UNITED STATES MARINE CORPS
INTERNET PROTOCOL VERSION 6 (IPV6)
TRANSITION PLAN

Release 1.0

30 July 2004

Prepared by:

Headquarters Marine Corps Command, Control, Communications, and Computers
Plans and Policy Division

Table of Contents

Tables

Figures

Program of Record Survey Responses

1 INTRODUCTION

1.1 Overview

In a series of three policy memoranda, the Assistant Secretary of Defense for Networks and Information Integration (ASD NII), also designated Department of Defense Chief Information Officer (DoD CIO), established the goal of transitioning all DoD enterprise-wide networks from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6). The memoranda set the goal of completing transition by Fiscal Year (FY) 2008. This transition plan constitutes the Marine Corps' component of the DoD transition plan.

The Naval Transformation Roadmap describes a transformational process that focuses on accelerating the speed and accuracy of information gathering, assessment, decision and action at every level of command. The Roadmap identifies FORCEnet as the integral Naval component of Global Information Grid (GIG). Naval Power 21 and the Naval Operating Concept (NOC) state that FORCEnet enables Sea Strike, Sea Shield, Sea Basing, Sea Warrior, Sea Enterprise, Sea Trial, Expeditionary maneuver Warfare (EMW), Operational Maneuver from the Sea (OMFTS), and Ship to Objective Maneuver (STOM). All of these warfare concepts require a network that links disparate systems and provides end-to-end connectivity for sensors and data. IPv6 has been designated as the network layer protocol to provide internetworking capability to the GIG.

IPv4 is the currently mandated internetworking protocol for all DoD. The achievement of net-centric operations and warfare depends on effective implementation of IPv6. The transition from IPv4 to IPv6 involves wholesale analysis and testing of current information technology. A large number of hardware and software systems including applications will need to be upgraded or replaced. Major assessments will need to be made with regard to engineering, procurement, testing, and deployment. During the transition phase, new or modified IPv6-capable systems and applications will need to interoperate with the existing IPv4 systems and applications without degradation in performance, reduction in availability, or compromise of security.

The Marine Corps will meet the transition challenge with an integrated enterprise approach combining planned product replacements and spiral development with aggressive gap analysis to identify those systems without a defined path to IPv6. New systems acquired and procured will be IPv6 capable; those new systems that cannot meet this goal will have a contractual path to IPv6 for the future. Legacy systems that cannot or should not be upgraded to IPv6 will be addressed case by case.

1.2 IPv6 Drivers

ASD NII directed transition to IPv6 due to the fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting the long-term requirements of the DoD. The DoD goal is to complete the transition to IPv6 for all inter and intra networking across the DoD by FY 2008. IPv6 is a key enabler to the strategic network tenets of Marine Corps Enterprise Information Technology Services, Net-Centric Enterprise Services, FORCEnet, and the Global Information Grid (GIG).

In January 1996, the Internet Engineering Task Force (IETF) adopted an improved version of IP – that is, IPv6 – as the replacement for the current version. IPv6 uses 128 bits to represent addresses. In addition, other improvements were made relative to IPv4, based on a generation of experience. Highlights of the IPv6 improvements are listed below. More detail can be found in the IPv6 Transition Assessment Guide in Appendix A.

- New Header Format – The streamlined IPv6 header is more efficiently processed at intermediate routers.
- Large address space – IPv6 has 128-bit (16-byte) source and destination addressing allowing over 3.4 x 10^{38} possible combinations.
- Efficient and Hierarchical Addressing and Routing Infrastructure – IPv6 global addresses create an efficient routing infrastructure.
- Stateless and Stateful Address Configuration – An IPv6 host can automatically configure itself without the use of a stateful configuration protocol such as Dynamic Host Configuration Protocol (DHCP).
- Built-in Security – Support for IPSec is an IPv6 protocol suite requirement.
- Better Support for QoS – Because the traffic is identified in the IPv6 header, support for QoS can be achieved even when the packet payload is encrypted through IPSec.
- New Protocol for Neighboring Node Interaction – The Neighbor Discovery protocol allows more efficient multicast and unicast Neighbor Discovery messages.
- Extensibility – IPv6 can easily be extended for new features by adding extension headers after the IPv6 header.

1.3 IPv6 Transition Approach

The improvements in IPv6 have led to a different IP header and suite of options. Anything in a network that deals directly with the IP layer (or interprets or manipulates an IPv4 address) will be affected by IPv6, or will have to coexist with it. Any application that requests network services may be affected. This includes computer operating systems, routers, networked printers and copiers, network management systems, video teleconferencing (VTC) systems, network servers, firewalls, intrusion detection systems, network encryptors, and tactical systems.

IPv6 is not directly backward compatible with IPv4. Therefore, various mechanisms have been developed to allow the two protocols to coexist and interoperate during the transition phase from IPv4 to IPv6. These mechanisms include (1) incorporating both IPv4 and IPv6 support in routers and computers (dual stacking), (2) tunneling IPv6 traffic through IPv4 networks (and vice versa), and (3) placing translation gateways between IPv4 and IPv6 networks. Coexistence of IPv4 and IPv6 introduces security concerns, complexity, and limitations that would not exist on a pure IPv4 or IPv6 network. However, these mechanisms are required to transition from IPv4 to IPv6 on Marine Corps networks.

During transition, the Marine Corps will use these mechanisms as required to maintain interoperability across the MCEN between IPv4 and IPv6 networks. ASD NII has established the goal of enabling IPv6 on all DoD networks by FY 2008. However, many legacy systems will need to coexist with IPv6 networks beyond this established date due to fiscal or programmatic constraints.

The Marine Corps is undergoing a transformation of the Marine Air Ground Task Force (MAGTF). The MAGTF will provide an increased range of options for regional engagement, crisis response, and sustained land force operations using Sea Basing and Ship to Objective Maneuver (STOM). Program offices for many of the systems that will be used beyond 2008 have already been established. Transition of these systems is particularly critical to achieving IPv6 internetworking. Systems that will support the MAGTF in 2008 and beyond include: Tactical Data Network (TDN) for networked tactical data communications, Transition Switch Module (TSM) for tactical voice communications, Joint Tactical Radio System (JTRS) for wireless tactical communications, and Command and Control On-the-move Network Digital Over-the-horizon Relay (CONDOR) for expeditionary data bridging of dispersed combat nodes.

IPv6 has additional features beyond just a larger address space. The merit of these other IPv6 features will be identified as a detailed architecture for the future MAGTF and its component systems is developed. The operational and technical requirements for the MAGTF will evolve with time.

1.4 Structure of Marine Corps IPv6 Transition Plan

The structure of the Marine Corps IPv6 Transition Plan is intended to support the concept of operations for achieving transition. Chapter 2 starts with the high level policies directing the transition, progresses to Marine Corps specific guidance, and then outlines how the Marine Corps will manage implementation of the guidance. Roles and responsibilities of agencies involved in the transition are identified.

The first step to transitioning to IPv6 is ensuring that information technology purchased from this point forward offers the IPv6 capability that will be needed by 2008. Procurement guidance and acquisition directives mandating incorporation of IPv6 capability into current activities are presented in Chapter 3. The waiver process for systems and software that will not transition is also addressed.

Chapter 4 presents the plan of action and milestones (POA&M) for transitioning Marine Corps networks to IPv6. Coordinated, intelligent transition requires accurate knowledge of the ability of individual programs and software applications to support the transition. Appendix A contains an assessment guide to aid individual program managers and software functional area managers in completing a survey for their system or application. The survey for programs of record is presented in Appendix B and the survey for software applications is in Appendix C. Armed with the timelines and funding requirements identified in survey responses, Marine Corps transition managers can then determine the critical path for executing transition to IPv6 and manage efforts and resources to transition interrelated and dependent systems in the most efficient manner. The transition to IPv6 must not interrupt operational communications.

Chapter 5 covers programs and budgets from DoD and USMC. Funding will likely drive execution of transition and this chapter will present the budget for IPv6 effort.

Appendices D and F contain a roll up all applications and systems in USMC inventory and annotates when each is anticipated to be IPv6 capable.

2 IPV6 TRANSITION GOVERNANCE

2.1 Policies

2.1.1 DoD Policy

To achieve the stated goal of completing the transition to IPv6 for all DoD networking by FY 2008 in an integrated, secure, and effective manner, a set of near-term actions were tasked by the 9 June DoD ASD NII policy memorandum. These are:

- As of October 2003, all GIG assets being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems),
- Significant portions of the GIG will transition to IPv6 between FY 05-07 to build confidence for completing the transition,
- DISA will acquire and manage IPv6 addresses for DoD; including the establishment of address and naming conventions,
- No IPv6 implementations on networks carrying operations traffic within DoD at this time *(*This is a temporary measure to ensure that security concerns during a transition are addressed in the transition plan.), and
- The development of an IPv6 Transition Plan.

The Office of the DoD CIO (in consultation with the Joint Staff) was tasked to lead the development of a DoD transition plan.

2.1.2 Marine Corps Policy

Marine Corps' policy governing transitioning to IPv6 will comply with the directives and guidelines issued by the DoD. The Marine Corps will participate with DISA and various Joint agencies to develop DoD and Joint policies to assure continuity among all the Services. HQMC C4 is leading the development of the Marine Corps transition plan and will represent the Marine Corps as a member of the DoD IPv6 Transition Implementation Panel. A Marine Corps IPv6 Transition Planning Working Group comprised of subject matter experts (SMEs) has been established to identify affected Marine Corps programs and execute specific tasks necessary to transition to IPv6. In accordance with DoD policies, the Marine Corps will:

- Propose, coordinate, and implement IPv6 pilots
- Participate in IPv6 working groups and management structure
- Implement IPv6 procurement requirements
- Establish a waiver process for IPv6 non-compliance
- Plan, program for, engineer, test, and transition Marine Corps networks
- Use DISA to obtain IPv6 addresses
- Compile a list of software that directly interfaces with IP, and determine how it will be addressed for IPv6

- Train network managers and planners.

2.1.3 Definitions

2.1.3.1 IPv6 Capable

An IPv6 capable system or product will be capable of receiving, processing, and forwarding IPv6 packets, and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific current criteria to be IPv6 capable are:

- Conformant with JTA developed IPv6 standards profile
- Maintaining interoperability with IPv4
- Existence of migration path and commitment to upgrade as IPv6 evolves
- Availability of contractor/vendor IPv6 technical support

2.1.3.2 IPv6 Compliant

In cases where procuring, acquiring or developing IPv6 capability is not currently possible then such acquisitions, systems or programs will be considered compliant if a funded contractual commitment to upgrade to IPv6 by the beginning of FY 2007 is in place. Alternatively, IPv6 compliance exists if a documented IPv6 capable technology refresh program will be fielded by the beginning of FY 2007.

2.1.3.3 IPv6 Enabled

Identification as IPv6 enabled is based solely on manufacturer's claims and testing. This is a commercial classification and is not currently associated with any government sponsored testing. One possible indicator would be the IPv6 Ready Labels shown in Figure 1 and found at http://www.ipv6ready.org/frames.html.

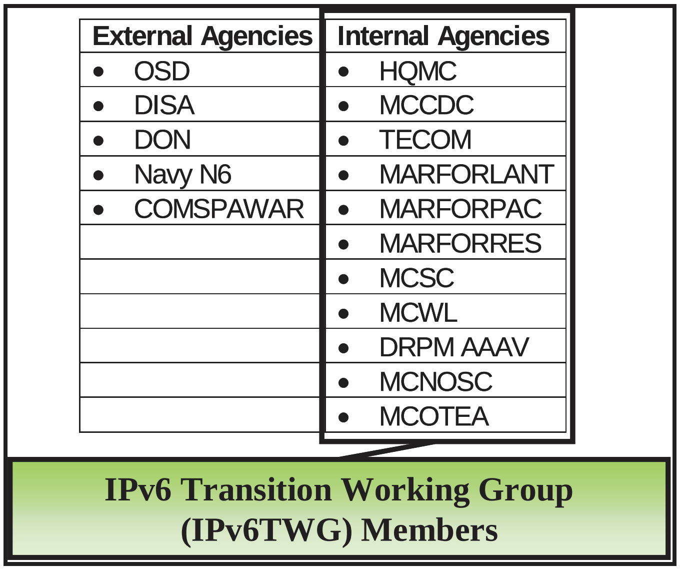
Figure 1. IPv6 Ready Logos

2.2 Transition Management Structure

The transition from IPv4 to IPv6 is a task of great magnitude and complexity. The scope of the transition extends to every system, network, program, device, or component of the GIG that uses IP in any manner. It includes the obvious communications systems, as well as the more obscure elements such as sensors and weapon systems. It also includes both the tactical and the supporting (garrison) domains of the Marine Corps.

To meet this unique challenge, the Marine Corps has established the IPv6 Transition Working Group (IPv6TWG) to serve as the umbrella organization to regulate and control the governance, development, implementation, and management of the transition. To manage change throughout such a broad spectrum of systems, it is imperative that the transition strategy be developed in cooperation with all of the agencies and organizations that are affected or impacted by the transition. Figure 2 shows the members of the IPv6TWG. Roles and responsibilities of each are discussed in Section 2.3 below.

HQMC C4 and the IPv6TWG will direct and coordinate efforts of internal agencies, program managers, acquisition professionals, commanders, comptrollers, contracting officers, and purchasing officials. Additionally, HQMC C4 will serve as a conduit for coordinating Marine Corps efforts with external agencies to ensure that IPv6 is implemented simultaneously on inter-dependent platforms. IPv6 transition on systems with cross-service dependencies must be coordinated to prevent adverse impact on operational capabilities and communications.



External Agencies	Internal Agencies
• OSD	• HQMC
• DISA	• MCCDC
• DON	• TECOM
• Navy N6	• MARFORLANT
• COMSPAWAR	• MARFORPAC
	• MARFORRES
	• MCSC
	• MCWL
	• DRPM AAAV
	• MCNOSC
	• MCOTEA

Figure 2. IPv6 Transition Managers

2.3 Roles and Responsibilities

2.3.1 IPv6 Transition Working Group (IPv6TWG)

The IPv6TWG will coordinate all aspects of the transition, including governance, acquisition and procurement, POA&M, and Programs and budgets. Marine Corps efforts will be coordinated across all DoD by identifying the applicable points of contact and incorporating DoD guidance in Marine Corps policy. Responsibilities of the IPv6TWG are:

- Coordinate Marine Corps activities with the transition efforts of external agencies

- Involve OPFORs in transition planning
- Capitalize on lessons learned from Y2K planning to guide IPv6 transition efforts
- Provide Marine Corps briefings to internal and external agencies
- Generate and update the Marine Corps IPv6 Transition Plan as required

2.3.2 HQMC

HQMC C4 will establish and lead the IPv6 Transition Working Group and develop policy for the Marine Corps implementation of IPv6. Establish a strategy for transitioning Marine Corps systems and networks to IPv6 capability.

CIO will ensure applications on the software baseline are assessed and enforce transition policies through institution of a waiver process. The survey in Appendix C will be used to report IPv6 transition plans for software applications.

2.3.3 MCCDC

MCCDC will assess the Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities (DOTMLPF) impact of IPv6 implementation and recommend or implement required changes. Ensure IPv6 is included in requirements documents.

2.3.4 TECOM

Assess impact of IPv6 transition on formal schools and recommend or implement required changes.

2.3.5 Marine Forces Commanders

Represent the OPFORs needs and serve as a conduit to affect IPv6 transition in the OPFORs. Assess the impact of IPv6 transition on the OPFORs. Provide survey data for locally procured non-Program of Record (POR) systems and application software.

2.3.6 Acquisitions Community

COMMARCORSYSCOM and DRPM AAAV will ensure all applicable acquisitions are IPv6 capable and compliant in accordance with IPv6TWG definitions and DoD, DoN, and HQMC policy and guidance; assess impact of IPv6 transition on programs of record and recommend or implement required changes. Also:

- Provide new or improved capabilities offered by IPv6 earlier in the system life cycle if feasible.
- Minimize the need to retrofit solutions and upgrades for systems currently being developed by acquiring IPv6 capable products now.
- Mitigate the risks associated with new technology or protocol adoption through program management best practices.

- Assess cost and scheduling impacts of IPv6 transition. Complete the survey in Appendix B for each Program of Record. Chapter 4 provides amplifying instructions for completing the survey.

Due to the large number of programs that must implement IPv6, coupled with the technical and logistical complexities of each program, it will be the responsibility of the Product Group Directors (PGDs) and their Program Managers to create their own IPv6 transition plans and establish individual timelines for IPv6 adoption. Funding priorities should be established by realistically balancing the cost of transition against relevance to the warfighter. Every effort should be made to accomplish transition using already programmed technology refresh funding. Identify cases where improved capabilities afforded by IPv6 offer significant advantage over current implementation.

Appendix A of this document is provided as an aid for Program Managers to complete the survey in Appendix B. Product Group and program responses to the survey will identify two timelines if applicable – the timeline for IPv6 transition using current funding and the timeline to accomplish IPv6 transition by 2008; funding associated with accelerated transition shown in the latter timeline will also be identified. Survey responses will be submitted to the IPv6TWG, examined for compliance, and added as an annex to the Marine Corps' transition plan. Aggregation and analysis of survey responses will enable realistic enterprise IPv6 Transition Planning.

MCTSSA will develop and implement test procedures to assure IPv6 compliance and interoperability in tactical systems. MCTSSA will also participate in IPv6 testing via the Defense Research and Engineering Network (DREN).

2.3.7 MCWL

Participate in development of testing procedures and objectives to determine IPv6 capable systems. Perform proof of concept demonstrations and technology exploration for use of IPv6 in tactical networks. Extend connection to the DREN from MCNOSC to take part in IPv6 testing.

2.3.8 MCNOSC

Provide Marine Corps IPv6 test network via the DREN. Participate in development of testing procedures and objectives to determine IPv6 capable systems. Develop IPv6 addressing scheme. Provide certification and accreditation of IPv6 nodes of MCEN. Assist in the development of the transition plan for the MCEN.

2.3.9 MCOTEA

Maintain awareness of IPv6 transition plan; assess impact of IPv6 implementation and recommend or implement required changes to operational test and evaluation activities.

2.3.10 External Agencies

OSD, through DoD CIO, provides policy and guidance for execution of the IPv6 transition and retains final approval authority for waivers.

DISA is the executive agent for DoD IPv6 transition. DISA will provide all IPv6 addresses and coordinate the transition via an overarching program office. DISA will represent DoD in the standards bodies for IPv6. A Preferred Products List (PPL) will be maintained at DISA.

DoN oversees the integration of Naval transition plans and is in the reporting chain for submission of Navy and Marine Corps IPv6 Transition Plans to OSD.

COMSPAWAR the Navy's C4I Chief Engineer is designated the IPv6 transition technical lead for development and execution of the Navy IPv6 transition plan.

3 ACQUISITION AND PROCUREMENT OF IPV6 CAPABILITIES

In compliance with the DoD policy, all Marine Corps products and systems that are procured, acquired, or in development after 1 October 2003 must be capable of operating in IPv4 and IPv6 networks. Adherence to this plan will minimize the need to retrofit products and systems later in their life-cycle as the GIG migrates to an all IPv6 environment. The DoD CIO expects the Components, including the Services, to be responsible for ensuring that this policy is implemented. Program Managers and Procurement Executives for the Marine Corps are to include IPv6 implementation requirements in their planning and programming submissions, as well as in contracts and RFPs.

3.1 Procurement Guidance

Guidance must be provided to the procurement and acquisition community to properly establish and execute the contractual means to mandate the implementation of IPv6. In addition, solution providers will need guidance in determining their compliance to being IPv6 capable. HQMC C4 will provide programmatic, technical, and logistical guidance for purchasing IPv6 capable technology. The IPv6TWG will distribute this guidance to all working group members.

3.2 Acquisition Directives

DoD CIO has a stated goal to transition all DoD networking capabilities to the next generation of the Internet Protocol, IPv6 by FY 2008. The implementation of this guidance requires close scrutiny of program Key Performance Parameters, contract specifications, technical specifications, and required modifications to programs existing in FY 2008.

For systems acquired after 1 October 2003, contractual language is needed to clearly articulate the Marine Corps' intent and definition of being "IPv6 capable" as described in Section 2.1.3. At a minimum, acquisition authorities will ensure the technical standards outlined in the Joint Technical Architecture (JTA) are articulated in contractual language for systems and components that use or interface with Internet Protocol (IP) protocols. The technical standards or Requests for Comments (RFCs), defined by the Internet Engineering Task Force (IETF), continue to evolve on a periodic basis. The JTA is thus defined by version identification and should be referenced accordingly. JTA version 6.0 (2003) incorporates the first set of IPv6 RFCs defining "IPv6 capable." This will result in systems capable of processing data packets using either IPv4 or IPv6 addresses until the GIG is eventually transitioned to IPv6.

Acquisition Programs can go through or be in any of four basic phases: Concept Refinement, Technology Development, System Development and Demonstration, and Production and Deployment. Each of these phases can be associated with both documentation and required reviews. As programs migrate to IPv6, an IPv6-centric review of the program needs to be part of the program management process. A preliminary assessment of reviews and documents that will require some level of IPv6 review is described in Table 1.

Acquisition Phase	Document/Review
Concept Refinement	Concept Decision Review
	Initial Capabilities Document
	Assessment of Alternatives Plan
	Milestone A Review
Technology Development	Technology Development Strategy
	Development of Initial TEMP
	Capability Development Document
	Milestone B Review
	System Readiness Review (SRR)
System Development & Demonstration	Acquisition Strategy
	Key Performance Parameters
	Initial ISP
	Pre-Planned Product Improvement Plan
	Design Readiness Review
	Updated TEMP
	Capability Production Document
	Milestone C Review
	System Specification
	Program Design Review (PDR)
	Critical Design Review (CDR)
	Technical Readiness Review (TRR)
	System Functional Review (SFR)
	Preliminary Design Readiness Review (PDRR)
	System Validation Review (SVR)
Production and Deployment	Updated Acquisition Strategy
	Updated ISP
	Updated TEMP
	Low Rate Initial Production Review/OT&E
	Full Rate Production Review
	CJCSI Interoperability Certification
	Capability Production Document (CPD)
	Engineering Change Proposal (ECP)
	Block Upgrades

Table 1. IPv6 Related Program Documents and Reviews

Table 1 lists generic program documents, activities, and reviews where the review of IPv6 planning may influence and support the program's transition. In addition, related program acquisition contracts can serve as a valid venue to review and evaluate the compliance of programs within the framework of IPv6 planning.

3.2.1 Milestone Decision Authority

The acquisition authority to approve the further development of acquisition programs rests with the applicable Milestone Decision Authority (MDA) pursuant with SECNAVINST 5000.2. The MDA serves as the decision authority for assigned programs and ensures that programs have identified and implemented applicable IPv6 requirements.

The MDA assignments are:

- USD(AT&L) for ACAT ID (Defense Acquisition Board) programs.
- ASN(RD&A) for ACAT IC (Navy Component) programs.
- DoD CIO for ACAT IAM programs.
- ASN(RD&A) for DON ACAT IAC programs unless this authority is specifically delegated.
- PEOs, SYSCOM Commanders, and DRPMs, or designated flag officer or Senior Executive Service (SES) official, are assigned authority for and shall designate ACAT III or IV programs unless ASN(RD&A) elects to retain or otherwise delegate this authority.

