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

Special Publication 500-273

USGv6 Test Methods: General Description and Validation

National Institute of Standards and Technology

Stephen Nightingale, Erica Johnson and Timothy Winters

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

Special Publication 500-273

NIST Special Publication 500-273

USGv6 Test Methods: General Description and Validation – Version 2.0

National Institute of Standards and Technology

Stephen Nightingale, Erica Johnson, Timothy Winters

Internetwork Technologies

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

23 September 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 500-273
Natl. Inst. Stand. Technol. Spec. Publ. 500-273, 34 pages (23 September 2009)

Acknowledgements

This document emerged from a protracted period of discussions with a number of stakeholders including the Federal IPv6 working group, chaired by Pete Tseronis of the US Department of Energy. Discussion with members of the IPv6 Ready Logo program, led by Hiroshi Esaki of the University of Tokyo helped also, in addition to specific technical contributions to the test program infrastructure. Particularly strong contributions came from the InterOperability Laboratory of the University of New Hampshire.

The staff at ICSA Labs including Guy Snyder and Brian Monkman helped with the sections on security and network protection, as did Mark Carson, Sheila Frankel, Darrin Santay and Jean-Cyrus Angbo of NIST. Doug Montgomery offered general guidance and comment. Fang-Yu Ling of Taiwan Telecommunications laboratories also commented.

The documents suitability as input to the accreditation process was also vetted by Sally Bruce, Jeffrey Horlick and Dana Leaman of NVLAP, and Gordon Gillerman of NIST Standards Services.

Table of Contents

Executive Summary

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

- Accreditation organizations who are signatory to the International Laboratory Accreditation (ILAC) mutual recognition arrangement,
- Testing laboratories who will apply to such an accreditor for USGv6 profile testing accreditation, and
- Test method developers who develop abstract and/or executable tets and test methods for USGv6 capable hosts, routers and network protection devices.

Taken together with the abstract test specifications published at the USGv6 testing website [14] it provides the essential material for accreditors to establish testing programs compliant with ISO/IEC 17025 [3] and for test laboratories to seek accreditation for USGv6 test methods. The motivation for this testing program follows from the publication of NIST SP 500-267 "A Profile for IPv6 in the U.S. Government – Version 1.0[1]" [2] which provides recommendations to Federal Government agencies for product level acquisitions in the adoption of IPv6. In that document we suggest that "product testing services are likely needed to ensure the confidence and to protect the investment of early IPv6 adopters". We surveyed the existing IPv6 testing programs, and concluded that a distinct USG testing program is needed, but with the commitment to harmonization and convergence into a broad collaborative user/vendor testing initiative, in which the technical and procurement requirements of the USG can be accommodated.

Among the existing IPv6 testing schemes both the IPv6 Ready Logo [7] and the DoD IPv6 capable certification testing process [8] embrace conformance testing and interoperability testing of IPv6 hosts and routers. As of March 2009 the DoD has ceased separate testing of IPv6 products in favor of testing to Unified Capabilities Requirements [15]. The IPv6 Ready Logo uses abstract test specifications, subjected to member review, and interoperability testing allowing for a flexible range of network architectures. Their IPv6 stack requirements are defined implicitly using abstract test specifications for a range of Core + Applications + other functions. NIST has signed memoranda of understanding with appropriate members of the IPv6 Ready Logo program to secure use of their test specifications as the initial basis for the USGv6 Test Program. As this test program evolves, selected subsets of these tests, possibly with modifications and additions necessary to address specific requirements of the USGv6 Profile, will be published.

The USGv6 Test Program is designed to support multiple independent and autonomous test laboratories, and first, second and third party testing scenarios. In order to promote general confidence in test results in this environment and to insure both reproducibility and equivalence of test methods, the USGv6 Test Program requires that tests be conducted at ISO/IEC 17025 [3] accredited laboratories. The means by which the test methods of a given laboratory are accredited are the main subject of this publication

The IT accreditation landscape has changed in recent years. Where it was once possible to designate a single, usually government-run accreditor, there is now competition from private accreditors who compete on a level playing field. The laboratory accreditation organizations qualifications include compliance with ISO/IEC 17011 [4], and being signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Agreement (MRA) [16]. In order to promote comparability of test results across the accredited testing laboratories we encourage qualified accreditors to collaborate with NIST in the development of IPv6 testing specific accreditation requirements in addition to the general requirements of ISO/IEC 17025 [3] in the accreditation of IPv6 testing laboratories. This document is intended to provide guidance to any and all accreditors and test laboratories on units of

[1] Hereafter known as the USGv6 profile.

accreditation, standard reference tests, test method validation criteria, and, crucially, feedback mechanisms to maintain quality improvement in test suites, in addition to maintaining consistency of test interpretations.

Securing the network is critical, and the USGv6 profile includes provisions for edge protection products such as firewalls, collectively known as network protection devices (NPDs), and also for IPSec. NPD testing involves functional testing, local interface, environment, and document inspection. Network protection test specifications have been developed and are available at the USGv6 testing website.

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 500-281 *USGv6: Management, Processes and Stakeholders* [19]. It can be used by non-governmental 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 General Discussion of IPv6 Product Testing

The USGv6 profile defines requirements for host, router and network protection devices (NPD). Each of these product types defines a set of unconditional mandatory requirements, and provides several sets of "configuration options" that provide additional requirements that can be selected at the discretion of the profile user. Individual technical requirements are categorized as being mandatory, conditionally mandatory (based upon configuration options), or optional.

It has become the practice for networking products to be subjected to two different types of testing, for interoperability and for conformance (IPv6 Ready Logo [7], JITC [8]). Conformance tests a node against the protocol specification, and usually involves testing against protocol specific test tools. Interoperability tests nodes' ability to interwork in multi-vendor groups, over single or connected subnetworks. In a mature technology line, interoperability is prioritized over conformance, since the ability to communicate with the installed base is paramount. While the interoperable base is small , it is easier for a few implementors to make agreements yielding interoperability without strict conformance. For this reason, the results of conformance testing assume a greater importance earlier in a technology's lifecycle.

As a prudent step to secure procedurally correct testing, the USGv6 testing program requires that testing be done in laboratories accredited for the test methods in this document in accordance with ISO/IEC 17025 [3]. That standard refers to general testing requirements and so this document specifies the technical test methods involved in IPv6 product testing. This embraces both the conduct of each type of testing and the validation of test methods.

The foundation of each testing framework is a set of published test specifications, traceable to the consensus protocol standards. An initial basis set of abstract tests have been made available to the USGv6 testing program through agreements with IPv6 Forum members and the IPv6 Ready Logo program [7]. This provides coverage for some, but not all of the requirements in the USGv6 profile. For every abstract test specification, and corresponding executable test method, there must be a validation plan. abstract test specifications are initially validated against protocol specifications or standards. This is necessarily an informal heuristic step, as the RFCs underlying the profile are informally written in natural language text[2]. Even so, this process gives some confidence in the integrity of the abstract test specifications so that executable test methods can be validated against these abstract test procedures. Conformance, interoperability and network protection device (NPD) testing have different traceability chains, and these are further detailed below. Tests, like software, are always works in progress. In continuous operation there will be bugs, and needed interpretation. In order to converge on a truly interoperable community, it

[2] As opposed to a formal language specification.

is necessary that tests be maintained in synchronization across all participating laboratories, and test interpretations be agreed among laboratories, test method suppliers, producers and specifiers.

