Internet2
3025 Boardwalk #200
Ann Arbor, MI 48108
Attn: Guy Almes, Chief Engineer
27 February 2004

Office of Policy Analysis and Development
National Telecommunications and Information
Administration, Room 4725
Attn: Internet Protocol, Version 6 Proceeding
1401 Constitution Ave., NW
Washington, DC 20230

On behalf of Internet2, I am pleased to submit this response to your request for comments. Led by more than 200 U.S. universities, working with industry and government, Internet2 is developing and deploying advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Internet2 recreates the partnerships among academia, industry, and government that helped foster today's Internet in its infancy. One key Internet2 activity is the provision to our members of the Abilene advanced production IP backbone network, which facilitates very-high-speed connectivity among our members. For more information about Internet2, visit www.internet2.edu.

Comments organized parallel to Sections II-V of the Request. Comments or questions on these comments should be sent to `Guy Almes <almes@internet2.edu>`.

II. Potential Benefits and Uses of IPv6

II.A. Increased Address Space

"The task force ... seeks comment on the potential uses for this greatly expanded pool of addresses."
Before delving into how IPv6 might make use of its increased address space, it is very important to reflect on some key elements of the original IPv4 architecture. All the early papers and practice on the Internet architecture stress that each computer attached to the Internet will have a globally unique IP address. Typical is this passage from Doug Comer's 1988 text on TCP/IP: "Each host on the Internet is assigned a unique 32-bit Internet address that is used in all communication with that host." (Douglas Comer, *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Prentice-Hall, 1988.) Thus, if one speaks of the IPv4 architecture, it is understood that globally unique IP addresses per host is part of that architecture. Further, the applications-level flexibility provided by globally unique addresses helps explain the ongoing vitality of applications innovation within the Internet. If, for example, a hard decision had been made at the outset of the Internet that some hosts would be clients and others would have been servers, then this would have constrained and ultimately weakened the early work on voice over IP, on person-to-person chats, and on teleconferencing.

The original IPv4 address space cannot sustain the original IP addressing architecture, given the dramatic growth in the number of devices capable of performing as IP hosts, now or soon

including PDAs, mobile phones, and other appliances. Given this growth in the number of hosts, we must either expand the number of addresses or change the architecture. IPv6 implements the former option, while the widespread deployment of NATs as *the* solution implements the latter. We therefore argue that the deployment of IPv6 is architecturally conservative, in that it maintains the essence of the Internet architecture in the presence of an increasing number of hosts, while NAT deployment is architecturally radical, in that it changes the essence of the Internet architecture.

By taking this architecturally conservative approach, IPv6 retains the ability of the Internet to enjoy its classic strength of applications innovation. While it is difficult to predict exactly what forms future applications innovation might take, a few examples will help.

- The new generation of SIP-based interpersonal communications applications, including voice over IP, innovative forms of messaging, presence, and conferencing, make effective use of central servers to allow users to locate each other, but then also makes effective use of direct host-to-host communications in support of the actual communications. This enables applications flexibility and allows for high performance.
- Other conferencing applications, such as VRVS, also require direct host-to-host communications and break when either user is placed behind a NAT.
- The new Grid computing paradigm supports high-speed distributed computing by allowing flexible patterns of computer-to-computer communications. The performance of such systems would be crippled were it required for servers to be involved in these computer-to-computer communications.

The point to be stressed, however, is the difficulty of anticipating such applications.

"The task force understands that [NAT and CIDR] have slowed the consumption of available IPv4 addresses. We seek comment on the accuracy of this understanding. ... We seek comment on the effects that NATs may have on network performance and network reliability."
The introduction of CIDR has been useful and architecturally benign. Its success has been moderate and its negative side-effects few. The principles of CIDR are carried forward into IPv6, and thus CIDR specifics do not seem to be key to understanding the importance of IPv6.

