internet Protocol," http://en.wikipedia.org/wiki/Internet_Protocol.

[102] *See* hyperdictionary 2004, "Quality of Service: Dictionary Entry and Meaning," http://www.hyperdictionary.com/search.aspx?define=quality+of+service (quality of service is "the performance properties of a network service, possibly including throughput, transit delay, and priority").

[103] *See* Hain Comments at 3; Internet2 Comments at 3-4.

[104] *See Protocol Dictionary*, "IPv6 (IPng): Internet Protocol version 6,"http://www.javvin.com/protocolIPv6.html

[105] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," App. A, at 30 (1998), http://www.ietf.org/rfc/rfc2460.txt.

[106] Lawrence Roberts, "QoS Signaling for IPv6," sec. 1.1, at 2 (Dec. 11, 2003), http://ftp.tiaonline.org/tr-34/tr3417/Working/Dec-03.

[107] The presence of NATs may also complicate deployment of QoS. *See* Internet2 Comments at 4.

in the transmission path. Such a deficiency could negate QoS gains realized in the rest of the network path. From a commercial standpoint, moreover, service providers will not offer QoS support unless the offered differential in service quality translates into increased revenues from customers (i.e., only if QoS utilization translates to improved service for the user and higher revenue for the provider).

2.1.5 Reduced Network Administration Costs

Experts have suggested that IPv6 will reduce network administration costs in the long run if enterprises reorganize their networking structure and operating processes to take advantage of IPv6's capabilities and remove NATs from their networks.[108] For example, the autoconfiguration feature available in IPv6 can simplify the connection of hosts and other devices to the Internet, thus reducing management overhead for network administrators.[109] The vast number of addresses available under IPv6 could simplify (and thus reduce the costs of) subnet management because each subnet could be given substantially more address space than the number of nodes that could be connected to it.[110]

If adoption of IPv6 motivates an organization to dispense with NATs, network administrators could more effectively use ping, traceroute, and other tools to diagnose network problems or to debug applications between pairs of hosts.[111] Removal of NATs could also simplify use of multivendor networking solutions.[112] Furthermore, decreasing the number of processing functions in a network (*e.g.*, by eliminating NATs) could reduce the number of components that can fail, increase network resilience, and reduce management complexity and support costs.[113]

---

[108] Interview with John Streck, Centaur Labs (Mar. 2004) The cost to upgrade to IPv6 and adjust a network to use the capabilities of IPv6 (*e.g.*, remove NATs) could be very costly depending on the specific setup of a particular network.

[109] *See* Cisco Comments at 5; GSA Comments at 6; Microsoft Comments at 5; Sprint Comments at 8. With autoconfiguration, a user can simply plug a host device into the network and it will automatically configure an IP address and network prefix and find all available routers. GSA Comments at 6.

[110] *See* Cisco Comments at 4.

[111] *See* Internet2 Comments at 2-3 ("expert ISP engineers and ordinary users have their time wasted trying to debug network problems either caused by the NAT boxes or made more difficult to diagnose by the NAT boxes").

[112] NAv6TF notes that voice and data are converging into one platform. NAv6TF Comments at 23. If middleware, such as gateways and NATs, is required everywhere, the cost for single-vendor solutions may be containable, but multi-vendor solutions will be a costly interoperability event.

[113] *See* Cisco Comments at 4.

To the extent that the administration cost savings of IPv6 depend on the removal of NATs, the potential savings may be constrained by the likely persistence of those devices in an IPv6 environment. More generally, immediate reductions in administrative costs flowing from adoption of IPv6 will probably not offset the costs of transition to IPv6,[114] although the cumulative savings could eventually exceed transition costs. Most networks will likely not see a net reduction in costs for at least 5 to 10 years after initial IPv6 deployment, depending on the priority assigned to upgrading of systems, specific network complexities, and other issues that could arise during transition.[115] Additionally, some experts have stated that there will not be aggregate administrative reductions because new IPv6 issues related to new/advanced applications and projected increases in Internet traffic could require added costs, including additional administrative activities.[116] However, this development still implies a decrease in the cost per unit of information exchanged.

In summary, during the extended transition period in which IPv4 and IPv6 support will be required, the operation expense (OPEX) for network operations will likely see a measurable increase *not* decrease. Any OPEX cost reduction will probably not be realized until significant operational experience has been gained at all levels of the network, including the application developer and user levels. This may not accrue for 10 or more years, if ever.[117]

2.1.6 Increased Overall Network Efficiency

Removal of NATs would likely result in fewer processing steps and reduced transmission bottlenecks.[118] The change to a fixed header size in IPv6 could yield processing efficiencies, and deployment of IPv6 could also allow routing tables to be reduced in size and redesigned for

---

[114] See Section 2.2 for more information on the indirect costs incurred to transition to IPv6.

[115] This observation is based on extensive literature reviews, stakeholder and expert interviews, and RFC comments.

[116] *See* interview with John Streck, Centaur Labs (Mar. 2004).

[117] To the extent that countries other than the United States have had a significant head start with IPv6 networks, organizations in those countrieswill have a more mature workforce to service businesses using IPv6 along with IPv4 networks. See Section 1.2 *supra* for more information on public- and private-sector IPv6 efforts, both domestically and internationally. As a result, non-U.S. companies could realize reduced administration costs more quickly. However, U.S. firms should be able to learn from these experiences and reduce the negative impact relatively quickly. See Section 3.1, *infra,* for more information on first-mover advantages.

[118] Network processing to maintain NAT translation tables can cause a bottleneck if network traffic grows very rapidly.

maximum efficiency.[119] Some experts have said that such benefits will result only when IPv6 use is widespread.[120] The potential increase in overall network efficiency, moreover, may be difficult to correlate with adoption of IPv6. A much better benchmark, and the metric of greatest interest to the user community, is whether the performance of E2E and other applications improves significantly when using IPv6 transport.

2.1.7 Summary

As the foregoing discussion indicates (and as Table 2-1 summarizes) adoption of IPv6 can potentially produce measurable benefits for users, equipment vendors, and service providers. The largest likely benefits will be realized in the areas of increased address space (and associated

Table 2-1. Overview of IPv6 Benefits

Benefits	Magnitude of Potential Benefits	Timing Issues	Likelihood of Occurrence	Key Factors in Realizing Benefits of IPv6
Increased address space	Large	U.S. does not face a near-term shortage	Medium/High	Removal of NATs Growth in number of end-to-end and other applications
Simplified mobility	Large	New applications will likely flow from Asian test markets	Medium/High	Growth/demand for new applications
Reduced network administration costs	Modest	Cost may increase during transition	Medium (in the long term)	Removal of NATs
Increased security	Modest	Unclear when large scale adoption of IPsec will occur	Low/Medium	Development of PKI Removal of NATs
Improved overall network efficiency	Modest	Efficiency may not improve until after large scale transition	Low	Removal of NATs
Improved QoS capabilities	Modest/Small	Few benefits in the near future	Low	Ongoing standardization and subsequent implementation of QoS "flow label" field

Source: Estimates based on RFC comments and discussions with industry stakeholders.

[119] In this statement, "routing tables" generally refers to backbone routers. As the number of IP addresses has grown, the routing tables of backbone routers tracked individual IP addresses rather than hierarchical mapping, in which one IP address can afford entry to many others. In IPv6 routing tables, a more hierarchical approach could be used to reduce the size of backbone routing tables, as well as those of all routers. The potential network efficiency gains, however, would be experienced at the backbone level.

[120] Interview with John Streck, Centaur Labs (Mar. 2004).

innovations in services and applications) and improved mobility. Additional work must be done (*e.g.*, removal of NATs, standards setting) to fully capture the potential benefits. Although the long-term benefits may be considerable, the short-term benefits for many organizations may not exceed the costs of moving from IPv4 to IPv6 on an accelerated basis.

2.2 Stakeholder Costs of Adopting IPv6

The potential costs associated with deploying IPv6 comprise a mixture of hardware, software, labor, and miscellaneous costs. The transition to IPv6 is not analogous to turning on a light switch; instead, many different paths to some level of IPv6 deployment can be forged. Each organization or user throughout the Internet supply chain will incur some costs to transition to IPv6, primarily in the form of labor and capital expenditures required to integrate IPv6 capabilities into existing networks.

Expenditures and support activities will vary greatly across and within stakeholder groups depending on their existing infrastructure and IPv6-related needs. By and large, ISPs offering service to a large group of customers will likely incur the most transition costs, while independent users will bear little, if any, costs.[121] Factors influencing these costs include

- the type of Internet use or type of service being offered by each organization;
- the transition mechanism(s) that the organization intends to implement (*e.g.*, tunneling, dual-stack, translation, or a combination);
- the organization-specific infrastructure comprised of servers, routers, firewalls, billing systems, and standard and customized network-enabled software applications;
- the level of security required during the transition; and
- the timing of the transition.

Table 2-2 provides a list of potential costs incurred by stakeholder group and gives a percentage breakdown by cost category. Table 2-3 provides

[121] This assumes that adoption occurs after routine cyclical upgrades provide IPv6 capabilities in hardware and software to the user community.

an item-by-item list of the costs to deploy IPv6 by stakeholder group; this is a relative comparison of costs and should not be used to infer the actual size of each cost. As part of the discussion in this section we

Table 2-2. Overview of IPv6 Costs

Stake-holders	Total Cost	Transition Cost Breakdown[a]			Timing Issues	Key Factors in Bearing Costs
		HW	SW	Labor		
Hardware Vendors	Low [b]	10%	10%	80%	Currently most are providing IPv6 capabilities	Rolling in IPv6 as standard R&D expense; international interest and future profits incentivize investments
Software Vendors	Low/Medium[c]	10%	10%	80%	Currently some are providing IPv6 capabilities	Interoperability issues could increase costs
Internet Users	Low/Medium	10%	20%	70%	Very few currently running IPv6; HW and SW will become capable as routine upgrade; size of enabling cost should decrease over time	Users will wait for significantly lower enablement costs or (more probably) a killer application requiring IPv6 for end-to-end functionality before enabling
Internet Service Providers (ISPs)	High[d]	15%	15%	70%	Very few are offering IPv6 service; no demand currently; very high cost currently to upgrade major capabilities	ISPs see low or nonexistent ROI, high costs, and high risk

Source: RTI estimates based on discussions with 26 industry stakeholders, RFC responses, and extensive literature review.

[a]These costs are estimates based on conversations with numerous stakeholders and industry experts. Several assumptions underlie them. First, it is assumed that IPv6 is not enabled (or "turned on") or included in products and no IPv6 service is offered until it makes business sense for each stakeholder group. Additionally, the hardware and software costs are one-time costs. However, labor costs could continue for as long as the transition period and possibly longer.

[b]For hardware vendors producing high-volume parts that require ASIC changes, the costs could be very high and would not be offered until the market is willing to pay.

[c]Software developers of operating systems have and will incur a relatively low cost; however, application developers will incur greater costs, designated as *medium*.

[d]The cost for ISPs is particularly high if the ISP manages equipment at user sites, because premises equipment is more costly to manage and maintain.

Table 2-3. Relative Costs of IPv6 Deployment by Stakeholder Group[a]

Item	Hardware, Software, Service Providers	ISPs	Enterprise Users
Hardware			
Replace interface/line cards	L		M
Replace routing/forwarding engine(s)[b]	M	M	
Replace chassis (if line cards will not fit)		M	M
Replace firewall		M	M
Replace billing systems		L	
Software			
Upgrade network monitoring/management software		L	L
Upgrade operating system		M	S
Upgrade applications:			
• Servers (Web, DNS, FTP, mail, music, video, etc.)			S
• ERP software (e.g., PeopleSoft, Oracle, SAP, etc.)			L
• Other organization-specific, network-enabled applications			L
Labor			
Train networking/IT employees	L	L	L
Design IPv6 transition strategy and a network vision	M	L	M/L
Implement transition:			
• Install and configure any new hardware	S	L	L
• Configure transition technique (e.g., tunneling, dual-stack, NAT-PAT translation)	M	M	M
• Upgrade all software (see Software section above)		S/M	S/M
• Extensively test before "going live" with IPv6 services		L	L
Maintain new system		M/L	M/L
Other			
IPv6 address block(s)			S
Lost employee productivity[c]		M	M
Security intrusions[d]		L	L
Foreign activities		M	M
Interoperability issues		M/L	M/L

Source: Estimates based on discussions with 26 industry stakeholders, RFC responses, and literature review.

[a]The relative designation (S = small, M = medium, and L = large) indicates the estimated level of cost to members of the specific stakeholder group. These costs are not incremental, rather they reflect differences in costs between stakeholder groups.

[b]The "brains" of the router, usually in the line card form.

[c]Because of unexpected down-time during transition period.

[d]Based on unfamiliar threats.

provide some insight into which stakeholder groups will end up bearing the costs or appropriating the benefits associated with IPv6.[122] The following sections are qualitative in nature and focus on the costs likely to be incurred by each stakeholder group and how the timing of the transition affects these costs.

2.2.1 Hardware, Software, and Services Providers

Vendors that provide products and services include: networking hardware companies, such as router and firewall manufacturers; networking software companies, including operating system and database management application developers; and service vendors comprised of companies that offer training, service and support. These companies need to integrate IPv6 capabilities into their products and services, if they have not already done so, as a precursor to all user transitions. Once IPv6-capable products are installed in user networks, ISPs will be enabled to offer IPv6 service (see Section 2.2.2 *infra* for more on ISP costs), and users will be able to purchase IPv6-enabled devices and applications. Many companies in this category are already developing, and some are even selling, IPv6 products and services.