The Milestone Decision Authority (MDA) will be a key enforcer of transition of programs to IPv6. Reviews and oversight conducted as a normal part of MDA responsibilities will include specific focus on the impact of IPv6 to the program under review.

3.2.2 Technology Development

Technology development is normally part of pre-systems acquisition effort conducted prior to program initiation. For programs in this phase, only IPv6 capable products or systems should be considered unless there is a specific operational or risk mitigating requirement to include non-IPv6-capable items. These items should be tracked and a properly resourced upgrade/replacement plan put in place.

3.2.3 System Development and Demonstration

System development is a process where the best concept(s) are pursued and demonstrated. PMs of systems within a System of Systems (SoS) or a Family of Systems (FoS) shall coordinate with each other to provide sufficient information to the ASN(RD&A) and the MDAs so that appropriate decisions can be made across platform and system domains. This is the critical acquisition phase where the majority of testing and certifications are conducted. Three major IPv6 oriented types of certifications are anticipated – commercial products suitable for IPv6 use, typically enumerated in a preferred product list; government-certified programs providing tested products or systems, typically completed as a part of normal programmatic testing; and end-to-end systems testing conducted across product lines.

3.2.3.1 Preferred Product List (PPL) Development

A list of IPv6 enabled, interoperable products will be compiled and maintained at DISA. All agencies implementing and testing IPv6 products will provide their data to the IPv6TWG for this repository.

3.2.3.2 Program and System Testing

Individual Marine Corps programs will conduct necessary IPv6 developmental and system operational testing to ensure program capabilities to allow for IPv6 transition and fielding. Marine Corps test networks established at MCNOSC, MCTSSA, and MCWL will be used for these tests.

DISA, in coordination with the Components, will develop an IPv6 Master Test Plan that is updated annually. This Test Plan will be used to guide and manage the integrated IPv6 T&E program. The Plan will consolidate all IPv6 testing activities and will ensure critical issues are addressed. It will also highlight testing issues and areas for additional testing in the future. All IPv6-related T&E done by Components will be coordinated with this program.

The Joint Interoperability Test Command (JITC) will certify all Marine Corps programs for IPv6 interoperability as part of their joint certifications. Individual system-level test results may be used as a part of the JITC certification.

3.2.4 Production Deployment

In general two categories of fielding strategies are considered once a system is developed: Low Rate Initial Production or Full Rate Production. Programs in production deployment will be asked to review their information exchange requirements and their C4ISP documents to make necessary plans for IPv6 transition planning.

3.2.5 Operations and Support

Programs that are currently in the Operations and Support phase of the acquisition cycle are considered “legacy programs” for the purpose of IPv6 transition and should be evaluated to determine if they require interaction with the IPv6 architecture. There are three categories into which these legacy programs may be categorized – those to be refreshed, those to be retained and those to be retired. “Refreshed” programs will be those that shall enter a new development phase where significant changes will be made to the program to allow IPv6 compliance. “Retained” programs will be those that may not require a full development effort. Changes shall be more along the lines of minor interface changes or other such items. “Retired” programs will be those that shall be deleted from the Marine Corps inventory because they are approaching end of life or are being replaced by newer programs. The PM will work with the resource sponsor to determine if the program should enter a development phase for the purpose of transitioning to IPv6. In all cases, additional funding required must be identified to the IPv6TWG for inclusion in future IPv6 planning efforts.

3.3 Compliance with Procurement Policy and Waiver Process

IPv6 waivers may be granted based on operational need, business case, or impact on achieving GIG architecture.

For procurements, an IT waiver process is already in place under governance of HQMC C4 CIO. IPv6 waivers for IT procurements will use this same process expanded on as shown in Figure 3. HQMC C4 CIO may grant a waiver for up to one year. This waiver must be routed to DoD CIO for final approval at least ten days prior to the effective date of the waiver. DoD CIO has ten days to disapprove the waiver.

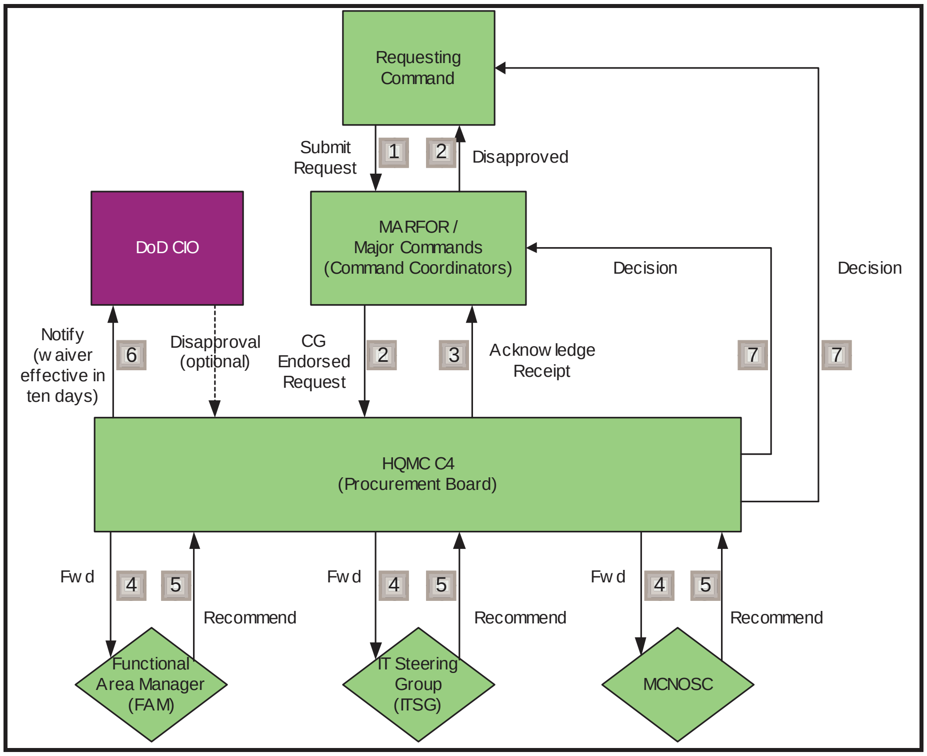


Figure 3. IPv6 Waiver Process For Procurements

For acquisitions, if migration to IPv6 is not warranted due to cost, schedule, or technical reasons, a business case together with acceptance of this factor by the user/operator of the "system" will be provided to the DoD CIO who, in consultation with the appropriate MDA, Joint Staff, or business area warfighter domain owner, will determine if a waiver shall be granted.[1]

3.4 Roles and Responsibilities for Acquisition and Procurement

3.4.1 Program Managers

[1] DoD Memorandum, DoD JTA Version 6.0, dtd 24 Nov 2003

Program Managers are responsible for overseeing all systems engineering development for their programs and will ensure that transition planning to IPv6 is conducted, including reviewing all necessary IPv6 requirements and formats. The PM will also generate any waiver requirements necessary to transition a program to IPv6 through the responsible MDA.

For ACAT Programs, the PM is responsible for including IPv6 requirements in the Information Support Plan (ISP) described in CJCSI 6212.01C and the Test and Evaluation Master Plan (TEMP) described in DoDI 5000.2. The ISP shall contain the IPv6 standards in the Technical View (TV-1) required by the program or system. The TEMP shall contain the testing requirements for IPv6 interoperability and will be based on interfaces and standards identified in the ISP and CDD/CPD.

To initiate the formation of a baseline of programs based on IPv6 transition plans and status, the PM will need to complete a self-program appraisal. The contents of the IPv6 Transition Survey template are assigned in Appendix B.

The following specific actions are required of Program Managers:

- Conduct an internal review of all programs/systems under program manager control to identify those programs and systems affected by the transition to IPv6. Include legacy programs that will still be fielded and operating in 2008. Provide a separate list of programs that will be retired and no longer fielded.
- Respond to the IPv6 Transition Survey in Appendix B no later than 01 September 2004 in coordination with your MDA.
- For "Integrating PMs" – defined as those PMs procuring items developed by other Programs of Record, the following actions shall be taken.
    - Identify PORs and the responsible MDA. The responsible MDA/PM shall be responsible for IPv6 transition planning.
    - Identify non-POR items being procured and fill out complete survey information as appropriate.
    - Build contracts, procurements and cross-PM agreements with language ensuring IPv6 compliance in accordance with current directives.

3.4.2 Procuring Agencies

Procuring Agencies, including Commanders and Comptrollers, will institute appropriate purchase and budget approval procedures to ensure compliance with IPv6 policy and JTA standards profile. Procure only network software and hardware that is IPv6 enabled.

3.4.3 Contracting Officers

Contracting officers and purchasing officials will screen information technology products and services for IPv6 policy compliance prior to signing contracts or approving purchases.

4 TRANSITION PLAN OF ACTION AND MILESTONES (POA&M)

The DoD IPv6 Transition Plan identifies eight categories of activities in which Components and the Services are expected to work cooperatively towards the development of documents and products, or comply with the recommendations of the DoD to furnish documentation and execute the pertinent elements of the DoD transition plan. The roles and responsibilities of the Marine Corps, as they pertain to each category, are discussed below. The categories of activities are:

- Networking and Infrastructure
- Addressing
- Information Assurance
- Pilots Programs, Testing, and Demonstrations
- Applications
- Standards
- Legacy Transition
- Training and Policy Development

The approach the Marine Corps is taking to conduct IPv6 transition consists of the following steps:

- Baseline existing COTS/GOTS Software and Hardware
  - Assess compatibility with IPv6
  - Assess timeline to support IPv6
  - Identify Critical Path to Achieve Enterprise IPv6 capability
- Identify and request funding required
  - Personnel, Testing, Education, Hardware/Software upgrades
  - Pilots, Cost of running dual stack network
- Plan and Implement Backbone Architecture
- Coordinate Efforts with other C/S/A

The IPv6TWG will refine the transition timeline in Figure 4 once adequate response from MCSC Program Managers, DRPM AAAV, and software functional area managers (FAMs) has been obtained.

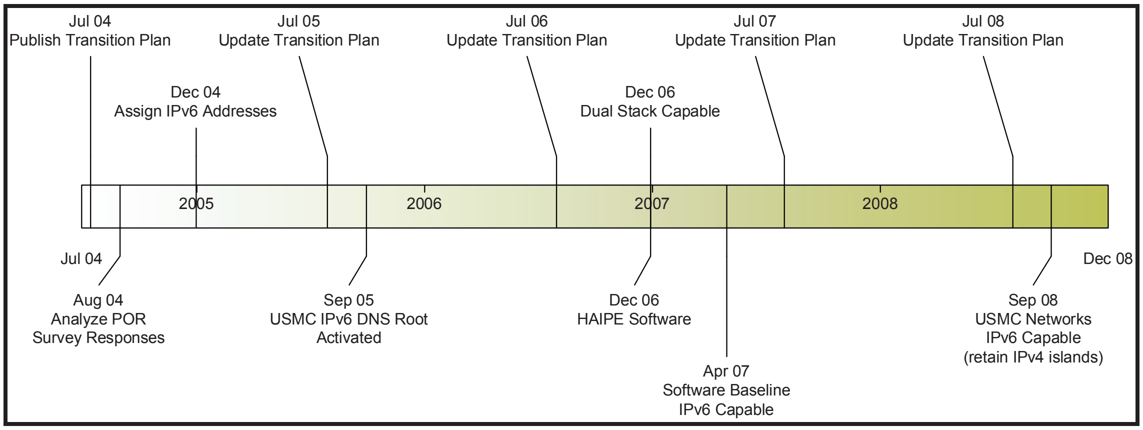


Figure 4. IPv6 Transition Timeline

Based on Marine Corps involvement in each of the categories outlined above and expounded on in the remainder of this chapter, the following milestones have been identified:

2004	May	Task PMs, DRPM, and Software FAMs to complete assessment survey
	July	Publish USMC Transition Plan
	Aug	Software Baseline Assessed
	Aug	Survey responses from PMs and DRPM AAAV complete
	Sep	Identify Core networking and infrastructure systems
	Oct	Develop NOC Process, Policies, to support v4/v6 operation
	Dec	Assign IPv6 Addresses
2005	July	Update Transition Plan
	Sep	USMC IPv6 DNS Root and network services activated
	Dec	High Assurance Internet Protocol Encryption (HAIPE) Hardware available
2006	July	Update Transition Plan
	Dec	Dual Stack Capable
	Dec	HAIPE Software available
2007	July	Software Baseline IPv6 Capable
	Apr	Update Transition Plan
2008	July	Update Transition Plan
	Sep	USMC Networks IPv6 Capable

Figure 5 shows the timeframe associated with each milestone and concurrency of transition efforts.

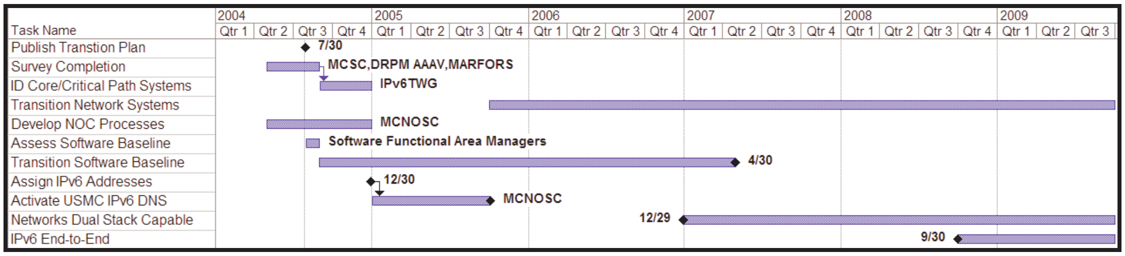


Figure 5. IPv6 Transition Milestones

4.1 Networking and Infrastructure

The IPv6 migration is being planned to develop in two directions: from the core infrastructure toward the edge, and from the end-user toward the core. Each path can progress independently of the other, with mechanisms in place, such as tunneling and translation, to allow services to be provided between entities, should one path be ready before the other. The core DoD networking and infrastructure systems include the Non-secure IP Router Network (NIPRNET), the Secret IP Router Network (SIPRNET), the Gigabit Switched Router (GSR) network, the Joint Warfighter Intelligence Communication System (JWICS), the Defense Research and Engineering Network (DREN), and the Defense Information System Network – Leading Edge Services (DISN-LES). The DoD Components are to identify similar core networking and infrastructure systems and plan their transition to IPv6 accordingly. All Components will plan, program for, engineer and implement IPv6 in their core and edge networks IAW the guidance in the approved DoD Transition Plan (specifically the DoD Network & IA System Transition Design).

The DoD networks mentioned above provide long haul networking services. The Marine Corps will interface with each as the IPv6 transition mechanisms are identified. Operational Marine Corps networks are exposed to a much more rugged, mobile, and hostile environment and are highly customized for tactical operations. The Marine Corps needs to plan for transition of such core networks as the Tactical Data Network (TDN), Enhanced Position Location Reporting System (EPLRS) and the Single Channel Ground and Airborne Radio System Advanced System Improvement Program (SINCGARS ASIP). Linking the upper and lower echelon services, the Marine Corps will use the Joint Tactical Radio System (JTRS), which also must transition to IPv6.

Transitioning the core services to IPv6 will put demands on other network related features and functions, such as performance and network management, but security and information assurance cannot be compromised. To ensure continued security, DISA, with the coordination of the Components (including NSA) will develop a time-phased Network & IA System Transition Design. This will be updated yearly and serve as the framework for DoD's network transition to IPv6.

The Marine Corps will provide support to the DoD to develop a Network and IA System Transition Design. IA issues will be discussed further in Section 4.3 below.

The transition of network services and routing functions must also be coordinated with the transition of the core network. DISA (with the support of Components) will assess the impacts of the IPv6 transition on all critical network services, for both classified and unclassified networks. These will include, but not necessarily be limited to, DNS, network time services, and Public Key Infrastructure (PKI). Recommendations will be provided to DoD CIO on how to address any issues (e.g., schedule, technical, resource).

DISA, in collaboration with DoD components, will develop a standard DoD IPv6 hierarchical routing architecture that takes maximum advantage of route summarization.

The Marine Corps will support DISA in assessing the impacts of the IPv6 transition on all critical network services. Domain Name Service (DNS) and route summarization are of particular interest to the Marine Corps due to the mobile nature of Marine Corps networks. In operational networks the Marine Corps employs Dynamic DNS to enhance the ability to support DNS for mobile users and subnets. Specific routing concerns are discussed in Section 4.2 below.

4.2 Addressing

The DoD has designated DISA to be the controlling organization for all matters pertaining to the procurement and management of IPv6 addresses. This is essentially the same role that DISA has been performing for IPv4.

DISA, in collaboration with DoD components, will develop a hierarchical IPv6 addressing architecture and address allocation scheme that optimizes joint E2E performance, interoperability, and scalability. The DoD IPv6 addressing architecture and address allocation scheme will be compliant to the greatest extent possible with current American Registry for Internet Numbers (ARIN) IPv6 address allocation and assignment policy.

DISA, in collaboration with DoD components, will assess the impacts of deploying IPv4/v6 within DoD organizations utilizing private IPv4 Intranets and NAT. The Marine Corps will participate in this assessment as well as planning for address architecture and naming conventions.

Developing a hierarchical IPv6 addressing architecture will be particularly challenging for mobile Marine Corps networks. Typically, hierarchically designed network address schemes are designed by assigning IP address blocks to networks based on geographical location. Doing so enables routers to aggregate or summarize routes, conserving memory and bandwidth used for management. But mobile networks are seldom confined to a geographical area for extended lengths of time. This will pose a challenge to network designers.

4.3 Information Assurance

Security and Information Assurance (IA) must be assured on any DoD network. Without the highest level of security and IA, a network is a threat to our operational security and safety. For this reason, it is imperative that IPv6 not be used on any operational network, or any DoD network carrying sensitive information, until it is completely compliant with all NSA requirements. DISA, in conjunction with NSA and other Components, will update the DISN Security Architecture to include IPv6. Further, DISA will assist Components in updating their System Security Authorization Agreements (SSAAs) and connection requests to support IPv6 implementation efforts.

4.4 IPv6 Pilots

Pilot programs will provide the Marine Corps with valuable IPv6 experience directly relevant to DoD networks and applications. Marine Corps IPv6 Pilot Implementation Plans will address the following:

- Program to IPv6 Compatibility
- Program to IPv6 Compliance
- Program Interoperability
    - Address Risk Reduction

The DoD CIO (in coordination with the Components) will identify the set of implementation pilots and schedule. The Components will implement them.

A proposed implementation plan for each Marine Corps IPv6 pilot will be developed. At a minimum, this plan will be coordinated with DISA, NSA and JS and DoD CIO. This will include a technical description of what is planned, a detailed schedule (including engineering, testing phases) and critical dependencies. Pilot Implementation Plans will focus on demonstrating “end-to-end” IPV6 capabilities in a secure environment and will address the steps to be taken to achieve security certification and accreditation, as appropriate, for the Pilot. Each pilot will progressively increase the number of applications that are IPV6 enabled and the associated network scope. Semi-annual reports will be submitted to DISA providing the status of the pilot’s implementation, identify lessons learned and surface any outstanding issues.

It is the responsibility of each Component sponsoring a pilot implementation to provide adequate resources. This includes any hardware and software upgrades required as well as training to ensure that systems support staff are fully prepared to resolve any problems that arise as a result of pilot implementations. Marine Corps, as well as GIG, facilities and capabilities will be upgraded as necessary to support each pilot.

The availability of resources for a pilot program is a concern, but the benefits to be gained make it a worthwhile investment. One of the undertakings of the Marine Corps’ IPv6TWG will be to identify additional IPv6 pilot program candidates for the DoD to consider.

4.5 Applications

All software applications that fail to make exclusive use of sockets established using the application program interfaces inherent in operating systems must be transitioned to IPv6 if they are to remain in use. A dual stack approach will be taken on the backbone to maintain backwards compatibility and to provide a fallback condition in the event that any problems occur with the transition. The Marine Corps will maintain a comprehensive list of existing COTS and GOTS software that directly interfaces with

IPv4. Appendix E contains a list of applications used in the Marine Corps. The list identifies whether each application is currently IPv6 capable, will be made IPv6 capable, or remain as is until terminated; an associated schedule is provided where applicable. DISA will maintain a web-accessible consolidated list of applications identified across DoD.

DoD Components will be responsible for transitioning their existing IPv4 only software to IPv4/v6 compliance no later than April 30, 2007. Components are responsible for resourcing this requirement.

DISA in conjunction with the Components will develop processes and procedures to identify, test, and certify IPv4/v6 capable software as part of the IPv6 Master Test Plan. Particular emphasis will be placed on testing end-to-end compatibility and interoperability of legacy software components as they are upgraded to become IPv6 capable.

The task of completing a comprehensive application evaluation and transition program to track all software applications within the Marine Corps will require development time and will likely incur labor costs to modify, test, and integrate software code, especially in cases where products must be retrofitted. For legacy systems, the upgrades may be available through the normal refresh cycle, but this will not be true in all cases.

4.6 Legacy Transition

Legacy systems seldom stand idle. Sooner or later they are either upgraded or phased out. Without any consideration to IPv6, there are those legacy systems that will be phased out simply due to their current state of obsolescence. The remaining systems must be evaluated based on their projected need, projected capabilities after being upgraded, and their ability to transition or co-exist in an IPv6 net-centric environment. For some systems, the integrated logistics support plan or the post-deployment support plan can serve as a contractual vehicle to upgrade a system to IPv6. However, contract terminology must be carefully stated. There are documented cases where a customer, expecting new software as part of his maintenance agreement, did not distinguish between software upgrades and new software version releases, e.g., expecting Windows 2000 as an upgrade for Windows NT. IPv6 is not an upgrade of IPv4. It is a new protocol that is essentially incompatible with IPv4.

Legacy systems will likely be much more difficult to transition than developmental systems. Many legacy systems may have hard-coded IP addresses and embedded software which will be difficult to modify. In addition, operational systems will need to be retrofitted in the field and tested. For these reasons, it is recommended that program managers of legacy systems develop an incremental transition plan that can be monitored, measured, and evaluated throughout the transition period. It will be the responsibility of the IPv6TWG to work with the legacy system program managers to develop a timeline of transition milestones.

4.6.1 Critical Path for Systems Transition

4.6.1.1 Marine Corps Baseline

Before system integration can proceed, the Marine Corps must establish its current baseline. Current institutional and operational communications architectures, as well as all Marine Corps acquisition systems that are under development must be analyzed and assessed for support of IPv6. Analysis of the baseline will be used to determine which systems are most critical for implementing IPv6 and to help identify technical and programmatic issues. The primary product of this task is to define and evaluate the scope of the IPv6 transition effort.

4.6.1.2 Baseline Methodology

To establish the baseline, the survey in Appendix B will be distributed to MCSC and DRPM AAAV. The nature of the survey was to determine the following:

- Developmental state of each program
- How IPv4 is currently implemented
- The impact of adding IPv6 capabilities
- Technical and logistical issues, and
- Willingness to be an IPv6 early adopter.

4.6.1.3 Analysis of Survey Responses

Those programs that provide a connection to other systems must be identified. These are programs that represent the critical transition path for Marine Corps networks. The timeline established for critical path systems to transition to IPv6 will drive the timelines for dependent systems, therefore, critical path systems will receive priority consideration for resource allocation and transition effort. Factors to consider when selecting these programs include:

- The need to interoperate with other IPv6 systems (i.e., Joint, Allied, NATO, etc.)
- The operational importance of the program
- The projected life cycle or longevity of the program.

