Could IPv6 Improve Network Security? And, If So, at What Cost?

BRENT ROWE AND MICHAEL GALLAHER[*]

ABSTRACT

Industry stakeholders and Internet experts generally agree that IPv6-based networks in many ways would be technically superior to IPv4-based networks. The redesigned header structure in IPv6, including new flow labels, and the enhanced capabilities of the new protocol could provide significant security benefits to Internet users, network administrators, and applications developers. However, there is disagreement about the characteristics and timing of the potential security benefits associated with IPv6. Some experts believe that widespread IPv6 adoption could spur increased research and development of and interest in transitioning to a new network security model, in which techniques such as Internet Protocol Security (IPSec) could be more commonly and effectively used. However, the costs of a transition to IPv6 could be substantial, and the benefits are still rather speculative. Further, there is uncertainty about whether and to what extent IPv6 adoption will occur. This paper investigates the question of whether IPv6 could help improve computer network security and, if so, at what cost. Based on a study conducted for the Department of Commerce IPv6 Task Force, our paper provides a qualitative assessment of the potential security effects of a transition to IPv6, as well as a quantitative analysis of the likely costs of IPv6 adoption to be borne by users, Internet service providers, and vendors in the United States. The results of our analysis should be useful to both industry and government in decisions related to investments in network security and IPv6.

Designed almost 10 years ago, Internet Protocol version 6 (IPv6) has slowly been integrated into most major networking hardware and software sold today. Cameras, cell phones, and refrigerators are beginning to be equipped with IPv6 addresses in an effort by vendors to use the characteristics of IP, while realizing the limits of IPv4. Today, the majority of routers sold are IPv6 capable, and in two to three years, most operating systems and application software on the market will be IPv6 capable (in 2004, Sony successfully integrated

[*] Brent Rowe is economist at RTI International. He also serves as corresponding member of IEEE USA's Committee on Communication and Information Policy.

IPv6 addresses into all of its Internet-capable products). Assuming demand for IPv6-based applications increases and users begin to enable IPv6 in consumer products and corporate networks, this paper investigates whether networking security could be improved and, if so, at what cost.

Industry stakeholders and Internet experts generally agree that IPv6-based networks, in many ways, would be technically superior to IPv4-based networks. The increased address space available under IPv6 could stimulate development and deployment of new communications devices and new applications. It also could enable network restructuring to a more hierarchical structure, possibly without Network Address Translation (NATs), to occur more easily. The redesigned header structure in IPv6 (which includes new flow labels) and the enhanced capabilities of the new protocol could provide significant security benefits to Internet users, network administrators, and applications developers.

However, the timing of significant U.S. IPv6 adoption is very speculative. Currently, the installed base of network-based vendor and propriety products (hardware and software), as well as networking IT staff skills and organizational procedures and policies are all rooted in IPv4 characteristics and capabilities. As such, our interviews have indicated that many people will likely continue to use IPv4 for many years to come. Further, some security experts and researchers propose that an entirely new communications infrastructure should be developed, possibly without the use of the Internet protocol (IP). The National Science Foundation (NSF) is sponsoring an initiative called the Global Environment for Networking Investigations (GENI) aimed at researching such possibilities and could spend as much as $300 million over the next several years.[1] Some suggest that organizations should not incur costs to move to IPv6 but, rather, should wait to transition to an entirely new communications infrastructure.

As organizations weigh these broad considerations, it is also important to note that there is disagreement among security experts

[1] Currently, the GENI initiative is in the early stages, but it is anticipated that it will include both a research grant program and a experimentation facility designed for exploratory research and testing. NSF managers and others note that open-ended research aimed at identifying a completely new, more secure and useable networking infrastructure is ongoing currently, but that the NSF initiative, which seeks to involve other government agencies, as well as the private sector and other countries, will greatly increase the funding available for and interest in such research (Markoff 2005). More Information on the GENI Initiative can be found at NSF's Web site at http://www.nsf.gov/cise/geni/.

about the characteristics and timing of security benefits associated with IPv6. Some experts believe that IPv6 could spur increased research and development (R&D) of and interest in transitioning to a new network security model, in which techniques such as Internet Protocol Security (IPsec)[2] could be more commonly and effectively used. However, many of IPv6's enhanced capabilities have also been made available in IPv4, albeit with varying levels of performance. As a result, vendors and consumers may continue to use IPv4 for a significant 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 "middleboxes," such as NAT devices and firewalls, 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.

Further, widespread adoption of IPv6 will likely entail substantial transition costs because today's Internet comprises almost entirely IPv4-based hardware and software. We estimate the cost for all major U.S. stakeholders to transition to IPv6 during the period beginning in 1997 through 2025 to be approximately $25 billion. In addition to the explicit cost to transition, many experts have noted that using IPv6 networking could result in decreased network security for a certain period during which network operators become more familiar with the new protocol and hackers identify flaws in initial IPv6 implementations.

[2] IPsec is a set of protocols developed by the Internet Engineering Task Force (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 two 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 that are used to provide encryption and integrity protection. This is accomplished through a protocol known as Internet Key Exchange (IKE), which also allows hosts to mutually authenticate using digital certificates or other methods and negotiates the IPsec protections to be provided and the cryptographic algorithms to be used.

As part of a study performed for the Department of Commerce (DoC) IPv6 Task Force,[3] this paper's authors conducted extensive research, including more than sixty interviews with stakeholders,[4] performed a quantitative cost analysis of the development and deployment of IPv6 based on information gathered through interviews and secondary data sources; and developed a qualitative analysis of future benefits, using selected information from available resources.[5] This paper focuses on the potential security effects of IPv6 and the likely costs for the United States to transition to IPv6.

I. SECURITY IMPLICATIONS OF IPV6

Although the general consensus is that widespread IPv6 adoption could result in significant benefits to IT security, among other network performance improvements, significant disagreement exists concerning the size of these benefits and whether the incremental costs of IPv6 (versus IPv4) for some or all users would outweigh the costs of an accelerated transition from IPv4 to IPv6.[6]

[3] The National Institute of Standards and Technology (NIST) commissioned RTI International (RTI) to conduct an economic analysis of the costs and benefits of IPv6, entitled "IPv6 Economic Impact Assessment" (2005), which can be accessed at http://www.nist.gov/director/prog-ofc/report05-2.pdf. Further, the Department of Commerce IPv6 Task Force, co-chaired by NIST and the National Telecommunications and Information Administration (NTIA), released in January 2006 their "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" with which RTI assisted; it can be accessed at http://www.nist.gov/director/prog-ofc/IPv6-final.pdf. Much of the discussion in this report is based on information collected as part of research for these two studies.

[4] Throughout this paper, "stakeholders" refers to all major groups that have a role in (or have extensive knowledge of the implications of) transitioning the U.S. networking infrastructure to IPv6. Major groups included are infrastructure vendors; applications vendors; Internet service providers (ISPs); corporate, government, and institutional users; and other technical experts. Appendix 1 provides a list of some of the organizations and individuals who participated in our interviews.

[5] The information presented throughout this report is further supported by commenters to the DoC Request for Comments (RFC) (DoC, NIST and NTIA) announced in January 2004, our information discussions with industry stakeholders and experts, available literature, and participants at the July 28, 2004, DoC public meeting on IPv6 (DoC, NIST).

[6] The timing of the transition from IPv4 to IPv6 for any particular adopter, as well as the existing network infrastructure, could dramatically affect the costs incurred and the benefits realized.

Many experts and industry representatives contend that IPv6 would provide a greater level of security than is available under IPv4. NTT/Verio, a U.S. Internet service provider,[7] states that because IPv6 was "designed with security in mind," it is inherently more secure than IPv4, which does not have integrated security fields (DoC, NIST, and NTIA 2004).[8] Other industry representatives note that support for IPsec is "mandatory" in IPv6, but only "optional" in IPv4, which should lead to more extensive use of IPsec in IPv6 networks and applications (DoC, NIST, and NTIA 2004).[9] BellSouth suggests that incorporating IPsec into the IPv6 protocol stack may reduce incompatibility between different vendors' implementations of IPsec (DoC, NIST and NTIA, 2004).[10] Further, the massive increase in addresses made possible via IPv6 may enhance security by making it difficult for "hackers" to identify and attack IP addresses by performing exhaustive address and port sweeps (DoC, NIST, and NTIA 2004).[11]

Widespread deployment of IPv6 may indeed produce security benefits in the long term; however, the near-term benefits are much less clear. Although IPsec *support* is mandatory in IPv6, IPsec *use* is not. In fact, many current IPv6 implementations do not include IPsec (DoC, NIST, and NTIA 2004).[12] Although most parties believe that increased use of IPsec would improve security, others are less certain. Motorola asserts that IPsec, in its current form, cannot defend against denial-of-service attacks (DoC, NIST, and NTIA 2004).[13] BellSouth

[7] NTT/Verio was the first U.S. ISP to offer IPv6 service (Marsan 2004).

