



2003 Moonv6 FAQ

IPv6 adoption has been a forgone conclusion in Asia and Europe for almost three years. High Internet access penetration, and the phenomenal growth of cellular phone usage, has rapidly depleted the IPv4 address space availability for these regions and forced the unhealthy, widespread usage of NAT. IPv6, with its almost limitless supply of address space, and other protocol advancements, mitigates address shortage issues, eliminates the need for NAT, and provides a solid platform for IT advancement in these regions.

The North American IT community's interest in IPv6 has been somewhat lackluster in comparison. With access to almost 70% of the IPv4 address space, IP address shortages have not been a major issue. Consequently, the number of IPv6 related testbeds and experiments, and accordingly, the level of widespread experience with IPv6 pales in contrast to the support and experience found in places like Japan, Korea, and the EU.

In order to rectify this shortcoming, the North American IPv6 Task Force (NAv6TF), in collaboration with the University of New Hampshire Interoperability Lab (UNH-IOL), the Joint Interoperability Test Command (JITC), and the Department of Defense (DoD), is pleased to announce the development of **Moonv6**.

The Moonv6 project represents the most aggressive IPv6 interoperability and application demonstration event in the North American market to date. Moonv6 will provide a platform for the North American IT community to garner extensive, real world, IPv6 deployment experience. Additionally, it will serve as an opportunity for equipment and application vendors to demonstrate the maturity and robustness of their respective IPv6 implementations to prospective users and adopters of IPv6 (please see attachment for major IPv6 adoption announcement).

The following FAQ provides the basic details for the Moonv6 project. Additional information will be available at www.moonv6.org in August, 2003.

1. What is Moonv6?

Moonv6 is a multi-site, IPv6 based network designed to test the interoperability of various vendor-specific IPv6 implementations.

2. Who is organizing Moonv6?

Moonv6 is a collaborative project being facilitated by the North American IPv6 Task Force (NAv6TF), the University of New Hampshire Interoperability Lab (UNH-IOL), and the Joint Interoperability Test Command (JITC). The UNH-IOL has overall responsibility for organizing the Moonv6 event.

3. Where will the Moonv6 project take place?

Moonv6 is a multi-site event, occurring at locations across North America. Figure 1 identify the commercial, academic, and government participating locations.

