NIST Special Publication 500-267B
Revision 1

USGv6 Profile

Doug Montgomery
Mark Carson
Timothy Winters
Michayla Newcombe
Timothy Carlin

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

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

NIST Special Publication 500-267B
Revision 1

USGv6 Profile

Doug Montgomery
Mark Carson
Information Technology Laboratory
National Institute of Standards and Technology

Timothy Winters
Michayla Newcombe
Timothy Carlin
InterOperability Laboratory
University of New Hampshire

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Br1

February 2020

DRAFT

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

DRAFT

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 document reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

DISCLAIMER

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes standards research in support of the Federal IPv6 Program. Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

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.

DRAFT

National Institute of Standards and Technology Special Publication 500-267Br1
Natl. Inst. Stand. Technol. Spec. Publ. 500-267Br1, 24 pages (Month February 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Br1

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

Executive Summary

The Office of Management and Budget (OMB) directed [OMB-M05-22, OMB-IPv6] the National Institute of Standards and Technology (NIST) to develop the technical infrastructure (standards and testing) necessary to support wide scale adoption of IPv6 in the US Government (USG). In response, NIST developed the initial USGv6 Profile [SP500-267] to assist agencies in the development of acquisition requirements for IPv6 products and the USGv6 Test Program [SP500-281] to provide the means to assess product compliance to such requirements. In subsequent years additional USG policies [OMB-IPv6, FAR-2005-041, OMB-M17-06] have referenced various aspects of the USGv6 program [USGv6-Web].

In 2019 NIST undertook a significant revision of the USGv6 Profile and Test Program to update their technical specifications and to streamline their use in Federal procurement processes. The USGv6 Program was developed collaboratively with, and aligned to, industry led product test programs [IPv6-Ready, NIST-IPv6F].

This new profile provides significant revisions to the original USGv6 profile, including:

1. Separating the definition of general IPv6 capability definitions from their use in specific acquisition programs to permit other user groups to re-use the capability profiles and their aligned product testing programs. The NIST IPv6 Profile provides these general capability definitions. This revised USGv6 Profile is specified as a derivative of the base NIST IPv6 profile.

2. Updating the set of Internet Engineering Task Force (IETF) specifications that form the basis for the profile to their latest published versions. In particular, this revision, adopts the most recent, Internet standard, versions of the base IPv6 specifications.

3. Adding new specifications for important IPv6 capabilities that have been developed since the publication of the first profile.
    a. Highlights of these additions include technologies to support emerging use cases such as Internet of Things, and new forms of IPv6 transition technologies that focus on legacy support of IPv4 in IPv6 native networks.

4. Adding the ability to specify requirements for functionality necessary to support "IPv6-only" environments and better support for specification and test of IPv6 capable applications.

5. Removing specifications for IPv6 capabilities included in the first version of the profile but that have since failed to achieve significant support in commercial products and network deployments.

This USGv6 Profile is tightly integrated with the USGv6 Test Program, which provides standardized methods for testing products, accrediting independent laboratories and reporting product capabilities.

This profile is not subject to copyright and its reuse, either in its entirety, or in derivative works, is encouraged.

DRAFT

Abstract

This profile establishes a basic taxonomy of IPv6 capabilities, defined in terms of IETF specifications, resulting in specific capability labels for common network functions and usage scenarios. The profile maps each such labeled capability to one or more specific technical specifications, or parts of specifications. Each labeled capability adopts by reference the normative requirements of the cited specifications. In rare cases the profile may augment or modify the normative requirements of a base specification. The defined capability labels effectively form a vocabulary for expressing IPv6 requirements for, and documenting the IPv6 capabilities of, specific products. It is expected that this profile, when combined with the USGv6 Test Program, can facilitate the efficient adoption of IPv6 technologies in Federal information systems.

Keywords

Internet Protocol version 6; IPv6; standards profile; acquisition; USGv6, USGv6-r1, NISTv6; NISTv6-r1, USGv6 Test Program.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

