Special Publication 500-281

National Institute of
Standards and Technology
U.S. Department of Commerce

USGv6 Testing Program User's Guide

National Institute of Standards and Technology

Stephen Nightingale and Doug Montgomery

SP500-281-V1.0 November 30, 2009

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 500-281

USGv6 Testing Program User's Guide – Version 1.0

National Institute of Standards and Technology

Stephen Nightingale and Doug Montgomery

Internet and Scalable Systems Metrology

Advanced Network Technologies Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

30 November 2009

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Patrick Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 500-series reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 500-281
Natl. Inst. Stand. Technol. Spec. Publ. 500-281, 20 pages (30 November 2009)

Acknowledgements

Important input to this document was provided by Erica Johnson and Tim Winters of the University of New Hampshire InterOperability Laboratory.

Table of Contents

Executive Summary

This document forms part of the USGv6 Testing Program. It is specifically directed at:

- IPv6 product developers aiming to implement the USGv6 profile [2] for hosts, routers and network protection devices.
- USG Agencies acquiring IT products that contain USGv6 capabilities.

USG Agencies are interested in an orderly transition to using IPv6 in their day-to-day operations. Faced with a mandate, they want to acquire products with the best chance of interoperability going forward, while limiting incompatibilities with their installed base. NIST has developed the USGv6 profile, and a testing program that requires products to be tested in accredited laboratories, to provide increased confidence in their plug-and-play interoperability. However, because of the sheer number of standards included in the profile, and the potential for change in the associated testing infrastructure, the complexity of USGv6 provision is tricky to negotiate. This document identifies the elements and the players in the USGv6 field, and the standards and tests that are subject to lifecycle changes.

USGv6 product developers are interested in clear statements of the requirements for tailoring their products for government purchase. This document offers guidance on what to implement, and what to claim in the Suppliers's Declaration of Conformity [4,5].

1 Introduction

This document has been prepared for use in conjunction with NIST SP 500-267 A Profile for IPv6 in the U.S. Government [2] and NIST SP 500-273 USGv6 Test Methods: General Description and Validation [3]. It can be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document is intended to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor ought it be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official.

1.1 USGv6 Testing Program

The USGv6 profile was published in July 2008 with the intention of seeking compliant products after a two year period to allow for product implementation and tailoring. The profile specifies selections from over 150 RFCs and other standards, to allow for development of hosts, routers and network protection devices.

NIST has established the USGv6 testing program as a way to determine USGv6 compliance. The test program makes use of a set of abstract test specifications, each validated against the respective protocol specification. USGv6 products must be tested against tools validated to these tests, in laboratories accredited to ISO 17025. Having implemented and tested their products, developers must make their claims of USGv6 compliance in a systematic and standardized way. The Supplier's Declaration of Conformity [4,5] is a tool that offers a flexible means of constructing these claims, for the USGv6 stack.

USGv6 contains a wide range of elements, and the testing program includes artifacts that are subject to bug discovery and revision. Hence it is necessary to have in place a scheme to manage all these elements, that includes collaboration with the stakeholders.

1.2 Purpose, Scope and Document Structure

This document provides a user's guide to the USGv6 testing program. It gives an overview of the elements of the program. It offers guidance to Agencies on what to look for in USGv6-compliant products, and to IPv6 product suppliers on how to make their products USGv6 compliant. Some consequences of putting together a technical recommendation that is a compendium of large numbers of different, informal standards include:

1) Tests derived from informal standards are themselves informal, and

2) Changes to several of the standards spread over time lead to complex interoperability issues and potential compatibility problems.

A corollary of (1) is that informally derived tests have the characteristic of software, that they need debugging over several iterations of use. Where tests are lacking in coverage, conformance bugs and interoperability difficulties in USGv6 products can go undetected. A systematic revision schedule for tests

progressively increases accuracy and optimizes coverage, to cumulatively increase confidence in product interoperability.

The document gives an analysis of the lifecycles of standards, tests and IPv6 devices, and establish schedules for systematic change in the selection and update of these items. It also explains the requirements for Supplier's Declaration of Conformity (SDOC), to describe what it is and what it is not. This is not completely straightforward, given that vendors may test an IPv6 stack in multiple laboratories, and package it within many different devices for sale. The scope of this document therefore covers the management and reporting requirements of the USGv6 testing program.

Following this introduction, Section 2 introduces the elements of the testing program, including artifacts, processes and stakeholders involved in the USGv6 testing program. The interaction between stakeholders and processes is fundamental to the operation of the testing program. The lifecycles of the artifacts, and their impacts on interoperability, are explored in Section 3, and management of the testing program is discussed in Section 4. Section 5 is devoted to the definition and operation of SDOC.

1.3 Audience

The audience for this document is encapsulated by the set of stakeholders, and these are introduced in Section 3.

2 USGv6 Testing Program Elements

The principle objects that the USGv6 program is concerned with are hosts, routers and network protection devices, but there is a variety of intermediate artifacts that go towards evaluating these devices. Each of these artifacts is governed by a process and is subject to change in managed stages. For each artifact and its process a subgroup of stakeholders have a direct interest. In this section the set of artifacts is identified in Section 2.1. The processes associated with particular artifacts are explained in Section 2.2, and the stakeholders interested in these artifacts and processes are introduced in Section 2.3.