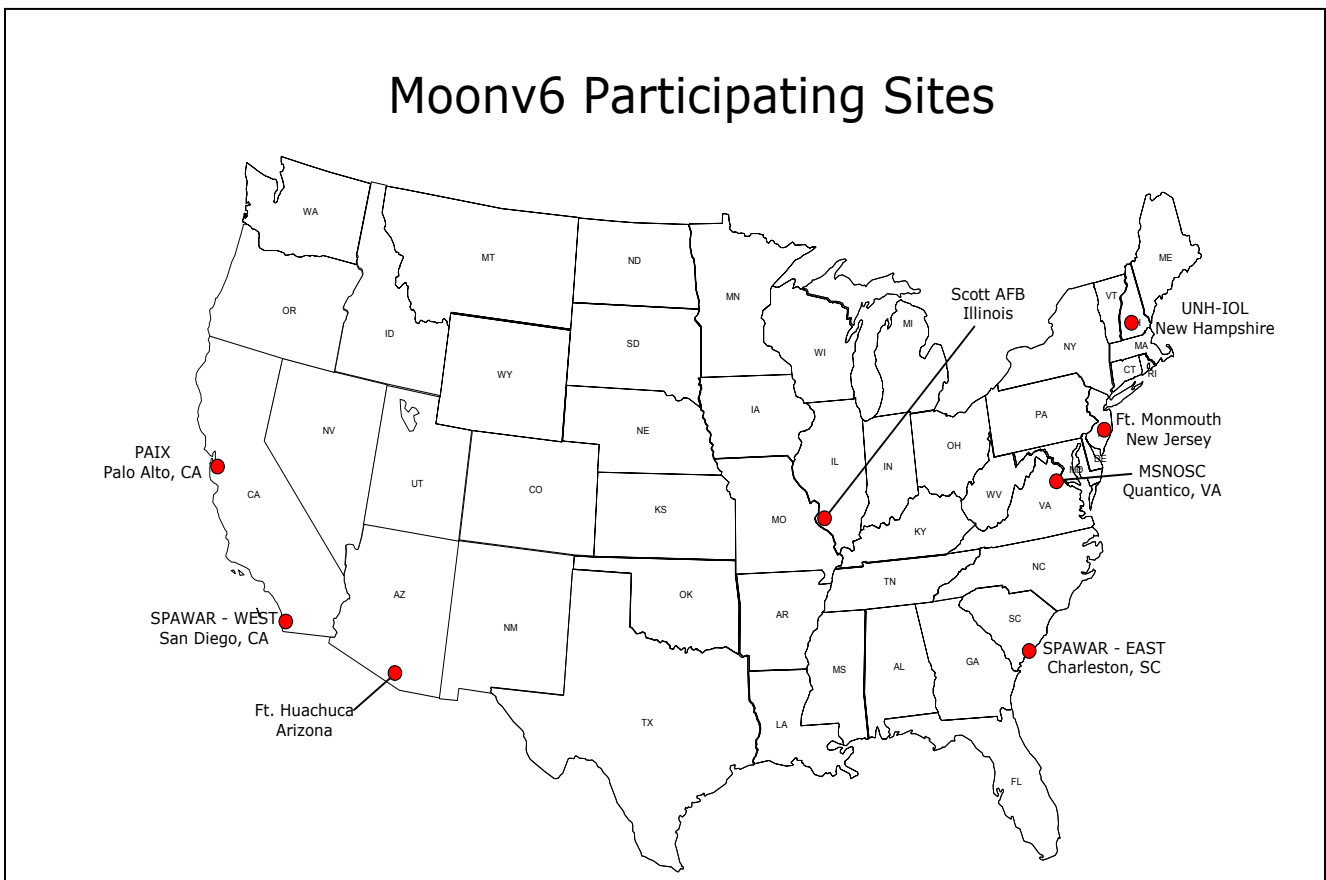


Figure 1: Moonv6 participation sites

4. Who can participate in Moonv6?

Moonv6 is designed to bring together industry, government and academia. Moonv6 is an open event and all vendors with IPv6-enabled product are encouraged to participate. Service providers with an IPv6 interest are also encouraged to contribute. There is no participation prerequisite to be affiliated with the US Department of Defense or the UNH-IOL.

5. Is there a cost to participate?

Yes. The Moonv6 fee for participation is \$2000 USD per company (for equipment and software vendors). This fee will be used to cover cost incurred by UNH-IOL to facilitate the Moonv6 event, including connection fees, lab expenses, and supplies (cables, PCs, etc.). However, current members of the IPv6 Consortium at the UNH-IOL will receive a participation fee waiver.

Service providers that wish to participate should contact Ben Schultz for details.

6. How long will the Moonv6 project last?

The Moonv6 event is segmented into two phases. Phase 1 will begin October 6, 2003 and last until October 17, 2003. Phase II will take place sometime in January 2004.

7. What are the equipment requirements?

Each vendor will be required to leave a representative platform at a minimum of 2 of the participating sites. Given the large number of sites, some vendors have allocated multiple units for the event. Each vendor is encouraged to provide as many platforms as possible. Equipment is only "on loan" and will be returned at the end of the project.

8. How long must the equipment be made available?

The Moonv6 project will remain operational from Phase I until through Phase II, which should occur in the January 2004 time frame. There will be interim testing in which your device(s) will be utilized. Consequently, each vendor will be asked to provide the equipment for approximately seven months.

9. What kind of support is required?

An engineering representative is required to be present at a minimum of one site; although vendors may have an engineering representative at each location their product is present. It is expected that support engineers can remotely configure devices present at the other sites in addition to performing local configuration. Supporting engineers do not need to be onsite for the entire seven months...only for the actual Phase 1 and Phase II events.