NATs, however, are another story. As noted above, the widespread deployment of NATs is architecturally radical and interferes with application innovation by removing the ability of one host to initiate direct communication with another host. Instead, all applications must be mediated by a central server with a global IP address. Apart from this major negative impact on application innovation, there are other negative impacts on performance and network management. The performance problems stem from the need to change the IP address and port numbers within the IP header and the TCP (or UDP, as appropriate) headers of packets. The resulting complexity will be a difficult-to-diagnose source of performance problems.

More dangerously, however, NATs destroy both global addressability (as mention above) and end-to-end transparency, another key Internet architectural principle. According to the principle of end-to-end transparency, all the routers and switches between a pair of communicating hosts simply pass IP packets along and do not modify their contents (apart from decrementing the TTL field of the IP header at each hop along the path). This principle is key to the support for new applications, and it also eases the task of debugging an application between a pair of hosts. When NAT and other middleboxes modify the contents of the packets, it becomes more difficult for applications developers to understand how to get new applications (those not known when the

given middlebox was designed) to work.

NAT boxes also break a number of tools, such as ping and traceroute, that depend on adherence to the classic Internet architecture and which are key to diagnosing network problems. Both 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.

Finally, note that NATs are deployed in a wonderfully incremental manner. This is a kind of strength, but it also makes it difficult to project the picture that will emerge if continued reliance on them continues. If IPv6 is not deployed so that our reliance on NATs as *the* solution to address scaling problems increases, we will begin to cascade NATs behind NATs and may eventually find ourselves one day in a situation like that reported by an ISP engineer from India who recently stated that they connected customers by cascading NATs five deep. The progressive difficulty of diagnosing performance and other network problems in this context will be severe.

II.B. Purported Security Improvements

While significant, IPv6's strengths in improving security should not be overstated or hyped. Careful distinction needs to be made with respect to several points.

- IPsec *is* important for security. This work will be key to scalable secure communications as the Internet continues to grow and as we continue to rely on it more and more.
- IPsec is important both for pure host-to-host and for support by gateways in a variety of ways.
- IPv6 was designed to support IPsec and complete implementations of IPv6 will include IPsec. (It should be noted, however, that many current implementations of IPv6 are not technically complete and do not support IPsec. This reflects the current immature state of IPv6 implementations.)
- When no NATs are in the path, IPv4 can also provide quite good support for IPsec. Thus, statements of the form “IPv4 supports IPsec almost as well as IPv6 does” are correct.
- But when NATs *are* present in the path, IPv4 will not be able to support IPsec well. Although we expect NATs to be less important in the IPv6 infrastructure, IPv6 NATs are conceivable and, when actually present, they would also defeat support for IPsec.

Thus, the key issue is not so much IPv4 *vs* IPv6 *per se*, but rather classic IP (either v4 or v6 but without NATs in the path) vs NATted IP.

II.C. End User Applications

IPv6 provides somewhat better support for changing the address blocks assigned to a set of hosts and, thus, will improve the ease with which address assignment within a site can be maintained. This will result in eventual reduced operational costs and better performance for end hosts with more appropriate address assignments.

IP mobility is quite a bit cleaner in an IPv6 context than in an IPv4 context. The number of steps involved is similar, but once achieved the path is more direct than with IPv4. This will help improve end-to-end performance in mobile contexts and will also remove sources of instability in these mobile IP contexts.

The IP header in an IPv6 packet contains a flow field that can help provide improved support

QoS. There are many uncertainties here, however, and this advantage should not be overstated. The basic problems are common to both IPv4 and IPv6. Again, in either case, the presence of NATs would complicate deployment of QoS and thus this adds to the broader notion of transparent and globally addressable IP (whether v4 or v6) as far stronger than either in a NATted environment.

"some have argued that NATs will not preclude peer-to-peer devices and applications."
For any given such device or application, this statement might possibly be true. Generally, though, two patterns emerge:

- The value of the device or application is reduced, since its usefulness requires such a workaround, and
- The workaround generally involves adding yet another middlebox or proxy server, thus increasing the complexity and/or cost and also usually reducing the performance and robustness of the application.