2.1 Artifacts

The **USGv6 profile, NIST SP 500-267** is the document that selects and organizes the IPv6 networking standards for Federal Government use. Initially published in July 2008, it is subject to annual revision. The profile is a compendium of networking standards, mostly RFCs published by the IETF. IETF standards are produced on a draft through to final sequence and once published as RFCs they are not revised, but may be superseded by a higher numbered RFC, e.g. RFC 2461 Neighbor Discovery superseded by RFC 4861. The USGv6 profile brings change slowly, to allow the industry time to make their products ready. The profile cites only final standards. Future versions introduce new standards as SHOULD+ with upgrade to MUST after 12 months or more. When a new MUST appears in the profile it is not required to test in a device that claims its support until 24 months after its elevation to MUST. Standards being deprecated will be indicated as SHOULD- for at least 12 months before being removed from the profile.

The **Supplier's Declaration of Conformity** (SDOC) is based on ISO/IEC 17050. SDOC stands as representative of the device supplier's claims of compliance for a host, router of network protection device. It contains a summarization of the functional categories supported with respect to the profile, and their tested status. Changes to SDOC arise from retesting and repackaging devices. Buyers should satisfy themselves that a device supported by SDOC does actually interoperate with their installed IPv6 network configuration.

Moving in to the testing infrastructure, **Abstract Test Specifications** are needed for conformance and for interoperability. These are based on individual RFCs, and individual tests are created with purposes specific to functions in the RFC. Test purposes differ for conformance and interoperability. Conformance tests are usually run against independent testing devices, and the object is to make sure that the device under test exhibits the specified behavior for each function tested. Interoperability tests are run in a configuration with two or more devices under test, and the object is to make sure that every device pair interoperates – in the case where they implement complementary and compatible protocols. The test specifications in use for both conformance and interoperability are largely the product of the IPv6 Ready Logo program. They have been under development over many revisions for several years. Test development is a discipline akin to software development so bugs can be written in and take time to discover and remove. Test specifications therefore improve over time, and with use. Memoranda of Understanding have been signed beween NIST and the developers of these test specifications to allow the USGv6 testing program to make free use of them. But since these tests were developed to meet the IPv6 Ready Logo profile, they differ somewhat from the requirements of the USGv6 profile. For this reason NIST has developed a set of **Test Selection Tables**, accessible from the USGv6 testing website [6], to select from the Ready Logo specifications' tests applicable to the USGv6 profile. In regard to their accuracy and reliability, since these tables simply make a selection of tests, their complexity is not great, and they should converge on the correct values after a very few iterations. Test specifications are also needed for network protection. The functional specifications are embodied within the profile, and tests

have been provided by ICSA Labs. These tests are new, and it is reasonable to expect some iterations of test and revise until their reliability is established. Following the initial period of review, all tests are frozen as of November 2009. This initial revision level is used for testing and declaration in SDOC.

2.2 Processes

Processes associated with USGv6 compliance include testing processes and management processes. These processes regulate the development of the artifacts, given above. They are discussed here as testing processes in Section 2.2.1, management processes in 2.2.2 and other processes in section 2.2.3.

2.2.1 Testing Processes

All testing is conducted using published test specifications, distinct and different for conformance, interoperability and network protection. All tests are derived from the published standards, in a process akin to software development. Testing finds bugs in devices under tests, but also finds bugs in the tests themselves. The tests must be shaken out thoroughly and converged on single interpretations for each test purpose.

Conformance Testing is conducted between the device under test and a special purpose test system. The test system executes tests that implement the purposes and procedures of the abstract test specifications listed at the project website. Abstract tests are periodically corrected and updated , so executable tests and test systems must also be fixed to maintain equivalence. Clearly there is a process of validation (see below) that reconciles abstract and executable test specifications. The standard taxonomy for conformance testing architectures describes combinations of protocol layer, and levels of control and coordination, and is given in ISO 9646 [7].

Interoperability Testing is conducted among several host or router devices under test, according to abstract tests that include a detailed configuration section, and procedures to be conducted manually. These tests, too, are periodically corrected and updated. There are however no 'executable' systems, and so no need for abstract to executable mapping, and no executable validation issue. The issue of equivalence is focused on how different test laboratories conduct the interoperability tests.

Network Protection Testing is conducted in conjunction with internal and public networks, according to published abstract test specifications. These tests are updated every six months, to eliminate bugs and also to account for newly arisen attack vectors. The issue of equivalence is focused on how different network protection testing laboratories conduct the tests.

2.2.2 Management Processes

The artifacts described earlier are used in the testing process described above. There is a set of management processes associated with these artifacts and the testing processes. These management processes are described here.

Abstract Test Development Abstract tests are used as the basis for testing compliance with the RFCs pertaining to IPv6. These are procedural descriptions each having a test purpose applicable to exercising

some functions of one or more RFCs. As a matter of record, most of the initial tests have been developed under the auspices of the IPv6Ready Logo. Some tests have been privately developed, e.g network protection tests by ICSA Labs, some by open source organizations such as Tahi, some by test labs such as UNH InterOperability Laboratory, some by collaboration with other organizations such as OSPFv3 by Taiwan Telecommunications Laboratories and some through USG funding. Tests once developed are released to the community of labs for a review period, corrected, agreed, and published with a revision number.

