NAVY INTERNET PROTOCOL VERSION 6 (IPv6) TRANSITION STRATEGY IN SUPPORT OF NETWORK-CENTRIC OPERATIONS AND WARFARE

Phuong Nguyen, Robert Ferro, Anh Nguyen, Steven Lam, Tuan Nguyen, Timothy Ho,
Roger Ogden, Daniel Greene, Mark Stell, Cam Tran, Albert K. Legaspi
SPAWAR Systems Center Pacific
San Diego, CA

ABSTRACT

Network-centric warfare is the operational concept that provides information sharing amongst a large array of networked nodes, including mobile platforms, sensors, space systems, weapons, munitions and war fighters. This information sharing enhances battle space situation awareness, which allows war fighters to get the right information at the right time and place, and to make the right decisions ahead of adversaries.

IPv6 is an enabling technology of network-centric operations and warfare for improving the scalability, robustness, agility, security, flexibility and manageability of military communication systems. The large address space, built-in stateless node discovery, Internet Protocol (IP) security (IPSec) and mobility functions offered in IPv6 will be an important enabler for information sharing and distribution amongst war fighters in a dynamic battle space environment.

As described in a mid-2003 memo[1]*, to achieve its vision of network-centric operations and warfare, the Department of Defense (DoD) established a goal to transition all military communications networks to IPv6 across the Global Information Grid (GIG), and for all systems that are part of the Defense Information System Network (DISN) that will interoperate with the GIG.*

The purpose of this paper is to present the Navy overall strategy of transitioning its critical network infrastructure to IPv6 to support network-centric warfare and fleet operations. The paper also highlights the U.S. Navy's recent accomplishments, namely the two Joint Staff IPv6 Operational Criteria - Criterion 4 (known as JCS 4) demonstrations of voice, data, and video integration. In addition, the paper discusses the way forward in light of the establishment and deployment of the multi-site Navy Technical Excellence Center with focus on current and future IPv6 test and evaluation – encompassing laboratory tests, field tests (i.e., experiments), demonstrations, and modeling and simulation – to address operational needs and requirements of the war fighters.

1. INTRODUCTION

To meet the DoD mandate for transition to IPv6, the Navy IPv6 Transition Project Office (NITPO) at the Space and Naval Warfare Systems Command Office of the Chief Engineer (SPAWAR 05) has established IPv6 transition strategy for the Navy. This includes the development of the Navy IPv6 Technical Transition Strategy (TTS), participation in all phases of planning, conducting, and reporting test and evaluation related to the Joint Staff IPv6 Operational Criteria, and establishment and deployment of the recently established Navy Technical Excellence Center (NTEC) with emphasis on current and future IPv6 test and evaluation (T&E) to address operational needs of the war fighters.

The remainder of the paper is organized as follows. Section 2 presents background information that includes the Navy IPv6 Technical Transition Strategy and the Joint Staff IPv6 Operational Criteria. Section 3 highlights recent accomplishments in terms of the two demonstrations of voice, data, and video integration over IPv6 related to the Joint Staff IPv6 Operational Criteria - Criterion 4. The way forward in view of the recent establishment and deployment of the Navy Technical Excellence Center is discussed in Section 4. Finally, Section 5 summarizes the paper with concluding remarks.

2. BACKGROUND

This section focuses on background information, technical and operational, that serves as a basis for subsequent sections. In particular, overview and highlights of the Navy IPv6 Technical Transition Strategy and the Joint Staff IPv6 Operational Criteria are provided in this section.

2.1 Navy IPv6 Technical Transition Strategy

The NITPO led the development the Navy IPv6 Technical Transition Strategy (TTS) to provide technical guidance for the key Navy programs to migrate from IPv4 to IPv6. The technical guidance aims to contribute to future enterprise information technology architecture, and to

[1] *ASD NII/DoD CIO Memo, Subject: Internet Protocol version 6 (IPv6)*, dated 9 June 2003.

FORCEnet, for implementation of the Global Information Grid (GIG).

