Department of Veterans Affairs

VA IPv6 Program Management Transition Office

IPv6 Enablement Support Services

IPv6 & USGv6 Compliance Test Capability - Draft

CLIN #: 0004AA

Contract: VA118-11-P-0096
Solicitation Number: VA118-11-RP-0611

February 23, 2012

Version 0.1

THE VENTURA GROUP, INC.

Revision History

Version	Purpose	Author	Function	Date
v1.0	Initial	TVG		02/23/2012

* The following symbols can be used to represent the type of change noted:

A = Added
M = Modified
D = Deleted

Table of Contents

1 EXECUTIVE SUMMARY 5

2 INTRODUCTION 8

2.1 REVIEW PROCESS 8
2.2 DOCUMENT USES 9
2.3 DOCUMENT OVERVIEW 9
2.4 MEDICAL DEVICE SPECIFICATIONS 13

3 VA MISSION CONSIDERATIONS FOR IPV6 COMPLIANCE TESTING 14

3.1 VA ENTERPRISE NETWORK CHALLENGES OF IPV6 14
3.2 VA EXISTING TEST CAPABILITIES 18
3.2.1 Enterprise Security Test Lab Solutions, located in Falling Waters, WV 18
3.2.2 Testing 20
3.2.3 Internet Gateway Lab, Falling Waters, WV 25
3.2.4 ESE Lab, Washington, DC 27
3.3 MEDICAL DEVICE COMPLIANCE TESTING 28
3.3.1 Medical Device Regulation 29
3.3.2 Medical Device Standards 30
3.3.3 Medical Device Communication 30
3.3.4 IEEE 11073: Health informatics - Medical/Health Device Communication Standards 32
3.3.5 Medical Device IPv6 Interoperability Compliance Testing 38

4 RELATED FEDERAL IPV6 TEST PROGRAMS 38

4.1 USGV6 TEST PROGRAM 38
4.1.1 USGv6 Test Process Overview 39
4.2 DOD IPV6 TESTING 42

5 VA IPV6 COMPLIANCE TESTING APPROACH 43

5.1 COMPLIANCE STRATEGY 44
5.2 SUCCESSFUL IPV6 DEPLOYMENT AND VA IPV6 COMPLIANCE PROCESS 47
5.3 IPV6 COMPLIANCE AND TAXONOMY OF DEVICE 49

6 ACHIEVING VA IPV6 COMPLIANCE – TESTING CLASSES 50

6.1 VA-SPECIFIC IPV6 TESTING CLASSES 51
6.1.1 USGv6 Compliance – IPv6 Conformance Testing 51
6.1.2 USGv6 Compliance – Interoperability Testing 53
6.1.3 VA IPv6 Compliance – Performance Testing 54
6.1.4 VA IPv6 Compliance – Regression Testing 57
6.1.5 VA IPv6 Compliance - Functional Testing 57
6.1.6 VA IPv6 Acceptance Testing 58
6.1.7 IPv6 Application Testing 59

7 VA IPV6 COMPLIANCE TEST ENVIRONMENTS 59

7.1 IPV4-ONLY 60
7.2 DUAL-STACK 61
7.3 IPV6-ONLY 62
7.4 TESTING THE TESTER 62

8 VA IPV6 PROFILE DEVELOPMENT PROCESS 64

8.1 VA IPV6 PROFILE APPROACH 64
8.2 VA IPV6 DEVICE COMPLIANT PROFILE TOOL 65
8.3 VA IPV6 COMPLIANCE SDOC REQUIREMENTS 67
8.4 VA IPV6 DEVICE COMPLIANT PROFILE AND SDOC REGISTRY 73

9 VA IPV6 PROFILE DEVELOPMENT CLASSES 73

9.1 HOSTS 74
9.1.1 Desktop/Laptop 75
9.1.2 Servers 75
9.1.3 Network Appliances 75
9.1.4 Medical Devices 75
9.2 ROUTERS 75
9.3 SWITCHES 76
9.3.1 L2-only 76
9.3.2 L3-aware 76
9.4 NETWORK PROTECTION DEVICES 76
9.4.1 FW 77
9.4.2 APPFW 77
9.4.3 IDS / IPS 77
9.5 APPLICATIONS / SW 77
9.6 SERVICES / ISPS 78
9.7 COMPARISON WITH USGV6 AND DOD 78

10 USGV6 LAB ACCREDITATION REQUIREMENTS 79

10.1 BENEFITS FOR VA BECOMING A USGV6 AND ISO 17025 ACCREDITED LAB 79
10.2 ISO 17025 ACCREDITATION REQUIREMENTS 80
10.2.1 ISO 9001 Accreditation (Optional) or a Quality Management System (Required) 81
10.2.2 ISO 17025 Test Lab Processes Required for Accreditation 81

11 VA IPV6 TEST LAB REQUIREMENTS SUMMARY 84

12 NEXT STEPS 89

12.1 DEFINING VA SPECIFIC GOALS 89
12.2 METHODOLOGY 89
12.3 EXECUTION 89
12.4 EVALUATION 90
12.5 REPORTING 90

13 REFERENCES 92

14 APPENDIX 1 – SAMPLE VA IPV6 HOST PROFILE 93

15 APPENDIX 2 – VA IPV6 PROFILE MATRIX – PROFILE CLASSES 95

16 APPENDIX 3 – VA IPV6 PROFILE MATRIX – RCF DESCRIPTIONS 96

17 APPENDIX 4 – MEDICAL DEVICES COMMUNICATIONS SPECIFICATIONS 97

List of Figures

FIGURE 1: VA IPV6 PROFILE PROCESS DEVELOPMENT 5
FIGURE 2: PROFILE CLASSES COMPARISON FOR USGV6, DOD AND VA 6
FIGURE 3: VA IPV6 TEST PROCESS EXPANSION FROM THE USGV6 TEST PROCESS 7
FIGURE 4 - VETERANS AFFAIRS HIGH-LEVEL WIDE AREA NETWORK ARCHITECTURE 14
FIGURE 5: IPV6 ARCHITECTURE AT THE ESSTL 25
FIGURE 6: INTERNET GATEWAY LAB CONFIGURATION 26
FIGURE 7: ESE LAB CONFIGURATION 28
FIGURE 8: MEDICAL DEVICE COMPONENTS 34
FIGURE 9: ZIGBEE MODEL 37
FIGURE 10: SDOC PRODUCT SUMMARY 41
FIGURE 11: SDOC TEST SPECIFICATION STATUS 41

FIGURE 12: SDOC TEST STATUS NOTES 42
FIGURE 13: DOD UNIFIED CAPABILITIES APPROVED PRODUCTS LIST 43
FIGURE 14: VA IPV6 COMPLIANCE TEST CAPABILITY DEVELOPMENT STRATEGY AND PLAN 46
FIGURE 15: KEY BUILDING BLOCKS OF SUCCESSFUL IPV6 DEPLOYMENT 48
FIGURE 16: VA IPV6 TEST CAPABILITY REQUIREMENTS – TEST CLASSES 51
FIGURE 17: IPV6 COMPLIANCE CONFORMANCE TEST BED 52
FIGURE 18: INTEROPERABILITY REFERENCE TEST SETUP 54
FIGURE 19: SNIPPET TAKEN FROM THE CONFORMANCE MATRIX 65
FIGURE 20: SNIPPET TAKEN FROM A DEVICE PROFILE (WORKSTATION) 66
FIGURE 21: THE US IPV6 PROFILE AND DOD UNIFIED CAPABILITIES REQUIREMENTS PRODUCT CLASSES 79
FIGURE 22: LAB MANAGEMENT AND ISO 17025 LAB ACCREDITATION REQUIREMENTS 82
FIGURE 23: ICMPV6, MTU, SLAAC, UNICAST PACKET, SCOPED ADDR, ADDR SEL, IPSEC 85
FIGURE 24: RH0, RTR ALERT 86
FIGURE 25: SNMPV3 86
FIGURE 26: MLD, MULTICAST 87
FIGURE 27: LAYER 4-7 SERVER BENCHMARK 87
FIGURE 28: ISP TESTING 88
FIGURE 29: HOST VALIDATION CONFIGURATION 88

1 Executive Summary

The development of the USGv6 Profile Process and Test Program was initiated by the OMB 05-22 memorandum to provide agencies with a common taxonomy and framework to provide acquisition specifications for IPv6 devices and an industry-based test program. The USGv6 effort was later included in the FAR as a requirement for agencies to utilize when acquiring IT devices. While the USGv6 program developed and administered by NIST goes a long way to provide agencies with a valuable tool to acquire IPv6 compliant devices, a review of specific VA mission and IT infrastructure requirements identify several areas that require expansion to meet VA's IPv6 transition needs.

This document provides an approach to expand upon the existing NIST USGv6 Profile and Test capability to meet VA's specific mission and IT requirements. Figure 1 shows an overview of the approach utilized to create a comprehensive VA IPv6 Profile process based on USGv6 and taking into account DoD requirements for VA/DoD interoperability and industry IPv6 standards inputs. In addition, this method takes into account medical device standards and requirements to meet VA specific medical device mission requirements. This approach allows VA to provide a more comprehensive in its use of Internet and related standards to more fully provide device compliant profiles for VA.

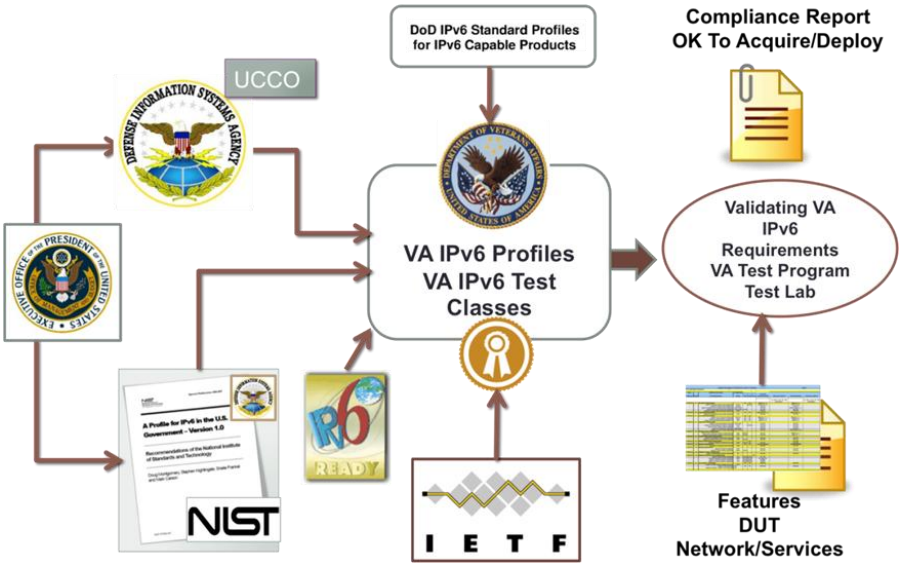


Figure 1: VA IPv6 Profile Process Development

The results of the VA IPv6 Profile process have been compiled into a VA IPv6 Profile Matrix that will be utilized as a tool to create device compliant VA IPv6 profiles. The tool is in the form of an easy-to-use excel spreadsheet that will allow VA profile developers to quickly develop specific IPv6 profiles based on specific requirements. In addition, a profile registry has been recommended as a method of registering profiles within VA for future use.

Furthermore, to expand the number of standards referenced, this effort expands upon the classes of devices identified within USGv6 to take into account a wider range of device classes utilized by the DoD. In addition, two completely new categories are added for "Application" and "Service" that will allow VA to develop specific standards-based profiles for a wider range of IPv6 acquisition and testing capabilities. Figure 2 shows the comparison of the USGv6 classes of devices compared with what is included within the DoD specifications and what are proposed for VA in this document.

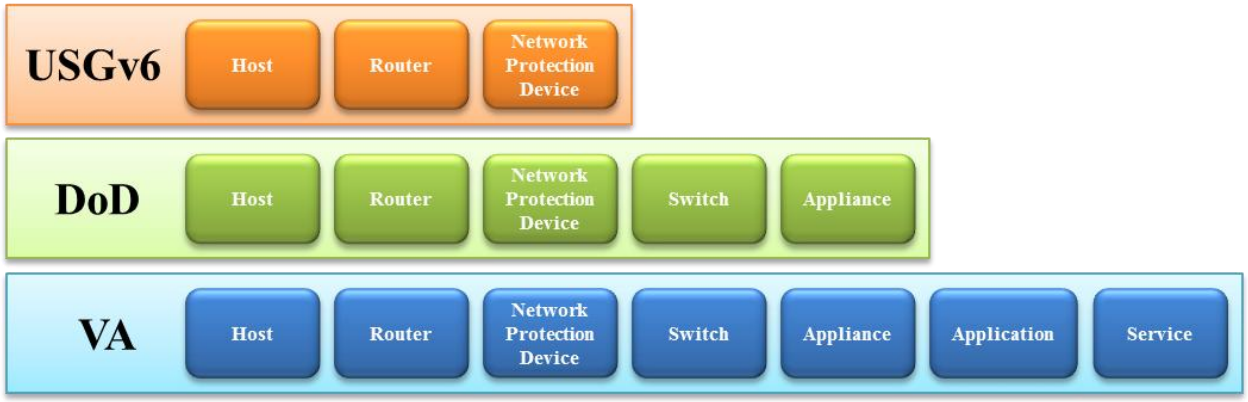


Figure 2: Profile Classes Comparison for USGv6, DoD and VA

Where the VA IPv6 Profile process expands upon the USGv6 Profile, the recommended VA IPv6 Compliance Test process contained within this document similarly expand upon the USGv6 Test Approach. Figure 3 shows the comparison of where the VA test process expands upon the compliance and interoperability tests included within USGv6 to add performance, regression, functional and VA compliance testing. These additional test suites close critical gaps VA requires to fully understand if and when an IPv6 product will meet specific mission and operational requirements.

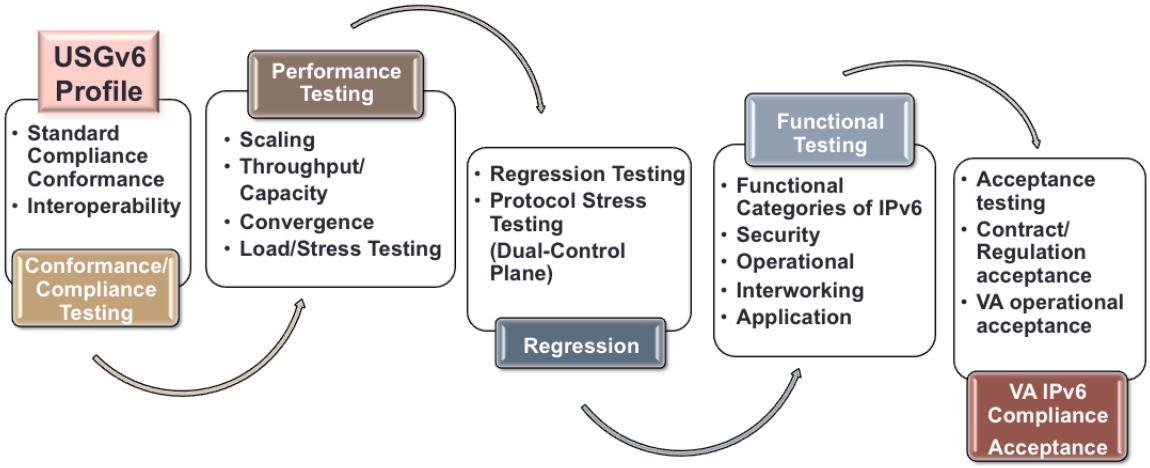


Figure 3: VA IPv6 Test Process Expansion from the USGv6 Test Process

Taken together, the VA IPv6 Profile Process and VA IPv6 Compliance Test Process provides VA with the critical tools necessary to acquire and test IPv6 products and provide the necessary level of assurance that will meet VA's mission requirements.

2 Introduction

This document defines and specifies IPv6 compliance specifications for VA. Its use can provide the VA with the ability to determine which network equipment and appliances meet the VA's IPv6 network requirements and determine the standards and specification that VA systems, equipment, applications, and devices must comply with in order to provide intended functionality in an IPv6 native environment. The specifications are based on the United States Government IPv6 (USGv6) profile and are supplemented with VA-specific IPv6 requirements that were not addressed in the National Institute of Standards and Technology (NIST) specifications.

This document is a VA IPv6 Compliant Testing Requirements Document that describes specific VA IPv6 Device profiles based on the USGv6 Profile, includes additional VA IPv6 requirements, and specifies minimum required configuration set for each network equipment type and minimal feature set for each application type.

This document will serve as the foundation for a VA IPv6 Compliant Test Design Document which will provide recommended methods for testing systems, equipment, applications, and devices for IPv6 compliance.

While considerable expertise and effort was employed to develop this document, it is recommended that the VA perform a rigorous internal and external review with stakeholder and other interested parties.

2.1 Review Process

It is recommended that the VA implement a formalization strategy for the IPv6 compliance specifications. While the included requirements and specifications are based on known standards, it is likely that most vendor hardware and software will be incapable of meeting all specifications for a given profile.

It is, therefore, recommended that the requirements and specifications be vetted by VA personnel with network and application expertise, VA enterprise architecture, and their industry partners, vendors, and value added resellers. Once a VA internal review is complete, it is recommended

that the VA request NIST review the profiles for IPv6 networks and applications and for medical device specifications. Additionally, the VA could issue a Request for Information (RFI) to industry to see if the profile requirements and specifications can be met in the required timeline.

Upon completion of the review, the profile requirements and specification would have dramatically more useful application across the VA, including architecture, engineering, and procurement activities.

2.2 Document Uses

This document has multiple, potential uses. The requirements and specifications defined here will have a direct use in defining test methods, procedures, and tools and in making the VA IPv6 test environment operational. In many cases it can support the development of vendor compliance testing for hardware, software, appliances, and devices and can be used in VA test labs to perform specific or integrated tests on individual system elements or integrated systems.

Another valuable use of this information is the development of future enterprise architectures that rely upon IPv6 infrastructure. These standards and specifications can serve as the foundation for communications technical architecture. The capabilities of IPv6 can then drive other architectural views that can dramatically impact the VA's communications future.

Another immediate use of the identified standards and specification profiles will be to translate them into procurement language. Upon completion of testing within various VA domains, the delta between capital equipment on-hand versus what is needed will become clearly understood. This document will serve as a guideline for procurement profiles and procurement standards and specifications for all related communications equipment. For engineering and design activities, this document can serve as a guide for trade-off studies with regards to functionality and services.

2.3 Document Overview

Section 1 - Executive Summary - provides a high level overview of the document contents.

Section 2 – Introduction – presents a capsule review of the specific subject matter discussed in each section.

Section 3 – VA Mission Consideration for IPv6 Compliance Testing - provides a description of the VA network topology along with a description of the enterprise services and the routing architecture. This discussion is required to address the complexities of the VA Enterprise as a whole. The VA Enterprise is designed around dual-plane core routing architecture provided by two separate Multi-Protocol Label Switching (MPLS) transport service providers, AT&T and Quest. A variety of WAN services such as Unicast, MPLS VPN, Multicast, Traffic Engineering, and Quality of Service are provided simultaneously. All of these services require different protocols, routing tables, routing methods, interoperability, and interworking running simultaneously that extend beyond the current testing provided by the USGv6 Profile.

It also reviews several of existing VA lab facilities from the perspective of their ability to test devices, applications, and services in IPv4 only, dual stack, and IPv6 only modes. While each lab's capabilities vary distinctly based on their primary purpose, they all have basic capabilities to test in IPv4 only mode, and are developing dual stack and IPv6 capabilities. The Enterprise Security Test lab in Falling Waters, WV, appears to be the most advanced in terms of mandate, technology base, and methods and procedures.

Testing of medical devices is reviewed from the perspective of the Food and Drug Administration's and the National Institute for Standards and Technology's (NIST) medical device profiles for communications using the OSI/IEEE X73 standards. It also addresses the testing of medical device communications, and several standards applicable to Health Informatics devices.

Section 4 – Related Federal IPv6 Test Programs - provides a detailed overview of the USGv6 testing standard developed by the National Institute of Standards and Technology (NIST SP 500-267), and addresses the test process, test specifications, and the Suppliers Declaration of Conformity (SDoC) requirements. A brief overview of the Unified Capabilities Requirements (UCR) standards profile is provided as a background to the development of the NIST USGv6 standards.

Section 5 – VA IPv6 Compliance Testing Approach - focuses on the VA IPv6 Compliance strategy approach establishes a direction for the agency to develop a comprehensive IPv6 &

USGv6 compliance test capability for IPv6 capable devices that takes into account all the latest developments and lessons learned from deployments in both large and medium service provider and enterprise networks across the world. The VA IPv6 compliance test capability is being designed keeping the test objectives based on the OMB mandate, which expects that all IT systems comply with IPv6 conformance, performance, interoperability, information assurance, stability and longevity without disrupting the current operations of the agency.

The section discusses the strategy and plan taking input from USGv6 profile process, DoD IPv6 profiles, experiences learnt from the IPv6 ready program and standard development organizations such as IETF. In this section we also share key IPv6 building blocks are considered as basis for VA IPv6 test capability requirements ensuring a successful transition to the IPv6 in VA networks.

Section 6 – Achieving VA Compliance – Testing Classes - discusses the VA test classes and includes a comprehensive list of test classes that all IPv6 capable products, services and application should undergo before any acquisition for live deployment in any of the VA networks. VA IPv6 test capability requirements extends these testing classes further to ensure that the products, applications and services that are needed by VA are evaluated comprehensively ensuring the compliance of the SDoC provided by the vendor. The VA test classes will consist of test cases that are based on VA use cases and validate the device under test for compliance to the VA deployment requirements. The section also describes the co-relation between all the test classes and the path VA should consider when subjecting IPv6 capable products through this evaluation process.

Section 7 - Test Environment – provides baseline testing parameters that, when specified and deployed, will be sufficient to ensure compliance/conformance and interoperability based on the requirements in both the relevant USGv6 Product Profiles as well as the VA-specific profiles. This is meant to not only comply with the FAR, but to also meet the VA-specific mission requirements (specifically including, but not limited to, the areas of functionality, security, software).

Section 8 – VA IPv6 Profile Development Process - defines the VA Conformance Matrix - a list of product classes and relevant specifications, combined to provide the definition of what "IPv6-capable products" means within the VA. The Conformance Matrix is intended to provide the guidance in the creation of specific device profiles, which will simply be a specific product class from the matrix with all of the conditional parameters identified as relevant or not. Once the device profile has been defined, this can be used by procurement, vendors, testing personnel, etc. in order to insure the best possible, IPv6 capable, outcome for the VA.

Section 9 – VA IPv6 Profile Development Classes - describes the Profile Development Classes utilized in conjunction with the VA IPv6 Profile Process. Within the NIST USGv6 Profile these classes focused on devices and were broken into three high-level categories: host, router, and network protection device. DoD also focused on device specific classes, but had a more granular breakdown of devices. In order to maintain greater interoperability with DoD and meet USGv6 requirements, VA took the combination of the device classes; however, VA went on to extend the profile development process beyond devices to include applications and services.

Section 10 – USGv6 Lab Accreditation Requirements - lays out the NIST and U.S. Government IPv6 (USGv6) testing approach and lab accreditation process. The process requires a prospective lab to undergo ISO 17025, NIST USGv6 special requirements, and quality management accreditations prior to any lab being authorized to test products for their compliance to the US IPv6 Profile. Each lab is also accredited for which role they play to procurement. In VA's situation, the 2nd Party Lab Accreditation would apply. In this section, all the requirements necessary for accreditation are discussed.

Section 11 – VA IPv6 Test Lab Requirements Summary - addresses the basic requirements for an IPv6 Test Lab in terms of facility and network and testing environment. The environment is comprised of network communication interfaces, network hardware, operating system software, and application software that are configured to provide assessment capabilities including native IPv6 capabilities, IPv4 over IPv6 tunneled capabilities, IPv6 over IPv4 tunneled capabilities, and dual stack IPv4/IPv6 capabilities. The section includes several scenarios of test equipment configurations.

Section 12 – Next Steps - defines VA specific goals as potential next steps. Use of this document will serve as the foundation for a VA IPv6 Compliant Test Design Document which will provide recommended methods for testing systems, equipment, applications, and devices for IPv6 compliance. Several specific goals can be achieved for the Core mission communities and the infrastructure as a whole through the application of Methodology, Execution, Evaluation, and Reporting methods and tools.

2.4 Medical Device Specifications

Medical device specifications are addressed from the perspective of the Food and Drug Administration's and the National Institute for Standards and Technology's (NIST) medical device profiles for communications using the OSI/IEEE X73 standards. These profiles address the layers of the OSI networking model and Wireless Personal Area Network wPAN technologies such as Bluetooth, Universal Serial Bus (USB), and ZigBee protocols. It is assumed that the medical devices capable of communicating via the Internet Protocol are tested for interoperations with IPv4. Since medical devices must adhere to standards at the application, presentation, session, and transport layers of the OSI model, these layers must be tested to ensure they are compatible with IPv6 at the network layer. If integration problems occur, there may be a need to develop "shim" protocols to solve these issues. Additionally, medical devices in a wPAN environment must communicate in a limited bandwidth environment. The size of the IPv6 header, the use of extension headers, and potentially large payloads in IPv6 packets could be an issue. Therefore, compression methods or IPv6 fragmentation may be necessary on networks with small Maximum Transmission Units (MTUs).

Appendix 4 contains a table of detailed requirements for medical devices communications.

3 VA Mission Considerations for IPv6 Compliance Testing

3.1 VA Enterprise Network Challenges of IPv6

The Veterans Affairs WAN architecture as depicted in Figure 4 - is a hierarchical network design implemented based on industry best practices. It utilizes a dual-plane core routing architecture provided by two separate Multi-Protocol Label Switching (MPLS) transport service providers, AT&T and Quest.