USGv6 Test Selection Abstract test specification documents refer to the broad range of functions in an RFC. Not all these functions are required for USGv6 compliance. Test selection tables are developed by the USGv6 program, to identify a base test specification and list the abstract tests that comprise the USGv6 compliant set, while also listing for clarity the set of tests not applicable to USGv6.

Laboratory Accreditation Each test laboratory that wants its results recognized for USG acquisition must seek accreditation to ISO/IEC 17025, through an ILAC recognized accreditation body.

Test Method Validation The abstract test specifications are written procedures. For conformance testing these need to be translated to executable form. The resulting test methods have to be equivalent to the abstracts. The assessment of this activity is part of the on-site assessment leading to accreditation for ISO/IEC 17025. Additionally, it is necessary to ensure that all test methods in use for each protocol generate identical results. This activity is ensured through the program of interlaboratory comparisons.

Interlaboratory Comparisons These ensure that test methods for the same protocol functionality across all different laboratories generate identical results. NIST will designate a single organization to perform interlaboratory comparisons, and distribute results to test laboratories and accreditors as appropriate. This avoids the problem of multiple accreditors having different schemes that may not harmonize.

Revision Management From the outset we anticipate changes to RFCs, profile versions and tests, all leading to the need for IPv6 device changes. For example the USGv6 profile is subject to annual revision. Though these changes are expected to be highly conservative, new functionalities will be introduced as SHOULD+ and remain there for 12 months or more, before being moved to MUST. Some functions may be phased out, signaled by change from MUST to SHOULD- and eliminated from the profile after a further 12 months.

Test specifications are also subject to change, based on bug fixing and adding missing test coverage. These changes occur no more frequently than every 6 months. Specific cases for change are detailed later in Section 3, Lifecycles.

2.2.3 Other Processes

SDOC Production. After testing devices in an accredited laboratory, product vendors develop a Suppliers Declaration of Conformity in compliance with ISO/IEC 17050:2004 [4,5] serving as indication to purchasers that required testing has taken place. Whether a test laboratory wants to offer the service of SDOC creation after testing is a matter between the lab and its customer. SDOC production is fully discussed in Section 5.

2.3 Stakeholders

The producers and consumers of the artifacts and processes constitute the stakeholders in the USGv6 testing system. These are identified here.

USG Agencies have a primary interest in making sure that IT products with IPv6 capabilities are available to meet their acquisition requirements.

Testing Laboratories are central to the USGv6 testing process. Each such laboratory seeks accreditation from an ISO 17011 compliant, ILAC signatory, accreditation body. Test laboratories may conduct any of conformance, interoperability or network protection testing. 1st, 2nd and 3rd party labs are recognized: a 1st party lab is associated with the product developer. A 2nd party lab is associated with a USG agency. a 3rd party lab is independent.

Test Method Developers including open source suppliers such as Tahi[1] and private sector developers, who develop IPv6 test methods for conformance and interoperability, based on the abstract test specifications. In conjunction with test laboratories, test method developers take part in interlaboratory comparisons to make sure that test results for the same test using different methods in different labs are equivalent.

Accreditors - The role of an accreditor is to assess test laboratories for their compliance with ISO/IEC 17025 [8]. These are the quality provisions for testing. All assessors develop programs that build in technical test methods and assess technical competence. In the case of USGv6 the technical requirements are based on NIST SP 500-273 [3].

IPv6 Device Developers develop hosts, routers and network protection devices which, when offered for sale to the US government, shall be tested according to the criteria described here and in NIST SP 500-273.

NIST and the USG test program - NIST is a technology agency of the US government charged with creating a standard for IPv6 devices, and a means of determining compliance to that standard. NIST SP 500-267 is that standard. NIST SP 500-273 and this testing program are the means of establishing compliance.

[1] Tahi: www.tahi.org.

3 USGv6 Element Lifecycles

USG Agencies procuring IPv6 products are advised to consider first those with up to date test results. The consideration of what constitutes 'up-to-date' is a little complex as it involves annual profile updates with 24 month delayed effective dates, 6 monthly changes to test specifications and late availaibility test specifications. The following table itemizes the changes to artifacts that can impact interoperability in the Agency's installed base. Acquisitions based on USGv6 profile version 1.0 will establish that installed base, so subsequent versions should be incremental, not revolutionary, and highly conservative.

Changes to test specifications may have an effect on interoperability to the extent that functions previously not tested, or insufficiently tested, are in unknown status with respect to their conformance or interoperability. The subsequent test change can highlight latent conformance or interoperability problems already in the installed base. Buyers must separately ensure that their device suppliers are prepared to work with the complete community of vendors to correctly ensure conformance and interoperability. As the USGv6 profile is a procurement profile, it cannot *require* post-acquisition testing. However in Section 5 of the document, the conditions for declaring SDOC do describe conditions for the validity of a supplier's declaration.