Architectural emphasis concentrates on developing an enterprise level IPv6 addressing plan that aligns Navy to DoD allocation of addresses within a FORCEnet architectural framework. This addressing plan was developed by the Navy IPv6 Networking Working Group (WG) to request a contiguous /23 block of Navy IPv6 addresses for use on naval mobile tactical platforms (ships, submarines, aircraft, and unmanned vehicles) and fixed shore facilities (naval shore facilities and Marine Corps shore facilities). The Navy IPv6 addressing scheme calls for [1]:

- Mobile nodes to use the site/platform method of address assignment: all security enclaves at a site or on a platform are taken from a contiguous block, and thus can be summarized as a single route on the GIG core, regardless of the information assurance (IA) architecture;
- Fixed nodes to use geographical addressing: each site is given an address range from the address block assigned to the Network Operations Center (NOC) that the site uses to connect to the GIG core.

Overall, this IPv6 addressing scheme dovetails toward the following fundamental goals:

- Maximize route summarization (route aggregation) to ensure routing tables are kept small and address space scalable,
- Add flexibility to support many network and IA architectures,
- Minimize risk consistent with good management of IPv6 addresses.

In addition, this technical transition strategy intends to recommend both sequence and timelines for transition to IPv6, with core-to-edge deployment, which begins with Navy's critical infrastructure and ends with applications, so that end-to-end mission capabilities can be enhanced by this version of IP for information transfer, and achievement of the Net-Ready Key Performance Parameters [1]. This strategy is needed to assist program managers of key Navy programs in development of transition plans and budget submissions with technical rationale and justification for Program Objective Memorandum (POM) 08 and beyond.

2.2 Joint Staff IPv6 Operational Criteria

The Joint Staff has identified and issued a set of ten IPv6 operational criteria that must be satisfied for the Chairman of the Joint Chiefs of Staff (CJCS) to testify to Congress that IPv6 fulfills operational requirements of the DoD.

The DoD assigned responsibility for T&E of each criterion to a DoD Component. The responsible organization will coordinate with other DoD Components to plan, conduct, and report on engineering analyses, modeling and simulation (M&S), laboratory testing, and live network testing. Engineering studies and testing results, provided by the responsible DoD Component, will be evaluated by the Joint Staff and the Director, Operational Test and Evaluation (DOT&E) to determine if the criterion has been satisfied.

As listed in the DoD IPv6 Master Test Plan (MTP), the Joint Staff IPv6 Operational Criteria (known as JCS) are ([2], Table 3-1):

1. Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of High Assurance IP Encryptors (HAIPEs), integration of IPSec, and integration with firewalls and intrusion detection systems
2. Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment
3. Demonstrate equivalent to, or better performance than, IPv4 based network
4. Demonstrate voice, data, and video integration.
5. Demonstrate effective operation in low-bandwidth environments
6. Demonstrate scalability of IPv6 networks.
7. Demonstrate support for mobile terminals (voice, data and video)
8. Demonstrate transition techniques
9. Demonstrate ability to provide network management of networks
10. Demonstrate tactical deployability and ad hoc networking.

Each of these criteria is decomposed into levels depending on granularity with associated testable and verifiable measures of performance. In particular, capabilities to be demonstrated are identified at Level 1 decomposition, and specific technology, infrastructure, and functionality to demonstrate Level 1 decomposition are identified at Level 2 decomposition. The DoD IPv6 MTP defines Level 1 and Level 2 decomposition for each JCS; however, further levels of decomposition and specific T&E methods to demonstrate a specific criterion are left to the primary DoD Component responsible to the criterion [2].

The DoD assigned the U.S. Navy the overall responsibility to plan, conduct, and report test and evaluation for Criterion 4 and Criterion 10, known as JCS 4 and JCS 10 ([2], Table 3-1). As scheduled in the DoD IPv6 MTP, the U.S. Navy's current T&E effort concentrates on JCS 4. Two phases of testing and demonstrations associated with JCS 4 were accomplished in FY07. In addition, Level 3 decomposition related to Scalability and End-to-End Security has been identified.

