United States
Department of Veterans Affairs

Transition Plan
for
Internet Protocol Version 6 (IPv6)

Version 3.00
March 25, 2009

IPv6 Project Management Transition Office
Office of Information and Technology

SIGNATURE PAGE

The Department of Veterans Affairs (VA) Internet Protocol Version 6 (IPv6) Transition Plan, Version 3.00 is approved by:

_____ _____

Date

Chief Information Officer
Department of Veterans Affairs

TABLE OF CONTENTS

LIST OF EXHIBITS

1 EXECUTIVE SUMMARY

This IPv6 Transition Plan is intended to document the Department of Veterans Affairs (VA) network infrastructure conversion from an Internet Protocol version 4 (IPv4)-only network to a combined IPv4-IPv6 network. VA met its goal to demonstrate that both network protocols can operate in parallel as specified by the Office of Management and Budget (OMB) mandate M-05-22 dated August 2005 *[R1]* and its subsequent guidance documents. This demonstration was accomplished on March 17, 2008.

In meeting this goal, VA planned an orderly transition of all Internet Protocol (IP) capable network devices on its network infrastructure to be IPv6 capable. It also planned to obtain network management tools that are adequate for managing both network protocols in the network layer of the Open Systems Interconnection (OSI) model, and that communications security safeguard devices would be in place and fully functional.

The following subject areas are included in this plan. Following the character of a "living document", these subjects will be continually monitored and updated.

- Governance and Management
- Requirements
- Implementation Phases and Activities
- Acquisition and Procurement
- Implementation Strategy for VA Infrastructure IPv6 Enablement
- Assurance – Policy – Guidance
- Testing Plan
- Training Plan
- Transition Schedule and Milestones
- Potential IPv6 Applications and Pilot Activities

VA's network infrastructure currently consists of a core layer of network message routing devices, a distribution layer, and an access layer. A conceptual view of VA's Network Core is shown below. While the core layer is centrally controlled by the

Enterprise Infrastructure Engineering (EIE), the distribution layer is managed by various VA organizational elements. Cooperation is critical within the various VA operations to achieve full IPv6 transition. This cooperation is particularly critical amongst VA's Central Office (VACO) and other organizations including VA Veterans Integrated Service Networks (VISNs), VA Operational Regions, VA Regional Data Processing Center (RDPC), and/or all operations housing distribution layer infrastructure devices.

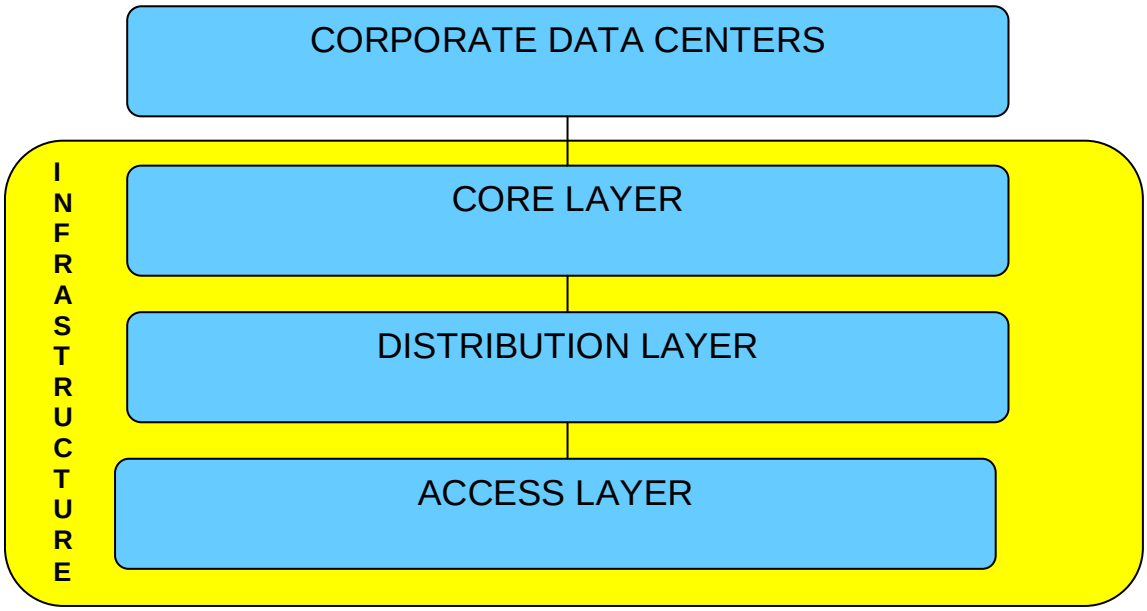


Exhibit 1. VA Infrastructure Conceptual View

The blue boxes in Exhibit 1 above represent conceptual layers of routing hardware and the lines of interconnections between them. All Data Centers connect to the core.

2 INTRODUCTION

2.1 PURPOSE

This document identifies the strategy VA adopted as a phased VA Wide Area Network (WAN) transition from its current IPv4-only based network to a future IPv6-only based network. It is a living document reflecting VA's ongoing goals, plans, progress, and required organizational and structural changes. The migration planning effort is underway but it will take several years to achieve final implementation.

2.2 BACKGROUND

2.2.1 OMB MANDATE & CIO COUNCIL GUIDANCE

In August 2005, OMB issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" mandating that all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure by June 2008 *[R1].*

The memo stated that each agency must take initial actions as follows:

November 15, 2005

- Assign an official to lead and coordinate agency planning.
- Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details).
- Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory.
- Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6.

February 2006

- Using the guidance issued by Chief Information Officers Council (CIO Council) Architecture and Infrastructure Committee, address each of the elements in Attachment C in your agency's IPv6 transition plan and provide the completed IPv6 transition plan as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming.
- Provide a progress report on the inventory and impact analysis, as part of the agency's Office of Enterprise Architecture Management (OEAM) submission to OMB.

June 30, 2006

- Complete inventory of existing IP compliant devices and

	technologies not captured in first inventory. • Complete impact analysis of fiscal and operational impacts and risks.
June 30, 2008	• All agency infrastructures (network backbones) must demonstrate that it can use IPv6 and agency networks must be able to interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy *[R2].*

All tasks, requirements and reports have been completed and submitted to OMB for VA.

Additionally, the mandate stated that the subjects described below would be evaluated using OMB's Federal Enterprise Architecture (FEA) framework:

- Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
- Develop a sequencing plan for IPv6 implementation, integrated with agency Enterprise Architecture.
- Develop IPv6-related policies and enforcement mechanisms.
- Develop training material for stakeholders.
- Develop and implement a test plan for IPv6 compatibility/interoperability.
- Deploy IPv6 using a phased approach.
- Maintain and monitor networks.
- Update IPv6 requirements and target architecture on an ongoing basis.

VA is currently addressing these areas.

2.2.2 ADDITIONAL GUIDANCE

While OMB's original mandate is often referred to as "transition", the mandate does not describe transition in the strict definition of the term as in one thing being replaced by something else. This mandate required all agencies to be using IPv6 on their network infrastructures along with IPv4. Guidance from both OMB and the CIO Council later described a phased-in methodology for all Federal government agencies, over an undefined period.

The CIO Council provided clarification regarding the definition of the backbone network as "the backbone network which includes the WAN core up to the local area network (LAN). The LAN demarcation point is the device (router or switch) which provides connectivity to remote client-based user devices, such as a workstation *[R2]*."

The CIO Council has interpreted the OMB mandate to require that the agency's network backbone be ready to transmit both IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. The Council has stated that the agency "must be able to demonstrate that they can perform at least the following functions, without compromising IPv4 capability or network security."

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN)."

Exhibit 2. OMB Mandate Interpretation

Taken from the CIO Council Document titled "Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6) Frequently Asked Questions," dated February 15, 2006.

2.2.3 SUBSEQUENT CIO COUNCIL GUIDANCE

Since 2006, the CIO Council has published a variety of guidance-related documents to further clarify IPv6 transition requirements. The latest draft published, ***"Planning Guide/Roadmap Toward IPv6 Adoption within US Government"***, Version 0.2, dated February 2009, details a more rational approach to IPv6 transition. This document describes tasks called "Quick Wins" to ensure that every agency is fully prepared for eventual IPv6 deployment.

CIO Council suggests that agencies accelerate their preparation for IPv6-enabled network service deployment even though there isn't a new "mandate" to force deployment. To meet this goal, VA must modernize its Information Technology (IT) infrastructure segment architecture and update its strategic plans.

The following areas, amongst others, will deliver Quick Wins:

- Establish a test lab to ensure a safe, controlled introduction of new technology into VA's network.
- Employ small-scale validation of IPv6 performance outcomes.
- Acquire IPv6 address space from the American Registry of Internet Numbers (ARIN).
- Deploy an IPv6 address management tool to assure the uniqueness and consistency of VA's addressing schema. The tool must be capable of tracking, allocating, and managing IPv6 space as well as IPv4 space.

- Update VA's Transition Strategy Plan to reflect the next steps in its IPv6 transition. This task must include new IPv6 agency policy and procedures so that deployment goals evolve to match new objectives along with new success metrics.
- Obtain senior-level management support to ensure agency-wide participation and support.
- Develop a concrete plan and business case to implement IPv6 application to support VA's mission.

2.3 SCOPE

This document establishes VA's IPv6 transition planning activities.

It applies to all VA centrally managed information technology (IT) assets under the authority of VA's CIO. All described engineering and test activities apply to specific VA infrastructures, network services and applications, as well as to VA's critical interfaces with external organizations. Described information technology assets include hardware, firmware, data, commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software.

This plan also defines high-level roles and responsibilities required to accomplish IPv6 transition. This transition plan will evolve over time and will, as policies and procedures are amended, incorporate all applicable VA Office of Information and Technology (OI&T), Office of Telecom, and VA Departmental guidelines. This plan will act as policy for all VA funded programs that fall under the purview of VA's CIO.

This plan should be used as guidance for all VA organizations and as a source for coordination information by business partners such as the Department of Defense / Military Health System (DoD/MHS), Indian Health System (IHS), and the Managed Care Support Contractors (MCSC).

The plan is relevant to all existing IPv4 hardware, software, and biomedical devices to ensure that they will interoperate within an IPv6-based information routing infrastructure, or that a migration plan is in place and an associated waiver is approved. The plan is also intended to facilitate coordination and collaboration among the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration (NCA), and all organizational elements within VA, as well as all business partners, to accomplish the transition.

2.4 ORGANIZATION

This plan delineates the roles and responsibilities of various stakeholders in Sections 3 and 5, and describes a phased approach for VA's transition in Sections 2, 5, 6 and 7 respectively. Transition schedules and reporting requirements are covered in Sections 8 and 12.

Appendix A lists acronyms used in the plan. Appendix B lists references, Appendix C lists transition mechanisms. Appendix D tabulates the major training areas pertaining to VA IPv6 transition, with an emphasis on the impact to VA.

2.5 BENEFITS OF TRANSITIONING TO IPv6 & WHY IPv6 IS IMPORTANT TO VA

The general rationale for the deployment of IPv6 has been the worldwide depletion of IPv4 address space with predictions for IPv4 address exhaustion in the 2008 to 2012 timeframe. Regardless of when it occurs, it is simply a matter of time before there will no longer be available address space with IPv4. IPv6 solves this problem by providing 50,000,000,000,000,000,000,000,000,000 available addresses, far beyond that of IPv4.

More recently, with technology transformation, there are also some practical and very beneficial uses noted with IPv6 that either would not be possible with IPv4, or at best, would be extremely difficult. An additional benefit of IPv6 over that of IPv4 is expected to be the enhanced security capability, with better safeguarding and protecting data and information. Examples of new technologies include, but are not limited to: Radio Frequency Identification (RFID) with a broad potential application, and sensor technology; some of which incorporate embedded techniques for control of multiple functions by any authorized device source with an appropriate level of access and authorization. RFID with IPv6 offers a potential for asset management inventory. This could be used for IT products and devices, real property, and even supply receipt, distribution and volume level management. Sensor technology will provide the ability to control lighting, heating, cooling, security access, and even traffic control and security monitoring, by desktop workstation or hand-held devices, with the appropriate level of access and authorization.

IPv4 is currently one of a number of internet standard networking protocols used by VA, its business partners and commercial industry, and has been in use for over twenty-five (25) years. It is deeply integrated into all aspects of VA, government and industry as a whole. IPv6 is the next generation of internet protocols. Transitioning to IPv6 is critical to VA for several reasons, which include but are not limited to the following:

- With the increasing number of Internet addressable devices worldwide, IPv4 addresses, especially within the commercial community, have become scarce. IPv6 will provide the Internet Protocol (IP) address spaces necessary to support future requirements. This capability helps satisfy the increased demand of emerging mobile or portable applications. This is an important feature for users needing to access the World Wide Web (WWW), home networks, e-mail, etc., using Layer 2 mobile wireless technologies such as “3G” *[R3]*. The Mobile IP protocol allows nodes to move transparently from one IP network to another without losing data or interrupting computer applications and settings. Mobile IP is built into the IPv6 protocol; for IPv4 it is an added function, not as efficient, and normally resulting in occurrences of delay or distortion, especially with motion or moving display viewing.

- IPv6 based networks are anticipated to be easier to manage, since IPv6 is being built to address many of the issues that currently require patching to overcome IPv4 limitations.
- IPv6 will facilitate implementation of end-to-end security in IPv6 native mode. Security features will provide capabilities for authentication, data integrity, replay protection, and confidentiality, all of which are critical functionality for VA. The significant number of addresses in an IPv6 subnet will enable the IPv6-enabled host or network to frequently change host addresses and eliminate perceived threats of being able to correlate address entries in remote access logs of web activity. Topology hiding can be used to prevent correlation of network addresses of other potential security targets. IPv6 also has secure neighbor discovery extensions for which there is no equivalent in IPv4.
- IPv6 packets are simplified and allow packet traffic prioritization. They can improve Quality of Service (QoS) for audio, video, and Voice over IP (VoIP). IPv6 packets contain a field, the flow label not found in IPv4, which allows routers along the connection path to treat traffic per flow with greater specificity or granularity. This is useful for streaming applications such as video conferencing and real-time VoIP data transmission.

2.6 STRATEGY

VA will rely heavily on technology refreshment in procuring IPv6 capable hardware and software as the primary method for long-term IPv6 migration. As part of this strategy, IPv6 co-existence mechanisms (see Appendix C) will be used to provide the ability of VA to operate both IPv4 and IPv5 concurrently without degrading or eliminating current vital services.

For those enclaves that cannot transition fully into the IPv6 mesh, islands of IPv4 operations may be required. In this case, VA traffic may be tunneled or translated into the larger IPv6 cloud, all using appropriate security measures and safeguards to prevent exposure to or opportunity for a breach of privacy or information access by unauthorized sources.

2.6.1 HOW IPv6 BENEFITS MAP INTO VA'S GOALS

IPv6 features contribute to meeting four of VA Strategic Plan goals. These are:

- Veteran-centric services
- Collaboration with other agencies
- Improved information security
- Emergency management

2.6.2 VA STRATEGIC GOALS MAPPED TO IPv6 FEATURES

VA strategic goals are aligned with the overall VA Strategic Plan and with current and planned organizational changes that are in progress and follow the principles of CORE.GOV, E-GOV, and LoB in the Federal Enterprise Architecture (FEA) model.

The strategic VA goals mapping to IPv6 features are illustrated in the following Exhibit.