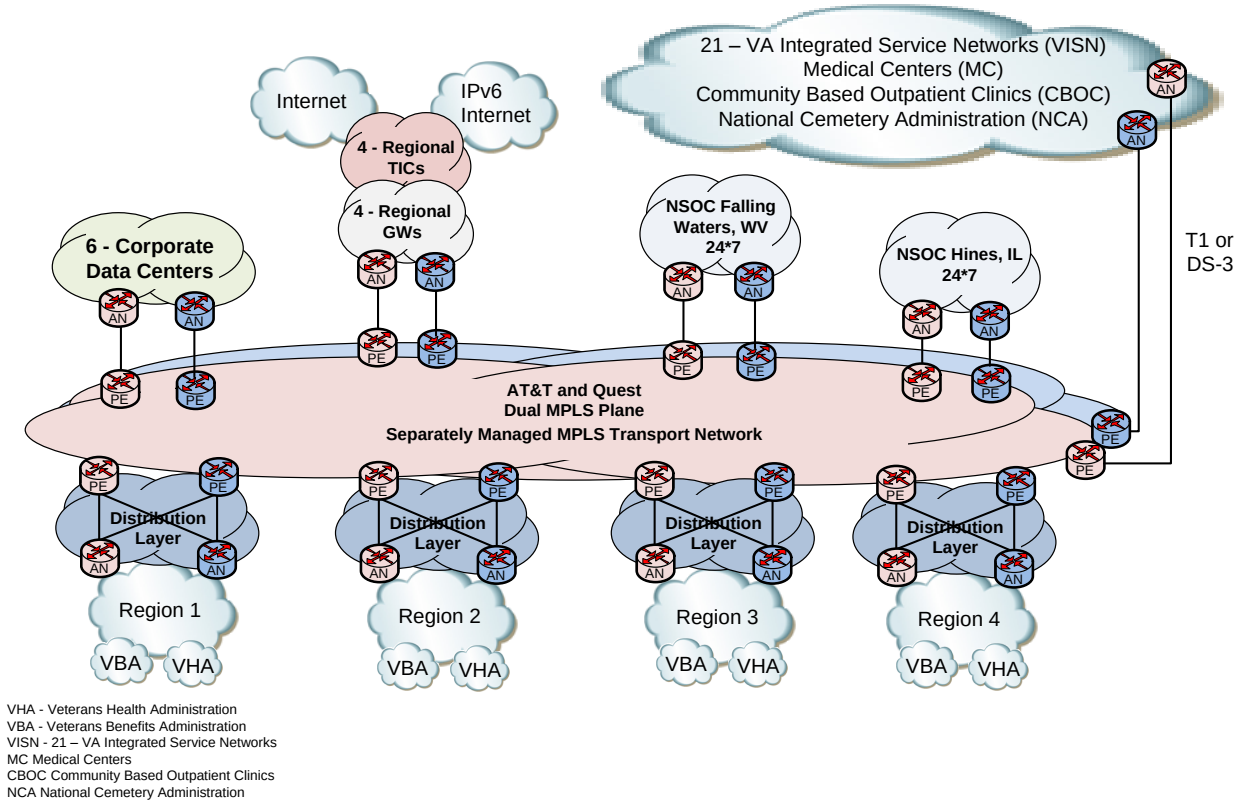


Figure 4 - Veterans Affairs High-Level Wide Area Network Architecture

The VA Architecture exploits routing protocol features in innovative ways to meet the performance requirements of VA customers. A variety of WAN services such as Unicast, MPLS VPN, Multicast, Traffic Engineering, and Quality of Service are provided simultaneously. All of these services require different protocols, routing tables, and routing methods.

The routing architecture is presently hierarchical and defined as core (along with MPLS label switching), distribution, and access (region) layers. This design is very effective for the VA enterprise network because it separates the backbone network roles and responsibilities from the customers, which improves scalability, performance, maintenance, stability, and security of the core network. The core layer provides high-speed backbone transport (from T-1 to Gig-E connections) and aggregates the distribution nodes.

The two routing protocols used within the VA network are Enhanced Interior Gateway Routing Protocol (EIGRP) and Border Gateway Protocol version 4 (BGPv4). EIGRP is highly preferred in order to take advantage of existing VA expertise and to be compatible with current infrastructure deployments. For interoperability, Open Shortest Path Forwarding (OSPF) is also under consideration and may be required as a standards-based alternative to EIGRP for compatibility between venders.

Interior routing is provided by Cisco model 7206 routing platforms configured for EIGRP, an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router.

The VA Enterprise resembles an Internet Service Provider (ISP) more than an enterprise network. Each of its customers is a separate autonomous network, has its own Autonomous System Number (ASN) and typically requires a variety of network services.

VA customers include:

- VHA - Veterans Health Administration,
- VBA - Veterans Benefits Administration,
- VISN - 21 VA Integrated Service Networks,
- MC - Medical Centers,
- CBOC - Community Based Outpatient Clinics, and
- NCA - National Cemetery Administration.

VA customer connections are accomplished via distribution nodes that aggregate Interior Gateway Protocol (IGP) routes within each of the four regions. Distribution nodes consist of a pair of routers, where the Provider Edge (PE) router is carrier-managed and the Access Node (AN) router is VA managed.

To communicate with external networks, Border Gateway Protocol (BGP) is implemented to separate the infrastructure routes from the customer routes and to control routing relationship between customer and external routing domains. Router next-hop reachability is resolved using different techniques depending on which of the following services are provided.

- Unicast (which includes standard IP and MPLS label switched path) uses BGP next-hop,
- MPLS Layer 3 VPN uses VPN Routing and Forwarding (VRF) table, or
- Multicast uses Reverse Path Forwarding (RPF).

For inter-AS traffic, BGP load sharing is implemented to allow AN routers to distribute outgoing and incoming traffic among multiple paths, taking advantage of the dual-plan MPLS architecture and distributing traffic equally. Each customer AS will have two exit points out of the Region via a circuit to each MPLS carrier network. The AN distribution routers will eBGP peer with both MPLS networks (a peer with AT&T AS 7018 and a peer with Qwest AS 209). Equal cost routing is implemented at distribution nodes so traffic is load shared between both MPLS connections.

Summary of VA ASNs[1]:

AS3143 VANET - Dept. of Veterans Affairs

AS29992 VA-TMP-CORE - Department of Veterans Affairs

Upstream VA Adjacency List:

[1] Source http://bgp.potaroo.net/

AS209	ASN-QWEST - Qwest Communications Company, LLC
AS10886	MAX-GIGAPOP - University of Maryland
AS1239	SPRINTLINK - Sprint
AS16967	SBCIDC-DLLSTX - AT&T Internet Services
AS7018	ATT-INTERNET4 - AT&T Services, Inc
AS4263	CERNET - California Education and Research Federation Network

For inter-AS traffic, symmetric routing is implemented to deliver traffic over the same path in both directions, optimize bandwidth utilization on links, enhance the ability to perform stateful inspection, and prevent traffic bouncing between ASs. VA Regions must split ingress and egress routes so one-half of their routes prefer one distribution node while the remaining routes will prefer the second distribution node.

The use of the Multi-Exit Discriminator (MED) attribute to set metrics provides external neighbors with the preferred path into an AS when there are multiple entry points into the AS. Additionally, the use of BGP communities are used to tag specific subnets, allowing BGP routes to be identified and metrics set according to specific route policies. All inbound routes from the MPLS networks to a region will have a specific community associated with them. The router configurations will set metrics inbound and outbound for routes using communities.

AN distribution routers have iBGP peering with each AN router within that region to exchange BGP routes. The routers will be configured to forward only the networks that belong to that region, which is accomplished with the use of route maps and prefix lists defining the prefixes belonging to a region.

Internet access is provided by four regional (one in each region) One-VA Trusted Internet Connection (also known as TIC, Office of Management and Budget (OMB) Memorandum M-08-05) Gateways that have been implemented to identify all system interconnections

and consolidate them into four VA gateways. The TIC optimizes the security of external network connections to the Internet.

Enterprise services delivered by the VA Enterprise to customers consist of:

- Web Services
  - HTTP
  - HTTPS
- Exchange E-Mail

The network is managed by two VA Network Security and Operations Center (NSOCs). Network Management is supported by the enablement of Simple Network Management Protocol (SNMP) on network devices, Secure Shell (SSH)/TACACS for in band access, System Logging (Syslog) of network events, and centralized Administration, Authentication, and Accounting (AAA). The network management application SolarWinds is used to monitor routers, switches, and provide configuration management and HP OpenView (NNM) is used for monitoring the status of managed nodes.

From a holistic view, IPv6 testing and evaluation requirements for the VA WAN extend beyond the current testing under the USGv6 Profile. The VA's unique requirements to test interworking between MPLS, EIGRP, BGP, IA, and Network Policy are so complex they are not considered by the USGIPv6 Profile. Therefore, the VA WAN T&E requirements for IPv6 must include testing that can only be satisfied by extensive system level testing utilizing the operationally fielded network configurations, with devices emulating the deployed environment.

3.2 VA Existing Test Capabilities

VA testing capabilities for devices, applications, and services are distributed amongst several lab facilities. Reviewed here are the following:

3.2.1 Enterprise Security Test Lab Solutions, located in Falling Waters, WV

3.2.1.1 Mission

Enterprise Security Test Lab Solutions serves as a security test and review environment for any VA Stakeholder who has a set of requirements and a need to know the validated security configuration profile of his hardware/software. As a part of the Office of Information Protection and Risk Management (IPRM), the Enterprise Security Solutions Test Lab (ESSTL), provides the VA with a holistic testing approach where performance, integration, and interoperability are evaluated.

The Integration Test Lab (ITL) mission is to provide an objective test environment to support all VA OI&T project initiatives, VA-NSOC security patch implementation, new product evaluations, security guidelines and policy compliance for VA IPRM through the testing of approved or pilot security architecture components. The ITL will provide measurable, repeatable input/output processes, system test criteria, and policy support and development for LAN/WAN Enterprise Architecture (EA). For ITL purposes the LAN/WAN EA is defined by the following three system characteristics: standard desktop operating systems and servers, standard software application suites residing on those systems, and standard configurations of the operating systems and application suites.

The ITL will develop and deliver detailed test reports and implementation guidance to the primary stakeholders regarding the outcome of its testing activities.

The ESSTL is charged with:

- Analyzing security configuration: change requests for new and emerging technologies;
- Testing new and emerging technologies: for compliance with NIST and other industry security standards;
- Analyzing business line security requirements based on input from the line's requirements documentation;
- Offering input and best practices on VA security policies and Federal mandates to ensure that new technologies comply;

- Providing input on proposed applications, systems and products;
- Testing and evaluating product security and interoperability within existing VA architectures; and
- Conducting monthly security testing reviews for patches and applications to mitigate risks and vulnerabilities.

The ESSTL has supported the following projects and programs:

- Antivirus (AV),
- Intrusion Prevention System (IPS),
- Data Loss Prevention (DLP),
- Medical Device Isolation Architecture (MDIA),
- Remote Computer Access,
- Federal Desktop Core Configuration (FDCC),
- Windows 2008 Server Security Hardening Guidelines, and
- VA Chief Information Officer Program Initiatives.

3.2.1.2 Operations

The ITL operations are centered around security performance, integration, and interoperability (PI&I) tests on any additions or changes to the OCIS core security architecture to insure the security of the predefined architecture is maintained at the highest possible level of confidence. Tests are designed to verify that a product does what it is advertised to do and nothing more, decreases or maintains the current risk level, and does not affect the performance or reliability of other applications or systems within the OCIS security architecture.

3.2.2 Testing

The ITL responds to three types of test requests. These are further explained in the paragraphs below. Both new and standing requests need to be in writing. The ITL tests products that add to

or change the security architecture, with approval by the ESSS Director. Requests can be made to ESSS in email VA ESSS@va.gov or hardcopy form to the ESSS Director. Requests must include the name and contact information of the requestor and or sponsor. A product details worksheet must include: product point of contact (POC), name of the product, desired deployment date, operating system, any unique connectivity issues, product status (whether new or replacement), and who is funding the project. New requests must include the system sensitivity categorization, preliminary risk assessment, test criteria, and use-case requirements documents that specify the desired deliverables from ITL, recommendations, test reports, and other implementation guidance. New requests may be changed to standing requests if there is perceived repetitive process requirement. A single change to the architecture would be a new request. Examples such as high priority security patches that affect the VA LAN/WAN EA or security architecture will be tested and a detailed security guide produced for the patch installation. Requests must include the name and contact information for the POC, the name of the product or appliance impacted, and the form in which the test report should be delivered.

3.2.2.1 Testing Methods

A common test methodology will be used to test every product. Specific tests will be used for each type of product tested. Depending upon the source of the product to be tested the scope of testing can evolve from simple compliance evaluations called Initial Product Review (IPR) to full domain integrated testing. Each level of testing builds criteria and understanding for the next level and provides valuable feedback to the VA for planning and executing security programs.

Test criteria are as follows:

> **Initial Product Review** - (IPR) evaluations are simple compliancy checks of the known product features e.g. FIPS 140-2 validated, known vulnerabilities, compliance with VA 6500, and special features. This level of evaluation is conducted when no VA requirements have been defined and the product shows potential value to the VA security posture. The source of this review is predominantly vendor discussions or ITARS requests. An IPR has two basic features; the product is not being directly evaluated in a "hands-on" environment, and no VA requirements have been clearly defined.

Security Assessment Report - (SAR) is a "hands-on" test of a product similar to an IRP where the product is directly evaluated, but no VA requirements have been clearly defined. An example of this would be the evaluation of Apple devices e.g. Ipad or iPhones and the competing eReaders or SmartPhones.

Evaluation Test Plan - (ETP) is a well planned and executed evaluation of a specific product against a pre-determined set of VA criteria defined by a program office or program manager. The ITL conducts keystroke by keystroke testing of the exact specification defined by the requestor. ITL personnel are not at liberty to modify any part of the test requirements without direct written consent of the program manager, even when they know something will fail. Tests are primarily a checklist from which there is no deviation or undefined tolerances.

One of the following methodologies listed below is used for testing:

3.2.2.1.1 Common Testing

Each product, independent of type, will be tested to insure it meets all of the following seven attributes or an implementation or configuration can be found such that the product can meet these attributes:

1. Corrects a vulnerability or provides an additional capability,
2. Does not introduce hidden functionalities which may be misused,
3. Does not reintroduce any old vulnerabilities,
4. Does not introduce any new vulnerabilities,
5. Does not degrade system reliability,
6. Does not degrade performance, and
7. Does not impair any critical applications interoperability.

Each product will be closely monitored within the testing environment to evaluate the impact of its modifications and affects upon a predefined computing environment.

3.2.2.1.2 Application Testing

Applications to be tested will be loaded on the ITL's standard systems. All required changes will be captured and reviewed for policy and security compliance. The system will then undergo PI&I assessment testing for ports, services, and protocols (PSP) using an active port scan, internal lab HIPS, and detailed administrative level scanning with standardized scanning tools to insure the application does not expose the machine to greater risk than before. A final report indicating the installation procedures and configuration for a secure policy compliant application, and lessons learned, will be completed and sent to the ESSS Director for approval and disposition.

3.2.2.1.3 Network Device Testing

Network devices will be introduced into the ITL integration testing network and configured as if they were within the VA network. All network changes will be captured and reviewed for policy and security compliance. The device will then be PI&I tested to insure the device did not expose the network to greater risk than before. If the network device is an active device then network load testing will also be accomplished to insure the device will not adversely affect the characteristics of the network. A final report indicating the installation procedures and configuration for a secure and policy compliant network device, exceptions noted, will be completed and sent to VANSOC for approval and disposition.

3.2.2.1.4 Appliance Testing

Any appliance machine (workstation or other device) will be introduced in the ITL integration testing network where appropriate and configured as if it were within the VA network. All network changes will be captured and reviewed for policy and security compliance. The appliance will then be PI&I tested to insure the appliance did not expose the network to greater risk than before. If the appliance is an active device then network load testing will also be accomplished to insure the appliance will not adversely affect the characteristics of the network. A final report indicating the installation procedures and configuration for a secure and policy compliant appliance, exceptions noted, will be completed and sent to IPRM for approval and disposition.

3.2.2.2 Reporting Method

The ITL will fully document all installation and configuration parameters in an Evaluation Test Plan report and will fully document all host and network policy and security findings in regards to each product tested. This will include a risk assessment based on a risk matrix provided by the requestor and gathered before and after the product testing. The preliminary results will be sent to the Director of ESSS approval. Once approved by ESSS, a final report will be sent to the product POC identified in the initial request and to IPRM for use as necessary in security policy development. The report will either be in secure email or hardcopy form and will not be shared with others unless approved by the ESSS Director and the product POC. In addition, the ITL will make a recommendation as to whether the product should become part of the VA core security architecture.

3.2.2.3 Safety

Using the ESSTL ensures that products meet security requirements prior to deployment. Through simulated VA environments, the lab has developed a testing mechanism to identify risks and develop strategies to protect VA information and systems. The lab offers users a more detailed level of security evaluation. It is an avenue that can be leveraged to build compliancy into existing or proposed applications or systems in accordance with NIST SP 800-64, Security Considerations.

All applicable VA safety regulations are adhered to and govern VA-ITL safety.

Safety regulations include:

VA Directive 7700, Occupational Safety and Health, dated July 8, 1998,

VA Handbook 7700.1, Occupational Safety and Health, dated July 8, 1998,

VA Handbook 5091, Occupational Health Services, dated April 15, 2002.

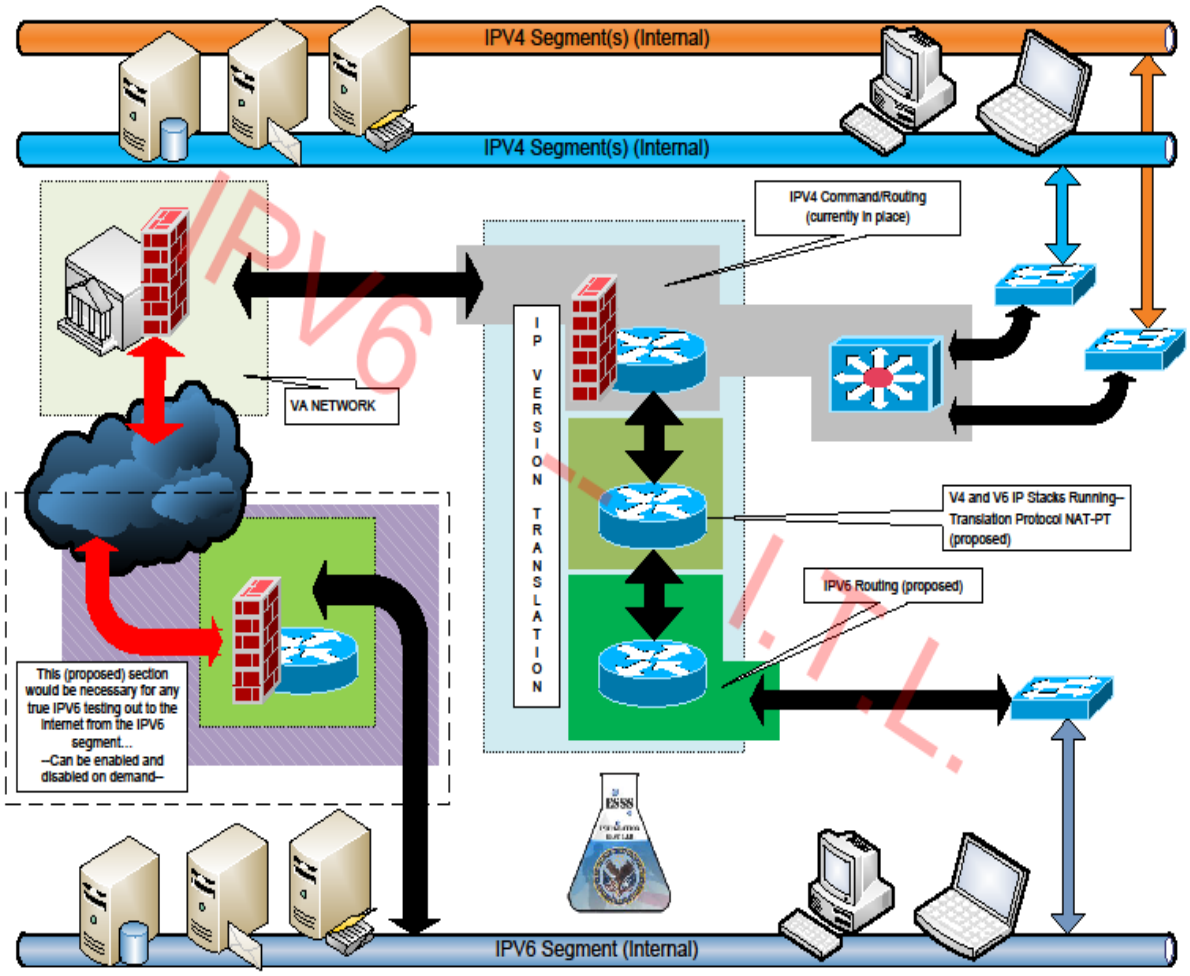


Figure 5: IPv6 Architecture at The ESSTL

3.2.3 Internet Gateway Lab, Falling Waters, WV

Purpose:

- Develop and validate fixes to existing Gateway issues,
- Test software/hardware updates,
- Develop and validate new Gateway functionality, and

- Training platform for understanding the Gateways.

The Internet Gateway lab can be used for a number of purposes. The Operations Support engineers use the lab to design changes requested by the VA. The Gateway Operations Midnight shift engineers could use the lab to understand and validate proposed changes. Additionally, items such as software/hardware upgrade testing as well as training on the gateways can be accomplished.

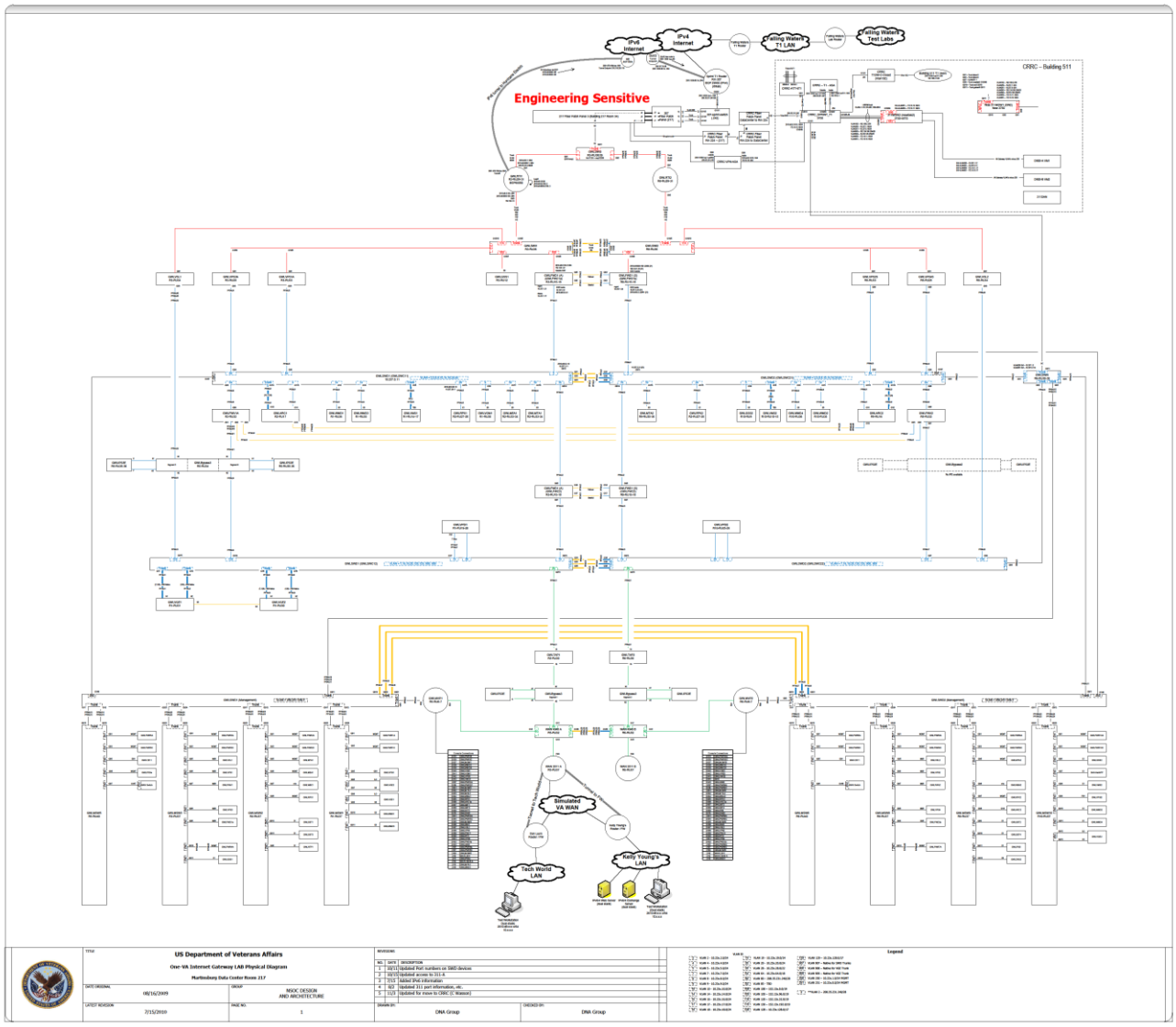


Figure 6: Internet Gateway Lab Configuration

In January 2012, the Internet Gateway lab successfully tested IPv6 transmissions, and as a result the Internet Gateway is receiving SMTP email from the Internet over IPv6. Four AAAA records were added to the mx20.va.gov email server definitions in DNS the same way as done for IPv4. The DNS will only hand out one A and one AAAA at a time, but subsequent requests will "round robin" through all four. These AAAA records point to F5 proxy devices in all 4 gateways, and those forwarded by email to the IronPort email devices over IPv4.

Statistics for the first 10 hours showed that about 1 in 200 or ½ of 1 percent of incoming email messages were coming in via IPv6. The VA is now showing "green" for all three public-facing network services – DNS, Mail, and Web – and for DNSSEC.

3.2.4 ESE Lab, Washington, DC

Intended to showcase IPv6 technologies via this lab, ESE uses it for IPv6 protocol testing. It is not being used to connect the IPv6 portion with internet connectivity to the backbone portion.

Testing capabilities include:

- Routing – the backbone portion to be isolated from the internet/internet2 connectivity;
- Basic Network Services (DC, DNS, DHCP) – set up to deal with DNSv6 and DHCPv6. Regarding Domain Controller - need to team up with the Lab in Falling Waters, WV for a more realistic setup;
- Network Security (FW, IDPS, security appliances) – tested the Cisco ASA and returned the on-loan units. For anything further, one needs to couple with the WAN Lab in Martinsburg WV;
- Other Network Services –currently have two tunnel servers from Hexago and NAT64 from Datatek; and
- User applications – only web and email services at this time.