Examples of such programs are TDN, SMART-T and TSM. These programs are expected to be the communications backbone of the Marine Corps for decades to come and must implement IPv6 no matter how daunting the task may appear.

The first course of action for analyzing the survey responses is to sort programs according to their stage of development or deployment. The categories are:

- Planning
- Development
- Production
- Fielding
- Legacy – PDSS stage
- Legacy – planned for phase-out

All programs in the planning phase should be designed with IPv4 and IPv6 capabilities. Programs in development should be expected to implement IPv6 during FY04 and FY05. Programs in production or the early stages of fielding are likely to be upgraded or improved within two or three years of initial fielding. They should be expected to implement IPv6 during the first or second release of a revision during FY06 and FY07. Legacy program that are not planned for phase-out should be IPv6 capable by FY08.

4.7 Standards

Technical standards defining IPv6 and related services are being developed by the IETF through the RFC standards-track process that includes proposed standards, draft standards, and Internet standards. IPv6 standards include the definition of the IPv6 packet header and address structure. Services include such features as routing, mobility, security, and auto-configuration. DISA will participate in the standards process to influence the development of those standards that are of particular interest to the DoD in general.

As previously mentioned, the IPv6 standards are regulated by the Internet Engineering Task Force (IETF) through the RFC standards process. The DoD Joint Technical Architecture (JTA) is used to identify standards that are relevant to DoD systems and to define implementation profiles of those standards. The JTA is a reference document that mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The JTA is mandated for use in the management, development, or acquisition of new or improved systems within DoD.

5 PROGRAMS AND BUDGETS

5.1 DoD Funding for IPv6 Transition

The DoD IPv6 Transition Plan describes the tasks and budget proposals for the DoD to implement IPv6. It also provides the guidelines for the other DoD Components and Services to do the same. The DoD budget is for the overall administration and engineering tasks associated with the transition. It is not for individual programs. The activities and services to be provided by the DoD include the following:

- Transition planning, monitoring, and managing
- Address space acquisition and management
- Network, security, and software engineering and integration
- Technical analyses, including modeling and simulation
- Infrastructure upgrades, and
- Pilot implementation, testing, and demonstrations

The transition planners will provide leadership, coordination, and integration support. They will be responsible for updating and integrating the transition plans, implementing schedules, conducting working group activities, and tracking implementation progress. All the technical services will be provided by DISA through the establishment of a Center for Excellence. The Center for Excellence will provide support for technical analyses, system design and planning, standards development, product assessment, implementation, and training.

To support this effort, the DoD has directed the Services (DON, Army and Air Force) to provide $2 million apiece to support the DoD IPv6 Transition Office at DISA. The DoD Transition Office in turn directed Services to use $300 thousand of their obligated $2 million for internal transition efforts. Funding that will be available for the Marine Corps is currently undetermined.

5.2 Marine Corps Funding Profile

The DoD transition plan indicates that the Components and Services should provide IPv6 transition services and activities that parallel those of the DoD. Each Component and Service should identify and submit its FY04-09 resource requirements for IPv6 transition to the DoD. Planning and programming submissions should include funding requirements for transition planning, engineering, testing, integration, infrastructure, and analyses.

Similar to the DoD budget structure, most of the Marine Corps IPv6 transition budget should be for the overall administration and engineering tasks associated with the transition and not for individual programs. Components, including services, are generally responsible for any additional costs associated with implementation pilots, contractual changes for systems under development, and any additional technology refreshes necessary to meet the FY 2008 schedule. In many cases it is expected that funding for legacy and developmental systems will come from existing budget lines, which usually address technology refreshment.

The transition of critical programs, legacy or developmental, must be addressed, and the guidelines from the DoD may need to be applied on a case-by-case basis so that no critical program is neglected.

5.2.1 Marine Corps Budget

The Marine Corps has defined its IPv6 transition tasks within four functions: Pilot and System Design, Testing, Transition Management and Awareness, and Installing/Operating Dual Stack Network. Based on early estimates and program manager responses, a projected budget for these tasks is shown in Table 2. Expenditures for each function are further detailed by type of appropriation in Section 5.3 below. Costs identified in this section are independent of funding already budgeted or planned. Further, no cost is projected or included for transitioning supporting infrastructure to IPv6 using NMCI.

Costs estimates will be refined through completion of Program of Record and Application Software surveys as described in Chapter 4.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
Testing							
Transition Management and Awareness							
Installing/Operating Dual Stack Network							
TOTAL							

Table 2. Marine Corps IPv6 Budget for FY 2004-2009 ($K)

5.2.1.1 Pilot and System Design

Pilot and System Design costs include modification of network layer interfaces in applications and Programs of Record; purchase or upgrade of operating systems; purchase or upgrade of IPv6 capable switches, routers, firewalls, and associated equipment; and research, design and testing of early adopters, and pilot program development. System Design also involves IA accreditation and enterprise architecture engineering.

5.2.1.2 Testing

Costs include recertification of programs related to weapons release, regression testing, System of Systems Testing (SoST), product assessment, modeling and simulation, interoperability and integration testing, standards development, and performance testing.

5.2.1.3 Transition Management and Awareness

Transition Management and Awareness includes policy setting, transition planning, enforcement, education and training, and working group activities.

5.2.1.4 Installing/Operating Dual Stack Network

Additional, previously unbudgeted costs will be incurred to field IPv6 systems and coordinate operation with other fielded systems. These costs are incurred due to the requirement to support both IPv4 and IPv6 during the transition and include both infrastructure and management.

5.3 Budget Execution

Tables 3 through 7 will be refined as surveys in Appendix B and C are collected and analyzed. Every effort will be made to accomplish transition of all systems to IPv6 using funds that are already budgeted. The costs identified in this section require additional appropriation and represent unplanned expenses incurred by IPv6 transition. Table 3 presents total estimated funding requirements by appropriation type and fiscal year. “Currently Budgeted” amounts reflect dollars planned for technology refresh, upgrade, and replacement. The amounts identified as “Requirement with IPv6” reflect the total of estimates returned by survey responses.

Appropriation	FY04 ($K)	FY05 ($K)	FY06 ($K)	FY07 ($K)	FY08 ($K)	FY09 ($K)	TY ($K)
RDT&E							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
PMC							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
O&M							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
TOTAL ADDITIONAL REQUIREMENT							

Table 3. Life Cycle Cost Estimate for IPv6 Transition ($K)

5.3.1 Research and Development Costs

RDT&E costs will be included in funding for individual programs of record at MCSC. Surveys completed by Program Managers will identify funding requirements. Table 4 shows estimated RDT&E dollars needed to support IPv6. Dollars shown here are based on the amounts shown as "Requirement with IPv6" in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Integration, Assembly, and Checkout							
- Manpower							
Testing							
- Development Testing							
- Operational Testing							
- JITC Certification							
- Manpower							
Transition Management and Awareness							
- Planning							
- Training							
- Manpower							
TOTAL							

Table 4. IPv6 Research and Development Costs ($K)

5.3.2 Procurements

PMC costs will be included in funding for individual programs of record at MCSC. Surveys completed by Program Managers will identify funding requirements. Table 5 shows estimated PMC dollars needed to support IPv6 transition. Dollars shown here are based on the amounts shown as “Requirement with IPv6” in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Pilot Implementation							
Installing/Operating Dual Stack Network							
- Hardware							
- Software							
- Operational/Site Activation							
Transition Management and Awareness							
- Training							
- Development Support							
TOTAL							

Table 5. IPv6 Procurements ($K)

5.3.3 Operations and Maintenance Costs

O&M costs will be included in funding for MCNOSC. Table 6 shows estimated O&M dollars needed to support IPv6 transition. Dollars shown here are based on the amounts shown as “Requirement with IPv6” in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Pilot Implementation							
Transition Management and Awareness							
- Manpower							
Installing/Operating Dual Stack Network							
- Hardware Sustainment							
- Software Sustainment							
- Manpower							
TOTAL							

Table 6. IPv6 Operations and Maintenance Costs ($K)

5.3.4 Manpower Costs

Table 7 presents a summary of manpower costs identified throughout this section.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- RDT&E							
Testing							
- RDT&E							
Transition Management and Awareness							
- RDT&E							
- O&M							
Installing/Operating Dual Stack Network							
- O&M							
TOTAL							

Table 7. IPv6 Manpower Costs ($K)

Appendix A. IPv6 Transition Assessment Guide

TRANSITION GUIDE PREAMBLE

The purpose of this Appendix is to help Program Managers evaluate the affects of IPv6 transition on their programs. Education on IPv6 needs to occur to enhance understanding of the implications associated with network layer transition. While this paper is not a detailed technical reference for IPv6 implementation it does promote a broad understanding of the transition challenges associated with building IPv6 capability into current systems. The paper is intended to spur thinking about and planning for changes that will result from IPv6 adoption as well as create awareness of new capabilities afforded by this protocol.

The template in Appendix B provides a checklist for evaluating how a program will transition to IPv6. It should be used in conjunction with this white paper to highlight areas requiring attention. The template will also provide important programmatic information to enterprise transition planners. Completed templates will be aggregated and used to organize transition efforts and validate requirements for additional funding.

Careful review and planning cannot capture all IPv6 implementation issues or guarantee system performance. The only way to be truly certain that a system or application is IPv6 capable is to test it on an IPv6 network. An IPv6 test network exists on the Defense Research and Engineering Network (DREN). Marine Corps agencies supporting IPv6 testing through the DREN are Marine Corps Network Operations Security Command (MCNOSC), Marine Corps Warfighting Lab (MCWL), and Marine Corps Tactical Systems Support Activity (MCTSSA). Program Managers are encouraged to seek support from these activities to test and evaluate the IPv6 capability of their hardware and software.

1 NETWORK COMMUNICATIONS

1.1 Seven Layer Model

Computer communications requires

(1) A connection,
(2) Protocols establishing rules for transferring information, and
(3) Application services that provide an interface with users or applications.

The Open Systems Interconnection (OSI) Reference Model describes how two points communicate on a network. Conceptually, each endpoint must complete the seven steps of the OSI Reference model for successful communications to take place. Figure 6[2] illustrates the OSI Reference Model and shows standard services, protocols and physical medium that are commonly associated with each of the seven layers. The lower three layers of the model are used when a message travels between two points on a network; the upper four levels are used at the source and destination to complete the information exchange. In addition to enabling features described in Chapter 3 of this Appendix, Internet Protocol (version 6 or version 4) provides the Network Layer service that contributes to computer communications by establishing rules for transferring information. Although “Internet Protocol” refers to a specific OSI Layer 3 entity, the Internet Protocol Suite commonly referred to as “TCP/IP” consists of both Layer 3 and Layer 4 protocols, of which Transmission Control Protocol (TCP) and IP are the most prevalent.

The transition to IPv6 will be quite similar to the Y2K transition. All operating systems, middleware, and applications will need to be examined for compatibility with the new standard and with published transition mechanisms. This transition is not a software-only event: many routers, switches, and other network devices will require replacement.

[2] Figure 6 from SearchNetworking.com website URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci523729,00.html. March 2004.

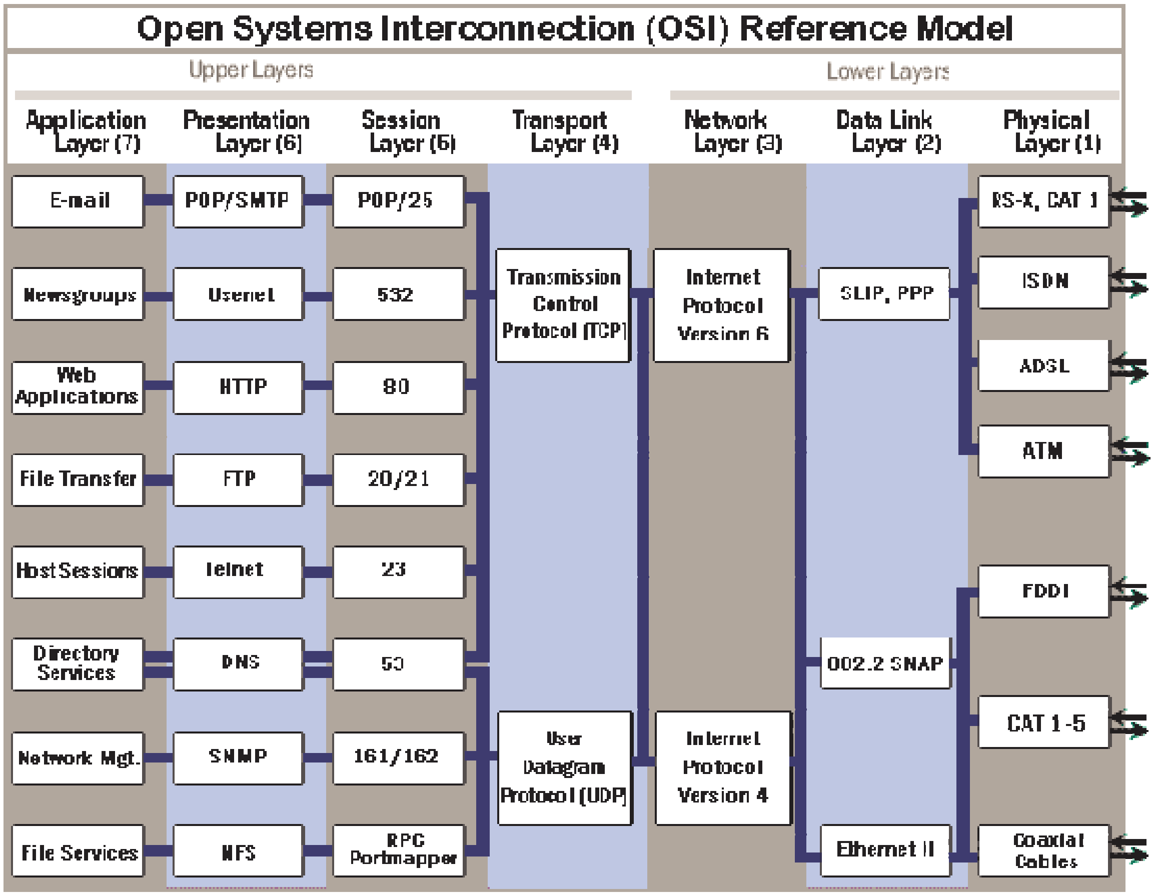


Figure 6. OSI Seven Layer Model

1.1.1 Internet Protocol

Understanding the role of IP in networking is critical to assessing the impact of transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). IP is used at every connection point, or interface, to the network. Interfaces are assigned addresses based on the Internet protocol used and determine if traffic on the network pertains to them by examining the destination IP address of all traffic received. IP is integral to the function of networking appliances such as routers, switches, and bridges. Any application that sends information over a network must pass through an interface to do so; how that application accesses the interface determines whether changing from IPv4 to IPv6 will affect its operation.

Internet Protocol (IP) provides a common logical interface to different networks. This logical interface takes the form of an IP header appended to a manageable portion of the data that must be transported. This combination of header and data is referred to as a packet. Once a packet successfully negotiates the network and reaches its intended destination the information contained in the packet is used according to the rules established by the higher-level protocols involved in the exchange (see Layers 4 through 7 of Figure 6).

IP provides best effort delivery of packets of information across a network. The Internet Protocol itself does not ensure these packets arrive in correct order or that they even arrive at all. Other protocols are used to guarantee delivery and reconstruct information by correctly combining the IP packets at their destination.

1.1.2 How Internet Protocol is used

Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) packets are created by appending a header (described in section 1.2) to a "payload" containing a manageable portion of the data being transported. Header fields carry information about the format of data contained in the payload and how the packet should be routed. Headers are examined at each node in the network that needs to determine routing. The payload contains the information that is being transported; the information in the payload is formatted using an upper layer protocol, such as Transfer Control Protocol (TCP) or User Datagram Protocol (UDP). In the case of IPv6, the payload can also contain extension headers. Extension headers are optional and carry additional instructions for processing the data contained in the payload; they offer the distinct advantage of being transparent to nodes in the path to the destination, facilitating efficient routing through the network.

To traverse portions of the network each IP Packet is encapsulated in additional Link Layer information needed to negotiate the paths between each node. The Link Layer Protocol used determines the maximum packet size allowed. For instance, Ethernet frames longer than 1518 bytes in length are ignored by Ethernet network interfaces. IP prevents oversize packets by fragmenting the data to pieces that will fit the maximum Message Transmission Unit (MTU) of the Link Layer Protocol. Figure 7 illustrates encapsulation of an IPv6 packet into a Link Layer Frame.

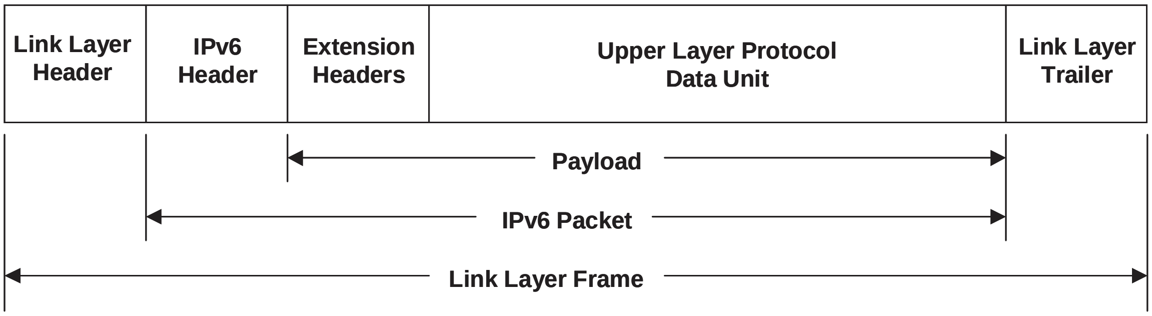


Figure 7. IPv6 Packet Encapsulation

Current IPv4 routers may be configured to support the recommended minimum MTU of 576 octets. For IPv6 routers the minimum length allowed is 1280 octets and the recommended MTU is 1500 octets; this larger MTU will allow Ethernet frames to carry forward without fragmentation.[3] The effects of increased packet size need to be evaluated on constrained bandwidth connections to determine the optimum MTU.

[3] Data Networks, IP and the Internet [electronic resource]: Protocols, Design and Operation by Martin P. Clark. Chichester, England; Hoboken, NJ: Wiley, 2003. Page 199.

1.2 IP Headers

IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4. A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats.[4]

IPv6 headers are designed to optimize the use of header space and minimize the processing time needed at intermediate nodes in the transmission path. Unlike IPv4 headers, IPv6 headers are fixed in length. Address length increased from 32 bits with IPv4 to 128 bits with IPv6, a four-fold increase in bytes used for addressing. However, IPv6 headers are not significantly larger than IPv4 headers; overall IPv6 header length remains fixed at 40 bytes (or octets) while IPv4 headers can vary in length from 20 to 60 bytes. Table 8 identifies some of the key differences between header implementations for each version.

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes or octets) in length.	Source and destination addresses are 128 bits (16 bytes or octets) in length.
Header length varies from 20 to 60 bytes	Header length is fixed at 40 bytes
IPSec support is optional.	IPSec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Both routers and the sending host do fragmentation.	Fragmentation is only done by the sending host, not by intermediate routers.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Routing architecture must support a 576-byte packet size (possibly fragmented).	Routing architecture must support a 1280-byte packet size (without fragmentation).

Table 8. IPv4 and IPv6 Header Comparison

1.2.1 IPv4 Header

IPv4 headers are structured as shown in Figure 8. The highlighted portions are removed from IPv6 headers.

[4] Microsoft Windows Server 2003 White Paper, September 2003. Page 2.

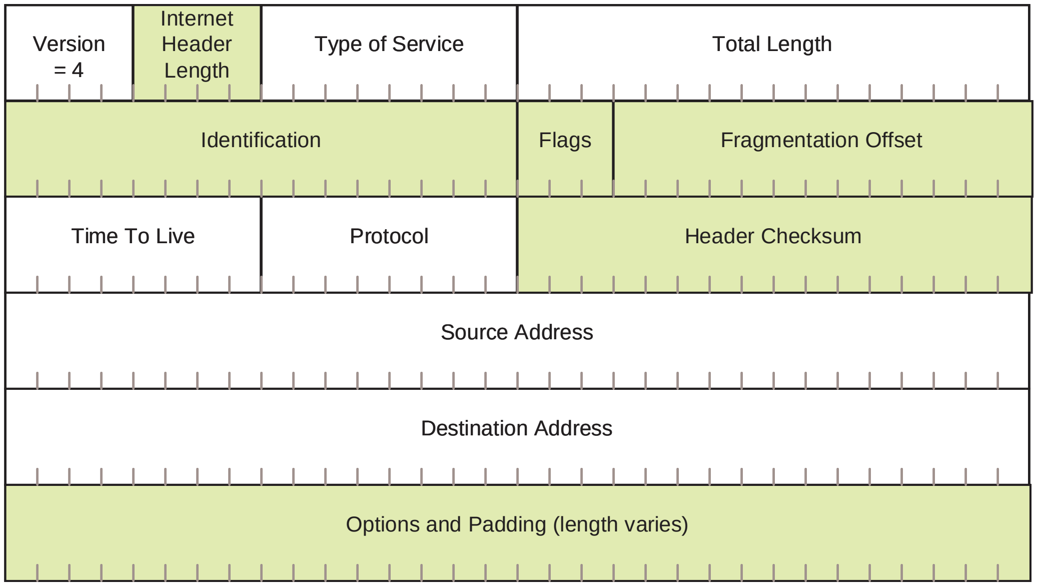


Figure 8. IPv4 Header

Version – Indicates the version of IP and is set to 4. The size of this field is 4 bits.

Internet Header Length – Indicates the number of 4-byte blocks in the IPv4 header. The size of this field is 4 bits. Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5 (5x4). IPv4 options can extend the minimum IPv4 header size in increments of 4 bytes. The maximum size of the IPv4 header including options is 60 bytes (15×4).

Type of Service – Indicates the desired service expected by this packet for delivery through routers across the IPv4 network. The size of this field is 8 bits, which contain bits for precedence, delay, throughput, and reliability characteristics.

Total Length – Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) and does not include link layer framing. The size of this field is 16 bits, which can indicate an IPv4 packet that is up to 65,535 bytes long.

Identification – Identifies this specific IPv4 packet. The size of this field is 16 bits. The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the Identification field value so that the destination node can group the fragments for reassembly.

Flags – Identifies flags for the fragmentation process. The size of this field is 3 bits, however, only 2 bits are defined for current use. There are two flags – one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.

Fragment Offset – Indicates the position of the fragment relative to the original IPv4 payload. The size of this field is 13 bits.

Time to Live – Indicate the maximum number of links on which an IPv4 packet can travel before being discarded. The size of this field is 8 bits. The Time-to-Live field (TTL) was originally used as a time count with which an IPv4 router determined the length of time required (in seconds) to forward the IPv4 packet, decrementing the TTL accordingly. Modern routers almost always forward an IPv4 packet in less than a second and are required by RFC 791 to decrement the TTL by at least one. Therefore, the TTL becomes a maximum link count with the value set by the sending node. When the TTL equals 0, an ICMP Time Expired message is sent to the source IPv4 address and the packet is discarded.

