GSA and IPv6 White Paper

February 12, 2004

Richard L. Williams, Chief
Applications Engineering & Technical Support
GSA Federal Technology Service
Office of Service Delivery (TOM)
10304 Eaton Place, Room 2-1002
Fairfax, VA 22030
Tel: 703 306-6290

EXECUTIVE SUMMARY

Rapid expansion of the Internet has created a "success disaster" in terms of IP addresses. The two most noticeable issues are *Internet address exhaustion* and *routing table size expansion*. Studies performed in the early 1990s showed that the current 32-bit Internet Protocol Version 4 (IPv4) address space would be exhausted between 2005 and 2011 if drastic measures were not taken. As a stop-gap measure, the Classless Inter-Domain Routing (CIDR) addressing policy was devised and implemented; but CIDR has merely postponed the inevitable Internet address exhaustion problem. Network Address Translation (NAT) routers and other equipment have also slowed the address growth problem. A new version of Internet protocol, IPv6, was proposed in the mid 90s, and a draft standard issued in 1998. Unfortunately, the Internet has grown so large, and is now so widespread geographically, that no single authority has the ability to order a "flag day", which was the old method of telling all users that as of a certain date, some change in the Internet (then called the "Arpanet") protocol would take place, and everyone had to conform or be left out. Since any major transition, such as that to IPv6, would involve substantial time, effort, and new equipment, the matter is by no means straightforward, especially since the Internet is now a well-established commercial entity, and not a research vehicle.

This paper addresses the IPv6 question from the standpoint of the Federal Government, and in particular, from that of GSA, as the prime supplier of telecommunications services to the Federal community. GSA has identified the following issues:

1. *Requirements for and benefits of IPv6.* Few specific "must have" areas have been identified. In general, arguments focus on the need to make many more *classes* of devices (beyond PCs) addressable and controllable over the Internet, thus enabling new *functionality*—the primary benefit of a switch to IPv6. The new functionality is only vaguely discernable at the present time, but is expected to materialize over a period of time, most likely 5-10 years. However, this gives the Government time to prepare by transitioning to IPv6-enabled or compatible hardware and software through the normal cycle of equipment replacement, something GSA can do in its new contract vehicles. At this point, no monetary value can realistically be placed on the benefits expected to accrue from IPv6. But this does not mean that the benefits will not be substantial, only that the applications cannot be predicted.

2. *Costs associated with deployment of IPv6.* Clearly any transition to a new technology will involve costs. Because there is limited immediate demand for IPv6, this allows the Government to phase it in gradually in most cases and thus take advantage of the normal replacement cycle for equipment, as discussed above. The costs to implement IPv6 break down into two areas: (1) hardware, software, staff resources to deploy IPv6; and (2) agency costs for training, operational changes.

3. *Transition to IPv6*. At the present time, transition to IPv6 is envisioned to be gradual. Because the IP address shortage is not expected to reach the critical stage for 5-10 years, a reasonable time frame for transition is 2005-2010. DoD has adopted a 2003-2008 time frame. Costs will be minimized with such a time frame, though of course any new ways of doing business which depend on the capabilities of IPv6 will incur transition costs. Presumably, however, there will be benefits offsetting the costs. Problems may arise for new applications which require IPv6, in which case no transition is possible, and also with legacy applications which are coded around IPv4. For these, recoding or entirely new application software will be required.

4. *Role for GSA in deployment of IPv6*. The role of GSA in deployment of IPv6 will be a function of Government policy as determined by the legislative and executive branches, of commercial trends, and of particular needs of agencies. Pending the issuance of such a policy, GSA can undertake certain actions. Among them are:

    - Make IPv6 available to all agencies. By making IPv6 compatibility a requirement for all future contract vehicles, GSA will be preparing the Government for the coming transition
    - Pressure agencies to transition by phasing out support for and availability of IPv4. This may be premature at the present time, given the expected transition timeframe.
    - Make transition assistance available. This would be a sensible way to assist agencies in their planning.
    - Develop Government-wide transition plan and schedule.