The test process is developed through test cases per VA client requirements. The process and test results are documented, and a summary report is prepared afterward.

Recent success on the IPv6-only capabilities include completions of DNSv6, DHCPv6, HTTP(s), and email testing in 2010 and early part of 2011. The ESE Lab shared the DNSv6 and DHCPv6 test results with Microsoft Sales Representative and got good marks.

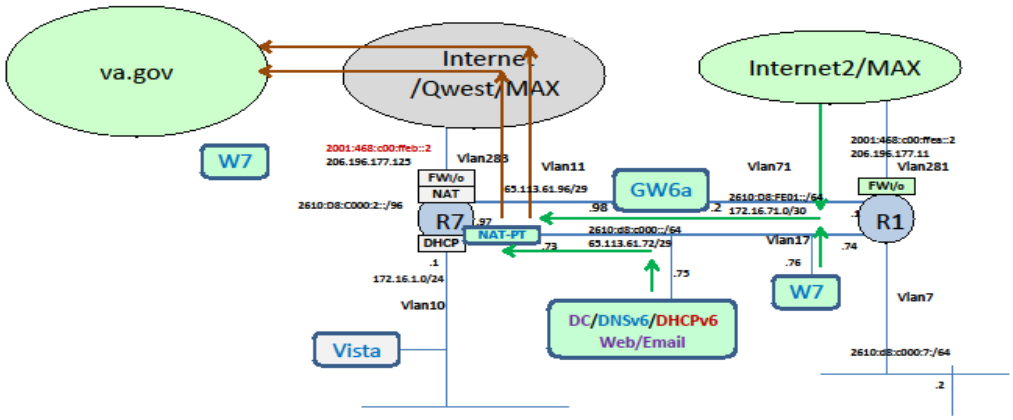


Figure 7: ESE Lab Configuration

3.3 Medical Device Compliance Testing

Medical device testing will be a critical aspect of the VA's transition to IPv6. Medical device communications is defined by the Food and Drug Administration's and the National Institute for Standards and Technology's (NIST) using OSI/IEEE 11073 (X73) standards. The X73 standards family addresses all of OSI layers and depends on many aspects of Wireless Personal Area Network wPAN technologies. AS medical devices are integrated into LANs so as to interact with networked, client/server applications, they must become Internet Protocol aware. Today, this means that many medical devices must interoperate over IPv4 and must be

transitioned to IPv6 as the infrastructure transitions to the new protocol. In essence, this means that the VA will need to ensure that medical devices are capable of communicating in an environment with which they may not have been built to interact. In order for medical devices to communicate in an IPv6 network environment there may be a need to develop "shim" protocols to ensure that session and transport segments can utilize IPv6 network services and to ensure that IPv6 can be encapsulated into wPAN frame technologies. IPv6 technology could be used to support IPv6 transport over constrained bandwidth environments.

Existing test programs, including those available from medical device vendors or NIST are likely insufficient to provide the assurance needed by the VA with regards to medical devices. These devices, used for patient care, are critical to health care service and can impact life or the quality of life. Therefore, it is critical that the VA advance the capability to test medical devices in an IPv6 environment.

3.3.1 Medical Device Regulation

The Food and Drug Administration's (FDA) Regulatory Agency, Center for Devices and Radiological Health (CDRH), regulates firms who manufacture, repackage, re-label, and import medical devices for sale in the United States. CDRH also regulates radiation-emitting electronic products (medical and non-medical) such as lasers, x-ray systems, ultrasound equipment, microwave ovens, and color televisions. The FDA uses a "premarket" review process to ensure regulated medical devices confirm to safety and quality standards.

Regulatory control depends on the medical devices class, from Class I through III. The device classification defines the regulatory requirements for a general device type. Most Class I devices are exempt from Premarket Notification; most Class II devices require Premarket Notification; and most Class III devices require Premarket Approval. The device classification is determined by the FDA and can be found in the FDA's classification database or using an identified device panel (medical specialty) to which your device belongs on the FDA's website.

3.3.2 Medical Device Standards

FDA/CDRH philosophy is that medical devices should, where possible, conform to recognized consensus standards to provide a reasonable assurance of safety and effectiveness for many aspects of medical devices. Conformance with recognized consensus standards may not always be a sufficient basis for regulatory decisions. For example, a specific device may raise a safety or effectiveness issue not addressed by any recognized consensus standard, or a specific FDA regulation may require additional information beyond what conformity to the recognized consensus standards provides.

The FDA focuses on the "least burdensome approach" in all areas of medical device regulation and implements more detailed requirement only when necessary to ensure safety and quality. This approach reflects a careful review of the relevant scientific and legal requirements and the least burdensome way for you to comply with those requirements. To simplify the premarket review process, medical device applications may utilize FDA recognized standards. While rare, some comprehensive consensus standards may include specific acceptance criteria that describe the relevant performance characteristics of that specific medical device. However, if standards do not provide clear acceptance criteria, other relevant, vertical standards can be used to provide and demonstrate device conformance. This guidance, provided by the FDA, leads to the assumption the all medical devices that must communicate over the Internet Protocol can demonstrate IPv6 conformance using known best practices and the USGv6 profile criteria. Conformance to recognized, consensus standards is voluntary and given the nature of the IPv6 Request for Comment (RFC) maturity, certain aspects of medical device capability, in an IPv6 environment, may require the development of unique conformance criteria and testing methodologies.

3.3.3 Medical Device Communication

While the FDA regulates medical devices, the standardization of communication protocols on medical devices is derived from the National Institute for Standards and Technology (NIST). NIST works with medical device vendors and domain experts to facilitate the development and adoption of standards for medical device communications throughout the healthcare

industry. NIST continues to develop and refine medical device communication test methodologies, tools, and tests. This approach enhances the standardized, consistent, and correct communication between medical devices, device-gateways, and communication infrastructures in a healthcare enterprise. The NIST efforts provide standards based validation of medical device communications resulting in enhanced, multi-vendor interoperability.

NIST is developing test methods and tools to support device communication in point-of-care and personal health settings. These tools are derived and implemented to demonstrate medical device communication requirements defined in the ISO/IEEE 11073 Medical Device Communication (x73) standards and enterprise/electronic health record framework defined in the Health Level 7 (HL7) messaging standard.

3.3.3.1 Medical Device Communications Testing

Medical devices, depending on the operating environment, need to communicate with many different devices and systems and may need to interface with devices of varying makes, models, and modalities in life or death scenarios. A point-of-care environment will require each class of medical device to use the same concepts, terminology, data organization, and protocols to seamlessly and reliably communicate physiological data. To demonstrate device commonality and interoperability, NIST is developing test tools and an international standards information model that provides important capabilities that will lead to device interoperability.

The Healthcare Information and Management Systems Society (HIMSS), identified "cross enterprise sharing of patient care device data" as one of their highest priorities. The goals established to meet this priority include shortening decision time, increasing productivity, minimizing transcription errors, and investing in and developing ways to correctly define and interpret the data exchanged. To meet the goals of sharing patient care information, reliable data communication among medical devices and clinical information systems is necessary. To ensure reliability, conformance and interoperability testing of medical device data communication is essential. Standardized testing supports:

- Reducing errors by automatic population of information systems,

- Saving time by automating capture of clinical data into Electronic Health Records (EHRs),
- Improving agility of enterprises to meet varied patient loads,
- Improving life-cycle cost of ownership, and
- Increasing access to patient data across devices and systems.

3.3.4 IEEE 11073: Health informatics - Medical/Health Device Communication Standards

ISO/IEEE 11073 (X73) is a standards family that defines the seven layer communications requirements for the "Medical Information Bus" (MIB). The objective of X73 is to standardize data communications for patient connected bedside devices, optimized for the acute care setting, and to allow clinicians to set up device communications in a "plug and play" fashion.

The primary goals of ISO/IEEE 11073 standards are to:

- Provide real-time plug-and-play interoperability for citizen-related medical, healthcare and wellness devices; and
- Facilitate efficient exchange of care device data, acquired at the point-of-care, in all care environments.

“Real-time” means that data from multiple devices can be retrieved, time correlated, and displayed or processed in fractions of a second. “Plug-and-play” means that all a user has to do is make the connection – the systems automatically detect, configure, and communicate without any other human interaction. “Efficient exchange of care device data” means that information that is captured at the point-of-care (e.g., personal vital signs data) can be archived, retrieved, and processed by many different types of applications without extensive software and equipment support, and without needless loss of information.

The standards are aimed at personal health and fitness devices, such as glucose monitors, pulse oximeters, weighing scales, medication dispensers and activity monitors, and at continuing and acute care devices, such as ventilators and infusion pumps. They comprise a family

of standards that can be layered together to provide connectivity optimized for the specific devices being interfaced. There are four main partitions to the standards, including:

- Device data, including a nomenclature, optimized for vital signs information representation based on a data model and device specializations;
- General application services, including polled and "event driven" services;
- Internetworking and gateway standards; and
- Data transport via guided and unguided media.

3.3.4.1 ISO/IEEE 11073-20101 [Base Standard]

Data attributes, assembly, and transmission between an agent (client) and manager (server) application are defined in the X73 base standard. The standard is subdivided into communication and information models. The communication model is based on the Open Systems Interconnection (OSI), 7-layer model. The information model defines the modeling, formatting, and the syntax for transmission coding of the objects.

The defined parts of the standards family are designed to allow communication according to OSI model principle. The arrangement of two or more medical devices or a medical device and a management application are considered a communications system, such that the components are capable of understanding and interacting.

Most medical device designs will focus on communications at Layer-2, the Data-Link Layer. Very small, medical device networks will utilize a relatively slow-speed Layer-2 technology, such as Bluetooth, to create a Wireless Personal Area Network (wPAN). Other technologies may extend the range and reach of the network to create Wireless Local Area Networks (wLAN).

In most environments, the Internet Protocol will be utilized as Layer-3 or the Network Layer. It is assumed that medical devices that require network services will be tested to interoperate over an IPv4 network.

3.3.4.1.1 Sample Health Device Profile (HDP) Using Bluetooth

Under Bluetooth, a profile defines the characteristics and features including function of a Bluetooth system. The Medical Working Group (Med WG) of the Bluetooth Special Interest Group (SIG) defined the Health Device Profile (HDP) specification that included the Multi-Channel Adaptation Protocol (MCAP) and made use of the Device ID Profile (DI). The following Figure 8 describes the architecture of a Bluetooth system with the HDP and applications.

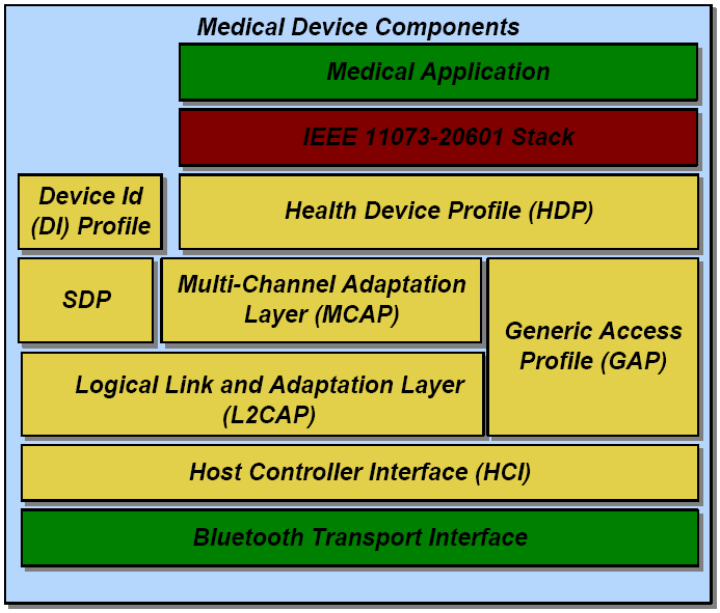


Figure 8: Medical Device Components

As shown in the figure, the Layer-3 technology is not defined. If the medical application requires access to Internet services, then the application must address all of the IP application socket requirements and the Logical Link and Adaptation Layer (L2CAP), Host Controller Interface (HCI) and Bluetooth Transport Interface service protocols must function in an IP environment.

3.3.4.2 ISO/IEEE 11073-20601 Personal Health Device Communications

The IEEE 11073-20601 defines Personal Health Device Communications. Because incompatible systems would slow the roll-out of useful personal health devices, efforts have been

made to ensure interoperability. The X73 PHD standards are characterized by a number of architectural decisions, including:

- A point-to-point connection is made between "Agent" and a "Manager",
- Transport agnostic (to facilitate porting to new communications channels),
- Object-oriented philosophy (to facilitate code re-use and simplify the introduction of new devices),
- Agents are self-describing (so Managers can understand the characteristics of the Agents),
- Extensible (to encompass new types of agent, and custom specializations of already-defined agents), and
- ASN.1 used to represent data structures and messages (to simplify parsing of messages).

The overall X73 system model is divided into three principal components, each of which is treated separately in IEEE 11073-20601.

- The Domain Information Model represents an agent as a set of objects. Each object has one or more attributes. Attributes describe measurement and status data that are communicated to a manager.
- The service model provides commands such as Get, Set, Action, and Event Report that are sent between the agent and manager to exchange data from the DIM.
- The communication model establishes a state machine for the Agent and the Manger, including states related to connection, association, and operation. The communication model also converts the abstract data modeling used in the Domain Information Model into a binary message format for transfer using the communication model.

3.3.4.3 IEEE 11073 [Transport Independent] Communication Standards

The IEEE X73 PHD standards define messages that travel between Agent and Manager, but not how those messages should be moved is not addressed. So far there are three transport technologies defined by the standard: Bluetooth, Universal Serial Bus (USB), and ZigBee.

These defined standards reside at Layer-2 of the OSI model and should be interoperable with both IPv4 and IPv6.

3.3.4.3.1 Bluetooth

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances for the creation of wPANs with high levels of security. Bluetooth is managed by the Bluetooth Special Interest Group (SIG). The Internet Engineering Task Force's (IETF) 6LoWPAN Working Group has developed a draft Request for Comment (RFC) for IPv6 over Bluetooth, draft-ietf-6lowpan-btle-05, Transmission of IPv6 Packets over Bluetooth Low Energy.

3.3.4.3.2 Universal Serial Bus (USB)

The Universal Serial Bus (USB) is an industry standard that defines the cables, connectors, and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices. USB standardizes the connection of computer peripherals to personal computers. USB technology can be used to for direct data transport, electrical power, or for communication protocols, including network adapter interfaces.

3.3.4.3.3 ZigBee

ZigBee is a specification for a suite of high-level communication protocols using small, low-power digital radios based on an IEEE 802 standard for wPANs. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other wPAN technologies, such as Bluetooth, and is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking. ZigBee has a defined rate of 250 kbps, suited for periodic or intermittent data or a single signal transmission from a sensor or input device.

The ZigBee standard defines a network layer that can be transported over a low-speed RF environment. However, like other low speed Layer-2 technologies, it can be made to interoperate with the Internet Protocol (IP).

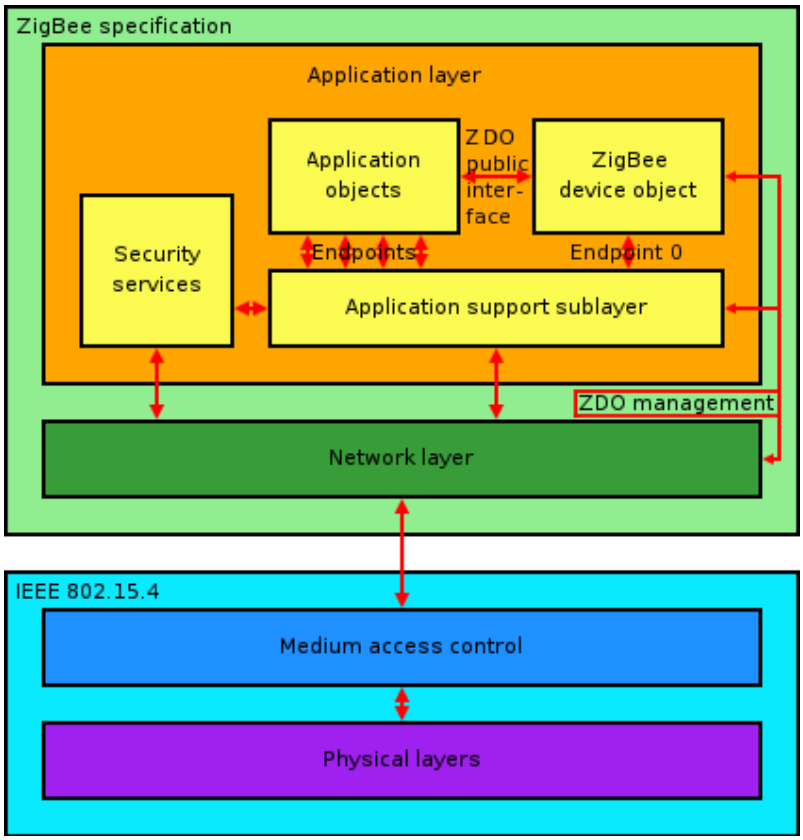


Figure 9: ZigBee Model

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-wPANs).

3.3.4.3.4 Shim Layer Protocols

IPv6 requires a layer-2 Minimum Transmission Unit (MTU) of 1280 Bytes, which is larger than the capability of wPAN technologies. In order to achieve IPv6 over wPAN, the IPv6 protocol may be required to fragment and reassemble packets or utilize a "shim" protocol that resides between the network and data-link layers. This shim layer may implement fragmentation, header compression, label handling, extension headers, network management, or other implementation solutions to provide IPv6 over wLAN solutions.

3.3.5 Medical Device IPv6 Interoperability Compliance Testing

X73 addresses the 7 layers of the OSI communications stack. In theory, Layer 3, the Network Layer, should be interchangeable between protocols that perform the network function. Medical devices operating in an IPv6 native environment must be able to pass IPv6 packets through existing Layer 2 frames.

History has demonstrated that transitioning from one protocol to another can cause interoperability issues. In the late 1990 and early 2000s, IPv6 implementations were not always successful on Ethernet Network Interface Cards (NIC). The NICs had difficulty identifying and encapsulating the IPv6 Packet.

Several issues may surface as the transition to IPv6 occurs. End devices, especially those with limited capabilities may have difficulty handling IPv6 packets for numerous reasons. Medical devices will need to be thoroughly tested in an IPv6 network environment to ensure that they function appropriately and that interoperability is demonstrated. Additionally, some devices may require other technological solutions in order to function in an IPv6 environment, including implementing unique capabilities of the IPv6 protocol or developing shim-layer protocols.

4 Related Federal IPv6 Test Programs

4.1 USGv6 Test Program

The U.S. Government test program is derived from the National Institute for Standards in Technology (NIST) Special Publication 500-273. In SP 500-273, the U.S. Government IPv6 test program is guided by (5) fundamental objectives:

1. Quality Components – Meaning that each test laboratory has a rigorous and validated accreditation per international specifications like the ISO 17025.
2. Traceability of Tests – Each test case has a basis in the current and recognized IPv6 international standards bodies.

3. There is a feedback mechanism. This mechanism is the U.S. Government IPv6 Testing Working Group.

4. There is test method validation – Meaning that the test cases, test procedures and testing tools are open, transparent, and repeatable.

5. Proficiency in testing and laboratory comparisons – All labs must demonstrate proficiency in IPv6 testing.

4.1.1 USGv6 Test Process Overview

Each test lab must prove they are certified by an approved international accreditation body. This accreditation follows the ISO 17025 process. In USGv6 testing, accreditations are broken up into (3) categories:

- 1st Party Test Lab – This lab usually belongs to the hardware or software vendor. The testing may or may not include interoperability testing.
- 2nd Party Test Lab – This lab belongs to the U.S. Government Agency that is procuring IT products. The VA can be accredited for this type of test lab.
- 3rd Party Lab – This lab belongs to an independent test facility. These test facilities normally do not belong to a U.S. Federal Agency unless they are chartered to only do testing. For example, the DoD's Joint Interoperability Test Command (JITC) or U.S. Air Force Operational Test and Evaluation Command (AFOTEC) could be considered 3rd Party Test Labs.

4.1.1.1 USGv6 Test Specifications

Each test lab must still produce test results in compliance with the current test specifications outlined in the USGv6 Test Methods website. This test specification outlines each of the conformance, interoperability, and functional network protection device (NPD)/security tests that must be performed and with what section of the U.S. Government IPv6 Profile section they correspond.

The test specifications are outlined in the same site under Test Specifications (http://www.antd.nist.gov/usgv6/test-specifications.html). For example, the 1st, 2nd, or 3rd Party

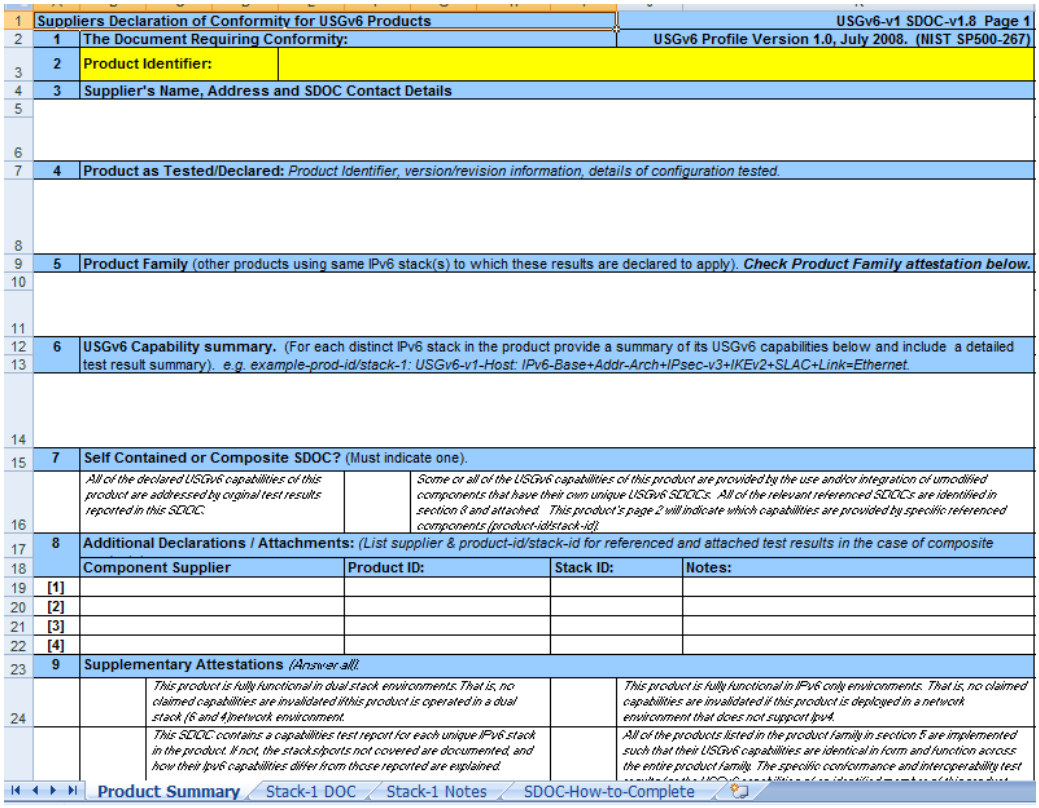
Test lab will open the current test specification for SLAAC v.1.1_C (Conformance). This specification outlines how to test Stateless Address Autoconfiguration (SLAAC) from a conformance perspective. Later in test case SLAAC v.1.1_I, the test specification outlines how to conduction Stateless Address Autoconfiguration (SLAAC) from an interoperability perspective.

These test specifications are updated frequently and are accessible on the website listed above.

4.1.1.2 Suppliers Declaration of Conformity (SDoC)

USGv6 Supplier's Declaration of Conformity (SDoC) is based on ISO/IEC 17050. The SDoC stands as a representative of the device supplier's claims of compliance for a host, router, or network protection product. A subset is shown in figures below [Figure 1Figure 10, Figure 11, Figure 12) It contains the following items:

- Background information on the product being tested (e.g. product class, description, and product overview characteristics);
- A listing of product specific items to be tested. It is recommended that the vendor use the template located on the NIST website here: http://www.antd.nist.gov/usgv6/docs/usgv6-v1-SDoC-v1.8.xls; and
- Next to each technical test requirement (i.e. an RFC), a status from the testing. If a product undergoes Conformance and Interoperability testing then the status of "Pass" or "Pass with notes." The "Pass with notes" status usually indicates the vendor did not successfully complete the test specification.