Protocol – Identifies the upper layer protocol. The size of this field is 8 bits. For example, TCP uses a Protocol of 6, UDP uses a Protocol of 17, and ICMP uses a Protocol of 1. The Protocol field is used to demultiplex an IPv4 packet to the upper layer protocol.

Header Checksum – Provides a checksum on the IPv4 header only. The size of this field is 16 bits. The IPv4 payload is not included in the checksum calculation as the IPv4 payload and usually contains its own checksum. Each IPv4 node that receives IPv4 packets verifies the IPv4 header checksum and silently discards the IPv4 packet if checksum verification fails. When a router forwards an IPv4 packet, it must decrement the TTL. Therefore, the Header Checksum is recomputed at each hop between source and destination.

Source Address – Stores the IPv4 address of the originating host. The size of this field is 32 bits.

Destination Address – Stores the IPv4 address of the destination host. The size of this field is 32 bits.

Options – Stores one or more IPv4 options. The size of this field is a multiple of 32 bits. If the IPv4 option or options do not use all 32 bits, padding options must be added so that the IPv4 header is an integral number of 4-byte blocks that can be indicated by the Internet Header Length field.

1.2.2 IPv6 Header

Figure 9 shows the fields in the IPv6 Header. The number of fields has been reduced and the address space has quadrupled. Overall header length is now fixed at 40 octets, thus eliminating the need for the “Internet Header Length” field used in IPv4 headers. Other changes are discussed in the description of each header field below.

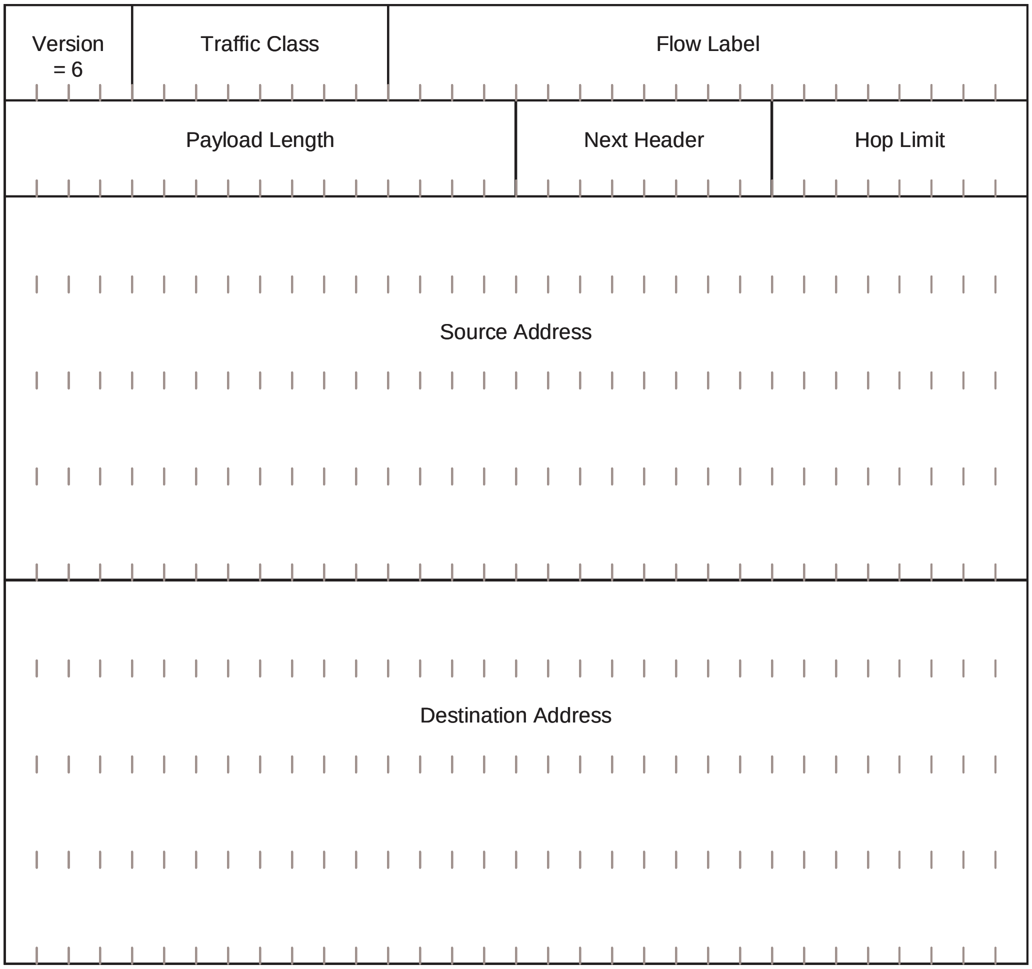


Figure 9. IPv6 Header

Version – 4 bits are used to indicate the version of IP and is set to 6.

Traffic Class – Indicates the class or priority of the IPv6 packet. The size of this field is 8 bits. The Traffic Class field provides similar functionality to the IPv4 Type of Service field. In RFC 2460, the values of the Traffic Class field are not defined. However, an IPv6 implementation is required to provide a means for an application layer protocol to specify the value of the Traffic Class field for experimentation.

Flow Label – Indicates that this packet belongs to a specific sequence of packets between a source and destination, requiring special handling by intermediate IPv6 routers. The size of this field is 20 bits. The Flow Label is used for non-default quality of service connections, such as those needed by real-time data (voice and video).

Payload Length – Indicates the length of the IPv6 payload. The size of this field is 16 bits. The Payload Length field includes the extension headers and the upper layer Protocol Data Unit (PDU).

Next Header – Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6). The size of this field is 8 bits. When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.

Hop Limit – Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. The size of this field is 8 bits. The Hop Limit is similar to the IPv4 TTL field except that there is no historical relation to the amount of time (in seconds) that the packet is queued at the router. When the Hop Limit equals 0, an ICMPv6 Time Exceeded message is sent to the source address and the packet is discarded.

Source Address –Stores the IPv6 address of the originating host. The size of this field is 128 bits.

Destination Address – Stores the IPv6 address of the current destination host. The size of this field is 128 bits. In most cases the Destination Address is set to the final destination address. However, if a Routing extension header is present, the Destination Address might be set to the next router interface in the source route list.

2 HOW THE NETWORK LAYER IS USED

2.1 Assigning IP Addresses

Any device or software application that intends to communicate across the network must have an IP address to originate from and an IP address or range of addresses to reach. Devices themselves do not have addresses; hardware interfaces and software ports have addresses. IP addresses can be statically assigned by administrators or dynamically assigned through Dynamic Host Configuration Protocol (DHCP) services. IPv4 and IPv6 each have implementations of DHCP. IPv6 further supports Stateless Address Configuration (see section 3.3.4).

2.2 Application Program Interfaces

Communication between a client program and a server program in a network is accomplished through the use of sockets. A socket is defined as "the endpoint in a connection." Sockets are created and used with a set of programming requests or "function calls" sometimes called the sockets application programming interface (API). Sockets can also be used for communication between processes within the same computer. Sockets can be implemented as “connectionless” or “connection-oriented.” Connectionless sockets use datagrams and exist only long enough for a single exchange to take place while connection-oriented sockets use streams and remain aware until terminated. The address of a socket in the Internet domain consists of the IP address of the host machine and a port number on that host. Port numbers are 16 bit unsigned integers. Standard services have established ports so that clients will know their addresses. For example, the port number for the FTP server is 21.

The formal requests for services and means of communicating with other programs that a programmer uses in writing an application program is called the application program interface. An API is the specific method prescribed by a computer operating system (OS) or by an application program for making requests of the operating system or other applications. Applications can be developed to use the services provided by operating systems to establish communications links with other hosts or applications. Alternately, some applications do not use the standard function calls in the operating system. Instead, connections to other hosts and applications may be established using hard-coded protocol implementations, ports, and addresses. Identifying these non-standardized applications is important since upgrading to operating systems with IPv6 capability will not alter the procedures coded in programs. Application programs with hard-coded API implementations will need to be replaced or undergo additional development, testing and certification. Because this is not readily apparent in an application, careful analysis of source code is required in order to make this determination. A very common hard-coded implementation is the loopback address, 127.0.0.0. Hardcoded addresses and implementations are among the principal reasons that IPv6 transition is an involved process.

3 IPV6 IMPLEMENTATION

3.1 Addressing

IPv4 addresses are represented in dotted-decimal format. This 32-bit address is divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated by periods. For IPv6, the 128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons. The resulting representation is called colon-hexadecimal. IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit.

Some types of addresses contain long sequences of zeros. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in the colon hexadecimal format can be compressed to "::", known as *double-colon*. For example, the link-local address of FE80:0:0:0:2AA:FF:FE9A:4CA2 can be compressed to FE80::2AA:FF:FE9A:4CA2.

The prefix is the part of the address that indicates the bits that have fixed values or are the bits of the network identifier. Prefixes for IPv6 subnet identifiers, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4. An IPv6 prefix is written in *address/prefix-length* notation. For example, 21DA:D3::/48 is a route prefix and 21DA:D3:0:2F3B::/64 is a subnet prefix. [5]

There are three types of IPv6 addresses – Unicast, Multicast, and Anycast. Table 9 compares addresses used in IPv4 to those used in IPv6.

IPv4 Address	**IPv6 Address**
Internet address classes	Not applicable in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6. "Link-scope all-hosts multicast" address, FF02::1 corresponds to IPv4 subnet-local address, 255.255.255.255
Not applicable in IPv4	Anycast addresses
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Autoconfigured addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)

[5] Microsoft Windows Server 2003 White Paper, September 2003. Pages 8-10.

IPv4 Address	IPv6 Address
Text representation: Dotted decimal notation	Text representation: Colon hexadecimal format with suppression of leading zeros and zero compression. IPv4-compatible addresses are expressed in dotted decimal notation.
Network bits representation: Subnet mask in dotted decimal notation or prefix length	Network bits representation: Prefix length notation only
DNS name resolution: IPv4 host address (A) resource record	DNS name resolution: IPv6 host address (AAAA) resource record
DNS reverse resolution: IN-ADDR.ARPA domain	DNS reverse resolution: IP6.ARPA domain

Table 9. IPv4 and IPv6 Address Convention Comparison[6]

3.1.1 Unicast Addresses

A unicast address identifies a single interface within the scope of the type of unicast address. With the appropriate unicast routing topology, packets addressed to a unicast address are delivered to a single interface.

The following types of addresses are unicast IPv6 addresses:

Global Unicast Addresses. Global unicast addresses are equivalent to public IPv4 addresses. They are globally routable and reachable on the IPv6 portion of the Internet. Unlike the current IPv4-based Internet, which is a mixture of both flat and hierarchical routing, the IPv6-based Internet has been designed from its foundation to support efficient, hierarchical addressing and routing. The scope, the region of the IPv6 internetwork over which the address is unique, of a global unicast address is the entire IPv6 Internet.

Local-Use Unicast Addresses. There are two types of local-use unicast addresses:

1. Link-local addresses are used between on-link neighbors and for Neighbor Discovery (ND) processes.

2. Site-local addresses are used between nodes communicating with other nodes in the same site.

Link-local addresses are used by nodes when communicating with neighboring nodes on the same link. For example, on a single link IPv6 network with no router, link-local addresses are used to communicate between hosts on the link. The scope of a link-local address is the local link. Site-local addresses are equivalent to the IPv4 private address space. Site-local addresses are not reachable from other sites, and routers must not forward site-local traffic outside the site. Site-local addresses can be used in addition to global unicast addresses. The scope of a site-local address is the site.

[6] Microsoft Windows Server 2003 White Paper, September 2003. Page 22.

3.1.2 Multicast Addresses

A multicast address identifies multiple interfaces. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address. A multicast address is used for one-to-many communication, with delivery to multiple interfaces. Interfaces may belong to more than one multicast group.

In IPv6, multicast traffic operates in the same way that it does in IPv4. Arbitrarily located IPv6 nodes can listen for multicast traffic on an arbitrary IPv6 multicast address. IPv6 nodes can listen to multiple multicast addresses at the same time. Nodes can join or leave a multicast group at any time.

3.1.3 Anycast Addresses

An anycast address also identifies multiple interfaces. With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface, the nearest interface that is identified by the address. The “nearest” interface is defined as being closest in terms of routing distance. An anycast address is used for one-to-“one-of-many” communication, with delivery to a single interface.

Packets addressed to an anycast address are forwarded by the routing infrastructure to the nearest interface to which the anycast address is assigned. In order to facilitate delivery, the routing infrastructure must be aware of the interfaces assigned anycast addresses and their “distance” in terms of routing metrics. At present, anycast addresses are only used as destination addresses and are only assigned to routers. Anycast addresses are assigned out of the unicast address space and the scope of an anycast address is the scope of the type of unicast address from which the anycast address is assigned.

3.2 Address Resolution

The Domain Name System (DNS) is used to resolve domain names (e.g., www.usmc.mil) by identifying the numeric address associated with it. Network routing is then possible based on the IP address returned by the DNS. DNS service is specific to IPv4 or IPv6. To resolve addresses across protocol boundaries, either a separate DNS service must exist for each Internet protocol or an application layer gateway must perform translation on addresses returned by the DNS answer message. DNS servers listing data for IPv4 (A records) and IPv6 (AAAA records) addresses can be configured to return IPv4, IPv6, or both addresses. The selection of which address type to return, or in which order, affects the type of IP traffic generated.

3.3 Features of IPv6

Systems currently operating on IPv4 were engineered to take advantage of features available in IPv4. Simply making these systems IPv6 capable will not take advantage of new features made possible by IPv6; applications ported to IPv6 will offer only the capabilities they had with IPv4. Planning and engineering efforts should provision for the enhanced feature set of IPv6. The following are features of the IPv6 protocol:[7]

3.3.1 New Header Format

The IPv6 header has a new format that is designed to keep header overhead to a minimum. This is achieved by moving both non-essential fields and optional fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header is more efficiently processed at intermediate routers.

3.3.2 Large Address Space

IPv6 has 128-bit (16-byte) source and destination IP addresses. Although 128 bits can express over 3.4 x 10^{38} possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization. Even though only a small number of the possible addresses are currently allocated for use by hosts, there are plenty of addresses available for future use. With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary.

3.3.3 Efficient and Hierarchical Addressing and Routing Infrastructure

IPv6 global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarizable routing infrastructure that is based on the common occurrence of multiple levels of Internet service providers.

3.3.4 Stateless and Stateful Address Configuration

To simplify host configuration, IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

One of the most useful aspects of IPv6 is its ability to automatically configure itself, even without the use of a stateful configuration protocol such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6). By default, an IPv6 host can configure a link-local address for each interface. By using router discovery, a host can also determine the addresses of routers, other configuration parameters, additional addresses, and on-link prefixes. Included in the Router Advertisement message is an indication of whether a stateful address configuration protocol should be used.

[7] Microsoft Windows Server 2003 White Paper, September 2003. Pages 2-3.

Address autoconfiguration can only be performed on multicast-capable interfaces.

3.3.5 Built-in Security

Support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations.

3.3.6 Better Support for QoS

New fields in the IPv6 header define how traffic is handled and identified. Traffic identification using a Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets belonging to a flow, a series of packets between a source and destination. Because the traffic is identified in the IPv6 header, support for QoS can be achieved even when the packet payload is encrypted through IPSec.

3.3.7 New Protocol for Neighboring Node Interaction

The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (nodes on the same link). Neighbor Discovery replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

3.3.8 Extensibility

IPv6 can easily be extended for new features by adding extension headers after the IPv6 header. Unlike options in the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

4 TRANSITION MECHANISMS FOR IPV6

IPv6 transition mechanisms are intended to provide a number of features, including:

- Incremental upgrade and deployment. Individual IPv4 hosts and routers may be upgraded to IPv6 one at a time without requiring any other hosts or routers to be upgraded at the same time. New IPv6 hosts and routers can be installed one by one.
- Minimal upgrade dependencies. The only prerequisite to upgrading hosts to IPv6 is that the DNS server must first be upgraded to handle IPv6 address records. There are no pre-requisites to upgrading routers.
- Easy Addressing. When existing installed IPv4 hosts or routers are upgraded to IPv6, they may continue to use their existing address.[8]

IPv6 provides an addressing structure called Compatibility Addresses that embeds IPv4 addresses within IPv6 addresses and encodes other information used by the transition mechanisms. The three methods available to enable IPv6 on an existing IPv4 network are Dual Stacking, Tunneling, and Translation. A combination of all three transition mechanisms will be used on Marine Corps networks.

4.1 Compatibility Addresses

To aid in the migration from IPv4 to IPv6 and the coexistence of both types of hosts, the following addresses are defined for IPv6:

4.1.1 IPv4-Compatible Address

The IPv4-compatible address, 0:0:0:0:0:0:*w.x.y.z* or ::*w.x.y.z* (where *w.x.y.z* is the dotted decimal representation of an IPv4 address), is used by IPv6/IPv4 nodes that are communicating using IPv6. IPv6/IPv4 nodes are nodes with both IPv4 and IPv6 protocols. When the IPv4-compatible address is used as an IPv6 destination, the IPv6 traffic is automatically encapsulated with an IPv4 header and sent to the destination using the IPv4 infrastructure.

4.1.2 IPv4-Mapped Address

The IPv4-mapped address, 0:0:0:0:0:FFFF:*w.x.y.z* or ::FFFF:*w.x.y.z*, is used to represent an IPv4-only node to an IPv6 node. It is used only for internal representation. The IPv4-mapped address is never used as a source or destination address of an IPv6 packet.

4.1.3 6to4 Address

[8] IP Next Generation Overview, accessible at http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html, by Robert M. Hinden, May 1995.

The 6to4 address is used for communicating between two nodes running both IPv4 and IPv6 over an IPv4 routing infrastructure. The 6to4 address is formed by combining the prefix 2002::/16 with the 32 bits of a public IPv4 address of the node, forming a 48-bit prefix. 6to4 is a tunneling technique described in RFC 3056.

4.2 Dual Stacking IPv4 and IPv6

As stated in section 1.2, a host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats. Dual Stacking is a model of deployment where all hosts and routers upgraded to IPv6 are "dual" capable. Dual Stacked hosts implement complete IPv4 and IPv6 protocol stacks. Due to the proliferation of IPv4 products, the transition to IPv6 will involve extensive enabling of dual-stack capability on networks. IPv6 provides support for the coexistence of both addressing schemes through Compatibility Addresses.

Since IP does not truly support two header formats for one packet, Dual Stacking actually implies the capability of a router or host to choose IPv4 or IPv6 for outbound traffic while retaining the ability to receive either header format.

4.3 Tunneling

Tunneling involves encapsulating IPv6 packets within IPv4 headers to carry them over segments of the end-to-end path where the routers have not yet been upgraded to IPv6. Tunneling allows isolated IPv6 hosts (i.e., located on a physical link which has no directly connected IPv6 router) to become fully functional IPv6 hosts by using an IPv4 multicast domain as their virtual local link to distant IPv6 networks.

4.4 Translation

Translation occurs at application layer gateways between portions of the network that are using different Internet protocols and allows the deployment of hosts that support only IPv6 on IPv4 networks. Because some features available in IPv6 do not translate to IPv4, Translation has limited value. IPv6 features such as flow control, multicast and unicast neighbor discovery, IPSec, and extension headers may not be supported when translated into an IPv4 network.

5 POTENTIAL CONSTRAINTS TO IMPLEMENTING IPV6

5.1 Network Appliance Memory

While support for IPv4 and IPv6 on the same router is generally a matter of upgrading the IOS and enabling routing features, there is a hardware requirement as well. Memory in routers is used to process routing requests, manage queues, and route traffic. Dual Stacking routers to support routing tables for IPv4 and IPv6 will require additional memory in most cases. The cost associated with adding memory to routers, servers, and other network appliances should not be overlooked when planning IPv6 transition.

5.2 Operating Systems

Production support for IPv6 does not exist in most operating systems in use in the Marine Corps today. Windows XP with service pack 1 or later is the first release of Microsoft operating system that advertises production IPv6 capability. Microsoft does not plan to support IPv6 with earlier versions of operating systems, including Windows 2000. Interoperability issues are likely to arise between early releases of IPv6 capable operating systems developed by different vendors.

5.3 Application Porting and Adding IPv6 Capability[9]

Applications can be developed so they are “agnostic” to the IP version in use. Software should rely on the IP stacks in COTS operating systems to the extent possible.

Many COTS and open source software applications already have some level of IPv6 support built in. The development cycles for this class of software tend to be relatively rapid so new versions should be continually examined for IPv6 functionality and maturity.

Few GOTS applications have IPv6 capabilities at this time. Porting will not enable all the functionality and capabilities of IPv6 in GOTS applications, just those that are already available with the current IPv4 software. Enabling advanced IPv6 features such as mobility, anycast addressing, and Quality of Service (QoS) will likely require additional software development, testing, and certification.

Adding IPv6 capability to applications while retaining support for IPv4 may not require significant additional effort. Vendors have stated the effort was “more tedious than difficult”. Developers can begin by downloading a scanning tool such as Sun’s IPv6 Socket Scrubber, Microsoft’s Checkv4, and Compaq’s IPv6 Porting Assistant for Tru64 Unix. These tools operate on source code to identify areas needing modification to support IPv6. Modifications can then be made to the source code and the software recompiled, tested, and certified for use. The Microsoft publication IPv6 Guide for

[9] Much of the content for this section was extracted from “Projected Impacts of IPv6 on the USN and USMC Enterprise” by Michael P. Brig. SPAWAR Systems Center Charleston.

Windows Sockets Applications[10] divides the software porting effort into five areas. These areas are:

1. Changing data structures.
2. Function calls.
3. Use of hard-coded IPv4 addresses.
4. User interface issues.
5. Elimination of user interface issues.

Scanning tools can identify lines of IPv4 socket code in applications and review and modify code with the new IPv6 socket API. Porting a socket application typically only requires a few lines of code change. Scanning tools can test code to help find any IPv4 dependencies and modify code so the application will be able to use IPv6.

It should be noted Microsoft has no plans to provide the IPv6 software libraries and function calls for Windows 2000. This complements Microsoft's strategy of providing a "production" IPv6 stack only for Windows XP (with Service Pack 1 or later) and later versions of the Windows OS.

Some GOTS applications are actually conglomerations of COTS applications and government developed code. Porting such an application might require a considerable coordination effort and involve multiple interdependencies. It is impractical to port a GOTS application if a critical COTS software component was not yet ported to IPv6. In this case, a Program Manager (PM) might simply replace that software component with a different commercial alternative but then other code changes would likely be required.

5.4 Compatibility of IPv4 and IPv6

Upper layer protocol checksums must support IPv6 headers. The current implementation of TCP and UDP for IPv4 incorporates into their checksum calculation a pseudo-header that includes both the IPv4 Source Address and Destination Address fields. This checksum calculation must be modified for TCP and UDP traffic sent over IPv6 to include IPv6 addresses.[11] In most cases interface with these upper layer protocols is provided by the operating system. Applications with hard coded upper layer protocol implementations will require development, testing and certification to enable IPv6 support.

Translation from IPv6 to IPv4 can result in loss of transfer of some IPv6 capabilities and interfere with end-to-end application performance. Refer to section 4.4 for additional considerations necessitated by network translation.

