DREN Helps Make the Transition to Internet Protocol version 6 (IPv6)

"The DoD IPv6 initiative and the DREN's lead role will blaze a trail for the U.S. military and for the civilian sector to follow." – Dr. Vinton Cerf, Government Computer News article 11/10/03

"One of the best reasons why the DREN IPv6 pilot has been developed is that it has given the DoD community a production environment to more directly test a functional network, as opposed to a closed, limited test network." – FY2007 DoD IPv6 Test and Evaluation Report to Congress

1. IPv6 Pilot Profile

The DoD's High Performance Computing Modernization Program (HPCMP) is responsible for the acquisition and modernization of the hardware, software, networks, and expertise that provide some of the world's most advanced computing capability in support of the DoD mission. The HPCMP user community includes over 4,300 users at nearly 200 DoD and other government laboratories, test centers, universities, and industrial locations. The nation-wide Defense Research and Engineering Network (DREN) provides the HPCMP user community with protocol-rich, high-availability, high-capacity, low-latency, secure connectivity between and among the DoD Supercomputing Resource Centers (DSRCs), HPCMP Affiliated Resource Centers (ARCs), and many external networks such as the Internet and the Internet2. In June, 2003, the DREN was designated as the first DoD IPv6 pilot network by the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer [ASD(NII)/ DoD CIO]. By July, 2005, the entire DREN wide-area network (WAN) was routinely supporting end-to-end IPv6 traffic, several sites were supporting IPv6 along with Internet Protocol (IP) version 4 (IPv4), and selected applications were IPv6 enabled. Performance and security were as good as and in some ways better than pre-IPv6 pilot levels, This was accomplished without additional personnel and with less than $100,000 in additional funding.

2. Situation

As part of DoD's information age transformation, the network is emerging as **the** single most important contributor to combat power and protection. Network-Centric Operations (NCO) provides an unprecedented potential to attain critical advantage over adversaries within available resources in the long-term. A DoD-wide Global Information Grid (GIG) is one of the key enablers that form the foundation of the DoD's NCO transformation. The GIG represents a globally interconnected, end-to-end set of information capabilities and processes for collecting, processing, and managing information on demand to warfighters, policymakers, and support personnel. The GIG fulfills a fundamental principle of NCO by securely connecting people and systems regardless of time or place, providing vastly superior situational awareness and better access to information for accelerated decision-making. The GIG supports all DoD mission areas.

On June 9, 2003, the DoD CIO issued a memorandum stating that the DoD information infrastructure of the future would depend on the effective implementation of IPv6 in building the GIG to achieve the DoD's NCO and warfare goals. As part of the DoD IPv6 transition planning process, specific pilots designed to build confidence in and facilitate the overall DoD transition to IPv6 would be identified. Effective implementation of IPv6 in concert with other aspects of the GIG architecture would depend, in part, on the ability to test the IPv6 functional capabilities of multiple devices operating simultaneously across several locations at full performance levels. To conduct such tests, a production-level wide-area test network supporting end-to-end IPv6 traffic would be required.

On June 27, 2003, the HPCMP was notified that DREN was the first DoD IPv6 pilot network. As the DoD's first IPv6 pilot network, the IPv6 pilot needed to be implemented in such a way that the lessons it learned (sometimes called best practices) could help facilitate the many IPv6 implementations that would follow. This influenced the DREN IPv6 pilot implementation, as follows:

- The scope of the IPv6 pilot included not just the DREN WAN, but selected local sites and core mission applications as well, rather than limiting the IPv6 pilot to IPv6 transport among a few nodes on the WAN without any local infrastructure or applications.
- The transition mechanism used was dual-stack throughout with minimal use of tunnels and no protocol translators.
- The IPv6 capabilities were limited to full parity with IPv4 without including any advanced IPv6 features.

The goals of the DREN IPv6 pilot in July 2003 were as follows:

1. To enable the entire DREN WAN to routinely support end-to-end IPv6 traffic between and among all DREN sites and multiple external peering networks.
2. To maintain the performance and security levels of the IPv6 pilot at the levels that existed prior to the IPv6 pilot.
3. To develop a process that would facilitate introduction of the IPv6 protocol suite at the IPv6 pilot sites, the DREN Network Operations Center (NOC), and the High Performance Computing (HPC) Computer Emergency Response Team (CERT); to use this facilitation process; and capture metrics from its use.
4. To enable IPv6 in selected applications provided by the HPCMP to the IPv6 pilot sites: network security products, a core mission application, and other applications/utilities.
5. To document and provide lessons learned to help facilitate DoD IPv6 implementations at the WAN-, site-, and applications-level on the DREN IPv6 knowledge base[1] web site. (This goal was later expanded to include facilitating Federal Agency and Department IPv6 implementations.)