[8] See NTT/Verio comments at 13 in Notice of Inquiry–Comments Received (DoC, NIST, and NTIA 2004) [hereinafter "Comments at X"]. Microsoft commenters also stated that IPv6 is a "new, more secure protocol" that could help make North America a "Safe Cyber Zone" (DoC, NIST, and NTIA 2004). See Ref. 10, Microsoft comments at 11.

[9] See, for example, Ref. 10, Cisco comments at 3; Ref. 10, GSA comments at 6; Ref. 10, MCI comments at 4.

[10] Ref. 10, BellSouth comments at 3.

[11] See Ref. 10, Cisco comments at 3.

[12] See, for example, Ref. 10, Alcatel comments at 4; Ref. 10, BellSouth comments at 3; Ref. 10, Cisco comments at 3, 17; Ref. 10, Internet2 comments at 3; Ref. 10, VeriSign comments at 9.

[13] Ref. 10, Motorola comments at 4.

questions whether IPsec can strictly eliminate "spoofing" (DoC, NIST, and NTIA 2004).[14] 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 (DoC, NIST, and NTIA 2004).[15] Other commenters note that IPsec provides only network-level security and, as a result, may need to be supplemented by other measures (DoC, NIST, and NTIA 2004).[16]

On the other hand, although optional, IPsec is being widely deployed in IPv4 (DoC, NIST, and NTIA 2004).[17] Several stakeholders have stated that there are no significant functional differences in the performance of IPsec in IPv6 and IPv4 networks (DoC, NIST, and NTIA 2004).[18] Any differences in performance are attributable to the presence of NATs in most IPv4 networks, which interfere with E2E communications using IPsec (DoC, NIST, and NTIA 2004).[19] Thus, to the extent that NATs persist in IPv6 networks, they may reduce the security benefits available via the new protocol.[20]

[14] Ref. 10, BellSouth comments at 4.

[15] Ref. 10, VeriSign comments at 2.

[16] See Ref. 10, Alcatel comments at 3 (need to secure critical subsystems such as neighbor discovery and routing); Ref. 10, Electronic Privacy Information Center (EPIC) comments at 2 (need to secure applications).

[17] See Ref. 10, Qwest Communications International Inc. (Qwest) comments at 4; VeriSign comments at 2.

[18] See Ref. 10, BellSouth comments at 3; Ref. 10, Cisco comments at 3; Ref. 10, Internet2 comments at 3.

[19] See Ref. 10, Internet2 comments at 3; Ref. 10, MCI comments at 5. Cisco asserts that work-arounds are becoming available that will permit E2E IPsec even across NATs. Ref. 10, Cisco comments at 3.

[20] Some commenters suggested that removing NATs to implement IPsec fully may reduce security for some users (DoC, NIST, and NTIA 2004). Other commenters suggested that deploying IPv6 may be hindered by the absence of IPv6-compatible security "tools" (e.g., firewalls, intrusion detection systems). Development and deployment of such tools, like the continued use of NATs, may interfere with E2E communications using IPsec (DoC, NIST 2004). Some commenters suggest that the removal of NATs to implement IPsec fully may reduce security for some users. See, e.g., Ref. 10, Motorola comments at 3.

Furthermore, experts generally agree that implementing any new protocol, such as IPv6, would be followed by an initial period of increased security vulnerability[21] and that additional network staff will be necessary to address new threats posed by a dual network environment (DoC, NIST, and NTIA 2004).[22] Current IPv4 users benefit from twenty years of effort spent 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 should help bring security levels in IPv6 networks up to the level of current IPv4 networks fairly rapidly (DoC, NIST, and NTIA 2004).[23]

A. Reevaluating the Security Model

To use fully the capabilities of IPv6 and IPsec to provide security on an E2E basis, enterprises would likely need to reexamine their existing security models (DoC, NIST 2004).[24] Most enterprises currently implement security measures at the perimeter of their corporate networks (e.g., with firewalls). By so doing, they can monitor and control outside access to hosts within the corporate network at a limited number of points, much as the rulers of a medieval city could control the flow of people in and out at a few gates cut into the city's walls. In that way, the enterprises can provide a desired level of security for their networks and their users at a reasonable cost in terms of equipment and personnel.

[21] Tassey, Gallaher, and Rowe (2006) provide a discussion of the public goods nature of complex standards such as IPv6 and the myriad of substandards that must be in place (and agreed on) to support a standard such as IPv6. The public goods nature of standards is related to the issue of decreased short-term security because without enough investment to ensure a certain minimum level of security risk associated with the move to IPv6, many organizations will wait to transition indefinitely. Private firms individually are not motivated to incur substantial costs for such infrastructure development and testing; therefore, they must rely on organizations such as the IETF and government agencies such as NIST.

[22] See Ref. 10, Cisco comments at 14; Ref. 10, Network Conceptions comments at 9.

[23] See Ref. 10, Internet Security Alliance (ISA) comments at 2.

[24] See, for example, Public Hearing Transcript, supra note 41, at 59 (remarks of Latif Ladid, NAV6TF), 149-151 (remarks of Preston Marshall, DARPA).

If an enterprise allows its employees to establish communications with nonenterprise users on an E2E basis, the enterprise is forced to use other security techniques. For example, the entire organization could adopt an E2E security approach instead of the traditional perimeter security model. Alternatively, the enterprise could retain its perimeter approach but open "holes" in that perimeter for certain communications (e.g., teleconferencing) or for certain employees. In either event, the enterprise would need to plan carefully to ensure that the new security model does not expose the enterprise to new external threats. Many enterprises may be reluctant to assume that risk, particularly when the benefits cannot be guaranteed.[25]

Implementation of E2E security might require developing new tools and policies. The principal impediment to widespread use of IPsec, for example, appears to be the absence of a public key infrastructure (PKI) and associated trust models, which are both necessary to effectively manage widespread IPsec operations (DoC, NIST, and NTIA 2004).[26] Extensive research must be conducted, and an organizational authority (trusted by all users) will need to be set up to manage the PKI system. Until the required security infrastructure is created and all privacy concerns and legal considerations are resolved (DoC, NIST, and NTIA 2004)[27], a process that could take several years, IPv6 is not likely to stimulate any more use of IPsec than IPv4 does today (DoC, NIST, and NTIA 2004).[28]

In summary, it is likely that in the short term (i.e., the first three to five years of significant IPv6 use) 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 would probably be found in IPv6 than in IPv4, and IPv4 networks would continue to have, at a maximum, the same level of security issues as they do

[25] It is difficult to implement a perimeter security model for a network with mobile users because, in a mobile environment, there may be no "perimeter" to defend. Thus, as more employees use mobile communications devices (e.g., phones, laptops, and PDAs), more enterprises will be compelled to develop alternatives to perimeter security, including E2E approaches (DoC, NIST, and NTIA 2004). See Public Hearing Transcript, supra note 41, at 156-157 (remarks of Preston Marshall, DARPA).

[26] See Ref. 10, BellSouth comments at 3; Ref. 10, Cisco comments at 3; Ref. 10, Hain comments at 4; Ref. 10, NAv6TF comments at 9; Ref. 10, NTT/Verio comments at 15.

[27] See Ref. 10, BellSouth comments at 4.

[28] See Ref. 10, BellSouth Comments at 3-4.

currently. In the long term (i.e., fifteen to twenty years), however, security may improve if organizations are motivated to restructure their networks and use E2E security mechanisms, such as IPSec.[29]

II. IPv6 Transition Costs

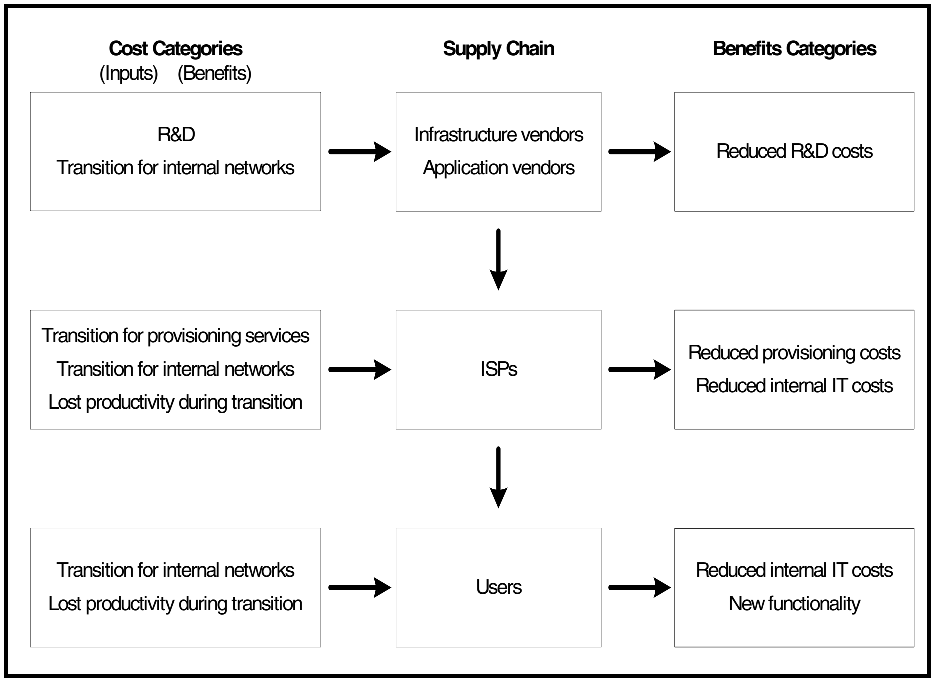
Potential IPv6 development and deployment scenarios and cost estimates were created using information provided in the thirty formal stakeholder interviews we conducted. We estimate the present value (PV) of incremental costs associated with IPv6 deployment over a twenty-five-year period to be approximately $25 billion ($2003),[30] primarily reflecting the increased labor costs associated with the transition. Although these cost estimates seem large, they are actually quite small relative to the overall expected expenditures on IT hardware and software. They are even smaller relative to the expected value of potential market applications that could result from IPv6 use and significant network improvements, including enhanced security.