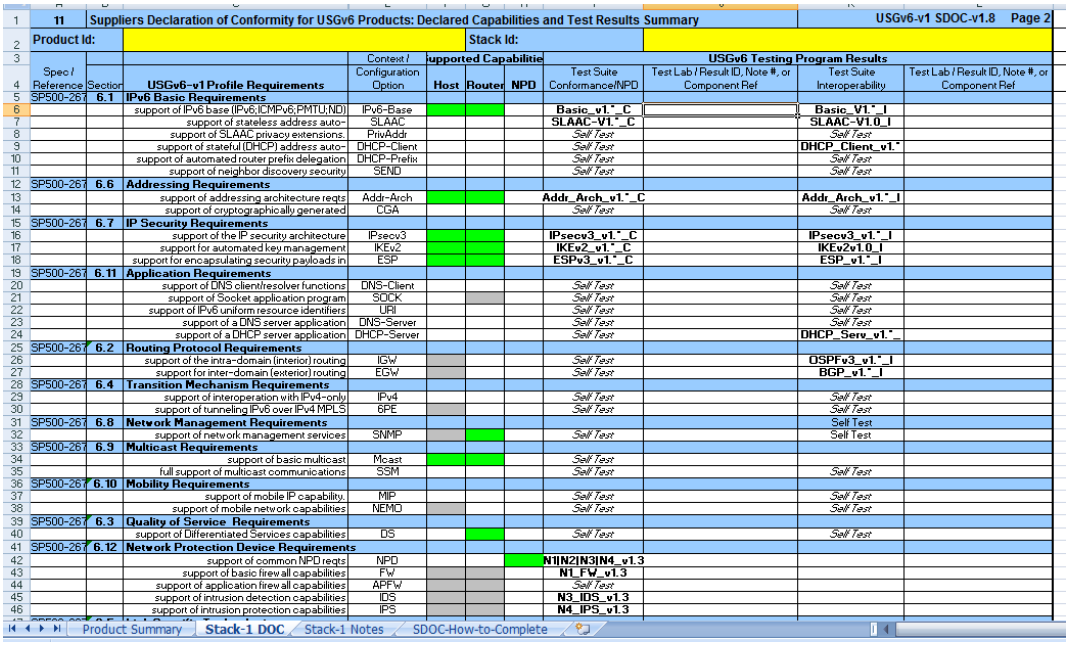
1	**Suppliers Declaration of Conformity for USGv6 Products**		**USGv6-v1 SDOC-v1.8 Page 1**
2	**1**	**The Document Requiring Conformity:**	**USGv6 Profile Version 1.0, July 2008. (NIST SP500-267)**
3	**2**	**Product Identifier:**	
4	**3**	**Supplier's Name, Address and SDOC Contact Details**	
5			
6			
7	**4**	**Product as Tested/Declared:** *Product Identifier, version/revision information, details of configuration tested.*	
8			
9	**5**	**Product Family** (other products using same IPv6 stack(s) to which these results are declared to apply). ***Check Product Family attestation below.***	
10			
11			
12	**6**	**USGv6 Capability summary.** (For each distinct IPv6 stack in the product provide a summary of its USGv6 capabilities below and include a detailed	
13		test result summary). *e.g. example-prod-id/stack-1: USGv6-v1-Host: IPv6-Base+Addr-Arch+IPsec-v3+IKEv2+SLAC+Link=Ethernet.*	
14			
15	**7**	**Self Contained or Composite SDOC?** (Must indicate one).	
16		*All of the declared USGv6 capabilities of this product are addressed by original test results reported in this SDOC.*	*Some or all of the USGv6 capabilities of this product are provided by the use and/or integration of unmodified components that have their own unique USGv6 SDOCs. All of the relevant referenced SDOCs are identified in section 8 and attached. This product's page 2 will indicate which capabilities are provided by specific referenced components [product-id/stack-id].*
17	**8**	**Additional Declarations / Attachments:** *(List supplier & product-id/stack-id for referenced and attached test results in the case of composite*	

	Component Supplier	Product ID:	Stack ID:	Notes:
[1]				
[2]				
[3]				
[4]				

23	**9**	**Supplementary Attestations** *(Answer all)*	
24		*This product is fully functional in dual stack environments. That is, no claimed capabilities are invalidated if this product is operated in a dual stack (6 and 4) network environment.*	*This product is fully functional in IPv6 only environments. That is, no claimed capabilities are invalidated if this product is deployed in a network environment that does not support Ipv4.*
		This SDOC contains a capabilities test report for each unique IPv6 stack in the product. If not, the stacks/ports not covered are documented, and how their Ipv6 capabilities differ from those reported are explained.	*All of the products listed in the product family in section 5 are implemented such that their USGv6 capabilities are identical in form and function across the entire product family. The specific conformance and interoperability test*

Product Summary | Stack-1 DOC | Stack-1 Notes | SDOC-How-to-Complete

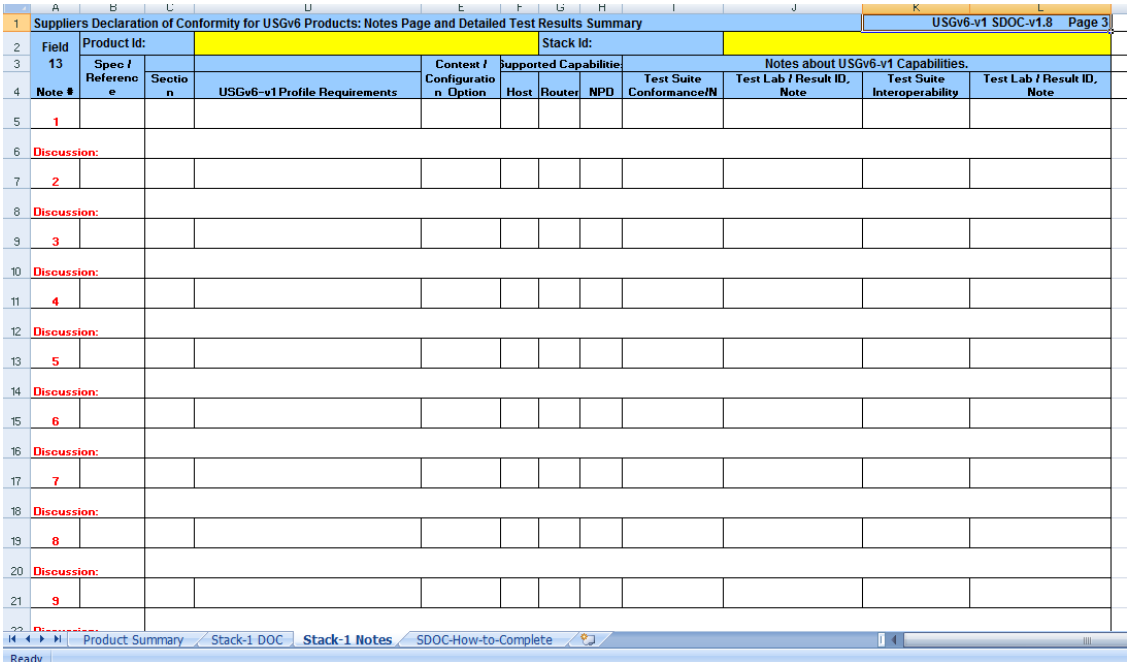
Figure 10: SDoC Product Summary



1	**11**	**Suppliers Declaration of Conformity for USGv6 Products: Declared Capabilities and Test Results Summary**							**USGv6-v1 SDOC-v1.8**	**Page 2**
2	**Product Id:**			**Stack Id:**						
3				Context /	**Supported Capabilities**			**USGv6 Testing Program Results**		
4	Spec / Reference	Section	**USGv6-v1 Profile Requirements**	Configuration Option	**Host**	**Router**	**NPD**	Test Suite Conformance/NPD	Test Lab / Result ID, Note #, or Component Ref	Test Suite Interoperability	Test Lab / Result ID, Note #, or Component Ref
5	SP500-267	**6.1**	**IPv6 Basic Requirements**								
6			support of IPv6 base (IPv6;ICMPv6;PMTU;ND)	IPv6-Base				**Basic_v1.*_C**		**Basic_V1.*_I**	
7			support of stateless address auto-	SLAAC				**SLAAC-V1.*_C**		**SLAAC-V1.0_I**	
8			support of SLAAC privacy extensions	PrivAddr				*Self Test*		*Self Test*	
9			support of stateful (DHCP) address auto-	DHCP-Client				*Self Test*		**DHCP_Client_v1.***	
10			support of automated router prefix delegation	DHCP-Prefix				*Self Test*		*Self Test*	
11			support of neighbor discovery security	SEND				*Self Test*		*Self Test*	
12	SP500-267	**6.6**	**Addressing Requirements**								
13			support of addressing architecture reqts	Addr-Arch				**Addr_Arch_v1.*_C**		**Addr_Arch_v1.*_I**	
14			support of cryptographically generated	CGA				*Self Test*		*Self Test*	
15	SP500-267	**6.7**	**IP Security Requirements**								
16			support of the IP security architecture	IPsecv3				**IPsecv3_v1.*_C**		**IPsecv3_v1.*_I**	
17			support for automated key management	IKEv2				**IKEv2_v1.*_C**		**IKEv2v1.0_I**	
18			support for encapsulating security payloads in	ESP				**ESPv3_v1.*_C**		**ESP_v1.*_I**	
19	SP500-267	**6.11**	**Application Requirements**								
20			support of DNS client/resolver functions	DNS-Client				*Self Test*		*Self Test*	
21			support of Socket application program	SOCK				*Self Test*		*Self Test*	
22			support of IPv6 uniform resource identifiers	URI				*Self Test*		*Self Test*	
23			support of a DNS server application	DNS-Server				*Self Test*		*Self Test*	
24			support of a DHCP server application	DHCP-Server				*Self Test*		**DHCP_Serv_v1.*_**	
25	SP500-267	**6.2**	**Routing Protocol Requirements**								
26			support of the intra-domain (interior) routing	IGW				*Self Test*		**OSPFv3_v1.*_I**	
27			support for inter-domain (exterior) routing	EGW				*Self Test*		**BGP_v1.*_I**	
28	SP500-267	**6.4**	**Transition Mechanism Requirements**								
29			support of interoperation with IPv4-only	IPv4				*Self Test*		*Self Test*	
30			support of tunneling IPv6 over IPv4 MPLS	6PE				*Self Test*		*Self Test*	
31	SP500-267	**6.8**	**Network Management Requirements**							Self Test	
32			support of network management services	SNMP				*Self Test*		Self Test	
33	SP500-267	**6.9**	**Multicast Requirements**								
34			support of basic multicast	Mcast				*Self Test*			
35			full support of multicast communications	SSM				*Self Test*		*Self Test*	
36	SP500-267	**6.10**	**Mobility Requirements**								
37			support of mobile IP capability.	MIP				*Self Test*		*Self Test*	
38			support of mobile network capabilities	NEMO				*Self Test*		*Self Test*	
39	SP500-267	**6.3**	**Quality of Service Requirements**								
40			support of Differentiated Services capabilities	DS				*Self Test*		*Self Test*	
41	SP500-267	**6.12**	**Network Protection Device Requirements**								
42			support of common NPD reqts	NPD				**N1|N2|N3|N4_v1.3**			
43			support of basic firewall capabilities	FW				**N1_FW_v1.3**			
44			support of application firewall capabilities	APFW				*Self Test*			
45			support of intrusion detection capabilities	IDS				**N3_IDS_v1.3**			
46			support of intrusion protection capabilities	IPS				**N4_IPS_v1.3**			

Product Summary | Stack-1 DOC | Stack-1 Notes | SDOC-How-to-Complete

Figure 11: SDoC Test Specification Status



	A	B	C	D	E	F	G	H	I	J	K	L
1	Suppliers Declaration of Conformity for USGv6 Products: Notes Page and Detailed Test Results Summary										USGv6-v1 SDOC-v1.8	Page 3
2	Field	Product Id:					Stack Id:					
3	13	Spec /			Context /	Supported Capabilities:			Notes about USGv6-v1 Capabilities.			
4	Note #	Reference	Section	USGv6-v1 Profile Requirements	Configuration Option	Host	Router	NPD	Test Suite Conformance/N	Test Lab / Result ID, Note	Test Suite Interoperability	Test Lab / Result ID, Note
5	1											
6	Discussion:											
7	2											
8	Discussion:											
9	3											
10	Discussion:											
11	4											
12	Discussion:											
13	5											
14	Discussion:											
15	6											
16	Discussion:											
17	7											
18	Discussion:											
19	8											
20	Discussion:											
21	9											

Product Summary | Stack-1 DOC | Stack-1 Notes | SDOC-How-to-Complete

Ready

Figure 12: SDoC Test Status Notes

4.2 DoD IPv6 Testing

The IPv6 test and evaluation history began in 2006 as a standalone certification program. It focused on standards compliance (conformance) and interoperability testing. As testing and standards development matured in the DoD, IPv6 testing was gradually incorporated into the Unified Capabilities product certification program. This program maintains a list of certified products called the Unified Capabilities Approved Products List (UC APL) and it is located here: https://aplits.disa.mil/processAPList.do. The DoD Information Systems Agency (DISA) Unified Capabilities Certification Office (UCCO) is the body that ultimately approves devices for certification; thus adding them to the UC APL.

This program uses the DoD's Unified Capabilities Requirements (UCR) 2008, Change 3 as its requirements specification. The majority of the standards within the U.S. IPv6 Profile and the DoD IPv6 Standards Profiles for IPv6 Capable Products are included in this program. However, the focus of testing is much broader than only looking at conformance and interoperability. They incorporate IA/Security and performance testing over both IPv4 and IPv6 as well. The VA is

looking to also incorporate this type of testing. As shown in Figure 13, the product profiles and testing requirements map directly to the DoD UCR 2008, Change 3.

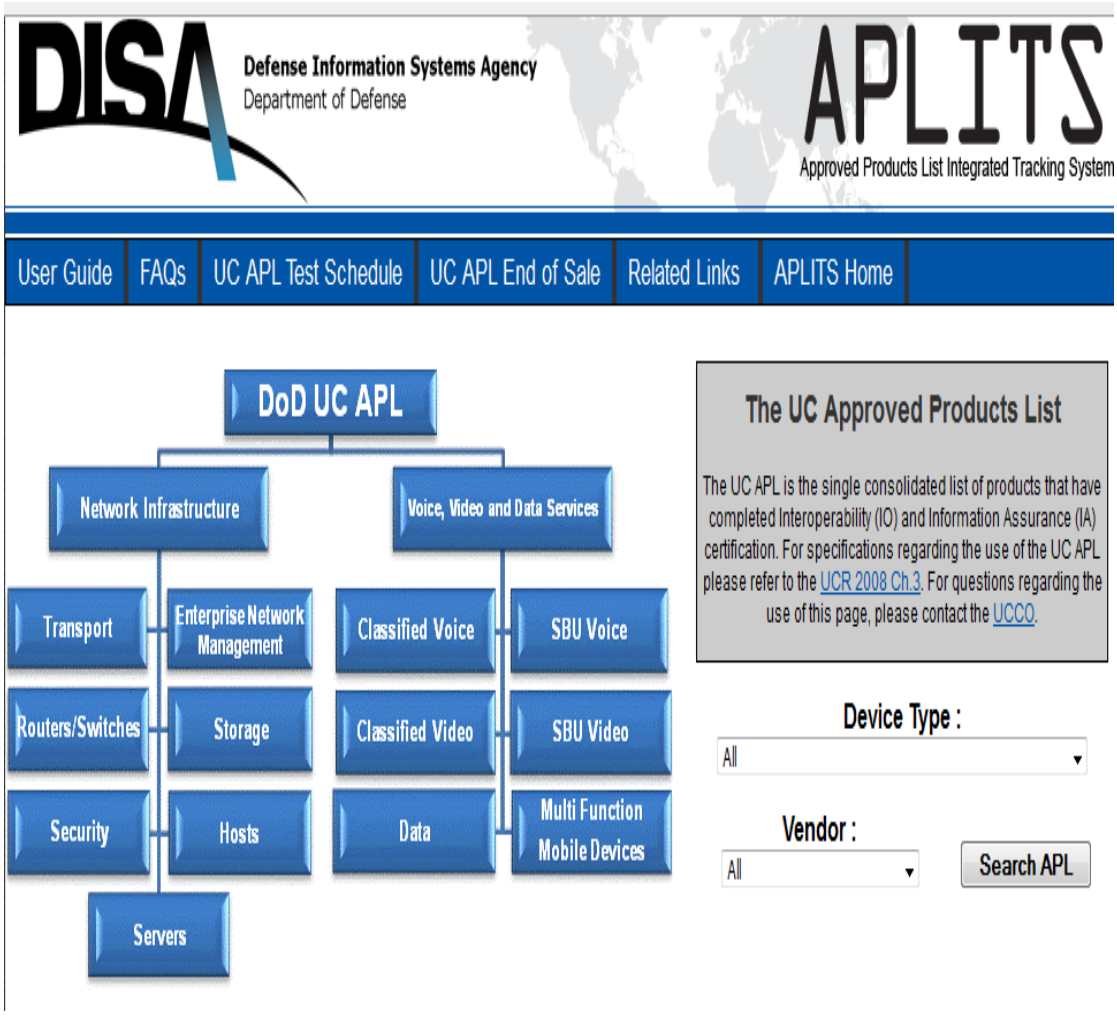


Figure 13: DoD Unified Capabilities Approved Products List

5 VA IPv6 Compliance Testing Approach

OMB's initial directive for the transition of Federal Agency systems to IPv6 is Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" August 2005. This memorandum mandated that all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure by June 2008. Subsequently, the Federal CIO issued additional mandates directing that all public/external facing services be IPv6

operational by end of FY2012 and all internal networks, systems, implement native IPv6 support for external services and services be transitioned to IPv6 operation by FY2014. On March 24, 2011, the VA Principal Deputy Assistant Secretary, Office of Information and Technology issued a directive reinforcing the VA's aim to achieve the Federal CIO Mandates, and added an additional goal of disabling IPv4 as a communication mechanism on all VA computing, application, and network resources.

5.1 Compliance Strategy

The VA IPv6 Compliance strategy approach establishes a direction for the agency to develop a comprehensive IPv6 & USGv6 compliance test capability for IPv6 capable devices that takes into account all the latest developments, deployments in both large and medium service provider and enterprise networks across the world. The VA IPv6 compliance test capability is being designed keeping the test objectives based on the OMB mandate, which expects that all IT systems comply with IPv6 conformance, performance, interoperability, information assurance, stability, and longevity without disrupting the current operations of the agency.

Through this approach VA may also consider having its own accredited USGv6 test lab by complying with USGv6 ISO 17025 Lab Accreditation process as described in earlier section.

The United States Government IPv6 (USGv6) Profile and Test Program were established by the National Institute of Standards and Technology (NIST), at the direction of the Office of Management and Budget (OMB), to provide agencies with a common taxonomy and framework to describe and procure equipment from the vendor community that met the agency's IPv6 requirements. While the USGv6 program provides agencies with a significant tool and set of capabilities, its focus is entirely on conformance and interoperability testing. It does not provide the ability to test on performance or full feature/functional parity between IPv4 and IPv6, or subjecting the IPv6 capable systems to longevity, stability, security and other functional verifications tests. Thus, the VA, as with other agencies, will need to supplement their acquisition requirements to ensure that they are acquiring IPv6 capable systems that truly meet or exceed their operational requirements.

In addition, the USGv6 process was established as a method for agencies to specify equipment acquisition requirements and have a level of assurance that reasonable tests were performed to show vendors were meeting those requirements. It does not help agencies achieve the same level of assurance regarding equipment that is already in use within their enterprise.

The VA IPv6 compliance approach identifies the strategy and plan that VA should adopt to meet the OMB mandates, while considering input from already developed USGv6 and DOD IPv6 profiles and keeping up at pace with the current ongoing efforts in the standard development organizations (SDOs) such as IETF. The plan needs to continuously be updated based upon new technological advancements that may simplify and improve the end-to-end network performance of the VA enterprise ecosystem.

It is expected that through this VA IPv6 Compliance strategy, the VA will be able to assess the ability of the IPv6 capable systems that it intends to deploy in its current infrastructure or upgrade in its current network. At the same time the VA will meet the acquisition life cycles for IT assets, and be able to guide its contracts and acquisition officers, system designers and integrators, testing and accreditation organizations and developers and update them with mandatory and conditional requirements that may be of common utility in acquiring specific IPv6 products and services.

This document seeks to assist the VA in formulating plans for the acquisition of IPv6 technologies, applications, services, and IPv6 capable devices (hosts, intermediate systems, protection devices). To achieve this, we develop VA IPv6 compliance test capability to help the VA determine which network equipment and applications meet VA's IPv6 network requirements. The VA IPv6 test capability is a comprehensive approach to assist the VA as it develops an IPv6 standards profile, based on the model shown in Figure 14. The test capability requirements will not only be based on the United States Government IPv6 (USGv6) profile and supplemented with VA-specific IPv6 requirements not covered within National Institute of Standards and Technology (NIST) specifications, but will also take into account DOD IPv6 Standard profile, Unified Capabilities Certification Office (UCCO), IPv6 forum testing program, and taking input from current progress at IETF and other related SDOs. This document presents

VA IPv6 Compliant Testing Requirements, VA IPv6 standard profiles, test classes, devices types, and minimum required configuration set for each network equipment type and minimum feature set for each application.

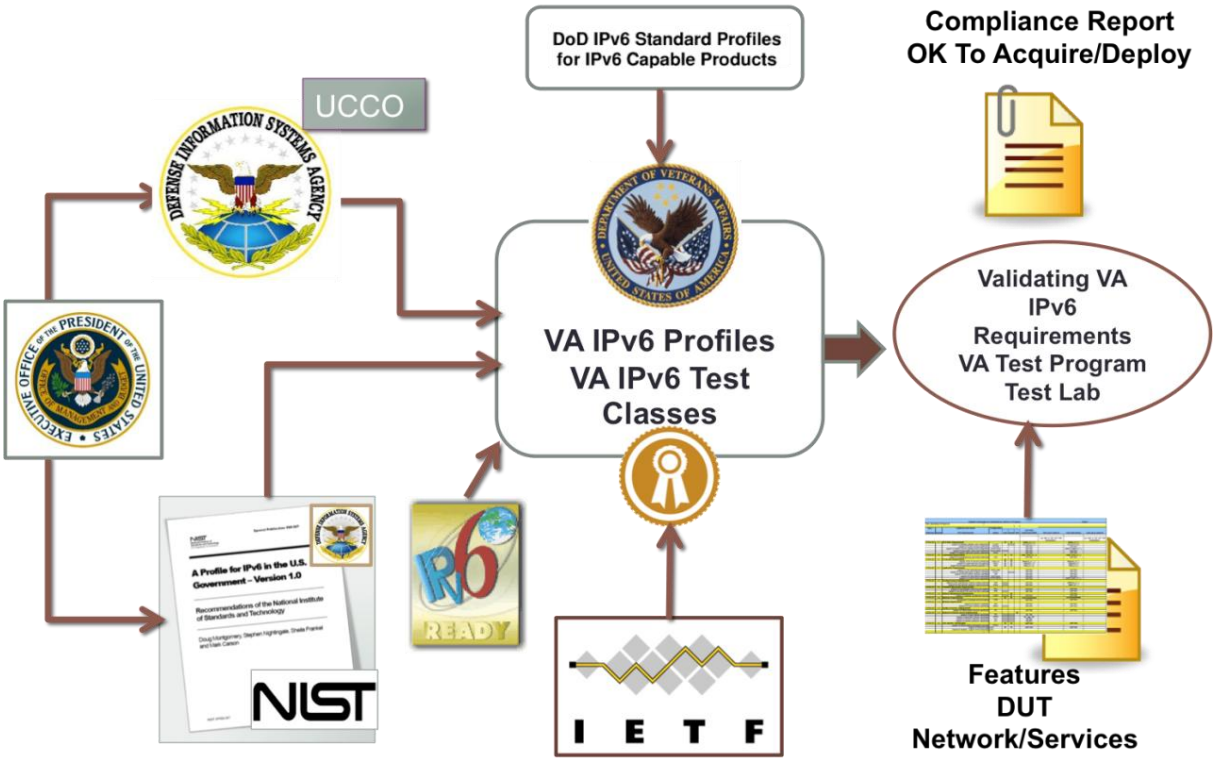


Figure 14: VA IPv6 Compliance Test Capability Development Strategy and Plan

It is well understood that the VA will implement dual-stack (IPv6 along with IPv4) support of VA external Internet Services and transition the VA internal networks, systems and services to a native IPv6-only operation from its current IPv4-only based operation. The transition plan will include provisions for the operation of legacy systems in isolated enclaves, which cannot be converted to IPv6.

VA IPv6 compliance testing requirements capture the testing and evaluation requirements through an implementation process by which a component or system is compared with VA specific requirements and standard specifications through a test method. The test procedures and processes that are part of the testing and evaluation process are quite broad, but can be described

as validating whether component or system requirements are performing as expected. The testing requirement development is an integral part of the process to develop a testing design document that recommends all of the steps and identifies estimated costs necessary for the VA to create an IPv6 testing capability to meet the VA IPv6 Compliant Testing Requirements Document.

Although the USGv6 Profile and other complementing IPv6 standard profiles help to fulfill the underlying requirements for IPv6 device acquisition, there are additional VA mission specific requirements that go far beyond the requirements contained in the USGv6 Profile, which are addressed through this effort. These additional constraints fall under the VA mission specific requirements such as functionality, security, or software applications that are not tested under the USGv6 Profile, and, therefore, must be included as a sub-set to the overall requirements for defining IPv6-Compliance for the VA.

5.2 Successful IPv6 Deployment and VA IPv6 Compliance Process

Given the widespread network deployments of IP related products in the VA internal networks and peering networks, there are significant risks associated with the deployment of semi-baked or non-compliant IPv6 devices in live operational networks. IPv6 is inevitable and the key decision to be made by each federal agency, including the VA, is what path it should take to transform successfully its current infrastructure to an IPv6 enabled/compliant infrastructure with minimal or no interruption of existing operational services. Successful deployment of IPv6 depends on how an agency implements compliance strategy for the IPv6 standard devices and uses a pragmatic approach while leveraging current investments.

There are four building blocks to a successful IPv6 deployment as shown in Figure 15, and VA will need to define and classify IPv6 devices that are deployed or can be classified under each building block. Through this effort we are updating the existing USGv6 IPv6 profiles process and building comprehensive VA IPv6 compliant testing requirements that would help the VA reach its goal for achieving end-to-end IPv6 services connectivity.

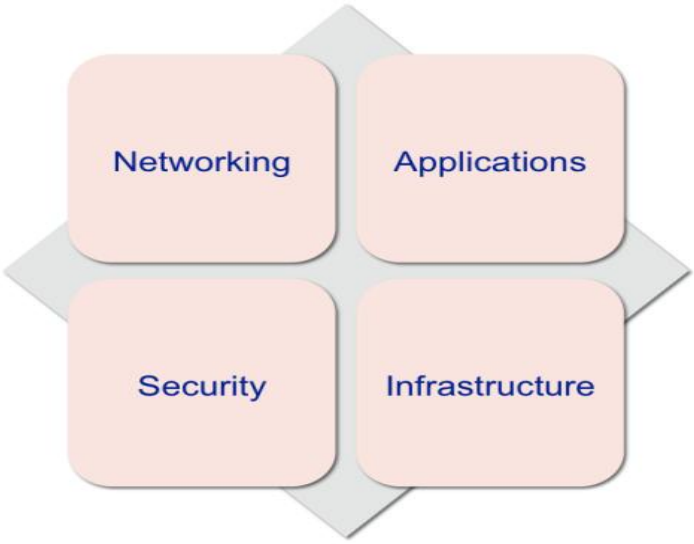


Figure 15: Key building blocks of Successful IPv6 Deployment

To assist the VA in achieving an optimized cost efficient and economical adoption of IPv6 technology analysis of significant technical gaps that exist in the VA IPv6 deployment is required, along with additional standards and testing infrastructures or additional profiles.