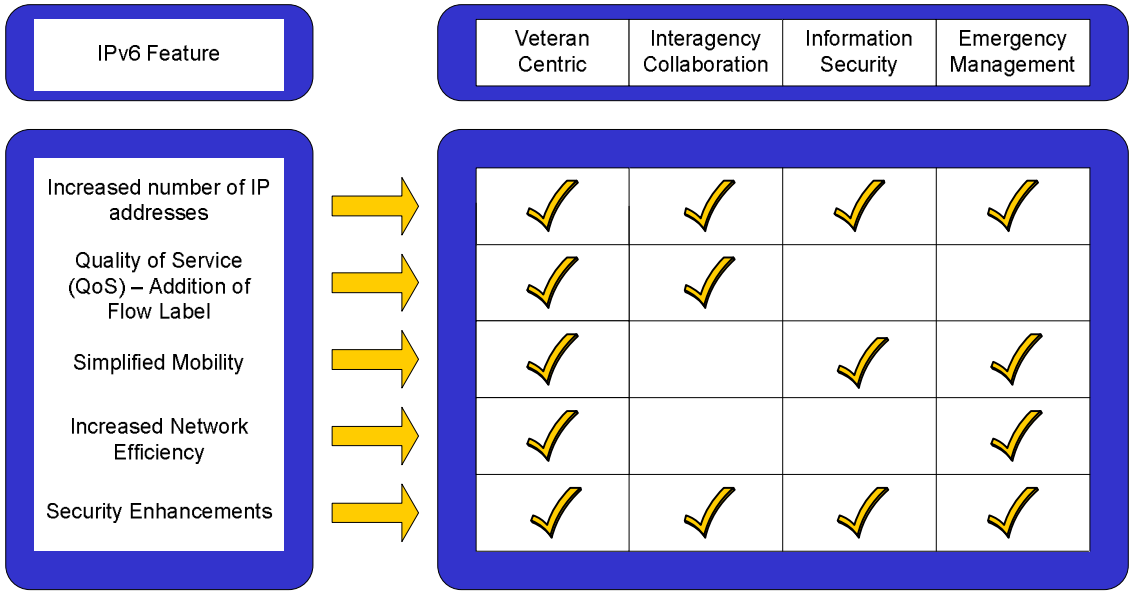


Exhibit 3. Strategic Goals Mapped to IPv6 Features

2.7 IPv6 TRANSITION ASSUMPTIONS

In developing the IPv6 Transition Plan, the following assumptions were made:

- VA will fund, schedule, and transition to an IPv6 Infrastructure (network backbone).
- IPv6 changes for VA encompasses VHA, VBA, NCA and other systems or infrastructure programs that must be programmed and/or budgeted within the respective and correlating Program Budget (OMB Exhibit-300) submission.
- VA will provide coordinated and sequenced training to WAN Managers, Network Administrators, and all IT and Telecommunications staff following IPv6 Transition Plan
- The Office of Information & Technology (OI&T) and the telecommunications organizations within VA will jointly prepare funding requirements and schedule to transition centrally managed assets and infrastructure:

- At this time, transition goals apply to IP-based systems and networks only. Future adaptation of Voice Over Internet Protocol (VoIP) will predicate common shared objectives.

- Configuration management (CM) is critical to successful transition. CM policies and procedures, now in place with the Enterprise Security Configuration Control Board (ESCCB), will continue. These policies and procedures are separate from this document, although available on the http://www.va.gov web site.

3 GOVERNANCE

3.1 STRUCTURE

The governance management structure for VA's IPv6 transition is illustrated in the Exhibit below:

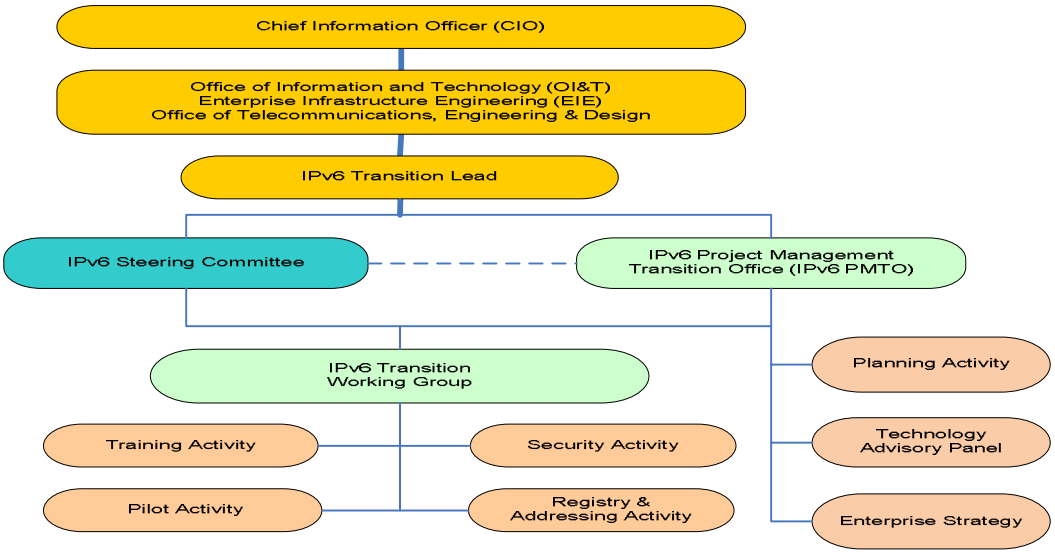


Exhibit 4. VA IPv6 Transition Governance Structure

3.2 ROLES AND RESPONSIBILITIES

Typically, governance roles and responsibilities include:

1. defining each area's specific role in the process,
2. setting policies which detail rules and methods to be followed in reporting to management,
3. communicating progress and issues to every member of the IPv6 Transition Team,
4. reviewing and approving status reports from management and team members, and
5. taking action to correct any deficiencies or violations.

The following sections address these roles and responsibilities.

3.2.1 VA CHIEF INFORMATION OFFICER

VA's Chief Information Officer (CIO) has the ultimate authority and responsibility for the smooth and timely IPv6 transition of the agency infrastructure and is responsible for enterprise-wide IPv6 migration. The CIO receives regular informational updates from the IPv6 Steering Committee leadership who coordinate IPv6 activities for all VA elements. The Steering Committee is headed by a member of OI&T, Office of Telecommunications, Engineering and Design.

3.2.2 VA - OFFICE OF INFORMATION & TECHNOLOGY, ENTERPRISE ARCHITECTURE & TELECOMMUNICATIONS

The vast majority of VA data information exchange, voice and video conferencing, and telecommunication telephony is now provided by disparate and non-integrated systems in VA. With implementation and migration to IPv6, the integration of these currently independently managed technologies may be considered in the future. The integration of these services would provide a more efficient use of resources and would ensure a sustained and responsive integrated network operations. In addition, the Office of Enterprise Architecture Management (OEAM), combined with a strategic goal of consolidated regions in VA, will provide a better management approach for the one-VA future topology goal for specific functional elements. This new structure is also aligned with the Federal Transition Framework (FTF).

VA's IPv6 transition office responsibilities for integrating and coordinating transition include:

- Managing IPv6 implementation to meet the business and technical requirements of VA's enterprise architecture.
- Supporting and coordinating updates of VA's IPv6 transition plan with VA's Enterprise Architecture (EA) and ensuring that VA transition plans are synchronized and consistent with EA, as well as VA's strategic goals.

- Leading the development of in-depth transition guidance and/or policies – and providing these results to VA Office of Policy and Procedure.
- Developing an implementation schedule in conjunction with VA field operations and other affected organizations.
- Leading or supporting VA IPv6 working groups by providing technical and project management support.
- Coordinating IPv6 implementation strategies with other federal agencies.
- Tracking IPv6 transition progress and providing assessment and recommendations.
- Providing IPv6 knowledge base throughout VA for information exchanges and outreach.

A technical outreach program is important to the success of VA's general IPv6 development effort. VA, through all IPv6 working groups, is interacting with other organizations involved in the deployment of IPv6. These organizations include federal agencies, the National Institute of Standards and Technology (NIST), the research and education community, commercial organizations and other standards organizations. Through technical outreach activities, VA will gain and share the most economical, reliable, secure, and expedient methods for deploying and maintaining an IPv6 infrastructure. It is through collaboration that unnecessary duplication of IPv6 efforts by Federal agencies, including VA, will be reduced.

3.2.3 VA IPv6 STEERING COMMITTEE

The Steering Committee was formed early in the project to direct all IPv6-related activities throughout the agency. The Committee is responsible for IPv6 policy and direction for the agency, coordinating and communicating amongst the active working groups, overseeing transition activities and progress including reviewing and approving transition plans, schedules, and documents.

To accomplish its mission, the Steering Committee initially established several technical working groups to connect various departments' technical expertise. Since VA met its June 2008 mandate, the Steering Committee continues its direction and coordination of future IPv6 transition and deployment.

Initially the Steering Committee established the following working groups:

- Enterprise Strategy Working Group
- Transition Working Group
- Registry and Addressing Working Group
- Training Working Group
- Security Working Group

In June 2008, these separate working groups were re-structured as three entities:

- The Steering Committee, which has overarching responsibility;
- The IPv6 Transition Working Group, which includes the separate activities of Registry and Addressing, Training, Security, and the IPv6 Pilot Activity Team; and
- The IPv6 Project Management Transition Office (PMTO), which includes Enterprise Strategy activities, the Technology Advisory Panel (TAP), and IPv6 planning activities.

3.2.3.1 VA IPv6 Project Management Transition Office (PMTO)

VA's original IPv6 Transition Office *[R4]* was responsible for ensuring a coherent, timely IPv6 transition across VA and through OEAM for providing common engineering solutions and guidelines designed from an enterprise perspective. The IPv6 PMTO continues to be responsible for:

- Coordinating transition planning, analyses, testing, and implementation efforts in VA.
- Promoting knowledge sharing.
- Ensuring that needed infrastructure is provided.
- Implementing a systematic program of outreach within VA's community.
- Ensuring that critical transition issues are prioritized and addressed.
- Ensuring compliance with an end-to-end IA approach through VA IPv6 Security working group in conjunction with VA Office of Policy and Procedure.
- Testing of security provisions measures.
- Conforming to established federal standards for security.
- Establishing and maintaining VA IPv6 Milestones and Objectives, with documented progress.
- Ensuring a timely, secure, and operationally effective IPv6 environment.
- Following VA's Desktop security Configuration provided through Federal Information Security Management Act (FISMA) reporting.
- Ensuring that IPv6 IA issues are identified and included in transition planning efforts.
- Developing a Partial Certification and Accreditation (C&A).package for IPv6 for approval by the Component Designated Approving Authorities (DAA) – VA CIO.
- Developing a vulnerability assessment for IPv6.
- Testing and evaluating results for IPv6 security devices.
- Providing oversight for the IPv6 transition efforts funded by VA.

- Ensuring executive-level awareness is provided for support and transition requirements.
- Providing frequent information updates and status briefings to VA's CIO, who is the principle authority for all efforts pertaining to IPv6 in VA.
- Providing information necessary to all VA system owners and managers for awareness of current and future plans with regard to VA and IPv6.
- Establishing a method for disseminating lessons learned and successes for future reference.
- Documenting and identifying resources needed for testing, engineering, and pilot implementations, as well as overall transition of legacy IT for transition.
- Identifying health information management, information technology, information assurance, and enterprise architecture programs that are compliant with federal IPv6 directives and current IPv6 transition plans.
- Working with existing VA functions, including OEAM to develop and implement IA policies, procedures, and programs.
- Coordinating efforts in VA as the CIO designated lead agent for IPv6, for a gradual, methodical and logical IPv6 transition. This includes planning, implementing and monitoring across VA and with other federal and private business partners.

3.2.4 VA IPv6 TRANSITION WORKING GROUP

The IPv6 Transition Working Group consists mostly of technical personnel and is responsible for developing, coordinating and implementing a cohesive transition plan for VA's migration to IPv6. Activities include:

- Conducting a requirements analysis of the IPv6 transition.
- Providing an approach that is practical and methodical, and ensures the integrity of data and information.
- Developing and implementing a test plan for compatibility and interoperability and in providing both proof-of-concept and demonstration of the activity.
- Managing the deployment of IPv6 capability in a phased approach.
- Updating VA IPv6 requirements and target architecture in coordination with VA OEAM.

3.2.4.1 VA IPv6 Registry and Addressing Activity

Registry and Addressing is responsible for:

- Evaluating IP addressing needs for VA's IPv6 transition.
- Requesting the IPv6 address block from American registry for Internet Numbers (ARIN).

- Developing and documenting a plan for allocating the addresses across VA.
- Developing a plan for managing IPv6 addresses.

3.2.4.2 VA IPv6 Security Activity

Security is responsible for:

- Completing the security risk assessment.
- Updating the Risk Assessment document.
- Initiating processes and documents necessary with C&A.
- Identifying and recommending noted IPv6 vulnerabilities.
- Attaining Interim Authority to Operate (IATO) or Full Authority to Operate (FATO).
- Reviewing and commenting on VA's Transition and Implementation Plans and security controls.
- Verifying security controls before, during and after testing.

3.2.4.3 VA IPv6 Training Activity

Training is responsible for evaluating, developing and implementing training approaches and programs for VA's IPv6 transition stakeholders. This group has produced a document describing how, when and for whom the entire integrated training program will be implemented and rolled out for all of VA.

3.2.4.4 VA IPv6 Pilot Activity

The new IPv6 Pilot Team is responsible for identifying an Pv6 application that demonstrates realistic merit for VA's use, giving the best value for the ultimate customer, the Veterans. It will also set in motion the steps required for implementation. These steps include providing planning and oversight, building a concrete pilot business case, developing a master schedule to contain timeframes for the designated pilot candidate, and arranging for the ultimate deployment of a successful IPv6 application pilot.

3.2.5 VA IPv6 PROJECT MANAGEMENT TRANSITION OFFICE (PMTO)

As an extension of the Steering Committee, VA's PMTO is responsible for day-to-day systems life-cycle management activities, including concept exploration, requirements gathering, technical design, acquisition and development, testing, deployment, sustainment and phase out. With VA CIO approval for each transition milestone, and with close coordinated efforts with the OEAM, each must work toward the acquisition of requirements to accomplish the phased transition from IPv4 to IPv6. The following are representative necessary activities PMTO performs:

- PMTO Assessment Phase representative activities:
  - Determine which VA assets may be impacted by IPv6 transition.

  - Determine how potentially impacted assets are interconnected to other VA assets, and what services they require from other VA assets.
  - Determine if a potentially impacted asset is compliant with federal and VA policy that specifies its level of IPv6 capability.
  - Determine the impact of IPv6 transition on an asset or assets.
  - Determine how much it will cost, directly or as labor, to transition the asset to IPv6.

- PMTO Implementation Phase representative activities:
  - Identify and address any necessary pre-implementation activities.
  - Begin development and testing processes.
  - Address IA concerns.
  - Coordinate Developmental Test and Evaluation (DT&E) with the Security NOC, to develop systematic approaches to centrally managed application testing, validation, and certification.
  - Procure replacements for existing systems/equipment that are not IPv6 capable (e.g., operating systems [OS], routers, firewalls, end user devices [EUD], including COTS and GOTS), and for all other legacy systems.
  - Coordinate IP address requirements with the Security NOC.
  - Transition, migrate, and implement critical systems to IPv6.
  - Configure equipment and circuits according to address and architecture plans.
  - Minimize potential security vulnerabilities by deploying only approved transition mechanisms (see Appendix C).
  - Enable IPv6 in IPv4 in virtual private networks (VPN).
  - Ensure systems can interface with business partners outside VA's domain, as appropriate and as required.
  - Ensure that all systems and components integrate communications and computing infrastructure requirements, and provide products/services that support VA systems and applications.
  - Ensure all new infrastructure acquired hardware and software include configurations that are IPv6 capable.
  - Develop IPv6 capable network architectures that must support the IPv6 capabilities of infrastructure assets.
  - Determine End-to-end IPv6 solutions, developed and tested in either closed enclaves or using tunneling through IPv4-only networks.
  - Work closely with VA's Certification and Accreditation Office in conducting network risk assessments and security policy compliance assessments, and in achieving the required level of C&A related to IPv6.

3.2.5.1 VA IPv6 Enterprise Strategy Working Group

Under PMTO, the Enterprise Strategy Working Group is an ad hoc group responsible for determining deployment strategy; deciding what the initial IPv6 architecture should be; researching future uses of IPv6 at VA; helping drive the transition strategy; and assisting all groups at VA to understand the long-term benefits of IPv6

3.2.5.2 VA Technical Advisory Panel (TAP)

The *Technology Advisory Panel* (TAP) is an ad hoc group managed by the PMTO consisting of VA engineers and sponsors as well as industry technology representatives. Its goal is to discuss IPv6 implementation strategies and explore planned use of existing or emerging technology solutions provided by technology representatives.

3.2.5.3 VA IPv6 Planning Activity

The *Planning Activity* is responsible for formulating and structuring plans leading to IPv6 deployment. This support is provided for both the IPv6 Transition Working Group and IPv6 Steering Committee.