1.2 Purpose, Scope and Document Structure

This document describes the test methods and traceability requirements necessary to operate a test laboratory for USGv6 profile compliance requirements. This includes conformance and interoperability testing of hosts and routers, and network protection device testing. Specific elements include: quality components, traceability of tests, test feedback mechanisms, scope of accreditation, test method validation and interlaboratory comparison.

The management of the USGv6 testing program is described in NIST SP 500-281 [19]. Current information is made available on the project website [14].

Quality Components

ISO/IEC 17025 describes general procedures for constructing and assessing test laboratory quality systems. It does not describe test method specific competencies. Accreditors develop free-standing testing programs based on ISO/IEC 17025 and incorporating test methods from the technical domain. For USGv6 those test methods are described in this document.

Traceability of Tests

At the root of the testing hierarchy is the set of base technical standards. For IPv6 these include the set of RFCs specified in natural language text by the Internet Engineering Task Force (IETF). Abstract test specifications are derived from these, describing also in natural language the configurations and procedures for testing the RFC functions. Since these are in natural language, the validation method to determine the correctness of these tests is informal expert review, according to systematic procedures published in here. We distinguish between test validation for conformance and interoperability and for NPD functional testing, in Section 4.1.

Feedback Mechanisms

In a technology as complex as IPv6, with upwards of 150 RFCs referenced in the profile, test coverage and correctness become an extensive management issue. It may be that the community of test laboratories discovers the need to alter, add or delete certain tests. We propose an assessment framework that makes sure test case fixes are communicated among, and agreed between, participating test laboratories, in Section 4.4.

Test Methods and Scope of Accreditation

The USGv6 profile [2] defines a range of capabilities applicable to configurations of host, router and NPD products. All hosts and routers must implement the IPv6 Core specifications (RFC 2460 et al)[3] and also the IPsec suite (RFC 4301 et al) – its function relies on the core, but its testing is separate. Optional groupings include also Mobility (RFC 3775 et al), Multicast (RFC 3810 et al) and Network Management (RFC 3411 et al). Network protection devices also require to be tested, and these include Firewalls, Application Firewalls, Intrusion Detection Systems and Intrusion Protection Systems. Their functions are directly specified in the USGv6 profile Section 6.12 [2]. All of these functions are subject to discrete test

[3] The set of RFCs and other protocol specifications within the scope of this testing document are fully specified in the bibliography of the USGv6 profile [2].

methods. Assessment for Accreditation requires a combination of these methods. An individual test laboratory may choose to test one or more product types, and provide one or more of these test methods. No test laboratory is obliged to provide all test methods. The list of test methods and Scopes of Accreditation can be found in further detail in Section 5.2.

Test Method Validation

The complexity of IPv6 functional categories is paralleled by complexity in Test Methods, over all types of testing. There are different validation requirements for conformance, interoperability and network protection device test methods. Test laboratories accredited for conformance use test methods comprising software and test scripts to achieve the test purposes of the abstract test specifications. Validation of these test systems entails resolving the behavior and outcomes of executing these tests, against the respective abstract test specifications. The informality of the RFCs and abstract test suites limits this also to being an informal, heuristic process. Test laboratories accredited for interoperability use procedural test methods for constructing heterogeneous configurations of hosts, routers and NPDs, using test traffic generators, and observing the results with respect to products under test. Validation of interoperability test methods is performed through review of test procedures and their execution, by many technical experts. The procedures for validation of conformance and interoperability test methods are described in Section 6.1.

Network Protection Devices act as inline filters to analyze and block or permit traffic flowing into and out of a protected network. The presumption is that they can be compromised either physically, or by packet flows in either direction. They include requirements for managing packet traffic, configuring filters, logging, user documentation and administrative security. Testing of NPDs is required not only to exercise packet traffic flows, but also to exercise administrative functions to assess the integrity of logged messages, and to assess the documentation. Generally, validation of the functions of filters, administrative control, logging and documentation will be through manual analysis. This is detailed in Section 6.3.

The characterisitic of network protection devices is that they are designed to protect against known attacks, and able to be configured to protect against newly discovered attacks. Such new attacks cannot of their nature be tested for before acquisition. Since USGv6 is a procurement profile based on Supplier's Declaration of Conformity, we cannot require post-procurement re-testing to cover emerging threats explicitly. The update lifecycle for test specifications is six monthly. We should anticipate that threats emerge on their own schedule, but the required testing that encapsulates these threats will be updated on the six monthly cycle. Of course network protection products are expected to be configurable to handle new threats as soon as they appear.

Proficiency Testing and Interlaboratory Comparisons

As part of assessment for accreditation, the laboratory and its staff undergo proficiency testing to determine the laboratory's competence to apply the test methods within its scope. As a related, but separate issue, each laboratory must be able to show equivalence of results among identical products tested in any laboratory that operates the USGv6 test program. Proficiency testing and interlaboratory comparisons are described in Section 7.

1.3 Lifespan

The provisions of this testing guidance document remain in effect through the lifetime of the successive versions of the USGv6 profile. Active USG management of the USGv6 testing program will continue at least 24 months beyond the last iteration of the profile. The timing of cessation of active management is to be determined. It is our intention to secure continuity through merger with other testing programs.

However, the total lifespan of USGv6 Profile compliance testing includes within it a lifecycle model that encompasses changes to the profile and to the test specifications that have impacts on the developing Interoperable base. This lifecycle model is discussed in the management document [19].

1.4 Audience

The USGv6 profile and its testing program draw a set of stakeholders into a set of relationships. These relationships influence the processes of IPv6 product acquisition, testing, development and specification. The stakeholders include: USG agencies, IPv6 stack developers, accreditors, test laboratories,and test developers. This document details the relationships and processes involved in establishing compliance of IPv6 products to the USGv6 profile 1.

Accreditation organizations assess, audit and accredit test laboratories using the quality processes in ISO/IEC 17025 [3] and with scopes of accreditation that are aligned with test methods as described in Section 5. Organizations qualified as accreditors include those signatory to the International Laboratory Accreditation Co-operation (ILAC), that are peer assessed to be compliant with ISO/IEC 17011 [4].

Testing laboratories conduct conformance and interoperability testing of hosts and routers, and also network protection devices, for USGv6 compliance. Organizations eligible to be USGv6 testing laboratories include 3rd party – independent laboratories, 2nd party laboratories that operate as part of a USG agency and 1st party laboratories that operate as part of an IPv6 product vendor. To qualify, any of these organizations must be accredited under ISO/IEC 17025 [3] for one or more of the test methods described in this document.

