



# Spiraling Information Demands – The Way Ahead With IPv6

Kristopher L. Strance

Office of Assistant Secretary of Defense

*The achievement of Net-Centric Operations and Warfare (NCOW), envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms, facilities, people, and information, depends on effective implementation of Internet Protocol Version 6 (IPv6) in concert with other aspects of the GIG architecture.*

– Department of Defense Chief Information Officer (DoD CIO) Memorandum, June 2003

IPv6 is the next-generation network layer protocol for the Internet and the DoD GIG.

The current version of IP, IPv4, was developed in the 1970s and is the basis of interoperability for today's Internet and many DoD networks. However, IPv4 has limitations that inhibit the end-to-end paradigm of the Internet and achievement of the DoD's vision of net-centric operations.

IPv6 has been under development by the Internet community for more than a decade and is designed to overcome IPv4 limitations by greatly expanding available IP address space and integrating features such as end-to-end security, mobile communications, Quality of Service (QoS), and simplified network management. The numerous fixes and extensions implemented to overcome IPv4 limitations often have increased network complexity and slowed network performance. The DoD transition to IPv6 will add functionality and reduce network complexity.

## Why Is IPv6 Transition Important to the DoD?

The DoD seeks to build a *more* agile, robust, interoperable, and collaborative net-centric environment where warfighters, intelligence, and business users share information on a secure, dependable, and global network. This NCOW network will enable superior decision-making and more effective military operations through network ubiquity and scalability, globally routable addresses, network support of QoS, enhanced plug-and-play/mobility, auto-configuration, improved multicast, end-to-end security, and improved network maintainability.

In the GIG, IP is the common network protocol that allows all types of data to move seamlessly on the GIG's diverse transport layer which includes landline, radio, and space-based elements. Due to fundamental limitations of the current IPv4 protocol for the long-term networking requirements of

the DoD and commercial community, IPv6 is a critical enabler in achieving the DoD's vision of the NCOW.

## Challenges of Transitioning to IPv6

The DoD strategy for transitioning to IPv6 is based on technology refreshment of the DoD Information Technology (IT) infrastructure. This poses a daunting challenge since this infrastructure is distributed across all DoD components, geographically dispersed, and managed through a complex and interdependent mesh of DoD programs and projects. The IPv6 technologies to support the operational needs of this varied set of users are still being developed, especially with respect to security and mobility. The DoD faces specific challenges in the following four categories:

- Prioritizing IPv6 resources by DoD components.
- Training experienced IPv6 IT staff to support testing, operations, and maintenance.
- Availability of IPv6 capable products and advanced IPv6 features.
- Scheduling dependencies and coordinating DoD networks.

To manage the security challenges and associated risks, the DoD has established a set of milestone objectives to guide the development of information assurance security configurations and allow transition to occur only after understanding the vulnerabilities. Milestone Objective 1 provides DoD components the *authority to operate using IPv6 within approved isolated network domains* (enclaves). Milestone Objective 2 provides *authority to operate using IPv6 across cooperative multi-domain environments* (transport). Milestone Objective 3 will be reached when *Defense Information Systems Networks and DoD components' core IP infrastructures are capable of accepting, routing, and processing IPv6 protocol traffic* while providing parity to IPv4.

The DoD intends to manage transition risks in the areas of interoperability,

performance, and security by a measured and controlled approach and to field IPv6 capabilities using pilot implementations and test and evaluation activities. The DoD IPv6 Master Test Plan<sup>1</sup> identifies 17 DoD test facilities and networks to conduct IPv6 test and evaluation. One of the DoD test networks is the Defense Research and Engineering Network (DREN). DREN provided an early DoD network IPv6 pilot implementation, primarily to support DoD IPv6 research and test requirements. Although the DREN only partially represented the DoD's complex networks, valuable lessons have been learned, including the following:

- IPv6 performance was approximately the same as IPv4 on various stress tests.
- Using defense-in-depth concepts, IPv6 security was comparable to IPv4 for Wide Area Network and site protection.
- Training requirements were minimal for personnel already familiar with IPv4.
- Most equipment at the sites could be upgraded to IPv6.

More work is required in test and pilot implementations. However, early DREN efforts and results provided an optimistic start.

## Way Ahead

The DoD embarked on the journey to IPv6 in June 2003 when the DoD CIO established the goal to transition to IPv6 by fiscal year 2008. We have further refined the goal to transition our core networks to provide a service offering of IPv6 by that date, with other DoD networks, infrastructures, and applications to follow. The road map to achieve this goal is being developed now. The Defense Information Systems Agency (DISA) has developed, and is now executing, IPv6 transition plans for our core enterprise networks. DISA is integrating the IPv6 implementation schedules for other DoD component core networks



## Get Your Free Subscription

Fill out and send us this form.