The majority of the costs being incurred by hardware and software developers include labor-intensive research and development (R&D) costs and training costs. These costs, however, have not been large enough to deter development of IPv6 capabilities. R&D activity has generally been conducted in small intracompany groups dedicated to developing IPv6-capable products with, to date, limited, small-scale interoperability testing with other hardware and software makers. Based on industry experience with the early deployments of IPv4 equipment, large-scale deployment may bring to light additional interoperability problems.[123]

The future cost of interoperability testing could be substantial but such testing is essential if IPv6 is to become seamlessly pervasive. Without interoperability testing, IPv6 capabilities could have little practical use.[124] Recently, the Department of Defense, in collaboration with several industry stakeholders and the University of New Hampshire, launched

---

[122] A market analysis to project the prices of specific products and services is beyond the scope of this study.

[123] This information was gained from interviews with representatives of Nortel Networks.

[124] *See* Cisco Comments at 27; Motorola Comments at 5-6. See Section 2.3.1 *infra* for more information on interoperability costs and considerations.

the Moonv6 test bed, which has stimulated interoperability testing to be conducted between both U.S. and foreign vendors wishing to offer IPv6 products or services.[125]

In the next several years, foreign activities will likely affect IPv6 transition costs borne by hardware, software, and service vendors. Several commenters noted that, as foreign companies and corporations encounter and solve various deployment issues, U.S. vendors will see lower implementation costs.[126] As products mature, fewer vulnerabilities are found, thus lowering implementation costs. The United States is likely to benefit from the current experience being gained by foreign activities. However, a point of diminishing returns is likely, although it is difficult to say when.[127] In addition, several commenters stated that substantial foreign competition could drive up the prices of U.S. companies' products and services because with less market share they would not be able to spread R&D costs across a large customer base.[128]

2.2.2 ISPs

ISPs comprise two main groups, which often overlap—regional and national companies that provide internet access service to corporate, governmental, nonprofit, and independent Internet users (*e.g.*, AOL, Earthlink) and national companies that own and maintain the backbone hardware and software of the Internet (*e.g.*, MCI, Sprint, AT&T). Often companies that own the backbone Internet infrastructure provide Internet access service to customers through a subsidiary. Today, most backbone transport networks have already upgraded their major routers and routing software to accommodate IPv6. Thus, we focus on smaller ISPs that have large customer service provision capabilities. This group will likely incur the bulk of the transition costs as they enable IPv6 hardware and software applications and work through system interoperability problems. To date, however, there has apparently been little demand for IPv6 service or applications in the United States. As a result, given the costs to reconfigure networks, experts and industry stakeholders agree that U.S. ISPs are currently not positioned to realize

---

[125] *See* Cisco Comments at 21, and Cover Letter at 1; Hain Comments at 8-10; NAv6TF Comments at 21, 36, 43; NTT/Verio Comments at 28.

[126] *See* BellSouth Comments at 6; Cisco Comments at 13.

[127] *See* Cisco Comments at 13. See Section 3.1 for more detail on such "first-mover" considerations.

[128] *See id.* at 13; Dillon Comments at 1.

a positive return on investment from large-scale offerings of IPv6 service.[129]

For ISPs to offer a limited amount of IPv6 service, they would need to integrate some transition mechanism(s), such as tunneling.[130] The costs of doing so will probably not be large.[131] If several routers and service provisioning software are upgraded and limited testing is performed, IPv6 service could be provided to a limited number of Internet users today at minimal additional cost. Currently ISPs are performing some limited testing.[132] However, before ISPs elect to offer widespread IPv6 service, they will need assurances that current service offerings would not be affected in any way. This would likely require much more testing and significant additional hardware, software, and training costs,[133] possibly increasing the costs by 100 to 200 percent more than would be incurred for a more limited service roll-out, depending on the number of affected customers and the nature of an ISP's infrastructure.

Assuming that IPv6 products and services in the Asian market are transferable to the U.S. market, those ISPs offering IPv6 services abroad will have absorbed some of the initial development costs. R&D costs attributable to IPv6 implementation, like any other advanced technology, can be borne by early adopters. However, excessive delay by U.S developers may not allow them to charge early adopter premiums if mature competing products from foreign markets are already in place.[134] However, such costs are not likely to be a dominant factor for most application services.[135]

In the United States today, NTT/Verio is currently the only ISP providing end-to-end IPv6 service;[136] however, they began replacing and upgrading hardware and software components to be IPv6 capable as early as 1997. By spreading out transition costs, including hardware and software costs, training, and the development of network administration software tools, NTT/Verio was able to upgrade for almost no additional

---

[129] *See* NAv6TF Comments at 24.

[130] Tunnel brokers can also enable two IPv6 networks to connect over an IPv4 network.

[131] This information was gained in interviews with representatives of AT&T.

[132] *Id*.

[133] *Id*.

[134] See Section 3.1 *infra* for more detail on the first-mover advantage discussed here.

[135] *See* Cisco Comments at 13.

[136] NTT/Verio is not providing IPv4 to IPv6 or IPv6 to IPv4 service; therefore, customers would need to maintain dual-stack networks themselves or integrate translation techniques to continue to communicate with IPv4 networks.

costs above standard upgrade, training, and testing costs.[137] Although the transition may not be as inexpensive for other ISPs, NTT/Verio's experience illustrates how careful planning can help reduce transition costs.

Almost all experts agree that a shift to IPv6 over a short period of time will be more expensive than performing the transition as part of a normal life-cycle update. Transition technologies were specifically designed to enable a prolonged overlap and to minimize deployment and operational interdependencies. Rather than forcing a short-term shift, many experts suggest that a reasonable deployment plan would focus on replacing as much IPv4-only hardware and software as possible through normal life-cycle updates. Over any period of acquisition, turning on IPv6 for routine use should only occur after a critical mass of IPv6-enabled replacement technology and training are in hand.[138]

Thus, until customers begin demanding IPv6 service, most U.S. ISPs have no incentive to incur any major additional costs; in 5 to 10 years, however, as more hardware and software become IPv6 capable through cyclical replacements, continued standardization efforts of the IETF,[139] and testing by many parties, ISPs will probably be in a position to recoup investment costs associated with IPv6 service.

2.2.3 Internet Users (Corporate, Government, Nonprofit, and Independent)

Costs to upgrade to IPv6 for Internet users vary greatly. Independent Internet users, including residential users and small and medium enterprises (SMEs) who do not operate servers or any major database software, will only need to upgrade networking software (*e.g.*, operating systems) and one or more small routers to gain IPv6 capabilities. This cost will be relatively minimal if the hardware and software are acquired through routine updates.

Organizations, such as corporations, government agencies, and nonprofits, will incur many more costs than home or small network users, but the relative level of these costs will depend on the extent to which a specific organization wants to operate IPv6 applications and whether it

---

[137] NTT/Verio Comments at 21.

[138] *See* Cisco Comments at 12-13.

[139] Some experts have stated that certain inadequacies exist in IPv6 standards, such as management information base and billing systems specifications, and that others may develop as IPv6 testing continues. *See* Cisco Comments at 17; NAv6TF Comments at 32-33.

intends to connect to other organizations using IPv6. The magnitude of the transition costs is still uncertain because only a few test beds and universities have made large-scale transitions. According to officials at Internet2, the time and effort needed to transition their backbone to IPv6 was minimal, and no significant system problems have been encountered.[140] However, Internet2 indicated that their experimental system was implemented and is maintained by leading industry experts. It is unclear what issues might arise from implementation by less experienced staff. Tony Hain points out, however, that if normal upgrade cycles are assumed to provide IPv6 capabilities, transition costs will be limited to training and some reconfiguration.

Internet users, as a whole, constitute the largest stakeholder group. The robustness of this sector allows for a more detailed explanation of costs broken out by hardware, software, labor, and other costs.

Hardware Costs

Depending on individual networks and the level of IPv6 use, some hardware units can become IPv6 capable via software upgrades. However, to realize the full benefits of IPv6 most network hardware will need to be replaced.[141] Specifically, high-end routers, switches, memory, and firewalls all will need to be upgraded to enable large scale IPv6 use within a network. It is generally agreed that to reduce hardware costs, all or the majority of hardware should be upgraded to have IPv6 capabilities as part of the normal upgrade cycle (generally occurring at least every 3 to 5 years for most routers and servers, but potentially longer for other hardware such as mainframes). At that time, IPv6 capabilities should be available and included in standard hardware versions. In the short term, replacement of some forwarding devices and software could be used to set up small-scale IPv6 networks.

Software Costs

Significant software upgrades will be necessary for IPv6 use; however, similar to hardware costs, many of these costs will be negligible if IPv6 capabilities are part of the routine requirements in periodic software

---

[140] Internet2 is a network of approximately 200 educational and institutional Internet users. The 11 backbone routers that support the Internet2 network have recently been upgraded to new Juniper routers, which are dual-stack with IPv4- and IPv6-enabled hardware.

[141] *See* BellSouth Comments at 5.

upgrades.[142] Software upgrades include server software, operating systems, business-to-business (B2B) software, networked database software, network administration tools, and any other organization-specific network-enabled applications. Currently, the main software cost that user organizations envision pertains to element management systems, network management systems, and operations support systems that are often network specific and will need coding to adjust for IPv6. If Internet users upgrade their commercial application software in 2 or more years hence, they should have IPv6 capabilities, although they will still need to upgrade their company-specific software.

Labor Costs

According to experts, training costs are likely to be one of the most significant upgrade costs,[143] although most view it as a one-time cost that could be spread out over several years. The actual cost depends on the level of understanding necessary for network administration staff. On a daily basis, the change in operating procedure for IPv6 will be minimal.[144] Most network staff, however, will need a full understanding of the required network infrastructure changes and how they might affect security or interoperability.[145] NAv6TF notes that the relative programming skills of software engineers at a particular company could drastically affect upgrade costs.[146] A company with more skillful programmers might have to hire one additional employee, while another might need three or four, during a transition period that could last 5 or 10 years.

Similarly, training costs may be minimal for large organizations with existing IPv6 expertise (*e.g.*, universities). For small to mid-size organizations where information technology (IT) staff perform multiple functions, staff training could be a significant share of the IPv6 transition costs. If staff will need to alter their general activities based on IPv6 use, staff training will be necessary for them, though generally this should not

---

[142] *See id.* at 6; Dillon Comments at 2; Hain Comments at 11. Cisco additionally indicated that these costs can be amortized over a gradual development cycle. Cisco Comments at 11.

[143] *See* GSA Comments at 8; Hain Comments at 13, 14-15; NAv6TF Comments at 28.

[144] Network operators will have to learn to write and understand IP addresses written as colon-delimited hexadecimal (*e.g.*, 3ffe:3700:1100:0001:d9e6:0b9d:14c6:45ee) for IPv6 addresses, as opposed to dotted decimal addresses (*e.g.*, 127.144.76.58) used in IPv4.

[145] *See* Cisco Comments at 12.

[146] *See* NAv6TF Comments at 29.

occur.[147] If customers will be affected in any way, sales staff and any other employees who interact with customers periodically will need to understand the potential problems and benefits that could affect their relationships with customers.

Additional labor will be needed to run testing activities, to install and configure new hardware, software, and transition mechanism(s), and to maintain the new dual-stack (*i.e.*, IPv4 and IPv6) network. As the transition takes place, a more complex network will likely require additional network administration costs in the short term. For example, in a dual-stack network, two standards will have to be supported; thus, security intrusions will likely increase significantly (attributable to a lack of awareness of or a lack of experience with IPv6 security "holes"). These costs would be highest in an expedited deployment scenario. Costs would be lower in a gradual migration scenario where much of the testing and problem resolution can be completed over a gradual period or through shared initiatives.[148] For U.S. vendors, costs would also be lower in a scenario where the early deployment issues are encountered and resolved in foreign countries.[149]

2.2.4 Hypothetical Case Study: Enterprise Adoption of IPv6

The costs associated with an enterprise adoption of IPv6 can best be illustrated through a hypothetical case study. Company A, a medium-to-large enterprise with an IPv4-only corporate network, determines that to contact Company B via an IPv6 connection, Company A needs to begin migrating its network to IPv6. This transition will cause Company A to incur costs mainly in the areas of hardware, software, and labor costs, but other costs may arise from unforeseen security threats and other hurdles (*e.g.*, interoperability) that are difficult to predict.

Company A's network infrastructure, combined with its present and desired future applications strategies, will determine the appropriate transition process and costs. For the purposes of this case study, we assume that Company A has eight core routers, 150 distribution switches, and four firewalls, all with varying individual costs. The primary

---

[147] Once dual-stack capabilities are enabled by default in a host operating system (*e.g.,* as Microsoft plans to do in the next version of Windows), the user should not be aware whether IPv4 or IPv6 packets are being sent or received. Thus, no training should be necessary, unless new IPv6-specific applications are required.

[148] *See* BellSouth Comments at 6; Cisco Comments at 12; Hain Comments at 16.

[149] *See* BellSouth Comments at 6; Cisco Comments at 13.

applications that the company uses include limited video conferencing, some streaming video, and a company-wide inventory database. Company A has three full-time network specialists and allocates approximately $2,500 per year on training per employee. Table 2-4 provides a breakdown of the infrastructure owned by Company A and its annual spending on IT staff and training.

Table 2-4. Infrastructure Components and Associated Cost/Value

Network Component/Costs	Number of Units	Average likely Cost or Value (per unit)	Total Value/Cost
Router	8	$15,000	$120,000
Distribution Switches	150	$10,000	$1,500,000
Firewall	4	$1,500	$6,500
Network Specialist (1 FTE)	3	$55,000	$165,000/year
Training	3	$2,500	$7,500/year
TOTAL			**$1,799,000**

Source: RTI Networking Staff.

In order to get immediate connection capabilities, Company A plans to establish a limited IPv6 network over a 6- to 12-month period; however, the majority of costs will be spread out over a transition period lasting several years, at a minimum. In the most likely scenario, Company A will follow a migration path that gradually increases the number of applications running IPv6 and the ability of the network to handle more IPv6 traffic. Table 2-5 compares the costs as Company A progresses through the various stages of its migration strategy.