IPv6 product developers seek testing in one or more accredited laboratories, and having passed all relevant tests declare a Supplier's Declaration of Conformity (See USGv6 profile Section 7 [2] and NIST SP 500-281 [19]). Developers are eligible to operate their own accredited laboratory for the conformance testing methods listed in Section 5. They MUST seek testing for interoperability and network protection testing (if applicable) in a 2nd or 3rd party testing laboratory.

A USG agency's relationship with USGv6 compliance is mostly confined to acquisition of tested products having SDOC, as governed by the Federal Acquisition Regulations. An agency may choose to operate a test laboratory for interoperability and/or network protection.

1.5 Normative Terminology

The terminology used to describe requirements levels in the profile include: "mandatory", "optional" (with their common meaning), and "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" which are to be interpreted as described in RFC 2119 [13]. In addition, the profile adopts the use of the term "SHOULD+"to indicate a requirement that is equivalent to "SHOULD" in this version of the specification, but is expected to be elevated to a "MUST" in future versions.

The use of MUST, MAY and SHOULD within this testing document refers to the requirements for testing, as distinct from the requirements for IPv6 implementation. More commonly, requirements in this document are expressed as declarative text.

2 Linkage to the Accreditation Infrastructure

There has been for many years in industrialized economies a system where acquisition authorities and government entities require compliance to particular standards. Test laboratories are established to test artifacts and systems against reference materials. National measurement laboratories such as NIST in the United States, and the National Physical Laboratory in the United Kingdom develop methods for improving precision in measurements of standard reference materials. Accreditation bodies assess the integrity of test laboratories use of the testing materials, and create an umbrella for the community of test laboratories so that the results from every lab are equivalent.

The International Laboratory Accreditation Cooperation (ILAC) operates a peer assessment system to provide confidence in laboratory accreditation. ILAC MRA signatories operate in accordance with the standard for accreditation systems, ISO 17011 [4]. One or more qualified accreditors may be interested in establishing programs of accreditation for IPv6 testing laboratories.

2.1 The Role of the Accreditor

Qualified Accreditors include those bodies compliant with ISO 17011 [4] who are also signatory to the International Laboratory Accreditation Co-operation (ILAC) Mutual Recognition Agreement. When such an accreditor establishes an accreditation program, there are three components: quality, technical test method, and interlaboratory coordination:

- Assessment of the testing process, laboratory management, and quality control. These are covered by implementing ISO 17025 [3], General Requirements for the Competence of Calibration and Testing Laboratories. This is the quality component.

- Assessment of the operation of the test method, and validation of the test method. This is the technical component, and for our purposes the technical content includes conformance and interoperability testing of IPv6 products, and functional testing of network protection devices.

- Oversight of the coordination between test laboratories participating in the IPv6 testing program. Because of the potential for multiple accreditors entering the IPv6 space, it is particularly important to coordinate comparability of test results from accredited laboratories across test methods, products and test laboratories results. The USGv6 testing program will designate a single organization to conduct interlaboratory comparisons, subject to the agreement of participating accreditation bodies.

The second and third items above are described in this document.

2.2 The Role of the Program Sponsor

Accreditors generally establish programs based on an expressed stakeholder need. The USGv6 Profile was authorized by the Office of Management and Budget Memorandum 05-22 [1], and published by NIST. The associated testing program is sponsored by NIST. The sponsor's role includes identifying the standard reference materials, test methods, and methods of validating operational tools against the reference standards. The content of this document is the expression of responsibility for establishing test methods for IPv6 products under the Profile.

The program sponsor may also designate one or more agents to conduct and coordinate the program of interlaboratory comparisons discussed in Section 7.

Ongoing coordination between profile requirements and testing infrastructure is also provided by NIST, through the testing website [14] and the mailing list at usgv6-testing@nist.gov.

3 Testing Frameworks

"IPv6" is actually a large and complex collection of protocols and functions necessary to define the new Internet Protocol (IP) as well as its implications for other protocol layers and the interfaces between them. There are ways to test this nexus of protocols by isolating particular protocols in particular stacks, or by assessing the aggregate behavior of the aggregate stacks/network. The isolation testing methods include conformance testing, and also functional and security testing. Interoperability testing tests the aggregate behavior by providing a realistic test of a product's behavior in a networked system. There is no widely known and agreed published methodology for interoperability testing. There are "operational" definitions, including the scheme operated by JITC for the DoD, and the IPv6 Ready Logo scheme. The JITC scheme entails connecting the Device under Test (host, router, or other product allowed by the DoD Profile) to a configuration that emulates DoD's Global Information Grid (GIG), and running the tests published in the DoD Generic Test plan [8]. These generally involve operating end-user applications and analyzing the results.

The IPv6 Ready Logo interoperability testing scheme is defined operationally in the documents published at http://www.ipv6ready.org. It usually entails a configuration with one or more hosts under test, and one or more routers under test. If the Tahi interoperability toolkit (http://www.tahi.org) is employed, the configuration includes a test manager, open source reference implementations, packet trace and analysis tools, and four connected subnetworks including one with Devices Under Test attached. There is great flexibility in creating the configuration of products to test.

The common requirement for interoperability testing is one or more points of control and observation for introducing traffic and analyzing and interpreting results. Architectures vary, however, and some methods require testing against a particular enterprise network, while others emphasize testing against a diverse plug-and-play set of products. Each of these methods has merit, but for preparing to introduce IPv6 products into a general market, the second method seems most useful. The first method has merit in conjunction with acceptance testing against the buyer's installed network, to demonstrate interoperability.

For conformance testing, ISO 9646 [10] describes a rich set of methods including single and multi-layer methods, point-to-point or transverse methods, and methods involving explicit test protocol coordination, or by human coordination between the application end-points. Most current executable methods seem to be multi-layer, loosely coordinated types. Any methods from the full ISO 9646 range are permissible.

Network protection device capabilities must include very general product configurability, logging, environmental security and packet filtering. Testing these capabilities requires physical access and inspection. The testing framework must have local access to accommodate these needs.

Separate testing frameworks are required for the conduct of conformance, interoperability and network protection testing. A framework includes the test methods and the procedures required to validate and maintain them, and the broad constraints for the conduct of each of these types of testing. The constraints on testing conduct are given here.

3.1 Performing Conformance Testing

The elements required to conduct conformance testing include the following:

- Any host or router claiming conformance to the USGv6 Profile MUST demonstrate evidence of Conformance to the USGv6 abstract test specifications.
- Conformance testing MUST be done by a facility accredited to ISO 17025 by an organization which may be controlled by the product supplier (1st party), by the US Government (2nd party) or by an independent testing organization (3rd Party). This does not preclude test laboratory staff traveling to the customer's site to conduct testing.
- The technical test methods for Conformance MUST follow and reference these guidelines.
- Products to be tested MUST include USGv6 profile functions as given in Appendix A and the Node Requirements Table.
- For each functional category and USGv6 profile configuration option, testing MUST be according to the conformance abstract test specifications published at the USGv6 testing website [14].
- To claim conformity in a SDOC, an IPv6 stack MUST pass all of the tests associated with unconditional MUSTs and all those conditional MUSTs associated with claimed IPv6 stack functionality as per the USG IPv6 profile. Additionally, a stack MUST pass all those tests for which functionality is claimed, associated with SHOULD functions in the RFC or standard.
- The quality provisions of ISO17025 [3], including those relating to repeatability and reproducibility of testing, apply also to conformance testing of host and routers.

