Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	**)**	
	)	
Deployment of Internet Protocol,	**)**	
Version 6	**)**	
	)	
Request for Comments by the	**)**	**Docket No.**
National Telecommunications and	**)**	**040107006-4006-01**
Information Administration and by the	**)**	
National Institute of Standards and	**)**	
Technology	**)**	
	)	

COMMENTS OF SPRINT CORPORATION

Sprint Corporation ("Sprint") hereby respectfully submits its comments on the *Notice of Inquiry* issued jointly by the National Telecommunications and Information Administration ("NTIA") and the National Institute of Standards and Technology ("NIST") in the above-captioned docket, 69 F.R. 2890 (January 21, 2004). NTIA/NIST have asked parties for their views on a number of issues "implicated by the deployment of Internet Protocol version 6 ("IPv6") in the United States." *Id.* Sprint addresses *seriatim* below various issues discussed in the *Notice*.

I. Background

The Internet is built on the foundation of the TCP/IP (Transport Control Protocol/Internet Protocol) protocol suite.[1] Although "[t]he current generation of IP, version 4 (IPv4) has been in use for more than twenty years, and has supported the Internet's phenomenal growth over the last decade," 69 F.R. 2890, in the early 1990s various Internet stakeholders began to recognize the possibility that the IPv4 address and routing functions would, at some point in the not so distant future, no longer be able to accommodate the Internet's continued growth. Indeed, the Internet Engineering Task Force's (IETF) Address Lifetime Expectations (ALE) working group estimated that IPv4 address space exhaustion could occur as early as 2005 and even earlier if the Internet found a "killer application." The IETF formed a sub-group to explore and specify an IP Next Generation (IPng) protocol. IPv6, as IPng is officially called, was recommended in July 1994 and made a Proposed Standard in November 1994.[2] IPv6 is an evolutionary step from IPv4 and is designed as a long term solution to the severe addressing and routing problems that have developed with IPv4. IPv6 is also designed to improve upon other features in IPv4 as well as add new features that the Internet will need in foreseeable future.

Sprint has, since 1997, been actively involved in the standardization, testing, and deployment of IPv6. Sprint was an earlier adopter of IPv6 in an experimental stance, and not only keeps an active test-bed for IPv6, but is involved in the evolution and standardization of the protocol.

II. Potential Benefits and Uses of IPv6

[1] It is highly likely that the original designers and developers of the TCP/IP protocol suite did not envisioned that the Internet would become such a critical resource to government, industry and the general public. It is also unlikely that they anticipated that usage of the Internet would grow exponentially.

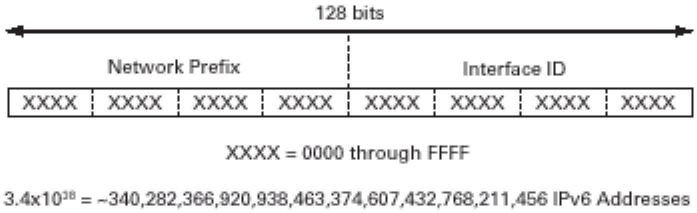
[2] The recommendation is documented in RFC 1752.

A. Increased Address Space

The primary reason for developing the next generation Internet Protocol was the expected address exhaustion of IPv4. Each address must uniquely identify a particular host interface and provide enough information to route the packet from anywhere on the network to that interface. The version 4 packet header includes a 32-bit address field, providing approximately 4.3 billion unique bit combinations, with useable addresses divided into three classifications: 126 class-A networks, each of which can support about 16.8 million unique addresses; 16,382 class-B networks, each of which can each support 56,535 addresses; and 2 million class-C networks, each of which can support 254 hosts. The remaining addresses are reserved for other uses, decreasing the theoretical limit to about 3.7 billion addresses.

The availability of an almost unlimited number of IP addresses is the most compelling benefit of implementing IPv6 networks. Compared to IPv4, IPv6 increases the number of address bits by a factor of 4, from 32 bits to 128 bits. The 128 bits provide approximately $3.4x10^{38}$ addressable nodes, enough to allocate about 1030 addresses to every person on this planet. Figure 1 shows the general format of an IPv6 address.