3.3 REPORTING

OMB requires quarterly submission of reports showing progress toward the transition to IPv6. The compiled reports constitute the basis for IPv6 compliance in VA.

The previous requirements are in addition to the original OMB Mandate requirements stemming from OMB memo M-05-22, which are:

- ✓ November 15 2005
  - ✓ Assign an agency lead to lead and coordinate planning.
  - ✓ Inventory of routers, switches, and hardware firewalls.
- ✓ February 28 2006
  - ✓ VA IPv6 Transition milestones and progress report on inventory and impact analysis submitted as part of VA Enterprise Architecture.
- ✓ June 30 2006
  - ✓ Inventory of all infrastructure hardware and software.
  - ✓ Impact Analysis of fiscal and operational risks.

- ✓ June 30 2008
  - ✓ Backbone network infrastructure must demonstrate its ability to use IPv6, and all VA networks must demonstrate its interface with VA's backbone infrastructure.
  - ✓ All applications and product features developed or acquired after July 2005 are IPv6 compliant or have a scheduled refresh/migration path in place with a commitment to upgrade to IPv6.

3.4 MAINTAINING VA IPv6 TRANSITION PLAN

VA's IPv6 Transition Plan will focus well into the future and will additionally include:

- The process for assignment and registration of Internet Protocol address space for all VA sponsored data networks and systems, with oversight by OEAM, will include management of VA IPv6 address allocation, registration and control, is anticipated to be through VA's Network Operations Center (NOC), to promote interoperability and security.
- An additional coordinated role by OEAM in providing the overall technical coordination, engineering, guidance, and assistance across VA, which are needed to support an integrated and logical IPv6 transition.
- Coordinating VA IPv6 standards, through the Office of Policy and Procedure.
- Providing top level IPv6 networking service support for VA, including Internet root server(s), and Internet Service Provider (ISP) service.
- Continued updates of CIO Directives to insure product compliance for interoperability testing and certification of IPv6 products and capabilities, according to the established OMB directives, now in draft documents developed by NIST.
- A transition of responsibility from VA IPv6 Working Groups to that of VA System owners and managers as it relates to all elements and functions identified in VA's IPv6 Transition Plan that covers the transition to IPv6 for VA.

4 REQUIREMENTS

4.1 HIGH-LEVEL REQUIREMENTS DEFINITION

The OMB mandate for June 2008 (Memorandum M-05-22) and guidance from the Federal CIO Council Architecture and Infrastructure Committee required that Federal organizations "conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements."

These requirements resulted in an assessment phase consisting of: developing acquisition and procurement strategies; identifying hardware and software to be transitioned, replaced, or removed; identifying funding requirements; identifying training requirements; addressing Information Assurance (IA) concerns; and identifying compliance standards.

The requirements for the transition of the network infrastructure to IPv6 capability lead to a network state where IPv6 traffic can be handled in a secure manner. As the OMB mandate for June 2008 stated:

"Specifically, any new IP product or system developed, acquired, or produced must:

- Interoperate with both IPv6 and IPv4 systems and products,
- If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features by June 2008, and
- Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management *[R1]*."

In addition, the Federal CIO Council Architecture and Infrastructure Committee's IPv6 Transition Guidance stated:

"Agencies must be able to demonstrate they can perform at least the following functions, without compromising IPv4 capability or network security:

- Transmit IPv6 traffic from the Internet and external peers, through the network infrastructure (core), to the LAN.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
- Transmit IPv6 traffic fro the LAN, through the network backbone (core), to another LAN (or another mode on the same LAN) *[R5]*."

The requirements for June 30, 2008 are for the network infrastructure (core). The guidelines stated that IPv6 does not need to be operationally enabled (e.g., turned on) by June 30, 2008, but the network infrastructure must be ready to pass IPv6 traffic and support IPv6 addresses. Applications, peripherals, and other IT assets that are not included in the execution of the functions noted above are not covered by the June 30, 2008 deadline. Agencies will verify this new capability through testing activities and must demonstrate evidence of having done so. Agencies are also required to maintain security during and after adoption of IPv6, at the same risk level now in place.

The requirements for IPv6 capability on VA's infrastructure are based on the OMB mandate and Federal CIO Council guidance. As such, they may be summarized as follows:

By June 2008:

- Acquired products or systems must interoperate with IPv6 and IPv4 systems and products.
- Acquired products must have technical support for development, implementation, and management.

4.2 CAPACITY REQUIREMENTS

The high-level requirements from OMB do not include network capacity. The capacity requirement stipulated that devices processing IP packets must have sufficient capacity to handle both IPv4 and IPv6 simultaneously under the anticipated loads.

4.3 SECURITY REQUIREMENTS

It is necessary to identify existing requirements under IPv4 to inspect network traffic in firewalls and in intrusion detection/prevention (IDS/IPS) products. After implementation of IPv6-relevant firewalls and IDS/IPS systems, an assessment is needed to ensure that security posture has not been reduced to an unacceptable risk level. Network security must be at the same level or greater as IPv4 with IPv6 implementation.

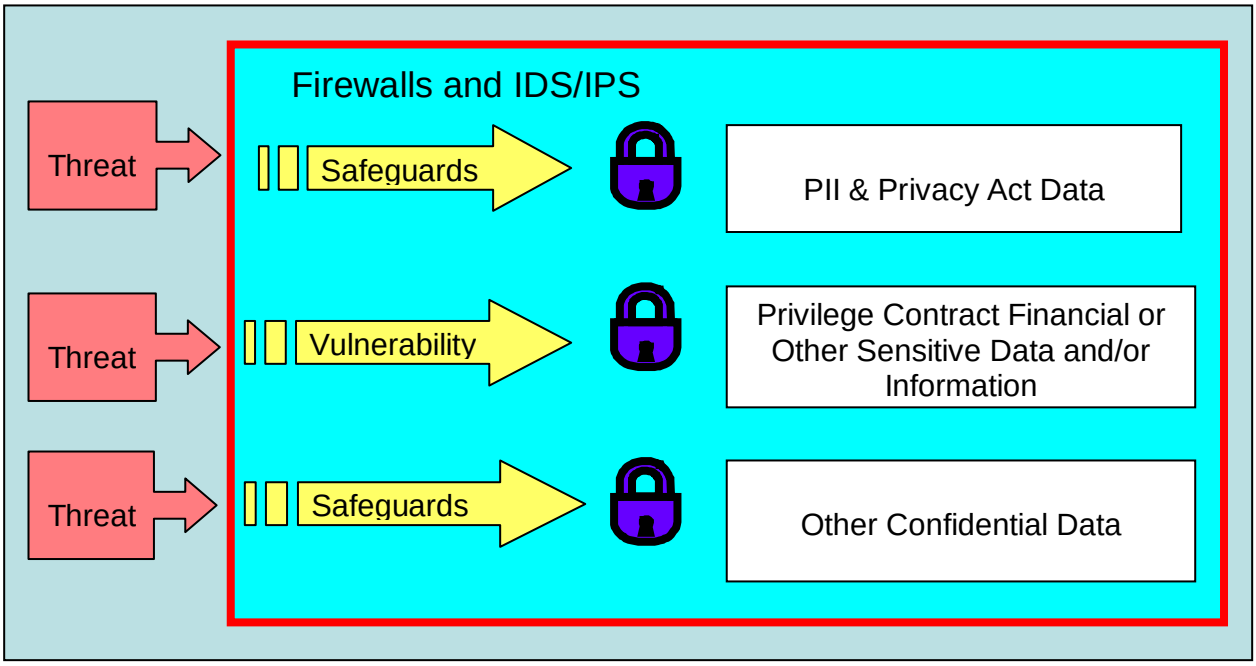


Exhibit 5. Consistent Prevention, Monitoring and Threat Detection

VA will sustain due diligence pertaining to confidentiality, integrity, and availability for all data and information that is accessed, used, developed, shared, transmitted, or stored. In addition, a continuing approach for risk impact assessment will be used with a prior determination made as to whether a potential or known threat is: Low, Moderate, or High, and appropriate and subsequent actions will immediately be initiated.

4.4 IPv4 NETWORK REQUIREMENTS

To ensure that there is no degradation of network capability caused by the introduction of IPv6, an assessment of IPv4 requirements is needed. For example, reviews of various surveys of IPv4 requirements identified in the Internet Engineering Task Force (IETF) standards can promote continued use of some products with the introduction of IPv6 capability.

4.5 IPv6-ADDRESSING REQUIREMENTS

The large number of IPv6 addresses now available to VA need to be managed. Processes are needed to conduct initial address allocation (likely in blocks) and subsequent management of the addresses. The IPv6 Registry and Addressing Working Group has developed an addressing plan for this purpose, and the same working group is now working with the IPv6 Steering Committee and VA NOC to devise a coherent process plan that will be coordinated through VA's Office of Policy and Procedure.

4.6 DOMAIN NAME SERVICE REQUIREMENTS

An IPv6-capable domain name service (DNS) may be needed. However, the issue of DNS along with a well thought out plan for implementation is still being addressed at this time. If a DNS server methodology is implemented, it must handle both IPv4 and IPv6 traffic requests.

4.7 TESTING REQUIREMENTS

To ensure an acceptable level of risk with a VA IPv6-capable network, testing and results analysis of the testing must be conducted, on both laboratory and network environments. A VA IPv6 Testing Plan has been drafted and will be recommended for approval to VA's Designated Approval Authority (DAA) who is CIO.

4.8 STANDARDS REQUIREMENTS

All federal agencies must comply with NIST standards. Additionally, there has been an OMB memo issued (M-07-11 dated March 22, 2007) directing conformity with: the National Institute of Standards and Technology (NIST), the Department of Defense (DoD); and the Department of Homeland Security (DHS) standards. VA's working groups have worked closely with VA Office of Policy and Procedures, with the NSOC, and with OCIS in preparation of all documents pertaining to standards. NIST and OMB maintain congressional authority to publish and direct specific compliance of standards for all federal agencies.

4.9 FUNDING REQUIREMENTS

Many VA Programs have provided OMB Exhibit-300 funding needs, which are related and include baseline-projected expense for implementing IPv6. This information is maintained at www.va.gov under the EA 4.2 initially published in February 2007.

The following text is transcribed from the most recent DoD IPv6 transition plan and is included because it closely aligns with VA perspective and goals. This provides excellent guidance upon which VA can develop similar plans in meeting funding requirements.

The DoD's IPv6 transition strategy is designed to manage overall cost through incremental technology-refreshment and manage the risks associated with the DoD transition to IPv6. By starting to procure IPv6 capability beginning July 2005, the DoD is building an inventory of the access that are ready to operate with IPv6. In addition, by building IPv6 into the major next

generation transformational capabilities being developed now and in the future, the DoD will avoid later transition costs when these systems become operational. This strategy also allows the DoD to leverage ongoing commercial and industrial IPv6 work to better meet DoD needs.

Even with this strategy, there will be additional costs for this major technology transition to occur in the manner that protects enterprise interoperability, security, and performance. These additional costs are expected to be in the areas of:

- *Planning, engineering, technical assessments, and training to support a coherent IPv6 transition.*
- *Pilot IPv6 implementations and test beds necessary to minimize transition risks and demonstrate transition readiness, including necessary infrastructure.*
- *IPv6 modifications to current development effort.*
- *Selective equipment and/or software replacements/modifications where timely technology-refreshments are not programmed.*

The DITO will minimize the additional cost by harmonizing enterprise transition efforts such as developing common engineering solutions, sharing knowledge and avoiding duplicative testing and demonstrations. The transition office is responsible for providing overall technical assistance, performing engineering analyses of critical DoD issues, coordinating DoD-wide IPv6 transition planning and working group efforts, integrating IPv6 tests and demonstrations, and tracking implementation progress [R4].

As previously noted, VA has initiated efforts toward inclusion of additional funding requirements for IPv6 into many VA Program Funding Requirements (OMB Exihibit-300). VA's IPv6 Lead has requested funding for FY 2011-2014 in support of transition efforts.

5 IMPLEMENTATION PHASES AND ACTIVITIES

The implementation phases and activities will be refined in future revisions of the transition plan. The current implementation strategy is to deploy IPv6 on the core of VA's backbone network and expand the deployment over time to the lower network levels (see Fig 1).

The initial VA infrastructure implementation will be under the oversight, management and coordination of VA's IPv6 PMTO. The PMTO will assume responsibility for IPv6 oversight, management, and coordination activities within the given areas of responsibility for execution of individual tasks within their Program Offices, and are required to develop Transition Plans for their individual programs as road maps to follow in executing IPv6 activities. VA will employ (and to some degree already has) an IPv6 phased approach as follows:

- Assessment Phase
  - Acquisition review Sub-phase
  - Asset and Existing Architecture Identification Sub-phase
  - IPv6 Compliance and Transition Impact Sub-phase
  - Funding Requirements Sub-phase
- Implementation Phase
  - Development and Testing Sub-phase
  - Early Migration Sub-phase
  - Intermediate Transition Sub-phase
  - Final Transition Sub-phase

5.1 ASSESSMENT PHASE

The Assessment Phase consists of those activities required to:

- Identifying current and planned acquisitions.
- Determining which VA hardware and software assets may be potentially impacted by IPv6 transition, how they are inter-related, and which assets must be transitioned, replaced, or removed.
- Identifying which assets are IPv6 compliant and determining the impact of transitioning those that are not.
- Determining funding requirements for transitioning hardware and software to IPv6.

Acquisition Review Sub-phase	Asset & Existing Architecture Identification Sub-phase	IPv6 Compliance & Transition Impact Sub-phase	Funding Requirements Sub-phase
• Identify current and planned acquisitions • Ensure RFI & RFP contain VA mandated IPv6 compliance language. • Ensure contract vehicles contain VA mandated IPv6 compliance language and address measures to transition to IPv6.	• Identify VA hardware and software assets. • Determine IPv6 transition impact. • Develop Initial Asset and Existing Architecture Identification Assessment. • Conduct architectural reviews during IPv6 assessments.	• Identify assets that are IPv6 compliant. • Develop IPv6 Compliance and Transition Impact Assessment Report.	• Identify funding requirements for transitioning hardware and software to IPv6. • Link IPv6 requirements to budget initiatives.

Exhibit 6. Assessment Phase Activities

5.1.1 ACQUISITION REVIEW SUB-PHASE

The Acquisition Review identifies current and planned acquisitions and ensures that all VA acquisition related documentation, including all requests for information (RFI), requests for proposal (RFP) and contract vehicles developed by the program/project

office, contain VA's mandated IPv6 compliance language. All contracts must also address measures to transition to the IPv6 environment.

5.1.2 ASSET AND EXISTING ARCHITECTURE IDENTIFICATION SUB-PHASE

Actions will be taken to determine which VA hardware and software assets may be potentially impacted by IPv6 transition, how they are inter-related, and which assets must be transitioned, replaced, or removed. These identification activities will be applied to all VA infrastructure, network services and applications, as well as to interfaces with external organizations. All VA program/project offices are responsible for executing an initial assessment and producing an Initial Asset and Existing Architecture Identification Assessment. From these the work required to execute an initial IPv6 Compliance Assessment can be determined, which will be coordinated through with VA OEAM.

To ensure an entire system and its interrelationships are identified properly; program managers should employ architectural views when performing IPv6 assessments. The program/project manager is not only concerned about the IPv6 capability of any Government-Off-The-Shelf (GOTS) application being developed, but also all the supporting Commercial-Off-The-Shelf (COTS) applications and operating systems that form the components of the entire system. If an identified asset exchanges data with another asset, then IPv6 transition for both assets must be coordinated.

5.1.3 IPv6 COMPLIANCE AND TRANSITION IMPACT SUB-PHASE

This Sub-phase identifies which assets are IPv6 compliant and determines the impact of transitioning those that are not. The compliance and impact assessment activities will be applied to all VA infrastructure, network services and applications, as well as to interfaces with external organizations. All VA program/project offices are responsible for conducting an initial assessment and producing an IPv6 Compliance and Transition Impact Assessment Report.

The determination as to whether an asset/application is IPv6 compliant will be based on current NIST guidance, criteria and certification. In determining the degree of transition impacts on systems/assets/applications that are either not IPv6 compliant or depend upon assets that are not IPv6 compliant, consider: End-of-life; Technology refresh cycles; External communications, and Dual Stacking capability (See Appendix C).