3. NAVY'S IPV6 DEMONSTRATIONS OF VOICE, DATA, AND VIDEO INTEGRATION

The U.S. Navy has been conducting, in phases, T&E activities related to JCS 4 to demonstrate simultaneous voice, data, and video over shared IPv6 networks. Two phases have been completed. The first phase of JCS 4 demonstration was conducted as a test event within the collaborative Moonv6 project in FY07. The Moonv6 project consists of the University of New Hampshire InterOperability Lab (UNH-IOL), the North American IPv6 Task Force (NAv6TF), Internet2, the Joint Interoperability Test Command (JITC), and other DoD agencies and services, including the U.S. Army, Air Force, Navy, and Marines. The objective of this test is to demonstrate Quality of Service (QoS) capabilities of IPv6 networks using Differentiated Services (*DiffServ*) [3-5].

The second phase of the JCS 4 test [6] was intended to demonstrate (i) transport control capabilities of IPv6 networks using Real-Time Transport Protocol (RTP) [7], and (ii) session signaling capabilities of IPv6 networks using the Session Initiation Protocol (SIP) [8].

Salient details and main results of, as well as key lessons learned from the two demonstrations are presented in the next two subsections.

3.1 JCS 4, Phase 1 – Moonv6 Demonstration of QoS Capabilities of IPv6 Networks Using *DiffServ*

During the first phase of a JCS 4 T&E, the U.S. Navy conducted both laboratory test and wide-area network (WAN) test. While the laboratory test was set up in a controlled and geographically confined environment, the WAN test was more realistic as it was subject to real-world conditions. Specifically, the WAN test was scheduled from 31 October through 17 November 2006 as a FY07 Moonv6 test event between a testbed located at SPAWAR Systems Center Pacific (SSC Pacific) in San Diego, California, and another test setup at JITC, Fort Huachuca, Arizona. Figure 1 depicts the test setup and environment for the Moonv6 demonstration of QoS capabilities of IPv6 networks using *DiffServ* for service differentiation.

The objective of this distributed testing was to demonstrate the marking of the IPv6 packets with *DiffServ* code points (DSCPs) at Edge Routers and transmission to a remote site across a domain that simulates the GIG and its *DiffServ* policy via the Defense Research and Engineering Network (DREN). The key feature of the FY07 Moonv6 demonstration was the implementation of DSCP markings for four traffic categories — Voice (signaled), Video (signaled), Chat, and Web Browsing — based on the DSCP assignment scheme proposed by the GIG QoS Working Group (WG) [5] to enable end-to-end QoS interoperability across the GIG.

As illustrated in Figure 1, test traffic was generated at SSC Pacific by an IxChariot Endpoint, a software-based traffic generator and application emulator hosted on a PC, and SmartFlow, a software-based traffic generator hosted on a SmartBits chassis. Generated traffic was marked with appropriate DSCP values at the Edge Router before transmitting to a remote site by way of DREN. On the receiver site at JITC, an IxChariot Endpoint was attached to the GIG core via an Edge Router that was configured to mark IPv6 packets according to DSCP assignments proposed by the GIG QoS WG.

The Moonv6 demonstration successfully verified that IPv6 packets could be marked with DSCPs, transmitted to remote site of a wide-area network of the GIG via DREN, and received at the remote end with the same DSCP values, i.e., DSCP markings were successfully passed via the simulated GIG core network at JITC.

During the Moonv6 demonstration, IPv4-in-IPv4 and IPv6-in-IPv4 tunnels were configured between the Edge Router at SSC Pacific and the CE (Customer Edge) Router (i.e., router at the customer premises) at JTIC, Fort Huachuca. As such, all traffic was tunneled via DREN as Generic Routing Encapsulation (GRE)-encapsulated IPv4 packets. Attempts to tunnel IPv6 traffic via an IPv6 tunnel across DREN failed due to a possible bug in the firewall software installed on Juniper network devices. As a result, DREN administrators were notified and they subsequently submitted a trouble report to Juniper Networks to have the problem fixed.

In conjunction with the Moonv6 demonstration, laboratory testing was extensively conducted to verify basic QoS functionality using the *DiffServ* mechanism for a commercial off-the-shelf (COTS) Cisco router that was used as Edge Routers for the two test sites illustrated in Figure 1.

