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

Special Publication 500-267

A Profile for IPv6 in the U.S. Government – Version 1.0

Recommendations of the National Institute of Standards and Technology

Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson

NIST Special Publication 500-267

A Profile for IPv6 in the U.S. Government – Version 1.0

Recommendations of the National Institute of Standards and Technology

Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson

Information Technology Laboratory

Attn: USGv6 Project
National Institute of Standards and Technology
Gaithersburg, MD 20899-8920
usgv6-project@antd.nist.gov

July 2008

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology

James M. Turner, Deputy 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 500-267
NIST SP 500-267, 76 pages, (July 2008)

Acknowledgements

The authors would like to acknowledge the members of the Federal Government IPv6 Working Group for their keen and insightful assistance throughout the development of the document, and the members of the wider Federal Government who offered useful technical and editorial comments. During the investigation, development and initial review of this document, many people and organizations were consulted and offered technical and procedural insights. Of particular note are the more than 500 comments from more than 50 sources in Government and industry that we received during the two public comment periods on the earlier drafts. Continuing dialogue among members of the Federal IPv6 Working Group, in particular Pete Tseronis, Carol Bales, Kshemendra Paul and Roxie Murphy, has helped significantly to shape this technical profile, and several potential policy issues surrounding it.

This profile has undergone several iterations of harmonization with the DoD Standard Profiles for IPv6 Capable Products. We would like to acknowledge the fruitful input and discussions with the participants in the DISR IPv6 Standards Working Group, in particular: Ralph Liguori, Ed Jankiewicz, Jeremy Duncan and Kris Strance. Both profiling efforts have benefited from these exchanges.

Planning for the compliance testing program to support this profile benefited greatly from all the participants who attended two public workshops on the topic. In particular representatives of the IPv6Ready Logo program (Erica Johnson and Tim Winters), the Joint Interoperability Test Command (JITC) IPv6 test program (Jeremy Duncan), and the TAHI project (Hiroshi Miyata and Chih-Cheng Tsao), among others, helped us understand existing efforts and how they might be leveraged.

We also appreciate the invaluable assistance of colleagues here at NIST, including Tim Polk, William MacGregor, Gordon Gillerman, Darrin Santay, Joyce Malones, Karen Scarfone and Tim Grance, who reviewed drafts of this document and/or contributed to its technical content.

Table of Contents

List of Appendices

Executive Summary

The suite of protocols commonly known as Internet Protocol version 6 (IPv6) has been under design and development within the Internet Engineering Task Force (IETF) and the Internet industry for over 10 years [1]. This industry led effort was initiated in the early 1990's to address perceived scaling problems in the Internet's addressing and routing architectures. Today stable standards exist for basic IPv6 functionality. Commercial implementations and services based upon these specifications are emerging, and vendors and large user groups are pursuing significant product development and technology adoption plans for IPv6.

The United States Government (USG) is one such large user group, and most Agencies across the government are beginning to plan for the adoption and deployment of IPv6 technologies in response to: mission driven technical and economic assessments of the technology [161]; broad Government policies [166] [167] [170]; the product release plans of major vendors; and, the plans and actions of other organizations on the Internet.

Given the prevalence and importance of Internet technologies in Federal information technology (IT) systems today and the nature and scale of both the opportunities and risks associated with significant deployments of new networking technologies, NIST was tasked [166] with an effort to evaluate the need for additional standards and testing infrastructures to support USG plans for IPv6 adoption. As part of this effort we examined the state of IPv6 specifications published by the IETF; the present state of maturity of commercial implementations; the evolving Department of Defense IPv6 profile [152] and product testing program [153]; and, national and international profiles and testing programs driven by the vendor communities [151][176] [178]. The objective of this analysis was to determine: (a) where significant technical gaps exist in the near term technical landscape for IPv6 deployment; (b) what, if any, additional standards and testing infrastructures and processes are needed to assist Federal agencies to achieve safe and economical adoption of this new technology.

Our findings from these efforts include:

1. A subset of network layer IPv6 specifications has stabilized and operationally viable commercial implementations of these specifications are becoming available. Agency budgeting, procurement and deployment planning, could benefit from a common identification and definition of such IPv6 capabilities.

2. While significant commercial implementations have and continue to emerge, broad vendor product lines are currently at varying levels of maturity and completeness. Until there is time for significant market forces to effectively define *de facto* standard levels of completeness and correctness, product testing services are likely needed to ensure the confidence and to protect the investment of early IPv6 adopters.

3. The current state of IPv6 security and network protection technologies and operational knowledge lags behind that of IPv4 and the existing Internet. Additional efforts are required to "raise the bar" in these areas to ensure the safety of IPv6 deployments in operational Federal information technology systems.