    GSA's FTS2001 contract has been used recently by the National Guard in their procurement of their new national network, Guardnet, which supports IPv6 connectivity, so GSA is on the forefront of offering IPv6 capabilities.[*]

Many companies are now shipping products based on IPv6. Included are host implementations by Apple, BSDI, Bull, Digital, Epilogue, FreeBSD, FTP Software, Hitachi, HP, IBM, INRIA, Interpeak, Linux, Mentat, Microsoft, NetBSD, Nokia, Novell, NRL, NTHU, OpenBSD, Pacific Softworks, Process Software, SICS, SCO, Siemens Nixdorf, Silicon Graphics, Sun, UNH, and WIDE. Router implementations are available from 3Com, 6WIND, Bay Networks, cisco Systems, Digital, Hitachi, IBM, Merit (routing protocols), Nokia, NTHU, Sumitomo Electric, and Telebit Communications.[†]

The purpose of this paper is not to study these issues exhaustively but to bring out the main points associated with each, so that further study can be undertaken in the most important areas.

---

[*] Guardnet does not yet use IPv6 in its operations.

[†] Source: Sun, http://playground.sun.com/pub/ipng/html/ipng-main.html

SECTION 1 OVERVIEW

In the last decade, there has been a tremendous increase in the number of users and information providers on the Internet. The requests for computer Internet addresses and for easier methods of configuring large computer networks have increased correspondingly. With this growth unfortunately, addressing issues have also arisen. The two most noticeable issues are Internet address exhaustion and routing table size expansion. Studies performed in the early 1990s showed that the current 32-bit Internet Protocol Version 4 (IPv4) address space would be exhausted between 2005 and 2011 if drastic measures were not taken. In east Asia, which was assigned fewer addresses to start, the problem has already become acute.[‡] As a stop-gap measure, the Classless Inter-Domain Routing (CIDR) addressing policy was devised and implemented; but CIDR has merely postponed the inevitable Internet address exhaustion problem. On the other hand, routing tables are growing at 1.5 to 2.0 times of memory technology. In July 1992, IETF called for proposal for a next generation Internet (IPng). An IPng area was formed in November 1993. Subsequently, the area developed a new Internet protocol known as Internet Protocol version 6 (IPv6). Unfortunately, the Internet has grown so large, and is now so widespread geographically, that no single authority has the ability to order a "flag day", which was the old method of telling all users that as of a certain date, some change in the Internet (then called the "Arpanet") protocol would take place, and everyone had to conform or be left out. Since any major transition, such as that to IPv6, would involve substantial time, effort, and new equipment, the matter is by no means straightforward, especially since the Internet is now a well-established commercial entity, and not a research vehicle.

This paper addresses the IPv6 question from the standpoint of the Federal Government, and in particular, from that of GSA, as the prime supplier of telecommunications services to the Federal community. GSA has identified the following issues:

1. Requirements for and benefits of IPv6
    - What are Government-unique requirements which can only be satisifed with IPv6?
    - What are shared Government and private-sector requirements which can only be satisfied with IPv6?
    - What will happen to Government operations if IPv6 is not adopted?
    - What benefits are expected to accrue to agencies from use of IPv6?

2. Costs associated with deployment of IPv6
    - What are costs in terms of hardware, software, staff resources to deploy IPv6?
        -Planning

[‡] John Lui, "Asia running out of IP-address room", CNET Asia, 28 May 2003, http://www.zdnet.com/2100-1103_2-1010666.html?tag=fdfeed.

-Transition
-Implementation
-Operation

- What are costs in terms of agency training, operational changes?

3. Transition to IPv6
    - What are obstacles and pitfalls?
    - What is a reasonable time frame for transition (beginning, end)
    - Who will bear the costs?