Figure 1: IPv6 Address Format



The ability to provide a unique address for each network device enables end-to-end reachability, which is especially important for residential IP telephony. IPv6 also provides full support for application protocols without requiring special processing at the edges of the networks, eliminating the problems associated with Network Address Translation ("NAT").

Perhaps the only problem with the IPv6 protocol is that its implementation schedule has always been uncertain. Thus, the industry has had to develop interim solutions to extend the lifetime of the fixed 32-bit IPv4 address space. A collection of solutions, including tighter policies on network allocation, reclaiming allocated but unassigned addresses, Classless Interdomain Routing (CIDR), and NAT have been utilized.[3]

Collectively, these new policies and protocols push the practical limit of the address space substantially higher. For example, NAT breaks the theoretical limit of 3.7 billion, by allowing a single public address to be used by multiple hosts.[4] This technique allows a NAT to act as a router between addresses that are known only to the internal organization and valid public addresses. The dynamic allocation of Internet addresses to internal host packets allows an entire network to be supported by a handful of addresses, or potentially a single address. By using unique transport layer identities, each session between an internal and external host can be identified and properly routed, without additional configuration on either end of the communication. A widespread implementation of this technique would virtually remove the theoretical bounds of the 32-bit IPv4 address space.

NAT, however, is not without limitation. Many view address translation as a poor solution to the addressing problem because the Internet Protocol was designed to carry packets from source to destination (end to end). Protocols, application software, and routers have been designed around

[3] CIDR ties contiguous networks of a single class together, thereby allowing for the routing of multiple adjacent networks by a single network prefix. The reverse is also true. A large network, such as a class A, could be split. Each portion could then be assigned to multiple entities who, in turn, would use the final bits of the network to uniquely identify their sub-networks. Unfortunately, this slightly complicates packet routing and increases routing table size, with core nodes already handling high numbers of entries. The network portion of the address, which used to be implicitly known by the class, would have to be explicitly specified as a network mask.

[4] Although RFC 1631 proposed the idea of NAT in 1994, its implementation on a wide scale is a recent development and is a direct result of the "address crunch."

this fundamental principal, and thus the use of NAT may require an Application Layer Gateway ("ALG") for processing. Moreover, some security models require addresses and ports to remain unmodified and others, *e.g.,* those using upper-layer encryption explicitly prevent modification from occurring. One or more translation that servers the route between the source and destination host potentially creates problems, the scope of which is not fully known.

B. Security Benefits

The authentication header ("AH") and encapsulated security payload ("ESP") are the security mechanisms of the Internet protocol security architecture. The IP security mechanisms, AH and ESP provide for authentication, integrity and confidentiality. The AH and ESP are defined for both IPv6 and IPv4. However, while implementation of these security mechanisms is mandatory for IPv6, it is optional for IPv4.

The "IPv6 Authentication Header," is an extension header that provides authentication and integrity to IP datagrams, thereby ensuring that the sender and receiver are who they claim to be. While the authentication header design calls for it to be algorithm-independent and to support many different authentication techniques, the use of MD5 is proposed to help ensure interoperability within the worldwide Internet.[5] The MD5 value is entered into the authentication header at the source assuring that the packet was sent by the originating source. If an intermediary were to modify the packet in route to its destination, the destination would receive an error message stating that the value of the MD5 and the packet's content do not match. This eliminates a significant portion of network attacks, including host masquerading attacks.

[5] MD5 is the latest in a series of techniques in which the function takes an arbitrary-length message and transforms it into a fixed-length quantity. MD stands for message digest, which is simply a hash function.

Of course the use of authentication, integrity and encryption adds to IP processing costs and increases communication latency. Nonetheless, the availability of security services for end-use and infrastructure protection is worth the cost.

IP security is a requirement of the IETF's specification for IPv6. It is an enhancement to the Internet Protocol that provides encryption and authentication at the transport layer (layer 3 of the OSI model). Users are generally unaware of the function that IP security performs throughout the network, including the fact that the IP security functionality is tunneling their data through insecure networks.