Thus, while it's hard to argue a negative, the apology for NATs here is very weak. The specific problems mentioned will have the general effect of inhibiting the development and deployment and use of the devices and applications referred to.

II.D. Network Evolution

"... some observers have claimed that the increase in address space afforded by IPv6 is the only compelling reason for adopting the new protocol, not the availability of other capabilities. The task force seeks comment on this assertion."
Taken positively, this assertion is true. That is, without undercutting the value of the 'other capabilities' (such as somewhat stronger support for IPsec, IP mobility, address renumbering, and QoS), the deep value of permitting the Internet to grow while retaining the strengths of global addressability and end-to-end transparency at the core of the classic IP architecture must not be underestimated. The real issue is not IPv4 *vs* IPv6, but IP with transparency *vs* IP with NATs along almost all paths.

II.E. Other Benefits and Uses

"... does VoIP represent the kind of application that could drive IPv6 adoption, and if so, how? Will IPv6 improve the performance of VoIP?"
As with other points in section II, the issue is not IPv4 *vs* IPv6, but rather transparent IP *vs* NATted IP. With classic IP with end-to-end transparency and global addressability, SIP-based VoIP will be able to benefit from servers for the purpose of allowing users to identify and connect to each other, but then, when the actual voice packets begin to flow, those voice packets can go directly from source to destination without needing to go through an intermediate server. And, in this setting, once the voice packets begin to flow, any instability in that intermediate server will not cause the voice flow to fail. Thus, both performance and robustness will benefit. Again, this would be true for either IPv4 or IPv6, provided that no NATs are in the path between the two endpoints. But, of course, the widespread deployment of VoIP would require just the kind of massive increase in the number of IP devices that the limited 32-bit IPv4 address space cannot support. Thus, this becomes *de facto* a case for IPv6.

"We also seek comment on any spectrum management issues that might arise when IPv6-based wireless and hybrid networks are used to support mobile and fixed applications."

Without giving a complete answer (which would be beyond my scope of expertise), I would point out that VoIP using the IEEE 802.11b 'WiFi' protocols are being experimented on at least one Internet2 member campus, and experience with that will likely help us over time to judge the answers. Note that, even apart from any issues of VoIP, university campuses are ideal places for deploying 802.11b/g in support of laptop and PDA uses. As IPv6 support in these environments begins to emerge, it appears very likely that various forms of VoIP will be explored on our campuses.

Finally, it should be stressed that IPv6 is likely to be important internationally. Moreover, since our international colleagues, especially in the Asia/Pacific and the European regions, suffer from address shortage much more than we do, they are moving forward on IPv6 technology development and on IPv6 deployment at a vigorous rate. To the degree that strong IPv6 infrastructure, IPv6-based applications, and content reachable via IPv6 infrastructure is of value in the United States, this should motivate our work on IPv6. It should be noted, at least in passing, that IPv6 developers all over the world have benefitted greatly from IPv6 software development done overseas.

III. Cost of IPv6 Deployment and the Transition from IPv4 to IPv6

III.A. Cost of Deploying IPv6

III.A.1. Hardware Costs

We discuss, in turn, hosts, routers, and (layer two) switches.

- Host computers, be they laptops, large files servers, supercomputers, or PDAs, will naturally support both IPv4 and IPv6 once the appropriate operating software is deployed (*cf* II.A.2 below).
- High-end and mid-range routers of recent design almost always have excellent support. Although examples could be drawn from other vendors, it might be useful to note our experience with the upgrade of the Abilene backbone of Internet2 from 2.4 Gb/s to 10 Gb/s. Before deciding on which router to procure, we tested performance with identical tests for IPv4 and IPv6 traffic. To our surprise, we found that performance on the Juniper T-640 was excellent and in fact indistinguishable between v4 and v6. Ongoing performance testing within the now-operational 10-Gb/s Abilene backbone again shows excellent and indistinguishable performance in our specific tests which use gigabit Ethernet test hosts.
- The case for layer-two switches is even easier, since these devices are ignorant of the version of IP being used. The one problem area lies with multicast; some ethernet switches provide specific support for IPv4 multicast, and this will have to be extended to IPv6 multicast if this approach to multicast support is to be continued.