3.2 Performing Interoperability Testing

The elements required to conduct interoperability testing include the following:

- Any host or router claiming compliance with the USGv6 profile MUST demonstrate evidence of interoperability with three or more existing independent implementations of IPv6 to include one each of a host and a router, where appropriate.
- Interoperability testing MUST be done in a facility accredited to ISO 17025 by an organization controlled by the US Government (2nd party) or an independent testing organization (3rd Party).
- The technical test method(s) for interoperability MUST follow and reference these guidelines.
- Until further requirements are specified, successful conformance testing as per Section 8.2 MUST be pre-requisite to the applicable interoperability testing.
- Products to be tested MUST include USGv6 profile functions as given in Appendix A and the Node Requirements Table of the profile [2].
- For each functional category and configuration, testing MUST be according to the interoperability abstract test specifications published at the USGv6 testing website [14].
- For each unit of accreditation as listed in Section 5.2.2, interoperability testing among several products MUST be conducted in a single laboratory. However for different units of accreditation, a product vendor may choose different laboratory and interoperability partnering arrangements, even for the same product.
- To claim compliance to the USGv6 Profile in an SDOC, a n IPv6 stackMUST pass all of the tests associated with unconditional MUSTs and all those conditional MUSTs associated with claimed USGv6 configuration options as per the USGv6 Profile. Additionally, a stack MUST pass all those tests for which functionality is claimed, associated with SHOULD functions.
- The quality provisions of ISO17025 [3], including those relating to repeatability and reproducibility of testing, apply also to interoperability testing of host and routers.

3.3 Performing Network Protection Testing

The elements required to conduct network protection device testing include the following:

- Any network protection device (IDS, IDP, Firewall or Application Firewall) claiming conformance to the USGv6 profile MUST demonstrate evidence of functionality as specified in the USGv6 profile Section 6.12 [2].
- Network protection device testing MUST be done in a laboratory accredited to ISO/IEC 17025 [3] for the applicable IPv6 test methods by an organization which may be controlled by the US Government (2nd party), or by an independent organization (3rd Party).
- The technical test methods for network protection devices MUST meet the functional criteria specified in Section 4.2.4 of this document.
- To claim compliance in an SDOC, an NPD MUST pass the applicable tests that are associated with unconditional MUSTs and all those conditional MUST associated with claimed product functionality as per the USGv6 Profile. Additionally, a product MUST pass those tests for which functionality is claimed, associated with SHOULD functions in the associated specification.
- The quality provisions of ISO17025 [3], including those relating to repeatability and reproducibility of testing, apply also to testing of network protection devices.

4 Traceability of Tests

The Problem

> A problem that arises when test developers individually develop tools and tests against a specification is the lack of synchronization that arises among the implementations in test coverage and test interpretation. We get around this problem by establishing a canonical set of tests and test interpretations, and requiring all implementations to validate against that set. This section discusses the traceability scheme that ensues.

The objective of testing is to determine whether a product complies with a given specification. In physical artifact testing a comparison is usually made of test results of the product against the requirements of the specification, accurate to a stated uncertainty. For the purpose of assessing IPv6 products, the specification is the USGv6 profile [2] and the compendium of RFCs it references. Applicable products include hosts, routers and network protection devices. Tests are derived from the protocol specifications and verified in a peer evaluation process, by test laboratories and test tool developers. These then serve as the traceability root against which executable tests are validated. This section establishes the traceability chains for conformance, interoperability and network protection, in Section 4.1. Validation procedures for each test specification are stated in Section 4.2.

A measurement result is complete only when accompanied by a quantitative statement of its uncertainty. NIST policy, as expressed in NIST Technical Note 1297, 1994 [11] is that measurement results be accompanied by such statements, and that a uniform approach to measurement uncertainty be followed. This is developed in Section 4.3. Test development is a discipline akin to software development, As such it benefits from a review process involving deep and wide analysis by many experts. This is a process of feedback and continual improvement.This is further elaborated in Section 4.4.

4.1 Traceability Chains

Conformance and interoperability tests are derived from the RFCs by systematic, but informal procedures. Executable tests are derived from these abstract tests by similarly informal procedures. This section identifies the traceability chains from RFCs through to executables. Their validation is described in Section 6. For Network Protection Devices, the USGv6 profile Section 6.12 is the specification. Validation and traceability methods for these are discussed in Section 4.1.2.

4.1.1 Traceability Chain for Conformance and Interoperability Testing.

Base Specifications: The RFCs and other specifications selected by the USGv6 profile (current version).

Reference Tests: Abstract test specifications for each product type (hosts and routers) for the combinations of base specifications that exist, these are listed at the USGv6 testing website [14].

Executable Test Methods: For each reference test suite listed, above, the executable test method comprises tests and test execution software and hardware. An executable test method may combine the tests of one or more abstract test specifications. The validation of these executable methods is described in Section 6. Validation MUST be conducted in an appropriately accredited test laboratory accredited with respect to the USGv6 Test Program.

4.1.2 Traceability Chain for Network Protection Testing

The system of traceability for network protection is essentially the same as that for conformance and interoperability testing.

Base Specification: USGv6 profile, Section 6.12 (current version).

Reference Tests: For each network protection device type: firewall, application firewall, intrusion detection system, intrusion detection and protection system, tests MUST be derived from the functions given in the base specification. Abstract test suites for these are listed at the USGv6 testing website [14].

Executable Test Methods: The test methods include written procedures as well as some automation. The reference tests establish the minimum set. NPD testing involves exploratory testing at the discretion of the laboratory. In order to retain traceability, the newly created tests must show their derivation from the specification and additionally the rationale for their deviation from the closest applicable reference test. Since the actual set of tests is constructed at the time of testing, the laboratory MUST apply and document a procedure for validating each of the tests developed at execution time, after live testing and before issuing the test report.

4.2 Reference Test Validation

The abstract tests described in Section 4.1 are the reference against which all executable tests are validated. Conformance test methods are the most potentially automatable, so validating them involves running the executable tests and reconciling the results against the abstracts. This is elaborated in Section 4.2.2. Interoperability tests are procedural and there may be no specific test tools derived. Validating them involves stepping through the abstract tests and reconciling the results of all participant products. This is elaborated in Section 4.2.3. Network Protection device test validation is described in Section 4.2.4.

4.2.1 General

- The USGv6 Profile is the compendium document that lists RFCs and other standards, which are the base specifications that abstract test specifications for conformance and interoperability are derived from.
- RFCs are written in natural language text and therefore they are informal. Any tests derived from these are also informal.
- Target products for conformance and interoperability testing include hosts and routers.
- The impetus of validation comes from the uncertainty of the method of deriving test specifications from RFCs. Since protocol specifications are written in natural language, the general answer to this is that there is no formal proof, therefore we must use heuristic, “trial and error” methods to increase our confidence in the test.
- For each abstract test specification, the set of RFCs contained shall be analysed for testable functionality, including not only MUST and SHOULD designated functions, but also functions specified by imperatives and declarative statements in the running text.