IP security works with IPv6 extension headers. The authentication header, AH, the encapsulation security payload header, ESP, and the Internet key exchange, IKE, perform the authentication, encapsulation, encryption and functions collectively or individually. It is possible to only use only authentication by adding the AH header. While this does not protect the data with encryption, it does use less overhead and therefore the entire process is faster. The authentication header will protect the entire packet even the part before the AH header by verifying that the sender is who he says he is.

C. End User Applications

1. Mobile IPv6

IP mobility is also a standardized part of IPv6. In Mobile IPv6, each mobile node is identified with a static home address, independent of its current point of attachment to the Internet. The home address is stored by the Home Agent ("HA") router in the home network. When the mobile node is attached to a foreign link, it is addressable by a "care of address," in addition to its home address. There may be several care of addresses defined for the mobile node, but only one, the primary care of address, is bound to a specific home address at any one time.

The care of address provides information about the mobile node's current location. The mapping or association between the current care of address and the home address is called "binding."

Although IPv4 provides for IP mobility, IPv6 provides enhanced support for such mobility. Moreover Mobile IPv4 is not deployed widely enough to satisfy current mobility needs. And, a shortage of globally routable IPv4 addresses and the use of private IPv4 addresses with NATs hamper Mobile IPv4 deployment in many cases. The benefits of Mobile IPv6 compared to Mobile IPv4 include:

- The huge address space of IPv6 makes Mobile IPv6 deployment more straightforward.
- IPv6 address auto-configuration simplifies the care of address assignment for the mobile node. It also eases the address management in a large network infrastructure.
- Optimized routing: Mobile IPv6 avoids so-called triangular routing of packets from a correspondent node to the mobile node via the Home Agent. This reduces transport delay and saves network capacity.
- No need for foreign agents with Mobile IPv6.
- Uses IP Security for all security requirements.

Implementing application layer Mobile IPv6 in 2G and 3G mobile networks primarily requires application layer IPv6 support from the network, the installation of a Home Agent (HA) router in the home network, the use of mobile terminals supporting Mobile IPv6 and the implementation of IP security. Further, Mobile IPv6 is a highly feasible mechanism for implementing static IPv6 addressing for mobile terminals. In this case, the Mobile IPv6 home address is the static address and the mobile node can always be reached using the same globally unique IPv6 address, independent of its current location. Many applications and services, such as Push-To-Talk, need static IP addresses/static user identity.

Mobile IPv6 is also a promising technology that complements the link layer (layer 2) mobility in CDMA mobile networks. Mobile IPv6 can handle the mobility management in multi-access networks (*e.g.* a network with WCDMA and WLAN coverage using multi-mode mobile terminals supporting both technologies).

2. IPv6 address auto-configuration

IPv6 address auto-configuration is a highly useful feature of IPv6. This feature allows for the address to configure itself automatically, thereby eliminating the need for use of a stateful configuration protocol, such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6). By default, an IPv6 host can configure a link-local address for each interface. By using router discovery, a host can also determine the addresses of routers, additional addresses, and other configuration parameters. Included in the Router Advertisement message is an indication of whether a stateful address configuration protocol should be used.

Address auto-configuration can only be performed on multicast-capable interfaces. Address auto-configuration is described in RFC 2462, "IPv6 Stateless Address Auto-configuration." There are three types of auto-configuration:

1. Stateless: Configuration of addresses is based on the receipt of Router Advertisement messages. These messages include stateless address prefixes and require that hosts not use a stateful address configuration protocol.

2. Stateful: Configuration is based on the use of a stateful address configuration protocol, such as DHCPv6, to obtain addresses and other configuration options. A host uses stateful address configuration when it receives Router Advertisement messages that do not include address prefixes and that require the host use a stateful address configuration protocol. A host will also use a stateful address configuration protocol when there are no routers present on the local link.

3. Both: Configuration is based on receipt of Router Advertisement messages. These messages include stateless address prefixes and require that hosts use a stateful address configuration protocol.