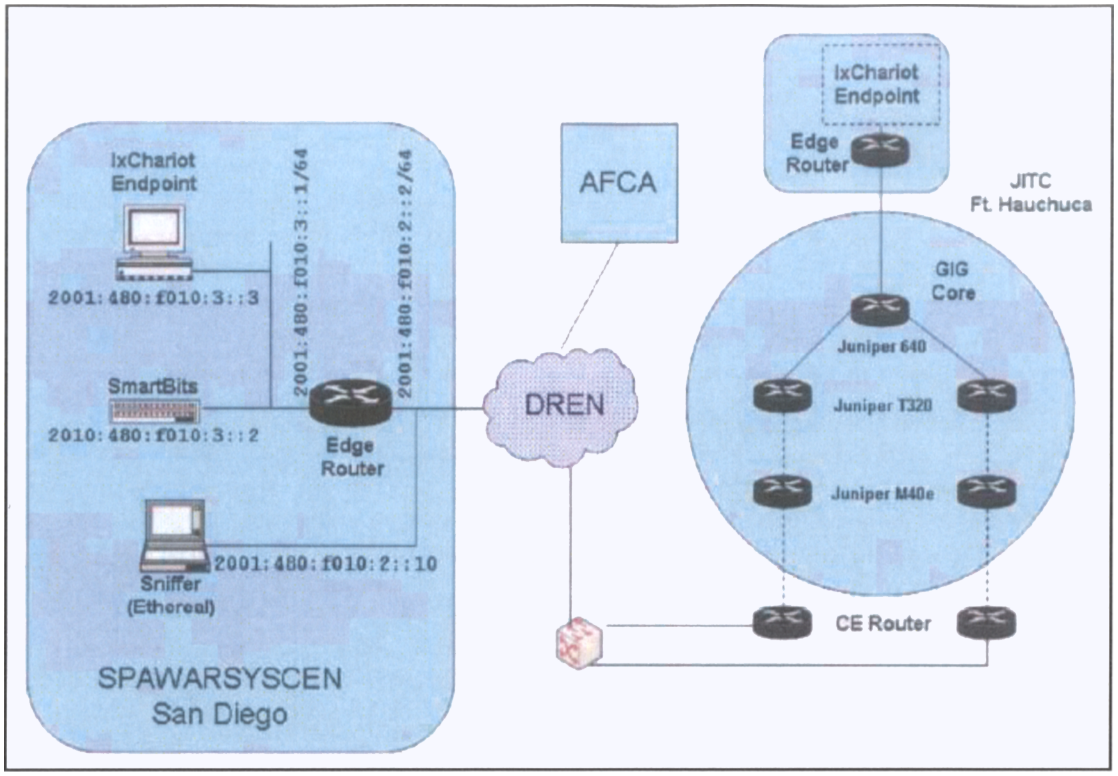

Figure 1. Test Setup for the JCS 4, Phase 1 (Moonv6) Demonstration

Laboratory test results showed that the router under test supported basic functionality when using *DiffServ* service differentiation to provide QoS for different traffic classes (Voice, Video, and Data). One deficit found was that the Low Latency Queuing (LLQ) — for assigning high priority to voice traffic to reduce latency and jitter — was not supported by Cisco IOS (Internetwork Operating System) during the test period. A workaround using the Priority Queuing (PQ) was configured for the voice traffic to yield approximately the same functionality.

In addition, the U.S. Navy IPv6 T&E Team has identified Level 3 decomposition for *DiffServ* capabilities in terms of Scalability and End-to-End Security that require further testing, and modeling and simulation (M&S).

3.2 JCS 4, Phase 2 — Demonstration of Real-Time Transport Protocol (RTP) and Session Initiation Protocol (SIP) Capabilities over an IPv6 Network

The objective of the second phase was two-folded: (i) to demonstrate transport control capabilities over IPv6 using Real-Time Transport Protocol (RTP); and (ii) to demonstrate session signaling capabilities over IPv6 using Session Initiation Protocol (SIP) [6].