The USGv6 profile includes upwards of 150 RFCs and other standards. Full coverage entails tests for each, but due to the complexity of the problem, test specification development lags protocol specification and implementation development considerably. The situation is that there is a core of protocols for which tests are mature, a further range for which they are under active development, and yet more protocols for which test development has not yet started. This situation is reflected in the testing and reportage requirements as verified by the SDOC provisions in Section 5. The table below takes account of the variations in test maturity: where mature tests exist, they are required to be passed if claimed in SDOC; where tests are undergoing periodic major revisions, suppliers are required to test against the new tests and improved tests by 6 months after the revision; where only minor test revisions are published, suppliers with products already tested are not obliged to retest.

Item	Conditions and Events	Impact on Vendor	Impact on USG Agencies
1	**Event**: USGv6 Profile version 1.0 (July 2008)	Signal to IPv6 suppliers to implement MUST capabilities.	Plan for IPv6 compliant product acquisition, with a 2 year time horizon.
-	**Condition**: Conditional MUST functions (C(M)) in the profile.	Implemented by suppliers who elect to support C(M) capabilities (See the Node Requirements Table in the profile).	-
-	**Condition**: SHOULD and SHOULD+ functions in the profile.	Not required for USGv6 compliance, but implemented by vendor choice. Some Agencies may seek these functions.	-

2	E**vent**: Profile version up (e.g. Version 2.0 and later).	Signal to vendors to start planning for new SHOULD+s, and start implementing new MUSTs.	IPv6 plans can include the new capabilities.
3	**Event**: Jan 2010 – July 2010	Accredited test laboratories open for business. Product vendors can test their USGv6 stacks.	Agencies can work with vendors to tailor products to specific functional needs, or wait till July for COTS products.
4	**Event**: July 2010	Vendors issue SDOC with claims of supported and tested capabilities, citing test results in accredited labs.	Buyers may use the profile to express requirements for USGv6 capabilities. These include standard configurations, or Agency specific capabilities.
5	**Condition**: Post July 2010 test provision as below.	----------	----------
6	**Condition**: No test selections exists for USGv6-v1-Capable requirements	Claims of support can be made in SDOC, only subject to local testing outside the scope of this program.	Test results for these capabilities are **not** traceable through the accreditation structure of this program. Agencies may specify their own verification requirements.
7	**Condition**: Test selections exists for specific capabilities within the profile.	SDOC claims MUST be supported by results from accredited test laboratories.	Test results for these capabilities **are** traceable through the accreditation structure of this program. Agencies may verify by contacting the accredited test laboratory.
8	**Event**: New test selections become effective or new major version number of test specification is published.	Products claiming the related functions in SDOC must test by 6 months after publication.	USG agencies may seek IPv6 products with SDOC that specifies compliance to the profile based on the new tests, by 6 months after their publication date.
10	**Event**: New minor version number change of test specification	No requirement for retest of products already claiming SDOC for these functions.	USG agencies continue to seek IPv6 products with SDOC that specifies the ruling major version of the tests.

3.1 Narrative Description of Lifecycle Table

Changes to the USGv6 profile and the testing infrastructure have impacts on all the stakeholders. The above table highlights the effect of these changes on product vendors and their customers, the USG Agencies in particular. Items 1 and 2 concern the impact of introducing and upgrading the profile, which goes through yearly revisions. Version 1.0 of the profile has no immediate impact on the agencies, but is a signal to product vendors to implement the mandatory capabilities. Conditional Musts and Shoulds are only implemented if chosen by the vendor, or in response to RFP. The annual revision of the profile signals what capabilities are required in the future, but will not become effective for 2 years if new MUSTs, 3 or more years if new SHOULD+s.

Items 3 and 4 denote timing events. The USGv6 testing program is actively testing products from about January 2010 onwards. Version 1.0 of the profile becomes effective in July 2010, and agencies are seeking USGv6 products in IT acquisitions from then onwards.

Items 6 through 10 of the table are concerned with the provision of tests for conformance, interoperability and network protection, for the compendium of capabilities in the profile. There are some capabilities for which tests exist at the outset, and some capabilities for which tests do not yet exist. The USGv6 testing website [6] gives up to date details of test status and contains also the tests. For some capability implemented, where no test exists as yet, the supplier can claim this in their SDOC, subject to in-house testing only. Where a test specification is already in existence at the launch of the testing program, products claiming support must be tested, and evidence of testing in an accredited laboratory, must be included in the declaration. When a new test specification is introduced after the launch of the testing program, the supplier has a 6 month grace period before claims of implementation must be tested and recorded in the SDOC. If a test specification is revised with only minor changes, no retest is required.

4 Management

Publication of NIST SP 500-273 [3] was the signal to accreditors to develop accreditation programs, and test laboratories to choose test methods from Section 5 of that document and to seek accreditation. With the formal designation of test specifications as "Version 1.0" in November 2009, the pieces are in place for laboratories to open for testing business.

