DEPARTMENT OF COMMERCE

National Institute of Standards and Technology
National Telecommunications and Information Administration

Docket No. 040107006-4006-01

Request for Comments on Deployment of Internet Protocol, Version 6

BellSouth Response

March 5, 2004

Contact Information:

Robert Wright
bob.wright@bellsouth.com
404-986-0748

Cristin Flynn
cristin.flynn@bellsouth.com
703-607-4918

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
National Telecommunications and Information Administration

I. Summary

BellSouth supports further evaluation, planning, and testing which will lead to the deployment of IPv6 into our nation's networks. The adoption of IPv6 will be an important step towards building an Internet for the future. IPv6 will provide address space for millions of future devices that are likely to require connectivity to the Internet, and will spur innovation and development of new applications and services that ride on the IPv6 platform.

BellSouth encourages the United States to provide incentives that promote development of new IPv6 based applications and incentives that encourage transition to network infrastructures which support IPv6. We expect that the technical and economic benefits of IPv6 will begin to have an impact in 2006 and that these impacts will grow so that wide spread support for IPv6 will be required in the 5-10 year timeframe. While limited deployment will occur prior to 2006, the interim focus of incentives should encourage analysis, testing and planning initiatives to ensure that networks remain secure and stable during the transition to IPv6 and that the U.S. vendors and service providers are positioned to expedite IPv6 transition plans if market conditions change.

Security and stability of the existing network must be a fundamental requirement of the transition. During the transition period, IPv4 and IPv6 will coexist. The resultant increase in complexity reinforces the need to ensure adequate time and effort is allocated to planning and testing phases of the transition. Incentives should be provided for service providers to take allotments of IPv6 addresses, begin testing, and gain operational experience.

Specific attention should be given to both the technical and non-technical issues for establishing trust models and developing a Public Key Infrastructure (PKI) that is capable of supporting security in widespread IPv6 deployment. An effective PKI infrastructure is required so that the IPsec security capabilities, already optional in IPv4, can be efficiently utilized. A robust PKI infrastructure would also provide significant benefits for security and commercial applications in many areas other than just IPv6.

Existing IPv4 protocol extensions, such as Network Address Translation (NAT), may continue to persist and provide benefits in IPv6 environments, so the future role of these extensions should be analyzed and enhanced as appropriate.

While we encourage government support for IPv6 transition planning initiatives, market forces, and not government intervention, should be the primary driving force for actual deployment of IPv6 infrastructure. Government intervention could result in unwarranted costs and inefficiencies that would outweigh potential benefits.

II. Potential Benefits and Uses of IPv6

Increased Address Space

Network Address Translation (NAT) protocol, Classless Inter-Domain Routing (CIDR) and Dynamic Host Configuration Protocol (DHCP) have all slowed the consumption of IPv4 addresses. Some industry analyses indicate that the IPv4 address space could last up to 20 years if there are no significant changes in the slope of the deployment curve as a result of new applications, technology innovations, or changes in the distribution methods for IPv4 address blocks.

BellSouth expects the development of mobile applications and applications that are not easily made compatible with NAT and DHCP will change the slope of the deployment curve to a degree that may require the wide spread support of IPv6 addressing within 5-10 years. There are several applications that can benefit from the future deployment of IPv6 and its enhancements revolving around third generation cell phone and telecommunication products. The most significant and obvious benefits would be the increased IP addressable space, opportunities to implement quality of service in new ways, and potential security enhancements. The IPv6 Hierarchical Address Space will support the predicted increase in the number of network connected products per individual. It will also provide stateless address auto-configuration and allow a device to get an IPv6 address associated with its location. These capabilities will allow for seamless interoperability between service providers. IPv6 will also simplify the initial host configuration and the process of renumbering.