In sum, our hosts and switches support IPv6 with no upgrade required, and an increasing number of our routers naturally support IPv6 as those routers are replaced in the normal course of things with more modern models.

One key comment that relates specifically to the router market is that, in order to compete effectively in certain international markets, Cisco, Juniper, and others find that they must provide excellent support for IPv6. Once they do so, that excellent IPv6 support naturally shows up in routers delivered to the domestic market. One could, in fact, argue that IPv6 should be encouraged as a way of encouraging American vendors of routers to be competitive in

international markets where IPv6 will be even more heavily (or more obviously) motivated.

One current sticking point is the very inexpensive routers produced for the residential market. These currently seldom support IPv6, but it should be pointed out that these low-end routers require no special hardware to accelerate the forwarding of packets and thus, simple software upgrades for these low-end routers could easily support IPv6. Given the pressure of international markets, this will naturally happen over time.

III.A.2. Software Costs

The key requirement is for the operating systems of our hosts to support IPv6. In systems from technical (and cultural) worlds as different as Microsoft Windows XP and Debian Linux, users commonly find that, when upgrading to a current version of those systems, IPv6 support is simply present. Although it will take a few years for the maturity of IPv6 support in host operating systems to catch up with that now present for IPv4, there is very good reason to be confident in this respect. The comment above under II.A.1 about the international market applies here also.

For any given application program, it is usually very easy to port the application from IPv4 to IPv6. The socket libraries are extremely similar, for example. The biggest challenge is not the barrier to porting, but rather the low/moderate motivation for doing the porting, given the current IPv4 environment. And, once the porting is done, users generally are not even aware that it has happened. For ordinary applications, this story will likely play out at a moderate pace and keep ahead of requirements.

Two software issues warrant particular comment. First, the DNS (Domain Naming System) which maps from strings such as www.internet2.edu to numeric IP addresses, has eased support for IPv6 by allowing existing IPv4-based DNS servers to provide mappings both for IPv4 and for IPv6. Internet2 and EDUCAUSE are cooperating in a project to provide DNS servers that receive mapping requests using IPv6, and to include experimental support in IPv6 for the top-level .edu domain. We hope that this will lead to effective support, within the university community, for native IPv6 DNS support of broad deployment and high quality.

Second, the really key task is to encourage application developers to take their best ideas for applications that demand classic transparent (non-NAT) IP and to test them in an IPv6 environment. Stimulating such work would allow the community to better understand the specifics of what is at stake in IPv6.

III.A.3. Training Costs

Since May 2001, Internet2 has run a series of IPv6 Training Workshops to make our campus network engineers comfortable with supporting and using IPv6 in operational settings. We have found this task much easier than for native IP multicast, another important advanced network service. The concepts of addressing, routing, DNS, and the configuration of routers and hosts, are quite easy for technical staff already experienced with these issues in an IPv4 context. We are now curtailing this workshop series and are instead making our training materials available to our member universities to help them on their broader on-campus training.

III.A.4. Other Costs

As mentioned earlier, router vendors and operating system software vendors generally understand that, in order to be able to succeed in international markets (especially in the Asia-Pacific region), they must provide seamless and high-quality support for IPv6. Similar statements are likely true for the broader application software market.

More subtly, we probably suffer from the difficulty that applications innovators face when they perceive that NAT boxes may be prevalent in the Internet environment. This discourages vigorous experimentation and development of applications that would leverage IPv6's capability to support transparent networking among hosts. The resulting 'chicken and the egg' situation probably carries substantial costs.