In Phase 1, Company A will transition from an IPv4-only network to an IPv4 network with IPv6 tunneling.[150] It will employ tunneling primarily to allow IPv6 communication with outside organizations and networks at a low cost; thus, they will employ host to host tunneling using a tunnel broker. By reconfiguring the network for tunneling and running dual-stack operating systems on hosts, this approach will provide IPv6

[150] Tunneling here and in the Table 2-5 refers to using tunneling techniques in one or more routers to enable IPv6 messages to traverse IPv4 networks, and running dual-stack operating systems on host computers. In order for any IPv6 applications to be used on IPv4-based computers, the operating system on each computer will need to support both the IPv6 and IPv4 protocol stacks.

Table 2-5. Transition Phases

Transition Phases	Relative Estimated Size of Cost	Costs			
		Hardware	Software	Labor	Other
Phase 1 (Minimal IPv6 using tunneling in a network)	Medium	Upgrading/ replacing 1+ backbone routers; replacing firewalls	Upgrading/ replacing any applications used specifically for IPv6	Existing IT personnel must be trained; new personnel may need to be hired to help install and run a dual-protocol network and address new/additional security concerns	Scheduled downtime; unexpected equipment and service outages; security threat effects
Phase 2[a] (Substantial IPv6 using a dual-stack network)	Large	Upgrading/ replacing remaining routers and all other networking hardware	Upgrading/ replacing all applications to be IPv6 capable	More IT training and network administration time/effort will be required before, during and after the installation; users might need to be trained to use new applications	Security threat effects
Phase 3[b] (Native IPv6 with IPv4 translation)	Small/Medium	Upgrading/ replacing gateways and other devices to perform translation	Depending on the translation mechanism, new software may be required	Time/effort to install and maintain translation devices; training and support for users running only IPv6 applications	Interoperability issues with external Internet users/networks[c]
Phase 4 (Native IPv6 only)	Small	None	None	Time/effort to remove translation devices and software	Lost business

Source: RTI estimates based on discussions with industry stakeholders.

[a]The costs described in Phase 2 assume that Phase 1 has been completed.

[b]The costs described in Phase 3 assume that Phase 2 has been completed.

[c]Security threats will continue but most likely at a reduced cost since IPv6 intrusions will be better understood.

connectivity for a limited subset of the company's hosts as a pilot group. Connectivity will later be extended to the entire corporate network and user base.

The extent of the costs associated with this first phase of migration will rely heavily on the presence of IPv6 capabilities within the network and host hardware and software.[151] After assessing hardware and software capabilities, Company A will need to develop a plan for how and when to incorporate IPv6 into its network; this will involve contributions from not only IT administrators, but also company leaders and/or any Internet users who can communicate the desire to have certain IPv6 capabilities. This process should take several months and could be quite costly in terms of labor effort.

Addressing specific expenditures, we note that Phase 1 equipment costs will include upgrading/replacing one or more routers to allow IPv6 tunneling and replacing firewalls and intrusion detection system (IDS) equipment for security. Unless Company A has an urgent need to gain IPv6 connectivity, it will incur these costs during a routine 3- to 5-year equipment upgrade cycle. Because most computer operating systems currently support IPv6 (*e.g.*, Windows and Linux), software costs for a pilot group of IPv6 users will be limited to any upgrades of applications to be used specifically with IPv6.

Labor and training costs will be a large part of this initial migration phase. Existing IT personnel must be trained to support IPv6. New personnel may be hired to assist with the operational overhead of running two Internet protocols on a network and to address potential security concerns commonly associated with any major IT transition. Scheduled downtime and unexpected outages of equipment and services related to upgrades will add additional costs.

As Company A decides to enable more internal Internet hosts to use IPv6, it will likely begin Phase 2 of its migration by integrating dual-stack capabilities into network routers that would allow more IPv6 messages to be sent and received, and would make such communication more efficient. Although Windows-based hosts could use Microsoft's Teredo to send IPv6 messages with no changes to existing routers, companies

---

[151] As routine upgrades take place, IPv6 capabilities will be part of installed hardware and software both at the host level and at the network level, though not on the same timeframe. Although the capabilities have to be enabled, or "turned on," the level of IPv6 capabilities will significantly affect transition costs.

interested in transitioning to IPv6 will likely enable dual-stack capabilities in their network routers, as well as on most or all of its network and IT infrastructure while maintaining normal IPv4 operation.[152]

Phase 2 will involve configuring dual-stack routers and running IPv4 and IPv6 simultaneously on most network equipment and hosts. Hardware not upgraded to IPv6 in Phase 1 will be upgraded during this phase. However, the majority of the costs will come from software upgrades and associated labor costs necessary to roll out new IPv6 service and applications to a large number of corporate users.[153] Training costs will also be incurred because these users need to be trained on new applications. Security issues will also require labor and possibly additional hardware and software.

In Phase 3 of Company A's migration plan, it will use IPv6 exclusively for network transmission, and use IPv6-to-IPv4 translation to interact with external IPv4 networks. The decision to move from Phase 2 to Phase 3 will turn on cost savings – whether the costs of network support for IPv4 exceed the costs of supporting IPv6. Estimated to be many years away, Phase 3 will most likely involve employing a predominantly IPv6 network with remaining "pockets" of IPv4 within the company. Resources continuing to run IPv4 even after this phase may include legacy equipment such as mainframes and databases that are too expensive to upgrade during Phase 3. The only likely equipment costs are gateways and other devices needed to perform IPv4/IPv6 translation for that legacy equipment. Labor costs may be incurred with the installation and maintenance of these translation devices. Additional labor costs may come from supporting a large base of users now running IPv6 natively and the associated issues that may arise.

Lastly, as IPv4 traffic becomes less common, Company A will decide not to support translation devices. In Phase 4, any networks or hosts still operating on IPv4 stacks will have to have translation devices to communicate with IPv6-only hosts or networks.

---

[152] Microsoft's Teredo allows an IPv6-over-IPv4 tunnel to originate at a Windows host, rather than at a router.

[153] During this phase, the majority of network management software and user software and applications will be IPv6-enabled.

2.3 OTHER TRANSITION ISSUES AND COSTS

2.3.1 Interoperability

The transition to IPv6 will be a long process and may never attain complete penetration before the protocol becomes obsolete. Experts predict that in 20 years most Internet users will be using IPv6, but pockets of IPv4 will still exist as parts of legacy systems.[154] Some firms will not find it cost-effective to convert large segments of their existing systems. Hardware and software interoperability is a key requirement for interconnecting networks across heterogeneous environments, and thus will be a major consideration in an enterprise's decision to adopt IPv6.

The developers of IPv6 recognized that there would likely be a lengthy transition period from IPv4 to the new protocol and strived to accommodate that fact.[155] Most directly, they created several mechanisms (*e.g.*, dual-stack, tunneling, and translation) to enable networks using either or both version of IP to communicate with each other. Those mechanisms were intended to eliminate deployment dependencies between and among vendors and networks and thereby to allow enterprises to decide when to adopt IPv6, if at all, based upon their own needs and goals, without regard to the decisions of other enterprises.[156] Interoperability will not be completely seamless in practice, however. Firms will have to address a number of issues in order to minimize interoperability problems during the transition from IPv4 to IPv6.

Interoperability Between IPv6 Hardware and Software Applications

Because IPv6 is an industry standard, hardware and software applications produced by different vendors in accordance with that standard should be interoperable. Put another way, there is nothing inherent in the protocol that should create an interoperability barrier. In general, experts believe that with international cooperation most implementation differences can be avoided and in the long run interoperability problems will be minimal because producers will quickly adjust to avoid any productivity losses from interoperability problems. To date, experience shows that no obvious problems arise in implementing

---

[154] Interview with John Streck, Centaur Labs (Mar. 2004).
[155] *See, e.g.*, Hain Comments at 10, 12.
[156] *See id.* at 10.

the IETF standards for IPv6, because major operating system and router vendors already have implemented and periodically demonstrated interoperability.[157]

However, some experts believe that in the short run differences in the implementation of IPv6 could potentially lead to interoperability problems in some areas.[158] For example, the protocol allows proprietary functions to be incorporated in areas such as optional headers that could lead to incompatibility. Conformance questions will need to be addressed. Experts believe that additional test beds and activities (such as testing activities currently being conducted as part of the Moonv6 test bed) are needed. In the absence of such action, future IPv6 products developed in one company might not be able to interact with those developed in another under the same general standards.[159] For these reasons, organizations should emphasize interoperability in any transition plan to minimize costs and efficiency losses.

Interoperability between IPv4 and IPv6 Hardware and Software Applications

Interaction or intercommunication between IPv6-only and IPv4-only hardware and software applications does create potential interoperability problems. Before a host on one network can communicate with a host on another network, the originating host will first have to determine which protocol(s) the receiving host supports and then make the necessary arrangements to send a recognizable message. This process could increase delay or decrease network efficiency. Both networks could mitigate these interoperability problems by deploying dual-stack capability. The IETF has reported, however, that dual-stack equipment does not eliminate interoperability concerns. For example, if an IPv6 node is placed in a mixed IPv6/IPv4 environment, it may encounter problems that lead to connection delays, poor connectivity, and network insecurity.[160]

Tunneling can also facilitate interoperability between IPv6 and IPv4 networks, but it also increases packet overhead. Although that would not

---

[157] *See* Cisco Comments at 17.

[158] *See* Hain Comments at 19; Lockheed Comments at 4-5; Motorola Comments at 9-10. Some commenters expressed the concern that flexibility in how IPsec is implemented could limit its effectiveness. *See* Hain Comments at 3-4; NAv6TF Comments at 35-36.

[159] *See* NAv6TF Comments at 24.

[160] *See* S. Roy, A. Durand, and J. Paugh, "Issues with Dual Stack IPv6 on by Default," at 1 (May 7, 2004), http://www.ietf.org/internet-drafts/draft-ietf-v6ops-v6onbydefault-02.txt.

create undue hardship for network routers, it would increase processing time and network overhead costs.[161] The interoperability benefits likely outweigh the additional costs. Most importantly, interoperability mechanisms, such as tunneling, allow an enterprise to transition to IPv6 at its own pace, lowering hardware and software costs, and minimizing the impact on existing operations.[162] Nevertheless, a company should bear the costs of interoperability in mind as it decides when and how to deploy IPv6.

2.3.2 Security in Transition

Section 2.1.2 discussed the security benefits of deploying IPv6, as compared to IPv4. Security concerns are not limited to the capabilities and vulnerabilities inherent in the individual protocols, however. As enterprises assess the merits of adopting IPv6, they must also consider the security issues that will arise during the transition period when both IPv6 and IPv4 are being used.

As noted in section 2.1.2, enterprises that operate dual-stack equipment will have to address the vulnerabilities of both protocols. The resulting security problems may not simply be additive; simultaneous use of both IPv6 and IPv4 may expose an enterprise to more attacks than the sum of the attacks that can be launched against each protocol. Dual-stack operation can raise other security problems, moreover, if consistent security policies are not created for both IPv6 and IPv4 traffic. If a firewall is not configured to apply the same level of screening to IPv6 packets as for IPv4 packets, the firewall may let IPv6 pass through to dual-stack hosts with the enterprise network, potentially exposing them to attack.[163]

Enterprises that achieve interoperability via tunneling could also expose themselves to external attacks and threats. IPv6 packets encapsulated in IPv4 tunnels could pass through IPv6 firewalls and launch attacks on IPv6 network host equipment.[164] Additionally, automatic tunneling mechanisms (*i.e.*, those in which the communicating parties do not have an active hand in establishing) are susceptible to packet forgery and

---

[161] *See* Hain Comments at 10 (tunneling increase overhead by 10 percent).

[162] *See* Cisco Comments at 12-13.

[163] *See* Roy, Durand, and Paugh, note 160 *supra*, § 3.3, at 10.

[164] *See id.*; Sean Covery and Darrin Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0), § 3.1.9.1, at 19 (appended to Cisco Comments). Attackers can also use IPv6-to-IPv4 translation to hide their identity and location and thus defeat defensive traceback efforts. Covery and Miller, *supra*, § 3.1.9.1, at 20.

denial of service attacks.[165] Although none of these transitional security concerns are insuperable, organizations planning to implement IPv6 must be aware of them and develop the necessary security policies to address them.

[165] Covery and Miller, note 164 *supra*, Sec. 3.1.9.1, at 19.

3 U.S. Competitiveness

Stakeholders agree that the market should and will be the primary driver for the adoption of IPv6. Some are concerned, however, about the implications for U.S. competitiveness if America lags behind other nations in the adoption of IPv6. Actions by governments in Asia and Europe to promote deployment of IPv6 in their countries suggests that those governments believe that there may be "first mover" advantages from early adoption of the new protocol. There have been reports that some foreign governments see an opportunity to leverage the development and deployment of IPv6 to strengthen their position in information technology and, specifically, in Internet equipment, software, and services.[166] U.S. stakeholders worry that if the United States loses its current technical and market leadership in the Internet sector, recapturing that position will be difficult.[167]

3.1 FIRST-MOVER ADVANTAGES

Companies that first adopt a particular technology ("first movers") may in some circumstances have the ability to create barriers to subsequent entry or to influence the adoption decisions of other companies. By so doing, the first mover may be able to dominate the markets associated with that technology and generate monopoly profits.[168]

---

[166] *See, e.g.*, Ikeda and Yamada, note 36 *supra*, at 2, 12; Hain Comments at 1; Motorola Comments, at 5; Dillon Comments at 1. *See also* Cisco Comments at 22 (Chinese carriers may feel political pressure to showcase China as a technology leader).