3. Approach

Six key factors made it possible for the DREN to implement IPv6 so quickly and at such a low cost: people, personality, process, procurement practices, basic network transport protocol, and the target IPv6 protocol suite. Even without these last four factors, the DREN would still have accomplished its IPv6 pilot goals, but it would have taken longer and might have cost more.

Whenever a change from the status quo occurs, the selection of the people to plan the change is critical. At the inception of DREN in 1992, the DREN Project Manager established a Technical Advisory Panel (TAP) with members from the DoD Services and participating defense Agencies. Each TAP member is a respected member of the DoD national networking community. Their track record in responding to the evolving networking requirements of the HPCMP user community ensured their selection as the group to make plans for the IPv6 pilot. Because the ASD(NII)/DoD CIO had designated DREN as the first DoD IPv6 pilot, typical enterprise-level questions (such as "Why should we do this?" or "Can't we wait to get started?") were already answered. Instead, the question facing the TAP was "How quickly can we make IPv6 happen?" In a series of meetings during July and August of 2003, the TAP established the goals of the DREN IPv6 pilot (see **Situation**), formed the core pilot implementation team (6 TAP members and an implementation manager), drafted a DREN IPv6 pilot implementation plan, and started working the plan. Limited portions of the DREN were supporting end-to-end IPv6 traffic by December 2003 and the entire DREN WAN and several sites were routinely supporting end-to-end IPv6 traffic by July 2005.

The second key factor in the success of the IPv6 pilot was the corporate personality of the HPCMP headquarters, the DSRCs, the ARCs, and the DREN networking community. Personnel at all levels, from upper management down to technical experts, were receptive to change and used to dealing with risk. They were willing to working in geographically dispersed teams on multi-year projects that provided benefits to the enterprise but did not immediately benefit their own local site. Such attitudes are an

important element of the HPCMP's on-going efforts to continuously improve the advanced computing capability that the HPCMP provides in support of the DoD mission.

The third key factor in the success of the IPv6 pilot was the process used to enable IPv6 transport at the IPv6 pilot sites. Although the TAP members had considerable collective experience in enabling new network technologies, they had never developed a knowledge diffusion process. The DREN transition to IPv6 was both a technology transition and an information diffusion challenge. Many of the personnel implementing IPv6 were learning about IPv6 at the same time that they were implementing it. The IPv6 pilot team's search for a process that addressed both challenges led to the TransPlant[2] facilitated planning process for diffusing and adopting emerging technologies. TransPlant was developed by the Software Engineering Institute (SEI) at Carnegie-Mellon University in the '90s. A series of presentations based on the SEI TransPlant process were prepared and used at each IPv6 pilot site and contributed to the successful introduction of the IPv6 protocol suite at the sites. Ten IPv6 pilot sites routinely support end-to-end IPv6 traffic. Additional DREN sites beyond those initially participating in the IPv6 pilot have volunteered to enable IPv6 transport at their sites.

The fourth key factor in the success of the IPv6 pilot was the HPCMP procurement practices. On the DREN WAN the network equipment was quite up-to-date (most of it less than 3 years old) and high-end (it is a high-capacity WAN). The infrastructure at the DSRCs and the ARCs was also quite up-to-date (most of their equipment was less then 4 years old) and high-end (they are supercomputing centers). The IPv6 support provided by this up-to-date equipment contributed to the IPv6 pilot success. Having this support already available reduced both the complexity involved in planning and the risk associated with implementing the IPv6 pilot. To enable IPv6 transport on the DREN WAN, no equipment needed to be replaced. To enable IPv6 transport at the sites, only two small routers needed to be replaced – one each at two different sites, at a total cost of less then $30,000.