This concept will allow to develop comprehensive VA IPv6 profile and define test classes to which we believe all IPv6 capable devices/applications or services should be subjected before adoption in VA networks.

It is well known that a subset of network layer IPv6 specifications have stabilized, and that there exist operationally viable commercial deployments. The VA could adopt and deploy these features incrementally. However, an end-to-end deployment of successful IPv6 network, services, and applications would require a customized test environment which is capable of mimicking the VA IPv6 current and future network architecture and validating minimal or no impact on existing services and applications during or after completion of IPv6 transition process. Hence it is extremely important that the IPv6 compliance test requirements are strictly followed and all the IPv6 systems are subjected to VA testing and are certified before the deployment.

VA IPv6 compliance test capability requirements would help the VA in establishing technology acquisition profile for IPv6 enabled devices, applications, and services to be procured and deployed in operational infrastructure. This requirements document builds upon USGv6 profiles, defines taxonomy of IPv6 capable systems and testing classes, identifies significant configuration options on current infrastructure components, establishes performance benchmarks for the IPv6 enabled systems, and differentiates the mandatory capabilities and optional capabilities. The outcome of this effort will help the agency establish its own USGv6 accredited lab and test programs that will provide the technical basis for the definition and demonstration of IPv6 capable and IPv6 compliance for the VA IPv6 procurements.

5.3 IPv6 Compliance and Taxonomy of Device

In specifying VA IPv6 compliance capability requirements for IPv6 enabled systems it is necessary to recognize that different types of devices play different roles in many protocol specifications. The IETF defines an IPv6 Node as a device that implements IPv6. The IETF IPv6 specifications recognize two types of Nodes, Hosts and Routers. IPv6 Node Requirements [RFC4294] expresses a general profile of device requirements in terms of these two device types. We adopt and maintain this taxonomy of device types in this profile. In addition, we believe the VA IPv6 compliance requirement should define additional profiles for applications, services, and network management that enable or simplify the operations, administration, and management (OAM). In addition, we inherit the profile for Network Protection Devices (NPDs), which often have only partial, or non-standard, Host and/or Router capabilities. When a specification that distinguishes Host and Router behaviors is cited for a device type in this profile, we implicitly mean that the required Host behavior applies to our Host device type and the required Router behavior applies to our Router device type.

A device claiming to conform to the Host requirements of this profile, must implement the Host behaviors (when distinguished) in the referenced specifications. Similarly, a device claiming to conform to the Router requirements of this profile, must implement the Router behaviors (when distinguished) in the referenced specifications. It should be noted that we use these notions of device types to identify and group sets of requirements into collections that

correspond to these two basic architectural roles. It is to be understood that any combination of the device type can be implemented together in one box, for example a firewall and a host could be bundled together.

In summary, we define the IPv6 enabled systems for VA IPv6 profiles in section 10 with each having its own functional categories of IPv6 capabilities (such as transitional, connection, technology, security, QoS, mobility, wireless etc.).

6 Achieving VA IPv6 Compliance – Testing Classes

USGv6 defines comprehensive procedural and documentation requirements for products claiming compliance with this profile. The foundation for all claims of compliance is based upon a product conformance and interoperability-testing program comprised of open consensus test suites, formally accredited testing laboratories, and approved accreditation bodies. VA IPv6 test capability requirements extend those testing classes to ensure that the products, applications, and services that are needed by the VA can be evaluated comprehensively. This will ensure that the SDOC is backed by a chain of traceability of results through labs accredited under ISO/IEC 17025 or labs appointed by VA to ensure the compliance of the SDOC provided by the vendor. As shown in Figure 16 below, VA is requiring the standard testing of IPv6 products, applications, and services in compliance with an USGv6 test program that mandates product conformance and interoperability testing. We believe that the VA IPv6 program should, additionally, subject the IPv6 capable systems to the additional functional, performance, regression and final compliance acceptance testing.

As shown in the Figure 16, part of the USGv6 profile shows that the compliance to the profile can be accomplished through conformance and interoperability testing. Hence, being "USGv6-V1-Compliant" may not be meaningful to agencies that have specific requirements and needs from IPv6 capable devices and services. These specific requirements are defined as part of the VA profiles. To achieve a comprehensive compliance, and to ensure that the device under test when deployed in the VA infrastructure will performed as per expectations, VA IPv6 test compliant requirements add additional test classes that should be executed to achieve a high level of compliance which may not be guaranteed by conformance and interoperability testing. The

VA test classes will consist of test cases that are based on VA use cases and validate the device under test for validation and compliance to the VA deployment requirements.

The chain of traceability for compliance test results is rooted in abstract test specifications. These test suites will be validated against public specifications (mainly IETF RFCs) and VA IPv6 specific requirements, and serve as the standard reference material for this test program. The genesis of these tests specifications, their evolution, and use in accredited or VA testing will be broadly classified under the following categories.

6.1 VA-Specific IPv6 Testing Classes

The VA specific testing classes are broadly classified under the following categories, as shown in the Figure 16. These categories build upon IPv6 conformance and interoperability within the USGv6 test program.

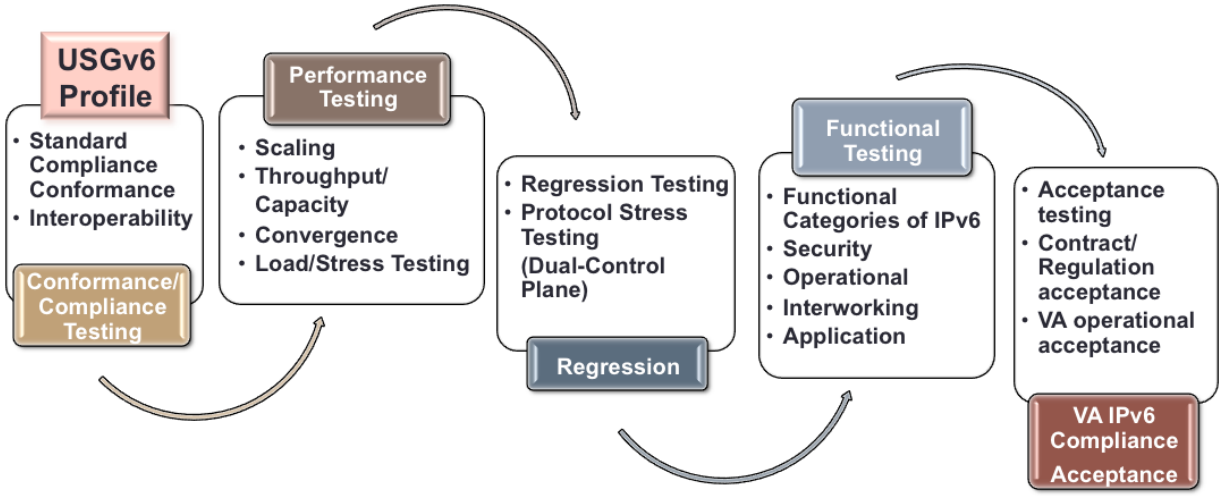


Figure 16: VA IPv6 Test Capability Requirements – Test Classes

6.1.1 USGv6 Compliance – IPv6 Conformance Testing

Conformance testing is to verify that a device or a system under test satisfies the criteria in a specified controlling document. The controlling documents may be from military, national, European, International, or IETF standardization bodies. The conformance testing ensures that

the networking devices are software compliant to the networking protocol specifications and standards as well as interoperability with existing products. As shown in Figure 17 below the DUT is isolated from the network and it is tested for its detailed compliance to each of the Requests for Comments (RFCs) in the US Government IPv6 Profile and the VA IPv6 Profile. In all of tests, the recognized and open test tool used is the TAHI tool. The TAHI conformance test tool runs on a standard Linux/UNIX system, and is located online here: http://www.tahi.org.

The results from the conformance testing helps increase the confidence of the agency and accelerates the time to adoption while ensuring the security in the field deployments by preventing incorrect protocol implementations. All IPv6 capable devices being considered to be deployed in VA IPv6 infrastructure should be subjected to conformance testing for key functional categories of IPv6 capabilities. Tests should not be limited to IPv6 basic functions, routing protocols, quality of service, transition mechanism, link specific, addressing, IP security, multicast, and other related application requirements which may be unique to the VA IPv6 environment.

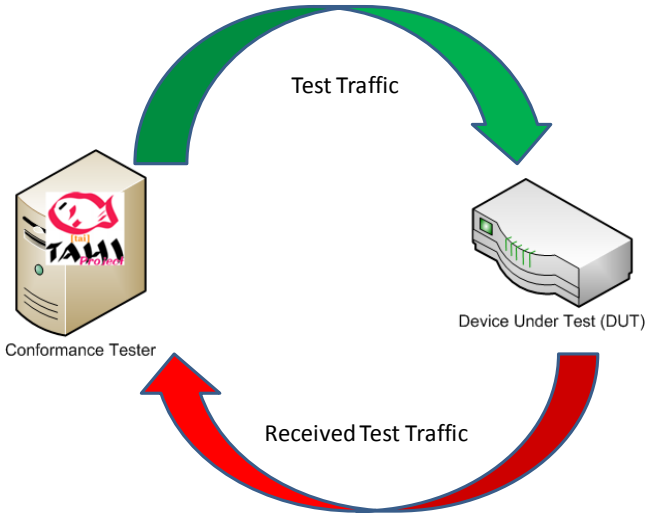


Figure 17: IPv6 Compliance conformance test bed

6.1.2 USGv6 Compliance – Interoperability Testing

Interoperability is the ability of the systems to provide services to and accept services from other systems, and to use the services exchanged to enable them to operate effectively together. The degree of interoperability should be defined when referring to specific requirements. The interoperability testing enables the working of such different implementations in harmony. As part of the VA IPv6 test capability compliance it is important that all network devices prior to deployment or enablement of IPv6 feature set are subjected to interoperability with similar products from multiple vendors so that VA is not forced to deploy products from a single vendor. The specific test cases that devices under test would be subjected to under interoperability testing will be tailored to VA IPv6 specific requirements. To achieve interoperability it is important that at least 2 or more product types from different vendors performing the same functions are connected together to achieve the same functionality level, as if the two products from the same vendor are connected. Figure 18below shows a reference test bed illustrating the interoperability between 2 or more end devices. For example, if IPv6 Stateless Address Auto configuration (SLAAC) is being tested, and the Device under Test is a router, then no less than three different host operating systems should be used to test this function.

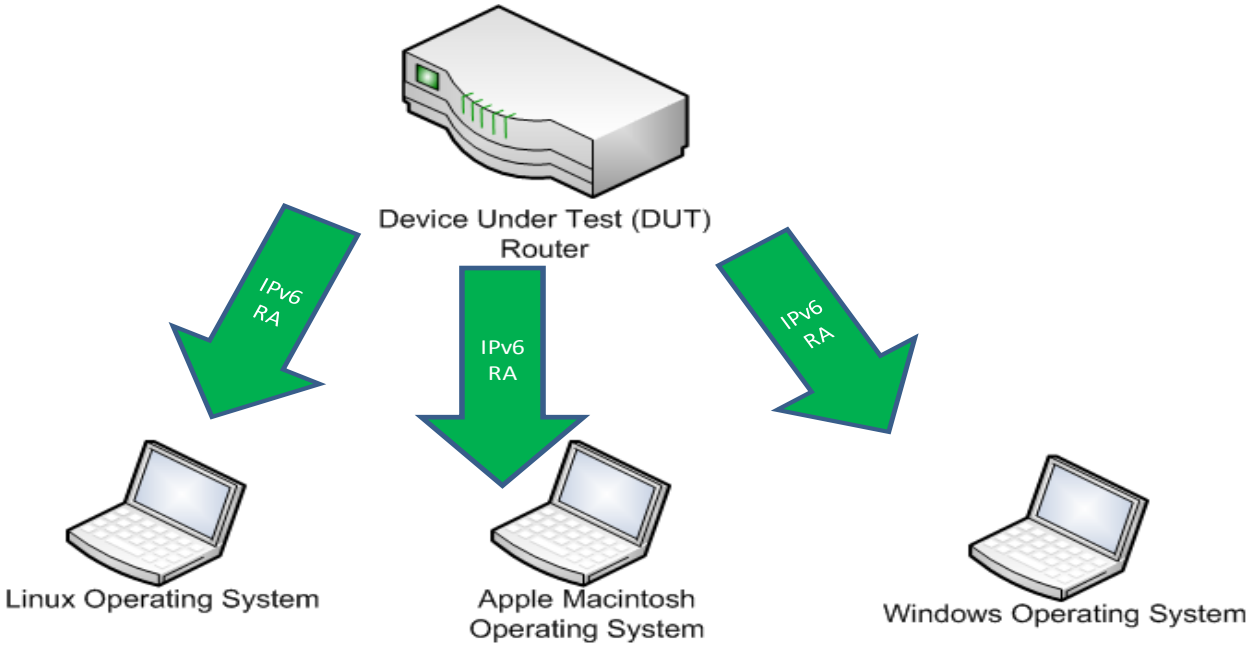


Figure 18: Interoperability reference test setup

6.1.3 VA IPv6 Compliance – Performance Testing

This test is added to the USGv6 profile testing requirements to ensure that all IPv6-capable devices that are deployed in VA networks are capable of achieving maximum throughput per VA IPv6 test capability requirements. Performance testing is a very important piece in the overall acceptance of a device under test for deployment. Performance testing helps in characterizing the performance of the data plane in forwarding IPv6 and IPv4 traffic. IETF RFC2544 defines how to characterize data plane performance. In addition to the throughput testing, performance testing evaluates the behavior of the device under test when it is subjected to operational transient conditions. This ensures that the devices under test do not fail in an operational environment when it experiences an unplanned transient event and it continues to perform its expected functions. The performance testing helps in assessing the basic throughput, frame loss, and latency variances. Major components of performance testing include, but are not limited to:

- **Throughput performance testing** (frame loss, latency, back-to-back):
    - The back-to-back test determines how the DUT responds to different quantities of frames with the minimum gap allowed by the protocol specification;

- The frame loss test determines how the DUT responds to streams with different loading;
- The throughput test finds the highest rate at which the DUT can forward frames without dropping any offered frame;
- The latency test reveals how much processing overhead the DUT requires to forward frames; and
- CPU utilization tests allows the operator to understand the percentage of CPU time utilized by the device under test during the traffic forwarding test, confirming if any of the frames are switched in software.

- **Stress Testing:** A testing method that exercises both the data forwarding performance concurrent with control plane stress is one of the most effective methods of measuring a router's performance. Hence, within VA IPv6 test capability compliance, this type of test is mandated and is required that all devices that are considered to be acquired for IPv6 deployment pass this rigorous test requirement.
- **Scaling Testing:** Scaling testing allows the agencies to evaluate and understand the ability of the IPv6-capable device to adapt to future network growth in terms of services, protocols, and functionalities and if it will be able to adopt the routing, subscriber, and services increments. Scaling testing results will help the VA ensure the economic viability of the selected IPv6-capable devices and support for the future network growth without forklift upgrades.

IPv6 Performance testing should be done in a similar nature by using an isolated Device under Test and a test tool; however, instead of conformance test traffic, the tool should test throughput, packet loss, and latency. Using RFCs 2544 and 5180 as guides, traffic mixes must use specific packet sizes and variations of TCP/UDP traffic. Table 1 is a methodology used in the IT industry to ensure devices are benchmarked as per specification. It is important to test using IPv4-only as a baseline, and then use a mix of IPv4 and IPv6, and then IPv6-only to evaluate the amount of performance degradation or performance gain.

Performance Test	Bytes of Data

IPv4-only	64, 128, 256, 512, 1024, 1280, 1518, 1522[1], 2048[1], 4096[1], 8192[2], 9216[1]
IPv6 and IPv4	64, 128, 256, 512, 1024, 1280, 1518, 1522[1], 2048[1], 4096[1], 8192[1], 9216[1]
IPv6 only	64, 128, 256, 512, 1024, 1280, 1518, 1522[1], 2048[1], 4096[1], 8192[1], 9216[1]

Table 1: IPv6 Performance Testing Environment

Test Traffic Mixes	Percent of Traffic
IPv4-only	100%
IPv6 only	0%

Table 2: IPv4-only Performance Testing Environment

Test Traffic Mixes	Percent of Traffic
IPv4-only	50%
IPv6 only	50%

Table 3: IPv4 and IPv6 Performance Testing Environment

Test Traffic Mixes	Percent of Traffic
IPv4-only	0%
IPv6 only	100%

Table 4: IPv6-only Performance Testing Environment

[2] Denotes jumbo-frames which are Ethernet frames larger than 1500

6.1.4 VA IPv6 Compliance – Regression Testing

Regression testing is a very crucial component of the testing realm that seeks to find new software or hardware errors in existing implementation after changes have been made to a system, such as functional enhancements, patches or configuration changes. Regression testing is mostly an automated set of tests that are executed to ensure that there is no functional impact following the changes made to the system. For VA IPv6 test compliance capability, it is important that all new upgrades and software patches are subjected to such a testing to ensure that a change such as a bug fix did not introduce new faults and whether the change in one part of the software affects the other parts of the software.

Protocol stress test confirms that the new releases, when subjected to the transient condition continue to fulfill the main functions of the devices for which they are deployed in the network. Protocol stress testing can be performed as part of the overall performance verification of the system where multiple features or protocols are enabled and the interaction and impact of scaling one sub-system on the other is measured through the CPU time utilization.

Common methods of regression testing include rerunning previously run tests and checking whether program behavior has changed and whether previously fixed faults have re-emerged.

Regression testing can be used to test a system efficiently by systematically selecting the appropriate minimum set of tests needed to adequately cover a particular change.

6.1.5 VA IPv6 Compliance - Functional Testing

Functional testing is a type of black box testing that verifies the specifications of the device under test. It offers a test environment that mimics the real-world parameters and examines the output and internal structure of the device which is rarely considered. As long the system is able to perform its core functions, the functionality testing does not look into the implementation details of the capabilities. Functional testing differs from system testing in that functional testing verifies an IPv6-capable product by checking it against the design document or specification, while the system testing a benchmark against the system requirements. Functional testing typically consists of following steps:

- Creation of use cases and identification of functions that an IPv6-capable device is expected to perform when deployed in real world environment (**Operational** test cases);
- Creation of the use cases that require interaction between the software modules of the device under test (**Interworking** - such as IGP BGP interaction, convergence of module impacts the convergence of the other);
- Creation of the use cases that requires aggregation of the heterogeneous networks (Interworking, such as border gateway aggregating layer 2 and layer 3 networks);
- The creation of input data based on the functional specifications;
- Determination of output based on the function specifications; and
- Comparison of actual version expected results.

6.1.6 VA IPv6 Acceptance Testing

VA IPv6 Test capability compliance requirements is a comprehensive suite of requirements that ensures that any IPv6-capable devices that go through the final stages of VA acquisition process have successfully passed all the test classes for each category of VA IPv6 profile. Acceptance testing is a classification or group of tests that together ensure that the device under test is capable of meeting or exceeding the agency's requirements based on pre-determined specifications or contract. (This may be for hosts, routers, network protection devices, network management systems, applications or services).

Acceptance testing can further be classified as user acceptance testing (in this case VA IPv6 acceptance testing), which is a process of obtaining confirmation that a system meets mutually agreed upon requirements. The confirmation is received following a series of trails and reviewing the results of all the tests defined above. The acceptance testing should also confirm the operational readiness of the IPv6-capable device thus ensuring that the processes and procedures are in place to allow the device to be used and maintained once deployed. This may include checks done for backward compatibility, procedures for disaster recovery, training for end users, maintenance procedures, and security procedures. In addition, the VA

IPv6 acceptance criteria requires the IPv6-capable product to be tested and evaluated against acceptance criteria as documented in a contract, before the system is accepted.

In regulation acceptance testing, an IPv6-capable product is tested to ensure it meets governmental, legal, and safety standards.

6.1.7 IPv6 Application Testing

IPv6-aware Applications are those software programs that have a listening and sensing function on the network interface. These applications have a well understood network service like DNS, DHCPv6, or HTTP. However, this testing should also include applications that provide network functions outside of standard network services like SQL database calls, JSON database connections, and network proxy traffic. Testing these functions must be done in the following three environments:

1. IPv4-only – Meaning all testing will done without any IPv6 support on the network;
2. Dual-Stack – Meaning that all done will be done with both IPv4 and IPv6 support on the network; and
3. IPv6-only – Meaning all testing will done without any IPv4 support on the network.

7 VA IPv6 Compliance Test Environments

The Test Environment being specified and deployed will be sufficient to ensure compliance/conformance and interoperability based on the requirements in both the relevant USGv6 Product Profiles as well as the VA-specific profiles defined above. This is meant to not only comply with the FAR, but to also meet the VA-specific mission requirements (specifically including, but not limited to, the areas of functionality, security, software). The benchmarks being targeted are based on four objectives, as follows.

1. Note that "Objective 1" is already a live requirement: "By December 2011 - All agency networked IT procurements comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6

capabilities". The goal of this document and process is to extend the VA acquisition rules to add additional, VA-specific requirements and characteristics.

2. "Objective 2": no later than September 2012, all public/external facing servers and services will support native IPv6 users. NIST is tracking this information publically at http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov and the VA-specific information is: http://usgv6-deploymon.antd.nist.gov/cgi-bin/cfo?agency=veterans.
3. "Objective 3" extends the IPv6 support requirement, "All internal infrastructure and applications will operate using native IPv6" by September 2014.
4. And finally, "Objective 4" - "all computing, application, and network resources will turn off IPv4 as a communication mechanism, and create isolated IPv4 enclaves for legacy systems that cannot convert to native IPv6 operations. These IPv4 enclaves must have a waiver from the VA CIO."

In addition to the **Conformance** and **Interoperability** test objectives included in USGv6, the overall VA testing procedures will incorporate the additional objectives of **VA Mission Requirements**, **Performance** and **IA/Security** testing. These objectives must be tested under 4 modes of operation:

1. Baseline,
2. IPv4-only,
3. Dual-Stack, and
4. IPv6-only.

7.1 IPv4-only

An IPv4-only test segment will be used to establish a baseline for performance comparisons. Baseline testing will verify that products perform as needed/claimed in an IPv4-only environment, as well as establish the actual performance values for the device under test. This will enable more accurate comparisons between the various testing scenarios. This will involve functional, scalability/performance, and interoperability testing.

Note that one area of functionality that must be assessed is the support for name lookup requests (DNS) versus any hard-coded IP (v4, "literal") addresses. Additionally, any reliance on non-IP

communications must also be evaluated. Sufficient test cases will be defined to establish baseline Performance levels in an IPv4-only deployment.

Although not technically part of the lab environment it is valuable to identify the key stakeholders from whom buy-in needs to be attained – the leads from each of the following areas (and other key stakeholders, as identified) must be given the opportunity to review the processes and procedures proscribed herein, and to recommend additional baseline requirements to test for/against (such as the number of packets per second of which a device fulfilling a given role must be capable).

7.2 Dual-stack

Dual-Stack testing will verify that products continue to function in a dual stack (IPv4 and IPv6 enabled) network, as well as evaluate the relative performance thereof. This includes comparing not only the "IPv4 performance" to "IPv6 performance", but also comparing the "IPv4 performance in an IPv4-only environment" to the "IPv4 performance in a Dual-Stack environment". Specifically, devices should perform adequately using either IPv4 or IPv6, with a preference on using IPv6 if both are present and provide equivalent connectivity.

Note that one area of functionality that must be assessed is the support for name lookup requests (DNS) versus any hard-coded IP (v4 or v6, "literal") addresses. Additionally, any reliance on non-IP communications must also be evaluated.

In addition to "parity" as described above, this area of testing will also focus on the protocol independent mode of operation – that is, in the most general sense, any device/application/service/solution should have neither a particular affinity to nor requirements for a specific protocol. Note that the general best practice of preferring native IPv6 connections vs. native IPv4 connections will also be verified when both protocols are present and otherwise equal.

"Simple parity" is not always attainable. In examples such as routers, the increased size of the packet header and address fields may limit the ability for a specific device to perform under dual-

stack conditions "on par" with IPv4-only performance. This must be factored into the specified requirement for the device to be used within a given role.

Sufficient test cases will be defined to verify that VA Mission Requirements, Interoperability concerns, Performance levels, standards Conformance, and IA/Security capabilities are met in a Dual-Stack deployment.

7.3 IPv6-only

In the interest of looking toward the future, as soon as CY 2015 within the VA, the ability for a device/application/service/solution to function without any IPv4 being present must be evaluated. The testing should verify that capabilities/performance/scalability does not suffer notably due to IPv4 being absent – that is, IPv6-based connectivity should be on par with IPv4 connectivity, with exceptions / limitations as mentioned above.

Note that one area of functionality that must be assessed is the support for name lookup requests (DNS) versus any hard-coded IP (v4 or v6, "literal") addresses. Additionally, any reliance on non-IP communications must also be evaluated.

Sufficient test cases will be defined to verify that VA Mission Requirements, Interoperability concerns, Performance levels, standards Conformance, and IA/Security capabilities are met in an IPv6-only deployment.

7.4 Testing the Tester

The devices and procedures performing the tests, and the procedures being used for the testing, must be evaluated against industry "current best practices/capabilities" as well as claimed/operational capabilities. The relevant standards must be decided upon and routinely evaluated/updated. Additionally, in accordance with the VA Test and Evaluation Plan, collaboration with regional Program Managers (PMs) will be a key component of the testing effort. The VA test team will interface with the regional PMs, insure that acquisitions understand the IPv6 capabilities required, and verify that systems currently in the acquisition, deployment, or production cycles conform as needed.

For example, best practices such as the following must be incorporated into the VA testing process:

- RFC 4148 - IP Performance Metrics (IPPM) Metrics Registry,
- RFC 1242 - Benchmarking Terminology for Network Interconnection Devices,
- RFC 2544 - Benchmarking Methodology for Network Interconnect Devices, and
- RFC 5180 - IPv6 Benchmarking Methodology for Network Interconnect Devices.

