DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	
Request for Comments on Deployment of Internet Protocol, Version 6	)	Docket No. 040107006-4006-01

COMMENTS OF MICROSOFT CORPORATION

Microsoft Corporation ("Microsoft") is pleased to submit to the Commerce Department these comments on the deployment of Internet Protocol, version 6 ("IPv6") in response to the Department's Request for Comments ("RFC").[1] Microsoft is a leader in software, services and Internet technologies for personal and business computing. We are working with our partners in industry to bring IPv6 into the marketplace, and we are committed to implementing IPv6 in our software.

The current Internet Protocol, version 4 ("IPv4") has fostered amazing growth and transformation of the Internet, and most users currently seem content with their IPv4 networks. Yet with the advent of new, Internet-capable devices and increasing concerns about the functionality, robustness, and security of the IPv4-based Internet, more advanced technologies are desirable. A gradual, market-based conversion to IPv6 is the most technologically feasible and least disruptive way of addressing these concerns and realizing the full promise of the Internet. As part of that effort, the government should

[1] Notice of Inquiry, 69 Fed. Reg. 2890 (Jan. 21, 2004).

consider acquiring IPv6-enabled software and hardware in order to meet government needs. However, governmental regulation of IPv6 is unwarranted and could be counterproductive.

These comments first provide information concerning IPv4 and its emerging weaknesses as Internet usage and service demands increase. They then describe why IPv6 is an important technology that overcomes IPv4's weaknesses and how the marketplace is transitioning to IPv6 at an appropriate pace. They conclude with our views concerning governmental action with respect to IPv6 deployment.

Internet Protocol, Version 4

The Internet Protocol ("IP") is the international standard protocol that defines how data is sent from one computer or device to another over the Internet. While that function sounds simple, the technical details of using and deploying IP are quite complex. In addition, because IP is fundamental to Internet connectivity, and is implemented in so many kinds of software and hardware, a change in IP is a daunting proposition.

IPv4 has now been in use for over 20 years. During that time, the Internet has grown from a small network for a relatively few researchers and government contractors to an indispensable and nearly ubiquitous avenue of communication, commerce, and entertainment for governments, educational institutions, corporations, and individuals. The IP-based Internet is truly a global network, and countries in which the Internet originally made slow inroads are now moving quickly to catch up. Indeed, it is probably fair to say that the Internet has grown larger and faster than anyone more than a few years ago thought possible. Although the Internet's exact size is unknown, almost 450 million

people have access to the Internet from a personal computer at home, and there are nearly 300 million users actively on the Internet, according to recent estimates.[2] In addition, new IP-based devices and services such as Personal Digital Assistants ("PDAs"), mobile telephones, multiplayer games, IP telephony, and videoconferencing are placing increasing demands on the Internet's performance.

This boom in Internet usage and the accompanying new demands on Internet service have underscored design weaknesses in IPv4 that are already beginning to affect the quality of service Internet users enjoy. These weaknesses include:

- *A lack of adequate address space to meet fast-growing demand*. IPv4 provides recognition of up to four billion addresses. While that number seems virtually unlimited, IP addresses have been rationed using short-term organization-specific solutions since the early 1990s. These solutions have been quite successful and have removed the appearance of IP scarcity for the average user. However, these solutions were not intended to be permanent, and the supply of addresses will face increasing pressure over time.
- *Address-conservation techniques causing a lack of end-to-end connectivity between computers and other devices*. To make the most out of limited address space, some users have adopted workaround technologies such as Network Address Translators ("NATs"), which map a single IP address to several private addresses. However, these technologies diminish the transparency of the Internet. They also interfere with end-to-end networking and with efforts to provide end-to-end security. In addition, when a NAT

[2] Nielsen//NetRatings, at http://www.nielsen-netratings.com/news.jsp?section=dat_gi.

fails, communications to and from all of the devices depending on the NAT are interrupted.