The fifth key factor in the success of the IPv6 pilot was the basic network transport protocol selected. The basic network transport protocol of the pre-IPv6 pilot DREN WAN had been the Multi-Protocol Label Switching (MPLS) protocol. The protocol-agnostic nature of MPLS was well suited to supporting the dual-stack WAN environment of the IPv6 pilot. Indeed, DREN previously supported both Asynchronous Transfer Mode (ATM) and IPv4 using MPLS. MPLS in conjunction with IPv6 Provider Edge (6PE) on the edge routers was used throughout the DREN WAN design. It should not be concluded, however, that MPLS is the only basic network transport protocol that could be used (although other networks have made the same choice). Instead, it was the homogeneity that this design allowed which contributed to the IPv6 pilot success. Keeping the IPv4 and IPv6 network topologies congruent minimized the impact of supporting both IPv4 and IPv6 protocol suites over one physical infrastructure. The pre-IPv6 pilot DREN NOC used IPv4 exclusively for network management, but during 2009 the DREN NOC is switching over to using IPv6, with IPv4 being used to manage legacy equipment that is IPv6-incapable.

The sixth key factor in the success of the IPv6 pilot was the target IPv6 protocol suite at the IPv6 pilot sites. The IPv6 protocol suite was deliberately limited to provide parity **only** with IPv4, excluding multicast and not including any advanced IPv6 features. This was a prudent decision to make in 2003, given the uncertainties associated with the then available implementations of any IPv6 protocol suite. During the 2003-2004 timeframe, if the DREN IPv6 pilot had not been able to provide end-to-end connectivity and functionality between the IPv6 pilot sites for an IPv6 protocol suite that was fully equivalent to that already being provided by IPv4, the potential benefits provided by the advanced features of IPv6 hardly mattered. Also, the HPCMP user community did not require the advanced features of IPv6 (for instance, supercomputers aren't very mobile). The IPv6 pilot achieved this by 2005. In late 2006 IPv6 multicast support was added, achieving full parity with IPv4. The IPv6 pilot has not attempted to support advanced features of the IPv6 protocol suite such as mobile IPv6 or end-to-end IP Security[3] (IPSec). However, users at some of the IPv6-enabled DREN sites have conducted several experiments to test various advanced features of IPv6.

4. Challenges:

A number of problems were encountered and most of them were solved by the DREN IPv6 pilot. Only those unique to IPv6 are discussed below, grouped as follows: Enterprise-level (affecting both the WAN and site infrastructures), Site Infrastructure, and Applications.

4.1 Enterprise-level Challenges

IPv6 connectivity from anywhere. Only a few of the DREN sites planned to support IPv6, yet the IPv6 pilot wanted to offer IPv6 connectivity to the entire HPCMP user community, including users at sites that only supported IPv4. Providing connectivity was complicated by the variety of operating systems on the users' desktop computers, which included versions of Microsoft Windows, Linux, UNIX, and Apple OS X. Connectivity was provided by installing a pair of Hexago[4] Gateway6 tunnel brokers at a total cost of less than $70,000, one for users at IPv4-only DREN sites, and one for users on the Internet[5].

Domain names in Domain Name Servers (DNS). This is a *Catch-22* question when planning to support IPv6: when to create the AAAA record in the DNS to associate the IPv6 address of a server with its domain name? The AAAA record should **not** be created until after **all** services running on a server have been IPv6-enabled. But even so, there is no "right" time. Many of the operating systems on today's laptop and desktop computers are IPv6-enabled by default (a major exception being Microsoft Windows XP). An IPv6-enabled system may make DNS queries for IPv6 addresses and then attempt to access them, **even though** the network it is on supports only IPv4. Such attempts can time out for various reasons, and the system will then fall back to IPv4. Timeouts can cause user frustration or confusion. The timeouts are often blamed on IPv6 (do a web search on "ipv6 web slow"), when IPv6 may not the problem[6]. The sooner the AAAA record is created, the more benefits that IPv6-enabled systems using the server will receive but the more likely it is that enterprise and external users without any or with limited IPv6 access may experience timeouts. The later the AAAA record is created, the fewer users that will experience timeouts, but at the cost of reducing the benefits from IPv6-enabling the server. The IPv6 pilot's interim answer was to create a new domain name for each IPv6-enabled server, either a new domain name (as Google did with ipv6.google.com) or a new sub-domain (as the IPv6 pilot did with www.v6.dren.net). This allowed IPv6 to be tested during development, but it is not a long term answer. Eventually, the IPv4 and IPv6 addresses of a server should be associated with the same domain name. Otherwise, what began as an interim answer can become permanent. The IPv6 pilot is continuing to investigate possible solutions. There is no clear-cut, problem-free answer to this question.