[167] *See* Alcatel Comments at 2; Cisco Comments at 24; Hain Comments at 8; NAv6TF Comments at 6-7.

[168] *See* P. Stoneman, *The Economics of Technological Diffusion* (2002).

First mover advantages arise from three general factors: (1) technology leadership, (2) preemption of scarce resources or assets, and (3) an ability to "lock in" users due to the high costs of switching to alternative technologies or products.[169] Because the principal resources underlying the Internet are information and human capital, and because markets for those resources are international, open, and highly mobile, it is unlikely that the second factor will confer any first mover advantages with respect to IPv6. On the other hand, first movers may gain learning and experience that will enable them to exert technology in the IPv6 market. If all companies are required to move along similar learning curves in developing and deploying IPv6 products and services, early movers may be able to sustain knowledge advantages, leading to lower costs or higher quality products and services.

Knowledge and experiences gained by early adoption could also allow first movers a competitive advantage in providing implementation services (potentially tied to hardware and software purchases). As in the early years of IPv4, many unforeseen issues are expected to arise during real-world implementation of IPv6. Resolving these issues will be an important factor in customers' purchase decisions. Hardware and software suppliers that develop this expertise early will be in a better position to attract and retain customers.

First-movers in IPv6 markets could also create high switching costs that "lock in" users (*i.e.*, that prevent or deter users from abandoning the first-mover's product in favor of a subsequently-offered substitute) and thus raise barriers to entry for latecomers to a market. Once users have invested resources in training staff to maintain and trouble shoot particular hardware and software systems it may become costly to switch. Familiarity and risk associated with change tend to support first-mover advantages.

Some industry experts question whether first movers will be able to capture sustainable competitive advantages in Internet markets. In the applications markets, for example, the rapid pace of technology advances makes sustaining first-mover technology or information advantages difficult.[170] In addition, the short life expectancy of Internet

---

[169] *See* M. Liberman and D. Montgomery, "First-Mover Advantages," 9 *Strategic Mgmt. J.* 41 (1988).

[170] *See* David Needle, "The Myth of the First Mover Advantage," *siliconvalley internet.com* (Apr. 5, 2000), http://siliconvalley.internet.com/news/article.php/3541_333311.

technologies and regular replacement of hardware and software applications reduce lock-in costs.

Information spillovers also work against first-mover advantages.[171] Deployment costs are typically more costly for innovators and early adopters of new technologies compared to the costs for imitators and later adopters. If U.S. companies are able to learn from the international community's early IPv6 adoption activities, this may lower the U.S. deployment costs and lead to competitive products and services with lower entry costs. Empirical research has shown that failure is also a common outcome for first-to-market participants.[172]

3.2 FIRST-MOVER ADVANTAGE AND U.S. COMPETITIVENESS

Judging from the published literature and the RFC comments, U.S. stakeholders are aware of first-mover concerns, but disagree about the potential competitive effects of the United States lagging behind other nations in deployment of IPv6. At this time, most markets for IPv6 products and services are in their infancy. Until applications and services markets begin to mature, it is not possible to determine whether efficiency gains or learning curve effects will generate sustainable first mover advantages. The following information would be needed to investigate fully potential first mover issues:

- the transferability of early lessons learned from one company or system to another;
- efficiency gains from economies of scope in applications markets (*e.g.*, bundling and product tie-ins); and

---

[171] The term "spillover" refers to the fact that some benefits of a particular economic activity (*e.g.*, R&D) frequently accrue ("spill over") to parties other than the one that originally undertook the activity. "Information" or "knowledge spillovers" result from the movement of information from the originating firm to other producers (*e.g.*, through publication of the originating firm's basic research, through "reverse engineering" of the originating firm's product by other firms, or by the movement of employees from the originating firm to other organizations). "Market spillovers" result when the operation of the market for a new product or process causes some of the benefits thereby created to flow to producers and consumers other than the innovating firm. *See*, *e.g.*, Bronwyn Hall, "The Private and Social Returns to Research and Development", in B. Smith and C. Barfield, eds., *Technology, R&D, and the Economy* 140 (1996); Adam Jaffe, "The Importance of 'Spillovers' in the Policy Mission of the Advanced Technology Program," *J. Tech. Transfer* 11 (1998); Zvi Griliches, "The Search for R&D Spillovers", NBER Working Paper No. 3768 (Nat'l Bur. Economic Res. 1991).

[172] *See* G. Tellis and P. Golder, "First to Market, First to Fail? Real Causes of Enduring Market Leadership," 37 *MITSloan Mgmt. Rev.* 65 (1996).

- user lock-in costs and the availability of interoperability solutions to minimize these costs.

An important point for this analysis is the fact that first-mover strategies are usually discussed with respect to the benefits and costs of innovation in applications. However, the issue here is the evolution of a critical infrastructure -- a standard. Standards provide several functions that *enable* innovation: (1) *reducing variety* (*i.e.*, one standard versus several incompatible protocols) and thereby presenting larger potential markets; (2) *providing information* (*e.g.*, format and timing of message transmissions) and thereby reducing the costs of innovation; (3) *assuring quality* (*e.g.*, accuracy and assurance of message delivery); and (4) *assuring compatibility/interoperability* (*e.g.*, seamless integration of sub networks and applications) and thereby realizing network externalities.[173]

This section discusses transition issues and their potential impact on competitiveness for U.S. vendors of IPv6 hardware and software applications and for U.S. users that rely on the Internet to provide their products and services.

3.2.1 Impact on U.S. Vendors of Internet Hardware and Software Applications

Several commenters voiced strong concern that other countries are advancing IPv6 at a much faster rate than the United States, and that without government action to stimulate or assist U.S. deployment, the United States could lose its leadership role in Internet issues.[174] Another commenter indicated that a lack of U.S. technical experience in new IPv6-based equipment and applications development could put domestic firms at a disadvantage, as other countries would be able to work without NATs and other IPv4 work-arounds.[175] Other commenters focused on resource constraints; if transition to IPv6 in the United States lags behind the international community, U.S. vendors will need to

---

[173] *See* Gregory Tassey, "Standardization in Technology-Based Markets," 29 *Res. Pol.* 587 (2000).

[174] *See* Alcatel Comments at 4; Hain Comments at 17-18; Lockheed Comments at 5; NAv6TF Comments at 6-7.

[175] Interview with representatives of Internet2 (designing the next generation of Internet applications will be simpler in IPv6 because developers will not need to build on the more than 20 years of work-arounds embedded in IPv4).

allocate resources to support both IPv4 and IPv6.[176] As a result, U.S. firms would have fewer resources to devote to IPv6-only products and services.

The requirement by potential first movers that the aforementioned economic levers from standardization be in place can act as a barrier to innovation because the profit potential is significantly reduced. Conversely, the cost of implementing a new standards infrastructure (as discussed in Section 2.2 *supra*) is substantial and not returnable to individual private firms. This situation raises a "chicken-or-egg" problem. ITEF has attempted to eliminate this concern by creating mechanisms to promote interoperability between IPv4 and IPv6 networks, thereby facilitating a gradual transition strategy.[177] However, the complexity of IPv6 implies the possibility that sequential and isolated implementations will not provide sufficient benefits of the types listed above to provide incentives to potential first movers. Thus, the possibility must be considered that a slow migration will also mean a slow realization of the potential greater benefits from IPv6. More concerted efforts in competitor nations to more rapidly implement IPv6 could provide advantages to those nations' domestic firms.

However, Internet equipment and software manufacturers already compete internationally and therefore should not be significantly affected by lagging U.S. adoption.[178] U.S. vendors will continue to develop and sell IPv6 products and services in the global marketplace even in the absence of U.S. adoption. Most of the major U.S. suppliers of hardware and software applications serve international markets and have subsidiaries in Asia and Europe. Technology developed and knowledge gained through subsidiaries' participation in regional markets where IPv6 activity is high should be transferable to the United States when U.S. deployment increases. This scenario will only hold, however, if learning economies in domestic markets are not essential to U.S. firms becoming competitive globally.[179]

---

[176] *See* Alcatel Comments at 4 (R&D activities could be diluted because new products and services will need to be dual protocol compatible, potentially causing U.S. companies to lag behind in developing next generation IPv6 applications).

[177] *See, e.g.*, Hain Comments at 10-12.

[178] *See* Cisco Comments at 11.

[179] This last point has some historical basis. Beginning in the 1980s, Japanese electronics firms regularly introduced new products into the Japanese domestic market first in order to gauge consumer reaction and gain production experience (lower cost) before committing to head-to-head competition in global markets. *See* Gregory Tassey, *The Economics of R&D Policy* (1997).

An important issue related to long-run U.S. competitiveness is the shift of intellectual (human) capital from domestic locations to foreign subsidiaries of U.S. companies. If much of the IPv6 research is conducted in Asia and Europe, this could lead to a trend of high-tech Internet applications development capabilities (and jobs) migrating to these regions. Even if the activities are associated with U.S. firms, this form of "outsourcing" could lead to shifts in intellectual capital and have implications for where the next generation of Internet capabilities is developed.

3.2.2 U.S. Corporate and Industrial Internet Users

U.S. companies that rely on the Internet to provide their products and services should not be substantially affected if the United States lags other parts of the world in IPv6 deployment. Large portions of the Internet will continue to operate in IPv4 and transition strategies have been, and will continue to be, developed to ensure interoperability between IPv4 and IPv6.

Several commenters suggested that government incentives could be used (*e.g.*, tax breaks or grants) to help offset transition costs.[180] In their view, those incentives could also be beneficial in the early stages of U.S. deployment to stimulate IPv6 adoption in enterprises.[181] However, other stakeholders have warned that government incentives would be unwise because they might skew the path of technology development or interfere with ongoing activities in the commercial marketplace.[182] These stakeholders prefer that government simply participate in the market by adopting IPv6 when it is beneficial to its needs.

Currently no productivity benefits for corporate or industrial uses are associated with operating IPv6 versus IPv4, and higher costs may be associated with early adoption of IPv6.[183] When more advanced IPv6 applications become available that represent efficiency gains, U.S. companies will be well positioned to take advantage of these opportunities. As discussed above, no market failures seem to exist that would limit rapid deployment of IPv6 once future applications emerge.

---

[180] *See* Motorola Comments at 2; NAv6TF Comments at 46.
[181] *See* Cisco Comments at 16; Motorola Comments at 2; NAv6TF Comments at 44.
[182] *See* Microsoft Comments at 12.
[183] Interview with John Streck, Centaur Labs (May 2004).

3.3 INTERNATIONAL INTEROPERABILTIY

Many of the issues related to general interoperability are even more relevant when discussed in an international context. Specific examples of international interoperability issues include different levels of conformance and implementation strategies across regions and legal and privacy implications of encryption restrictions across countries.

International interoperability issues associated with dual IPv4 and IPv6 network capabilities should be minimal because IPv4 is well established globally and can be used as a network foundation; however, interoperability between IPv6 applications needs to be tested more extensively in an international context.

Of particular significance to an international discussion is the impact of interoperability, or a lack thereof, on U.S. competitiveness both in Internet hardware and software and in other industries. The following sections address these issues.

3.3.1 Interoperability Implications for U.S. Competitiveness in Internet Hardware and Software Market

International interoperability generated by standardization tactics of individual countries can create market barriers for U.S. hardware and software suppliers by raising the cost for U.S. companies to compete in international markets. One such example is the current development of China's wireless standards. Until mid-May 2004, China intended to implement a new encryption standard for wireless communications and announced that verification of Wireless LAN Authentication and Privacy Infrastructure (WAPI) compliance would be part of its compulsory registration process for electronics.[184]

WAPI was portrayed as China's solution to the problem of securing wireless communication. However, multinational companies suggested that WAPI had security holes and gaps that would have created a burden for manufacturers who would have needed to meet one standard for China and another for the rest of the world.[185] The WAPI development is just one example of how a country could use a standard to create a trade barrier.

---

[184] *See* Grant Gross, "China agrees to drop WAPI standard," NetworkWorldFusion (Apr. 21, 2004), http://www.nwfusion.com/news/2004/0421chinaagree.html.

[185] *See* "China Promotes New Wireless Encryption Standard," PulseOnline (Dec. 2003), http://pulse.tiaonline.org/article.cfm?id=1911.

Even in a world where the international community cooperates to minimize problems, parallel ongoing development activities in Asia, Europe, and America will inevitably lead to interoperability issues, and companies that are active early in the process will have the opportunity to influence solutions and gain valuable experience. For example, to compete effectively in international router markets, U.S. suppliers will need to provide leading-edge support for IPv6. However, it may be more difficult to develop the needed capabilities if U.S. networks and services remain predominately IPv4-based. One commenter suggested that to compete in a global market with interoperability issues, IPv6 deployment should be encouraged domestically. As a result, American router vendors could move up the leaning curve more quickly and be competitive in international markets where IPv6 will be even more heavily (or more obviously) emphasized.[186] In other words, the usefulness of standards as a means of reducing interoperability problems, coupled with potential learning economies (a timing issue), are possible rationales for a more rapid transition to IPv6.

3.3.2 Implications for U.S. Competitiveness in Other Products and Services

U.S. suppliers of non-Internet-related hardware and software should not be put at a competitive disadvantage based on international interoperability issues, according to experts. In fact, for U.S. vendors, costs would also be lower in a scenario where the early deployment issues are encountered and resolved in foreign countries.[187]

In general, an embedded base of IPv4 equipment should not preclude the United States from the benefits of foreign IPv6 deployment, as long as there is a means to connect embedded IPv4 networks and equipment to newly-deployed IPv6 equipment when legacy application support is required. The developers of IPv6 have attempted to accomplish that goal by making IPv6 backward compatible with IPv4 via interoperability mechanisms.