As an interim measure until the increased address space of IPv6 becomes available, NAT technology has been deployed widely. NAT is often criticized as presenting inherent incompatibility problems, even though the technology reduces problems caused by shortages of IPv4 addresses. Yet methods to enhance NAT or provide work-arounds that reduce associated addressing and compatibility limitations are possible. These cannot provide the same "flat" addressability that IPv6 promises, but nevertheless might be employed in particular circumstances and could be enhanced over time to reduce the immediate need for IPv6. Applications which exhibit incompatibility with NAT might be accommodated in this manner to some significant degree. Such approaches should be more fully investigated, and the possibility of future applications being developed which provide NAT compatibility (rather than assuming NAT is a temporary problem to be ignored) should be explored for practical reasons.

Regarding NAT's being potential choke points, NAT's are orthogonal to "single point's of failure," similar to the case of routers or firewalls. Just as routers or firewalls can be implemented singly, resulting in a potential single point of failure, NATs can be implemented singly. However, where reliability is important it is better practice to implement routers (or firewalls) in a dual-failover fashion, where one router (or firewall) is a hot backup for the other "active" router (or firewall) in the pair, such that the single point of failure is eliminated. In fact, NAT is often performed by a router or firewall. Stateful failover to a backup router or firewall can be arranged where needed. Dual redundant network elements, however, do add to cost and are therefore not used unless needed. Whether or not a single point of failure is present is a matter of choice, not a result of using NAT (or firewalls, or routers).

Purported Security Improvements

IPsec is available in IPv6 by design, rather than as an IPv4 add-on. However, availability is not equivalent to usage. It may be that the security impact of IPv6 versus IPv4 is neutral. There seems to be no significant functional difference between IPsec used with IPv4 and IPsec used with IPv6.

From a theoretical perspective, it is unlikely that IPsec will be easier to use with IPv6 than it is with IPv4. However, IPsec has experienced practical growing pains including lack of compatibility between vendors and difficulty of key management. Incorporating IPsec into the IPv6 stack should significantly reduce (although probably not eliminate) incompatibility problems. The degree to which incompatibility would be improved needs further study.

Regarding difficulty of key management, manually configuring IPsec is suitable for small roll-outs, but problematic for large scale deployments. IPsec can easily be used in very limited specific cases. IPsec is much more difficult to use and support for wide scale deployment because of administrative overhead required to configure and manage keys. This administrative overhead can be reduced if other technologies, such as a viable Public Key Infrastructure (PKI) are available.

It is likely that IPsec implementation will have a significant dependence on the development of workable trust models that facilitate PKI. Currently IPsec is readily deployable in a limited sense, but disproportionately more costly and difficult to use as the scale increases. An effective PKI infrastructure is required so that the IPsec security capabilities, already optional in IPv4, can be efficiently utilized. Because PKI supports authentication, encryption, and non-repudiation, it provides fundamental capabilities and significant benefits for security and commercial application in many areas other than just IPv6. Notably, a well-designed PKI can help reduce the security risks of relying entirely on provisioning of static keys.

The availability of a Public Key Infrastructure would promote the deployment of IPv6. However, the social and business aspects of establishing identities and trust relationships must also be addressed. These social and business issues include privacy, and legal considerations which will be more difficult to resolve than the pure technical issues.

Even if IPsec is widely used, NAT is likely to continue to be desired by many. Since IPsec and NAT tend to be incompatible, problems are likely to occur. NAT has already been chosen and deployed widely, and there is no certainty whether NAT usage will decrease, increase, or remain steady over time. Many NAT users will not wish to expose their private addresses, regardless of the availability of IPsec. It is difficult to see IPsec adoption ever leading to the “elimination” of NAT, even though some may prefer that this would occur. To a large degree, whether the existence of NAT has caused the problem or whether the continued design of protocols known to be incompatible with widely deployed NAT has caused the problem is a philosophical matter. In any event, it is by no means determined that NAT usage can be eliminated.

It is true that widespread use of IPsec could make IP address manipulation by third parties less likely by authenticating IP addresses at the source (via AH or the authentication functionality included in ESP). However, address manipulation of packets in transit would still be possible where IPsec is not used. More to the point, a determined user could still arrange to generate packets with spoofed addresses prior to IPsec AH/ESP authentication being applied to those packets on their computer. And since IPsec is not a cost-less solution, it is unlikely to be desired everywhere. If IPsec were ever mandated, costs and incompatibilities would be problematic. Regardless, this issue is largely independent of IPv6 versus IPv4, since IPsec is available for both (optionally for IPv4, and by design for IPv6), and a determined user would still be able to write spoofed addresses into their own packets even if IPsec were used. Therefore it is difficult to see how IPv6 or IPsec could strictly eliminate spoofing.