Figure 1 provides the general framework used to identify stakeholder groups that will incur costs and realize benefits associated with the transition from IPv4 to IPv6. For the purposes of this study, the supply chain is segmented into four major stakeholder groups:

[29] According to Gallaher and Rowe (forthcoming), approximately three-fourths of organizations (ISPs, users, and vendors) participating in interviews indicated that they believe the government should have some role in the transition to IPv6 for both government and nongovernment organizations. See Gallaher and Rowe (forthcoming) for a more detailed discussion of the potential roles that government could play and the views of industry.

[30] All cost and benefit estimates are presented in 2003 dollars (hereinafter $2003).

FIGURE 1: SUPPLY CHAIN STAKEHOLDERS, COSTS, AND BENEFITS


Cost Categories
(Inputs) (Benefits)
Supply Chain
Benefits Categories
R&D
Transition for internal networks
Infrastructure vendors
Application vendors
Reduced R&D costs
Transition for provisioning services
Transition for internal networks
Lost productivity during transition
ISPs
Reduced provisioning costs
Reduced internal IT costs
Transition for internal networks
Lost productivity during transition
Users
Reduced internal IT costs
New functionality

- infrastructure vendors,
- application vendors,
- ISPs, and
- Internet users (e.g., infrastructure, corporate, government, institutional, and independent/home).

Infrastructure vendors include manufacturers of computer networking hardware (e.g., routers, firewalls, and servers) and systems software (e.g., operating system) that supply the components of computer networks. Major companies in this category include Microsoft, IBM, Juniper, Cisco, and Hewlett Packard.

Application vendors include suppliers of e-mail, file transfer protocol (FTP) and Web server software, and database software, such as enterprise resource planning (ERP) and product data management

(PDM) software. SAP and Oracle (which recently merged with PeopleSoft) are some of the largest companies in this group.

ISPs are companies that provide Internet connectivity to customers. National backbone ISPs (e.g., MCI, AT&T, and Sprint) provide connectivity to larger companies, some institutional users, and national and regional ISPs (e.g., AOL and Earthlink) that provide Internet connectivity to home and small business users.

Internet users represent a large, diverse group of entities ranging from corporate, institutional, and government organizations to independent users, including small businesses and residential households. A subset of this stakeholder group is infrastructure users, companies that use the Internet to provide products and services to customers. Mobile telephone service providers and services such as OnStar are examples of these companies.

We interviewed a group of thirty individuals representing each stakeholder group. In these interviews, we asked questions related to the timing of available IPv6 infrastructure components and applications and the likely adoption rates and costs for each stakeholder group. The information gathered informed the estimates presented below.

A. General Cost Categories

Labor resources will account for the bulk of the transition costs associated with IPv6. Although some additional physical resources may be needed, such as increased memory capacity for routers and other message-forwarding hardware,[31] these expenses are treated as negligible in our cost analysis because interview participants indicated that they were quite small compared to the labor resources required.

Labor resources needed to transition to IPv6 are linked to three general business activities within the internet supply chain—product development, internet provisioning services, and internal network

[31] Motorola notes that routers would need at least four times their current content addressable memory to operate as efficiently as they do today when accessing both IPv4 and IPv6 addresses in a dual-stake environment. Further expanded buffers and routing tables would need more memory (DoC, NIST, and NTIA 2004). See Ref. 10, Motorola comments at 6. Motorola notes that routers would need at least four times their current content addressable memory to operate as efficiently as they do today when accessing both IPv4 and IPv6 addresses in a dual-stake environment. Further expanded buffers and routing tables would need more memory. Also see Ref. 10, Alcatel comments at 4.

operations. Product development activities are conducted by infrastructure and application vendors; service provisioning activities are conducted by ISPs; and internal network operations are conducted by all vendors, ISPs, and users.

Table 1 shows the underlying transition cost categories included in each of the business activities. As is apparent, ISPs and users would incur costs in the same categories. Additionally, several other cost categories, such as network testing and standards and protocol development, span multiple business activities and, thus, several stakeholder groups.

TABLE 1: COST CATEGORIES BY BUSINESS ACTIVITY

Business Activity	**Product Development**	**Provisioning Services**	**Internal Network Operations**	**Brief Description**
Affected stakeholders	Vendors	ISPs	Vendors, ISPs, and users	
Cost categories				
R&D	●			Labor allocated to basic product design and development (e.g., coding or prototyping)
Product testing	●	●		Labor allocated to testing product interoperability, debugging, etc.
R&D staff training	●			Labor and training class expenses for R&D staff
Standards and protocol activities	●	●	●	Labor allocated to developing internal standards for company products
Network management software (upgrade)[a]		●	●	Labor allocated to network-specific management and monitoring software
Network testing		●	●	Labor allocated to testing interoperability between network components with IP capabilities
Installation effort		●	●	Labor allocated to installing IPv6 transition mechanisms
Maintaining network performance		●	●	Labor allocated to maintaining transition mechanisms, such as dual stack, and ensuring high network performance
Training (sales, marketing, and technical staff)	●	●	●	Labor and training class expenses for sales, marketing

[a] This category is intended to include the costs of upgrades to any network management tools, assuming that these costs result from the need to transition to IPv6 network management tools.

B. BASELINE IPV6 PENETRATION ESTIMATES

Based on information from interview participants, we estimated IPv6 penetration curves for the four major stakeholder groups. The penetration curves were used to develop the base case cost estimates, by year, presented in Section II.C.1.

1. STAKEHOLDER PENETRATION CURVES

The penetration curves presented in Figure 2 reflect cumulative IPv6 transition activities over time. The curves are dependent on each other in that hardware and software must be available prior to ISPs transitioning networks to support IPv6 users. The four curves in Figure 2 also represent different adoption activities for each of the four major industry stakeholder groups. The first two curves represent when IPv6 products and services will be *capable*, and the final two curves represent when components of the system will be *enabled*.[32] More specifically, the four curves can be interpreted as follows:

- By 2003, the average infrastructure (Inf) vendor will have integrated IPv6 capabilities into 30% of the routers and network products it offers.

- By 2008, the average application (App) vendor will have integrated IPv6 capabilities into 30% of the software it offers that uses network features.

- By 2010, the average ISP will have enabled 30% of its network to manage IPv6 transmissions.

- By 2012, the average user will have enabled 30% of its local network to handle IPv6 communications.

[32] Hardware and software become capable when the IPv6 functionality is integrated into products and purchased by organizations. According to Nortel Networks, IPv6-capable products were sold as early as 1997 (Shaikh 2005). However, even after the necessary networking components are IPv6 capable, they will need to be enabled (turned on) to support IPv6 communications.

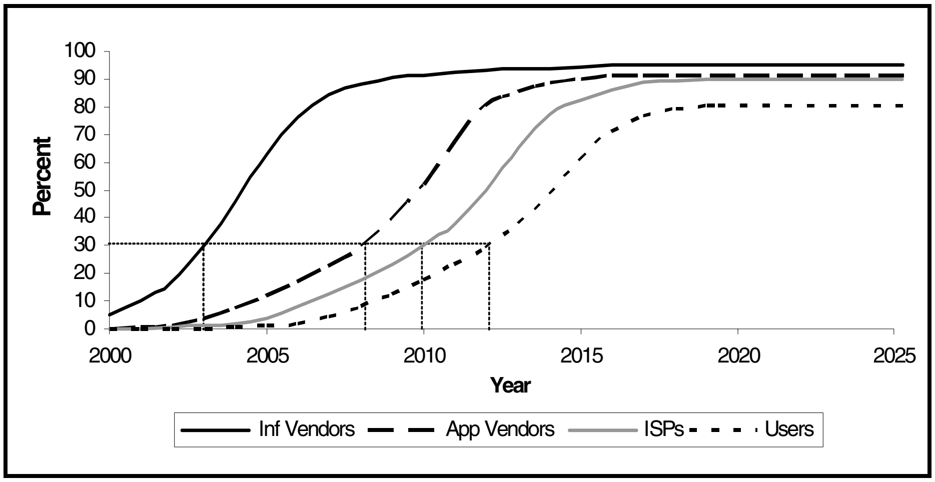
The penetration curves were developed based on interviews to reflect the likely distribution of IPv6 transition activity and hence provide the basis for estimating the time line of costs. Vendors were asked when they would have IPv6 products available, which provided information on the timing of their R&D activities. ISPs were asked when they expected to offer IPv6 services, indicating the timing of their enabling activities. Similarly, users were asked when they would enable parts of their system, also indicating enabling activities.