However, a few commenters indicated that an embedded base of IPv4 equipment and applications could function as a barrier that would isolate the United States from the benefits of foreign IPv6 deployments and/or test beds. Forward-thinking entrepreneurs might not be able to develop

---

[186] *See* Alcatel Comments at 2.

[187] *See* BellSouth Comments at 6.

new services based on IPv6 or may simply participate in the new economies emerging in other IPv6 geographies.

With respect to domestic innovation incentives, small and medium U.S. businesses have limited resources. Thus, if they encounter high costs due to partial IPv6 deployment domestically, or if foreign competition benefiting from learning economies elsewhere in the world penetrates the U.S. market, barriers to domestic innovation efforts could be significant. Incomplete deployment also may send inaccurate market signals and result in premature introduction of IPv6 products, which could be damaging to small and medium firms.[188]

Finally, in the transition to IPv6, one of the most important interoperability objectives is to ensure the security and stability of IP networks around the world. Therefore, any transition to IPv6 should move forward in a cautious and technology-sensitive way to minimize adverse effects for users. International standards development and coordination bodies should be used to vet technical issues pertaining to IPv6 migration and the coordination of interoperability issues.

[188] *See* Cisco Comments at 16.

4 Government's Role in IPv6 Development and Deployment

As discussed in the Section 2, many of the original concerns motivating the development of IPv6, such as limited address space and security, may not be driving forces behind further deployment of IPv6 in the United States, at least in the near term. That does not imply, however, that potential benefits of adopting IPv6 do not exist, nor does it mean there is no potential role for government – particularly the federal government -- in influencing the realization of those benefits. The RFC comments and interviews conducted as part of this study suggest that government could take one or more of the following courses:

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

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

This section addresses the circumstances that could warrant government action to stimulate deployment of IPv6 in the United States. Market failures are commonly cited as one of the primary motives for government involvement in technology development and deployment. Technological market failure refers to a condition under which either the producers and/or users of a technology underinvest relative to society's optimal level of investment. Basic research to support standardization, development of interoperability solutions, and conformance testing are all classic examples of where private returns on investment are not only less than social returns but are below minimum private sector rates of return (so-called "hurdle rates"). In such cases, the needed infrastructure technologies (infratechnologies) and supporting services are commonly supported by government research and development (R&D) and technology transfer activities.[189]

Both the level of investment and the timing of investments will affect the potential benefits from IPv6. Sufficient levels of investment are needed to minimize interoperability problems and to realize the positive network externalities generated by IPv6.[190] Because network externalities are difficult for the private sector to appropriate, the public sector frequently supports investment in infratechnologies, such as conformance testing mechanisms and certification protocols.

The timing of investments will affect costs and benefits. Accelerating deployment beyond normal equipment/software replacement life cycles will increase transition and replacement costs. Alternatively, lagging behind other nations in the deployment of technologies such as IPv6

---

[189] "Infratechnologies" are a diverse set of technical tools that are necessary to conduct efficiently all phases of R&D, to control production processes, and to execute marketplace transactions for complex technology-based goods. Examples include measurement and test methods, process and quality control techniques, evaluated scientific and engineering data, and the technical basis for product interfaces. These tools are called infratechnologies because they provide a complex but essential technical infrastructure. Many infratechnologies are adopted as industry standards, emphasizing their public good content. *See* Tassey, note 179 *supra*, at 71. *See also* Tassey, note 173 *supra*.

[190] Network externalities arise from the fact that the value of a network to its users typically increases with the number of people that can *access* the network. Similarly, networking effects arise from the fact that the value of a network also increases with the number of individuals actually *using* the network. When a consumer decides whether to purchase and use a networked product or service (such as an IPv6-capable device), that person considers only the personal benefits of that purchase, and ignores the benefits conferred on all other users (*e.g.*, those users who may now have a new opponent in a IPv6-based gaming service). The individual may choose not to purchase the networked product or service, even though that purchase may have increased overall economic welfare. In consequence, deployment of the service (and the equipment and technologies that make that service possible) will be less than it "should" be. *See* Michael Parkin, *Economics* 504-510 (1990); Robert Willig, "The Theory of Network Access Pricing" in *Issues in Public Utility Regulation* 109 and n.2 (H. Trebbing ed. 1979).

may have competitiveness implications if foreign countries can capture first-mover advantages. Government can affect market evolution through its role as a major consumer of IPv6 products and services. Its purchases for internal government use have the potential to influence the timing of IPv6 deployment by providing initial markets of sufficient size to enable learning curve progression by suppliers and to create product/service performance data for potential private sector consumers.

This section begins with a discussion of "market failure" issues that have the potential to prevent or delay the development and deployment of new technical developments such as IPv6. This discussion is followed by a summary of respondents' suggested roles for government in supporting IPv6 and a discussion of how they relate to barriers to IPv6 development and deployment.

4.1 MARKET FAILURES AND UNDERINVESTMENT IN IPV6

Risk and difficulties associated with appropriating returns, capturing economies of scope from investment in disruptive generic technologies, and acquiring the research capabilities to address complex, multidisciplinary research requirements can create potential barriers to innovation and technology adoption and, as a result, may lead to an underinvestment in or underutilization of a technology. The premise that markets may "fail" to invest in socially optimal amounts of R&D or new technologies has long been accepted by economists and is now being embraced by policy makers.[191] Much of the technological market failure literature focuses on underinvestment in innovation or in the creation or production of R&D-based technology. However, these economic arguments are also applicable to the purchase and use of the technology that results from R&D.

[191] The theoretical and empirical literature concludes that the private sector will underinvest in R&D because of market failures. For a recent survey of that literature, see S. Martin and J. Scott., "The Nature of Innovation Market Failure and the Design of Public Support for Private Innovation," 29 *Res. Pol*: 437 (2000); S. Martin and J. Scott, "Financing and Leveraging Public/Private Partnerships" (1998) (final report prepared for OECD working group on technology and innovation policy).

Below we discuss several aspects of market failure related to IPv6 technology. We divide the source of market failures into two broad categories:

- appropriability issues for which social benefits exceed private benefits; and
- lack of coordination in developing and deploying IPv6 technology.

As apparent in the discussions below, these sources of market failure and their underlying characteristics are not mutually exclusive; rather the underlying economic arguments are related. Most of market failures are linked to the public goods nature of the Internet, which as a large and complex infrastructure is strongly affected by both the development of interoperability solutions and private sector adoption of standards and related infratechnologies.

4.1.1 Social Benefits Exceed Private Benefits

Appropriability issues are at the heart of most market failures and can lead to underinvestment in technology development and deployment from society's perspective.[192] Underinvestment occurs because conditions exist that prevent firms from fully realizing or appropriating the benefits created by their investments, causing firms to view prospective investments as having expected rates of return below the firm's minimum acceptable rate of return (hurdle rate).[193] Although firms may recognize that there are spillover benefits to other markets or consumers, they are likely to ignore or heavily discount these benefits. Infratechnology research to support development of interoperability solutions, conformance testing, and other infratechnologies that become the basis of standards are all paradigmatic examples of cases where private returns to investment can be less than both social returns and private hurdle rates. As a result, those activities are frequently supported by government activities.[194]

---

[192] Appropriability refers to a firm's ability to collect rents from their investments in research and development (R&D). For example, patents are granted so that inventors can appropriate monopoly returns over a period of time from their research. Imitation and information spillovers frequently limit a firm's ability to appropriate return from investments and can create disincentives for conducting R&D.

[193] Much of the literature investigating market failures has presented the theories in the context of R&D investment. However, these insights are equally applicable for investments in the adoption and integration of new technologies such as IPv6.

[194] *See* Tassey, note 173 *supra*.

Spillovers and Appropriability Issues

Many factors affect a firm's ability to appropriate returns. Knowledge spillovers and ineffective patent protection are commonly cited as limits on a firm's ability to recoup R&D expenditures. Firms may underinvest if the nature of the technology is such that it is difficult to assign intellectual property rights. Additionally, knowledge and ideas developed by a firm may spill over to other firms during the R&D phase or after the new technology is introduced into the market. For example, an ISP working on research to develop mobile IPv6 products might see low or nonexistent returns because of rapid imitation that limits the probability that the firm can appropriate sufficient returns to cover its R&D investment. Moreover, because the standards associated with mobile IPv6 products must be, by definition, commonly used by competitors and customers, appropriability is virtually non-existent for the infratechnologies supporting standardization.

The presence of appropriability issues does not mean that a market failure will occur, however. For that to happen, the gap between social and private returns must be large enough to suppress private-sector investment. Individual firms are rarely able to capture all the social returns generated by their investments. In addition to spillovers to non-investing firms, well-functioning markets result in some benefits being captured by consumers as "consumer surplus." Otherwise, consumers would have no incentive to switch to the new technology. Both factors reduce profits for innovating firms. The existence of consumer benefits is part of the normal distribution of social returns and is only considered a market failure if those "market spillovers" are large enough to deter significantly private-sector investment well below socially optimal levels.

The RFC comments demonstrate that there is uncertainty among U.S. ISPs and the software community about whether the private returns from IPv6 deployment and its subsequent market opportunities will justify the costs associated with the transition.[195] However, these concerns are attributable less to appropriability issues and more to (1) uncertainties over users' willingness to pay for IPv6 products and services, and (2) the negative effect of relatively high corporate discount rates applied to the up-front, and potentially substantial, transition costs.

---

[195] *See* Internet2 Comments at 9; Motorola Comments at 9.

In apparent contradiction to the foregoing assessment, most commenters see no need for government intervention and expect market forces to generate sufficient returns to drive efficient development and deployment of IPv6 over time.[196] The transition technologies being developed and implemented by the IETF were intended to ensure that initially small negative network externalities would not hinder the adoption of IPv6. The IETF's objective is for IPv6 systems, devices, and products to be able to interoperate with IPv4 networks and devices, thereby avoiding the potential disincentive to first movers attributable to negative network externalities.[197]

Because of the public goods nature of the research needed to develop and deploy IPv6, some commenters see a continuing need for government support.[198] Appropriability issues are most likely to occur as part of the development of infratechnologies and generic technologies needed to enable IPv6. As a general rule, early actions or market interventions by government are likely to have the greatest impact on IPv6 deployment. One commenter notes that government activities that take place over the initial 3 years of IPv6 development and deployment may have significant long-term returns for both private (monetary) and public interest.[199]

Because of the public goods nature of networks, positive externalities generating excess social surplus are created with the establishment of networks. The telephone system is a frequently-cited example of how all participants benefit as a network grows. The central issues are when applications will materialize, and how long it will take to generate a critical mass to yield the network externalities needed for IPv6 to take off. There is no fundamental reason to believe that this will not happen as part of natural market forces. However, as will be investigated in the second phase of this study, it is possible that society could benefit from accelerating the natural market-based adoption process.

In general, the closer R&D activities move toward commercialization, the less government should be involved. Market forces should be allowed to drive research for product and service development, where there is a

---

196 *See* Lockheed Comments at 3; Microsoft Comments at 12-13; Motorola Comments at 8; Qwest Comments at 1.

197 *See* Cisco Comments at 25-26.

198 *See* NAv6TF Comments at 37-38; Sprint Comments at 14.

199 *See* Hain Comments at 20.

greater likelihood that firms will be able to appropriate adequate returns, and where innovators are more likely to face risk and reward conditions compatible with private sector investment criteria.

Monopoly Power

To the extent that any hardware or software vendor has monopoly power, then that vendor has the potential to exploit its market dominance to increase its private returns at the expense of social welfare. Related to IPv6, this could happen along two dimensions. Along one dimension, the monopolist could create or slow the resolution of the chicken-or-egg dilemma (discussed below) because of its critical position in the supply chain. For example, a monopolist may have a financial incentive to exploit its current technology (*i.e.*, IPv4) for as long as possible. Along a second dimension, the monopolist could attempt to slow the development of standards and protocols because it would be in a position to dictate technical characteristics (*i.e.*, to set and enforce its proprietary protocols).

However, commenters generally denied that monopoly power for IP products or services exists now or will develop in the future. IPv6 is a standard that is available to anyone, and there are enough IPv6-capable products available today to avert a monopoly.[200] Support for IPv6 is widespread in most hardware platforms deployed in service providers' networks today, and the standards are available and continue to evolve in the public domain.[201] Devices that are IPv6-capable are also being developed to be IPv4-capable as well. Additionally, IPv4 and IPv6 are substitutes; therefore, any company implementing IPv6 would need to compete with both the huge installed base of IPv4 products, new IPv4 products, and other IPv6 products.[202] One respondent pointed out that transition technologies were specifically designed to break the dependence of IPv6 applications and ISP routing services on one another.[203] Therefore, existence of a monopoly seems unlikely.

4.1.2 Lack of Coordination

Coordination failures arise from asymmetries in incentives or information between market participants, either among competitors or along the

---

[200] *See* Cisco Comments at 25; Hain Comments at 19; NAv6TF Comments at 39.
[201] *See* Qwest Comments at 4.
[202] *See* Cisco Comments at 25.
[203] *See id.* at 24-25.

supply chain. For example, firms acting in their self-interest may invest in standards or technologies that are not optimal for the industry as a whole, or competing implementation procedures developed independently may not interoperate. It has been shown that coordination activities can lower the cost of development and increase the quality of new technologies.[204]

Government's participation in the market as a major consumer and its mission to promote long-run national objectives positions it well to serve vital coordination roles. As an independent third-party, government can promote a collaborative process that facilitates all parties having the opportunity to be represented. Government can also help coordinate mutually beneficial outcomes, both vertically and horizontally, without concerns about collusion or anticompetitive practices.

Chicken-or-Egg Dilemma

When complementary products or services are needed to realize the benefits from a new technology, the potential for a chicken-or-egg dilemma arises. A well-known example of this phenomenon is the linkage between the adoption of high definition television (HDTV) sets and the availability of high definition content. In such cases, increased deployment of one of the component technologies generates externalities that increase the benefits to be derived from the adoption of the complementary technologies.