5.5 Security

Currently employed network security devices such as the Network Encryption System (NES), Fastlane, Taclane, and KY trunk encryptors must support IPv6. Firewalls

[10] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/ipv6_guide_for_windows_sockets_applications_2.asp

[11] Microsoft Windows Server 2003 White Paper, September 2003. Page 34.

must be upgraded or changed to support IPv6. Tunneling may present security and implementation challenges as encapsulated packets pass through firewalls. Firewalls will take time to examine encapsulated packets, increasing network latency and potentially affecting application performance.

Adoption of IPv6 on Marine Corps networks opens vulnerabilities from external IPv6 networks. Procedures for protecting from attacks and probes from IPv6 sources must be incorporated into current Information Assurance Vulnerability Alert (IAVA) and Naval Incidence Response Team (NAVCIRT) advisory procedures.

Dual stacking networks introduces vulnerabilities that would not exist on a single protocol network. Gateways providing protocol translation introduce another layer of complexity in the architecture and, therefore, another point that could be exploited by hackers or malicious code.

5.6 Technical and Programmatic Risks

Any IPv6 transition event that may delay scheduled program events introduces programmatic risk. Technical risks result if required capabilities are not available within an allotted timeframe. Examples of IPv6 transition events that may impact program schedules are:

- Availability of IPv6 capable hardware or software
- Software that must be recoded to support IPv6
- Operating System support for IPv6
- Reliance on an externally managed system that must transition first
- Proprietary implementations of IP that must be reengineered to support IPv6
- Security risks introduced by transition to IPv6

5.7 Implications of IPv6 Transition to Programs and Applications

Appendix B provides a checklist for identifying the IPv6 transition efforts needed for programs of record. Program Managers will use the checklist to focus engineers and planners on actions required to make their programs IPv6 capable. Enterprise planners will aggregate completed checklists to identify dependencies that will affect transition timelines. Completed templates will also facilitate efficient use of transition resources; both technical expertise and funding will be limited. Appendix C contains a similar checklist for software applications.

Appendix B. IPv6 Transition Survey for Programs of Record and Systems

Program of Record and System IPv6 Checklist

1. Software Support Activity:

PG:		PM Phone:	
PM:		PM Email:	

Prime Support Contractor:	

Enter ORGANIC if the PM Shop maintains the application with organic resources (Civilians and/or Marines)

2. System/product Identification:

a. System Name:				b. Acronym:			
c. Version #:		d. DADMS ID #:		e. DARS ID#:		f. MSTAR ID #:	

3. Program Status:

a. Current MS:		b. MS Date:		c. IATO Date:		d. ATO Date:	

4. Identify applications used: (Add more lines as required, see Type Code legend below)

Application Name	Purpose	Type	Version

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still available to the public.

S = Shareware **F** = Freeware

5. Identify reliance on IPv4: [Appendix A, Chapter 2]

a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	
b. Define how IP addresses are obtained: (static IP addresses, DNS lookup, DHCP, BOOTP, other)	

6. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6.	
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration). [Appendix A, Chapter 3]	
7. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation, i.e. processor or memory constraints, APIs, COE, etc.	
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, NCES, TDN, etc.) Upper Layer Protocols and applications.	
8. Programmatic impact(s):	
a. Schedule for system to be dual-stack and full IPv6 capable using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8a. EXAMPLE: FY07 $20K($5K), FY08 $8K($0) [Section 5.3 of the Transition Plan]	
b. Accelerated schedule for system to be dual-stack and full IPv6 capable if current Development Schedule does not meet the goal of IPv6 capable by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8b. EXAMPLE: FY07 $20K($5K), FY08 $8K($0) [Section 5.3 of the Transition Plan]	
9. Define technical and programmatic risks.	
10. Define Risk Mitigation Strategy for items identified in block 9.	
11. Can this system become a Marine Corps representative "early adopter"? (Yes / No)	

12. Recommendations: (Enter any comments or ideas you have that have a bearing on this initiative)
POC: Capt Dave Wallace, 703-693-3491,wallacedt@hqmc.usmc.mil

Appendix C. IPv6 Transition Survey for Software Applications

Software Application IPv6 Checklist

1. Software Support Activity:

FAM:		POC Phone:	
Sponsor:		POC Email:	

2. Identify applications evaluated: (Add more lines as required, see Type Code legend below)

Application Name (Acronym)	Purpose	Type	Version

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still available to the public.

S = Shareware **F** = Freeware

3. Identify Applications that are not IPv6 capable [Appendix A, Section 5.3]

Application Name (Acronym)	Describe dependence on IPv4	Impact (see Legend)	IPv6 Capable Date

Impact Code Legend:

Legacy = Application will be replaced before 2008 and will not transition.

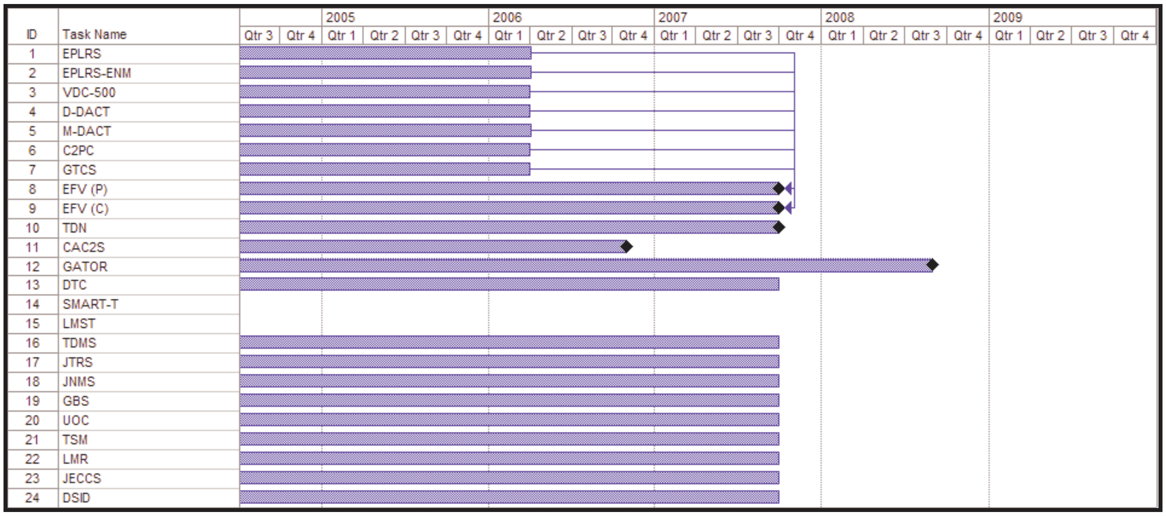
Mod = Application will be modified by date identified

Upgrade = New IPv6 capable version will be implemented by date identified

Waiver = Waiver will be submitted per guidance in Transition Plan [Section 3.3]

4. Transition Cost:	
Application Name (Acronym)	Cost schedule – list currently budgeted, such as for replacement or upgrade, and additional funding required (deficiency) for each FY to modify or upgrade software applications identified in 3 above. EXAMPLE: FY07 $10K($5K), FY08 $8K($0) [Section 5.3 of the Transition Plan]
5. Recommendations: (Enter any comments or ideas you have that have a bearing on this initiative)	
POC: Capt Dave Wallace, 703-693-3491,wallacedt@hqmc.usmc.mil	

Appendix D. List of Programs



ID	Task Name
1	EPLRS
2	EPLRS-ENM
3	VDC-500
4	D-DACT
5	M-DACT
6	C2PC
7	GTCS
8	EFV (P)
9	EFV (C)
10	TDN
11	CAC2S
12	GATOR
13	DTC
14	SMART-T
15	LMST
16	TDMS
17	JTRS
18	JNMS
19	GBS
20	UOC
21	TSM
22	LMR
23	JECCS
24	DSID

Figure 10. Program of Record Transition Timeline

IPv6 Survey D-1. Tactical Data Network

1. Program Name	Tactical Data Network
2. System/product identification	
a. Program Manager	LtCol J. D. Wilson
b. Program Group	MAGTF C4ISR
c. Milestone reached	C
3. POCs: (program and technical POCs, telephone number, address, email)	Project Officer: Capt C. J. Buchanan Team Leader: Ms. T. Conte
4. Identify Operating System(s) (OS) used	Windows NT Server 4.0
5. Identify applications used. All COTS and GOTS software should be identified.	Service Pack 6.A for NT 4.0 Video Driver: Matrox Millennium G200 Norton AntiVirus 7.6 Netscape Communicators 6.2 Walusoft TFTPSuitePro2000 3.6 Network Time Protocol (XNTP 3.5) Client/Server Window Service For Unix 1.0 Tera Term Pro 2.3 Printer Driver Tape Driver Norton SpeedDisk 5.0 Adobe Acrobat Reader 5.0 MetaIP 4.1 Enterprise Edition (with SP4) Internet Explorer 5.5SP2 NT Option Pack 4 (IIS 4.0 & FTP) SiteNet MultiLink 1.5 COE Kernel 3.4 HPOV NNM 6.1 DMS GWS 2.0.3 (Microsoft Exchange 5.5) Veritas Backup Exec 8.0.3166 Veritas Backup Exchange Module Install Shield Script 1.0 Norton Ghost 6.0 NNM-RME Integration Package CiscoWorks 2000 Roxio Easy CD Creator Power Console Plus U-Promote 4.61

	Card Wizzard 5.20.04
6. Define how each application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	No to all
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	TDN uses multiple COTS software products. Moving to Windows 2003 in order to facilitate IPv6 will require a new software baseline, so this will not be applicable to an upgraded system. It is not known how IP calls are implemented in the COTS software.
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	IP addresses are obtained via DHCP (NIPRNET), but the TDN DDS system supports DHCP.
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	Routers and switches and NICs will have to be upgraded, and a new software baseline will need to be developed.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6, IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	TDN will act as the conduit for tactical data traffic, so this would be pertinent to the system only in context of the applications it is supporting. Since this equates to all tactical data systems, all these capabilities will be leveraged as appropriate. They should all be available unless system performance is degraded.
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network	This is not well known at this time. We have hardware upgrades planned in FY-05-07 that will ensure our routers and switches are ready, the software should be in place by then also. Dependencies that we know of are: Operating System Routers & Switches Operator Training COTS applications (unknown)

services, etc.	Encryption Devices
b. Describe external systems with which your system is known to communicate using IP.	DTC, DISN, SIPRNet, NIPRnet
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	2005 – Upgrade TDN Gateway hardware 2006 – Upgrade DDS processors 2007 – Upgrade DDS routers and switches 2007 - Upgrade OS
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	2005 – Upgrade TDN Gateway hardware 2006 – Upgrade DDS processors 2007 – Upgrade DDS routers and switches 2007 - Upgrade OS
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	$5.3M will be needed to upgrade to Windows Server 2003. Although another OS upgrade will be needed in 2007, this will support the hardware upgrades so that we may use the dual stack capability. Hardware upgrades will cost about $26M. Total cost is $42M, but only 5.3 that is not already budgeted.
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	$5.3M in FY-05 is not budgeted for. This includes modifying the schoolhouse also.
11. Recommendations/Comments	
12. Is this program a good candidate to become a Marine Corps IPv6 “early adopter”?	Yes. Relatively low number of systems (507) with large return on investment (all tactical data comms). Compressing time to change over could yield economies of scale.

IPv6 Survey D-2. EFV (C)

EFV (C) Program of Record and System IPv6 Checklist

1. Software Support Activity:

PG:	Direct Reporting Program Manager (DRPM) Advanced Amphibious Assault (AAA)	PM Phone:	(703) 492-3300
PM:	Colonel Michael M. Brogan	PM Email:	BroganMM@efv.usmc.mil

Prime Support Contractor:	General Dynamics Amphibious Systems

Enter ORGANIC if the PM Shop maintains the application with organic resources (Civilians and/or Marines)

2. System/product Identification:

a. System Name:	Expeditionary Fighting Vehicle Command Variant					b. Acronym:	EFV(C)
c. Version #:	N/A	d. DADMS ID #:	N/A	e. DARS ID#:	N/A	f. MSTAR ID #:	N/A

3. Program Status:

a. Current MS:	B	b. MS Date:	Nov 2000	c. IATO Date:	FY 2007	d. ATO Date:	FY 2007

4. Identify applications used: (Add more lines as required, see Type Code legend below)

Application Name	Purpose	Type	Version
Windows NT Workstation	C2PC Operations	C	4.0
Windows 2000	Vehicle Operations	C	2000
Windows NT Server	C2PC Gateway	C	4.0 w/SP6a
Solaris	AFATDS Operations	C	2.5.1
Solaris	IOS(V)2 Operations	C	2.7
VxWorks	Vehicle Operations	C	5.4.2
AFATDS	AFATDS Operations	G	6.3.1 SP4
X Windows	Solaris Unix Operations	C	N/A
IOS (V)2	IOS(V)2 Operations	G	3.6
C2PC	C2PC Operations	G	5.9.0.3
Effects Management Tool	Allows track dissemination between AFATDS, IOS, and C2PC	G	6.3.1
EPLRS Network Manager	EPLRS Operation	G	4.0.2
Microsoft Internet Explorer	Web application	C	5.0
Adobe Acrobat Reader	Review .pdf files	C	4.0
Altiris Carbon Copy	Remote control application—provides the tools needed to remotely administer the EFV network from any onboard Data Processing Unit	C	5.6
Cryptek Secure Communications Printer Services	TS-21 Printer/Fax/Scanner Operations	C	N/A
GNU Ghostscript	allows UNIX machines to print to the Cryptek printer	C	7.04

Ghostgum Software GSview	allows UNIX machines to print to Cryptek Printer	C	4.2
Hummingbird Exceed	permits applications, normally available only on UNIX workstations, to be readily accessed from enterprise desktops	C	7.0
HP OpenView Network Node Manager	provides a variety of real-time views of your network status and alerts you to network problems remotely by pager or e-mail before they escalate into expensive downtime events	C	6.1
Internet Locator Server	Provides white board capablity	C	2.0
Leutron Vision Software Development Suite	Viewing live video from the Vehicle Thermal Viewer	C	1.93.001
Microsoft Exchange 2000 Enterprise Server	TDN Exchange Services	C	2000
TimeServ	Provides network time to all Data Processing Units (DPU's)	C	1.5
Microsoft Windows Services for UNIX®	Network File System	C	2.0
Microsoft Windows NetMeeting	can be used to remotely access computers for multiple purposes, hold a videoconference, transfer files and conduct a private chat	C	3.01
Redmon Redirction Port Monitor	allows printing from UNIX to NT	C	N/A
Symantec Norton Anti Virus	Network Virus Protection	C	2000
Symantec Norton Ghost Corporate Edition	Image System Software	C	7.5
3Com Boot Services OEM	Provides remote network booting and rebooting	C	1.02
WinZip	File compression	C	8.0
JAVA Run Time	JAVA Operations	C	N/A
Ground Tactical Communications Services	SP-TCIM/TacLink 3000 Operations	G	2.0.0.5
Test Utilities Client Processor Manager	Spray Cool Test Manager	G	3.0a
Test Utilities	Spray Cool Test Manager	G	3.0a
Mobility, Power Management, and Auxilary (MPA)	EFV Unique Software for Vehicle Operations	G	N/A
Control and Displays (C&D)	EFV Unique Software for Vehicle Operations	G	N/A

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still available to the public.

S = Shareware **F** = Freeware

5. Identify reliance on IPv4: [Appendix A, Chapter 2]

a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet routers and switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Define how IP addresses are obtained: (static IP addresses, DNS lookup, DHCP, BOOTP, other)	Static IP addresses. EFV unique MPA and C&D software use hard-coded IP addresses and will require further development, testing, and certification to support dual stack IPv4 and IPv6 functionality.
6. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6.	1) EFV unique MPA and C&D software will require software code modification to support dual stack IPv4 and IPv6 functionality. 2) C2PC software code modification will be required to support dual stack IPv4 and IPv6 functionality (Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 4) Upgrades will be required to support dual stack IPv4 and IPv6 routing functionality for all Ethernet switches, Ethernet routers, EFV unique displays, EPLRS Radios, VDC-500, and SP-TCIM/TacLink 3000 modems. 5) AFATDS software code modification will be required to support dual stack IPv4 and IPv6 routing functionality (Army/Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 6) IOS (V2) software code modification will be required to support dual stack IPv4 and IPv6 routing functionality (Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 5) EFV will be required to upgrade, integrate, and test all operating systems and applications to a dual stack IPv4 and IPv6 capability.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration). [Appendix A, Chapter 3]	This depends on the modification of the Marine Air Ground Task Force (MAGTF) architecture migration to support both IPv4 and IPv6 routing functionality.
7. Dependencies:	

a. Describe technical dependencies that will impact the system with IPv6 implementation, i.e. processor or memory constraints, APIs, COE, etc.	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet routers and switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, NCES, TDN, etc.) Upper Layer Protocols and applications.	AFATDS, IAS, IOW, DACT, GCCS, TBMCS
8. Programmatic impact(s):	
a. Schedule for system to be dual-stack and full IPv6 capable using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	The EFV(C) is under development and is expected to obtain a Milestone C decision in late FY05 and reach IOC in FY08. DRPM AAA's technology migration plan will begin IPv6 development in FY05 and expect to be fully capable of IPv4 and IPv6 by FY08. However, a dual stack IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to AFATDS, IOS(V2), C2PC, and GTCS software.
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8a that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
b. Accelerated schedule for system to be dual-stack and full IPv6 capable if current Development Schedule does not meet the goal of IPv6 capable by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	Not Applicable
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8b that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
9. Define technical and programmatic risks.	
An IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to AFATDS, IOS(V2), C2PC, GTCS software, EPLRS, and the VDC-500.	
10. Define Risk Mitigation Strategy for items identified in block 9.	
Can only be addressed by the USMC	
11. Can this system become a Marine Corps representative "early adopter"? (Yes / No)	No

IPv6 Survey D-3. EFV (P)

EFV (P) Program of Record and System IPv6 Checklist

1. Software Support Activity:

PG:	Direct Reporting Program Manager (DRPM) Advanced Amphibious Assault (AAA)	PM Phone:	(703) 492-3300
PM:	Colonel Michael M. Brogan	PM Email:	BroganMM@efv.usmc.mil

Prime Support Contractor:	General Dynamics Amphibious Systems

Enter ORGANIC if the PM Shop maintains the application with organic resources (Civilians and/or Marines)

2. System/product Identification:

a. System Name:	Expeditionary Fighting Vehicle Personnel Variant					b. Acronym:	EFV(P)
c. Version #:	N/A	d. DADMS ID #:	N/A	e. DARS ID#:	N/A	f. MSTAR ID #:	N/A

3. Program Status:

a. Current MS:	B	b. MS Date:	Nov 2000	c. IATO Date:	FY 2007	d. ATO Date:	FY 2007

4. Identify applications used: (Add more lines as required, see Type Code legend below)

Application Name	Purpose	Type	Version
Windows 2000	Vehicle Operations	C	2000
Windows NT Server	C2PC Gateway	C	4.0 w/SP6a
VxWorks	Vehicle Operations	C	5.4.2
C2PC	C2PC Operations	G	5.9.0.3 SP4
JAVA Run Time	JAVA operations	C	N/A
Mobility, Power Management, and Auxilary (MPA)	EFV Unique Software for Vehicle Operations	G	N/A
Control and Displays (C&D)	EFV Unique Software for Vehicle Operations	G	N/A
Fire Control (FC)	EFV Unique Software for Vehicle Weapon Employment	G	N/A
Altiris Carbon Copy	Remote control application—provides the tools needed to remotely administer the EFV network from any onboard Data Processing Unit	C	5.6
Ground Tactical Communications Services	SP-TCIM/TacLink 3000 Operations	G	2.0.0.5

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still available to the public.

S = Shareware **F** = Freeware

5. Identify reliance on IPv4: [Appendix A, Chapter 2]

a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	MPA, C&D, and FC EFV unique software use OS function calls and protocol stacks. All COTS and GOTS products are not under control of the EFV program office.

b. Define how IP addresses are obtained: (static IP addresses, DNS lookup, DHCP, BOOTP, other)	Static IP addresses. EFV unique MPA, C&D, and FC software use hard-coded IP addresses and will require further development, testing, and certification to support dual stack IPv4 and IPv6 functionality.
6. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6.	1) EFV unique MPA, C&D, and FC software will require software code modification to support dual stack IPv4 and IPv6 functionality. 2) C2PC software code modification will be required to support dual stack IPv4 and IPv6 functionality (Marine Corps responsibility). EFV will be required to integrate and test this new functionality. 4) Upgrades will be required to support dual stack IPv4 and IPv6 routing functionality for all Ethernet switches, EFV unique displays, EPLRS Radios, VDC-500, and SP-TCIM/TacLink 3000 modems. 5) EFV will be required to upgrade, integrate, and test all operating systems and applications to a dual stack IPv4 and IPv6 capability.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration). [Appendix A, Chapter 3]	This depends on the modification of the Marine Air Ground Task Force (MAGTF) architecture migration to support both IPv4 and IPv6 routing functionality.
7. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation, i.e. processor or memory constraints, APIs, COE, etc.	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, NCES, TDN, etc.) Upper Layer Protocols and applications.	IOS, DACT, GCCS
8. Programmatic impact(s):	

a. Schedule for system to be dual-stack and full IPv6 capable using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	The EFV(P) is under development and is expected to obtain a Milestone C decision in late FY05 and reach IOC in FY08. DRPM AAA's technology migration plan will begin IPv6 development in FY05 and expect to be fully capable of IPv4 and IPv6 by FY08. However, a dual stack IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to AFATDS, IOS(V2), C2PC, and GTCS software.
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8a that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
b. Accelerated schedule for system to be dual-stack and full IPv6 capable if current Development Schedule does not meet the goal of IPv6 capable by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	Not Applicable
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8b that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
9. Define technical and programmatic risks.	
An IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to C2PC, GTCS software, EPLRS, and the VDC-500.	
10. Define Risk Mitigation Strategy for items identified in block 9.	
Can only be addressed by the USMC	
11. Can this system become a Marine Corps representative "early adopter"? (Yes / No)	No

IPv6 Survey D-4. CAC2S

1. Program Name	Common Aviation Command and Control System
2. System/product identification	CAC2S
a. Program Manager	PM Operations Centers
b. Program Group	Product Group 11, Battlespace Management and Air Defense Systems (BMADS)
c. Milestone reached	B
3. POCs: (program and technical POCs, telephone number, address, email)	Team Lead: LtCol Jeff Speights, (703)432-4104, speightsjs@mcsc.usmc.mil System Engineer: Maj Todd Emo, (703)432-4086, emotr@mcsc.usmc.mil
4. Identify Operating System(s) (OS) used	VxWorks 5.4, Win2000, Solaris
5. Identify applications used. All COTS and GOTS software should be identified.	**GOTS:** SSDS MK II MTS **COTS:** AccessNet Ternion- FLAMES Gallium InterMAPhics Various MS Products Exceed (Unix emulation)
6. Define how <u>each</u> application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	GOTS – yes; COTS –no.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	Sockets The COTS products use O/S function calls.
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	The system uses both DHCP and Static IP addresses under administrator control. Certain radar interfaces currently use hard-coded IP addresses.
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008.	Dual Capability: o Replace system routers and switches to obtain full IPv6 capability external to this system.