- *Growing numbers of addresses increasingly burdening the means of routing communications*. The Internet's routing tables and other means of routing network communications are becoming increasingly burdened and inefficient due to the sheer number of Internet addresses and the related practices for allocating these addresses. The resulting costs and delays may prove to be a larger problem than IPv4's constraints on the absolute number of available addresses.
- *The need to support new network services that did not exist when IPv4 was developed*. Technology advances and the evolution of the Internet over the last 20 years have led to new requirements in areas such as security, mobility and quality of service that IPv4's design did not take into account. While it is possible substantially to address these requirements in IPv4, such work-around solutions can be complex and inefficient.

IPv6 Is an Evolutionary but Important Improvement over IPv4

IPv6 was designed to overcome the weaknesses of IPv4 described above, to enable new computing and communications paradigms, and to provide a flexible and operationally robust platform for future Internet growth. IPv6's advantages over IPv4 include:

- *IPv6 positions the Internet for future growth*. IPv6 increases the size of each address from 32 to 128 bits, vastly increasing the number of available

addresses and virtually eliminating the need for NATs and other address-conservation techniques with their attendant disadvantages.

- *IPv6 supports end-to-end connectivity*. Because every individual device connected to the Internet will be able to have its own IP address, IPv6 promotes speed and quality of service and facilitates applications such as IP telephony and video teleconferencing. IPv6 also restores the original objective of Internet architecture to enable end-to-end communications by permitting routing of communications around failures in the network.
- *IPv6 provides a framework for end-to-end trustworthy networking*. Through built-in security and support for authentication and privacy capabilities, IPv6 promotes end-to-end trustworthy networking.
- *IPv6 will enable more efficient routing of network communications*. IPv6's large address space can be allocated in a hierarchical manner that reflects the current topology of the Internet. This hierarchical allocation and its better route aggregation framework should permit greater efficiency in the routing of network communications.
- *IPv6 better handles mobile applications and services*. IPv6 provides native redirection features and capabilities for facilitating device and user movement. These features better enable mobility of networked wireless services and simplify the design and construction of wireless networks.
- *IPv6 permits easier networking*. IPv6 offers a stateless autoconfiguration feature that will allow "plug and play" use of devices.

- *IPv6 enables exciting new products and services*. These features will allow developers to offer exciting IP-based applications that fundamentally change users' Internet experiences.

Despite these advantages, IPv6 is an evolutionary step beyond IPv4. IPv6 uses translators that provide backward compatibility with IPv4. The translators allow users to migrate to IPv6 gradually. IPv4 use probably will continue for some time, and NATs and other IPv4 work-around strategies allow users to avoid or mitigate many of its shortcomings. However, the available work-around strategies have their own disadvantages. Moreover, the long-term productivity benefits and enhanced technological features of IPv6, including security, mobility and enhanced quality of service, outweigh the costs and disruption of conversion, particularly since these costs can be managed and perhaps reduced by careful planning and a gradual, market-based conversion strategy. Assuming continued exponential growth in both the number of devices connected to the Internet and the overall level of network traffic, IPv6 conversion is probably a necessary step to sustain the health and realize the full promise of the Internet.

Marketplace Forces Are Working to Deploy IPv6 at an Appropriate Pace

While deployment of IPv6 offers significant promise, the conversion from IPv4 to IPv6 is a large task that ultimately will affect nearly all network architectures, applications and systems. The task is similar in scope and probably even more complex than preparation for the Year 2000, except there is no unmoveable deadline for IPv6 deployment. Transitioning from IPv4 to IPv6 will be expensive, although overall

deployment costs are hard to estimate. Given the magnitude of the project and the lack of specific deadlines, hardware and software designers, network providers, and users are generally approaching the conversion from IPv4 to IPv6 judiciously to avoid costly missteps. From our perspective, it appears that the marketplace is working – providing for continuing support of IPv4 applications but preparing for an eventual transition to a native IPv6 network.

Availability of IPv6-Enabled Software

We are most familiar with our own efforts to facilitate the conversion to IPv6.[3] Microsoft is not a newcomer to IPv6; we understand its importance and have a long-term commitment to its implementation and its success.

Microsoft Research has been contributing to the Internet Engineering Task Force ("IETF") IPv6 standard-setting effort since 1996, when the specifications for IPv6 were not yet completed. In early 1998, Microsoft Research made available to the IPv6 standards development community an early version of an IPv6 protocol.

We already have incorporated some IPv6 technology into our existing software:[4]

- In March 2000, we released a technology preview for the Windows 2000 operating system. This preview allowed software developers to familiarize themselves with the capabilities of IPv6 and to enable their applications to use IPv6.

[3] Others have sought to compile lists of IPv6-enabled offerings, and those lists indicate that a range of offerings is available from numerous sources. *See, e.g.,* http://www.ripe.net/ripe/meetings/archive/ripe-37/presentations/ripe-ipv6-status-hinden/sld013.html; http://playground.sun.com/pub/ipng/html/ipng-implementations.html.

[4] Further information concerning Microsoft software with IPv6 capabilities is available at http://www.microsoft.com/windowsserver2003/technologies/ipv6/default.mspx.

- In October 2001, Microsoft released the Windows XP operating system with a developer preview IPv6 production stack. We enabled key components for IPv6 so that software developers could begin enabling their applications for IPv6, or for both IPv4 and IPv6.
- In March 2003, we released Windows Server 2003 with the first edition of Microsoft's IPv6 production stack and IPv6-enabled components.
- In July 2003, Microsoft released the Advanced Networking Pack for Windows XP. This release contains support for peer-to-peer networking and IP-based tunneling technology that provides the ability to provide IPv6 addresses over IPv4-based NATs.
- Windows CE .NET versions 4.1 and later provide production-quality IPv6 support.
- An ever-increasing number of Windows applications also are IPv6-enabled.

Microsoft is working hard to simplify the challenge of IPv6 deployment by making the transition as transparent to users as possible. For example, we have included tunneling technologies in our software to allow IPv6-enabled systems automatically to communicate over IPv4 networks and to interact with IPv4 systems.

Moving forward, we are committed to supporting our customers' needs and rollout schedules for IPv6. We fully intend to provide native IPv6 support in future software. We expect to incorporate additional IPv6 capabilities into software to meet our customers' evolving needs. We will also continue to participate in the IPv6 standards process with other industry leaders to enrich the technology further.

Deployment in General

To date, most users have seen little need to switch to IPv6 because they are content with their IPv4 networks. Only recently have all the necessary pieces of the IPv6 conversion puzzle begun to come together to make large-scale IPv6 deployment economically feasible and more technologically compelling.

Not surprisingly, IPv6 adoption is proceeding fastest in Asia, which has small allocations of IPv4 address space and where widespread use of broadband Internet connectivity and mobile devices have created a surging market for new IP capabilities.

IPv6 adoption has proceeded slowly in the United States, but is likely to accelerate as IPv6 network solutions and applications become more available, robust and affordable. It is important to remember that IPv6 was designed to accommodate a gradual deployment. That is exactly what we see happening, as most users wait for applications taking advantage of IPv6's unique capabilities before making a serious infrastructure commitment to IPv6 conversion. We see most early activity relating to IPv6 conversion taking place at the edge of the network. Service providers will deploy native IPv6 routing in response to customer demand as they replace their deployed network equipment. A few users have expressed interest in "greenfield" deployments using IPv6 natively. Such interest has been limited to the relatively small number of users, particularly government users, who are building networks from scratch.

Far from the possible "chicken-and-egg problem" described in the RFC, we expect a market-based, mutually reinforcing cycle of IPv6 capabilities and customer demand to accelerate the pace of deployment over the next several years. As described above, we and other software developers have been proceeding apace to release IPv6-

enabled software. We expect increasingly to see IPv6-based applications driving demand for IPv6 capabilities. Users will be able to operate such software in part over IPv4 networks because of features such as automatic tunneling. However, if such offerings are successful, Internet service providers likely will migrate to native IPv6 capabilities as they update and upgrade their networks, and software developers inevitably will respond to marketplace demand by introducing more IPv6-based software. International development of IPv6 networks and services will also encourage the U.S. market to transition to IPv6.

The Government's Role with Respect to IPv6 Deployment

The RFC asks fundamental questions concerning the government's role with respect to IPv6 deployment. The remainder of these comments addresses those questions.

The Government Should Consider Adopting IPv6 For Its Own Use

The government is a major purchaser of information technology software and hardware with a typically long procurement and in-service life cycle. For all the reasons described above, IPv6 is an important technology for both public and private sector customers, and will become more so within the planning horizon for government information technology acquisitions. Accordingly, we encourage the government to consider embracing IPv6 for its own use.

The government's early adoption of IPv6 would be consistent with the President's National Strategy to Secure Cyberspace ("National Strategy").[5] Priority IV of the National Strategy emphasizes the government's duty to secure its information systems: "Federal agencies should become early adopters of new, more secure systems and protocols where appropriate."[6] IPv6 is precisely such a new, more secure protocol. The government's transition to IPv6 would be a significant step towards meeting the National Strategy's objective of making North America a "Safe Cyber Zone." In addition, the Government's transition to IPv6 could underscore the government's own commitment to cyberspace security as it works with other countries to enhance the security of global Internet networking.[7]

Microsoft applauds the government users that already have shared a roadmap for their migration to IPv6. Until developers have a clear understanding of their customers' IPv6 needs and objectives, progress toward IPv6 implementation is likely to suffer from a mismatch between available infrastructures and applications on one hand and customer needs on the other. Government customers can help avoid this mismatch by clearly articulating their IPv6 program needs and implementation timetable, and by procuring infrastructure and software that meets those needs. Such customers are also likely to serve as helpful exemplars of an IPv6 transition strategy.

We are always interested in learning about our customers' needs. We are already engaged in dialogue with government customers to discern the government's IPv6 needs

---

[5] National Strategy To Secure Cyberspace (Feb. 2003), available at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[6] National Strategy to Secure Cyberspace, p. 43.

[7] National Strategy to Secure Cyberspace, p. 51.

and to see how we and our partners in industry can help to meet those needs. We would be pleased to broaden and deepen those dialogues across the government.

No Further Government Action Is Warranted at this Time

Microsoft believes that software and hardware manufacturers increasingly will provide affordable IPv6 offerings attractive to customers because of IPv6's technical merits. Thus, the ordinary operation of the commercial marketplace, including the government as a customer, is likely to lead gradually to widespread use of IPv6 in the foreseeable future.

It is unnecessary and would be ill advised for the government to regulate or subsidize a particular IPv6 implementation approach. This might skew the path of technological development or might interfere with a commercial marketplace that appears to be working. As the RFC recognizes, the market is normally quite effective at spurring innovation and directing investment towards technologies of merit. Any mandates or incentives that favor one version of IP over another, or one approach to IPv6 conversion over another, could skew the market's ability to determine the value of IPv6 and other technologies. Affecting the market's impartiality in choosing winners and losers could also lock in methods or technologies that may prove to be poor choices in the long run.[8]

Nothing about the current state of IPv6 deployment suggests that there has been a market failure that would justify government intervention with its attendant risks. The proliferation of IPv6-enabled offerings likewise makes clear that the private sector is

[8] For the same reason, it is important that the government decide whether and how to convert to IPv6 (or not) based on its technological merits and ability to meet the government's own information technology needs. The government should not adopt IPv6 simply to promote or hasten its adoption by the private sector. Doing so would be tantamount to regulation or subsidization, and could have the same counterproductive effects.

investing in IPv6 development without government intervention or subsidies. At this time it simply does not appear that the development of IPv6 networks and applications needs government mandates or financial subsidies.

Nonetheless, as is the case with any important area of private sector activity, there is clearly a national interest in the orderly development and deployment of IPv6. Accordingly, as part of its general governance responsibilities, it is appropriate for the government to monitor and periodically solicit industry's and users' views on the pace and direction of IPv6 implementation and on any obstacles that they are encountering.

Conclusion

We hope the Commerce Department finds these comments helpful as it considers the deployment of IPv6, including the government's role in the transition. Microsoft is excited about IPv6's potential to enhance the computing and communication experiences of users around the world. We are also aware of the costs and disruption that transition to IPv6 will entail. We look forward to working cooperatively with our partners and customers to address the challenge of strengthening the IP foundations of the Internet.

Dated: March 8, 2004

By: _____

Bill Guidera
Policy Counsel
Law and Corporate Affairs
Microsoft Corporation
1401 I Street, NW
Suite 500
Washington, DC 20005

bguidera@microsoft.com
(202) 263-5914