Overall, RTP and SIP are enabling technologies — SIP, an application-layer control protocol widely used for signaling Voice over IP (VoIP), multimedia distribution, and multimedia conferences; and RTP, on top of User Datagram Protocol (UDP), providing a real-time transport mechanism for use in application-layer control (signaling) protocols including SIP. As specified by RFC 3550, RTP provides end-to-end network transport functions for applications transmitting real-time data, typically voice and video. Without a flow control mechanism, RTP is augmented by the RTP Transport Control Protocol (RTCP), also called Real-Time Transport Control Protocol, that allows monitoring of data delivery to support scalability in large multicast networks, and provides minimal control and identification functionality. The primary function of RTCP is to provide feedback on the quality of data distribution [7]. SIP, as specified by RFC 3261, is a general-purpose tool for creating, modifying, and terminating sessions that works independently of underlying transport protocols as well as the type of session being established. Similar to HyperText Transfer Protocol (HTTP), SIP provides a text-based request-response transaction mode [8]. With the explosive growth of and demand for multimedia applications, SIP has become a prominent element of the

IP Multimedia Subsystem (IMS) architecture for delivering IP multimedia to mobile users.

Test and evaluation for the second phase of JCS 4 was carried out at SPAWAR Systems Center San Diego. Figure 2 provides a notational test setup and environment of the SIP-RTP testbed.

The software application eyeBeam version 1.5 (CounterPath, http://www.counterpath.com) was selected, after deliberation, from a list of Softphones because it supported SIP and RTP/RTCP protocols over IPv4, and, during the period of testing, a beta version over IPv6 was made available. Furthermore, it was (and is) a full-featured, COTS application with the potential of wide spread use due to its low cost.

As depicted in Figure 2, the eyeBeam 1.5 Softphone and the software-based traffic generator IxChariot were installed on two laptops and one desktop. The three nodes were connected either in an IPv4 (only) network or IPv6 (only) network by three routers via two satellite simulators (denoted as Link Simulators in Figure 2).

Capabilities of the SIP and RTP/RTCP protocols over IPv6 and IPv4 were compared when testing the following:

- Voice Transfer (one-to-one), using the Voice Speedex Wideband FEC (64K) Codec
- Video Transfer (one-to-one), using the High Quality H.326 Codec
- Data Transfer – Instant Messaging (IM) using the SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) protocol suite from the Internet Engineering Task Force (IETF) [9]

During the test, jitter, and latency were measured by IxChariot, bandwidth was measured by Ethereal — now known as Wireshark — (denoted as Sniffer in Figure 2), and call quality was subjectively evaluated by the Mean Opinion Scoring (MOS) technique.

Test results showed that audio call quality over IPv6 was virtually indistinguishable compared to IPv4. There was a small increase in bandwidth usage corresponding to IPv6's larger header size. Jitter and latency were significantly greater than those of IPv4 but not enough to make a difference in voice quality of the call in this test setup and environment.

Video connections were also found to be virtually indistinguishable from the same video transfers over IPv4. Jitter and latency were again greater for IPv6, but not enough to make a difference in perceived video quality under test conditions.

For data transfers using Instant Messaging (IM) feature of eyeBeam 1.5 Softphone, no difference was found in the operation or quality of IM over IPv4 and IPv6.