See Chapter IV.	Full Capability: o Replace system routers and switches with IPv6 capable H/W o Significant modification to approximately 6 interface software SCIs o Transition to next version of O/Ss that support IPv6
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6, IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	None at this time.
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	VxWorks support for IPv6. Win2000 (DII-COE O/S) support for IPv6 Transition of external systems identified in 8.b.
b. Describe external systems with which your system is known to communicate using IP.	SIPRNet NIPRNet GCCS I3/IAS AFATDS TBMCS CEC CDLMS EPLRS
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	Detailed schedule being analyzed by development prime contractor. Dual IPv6 is anticipated by 2006.
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	Detailed schedule being analyzed by development prime contractor. Dual IPv6 is anticipated by 2006. CAC2S system fields in 2007.

c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	Unknown at this time. Clearly involves some hardware replacements and software modifications, as well as dependencies on several other DoD systems. Prime contractor is currently developing a cost impact.
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	IPv6 implementation requirements for security re-certification.
11. Recommendations/Comments	
12. Is this program a good candidate to become a Marine Corps IPv6 "early adopter"?	No. Critical dependencies on other Navy and Joint programs limit Marine Corps flexibility.

IPv6 Survey D-5. GATOR

1. Program Name	**Ground Air Task Oriented Radar (GATOR)**
2. System/product identification	Not assigned
a. Program Manager	Mr. John McGough, (703) 432-4217
b. Program Group	BMADS Radar
c. Milestone reached	MSA, MSB scheduled for DEC04
3. POCs: (program and technical POCs, telephone number, address, email)	Capt. Kenneth VanZandt, (703)432-4246, vanzandtkl@mcsc@usmc.mil GySgt Hondo Shaver, (703) 432-4228, shaverhj@mcsc.usmc.mil
4. Identify Operating System(s) (OS) used	TBD
5. Identify applications used. All COTS and GOTS software should be identified.	TBD
6. Define how each application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	Pre MSB no code has been written. This system will be fielded after FY08. All requirements for IPV6 should be addressed during the system design and development process.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	UNK
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	UNK
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	UNK
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6,	UNK

IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	UNK
b. Describe external systems with which your system is known to communicate using IP.	UNK
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	This system will be fielded after FY08. All requirements for IPV6 should be addressed during the system design and development process.
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	UNK
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	UNK
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	UNK
11. Recommendations/Comments	None
12. Is this program a good candidate to become a Marine Corps IPv6 “early adopter”?	No, The system is not scheduled to field until after FY08

IPv6 Survey D-6. Firefinder Radar System

1. Program Name	**Firefinder Radar System, AN/TPQ-36 (V)8 (USA), AN/TPQ-46A (USMC)**
2. System/product identification	AN/TPQ-36 (V)8 (US Army), AN/TPQ-46A (USMC)
a. Program Manager	Mr. John McGough, (703) 432-4217
b. Program Group	BMADS Radar
c. Milestone reached	Sustainment
3. POCs: (program and technical POCs, telephone number, address, email)	GySgt Hondo Shaver, (703) 432-4228, shaverhj@mcsc.usmc.mil POC Mary Ann Pursley, DSN 639-3651, Comm (580) 442-6351.
4. Identify Operating System(s) (OS) used	Linux, Sun Solaris, Windows
5. Identify applications used. All COTS and GOTS software should be identified.	Red Hat Linux, Sun Solaris, FFPAS
6. Define how <u>each</u> application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	YES, The source code for this system is owned and maintained by the US Army's Fort Sill Software Engineering (FSSE) Center, Ft Sill, Oklahoma. POC Mary Ann Pursley, DSN 639-3651, Comm (580) 442-6351.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6,	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.

IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
b. Describe external systems with which your system is known to communicate using IP.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.
11. Recommendations/Comments	None
12. Is this program a good candidate to become a Marine Corps IPv6 "early adopter"?	Possibly because IPV6 is scheduled for fielding in4Qtr Fy07 by the US Army through FSEE.

Appendix E. Application Baseline

Application Listing E-1. COTS

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
					Legacy = Will not transition **MM/YY** = Capability Date **UN** = Undetermined **None** = Unaffected
ActivCard Gold		2.X	Activcard Corporation		UN
Active Perl		Build 633	ActiveState Tool, Inc	M&RA (MMSB)	UN
Adobe GoVideo			Adobe		UN
Adobe Illustrator 10			Adobe		UN
Adobe Premiere			Adobe		UN
FormFlow		2.23	Adobe		UN
Adobe InDesign			Adobe		UN
Adobe Pagemaker		7.0	Adobe		UN
Acrobat Distiller		5	Adobe Systems Inc.	M&RA (MMSB)	UN
Adobe Acrobat		6.0	Adobe Systems Inc.		UN
Adobe After Effects			Adobe Systems Inc.		UN
Adobe LiveMotion			Adobe Systems Inc.		UN
Adobe Photoshop		7.0	Adobe Systems Inc.		UN
Total Eclipse	Eclipse	v3.0.2.3	Advantage Software	SJA	UN
Alcatel VPN Client			Alcatel		UN
Cold Fusion		Sever 5.0 / Ultradev Studio 4.5	Allaire Corporation	MCLB Barstow	UN
XML Spy Professional			Altova, Inc.	M&RA	UN
Apple Quicktime Movie and Audio Viewer		v4.12	Apple		UN
Arbortext Adept Editor		4.2.1, 8	Arbortext	MARCORSYSCOM	UN
Autodesk AutoCAD			Autodesk		UN
Avid DV Express		3.0	Avid		UN
Axent Enterprise Security Manager	ESM	v5.1	Axent Technologies		UN
Axent Intruder Alert		v3.5	Axent Technologies		UN
SNA/NJE Enterprise Print Server		v3.0.21	Bar Systems Inc.		UN
Mobius DocuAnalyzer			Bateleur		UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
Mobius DocumentDirect			Bateleur		UN
Mobius ViewDirect for Networks		3.3	Bateleur		UN
BelArc Advisor			Belarc		UN
Golden32		5.6	Benthic Software	MCB Camp Lejeune / AC/S Installations and Environment Department	UN
Blinker		5.1, 6	Blinkinc	MARCORSYSCOM	UN
Remedy HelpDesk			BMC Software		UN
Borland Resource Workshop		4.5	Borland	MARCORSYSCOM	UN
Delphi Enterprise		6	Borland Intl.	1st MAW, ALD-IT	UN
Hot Docs		v5.2	Capsoft		UN
Object Nationalizer		1.5.1	Centura Software Corporation	MCAS Beaufort	UN
Citrix Independent Computing Architecture Client	Citrix ICA	6.2	Citrix		UN
Citrix Metaframe XP			Citrix		UN
Direct Edit		2.5	Codeholio	MARCORSYSCOM	UN
Cognos Suite			Cognos		UN
BP+D320Win		4	Computer Associates	TECOM(MCI)	UN
BPWIN		4	Computer Associates	MARCORSYSCOM	UN
Clipper		5.3b	Computer Associates	MARCORSYSCOM	UN
ERWIN		4	Computer Associates	MARCORSYSCOM	UN
DevPartner		7	Compuware	MCDDC, (M&RA HQMC)	UN
Corel Draw 11			Corel Corporation		UN
Crystal Decisions Crystal Reports		DVPRC	Crystal Decisions		UN
Time Matters		v3.0(03)	DATA.TXT Corporation		UN
DBMax		1.4	David Kennedy	MARCORSYSCOM	UN
Discreet Cleaner		5	Discreet		UN
RoboDeluxe		2002	eHelp	MARCORSYSCOM	UN
ARC Product Suite			ESRI		UN
Diskkeeper		6.0	Executive Software		UN
OCR (Client)		3.5	Expervision, Inc.	M&RA (MMSB)	UN
InfoWorkSpace		2.1	Ezenia		UN
FiveWin for Harbour		2.3	FiveTech	MARCORSYSCOM	UN
WinDBU		3.3	FiveTech	MARCORSYSCOM	UN
ForTheRecord-Gold	FTR		FTR Limited		UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
HP OpenView			Hewlett-Packard		UN
PictPlus 50		5	Informatik, Inc.	M&RA (MMSB)	UN
NetAdvantage Enterprise Edition		2003	Infragistics	Marine Forces Reserve	UN
VBAssist		5	Infragistics	MCDDC, (M&RA HQMC)	UN
Quicken 2003			Intuit		UN
IPIX		v6.2.0.5	IPIX Infomedia Group		UN
Janus GridEx		2000	Janus Systems	Manpower & Reserve Affairs, Headquarters, U.S. Marine Corps	UN
Lead Tools		9	Lead Technologies, Inc.	M&RA (MMSB)	UN
Pop-up Menu Creator		4.6.2	Lifteris Heritou	MCCDC M&RA	UN
Lotus Domino		4.6.6, R5.0.1	Lotus		UN
Lotus Domino Designer		R5	Lotus	MARCORSYSCOM	UN
Lotus Notes			Lotus		UN
Lotus Notes Client and Designer		5.0.8	Lotus	MARCORSYSCOM	UN
Cold Fusion Server		5	Macromedia	TECOM (Command and Staff College)	UN
Cold Fusion Studio		4.5.2	Macromedia	TECOM (Command and Staff College)	UN
Flash MX		6	Macromedia	MCB Camp Pendleton, AC/S Environmental Security, MARCORSYSCOM	UN
Flash Player		5.0	Macromedia		UN
Macromedia Director			Macromedia		UN
Macromedia Dreamweaver MX		MX	Macromedia	TECOM, MCCDC, AAAV	UN
Macromedia Fireworks			Macromedia		UN
Macromedia Shockwave		v8.0	Macromedia		UN
PVCS Configuration Builder		5.3.00	Merant	MARCORSYSCOM	UN
WinRunner Professional		7.5	Mercury Interactive	MARCORSYSCOM	UN
Microsoft SharePoint Portal Server			Micorsoft		UN
.NET FRAMEWORK	.NET	1.1	Microsoft	HQMC, M&RA, Personnel Management Support Branch (MMSB) MM,	UN
Front Page 2002		2002 Professional, 2003	Microsoft	III MEF, MARCORSYSCOM, MCLB Barstow, PAO, MCB Quantico, MCCDC, EFDC, Doctrine Division (C-42)	UN
Image Composer		1.5	Microsoft	MARCORSYSCOM	UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
Internet Information Server	IIS	4.0	Microsoft		UN
Microsoft Access 2000			Microsoft		UN
Microsoft Data Access Components		1	Microsoft	HQMC, M&RA, Personnel Management Support Branch (MMSB) MM,	UN
Microsoft Excel 2000 (Bundled w/App Suite)			Microsoft		UN
Microsoft FrontPage 2003			Microsoft		UN
Microsoft Internet Explorer		6.0	Microsoft		UN
Microsoft Office 2000 Professional		SP2	Microsoft		Capable
Microsoft Outlook 2000			Microsoft		UN
Microsoft Powerpoint 2000			Microsoft		UN
Microsoft Project 2002			Microsoft		UN
Microsoft Publisher			Microsoft		UN
Microsoft Systems Management Server	SMS	v2.0	Microsoft		UN
Microsoft Visio Professional 2002			Microsoft		UN
Microsoft Visual InterDev		6	Microsoft		UN
Microsoft Visual Studio		.NET 2002	Microsoft	MCLC	UN
Microsoft Word 2000			Microsoft		UN
MS SQL Server			Microsoft		UN
MSDN Universal Subscription			Microsoft	MCCDC, MARCORSYSCOM	UN
NetMeeting		v3.01	Microsoft		UN
Visual Basic Enterprise		6	Microsoft	MARCORSYSCOM, MCCDC, EFDC, DOCTRINE DIVISION (C-42)	UN
Visual C++		4, 5, 6	Microsoft	M&RA (MMSB)	UN
Windows 2000 Professional		SP3 SRP1	Microsoft		UN
Windows Media Player v7.0.0			Microsoft		UN
Windows NT Workstation		4.0 SP6A	Microsoft		UN
Windows XP		SP1, SP2, SP3	Microsoft		Capable
Maximo			MRO Software		UN
NCS ScanTools		2.303	NCS Pearson	TECOM (MCU)	UN
Scan Tools II Application Development		UNKNOWN	NCS Pearson	MARCORSYSCOM	UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
Nestor Reader		5.2	NCS, Inc.	M&RA (MMSB)	UN
Netscape Communicator		4.79	Netscape		UN
One View: Object Manager		9	Network Imaging Corporation	M&RA (MMSB)	UN
Winzip Self Extractor		2.1	Nico Mak Computing Inc.	MARCORSYSCOM	UN
ASP TreeView		Classic Pro & XP styles	obout, inc	MCLC Blount Island Command	UN
FiveWin Enterprise		1.9.2	Omicron Software Publishing Corp.	MARCORSYSCOM	UN
Onset MetaMessage for Wireless			Onset Technology		UN
J-Initiator			Oracle		UN
Oracle 9i			Oracle		UN
Oracle Internet Application Server		9ias	Oracle		UN
Oracle Portal			Oracle		UN
PIXTOOLS		4.2	PIXTOOL Translations, Inc.	M&RA (MMSB)	UN
Process Model		4.2.7	Process Model Inc.	MARCORSYSCOM - MCTSSA	UN
Bonapart		3.3.30	Proubis GmbH	MARCORSYSCOM - MCTSSA	UN
Quark Xpress		6.0	Quark		UN
Knowledge Expert for Oracle Administration		Unknown	Quest	MARCORSYSCOM	UN
Knowledge Expert for PL/SQL Development		Unknown	Quest	MARCORSYSCOM	UN
SQL Navigator expert edition			Quest	MCDDC, (M&RA HQMC)	UN
Tool for Oracle Application Developers		7.5	Quest Software	MCAS Cherry Point, North Carolina	UN
Powermapper		3	Qwerk Software	Advanced Amphibious Assault	UN
Rational Rose		2	Rational Software	MARCORSYSCOM - MCTSSA	UN
Rational Suite		3	Rational Software Corporation	Advanced Amphibious Assault	UN
Real Networks Real Player 8		8	Real Networks		UN
MGI Videowave 5.0		5.0	Roxio		UN
Roxio Easy CD Creator v5		v5	Roxio		UN
Maruo Editor		3.19	SAITO Kikaku	MCAS Iwakuni	UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
ABC Technologies OROS			SAS		UN
Dragon Naturally Speaking		v6.1	ScanSoft Inc.		UN
OmniPage Pro 12 Office			ScanSoft Inc.		UN
Crystal Reports 8.5 Developers Edition		8.5	Seagate Software, Inc	MCLB Albany ACS/LOGS - Consolidated Material Service Center	UN
InFocus		4.1.2	SSB Technologies, Inc.	TECOM (MAGTFTC, 29 Palms CA)	UN
Java Development Kit	JDK	1.2	SUN Microsystems	HQMC I&L Department	UN
PowerBuilder Enterprise Series		3.04	Sybase Incorporated	Advanced Amphibious Assault	UN
Sybase Enterprise Application Studio		7	Sybase Incorporated	Advanced Amphibious Assault	UN
PowerBuilder		8	Sybase, Inc	M&RA (MMSB), MARCORSYSCOM	UN
Norton Antivirus Corporate Edition		v7.6	Symantec		UN
Symantec Ghost			Symantec		UN
WinFax Pro			Symantec		UN
Syntrillium Cool Edit Pro			Syntrillium		UN
TeamStudio		Edition 17	TeamStudio, Inc.	MARCORSYSCOM	UN
X-Tie RT		RT	Teledyne Brown Engineering	Advanced Amphibious Assault	UN
Perl		5.8	The Perl Foundation	MCB Camp Pendleton Communication/Information Systems	UN
Form Fix		2.8	TMS Sequoia, Inc	M&RA (MMSB)	UN
Ulead PhotoImpact/Explorer/Express			Ulead		UN
Universal Tax Systems TaxWise			Universal Tax Systems		UN
SQL Navigator		3.2	UNKNOWN	MARCORSYSCOM	UN
WinEdit		99, April Build (99e)	UNKNOWN	MARCORSYSCOM	UN
Veritas Backup Exec		8.6	Veritas		UN
WinWay Resume			Winway		UN
WinZip		v8	Winzip Computing Inc		UN
Reflection		10.x	WRQ		UN
Crimson Editor		3.5.1	www.crimsoneditor.com	MARCORSYSCOM	UN
Exceed Zip Compression Library		4.5	Xceedsoft	MARCORSYSCOM	UN

Application Name	Acronym	Version	Manufacturer	FAM or Sponsor	IPv6 Impact
Bolton James Masterkey Plus	MK+				UN
Common Operating Environment Message Processor	COE MP				UN
Drafting Libraries WILLS		v7.0		SJA	UN
Fleet Anywhere					UN
Military Justice				SJA	UN

Application Listing E-2. Deployable Applications

Application Name	Acronym	FAM	Owner	IPv6 Impact
				Legacy = Will not transition **MM/YY** = Capability Date **UN** = Undetermined **None** = Unaffected
Air Defense Communications Platform	ADCP	AVN	USMC	UN
Advanced Tactical Air Reconnaissance System	ATARS	AVN	USN	UN
Common Aviation Command and Control System	CAC2S	AVN	USMC	UN
Communications Air Support Central	CASC	AVN	USMC	UN
Marine Air Traffic Control And Landing System	MATCALS	AVN	USMC	UN
Multifunction Information Distribution System	MIDS	AVN	USMC	UN
NALCOMIS History Retrieval System	NALC HIST RET	AVN	USN	UN
NALCOMIS Intermediate Maintenance Activity - Legacy	NALC IMA - LEGACY	AVN	USN	UN
NALCOMIS Intermediate Maintenance Activity - Optimized	NALC IMA-O	AVN	USN	UN
NALCOMIS Organizational Maintenance Activity - Legacy	NALC OMA - LEGACY	AVN	USN	UN
NALCOMIS Organizational Maintenance Activity - Optimized	NALC OOMA	AVN	USN	UN
Naval Aviation Logistics Command Management Information System	NALCOMIS *	AVN	USN	UN
Optimized Naval Aviation Logistics Command Management Information System	Optimized NALCOMIS	AVN	USN	UN
Relational Supply	R Supply	AVN	USN	UN
Theater Battle Management Core Systems	TBMCS	AVN	AF	UN
Tactical EA-6B Mission Planning System	TEAMS	AVN	USN	UN
Electronic Key Management System	EKMS	C4	NSA	UN
Ground Mobile Forces Network Planning Prototype	GMF NETPLAN	C4	AR	UN
Ionospheric Communications Enhanced Area Coverage Predictions	ICEAREA	C4	DoC	UN
Ionospheric Communications Enhanced Profile Analysis and Circuit Prediction	ICEPAC	C4	DoC*	UN
Joint Defense Information Infrastructure Control Systems – Deployed	JDIICS-D	C4	DISA	UN
Automated Information Systems for Personal Computers	AISPC	I&L	USN/USMC	UN
Automatic Identification Technology	AIT	I&L	AR	UN

Application Name	Acronym	FAM	Owner	IPv6 Impact
Asset Tracking Logistics And Supply System II+ Desktop	ATLASS NTCSS DESKTOP	I&L	USMC	UN
AutoCAD Lite 2002	AutoCAD Lite 2002	I&L	USN	UN
Aviation Maintenance Material Management	AV3M	I&L	USN	UN
Aviation Maintenance Material Management - Data Entry	AV3M DE	I&L	USN	UN
Broadened Arrangement of Resources from a Basic Accessory Relocation Application Supply Inventory Reporting Systems	BARBARASIRS	I&L	USMC	UN
Terminal Emulation	E-TERM	I&L	USN/USMC	UN
Fuels Automated System	FAS	I&L	DLA	UN
Inflight Refueling System	IFR	I&L	USN	UN
Local Asset Management System	LAMS	I&L	USN	UN
Logistics Sustainment Analysis and Feasibility Estimator	LOGSAFE	I&L	Joint	UN
Fleet Automated Control Facts Tracking System - NTCSS	NTCSS FACTS	I&L	USN	UN
Integrated Barcode System - NTCSS	NTCSS IBS	I&L	USN	UN
Naval Tactical Command Support System Relation Supply I	NTCSS R-SUPPLY I	I&L	USN	UN
Ships and MALS Automated Reconciliation Tracking System - NTCSS	NTCSS SMARTS	I&L	USN	UN
Ported SNAP Workstation Load	PSNAP WRKSTA LOAD	I&L	USN	UN
Fleet Automated Control Facts Tracking System - Retrograde Shipping PSNAP I NT	PSNAPI FACTS/NT-R	I&L	USN	UN
Fleet Automated Control Facts Tracking System - Transhipping PSNAP I NT	PSNAPI FACTS/NT-T	I&L	USN	UN
Fleet Imaging Management System - PSNAP I	PSNAPI FIMS	I&L	USN	UN
Integrated Barcode System - PSNAP I NT	PSNAPI IBS-NT	I&L	USN	UN
Ported SNAP I Organizational Maintenance Management System	PSNAPI OMMS	I&L	USN	UN
Ships and MALS Automated Reconciliation Tracking System - NT	PSNAPI SMARTS-NT	I&L	USN	UN
Ported SNAP I Shipboard Uniform Automated Data Processing System	PSNAPI SUADPS	I&L	USN	UN
PSNAP I TYCOM Alternative Program TAC 3	PSNAPI TAC3WW	I&L	USN	UN
Support Equipment Resources Management Information System	SERMIS	I&L	USN	UN
Support Equipment Standardized System	SESS	I&L	USN	UN

Application Name	Acronym	FAM	Owner	IPv6 Impact
Theater Medical Information Program	TMIP	I&L	USN	UN
Discrimination and Sexual Harassment Reporting Program	DASH	IG		UN
Marine Corps Command Climate Assessment System for Windows	MCCASWin	IG	USMC	UN
Commanders Tactical Terminal	CTT	INTEL	AR	UN
Deployable Geospatial Information Library Workstation	DGIL	INTEL	USMC	UN
Deployable Geospatial Information Library (Server)	DGIL (Server)	INTEL	USMC	UN
Department of Defense Intelligence Information System	DODIIS	INTEL	DIA	UN
Digital Terrain Analysis Mapping System	DTAMS	INTEL	USMC	UN
Intelligence Analysis System	IAS	INTEL	USMC	UN
Intelligence/Operations Workstation	IOW	INTEL		UN
Joint Collection Management Tool	JCMT	INTEL	AR	UN
Joint Deployable Intelligence Support System	JDISS	INTEL	Joint	UN
Joint Services Imagery Processing System-NAVY	JSIPS-N	INTEL	USN	UN
Joint Worldwide Intelligence Communications System	JWICS	INTEL	DIA	UN
Marine Expeditionary Force Intelligence Analysis System	MEF IAS	INTEL	USMC	UN
Multiple Source Correlation System	MSCS	INTEL	USMC	UN
Secondary Imagery Dissemination System	SIDS	INTEL	USMC	UN
Ships Signal Exploitation Equipment	SSEE	INTEL	USN	UN
Technical Control and Analysis Center	TCAC	INTEL	USMC	UN
Technical Control and Analysis Center-Product Improvement Program	TCAC-PIP	INTEL	USMC	UN
Tactical Electronic Reconnaissance Processing and Evaluation System	TERPES	INTEL	USMC	UN
Tactical Exploitation System - Navy	TES-N	INTEL	USN	UN
Tactical GeoSpatial Information Library (Server)	TGIL	INTEL	USMC	UN
Team Portable Collection System	TPCS	INTEL	USMC	UN
Tactical Reconnaissance Intelligence Exchange Service	TRIXS	INTEL	AR	UN
Tactical Remote Sensor System	TRSS	INTEL	USMC	UN
Marine Integrated Personnel System	MIPS	M&RA	USMC	UN
HF Antenna Profiles	HFANT	MCCDC	DoC	UN