Participants should anticipate sending no more than two representatives to any one site due to limited space and access in some locations. Vendors wishing to send more than two engineers to UNH will be required to pay an extra \$500/engineer.

NOTE: If you are sending a representative to the JITC site, please send security information (including clearance levels) to Captain Dixon (the JITC site coordinator) one month early so he can process any administrative issues. Sending foreign nationals as company representatives to the JITC site is not recommended.

10. When should vendor product be available at the participating sites?

According to the schedule, equipment for Phase I should arrive before September 10th, 2003. This will give Moonv6 personnel adequate time to setup, install and configure equipment & applications. Equipment may arrive earlier than September 10, 2003. Delivery dates for Phase II are TBA and will be made available on the website (www.moonv6.org)

11. Is any training required?

It may be necessary for vendors to provide instruction to Moonv6 support staff (IOL, DoD, or Service Provider) on the configuration and support of provided equipment and/or applications prior to Phase 1. Additionally, vendors are asked to provide adequate documentation and also access to support engineers during the hiatus between Phase 1 and Phase II.

12. What will be tested during the Moonv6 event?

Moonv6 is an extensive interoperability and testing event and will cover multiple areas, including:

- Core Protocol Functionality (RFC compliance, tunneling, transition mechanisms, PPP, etc.)
- Router Functionality (RIGng, BGP4+, OSPFv3, integrated IS/IS, etc.)
- Mobility support
- Network support services (DNS, NFS, E-mail and web services, etc.)
- Applications (Streaming media, web browsing, SSH, common business apps, etc.)
- Security (host system security, router security, red teaming)

13. Will results from Moonv6 testing be made available?

UNH-IOL will publish a whitepaper with the Moonv6 testing results. This will be a generic list of issues encountered, temporary solutions (if any) and long-term solutions. It will also document the methodologies used in the testing and the network topologies. Individual vendor results may or may not be included as separate private reports (this is currently TBA).

14. Will vendor specific results from Moonv6 be published?

No. Vendor specific results will be kept private. For reference, UNH-IOL will document specific device behavior and may privately contact individual vendors for an explanation of issues after the event. UNH-IOL may produce feedback reports for participating vendors on their product only.

15. Who should I contact if I want to participate?

Ben Schultz (UNH-IOL)

Desk +1 (603) 862-3332

Mobile +1 (603)205-4180

Email schultz@iol.unh.edu

Captain Roswell Dixon

Desk +1(520)538-5269

Mobile +1 (520) 245-0002

E-mail: dixonr@fhu.disa.mil



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

June 9, 2003

CHIEF INFORMATION OFFICER

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
COMPONENT ACQUISITION EXECUTIVES**

SUBJECT: Internet Protocol Version 6 (IPv6)

**Reference: DoDD 8100.1 Global Information Grid Overarching Policy,
September 19, 2002**

This memorandum provides DoD policy for Enterprise-wide deployment of IPv6. Currently, Internet Protocol version 4 (IPv4) represents the mandated internetworking protocol for the DoD. The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities (ref a), depends on effective implementation of IPv6 in concert with other aspects of the GIG Architecture.

IPv6 is the next generation network layer protocol of the Internet as well as the GIG, including current networks such as NIPRNET, SIPRNET, JWICS, as well as emerging DoD space and tactical communications. Implementation of IPv6 is necessary due to fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting long-term requirements of the commercial community and DoD. IPv6 is designed to overcome those limitations by expanding available IP address space to accommodate the worldwide explosion in Internet usage, improving end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens. Furthermore, IPv6 is designed to run well on the most current high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and without experiencing a significant decrease in capacity on low bandwidth systems.