Participating stakeholders agree that IPv6 adoption rates will differ significantly across and within individual companies. For example, users in the financial, telecommunications, and defense sectors will likely be more aggressive in transitioning to IPv6 compared to other sectors that manage less-sensitive information. Also, within a company, certain divisions or business operations will transition before others.

The average penetration estimates presented in the curves in Figure 2 capture both differences in adoption rates across companies and the gradual adoption process within companies.[33]

[33] Note that the penetration curves should neither be interpreted as the percentage of companies that have transitioned to IPv6 nor as the volume of IPv6 traffic. For example, we project, based on information from participating stakeholders, that most ISPs will be offering some level of IPv6 service in the near future by enabling a limited portion of their network; however, it could take several more years for all internal or provisioning networks to be completely IPv6 enabled.

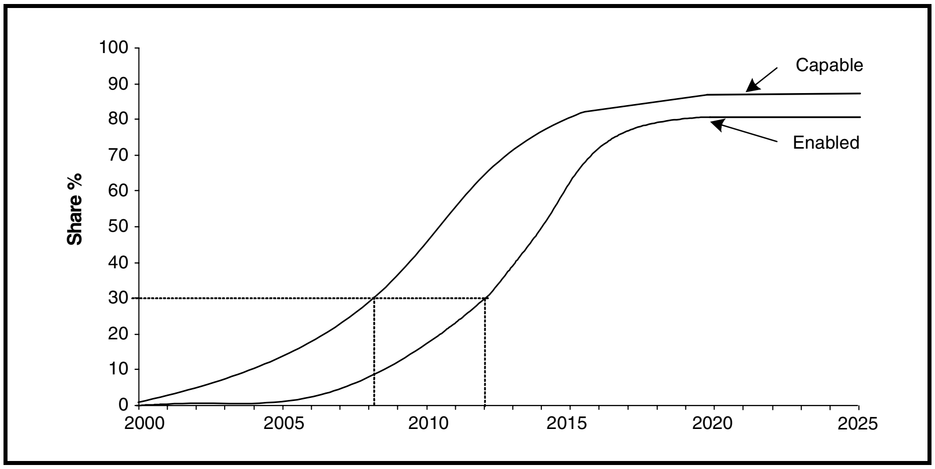
FIGURE 2: PENETRATION ESTIMATES OF IPV6 IN THE UNITED STATES



2. USERS' CAPABILITIES AND ENABLING CURVES

We asked stakeholders participating in interviews to identify the time by which users will have IPv6 capabilities and, subsequently, when they would probably enable IPv6. Figure 3 presents users' capable and enabled penetration curves and illustrates the lag between when users obtain IPv6 capabilities through product replacement/upgrades and the time at which they decide to enable these products. The enabled curve in Figure 3 is the same as the users' enabled curve in Figure 2.

FIGURE 3: IPV6-CAPABLE AND IPV6-ENABLED U.S. USER NETWORKS



Users will acquire IPv6 capabilities primarily as part of routine hardware and software upgrades. For example, we project that 30% of users' systems will be IPv6 compatible by 2008. Nearly all edge routers[34] being sold today are IPv6 capable, either in hardware or software, according to participating stakeholders. Large organizations, which routinely upgrade their networking components, should have IPv6 capabilities in the next five to seven years. However, medium and small businesses and independent users will likely not upgrade in significant numbers for several more years.

On average, we estimate that IPv6 hardware and software will be enabled approximately five years after users receive IPv6 capabilities. For example, we project that users will have enabled 30% of their systems by 2012. As initial operating systems and routers become enabled and early adopters provide "lessons learned," IPv6 adoption

[34] By edge routers, we mean the majority of routers used by enterprise users. This does not include larger backbone routers used by ISPs and large enterprises.

activities will likely accelerate as users begin to transition a significant share of their applications.[35]

C. BREAKDOWN OF COSTS

Based on the penetration projections and methodology described above, we estimate that expenditures for U.S. stakeholder groups to transition to IPv6 will be approximately $73 billion over the period 1997 to 2025.[36] These transition costs equate to a PV, discounted to 1997, of $25 billion ($2003). The year 1997 is used as the base year because it is the year in which IPv6 costs were first incurred. From this point forward, all costs are in $2003 and are discussed in PV terms, referenced to 1997.

Table 2 provides estimated annual transition costs broken down by stakeholder group. Government and nongovernment users account for approximately $23 billion of total U.S. IPv6 development and deployment costs (about 91%) with nongovernment users representing the large majority, $22 billion of the U.S. total (85%).[37] The remaining costs are associated with total vendors, $2 billion (7%), and total ISPs, $136 million (0.5%).

For infrastructure and application vendors, Table 2 breaks out costs into additional R&D costs necessary to integrate IPv6 into products ($1,855 million in PV 2003 dollars) and additional IT costs to transition internal company networks to IPv6 ($121 million). For ISPs, costs are broken into additional IT costs to transition service

[35] It is important to note, as mentioned previously, that many assumptions had to be made to perform this analysis (e.g., IPv6 demand will increase and IP will remain the communications medium of choice). We relied on interviews with industry experts and a variety of stakeholders representing all affected groups, so our transition timing and cost projections are intended to provide informed estimates to assist network operators and policy makers considering the impact of IPv6 adoption and its likely timing.

[36] These years were selected because our analyses used "adoption" rates beginning with some infrastructure vendors in 2000, continuing until 2020. Thus, we estimated costs both before and after enablement/integration of IPv6.

[37] We calculated all stakeholder cost estimates based on aggregated data provided by stakeholders in the interview phase. As such, we estimate government user costs will be approximately $1.7 billion, and nongovernment user costs will be approximately $21.6 billion. The sum is $23.2 billion. This amount is 92% of the estimated total cost to all stakeholders.

provisioning networks[38] to IPv6 ($121 million) and additional IT costs to transition internal company networks to IPv6 ($15 million).

1. COST CATEGORIES AND SUPPLEMENTAL DATA

This cost analysis focuses on valuing the labor activities associated with the transition from IPv4 to IPv6. Over the next four or five years, the vast majority of network hardware, operating systems, and network-enabled software packages (e.g., databases, e-mail) are likely to be sold with IPv6 capabilities. Based on information provided by participating stakeholders, we predict that IPv6 capabilities will penetrate the hardware and systems software markets and become integrated into ISP and user networks in an additional two to three years as part of routine upgrade cycles with little to no increase in product price (marginal cost) to ISPs and users.[39] Thus, our analysis assumes that hardware and software costs to upgrade to IPv6 will be negligible for most Internet users (i.e., the upgrade costs will be no different than routine annual upgrade costs without IPv6) and that labor costs will constitute the majority of the cost of upgrading to IPv6 for users.

Labor costs for ISPs and users were estimated by determining the share of IT staff resources needed to facilitate the transition to IPv6 and applying this share to the total population of IT staff involved in Internet activities. We asked interview participants to estimate the percentage of staff time required for enabling IPv6. U.S. Bureau of Labor Statistics (BLS) employment figures were used to determine the number of ISP and user IT staff supporting Internet activities.

Wage data for each occupational category were also obtained from BLS. A single aggregate IT staff wage rate was calculated by weighting the category wage by the number of employees in each

[38] "Provisioning networks," as discussed in this paper, are defined as ISP subnetworks responsible for providing connectivity to the Internet to customers. These networks are always separate from internal networks used by employees.

[39] The exception is that for ISPs and large enterprises the transition of some networking pieces to IPv6 may require additional hardware and software costs. For example, additional memory will be needed in forwarding hardware pieces to continue current network performance given the larger size (128 bits vs. 32 bits in IPv4) of IPv6 addresses. Additionally, mainframes and billing systems might need hardware or software upgrades ahead of routine upgrades, which occur very infrequently for these devices, depending on the specific needs of a network (DoC, NIST, and NTIA 2004). See Motorola comments at 6; Alcatel comments at 4.

category. The average IT staff wage ($2003) is estimated to be approximately $68 per hour.