**517 SMXS/MXDEA**

**6022 FIR AVE**

**BLDG 1238**

**HILL AFB, UT 84056-5820**

**FAX: (801) 777-8069 DSN: 777-8069**

**PHONE: (801) 775-5555 DSN: 775-5555**

Or request online at [www.stsc.hill.af.mil](http://www.stsc.hill.af.mil)

NAME: \_\_\_\_\_

RANK/GRADE: \_\_\_\_\_

POSITION/TITLE: \_\_\_\_\_

ORGANIZATION: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

BASE/CITY: \_\_\_\_\_

STATE: \_\_\_\_\_ ZIP: \_\_\_\_\_

PHONE: (\_\_\_\_) \_\_\_\_\_

FAX: (\_\_\_\_) \_\_\_\_\_

E-MAIL: \_\_\_\_\_

### CHECK BOX(ES) TO REQUEST BACK ISSUES:

MAR2006 ☐ PSP/TSP

APR2006 ☐ CMMI

MAY2006 ☐ TRANSFORMING

JUNE2006 ☐ WHY PROJECTS FAIL

JULY2006 ☐ NET-CENTRICITY

AUG2006 ☐ ADA 2005

SEPT2006 ☐ SOFTWARE ASSURANCE

OCT2006 ☐ STAR WARS TO STAR TREK

NOV2006 ☐ MANAGEMENT BASICS

DEC2006 ☐ REQUIREMENTS ENG.

JAN2007 ☐ PUBLISHER'S CHOICE

FEB2007 ☐ CMMI

MAR2007 ☐ SOFTWARE SECURITY

APR2007 ☐ AGILE DEVELOPMENT

MAY2007 ☐ SOFTWARE ACQUISITION

JUNE2007 ☐ COTS INTEGRATION

TO REQUEST BACK ISSUES ON TOPICS NOT LISTED ABOVE, PLEASE CONTACT <STSC.CUSTOMERSERVICE@HILL.AF.MIL>.

into the enterprise networks transition plans. We have developed a DoD IPv6 master test plan to coordinate all IPv6 related testing activities across the DoD and promote efficient use of DoD test and evaluation resources. The DoD has acquired IPv6 address space and is developing a DoD IPv6 addressing plan. We recognize that DoD IPv6 transition progress depends, to a great degree, on industry's transition to IPv6. The DoD continues to collaborate with industry standard's bodies to ensure DoD requirements are reflected in evolving IPv6 standards.

Effective implementation of IPv6, through synchronized planning and comprehensive testing, in concert with other aspects of GIG architecture development, will enable the DoD to achieve the net-centric vision. ♦

### Note

1. Can be accessed at <<https://gesportal.dod.mil/sites/JITCIPv6/tewg/default.aspx?RootFolder=%2fsites%2fJITCIPv6%2ftewg%2fDocument%20Library%2f1%2fJoint%20Staff%20IPv6%20Operational%20Criteria&View=%7bA84A1771%2d0AC1%2d4003%2dB341%2dC6D8EF28FA40%7d>>, but a DoD Common Access Card is required.

### Continued From Page 10

those attributes critical to the realization of interoperable shared services throughout the DoD.

**Way Ahead.** A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when military services, agencies, and mission partners create reusable *building blocks* through the use of services. NCES is a key provider of building block services as part of the common infrastructure to be leveraged across the DoD and its mission partners in the development of information sharing capabilities.

The NCES program needs to continue working collaboratively with the DoD community to expedite the delivery of its common infrastructure services, related standards, and guidance for using its services. ♦

### References

1. DoD CIO. "Department of Defense Net-Centric Services Strategy." Washington: DoD CIO May 2007.

## About the Author

**Kristopher L. Strance** currently serves as a senior IT analyst in the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII)/DoD CIO. He is responsible for development of DoD policy for IT and National Security Strategy (NSS) interoperability, IP convergence, VoIP, and IPv6 transition. Strance has more than 30 years of experience in IT and NSS, including policy, planning, development, programming, and operational employment. His technical and management experience includes key policy and planning positions working directly for senior government executives. Strance has a bachelor's degree in biology and chemistry from the University of New Mexico. He received his commission as an Ensign in the U.S. Navy in 1975 and was designated as a Naval Flight Officer in 1976.

### OASD (NII)

#### DoD CIO

**1851 S Bell ST STE 7000**

**Arlington, VA 22202**

**Phone: (703) 607-0249**

**E-mail: kris.strance@osd.mil**

2. DoD CIO. "Implementing the Net-Centric Data Strategy, Progress and Compliance Report." Washington: DoD CIO Aug. 2006.
3. DoD CIO. "PDM III Core Enterprise Services." Washington: DoD CIO Sept. 2006.

## Author Contact

**Ann H. Kim**

**DoD CIO**

**Information Policy Directorate**

**1851 S Bell ST STE 600**

**Arlington, VA 22202**

**Phone: (703) 602-0940**

**E-mail: ann.kim@osd.mil**

**Carol Macha**

**DoD CIO**

**Information Policy Directorate**

**1851 S Bell ST STE 600**

**Arlington, VA 22202**

**Phone: (703) 602-2720 ext. 145**

**E-mail: carol.macha@osd.mil**