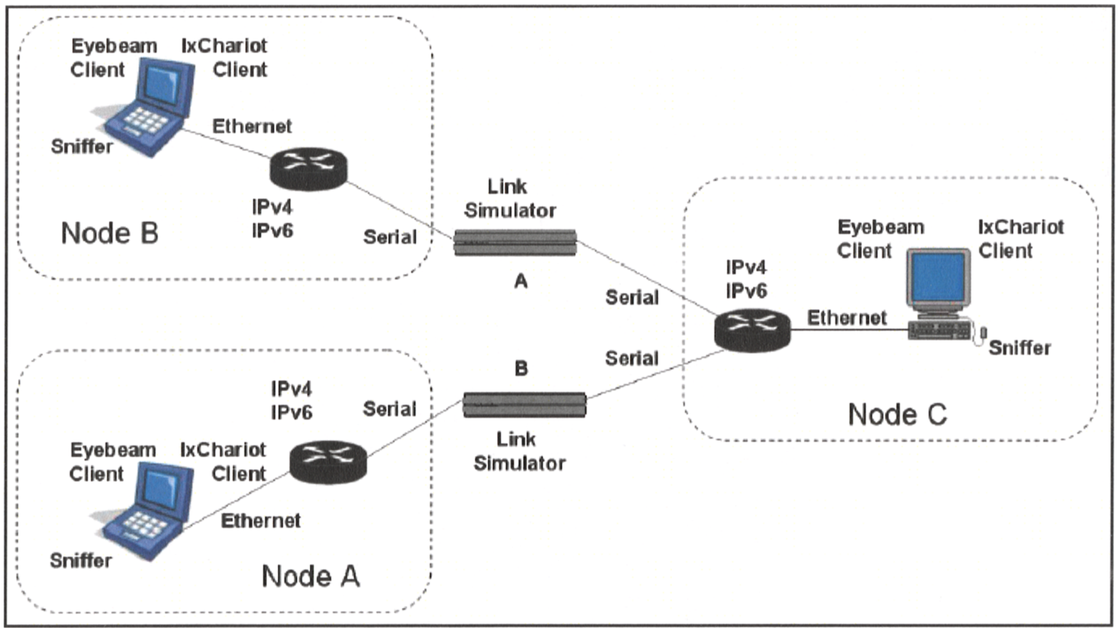

Figure 2. Test Setup for the SIP-RTP/RTCP Testbed of the JCS 4, Phase 2 Demonstration

Overall, there was no perceived difference in the quality of voice, video, and data transfers during operation of the eyeBeam 1.5 Softphone over IPv4 and IPv6 in the controlled lab environment. While the basic operational functionality of SIP and RTP/RTCP were successfully demonstrated and their comparable performance confirmed, the Navy IPv6 T&E Team has identified Level 3 decomposition for SIP capabilities related to Scalability and End-to-End Security that require further testing, and modeling and simulation (M&S).

4. THE WAY FORWARD: THE NAVY TECHNICAL EXCELLENCE CENTER (NTEC)

According to the publication *Joint Net-Centric Operations Campaign Plan* [10] developed by the Joint Community Warfighter (JCW) Chief Information Officer (CIO), also serving as the Joint Staff/J-6 Director,

> "*The transition to IPv6 will be a gradual, market-driven process dictated by industry's distribution of IPv6 standards, equipment and services. The joint community requires a strategy and means to validate performance of essential network services during DoD migration to IPv6.*" ([10], page 15)

To validate performance and capabilities of IPv6, the DoD has developed the IPv6 Master Test Plan [2] that includes the Joint Staff IPv6 Operational Criteria. In this forward direction, the Navy IPv6 Transition Project Office (NITPO) has recently taken the initiative to establish the Navy Technical Excellence Center (NTEC), a multi-site IPv6 Laboratories located at the SPAWAR Systems Center Pacific, San Diego, California; the SPAWAR Systems Center Pacific C4ISR Department (Code 5200), Pearl Harbor, Hawaii; and U.S. Naval Research Laboratory (NRL), Washington, D.C. The primary mission of NTEC is to conduct current and future IPv6 test and evaluation to meet operational requirements of the war fighters. Figure 3 depicts, by way of a notational setup, the distributed laboratory environment of NTEC that is interconnected via DREN utilizing transport connections of OC-12 (with transmission speeds of up to 622.08 Mbps) or greater.

NTEC is being developed and deployed in phases to support not only "core" users but also "edge" users (i.e., "first tactical mile" users) by leveraging various operational scenarios such as ship-to-ship, ship-to-shore, ship-to-shore-to-ship, and aircraft reach-back to the shore via ship or airborne relay.