4.2 Site Infrastructure Challenges

Motivation. Consider this apocryphal story: 'Three stonemasons were building a cathedral when a stranger wandered by. The first worker was toting rocks to a pile, near a wall. "What are you doing?" said the stranger. "Can't you see that I'm carrying rocks?" was the reply. The stranger asked the second worker, "What are you doing?" "I'm building a wall," he replied. A few steps away, the stranger came upon a third worker. "What are you doing?" he asked. This worker smiled. "I'm building a cathedral to the glory of God!" was the reply.' Three people, one mission, three viewpoints (and consequently motivation). It was worth the time taken to establish a link between the local site's part in the IPv6 pilot and the DoD enterprise requirement (see **Situation**). An up-front part of each on-site TransPlant briefing was spent establishing a link to the DoD enterprise requirement. Time and again site personnel changed their feeling that the IPv6 pilot was just something that a remote headquarters was imposing on them into a feeling that this was something that would result in better support for the HPCMP user community.

IP addresses in DNS. Installing and operating an infrastructure that supports secure, automatic registration of IPv4 public address in a DNS using DHCP is challenging enough in an IPv4-only

environment, as the TAP knew from experience. Products to support DHCPv6 in an IPv6-only environment existed in the 2003-2004 timeframe, but the IPv6 pilot team was unable to find a combination of products and configurations that would support secure, automatic registration of both IPv4 and IPv6 public addresses. Consequently, while the IPv6 pilot used stateless IPv6 address auto-configuration (SLAAC), the resulting IPv6 addresses were manually rather than automatically registered in DNS. This worked well, although on systems running Microsoft Windows it was necessary to disable temporary global IPv6 address generation (which is on by default). The IPv6 pilot team is continuing to search for products that can meet their requirements.

Network Security Products. During the IPv6 pilot implementation security products with IPv6 capabilities, including Intrusion Detection (ID), firewalls, Intrusion Prevention, virus scanners, and port scanners were not as mature nor as widely available as they were for IPv4. The situation has improved since then, but adequate IPv6 security still requires some product research and careful planning. To maintain security on an IPv6-enabled network can require the use of products that are new or may be unfamiliar to security managers, who are already struggling to maintain security on their existing IPv4 networks. In 2003 the IPv6 pilot was able to find the necessary products, although often they were open source or still under development, in all categories save one: ID. To perform inspection of IPv6 packets, the IPv6 pilot had to add IPv6 support to the source code for the ID software already deployed on the DREN called the Joint ID System, or JIDS. JIDS is a DoD version of the Network ID software from Lawrence Livermore National Laboratory. The IPv6 pilot also had to add IPv6 packet analysis support to SNORT, an ancillary tool used by the JIDS. One highly skilled network engineer worked for almost three months to make the necessary changes in JIDS and SNORT. This work was completed in 2003, and the HPC CERT deployed the IPv6-enabled JIDS across the DREN WAN in 2003-2004. The HPC CERT has since deployed additional ID products. Dual-stack capable firewalls only become available in 2005. Initially the IPv6 pilot team needed to configure multiple firewalls in parallel at a few sites, because no single device could simultaneously satisfy some sites OC-48c (2.488Gbps) bandwidth and dual-stack protocol filtering requirements.

4.3 Application Challenges

Application Support for IPv6. Few of the over three hundred commercial and open source applications running on the supercomputers at the DSRCs and ARCs supported IPv6 in 2003. Two-thirds of them didn't need to – all they did was crunch numbers. For the few that also did inter-computer communications, it was deemed acceptable that they continue to use IPv4, because (1) the DREN WAN would still support IPv4 transport for many years, and (2) only their developers could IPv6-enable the applications. From 2003 when the developers of commercial applications were first surveyed until 2005 when they were surveyed again, the situation improved in two ways. (1) A few more applications gained IPv6 support, and (2) A majority of the developers became aware of the DoD requirements for IPv6 and developed business plans to IPv6-enable their applications. However, they still waited for an acquisition requiring IPv6 support that was willing to pay for the capability before adding it. This survey was done only for applications that ran on supercomputers. Its applicability in other application areas is unknown.

Core Mission Application: **The** core mission application for the HPCMP is Kerberos[7]. The HPCMP requires all HPCMP users to use the Kerberos software suite for strong user authentication, single sign-on, end-to-end encryption of all terminal sessions with HPCMP computers, and end-to-end encryption of all file transfers from/to HPCMP computers. For historical reasons Kerberos has never been widely used, but it has been an integral part of the HPCMP security profile since 1998. The Massachusetts Institute of Technology developed Kerberos, and had already done most of the work required to IPv6-enable Kerberos by the time the IPv6 pilot was established. In 2004 the IPv6 pilot team only needed to add support for one-time passwords and fix some minor bugs. It was then ready for deployment.