5.1.4 FUNDING REQUIREMENTS SUB-PHASE

Actions will be taken to determine funding requirements for transitioning hardware and software to IPv6. As prescribed by OMB, the normal life-cycle refresh cycles in IT are relatively short, and should provide the opportunity for IPv6 capable product transition, which could be integrated into the normal technology refresh cycle. All VA purchasing from mid 2005 onward was directed to ensure assets were IPv6 capable to assist base level planning which would be IPv6 capable by 2008, and no additional Program Objectives Memorandum (POM) cycle funding required. However, there have been additional expenses identified for replacement of products with IPv6 capability, above and beyond replacement costs that would have been incurred for replacement with IPv4 product equivalent replacement. As the 2008 deadline for IPv6 capability approaches,

the concept of adding IPv6 to POM cycles has become a reality. Therefore, as warranted, IPv6 requirements should be linked to budget initiatives (e.g., 1% IT withhold and OMB Budget Exhibit 53).

5.2 IMPLEMENTATION PHASE

The Implementation Phase will consists of those activities required to transition all VA assets from IPv4 only to that of either a dual-stack IPv4/IPv6 environment or a native IPv6 environment. VA shall use appropriate transition mechanisms – including dual-stack, tunneling, and translation to effect the transition (see Appendix C). Using an iterative approach may result in the infrastructure and individual applications being in different stages of transition, which will require the simultaneous use of all mechanisms available. Early adopters potentially may run IPv6 initially only in their enclaves, followed by tunneling between enclaves through the enterprise infrastructure. Configuration management practices will be implemented to assure successful transition.

Development and Testing Sub-phase	Early Migration Sub-phase	Intermediate Transition Sub-phase	Final Transition Sub-phase
• Develop or identify IPv6 capable implementations • Develop IPv6 capable configurations • Developmental Test and Evaluation (DT&E) • IPv6 capable test facility deployment • Test pilots	• Deploy IPv6 capable implementations • Identify IPv4 legacy systems and apply for waivers • Final DT&E • Operational Pilots • Field Trials • Vulnerability mitigation identification	• Deploy and enable IPv6 operational configurations • Final OT&E • Plan for de-commissioning of IPv4 legacy systems	• Networks & systems are IPv6 enabled • Phase out IPv4 • De-commission legacy IPv4 systems by plan

Exhibit 7. Implementation Phase Activities

Note: Two terms are key to the transition: "IPv6 capable" and "IPv6 enabled."

- An "IPv6 capable" system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4.
- "IPv6 enabled" describes a condition achieved as the result of actions taken during the Intermediate Transition Sub-phase. The transition of existing IPv4-

only assets will near completion and test and evaluation activities will wind down. VA will be considered "IPv6 enabled" at the end of this phase.

5.2.1 DEVELOPMENT AND TESTING SUB-PHASE

During the Development and Testing (D&T) Sub-phase, IPv6 capable implementations and configurations of VA assets will be either developed or identified for testing. Testing and development activities will normally run concurrently. Development activities may differ for existing VA assets that require modification, versus new assets under development or planned.

Testing activities will include traditional DT&E, IA Certification Test and Evaluation (CT&E), and interoperability test and evaluation (IOP). In support of these test methodologies, IPv6 capable test facilities (test beds) will be required.

Application testing is essential to ensure that VA IPv6 components are IPv6 capable by FY 2008. Regardless of vendor compliance statements, IOP is imperative to ensure the integration and interoperability of components through the test and evaluation process. Each VA Program must determine the necessary amount of testing to determine compatibility. Application testing should be included as part of any normally scheduled D&T planning.

Once all of the assets associated with a system are IPv6 capable, they must be tested in all architectural configurations planned for deployment. These test scenarios may take place in test beds or test pilots limited to a single enclave. The lessons learned should then be incorporated into the operational pilots and field trials associated with operational test and evaluation (OT&E) activities during the Early Migration Sub-phase.

5.2.2 EARLY MIGRATION SUB-PHASE

At the completion of the Early Migration Sub-phase, all VA assets will be IPv6 capable. The only exceptions will be certain IPv4 legacy systems that will require a waiver. With the exception of these legacy systems, all assets that are not yet IPv6 capable must be replaced during this sub-phase. Testing of architectural configurations not tested in the D&T sub-phase will be completed in operational pilots. Once all DT&E activities are completed, field trails supporting OT&E will occur and must include Security Test and Evaluation (ST&E). Lessons learned during field trials will be incorporated into the final operational designs deployed during the Intermediate Transition sub-phase. Specifically, vulnerabilities identified as part of ST&E must be mitigated before full operational deployment of IPv6 can occur.

5.2.3 INTERMEDIATE TRANSITION SUB-PHASE

At the completion of the Intermediate Transition Sub-phase, all VA assets, with the exception of those few remaining legacy systems under waiver, will be IPv6 enabled and running IPv6 operational configurations. Testing of vulnerability mitigations and operational configurations not tested in the Early Migration sub-phase will be completed in initial deployments. Once all ST&E and OT&E activities are completed, full operational deployment of IPv6 configurations will occur. Lessons learned during operational deployments will be incorporated into plans for the final de-commissioning of IPv4 legacy systems.

5.2.4 FINAL TRANSITION SUB-PHASE

At the completion of the Final Transition Sub-phase, IPv4 will be phased out in VA's network. With the exception of IPv4 legacy systems, all VA networks and systems will be IPv6 enabled over time, native IPv4 support will be disabled and legacy IPv4 systems will be de-commissioned.

6 ACQUISITION AND PROCUREMENT

An integral requirement of the OMB M-05-22 mandate is that federal agencies require all IP-aware devices purchased by the agencies to be IPv6-compliant.

VA's initial definition of IPv6-compliant devices, product or service, consistent with OMB, NIST and the IETF, is that a product shall:

- be capable (once IPv6-enabled) of receiving, processing and forwarding IPv6 packets and interfacing with other systems and protocols using the IPv6 protocol in a manner similar to that of IPv4;
- be able to operate on a network supporting IPv4 or both IPv4 and IPv6;
- have available contractor/vendor IPv6 technical support for development, implementation and fielded product management;*[R1]* and
- maintain the same security or provide a greater level of security than is now in place.

6.1 IPv6 CAPABLE SYSTEM, DEVICE AND/OR PRODUCT

For systems, devices and/or products which do not meet the IPv6 capable requirement stated above, VA's CIO may waive the requirement of IPv6 capability based on consideration of an operational need or a business case, including long-term resource implications across the enterprise infrastructure. Some possible reasons for granting a waiver include:

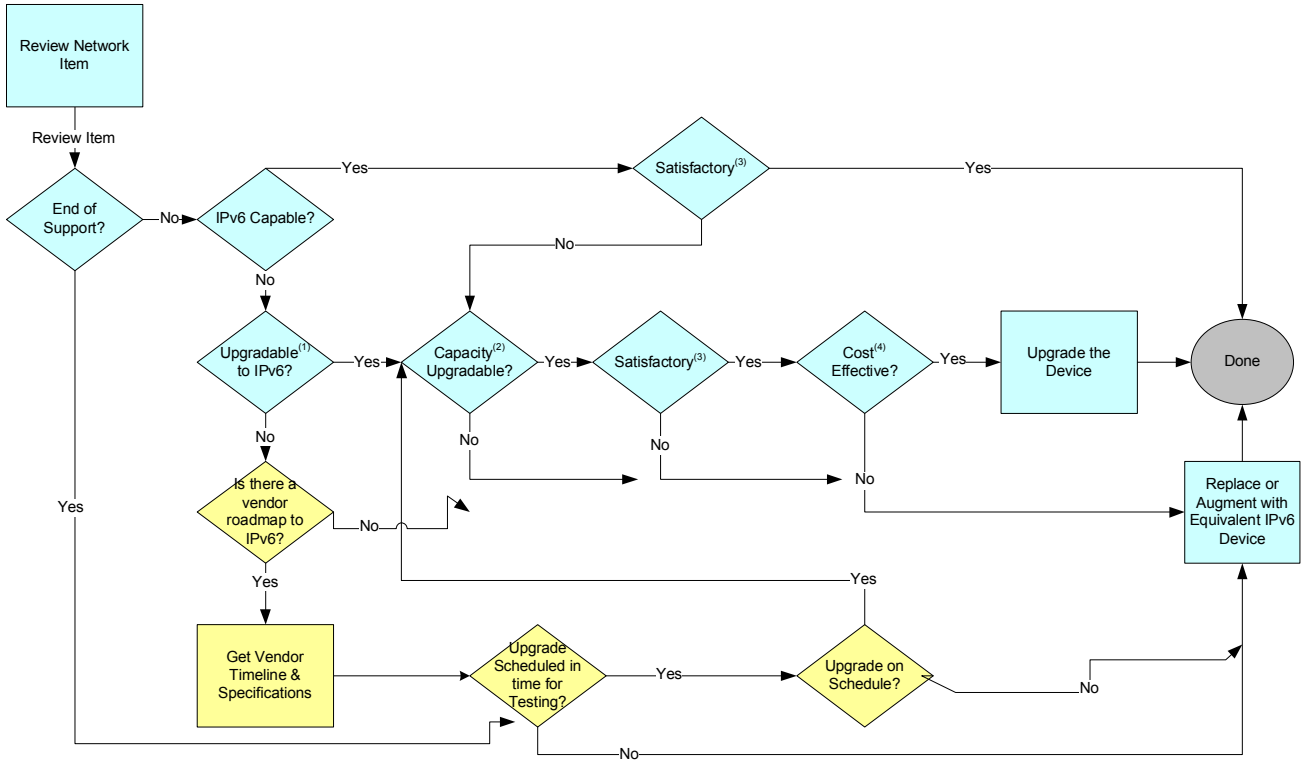
- The system, device and/or product, is not now and never will be planned for connection to VA's network.
- The system, device and/or product, meets a critical need and an IPv6-capable product is not currently available.
- The cost for an IPv6-capable system, device and/or product, compared to the cost of an equivalent IPv4 product; could result in an unacceptable delay in acquisition or possibly prohibit delivery of VA benefits which are required.
- The security threat and risks of implementing the IPv6 system, device and/or product, will be greater than the normal acceptable level.

6.2 INFRASTRUCTURE UPGRADE

VA conducted two separate inventories of IP devices on its infrastructure. These inventories revealed the following categories of equipment:

- Devices that are obsolete and need to be replaced.
- Devices that would be IPv6 capable, but require upgrade of internet operating system (IOS), memory, etc.
- Devices that are IPv6 capable now.

The process of assessing the status of the infrastructure devices and performing the necessary upgrades is depicted in the following diagram.



1. **Upgradable to IPv6** – The possibility of modifying a product so that it is IPv6 capable. An assumption is that after the product is upgraded it will continue to be IPv4 capable as well as IPv6.
2. **Capacity Upgradable** – The possibility of modifying an IPv6 product so that it is capable of performing in a specific use, e.g., by increasing memory capacity or processor speed.
3. **Satisfactory** – The capability of an IPv6 product to perform in a specific manner.
4. **Cost Effective** – The economic advisability of upgrading an IPv4 product so that it is IPv6 capable.

Exhibit 8. VA Infrastructure Assessment Process

OMB initially required that all agencies provide an inventory of all infrastructure components and elements. VA completed the following steps:

- Consolidate first and second OMB inventory into a master infrastructure inventory (first inventory has some routers and devices not in the second inventory).

- Complete and confirm information in the master infrastructure network inventory. This includes replacing fields in the second OMB inventory marked "sensitive" with the required information in the master infrastructure network inventory.
- Verify devices that have been documented to be replaced actually are replaced. This will require contacting the appropriate system owners or managers regarding specific infrastructure network devices.
- Obtain further inventory details, such as memory and processor capacity. With devices other than routers, this may include: model; type; chassis; etc. This would describe any item or element pertinent to the ability of the infrastructure IP-capable device to be IPv6-capable/compliant not previously captured by OMB required inventory. The specific information gained could be used as justification for replacement or upgrade to that of an IPv6-compliant system, device and/or product.
- Match routers against current IPv6 roadmap.
- For devices that will not be replaced as part of technology refresh before year end of 2007:
  - Document what would be required to upgrade or replace.
  - Provide a costs estimate for the upgrade and/or replacement.
  - Determine the acceptability of upgrade, including consideration of IPv6 readiness, capacity, and expected remaining life cycle.
  - Purchase the upgrade and/or replacement.
  - Install and test the upgrade and/or replacement.
- Provide baseline router configurations for OMB compliance testing. Any testing result should map directly to systems, devices and/or products that comprise the infrastructure, prior to the June 2008 mandate.

The above activities are applicable to all types of IP-aware systems, devices, and/or products on VA's infrastructure network including, routers, firewalls, and IDS/IPS and are intended to be similar for all OMB mandated inventory upgrade/refresh efforts across VA.

There will be a regular status meeting between VA's IPv6 Transition Office and those responsible for conducting the inventory upgrade, as well as key stakeholders or system/program managers. Status reports will include:

- Breakdown of system, device and/or product status ensuring borderline items are clearly identified.
- Updated costs estimates or expectations related to funding.
- Identification of areas that require special attention and/or escalation.
- Verification that transition milestones are met.
- Documentation of all milestones, tasks and progress.

For IP-capable devices, particularly those devices closely tied to security, there must be a mapping that the IPv6-capable device will sufficiently meet agency and federal security requirements. A system, device and/or product should not be considered IPv6 capable if it does not provide an acceptable level of security with IPv6 enabled.

7 IMPLEMENTATION STRATEGY

The implementation strategy for VA infrastructure IPv6 enablement will be refined in future revisions of VA's IPv6 Transition Plan.

7.1 INFRASTRUCTURE DEFINITION

From the enterprise architecture perspective, the infrastructure consists of the facilities, services, and network devices needed for data communication among VA communities. For IPv6 planning purposes, VA's infrastructure include all network components contained in the core, distribution, and access levels, as shown in Fig 1 and the following more detailed conceptual view (Exhibit 7).

Corporate data centers connect via distribution nodes to the core layer. Connection to the external Internet is via the secure enterprise internet gateways that operate in the core layer. All other VA connections, from Veterans Health Administration, Veterans Benefit Administration, and the National Cemetery Administration, are via distribution nodes at the access layer. Distribution nodes consist of a pair of routers, one of which is carrier-managed and the other VA-managed on a regional basis.

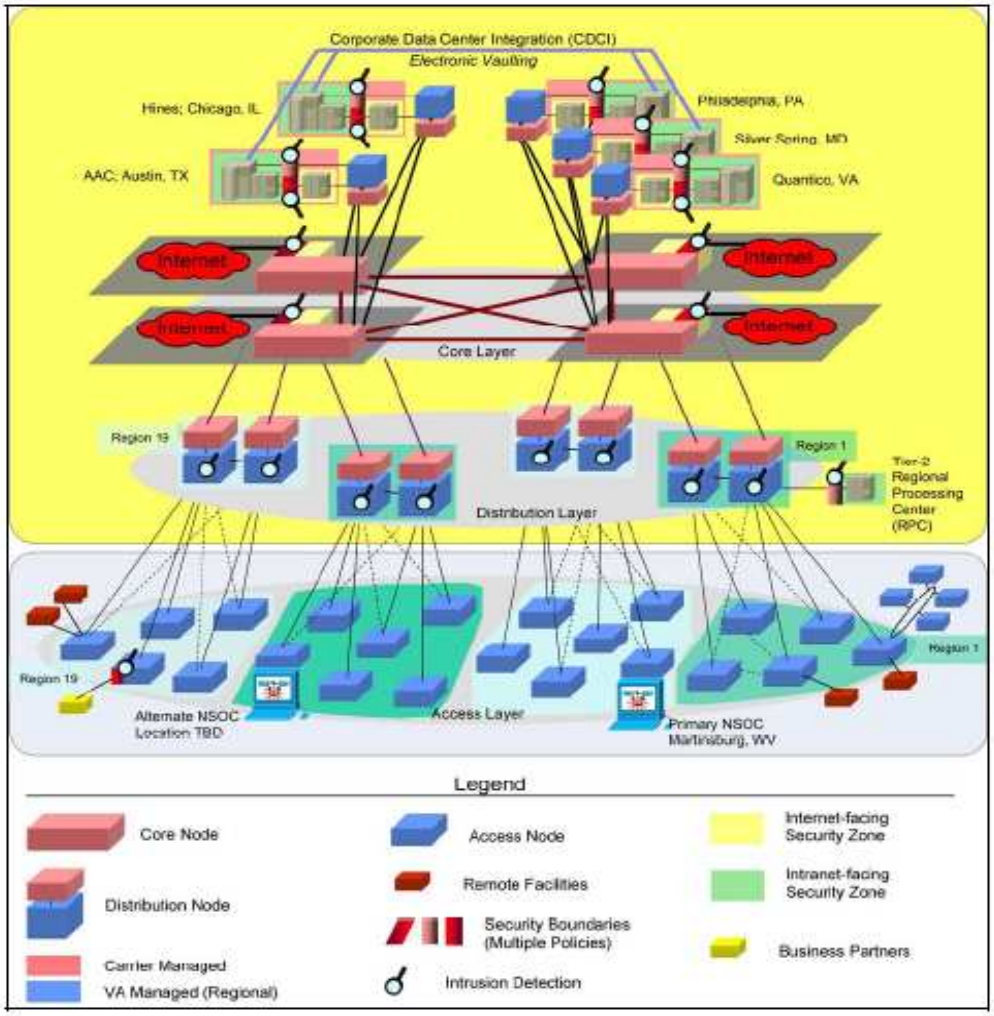


Exhibit 9. VA Infrastructure Concept Illustration

7.2 STRATEGY SELECTION

Three methods were considered by VA's Transition Working Group to determine the preferred or best practice approach for enabling IPv6 on VA's infrastructure, which are:

- Dual-stack – a mechanism by which both Ipv4 and IPv6 run concurrently
- Tunneling – IPv6 packets are encapsulated within IPv4 headers allowing them to be transported across and IPv4 network
- Translation – a means of converting IPv4 packet to IPv6 and vice versa

Each transition strategy has corresponding advantages and disadvantages in the areas of performance, security and cost. Of the three methods, VA has selected dual-stack as the preferred method, followed by tunneling (hardened secure mode) during deployment or where dual-stack isn't possible. Translation will only be considered as last resort,

since the use of NAT breaks the security international standard organization (ISO) model.

Primary considerations in selecting dual-stack are:

- Security
- Forward and backward compatibility
- Level of effort required (including Training relevant required Certifications)

In a dual-stack environment IPv4 and IPv6 protocols coexist and are supported by IPv6 compliant OSI level 3 devices such as routers. Dual-stack is considered the most practical mode, providing a return on investment over the course of time and will eventually reduce the level of effort related to operations. Dual-stack is considered best practice by multiple sources.

IPv6 deployment will be a multi-year process. During the transition, tunneling may be used for several years. Tunneling IPv6 over IPv4 transport will initially be the most common technique. Over time, tunneling IPv4 over IPv6 transport will become more prevalent. When a tunnel is implemented, proper data security review processes must be followed.

Translation is discouraged except where absolutely required for short-lived critical situations. Translation typically requires breaking the internet protocol end-to-end transparency model and minimally adds the same level of complexity as network address translation. Translation should only be considered for use at the network edges and not the core, if determined as the only possible solution.

7.3 INTEGRATED REQUIREMENTS DESIGN (IRD)

The OEAM must prepare and continually update the Integrated Requirements Design (IRD) for VA as a perpetual and working document. This will be key critical to future success with any phase of implementation for IPv6 in VA.

At a minimum, the level of effort will include activities to:

- Conduct technology readiness assessments.
- Incorporate elements of this Plan into VA Enterprise Architecture Plan.
- Provide architectural and engineering reviews.
- Integrate requirements across VA.
- Develop engineering design specifications that meet interoperability, IA, and information exchange needs of VA.

7.4 SECURITY INFRASTRUCTURE

According to VA's Future Architectural Vision (One-VA), VA's Transformation to IPv6 will eventually provide a complete IPv6-capability across VA Intranet and onto the Internet.

The practical utilization of IPv6 at this time is expected to result for the implementation of MS Windows Server combined with the desktop MS Vista client upgrade. With these two conditions being met, there will be a greater potential application of functionality.

Additionally, once in place, IPv6 expanded addressing will provide the ability to establish positive veteran authentication with non-repudiation to the application level, as well as the ability to identify client location information. This will provide opportunities for expanded telemedicine with HIPAA compliance privacy, IA, and other security concerned directly with the veteran at home.

To realize this vision of IPv6 capability in VA, adequate security infrastructure must be in place and manageable to assure an acceptable level of security risks at all times. The current benchmark for this risk posture is the current One-VA WAN and Enterprise Cyber Security Infrastructure Project (ECSIP) Gateway. These were last certified and approved to operate in 2005.

In achieving this objective, firewalls must support the same level of packet inspection in IPv6 as for IPv4 at the same performance levels. In addition, special attention and consideration must be given to extension headers, which are not present in IPv4. Additionally, all network security devices, including intrusion detection and prevention and virus protection products, must provide adequate protection for VA's infrastructure. These types of products must compensate for the additional threats and vulnerabilities associated with the introduction of IPv6 and adhere to the evolving certification standards now in draft maintained by NIST.

7.5 IP ADDRESSING

The composition of addresses will change significantly, and it is unlikely any number will be easily remembered, such as the IPv4 example 10.63.45.3 address.

7.5.1 IPv6 ADDRESS SPACE

Address space is issued and controlled by the American Registry of Internet Numbers (ARIN).

VA requested and received the IPv6 address range beginning at:

2610:00D8:0000:0000:0000:0000:0000:0000

and ending at:

2610:00D8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

The above-abbreviated form is: 2610:D8::/32

ARIN has reserved a /29 IPv6 address block beginning at IPv6 address 2610:D8:: and ending at 2610:00D8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF which will allow allocation of seven additional /32 blocks adjacent to the 2610:D8::/32 to be allocated to VA as needed and requested *[R6]*.

7.5.2 IPv6 ADDRESSING STRATEGY

VA's IPv6 address space will be partitioned as later detailed. An assumption is that the largest prefix that will be constructed is a /64 block. This reflects the best practice noted by the IETF.

Based on discussion within the Registry and Addressing working group, some preliminary concepts have been drafted as follows:

- VA provides for 4,294,967,296 /64 subnets; the amount of address space available to VA for defining networks is equivalent to the entire IPv4 address space for hosts.
- Of 4 possible /34 blocks, one /34 block (representing 1,073,741,824 possible /64 subnets) will initially be available for allocation.
- The remaining /34 blocks or 3,221,225,472 /64 subnets will be reserved for future use. This will support network growth, enabling applications that are not yet defined, and future renumbering requirements.
- The unreserved /34 block will be used to allocate eight /37 blocks, four will support VA "super-regions" and one will support addressing for VA's infrastructure network. Each /37 block can support 134,217,728 /64 subnets. Three /37 blocks representing 402,653,184 /64 subnets will be reserved for future use.
- Eight /40 blocks, each representing an autonomous system (AS)/region will be allocated from each /37 super-region. With 4 super-regions, there will be allocations for 32 "regions." With /37 blocks allocated for 7 super-regions (one /37 block is allocated to the region), it will be possible to support 56 AS/regions.
- It will also be possible to allocate 256 /48 blocks within each AS/region each allocated to a facility. The initial allocation to a facility will be a /52 block. Each facility will be able to allocate 4,096 /64 subnets within its local network.

VA shall standardize addressing format for network devices with differing profiles. Standardized address blocks shall be assigned for virtual LANs (VLANs) supporting classes of specific network devices that have varying security requirements. The current visualization is having VLAN/subnets that uniquely identify network devices with specific security requirements, which will allow WAN support personnel to easily identify them.

If a facility requires more than one subnet to support each VLAN type, the facility shall request these additional subnets from the national IPv6 addressing organization. These additional networks shall be recorded in a database that WAN, NOC, engineering, operations and security personnel shall have access to.

The following 16 different VLAN types were identified at the addressing planning workshop. More may be identified as they are defined.

- BCMA – bar code medication administration (wireless)
- Network devices – switches
- Imaging – Vista
- Video Conferencing
- VoIP
- Workstations
- Multifunction devices
- Printers
- Thin clients
- Servers – global
- Servers – local
- ECSIP Devices
- NOC Devices
- VBA – isolated because they are excluded from VHA security requirements
- Wireless
- Private groups – to be determined

The first instance of a VLAN subnet supporting a specific network device or security demarcation shall be identified identically across VA (using some bit arrangement in the /52-/64 address space allocated to a facility). The national office shall maintain a database of assigned VLANs for requests from facilities for additional VLANs/subnets.

7.5.3 ADDRESS MANAGEMENT

With this addressing plan, a large number of addresses are being reserved for future use. A process will need to be developed to manage address assignments, including the following functions:

- Allocate top-level address blocks to organization units.
- Distribute addresses within assigned blocks to sub-organizations, networks and devices.
- Return unneeded address blocks to the address management authority.

7.5.4 DOMAIN NAME SERVICE (DNS)

All DNS devices on VA's network will, at a minimum, support IPv4. It may be possible to use the existing IPv4-enable DNS infrastructure to support the DNS requirements of

dual-stack devices deployed on VA's infrastructure network. The DNS servers currently implemented on the infrastructure network and at VA ESCIP gateways support resolving IPv6 address records (AAAA records) and reverse address records, as well as adding these IPv6 address specific records to the DNS database. Existing DNS servers are sufficiently configured to support VA's infrastructure network IPv6 deployment, however other factors poise consideration.

In most instances, DNS will *overlap*, although in some instances must be considered in *parallel* with:

- Firewall – method, provision, type
- Packet Inspection
- Intrusion Detection System
- Intrusion Prevention System

Due to the risk associated with reverse look-up, additional consideration is believed to be appropriate with regard to DNS in VA. Additionally, the approach to manage DNS in the same manner to that of an IPv4 only environment; may not be the best or even possible.

7.5.4.1 Proposed IPv6 Addressing Guidelines

Nodes that are to only be reachable inside of a site:

- These nodes will be manually or automatically configure with Local IPv6 addresses. They will not be assigned IPv6 global Unicast addresses.
- The local DNS should be configured to include the Local IPv6 addresses of these nodes.
- Nodes with only Local IPv6 addresses must not be installed in the global DNS.

Nodes that are to be reachable from inside of the site and from outside of the site:

- These nodes will be manually or automatically configured with global addresses. They will not be assigned Local IPv6 addresses (for simplicity)
- The local DNS should be configured to include the global addresses of these nodes.
- These nodes should also be installed in the global DNS.

7.5.4.2 Proposed IPv6 Implementation Guidelines

Configure your internal name servers should be configured to forward queries that can't be resolved to the external name server. Your external DNS records are configured to contain only a small zone file for your domain, listing things such as Web and File Transfer Protocol (FTP) server addresses and any server addresses you want to publish to the world. Your internal servers hold only the DNS records for your internal networks. When internal users look up host names, the query is answered by internal DNS servers, even if the request is forwarded to an external DNS server for resolution. Internet users who look up host names in your domain are answered by external DNS servers that only know about the publicly accessible resources.

7.5.5 ROUTING

IPv6 routing will function independently of IPv4 routing. VA can decide to implement an IPv6 routing infrastructure that is identical to the IPv4 routing infrastructure, but there is no technical requirement that it actually be identical. During the transition, and because the IPv6 routing infrastructure will not have been completely built-out, it is not expected that IPv6 routing will be the same as with IPv4 routing, but the goal will be to have IPv4 and IPv6 routing the same, to the extent possible.

It is not expected that IPv6 routing will have any impact on the IPv4 routing, although this must be monitored and ensured.

Since the IPv4 and IPv6 routing tables will operate independently of each other, there will be no technical reason why generalizations about one internet protocol routing table or implementation can be applied to the other, and additionally the structural composition of each remains different.

There are some significant differences in the behavior of the IPv6 routing system, compared to IPv4. First, the global IPv6 Internet is still of less size currently than that of the IPv4 Internet, although IPv6 continues to grow and expand daily. This imbalance poses complexity in comparison of IPv6 routing to that of IPv4. Additionally, IPv6 routing presents two characteristics that must be addressed and resolved by VA during the IPv6 transition.

- Network interfaces with multiple global IPv6 addresses are prone to asymmetric routing, which is often undesirable. This is mostly due to improper implementation of source address selection.
- The IPv6 Internet is still largely approached as an overlay network over IPv4 and IPv6 tunnels distort the inter-area link metrics (number of hops in AS paths) and mislead routing algorithms.

Both issues are expected to diminish over time when native IPv6 routing has become ubiquitous and the address selection has been properly implemented per IETF recommendations. During the interim period, one has to exercise adjustments and avoidance such as permitting only the Unicast address with the broader scope (global site) to be assigned to each interface as necessary.

7.5.6 NETWORK MANAGEMENT

The approach to identification, management and mitigation of IPv4 and IPv6 traffic issues must be determined. Some probable occurrence scenarios are:

- IETF IPv6 management standards equivalent to IPv4 management standards have not been defined or implemented in VA infrastructure network devices.
- IPv6 management standards equivalent to IPv4 management standards have been defined, but the equivalent functionality is not available on an IP-capable device.
- Vendor-specific IPv6 management standards equivalent to IPv4 management standards have not been defined by the vendor.

- The vendor has not implemented vendor-specific IPv6 management standards on all platforms and operating system releases.
- Technical support by vendors is lacking or not available.

VA's IPv6 implementation must identify what features are IPv4-specific and identify the IPv6-specific equivalent(s) that can also be implemented using common standards.

- IPv6 network management must be addressed in terms of fault, configuration, accounting, performance, and security functions. Network connectivity to support these functions can be on IPv4 for a foreseeable future and ultimately migrate to IPv6.
- As it is with routers, all measurement devices must ensure the ability to sustain IPv6 traffic, such as network probes, packet filtering, etc.

7.5.7 NETWORK MEASUREMENT

IPv4-based measurements and metrics on the production VA infrastructure must likewise be implemented with IPv6. The measurements and metrics noted with VA EA include specific measurements combined with a guarantee of measured service(s).

Periodic stress-testing, such as throughput capacity measurements completed on the infrastructure network using IPv4-based traffic, must also be accomplished using IPv6-based traffic. It must be ensured that both IPv4 and IPv6 measurements which stress-test the infrastructure network do not impact or degrade the infrastructure capability in processing of production network traffic; likewise, it must be ensured that one does not impact, degrade or cause interference with the other. Automatic mechanisms could be in-place to ensure that stress testing does not occur on infrastructure network links that are already reaching capacity, by re-routing, etc. Mechanisms could be to transmit measurement traffic classified as Less than Best Effort (LBE) where measurement traffic would be given lower priority than that of normal production traffic on the link.

7.5.8 MANAGEMENT TOOLS

In conjunction with efforts noted in the previous Network Measurement section; it is essential that management data is collected regarding IPv4 traffic and IPv6 equivalents, and that each can be measured by the management tools.

COTS or GOTS tools that could be evaluated for this purpose include:

- Cisco Works
- Hewlett Packard OpenView
- IBM Tivoli
- Brix Networks

Open source tools that could be evaluated include:

- AS-path
- IPFlow
- Mping

- Argus
- Ethereal/Wireshark

8 ASSURANCE – POLICY – GUIDANCE

The addition of the IPv6 communications protocol to those available on VA's infrastructure is considered an enhancement to the current capability that includes IPv4. It should not be necessary to conduct a full C&A review. According to NIST however, a partial C&A is required, which must address the components and elements and/or systems or devices that change, and risks mitigation and safeguards must be included.

IA is also a federally required element for concern and consideration, which stipulates that a standard must be achieved and maintained, providing an acceptable level of exposure, access and authorization which is necessary and related to the integrity of data and information accessed, transferred, or stored in VA. The IA program in VA continues to provide a host of training and compliance means and measures through VA's OCIS web site link.

8.1 DEVICE CONNECTIVITY

Prior to the completion of IPv6 testing and the upgrade of VA network infrastructure to IPv6 by June 2008, VA seeks to control the connection of IPv6 capable devices to the network.

To accomplish this, a memorandum has been prepared for circulation to VA staff requiring CIO approval prior to the connection of any IPv6 enabled device to VA's network infrastructure.

The process for obtaining CIO approval includes the following steps:

1. Requestor must prepare a written request to connect an IPv6 device/software to VA network. The request should describe the following:
   - The device or software to be put on VA's network
   - Where on the network the device/software will reside
   - When and for how long the device/software will remain on the network
   - The reason the device/software needs to be connected to the network
2. The requests will be reviewed by the IPv6 Transition Office and other areas, such as Security and the NOC. Approval or disapproval of any request will be granted based on feedback from the reviewers.

8.2 VA DIRECTIVES

Future VA Directives, including VA 6500 Directive Information Security Program, will contain portions, elements, or specific information deemed necessary as it pertains to IPv6 security and security related provisions. Supplemental VA Handbooks, which address specific elements, composition and security measures, are also being developed.

8.3 CIO COUNCIL GUIDANCE

According to the Federal CIO Council Architecture and Infrastructure Committee, as well as other federal guidance, agencies "are required to conduct risk assessments and develop security plans in accordance with the Federal Information Security Management Act (FISMA) and as required by national security policy, OMB policy and in accordance with NIST standards and guidance as necessary *[R5]* ." For IPv6, the existing network risk assessment and security plan are being updated to reflect changes made to implement the additional protocol.

8.4 ASSESS SECURITY POSTURE

The following steps will be followed when assessing security posture:

- Identify existing IPv4 security baseline
- Document changes due to IPv6 capability
- Demonstrate maintenance of the security baseline

8.5 UPDATE SECURITY PLAN

The security plan for the existing IPv4 network will be reviewed and updated as required. Topics of relative and specific concern with IPv6 include the following:

- Network architecture
- Interconnection policy
- Security controls
- Security devices and settings
- Operations and maintenance policies and procedures
- Administrative and technical policies and procedures

8.6 SECURITY RISK ASSESSMENT

The following will be used to determine, identify and address the risks over and above those identified for the IPv4 network.

- Identify assets – these are the additional assets required with IPv6
- Identify vulnerabilities – these are additional network vulnerabilities caused by or as a direct result of IPv6
- Identify threats – these are any additional threats pertaining to the IPv6-enabled infrastructure
- Determine effects of threat to vulnerability ratio – assess the potential for all identified or known threats to exploit the additional vulnerability and the probability of an occurrence
- Prioritize high risks – rank the risks from the threats, vulnerabilities, and likelihood of occurrence in order of importance
- Accept, transfer, or mitigate the high priority risks – mitigation may be accomplished by upgrading existing security controls such as firewall and

intrusion prevention systems, or by adding additional security controls, such as router-to-router authentication

Based on the risk assessment, identify any additional security controls that should be in place.

8.7 MAINTAIN SECURITY DURING TRANSITION

During the transition to IPv6 on VA's infrastructure, the security posture will be in a state of flux. Initially, a very small cross section of VA's enterprise infrastructure will be enabled. Security will be maintained during transition through the following strategies:

- Prevent unauthorized access to the IPv6 network
- Control authorized use of the IPv6 network during the transition
- Use IPv4 only for production traffic until such time that security provisions are deemed adequate with IPv6
- Monitoring presence of IPv6 traffic

8.8 MAINTAIN IPv4 PRODUCTION NETWORK FUNCTIONALLY

The current IPv4 production network will continue to be monitored, measured and maintained with at least the same level that is currently in place. When situations permit such service trials, inject slight loaded IPv6 scenarios and observe the network performance as part of the testing.

9 TEST PLAN

VA's IPv6 Test Plan will be provided as a separate document, although the principles contained herein will be followed.

The primary objective of this testing was to verify proof-of-concept for network configurations to support the documented demonstration of functions described by the CIO Council. These have been previously noted in this document, which are:

- Transmit IPv6 traffic from the Internet and external peers, through the network infrastructure (core), to the LAN.
- Transmit IPv6 traffic from the LAN, through the network infrastructure (core), out to the Internet and external peers.
- Transmit IPv6 traffic from the LAN, through the network infrastructure (core), to another LAN (or another node on the same LAN).

Exhibit 10. Specific Required Testing Functions

There are also three types of testing that can be performed:

- Testing to assess a system, device, product and/or service IPv6 capability relating specifically to performance and interoperability in a controlled environment
- Field evaluation of equipment and/or configurations in a test lab environment
- Pilot implementation

The proposed VA IPv6 Testing Plan involves a specific segment of VA's enterprise infrastructure, and will represent the entire VA enterprise suite of devices and products currently in place, which will result in verification as proof-of-concept, and provide demonstration of success with captured and pre-defined performance measures and results.

A VA IPv6 Test Plan has been provided and was approved by the CIO along with all associated efforts, documentation and implemented measures for safeguarding data and information. It will do the following:

- Establish a coordinated approach to test and evaluation in support of the transition to IPv6.
- Identify key IPv6 issues to resolve through testing, and identify the strategies for addressing those issues.
- Promote efficient use of resources.
- Define a process to consolidate and evaluate test results.
- Identify areas where further testing is needed.
- Continue to seek optimal use of IPv6 in providing or meeting mission requirements.

Although testing will provide a means for VA personnel to gain experience, exposure and familiarity with IPv6, a comprehensive VA IPv6 Training Plan is anticipated to better serve in meeting this need. Additionally, it is anticipated that over a span of time, the Training Plan will provide exposure, familiarity and experience in the most efficient manner possible for a select category of personnel with varied responsibility and levels of training, who will become involved with IPv6 as a matter of day-to-day responsibility.

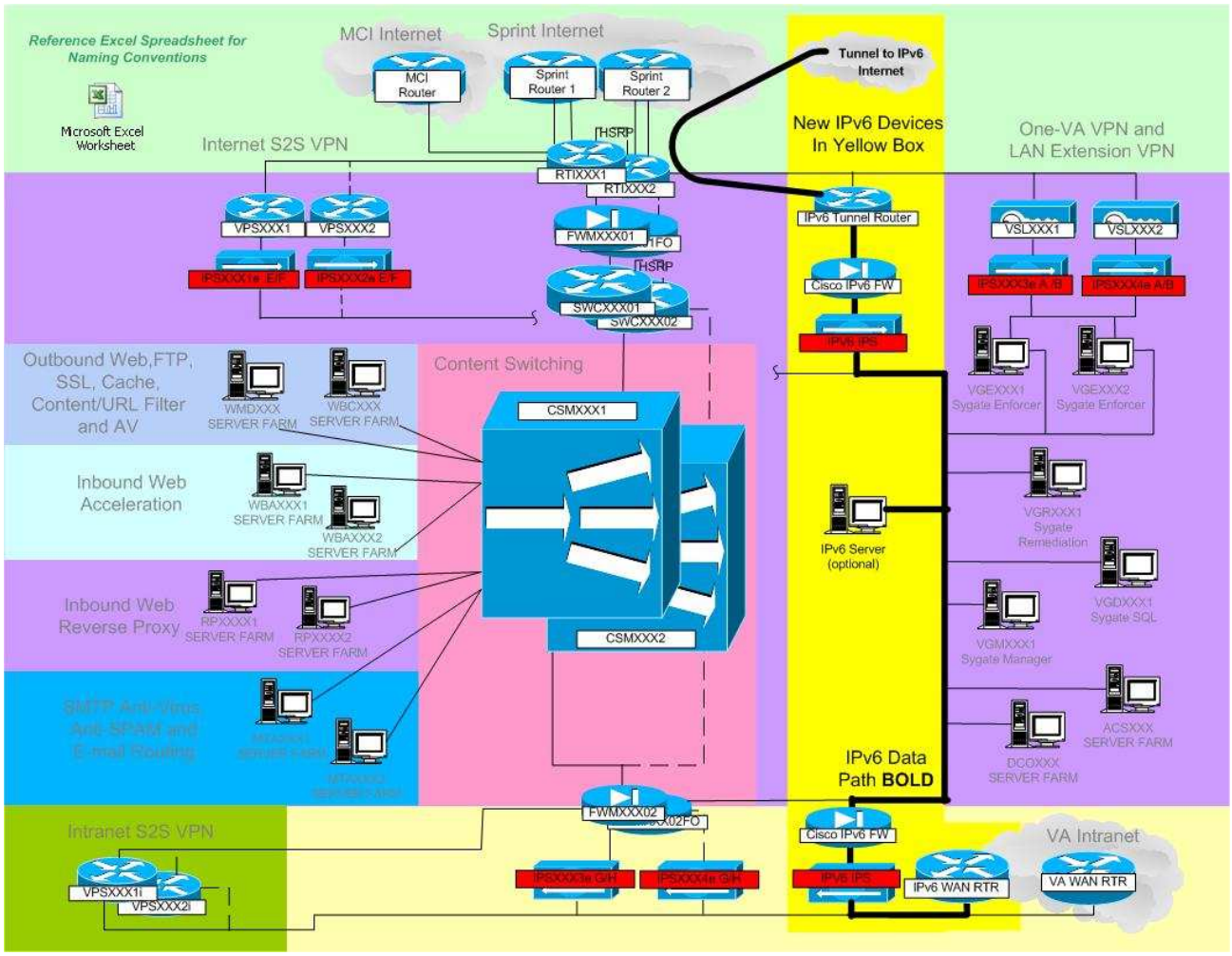


Exhibit 11. VA Enterprise Infrastructure IPv6 Testing Path

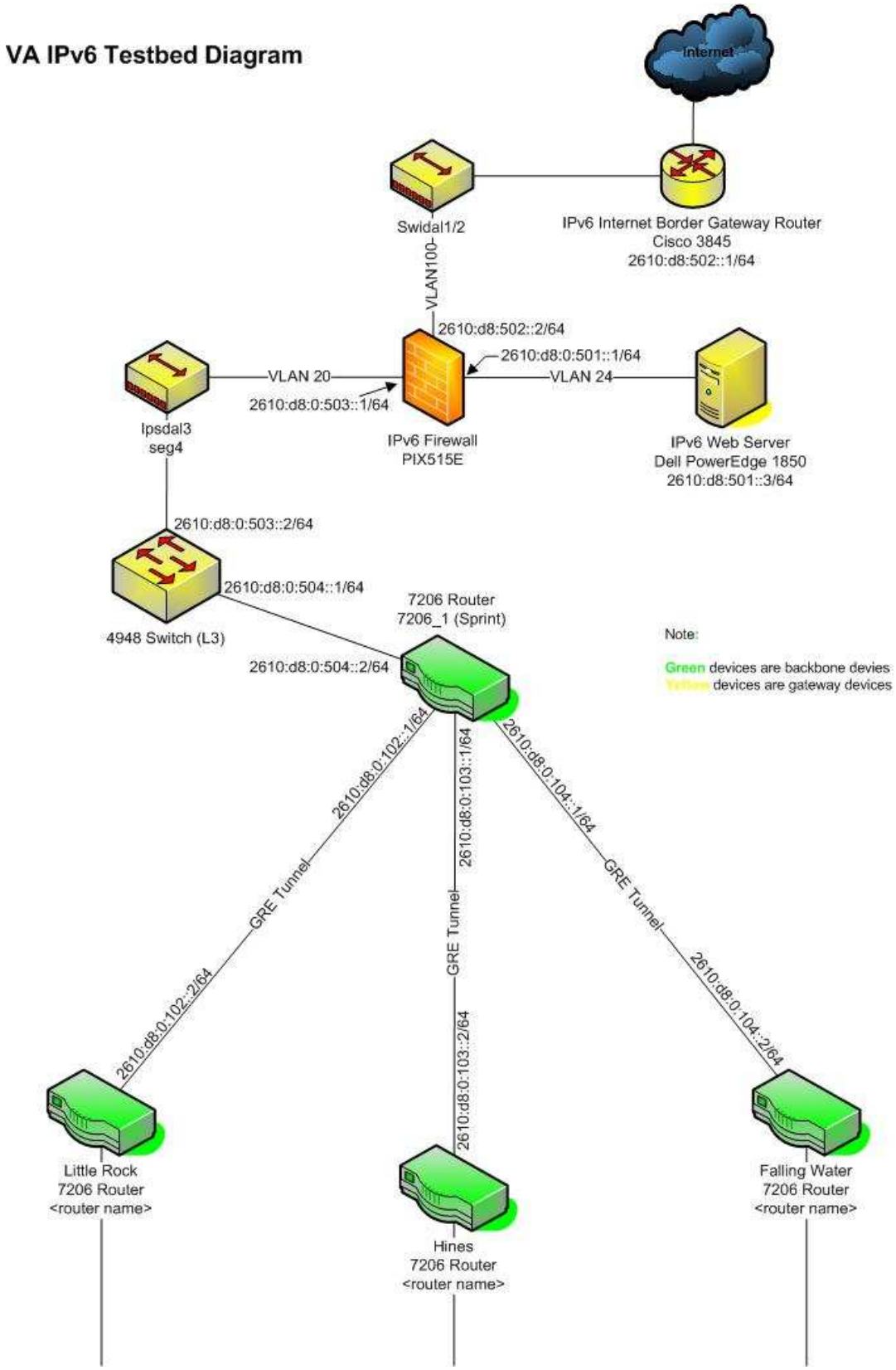


Exhibit 12. VA IPv6 Testbed Diagram

10 TRAINING PLAN

10.1 BACKGROUND

VA recognized that IPv6 is a new technology and training of technical personnel is a key component of a successful transition.

VA's training working group started planning early in the process with a survey of the technical community to determine what potential audiences exist within VA. As a result of the survey, three target populations were identified.

- Architectural population: Enterprise Architecture personnel, Network Managers, Technical Managers, Telecommunication Managers, Security Managers
- Operational population: Network Engineers, Network Specialists, System Developers, Telecommunications Specialists, Support personnel (This class involves hands-on laboratory sessions.)
- General population: Management and Users. A general introductory IPv6 video has been produced and is available on VA's Knowledge Network located at http://vaww.sites.lrn.va.gov/vacatalog/cu_detail.asp?id=23411 .

10.2 TRAINING OFFERINGS

Training will be conducted by a training vendor and will meet the needs of both technical and non-technical VA personnel in five different phases:

- **Train-the-trainer:** Training was initially presented in the traditional "train-the-trainer" format. Selected VA personnel were trained in order to present the material to VA personnel in the field.
- **Architectural:** The architectural training is comprised of both theory and demonstrations, and is being developed specifically for technical VA personnel who will not need "hands-on" technical instruction. The expected enrollment in this course is 25. The classes in this phase will be video taped or recorded on DVD for use as a future training tool.
- **Operational:** The operational training comprises "hands-on" technical instruction, and includes both theory and hand-on exercises. This course is specifically designed for technical VA personnel. The expected enrollment in this is 11-13. The classes in this phase will also be videotaped or recorded on DVD for use as a future training tool.
- **Specialized:** Some employees may require training in appliances which run on various operating systems and applications. In these cases, the course content of the primary training may not address this need, and specialized training may need to be developed by VA personnel who have been trained and certified.

- **General:** The video training mentioned above will be conducted by in-house personnel who have received IPv6 Certification after completing the previously-mentioned train-the-trainer instruction. This training will be presented to VA personnel and may be tailored to different VA audiences. This training will be presented on video, DVD, or web based.

Course content will consist of technical as well as administrative topics.

10.3 VA IPv6 CERTIFICATION

As a component of the training, participants will be required to pass an evaluation in order to obtain certification with IPv6. Certification requirements are listed below. During the initial phase of training (train-the-trainer), the certification exam will be designed and administered by the training vendor. Subsequent training and exams will be administered by those certified VA personnel who attended and passed the train-the-trainer course.

10.4 THE CERTIFICATION PROCESS

A major component of the training is an examination taken by the IPv6 course participants. Participants will be certified in IPv6 methodology when they pass the examination. All VA personnel must be certified to be allowed to work with VA IPv6-enabled equipment and the network.

The training vendors will conduct at least one trial class for selected VA personnel. This class will be the pilot for the certification process, and will use an evaluation methodology approved by VA. The certification examination will be designed using input from participant and trainer evaluations, and participant and trainer round-table discussions.

VA personnel who attend and pass the course will be certified. The training vendor and those VA-certified personnel will conduct all subsequent phases of the course.

10.5 TRAINING REQUIRED

The transition from IPv4 to IPv6 requires training for network engineers, network administrators, security professionals, application developers, and business managers. The IPv6 challenge is to incorporate IPv6 training efforts into current VA and component and joint training programs, without creating redundancies. A list of the technical training topics is included in Appendix D.

Training is essential for the successful transition to IPv6. IPv6 contains an extended feature set, the implementation of which is still in the development stage. The current business model, which relies heavily on protecting the network with such equipment as intrusion detection devices and firewalls, requires re-engineering. These devices will require technology refreshes, and the respective administrators will require training and certification on the new technology.

Before IPv6 implementation can begin, the appropriate VA personnel previously identified by category, need to be IPv6 trained. All VA IT and Telecommunication staff should familiarize themselves with IPv6 prior to formal training to help determine and

identify which personnel need which type of IPv6 training. Training needs will be diverse and will likely be complex. For example:

- Systems managers must learn how to configure and manage IPv6 on network devices and upgrade servers to IPv6.
- Program managers and acquisition executives will need information in order to evaluate and purchase IPv6 capable products and services.
- Software developers will need to understand the impact of IPv6 on existing applications to select co-existence mechanisms.
- Network managers and operators will need to thoroughly understand IPv6 operations, routing in IPv6 networks, and network services such as DNS and Dynamic Host Configuration Protocol (DHCP).
- Those responsible for IA will require information on IPv6 security vulnerabilities.

10.6 TRAINING SCHEDULE

The following training has been scheduled. Regional Chief Technology Officers (CTO's) will identify 20 individuals (10 for the Architectural class and 10 for the Operations hands-on class) from their region to participate. Regions 1 and 2 will be given first priority for the classes in Salt Lake and Regions 3 and 4 will be given first priority for the classes in the Washington, DC area.

Training Type	Date	Class Size	Duration	Location
Architectural Pilot Class	10/23/07 – 10/26/07	20	3 ½ Days	Washington, DC
Operational Pilot Class	01/28/08 – 02/01/08	20	5 Days	Washington, DC
Architectural Class	2/12/08 – 2/15/08	20	3 ½ Days	Salt Lake City OI Field Office
Operational Class	2/18/08 – 2/22/08	20	5 Days	Salt Lake City OI Field Office
Architectural Class	3/4/08 – 3/7/08	20	3 ½ Days	Herndon, VA (Washington, DC area)
Operational Class	3/19/08 – 3/14/08	20	5 Days	Herndon, VA (Washington, DC area)
Security Issues	Week of 5/12/08	TBD	TBD	VA InfoSec 2008
TBD	Week of 07/07/08	TBD	TBD	VA Information Technology Connection Conference

10.7 COURSE DOCUMENTATION

All course material, including training manuals, instructor guides, instructor notes, user guides, video tapes, DVDs, participant evaluations and any other material designed for these training sessions becomes VA's sole property.

11 TRANSITION SCHEDULE

In the original August 2005 memo, "Transition Planning for Internet Protocol version 6 (IPv6)", OMB established June 2008 as the date by which "all federal agencies' network infrastructure must be using IPv6 and agency networks must interface with this infrastructure". Although subsequent guidance softened this requirement, in initial planning, VA's IPv6 working groups committed to and established a goal of March 2008 to meet the deadline. VA met the goal and proved its compliance on March 17, 2008, allowing the additional calendar time to execute bonus multi-agency testing.

VA's IPv6 Transition Schedule identified various aspects depicted at a high level. The Transition working group approved and forwarded the original master schedule plan to VA's Steering Committee, which is responsible for tasks and resources involved in the project. The original plan was only the beginning and was the basis of the Time Line illustrated below. The plan below, while not absolutely complete, starts well after the successful IPv6 network test which met OMB's mandate of June 2008. This Time Line shows the start of an aggressive IPv6 "proof of concept" Pilot Program and continuous activities to enable successful IPv6 deployment. These factors will play a large part in the rapid implementation phase of the future.

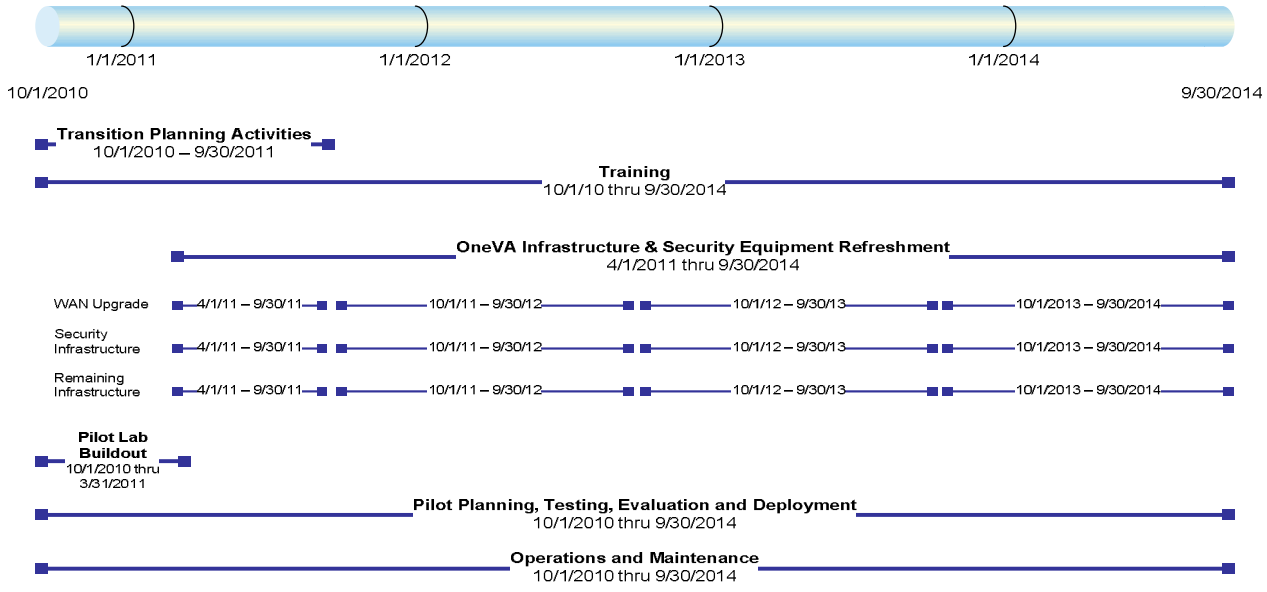


Exhibit 13. VA IPv6 Transition Schedule

12 MILESTONES, ACTIVITIES AND TIMELINES

With careful coordination between all VA activities including VHA, VBA, NCA, and all other VA Programs, the infrastructures that support VA applications will be transitioned from IPv4 to IPv6. The actual transition will be a multi-phased process based on time

and functionality. Transition mechanisms will be installed and enabled, program by program and site by site to provide a core suite of IPv6 functionality.

VA has yet to establish the goal of completing the transition to IPv6 for all VA infrastructure networks, although the initial OMB mandate was met as previously described. Successful transition must consider the diverse and evolving nature of VA internal networks. A successful transition will ensure the necessary IPv6 infrastructure is available, that transition issues are addressed, and that all VA applications will continue to work over IPv6 networks.

VA Enterprise Architecture Version 4.2 provides specific timelines for nearly all VA Programs, and includes target dates for IPv6 capability with each program [R8]. This is the proposed schedule VA will follow in order to carry out an enterprise-wide IPv6 implementation.

APPENDICES

A. Acronyms/Abbreviations List

B. References

C. Transition Mechanisms

D. Technical Training Topics

Appendix A – Acronyms/Abbreviations List

ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASN	Autonomous System Number
ASM	Any source multicast
BCMA	Bar Code Mediation Administration (wireless)
C&A	Certification and Accreditation
CIDR	Classless Inter-domain Routing Protocol
CIO	Chief Information Officer
CM	Change Management
CM	Configuration Management
COTS	Commercial-Off-The-Shelf
CT&E	Certification Test & Evaluation
CTO	Chief Technology Officer
D&T	Development and Testing
DAA	Designated Approving Authorities
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	Domain Name Service
DoD	Department of Defense
DT&E	Developmental Test & Evaluation
EA	Enterprise Architecture
ECSIP	Enterprise Cyber Security Infrastructure Project
EOIP	Ethernet over Internet Protocol
ESCCB	Enterprise Security Configuration Control Board
EUD	End User Devices
FATO	Full Authority to Operate

FEA	Federal Enterprise Architecture
FISMA	Federal Information Security Management Act
FTF	Federal Transition Framework
FTP	File Transfer Protocol
FY	Fiscal Year
GOTS	Government-Off-The-Shelf
HR	Human Resources
IA	Information Assurance
IATO	Interim Authority to Operate
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IHS	Indian Health System
IOP	Interoperability (test and evaluation)
IOS	Internet Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRD	Integrated Requirements Design
ISO	International Standard Organization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LBE	Less than Best Effort
MCSC	Managed Care Support Contractors
MHS	Military Health System
MPLS	Multi-Protocol Label Switching

NAT	Network Address Translation
NCA	National Cemetery Administration
NIC	Network Information Center (also called Domain Name Registry)
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSOC	National Security Operations Center
OCIS	On Call Internet Services
OEAM	Office of Enterprise Architecture Management
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OPSEC	Operations Security
OS	Operating Systems
OSI	Open Systems Interconnection
OT&E	Operational Test and Evaluation
PII	Personal Identification Information
PM	Program Manager
POM	Program Objectives Memorandum
QoS	Quality of Service
RDPC	Regional Data Processing Center
RFI	Request for Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
ST&E	Security Test & Evaluation
VA	Department of Veterans Affairs
VACO	Veterans Affairs Central Office
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration

VISN	Veterans Integrated Service Networks
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B – References

R1. "Transition Planning For Internet Protocol Version 6 (IPv6)," Office of Management and Budget (OMB) Memorandum M-05-22, August 2005.

R2. "Federal Government Transition Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6) Frequently Asked Questions," CIO Council, February 15, 2006.

R3. "Bitpipe" web site, http://www.bitpipe.com/tlist/3G-Wireless.html

R4. Initial descriptive text for VA IPv6 Transition Office has extensively referenced "The Department of Defense Internet Protocol Version 6 Transition Plan (Version 2)," dated June 30, 2006.

R5. "IPv6 Transition Guidance," Federal CIO Council Architecture and Infrastructure Committee, February 2006.

R6. Communication from David Huberman, Technical Specialist, ARIN to Michael Adams, ESIP, VA.

R7. "The Business Case and Roadmap for Completing IPv6 Adoption in US Government", Version 0.1, CIO Council, December 2008.

R8. "Planning Guide/Roadmap Toward IPv6 Adoption within the US Government" Version 0.2, CIO Council, February 2009.

Appendix C – Transition Mechanisms

{Source: DoD/MHS Transition Plan – August 2007}

Transition will introduce IPv6 to existing networks, as well as create new networks using IPv6. It is not anticipated that the transition will be able to occur simultaneously across all systems and networks. IPv6 is not directly compatible with IPv4, which requires that transition mechanisms be put into place to accommodate interoperability between systems that have transitioned with those that have not. There are **three major and one hybrid** transition mechanism under consideration by VA:

- Dual Stack
  - Most versatile
  - High complexity
  - Required through most of the Implementation Phase
- Tunneling
  - Least versatile
  - Low complexity but labor intensive
  - Will likely be deployed during many of the first implementations
- Dual Stack/Tunnel Hybrid (variation of dual stack)
  - Very versatile
  - High complexity
- Translation
  - Currently prohibited by many agencies – as this breaks the security model
  - Medium complexity but requires additional hardware
  - Deployed only as a last resort

DUAL STACK

Dual Stack refers to the capability of a system to support both IPv4 and IPv6 (Figure B-1). When a dual-stack capable system has IPv6-capable connectivity through to a destination dual-stack system, that communication will use IPv6. If that same dual-stack capable system does not have IPv6-capable connectivity or the destination system is not IPv6-capable, that communication will use IPv4. This solution ensures backward compatibility with legacy IPv4-only systems while progressing toward the goal of complete IPv6 transition. The dual-stack approach is key to VA transition to IPv6.

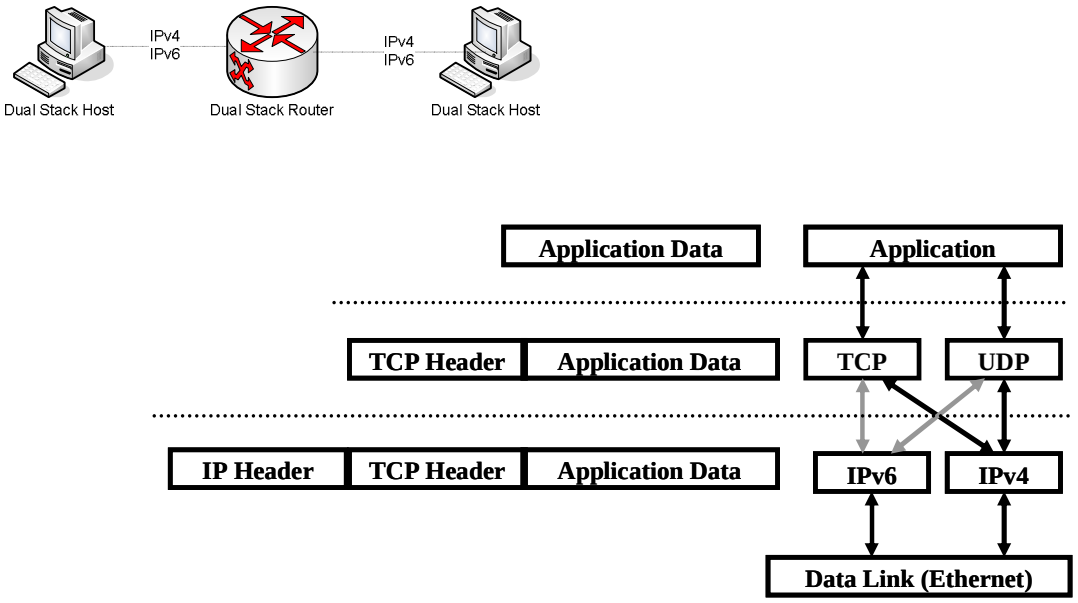


Figure B-1. Basic Dual Stack

A more complete example of dual stack configuration is shown in Figure B-2 below.

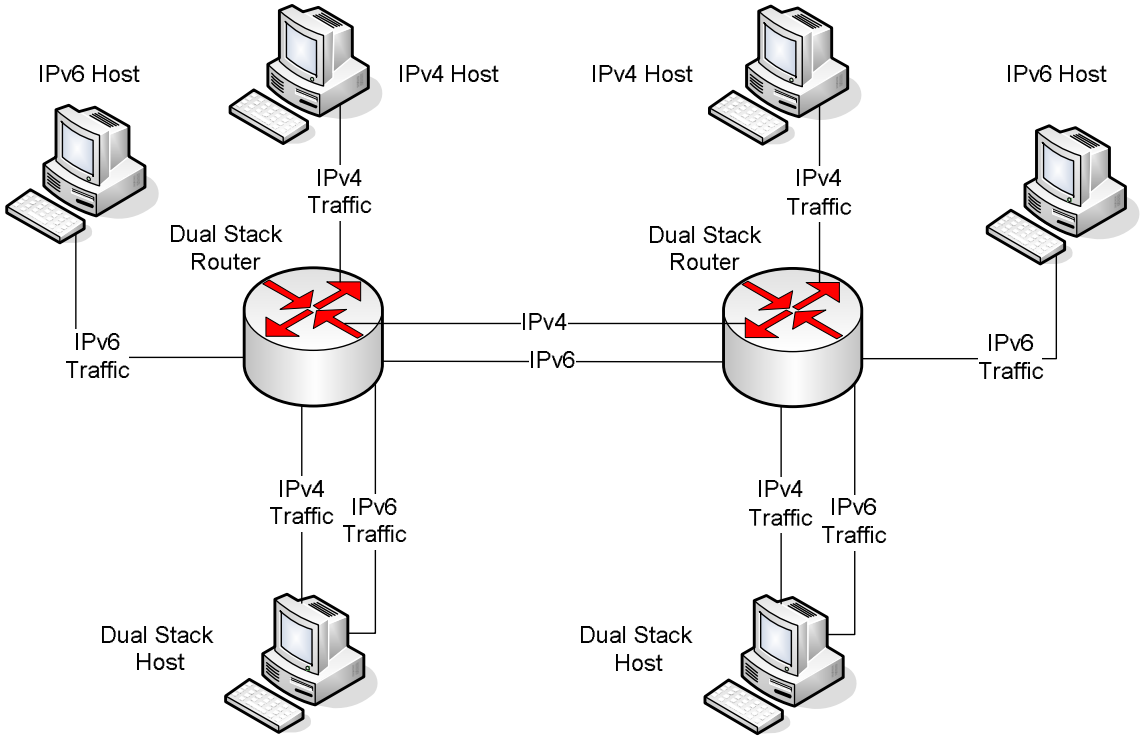


Figure B-2. Dual Stack Example

DUAL STACK/TUNNEL HYBRID

A Dual Stack/Tunnel Hybrid configuration is also possible, as illustrated in Figure B-3 (see following section for a description of pure tunneling). The packets are IPv4 or IPv6 in the LAN and the architecture supports IPv4, IPv6 and dual stack hosts, but requires dual stack interior routers. IPv6 packets are tunneled through the core with no impact on existing IPv4 core infrastructure, but the edge router must support dual stack and tunnels. This configuration is used to implement DoD MO2 IA architecture (enclave-to-enclave) and supports all stages of the MHS IPv6 Implementation Phase (through FY15).

Difficulties with this architecture include: shared infrastructure must support two protocols, additional CPU and memory overhead may impact application performance, may require upgrade of existing hardware and software, and is labor intensive for large numbers of tunnel end-points.

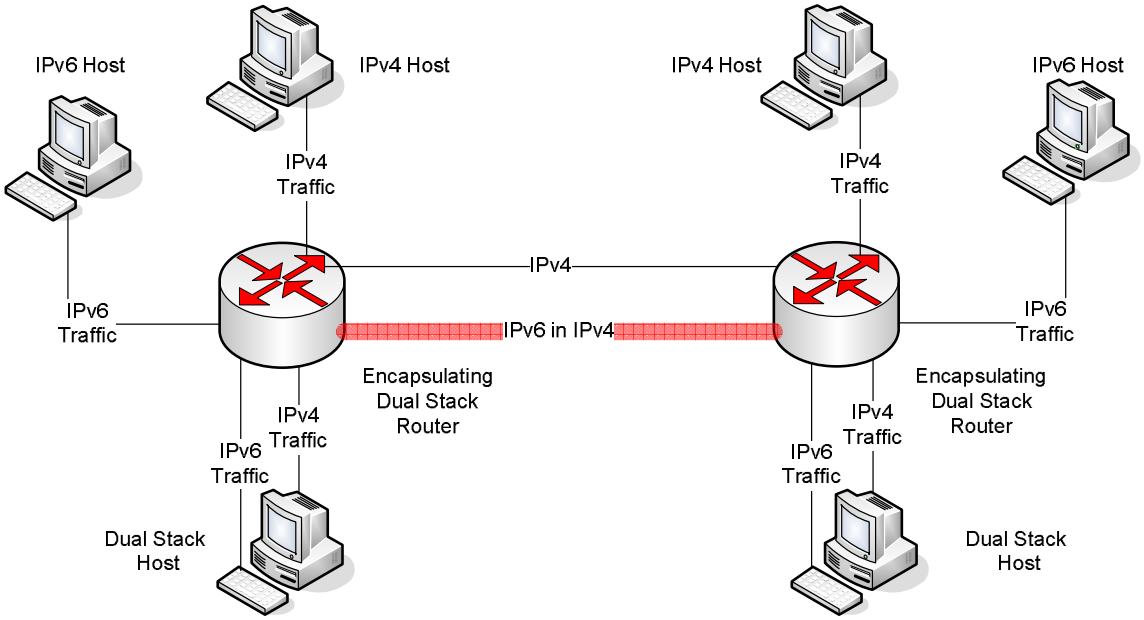


Figure B-3. Dual Stack/Tunnel Hybrid

TUNNELING

An IPv6 island is a network made of IPv6 links directly connected by IPv6 routers. In the early days of IPv6 deployment, there will be many IPv6 islands. IPv6 in IPv4 tunnels are used to connect those islands together. In each island, one (or more) dual stack routers are designated to encapsulate and decapsulate IPv6 packets within IPv4 packets. Tunneling is a transition mechanism designed to accommodate an environment in which end systems running one version of IP must communicate through a network that is running a different version of IP (Figure B-4). For environments where there is a community of end systems running IPv6 that must communicate with each other through a legacy IPv4 network, 6-4 Tunneling would be used. On the other hand, for environments where there is a community of end systems

running IPv4 that must communicate with each other through a new IPv6-only network, 4-6 Tunneling would be used. A current example of 6-4 tunneling is demonstrated with experimental IPv6 networks that use the IPv4-only Internet to communicate between IPv6 test sites.

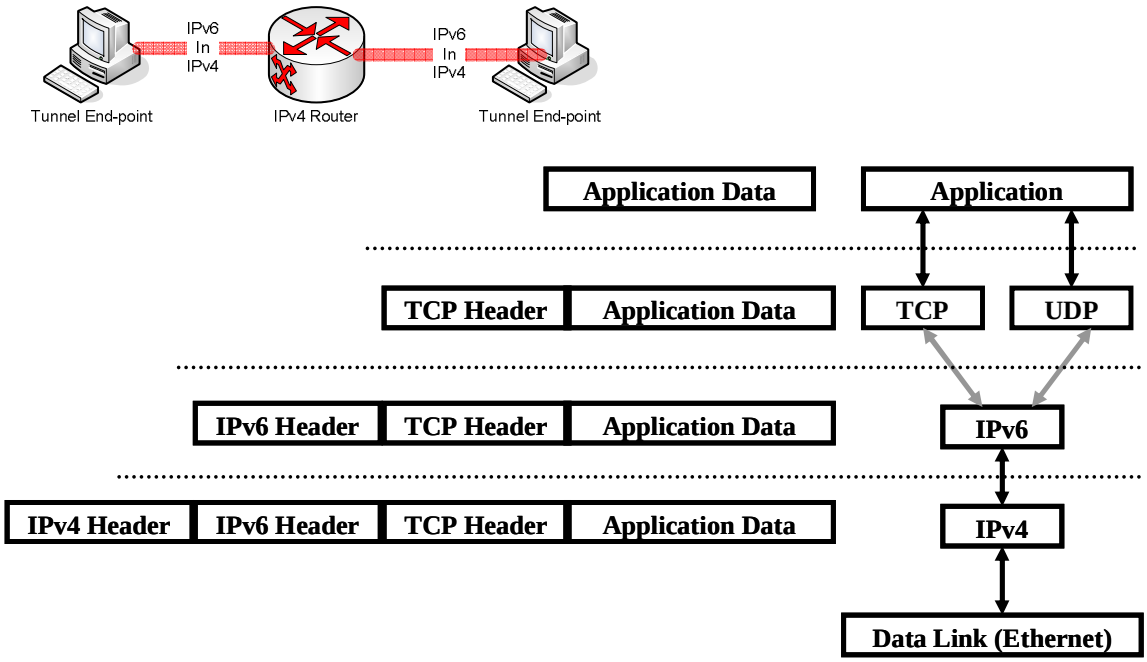


Figure B-4. Host-to-Host Tunneling

While the host-to-host configuration has tunnel end-points residing on hosts (workstations or biomedical devices), there can also be router-to-router tunneling (Figure B-5) where end-points reside on routers.

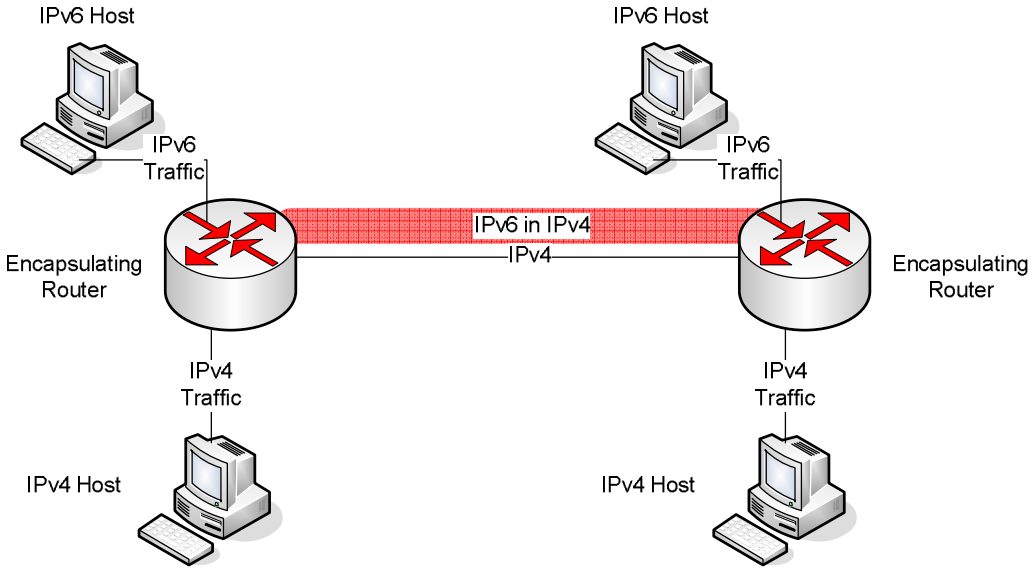


Figure B-5. Router-to-Router Tunneling

TRANSLATION

While tunneling is used to connect systems running the same protocol through a network running a different protocol, translation is used to interconnect end systems running different protocols (Figure B-6). If one system builds IPv6 packets and sends them to a system that is IPv4-only, the destination system cannot accept the information due to improper format. To provide interoperability, a translator would convert the IPv6 packets to IPv4 format and forward them to the destination system. There may be some feature loss in this case due to the differences in the protocols. In the reverse direction, the IPv4 packets from the IPv4-only end system would have to be converted to IPv6.

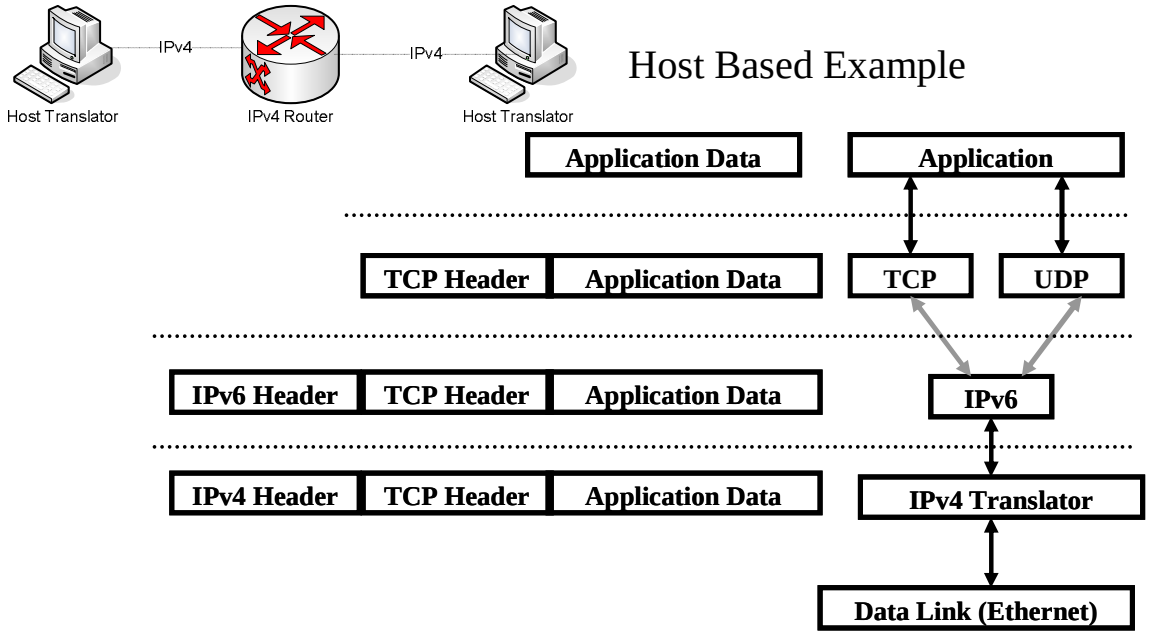


Figure B-6. Host Based Translation

A second type of translation is the Network Address Translation-Protocol Translation (NAT-PT), where translation occurs on a NAT-PT device (See Figure B-7). One advantage is that NAT-PT requires no changes to existing hosts.

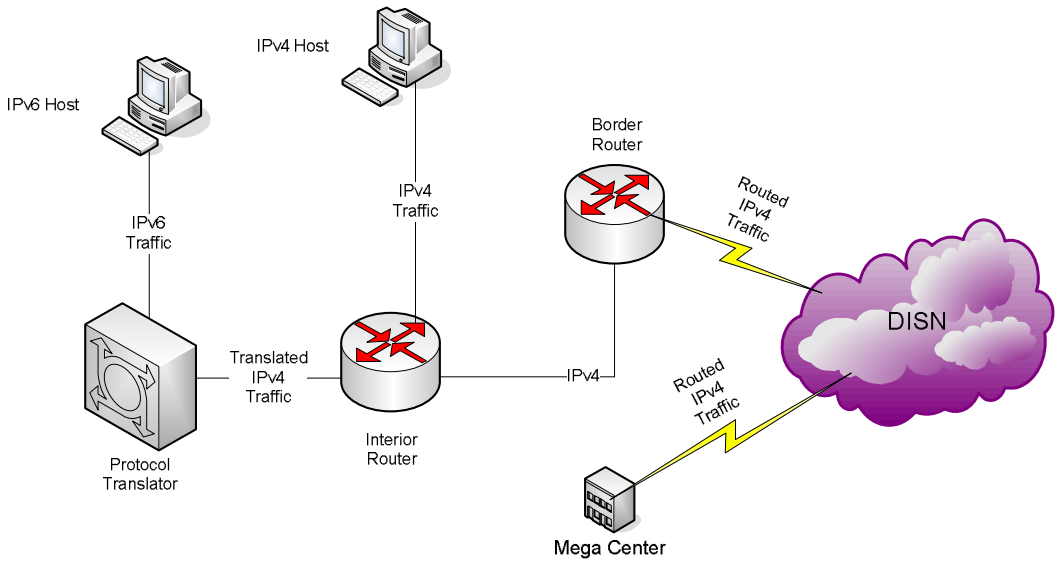


Figure B-7. NAT-PT Translation Example

Note: In VA the NOC or N/SOC is equivalent to the DISN in DoD.

Appendix D – TECHNICAL TRAINING TOPICS

IPv6 Addressing/Routing/Packet Filtering

- IPv6 Header and Extension Headers
- IPv6 Addressing Architecture
- IPv6 Data Link protocols
- IPv6 and MPLS
- IPv6 and Layer-2 and/or Layer-3 VPN
- Deploying Dual-Stack
- ICMPv6 and Neighbor Discovery Protocol
- Routing with EIGRPv6
- Routing with OSPFv6
- Routing with MBGP
- Enable authentication for Routing Protocols
- Graceful Restart for Routing Protocols
- Implementing Anycast
- Configuring IPv6 Packet Filtering
- Troubleshooting the IPv6 Network
- IPv6 paradigm shift: “New Thinking”
- Implementing Security (IPv4 NAT to IPv6)
- Routing with RIPng
- Routing with Integrated IS-IS Protocol

Network Services

- QoS Provisioning (*Diffserv, IntServ, Traffic Class, Flow Label, etc.)
- IPSec (A, ESP)
- Mobile IP
- Using DHCP with IPv6 in troubleshooting/configuration capacity
- Using SSH with IPv6 in troubleshooting/configuration capacity
- Using SSH/Ping/Telnet/FTP/TFTP with IPv6
- Authentication/Authorization/Accounting with IPv6 (RADIUSv6)
- IPv6 Prefix delegation

- Firewall/IDS/IPS
- IPv6 Network Management (CiscoWorks, CSM, ACS, NetScout)-using these tools in an IPv6 environment*
- SNMP for IPv6 Network Management – (SNMPv3 – optional)
- Implementing Multicast Service (ASM, SSM) – optional

* indicates applicable to Operational Group training, only

End Points

- IPv6 Host Configurations (Solaris, MS Windows) – stateful and stateless DHCP
- Auto Configuration
- Dual-stack issues

Administrative Topics

- Contact lists
- Trouble reporting
- Change management