Network “traceability” is somewhat separable from spoofing. That is, there are other potential ways of tracing communications than by IP address alone. Even though address spoofing cannot be entirely precluded, formation of IPsec VPNs could indirectly aid network traceability when that formation is predicated on the use of shared secrets or distributed certificates, which themselves can be associated with specific entities or persons (as long as these secrets shared are sufficiently unique and are not stolen). This increase in traceability would result from the distribution and management of those shared secrets or certificates, however, rather than from the AH or ESP capabilities of IPsec. IPsec could become a method of utilizing the shared secrets or certificates to this end, as opposed to directly / inherently generating the increased traceability. This would support the need for development of an effective PKI and associated trust models in order to facilitate the aforementioned distribution and management.

End User Applications

While it may be true that the original philosophical vision of the Internet included allowing peer-to-peer addressability, private addresses and NAT have been widely deployed without concern for this original philosophy. Considerable effort and difficulty would therefore be encountered in any effort to return the Internet to this original philosophy. A change of this sort would be quite costly. Furthermore, many users and enterprises do not care about the original philosophy, such that it is not a driving issue worthy of expending scarce resources. Instead they merely want peer-to-peer applications to work. Enabling these applications to work does not require returning the Internet to the originally envisioned philosophy, but instead can be achieved by work-arounds and incremental designs and implementations that are considerably more manageable and affordable. In some respects middleboxes may run counter to the original Internet design philosophy, but it is debatable whether or not the existence and use of middleboxes must interfere with peer-to-peer applications inherently. It is certainly true, however, that efforts to ensure compatibility are required to prevent such interference.

Since security is important, firewalls, intrusion detection systems and other security middleboxes are unlikely to disappear. Over time, history shows that middleboxes can be made compatible with peer-to-peer applications. Initially, peer-to-peer VoIP applications using protocols such as H.323 and SIP would not work with firewalls, particularly firewalls employing NAT. Over a time period of 2-3 years, these incompatibilities have to large degree been addressed, indicating that satisfactory results are obtainable. Middleboxes will certainly persist and are likely to become even more widespread in type and number, regardless of whether IPv6 is adopted or not.

Network Evolution and Other Benefits

It is agreed by many that the only IPv6 advantage that cannot be effectively duplicated (except partially via NAT) in the IPv4 space is the additional addresses provided.

Whether or not IPv6 would be advantageous in terms of smaller header sizes (e.g., for applications such as VoIP), or whether optional headers would result in increased overhead, should be investigated in more detail considering specific implementations and architectures. All associated communications streams should be included, such as TCP plus RTCP/UDP plus RTP/UDP in the case of VoIP.

Some say BGP is already overloaded so trying to secure it will be the straw that breaks the camel’s back. Others want to extend it regardless of those concerns. There is an opportunity to build in secure BGP for IPv6 before the load grows to the point it becomes operationally complex to do so.

Software routing of IPv6 has not received the level of performance optimization as IPv4 routing. Hardware routing is still being added to many vendors capabilities, but the equipment capabilities are expected to be resolvable through deployment experience. Many vendors are already incorporating support for IPv6. This includes a number of major firewall and router vendors. However, two potential concerns require consideration. First, assuring compatibility necessitates costly testing especially when integrating multiple products to form network and service architectures. Secondly, performance is key. Software routing of IPv6 is too slow. Hardware routing is being added on various vendor roadmaps. While software implementation of IPv6 may be sufficient at the edges, hardware processing of IPv6 is needed in the network to reduce unacceptable congestion and latency.