Ongoing management of the testing program includes:

- Maintaining the testing program website [6] to keep the list of accreditors and test laboratories up to date.
- Promoting dialogue and agreement on interpretation and editing of the test selection tables and test specifications. These are also published at the website.
- Sourcing new test specifications for USGv6 capabilities where such tests are not available at the outset.
- Hosting the mailgroup: usgv6-testing@nist.gov for the use of participating laboratories, accreditors and test developers. Discussions and decisions of the mailgroup are made available to the stakeholders.
- Hosting an annual meeting at NIST to resolve test specification issues, interoperability issues, and at the same time review the effectiveness of the testing program.
- Continuing to promote harmonization activities with other IPv6 testing programs around the world in good standing.

Management of the USGv6 testing program is conducted through the mailgroup, the website and in occasional face-to-face meetings.

5 Claims of Product Compliance

USG agencies seeking to buy USGv6 compliant products are advised to look at the Supplier's Declaration of Conformity (SDOC {4,5]. The details of what is included in SDOC are given in Sections 5.1 and 5.2. The question of what products can be claimed as equivalent to the tested version and included in the same SDOC is discussed in Section 5.3. Finally, the vendor's test process culminating in the production of SDOC is given in Section 5.4. A template for the SDOC is given in Appendix 1.

5.1 Preliminary Requirements

Product vendors are advised to use the USGv6 checklist given as an appendix in the USGv6 profile [2] as a means to document the capabilities implemented in their host, router or network protection device. This is input to the testing process, and the device tested in a laboratory accredited for USGv6. The list of accredited test laboratories and supporting accreditors is given at the USGv6 testing website [6].

A product vendor who seeks to test in an accredited laboratory MUST submit a list of the functions claimed. This list MUST include all of the unconditional must requirements for a device, plus those musts that are conditional on options required for a particular procurement request. The conditions and configuration options are defined in the host, router and network protection device templates in Sections 3, 4 and 5 of the USGv6 profile [2].

5.2 Test Selection Requirements

The tests for conformance, interoperability and network protection are published on the USGv6 website [6]. The USGv6 profile includes 12 functional areas, with over 150 RFCs and standards in total. 100% coverage is an ambitious long term goal, but for the foreseeable future there will be gaps in coverage, test suites missing. In making claims of conformance, a vendor must run the tests where they exist. Where tests do not exist, claims of functionality may be made, where those functions are implemented. If a test suite is added, vendors claiming that function MUST run and pass the tests within 6 months of their accession.

The basic set of tests derive from the IPv6 Ready Logo, ICSA Labs, and other sources, and constitute a superset of possible USGv6 tests, per RFC covered. The USGv6 website contains test selection tables that identify from the basic tests those tests applicable to USGv6 profile testing.

5.3 Test Pass Requirements

For hosts, routers and network protection devices the unconditional MUSTs in the USGv6 Node Requirements Table define the minimal capabilities that constitute a "USGv6-V1-Capable" product (see the USGv6 profile [2], Section 7.2 Compliance).

IPv6 device suppliers may be offering products that offer vendor specific functionality packages that go beyond the above specified minimum and these will be reflected in claims of feature support. Every product that is associated with a SDOC MUST have evidence of passing:

- The unconditional MUST functions listed in the Node Requirements Table. This entails passing tests of the MUST requirements in each RFC so listed.
- For every functional category claimed in the SDOC the conditional MUST functions listed in the Node Requirements Table. This entails passing the MUST requirements in each RFC so listed.

- For every RFC listed as SHOULD in the Node Requirements Table and claimed in the SDOC, the MUST requirements within the specification MUST be passed.

At any stage in the evolution of the USGv6 Profile and testing program, the test infrastructure will be continuously improved. This means there are functions and RFCs specified in the Profile, for which a Test Specification is not yet available. In these cases the developer MUST be able to identify such testing as was done.

5.4 **Composite Products**

Composite products (i.e., products who's USGv6 capabilities are provided by the application or integration of one or more distinct components) can inherit the USGv6 test results of their individual component parts. To do so the precise component parts and their test specific test results must be documented. The USGv6 testing program recognizes three cases of composite product:

1. Application of a single USGv6 Component - A vendor bundles a composite product in which the all the capabilities within the scope of the USGv6 profile are provided by a single, independent product (e.g., stock OEM operating system on commodity hardware), that itself has completed testing. In this case, the vendor of the composite product does not need to repeat conformance or interoperability testing. The composite product vendor must still complete an SDOC for the final product; in particular the product description and declaration (pages 1 and 2). Note that this declaration requires that the composite product vendor to attest to the following.

- "All of the USGv6 capabilities of the products cited this SDOC are provided by a single, unmodified, component referenced above. The conformance and interoperability test results for the USGv6 capabilities of this component are documented in the attached document. This SDOC attests to the fact that these USGv6 capabilities are unmodified in their use in the products cited above."

A copy of OEM vendor's SDOC must be attached so as to detail the complete set of USGv6 capabilities declared and tested for the product.
This case is primarily intended to address the OEM operating system on commodity hardware scenario. It should be noted that though, that this scenario is equally applicable to a single vendor that employs the same distinct IPv6 components in a series of products.

2. Integration of multiple USGv6 components - A vendor bundles a composite product who's USGv6 capabilities are provided by the integration of two or distinct products that have been (at least) conformance tested in isolation. The composite product vendor must complete unique interoperability testing of the entire integrated product, but may reference the conformance test results of the individual components. Note that this declaration requires that the composite vendor attest to the following:

- "The USGv6 capabilities of the products cited in this SDOC are provided by the integration of two or more unmodified components cited above. The results from the conformance tests of these independent components are documented by attaching their SDOCs and identifying the appropriate component for each USGv6 capability they provide in the composite product."

In this scenario, the composite product vendor provides copies of the SDOCs for each distinct component and a unique SDOC for the composite product. For each USGv6 capability claimed for the composite product, a distinct interoperability test result must be cited. If conformance test results are to be inherited

from a previous component test, the composite product SDOC must clearly state which component is providing each capability and conformance test result.

3. Opaque application or integration of USGv6 components - A vendor supplies a product for which he does not wish to disclose whether all or parts of the stack derive from another product or supplier. In this scenario the vendor must complete both conformance and interoperability testing of the complete product offering as if it is a wholly unique implementation. The SDOC must be completed in full by the final product vendor.

5.5 Product Families

A single vendor may identify "product families", as a set of distinct product offerings (e.g., unique product name, version, configuration) that have identical and unmodified USGv6 capabilities. That is, the products only vary in ways that do not impact the capabilities within the scope of the USGv6 profile.

In this scenario, the product family can inherit the test results of one of its members. The vendor must supply and SDOC that identifies the specific product configuration that was tested, but can then list additional product configurations that are declared within the same family, and thus share the same test results. Note that the declaration of a product family requires that the vendor to attest to the following.

- "All of the products listed in this product family are implemented such that their USGv6 capabilities are identical in form and function across the entire product family. The specific conformance and interoperability test results for the USGv6 capabilities of an indentified member of this product family are provided in this SDOC. This SDOC attests to the fact that these tested USGv6 capabilities are identical in form and function for all the products cited above."

5.6 Traceability and Applicability of Test Results

The concepts of composite products and product families have been developed to ease the vendor's burden for duplicative testing, while maintaining an acceptable level of product assurance and traceability of results within the USGv6 test program. We rely on the test lab / vendor relationship to establish and document the scenarios in which product families and composite products may inherit a prior test result. It is expected that all such vendor claims of inherited test results can, and will be, explicitly affirmed by the cited test labs should a user decided to verify the test results claimed in any given SDOC.
Each lab may establish the procedures by which composite products and product families are identified, as long as they meet the requirements and guidelines provided by the USGv6 program. In the end, we rely on the natural tension between a lab's desire to maintain its reputation and accreditation in the USGv6 test program and its desire to avoid duplicative testing for its customers, the product vendors. A given lab, for example, might require sample testing of two or more product configurations before being willing to attest to inherited results for an entire family or a composite product. All claims and reports of test results should always explicitly indicate what product configurations were actually tested and which additional configurations those results are deemed applicable to.
Note also, that should a lab determine that at some point that there is reason to suspect that the validity of previously identified and agreed upon inherited test results, the lab is free to request further tests from the vendor and/or modify the set of products for which it is willing to affirm test results for. It is expected that it is in all parties best interests (i.e., vendors, test labs, accreditors, and users) to efficiently identify and resolve such issues.

5.7 USGv6 Device Supplier's Process

This section describes the process that suppliers of IPv6 devices will go through, from specification through testing, to USG acquisition, via SDOC production. This is expressed in the context of the triggering events.

Event: new version of USGv6 profile published.

IPv6 vendors with hosts, routers and/or network protection devices design and develop new products, or upgrades to existing products, to meet the USGv6 profile capabilities. The profile timeline allows for this development to take up to 24 months.

Event: USGv6 test specification published.

Initial draft test specifications for capabilities specified in the USGv6 profile are published. Vendors can test in-house for conformance against these specifications.

Event: Test laboratories accredited for conformance, interoperability and network protection test methods.

IPv6 vendors can establish their own test laboratories for conformance, or seek testing in a 2nd or 3rd party laboratory. Interoperability testing and network protection testing are required to be done in 2nd or 3rd party test laboratories.

IPv6 vendors create a Supplier's Declaration of Conformity, listing USGv6 capabilities tested and passed. Considering the configuration of a USGv6 device contains multiple testable capabilities, it is likely that the SDOC records testing for different capabilities done in different test laboratories at different times. There is no USG requirement that testing be done at a single location.

Event: Federal Acquisition Regulation becomes effective.

Federal Acquisition Regulations require that USG agencies acquire tested USGv6 capable products. IPv6 vendors market to agencies based on their stated requirements. Agencies seek to validate claims of functional support by inspecting the SDOC.

6 Bibliography and References

[1] OMB M-05-22 Transition Planning for Internet Protocol Version 6 (IPv6), Office of E-Government and Information Technology, Office of Management and Budget, August 2005. http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2005/m05-22.pdf

[2] NIST SP 500-267 A profile for IPv6 in the U.S. Government – Version 1.0, Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson, National Institute of Standards and Technology, July 2008. http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

[3] NIST SP 500-273 IPv6 Test Methods: General Description and Validation, Stephen Nightingale, Erica Johnson and Tim Winters, National Institute of Standards and Technology, August 2009. http://www.antd.nist.gov/usgv6/NIST-SP-500-273.v1.pdf

[4] ISO/IEC 17050-1:2004 Conformity Assessment – Supplier's Declaration of Conformity – Part 1: General requirements. http://www.iso.org/iso/

[5] ISO/IEC 17050-2:2004 Conformity Assessment – Supplier's Declaration of Conformity – Part 2: Supporting documentation. http://www.iso.org/iso/.