4. While, in general, the proliferation of technology standards is to be avoided, the existing DoD and industry profiling and testing efforts are currently not well suited in content, or governance, for the perceived requirements of the USG as a whole. In the near term, the broad requirements of civilian agencies can be better met by a distinct profile and testing program. In the long term we are committed to the harmonization and convergence of these efforts into broader, international

collaborative user/vendor profiling and testing initiatives in which the technical and process requirements of the USG can be fully accommodated.

5. Some key IPv6 design issues remain unresolved. As the USG begins to undertake significant operational deployments and investments in IPv6 technology, additional efforts are warranted to ensure that the eventual resolution of these design issues remains consistent with USG requirements and investments.

This document recommends a technology acquisition profile for common IPv6 devices to be procured and deployed in operational USG IT systems. It is intended to address several aspects of findings 1, 3, 4 and 5 above and will be augmented by additional documents and activities including:

- Development of guidance for the secure deployment of IPv6 to further address findings 3 and 5.
- Development of an open public testing program for IPv6 technologies [160] to further address finding 2.

This standards profile is meant to: (a) define a simple taxonomy of common network devices; (b) define their minimal mandatory IPv6 capabilities and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans; and, (c) provide the technical basis upon which future USG polices can be defined. The scope of the device taxonomy and the selection of mandatory capabilities and identified options are purposefully conservative in some ways; defining systems and capabilities that are thought to be of common utility to the USG as a whole. In other ways, this profile "raises the bar" for some areas of IPv6 technology that are thought vital to protect the current and future security of Federal IT systems and to protect the economic investment of early adopters.

The profile and associated test program will provide the technical basis for the definition and demonstration of "IPv6 Capable" and "IPv6 Compliant" for USG procurements. The profile is forward looking and as such we recommend that users and vendors be given 24 months after publication of the latest version to respond to any new technical requirements.

Note that it is fully expected that agencies would further augment and/or modify these specifications to meet the requirements of specific IT system procurements and policies. In particular, the profile defines certain significant configuration choices that must be made and specified to fully articulate the set of mandatory requirements for each class and/or instance of device.

1. Introduction

This profile has been prepared for use by Federal agencies. It can be used by other organizations on a voluntary basis and is not subject to copyright. If used in other (non-USG) contexts, accurate attribution/citation is desired so as to avoid confusion.

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 this profile to 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 Purpose and Scope

This publication seeks to assist Federal agencies in formulating plans for the acquisition of IPv6 technologies. To achieve this, we define a standards profile for IPv6 in the USG that is intended to be applicable to all future uses of IPv6 in non-classified, non-national security [157] federal IT systems. The standards profile is meant to: (a) define a simple taxonomy of common network devices; (b) define their minimal mandatory IPv6 capabilities and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans; and, (c) provide the technical basis upon which future USG polices can be defined. A profile in this context is a compendium of protocol specifications, with normativity statements (MUST, SHOULD, MAY, etc) highlighted or strengthened. Most specifications identified are published by the IETF, though USG, DoD, IEEE, ISO/IEC and other organizations publications are not precluded. Common use of the word *specification* in this profile implies no particular publisher.

The profile is meant to be a landmark to guide the acquisition of significant new IPv6 capabilities for operational Federal IT systems. No attempt has been made to grandfather existing early implementations, or cover potential non-production level uses of the technology in test-beds, pilots, etc. In summary, the profile is meant as a strategic planning guide for future acquisitions and as such appropriate lead times must be allowed between its publication and its use in procurements. Other uses of this profile, without agency specific refinement, are not recommended. In particular, this acquisition profile should not be thought of as a deployment or transition guide or as suggesting operational requirements for USG networks. Guidance and policies covering these other, post acquisition, issues are outside the scope of this profile.

The scope of the device taxonomy and the selection of mandatory capabilities and identified options are purposefully conservative in some ways; defining systems and capabilities that are thought to be of common utility to the USG as a whole. In other ways, this profile “raises the bar” for some areas of IPv6 technology that are thought vital to protect the current and future security of Federal IT systems and to protect the economic investment of early adopters.

It is fully expected that agencies will further augment and/or modify these specifications to meet their own requirements when making IT system specifications and policies. To assist in such a process, this profile defines a number of configuration options that a user (e.g., acquisition authority) must specify to fully articulate the IPv6 capability requirements of specific procurements. But, beyond selection among configuration options, agencies with specific mission requirements might substantially modify the conformance requirements of the technical profile. Where this is done, care needs to be taken to insure that systems that meet the new, derivative requirements remain interoperable with systems that conform to this profile.