Application Name	Acronym	FAM	Owner	IPv6 Impact
Joint Enhanced Core Communications System	JECCS	MCCDC	USMC	UN
Systems Planning Engineering and Evaluation Device	SPEED	MCCDC	USMC	UN
Advanced Combat Direction System	ACDS	PP&O	USN	UN
Automated Digital Network System	ADNS	PP&O	USN	UN
Automated Deep Operations Coordination System	ADOCS	PP&O		UN
Advanced Field Artillery Tactical Data System	AFATDS	PP&O	AR	UN
Amphibious Assault Direction System	AN/KSQ-1	PP&O	USN	UN
Afloat Planning System	APS	PP&O	USN	UN
Advanced Refractive Effects Prediction System	AREPS	PP&O	USN	UN
Expeditionary Air Defense System	EADS	PP&O	USMC	UN
Enhanced Position Location Reporting System	EPLRS	PP&O	AR	UN
Explosives Safety Technical Data Collection	ESTDC	PP&O	USMC	UN
Global Command and Control System - Maritime	GCCS-M	PP&O	USN	UN
Geophysical Fleet Mission Program Library	GFMPL	PP&O	USN	UN
Global Status of Resources and Training System	GSORTS	PP&O	Joint	UN
Hazard Prediction And Assessment Capability	HPAC	PP&O	USN	UN
Integrated Marine Multi Agent Command and Control System	IMMACCS	PP&O	USMC	UN
Joint Maritime Command Information System	JMCIS	PP&O	USN	UN
Joint Munitions Effectiveness Manuals	JMEMS	PP&O	USN	UN
Joint METOC Viewer	JMV	PP&O	USN	UN
Joint Targeting Toolbox	JTT	PP&O	Joint (AF)	UN
Joint Universal Lessons Learned System	JULLS	PP&O	Joint	UN
Joint Warning and Reporting Network	JWARN	PP&O	USMC	UN
Marine Corps Fire Support System	MCFSS	PP&O	USMC	UN
Message Formatter and Transmitter	MFT	PP&O	USN	UN
USNAmmunition Master Technical File	NAMT	PP&O	USMC	UN
Nearest Station Utility	NEAREST	PP&O	AF	UN
Naval Tactical Command Support System II Desktop	NTCSSII	PP&O	USN	UN
Metrology Requirements On-Line Query	PCMETROQ	PP&O	USN/USMC	UN

Application Name	Acronym	FAM	Owner	IPv6 Impact
Palm Client Software (For Use with IFR System)	PCS	PP&O		UN
Satellite, NexRad, DiFax, Fusion Display program	SANDS	PP&O	USN	UN
Scheduled Advanced Risk Analysis	SARA	PP&O	USN	UN
Solar/Lunar Almanac Program	SLAP	PP&O	USN	UN
Stick Length Interactive Indicator	SLIC	PP&O	USN	UN
Shipboard Uniform Automated Data Processing System	SUADPS	PP&O	USN	UN
Tactical Automated Mission Planning System	TAMPS	PP&O	USN	UN
Program for Medical Supply and Re-Supply	TCAM	PP&O	Army	UN
Tactical Combat Operations	TCO	PP&O	USMC	UN
Tactical Defense Message System	TDMS	PP&O	DISA	UN
Tracking System for Medevac	TRACES	PP&O	AF	UN
VOICE OF AMERICA Area Coverage Predictions	VOAAREA	PP&O	DoC	UN
VOICE OF AMERICA Analysis and Circuit Prediction	VOACAP	PP&O	DoC	UN
Electronic CAD/PAD Technical Manual For Cartridge And Propellant Actuated Devices – NAVAIR 11-100-1.1 CD		PP&O	USMC	UN
METCAST		PP&O	USN	UN
Weather Trac		PP&O	USN	UN
Global Tracks		PP&O	USN	UN
Weather View		PP&O	USN	UN
Quest Suite		PP&O	USN	UN
* On Baseline				

Application Listing E-3. GOTS

Application Name	Acronym	Version	IPv6 Impact
			Legacy = Will not transition **MM/YY** = Capability Date **UN** = Undetermined **None** = Unaffected
2002 USMTF User Format	USMTF	2002	UN
2003 USMTF User Formats - United States Message Text Formatting	USMTF	2003	UN
Ada Fund Administrator Tracking System	ADAFATS	1	UN
Admin/Tech 1		2.4	UN
Admin/Tech 2		2.4	UN
Advanced Field Artillery Tactical Data System	AFATDS	6.3.2	UN
Advanced Refractive Effects Prediction System	AREPS	3.21	UN
Aeronautical Information System	AIS	1	UN
Aircraft Engine Management System	AEMS	1	UN
Aircraft Familiarization 747		1	UN
Aircraft Familiarization B-1B		1	UN
Aircraft Familiarization C-130		1	UN
Aircraft Familiarization C-17		1	UN
Aircraft Familiarization C-5 Galaxy		1	UN
Aircraft Familiarization F117a		1	UN
Aircraft Familiarization F-15		1	UN
Aircraft Familiarization F-16		1	UN
Aircraft Familiarization F-18		1	UN
Aircraft Familiarization KC-10 / DC-10 / MD-11		1	UN
Aircraft Familiarization KC-135		1	UN
Aircraft Familiarization T-38		1	UN
Aircraft Inventory Readiness And Reporting System	AIRRS	2.01	UN
Aircraft Material Readiness Report	AMRR	2.07L	UN
Airfield Obstruction Tracking, Analysis, And Management System	AIROBS	1.1	UN
Albany Publishing System		1	UN
American Corrections Association Database	ACA Database	Unk	UN
Answer Sheet Manager		5	UN
Apparatus Driver/Operator – ARFF Training	Driver/Operator ARFF	1.0 August 2003	UN
ArcGIS 8 - Cherry Point Tool Set		3.0.1	UN
Army Training Requirements And Resources System	ATRRS	Rel 2.1	UN

Application Name	Acronym	Version	IPv6 Impact
Asset Tracking Logistics And Supply System	ATLASS	4	UN
Asset Tracking Logistics And Supply System II+	ATLASS II+	807-02.00.05	UN
Asset Tracking Logistics And Supply System II+	ATLASS II+	807-02.00.20	UN
Authorization Strength & Manning Levels	AUTH STR&MAN	1	UN
AutoDIN Breakout	AUTODIN	1	UN
Automated Air Load Planning System	AALPS	4.3	UN
Automated Air Load Planning System	AALPS	4.3.2	UN
Automated Carousel System	ACS	1	UN
Automated Claims Information System 2000	ACIS 2000	1	UN
Automated Compliance Evaluation	ACE	4.3	UN
Automated Cost Estimating Integrated Tool	ACEIT	6.0a	UN
Automated Data Inquiry For Oil Spills	ADIOS	2	UN
Automated Fitness Report System	AFRS	1	UN
Automated Government Transportation Request 2002	AGTR	2002	UN
Automated Heat Stress System	AHSS	1	UN
Automated Inspection Reporting System - Checklist	AIRS	1.1	UN
Automated Inspection Reporting System - Igmc	AIRS	1.3	UN
Automated Inspection Reporting System - Inspection	AIRS	1	UN
Automated Leads Management Reporting System	ALMRS	1	UN
Automated Manifest System Tactical	AMS-TAC	3	UN
Automated Navy Comsec Reporting System	ANCRS	4.1.1	UN
Automated Postal Locator System	APLS	1	UN
Automated Procurement Subsystem	MUMMS SS05	1	UN
Automated Quality Assurance Support	AQAS	2.5	UN
Automated Recruit Management System	ARMS	1	UN
Automated Security Control Program	ASCP	4.0C	UN
Automated Security Control Program - Command Level	ASCP	4.0C	UN
Automated Standard Administrative Programs	ASAP	2002.2	UN
Automated Technical Order Management System	ATOMS	1.4	UN
Automated Toxic Release Inventory Reporting System 2001	ATRS 2001	6.02.00	UN
Automated Training And Readiness Information Management System - Headquarters Key	ATRIMS-HQKEY	2.0.00	UN
Automated Training And Readiness Information Management System (98m)(MACCS)	ATRIMS-MACCS	3	UN
Automated Travel Order System Plus	ATOS+	040-05.04.05	UN
AV8B Hover Performance Program		1.28	UN

Application Name	Acronym	Version	IPv6 Impact
Aviation Logistics Department End Of Month	ALDEOM	2002.0.0	UN
Aviation Maintenance Training Continuum System (AMTCS) Software Module (ASM)	AMTCS-ASM	2	UN
Aviation Maintenance Training Continuum System (AMTCS) Support Software Suite For Interactive Courseware (ICW)	AMTCS-ICW	1	UN
Aviation Material Maintenance Management	AV3M	004-14.00.00	UN
Aviation Storekeeper Information Tracking System	ASKIT	7	UN
Basics Of Naval Explosives Hazard Control And Naval Explosives Safety Supervisors/Managers Orientation	AMMO-18/AMMO-49	2.3	UN
Blackberry Server Software		3.1	UN
BNA - By Name Assignment	BNA	1	UN
Bond & Allotments		1	UN
Breakout Program	BREAKOUT	27-May-03	UN
Broadened Arrangement Of Resources From A Basic Accessory Relocation Application - Supply Issue And Recovery System 2000	BARBARA SIRS	1.3.136	UN
Bureau Of Naval Personnel	BUPERS	1	UN
CA$HLINK II	CA$HLINK II	3.1.139E	UN
Cadet Records Manager		2.1	UN
Cargo Movement Operations System	CMOS	6	UN
Cargo Movement Operations System	CMOS	6.1.3	UN
Cartridge / Propellant Actuated Device	CAD PAD	1-Jan-03	UN
Casa / Rasa Database Utilities		2	UN
Case Overview Reconciliation And Performance System	CORPS	1.3.4	UN
Casualty Estimation Model		4.0.1	UN
Cataloging Reengineering System	CRS	1	UN
CATT MSL/LRRD Module		1.1	UN
Certest		4	UN
Certest Computer-Based Final Exams	CERTEST	1.03	UN
Certest Computer-Based Testing Program	CERTEST	5	UN
Chemical Reactivity Worksheet		1.5	UN
Child And Spouse Abuse System		4.1	UN
Civilian Servicing Unit Application	CSU	11	UN
Civilian Servicing Unit Application - Citrix Web Client	CSU Citrix Web Client	7.1	UN
Close Combat Marine		RC5	UN
CMC Preparation Briefs	CMCPB	1.1.0.0	UN
CMC Unfunded Priority List	UPL	1.3.0.2	UN

Application Name	Acronym	Version	IPv6 Impact
COE Message Processor	CMP	4.2.0.0	UN
Combat Development Tracking System		2	UN
Combat XXI		3	UN
Command & Control Personal Computer	C2PC	5.8.2	UN
Command & Control Personal Computer	C2PC	5.9.0.3	UN
Command Automated Program/Information System	CAPS	3	UN
Command Core System	CCS	4.4	UN
Commanding Officers Readiness Reporting System	CORRS	4.09	UN
Commercial Activities Management Information System	CAMIS	1	UN
Commercial Asset Visibility 2 (Production)	CAV II	4	UN
Commercial Asset Visibility 2 (Training)	CAV II (TRAINING)	4	UN
Common Logistics Command And Control System	CLC2S	2	UN
Compare		2	UN
Composite Healthcare System II	CHCSII	5.1	UN
Computer Aided Embarkation Management System	CAEMS	6.4	UN
Computer Aided Load Manifesting	CALM	5.7	UN
Computer Aided Management Emergency Operations Suite	CAMEO	fm	UN
Computer Assisted Logistics And Test Equipment Calibration System	CALTECS	5	UN
Computer Benchbook		2002	UN
Computer Optimized Batch Reconciliation Application On The Web	COBRA (SABRS)	1	UN
Computerized Accounts Payable System For Windows	CAPS-W	5.6	UN
Computerized Self Evaluation Checklist	CSEC	3.2	UN
Configuration Management Information System	CMIS	5.2.2	UN
Configuration Management Information System Web	CMIS WEB	1	UN
Confined Space Emergency Response Series		2	UN
Consequences Assessment Tool Set	CATS-JACE	1.0.81	UN
Construction Criteria Base	CCB	62	UN
Construction Criteria Base	CCB	60A	UN
Contingency Operations Support Tool	COST	5	UN
Contractor Performance Assessment Reporting System	CPARS	1	UN
Contracts Directorate Document Control System		1	UN
Contribution-Based Compensation And Appraisal System For The Internet	CAS2NET	1.2	UN
CorpsCon	CORPSCON	5.11.08	UN
Corpsmet95	CORPSMET95	1.3	UN

Application Name	Acronym	Version	IPv6 Impact
Corrections Management Information System		7	UN
CSRS And FERS Benefits Calculator		unk	UN
Customer Complaint Report Of Discrepancy	CCRODS	2.5	UN
Daily Process Report Management Program	DPR	8-Sep-03	UN
DANTES Automated Test Inventory Program	DATIP	8/19/1998	UN
Data Analysis Reconciliation Tool	DART	2.3.47	UN
Data Elements		1	UN
Data Entry	DE	1	UN
DAWIA Reporting Program		1.0.0.7	UN
Dd1391 Processing Program		2002	UN
Defense Acquisition Deskbook	DAD	3.8	UN
Defense Acquisition University	DAU	2	UN
Defense Automatic Addressing System Center Automated Message Exchange System	DAMES	2.20 build 054	UN
Defense Casualty Information Processing System	DCIPS	7.0.4	UN
Defense Casualty Information Processing System Forward	DCIPS FORWARD	3.2	UN
Defense Civilian Payroll System	DCPS	6	UN
Defense Civilian Personnel Data System	DCPDS	11i	UN
Defense Clearance & Investigation Index	DCII	website	UN
Defense Enrollment Eligibility Reporting System	DEERS	5.2.0.32	UN
Defense Industrial Financial Management System	DIFMS	02B	UN
Defense Medical Logistics Support Services	DMLSS	3.05	UN
Defense Message System	DMS	3	UN
Defense Property Accountability System With EUREKA: Report Designer	DPAS - REPORT DESIGNER	16.4.04	UN
Defense Property Accountability System With EUREKA: Report Viewer	DPAS - REPORT VIEWER	16.4.04	UN
Defense Security Assistance Management System	DSAMS	6.08	UN
Defense Table Of Official Distances	DTOD	1	UN
Defense Transportation Tracking System	DTTS	1	UN
Defense Travel System (Enhanced Jefferson)	DTS	1.5	UN
DEMP TAV 2001	DEMP TAV 2001	2.0.3	UN
Dental Common Access System	DENCAS	2	UN
Dental Common Access System (Remote)	DENCAS(R)	1.1	UN
Department Of The Army Electronic Tech Manual		1	UN
DepCon		6.1	UN
Depot Maintenance	DMMS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Deserter Process		1	UN
Detailed OPTAR Listing And Reporting System	DOLARS	5.4.4	UN
Direct Support Stock Control Subsystem	DSSC	1	UN
Distribution Standard System	DSS	8	UN
DLA Catalog Of Map Products (E-Catalog)	DLA E-CATALOG	1.3.1	UN
Document Tracking And Management System	DTMS	1	UN
Document Tracking System	DocTrack	1.04	UN
DoD Core Document System	COREDOC	3.1D	UN
DoD Drug Testing Program	DTS-CCS	5.1	UN
DoD Fuelmaster		1.0.0.6 SP1	UN
DoD Metrology Information And Document Automation System	DODMIDAS	2	UN
DoD PKI Tracking Tool		3	UN
Driver/Operator Pumper		1	UN
Due And Status File Management Program	DASFMP	28-Feb-03	UN
Duty Limit Database	DLD	1	UN
E-Catalog	E-CAT	1.3.1	UN
Econpack (Economic Analysis)		2.1.2	UN
EFDC Intranet	EFDC INTRANET	1	UN
Effects Management Tool	EMT	6.3.2.0	UN
Electronic Account Government Ledger System	EAGLS	7	UN
Electronic Attorney Desktop		Nov-00	UN
Electronic Document Access	EDA	6.1.1	UN
Electronic Maintenance System (EMS-2) Viewer	EMS-2 VIEWER	2.7.2.3	UN
Electronic Personnel Security Questionnaire - Security Officer Edition	EPSQ SECURITY OFFICER	2.2	UN
Electronic Personnel Security Questionnaire-Subject Edition	EPSQ - SUBJECT EDITION	2.2	UN
Electronic Point Of Sales	EPOS	2	UN
Electronic Project Procurement Generator	EPPG	1	UN
Emergency Management Information System-Detached	EMIS - Detached	3.2	UN
Emergency Response Map Book For ARCVIEW 3.2a		1	UN
Emergency Response To Terrorism		36130	UN
Enhanced Calibration Capability		1	UN
Enhanced Position Location Reporting System Radio Set CBT		UNK	UN
Enlisted Assignment Model	EAM	3.2.3.0	UN
Enlisted Assignment Model Monitor	EAMMON	1.0.0.2	UN

Application Name	Acronym	Version	IPv6 Impact
Enlisted Staffing Goal Model	ESGM	3.2.1.0	UN
Environmental Knowledge And Assessment Tool	EKAT	1	UN
Environmental Reporting Assist File	ERAF	Jul-98	UN
Epidemiological Information 2000	EPIINFO2000	2	UN
Essex Replacement Program	ERP	1	UN
Estimating Supplies Program	ESP	2	UN
Exceptional Family Member Program	EFMP	1	UN
Experimental Advanced Instructional Design Advisor	XAIDA	5.2B	UN
Explosive Ordnance Disposal Tactical Decision Aids	EOD TDA	1.6	UN
Explosives Safety Siting Module	ESS	5	UN
Explosives Safety Technical Manuals CD-Rom	ESTM	1.1	UN
Extensible Business Intelligence Toolkit (Client)	xBIT	1.0.4.0	UN
Extensible Business Intelligence Toolkit (Server)	xBIT	1.0.0.0	UN
Facilities Assessment Inspection Module	FAIM	1.2	UN
Facilities Degradation Module	FDM	5.02	UN
Facilities Engineering Department (Fed) Database		1	UN
Facilities Integration Website	FI (Web)	7	UN
Facilities Project Database	FPD	1	UN
Facilities Sustainment Model	FSM	2.04	UN
Federal Logistics	FEDLOG	5.5	UN
FieldAce	FIELDACE	2.1	UN
File Transfer Program	FTP	1.2.1	UN
Financial Air Clearance & Transportation System	FACTS	2	UN
Financial Information Management System II	FIMS II	1	UN
Firehouse Software		5.4.99	UN
First Aid First Responder Training		Aug-02	UN
Fish And Wildlife Conservation Tracking System	FAWCTS	5.1	UN
Fleet Imaging Management System	FIMS	1	UN
Forces Command JTAO CBT Modules 1-14		Jun-00	UN
FORSCOM JTAO		Sep-00	UN
Frequency Assignment Retrieval System	FARS	1.3.2	UN
Fuels Automated System (Fuels Control Center)	FAS FCC	1027	UN
Fuels Manager		4.2.0.451	UN
General Campaign Analysis Model	GCAM	3.2	UN
General NOAA Oil Modeling Environment	GNOME	1.2.4	UN
Geophysics Fleet Mission Program Library	GFMPL	2.8u	UN

Application Name	Acronym	Version	IPv6 Impact
GeoTrans	GEOTRANS	2.2.2	UN
Global Air Transportation Execution System	GATES	2.07	UN
Global Air Transportation Execution System Web	GATES WEB	5	UN
Global Decision Support System	GDSS	4.4a	UN
Global Freight Management System	GFM	1	UN
Global Transportation Network	GTN	3.12.5b	UN
Graphical User Interface Logistics On-Line Application		LOLA 97 dtd March 2003	UN
Greenheck Computer Aided Product Selection	CAPS	1.11	UN
Groups Operational Passenger System	GOPAX	1	UN
H Series ACODP Handbook		1	UN
Hawk Weapon System History Database		1.1	UN
Hazard Prediction And Assessment Capability	HPAC	4.0.1	UN
Hazardous Material Information Control System	HICS	4	UN
Hazardous Material Information System	HMIS	1.5	UN
Hazardous Material Management System	HMMS	3.2203	UN
Hazardous Material Management System	HMMS	4	UN
Hazardous Materials Awareness		Nov-99	UN
Hazardous Materials Incident Commander		May-02	UN
Hazardous Materials Operations		Nov-99	UN
Hazardous Materials Technician	HAZMAT TECHNICIAN	Aug-99	UN
Hazardous Substance Management System	HSMS	2.4.1	UN
Hazmat Support Material 1998 Edition		3	UN
HazTrack		1	UN
Headquarters Award Board 2000	HQAB 2000	1	UN
Headquarters Marine Corps Awards Board		1	UN
Headquarters Master File	HMF	1	UN
High Priority Special Interest Aircraft	HIPRI-SPINTAC	1.2.7	UN
Host Nation Spectrum Worldwide Database	HNSWD	3	UN
Hotspots Analysis And Reporting Program	HARP	11.1	UN
HQMC Environmental Applications Portal	HEAP	1	UN
IETM Digital Technical Control Facility		5-Sep-01	UN
IETM For Employing Joint Tactical Communications	CJCSM 6231	Rel 7, Nov 2002	UN
IETM Tactical Data Network Gateway		5-Jun-01	UN
IETM Tactical Data Network Server		5-Jun-01	UN
IMA Naval Aviation Logistics Command Information System	IMA NALCOMIS	120-03/04.120	UN

Application Name	Acronym	Version	IPv6 Impact
Incremental Initial Active Duty Database	IIADT	1	UN
Infantry Capabilities Assessment Model	ICAM	3	UN
Inquiry Response System	IRS	1.2.5.0	UN
Integrated Booking System	IBS	6.0n	UN
Integrated Computerized Deployment System	ICODES	5.3.1	UN
Integrated Geographic Information Repository Common Tool Set For ArcGIS 8	IGIR COMMON TOOL SET	1	UN
Integrated GPS Radio System II	IGRS II	1.07	UN
Integrated Multi-Year Prioritization And Analysis Tool (Formerly BUILDER)	IMPACT	2.2	UN
Intelligent Road/Rail Information Server	IRRIS	1	UN
Interactive Authoring And Display System	IADS	3.2.5	UN
Interactive Electronic Technical Manuals	IETM	UNK	UN
Intermodal Cargo Container/Convention For Safe Container (CSC) Reinspection Cbt, Ammo-43	AMMO-43	1	UN
International Deminer's Guide To UXO Identification, Recovery & Disposal		1	UN
Internet Navy Facility Assets Data Store	INFADS	1	UN
Inventory Control Forecasting Subsystem Of ICP	ICF SS03	1	UN
Inventory Control Point	ICP	1	UN
Inventory Control Project Requirements File Follow-up Subsystem Of ICP	PRF-FOLLOW UP	1	UN
Inventory Control Replenishment Review Subsystem Of ICP	REP REVIEW	1	UN
Investment Advisor Toolkit	IAT	1	UN
Item Applications	ITEM APPS SS09	1	UN
JBox OMF Loader		4.02	UN
Joint Air Logistics Information System	JALIS	2	UN
Joint Automated CEOI System	JACS	1.3	UN
Joint Aviation Technical Data Integration	JATDI.REDSTONE.ARMY.MIL	Web	UN
Joint Card Maintenance		3.05	UN
Joint Computer-Aided Acquisition And Logistics Support	JCALS	3.1.1	UN
Joint Duty Assignment Management Information System	JDAMIS	1.5.8	UN
Joint Engineering Data Management Information & Control System	JEDMICS	3.2	UN
Joint Engineering Data Management Information & Control System	JEDMICS	3.4	UN
Joint Engineering Data Management Information & Control System	PC JEDMICS	2.5.1	UN