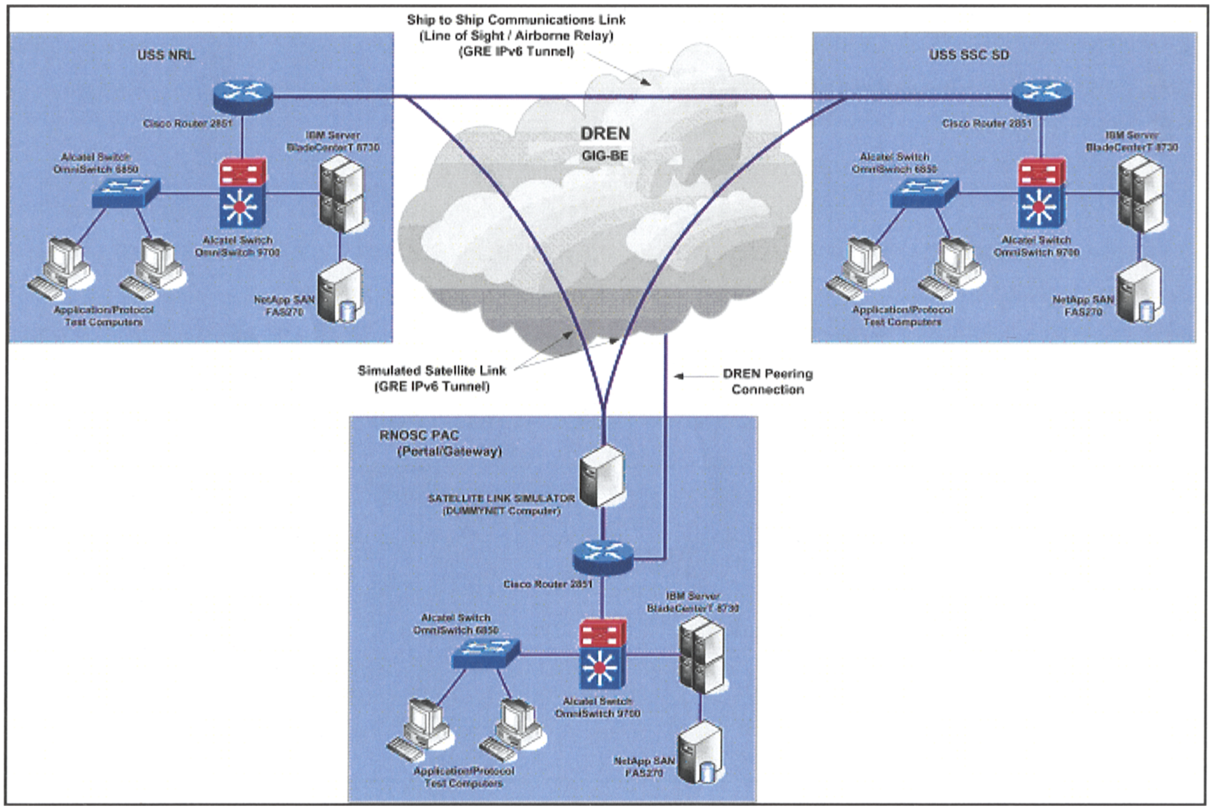
Ship to Ship Communications Link
(Line of Sight / Airborne Relay)
(GRE IPv6 Tunnel)
USS NRL
Cisco Router 2851
IBM Server BladeCenterT 8730
Alcatel Switch OmniSwitch 6850
Alcatel Switch OmniSwitch 9700
NetApp SAN FAS270
Application/Protocol Test Computers
DREN
GIG-BE
USS SSC SD
Cisco Router 2851
IBM Server BladeCenterT 8730
Alcatel Switch OmniSwitch 6850
Alcatel Switch OmniSwitch 9700
NetApp SAN FAS270
Application/Protocol Test Computers
Simulated Satellite Link
(GRE IPv6 Tunnel)
DREN Peering Connection
RNOSC PAC
(Portal/Gateway)
SATELLITE LINK SIMULATOR
(DUMMYNET Computer)
Cisco Router 2851
IBM Server BladeCenterT 8730
Alcatel Switch OmniSwitch 6850
Alcatel Switch OmniSwitch 9700
NetApp SAN FAS270
Application/Protocol Test Computers

Figure 3. Notational Setup Illustrating the Distributed IPv6 Laboratory Environment at the multi-site NTEC