III.B. Transition Costs and Considerations

III.B.1. Migration from IPv4 to IPv6 and the Coexistence of Dual Protocols

"The task force seeks comment on the costs and any other issues related ... to ... migration from IPv4 to IPv6."
This is serious issue and we will all learn as we go forward. As mentioned above, however, the strong similarity between IPv4 and IPv6 with respect to their addressing, routing, and other concepts ease training costs and also make coexistence not particularly burdensome. (This contrasts, for example, with the situation in the late 1980s when many university networks were running IPv4 and DECNET Phase IV in a similar dual-stack approach; the much weaker conceptual similarity caused operational difficulties.) Overall, I do not expect the burden to be severe.

During the period of coexistence, the following elements will be important. First, mundane applications such as email and web browsing will likely work well with email clients and web browsers ported to interact with both v4 and v6 servers. This will be almost invisible to users, who will seldom notice when their browser using IPv6 to interact with a particular web server.

Second, we foresee a period in which tunneling is used to connect IPv6-capable hosts with the IPv6 Internet over portions of the Internet that still support IPv4 only. This temporary period of perhaps several years will be more difficult operationally than the ongoing minor problems of running dual-stack. Fortunately, tunneling approaches with increasing ease of use and reliability are coming.

Third, within a few years, we expect the vast majority of campus LANs and hosts on those LANs to become IPv6-capable. During this period, users will gradually become aware of IPv6 and will gradually get to experience the innovative applications that work well except when transitioning NATs. As the request notes, islands of IPv4-only support will persist indefinitely.

Fourth, at some point, the motivation for continuing to support IPv4 will diminish. I would stress, however, that this will be many years and also that the nature and timing of this are highly uncertain. We should be prepared for a significant period of dual-stack use and operations.

III.B.2. Security in Transition

The period of dual-stack IPv4 *and* IPv6 networking will be an interesting one for network security. One trend in network security is to move away from reliance on 'perimeter firewalls' that protect machines 'inside' from the nastiness of machines 'outside' the firewall. One obvious problem with this perimeter firewall approach is the physical movement of laptops between inside and outside settings, often on a daily basis. The many forms of tunnel-based VPNs are another contributor to this. The emergence of dual-stack hosts will likely be yet another pressure on perimeter firewall approaches during transition.

It should be stressed, however, that security approaches that move beyond the perimeter firewall approach should work well in the IPv6 context, including in the dual-stack IPv4/IPv6 context.

III.B.3. Other Transition Concerns

One key point of technology uncertainty is that of evolving support within IPv6 for multihoming, as for example, when a given host receives two different IPv6 addresses, one from each of the two or more IPv6 ISPs that a campus might have. At the present, multihoming support is evolving and yet several of the registries are drawn to address allocation policies that assume that multihoming is a current reality. We expect that, until multihoming is sorted out, there will be a need for universities to receive provider-independent address prefixes from the registries. Supporting this while tracking the transition to multihoming will present challenges to these registries.

IV. Current Status of Domestic and International Deployment

IV.A. Appropriate Metrics to Measure Deployment

Identifying and applying appropriate metrics will be important and difficult. One suggestion would be to ask each major router and operating system vendor to track how many *IPv6 capable* system they ship (regardless of whether IPv6 is actually configured or used). I suspect that the majority of such boxes being shipped will soon by IPv6-capable.

It would be possible for Internet2 to support Commerce efforts to apply other very different kinds of metrics, such as the number of universities and perhaps hosts on university LANs, that are IPv6 capable. This would have two attractions:

- Given the communications between Internet2 and its member universities, it might be easy to do this tracking at relatively moderate cost, and
- Given that so many young adults are acquiring and evolving their style of using the Internet while they are students at our member universities and given that these young adults will likely be exposed to high-quality IPv6 infrastructure and applications while in college, tracking student usage might allow a kind of 'early warning' of the onset of new patterns of IPv6 deployment and usage and thus might allow relatively accurate projections of future deployment and use in the broader Internet.

Such a cooperative effort could be discussed.

IV.B. Private Sector and Government Deployment Efforts

The Internet2 networking infrastructure consists of the campus LANs of its (more than) 200

member universities, a national 10-Gb/s backbone called Abilene, and a set of gigaPoPs that connect these universities to Abilene.