BLS occupational categories are not available for infrastructure and application vendors staff engaged in product R&D, even though R&D expenditures are predominantly labor costs. Thus, for infrastructure and application vendors, IPv6 transition costs were calculated as a share of R&D expenditures. The share and timing of R&D expenditures were estimated based on the interviews. Annual R&D expenditures for Internet infrastructure and application venders were obtained from the National Science Foundation (NSF) (2002).[40]

Table 2: Estimated U.S. IPv6 Adoption Cost Totals, Broken Out by Each Stakeholder Group ($ Millions)

Year	Infrastructure Vendors		Application Vendors		Total Vendors
	R&D	Internal	R&D	Internal	
1997	17.7	0.0	0.0	0.0	17.7
1998	47.3	0.0	0.5	0.0	47.8
1999	88.6	0.0	2.1	0.0	90.7
2000	160.9	0.0	9.1	0.0	170.1
2001	234.8	0.2	21.9	0.0	256.9
2002	302.7	0.7	35.3	0.2	338.9
2003	329.3	1.5	49.1	0.3	380.2
2004	295.3	2.8	58.4	0.6	357.2
2005	223.0	5.5	71.3	1.2	301.0
2006	143.2	8.8	87.4	1.9	241.3
2007	79.7	11.7	100.4	2.6	194.5
2008	44.3	14.4	142.6	3.2	204.6
2009	25.8	16.8	169.6	3.7	216.0
2010	19.2	19.9	203.1	4.4	246.6
2011	16.2	25.0	171.2	5.5	218.0
2012	14.0	31.1	86.3	6.9	138.3
2013	10.3	35.1	48.0	7.8	101.2
2014	5.2	34.5	23.1	7.6	70.3
2015	2.2	27.8	4.5	6.1	40.6
2016	0.0	20.0	1.0	4.4	25.4

[40] To proxy for R&D expenditures, we used NSF data. For Internet infrastructure and application vendors, we used a combination of R&D figures for Software Publishing, Computer and Peripheral Equipment, and Other Computer and Electronic Products. See Table E-2 in NSF's report entitled "Research and Development in Industry: 2000."

2017	0.0	14.1	0.0	3.1	17.2
2018	0.0	9.5	0.0	2.1	11.6
2019	0.0	5.9	0.0	1.3	7.2
2020	0.0	3.6	0.0	0.8	4.4
2021	0.0	2.0	0.0	0.4	2.5
2022	0.0	0.9	0.0	0.2	1.1
2023	0.0	0.4	0.0	0.1	0.5
2024	0.0	0.2	0.0	0.0	0.2
2025	0.0	0.0	0.0	0.0	0.0
Total	2,059.8	292.6	1,284.8	64.7	3.701.9
Present Value (2003)	1,284.8	99.3	571.0	21.9	1,977.0

Year	ISPs		Total ISPs	Govt. Users	Non-govt. Users[a]	Grand Total
	Pro-vision	Internal				
1997	0.0	0.0	0.0	0.0	0.0	17.7
1998	0.0	0.0	0.0	0.0	0.0	47.8
1999	0.1	0.0	0.1	0.0	0.0	90.8
2000	0.6	0.0	0.6	0.3	3.7	174.7
2001	1.5	0.0	1.5	3.5	45.5	307.5
2002	2.4	0.1	2.5	12.6	162.3	516.4
2003	4.7	0.2	5.0	25.7	330.5	741.4
2004	8.3	0.4	8.7	47.6	610.9	1,024.3
2005	12.5	0.8	13.3	92.6	1,189.4	1,596.2
2006	14.9	1.3	16.2	148.3	1,905.2	2,311.0
2007	17.5	1.7	19.2	198.9	2,554.6	2,967.1
2008	20.3	2.1	22.4	244.8	3,145.1	3,616.9
2009	25.1	2.5	27.6	284.8	3,659.7	4,188.1
2010	31.8	3.0	34.7	337.6	4,338.2	4,957.1
2011	40.7	3.8	44.4	423.8	5,446.4	6,132.6
2012	43.0	4.7	47.7	527.9	6,783.9	7,497.8
2013	34.1	5.3	39.4	595.4	7,651.2	8,387.3
2014	22.1	5.3	27.3	584.5	7,512.0	8,194.2
2015	15.1	4.4	19.5	471.6	6,063.0	6,594.9
2016	9.3	3.3	12.6	339.6	4,367.8	4,745.4
2017	5.1	2.5	7.6	239.3	3,081.1	3,345.2
2018	2.6	1.8	4.4	162.4	2,092.3	2,270.7
2019	0.9	1.2	2.2	100.4	1,294.7	1,404.4
2020	0.4	0.8	1.2	61.6	795.6	862.8
2021	0.1	0.5	0.6	34.5	446.3	483.9
2022	0.0	0.2	0.3	15.8	204.1	221.3

2023	0.1	0.1	0.1	6.7	86.5	93.7
2024	0.0	0.0	0.0	2.9	37.0	40.1
2025	0.0	0.0	0.0	0.7	8.8	9.5
Total	313.0	46.1	359.1	4,963.8	63,816.0	72,840.7
Present Value (2003)	120.7	15.3	136.0	1,683.4	21,637.9	25,434.3

a This does not include vendors' and ISPs' internal network transition costs. See separate columns.

2. Internet Users' Costs

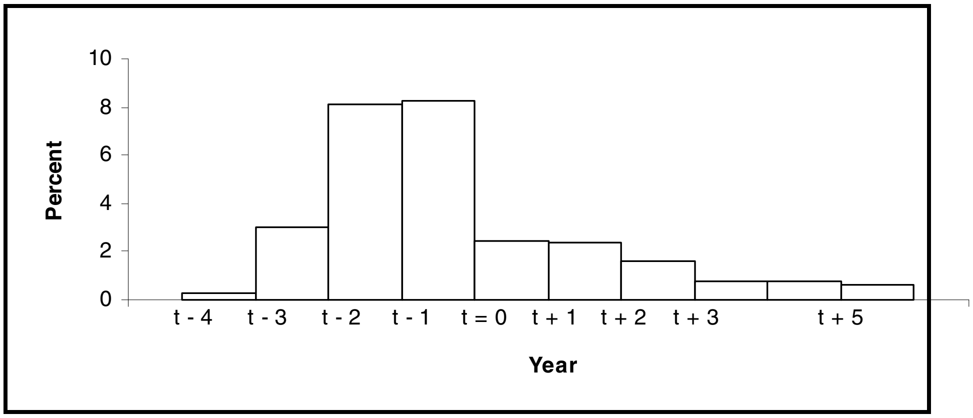
In this paper, we provide further analysis and discussion for users' costs.[41] To transition to IPv6, we estimated that users will spend approximately $23.3 billion between 1997 and 2025 (see Table 2 for annual breakdowns). This number includes both government and nongovernment costs totaling $1.7 billion and $21.6 billion, respectively.[42]

Figures 4 and 5 were used to develop the time series of costs shown in Figure 6 for Internet users. As shown in Figure 4, most user costs occur in the two-year period prior to enabling IPv6 capabilities, with follow-up transition activities ongoing for an additional five years. Combining data provided by interview participants with the penetration curve in Figure 5 results in the time-series cost curve in Figure 6 (see Appendix 2 for a detailed description of the data calculations performed). Annual costs for users are projected to peak around 2013.

[41] NIST's "IPv6 Economic Impact Assessment" (2005) and Gallaher and Rowe (forthcoming) provide a breakdown of the cost calculation and a related discussion for ISPs', infrastructure vendors', and application vendors' costs.

[42] These figures are based on information provided by stakeholders participating in our interviews.

FIGURE 4: PERCENTAGE OF IT STAFF DEDICATED TO IPV6 TRANSITION FOR INTERNET USERS



A. ASSUMPTIONS AND UNDERLYING DATA: USER ESTIMATES

Internet users form the largest stakeholder group with approximately 2,200,000 IT staff are directly affected by the transition to IPv6.[43] In Table 3, the relative cost distribution is broken down for users into activity categories. However, the costs will likely vary widely for individual organizations within each user group—corporate, institutional, government, and independent users. For example, based on information provided by stakeholders, we believe that independent users, comprising of home users and small businesses, will incur virtually no cost to move to IPv6 because they would gain IPv6 enablement over time without additional testing and installation costs.[44]

[43] This figure represents our estimate based on BLS data and stakeholder interviews. IT staffing figures, including wage rates, were determined using data from the U.S. Department of Labor, Bureau of Labor Statistics (BLS) (2003).

[44] These users do not have network management software or major networking hardware that would need to be enabled. Routing upgrades would provide equipment and software that would be IPv6 enabled several years into the future, but no additional cost should be seen.