4. Role for GSA in deployment of IPv6
    - Make available to all agencies
    - Pressure agencies to transition by phasing out support for and availability of IPv4
    - Make transition assistance available
    - Develop Government-wide transition plan and schedule
    - Public policy aspects of IPv6 question

The purpose of this paper is not to study these issues exhaustively (that would require a much longer paper and much greater effort, including extensive discussions with agencies), but to bring out the main points associated with each, so that further study can be undertaken in the most important areas.

SECTION 2 REQUIREMENTS FOR AND BENEFITS OF IPV6

IPv6 has following enhancements over IPv4.

- Expanded address space
- Improved option mechanism
- Address autoconfiguration
- Increased address flexibility
- Support for resource allocation
- Security capabilities

The most obvious change in going from IPv4 to IPv6 is the increase in the address space from 32 bits in IPv4 to 128 bits in IPv6. This will allow for the connection of far more devices to the Internet (or any network using IP). Though this comes at the price of larger packet headers (40 vs. 20 bytes) and associated processing requirements, that should pose only minimal problems because of the steadily increasing speed of computer hardware, with speeds doubling roughly every 18 months to 2 years. A key advantage of the larger packet header is the ability to implement Quality of Service (QoS) technologies. Address autoconfiguration mechanism are designed to allow plug-and-play of network devices – simply plug in the host machine and it will automatically configure IP address, network prefix, and automatically find all available routers. This feature will reduce the management and operation overhead. IPv6 security is an integrated implementation of Internet Protocol Security (IPsec) policies and procedures. IPsec is mandatory for IPv6 but optional for IPv4.

At the present time, few specific pressing needs for the increased address space offered by IPv6 can be identified; only general trends are emerging.

Government-unique requirements

These will need to be defined in conjunction with agency discussions, but special DoD requirements may be anticipated, together with HHS. Typically these applications would arise when battlefield management requires communications with many devices, possibly carried by individual soldiers. For example, deployment of Mobile Ad-Hoc Networks (MANETs) in battlefield conditions may be extended to require IP addresses for the various pieces of equipment carried by each soldier. Another possibility is use of extended IP addresses in conjunction with RFID devices. While not every RFID device will be capable of communications, it may be desirable for boxes or containers, which can report on contents.

Shared Government and private-sector requirements

In general, IPv6 is envisioned as a means to facilitate the move from PC-only networks to networks in which the network enables entertainment media, conferencing, and command and control of devices and appliances. Of course, this can be extended to automobiles and portable devices of all types, linked by means wireless connections, leading to improved transportation systems, for example. It is the extension to new *types* of devices that perhaps poses the greatest threat to the current address space of IPv4. At the present time, the uses of such networks are not well-defined, but evolutionary

development can be expected to occur, just as it did with the PC, for which, in 1978, people had only general ideas about what it might be able to do. The Government can be expected to move in parallel with the private sector with respect to such generalized networks, as they will become common business tools. The same remarks apply to the QoS expected to be available with most implementations of IPv6.

What will happen to Government operations if IPv6 is not adopted?

Because applications of IPv6 are only vaguely defined, it is difficult to pinpoint problems which will arise if IPv6 is not adopted. At this point, about all that can be said is that the Government may fall behind the private sector in its ability to carry out business in the most efficient manner, and ultimately in its ability to communicate effectively with citizens. The improved security features of IPv6 would also be unavailable to Government, making it more vulnerable to security problems.

What benefits are expected to accrue to agencies through use of IPv6?

The benefits expected include more efficient internal operations and business processes, more efficient physical infrastructure (buildings, transportation), and better interaction with mobile users. Development and optimization of such systems will likely require substantial time, however.

SECTION 3 COSTS ASSOCIATED WITH DEPLOYMENT OF IPV6

As with any major technology change, costs may be broken down into two areas

1. Technology: Costs to deploy the technology
2. Human factors: Costs to change the way people go about their business

Technology costs

Technology costs break down into four areas: (1) planning, (2) transition, (3) implementation, and (4) operation.