Similarly, for IPv6, the chicken-or-egg dilemma can be defined as the presence of disincentives for investment in supporting infrastructure until applications are deployed, contrasted with disincentives for investment in applications until supporting infrastructure is in place. If equipment manufacturers and software manufacturers are reluctant to make the first-mover investments until complementary IPv6 infratechnologies/standards are in place, a chicken-or-egg dilemma could materialize.

Several commenters said that there is a chicken-or-egg problem associated with IPv6. In their view, demand is not currently high enough

---

[204] Van Huyck, Battalio, and Beil showed that in the absence of communication, strategic uncertainty can lead to coordination failures resulting in suboptimal market equilibrium. J. Van Huyck, R. Battalio, and R. Bell, "Strategic Uncertainty, Equilibrium Selection Principles, and Coordination Failure in Average Option Games," 106 *Q. J. of Econ.* 885 (1991); J. Van Huyck, R. Battalio, and R. Bell, "Tacit Coordination Games, Strategic Uncertainty, and Coordination Failure," 80 *Am. Econ. Rev.* 234 (1990).

to push vendors and ISPs to deploy IPv6 products and services, while uncertainty exists on the part of potential buyers of those products and services regarding the nature, degree, and timeliness of IPv6 benefits.[205] Commenters holding this view also suggested that government could act as a source of information to help resolve this chicken-or-egg dilemma. Infrastructure issues, such as the prevalence of NAT boxes and fear of interdependence between IPv6 applications and ISP routing services, are among the reasons why some networks are not testing and developing IPv6 applications.[206]

However, most commenters indicated that no chicken-or-egg problem exists, noting that markets are pushing IPv6 development and deployment in an appropriate time frame. They stated that transition mechanisms were designed specifically to circumvent this problem from a technical perspective and noted ongoing development activities resulting from market demand.[207]

Based on a review of the RFC responses and interviews with stakeholders, it is unlikely that IPv6-related chicken-or-egg issues will affect the development and deployment of IPv6. In general, IPv6 is not a totally new infrastructure. IPv6 and IPv4 are not exclusively different alternatives in that most benefits associated with IPv6 can also be realized by an enhanced IPv4 system (however, at potentially greater costs). For this reason, IPv6 will likely be deployed over time, and to differing degrees, by various stakeholder groups, as opposed to a mass migration. Because IPv6 and IPv4 are designed to be interoperable during the transition period, moreover, this mitigates any potential chicken-or-egg dilemma.

The chicken-or-egg issue can also be stated in terms of uncertainty over users' willingness to pay for IPv6-enabled products. Consumer's valuation of products and services, however, is typically not a market failure issue. For a problem to exist, barriers to market growth, in particular, market aggregation must be demonstrated. As pointed out in Section 3, large markets based on a new standard do not necessarily materialize instantly. Small market segments can appear that do not

---

[205] *See* Hain Comments at 18; Internet2 Comments at 2; Lockheed Comments at 6; Motorola Comments at 2-3.

[206] Once large-scale transition begins, most software would be IPv6 enabled within 24 months through general market forces. *See* Internet2 Comments at 2.

[207] *See* Cisco Comments at 25; Microsoft Comments at 9; NAv6TF Comments at 38; Qwest Comments at 2-3.

initially benefit from significant externalities. In fact, aggregation to larger markets typically occurs over time.

Segmentation, especially if accompanied by interoperability problems across segments can inhibit the aggregation process. The ITEF transition strategy is designed to avoid such a situation by allowing initially small IPv6 markets to coexist (interoperate) with IPv4 applications, thereby avoiding an all-or-nothing transition. Nevertheless, coexistence does not guarantee market agglomeration for IPv6 applications.

In summary, the prevailing view seems to be that the drivers for IPv6 technologies will be consumer and enterprise applications that require IPv6 or that are impractical and more costly to implement via IPv4. Once these technologies materialize, ISPs should be able to rapidly enable hardware (which should already be IPv6 capable). Assuming that the initial markets are sufficiently large to enable at least modest network externalities and that adequate interoperability is provided, users will likely move quickly to make the required investments to adopt IPv6 software applications.[208]

Standards, Protocols, and Conformance

The enabling of IPv6 technology cannot occur in the absence of standards and protocols that facilitate the coordination of the technologies along the supply chain and across different suppliers. Standards are a classic example of a public good because they represent a type of infrastructure where spillovers are not only socially desirable but necessary (a standard by definition implies common [nonrivalrous] use). In general, the Internet, by its very nature, is an open system, and the value of IP standards increases with the free flow of information. As a result, there has been, and will continue to be, an important role for government in how the Internet and related technologies evolve.

IPv6 development has been the subject of public and private research for many years, with the majority of findings residing in the public domain. However, many issues still must be addressed with respect to both infrastructure and applications. Private returns alone are not likely to

[208] *See* Lockheed Comments at 3; NAv6TF Comments at 38.

provide sufficient motivation to stimulate investments in these areas.[209] Because network externalities generated by nonproduct standards cannot be appropriated, private incentives to participate in the standards development process are typically well below socially optimal benefits and lead to suboptimal levels of participation.[210] For this reason, the public sector has a stake in the IPv6 standards development process, program coordination, technology development, and information dissemination. As noted above, government agencies are in a unique position to promote collaborative processes.

Government could also participate in implementing IPv6 through activities such as conformance testing.[211] Most respondents to the RFC indicated that government could continue and even expand its coordination and funding of research to develop solutions to interoperability problems. Test trials and roadmap processes are critical for IPv6 systems developers and implementers. For example, respondents proposed that the U.S. government could support IPv6 research into interoperability with existing IPv4 systems[212] in addition to coordinating trials and tests of new IPv6-enabled devices—routers, hosts, PDAs, etc. Government could support both the harmonization of standards and interoperability testing activities, such as those currently being developed and performed by the University of New Hampshire, the TAHI project, and the European Telecommunications Standards Institute (ETSI).[213]

---

[209] This reflects RTI's judgment based on the RFC comments, the relevant literature, and interviews with industry stakeholders

[210] *See* Tassey, note 173 *supra*.

[211] Government agencies have a proven history of working with private-sector organizations to provide conformance testing and validation certificates. For example, NIST recently led the selection and testing of the Advanced Encryption Standard (AES) that specifies a cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. It is anticipated that the AES will be used widely on a voluntary basis by organizations, institutions, and individuals outside of the U.S. government and outside of the United States. As part of the development process, algorithm testing was conducted under the Cryptographic Module Validation Program (CMVP), run jointly by NIST and the Communications Security Establishment (CSE) of the Government of Canada. Commercial, accredited laboratories also test cryptographic implementations for conformance to NIST's standards, and if the implementations conform, then NIST and CSE issue jointly signed validation certificates for those implementations. *See* National Institute of Standards and Technology, *Report on the Development of the Encryption Standard (AES)* (Oct. 2002), http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf.

[212] *See* Motorola Comments at 2.

[213] *See* NAv6TF Comments at 24.

4.2 POTENTIAL ROLES FOR GOVERNMENT INVOLVEMENT IN IPV6

The general consensus is that market forces should be allowed to drive the transition from IPv4 to IPv6. No stakeholder indicated that significant market impediments exist for the adoption of IPv6; thus, all stakeholders believed that the federal government should refrain from actions that would significantly interfere with market forces. As MCI points out, "Although the deployment of IPv6 has occurred more slowly than was anticipated when the IETF began work on IPv6, there is no evidence of a market failure warranting government intervention. To a great extent, the current pace of IPv6 deployment reflects the normal weighing of benefits and costs that is associated with any technology deployment."[214]

Many respondents referenced the GOSIP mandate and indicated that widespread concern and a lack of confidence remained within the computer networking community regarding government-led standardization activities.[215] One expert suggested that considering the negative impact of the GOSIP initiative, government should not consider a mandate for IPv6 but rather contribute to the development and deployment of IPv6 by facilitating testing and other collaborative efforts.[216] All stakeholders agreed that a mandate for IPv6 is not appropriate at this time.

However, in partial contrast, most respondents also emphasized the public good nature of IPv6 and suggested that the public sector should

---

[214] MCI Comments at 6.

[215] In the 1990s, the government decided to initiate the GOSIP, or Government Open Systems Interconnection Profile, mandate to force the conformance of an Open Systems Interconnect (OSI) standard. In this instance, the U.S. government mandated that all government agencies use GOSIP. According to RFC 1169, published by IAB, GOSIP was "needed because OSI standards allow many potential options and choices, some of which are incompatible." V. Cerf and K. Mills, "RFC 1169—Explaining the Role of GOSIP" (1990), www.faqs.org/rfcs/rfc1169.html. Although more than 20 different agencies participated in developing the GOSIP specifications, a 1992 survey of buying plans at several large government agencies revealed that only 20 percent had begun to implement the GOSIP standards, and only Hewlett-Packard Co. and Novell, Inc., had GOSIP-certified products available (*InformationWeek*, 1992). Few OSI applications ever became available; thus, government agencies generally continued to use and expand their use of the Internet Protocol Suite (IPS). In 1995, the Secretary of Commerce removed the mandate on OSI usage by government agencies. According to a bulletin released by NIST in May 1995, the Federal Internetworking Requirement Panel concluded that "federal government agencies should have flexibility to select networking protocol standards based on such factors as interoperability needs, existing infrastructure, costs, the availability of marketplace products, and status of a protocol suite as a standard." National Institute of Standards and Technology, "Standards For Open Systems: More Flexibility For Federal Users" (1995), http://www.itl.nist.gov/lab/bulletns/archives/b595.txt.

[216] Interview with John Streck, Centaur Labs (October 2003).

foster development and deployment. This was frequently linked to concerns that the United States is lagging behind in developing and deploying IPv6 and that U.S. competitiveness and IT leadership will suffer without appropriate government activity. In addition to national competitiveness, security issues were also cited as a motivating factor for government involvement in IPv6. Although there was no agreement on whether IPv6 would lead to security improvements, the public goods nature of Internet security in general was acknowledged along with concerns regarding the maintenance of security during the transition to IPv6.[217] For example, commenters suggested that both government and the private sector need to work on trust relationships and key management (*e.g.*, PKI development).

Based on responses to the RFC and interviews by RTI with industry stakeholders, potentially helpful government activities that may support the development and deployment of IPv6 fall into three areas:

- government support for R&D;
- government as a consumer; and
- information dissemination.

4.2.1 Government Support for R&D

All respondents suggested the government should support certain types of R&D activities. Several groups that currently perform (or did so in the past) Internet-related testing and/or research were mentioned: NIST, the National Science Foundation (NSF), the Department of Energy (DOE), NASA, and Advanced Research Projects Agency/Defense Advanced Research Projects Agency (ARPA/DARPA). It was stated that organizations such as NIST and NTIA are ideally positioned to help foster and facilitate universities and government collaboration with industry.[218]

To ensure that IPv6-enabled services are deployed in a timely manner, the government could work to ensure that the necessary base of skilled human resources is available, that the research effort is sustained, and that standards and specifications work is accelerated. Suggestions for specific research focus areas include interoperability, security, multihoming, and transition mechanisms, among others. Additionally, the government might support the development of new applications and

---

[217] *See* Cisco Comments at 26-27; Microsoft Comments at 11.

[218] *See* Network Conceptions Comments at 23.

possibly initiate test beds similar to Moonv6, as appropriate to the needs of its agencies. Government funding for advanced test bed deployment could be made available and advertised appropriately. However, commenters mentioned that such funding should not be used to pick technological winners or losers.[219]

Some of the areas that commenters identified for further research include the following:[220]

- testing of IPv6's interoperability with existing IPv4 systems;
- techniques to improve the performance and efficiency of IPv6 for key applications such as VoIP;
- mobile IPv6 routing;
- routing limitations in which the cost of a multihomed site is not completely borne by that site, but rather by the network as a whole;
- performance in dual IPv4/IPv6 environments;
- security in dual-stack environments;
- intrusion detection techniques for IPv6, including implications for changes in the use of tunneling and NATs;
- privacy implications of IPv6;
- PKI scalability and trust models; and
- secure Border Gateway Protocol (BGP) implications.

4.2.2 Government as a Consumer

Most commenters stated that government intervention to direct the markets for IPv6 products and services would be unwarranted and potentially harmful. However, all respondents indicated that government has an important role to play as a major consumer of IPv6 products and services. From this perspective, federal agencies could play a significant role as early adaptors of IPv6.[221]

One commenter suggested that the lack of interest in IPv6 from government agencies—other than DoD—is acting as an impediment to the development and deployment of IPv6.[222] Several commenters suggested that all government agencies should adopt the same schedule as the DoD, or something very similar, beginning as soon as possible.

---

[219] *See* NAv6TF Comments at 43; Lockheed Comments at 2-3; Microsoft Comments at 12.

[220] *See* BellSouth Comments at 9; Cisco Comments at 28; Motorola Comments at 9; NAv6TF Comments at 44.

[221] *See* MCI Comments at 9.

[222] *See* Cisco Comments at 26.

However, most commenters suggested government agencies adopt IPv6 only when such adoption meets agency needs. They also recommended against requiring state and local governments to establish specific IPv6 deployment schedules.