4.2.2 Conformance

- Conformance test topologies include a target device under test, and one or more pieces of test equipment connected over an IPv6 network. These will typically be in the configurations described in ISO 9646-2 [10], and are distinct from interoperability testing configurations.
- Conformance abstract test specifications include a test purpose, reference to RFCs or standards, setup information, a procedure describing packet flows and packet field values, and an observable result. For convenience of reference they also include a systematic test identifier and/or title.
- The objective of a conformance test is to determine whether a device under test can realize the isolated behaviors specified in a set of RFCs or standards.
- For conformance testing, the coverage criteria recommended are those given in ISO 9646-2, Sections 10.1 to 10.4 [10]. Validation of abstract test specifications for conformance mirrors these procedures.
- Validation is the procedure that resolves the abstract tests against the RFC functional analysis.

4.2.3 Interoperability

- Interoperability test topologies include one or more target devices under test, one or more host or router reference stacks, or test equipment including traffic generators and logging/analysis tools.
- Interoperability abstract test specifications include a test purpose, reference to RFCs or standards, setup information, a procedure describing packet flows and packet field values, and an observable result. For convenience of reference they also include a systematic test identifier and/or title.
- The objective of an interoperability test is to determine whether a device under test can realize the aggregate behaviors specified in a set of RFCs or standards.
- In all types of interoperability testing, actual IPv6 nodes communicates with each other. Traffic is driven through applications at one or more nodes. The construction, purposing and analysis of tests are not otherwise different than conformance. The validation methodology is the same, allowing for these architectural differences.

4.2.4 Network Protection

- The USGv6 profile Section 6.12 [2] is the base specification for network protection devices (NPDs). NPD tests are traceable to this specification.
- Testing, traceability and validation for network protection functionality assessment differ from those operations for conformance and interoperability testing. The specification for network protection devices calls for general, configurable, extensible capabilities rather than specific settings or protocols. Validation MUST take account of the following tenets:
    - Tests must employ sampling methods to provide evidence that the required capability exists and functions properly.
    - The requirements that various capabilities be administratively configurable imply that a sizeable proportion of the tests will involve demonstration of administrative interfaces and hence less amenable to automation or scripting.
    - Some level of penetration testing is needed to demonstrate the assurance aspects of some of the requirements, such as security of administrative controls.

  - Testing the performance under load/fail safe requirements will require sufficient test traffic generation capacity to reach the design limits of the product being tested.
- Section 6.2 below documents the completion of an executable test suite instance.

4.3 A Statement of Measurement Uncertainty

Measurement uncertainty is not defined for software testing methods.

4.4 Test Feedback Mechanisms

The abstract test specifications initially approved as the reference tests may have errors and omissions. These will be uncovered in the course of testing experience. There may also be differences of interpretation. It is important that test methods be improved in a timely fashion. It is also important that corrupted tests not affect the overall integrity of results. Corrupted tests will be addressed by community and stakeholder agreement. Subject to agreement, they may be withheld from the test base until the next revision, or retained for continuous use. The overriding concern is that each test reflects a single interpretation of the applicable RFC paragraph. The community and stakeholders in this context includes representatives of IPv6 product developers, users and the testing industry. Consistency of interpretation is essential to the quality of the aggregate testing and the stakeholders confidence that compliant products will meet users needs.

The mechanism for achieving feedback includes discussion and agreement on test interpretations and test specifications, through a mail group: usgv6-testing@nist.gov. All test developers and test laboratories engaged in testing with respect to the USGv6 testing program MUST actively participate in this mail group. In addition an annual face-to-face meeting is held at NIST where disputed tests are discussed and resolved. This is the same meeting and the same process as resolving differences following inter-laboratory comparison tests (See Section 7). Disputed tests and their resolutions will be published by NIST following the meeting, and also recorded in the test selection tables.

5 Test Methods and Scope of Accreditation

The USGv6 profile identifies a complex set of functional capabilities that include Core IPv6 in addition to Addressing, Routing, IPsec and several others. The business of operating an accredited test laboratory involves selecting areas of technical expertise and operating the tests applicable to these areas. A test laboratory can be accredited for as little as one method. No test laboratory is compelled to provide coverage for all test methods.

The sum total of all test methods that a test laboratory supports constitutes its Scope of Accreditation. Test methods are linked with test specifications. There are conformance and interoperability test specifications for the USGv6 capabilities of IPv6 hosts and routers. There are network protection test specifications for NPDs.

The set of test methods listed below is separated into conformance, interoperability and network protection methods. Each method is identified with a number and a label identifying the functionality, per the USGv6 profile node requirements table. For example F1_C IPv6 basic requirements is the test method for the functions tabulated on pages 50-51 of the profile version 1.0. The associated tests are listed on the USGv6 testing website. These methods and tests are linked to actual testing by executable test methods. These are discussed in Section 6.

5.1 Conformance Test Methods

For conformance there are 30 or more discrete test methods identified by an F number, for example F2 is the method for SLAAC, with an associated conformance test suite. There are also aggregate test methods, identified as H1 for hosts and R1 for routers. These are for the convenience of test laboratories who want to operate the minimum common set for a host or a router. Any test laboratory can offer the conformance test methods, 1st, 2nd or 3rd party.

Method H1: USGv6-V1-Capable Host Requirements

- **IPv6 Basic Requirements** – see USGv6 profile Section 6.1.
  - **SLAAC** – require support of stateless address auto-configuration.
  - **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.
- **Addressing Requirements** – see USGv6 profile Section 6.6.
- **IP Security Requirements** – see USGv6 profile Section 6.7.
  - **IPsec-V3** – require support of the IP security architecture.
  - **IKEv2** – require support for automated key management.
  - **ESP** – require support for encapsulating security payloads in IP.
- **Multicast Requirements** – see USGv6 profile Section 6.9.
- **Link Specific Technologies** – see USGv6 profile Section 6.5.
  - **Link** – require support of 1 or more link technologies.

Method R1: USGv6-V1-Capable Router Requirements

- **IPv6 Basic Requirements** – see USGv6 profile Section 6.1.
  - **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.

- **Addressing Requirements** – see USGv6 profile Section 6.6.
- **IP Security Requirements** – see USGv6 profile Section 6.7.
    - **IPsec-V3** – require support of the IP security architecture.
    - **IKEv2** – require support for automated key management.
    - **ESP** – require support for encapsulating security payloads in IP.
- **Network Management Requirements** – see USGv6 profile Section 6.8.
    - **SNMP** – require support of network management services.
- **Multicast Requirements** – see USGv6 profile Section 6.9.
- **Quality of Service Requirements** – USGv6 profile see Section 6.3.
    - **DS** – require support of Differentiated Services capabilities.
- **Link Specific Technologies** – see USGv6 profile Section 6.5.
    - **Link** – require support of 1 or more link technologies.

Method F1: IPv6 Basic Requirements – see USGv6 profile Section 6.1.