D. Network Evolution

Sprint is confident that IPv4 will give way to IPv6 over the course of the next several years. However, there will be no "global cutover" to IPv6. It would be simply impossible to orchestrate such a sweeping change. For this reason, the IETF has developed a "toolkit" of transition mechanisms that will provide for the smooth upgrade to IPv6 on a global basis. There are three main transition mechanisms – Dual Stack, Tunneling, and Translation.

Dual-Stack systems have both IPv4 and IPv6 addresses and capability. A machine configured in this manner has complete interoperability with any IP-based node. It uses v4 to communicate with v4-only machines, and v6 to communicate with v6-only nodes. As long as the intervening network fabric (the switches and routers and other devices which form the Internet) is IPv6-capable, a dual-stack machine should have any-to-any connectivity.

Tunneling is a technique where islands of IPv6 nodes can communicate with other islands of IPv6 nodes over an intervening IPv4 network (or *vice versa*). In this case, the nodes have complete end-to-end v6 capability, but as the packets travel over the predominantly IPv4 Internet (IPv6 packets encapsulated in IPv4 packets). However, all of the advanced features of v6 pertaining to packet transport are not available and tunneling does not allow v6 nodes to talk to v4 nodes.

Translation is a mechanism where IPv6 packets are translated by an intermediate system into IPv4 packets (and *vice versa*). This allows v6 and v4 machines to communicate, but as with tunneling, not all of the advanced features of IPv6 are available to the application. Translation allows newly deployed IPv6-only nodes to access legacy IPv4-only machines on the Internet.

It appears that entities looking to transition to IPv6 will use a number of methods in their integration process. And, depending upon the adopting entities' geographic location, it may be easier and more cost effective to start out by building IPv6 only networks due to limited IPv4 addresses availability. Regardless of which mechanism(s) are chosen, interoperability between v4 and v6 should become a common feature of the Internet. Eventually however, the Internet (as well as private IP-based networks) will completely migrate to IPv6.

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

Expectations for IPv6 are high because it is perceived as the protocol of the next generation Internet. As described above, IPv6 deploys a new data plane to fix various addressing and efficiency problems with IPv4, and a new routing control plane to effectively make use of the new addresses. The impact of the new data and control planes on today's networks is significant. Failures or interruption are unacceptable in mission critical networking environments.

Nonetheless network operators and service providers are facing difficult questions, particularly questions involving the migration for IPv4 to IPv6. To answer these questions with certainty, they need assurance that, in their particular networks, IPv6 will provide:

- Rapid expansion needed for more users and devices.
- Smooth transition and coexistence with IPv4.
- Robust network failure recovery.
- Deliverable quality of service.
- Improved network security.

There is also the added challenge of managing routers that support both IPv6 and IPv4 networks, with two sets of control and data planes. This can add significant resource requirements on personnel that administer these routers. Additional transition mechanisms like tunneling and application/address translation add complexity to router design.

For end users, IPv6 improves productivity by enabling network connectivity via a wider range of media and delivery mechanisms. But for general acceptance, the new IPv6 networks must demonstrate responsiveness at least equal to that of IPv4. In addition, while several end user environments and applications like Windows XP, Linux, and email support IPv6 today, more applications are needed to enhance IPv6's overall acceptance.

Many observers believe that IPv6 is inevitable for mobile networks. The emergence of mobile data services such as wireless data, picture mail and text messaging will influence a quick adoption of IPv6. The arrival of new generations of network technologies should lead to a proliferation of on-line mobile terminals. And with respect to CDMA networks the adoption of f IPv6 will make it possible to assign a permanent IP address to every on-line mobile terminal and to introduce the concept of "always on" permanent connection to the IP data network, even when the user's device is inactive.