FIGURE 5: PERCENTAGE OF U.S. USER NETWORKS IPV6 ENABLED

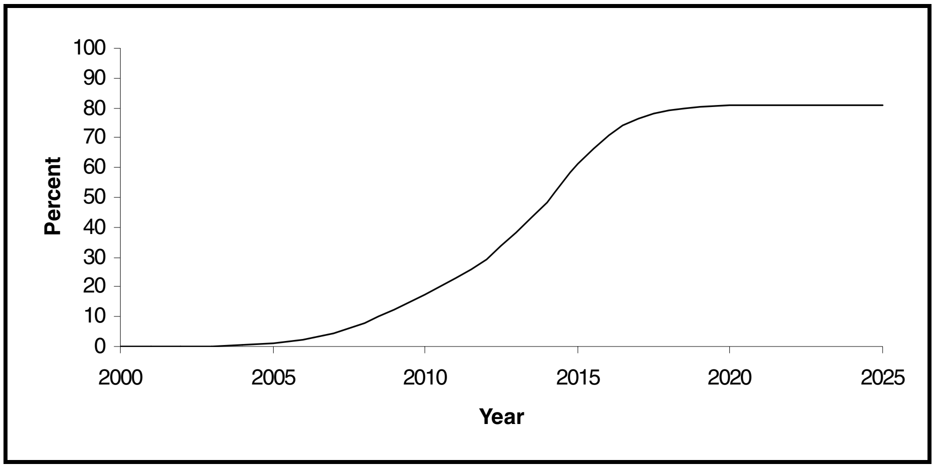


FIGURE 6: ANNUAL SPENDING BY U.S. USERS TO BECOME IPV6 ENABLED

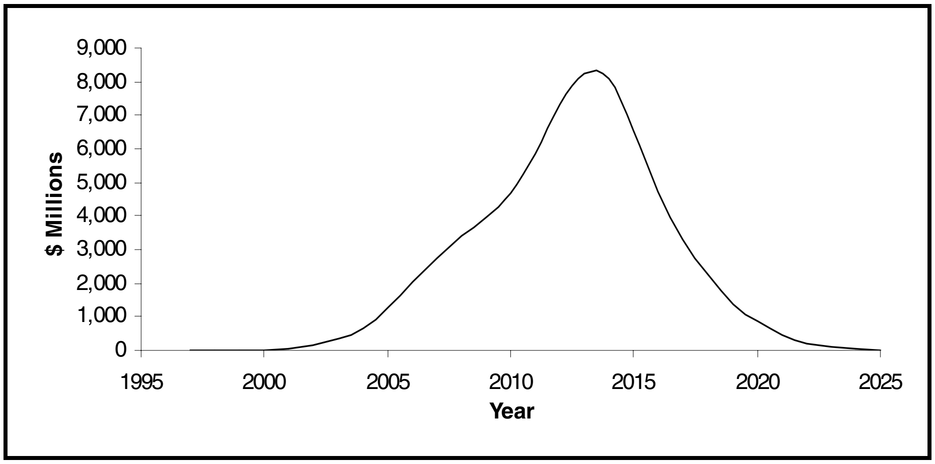


TABLE 3: DISTRIBUTION OF IPV6-RELATED TRANSITION COSTS FOR USERS

Category	Distribution of Total Transition Costs
	Internal Network Costs
Network management software (upgrade)	18%
Network testing	18%
Installation effort	24%
Maintaining network performance	16%
Training (sales, marketing, and tech staff)	24%

Medium-sized businesses, on the other hand, will likely incur the largest relative increase in IT spending to transition to IPv6. The majority of these costs will be related to core networking operations and staff training, the size of which does not increase proportionally to the size of an organization. As a result, the cost per IT staff for medium-sized businesses will be larger than for larger businesses.

Regardless of cost differences, which are nonlinear in relation to organizational size, in general, users' costs will depend heavily on several common factors:

- existing organizational network infrastructure, including servers, routers, firewalls, billing systems, and standard and customized software programs;
- the type of organization (i.e., some types of services could be interrupted/damaged during a transition);
- the future needs/desires of the organizational network; and
- the level of security required during the transition.[45]

[45] For example, an e-business would be much more reliant on the security of their network than a lumber manufacturer. Although the lumber manufacturer may experience problems related

As an example, the Defense Research and Engineering Network (DREN), the Department of Defense's recognized research and engineering network, recently completed an IPv6 pilot project in which IPv6 was deployed in infrastructure components in the core network and at twelve High Performance Computer Centers (HPCs). This process included the upgrading of networks, DNS software, other IP infrastructure, computer server operating systems, and desktop operating systems at each HPC.

Costs for transitioning each site included hardware—between $500 and $2,000 per router to expand the memory;[46] training—between $30 and $2,500 per person at each site, plus their time;[47] and installation labor—approximately 400 hours of labor to transition numerous high-capacity networking components.[48] This process took approximately six to nine months to complete. DREN had previous experience in both testing IPv6 and working with operational IPv6 networks; therefore, transition costs are likely to be low compared to many other organizations (Baird 2004).

D. ALTERNATE IPV6 DEPLOYMENT SCENARIOS

Although our base case estimates are based on a wide breadth of information from stakeholders and experts, we concede that they could be either too aggressive or not aggressive enough. To address such

to a breach in security, they can continue to operate the plant. The e-business could be affected much more significantly by one-time or more frequent security problems during a transition to IPv6.

[46] We received this information during a phone interview on September 17, 2004, with John M. Baird, IPv6 Pilot Implementation Manager with the DoD High Performance Computing Modernization Program (HPCMP). According to Baird, assuming a router runs at 40% of capacity regularly, if IPv6 addresses are used, the same routers would regularly be running at 80% of capacity. Therefore, routers will need approximately double the memory to ensure spikes do not crash the systems.

[47] Several sites purchased commercial training at a cost of between $600 and $2,250 per person; DREN provided a half-day on-site orientation, training, and planning seminar, and staff used numerous books, CDs, and videos to help them understand the implications of IPv6.

[48] Each site had several computers, massive file servers, a few high-speed networks, and an average of approximately forty-five desktop/laptop computers and visualization workstations.

concerns, we asked interview participants to speculate about the possibility of alternate scenarios. When asked about the possibility that the transition could take longer to occur, all respondents indicated that the costs would be the same as the base case. However, stakeholders indicated that IPv6 penetration could occur much more quickly than the "base case" scenario if, for example, some new application was developed that was highly demanded and required IPv6. In this case, the costs would be much higher. Figure 7 presents the most likely transition timelines for IPv6 costs (to be borne by all stakeholders) based on the interviews we conducted. In general, this "base case" reflects the penetration of IPv6 *capabilities* as part of normal hardware and software upgrades and the *enabling* (turning on) of IPv6 capabilities at a later time as applications become available and demand for IPv6 functionality grows.

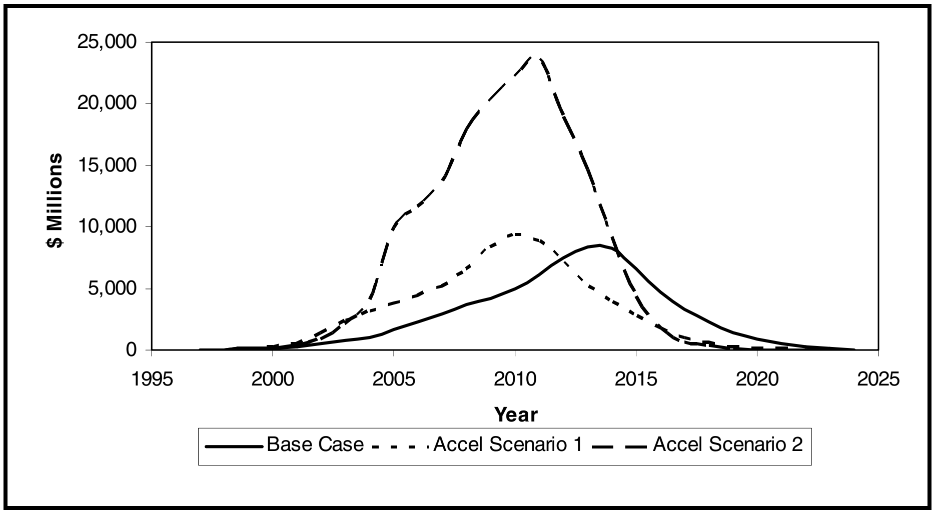
Participating stakeholders indicated that there is significant uncertainty about the projected timeline for IPv6 deployment. As a result, interview participants were asked to estimate differences in costs under two alternative accelerated deployment scenarios:

1. Scenario 1: IPv6 capabilities are enabled at the same time as capabilities are acquired (i.e., during routine upgrades of hardware and software).

2. Scenario 2: The penetration of IPv6 capabilities is accelerated as well, leading to the early replacement of some hardware and software. Enabling is therefore further accelerated to match the earlier acquisition of capabilities compared to Scenario 1.