Method F2: Stateless Address Auto-configuration – see USGv6 profile Section 6.1.

- **SLAAC** – require support of stateless address auto-configuration.

Method F3: Privacy extensions for IPv6 SLAAC Requirements – see USGv6 profile Section 6.1

- **PrivAddr** – require support of SLAAC privacy extensions.

Method F4: DHCP Client – see USGv6 profile 6.1.

- **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.

Method F5: Prefix Delegation – see USGv6 profile Section 6.1.

- **DHCP-Prefix** – require support of automated router prefix delegation.

Method F6: Secure Neighbor Discovery Requirements – see USGv6 profile Section 6.1.

- **SEND** – require support of neighbor discovery security extensions.

Method F7: Addressing Requirements – see USGv6 profile Section 6.6.

Method F8: Cryptographically Generated Addresses – see USGv6 profile Section 6.6.

- **CGA** – require support of cryptographically generated addresses.

Method F9: DNS Client – see USGv6 profile Section 6.11.

- **DNS-Client** – require support of DNS client/resolver functions.

Method F10: Socket API for IPv6 – see USGv6 profile Section 6.11.

- **Sock** – require support of Socket application program interfaces (**Host only**).

Method F11: URI Generic Syntax – see USGv6 profile Section 6.11.

- **URI** – require support of IPv6 uniform resource identifiers.

Method F12: DNS Server Functions – see USGv6 profile Section 6.11.

- **DNS-Server** – require support of a DNS server application.

Method F13: DHCP Server Functions – see USGv6 profile Section 6.11.

- **DHCP-Server** – require support of a DHCP server application.

Method F14: Interior Routing Protocol– see USGv6 profile Section 6.2.

- **IGW** – require support of the intra-domain (interior) routing protocols (**Router only**).

Method F15: External Routing Protocol– see USGv6 profile Section 6.2.

- **EGW** – require support for inter-domain (exterior) routing protocols (**Router only**).

IP Security Requirements – see USGv6 profile Section 6.7.

- **Method F16: IPsec-V3** – require support of the IP security architecture.
- **Method F17: ESP** – require support for encapsulating security payloads in IP.
- **Method F18: IKEv2** – require support for automated key management.

Method F19: Transition Mechanism Requirements – see USGv6 profile Section 6.4.

- **IPv4** – require support to enable interoperation with IPv4-only systems.

Method F20: IPv6 Provider Edge MPLS Tunneling – see USGv6 profile Section 6.4.

- **6PE** – require support of tunneling IPv6 over IPv4 MPLS services (**Router only**).

Method F21: Network Management Requirements – see USGv6 profile Section 6.8.

- **SNMP** – require support of network management services.

Method F22: Multicast Requirements – see USGv6 profile Section 6.9.

- **MLDv2 - MLD Version 2 for IP**
- **Unicast-Prefix-based IPv6 Mcast Address**
- **Allocation Guidelines for IPv6 Mcast Addrs**

Method F23: Source-Specific Multicast for IP Requirements – see USGv6 profile Section 6.9.

- **SSM** – require full support of multicast communications.

Method F24: Mobility Requirements – see USGv6 profile Section 6.10.

- **MIP** – require support of capability for this host to be a mobile node.

Method F25: NEMO Basic Support – see USGv6 profile Section 6.10.

- **NEMO** – require support of mobile network capabilities (**Router only**).

Method F26: Quality of Service Requirements – USGv6 profile see Section 6.3.

- **DS** – require support of Differentiated Services capabilities.

Method F27: Explicit Congestion Notification (ECN) to IP – USGv6 profile see Section 6.3.

Method F28: Link Specific Technologies – see USGv6 profile Section 6.5.

- **Link** – require support of 1 or more link technologies.

Method F29: Packet Compression Technology Requirements– see USGv6 profile Section 6.5.

- **ROHC** – require support of robust packet compression services.

Method F30: Stateless DHCP Service for IPv6 - see USGv6 profile Section 6.1.

- **SL DHCP-Client** - Stateless DHCP Service for IPv6.

5.2 Interoperability Test Methods

The intuitive way to do interoperability testing is on a product-by-product basis, testing hosts against hosts, hosts against routers and routers against routers, then guiding and observing their aggregate behaviors. However in practice the range of configurable options in the USGv6 profile is so flexible that in the end it is better to construct interoperability test suites per RFC, and run the sets of tests required according to each product's configuration. For this reason, the interoperability test methods are structured identically with the conformance test methods. These are duplicated here. The test suites associated with these methods are uniquely applicable to interoperability testing.

Method H1: USGv6-V1-Capable Host Requirements

- **IPv6 Basic Requirements** – see USGv6 profile Section 6.1.
  - **SLAAC** – require support of stateless address auto-configuration.
  - **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.
- **Addressing Requirements** – see USGv6 profile Section 6.6.
- **IP Security Requirements** – see USGv6 profile Section 6.7.
  - **IPsec-V3** – require support of the IP security architecture.
  - **IKEv2** – require support for automated key management.
  - **ESP** – require support for encapsulating security payloads in IP.
- **Multicast Requirements** – see USGv6 profile Section 6.9.
- **Link Specific Technologies** – see USGv6 profile Section 6.5.
  - **Link** – require support of 1 or more link technologies.

Method R1: USGv6-V1-Capable Router Requirements

- **IPv6 Basic Requirements** – see USGv6 profile Section 6.1.
  - **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.
- **Addressing Requirements** – see USGv6 profile Section 6.6.
- **IP Security Requirements** – see USGv6 profile Section 6.7.
  - **IPsec-V3** – require support of the IP security architecture.
  - **IKEv2** – require support for automated key management.

    - **ESP** – require support for encapsulating security payloads in IP.
- **Network Management Requirements** – see USGv6 profile Section 6.8.
    - **SNMP** – require support of network management services.
- **Multicast Requirements** – see USGv6 profile Section 6.9.
- **Quality of Service Requirements** – USGv6 profile see Section 6.3.
    - **DS** – require support of Differentiated Services capabilities.
- **Link Specific Technologies** – see USGv6 profile Section 6.5.
    - **Link** – require support of 1 or more link technologies.

Method I1: IPv6 Basic Requirements – see USGv6 profile Section 6.1.

Method I2: Stateless Address Auto-configuration – see USGv6 profile Section 6.1.

- **SLAAC** – require support of stateless address auto-configuration.

Method I3: Privacy extensions for IPv6 SLAAC Requirements – see USGv6 profile Section 6.1

- **PrivAddr** – require support of SLAAC privacy extensions.

Method I4: DHCP Client – see USGv6 profile 6.1.

- **DHCP-Client** – require support of stateful (DHCP) address auto-configuration.

Method I5: Prefix Delegation – see USGv6 profile Section 6.1.

- **DHCP-Prefix** – require support of automated router prefix delegation.

Method I6: Secure Neighbor Discovery Requirements – see USGv6 profile Section 6.1.

- **SEND** – require support of neighbor discovery security extensions.

Method I7: Addressing Requirements – see USGv6 profile Section 6.6.

Method I8: Cryptographically Generated Addresses – see USGv6 profile Section 6.6.