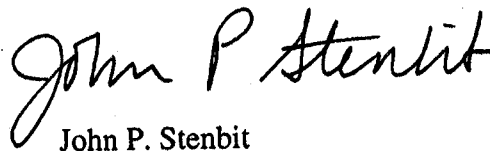
While the precise timing and speed of commercial deployments utilizing IPv6 are uncertain, it is expected to replace IPv4 over the next several years. The significant installed base of IPv4 technology worldwide will likely result in an extended transition period where both protocols coexist. Therefore, a transition to IPv6 presents DoD with a number of opportunities and challenges that must be addressed through an overall enterprise transition strategy. The IPv6 transition across DoD will consider operational requirements, information assurance and costs, while maintaining interoperability within the Department, across the Federal Government, among our allies, and with coalition partners in addition to the civilian and commercial sectors. This overall strategy will be part of the GIG integrated architecture, appropriately recognizing Federal level initiatives and in concert with industry and international standards-making bodies. This memo provides the guidance to ensure that a DoD transition occurs in an integrated, timely and effective manner.

The DoD goal is to complete the transition to IPv6 for all inter and intra networking across the DoD by FY 2008. To enable this transition it is DoD policy for all Information Technology (IT) and National Security Systems (NSS) which make up the GIG (ref a) that:

- As of October 1, 2003, all GIG assets being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities). This explicitly includes all acquisitions that reach Milestone C after October 1, 2003. The next version of the Joint Technical Architecture (JTA) will reflect this requirement.
- Segments of the GIG will complete transition over the time frame from FY 05 to FY 07. These segments and their transition dates will be specified as part of the planning process described herein.
- Specific near-term IPv6 implementation pilots, demonstrations, and testbeds will be identified by the DoD CIO within 30 days as part of the transition planning process described herein. These pilots will be designed to build confidence in facilitating the overall DoD transition to IPv6. DoD Components and Services shall undertake and participate in these activities in an aggressive manner.
- No implementations of IPv6 shall be permitted on networks carrying operations traffic within DoD at this time. This is consistent with the initial results of the information assurance risk assessment of IPv6 security implications done by the Information Assurance Panel of the Military Communications Electronics Board. These implementation guidelines are considered temporary and, in order to meet the above stated goals, will be reconsidered as part of the IPv6 transition plan.

- The Defense Information Systems Agency (DISA) shall acquire IPv6 address space sufficient to meet DoD's five year estimated requirements and initiate acquisition of IPv6 addresses to meet all future DoD requirements by September 30, 2003.
- DISA shall continue to manage DoD IP address allocation, registration and control on an enterprise basis to promote interoperability and security. DISA is the DoD Central Registration Authority (CRA) for assignment and registration of Internet Protocol (IP) address space for any and all DoD sponsored data networks and systems. DISA shall establish and maintain an effective program for accurate management and accounting of all DoD-owned IP addresses. As part of this requirement, DISA shall work with Components and Services to establish an IPv6 address-space and naming convention schema by December 30, 2003.
- DoD users will only acquire IP address space originating from DISA.
- Finally, the DoD CIO will lead, in consultation with the Joint Staff and with the participation of DoD Components and Services, the development of a draft IPv6 transition plan within one month from the date of this memo with completion of the plan within three months from the same date. The IPv6 transition plan for DoD will include:
 - Recommended transition strategy, which includes milestones and criteria for transition of legacy, upgraded, and new IP-based capabilities and systems.
 - Means for adjudicating potential Component claims that a particular GIG asset should not or cannot be transitioned to IPv6 in the timeframes noted above.
 - Recommended technical strategy that supports, for a limited period of time, the coexistence of IPv4 and IPv6.
 - Identification of what needs to be done to ensure readiness for transition, and of the required resources, organizational roles and responsibilities. This includes the early identification of specific implementation pilots necessary to reduce transition risk.
 - Identification of additional policy guidance needed.

The ASD (NII)/DoD CIO focal point for this effort is Ms. Marilyn Kraus, who can be reached at (703) 607-0255 or marilyn.kraus@osd.mil.


John P. Stenbit