Figure 7 illustrates the time series of costs under the base case and two accelerated deployment scenarios in $2003. In Scenario 1, participating stakeholders indicated that the level of effort (labor hours) associated with the transition to IPv6 will increase by approximately 5% as activities are compressed as a result of accelerating enablement by three years. This 5% increase in effort, along with accelerating the time series of costs by three years, leads to a 25% increase in the PV of U.S. deployment costs.

FIGURE 7: TIMELINE OF COSTS FOR BASE CASE AND ACCELERATED DEPLOYMENT SCENARIOS



In Scenario 2, participating stakeholders indicated that accelerating the replacement of hardware and software by one year, in addition to a four-year acceleration of enablement, would significantly increase the cost of IPv6 deployment. Scenario 2 represents approximately a 285% increase in the PV of U.S. deployment costs. In other words, the degree of acceleration significantly affects the PV of the costs incurred.

Of note, these estimates do not try to estimate additional indirect costs associated with increased problems, such as new security breaches and/or interoperability problems, if a decrease in testing time results in less secure or more inefficient organizational networks for a certain period. However, industry and expert interviews indicate, empirically, that these costs would likely be incurred during an accelerated transition.

III. CONCLUSION

IPv6 adoption could contribute to the improvement of network security for all users and subsequently reduce limitations for vendors developing products that require E2E security. By stimulating the development of new security models and motivating organizations to consider restructuring their network architecture, IPv6 could have a significant positive effect on security. However, IPv6 adoption is not certain—some stakeholders may prove quite resistant to incurring any costs (and possibly not seeing any benefits, at least initially), and research on alternate Internet redesign ideas (e.g., to develop a non-IP-based communications infrastructure) continues.

Further, IPv6 adoption will cause new security holes to develop, and although many user applications and organizational network components are currently IPv6 capable (or will be very soon) and U.S. government agencies are planning to enable IPv6 by 2008, widespread adoption of IPv6 (requiring enablement of related infrastructure and applications) is likely several years away for nongovernmental organizations. Any transition will result in costs to all stakeholders, particularly if users decide to upgrade network equipment to gain IPv6 capabilities prior to routine upgrade cycles. Given the qualitative nature possible in any analysis of the benefits of IPv6, no general conclusions can be drawn concerning the net effects of a transition to IPv6. Stakeholders will have to make their decisions individually based on what they observe as their costs and potential benefits, as they consider when (or whether) to transition to IPv6.

APPENDIX 1: INTERVIEW PARTICIPANTS

The following is a list of organizations and individuals who participated in our interviews:

- **Infrastructure Vendors:** Boeing Integrated Defense Systems, Hewlett-Packard Company, Microsoft, Native6, Nortel Networks

- **Application Vendors:** Arkivio, Hexago, Level7, Mentat, OnStor, Inc., Red Storm Entertainment Inc.

- **Internet Service Providers (ISPs):** AT&T, Earthlink, Qwest, Sprint, Teleglobe, NTT/Verio

- **Infrastructure Users:** Motorola, Nextel, Nokia, Panasonic

- **Internet Users:** The Boeing Company, CENTAUR/NC State University, Defense Research Engineering Network (DREN), ESNet, Internet2, U.S. Army

- **Other Interested Parties**: IPv6 Forum, North American IPv6 Task Force (NAv6TF), Paul Francis

APPENDIX 2: EXPANDED METHODOLOGY

In this appendix, we describe how our penetration estimates were created and the methodology we used to calculate the costs to stakeholders.

PENETRATION ESTIMATES FOR IPV6

As part of our interviews, information was collected on the timing of the development and deployment of IPv6 products and services. This information included the following:

- when IPv6 capabilities will be integrated into infrastructure hardware and systems software and offered to customers;

- when IPv6-capable applications will be available;

- when IPv6 capabilities will be in place within ISP and users' networks; and

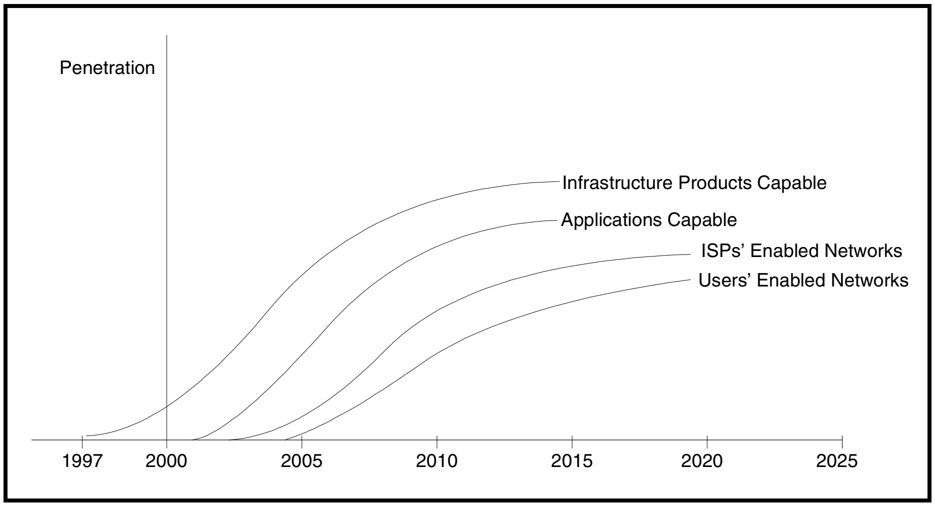
- when IPv6 will be enabled,[49] or turned on, by ISPs and users.

The penetration of IPv6 is likely to be a gradual process and will probably never reach 100 percent of applications or users. Figure A2-1 illustrates the structure by which the cost analysis uses the timing associated with the development (availability) of IPv6 infrastructure products (hardware and software) and applications, as well as the enabling of these products and applications by ISPs and users.[50] Events are generally sequential in that ISPs enabling their network is conditional on the availability of IPv6-capable hardware and software. These four curves are the key penetration metrics for the cost analysis because they capture the timing of expenditures. Section II provides estimated penetration curves generated based on the information from the interviews.

[49] For the purposes of this paper, "enabled" is generally defined as the establishment of some form of IPv6 connectivity and, when looking at an overall network's adoption, that some percentage of IP-dependent applications can operate in IPv6. When specific infrastructure components or applications are described as IPv6 enabled, this does not refer to the entire network but merely to that product's ability to function via IPv6 once it has been turned on.

[50] Figures A2-1 through A2-4 should be interpreted only as examples used to help explain the methodology we used to estimate the costs of transitioning to IPv6. These figures do not represent our actual estimates.

FIGURE A2-1: EXAMPLE OF PENETRATION CURVES USED FOR COST ANALYSIS



For vendors, R&D expenditures to integrate IPv6 into their products are the primary expenditure category associated with the transition from IPv4 to IPv6. The primary expenditures for ISPs and users are labor costs associated with enabling IPv6 capabilities. As a result, these four penetration curves are used to determine the timing of development and deployment costs associated with IPv6.

Note that the penetration of IPv6 capabilities (i.e., when ISPs and users have IPv6-capable infrastructure components and applications in place, but they are not enabled) is not a key component in determining the timing of costs for these two groups. This is because the incremental variable cost of IPv6 products is negligible compared to IPv4 products—almost all the costs are associated with applications' R&D and enabling IPv6 functionality.[51] As a result, the penetration of capabilities is not a factor in determining baseline transition costs. However, the penetration of capabilities is important in assessing the alternative deployment scenarios presented in Section II.D in the body

[51] We generally assumed, based on information provided by participating stakeholders, that routine upgrades will provide hardware and software upgrades necessary prior to IPv6 enablement for almost all ISPs and user networks and that all interoperability problems have been solved (otherwise, purchasers could incur these latter costs).

of the paper. As discussed in that section, the penetration of capabilities provides an upper bound on how much the enabling of IPv6 can be accelerated without adding the costs of early retirement of hardware and software.

QUANTITATIVE COST ESTIMATION METHODOLOGY

The penetration curves described above, representing the estimated share of infrastructure products and applications that are IPv6 capable and the share of networks that are IPv6 enabled at a given time, imply that the costs will be distributed over time as stakeholders gradually engage in transition activities. These curves represent the *point in time* when products and applications become available to customers and networks become enabled. However, activities leading to and supporting these achievements/milestones are distributed before and after the point of product roll out or system enabling.

Figure A2-2 provides an *example* of the potential time distribution of labor expenditures surrounding the enablement of a network system.[52] To be clear, this figure represents the likely cost distribution for *one* user, not all U.S. users. In the figure, t = 0 represents the date when the system is enabled. However, the majority of the costs are borne prior to t = 0 as networking staff are trained and the system is reconfigured. Lower costs associated with testing and monitoring are then experienced after the enabling date.

Costs are expressed as the percentage of an IT staff's time devoted to IPv6 transition activities. Thus, in this example, 10% of a company's IT staff in the year prior to becoming enabled (t – 1) will be devoted to the IPv6 transition. In the year after enabling (t + 1), the share of resources decreases to 5% of IT staff time. This number is multiplied by the average IT staff wage rate to obtain the cost per IT staff member associated with the IPv6 transition for each year before and after enabling IPv6 systems.