The characteristics being evaluated include, but are not limited to:

- Throughput – The maximum amount of data (frames) the device is capable of sending/receiving without dropping frames;
- Delay – The time needed for a packet to be transmitted and fully received by the destination (one-way or round-trip);
- Loss – The portion of packets transmitted, but not received by the destination compared to total number or packets transmitted (one-way or round-trip);
- Jitter – The variation in delay between all packets in a stream taking the same route;
- Latency – The time it takes for one packet to be sent and received. This process will involve the device time stamping the packet;
- Packet reordering – The portion of packets delivered to the destination in the wrong order compared to total number of packets;
- Bulk transfer capacity – The measure of a network's ability to transfer significant quantities of data with a single congestion-aware transport connection [e.g., Transmission Control Protocol (TCP)] per unit of time;
- Link bandwidth capacity – The theoretical maximum amount of data that the link can support;
- Link utilization – The fraction of the total link capacity underutilization; and
- Packet duplication – Multiple packets are an inefficient use of network resources.

8 VA IPv6 Profile Development Process

8.1 VA IPv6 Profile Approach

NIST Special Publication 500-267, A Profile for IPv6 in the U.S. Government – Version 1.0 provides agencies with a taxonomy and framework to specify IPv6 requirements on a device level basis. This means that the USGv6 Profile is not a single profile to be utilized for acquisition purposes, but a profile process that agencies can utilize to build device compliant profiles to provide vendors with detailed IPv6 specifications based on Internet standards (RFCs). The use of the USGv6 Profile and Testing process was mandated by changes to the FAR that occurred in July of 2010.

The development process NIST utilized for the USGv6 Profile took into account industry work from groups such as the IPv6 Ready Logo program and from other Federal IPv6 profile activities, specifically those within the DoD at DISA. The VA IPv6 Profile approach utilized the USGv6 profile as a foundational starting point in developing the specific IPv6 profile requirements for VA. This approach could have relied solely on the USGv6 Profile process to develop device compliant profiles. However, it was clear that VA had many unique requirements associated with its mission that could levy additional requirements on IPv6 devices within the Department. One example of this is the need for interoperability with DoD for a range of activities such as the sharing of electronic health records. Another example of VA specific requirements is on the use of medical devices within the Enterprise and the specialized testing requirements associated with those. In addition, the VA found that the standards within the NIST USGv6 Profile have not been recently updated and required refreshing to stay current with commercial industry deployment.

Outside of the breadth of standards that are referenced in the USGv6 Profile, there has been a strong interest within VA and other agencies to extend the profile process beyond the current scope of devices (host, router, and NPD) to include other items such as applications and services. The VA IPv6 Profile process has captured this desired expansion to provide the taxonomy and framework to specify IPv6 requirements for applications and services in addition to devices.

The VA IPv6 Profile process expands on the USGv6 Profile process to allow users to create device, application, and/or service compliant profiles to meet a specific requirement that can be utilized for acquisition and a range of test specifications. The VA IPv6 Profile process is intended to be utilized with the overall test approach and test requirements. It is still able to build off the USGv6 Test approach and accredited test labs.

8.2 VA IPv6 Device Compliant Profile Tool

Given the diverse nature of the VA's operating environment it is not feasible to have a single profile for every possible device within a specific category. For this reason, the Conformance Matrix defined as part of this process [Figure 19, Figure 20] is intended to provide guidance in the construction of product profiles by listing the specific applicable standards and calling out specific requirements. The intention is for a Program Manager to work with procurement to define what is truly needed for a given project, solution, purchase, etc., and to take the relevant column from the Conformance Matrix to build a specific device profile.

	Hosts					Routers			VA-Sw		VA-NPD						Services				
																	Endpoint				
	USGv6	Desktop/laptop	Servers	Network Appl.	Medical Devices	USGv6	VA	VA-Consumer	L2-only	L3-aware	NPD	FW	APPFW	IDS	IPS	Applications / SW	SaaS	PaaS	IaaS	ISP	RFC Desc:
USGv6 Derived RFC-based Requirements																					
1772						CM	M	CM										CM	M	CM	BGP - Internet
1981	M	M	M	M	M	M	M	M		M							M	M	M	M	PathMTUD
1981#section-4	M	M	M	M	M	S+	M	M		M									M	M	PathMTUD:Discovery Protocol Reqs
2404	M	M	M			M	M	M		M											HMAC-SHA1-96
2410	M	M	M			M	M	M		M											NULL Encr
2451	M	M	M			M	M	M		M											ESP CBC mode Algs
2451#section-2.6	M	M	M			M	M	M		M											ESP CBC mode Algs:3DES-CBC
2460	M	M	M	M	M	M	M	M		M						M	M	M	M	M	IPv6
2460#section-2	M	M	M	M	M	M	M	M		M						M	M	M	M	M	IPv6 Packets: send, receive
2460#section-2						M	M	M										CM	M	M	IPv6 packet forwarding
2460#section#section-4	M	M	M	M	M	M	M	M		M						M	M	M	M	M	IPv6:Ext Hdr

Figure 19: Snippet taken from the Conformance Matrix

The overall matrix covers a wide range of product classes and calls out the relevant standards (in the categories discussed: "USGv6, RFC", "USGv6, non-RFC", "Non-USGv6, RFC" and "Non-USGv6, non-RFC"). For example, a Program Manager looking to procure a Workstation device would take the Workstation column requirements and simply identify all of the Conditionally

Mandatory (CM) parameters as Mandatory (M) or unneeded (blank). The resulting specific "Device Profile" would look something like the following, but having every M included (and whitespace optionally removed for clarity).

1981	M	PathMTUD
1981#section-4	M	PathMTUD:Discovery Protocol Reqs
2404	M	HMAC-SHA1-96
2410	M	NULL Encr
2451	M	ESP CBC mode Algs
2451#section-2.6	M	ESP CBC mode Algs:3DES-CBC
2460	M	IPv6
2460#section-2	M	IPv6 Packets: send, receive
2460#section#section-4	M	IPv6:Ext Hdr
2460#section-4.3	M	IPv6:Ext Hdr:HbH, Unrecognized
2460#section-4.3	M	IPv6:Ext Hdr:FragHdr
2460#section-4.3	M	IPv6:Ext Hdr:DestOpt
2464	M	IPv6 over Foo:Ethernet
2474	M	DiffServ
3306	M	Mcast UniPrefix
3307	M	Mcast Alloc Guidelines
3484	M	DefAddrSel
3596	M	DNSv6-Client
3596#section-2.1	M	DNSv6-Client:AAAAs
3596#section-2.5	M	DNSv6-Client:PTR (ipv6.arpa)
3775#section-8.1	M	MIPv6:All nodes as CN
3810	M	Mcast MLDv2
3879	M	Deprec SLAs
4007	M	Scoped Addr Arch
4007	M	Scoped Addr Arch - manual configuration?
4193	M	ULAs
4213#section-2	M	Transition Mechanisms:Dual Stack
4291	M	AddrArch
4301	M	Security Arch

Figure 20: Snippet taken from a Device Profile (Workstation)

Note that there are items in the Conformance Matrix that are listed as Mandatory – either inherited from USGv6 requirements or because they are beneficial, highly recommended, and should be readily available. In the event that no available product meets a Mandatory requirement, if that Mandatory requirement is not suitable for a given product, or if the requirement is superseded by other, better capabilities, a waiver can be issued from the CIO for that product.

8.3 VA IPv6 Compliance SDoC Requirements

As mentioned previously, the SDoC calls out what test specifications were run during testing. This is shown in Figure (x), however the degree of difficulty for a procurement manager to decipher what standards were successfully tested is very high. Only by digging into each of the test specifications, can a procurement manager determine this information.

Moving forward, VA procurement managers should use Table 5 below to determine whether the standard was tested per the VA IPv6 Product Profile. The Table contains test cases identified in GREEN and items that do not have test cases identified in RED. Part of the USGv6 process is that items marked "Self Test" are the responsibility of the vendor to self-certify based in the absence of test case.

RFC	RFC Desc:	USGv6 Test Case Mappings
1772	BGP - Internet	BGP_v1.1_I
1981	PathMTUD	Basic_v1.2
1981#section-4	PathMTUD:Discovery Protocol Reqs	Basic_v1.2
2404	HMAC-SHA1-96	Self Test
2410	NULL Encr	Self Test
2451	ESP CBC mode Algs	Self Test
2451#section-2.6	ESP CBC mode Algs:3DES-CBC	Self Test
2460	IPv6	Basic_v1.2
2460#section-2	IPv6 Packets: send, receive	Basic_v1.2
2460#section-2	IPv6 packet forwarding	Basic_v1.2
2460#section#section-4	IPv6:Ext Hdr	Basic_v1.2
2460#section-4.3	IPv6:Ext Hdr:HbH, Unrecognized	Basic_v1.2
2460#section-4.3	IPv6:Ext Hdr:FragHdr	Basic_v1.2
2460#section-4.3	IPv6:Ext Hdr:DestOpt	Basic_v1.2
2464	IPv6 over Foo:Ethernet	Basic_v1.2
2467	IPv6 over Foo:FDDI	Self Test
2473	Generic Packet Tunneling	Self Test
2474	DiffServ	Self Test
2475	DiffServ Arch	Self Test
2491	IPv6 over Foo:NBMA	Self Test
2492	IPv6 over Foo:ATM	Self Test
2497	IPv6 over Foo:ARCnet	Self Test
2507	IP Hdr Comp	Self Test
2526	Subnet Anycast Addr	Self Test
2545	BGP-MP for IPv6 IDR	Self Test

2590	IPv6 over Foo:Frame Relay	Self Test
2597	DiffServ AF PHB	Self Test
2671	DNSv6:EDNS0	Self Test
2675	Jumbograms	Self Test
2711	RtrAlert	Self Test
2740	OSPFv3	OSPFv3_v1.2
2784	GRE	Self Test
2983	DiffServ + tunnels	Self Test
3086	DiffServ PDB (Per Domain Behav)	Self Test
3095	ROHC RTP, UDP, ESP and uncomp	Self Test
3140	DiffServ PHBs	Self Test
3146	IPv6 over Foo:Firewire (IEEE 1394)	Self Test
3168	IP + ECN	Self Test
3173	IP Payload Comp	Self Test
3226	DNSSEC & IPv6 Msg Size Reqs	Self Test
3241	ROHC over PPP	Self Test
3246	DiffServ EF PHB	Self Test
3247	DiffServ EF PHB Supplemental	Self Test
3260	DiffServ Clarification / Terms	Self Test
3289	DiffServ MIB	Self Test
3306	Mcast UniPrefix	Self Test
3307	Mcast Alloc Guidelines	Self Test
3315	Stateful DHCPv6-Server	DHCP-Server-v1.0
3315	Stateful DHCPv6-Client	DHCP_Client_v1.0 I
3315	Stateful DHCPv6-Client - be able to disable it!	DHCP_Client_v1.0 I
3411	SNMPv3	Self Test
3412	SNMP Message Process and Dispatch	Self Test
3413	SNMP Apps	Self Test
3413#section-1.2	SNMP Apps:Command Responder	Self Test
3413#section-1.3	SNMP Apps:Notification Generator	Self Test
3414	SNMPv3:User-based Sec Model	Self Test
3484	DefAddrSel	Addr_Arch_v1.2
3484#section-2.1	DefAddrSel:ConfigurablePolicies	Self Test
3493	Basic Socket API v6	Self Test
3526	More MODP DH groups for IKE	Self Test
3542	Adv Socket API v6	Self Test
3566	AES-XCBC-PRF-128	IKEv2_v2.0
3572	IPv6 over Foo:MAPOS (SONET/SDH)	Self Test
3596	DNSv6-Server	Self Test
3596	DNSv6-Client	Self Test

3596#section-2.1	DNSv6-Client:AAAAs	Self Test
3596#section-2.5	DNSv6-Client:PTR (ipv6.arpa)	Self Test
3602	IPsec:AES-CBC	Self Test
3633	DHCPv6-Prefix Delegation	Self Test
3678	Socket API Extension for MCAST Src Filters	Self Test
3686	IPsec: AES-CTR	Self Test
3736	Stateless DHCPv6	Self Test
3775	MIPv6	Self Test
3775#section-8.1	MIPv6:All nodes as CN	Self Test
3775#section-8.2	MIPv6:RouteOpt	Self Test
3775#section-8.2	MIPv6:DisableRouteOpt	Self Test
3775#section-8.3	MIPv6:All IPv6 Rtrs	Self Test
3775#section-8.4	MIPv6:HA	Self Test
3775#section-8.5	MIPv6:MN	Self Test
3810	Mcast MLDv2	Self Test
3843	ROHC for IP	Self Test
3879	Deprec SLAs	Addr_Arch_v1.2
3948	ESP:UDP	Self Test
3956	Mcast ERP	Self Test
3963	NEMO	Self Test
3971	SEND	Self Test
3972	CGAs	Self Test
3986	URI: Generic Syntax	Self Test
4007	Scoped Addr Arch	Addr_Arch_v1.2
4007	Scoped Addr Arch - manual configuration?	Addr_Arch_v1.2
4022	TCP MIB	Self Test
4038	Application Transition	Self Test
4087	IP Tunnel MIB	Self Test
4106	IPsec:AES-GCM	Self Test
4106#section-6	IPsec:AES-GCM:128b ICV	Self Test
4106#section-8.1	IPsec:AES-GCM:128b keys	Self Test
4113	UDP MIB	Self Test
4191	DefRtrPref	Self Test
4192	IP Forwarding	Self Test
4193	ULAs	Addr_Arch_v1.2
4213	Transition Mechanisms	Self Test
4213#section-2	Transition Mechanisms:Dual Stack	Self Test
4213#section-3	Transition Mechanisms:Conf Tunnels	Self Test
4271	BGP-4	BGP_v1.1_I
4282	MIPv6:NetAccessID	Self Test
4283	MIPv6:MN ID	Self Test

4291	AddrArch	Self Test
4292	IP Fwd MIB	Self Test
4293	IP MIB	Self Test
4295	MIP MIB	Self Test
4301	Security Arch	IPsecv3_v1.3
4301#section-4.1	IGW or IPv4:Security Arch:Transport Mode SAs	IPsecv3_v1.3
4301#section-4.5.1	Security Arch:Manual SA/Keying	IPsecv3_v1.3
4301#section-4.5.2	Security Arch:Auto SA/Keying	IPsecv3_v1.3
4302	AH	Self Test
4303	ESP	IPsecv3_v1.3
4306	IKEv2	IKEv2_v1.1
4306#section-3.3.3	IKEv2:ESN	IKEv2_v1.1
4306#section-4	IKEv2:PSK	IKEv2_v1.1
4306#section-4	IKEv2:RSA	IKEv2_v1.1
4306#section-4	IKEv2:NATT	IKEv2_v1.1
4307	IKEv2:CryptoAlgs	IKEv2_v1.1
4307#section-3.1.1	IKEv2:CryptoAlgs:3DES-CBC	IKEv2_v1.1
4307#section-3.1.1	IKEv2:CryptoAlgs:AES-CBC w/ 128b keys	IKEv2_v1.1
4307#section-3.1.1	IKEv2:CryptoAlgs:HMAC-SHA-1	IKEv2_v1.1
4307#section-3.1.3	IKEv2:CryptoAlgs:AES-CTR w/ 128b keys	IKEv2_v1.1
4307#section-3.1.4	IKEv2:CryptoAlgs:HMAC-SHA1 as a PRF	IKEv2_v1.1
4307#section-3.1.4	IKEv2:CryptoAlgs:AES128-XCBC-PRF	IKEv2_v1.1
4307#section-3.1.5	IKEv2:CryptoAlgs:AES-XCBC-MAC-96	IKEv2_v1.1
4308	Crypto Suites	Self Test
4308#section-2.1	Crypto Suites:VPN-A	Self Test
4308#section-2.2	Crypto Suites:VPN-B	Self Test
4309	IPsec: AES-CCM	Self Test
4338	IPv6 over Foo:Fibre Channel	Self Test
4361	Node Specific Client IDs for DHCPv4	Self Test
4362	ROHC - Link Assisted for IP/UDP/RTP	Self Test
4434	IPsec:AEX-XCBC-PRF-128	IKEv2_v2.0
4443	ICMPv6	Basic_v1.2
4543	IPsec:AES-GMAC	Self Test
4543#section-5.4	IPsec:AES-GMAC:NULL ENCR, AUTH-AES-GMAC	Self Test
4543#section-5.4	IPsec:AES-GMAC:AUTH-AES-GMAC	Self Test
4552	Auth/Conf for OSPFv3	OSPFv3_v1.2
4581	CGA:Ext Field Format	Self Test
4584	Socket API Extension for MIPv6	Self Test
4594	DiffServ Config Guidelines	Self Test
4601	Mcast PIM-SM	Self Test

4604	Mcast MLDv2 SSM	Self Test
4607	Mcast SSM	Self Test
4609	Mcast PIM-SM Sec Issues/Enhancements	Self Test
4718	IKEv2:Clarifications & Impl Guidelines	IKEv2_v1.1
4760	BGP-MP	BGP_v1.1_I
4798	6PE	Self Test
4807	IPsec Policy DB Conf MIB	Self Test
4809	CertMgmtProfile	Self Test
4815	ROHC Profiles for RTP, UDP, ESP and Uncomp Clarifications	Self Test
4835	CryptoAlgs	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:3DES-CBC Encr	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:NULL Encr	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:AES-CBC w/ 128b keys	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:AES-CTR w/ 128b keys	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:HMAC-SHA-1	ESP-v1.1
4835#section-3.1.1	CryptoAlgs:AES-XCBC-MAC-96	ESP-v1.1
4835#section-3.1.2	CryptoAlgs:AES-CCM w/ 128b keys	ESP-v1.1
4835#section-3.2	CryptoAlgs:HMAC-SHA-1	ESP-v1.1
4835#section-3.2	CryptoAlgs:AES-XCBC-MAC-96	ESP-v1.1
4861	ND	Basic_v1.2
4861#section-4.1	ND:RD	Basic_v1.2
4861#section-4.2	ND:RD	Basic_v1.2
4861#section-4.6.2	ND:PD	Basic_v1.2
4861#section-7.2	ND:ND	Basic_v1.2
4861#section-7.2.3	ND:DAD	Basic_v1.2
4861#section-7.2.5	ND:NA and NS	Basic_v1.2
4861#section-7.3	ND:NUD	Basic_v1.2
4861#section-8	ND:Redirect	Basic_v1.2
4862	SLAAC	SLAAC-v1.1
4862#section-5.3	SLAAC:Link Local	SLAAC-v1.1
4862#section-5.4	SLAAC:DAD	SLAAC-v1.1
4862#section-5.5	SLAAC:Global	SLAAC-v1.1
4862	SLAAC:DisableGlobal	SLAAC-v1.1
4868	HMAC-SHA-256	IKEv2_v2.0
4868#section-2.3	HMAC-SHA-256-128	IKEv2_v2.0
4868#section-2.3	HMAC-SHA-256-128	IKEv2_v2.0
4868#section-2.4	HMAC-SHA-256 as PRF	IKEv2_v2.0
4869	SuiteB Crypto Suites	Self Test
4877	MIPv6:IKEv2 / Revised IPsec Arch	Self Test
4884	Ext ICMP (MultiPart)	Self Test

4891	Using IPsec to secure v6 in v4 (Prot41)	Self Test
4941	Privacy Ext for SLAAC	Self Test
4941	Privacy Ext for SLAAC - MIP	Self Test
4944	IPv6 over Foo:IEEE802.15.4	Self Test
4945	PKI profile of IKEv1, IKEv2 and PKIX	Self Test
4982	SEND:CGA:Multiple Hasl Algs.	Self Test
4995	ROHC	Self Test
4996	ROHC TCP	Self Test
5014	Socket API for Src Addr Sel	Self Test
5072	IPv6 over Foo:PPP	Self Test
5095	Deprecate RH0	Basic_v1.2
5114	IKEv2:Addl DH groups	Self Test
5114#section-2.3	Addl DH groups:DH MODP grp 24	Self Test
5114#section-3.2	Addl DH groups:DH MODP grp 24	Self Test
5175	RA Flags Option	Self Test
USGv6 Derived non-RFC-based Requirements (SP500-267)		
Section 6.12.3.1	IPv6 connectivity	NPD_v1.3
Section 6.12.3.2	Dual Stack	NPD_v1.3
Section 6.12.3.3	Administrative Functionality	NPD_v1.3
Section 6.12.3.4	Authentication and Authorization	NPD_v1.3
Section 6.12.3.5	Security of Control and Comms	NPD_v1.3
Section 6.12.3.6	Persistence	NPD_v1.3
Section 6.12.3.7	Logging and Alerts	NPD_v1.3
Section 6.12.3.8	Fragmented Packets Handling	NPD_v1.3
Section 6.12.3.9	Tunneled Traffic Handling	NPD_v1.3
Section 6.12.4.1.1	Port/protocol/address blocking	NPD_FW_v1.3 & NPD_APFW_v1.3
Section 6.12.4.1.2	Asymmetrical Blocking	NPD_FW_v1.3 & NPD_APFW_v1.3
Section 6.12.4.1.3	IPsec Traffic Handling	NPD_FW_v1.3 & NPD_APFW_v1.3
Section 6.12.4.1.4	Performance Under Load, Fail Safe	NPD_FW_v1.3 & NPD_APFW_v1.3
Section 6.12.4.2.1	No violation of trust barriers	NPD_APFW_v1.3
Section 6.12.4.2.2	Session Traffic Auth	NPD_APFW_v1.3
Section 6.12.4.2.3	Email, File Filtering	NPD_APFW_v1.3
Section 6.12.5.1.1	Known Attack Detection	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.1.2	Malformed pkt detection	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.1.3	Port scan detection	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.1.4	Tunneled traffic detection	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.1.5	Logging and Alerts	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.1.6	Performance Under Load, Fail Safe	NPD_IDS_v1.3 & NPD_IPS_v1.3
Section 6.12.5.2.1	Intrusion Prevention	NPD_IPS_v1.3

Table 5: USGv6 Standards to USGv6 Test Case Mappings

8.4 VA IPv6 Device Compliant Profile and SDoC Registry

The IPv6 Profile Process provides the VA with a powerful tool to develop comprehensive IPv6 specifications for devices, applications, and services. While this allows VA organizations to create numerous IPv6 profiles that meet specific mission requirements, it could become extremely difficult to manage numerous, overlapping profiles and their related SDoCs.

The ability for the PMTO or other VA organizations to create VA-wide profiles that can be utilized by various VA organizations is essential to properly managing the VA IPv6 Profile Process. The use of a central "Registry" for profiles will provide a method to limit the number of profiles to a manageable number, which will result in lower cost and interoperability issues.

The initial registry can be established under VA's IPv6 Sharepoint Site. Eventually, the IPv6 Device Compliant Profiles should be added to VA's Technical Reference Model (TRM) as part of VA's Enterprise Architecture.

9 VA IPv6 Profile Development Classes

An important consideration in the definition of a testing program is to determine which tests are relevant/required for which classes of equipment or services. As the underlying subset of requirements is set in NIST's "A Profile for IPv6 in the US Government – Version 1.0" (USGv6, SP500-267) these will be referenced herein. USGv6 intentionally defines a "simple taxonomy" that should be applicable to the vast majority of devices. However, the VA has specific mission needs that necessitate additional specification granularity and functional requirements, and this classification methodology is defined below to meet those needs and to provide additional guidance to the acquisitions operations therein.

It is also worth mentioning that the USGv6 process only deals with RFC Conformance and Interoperability – not performance, additional IA/security considerations or any VA-specific needs. The process is meant to be flexible; defining certain levels of required capabilities and a wide range of optional / should capabilities. See Appendix 3 for a summary of the USGv6 requirements, as well as the matrix of VA-specific (derived and additional) requirements.

Definitions:

1. **Host:** any Node that is not a Router. A Host's primary purpose is to support application protocols that are the source and/or destination of IP layer communication.
2. **Network Appliances:** These are simple end nodes such as PDAs, Internet applications, sensors, medical devices, or home automation devices.
3. **Router:** A Node that interconnects sub-networks by packet forwarding. A Router's primary purpose is to support the control protocols necessary to enable interconnection of distinct IP sub-networks by IP layer packet forwarding.
4. **Network Protection Device:** Firewalls or Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.
5. **Network Management:** Protocols or systems for management of IPv6 enabled networks. These may also include probes that may be used to measure the network latency, recovery times, and other performance parameters.
6. **Applications:** All applications that enable hosts/workstations or other IPv6 enabled system that are functionally critical to VA and may be impacted by the transition from IPv4 to IPv6.
7. **Services:** These are network services that provide end-to-end connectivity to VA site offices such as Layer 3 VPN services, site connectivity or residential services.

It is believed that most of the devices in current VA infrastructure should fall into one of the above categories. In the following sections we discuss the IPv6 product profiles, the related requirements for each profile, and the test classes that should be considered as part of the VA IPv6 compliance test capabilities.

9.1 Hosts

Per the USGv6 (and, indeed, the Internet Engineering Task Force – IETF) a host is any node that is not a router. USGv6 also cautions that "The selection of major additional capabilities brings many issues of cost, complexity, availability, and security with them" – and this should be considered when defining or expanding these requirements.

As referenced above, USGv6 defines hosts to include everything that is not a Router (or Network Protection device) and it acknowledges that "modifications of the requirements" may be

necessary. The guiding principles for those modifications, wherein the VA will have several categories of "Hosts", is as follows.

9.1.1 Desktop/Laptop

Fitting the traditional concept of a Host is the average user workstation / interface mechanism – within the VA. These are most often Microsoft Windows-based, but may also include devices running Apple Mac OSX or any one of various Linux/Unix distributions, on a PC / thick-client device acting as the client-side in most sessions.

9.1.2 Servers

While a typical Server falls within the USGv6 definition of a Host within the VA, a category for Servers is defined to encompass (and require) various server-side requirements. Within the VA, the platforms in question will most often be Microsoft Windows or any one of various Linux/Unix distributions.

9.1.3 Network Appliances

A VA-specific categorization for Networked Appliances is also defined, the primary characteristic of which is that it is a dedicated-purpose device, vs. a general purpose server implementation. Examples include simple end nodes such as PDAs, sensors, or home automation devices.

9.1.4 Medical Devices

One area of special concern, and of specific importance within the VA's operating environment, is the broad range of special-purpose medical devices. While these devices have a broad range of non-network-centric requirements and certifications, a subset of these devices (any that are network-connected) will also be required to meet some level of IPv6 conformance and capability.

9.2 Routers

Per the USGv6 (and, indeed, the Internet Engineering Task Force – IETF) a router is a node that interconnects sub-networks by packet forwarding. While the definition of a router is consistent

between USGv6 and the VA profile, the conformance matrix (Appendix 2) serves to refine the actual requirements.