Application Name	Acronym	Version	IPv6 Impact
Joint Engineering Data Management Information & Control System – Imager	JEDMICS-IMAGER	5.1.1.2	UN
Joint Engineering Data Management Information & Control System – INDEXR	JEDMICS-INDEXR	2.2.365	UN
Joint Federal Travel Regulation – CD	JFTR	1	UN
Joint Force Requirements Generator II	JFRG II	1.4.0.1	UN
Joint Force Requirements Generator II	JFRG II	1.4.1.2	UN
Joint Logistics Warfighting Initiative	JLWI	2	UN
Joint METOC Viewer	JMV	3.7.0.0	UN
Joint Mission Planning System	JMPS	1	UN
Joint Personnel Adjudication System	JPAS	1	UN
Joint Total Asset Visibility	JTAV	2.4	UN
Jumpers		2	UN
Knowledge For Acquisition In The 21st Century	K21	2	UN
Lakes Helper		1	UN
Libronix Digital Library System		1.1A	UN
Local Asset Management System	LAMS	4	UN
Local Finance		1	UN
Local Intranet		2	UN
Local Logistics	LOGS	1	UN
Local Manpower		1	UN
Locator	LOCATOR	1	UN
Logbook		1.12b2	UN
Logical Lock Killer		1	UN
Logistics Bases Inventory Visibility Phase II	LBIV-II	1	UN
Logistics Information Network	LINK	1	UN
Logistics Integrated Database	LIDB	6	UN
Logistics Management Information System	LMIS	1	UN
Logistics Management Information System 7 Way Reference	7WAYXREF	1	UN
Lotus Notes/Domino		6	UN
Macromedia Director MX 2004		MX 2004	UN
Magic		5.02	UN
Mailgram Model		4.2.6	UN
Maintenance Automated Program	MAP	3	UN
Maintenance Center Asset Tracking System	MCATS	1.05	UN
Maintenance Center Document Retrieval System	MCDRS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Manning Level Process	MLP	3.1.0.0	UN
Manpower Assignment Support System 2001	MASS 2001	2	UN
Manpower Management System	MMS	1	UN
Manual On Uniform Traffic Control Devices 2000		2000 0601	UN
Marine Air Ground Task Force	MAGTF	1	UN
Marine Air Ground Task Force-Logistics Automated Information System Suite	MAGTF-LOGAIS Suite	7	UN
Marine Ammunition Accounting And Reporting System	MAARS II	II	UN
Marine Clothing Sales Store Subsystem of DSSC	MUMMS SS07	1	UN
Marine Corps Action Tracking System	MCATS	1	UN
Marine Corps Automated Instructional Management System 32 (Client)	MCAIMS 32	4.0 (G)	UN
Marine Corps Automated Instructional Management System 32 (Standalone)	MCAIMS 32	4.0 (G)	UN
Marine Corps Automated Instructional Management System Plus (Client)	MCAIMS PLUS	3.0 Rev A	UN
Marine Corps Automated Instructional Management System Plus (Standalone)	MCAIMS PLUS	3.0 Rev A	UN
Marine Corps Automated Settlement Sheet Process	MCASSP	2003.2.00	UN
Marine Corps Climate Assessment System For Windows	MCCASWin	1.1	UN
Marine Corps Department Of Defense Automatic Addressing Directory		1	UN
Marine Corps Distance Learning	MCDL	3	UN
Marine Corps Drug Testing Program		5.1.2	UN
Marine Corps Electronic Forms System	MCEFS	2.23.2	UN
Marine Corps Enterprise Network Data Warehouse	MCEN DW	1.2	UN
Marine Corps Equipment Readiness Information Tool	MERIT	1.1.0.0	UN
Marine Corps Exchange	MCX	1	UN
Marine Corps Food Management Information System	MCFMIS	6.1.1	UN
Marine Corps Handheld Inspection Program	MCHIP	1	UN
Marine Corps Housing Automated System	MCHAS	2.5a	UN
Marine Corps Housing Automated System For The Internet	iMCHAS	3	UN
Marine Corps Institute Automated Integrated System	MCIAIS	UNKNOWN	UN
Marine Corps Integrated Maintenance Management System	MIMMS	1	UN
Marine Corps Medical Entitlements Data System	MCMEDS	2.01	UN
Marine Corps Mishap Tracking System	MARTRAK	1	UN
Marine Corps Mobilization Planning System	MCMPS	4.3.3	UN
Marine Corps PFT Calculator		2	UN

Application Name	Acronym	Version	IPv6 Impact
Marine Corps Publications Distribution System	MCPDS	1	UN
Marine Corps Publications Electronic Library	MCPEL	1	UN
Marine Corps Readiness Equipment Module	MCREM	26-Sep-03	UN
Marine Corps Recruiting Command Automated Enlistment Package	AEP	2	UN
Marine Corps Recruiting Information Support System For Recruiting Stations	MCRISS-RS	1.1.20	UN
Marine Corps Reserve Online Exit Survey II	MCROLES II	1	UN
Marine Corps Reserve Recruit Auto Waiver System	MCRRAWS	1	UN
Marine Corps Total Force System	MCTFS	1	UN
Marine Corps Training, Exercise And Employment Planning - Management Tool	MCTEEP-MT	3	UN
Marine Corps Unified Material Management System	MUMMS	1	UN
Marine Equity Model	MEM	3.0.1.0	UN
Marine For Life	M4L	web	UN
Marine Forces Enlisted Administrative Separation System	MCEAS	1	UN
Marine Forces Reserve Order Writing System	ROWS	ITD061-00 2001.2.15	UN
Marine Interactive Computer Aided Provisioning System	MICAPS	4	UN
Marine Officer Specialty Training Allocation System	MOSTAS	3.1.1.0	UN
Marine On Line	MOL	2	UN
Mass Administration Tool		1	UN
Master Header Information File Subsystem Tdms	MHIF	1	UN
Material Acquisition And Tracking System	MATS	1	UN
Material Capability Decision Support System	MCDSS	4.1	UN
Material Capability Decision Support System	MCDSS	4.2	UN
Material Forecast Management Plan	MFMP	1	UN
Materiel Readiness Management System 2000	MRMS 2000	3.113 SP1	UN
Materiel Returns Program	MRP	1	UN
Max Responder		unk	UN
Measure Automated Information System - Personal Computer	MEASURE AISPC	4.3	UN
Measure Name And Address Query	MEASURE NAME AND ADDRESS QUERY	S	UN
Measure PC Inventory Query	PCINVQRY	W9808.31	UN
Mechanization Of Warehousing And Shipment Processing	MOWASP	1	UN
Mechanized Allowance List / Consolidated Memo Receipt Management Program	MAL/CMR	6-Mar-03	UN
MEPCOM Trans		1.00b4	UN

Application Name	Acronym	Version	IPv6 Impact
Message Analysis And Data Reduction For The Integration Of Links	MANDRIL	MC2.2 29May 2002	UN
Metcast Client	METCAST	1.7.0.0	UN
Metrology Products	METPRO	2.1	UN
MHE Dispatch System		1.1	UN
MICRODEM (Aka TERRA BASE II)		6.02	UN
Military Engineering Data Asset Locator System	MEDALS	1	UN
MISSA/MISSO Portal		1	UN
Mobile Electronic Warfare Support System CBT	MEWSS	1	UN
Modern Defense Civilian Personnel Data System	MDCPDS	Patch 36.1	UN
Module Test & Repair Suite	MTR SUITE	3.20.0	UN
Monitor Assignment Support System 2001	MASS 2001	2.03.10	UN
Monitor Assignment Support System Administration Tool	MASS Admin Tool	1	UN
MRP Reports Application	MRP	2	UN
Mr-Win6530	MR-Win6530	5.4.8	UN
MTMCCOM	MTMCCOM	4.4	UN
Multi-User Engineering Change Proposal Automated Review System	MEARS	9.1	UN
Munitions Survivability Software	MSS	UNKNOWN	UN
National Fire Incident Reporting System	NFIRS	5.2.1	UN
NAVAIR Industrial Material Management System	NIMMS	1	UN
NAVAIR Technical Publications Library Program	TPL	3.01	UN
Naval Ammunition Logistics Center P-800	NAVSUP P-800	Oct-02	UN
Naval Aviation Logistics Command Management Information System	NALCOMIS	122-03.05.18	UN
Naval Flight Weather Briefer	NFWB	4.2	UN
Naval Motor Vehicle And Railcar Inspection	AMMO-51	1.1	UN
Naval Supply Catalogue Manuals Program	NSCMP	1	UN
NavFit98a (Incl NavFit98 2.002.0021)	NAVFIT98A	2.002.0023	UN
Navy Air Force Interface	NAFI	4	UN
Navy College Management Information System	NCMIS	3	UN
Navy Dive Reporting System	DRS	5.1.5	UN
Navy Electronic Commerce On-Line	NECO	4	UN
Navy Integrated Training Resources Administration System	NITRAS WEB	2	UN
Navy Planned Maintenance System	NAVY PMS	2	UN
Navy Portable Flight Planning System	N-PFPS	3.2	UN
Navy Shore Installations Website	NSI	1	UN

Application Name	Acronym	Version	IPv6 Impact
Navy Training Management & Planning System	NTMPS	1	UN
NBC Defense Equipment Management Program	NBC DEMP	1	UN
NBC Terrorism Event		1	UN
NBC-Analysis		5	UN
NBC-Analysis For JSLNBCRS		3.4.2/E	UN
NBCD Equipment Assessment And Repair System	NBCD EARS	6.2	UN
Net Pay Process	NET PAY	1	UN
Netwars	NETWARS	2003-1	UN
NIOSH Pocket Guide To Chemical Hazards		2002-140	UN
Notice Of Eligibility For Disability	NOE	1	UN
Noxious & Nuisance Plant Management Information System		5	UN
NTCSS Integrated Barcode System	NTCSS IBS	894-02.00.30	UN
Officer Mobilization Model	OMM	Client 3.0.1.0.| Server 1.03	UN
Officer Rate Generator	ORG	3.0.2.0	UN
Officer Staffing Goal Model	OSGM	3.3.1.2	UN
On-Line Diary System	OLDS	1	UN
Operation Determined Vigilance	ODV	1	UN
Operational Data Store Enterprise	ODSE	1.11	UN
Operational Test And Evaluation Suite	OT&E	1.5	UN
Operations Research Cost Analysis	ORCA	1	UN
OPNAV Aviation Training Management System	OATMS	8	UN
Optical Digital Imaging Records Management System	ODI-RMS	6	UN
Optimized IMA Naval Aviation Logistics Command Information System	OIMA NALCOMIS	815-01/05/10	UN
Optimized OMA Naval Aviation Logistics Command Information System	OOMA NALCOMIS	825-03/04.00	UN
Optimum Path Aircraft Routing System	OPARS	3.1	UN
Oracle Training Administration	OTA	Bld8v1.2.3	UN
P&R Customer Support Database		1.0.0.0	UN
P&R Portal		2.0.6.0	UN
PC Enlisted Distribution Verification Report Program	PCEDVR	1	UN
PC Joint Engineering Data Management Information & Control System	PC JEDMICS	3.1	UN
PC Maintenance Information System Coordination Office	PCMISCO	1	UN
PC Marine Corps Integrated Maintenance Management System	PCMIMMS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Performance Evaluation System - Back Office	PES BACK OFFICE	9	UN
Performance Evaluation System (PES) Windows Front End (WinFE)	PES WinFE	3	UN
Permanent Change Of Station History	PCS HIST	1	UN
Permissions Management		1.01b1	UN
Persona		5	UN
Physical Readiness Information Management System	PRIMS	1.0.11	UN
Pilot Transportation Operational Personal Property System	PTOPS	1	UN
Plant Account		1	UN
PMS Viewer	PMS VIEWER	2	UN
Pollution Prevention Annual Data Summary	P2ADS	2000	UN
POM Initiative Builder	PIB	1	UN
Power Logistics 2000	POWERLOG	2.6.3	UN
PR Builder	PRB	3.1	UN
Practical Software And Systems Measurement		4.1	UN
PrepAS	PREPAS	1	UN
Principles Of Federal Appropriations Law		Fall 2002	UN
Probability / Consequence Software	PCS	4.2.5	UN
Procurement Management Reporting System	PMRS	10	UN
Product Data Reporting And Evaluation Program	PDREP	1	UN
Program And Budgeting Documentation Database	PBDD	3.0.2.1	UN
Program Budget Accounting System	PBAS	1	UN
Program Development Database	PDD	5.2.2.0	UN
Program Managers Workstation	PMWS	N-7.0A	UN
ProjectFix	PROJECTFIX	1	UN
Promotion Planning Process	PPP	3.0.1.0	UN
Property Accountability		1.00b1	UN
Protective Structures Automated Design System	PSADS	1	UN
Provisioning	MUMMS SS10	1	UN
Publications Library Management System	PLMS	2.13	UN
Quick Weather		1	UN
Radioactive Item Data	RAID	3.0.1	UN
Range Facility Management Support System	RFMSS-C	3.5B05	UN
Rape And Sexual Assault	RASA	3.1	UN
Recognition Of Combat Vehicles	ROC-V	9.1.4	UN
Recruit Accountability Program/Permanent Personnel	RAS/PAS	4.5.6	UN

Application Name	Acronym	Version	IPv6 Impact
Accountability Program			
Recruit Admin		2.12b1.01	UN
Recruit Administration		2.03	UN
Recruit Distribution Model	RDM	3.1.1.0	UN
Recruit Evaluation		1.13 b1	UN
Recruit Lables		1.00 b8.01	UN
Recruiter Simulation Of John E. Little	RESJEL	2	UN
Recurring Reports	RECRPTS	1	UN
Relational Supply System	R-SUPPLY	822-01.01.57	UN
Remote Access Pay Transaction Reporting System	RAPTRS	2003.2.00	UN
Rental Facilities Management Information System	RFMIS	1	UN
Requisition Status Management System	RSMS	2002.0.0	UN
Reserve Enlisted Planning System	REPS	5.0.18	UN
Reserve Staffing Goal Model	RSGM	3.1.1.0	UN
Retail Ordnance Logistics Management System	ROLMS	9	UN
Retail Ordnance Logistics Management System CS	ROLMS	8.1	UN
Retired Process System	RETPAY	1	UN
Revised Battlefield Electronic Communications	RBEC	2.2.1	UN
Risk, Hazard And Value Evaluation	RHAVE	1.5.2	UN
SABRS Management Analysis Retrieval Tool System - Admin	SMARTS Admin	2003.02.00	UN
SABRS Management Analysis Retrieval Tool System - User	SMARTS User	2003.02.00	UN
SABRS Management Analysis Retrieval Tools System	SMARTS	2	UN
Safe-Range		2.2	UN
Safety Assessment For Explosives Risk	SAFER	2	UN
SAMS Joint Medical Work Station	SAMS_JMEWS	025-08.03.01 U1	UN
Science And Technology Operation Information Center	STOIC	2	UN
Seaway-Loggy		2	UN
Security Engineering Planning Assistant		1.5	UN
Separations And Retirement Support System	SARSS	1	UN
Servmart On-Line		1	UN
Set Assembly System	SAS	1	UN
Shipboard Explosives Safety	AMMO-69	1	UN
Shipping Mats 1.2.0		1	UN
Sierra Hotel Aviation Readiness Program - Service Release 1	SHARP SR-1	4.1 SR-1	UN
Single Site Storage Facility Warehouse Management System	SSSFWMS	3	UN
Situation Report Executive Information System	SREIS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Situation Report Executive Information System – DB Admin	SREIS-DB Admin	1	UN
Sked2-Preventative Maintenance Scheduling Program	SKED2	2.1	UN
Smart Card Technology		1.05	UN
Smart Dental Information	SDI	5.03	UN
SMU DOS		02.06.16	UN
Snap Automated Medical System	SAMS	025-08.02.00	UN
Snap Automated Medical System	SAMS	025-08.03.01	UN
Snap Automated Medical System DD2766 Print Utility	SAMS DD2766	025-08.03.01 U6	UN
Solar/Lunar Almanac Program	SLAP	1.3	UN
Spatial Data Standards For Facilities, Infrastructure And Environment	SDSFIE	2.3	UN
Special Automated Reduction System	SPARS	1.4	UN
Specrite		1.0A	UN
Specsintact	SI	4.0.548	UN
Spectrum Certification System	SCS	6.12	UN
Spectrum XXi		4.1	UN
Squadron Assistance / Risk Assessment	SARA	5	UN
Squadron Assistance / Risk Assessment	SARA	5.0.1	UN
Staff Tasking & Collaboration System	STACS	1	UN
Standard Accounting, Budgeting & Reporting System	SABRS	1	UN
Standard Automated Inventory And Referral System	STAIRS	1	UN
Standard Contract Reconciliation Tool	SCRT	1.3	UN
Standard Labor Data Collection & Distribution Application	SLDCADA	21.5-03	UN
Standard PMS Material Identification Guide	SPMIG	1.00.0002	UN
Standard Procurement System - Procurement Desktop - Defense	SPS PD2	4.2 Incr1 SR03	UN
Standard Tactical Receive Equipment Display	STRED	7	UN
Stanfins Re-Design One	SRD-1	1	UN
Statement Of Service	SOS	3.0.0.1	UN
Statement Of Work, CDRL, And Tracking Tool	SCATT	2002	UN
Statistics Reports	STATS	1	UN
Stock Control System	SCS	1	UN
Stock Control System	SCS	2	UN
Stock List 1-2/1-3	SL 1-2/1-3	1.2	UN
Stock Lists 1&2		1	UN
Storage Retrieval Asset Tracking Information System	STRATIS	701.02.05.00	UN

Application Name	Acronym	Version	IPv6 Impact
Stores Accounting Subsystem	MUMMS SS04	1	UN
Stratification		1	UN
Subsistence Total Order And Receipt Electronic System NT	STORES NT	2.3.88	UN
Support Equipment Management System-Web	SEMS-WEB	5	UN
Supported Activities Supply System	SASSY	1	UN
Survival Equipment Asset Tracking System/Increased Capabilities Program	SEATS/ICAPS	4	UN
Survivors Benefit Plan Valuation Program Suite	SBP Suite	37257	UN
System Planning, Engineering, And Evaluation Device	SPEED	9	UN
Table Of Manpower Requirements	TMR	1	UN
Tactical Network Analysis And Planning System Plus	TNAPS+	5	UN
Target Acquisition Weather Software	TAWS	3.1.3	UN
Target Force Planning Model	TFPM	3.0.1.0	UN
TAV Intransit Processing Station-Read	TIPS-READ	3.3.21	UN
TAV Intransit Processing Station-Write	TIPS-WRITE	3.3.68	UN
T-AVB Automated Load Planning System		2.8	UN
Technical Data Management System	TDMS	1	UN
Technical Publications Library Program	TPL	3	UN
Tecom Integrated Management System	TIMS	1	UN
Temporary Disability Retired List	TDRL	1	UN
Test Measurement And Diagnostic Equipment	TMDE	3	UN
Test Measurement, Diagnostic Information System (For The 21st Century)	TMDIS21	unk	UN
Theater Medical Information Program	TMIP	1.1.1.3	UN
Tier II Submit 2002		2002	UN
Timber Tool For Arcview 3.2a		3.2.2	UN
Toolbox		2.02	UN
Total Force Data Warehouse	TFDW	3	UN
Total Force Retention System	TFRS	5.0.8	UN
Total Force Retention System Extract	TFRS	1	UN
Total Force Structure Management System	TFSMS	1	UN
Total Information Gateway For Enterprise Resources	TIGER	1	UN
Toxic Release Inventory - Made Easy	TRI-ME	2.0.18	UN
Toxics Release Inventory Data Delivery System 2001	TRI-DDS	3.1.1	UN
Tracker	TRACKER	1	UN
Training Requirements And Resource Management System	TRRMS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Training Requirements And Resource Management System - Developer	TRRMS DEVELOPER	1	UN
Transportation Coordinator's Automated Information For Movement	TCAIMS	6.4	UN
Transportation Coordinator's Automated Information For Movement System II	TCAIMS II	3.01	UN
Transportation Management System	TMS	1	UN
Transportation Operational Personal Property Standard System	TOPS	9.5	UN
Transportation Voucher	TMS Freight Sys	1	UN
Tri-Service Medical Evaluation Program	TRI-MEP	1.0C	UN
Troop List System		1.11	UN
TS4317 OMF Loader		3.01	UN
Unexploded Ordnance Site Management Module	UXOSMM	1.2.244	UN
Uniform Automated Data Processing System	UADPS	1	UN
Unit Diary/Marine Corps Integrated Personnel System	UD/MIPS	2003.2	UN
Unit Diary/Marine Corps Integrated Personnel System-Client Only	UD/MIPS	2003.2	UN
Unit Diary/Marine Integrated Personnel System Patch	UD/MIPS	2003.2.01	UN
Universal Data Repository	UDR	1	UN
US Marine Corps Field-Return Ammunition Inspection Guide		4	UN
USMC Document Archive Search Tool		1.02	UN
USMC Recruit Manifest		4.02	UN
USMC War Reserve Application		1	UN
VEF Extract		1	UN
Verification Of Military Experience And Training System	VMET	1	UN
Virtual Battlefield System		1.9	UN
Virtual Collaborative Enterprise	VICE	1	UN
Virtual Online Logistics Transaction System PClink	VOLTS/PCLINK	3.12.047	UN
Virtual Program Management System	VPMS	1	UN
Visual Labmate		789	UN
Visual Logistics Information Processing System	VLIPS	1	UN
VLStrack	VLSTRACK	3.1.0.3	UN
VOAcap For Windows	VOACAP	04.0301W	UN
W2-W2c		2004.1.01	UN
W2-W2C Schoolhouse		2004.1.01	UN
War Reserve System	WRS	1	UN

Application Name	Acronym	Version	IPv6 Impact
Weapons Serial Tracking System		1	UN
Weather Display		9.6	UN
Web Access Defense Equipment Management Program	WX DEMP	2	UN
Wide Area Work Flow	WAW	2.0D.4	UN
Wide Area Work Flow-Receipts And Acceptance	WAW-RA	3.0.1.1	UN
Win Link 32		2.2.0	UN
Wincompare2		1.6	UN
Windows Integrated Automated Travel System	WINIATS	6	UN
Windows Integrated Automated Travel System	WINIATS	6.0.1	UN
Windows Standard Automated Logistics Tool Set	WINSALTS	5.02	UN
Wir On-Line Process Handler	WOLPH	1	UN
Work Year Personnel Cost	WYPC	1	UN
Year Group Steady State	YGSS	3.0.2.0	UN