Service providers are driven by the demands of their customers. A likely scenario for service providers to evolve to IPv6 would assume sufficient deployment of IPv6 applications in the consumer space to create demand for networked IPv6 services. Such applications would need to provide sufficient value for consumer adoption without WAN IPv6 capabilities, but still be enhanced by the availability of such WAN services. An application involving the ad hoc networking of consumer electronic devices may provide such a driver. Given the paucity of infrastructure for connectivity and the inconvenience of cabling in such environments, wireless technologies may predominate. Predicting the commercial availability and market success of wireless IPv6 enabled consumer electronics devices is somewhat speculative. While networked consumer electronics goods are emerging currently, the current generation typically assumes a wired infrastructure. Wireless technologies such as Bluetooth and UWB promise significant improvements by reducing cabling requirements but introduce additional operational issues in terms of device compatibility and auto-configuration that may be resolved by the 2006 timeframe. The development of appropriate energy sources (improved batteries, energy scavenging systems, etc) will influence the rate of deployment for portable personal consumer electronics devices and is harder to predict.

It is important to note that technical means are available in IPv4 to allow addressing devices within private address spaces (hidden behind NATs) and these means can potentially be improved and enhanced. Typically these approaches take the form of private-address endpoints registering in some fashion with an “address server” outside the NAT, with entities wishing to connect to a private-address endpoint obtaining addressability through the NAT to that otherwise hidden endpoint by first consulting (and optionally authenticating to) that server. Further investigation would be required to fully understand the possibilities, true limitations, possible advantages, and applicability of such methods in lieu of IPv6.

Availability of the technology is only one aspect. For these to be a successful driver of IPv6 deployment would require appropriate marketing and product concepts. It is not clear that the consumer electronics market space would necessarily align with the IPv6 in the same timeframe.

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

Hardware, Software, and Training

Because the security and stability of the communications infrastructure is vital to the U.S. economy, training and testing costs for transition to IPv6 are likely to be very significant. These costs would be highest in an expedited deployment scenario. Costs would be lower in a gradual migration scenario where the much of the testing and problem resolution can be completed over a period of time or through shared initiatives, possibly facilitated by the federal government. For U.S. providers, costs would also be lower in a scenario where the early deployment issues are encountered and resolved in foreign countries.

Except at endpoints, hardware would likely need to be replaced and infrastructure software would need to be upgraded in order to maintain acceptable performance. In addition, there will be requirements to upgrade management software to enable IPv6 compatibility and support. Element Management Systems, Network Management Systems, and Operations Support Systems may all require upgrades and the costs may be significant. The replacement or upgrade costs for hardware, infrastructure software and management software would be highest in an expedited deployment scenario. The costs would be lower in a gradual migration where IPv6 capable components would be deployed as part of normal infrastructure upgrades and replacements.

Opportunity costs of waiting to deploy IPv6 are currently undefined and require further consideration.

Transition Costs and Considerations

Transition costs are thought to be considerable but require further investigation. Incompatibilities, bugs, and increased complexity leading to security problems are just a few of the difficulties expected to increase costs.

Multiple transition mechanisms may have to be employed in different scenarios / services, further increasing cost and effort. In many cases during the transition, IPv6 may be tunneled through IPv4. This will enable IPv6 applications to adequately communicate through selected existing IPv4 infrastructure, with resultant cost efficiencies. This scenario will have potential opportunity/capability limitations, all of which will require consideration, because it will not be possible to utilize IPv6 features in that “core” network tunnel. Due to cost issues and other reasons, this scenario may be exist for a period of time, but the ultimate goal must be a pure infrastructure, so that IPv6 capabilities will be accessible throughout the network.

The transition period may be lengthy, additionally increasing costs in the aggregate. It may be preferable to incur some costs relatively early while delaying other costs until the “switchover” point (or the point at which gradually-included IPv6 capabilities are actually enabled) is closer. Absent a facilitative environment, however, costs and efforts may be delayed until unequivocally required, possibly resulting in inefficiencies that will amplify total costs nationally.

The transition is likely to include an increased number of exploitable flaws, resulting in security problems. Additional efforts will be required to deal with these, but currently the extent of those efforts and the associated costs are undefined pending further investigation.