On the other hand, the federal government could encourage its own networks to formulate transition plans and begin implementing IPv6 as soon as practical. Where appropriate, intragovernment guidelines could be drafted to require suppliers of IP products and services to provide IPv6-compatible versions by a certain date. GSA could potentially take on the role of government-wide planning for transition to IPv6 by formulating procurement guidelines for all agencies and providing support in the development of their transition strategies and IPv6 implementation goals.[223]

4.2.3 Information Dissemination

The federal government has an important role in disseminating information and providing training support to promote and lower the cost of IPv6 deployment. The government can help to ensure that all stakeholders are aware of the benefits and costs of IPv6 and disseminate information to individual companies to promote the development of cost-effective transition strategies.[224]

Government could engage in awareness campaigns and provide training resources to disseminate information on IPv6. In addition to attending and presenting at networking conferences that large corporations attend, small business users could be targeted through organizations such as the Small Business Association (SBA) or NIST's Manufacturing Extension Partnership (MEP) program. Many small businesses could potentially realize benefits through IPv6 adoption.[225]

A key component of any company's transition strategy will be staff training and education. Training and education are likely to be one of the greatest cost components associated with adopting IPv6. Not only will existing staff need to be retrained, but many new graduates will also need additional specific training because universities are not producing sufficient numbers of IPv6-aware network engineers.[226] Cisco Systems

---

[223] GSA Comments at 11.
[224] *See* Dillon Comments at 2.
[225] *See* Network Conceptions Comments at 2.
[226] *See* Hain Comments at 13.

suggests that until the IPv6 "educated base" is expanded, meaning that networking students learn about IPv6 technology, training costs will be very large. Other commenters agree and suggested that government involvement could offset some of this cost.[227]

Government could continue, and possibly expand, its collaborations with universities to provide centers of learning for IPv6. This could include seminars, workshops, and training classes to support local businesses. Classes focused on teaching the business community the technical specifics of IPv6 implementation (*e.g.*, transition techniques and required hardware and software upgrades/replacements) and use (e.g., applications and tools) have the potential to lower the cost of and accelerate the deployment of IPv6.

Additionally, the government could increase its participation in groups such as the IETF to help develop "best current practices" to be used in these education programs or merely posted for use by government agencies and U.S. companies.[228] The government could also create and maintain an information library of IPv6 information and resources that interested parties can access.[229] The NAv6TF goes further, suggesting that the government encourage the integration of IPv6 through the creation of a favorable, stable, and government-supported program to avoid the development of fragmented approaches.[230]

In general, many commenters agreed that, by actively supporting and funding training opportunities and promotional activities, government could help lower the cost of IPv6 deployment.[231]

---

[227] *See* Cisco Comments at 29; Dillon Comments at 2; NAv6TF Comments at 45-46.

[228] *See* Cisco Comments at 28.

[229] *See* Hain Comments at 18.

[230] NAv6TF Comments at 45-46.

[231] *See* Cisco Comments at 28-29; Dillon Comments at 2; GSA Comments at 11; Internet2 Comments at 10; NAv6TF Comments at 45-46.

Glossary

Sources used to compile this glossary were Webopedia (http://www.pcwebopedia.com/) and hyperdictionary (http://www.hyperdictionary.com/).

3GPP: 3rd Generation Partnership Project (3GPP), a GSM-based consortium advocating standardization for mobile communications, who published Release Five of the Universal Mobile Telecommunications System (UMTS) standard mandating the use of IPv6 by wireless vendors.

Always-on applications: Applications that are always able to accept a connection from a host on the Internet. Such applications need to be running on a host that has a unique, globally accessible IP address. An increase in the number of always-on application would require a concomitant increase in IP address space.

APNIC: Abbreviation for the Asia Pacific Network Information Centre, one of four nonprofit organizations that register and administer IP addresses. APNIC serves the Asia Pacific region, which consists of 62 economies.

Application layer: The top layer of the OSI seven-layer model. This layer handles issues like network transparency, resource allocation, and problem partitioning. The application layer is concerned with the user's view of the network (e.g., formatting electronic mail messages).

ARIN: Acronym for the American Registry for Internet Numbers. ARIN, founded in 1997, is a nonprofit organization that registers and administers IP numbers for North America, a portion of the Caribbean and sub-Saharan Africa. ARIN is one of four regional Internet registries.

B2B solutions: Short for business-to-business, the exchange of services, information, and/or products from one business to another, as opposed to between a business and a consumer (B2C).

Backbone ISP: A large ISP that manages Internet traffic on a national or regional scale, using extremely large routers and other hardware and software network components.

Billing system: System that tracks customer usage of services, and calculates the impact on a customer's account, based on the price of the services. Billing systems have come to include noncore functionality such as customer management, integration with payment gateways, and statistical analysis.

Bit: Short for binary digit, the smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1. More meaningful information is obtained by combining consecutive bits into larger units. For example, a byte is composed of 8 consecutive bits.

Bootstrap Protocol: Allows a diskless client machine to discover its own IP address, the address of a server host, and the name of a file to be loaded into memory and executed.

Byte: Binary term, a unit of storage capable of holding a single character. On almost all modern computers, a byte is equal to 8 bits. Large amounts of memory are indicated in terms of kilobytes (1,024 bytes), megabytes (1,048,576 bytes), and gigabytes (1,073,741,824 bytes).

Conformance test: A test performed by an independent body to determine if a particular piece of equipment satisfies the criteria in a specified controlling document, such as a Federal standard, an American National Standard, a Military Standard, or a Military Specification.

Data link layer: Layer two, the second lowest layer in the OSI seven-layer model—it splits data into frames for sending on the physical layer and receives acknowledgement frames. It performs error checking and retransmits frames not received correctly. It provides an error-free virtual channel to the network layer. The data link layer is split into an upper sublayer, Logical Link Control (LLC), and a lower sublayer, Media Access Control (MAC).

Diffserv: Is an architecture for providing different types or levels of service for network traffic. One key characteristic of diffserv is that flows

are aggregated in the network, so that core routers only need to distinguish a comparably small number of aggregated flows, even if those flows contain thousands or millions of individual flows.

DNS: Short for *Domain Name System* (or *Service*), an Internet directory service that translates alphabetic domain names into numeric IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on numeric IP addresses. Every time you use a domain name in an e-mail address or Web address, the name must be translated into a corresponding IP address. For example, the domain name *www.cisco.com* might translate to *198.105.232.4*. DNS servers hold the directories that translate a name to an IP address.

The DNS system is, in fact, its own hierarchical network. If one DNS server doesn't know how to translate a particular domain name, it asks, or refers the requestor, to another one, and so on, until the correct IP address is resolved.

Domain Name: A name that generally identifies an organization on the Internet (e.g., *Cisco.com*). Multiple host URLs can be specified in each domain (e.g., *www.support.cisco.com*, *www.sales.cisco.com*, etc.). Each name (or URL) corresponds to a numeric IP address which may be retrieved (resolved) by contacting the appropriate Domain Name Server.

DSL: Refers collectively to all types of digital subscriber lines; the two main categories are ADSL and SDSL. Two other types of xDSL technologies are high-data-rate DSL (HDSL) and very high DSL (VDSL). DSL technologies use sophisticated modulation schemes to pack data onto copper wires.

Dual stack: A network node running both IPv4 and IPv6 protocol stacks (or possibly others) at the same time. Such a machine can act as a protocol converter between the two networks.

Dynamic Host Configuration Protocol: A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.

This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

End-to-end applications (E2E): applications which communicate on the Internet in such a way that each application can originate a direct connection to the other.

Enterprise Resource Planning (ERP) software: A business management system that integrates all facets of the business, including planning, manufacturing, sales, and marketing. As the ERP methodology has become more popular, software applications have emerged to help business managers implement ERP in business activities such as inventory control, order tracking, customer service, finance, and human resources.

Firewalls: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Global Information Grid (GIG): Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

GSM: Short for Global System for Mobile Communications, one of the leading digital cellular standards. GSM uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency. GSM was first introduced in 1991. As of the end of 1997, GSM service was available in more than 100 countries and has become the de facto standard in Europe and Asia.

Header: The header is the part of a packet containing administrative information (such as destination address or encryption type). The header is used by the network and/or host in delivering and presenting the payload information to the recipient application.

Host: (1) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address. The system that

contains the data is typically called the host, while the computer at which the user sits is called the remote terminal; (2) A computer system that is accessed by a user working at a remote location.

IETF: Internet Engineering Task Force, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

Instant messenger: Allows users to send and receive short messages instantly.

Interoperability: The ability of software and hardware on different machines from different vendors to share data.

Internet2: a consortium being led by 206 universities working in partnership with industry and government to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet. Internet2 is recreating the partnership among academia, industry, and government that fostered today´s Internet in its infancy.

Internet Control Message Protocol (ICMP): An extension to the Internet Protocol (IP) that allows for the generation of error messages, test packets, and informational messages related to IP. It is defined in STD 5, RFC 792.

Internet Protocol (IP): IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system. It allows users to address a package and drop it in the system, but there is no direct link between the user and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Internet service provider (ISP): A company that provides access to the Internet. For a monthly fee, the service provider gives users a software package, username, password, and access phone number. Equipped with a modem, users can then log on to the Internet and browse the World Wide Web and USENET and send and receive e-mail. In addition to serving individuals, ISPs also serve large companies, providing a

direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs). ISPs are also called IAPs (Internet Access Providers).

IP stack: A particular software implementation of a computer networking protocol suite. Strictly speaking, the suite is the definition of the protocols and the stack is the software implementation of them.

IPv4: Internet protocol version 4. IPv4 is the current IP version used on the Internet.

IPv6: Internet protocol version 6. IPv6 is the latest iteration of IP for the Internet.

Moonv6: A collaborative effort between the North American IPv6 Task Force (NAv6TF), the University of New Hampshire-InterOperability Laboratory (UNH-IOL), the Joint Interoperability Testing Command (JITC) and various other DoD agencies, and Internet2. Taking place across the United States at multiple locations, the Moonv6 project represents the most aggressive collaborative IPv6 interoperability and application demonstration event in the North American market to date.

Network layer: The third lowest layer in the OSI seven-layer model, the network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.

Node: In networks, a processing location, so a node can be a computer or some other device, such as a printer. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.

North American IPv6 Task Force (NAV6TF): A subchapter of the IPv6 Forum dedicated to advancing and propagating IPv6 *(Internet Protocol, version 6)* in the North American continent. Comprising individual, rather than corporate, membership, the NAv6TF mission is to provide technical leadership and innovative thought for the successful integration of IPv6 into all facets of networking and telecommunications infrastructure, present and future.

OSI or OSI seven-layer model: A model of network architecture and a suite of protocols (a protocol stack) to implement it, developed by ISO in 1978 as a framework for international standards in heterogeneous computer network architecture. The OSI architecture is split between

seven layers, from lowest to highest: 1 physical layer, 2 data link layer, 3 network layer, 4 transport layer, 5 session layer, 6 presentation layer, 7 application layer. Each layer uses the layer immediately below it and provides a service to the layer above. In some implementations a layer may itself be composed of sublayers.

OSPF (Open Shortest Path First): An interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm.

Packet: A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams and are comprised of an "administrative" header and a payload

Physical layer: Layer one, the lowest layer, in the OSI seven-layer model, concerning electrical and mechanical connections to the network. The physical layer is used by the data link layer. Example physical layer protocols are CSMA/CD, token ring, and bus.

Protocol: An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used; data compression method, if any; how the sending device will indicate that it has finished sending a message; and how the receiving device will indicate that it has received a message. There are a variety of standard protocols from which programmers can choose. Each has particular advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.

Proxy: A device that acts on behalf of another device by taking on its identity to interact with the outside world.

RIPE NCC: Short for the Réseaux IP Européens Network Coordination Centre, RIPE NCC is one of four regional Internet registries that supply and administer IP addresses. Founded in 1989, RIPE NCC is a nonprofit organization. RIPE NCC provides IP numbers to Europe, the Middle East, and parts of Africa and Asia.

Router: A device that forwards data packets along networks, a router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets,

and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

Segment: In networks, a section of a network that is bounded by bridges, routers, or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN. Most network traffic will remain within a single segment, enjoying the full 10 Mbps bandwidth. Hubs and switches are used to connect each segment to the rest of the LAN.

Server: A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers. A database server is a computer system that processes database queries. Servers are often dedicated, meaning that they perform no other tasks besides their specific server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Translation: the process of translating one protocol to another such that users of either protocol can communicate in their native mode. Limitations arise when one protocol has elements which can not be translated into the other protocol.

Transport layer (Or "host-host layer"): The middle layer in the OSI seven-layer model. The transport layer uses the network layer to establish a conversation between two hosts. An example is the transmission control protocol (TCP), which provides a virtually error-free point-to-point connection that allows messages to arrive uncorrupted and in the correct order.

Tunneling: A technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. Tunneling is also called encapsulation.

UMTS: Short for Universal Mobile Telecommunications System, a 3G mobile technology that will deliver broadband information at speeds up to

2Mbps. Besides voice and data, UMTS will deliver audio and video to wireless devices anywhere in the world through fixed, wireless, and satellite systems.

VoIP: Voice over IP. Using an IP network to carry voice data.
WAPI: China's Wi-Fi GB 15629.11-2003 encryption standard, which differs from the existing IEEE 802.11 global standard.

References

American Registry for Internet Numbers (ARIN). <http://www.arin.net/policy/index.html>. Obtained on May 15, 2004.

Arano, Takashi. June 2003. "IPv6 Market Opportunities—Real Business Challenges in Japan." Presented at the U.S. IPv6 Summit.

Arrow, K.J. 1962. "Economic Welfare and the Allocation of Resources for Invention." In *The Rate and Direction of Inventive Activity*, Universities-National Bureau Committee for Economic Research, pp. 609-625. Princeton: Princeton University Press.

ASTM International. 2001. "Mechanically Attached Pipe Fittings." *Standardization News*. As accessed on November 8, 2002. <http://www.ast.org/SNEWS/NOVEMBER_2001/case_nov01.html>.

Baldwin, W.L., and J.T. Scott. 1987. *Market Structure and Technological Change*. London: Harwood Academic Publishers.

BizRate.com. 2003. "Consumers Continue to Buy Online in Q1 2003, Despite War and Iraq." <http://merchant.bizrate.com/oa/general/press/release.xpml?rel=144>.