[52] Figure A2-2 is an example distribution based on our research and interview activities. User-specific distributions are presented in Section II.C.2.

FIGURE A2-2: EXAMPLE OF THE DISTRIBUTION OF IT STAFF RESOURCES NEEDED TO ENABLE IPV6 IN A USER NETWORK

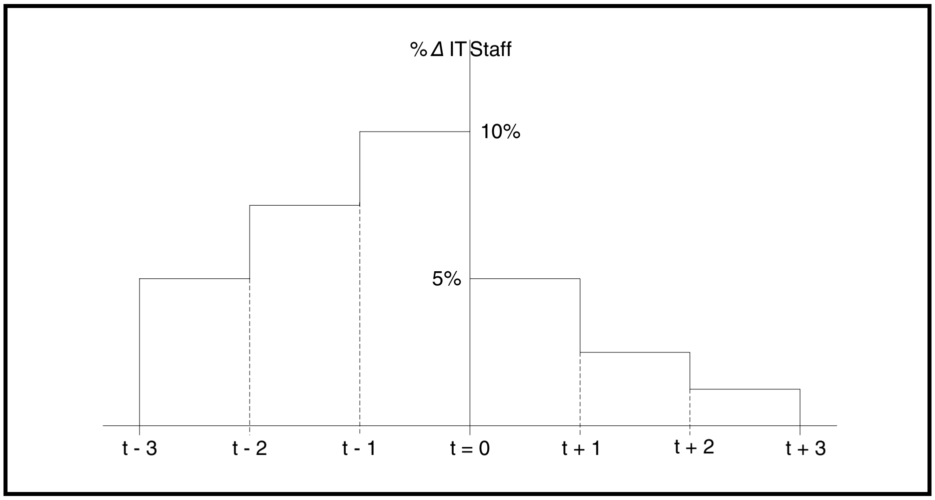
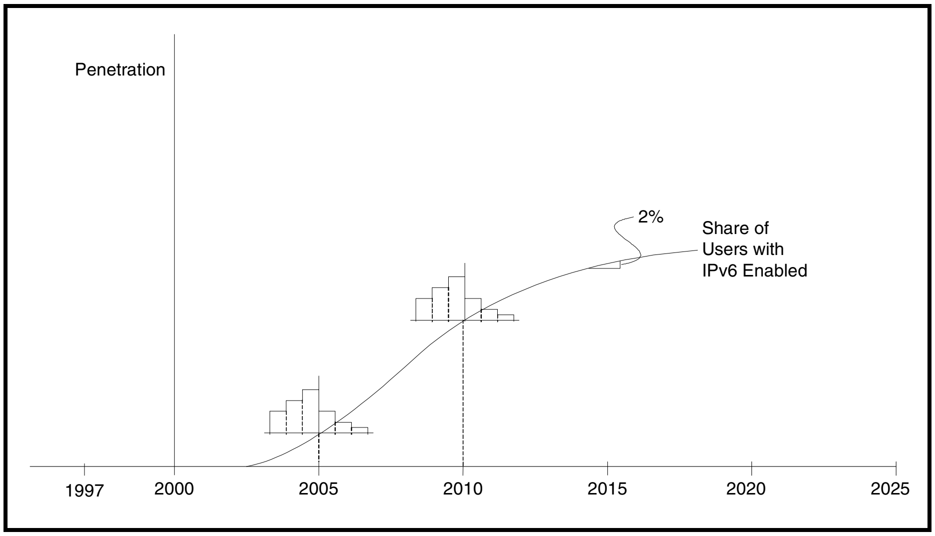


Figure A2-3 shows the penetration of IPv6-enabled user systems and determines the timing of the costs. For example, in this hypothetical figure, 2% of systems are enabled in the year 2015 (t = 0).[53] This implies that 2% of affected U.S. IT staff[54] in 2014 (t – 1) were devoting 10% of their time to IPv6 transition activities, and 2% of affected U.S. IT staff in 2015 (t = 0) were devoting 5% of their time to IPv6 transition activities (BLS).

[53] This means that in the year 2015, 2% of users enabled or "turned on" IPv6 capabilities. This does not mean that only 2% of all users are enabled by this point.

[54] IT staffing figures, including wage rates, were determined using data from the U.S. Department of Labor, BLS.

FIGURE A2-3: EXAMPLE OF U.S. USER ENABLEMENT OVER TIME

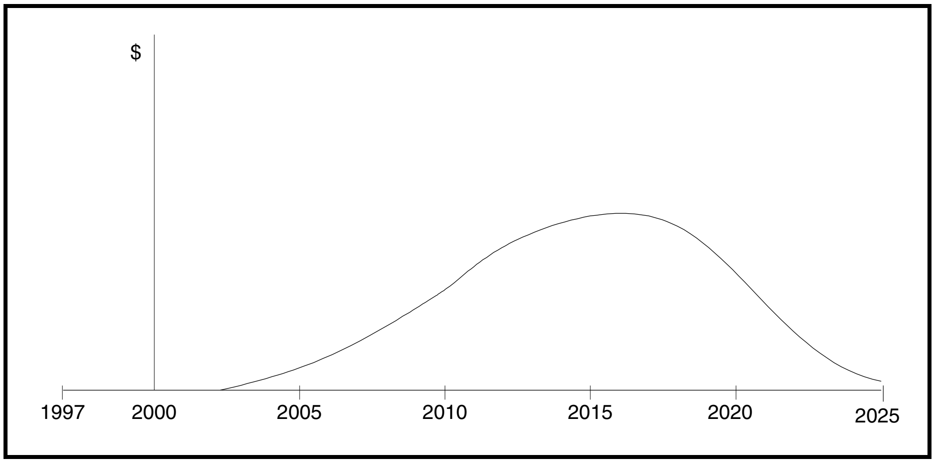


Combining the distribution of costs surrounding enabling (Figure A2-2) and the timing of system enabling (Figure A2-3)[55] yields the cumulative cost curve shown in Figure A2-4. As shown in Section II.C for user costs, this cost distribution–timing approach is used to calculate the time series of transition costs for:

- infrastructure vendors' product development,
- application vendors' product development,
- ISP's provisioning service enabling, and
- users' system enabling.

[55] The main curve in Figure A2-3 is the same as the "Users" Enabled Networks" curve in Figure A2-1.

FIGURE A2-4: EXAMPLE OF U.S. USERS' TRANSITION COSTS OVER TIME



REFERENCES

1. Baird, J.M. 2004. Interview by RTI. September 17. IPv6 Pilot Implementation Manager with the DoD High Performance Computing Modernization Program (HPCMP).

2. Gallaher, M.P.and B.R. Rowe. 2005. *Planning Report 05-2: IPv6 Economic Impact Assessment*. Report prepared for National Institute of Standards and Technology (NIST), RTI International. http://www.nist.gov/director/prog-ofc/report05-2.pdf.

3. Gallaher M.P. and B.R. Rowe. Forthcoming. The costs and benefits of transferring technology infrastructures underlying complex standards: The case of IPv6. *Journal of Technology Transfer*.

4. Markoff, J. 2005. Early look at research project to re-engineer the Internet. *New York Times*, August 29, 2005. http://www.nytimes.com/2005/08/29/technology/29internet.html.

5. Marsan, C.D. 2004. Verio first to offer commercial IPv6 service. *Network World*. January 5, 2004. http://www.networkworld.com/newsletters/isp/2004/0105isp1.html.

6. National Science Foundation (NSF) 2003. Table E-2. Research and development in industry: 2000. http://www.nsf.gov/statistics/srs02403 (accessed March 12, 2006).

7. Shaikh, K. 2005. IPv6—The path to secure converged networks. *6Sense Newsletter* 2, no. 2 (January), http://www.usipv6.com/6sense/2005/jan/08.htm.

8. Tassey, G., M. Gallaher, and B. Rowe. 2006. Complex standards and sustained innovation: The Internet protocol. Working Paper.

9. U.S. Department of Commerce. National Institute of Standards and Technology (NIST). 2004. Deploying IPv6: Exploring the issues. Transcript of Department of Commerce IPv6 Public Meeting 07-28-2004. http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/webcast.html.

10. U.S. Department of Commerce. National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA). IPv6 Notice of inquiry—Comments received. http://www.ntia.doc.gov/ntiahome/ ntiageneral/ipv6/commentsindex.html (updated March 2004).

11. U.S. Department of Commerce. National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA). 2006. Technical and economic assessment of Internet protocol version 6 (IPv6). http://www.nist.gov/director/prog-ofc/IPv6-final.pdf.

12. U.S. Department of Labor. Bureau of Labor Statistics. 2003. National occupational employment and wage estimates. http://www.bls.gov/oes/2003/may/oes_15Co.htm (accessed March 12, 2006).