(1) Planning. Agencies will have to plan how they will phase IPv6 into their operations. It may be safely assumed that all equipment purchased after a certain date will be capable of running under either IPv4 or IPv6, with automatic sensing as to which protocol is in use. Changing operations may be more complex if advantage is to be taken of IPv6 features. Plans for retrofitting old equipment, if necessary, must also be drawn up.

(2) Transition. This will be most critical in those areas where operations are going to change as a result of new IPv6 capabilities. Where there is no operational change, use of hardware which can operate under either protocol should eliminate most transition problems, with older IPv4-only equipment eventually becoming obsolete for other reasons and eliminated. It can safely be assumed that equipment manufacturers such as Cisco will deploy the software needed to handle the overlap period, and ensure smooth transition at that level.[§] In general, equipment providers and service providers are well prepared to handle a possible IPv6 transition because it is their business to adopt new standards as quickly as possible.

(3) Implementation. It will be necessary to replace all existing IPv4 hardware with new hardware that can handle both IPv4 and IPv6, or IPv6 only. As this includes nearly every PC in existence, millions of switches and routers, and many mobile devices, that will not be inexpensive. However, the cost issue is mitigated by the fact that transition to IPv6 is expected to take many years, and most of today's equipment will have been scrapped long before IPv6 takes over and IPv4 is permanently retired.

(4) Operations. New operational capabilities taking advantage of IPv6 capabilities may require more microprocessor-based devices, and thus more trained staff to operate and maintain them. If operations change, then training for all staff in new procedures will become necessary. If applications programs need to be modified or new ones written, costs could become high.

[§] Three methods have currently been defined to handle networks during the transition period. The first is use of dual stacks in all equipment, an IPv4 stack and an IPv6 stack, with the correct one selected automatically. The second is use of tunneling, in which IPv6 networks are connected through IPv4 network clouds by means of a tunnel. The third is a translation mechanism built into IPv6 devices which allow them to talk to IPv4 devices.

Human factors costs

These costs tend to be underestimated because people tend to underestimate the difficulty and time associated with changes in business practices (or home activities). In general, it can be assumed that, in addition to transition costs, there will be a period of adjustment to new technology during which productivity may actually decrease. Some workers may never feel comfortable with it. IPv6 is fortunately buried far down in the technology infrastructure, (unlike the PC), so these problems will most likely be less than in other cases. These costs have to be estimated on a case-by-case basis, and will be greatest when there are large operational changes in an office.

SECTION 4 TRANSITION TO IPV6

Obstacles and pitfalls

In the case of "disruptive" applications (those that can only work under IPv6), and which portend great benefits, there of course can be no "transition": the new hardware and software must be put in all at once. Since everything is unlikely to work smoothly at first, a shakedown period must be allowed.

Many application programs that utilize IPv4 addresses directly will have to be recoded to handle IPv6. If the programs are old, this may no longer be feasible, and these programs will have to be replaced by newer ones. If the applications were custom-written, and the original writers are no longer available, then new custom applications may have to be commissioned. This may be a lengthy process, with the need to test and debug any newly created software.

What is a reasonable time frame for transition (beginning, end)?

IPv6 hardware and software has been available since the late 90s, but there has been little thus far in the way of transition. Except for east Asia, where problems are more acute, it is likely that serious transition efforts to IPv6 will not begin on a wide scale for another year or so. However, DoD has already committed itself to IPv6, and requires all acquisitions as of October, 2003 to be IPv6 compatible. DoD expects to complete its transition in 2008, taking five years for the process. In general, five years appears to be a reasonable transition time frame, as few pieces of computer and networking equipment have a useful life which is longer than this, and it allows ample time for all the implementation issues discussed in the previous section to be addressed. If agencies begin to transition in the 2005 time frame, the transition process for the Government will be complete around the end of the decade.