Adding IPv6 support to other applications/utilities. The IPv6 pilot did not add IPv6 support to any applications beyond Kerberos. The utilities that came with the various operating systems were already

IPv6-enabled, and there were no other critical application requirements. In preparation for possible application conversions, however, the IPv6 pilot team surveyed available tools for and documents about analyzing application source code and developed guidelines for making the necessary modifications. The results are available on the IPv6 knowledge base.

5. Conclusion:

The goals of the IPv6 pilot were achieved with less than $100,000 in additional funding and without additional personnel. One of the real surprises from the IPv6 pilot was how little time was required to enable IPv6 at the IPv6 pilot sites. The details of how the IPv6 pilot measured success (metrics), including the time required, are available on the IPv6 knowledge base. Performance and security are as good as and in some ways better than they were before the IPv6 pilot. The lessons learned by the DREN IPv6 pilot team have been shared with many organizations through conference presentations, journal papers, magazine articles, interviews, the IPv6 knowledge base[1], and participation in DoD, Intelligence Community, Federal, and industry working groups and workshops. The DREN IPv6 pilot team continues to share lessons learned from its years of experience in operating a production IPv6-enabled environment through the Federal CIO Council Architecture and Infrastructure Committee's IPv6 Working Group[8] and various DoD and industry groups.

The success of the DREN IPv6 pilot was the result of both good initial positioning and a series of good decisions. But it goes much deeper than that. Rather than a temporary test bed that would be built up and then torn down once IPv6 support was demonstrated, the outcome of the IPv6 "pilot" fundamentally changed the DREN and the IPv6 pilot sites, so that they could meet the present need of the DoD for a production-level wide-area test network while also enabling them to meet the future needs of the HPCMP user community. In 2009 the DREN will complete the transition in implementation as well as in mindset from being an IPv4 network which supports IPv6 to being an IPv6 network with legacy support for IPv4. As the December 2008 policy changes[9] by the Number Resources Organization, the American Registry for Internet Numbers, and the other Regional Internet Registries show, a fundamental shift from IPv4 to IPv6 is underway. It is now time for federal stakeholders to travel the trail blazed by the DREN.

For More Information:

High Performance Computing Modernization Program
Defense Research and Engineering Network
10501 Furnace Road, Ste 101
Lorton, VA 22079

Walt Williams, DREN Program Manager
(703) 812-8205 wwilliams@hpcmo.hpc.mil
John Baird, IPv6 Implementation Manager
(703) 402-9638 baird@hpcmo.hpc.mil

Ron Broersma, DREN Chief Engineer
(619) 553-2293 ron@spawar.navy.mil
Tim Owen, Senior Network Engineer
(703) 812-8205 towen@hpcmo.hpc.mil

[1] https://kb.v6.dren.net allows read-access to DoD Common Access Card (CAC) holders. Read-access may be granted for other members of the federal IPv6 community upon request. Send email to kbwebmaster@hpcmo.hpc.mil.
[2] www.sei.cmu.edu/news-at-sei/features/2001/4q01/feature-4-4q01.htm and www.sei.cmu.edu/pub/documents/98.reports/pdf/98tr004.pdf.
[3] While the IPv6 pilot did not try to support end-to-end IPSec, the DREN WAN uses IPv4 IPSec for edge-to-edge encryption of IP packets (both IPv4 and IPv6) while transiting the WAN. In 2009, the DREN is planning to shift to IPv6 IPSec encryption.
[4] www.hexago.com.
[5] www.v6.dren.net/pub-broker is publicly accessible. A partial list of IPv6-enabled web sites is available at www.v6.dren.net.
[6] www.sixxs.net/faq/dns/?faq=ipv6slowconnect describes one DNS-related problems, and tells how to identify many DNS-related problems. Limited or erratic end-to-end IPv6 connectivity can also cause timeouts.
[7] web.mit.edu/Kerberos.
[8] A comprehensive presentation to the Working Group occurred in September 2006, and was updated in April 2008. Both are available on the www.core.gov web site. Log in using the Ecco collaboration tool under the Cross-Agency Collaboration tab and use the Community Explorer to expand CORE\IPv6 General Information\IPv6 Agency Leads\DREN to view the presentations.
[9] www.nro.net/documents/IGF_IP_Statement.pdf