- **CGA** – require support of cryptographically generated addresses.

Method I9: DNS Client – see USGv6 profile Section 6.11.

- **DNS-Client** – require support of DNS client/resolver functions.

Method I10: Socket API for IPv6 – see USGv6 profile Section 6.11.

- **Sock** – require support of Socket application program interfaces (**Host only**).

Method I11: URI Generic Syntax – see USGv6 profile Section 6.11.

- **URI** – require support of IPv6 uniform resource identifiers.

Method I12: DNS Server Functions – see USGv6 profile Section 6.11.

- **DNS-Server** – require support of a DNS server application.

Method I13: DHCP Server Functions – see USGv6 profile Section 6.11.

- **DHCP-Server** – require support of a DHCP server application.

Method I14: Interior Routing Protocol– see USGv6 profile Section 6.2.

- **IGW** – require support of the intra-domain (interior) routing protocols (**Router only**).

Method I15: External Routing Protocol– see USGv6 profile Section 6.2.

- **EGW** – require support for inter-domain (exterior) routing protocols (**Router only**).

IP Security Requirements – see USGv6 profile Section 6.7.

- **Method I16: IPsec-V3** – require support of the IP security architecture.
- **Method I17: ESP** – require support for encapsulating security payloads in IP.
- **Method I18: IKEv2** – require support for automated key management.

Method I19: Transition Mechanism Requirements – see USGv6 profile Section 6.4.

- **IPv4** – require support to enable interoperation with IPv4-only systems.

Method I20: IPv6 Provider Edge MPLS Tunneling – see USGv6 profile Section 6.4.

- **6PE** – require support of tunneling IPv6 over IPv4 MPLS services (**Router only**).

Method I21: Network Management Requirements – see USGv6 profile Section 6.8.

- **SNMP** – require support of network management services.

Method I22: Multicast Requirements – see USGv6 profile Section 6.9.

- **MLDv2 - MLD Version 2 for IP**
- **Unicast-Prefix-based IPv6 Mcast Address**
- **Allocation Guidelines for IPv6 Mcast Addrs**

Method I23: Source-Specific Multicast for IP Requirements – see USGv6 profile Section 6.9.

- **SSM** – require full support of multicast communications.

Method I24: Mobility Requirements – see USGv6 profile Section 6.10.

- **MIP** – require support of capability for this host to be a mobile node.

Method I25: NEMO Basic Support – see USGv6 profile Section 6.10.

- **NEMO** – require support of mobile network capabilities (**Router only**).

Method I26: Quality of Service Requirements – USGv6 profile see Section 6.3.

- **DS** – require support of Differentiated Services capabilities.

Method I27: Explicit Congestion Notification (ECN) to IP – USGv6 profile see Section 6.3.

Method I28: Link Specific Technologies – see USGv6 profile Section 6.5.

- **Link** – require support of 1 or more link technologies.

Method I29: Packet Compression Technology Requirements– see USGv6 profile Section 6.5.

- **ROHC** – require support of robust packet compression services.

Method I30: Stateless DHCP Service for IPv6 - see USGv6 profile Section 6.1.

- **SL DHCP-Client** - Stateless DHCP Service for IPv6.

5.3 Network Protection Test Methods

Network protection test methods cover firewall, application firewall, intrusion detection and intrusion protection systems, and there are tests associated with these. A 2nd or 3rd party test laboratory may offer these tests.

USGv6-V1 NPD Requirements:

– **Network Protection Device Requirements** – see USGv6 profile Section 6.12 [2].

- **Method N1 – FW** – require support of basic firewall capabilities.
- **Method N2 – APFW** – require support of application firewall capabilities.
- **Method N3 – IDS** – require support of intrusion detection capabilities.
- **Method N4 – IDP** – require support of intrusion protection capabilities.

5.4 Combinations and Restrictions

1. There are test methods and scopes of accreditation for conformance, interoperability and network protection.
2. In general, test laboratories may be 1st, 2nd or 3rd party. A 1st party laboratory is associated with the product vendor. A 2nd party laboratory is associated with an acquisition authority. A 3rd party laboratory is independent.
3. 1st, 2nd and 3rd party laboratories may perform one or more conformance testing methods. A 1st party laboratory may offer 3rd party services for conformance testing to other vendors.
4. 2nd and 3rd party laboratories may perform one or more interoperability test methods, or one or more network protection test methods. Any results of interoperability testing by a 1st party laboratory will not be recognized by the USGv6 testing program.
5. A single IPv6 stack may complete the USG testing requirements in multiple test laboratories, considering each laboratory's scope of accreditation for different functional categories.

6 Test Method Validation

An executable test method is the product of a test tool, an abstract test specification, and quality procedures to ensure the tool produces results identical to the test specifications. A test laboratory may use open source, commercial or home grown tools to execute the tests. It is the responsibility of each test laboratory to validate the tools it is using and this procedure and associated records will be part of the on-site assessment leading to accreditation. A system where one or more test laboratories and test tool suppliers collaborate in tool validation, is also acceptable. The system and its participants should be adequately documented.

Validation of conformance and interoperability test systems is functionally equivalent and procedures for these are given in Section 6.1. Validation procedures for Network Protection are discussed in Section 6.2.

6.1 Conformance and Interoperability Test Method Validation

In addition to the method and objective of validation for conformance and interoperability given here, additional requirements are levied for the test capture and report structure.

Method:

Conformance and interoperability executable test methods MUST conform to the latest released abstract test specifications or reference tests. These test methods are validated using the procedures below:

1) Executable test methods per each abstract test specification may be cross-examined by an accredited laboratory, a consortium of accredited laboratories, or a consortium of test method developers with applicable technical knowledge to ensure comparable testing results.
2) Cross-examination Procedure:

   The laboratory may use the "golden node" method in order to obtain a set of results. (Refer to the test capture file and report structure requirements below). This is defined as follows:

   > Two or more instances of a designated IPv6 node subject to the same testing procedures using different test tools shall produce comparable results. This method is ideal for when two or more test tools exist for a given abstract test specification.

   This testing is typically against an open source or freely available implementation. The implementation may not pass 100% however the test procedures and observable results MUST be comparable to the abstract test specification.

   a) If one executable test method exists, a single technical expert may examine the test results.
   b) If multiple executable test methods exist, all test results MUST be comparable and consistent.

   The cross-examiner shall send comments to the laboratory if deviation from the abstract test specification was observed. The laboratory will have ability to comment and action MUST be taken to resolve the comments before test method acceptance. Action may result in a change to the abstract test specification, change in executable test tool or no change necessary. The resolution MUST be a consensus between the cross-examiner and laboratory(s). Alternative technical experts may be requested if consensus can not be achieved.

1) Each test method per abstract test specification may be validated against an approved test tool designed to examine the executable results. This test tool must be developed by an alternative laboratory or facility.

2) All accredited test laboratories MUST participate in interlaboratory comparisons. Refer to Section 7.