9.3 Switches

The VA Conformance matrix creates two network device classes that do not exist within USGv6. These are specifically for switching infrastructure gear. Switching is primarily a Layer2 function, most often operating on Ethernet frames vs. IP (IPv4 or IPv6) packets.

9.3.1 L2-only

A Layer2-only (L2-only) switch will be defined as a switching device that has no knowledge of, or impact on, Layer3 (L3) packet forwarding. Note that an L2-only switch may be managed, via IPv4 and/or IPv6, and the IPv6 conditional requirements in the conformance matrix for these devices are solely with regards to that management functionality. If the L2-only switch is unmanaged, truly unaware of L3 altogether, there are no IPv6 requirements except insofar as it must forward frames containing IPv6 packets.

9.3.2 L3-aware

A Layer3-aware (L3-aware) switch is a switching device, still primarily operating at Layer2 (L2) – however the device has some knowledge of Layer 3. This knowledge may include, but is not limited to, L3-aware functionality such as Multicast Listener Discovery (MLD) snooping or various Quality of Service (QoS) options. L3-aware switches also have IPv6-capable management requirements.

9.4 Network Protection devices

Per the USGv6 a Network Protection device is defined to include Firewalls or Intrusion Detection/Prevention devices that examine and selectively block or modify network traffic. These are devices that may often function similarly to other node types, but have specific design goals and considerations that differ from the more prototypical hosts and routers. Within the USGv6/NIST SP500-267 publication are non-RFC requirements for these device types.

The over-arching Network protection device category defines the minimal requirements that will apply to all of the following device types.

9.4.1 FW

USGv6 defines firewalls as devices that allow granular packet matching based on IP and Transport layer characteristics such as addressing, extension header, and port semantics – then permit or block traffic based on that matching.

9.4.2 APPFW

Similar in concept to a firewall, and application layer firewall is capable of matching application-specific characteristics (explicitly calling out email and file sharing) – and permit or block traffic based on that matching.

9.4.3 IDS / IPS

An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) fulfills the role of matching known malicious/hostile traffic or anomalous traffic patterns and either alerting (IDS) or actively blocking (IPS) these packets/sessions. Note that USGv6 requires that an IPS meet all of the IDS specifications, as well as actively mitigating threats.

9.5 Applications / SW

Not covered within the USGv6 definitions, the VA must also require that software being procured conform to IPv6-specific requirements. In the most general sense, all software should be capable of functioning in both Dual-Stack and IPv6-only modes of operation.

Important considerations for IPv6-enabled software are:

- The software application can function the exact same way in an IPv6-only environment, and
- The software coding for all network interfaces is in compliance with numerous IEEE and IETF standards supporting IPv6 socket implementation.

9.6 Services / ISPs

Categories of services have been defined, to include:

- Software as a Service (SaaS): single-component, outsourced solutions,
- Platform as a Service (PaaS): externally hosted, managed server instance,
- Infrastructure as a Service (IaaS): externally hosted, managed environments, and
- Internet Service Provider (ISP): internet / commodity connectivity being provided.

9.7 Comparison with USGv6 and DoD

The US Government and DoD IPv6 specifications call out numerous device and product classes. The similarities and differences are not always apparent. The US IPv6 Profile and DoD Unified Capabilities Requirements product classes and their relationships are shown in Figure 21 below.

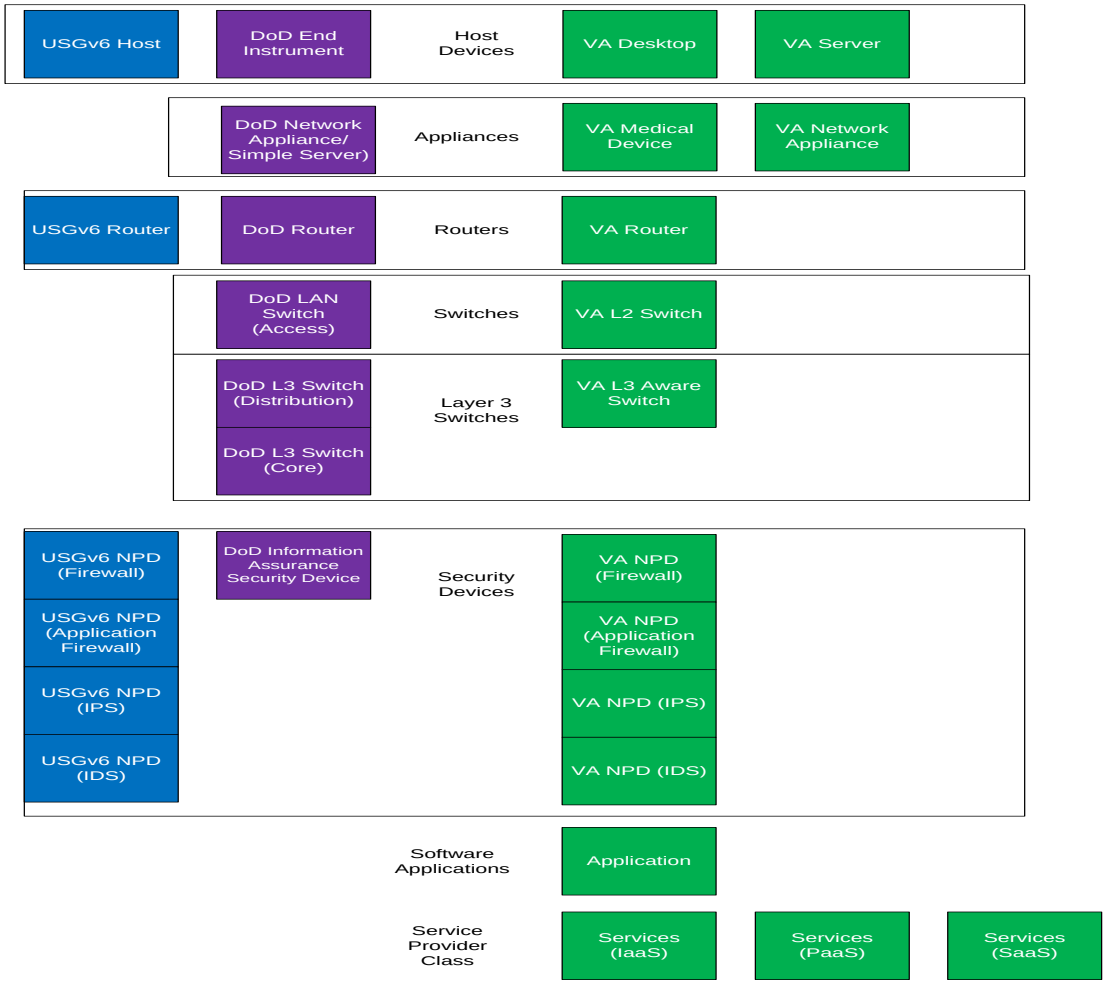


Figure 21: The US IPv6 Profile and DoD Unified Capabilities Requirements product classes

10 USGv6 Lab Accreditation Requirements

10.1 Benefits for VA becoming a USGv6 and ISO 17025 Accredited Lab

For any organization, it would beneficial for any accreditation of its testing processes and test management. Given the current nature of official testing and accreditation at the VA, gaining accreditation would have substantial cascading benefits.

Some of these are:

- Quality Management – This has cascading benefits throughout the organization not limited to the test lab. Gaining ISO 9001 or 17025 accreditation gives an organization a

clear understanding of quality control, audit management, organizational understanding, and more willingness to be transparent on test results. In turn, the VA as a whole can benefit with these well-defined and well-tested management functions. For example, an agency may adopt a pilot for an ITIL (Information Technology Infrastructure Library) to help improve its help-desk processes and functions. This pilot usually expands to include change and configuration control and incidence response. Later, the entire organization has adopted ITIL as an overall practice. The same can be said for ISO accreditations.

- Test process and rigger – Having an accredited test lab will improve the efficiency and understanding of test results. Test engineers will clearly understand their roles and test mechanisms. Doing so will make the VA IT test processes accepted within the entire agency.
- Full IPv6 testing result understanding – It is common in any test organization that not every result makes it for public consumption. It is easy to tell this by looking at the case of the University of New Hampshire – Interoperability Lab (UNH-IOL's) USGv6 Tested Products List. The list features products undergoing the IPv6 test specifications. While most will pass, others have in the notes section of the Suppliers Declaration of Conformance (SDoC) notations that aren't always clear. If the VA were to be an accredited lab requiring vendors to undergo 2nd Party Lab testing at their accredited lab, a full understanding of the "pass with exceptions" can be fully understood and documented internally to VA.
- A Ready-Made IPv6 Training Facility – By having a USGv6 accredited lab, a fully functioning IPv6 test facility must be in place. Therefore, this gives the VA a place to provide VA-internal, hands-on training without having to outsource to third-party training providers.

10.2 ISO 17025 Accreditation Requirements

The International Organization for Standardization (ISO) developed a process for accrediting test and calibration laboratories. This accreditation process has numerous requirements as shown in Figure 22. There are numerous similarities with the ISO 9001 accreditation. This is basically

because the ISO 9001 standard has everything to do with quality management systems. So a test lab looking to do ISO 17025 accreditation should really already have ISO 9001 accreditation. It is not a requirement, but very helpful. Below is a listing of what the ISO 17025 accreditation requires of each test lab. Requirements are also shown in Figure 22 below.

10.2.1 ISO 9001 Accreditation (Optional) or a Quality Management System (Required)

Although the ISO 9001 accreditation is optional, the test lab should at least demonstrate a repeatable, proven, and accurate quality management system. The quality management system must maintain the following:

- Quality Control Manual;
- Control of documents – the documentation authoring and reviewing workflow must be articulated in a repeatable process;
- Control of Records - showing that all records are organized, legible, and readily identifiable; and
- Measurement, analysis, and improvement – showing the auditing, measurements/testing and improvement processes.

10.2.2 ISO 17025 Test Lab Processes Required for Accreditation

Given the comprehensive nature of ISO 9001, the ISO 17025 test lab requirements include how testing, sampling, and records are maintained. In Figure 22 below, the main requirements are:

- Organization,
- Testing,
- Test Processes,
- Sampling,
- Sample Handing, and
- Records Maintenance.

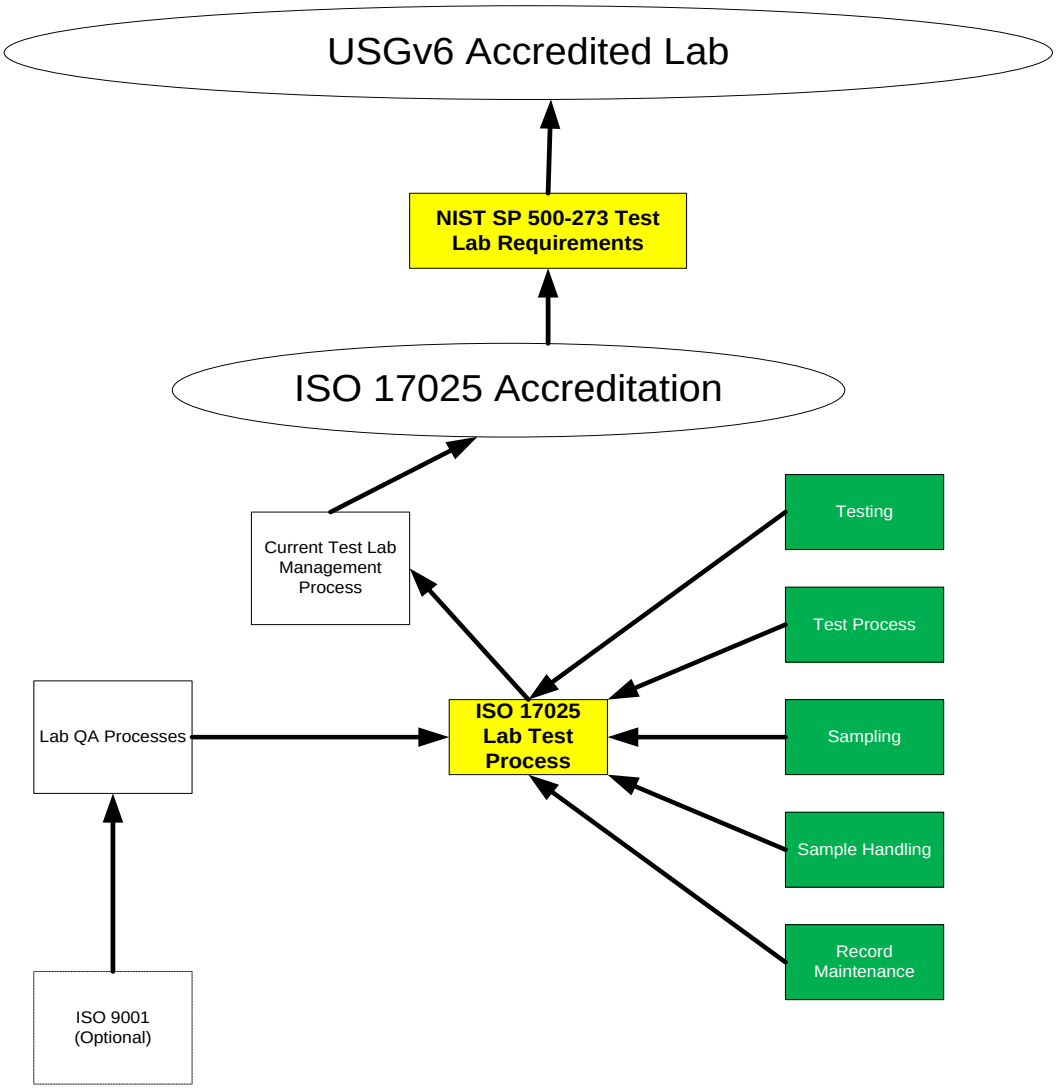


Figure 22: Lab Management and ISO 17025 Lab Accreditation Requirements

10.2.2.1 Organization Requirements

The test lab must have a documented organization that is well understood within the lab. This includes that personnel know their job descriptions. It also includes technical responsibilities like who is responsible for calibration of test tools and who is responsible for the conduct of testing.

10.2.2.2 Testing Requirements

The test lab must have a documented process for testing. According to USGv6, the test lab must have the most current test specifications available. All tests must be documented and recorded using the lab's test process. If there are added test cases outside of the standard USGv6 that are specific to VA, like performance and security-related tests, the test procedures must be located in the lab as well. Training of the test execution must also be part of this requirement. Each tester must have a professional understanding of how to test in the USGv6 process.

10.2.2.3 Test Process Requirements

The test lab must have a documented understanding of the test process. Once a product is in-process, what happens next? What are the steps from pre-documentation, to test execution, to re-testing on non-conforming items, validating test results, and finally test reporting and documentation? The test reporting should following the quality management system in the documentation processes.

10.2.2.4 Sampling Requirements

With all highly visible test programs (Common Criteria, FIPS 140-2 and USGv6) there are sampling of tests for collaborative reviews that must take place.

10.2.2.5 Sample Handling Process Requirements

The USGv6 sampling is done in a virtual basis on the USGv6 Test Program website here: http://www.antd.nist.gov/usgv6/interlab.html under the Inter-Lab Comparisons. SP 500-273 also mandates this process. Once the test lab reaches ISO 17025 accreditation, a separate and more specific verification takes place by the list of accredited USGv6 Accreditation Bodies (AB). The test lab must be able to demonstrate the sampling process outside the USGv6 process as well. The internal lab process must feed into the overall USGv6 test program process.

10.2.2.6 Records Maintenance Requirements

If the test lab is following the ISO 9001 process or a process similar in nature, then the requirements are identical. The lab must have a physical location for all the records and documentation processes identified above.

11 VA IPv6 Test Lab Requirements Summary

The test environment shall consist of hosts, servers, and networks that are able to emulate the VA Local Area Networks and Wide Area Networks, including interfaces to service providers. Ideally, completely discrete instances of these will exist for each of the separate test categories; (Baseline (IPv4-only), Dual-Stack (IPv4 and IPv6) and IPv6-only) as this enables simultaneous testing of different solutions within different testing categories (as well as providing a certain level of redundancy). However, for financial and physical footprint reasons, it may be more feasible to have a single test environment with pre-planned configurations to change the test category being utilized at any point in time.

The environment is comprised of network communication interfaces, network hardware, operating system software, and application software that are configured to provide assessment capabilities including native IPv6 capabilities, IPv4 over IPv6 tunneled capabilities, IPv6 over IPv4 tunneled capabilities, and dual stack IPv4/IPv6 capabilities. Traffic and threat generators are used in-line with actual clients and servers to provide a test environment as operationally realistic as possible for testing the network and Information Assurance devices.

Products to be tested will be provided either by the CIO's office (or subcomponents thereof) or by the individual VA organizations/regional offices. Each will have the responsibility to provide resources, additional test equipment as needed, and any additional requirements against which to test. Collaboration, therefore, is required to make efficient use of resources. The VA IPv6 Program Management Transition Office (PMTO) will coordinate these efforts.

It is envisioned that, at least at first, the VA Testing Effort will be focused on the supplemental extensions to the USGv6 profiles/VA-specific testing concerns. This effort can, therefore, rely

upon USGv6 test results for a wide variety of characteristics and then solely focus on the VA's additional requirements.

In the simplest sense, the test lab should fulfill three sets of requirements:

1. Have a suitable facility / environment to perform the required testing; specifically regarding HVAC, AC and DC power, rack space and network connectivity (LAN/WAN);
2. Have representative samples of the components widely used within the VA network; specifically regarding routers, switches, VPN implementations, IDS/IPS solutions, Network Management and Monitoring Solutions, host and server platforms, services/solutions; and
3. Have suitable test equipment to verify that VA Mission-specific requirements are met, and verify that suitable Performance levels and IA/Security capabilities (defined herein, or later identified) are met. If full USGv6 lab accreditation is pursued, additional requirements will be defined at that time.

The various test scenarios will require modified lab topologies, hypothetically identified as:

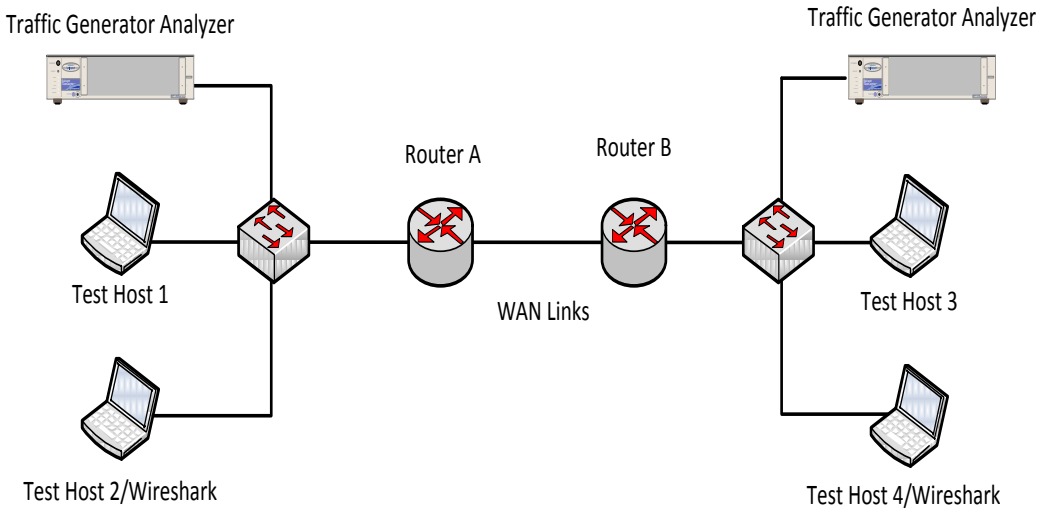


Figure 23: ICMPv6, MTU, SLAAC, Unicast Packet, Scoped Addr, Addr Sel, IPsec

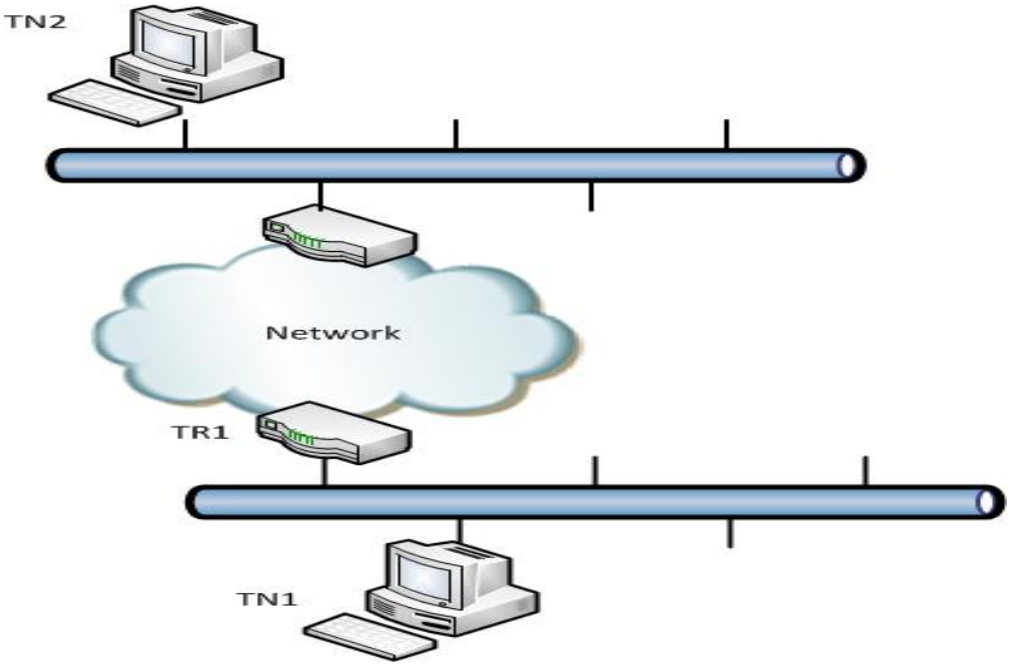


Figure 24: RH0, Rtr Alert

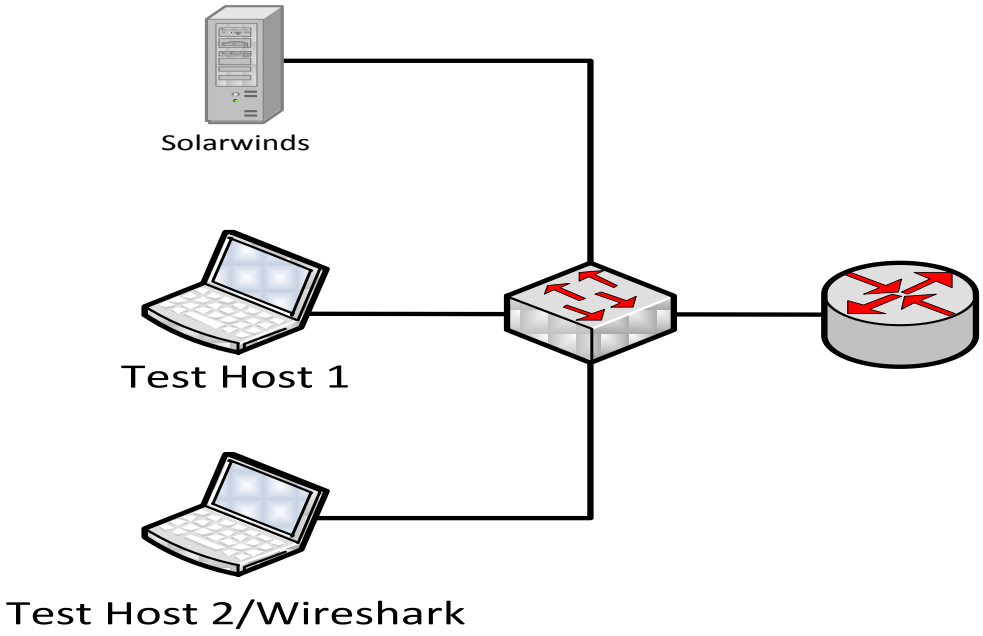


Figure 25: SNMPv3

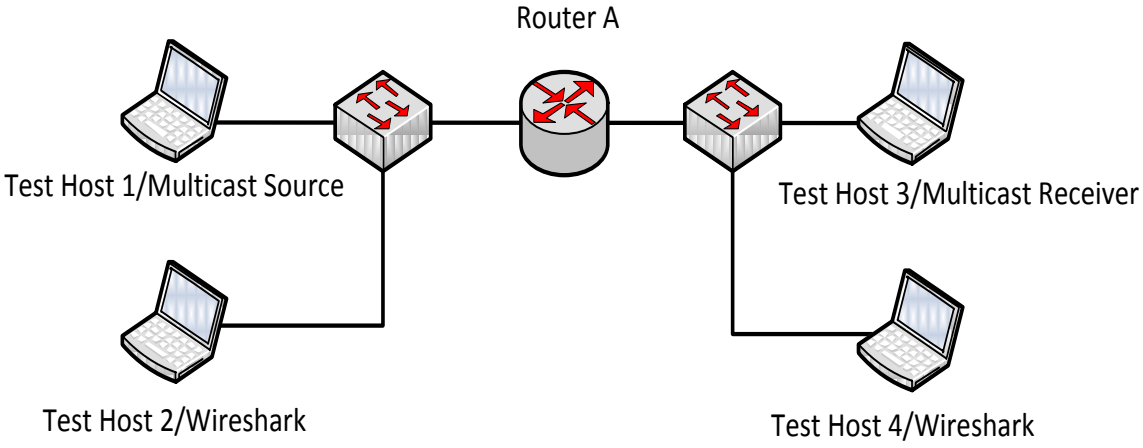


Figure 26: MLD, Multicast

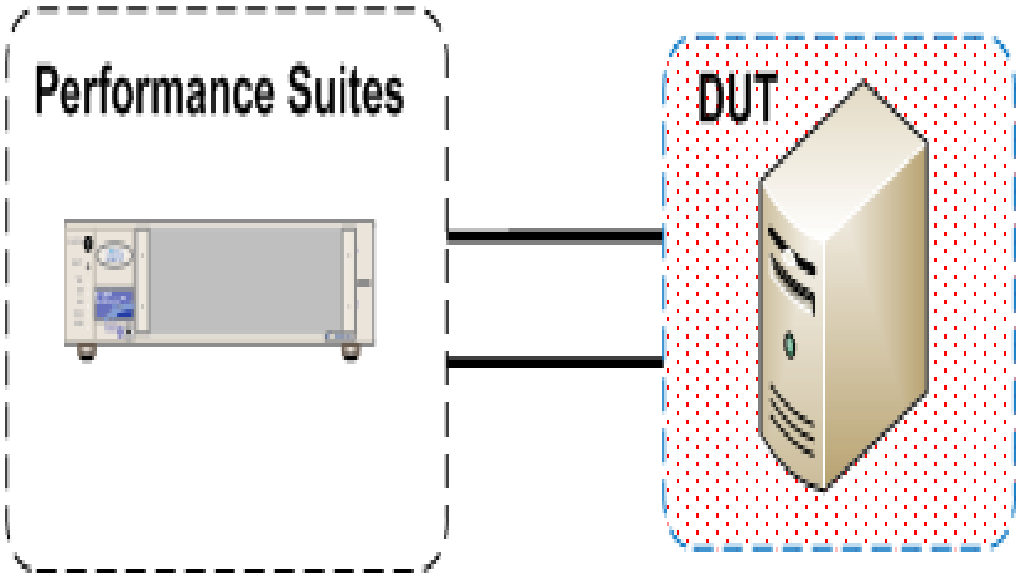


Figure 27: Layer 4-7 Server Benchmark

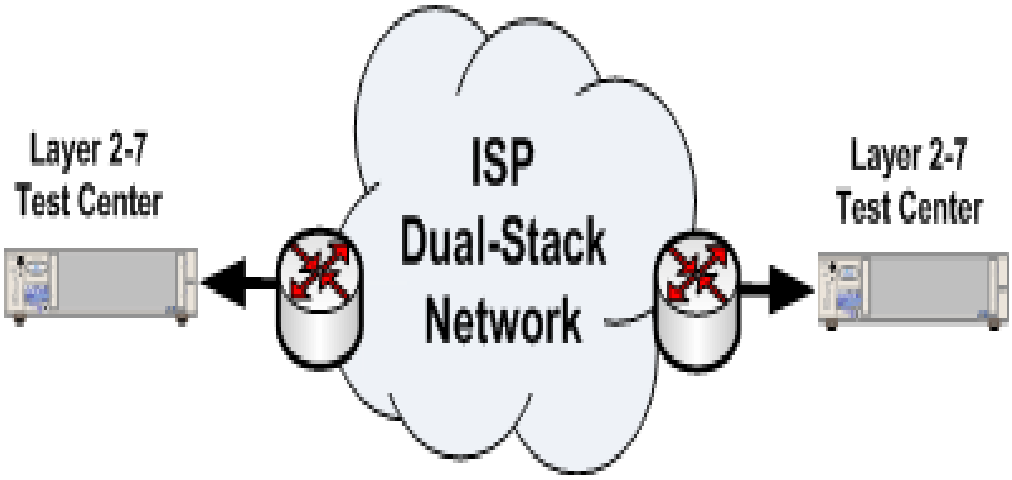


Figure 28: ISP Testing

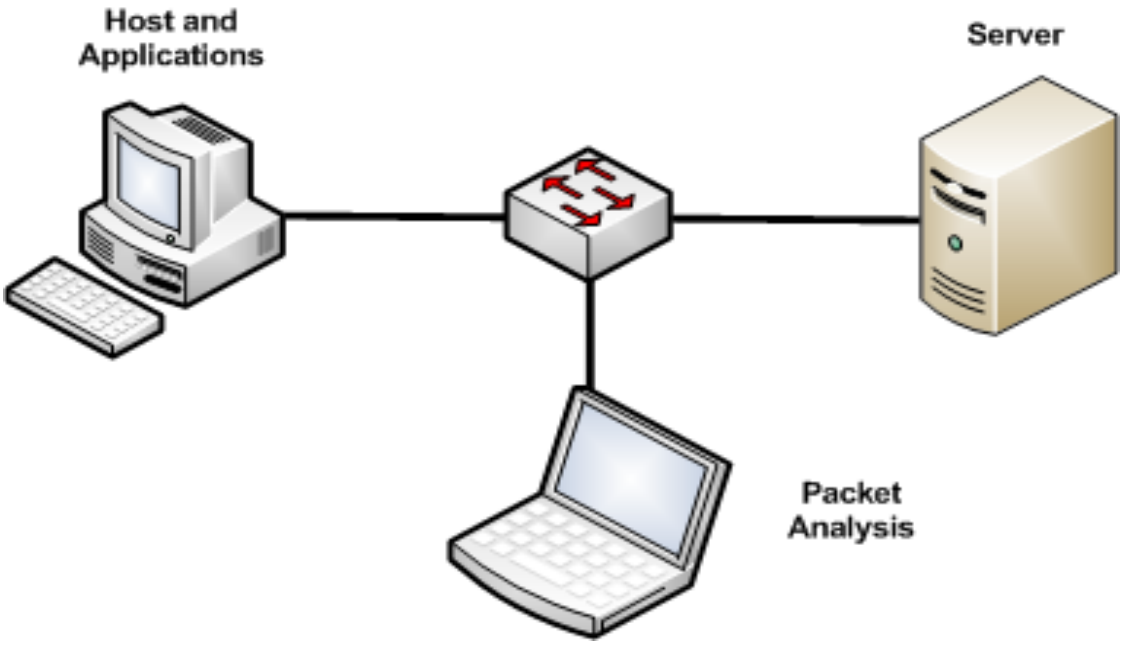


Figure 29: Host Validation Configuration

Each of those hypothetical architectures would need to be replicated (or able to be recreated as needed) for each of the test scenarios (IPv4-only, Dual-Stack, IPv6-only).

If it is decided that the VA Testing Effort shall be capable of fulfilling the entirety of the USGv6 testing requirements, a significant amount of resources and effort will be required. If this path is chosen/pursued, in addition to the time and resources necessary, it is recommended that the VA Testing Facility become accredited by NIST, coordinating with either usgv6-project@nist.gov or night@nist.gov – at which point the lab would not require external testing of products in order to comply with USGv6 requirements. In fact, suppliers and other federal agencies could come to the VA test lab to attain compliance.

12 Next Steps

12.1 Defining VA Specific Goals

Use of this document will serve as the foundation for a VA IPv6 Compliant Test Design Document which will provide recommended methods for testing systems, equipment, applications, and devices for IPv6 compliance. Working in conjunction with CIO and its affiliated partners, specific goals can be achieved for the Core mission communities and the infrastructure as a whole.

12.2 Methodology

The requirements and specifications defined here will have a direct use in defining test methods, procedures, and tools and in making the VA IPv6 test environment operational. In many cases it can support the development of vendor compliance testing for hardware, software, appliances, and devices and can be used in VA test labs to perform specific or integrated tests on individual system elements or integrated systems. Obviously all partners will need to share in the requirements and asset building for a proper scope of what should be tested and how that plan will be executed and rolled out across the enterprise.

12.3 Execution

Once the proper partnerships have acquired the necessary documents, a Network wide plan will need to be developed using various test labs in local regions and under CIO guidance and OMB mandates. The immediate test guidance should follow Routing set up to deal with DNSv6 and DHCPv6. The backbone portion should be isolated from the Internet/Internet2 connectivity and

Basic Network Services (DC, DNS, DHCP). If anything further is required, we need to couple with the WAN Lab in Martinsburg WV. Other Network Services currently include two tunnel servers from Hexago and NAT64 from Datatek. User applications include only web and email services at this time.

Each test lab must still produce test results in compliance with the current test specifications outlined in the USGv6 Test Methods website. This test specification outlines each of the conformance, interoperability, and functional network protection device (NPD)/security tests that must be performed with whatever section of the U.S. Government IPv6 Profile section they correspond.

12.4 Evaluation

The U.S. Government test program is derived from the National Institute for Standards in Technology (NIST) Special Publication 500-273. In SP 500-273, the U.S. Government IPv6 test program is guided by (5) fundamental objectives:

1. Quality Components – Meaning that each test laboratory has a rigorous and validated accreditation per international specifications like the ISO 17025.
2. Traceability of Tests – Each test case has a basis in the current and recognized IPv6 international standards bodies.
3. There is a feedback mechanism. This mechanism is the U.S. Government IPv6 Testing Working Group.
4. There is test method validation – Meaning that the test cases, test procedures and testing tools are open, transparent, and repeatable.
5. Proficiency in testing and laboratory comparisons – All labs must demonstrate proficiency in IPv6 testing.

12.5 Reporting

Testing will require many phases from which multiple reports from various tools for IPv6 acceptance will be derived. Using VA mission statements and all VA stake holders, it will be

necessary to bring this reporting to a single focal point for review and examination by all VA IT business units. Once this is vetted, an outlying plan can be developed using conformity to start the deployment of IP6 across the VA organization.

13 References

OSI/IEEE X73:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54328

Suppliers Declaration of Conformity (SDoC): http://w3.antd.nist.gov/usgv6/sdoc.html

Unified Capabilities Requirements: http://w3.antd.nist.gov/usgv6/sdoc.html

NIST SP 500-273: http://w3.antd.nist.gov/usgv6/NIST-SP-500-273.v1.final.pdf

ISO 9001: http://www.iso.org/iso/iso_9001_2008

ISO 17025: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883

DoD UCR 2008, Change 3: http://jitc.fhu.disa.mil/jitc_dri/jitc.html

USG IPv6 Profile: http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

USGv6 Testing website: http://www.antd.nist.gov/usgv6/

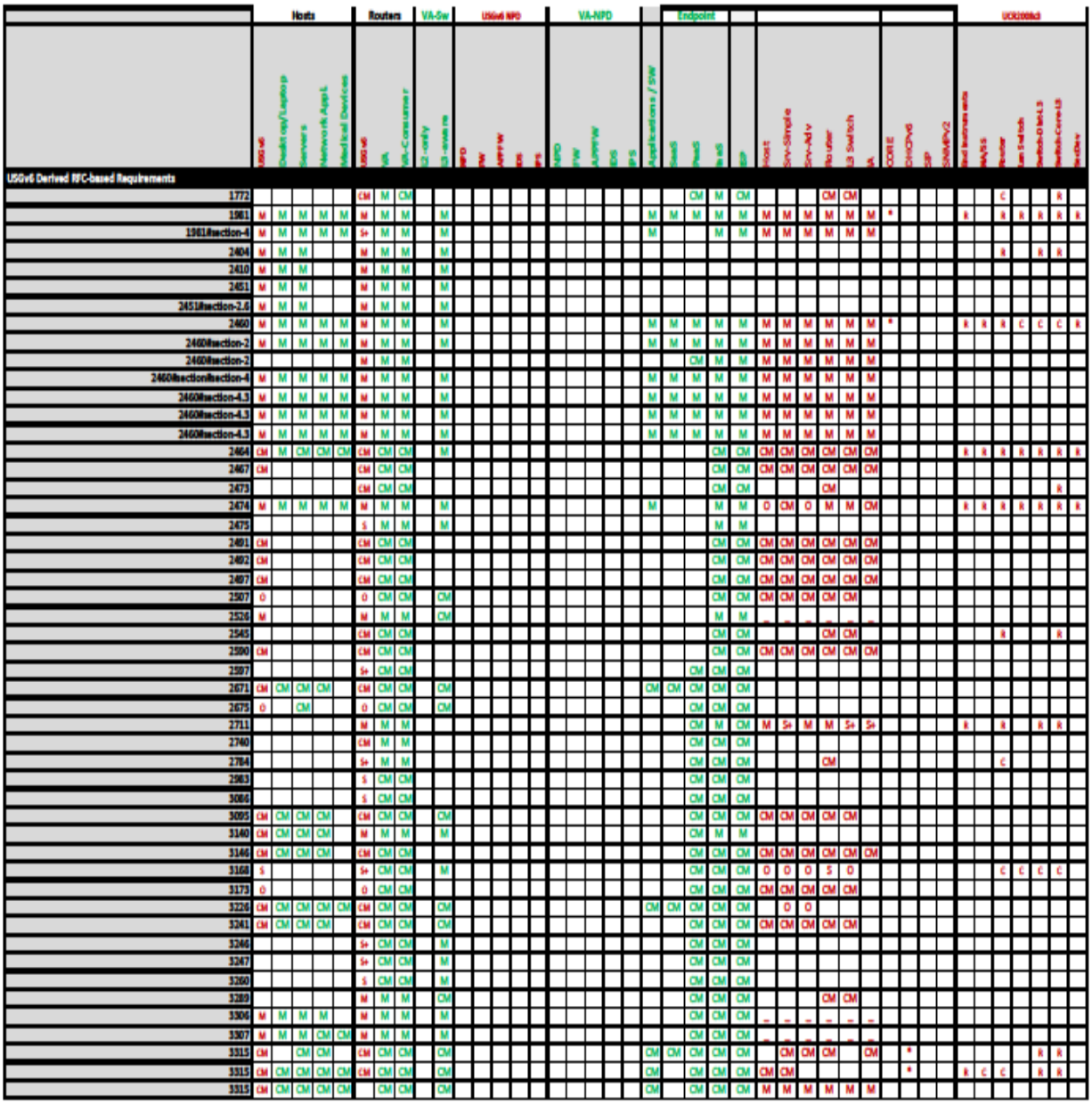
FDA Regulations of Medical Devices:
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/default.htm

14 Appendix 1 – Sample VA IPv6 Host Profile

Sample VA IPv6 Host Profile

1981	M	PathMTUD	Required		http://tools.ietf.org/html/rfc1981	2010/07
1981#section-4	M	PathMTUD:Discovery Protocol Reqs	*		http://tools.ietf.org/html/rfc1981#section-4	2010/07
2404	M	HMAC-SHA1-96	*		http://tools.ietf.org/html/rfc2404	2010/07
2410	M	NULL Encr	*		http://tools.ietf.org/html/rfc2410	2010/07
2451	M	ESP CBC mode Algs	*		http://tools.ietf.org/html/rfc2451	2010/07
2451#section-2.6	M	ESP CBC mode Algs:3DES-CBC	ESP		http://tools.ietf.org/html/rfc2451#section-2.6	2010/07
2460	M	IPv6	*		http://tools.ietf.org/html/rfc2460	2010/07
2460#section-2	M	IPv6 Packets: send, receive	*		http://tools.ietf.org/html/rfc2460#section-2	2010/07
2460#section#section-4	M	IPv6:Ext Hdr	*		http://tools.ietf.org/html/rfc2460#section#section-4	2010/07
2460#section-4.3	M	IPv6:Ext Hdr:HbH, Unrecognized	*		http://tools.ietf.org/html/rfc2460#section-4.3	2010/07
2460#section-4.3	M	IPv6:Ext Hdr:FragHdr	*		http://tools.ietf.org/html/rfc2460#section-4.3	2010/07
2460#section-4.3	M	IPv6:Ext Hdr:DestOpt	*		http://tools.ietf.org/html/rfc2460#section-4.3	2010/07
2464	M	IPv6 over Foo:Ethernet	LINK		http://tools.ietf.org/html/rfc2464	2010/07
2474	M	DiffServ	DS		http://tools.ietf.org/html/rfc2474	2010/07
3306	M	Mcast UniPrefix	*		http://tools.ietf.org/html/rfc3306	2010/07
3307	M	Mcast Alloc Guidelines	*		http://tools.ietf.org/html/rfc3307	2010/07
3484	M	DefAddrSel	*	Revision underway: 3484-bis	http://tools.ietf.org/html/rfc3484	2010/07
3596	M	DNSv6-Client	DNS-Client		http://tools.ietf.org/html/rfc3596	2010/07
3596#section-2.1	M	DNSv6-Client:AAAAs	DNS-Client		http://tools.ietf.org/html/rfc3596#section-2.1	2010/07
3596#section-2.5	M	DNSv6-Client:PTR (ipv6.arpa)	DNS-Client		http://tools.ietf.org/html/rfc3596#section-2.5	2010/07
3775#section-8.1	M	MIPv6:All nodes as CN	MIP		http://tools.ietf.org/html/rfc3775#section-8.1	2010/07
3810	M	Mcast MLDv2	*	Updates 2710!	http://tools.ietf.org/html/rfc3810	2010/07
3879	M	Deprec SLAs	*		http://tools.ietf.org/html/rfc3879	2010/07
4007	M	Scoped Addr Arch	*		http://tools.ietf.org/html/rfc4007	2010/07
4007	M	Scoped Addr Arch - manual configuration?	*		http://tools.ietf.org/html/rfc4007	2010/07
4193	M	ULAs	*		http://tools.ietf.org/html/rfc4193	2010/07
4213#section-2	M	Transition Mechanisms:Dual Stack	IPv4		http://tools.ietf.org/html/rfc4213#section-2	2010/07
4291	M	AddrArch	*		http://tools.ietf.org/html/rfc4291	2010/07
4301	M	Security Arch	*		http://tools.ietf.org/html/rfc4301	2010/07
4301#section-4.1	M	IGW or IPv4:Security Arch:Transport Mode SAs	IGW,IPv4		http://tools.ietf.org/html/rfc4301#section-4.1	2010/07
4301#section-4.5.1	M	Security Arch:Manual SA/Keying	*		http://tools.ietf.org/html/rfc4301#section-4.5.1	2010/07
4301#section-4.5.2	M	Security Arch:Auto SA/Keying	*		http://tools.ietf.org/html/rfc4301#section-4.5.2	2010/07
4303	M	ESP	IPsec-v3		http://tools.ietf.org/html/rfc4303	2010/07
4306	M	IKEv2			http://tools.ietf.org/html/rfc4306	2010/07
4306#section-3.3.3	M	IKEv2:ESN	IKEv2		http://tools.ietf.org/html/rfc4306#section-3.3.3	2010/07
4306#section-4	M	IKEv2:PSK	IKEv2		http://tools.ietf.org/html/rfc4306#section-4	2010/07
4306#section-4	M	IKEv2:RSA	IKEv2		http://tools.ietf.org/html/rfc4306#section-4	2010/07
4307	M	IKEv2:CryptoAlgs	IKEv2		http://tools.ietf.org/html/rfc4307	2010/07
4307#section-3.1.1	M	IKEv2:CryptoAlgs:3DES-CBC	IKEv2		http://tools.ietf.org/html/rfc4307#section-3.1.1	2010/07
4307#section-3.1.1	M	IKEv2:CryptoAlgs:AES-CBC w/ 128b keys	IKEv2		http://tools.ietf.org/html/rfc4307#section-3.1.1	2010/07
4307#section-3.1.1	M	IKEv2:CryptoAlgs:HMAC-SHA-1	IKEv2		http://tools.ietf.org/html/rfc4307#section-3.1.1	2010/07
4307#section-3.1.4	M	IKEv2:CryptoAlgs:HMAC-SHA1 as a PRF	IKEv2		http://tools.ietf.org/html/rfc4307#section-3.1.4	2010/07
4443	M	ICMPv6	*		http://tools.ietf.org/html/rfc4443	2010/07
4604	M	Mcast MLDv2 SSM	SSM		http://tools.ietf.org/html/rfc4604	2010/07
4835	M	CryptoAlgs	IPsec-v3		http://tools.ietf.org/html/rfc4835	2010/07
4835#section-3.1.1	M	CryptoAlgs:3DES-CBC Encr	ESP		http://tools.ietf.org/html/rfc4835#section-3.1.1	2010/07

15 Appendix 2 – VA IPv6 Profile Matrix – Profile Classes



16 Appendix 3 – VA IPv6 Profile matrix – RCF Descriptions

	RFC Desc:	USGv6 Content:	Misc. & USGv6 Comments:	URL / reference:	USGv6 Date added:
USGv6 Derived RFC-based Requirements					
1772	BGP - Internet	BGP,MP			2010/07
1981	PathMTUD	Required			2010/07
1981#section-4	PathMTUD:Discovery Protocol Reqs	*			2010/07
2404	HMAC-SHA1-96	*			2010/07
2410	NULL Encr	*			2010/07
2451	ESP CBC mode Algs	*			2010/07
2451#section-2.2	ESP CBC mode Algs:3DES-CBC	MP			2010/07
2460	IPv6	*			2010/07
2460#section-3	IPv6 Packets: send, receive	*			2010/07
2460#section-3	IPv6 packet forwarding	*			2010/07
2460#section#section-4	IPv6:Ext Hdr	*			2010/07
2460#section-4.3	IPv6:Ext Hdr:HbH, Unrecognized	*			2010/07
2460#section-4.3	IPv6:Ext Hdr:FragHdr	*			2010/07
2460#section-4.3	IPv6:Ext Hdr:DestOpt	*			2010/07
2464	IPv6 over Foo:Ethernet	LINK			2010/07
2467	IPv6 over Foo:FDDI	LINK			2010/07
2473	Generic Packet Tunneling	IPv6			2010/07
2474	DiffServ	DS			2010/07
2475	DiffServ Arch	DS			2010/07
2491	IPv6 over Foo:NBMA	LINK			2010/07
2492	IPv6 over Foo:ATM	LINK			2010/07
2497	IPv6 over Foo:AR Cnet	LINK			2010/07
2509	IP Hdr Comp	*			2010/07
2526	Subnet Anycast Addr	*	Unofficial exception for /127s?		2010/07
2545	BGP-MP for IPv6 IDR	BGP,MP			2010/07
2590	IPv6 over Foo:Frame Relay	LINK			2010/07
2597	DiffServ AF PHB	DS			2010/07
2671	DNSv6:EDNS0	DNS-Client			2010/07
2675	Jumbograms	*			2010/07
2711	RtrAlert	*			2010/07
2740	OSPFv3	IGP	Deprecated by 5340 now ... ?		2010/07
2784	GRE	IPv6			2010/07
2983	DiffServ + tunnels	DS			2010/07
3086	DiffServ PDB (Per Domain Behav)	DS			2010/07
3095	ROHC RTP, UDP, ESP and uncomp	ROHC			2010/07
3140	DiffServ PHBs	DS			2010/07
3146	IPv6 over Foo:Firewire (IEEE 1394)	LINK			2010/07
3168	IP + ECN	ECN			2010/07
3173	IP Payload Comp	*			2010/07
3226	DNSSEC & IPv6 Msg Size Reqs	DNS-Client			2010/07
3241	ROHC over PPP	ROHC,LINK			2010/07
3246	DiffServ EF PHB	DS			2010/07
3247	DiffServ EF PHB Supplemental	DS			2010/07
3260	DiffServ Clarification / Terms	DS			2010/07
3289	DiffServ MIB	SNMP			2010/07
3306	Mcast UniPrefix	*			2010/07
3307	Mcast Alloc Guidelines	*			2010/07
3315	Stateful DHCPv6-Server	DHCP-Server			2010/07
3315	Stateful DHCPv6-Client	DHCP-Client			2010/07
3315	Stateful DHCPv6-Client - be able to disable it!	DHCP-Client			2010/07
3411	SNMPv3	SNMP			2010/07
3412	SNMP Message Process and Dispatch	SNMP			2010/07
3413	SNMP Apps	SNMP			2010/07
3413#section-1.3	SNMP Apps:Command Responder	SNMP			2010/07
3413#section-1.3	SNMP Apps:Notification Generator	SNMP			2010/07

17 Appendix 4 – Medical Devices Communications Specifications

Medical Device Communications Requirements Profile			
MD Description:			
Reference	Title	Requirement	Result
Medical Device Requirements			
IEEE 11073	Personal Health Device "Framework"	TBD	
Health Informatics: Point of Care (PoC) Device Communications			
11073-00101	Part 00101: Guide—Guidelines for the use of RF wireless technology		
11073-10101:2004(E)	Part 10101: Nomenclature		
11073-10201:2004(E)	Part 10201: Domain information model		
11073-20101:2004(E)	Part 20101: Application profile - Base standard		
11073-30200:2004	Part 30200: Transport profile - Cable connected		
11073-30300:2004(E)	Part 30300: Transport profile - infrared wireless		
Application Profile			
IEEE Std 11073-20601	Optimized Exchange Protocol		
IEEE Std 11073-20601a	Optimized Exchange Protocol (Amend)		
Device Specialization (Existing)			
IEEE Std 11073-10404	Pulse Oximeter		
IEEE Std 11073-10407	Blood Pressure Monitor		
IEEE Std 11073-10408	Thermometer		
IEEE Std 11073-10415	Weighing Scale		
IEEE Std 11073-10417	Glucose Meter		
IEEE Std 11073-10420	Body Composition Analyzer		
IEEE Std 11073-10421	Peak flow		
IEEE Std 11073-10441	Cardiovascular Fitness & Activity Monitor		
IEEE Std 11073-10442	Strength Fitness Equipment		
IEEE Std 11073-10471	Independent Living Activity Hub		
IEEE Std 11073-10472	Medication Monitor		
Device Specialization (In Revision)			
IEEE Std 11073-10404	Pulse Oximeter (Revision)		

IEEE Std 11073-10417	Glucose Meter (Revision)		☐
IEEE Std 11073-10441	Cardiovascular Fitness and Activity Monitor (Revision)		☐
Device Specialization (In Development)			
IEEE P11073-10406	Basic ECG (1 to 3-Lead)		☐
IEEE P11073-10413	Respiration Rate Monitor		☐
IEEE P11073-10418	INR (Blood Coagulation)		☐
IEEE P11073-10419	Insulin Pump		☐
			☐
wPAN Related RFCs (Active Internet Drafts)			
RFC 4919 (draft-ietf-6lowpan-problem)	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals		☐
RFC 4944 (draft-ietf-6lowpan-format)	Transmission of IPv6 Packets over IEEE 802.15.4 Networks		☐
RFC 6282 (draft-ietf-6lowpan-hc)	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks		☐
draft-ietf-6lowpan-btle-05	Transmission of IPv6 Packets over Bluetooth Low Energy		☐
draft-ietf-6lowpan-nd-18	Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN)		☐
draft-ietf-6lowpan-routing-requirements-10	Problem Statement and Requirements for 6LoWPAN Routing		☐
draft-ietf-6lowpan-usecases-10	Design and Application Spaces for 6LoWPANs		☐
draft-bormann-6lowpan-ghc-03	6LoWPAN Generic Compression of Headers		☐
draft-mariager-6lowpan-v6over-dect-ule-01	Transmission of IPv6 Packets over DECT Ultra Low Energy		☐
draft-sarikaya-6lowpan-cgand-02	Lightweight Secure Neighbor Discovery for Low-power and Lossy Networks		☐
			☐