[6] USGv6 Testing Website, http://www.antd.nist.gov/usgv6/testing.html.

[7] ISO 9646-2:1994 Information technology – Open Systems Interconnection – Conformance testing methodology amd framework – Part 2: Abstract Test Suite specification. http://www.iso.org/iso/

[8] ISO/IEC 17025:2004 General requirements for the competence of testing and calibration laboratories. http://www.iso.org/iso/

[9] The RFC-Editor homepage, http://www.rfc-editor.org/.

7 Terms

Application Firewall a firewall that operates using application data filtering.

Conformance Testing Testing to determine if a device satisfies the criteria specified in a controlling document, such as an RFC.

Firewall A device that acts as a barrier to prevent unauthorized or unwanted communications between sections of a computer network.

Host Any node that is not a Router. In general this profile is limited to discussions of general purpose computers, and not highly specialized devices.

Interoperability Testing Testing to ensure that two or more communications devices can interwork and exchange data.

Network Protection Device A device such as a Firewall or Intrusion Detection device that selectively blocks packet traffic based on configurable and emergent criteria.

Network Protection Testing Testing that is applicable to network protection devices.

Request for Comment (RFC) – an Intenet standard, developed and published by the Internet Engineering Task Force.

Router a Node that interconnects subnetworks by packet forwarding.

USG The United States Government, comprising the Federal Agencies.

Appendix 1: Supplier's Declaration of Conformity: Template

The template for the Supplier's Declaration of Conformity is included here on the adjacent page. Some notes on the template are given below.

- Test Suite column where a test suite is identified by name, tests should be run in an accredited laboratory and passed. Where the cell is marked Self Test, no official test suite is yet available. The supplier uses in-house testing and may claim support.
- The SDOC comprises a high-level summary of the functional areas supported. It does not identify a 'blow-by-blow' account of all protocols tested within that functional area. Tested support can only be claimed if all the mandatory lines from the Node requirements Table within a functional area are also tested and passed.
- The test version numbers given in this template are listed with a major and a minor version number. Agencies and buyers are urged to compare product results against the currently in force major number, without regard to the minor number. Hence, '1.*' implies that1.1, 1.2, 1.3 and so on are all valid results.

Supplier's Declaration of Conformity for USGv6-v1.0 Products		Page 1
1	**Test Laboratory's Product Id**	
2	**Supplier's name, address and contact details**	
3	**Product Description: Product Name, S/W, H/W, H/W-S/W combination, Revision Level, Product Family.**	
4	**Product implementation summary, e.g. USGv6-v1-Capable+IPv4+DHCP-Client+DNS-Client+URI+Link=Ethernet**	
5	**The Document Requiring Conformity**	
USGv6 Profile version 1.0, July 2008.		
Check One	**Attestation**	
	The results of conformance and interoperability testing the USGv6 capabilities of this product are listed in this original SDOC. **-OR-**	
	The USGv6 capabilities of this product are provided by bundling in a single USGv6 stack, identified above. The results of conformance and interoperability testing are referenced by attaching the original SDOC. **-OR-**	
	The USGv6 capabilities of this product are provided by the integration of two or more components identified above. The results of conformance testing the independent components are referenced by attaching their SDOCs. The interoperability testing results are unique, referenced in this original SDOC and attested here.	
	Signature	**Date**
	Title	

Supplier's Declaration of Conformity for USGv6-v1.0 Products	Page 2
Test Laboratory's Product Id	<supplier to add>

This document summarizes specific details of a USGv6-v1.0 product or series. It is developed by the product supplier. Its consumer is the product buyer. Guidance for both parties is given below.

Guidance for Suppliers

The left half of the template (page 3) duplicates the configuration checklist, including all the mandatory functions for Host, Router and NPD. The right half of the template identifies the test selections for conformance and interoperability, with their current versions. Where a test label is given, these tests must be passed. In the cells where "Self Test" is written, there are no tests in existence today, and suppliers must test in-house. The columns to the right of the conformance and interoperability test labels respectively require supplier completion to identify the test laboratory where tested.

Further detailed guidance on how the SDOC instance can be created is given in NIST SP 500-281 "USGv6 Testing Program User's Guide". The guidance includes provision for how to test and/or represent composite products, that combine test results from different component parts. Recognizing that many vendors choose to market product lines and product families, note that claims should focus on compliance of the unique stack, and not the product label. Hence a single IPv6 stack may be installed in a variety of products differentially labelled, It is only required to test the unique stack once.