IV. Current Status of Domestic and International Deployment

Metrics should be developed to provide insight into the following areas:

1. Deployed IPv6 capability
2. IPv6 traffic volume
3. Availability of applications that derive significant benefits from the IPv6 protocol,
4. Availability of applications that cannot be made to function over enhanced IPv4,
5. Stability of the IPv6 protocol

Metrics for deployed capability could be based on percent of units shipped as well as on the percentage of the currently deployed infrastructure that is IPv6 enabled. These metrics should allow granular analysis based on the type of infrastructure, e.g. edge, middlebox, or core. It may also be beneficial to allow analysis by the domain in which the infrastructure is deployed, e.g. telecommunications service provider, corporate entity, educational entity, or government.

Traffic volume metrics are required because of the IPv6 capable infrastructure will not initially be configured to transport IPv6 traffic. Volume metrics should include sufficient granularity to enable analysis of IPv6 traffic volumes flowing from edge devices to core Internet backbone devices, IPv6 traffic flowing through core, and IPv6 traffic flowing to/from international destinations.

Application metrics should include information about the number of applications, either deployed or in the development pipeline, which would derive significant benefit from IPv6. Of particular interest would be applications which cannot co-exist with IPv4, even when enhanced to provide work-arounds for NAT incompatibility and addressability limitations.

Finally, it is important to develop metrics that reflect the stability of the IPv6 infrastructure. Such metrics would include the number of outages, security vulnerabilities, alerts, and patches that associated with the deployment of IPv6 enabled components.

V. Government's Role in IPv6 Deployment

It is likely that, at least in approximation, IPv4 and IPv6 are direct substitutes when work-arounds and add-ons such as widely deployed NAT are considered. It may be that only in cases where new services could not be provided using IPv4 in a relatively timely and cost-effective fashion would IPv6 be considered to be “building on” IPv4 to provide added capabilities of actual significance.

There may be cases where certain additional features of IPv6 could enable new services and features that would benefit security and better achieve objectives, for instance in some emergency or battlefield situations. However, the real question may be whether IPv6 is actually needed to enable these cases, or whether IPv4 (possibly with add-ons such as NAT, enhanced NAT, or other mechanisms, protocols, or approaches) would likewise be sufficient. Just because IPv6 has a feature which could be used in a particular manner to enable other desirable functions does not mean IPv6 is needed or even desirable given the associated difficulties, costs, etc. Unless IPv4 is a limiting factor even when considering reasonable add-ons or work-arounds, IPv6 features may be nice but not necessary.

In particular regarding security, simplicity is security's friend while complexity is not. Although for some scenarios IPv6 may be a more elegant approach in certain respects (compared to IPv4 with NAT, etc.), actual implementation might result in increased complexity that could negatively impact security. This might be true, for instance, where IPv6 and IPv4 were still required to co-exist, in which cases an IPv4 approach (even with add-ons as necessary) might be preferable. Additionally, if an "IPv6 approach" is meant to preclude middleboxes such as firewalls and IDS, which are central to most security implementations, then security would need to be re-examined in detail and security mechanism of equivalent effectiveness would need to be used. While providing packet authentication and encryption, it is unlikely that IPsec in itself can serve as an effective substitute for security best practices that incorporate firewalls and other layered defense-in-depth.

As set forth above, there are few market drivers for migration to IPv6 at the current time. Address space in the Domain Name System is predicted to last until 2010, providing a target date by which migration to IPv6 must be complete. As the IPv6 Forum recently noted, migration to v6 will be a process, and something that will not occur in an overnight, Y2K-like circumstance. (FN: IPv6 Forum, "IPv6: An Internet Evolution", at 4 (http://www.ipv6forum.com/navbar/papers/IPv6-an-Internet-Evolution.pdf). However, IPv6 remains a critical component for the Internet's coming of age, and that is scalability with the ability to incorporate millions, and potentially billions, of IP-enabled devices into the interconnected networks that comprise the Internet. The US Government plays a unique role in the ability to drive change and innovation; not through regulation, but through incentives, customer contracting and product demands.