Test Capture File Structure:
In order to facilitate comparison of results for the purpose of test method validation, the use of a common file format is extremely convenient. Each test procedure that produces a capture result is saved as a capture dump file in PCAP format [17]. The test capture result files MUST be named using the test number and extension. For example, Test 1.1 should have a corresponding test capture result 1.1.cap file.

Report Structure:
For the purpose of test method validation each executable test method MUST be able to be checked against and reconciled with the related aabstract test specification. One way to do this is to produce a report giving the test number and title along with a Pass or Fail result. The USGv6 test selection tables associated with the test specifications [14] offer a model for this.

Objective: To ensure that the procedures and observable results as listed in the reference tests are packet-for-packet and test-for-test comparable between executable test methods under validation.

6.2 Network Protection Test Method Validation

For the time being test capture and report structure requirements are not levied here. If they are found necessary to the operation of the program they will be identified at the USGv6 testing program website [14].

Method:

1) NPD abstract test suites represent the minimum compliant set. Executable procedures MUST be traceable to these tests.
2) Validation of this set occurs by execution against one or more sample implementation, and reconciliation of the results by two or more independent domain experts.

Objective: To ensure that the results of executing every test in the common reference set are procedurally and syntactically compatible among all laboratories accredited for this method.

7 Proficiency Testing and Interlaboratory Comparisons

Assessment for accreditation requires a laboratory to demonstrate its competence with the test methods in its scope of accreditation. The USGv6 testing program follows ISO/IEC Guide 43 [18] and distinguishes between proficiency testing for test method competence and proficiency testing for interlaboratory comparison.

- In a typical accreditation scheme the assessment occurs prior to initial accreditation and about every two years thereafter. Specific assessments are also conducted whenever a test laboratory adds new methods to its scope of accreditation.

It is a requirement of the USGv6 testing program that the results of testing in any and every accredited laboratory be field-for-field, packet-for-packet and test-for-test comparable. This is established via a system of interlaboratory comparisons. The program of interlaboratory comparisons will be held in the off-years between assessment years. It will involve sampling, not exhaustive testing, and will be scaled to be economically viable, not putting excessive burdens on a test laboratory's resources. The method described below provides each lab an opportunity to determine its equivalence with other labs, and work together to ensure identity of outcomes for identical tests. No proprietary secrets are given away, as the results pertain only to the samples distributed to the participating labs.

Method:

1. For each test method, NIST provides a sample implementation, at the USGv6 testing website (Provide link).
2. NIST also selects sample tests, from the test selection tables.
3. For every test lab that offers a given test method, they MUST complete the testing using the sample provided and make the results available to post on the USGv6 website.
4. The test lab may choose to be identified on the NIST website by an alias if they choose to remain anonymous, however their identity must be known by NIST.
5. Any participating test laboratory may compare the sample results to their own results and report discrepancies.
6. Any discrepancies between results can be discussed, and resolved by consensus on the mailgroup at usgv6-testing.
7. If consensus is not met, then NIST will provide final decision.

Timing:

1. Test Results for inter-laboratory comparison MUST be run and posted to the USGv6 Website for minimum 30 days prior to initial accreditation, and annually thereafter. This gives the usgv6 testing program, the accreditors and the test labs confidence in the equivalence of testing at the start.
2. NIST will host a meeting once a year in the Summer, where any test specification discrepancies, as highlighted by inter-laboratory comparisons or by normal testing operations, are discussed and resolved by consensus. NIST will publish the detailed resolutions of this meeting.
3. At the outset of the program, and 6 months prior to each annual meeting, NIST will prepare samples for testing and publish them at the website. All test labs will participate in the annual inter-laboratory comparison exercise.

8 Terms

Application Firewall a firewall that operates using application data filtering.

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

Firewall A product 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 products.

Interoperability Testing Testing to ensure that two or more USGv6 stacks can interwork and exchange data.

Network Protection Device A product 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.

Router a Node that interconnects subnetworks by packet forwarding.

SDOC: Supplier's Declaration of Conformity.

USG The United States Government, comprising the Federal Agencies.

9 Assessor Qualifications

For the purpose of conducting laboratory assessments the accreditation body will select assessors based on the requirements of ISO 17025, and also the technical requirements applicable to the subject area. The general requirements for assessor competence are drawn from ILAC Guide G11:07/2006 (ILAC Guidelines on Qualifications and Competence of Assessors and Technical Experts" [20]). Technical requirements for USGv6 assessment include:

- At least 4 years experience implementing or interpreting network protocol standards, or testing network protocol implementations.

- PREFERABLY some of that experience involving Internet protocols.

- It may be in practice not possible to find the ideal mix of skills in one candidate. It is ultimately the decision of the accreditor to select assessors based on the best available mix of skills at the time.

10 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] ISO/IEC 17025:1999 General Requirements for the Competence of Calibration and Testing Laboratories. http://www.iso.org/iso/

[4] ISO/IEC 17011:2004 Conformity Assessment – General Requirements for accreditation bodies accrediting conformity assessment bodies. http://www.iso.org/iso/

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

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

[7] IPv6 Ready Logo Program, IPv6 Forum, Erica Johnson and Yannick Pouffary, November 2007. http://www.ipv6forum.com/dl/white/IPv6_Ready_Logo_White_Paper_Final.pdf

[8] Department of Defense Internet Protocol Version 6 Generic Test Plan, version 2, Captain Richard J. Duncan, Joint Interoperability Test Command, Fort Huachuca, Arizona, September 2006. http://jitc.fhu.disa.mil/adv_ip/register/docs/dodipv6gpv3_aug07.pdf

[9] Department of Defense, Internet Protocol Version 6 Information Assurance Test Plan, National Security Agency, Draft, FOUO, undated.

[10] 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/

[11] Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results, Barry N. Taylor and Chris E. Kuyatt, U.S. Department of Commerce, National Institute of Standards and Technology, NIST Technical Note 1297, 1994. http://physics.nist.gov/Pubs/guidelines/TN1297/tn1297s.pdf

[12] A Strategy for Full Scale IPv6 Adoption Version 2.0, Federal CIO Council, Jim McCabe, June 20, 2008.

[13] Key words for use in RFCs to Indicate Requirement Levels, S. Bradner, RFC 2119, IETF Best Current Practice, March 1997. http://www.ietf.org/rfc/rfc2119.txt

14]USGv6 Testing Program website http://www.antd.nist.gov/usgv6/testing.html.

---

[15] DoD Unified Capabilities Requirements, http://jitc.fhu.disa.mil/apl/index.html.

[16] The International Laboratory Accreditation Cooperation (ILAC) http://www.ilac.org.

[17] The tcpdump/libpcap website. http://www.tcpdump.org.

[18] ISO/IEC Guide 43 Proficiency testing for interlaboratory comparisons, parts 1 and 2. http://www.iso.org/iso/.

[19] NIST SP 500-281 USGv6: Management, Processes and Stakeholders, Stephen Nightingale and Doug Montgomery, National Institute of Standards and Technology, (to be published).

[20] ILAC Guide G11:07/2006, ILAC Guidelines on Qualifications and Competence of Assessors and Technical Experts", The International Laboratory Accreditation Cooperation, http://www.ilac.org.