The use of WLAN technologies on public networks could also serve to speed up the arrival of Mobile IPv6. Today, there is more and more demand for the use of WLAN technologies on public networks. However, it appears that regulators may be the determining factor as to the use of WLAN technologies on public networks.[6]

There are other reasons to migrate to IPv6. For example, the increasing deployment of broadband access to the Internet is consuming permanent addresses and accordingly aggravating the address shortage under IPv4. Indeed, most high-speed access is in an always-on mode,

[6] Native mobility management using IPv6 and its straightforward solutions simplify the mobility management of a terminal on a network (auto-configuration, automatic renumbering) offering obvious advantages for this type of technology and making IPv6 a particularly attractive solution for mobility management in heterogeneous networks. This would be particularly true for mobile terminals via a WLAN which would lead to total and transparent mobility for the user.

meaning that the terminal is continuously on-line and therefore requires a fixed IP address. In practice, providers offering high-speed broadband access (via DSL or cable modem) continue to offer dynamic addressing. However, the uses developing around these permanent connections mean that ISPs cannot apply the same modem/subscriber ratios as for a dial-up connection. These ratios can grow from 1/10 or 1/20 for dial-up to 1/2 or 1/4 for DSL/cable modem access, thereby accelerating the consumption of IP addresses.

The development of on-line electronics is universally recognized as a potential lever for IPv6. Consumer electronics and appliances will be more frequently connected to Internet either as terminals, *e.g.*, television screens used to surf on Internet, or servers, *e.g.*, appliances in so-called automated homes. Plus, the use of portable terminals like PDAs is expected to increase in the future and they will likely also be on-line. The need for IP addresses generated by these announced developments will likely make the move to IPv6 networks an absolute necessity, at least for the networks providing for these types of applications.

IPv6 deployment need not be costly if IPv6 requirements are built into existing upgrade strategies.[7] Major global networking hardware and software vendors are supplying IPv6 technology by default in their upgrades, and the costs of IPv6 deployment will be an incremental part of overall upgrade costs.

Launching mass-market IPv6 services or migrating a large corporate network to IPv6 would be costly and difficult to do today. However, a carefully planned migration strategy that seeks to build IPv6 requirements into all new developments and upgrades could significantly

[7] The costs of IPv6 deployment will be highly contingent upon the business scenario in question, the network services and applications required, and the type of interworking solutions chosen.

reduce these costs and spread them over a number of years. In any event, although certain costs, such as staff re-training and upgrades to operations support systems, may well be unavoidable, ultimately, IPv6-only networks will enable users to realize cost savings since such networks will be simpler in design and require less network administration than IPv4 networks.

IV. Current State of Deployment

Sprint was an early adopter of the 6Bone and IPv6 testbed founded and administered by the IETF working group NGTRANS (Next-Generation Transition). Sprint has been allocated a prefix for its (and its customers') use on the 6Bone (prefix 3FFE:2900::/24). A delegation out of this prefix is given to any SprintLink customer who wishes to use Sprint as a connection to the 6Bone. This address space is non-portable (if said entity were to leave Sprint, of stop using SprintLink's IPv6 network for 6Bone connectivity, the address space cannot stay with the customer, and MUST be given back to Sprint).

Sprint peers with numerous other IPv6 players, and has one of the most well-connected IPv6 networks on the planet today. It does peering via BGP4+ through a combination of IPv6-over-IPv4 tunneling and through various native IPv6 exchanges.

In addition to connectivity and IPv6 address space (non-portable), Sprintv6.net also provides DNS forward and reverse services free of charge for IPv6.[8] When Sprint delegates a prefix to a customer, it requests that the customer give Sprint the hostname of its IPv6 DNS server, and Sprint will delegate that zone down to the customer.

[8] If customer uses Sprint's service for their current DNS, this is TOTALLY separate, and on different hardware than the normal Sprint DNS service. This service description applies only to Sprint's IPv6 deployment.

V. Conclusion

Given the significant benefits of IPv6 *vis-à-vis* IPv4, Sprint believes that market will require the widespread deployment of IPv6. Sprint, for one, will continue to push for such deployment. For this reason, Sprint does not believe that government needs to mandate IPv6 deployment, although the government may wish to consider funding additional research and development if necessary.

Respectfully submitted,

SPRINT CORPORATION

________/s/___________
Michael B. Fingerhut
401 9th Street NW, Suite 400
Washington, D.C. 20004
(202) 585-1909

Its Attorney

March 8, 2004