Nature of Government Action

The two most obvious options for government action are (1) the promotion of research and development; and (2) use of the government procurement processes. The Federal Government should encourage industry to develop IPv6 based applications and network enhancements. To the extent that market drivers are insufficient to promote innovation at an acceptable pace, the Federal Government can consider the grant process through the National Science Foundation (NSF) or the National Institute of Standards and Technology (NIST) to develop IPv6 based applications. The Federal Government can also work with educational Centers of Excellence to encourage further research and development of IPv6 based applications and network enhancements.

The Federal Government should consider its ability to be a demand driver through the government contracting process. Government contracting provides a useful tool to promote market demand for IPv6 infrastructure and IPv6 based applications. To the extent that the Federal government needs large IP address blocks or has applications that require use of IPSec, then IPv6 should be a consideration.

As noted above, the Federal government should use the contracting process once IPv6 based products and applications are available that add clear benefit to the needs of the Federal government. The Federal government should refrain from requiring use of IPv6 until market forces clearly support such action. As noted above, address space in IPv4 will not be threatened for several more years. Companies will not migrate to IPv6 unless capital expenditures allow for applicable equipment upgrades or network management, network security, or customer demands require migration. The Federal government should not force unnatural network migration, but should remain technology neutral, and encourage Internet Service Providers to consider IPv6 as soon as feasible.

Recognizing the market based challenges that impede IPv6 deployment, Japan and the European Commission have both taken steps to facilitate IPv6. As a part of the eEurope initiative, the European Commission is encouraging migration to IPv6 and provides financial support to Euro6IX and 6Net, two pan-European IPv6 networks. The Japanese government provides tax incentives to manufacturers and network operators. The "e-Japan Initiative" encourages first to market products and facilitates IPv6 deployment.

Tax incentives should be offered to encourage continued IPv6 research and to support IPv6 planning, testing, analysis, and possibly even participation in IPv6 standards efforts and consortia e.g. Internet 2/ 6Bone. Examples of specific areas for IPv6 research include:

- techniques to improve the relative performance and efficiency of IPv6 compared to IPv4, especially for key applications such as VoIP;
- performance in dual IPv4/IPv6 environment, including inter-working and mapping;
- techniques for implementing and managing IPv4/IPv6 coexistence and transition;
- security in dual IPv4/IPv6 environments;
- intrusion detection techniques for IPv6 environments, including the implications of changes in the use of tunneling and NAT;
- privacy implications of IPv6, including the reduced use of NAT in home premises LAN networks;
- best practice techniques for configuring and managing critical security components such as firewalls in IPv6 and IPv4/IPv6 environments;
- PKI scalability and trust models;
- secure BGP implementations.

Because IPv6 address allocation policies are more restrictive, incentives should be provided so that operators will take allotments of IPv6 addresses and gain operational experience. These incentives could be accomplished by publishing guidance that specific IPv6 pre-deployment activities qualify for the Research and Experimentation Tax Credit. Encouraging these types of pre-deployment work will help ensure a faster, more stable transition when business and economic drivers emerge.

To the extent that the pace of IPv6 deployment is a concern to the Federal government, tax incentives can also be offered to companies that run IPv6 in their networks. Tax incentives can encourage companies to expedite an IPv6 deployment strategy. For example, a tiered incentive program could be offered, such that companies that run IPv4 and provide IPv6 through tunneling, a higher separate incentive to companies that initiate a "dual stack" IPv4 and IPv6 operation, and the highest incentive to a company that migrates to full adoption of IPv6.

IPv6 deployment mandates should be avoided at all costs. As noted by the IPv6 Forum, the United States is not currently in a Y2K like environment, in which networks can suffer actual damage for failure to make necessary changes. IPv6 will be an enhancement to a growing and changing network environment. Given the state of the telecommunications industry and decreased spending on network build-outs, it would create additional stress on the industry to have to comply with an IPv6 deployment requirement. Such a requirement would add significant cost and overhead to many companies, but with little opportunity to recoup the cost of deployment or reap any significant benefit of network management or security. Innovation will come, and wireless devices and new applications will increase the demand for address space and other features that IPv6 will provide. However, IPv6 should not be developed unnaturally, and in a vacuum. Accordingly, the Federal government should refrain from establishing any IPv6 mandates, and continue to encourage innovation in the marketplace as the most effective and efficient demand driver.