Bush, George. 1990. Executive Office of the President. *U.S. Technology Policy*. Washington, DC: Office of Science and Technology Policy.

Bush, George W. February 2003. Executive Office of the President. *The National Strategy to Secure Cyberspace*. Washington, DC. <http://www.theshitehouse.gov/pcipb>.

Cerf, V., and K. Mills. 1990. "RFC 1169—Explaining the Role of GOSIP." Available at <www.faqs.org/rfcs/rfc1169.html>.

Charney, Ben. July 28, 2003. "U.S. Shrugs Off World's Address Space Shortage." CNET News.com. <http://news.com.com/2100-1033_3-5055803.html?tag=fd_lede1_hed> As obtained on May 10, 2004.

Cisco Systems. 2003a. "SAFE: A Security Blueprint for Enterprise Networks." <http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm>. Posted Wednesday, October 22, 2003. As obtained October 2003.

Cisco Systems. 2003b. "Software Products." <http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_the_abcs_ip_version_60900aecd800c 1129.html>. As obtained October 2003.

Clinton, William. 1994. *Economic Report of the President*. Washington, DC: U.S. Government Printing Office.

CNETAsia. 2003. "Japan, China, and South Korea to Develop IPv6 in Asia." <http://asia.cnet.com/newstech/systems/0,39001153,39162960.htm>. As obtained on April 1, 2004.

Coopers & Lybrand/TASC. 1994. The DoD Regulatory Cost Premium: A Quantitative Assessment.

David, P.A. 1987. "Some New Standards for the Economics of Standardization in the Information Age." In *Economic Policy and Technological Performance*, P. Dasgupta and P. Stoneman, (eds.), pp. 206-239. Cambridge: Cambridge University Press.

Deering, S., and R. Hinden. December 1998. "Internet Protocol, Version 6 (IPv6) Specification." RFC 2460. <http://www.faqs.org/rfcs/rfc2460.html>.

Department of Defense (DoD). 2002a. "C-17 Advanced Quality System." ASC Engineering Fact Sheet. As obtained on November 8, 2002. <http://public.ascen.wpafb.af.mil/success/C-17_Advanced_QuaPlity_3_07_.pdf>.

Department of Defense (DoD). 2002b. "Defense Standardization Program Case Study: Mechanically Attached Pipe Fittings." As accessed on November 8, 2002. <http://www.dsp.dla.mil/documents/cases/pipefitting.pdf>.

Department of Defense (DoD). 2002c. "Year 2001 Defense Standardization Program Award Nomination." As accessed on November 8, 2002. <http://engineering.wpafb.af.mil/engstds/DSP_Award_Fletcher.pdf>.

Department of Defense (DoD). June 13, 2003. "Briefing on New Defense Department Internet Protocol." <http://www.dod.mil/cgi-bin/dlprint.cgi?http://www.dod.mil/transcripts/2003/tr20030613-0274.html>.

Dixon, R.V. 2003. "IPv6 in the Department of Defense." Presentation at the North American IPv6 Task Force Summit, San Diego State University, San Diego, CA, June 23-27.

Durand, A., and C. Huitema. 2001. "The Host-Density Ratio for Address Assignment Efficiency: An Update on the H Ratio." IETF Networking Working Group public document RFC 3194. Reston, VA: Internet Society.

Fact Index. <http://www.fact-index.com>.

Fang, Ying, and Anjana Susarla. January 2001. "Measuring the Internet Economy." Paper prepared by Cisco Systems and the University of Texas at Austin. <http://www.internetindicators.com/jan_2001.pdf>.

TheFreeDictionary .Com. <http://computer-dictionary.thefreedictionary.com>.

Hain, T. 2001. "Introduction to IPv6." Presentation under Cisco. <http://radio-1.ee.dal.ca/~ilow/emerg/lectures/otherfiles/2>.

Hinden, R. and S. Deering. 1998. "Internet Protocol, Version 6 (IPv6) Specification." Network Working Group.

Huston, Geoff. 2003. "IPv6 Address Lifetime Expectancy—2003." <http://www.apnic.net/community/presentations/docs/_ietf/200307/v4-lifetime-20030715.ppt>.

Hyperdictionary. <http://www.hyperdictionary.com/>.

InformationWeek. August 17, 1992. "Idle GOSIP." *Executive Digest*, pg. 50.

Internet Corporation for Assigned Names and Numbers (ICANN). "About ICANN." <http://www.icann.org/general/abouticann.htm>. Last updated on August 22, 2003.

The Internet Engineering Task Force (IETF). Request for Comments. <http://www.ietf.org/rfc.html>.

Internet Society (ISOC). 2000. "A Brief History of the Internet." <http://www.isoc.org/internet/history/brief.shtml#Introduction>.

Internet Society (ISOC). 2001. "IPv6 and the Future of the Internet." <http://www.isoc.org/briefings/001>.

Internet Society (ISOC). 2002. "All About the Internet Society." <http://www.isoc.org/isoc/>. Accessed on December 9, 2003.

Internet Society Publications. January 2003. "Waiting for IP version 6." <http://ispcolumn.isoc.org/2003-01/Waiting.html>.

IPv6 Promotion Council of Japan. February 29, 2004. <http://www.v6pc.jp/en/council/detail/index.html>.

IPv6 Style. March 28, 2003. "E! Agriculture Experiment in Gifu Prefecture." <http://www.ipv6style.jp/en/action/20030328/index.shtml>.

Jaffe, A.B. 1998. "The Importance of 'Spillovers' in the Policy Mission of the Advanced Technology Program." *Journal of Technology Transfer* 23:11-19.

Jones, Dan. 2002. "European IPv6 Plan Comes Under Fire." <http://www.unstrung.com/document.asp?doc_id=12812&print=true>.

Krane, J., and J. Seewer. August 25, 2003. "Overloaded Grid May Get High-Tech Solutions." *The Enquirer.* <http://www.enquirer.com/editions/2003/08/25/loc_wwwloc4blkout.html>.

Kurose, James E., and Keith W. Rose. 2001. *Computer Networking: A Top-Down Approach Featuring the Internet*. Boston: Addison Wesley.

Ladid, Latif. 2001. "IPv6: The New Internet." Presented at the International Telecommunications Union (ITU) Informal Forum Summit in Geneva, France, December 1-3.

Leyden, D.P., and A.N. Link. 1999. "Federal Laboratories as Research Partners." *International Journal of Industrial Organization* 17:572-592.

Lieberman, M.B., and D.B. Montgomery. 1988. "First-Mover Advantages." *Strategic Management Journal* 9:41-58.

Light Reading. "Who Wants Cereva?" <http://www.lightreading.com/document.asp?doc_id=12575>. As obtained October 2003.

Line56. June 4, 2003. "Wal-Mart's RFID Mandate." <www.line56.com/print/default.asp?ArticleID=4710>.

Link, A.N., and J.T. Scott. 1998. *Public Accountability: Evaluating Technology-based Institutions*. Norwell, Massachusetts: Kluwer Academic Publishers.

Link, A.N., and J.T. Scott. 2001. "Public/Private Partnerships: Stimulating Competition in a Dynamic Market." *International Journal of Industrial Organization* 19:763-794.

Litan, R.E., and A.M. Rivlin. 2001. "Projecting the Economic Impact of the Internet." *American Economic Review* 91(2):313-317.

Liu, John. June 24, 2003. "No shortage of IP addresses: IP registry head." CNET Asia <http://www.asia.cnet.com/newstech/systems/0,39001153,39137540,00.htm>.

Marsan, Carolyn D. 2000. "Stanford Move Rekindles 'Net Address Debate.'" NetworkWorldFusion. <http://www.nwfusion.com/news/2000/0124ipv4.html>.

Marshall, Alex (ed.). 2002. "State of World Population 2002." United Nations Population Fund.

Martin, S., and J.T. Scott. 1998. "Financing and Leveraging Public/Private Partnerships." Final report prepared for the working group on technology and innovation policy at OECD.

Martin, S., and J.T. Scott. 2000. "The Nature of Innovation Market Failure and the Design of Public Support for Private Innovation." *Research Policy* 29:437-447.

McKinsey & Company. October 2001. "U.S. Productivity Growth, 1995-2000." <http://www.mckinsey.com/knowledge/mgi/reports>.

Moos, Terry. October 20, 2003. "The Race is on as Cisco Systems and Renault Win Murai Award for Innovative Mobile IPv6 e-Vehicle." News@Cisco. Accessed on October 20, 2003. <http://newsroom.cisco.com/dlls/ts_102003.html>.

Moschovitis Group, The. 1999. "History of the Internet—Chapter 4: Because It's There: 1979 – 1984." <http://www.historyoftheinternet.com/chap4.html>.

National Institute of Standards and Technology (NIST). 1995. "Standards for Open Systems: More Flexibility for Federal Users." <www.itl.nist.gov/lab/bulletns/archives/b595.txt>.

Needle, David. "The Myth of the First Mover Advantage." <http://siliconvalley.internet.com/news/article.php/3541_333311>. Obtained April 22, 2004.

Nelson, R.R. 1959. "The Simple Economics of Basic Research." *Journal of Political Economy* 67:297-306.

NetworkWorldFusion. 2000. "Stanford Move Rekindles Net Address Debate." <http://www.nwfusion.com/news/2000/0124ipv4.html>.

NetworkWorldFusion. May 21, 2004. "China Agrees to Drop WAPI Standard." <http://www.nwfusion.com/news/2004/0421chinaagree.html>. Obtained May 30, 2004.

Nikkei Weekly, The. October 2, 2000. "Japan Pushes New Internet Protocol." 38(1947):9.

National Institute of Standards and Technology (NIST). October 2002. *Report on the Development of the Encryption Standard (AES)*. <http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf>.

National Institute of Standards and Technology (NIST). January 18, 2004. "Request for Comments on Deployment of Internet Protocol, Version 6." Submitted by National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) on behalf of the Department of Commerce (DoC). Docket No. 040107006-4006-01.

Office of Management and Budget. 1996. *Economic Analysis of Federal Regulations under Executive Order 12866*. Washington, DC: OMB.

Office of Science and Technology Policy. 1994. *Science in the National Interest*. Washington, DC: Executive Office of the President.

Office of Science and Technology Policy. 1998. *Science and Technology: Shaping the Twenty-first Century*. Washington, DC: Executive Office of the President.

PulseOnline. 2003. "China Promotes New Wireless Encryption Standard." 3(2) <http://pulse.tiaonline.org/article.cfm?id=1911>. Obtained on April 23, 2004.

Rahamim, Uri. December 12, 2002. "Perspective: IPv6, the Net's Next Frontier." CNET News.com. Accessed February 15, 2004. <http://news.com.com/2010-1069_3-976872.html>.

Roberts, Lawrence G. December 12, 2003. "QoS Signaling for IPv6 QoS Support." Submission has been formulated by Caspian Networks to assist the Telecommunications Industry Association (TIA) Standards Committee TR-34.

Shah, Agam. 2003. "IDC: U.S. IT Spending to Grow Slowly." <http://www.infoworld.com/article/03/04/29/HNitspend_1.html>.

Stanford Research Institute (SRI). 1997. "The Role of NSF's Support of Engineering in Enabling Technological Innovation—Section IV: The Internet." <http://www.sri.com/policy /stp/techin/inter1.html>. Last updated February 14, 1997.

Stenbit, John P. June 9, 2003. "Internet Protocol Version 6 (IPv6)." U.S. Department of Defense memorandum of intent. Washington, DC: U.S. Department of Defense.

Stiglitz, J.D. 1988. *Economics of the Public Sector*. New York: W.W. Norton & Company.

Streck, John, Centaur Labs. Personal communication with Brent Rowe and Mike Gallaher, RTI International. March 2004.

Stoneman, P. 2002. *The Economics of Technological Diffusion.* Malden, MA: Blackwell Publishers Ltd.

Tassey, Gregory. 1996. "Choosing Government R&D Policies: Tax Incentives versus Direct Funding." *Review of Industrial Organization* 11(5): 579-600.

Tassey, G. 1997. *The Economics of R&D Policy*. Westport, CT: Quorum Books.

Tassey, G. 2000. "Standardization in Technology-Based Markets." *Research Policy*, 29(4):587-602.

Teece, D.J. 1980. "Economies of Scope and the Scope of the Enterprise." *Journal of Economic Behavior and Organization* 1:223-247.

Tellis, G.J., and P.N. Golder. 1996. "First to Market, First to Fail? Real Causes of Enduring Market Leadership." *Lone Management Review* Winter:65-75.

Thompson, Geoff. 2001. "FCC Folks Should Now Be Able to Pay Their Own Way." <https://grouper.ieee.org/groups/802/secmail/msg01843.html>. As obtained on November 8, 2002.

U.S. Department of Labor, Bureau of Labor Statistics (BLS). 2003. "2001 National Occupational Employment and Wage Estimates." <http://www.bls.gov/oes/2001/oes151071.htm>. As obtained on December 8, 2003.

Van Huyck, J.B., R.C. Battalio, and R.O. Beil, 1990. "Tacit Coordination Games, Strategic Uncertainty, and Coordination Failure." *American Economic Review*, 80(1):234-248.

Van Huyck, J.B., R.C. Battalio, and R.O. Beil. 1991. "Strategic Uncertainty, Equilibrium Selection Principles, and Coordination Failure in Average Option Games." The *Quarterly Journal of Economics* 106(3):885-911.

Webopedia. <http://www.pcwebopedia.com/>.

Wessel, Harry. July 27, 2003. "Instant Messaging Making its Mark at Work." *The Orlando Sentinel*.

Zaracostas, J. December 8, 2003. "U.N. Control of Web Rejected." <http://www.washtimes.com/world/20031208-125717-6682r.htm>.