Who will bear the costs?

In general, agencies will have to bear the costs, as no federal subsidy programs are in effect. However, as discussed in previous sections, if transition is planned carefully, little in the way of new equipment will have to be purchased for this purpose, as routine replacements and upgrades will take care of the problem as they can be expected to have IPv6 compatible hardware and software. New applications software, if required, and costs to implement "disruptive" applications, will of course be extraordinary expenses, but may save money in the long term. Much of this, however, may be considered analogous to the costs to agencies of implementing "service to the citizen" information systems—it is part of modern-day expectations.

SECTION 5 ROLE FOR GSA IN DEPLOYMENT OF IPV6

Make IPv6 available to all agencies through new contracts

Since there does not appear to be any reason why the Government should not move toward IPv6 over a 5 year transition time frame, GSA should make IPv6 compatibility a requirement for new hardware and software soon, perhaps as early as 2005, or with the Networx contracts. This would be in accordance with the DoD procurement policy discussed above, and would make transition to IPv6 fairly painless. One feasible approach would be to require all hardware to be IPv4/IPv6 capable for 5 years, and thereafter only IPv6 capability would be required.

Pressure agencies to transition by phasing out support for and availability of IPv4

This approach would have to be part of a Government-wide policy decision to implement IPv6 as rapidly as possible. As it would force a transition in a short time period, it would likely drive up costs to agencies, who would have to replace some equipment before the end of its useful life.

Make transition assistance available

To facilitate agency planning for transition, GSA could compile an IPv6 transition guidance manual or similar material. The material should address the process and procedure of transition to IPv6, and the key factors which agencies must consider in planning their IPv6 migration. Assistance could also take the form of engineering support, training, or hands-on help with development of new IPv6-enabled applications. GSA could contract with a number of vendors, who would be available on a GSA schedule or through a GWAC to any agency that required assistance in these areas. Agencies could then get the type of assistance they required from vendors who are familiar with GSA's approach to IPv6 and any Government-wide policies.

Develop Government-wide transition plan and timetable

GSA could also take on the role of Government-wide planning for transition to IPv6, including timetables. In this way, it could formulate guidelines for all agencies with respect to their transition strategies and IPv6 implementation goals. As part of this effort, GSA could make transition assistance available, and of course would require suitable IPv6 compatible hardware and software in all of its contracts and schedules.

Public policy aspects of IPv6 question

Migration to IPv6 is more than a technology problem, however. It involves policy issues concerning Government's role in moving the country toward IPv6, as a national standard which presumably will advance commerce and make the country more competitive. These decisions need to be made at the executive level, and then GSA will do its best to implement them.

Current availability

GSA's FTS2001 contract has been used recently by the National Guard in their procurement of their new national network, Guardnet, which features IPv6 compatibility, so GSA is already on the forefront of offering IPv6 capabilities.[**]

It should be noted that many companies are now shipping products based on IPv6. Included are host implementations by Apple, BSDI, Bull, Digital, Epilogue, FreeBSD, FTP Software, Hitachi, HP, IBM, INRIA, Interpeak, Linux, Mentat, Microsoft, NetBSD, Nokia, Novell, NRL, NTHU, OpenBSD, Pacific Softworks, Process Software, SICS, SCO, Siemens Nixdorf, Silicon Graphics, Sun, UNH, and WIDE. Router implementations are available from 3Com, 6WIND, Bay Networks, Cisco Systems, Digital, Hitachi, IBM, Merit (routing protocols), Nokia, NTHU, Sumitomo Electric, and Telebit Communications.[††] Other companies are expected to follow suit. Interoperability of products, however, may take a few years to be as transparent as IPv4 interoperability is today.

[**] Guardnet does not yet use IPv6 in its operations.

[††] Source: Sun, http://playground.sun.com/pub/ipng/html/ipng-main.html