IPv6 T&E activities, as defined by the DoD IPv6 Master Test Plan [2], include laboratory tests, modeling and simulation (for scalability testing), demonstrations, field tests (i.e., experiments). A list of T&E activities are being identified for the evaluation of IPv6 network architectures, functionalities, protocols, and applications to meet current and future DoD initiatives and operational requirements. These IPv6 T&E activities provide solutions for addressing operational issues involved early implementations taking advantage of advanced IPv6 features and related technologies including auto-configuration, the enhanced Open Shortest Path First (OSPF) v3 routing protocol, IPSec (HAIPE dynamic discovery), and mobility to support a typical operational scenario such as aircraft reach-back to the shore via ship or airborne relay. Lessons learned from T&E activities provide critical feedback during the IPv6 transition.

5. CONCLUDING REMARKS

Internet Protocol (IP) has become the corner stone of military communications networks. As an enabling technology, IPv6 can help improve scalability, robustness, agility, security, flexibility and manageability, as well as facilitate and innovate services and applications. However, little is known about the actual performance and capabilities of networks, devices, applications and services over IPv6 in operational environments.

The Navy IPv6 Transition Project Office (NITPO) has established an IPv6 transition strategy in supporting the DoD network-centric operations and warfare exemplified by the IPv6 Technical Transition Strategy (TTS) to assist program managers of key Navy programs in development of transition plans and budget submissions including technical rationale and justification for POM08 and beyond. Furthermore, SPAWAR Systems Center Pacific has been representing the NITPO/Navy in JCS 4 testing to demonstrate voice, data, and video integration. Two phases of JCS 4 testing were successfully completed in FY07 with the first phase demonstration conducted jointly with JTIC as a Moonv6 test event.

To meet operational requirements of the war fighters, the NITPO has established the distributed Navy Technical Excellence Center (NTEC) with emphasis on IPv6 T&E activities that encompass laboratory tests, experiments, demonstrations, and modeling and simulation as described in the DoD IPv6 Master Test Plan. The establishing and deploying of the NTEC together with other NITPO's IPv6 activities underline the U.S. Navy's way forward in supporting network-centric operations and warfare.

REFERENCES

[1] Department of Navy, *Navy Internet Protocol Version 6 (IPv6) Transition Strategy,* Version 1.0, 1 August 2005; signed by RDML Kenneth W. Deutsch, Director, Warfare Integration (N6F/N83), 22 March 2006.

[2] Department of Defense, *Internet Protocol Version 6 Master Test Plan,* Version 2.0, September 2006.

[3] Navy IPv6 Transition Project Office, *JCS Criterion 4, Phase 1: Demonstration of QoS Capabilities of IPv6 Using DiffServ (FY07 Moonv6 Demonstration): Test Report,* 23 December 2006.

[4] Nichols, K.; Blake, S.; and Baker, F., *Definition of the Differentiated Services Field (DS Filed) in the IPv4 and IPv6 Headers,* RFC 2474, December 1998.

[5] GIG QoS Working Group, *NCID T300 v3 QoS Draft DSCP Proposal-Proposal 2,* 21 July 2006.

[6] Navy IPv6 Transition Project Office, *JCS Criterion 4, Phase 2: Demonstration of Real Time Transport Protocol (RTP) and Session Initiation Protocol (SIP) Capabilities Over an IPv6 Network: Test Report, v1.0,* 27 September 2007.

[7] Schulzrinne, H.; Casner, S.; Frederick, R.; and Jacobson, V., *RTP: A Transport Protocol for Real-Time Applications,* RFC 3550, July 2003.

[8] Rosenberg, J.; Schulzrinne, H.; Camarillo, G.; Johnston, A; Peterson, J.; Sparks, R.; Handley, M.; and Schooler, E., *SIP: Session Initiation Protocol,* RFC 3261, June 2002.

[9] SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), http://www.ietf.org/html.charters/simple-charter.html

[10] Joint Community Warfighter (JCW) Chief Information Officer (CIO) (Director, Joint Staff/J-6), *Joint Net-Centric Operations Campaign Plan,* October 2006, http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf