United States

Department of Veterans Affairs

Transition Plan
for
IPv6 Enablement on the VA Network Backbone

Version 1.0

November 2006

IPv6 Transition Office
Telecommunications Operations Management Service (005N2)
Office of Information and Technology

Table of Contents

1 Executive Summary 4
2 Introduction 5
2.1 Purpose 5
2.2 Background 5
2.2.1 OMB Mandate and Guidance 5
2.2.2 Why IPv6 is Important to the VA 7
2.2.3 How IPv6 Benefits Map Into the VA's Strategy 8
3 Governance 9
3.1 Roles & Responsibilities 9
3.2 VA OI&T Chief Information Officer 9
3.3 OI&T, Office of Telecommunications 9
3.4 The VA IPv6 Transition Office 9
3.5 Steering Committee 10
3.6 Transition Working Group 10
3.7 Registry and Addressing Working Group 11
3.8 Training Working Group 11
4 Policy and Enforcement 12
4.1 Device Connectivity 12
5 Deployment Strategy 13
5.1 Strategy Selection 13
5.2 Implementation Strategy for Backbone IPv6 Enablement 13
6 Requirements 14
6.1 High-level Requirements Definition 14
6.2 Capacity Requirements 15
6.3 Security Requirements 15
6.4 Other IPv4 Network Requirements 15
6.5 Addressing Requirements 16
6.6 Domain Name Service Requirements 16
6.7 Testing Requirements 16
6.8 Standards Requirements 16
7 Acquisition and Procurement 17
7.1 Infrastructure Upgrade 17
8 Deployment, Implementation and Management 20
8.1 Backbone Definition 20
8.2 Security Infrastructure 21
8.3 IP Addressing 22
8.3.1 IPv6 Address 22
8.3.2 IP Addressing Strategy 23
8.3.3 Address Management 24
8.4 Domain Name Service 25
8.5 Routing 25
8.6 Network Management 26

8.6.1 Network Measurement 27
8.6.2 Management Tools 27
9 Assurance 28
9.1 CIO Council Guidance 28
9.2 Assess Security Posture 28
9.3 Update Security Plan 28
9.4 Security Risk Assessment 28
9.5 Maintain Security during Transition 29
9.6 Maintain IPv4 Production Network Functionality 29
10 Test Plan 30
11 Funding Requirements 32
11.1 Planning 32
11.2 Operations 32
12 Transition Schedule 33
13 Training Plan 34
13.1 Background 34
13.2 Training Offerings 34
13.3 VA IPv6 Certification 35
13.4 The Certification Process 35
13.5 Course Documentation 35
Appendix A: Acronyms and Definitions 37
Appendix B: References 38
Appendix C: Technical Training Topics 39

1 EXECUTIVE SUMMARY

The "Transition Plan for IPv6 Enablement on the VA Network Backbone" describes the transition of the current VA network backbone from an IPv4-only network layer to a combined IPv4 and IPv6 network layer. The goal of this transition is to operate with both network protocols in parallel by June 2008 as specified in the Office of Management and Budget mandate M-05-22 issued in August 2005.[1]

To meet this goal, it is necessary to ensure that all IP-capable network devices on the VA network backbone are IPv6 capable, that network management tools are adequate to the task of managing both network protocols in the network layer in the OSI model, and that communications security devices are in place and functioning adequately. The following areas are included in this plan and must be managed as the plan progresses.

- Governance
- Strategy
- Requirements
- Acquisition and Procurement
- Deployment and Implementation
- Assurance
- Test Plan
- Funding Requirements
- Sequencing
- Training Plan
- Training
- Risk Mitigation
- Personnel
- Operations

The VA network backbone consists of a core layer and a distribution layer (see Figure 1- VA Network Backbone Conceptual View). While the core layer is centrally controlled by VA Telecomunications Operations, the distribution layer is managed by various VA organizational elements. It is therefore necessary to achieve close cooperation between and among the VA Central Office and organizations within the VA Veterans Integrated Service Network (VISN) administrations where distribution layer backbone devices are located.

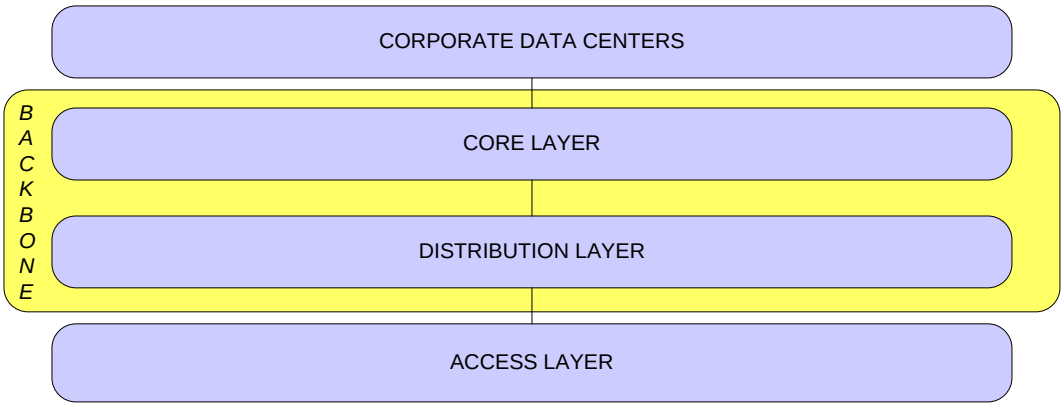


Figure 1- VA Network Backbone Conceptual View

[1] In August 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" mandating the deployment of IPv6 on federal government agencies' network backbones by June 2008.

2 INTRODUCTION

2.1 Purpose

This document summarizes the approach the VA is using to enable IPv6 on the VA network backbone. It is intended to be a living document which will reflect the VA's plans for completing the enablement of IPv6 on the network backbone.

2.2 Background

2.2.1 OMB Mandate and Guidance

As stated in the executive summary, in August 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" mandating the deployment of IPv6 on federal government agencies' network backbones by June 2008. In particular, the mandate specified that each agency must take specific actions, as described below:

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 and
- Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6 (see Attachment B for details).

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 Enterprise Architecture (EA) submission to OMB.

June 30, 2006

- Complete inventory of existing IP compliant devices and technologies not captured in first inventory, and
- Complete impact analysis of fiscal and operational impacts and risks.

June 30, 2008

- All agency infrastructures (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy. [2]

[2] Pages 1-2, "Transition Planning for Internet Protocol Version 6 (IPv6)," Karen S. Evans, Office of Management and Budget, August 2, 2005.

All tasks with completion dates no later than June 30, 2006, have been completed. Additionally, the mandate stated that the topics described below will be evaluated using OMB's enterprise architecture 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.

Note that while the mandated activity is frequently identified as a transition, the OMB mandate does not describe a "transition" in the strict definition of the term where something is replaced with something else. The mandate requires IPv6 be enabled on the backbone network along with IPv4.

The CIO Council has provided additional guidance in clarifying the meaning of the OMB mandate. Regarding the scope of the backbone network, the CIO Council has said that "the backbone network includes the wide area network (WAN) core up to the local area network (LAN). The LAN demarcation point is the device (e.g. router, switch) which services the workstations.[3]"

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)."

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

2.2.2 Why IPv6 is Important to the VA

The general rationale for the deployment of IPv6 has been the exhaustion of the IPv4 address space. One prediction is that the IPv4 address space will be exhausted by 2012.

In addition to an increased address space, IPv6 provides other benefits to the business as outlined below:

- **Quality of Service (QoS)** - IPv6 contains 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 VoIP which require real-time data transmission.

- **Simplified Mobility** - 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, home networks, e-mail, etc. using Layer 2 mobile wireless technologies such as those classified as "3G" technologies.[4] 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 is an added function.

- **Security Enhancements** - The abundant availability 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 has secure neighbor discovery extensions for which there is no equivalent in IPv4.[5]

- **Increased Network Efficiency** - The Internet Protocol was originally designed so that each packet, including addressing information, would be unmodified as it traveled between hosts.[6] The use of network address translation (NAT)[7], whose creation was initially driven by insufficient IP addresses, breaks this model. NATs complicate implementation of advanced network technologies and hinder network performance. After transitioning to IPv6, the primary motivator for NATs (globally routable address conservation) will be eliminated.[8]

---

[4] "Bitpipe" web site, http://www.bitpipe.com/tlist/3G-Wireless.html
[5] "Analysis of IPv6 Features and Usability," North American IPv6 Task Force Report, Wesley M. Eddy, William Ivancic, Josephy Ishac, September 6, 2006, pages 9-10
[6] "Internet Transparency," IETF RFC 2775, <http://www.ietf.org/rfc/rfc2775.txt?number=2775>
[7] "IP Network Address Translator (NAT) Terminology and Considerations," IETF RFC 2663, < ftp://ftp.rfc-editor.org/in-notes/rfc2663.txt>
[8] See IETF Internet-Draft "IPv6 Network Architecture Protection," http://www.ietf.org/internet-drafts/draft-ietf-v6ops-nap-03.txt for a discussion of how IPv6 can be used to provide the same security and management benefits associated with NATs.

IPv6 offers the potential and framework for these capabilities and benefits. Realization of these capabilities and benefits will require significant protocol development and design. Federal agencies, including the VA, must explore how IPv6 can help the agencies achieve their strategic mission.

2.2.3 How IPv6 Benefits Map Into the VA's Strategy

The VA Strategic Plan identifies four strategic goals where IPv6 features contribute to execution of these goals. These areas are:

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

These goals are mapped to IPv6 features in following table:

IPv6 Feature	Veteran Centric	Interagency Collaboration	Information Security	Emergency Management
Increased number of IP addresses	✓	✓	✓	✓
Quality of Service (QoS) – Addition of Flow Label	✓	✓		
Simplified Mobility	✓		✓	✓
Increased Network Efficiency	✓			✓
Security Enhancements	✓	✓	✓	✓

Figure 2 : IPv6 Features and VA Strategy

3 GOVERNANCE

3.1 Roles & Responsibilities

The governance for the VA IPv6 transition is illustrated in the below drawing, *Figure 3 - VA IPv6 Transition Governance Structure*.

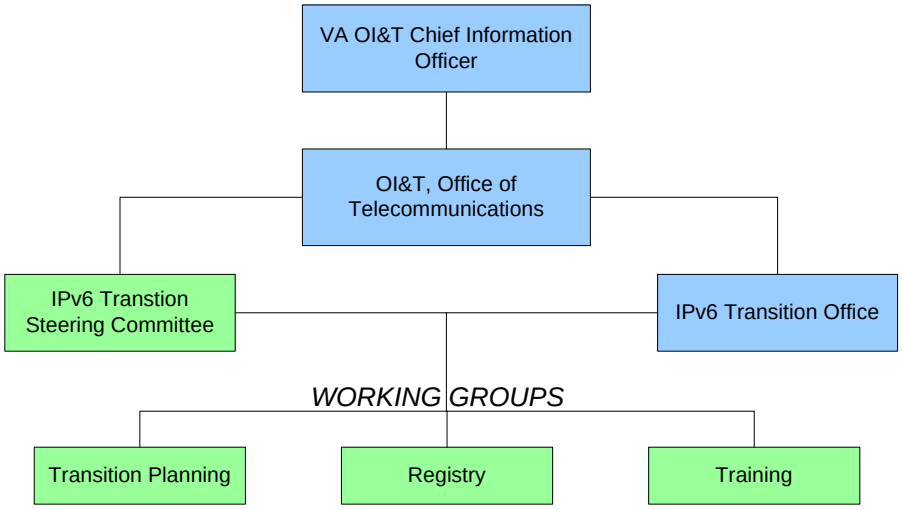


Figure 3 - VA IPv6 Transition Governance Structure

3.2 VA OI&T Chief Information Officer

The VA CIO has the ultimate responsibility for the smooth and timely transition of the agency backbone to IPv6. The CIO receives regular updates on the progress of the project from the Office of Telecommunications.

3.3 OI&T, Office of Telecommunications

The Office of Telecommunications has the day-to-day responsibility for the IPv6 transition activities. The Office of Telecommunications oversees the progress of the IPv6 transition office, the steering committee, and the working groups.

3.4 The VA IPv6 Transition Office[9]

The VA IPv6 transition office is responsible for the research, advice, planning, and coordination of the timely deployment of IPv6 on the VA network infrastructure. This office provides guidance, common engineering solutions, and guidelines designed from an enterprise perspective. The VA IPv6 transition office, in conjunction with VA Enterprise Architecture (EA), is responsible for coordinating transition planning, analysis, testing, and implementation efforts across the VA. The transition office is also responsible for promoting knowledge-sharing, ensuring that needed infrastructure is provided, and implementing a systematic program of

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

outreach within the VA community. The VA IPv6 transition office ensures that critical transition issues are prioritized and addressed.

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

- Managing the IPv6 implementation IPv6 to meet business and technical requirements presented in the VA enterprise architecture.
- Supporting and coordinating updates of the VA IPv6 transition plan with the VA Enterprise Architecture and ensuring that the VA transition plans are synchronized and consistent with the enterprise architecture.
- Leading the development of in-depth transition guidance and/or policies.
- 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 assessments and recommendations.
- Providing IPv6 knowledge base throughout the VA for information exchanges and outreach.

A technical outreach program is important to the success of the general IPv6 deployment effort at the VA. The VA, through the steering committee, the transition office, and the working groups is interacting with other organizations involved in the deployment of IPv6. These organizations include federal agencies, the research and education community, commercial organizations and standards organizations. Through technical outreach activities, the VA will gain and share the most economical, reliable, secure and expedient methods for deploying and maintaining IPv6 infrastructures. It is through collaboration that unnecessary duplication of IPv6 deployment efforts by federal agencies, including the VA, will be reduced.

3.5 Steering Committee

The steering committee was formed early in the project and comprises representatives from impacted areas throughout the agency. The steering committee established several technical working groups, described below, to leverage technical expertise throughout the VA. As the needs of the project evolve, the steering committee may establish or dissolve individual working groups.

The steering committee is responsible for setting policy and direction for the agency, coordination and communication between the working groups, overseeing transition activities and progress, and reviewing and approving transition plans, schedules, and documents.

3.6 Transition Working Group

The transition working group consists mostly of technical people and is responsible for developing, coordinating and implementing a cohesive transition plan for VA's migration to IPv6. Group activities include as a minimum:

- Conducting a requirements analysis of the IPv6 transition

- Developing and implementing a test plan for compatibility/interoperability
- Deploying with a phased approach
- Updating IPv6 requirements and target architecture

These activities will be monitored by OMB via the quarterly submissions by VA Enterprise Architecture.

3.7 Registry and Addressing Working Group

The registry and addressing working group is responsible for

- Evaluating IP addressing needs for the VA's IPv6 transition
- Requesting the IPv6 address block from ARIN
- Developing and documenting a plan for allocating the addresses across the VA
- Developing a plan for managing IPv6 addresses

3.8 Training Working Group

The training working group is responsible for evaluating, developing and implementing training approaches and programs for the VA's IPv6 transition stakeholders. The group will produce a document describing how, when, and for whom the entire integrated training program should be rolled out.

4 POLICY AND ENFORCEMENT

4.1 Device Connectivity

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

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

The process for obtaining CIO approval includes the following elements:

1. Requestor must prepare a written request to connect an IPv6 device/software to the VA network. The request should describe the following:

    - The device or software to be put on the VA network
    - Where on the network the device/software will reside
    - When and for how long the device/software will remain on the network
    - 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 will be granted based on feedback from the reviewers of these requests.

5 DEPLOYMENT STRATEGY

5.1 Strategy Selection

Three methods were considered by the VA transition working group to determine the preferred approach for enabling IPv6 on the backbone network:

- 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 an IPv4 network
- Translation – a means of converting IPv4 packets 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, the VA has selected dual stack as the preferred method, followed by tunneling during initial deployment or where dual stack isn't possible. Translation will only be considered as a last resort.

Primary considerations in selecting dual stack are:

- Security
- Forward and backward compatibility
- Effort required

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 a best practice by multiple sources.

IPv6 deployment is 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.

5.2 Implementation Strategy for Backbone IPv6 Enablement

The implementation strategy will be refined further in future revisions of the transition plan. However, the implementation strategy, as currently visualized, will be to enable IPv6 on the innermost core of the VA backbone network and work outward.[10]

[10] Andrew Delong, Network Engineer, VA Office of Information & Telecommunications/ IT Operations

6 REQUIREMENTS

6.1 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 require that federal organizations "conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements."

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

> "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."

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

"Agencies must be able to demonstrate they can perform <u>at least</u> 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)."

The requirements for June 30, 2008 are for the network backbone (core) only. IPv6 does not actually have to be operationally enabled (i.e. turned on) by June 30, 2008. However, network backbones must be ready to pass IPv6 traffic and support IPv6 addresses. Applications, peripherals, and other IT assets which are not leveraged in the execution of the functions mentioned above are not required for the June 30, 2008 deadline. Agencies are expected to verify this new capability through testing activities. They are also required to maintain security during and after adoption of IPv6."

Therefore, the requirements for IPv6 capability on the VA backbone are based on the OMB and Federal CIO Council mandate and guidance. As such they may be summarized as follows.

By June 2008,

1. Acquired products or systems must interoperate with IPv6 andIPv4 systems and products.
2. Acquired products must have technical support for development, implementation, and management.
3. It must be possible to transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.
4. It must be possible to transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
5. It must be possible to transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

We note the following regarding these requirements:

- Network capacity is not directly addressed. However, for IPv6 to co-exist with IPv4 in a dual stack architecture on the network backbone, the devices processing IP packets must have sufficient capacity to handle both protocols simultaneously. We note also that in the initial period of IPv6 capability the IPv6 traffic is expected to be relatively light.
- Security must be maintained at least to the original IPv4 level after introduction of IPv6.
- Network management capability must be available for IPv6.

As stated elsewhere in this transition plan, the VA has made the following decisions:

- Backbone routers will run dual stack, i.e., they will handle IPv4 and IPv6 in parallel.
- The backbone consists of the core and distribution layers of the VA network. Thus, the routers that connect a local network to the rest of the backbone are included in the target for IPv6 capability.

6.2 Capacity Requirements

Because the high-level requirements do not include overall network capacity, the capacity requirement is that devices processing IP packets must have sufficient capacity to handle both IPv4 and IPv6 simultaneously under the anticipated loads.

6.3 Security Requirements

The requirement is to avoid a reduction in security posture caused by the introduction of IPv6. It is therefore 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 will be needed to ensure that the security posture has not been reduced to an unacceptable level.

6.4 Other 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 IETF standards can promote their continuation with the introduction of IPv6 capability.

6.5 Addressing Requirements

Because of the large number of IPv6 address blocks available to the VA, an allocation scheme and process are needed to conduct initial allocation and subsequent management of the addresses.

6.6 Domain Name Service Requirements

An IPv6-capable domain name service is needed to translate between domain names and IPv6 addresses. The DNS servers must handle both IPv4 and IPv6 traffic and requests.

6.7 Testing Requirements

To ensure an acceptable level of risk on the IPv6-capable network, testing in the laboratory and on the network itself are needed.

6.8 Standards Requirements

Standards relevant to IPv6 capability must be identified. These are to be used in defining tests. For example, one source of standards may be the DoD "IPv6 Standard Profiles for IPv6 Capable Products."

7 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. As initially defined by the VA, an IPv6-compliant device 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 modes; and
- have available contractor/vendor IPv6 technical support for development, implementation and fielded product management.[11]

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

- The device is never connected to the VA network backbone.
- The device meets a critical need and an IPv6-capable version will not be available in time to meet the need.
- The cost for an IPv6-capable device compared to the cost of an equivalent IPv4-capable device could result in an unacceptable delay in acquisition of the IPv6-capable device.

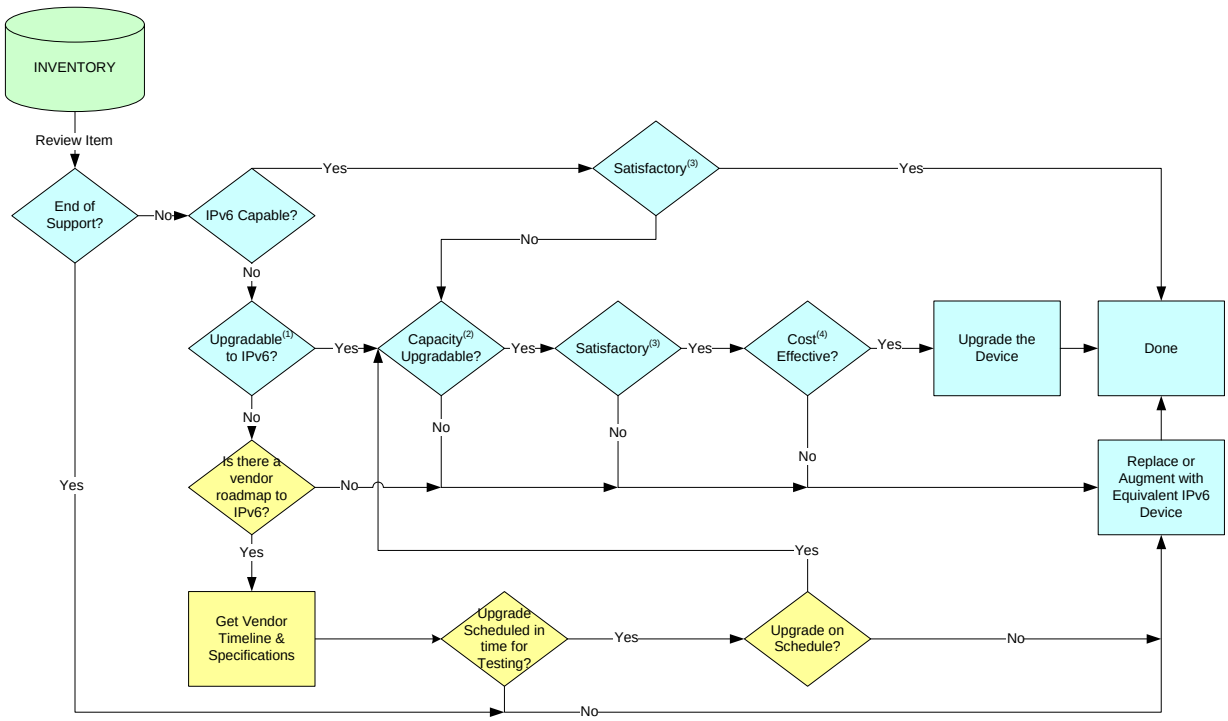
7.1 Infrastructure Upgrade

Two inventories of IP devices on the VA backbone have been conducted. These inventories revealed the following categories of equipment:

- Devices that are obsolete and should be replaced
- Devices that would be IPv6 capable but require upgrades to IOS, memory etc
- Devices that are IPv6 capable

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

[11] Pages 2-3, "Transition Planning for Internet Protocol Version 6 (IPv6)," Karen S. Evans, Office of Management and Budget, August 2, 2005.



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.

Figure 4 -Inventory Upgrade and Vendor Roadmap Tracking Process

Inventory activities are required of all parts of the Department with inventory in the VA backbone:

1. Consolidate first and second OMB inventory into a master backbone network inventory (first inventory has some routers and devices not in second inventory).
2. Complete and confirm information in the master backbone network inventory. This includes replacing fields in the second OMB inventory marked “sensitive” with the required information in the master backbone network inventory.
3. Verify devices that have been documented to be replaced actually get replaced. This will require contacting the appropriate points of contact regarding specific backbone network devices. POCs will need to be provided with a list of devices of concern and input obtained from them regarding their ability/plans to upgrade or replace the devices.
4. Obtain further inventory details, such as memory and processor information. With devices other than routers, this might be things such as chassis models, etc. This is essentially data describing anything that controls the ability of the backbone IP-capable device to be IPv6-capable/compliant that wasn't captured by the OMB inventories. This data will be used for justification that the device is IPv6-compliant/capable or must be upgraded or replaced.
5. Match routers against current IPv6 roadmap.

6. For devices that will not be replaced as part of technology refresh process before mid-2007 :
    a. Document what would be required to upgrade or replace the device.
    b. Provide cost of doing the required upgrade and pricing.
    c. Determine the acceptability of the upgraded device (consider IPv6 readiness, capacity, expected remaining lifetime).
    d. If purchase is approved, purchase the upgrade.
    e. If upgrade/replacement is purchased, install and test upgrade/replacement.
7. Provide baseline router configurations for OMB compliance testing. Devices tested should map directly to devices that are in the backbone or will be in the backbone by 2008.
8. Develop a phased plan for upgrading the backbone network, reflecting a strategy for upgrading the backbone network (e.g., "X number of routers will be upgraded during the weeks of xxx").

The above activities are applicable to all types of IP-aware devices on the VA backbone network (such as routers, firewalls network management devices and IDS/IPS devices) and are intended to be similar for all OMB mandated inventory upgrade/refresh efforts across the VA.

There should be a regular status meeting between the VA IPv6 Transition Office and the group(s) doing the inventory upgrade. Status reports could include:

- Breakdowns of device status and status reports ensuring borderline devices are being addressed.
- Updated cost expectations.
- Identification of areas that require special attention and/or escalation.
- Verification that transition milestones are being met.

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 device shouldn't be considered IPv6 capable if it won't be considered acceptably secure when IPv6 is enabled on the device.

Regardless which organizations or groups do the inventory upgrade process, the department/group responsible for implementing and operating the device must have buy-in that the upgraded device will sufficiently support their requirements.

8 DEPLOYMENT, IMPLEMENTATION AND MANAGEMENT

8.1 Backbone Definition

From the enterprise perspective, the backbone consists of the facilities, services, and network devices needed for data communication among the VA communities. For IPv6 planning purposes, the VA backbone includes all network components contained in the core, distribution, and access levels, as illustrated in Figure 1- VA Network Backbone Conceptual View.

Corporate data centers connect via distribution nodes to the core layer. Connection to the external Internet is made 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 made via distribution nodes at the access layer. Distribution nodes consist of a pair of routers, one which is carrier managed and the other which is VA managed on a regional basis.

This definition is depicted in *Figure 5 - Veterans Affairs Network*. The VA backbone items are highlighted in yellow and the remainder of the VA network infrastructure is displayed in blue.

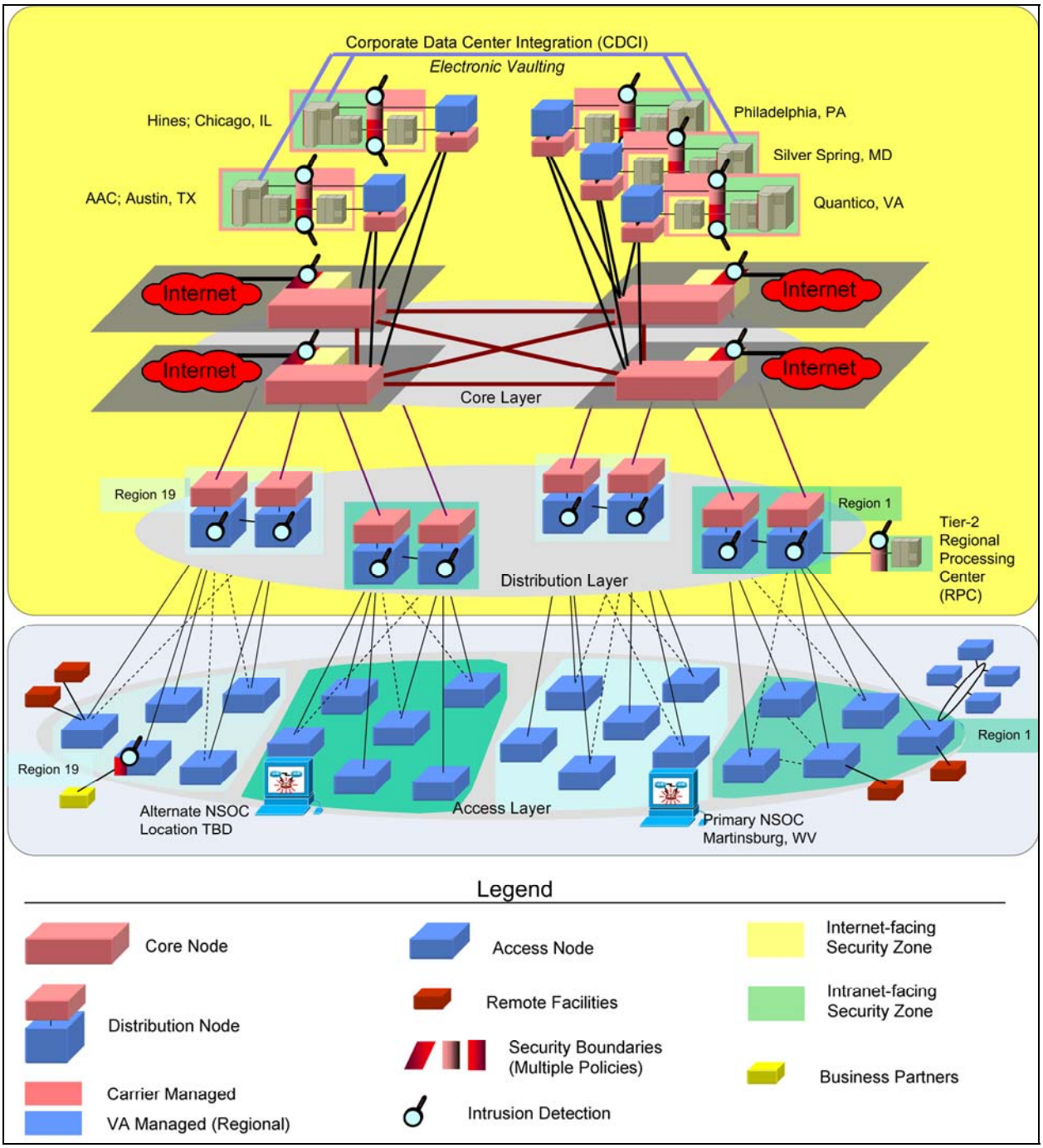


Figure 5 - Veterans Affairs Network

8.2 Security Infrastructure

According to the VA Future Architecture Vision,

> VA's Transformation to IPV6 will provide complete IPV6-compatibility across the VA Intranet and onto the internet before September 2008.

> However, the practical utilization of IPV6's increased application functionality will be delayed until MS Windows Server and Client operating environments can support this technology, and until a substantial percentage of VA's client base has upgraded their home and office computing environments to that IPV6 compatible technology.
>
> Once in place, IPV6 expanded addressing provides 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 compliant privacy and security, directly to the veteran at home.

To realize this vision of IPv6 capability in the VA, adequate security infrastructure must be in place to assure an acceptable level of security risk. The current benchmark for this risk posture is the current One-VA WAN and the ECSIP Gateway. These were security certified and approval to operate was obtained in 2005.

For example, firewalls must support the same level of packet inspection in IPv6 as for IPv4 at the same performance levels. In addition, special attention must be given to extension headers, which are not present in IPv4.

Additional network security devices, including intrusion detection and prevention and virus protection products, protect the VA backbone. These types of products must reflect the additional threats and vulnerabilities associated with the introduction of IPv6 capability. As part of the IPv6 transition, security products with IPv6 security capabilities are being reviewed. Attention is given to their set-up and configuration, in addition to their general IPv6 capability. As required, the security devices will be evaluated, upgraded, acquired, implemented and tested.

8.3 IP Addressing

8.3.1 IPv6 Address

The 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 abbreviated form is 2610:D8::/32 through 2610:D8::/32 from the American Registry of Internet Numbers (ARIN) .

ARIN has reserved a /29 IPv6 address block beginning at IPv6 address 2610:D8:: and ending at 2610:00DF: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 the VA as needed and requested.[12]

[12] Communication from David Huberman, Technical Specialist, ARIN to Michael Adams, ECSIP, VA.

8.3.2 IP Addressing Strategy

The VA IPv6 address space shall be partitioned as depicted in *Figure 6 - Graphical Representation of VA Address Allocation*. An assumption is that the largest prefix that will be constructed within the VA is a /64 block. While this assumption may change, it reflects the best current thinking of the IETF.

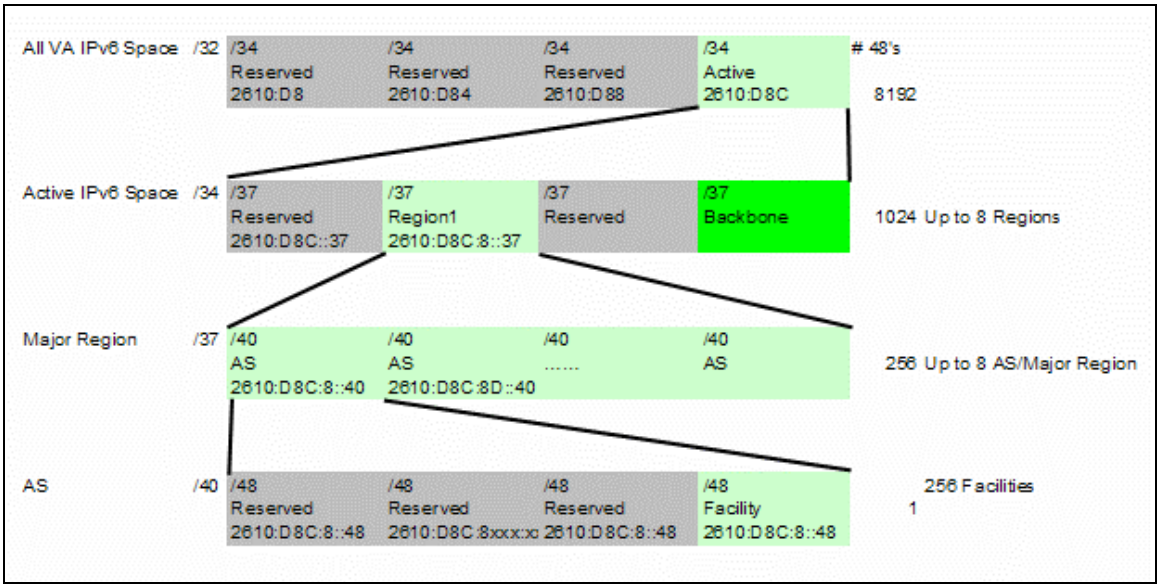


Figure 6 - Graphical Representation of VA Address Allocation

Based on discussions within the Registry and Addressing Working Group, some preliminary concepts have been drafted:

The VA was allocated the IPv6 address block 2610:d8::/32 by the American Registry for Internet Numbers (ARIN) for allocation within the enterprise. This provides for 4,294,967,296 /64 subnets; the amount of address space available to the VA for defining networks is equivalent to the entire IPv4 address space.

Figure 6 depicts the proposed partitioning of the total VA addressing space. Of 4 possible /34 blocks, one /34 block (representing 1,073,741,824 possible /64 subnets) will initially be available for allocation within the VA.

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 carve eight /37 blocks, four will support VA "super-regions" and one will support addressing for the VA backbone 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 can be allocated from each /37 or 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 be also possible to allocate 256 /48 blocks within each AS/region and each /48 block will be 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 network.

The VA shall standardize addressing format for network devices with differing profiles. Standardized address blocks shall be assigned for VLANs supporting classes of specific network devices that have varying security requirements. As visualized, having VLAN/subnets that uniquely identify network devices with specific security requirements 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 a 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're 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 the 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.

8.3.3 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 organizational units.
- Distribute addresses within assigned blocks to sub-organizations, networks and devices.

- Return unneeded address blocks to address authority.

8.4 Domain Name Service

All DNS devices on the VA network will, at a minimum, support IPv4. It will be possible to use the existing IPv4-enabled DNS infrastructure to support the DNS requirements of dual-stack devices deployed on the VA backbone network. The DNS servers currently implemented on the backbone network and at the VA ESCIP gateways[13] 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 the VA backbone network IPv6 deployment.[14]

The capability to reference IPv6 addresses using convenient DNS names will be considerably more important since IPv6 addresses are four times as long as IPv4 addresses. Additionally, the hexadecimal format typical with IPv6 addresses will initially confuse both end-users and network specialists. Tools to correctly format IPv6 addresses and ensure that IPv6 addresses are correctly configured in DNS server configuration files will be even more important than similar tools are for IPv4.[15]

The behavior of IPv6-enabled devices in cases where both IPv6 and IPv4 addresses are associated with a single DNS name must be understood and confirmed. For example, it is possible that users may experience extensive network delays because the user's computer is trying to reach a remote computer via IPv6 using an IPv6 address obtained from DNS. If the IPv6 path to the remote computer is not functional, the user's computer may appear to be idle for about 45 seconds because the user's computer is trying to reach the remote computer using IPv6 even though the computer has a functional path to the remote computer using IPv4. If the network support administrator learns that disabling IPv6 on the dual-stack computer solves a large percentage of trouble calls, IPv6 in a dual-stack environment will be deemed problematic by administrators and users alike.[16]

8.5 Routing

IPv6 routing will function independently of the IPv4 routing. The 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 IPv4 routing, but the goal will be to have IPv4 and IPv6 routing be the same.

[13] DNS servers that support the VA backbone network are based on a combination of Windows 2003 servers and Sun Solaris systems running BIND 9 DNS.
[14] Communication with the IPv6 Transition Office, Eric Jurasas, Hines, VA
[15] "IPv6 Network Administration," Nall Richard Murphy and David Malone, O'Reilly Publishing, 2005, pages 150-151.
[16] See http://v6fix.net/docs/wide-draft-v6fix.en and RFC 4472: "Operational Considerations and Issues with IPv6 DNS", http://www.ietf.org/rfc/rfc4472.txt?number=4472 for further discussion of DNS-related issues.

It is not expected that IPv6 routing will have any impact on the IPv4 routing, but this must be insured.

Since the IPv4 and IPv6 routing tables will operate independently of each other, there is no technical reason why generalizations about one internet protocol's routing table or implementation can be applied to the other Internet Protocol's routing table or implementation.

As far as routing is concerned, all design rules and strategies used in deploying IPv4 networks apply to IPv6. The approach has to be hierarchical and it has to observe the specifics of each layer of the network: core, distribution/edge, and access.

There are some significant differences in the behavior of the IPv6 routing system, compared to its IPv4 counterpart. First of all, the global IPv6 Internet is still by several orders smaller than the global IPv4 Internet. According to the CIDR report (data from February 2005), inter-domain routing tables contain more than 150 thousand IPv4 network prefixes but only about 700 IPv6 prefixes. The complexity of IPv6 routing is thus incomparable to its IPv4 counterpart. IPv6 routing still suffers from two characteristic problems that the VA needs to be aware as it moves forward:

1. 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.
2. The IPv6 Internet is still, by and large, an overlay network over IPv4 and its tunnels distort the inter-area link metrics (number of hops in AS paths) and mislead routing algorithms.

Both problems can be expected to disappear after IPv6 becomes more mainstream and the implementation stabilizes.

8.6 Network Management

Gaps between how IPv4 and IPv6 traffic is managed must be identified and mitigated. Gaps will likely occur in following scenarios:

- IETF IPv6 management standards equivalent to IPv4 management standards have not been defined or implemented in VA backbone network devices.
- IPv6 management standards equivalent to IPv4 management standards have been defined, but the equivalent functionality is not available on the 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.

The VA IPv6 implementers must identify what measurements are IPv4-specific and verify that both an IPv6-equivalent exists and can be measured.

- Like routers, it must be ensured that measurement devices, such as network probes, can keep up with IPv6 traffic.
- While it may be interesting to send/receive network management traffic via IPv6-transit, it is not required to fulfill the June 2008 mandate.

8.6.1 Network Measurement

IPv4-based measurements and metrics on the production backbone network must be performed via IPv6 on the backbone network.

Periodic stress-testing, such as throughput capacity measurements completed on the backbone network using IPv4-based traffic, must also be completed using IPv6-based traffic. It must be ensured that both IPv4- and IPv6-based measurements which stress-test the backbone network do not impact the backbone network's capability to process production network traffic. Automatic mechanisms could be in-place to ensure that stress testing does not occur on backbone network links that are already reaching capacity. One such mechanism could be to transit measurement traffic classified as Less than Best Effort (LBE); measurement traffic would be given lower priority than production traffic on the link.

8.6.2 Management Tools

In concert with work being done regarding network management, it must be confirmed what management data is collected regarding IPv4 traffic and that IPv6 equivalents can be measured by the management tool.

Commercial off-the-shelf tools that could be evaluated include:

- Cisco CiscoWorks
- Hewlett Packard Overview
- IBM Tivoli
- Brix Networks

Open source tools that could be evaluated include:

- AS-path
- IPFlow
- Mping
- Argus
- Ethereal/Wireshark

9 ASSURANCE

The addition of the IPv6 communications protocol to those available on the VA backbone is considered to be an enhancement to the current capability that includes IPv4. Therefore, it should not be necessary to conduct a full certification and accreditation (C&A) process to achieve authority to operate with IPv6. However it is necessary to demonstrate that the addition of the IPv6 protocol does not degrade the current level of security on the network.[17]

9.1 CIO Council Guidance

According to the Federal CIO Council Architecture and Infrastructure Committee, 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."[18] For IPv6, the existing network risk assessment and security plan must be updated to reflect the changes made to implement this additional protocol.

9.2 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

9.3 Update Security Plan

The security plan for the existing IPv4 network will be reviewed and updated as required. Topics to receive specific attention for IPv6 include the following:

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

9.4 Security Risk Assessment

To determine the risks over and above those identified for the IPv4 network will be identified and addressed.

- Identify assets – these are the additional assets required of IPv6
- Identify vulnerabilities – these are additional network vulnerabilities caused by the addition of IPv6

[17] Guidance received from VA Office of Cyber and Information Security (OCIS)
[18] Page 19, "IPv6 Transition Guidance," Federal CIO Council Architecture and Infrastructure Committee, February 2006.

- Identify threats – these are the additional threats identified as pertaining to the IPv6-enabled backbone
- Determine effects of threat to vulnerability – assess the potential for all identified threats to exploit the additional vulnerability
- Prioritize high risks – rank the risks determined 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 need to be in place.

9.5 Maintain Security during Transition

During the transition to IPv6 capability on the VA backbone, the security posture will be in a state of flux. Therefore, it will not be advisable to allow general usage of the IPv6 capabilities on the backbone as soon as they are put into place. Security will be maintained during the 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.

9.6 Maintain IPv4 Production Network Functionality

It is conceivable that addition of IPv6 capability on the VA backbone could interfere with the IPv4 capability. For example, the capacity of routers to handle IPv4 and IPv6 traffic simultaneously could be inadequate. This could result in a denial-of-service condition with respect to IPv4. Therefore, one of the assurance goals of the IPv6 transition is to monitor the potential and actual effects of IPv6 operation on the functionality of the IPv4 portion of the network.

10 TEST PLAN

The test plan will be provided as a separate document. The test plan is an OMB mandate requirement.

The primary objective of testing is to verify proof of concept for network configurations to support demonstration of the functions described by the CIO Council and documented below. While additional testing may be valuable and merited, verification of the VA strategy to fulfill the three CIO functions is essential to meeting the requirements of the OMB mandate.

- 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)."

Three types of testing can be performed:

- Testing to assess an individual product's IPv6 capability (conformant to agree upon RFC), performance, and interoperability.[19]
- Evaluation of equipment/configurations in a test lab environment
- Pilot implementations

To accelerate experimentation and to gain familiarity with IPv6, controlled IPv6 pilot testing and lab testing activities can occur in parallel. It will be necessary for the pilot testing to be performed in an isolated environment where native IPv6 packets are not transited across production VA networks. This requirement reflects the fact that pilot testing would be done on the VA networks before they are actually ready for production IPv6 traffic.

For controlled pilot network testing, steps are proposed in the following order:

1. A single isolated IPv6 test environment will be set up so that the IPv6 network behavior can be better understood in this network. The test environment may fit into a computer lab or could consist of interconnected computers sitting on desks and interconnected by a separate campus cabling scheme or VLAN.
2. Additional isolated IPv6 test environments will be created based on lessons learned in previously created test labs.
3. The isolated test environments will be interconnected with an acceptable tunneling technology that will ensure that only IPv4 packets are transited across the VA network. The test network will be connected to the VA network with routers that encapsulate all IPv6 traffic into IPv4 packets, with the assumption that the IPv4 traffic does not in any way represent a threat to the VA's production network capability.
4. Connecting pilot test networks to IPv6 networks outside the VA could also be considered.

It is not anticipated that adverse impacts will occur on the VA production network when native IPv6 is enabled and IPv6 traffic is transited on the VA production network. However, to ensure

[19] "Department of Defense Internet Protocol Version 6 Generic Test Plan Version 2", Defense Information Systems Agency, Joint Interoperability Test Command Fort Huachuca, Arizona.

the high level or reliability that the VA production network is required to maintain, lab performance and interoperability testing must be performed.

It is possible third-party organizations, such as the University of New Hampshire Interoperability Lab (UNH-IOL), have completed compliance tests for devices similar to those that must be tested on the VA backbone network. If the compliance requirements of third-party tests are a superset of the compliance requirements from this document's testing matrix, there is no VA justification for repeating these tests if the same model and configuration of IP-capable device has already been tested. If the device's IPv6 compliance characteristics have not been tested by another organization and the device is considered critical to the correct functionality of the VA backbone network or is core to the VA mission, the device should be tested for IPv6-compliance.

11 FUNDING REQUIREMENTS

11.1 Planning

The following text is transcribed from the DoD IPv6 transition plan and is included because it closely mirrors the VA's perspective and goals. The text provides excellent guidance upon which the VA can build its own case for funding.

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 assess 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 VA will avoid later transitional 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 a 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 efforts*
- *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.[20]

11.2 Operations

This section will be completed in a future version of the IPv6 Transition Plan.

[20] Page 28, The Department of Defense Internet Protocol Version 6 Transition Plan, version 2.0, June 2006

12 TRANSITION SCHEDULE

In their August 2005 memo, "Transition Planning for Internet Protocol version 6 (IPv6)", OMB set June 2008 as the date by which agencies' network backbones should be ready to use IPv6. As part of the initial planning, VA has set a preliminary goal of March 2008 for the transition of the backbone to IPv6.

Figure 7 - IPv6 Transition Schedule shows dependencies between the various aspects of the project depicted at a high level. The Transition Working Group has approved a master schedule plan which addresses the tasks and resources involved in the project. Additionally, each specific area such as addressing, testing, and training will be following a sub-schedule detailing individual activities. As issues arise, contingencies and options will be identified and reflected in the project schedule.

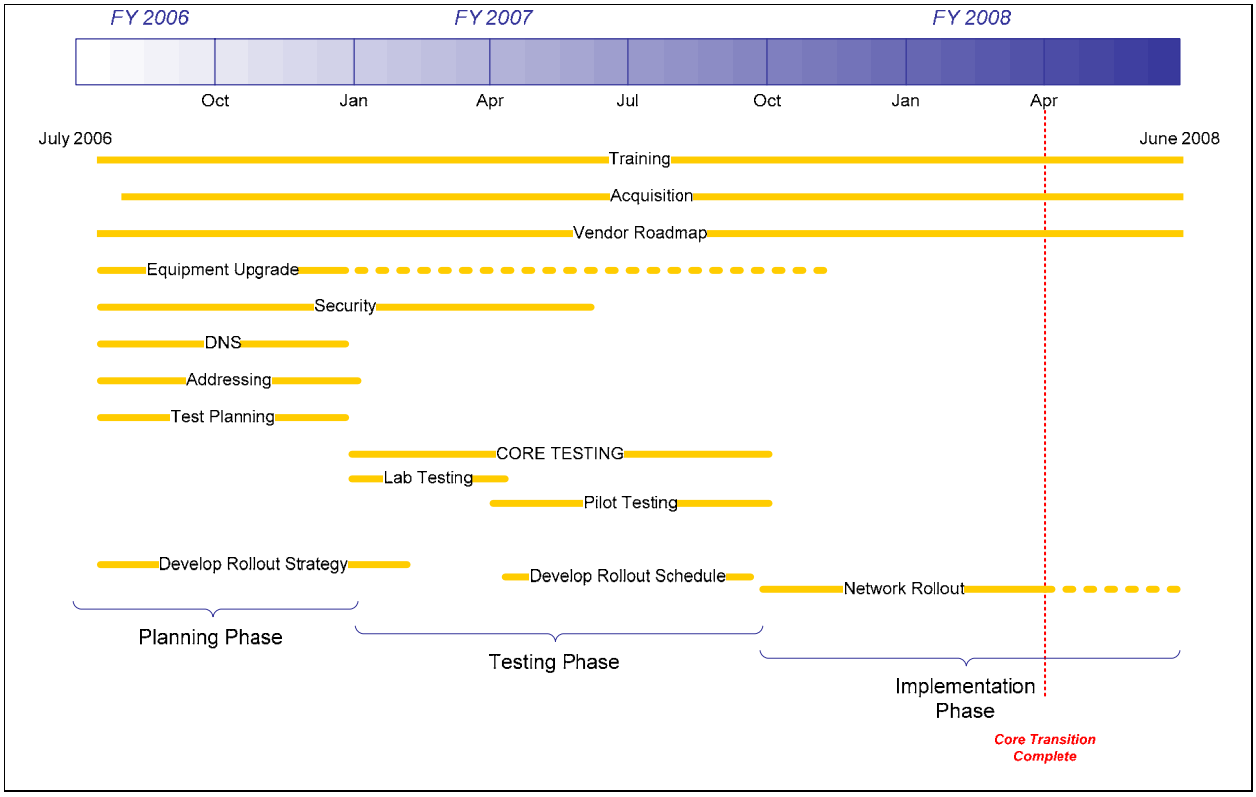


Figure 7 - IPv6 Transition Schedule

13 TRAINING PLAN

13.1 Background

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

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

- Architectural population: Enterprise Architecture personnel, Network Managers, Technical Managers, Telecommunications Managers, Security Managers
- Operational population: Network Engineers, Network Specialists, System Developers, Telecommunications Specialists, Support personnel
- General population: Management and Users

13.2 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:
(1) train-the-trainer, (2) architectural, (3) operational (4) specialized, and (5) general.

In addition to traditional stand-up training, the IPv6 training will be presented as a web-based version, as well as video and DVD.

- **Train-the-trainer**: Training will initially be presented in the traditional "train-the-trainer" format. Selected VA personnel will be trained in order to present the material to VA personnel in the field. Class size for this training has yet to be determined.

- **Architectural**: The architectural training comprises 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 theory and hands-on exercises. This course is specifically designed for technical VA personnel. The expected enrollment in this course 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 and a specialized training may be developed. If this training is necessary, it will 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 a video or DVD.

Course content will consist of technical as well as administrative topics as outlined in **Appendix C – Technical Training Topics**.

13.3 VA IPv6 Certification

As a component of the training, participants are required to pass an evaluation in order to be certified in IPv6 methodology. 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.

13.4 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 vendor 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 the 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 train all subsequent phases of the course.

13.5 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 the sole property of the VA.

APPENDICES

A. Acronyms and Definitions
B. References
C. Technical Training Topics

APPENDIX A: ACRONYMS AND DEFINITIONS

ACL	Access Control List
AH	Authentication Header
ARIN	American Registry for Internet Numbers
ASM	Any source multicast
BGP	Border Gateway Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
DREN	Defense Research and Education Network
Dual-stack	Both IPv4 and IPv6 protocol stacks operate in parallel on the same network device.
EA	Enterprise Architecture
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPcomp	IP payload compression
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LBE	Less than Best Effort
MBGP	Multi-protocol BGP
MPLS	Multi-Protocol Label Switching
MLD	Multicast Listener Discovery
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSPFv3	Version 3 of OSPF, which supports IPv6
QoS	Quality of Service
RFC	Request for Comments
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SOW	Statement of Work
SSH	Secure Shell
SSM	Source Specific Multicast
UNH	University of New Hampshire
VPN	Virtual Private Network

APPENDIX B: REFERENCES

"Analysis of IPv6 Features and Usability," North American IPv6 Task Force Report, Wesley M. Eddy, William Ivancic, Josephy Ishac, 2006, <http://www.nav6tf.org/documents/nav6tf.analysis_ipv6_features_and_usability.pdf>

"Department of Defense Internet Protocol Version 6 Generic Test Plan Version 2", Defense Information Systems Agency, Joint Interoperability Test Command, Fort Huachuca, Arizona.

"The Department of Defense Internet Protocol Version 6 Transition Plan," version 2.0, June 2006.

"Deploying IPv6 Networks," Popoviciu, Ciprian, Levy-Abegnoli, Eric, Grossetete, Patrick, Cisco Press, 2006

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

"Internet Transparency," Request for Comments 2775, Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2775.txt?number=2775>.

"IPv6 Fix," Cho Kenjiro, Jinmei Tatuya, Kunitake Koichi, Shimojo Toshio, Takeuchi Sohgo, Yamamoto Kazuhiko, 2005. <http://v6fix.net/docs/wide-draft-v6fix.en>

"IPv6 Network Administration," Nall Richard Murphy and David Malone, O'Reilly Publishing, 2005.

"Multiprotocol Extensions for BGP-4" Request for comments 2858, Internet Engineering Task Force, June 2000 < http://www.ietf.org/rfc/rfc2858.txt?number=2858>

"Operational Considerations and Issues with IPv6 DNS," Request for Comments 4472, Internet Engineering Task Force <http://www.ietf.org/rfc/rfc4472.txt?number=4472>

"Transition Planning For Internet Protocol Version 6 (Ipv6)," Office of Management and Budget (OMB) Memorandum M-05-22, August 2005

APPENDIX C: 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 (ie, 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 (AH, 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