Abilene itself has supported native IPv6 since summer 2002. As mentioned earlier, IPv6 performance with our current 10-Gb/s circuits and Juniper T-640 routers is excellent and indistinguishable from IPv4 performance in the same setting.

A increasing majority of our gigaPoPs now support dual-stack IPv4 and IPv6 connections to Abilene. The current state of this can be seen at the URL:
`http://abilene.internet2.edu/observatory/connection-technologies.html`
which shows a number of technical attributes of each direct physical connection to Abilene, including its presence or absence of support for IPv6.

More difficult at present is evaluating the degree of deployment within our university campuses. We believe that this is growing steadily and is limited primarily by demand and by the normal cycle of upgrading obsolete routers that do not support IPv6.

V. Government's Role in IPv6 Deployment

V.A. Need for Government Involvement in IPv6 Deployment

"The task force requests comment on whether a 'chicken and egg' problem exists that could hinder efficient deployment of IPv6"
To some degree, a chicken and egg problem surely does exist. The major problem is not the high cost of transition to (dual stack) support for IPv6, but rather than uncertainty among users and campus network managers over the nature, degree, and timeliness of benefit. On American university campuses, for example, the entire wired IPv4 campus LANs are almost purely NAT-free and thus support within IPv4 the kind of classic transparent environment that is generally only available with IPv6. The key current exception is the wireless 802.11 components of our campus LANs, in which NATs are often found.

Our current focus is on deployment and use within the university environment. Funding and other encouragement for the development of applications that will test the value of native (NAT-less) IPv6 would probably be the single greatest need. Absent clarity on this matter, the chicken and egg dynamic might be difficult to overcome in our particular setting.

V.B. Nature of Government Action

Strong cases can be made, I believe, for the following forms of government action.

Government as consumer. The leadership of the DoD in this area has been noted and is appreciated. Other examples of coordinated focused deployment by various government agencies might be very useful. The emphasis is not on simply stimulating the market for existing IPv6 products (though that would be somewhat helpful), but rather on working to clarify and explore the possible benefits of IPv6. Examples might be in SIP-based wired and wireless VoIP and messaging, perhaps in the context of civil defense developments.

Government support for research and development. (It should be noted that the existing Internet2/Abilene efforts mentioned in the request were not generally government funded.) The area of greatest need lies in exploring the applications story, particularly for direct host-

to-host native (non-NAT) IP infrastructure. Another area would be accelerating the maturing of IPv6 network software to lower the barrier for operating IPv6 networks and for ensuring that any temporary phase of immature IPv6 software does not create a security problem within the nascent IPv6 networking world. Accelerating technical development of multihoming and of such mundane network management tools as IP address renumbering would further lower barriers. Finally, investing in work on maturing and exploring the application of IPsec would yield benefits both for IPv6 and for the broad network security area.

Government funding of IPv6 deployment. Broader support for IPv6 within the federal networks that participate in the LSN Joint Engineering Team (JET) and focused attention on combining deployed IPv6 with improving security and network management would be very helpful. That said, most other forms of government funding of deployment seem to offer as much policy and practical difficulty as advantage. Possible exceptions might include support for training and for full inclusion of IPv6 within the DNS (including support for DNSset).

Government IPv6 mandates. As one who lived through the late 1980s and early 1990s GOSIP debacle, I am reluctant to suggest mandates. The 'government as consumer' approach in which the benefits of IPsec, end-to-end transparency, and mobility are leveraged in support of agency needs, might have many of the advantages of mandate with few of the problems.

Weaving these forms appropriately would have a solid and very positive effect.

Internet2 would welcome the opportunity to engage with your task force on any of these issues. As shown in this letter, the interests that we have in promoting a cost-effective very-high performance network infrastructure extending to the (IPv4 and IPv6) networks that connect our universities to universities internationally, combined with our abilities in introducing advanced network technology within the U.S. university environment, will allow us to contribute to government activities in this arena.