Test Laboratory and Accreditor Identifiers

Lab Abbreviation	Lab Details	Lab Contact	Accreditor
ICSA	ICSA Labs, http://www.icsalabs.com	Guy.Snyder@icsalabs.com	<tba>
IOL	University of New Hampshire InterOperability Laboratory, http://www.iol.unh.edu	Erica.Johnson@iol.unh.edu	<tba>
Self Test	Supplier's internal testing operation	<supplier adds here>	n/a

Guidance for USG Agencies and Other Buyers

This document identifies a USGv6 v1.0 networking product from the supplier given above. The declarations of conformity on Page 3 constitute the specification of the product and list USGv6-v1.0 capabilities implemented and tested. Only in the case where all functions listed as unconditional 'M' in the profile are implemented and tested, can the product be labelled "USGv6-v1.0-compliant". Networking stacks are complex and the many capabilities are tested separately, for conformance, and in combination, for interoperability. Buyers may want to verify information given in this document. The accredited laboratory where tested, and the laboratory's product test identifier are given for this purpose.

The test version numbers given in this template are listed with a major and a minor version number. Agencies and buyers are urged to compare product results against the currently in force major number, without regard to the minor number. Hence, ‘v1.*’ implies that v1.1, v1.2, v1.3 and so on are all valid results.

Supplier's Declaration of Conformity for USGv6-v1.0 Products										Page 3
Test Laboratory's Product Id										
Spec / Reference	**Section**	**Additional Information IPv6 Requirements**	**Configuration Option**	**Host**	**Router**	**NPD**	**Test Suite Conformance/NPD**	**Test Lab & Lister ID**	**Test Suite Interop**	**Test Lab & Lister ID**
								e.g <lab> & <ID> OR "Self Declaration"		**e.g <lab> & <ID> OR "Self Declaration"**
SP500-267	6.1	**IPv6 Basic Requirements**		**M**	**M**		**Basic_v1.*_C**		**Basic_V1.*_I**	
		support of stateless address auto-configuration	SLAAC				**SLAAC-V1.*_C**		**SLAAC-V1.0_I**	
		support of SLAAC privacy extensions.	PrivAddr				*Self Test*		*Self Test*	
		support of stateful (DHCP) address auto-configuration	DHCP-Client				*Self Test*		**DHCP_Client_v1.*_I**	
		support of automated router prefix delegation	DHCP-Prefix				*Self Test*		*Self Test*	
		support of neighbor discovery security extensions	SEND				*Self Test*		*Self Test*	
SP500-267	6.6	**Addressing Requirements**		**M**	**M**		**Addr_Arch_v1.*_C**		**Addr_Arch_v1.*_I**	
		support of cryptographically generated addresses	CGA				*Self Test*		*Self Test*	
SP500-267	6.7	**IP Security Requirements**		**M**	**M**					
		support of the IP security architecture	IPsec-V3	**M**	**M**		**IPsecv3_v1.*_C**		**IPsecv3_v1.*_I**	
		support for automated key management	IKEv2	**M**	**M**		**IKEv2v1.*_C**		**IKEv2v1.0_I**	
		support for encapsulating security payloads in IP	ESP	**M**	**M**		**ESP_v1.*_C**		**ESP_v1.*_I**	
SP500-267	6.11	**Application Requirements**								
		support of DNS client/resolver functions	DNS-Client				*Self Test*		*Self Test*	
		support of Socket application program interfaces	SOCK				*Self Test*		*Self Test*	
		support of IPv6 uniform resource identifiers	URI				*Self Test*		*Self Test*	
		support of a DNS server application	DNS-Sever				*Self Test*		*Self Test*	
		support of a DHCP server application	DHCP-Server				*Self Test*		**DHCP_Serv_v1.*_I**	
SP500-267	6.2	**Routing Protocol Requirements**								
		support of the intra-domain (interior) routing protocols	IGW				*Self Test*		**OSPFv3_v1.*_I**	
		support for inter-domain (exterior) routing protocols	EGW				*Self Test*		**BGP_v1.*_I**	
SP500-267	6.4	**Transition Mechanism Requirements**								
		support of interoperation with IPv4-only systems	IPv4				*Self Test*		*Self Test*	
		support of tunneling IPv6 over IPv4 MPLS services	6PE				*Self Test*		*Self Test*	
SP500-267	6.8	**Network Management Requirements**			**M**				Self Test	
		support of network management services	SNMP		**M**		*Self Test*		Self Test	
SP500-267	6.9	**Multicast Requirements**		**M**	**M**		**to be announced**		**to be announced**	
		full support of multicast communications	SSM				*Self Test*		*Self Test*	
SP500-267	6.10	**Mobility Requirements**								
		support of mobile IP capability.	MIP				*Self Test*		*Self Test*	
		support of mobile network capabilities	NEMO				*Self Test*		*Self Test*	
SP500-267	6.3	**Quality of Service Requirements**								
		support of Differentiated Services capabilities	DS				*Self Test*		*Self Test*	
SP500-267	6.12	**Network Protection Device Requirements**				**M**				
		support of basic firewall capabilities	FW				**N1_FW**			
		support of application firewall capabilities	APFW				**N2_App_FW**			
		support of intrusion detection capabilities	IDS				**N3_IDS**			
		support of intrusion protection capabilities	IPS				**N4_IPS**			
SP500-267	6.5	**Link Specific Technologies**		**M**	**M**		**Self Test**		**Self Test**	
		support of robust packet compression services	ROHC							
		support of link technology	Link=	**M**	**M**		**Self Test**		**Self Test**	
		(repeat as needed) support of link technology	Link=							