Table of Contents

1. Introduction 1

1.1. Audience 2

1.2. Profiling IPv6 Capabilities 2

1.3. Profile Structure: Functional Roles and Capability Groups 3

1.4. Profiling Products and Implementations. 3

2. Profile Scope, Applicability and Conventions 3

2.1. Scope and Applicability 3

2.2. Life Cycles and Change Management. 3

2.3. Statements of Requirements Levels 3

2.4. Profile Capabilities Table. 3

2.5. Capability Summary Strings. 4

2.6. Conformance, Testing and Reporting. 4

3. Selection of IPv6 Capabilities 6

3.1. IPv6-Only Capabilities 6

3.1.1. Selecting IPv6-Only Capabilities 6

3.2. Host Capabilities 7

3.2.1. Selecting Host Capabilities 7

3.3. Router Capabilities 8

3.3.1. Selecting Router Capabilities 8

3.4. Network Protection Product Capabilities 10

3.4.1. Selecting Network Protection Product Capabilities 10

3.5. Switch Capabilities 11

3.5.1. Selecting Switch Capabilities 11

3.6. Application and Services Capabilities 12

3.6.1. Selecting Application and Services Capabilities 12

4. Technical Definition of IPv6 Capabilities 13

4.1. IPv6-Only Capabilities 13

4.2. Basic Capabilities 13

4.3. Routing Capabilities 13

4.4. Quality of Service Capabilities 13

4.5. Transition Mechanism Capabilities 13

4.6. Link Specific Capabilities 13

4.7. Addressing Capabilities 13

4.8. Security Capabilities 13

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

4.9. Network Management Capabilities **13**
4.10. Multicast Capabilities **13**
4.11. Network Support Capabilities **14**
4.12. Application and Service Capabilities **14**
4.13. Switch Capabilities **14**
4.14. Network Protection Product Capabilities **14**
5. Profile Usage Guidance and Examples ***15***
Acknowledgments ***16***
Reference ***17***
Appendix A: Listing of USGv6-r1 Capability Templates ***19***
USGv6-r1: Host Capabilities: 19
USGv6-r1: Router Capabilities: 20
USGv6-r1: App-Serv | Switch | NPP Capabilities: 22
Appendix B: Change Log ***23***
Revision 1 – February 2020 23

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

1. Introduction

The Office of Management and Budget (OMB) directed [OMB-M05-22, OMB-IPv6] the National Institute of Standards and Technology (NIST) to develop the technical infrastructure (standards and testing) necessary to support wide scale adoption of IPv6 in the US Government (USG). In response, NIST developed the initial USGv6 Profile [SP500-267] to assist agencies in the development of acquisition requirements for IPv6 products and the USGv6 Test Program [SP500-281] to provide the means to assess product compliance to such requirements. In subsequent years additional USG policies [OMB-IPv6, FAR-2005-041, OMB-M17-06] have referenced various aspects of the USGv6 program [USGv6-Web].

In 2020 NIST undertook a significant revision of the USGv6 Profile and Test Program to update their technical specifications and to streamline their use in Federal procurement processes. The USGv6 Program was developed collaboratively with, and aligned to, industry led product test programs [IPv6-Ready, NIST-IPv6F].

This new profile provides significant revisions to the original USGv6 profile, including:

1. Separating the definition of general IPv6 capability definitions from their use in specific acquisition programs to permit other user groups to re-use the capability profiles and their aligned product testing programs. The NIST IPv6 Profile provides these general capability definitions. This revised USGv6 Profile is specified as a derivative of the base NIST IPv6 profile.

2. Updating the set of Internet Engineering Task Force (IETF) specifications that form the basis for the profile to their latest published versions. In particular, this revision, adopts the most recent, Internet standard, versions of the base IPv6 specifications.

3. Adding new specifications for important IPv6 capabilities that have been developed since the publication of the first profile.
    a. Highlights of these additions include technologies to support emerging use cases such as Internet of Things, and new forms of IPv6 transition technologies that focus on legacy support of IPv4 in IPv6 native networks.

4. Adding the ability to specify requirements for functionality necessary to support "IPv6-only" environments and better support for specification and test of IPv6 capable applications.

5. Removing specifications for IPv6 capabilities included in the first version of the profile but that have since failed to achieve significant support in commercial products and network deployments.

This USGv6 Profile is tightly integrated with the USGv6 Test Program, which provides standardized methods for testing products, accrediting independent laboratories and reporting product capabilities.

This USGv6 profile is specified as a derivative of a general NIST IPv6 capabilities profile. That is, this profile only describes changes and additions to the general capabilities profile necessary for support of USG acquisition programs. Any use of this USGv6 profile will require reference to and understanding of the base general capabilities profile:

- **"NIST IPv6 Profile", NIST Special Publication 500-267A revision 1, National Institute of Standards and Technology, February 2020, https://doi.org/10.6028/NIST.SP.500-267Ar1**

- The abbreviation **"NISTv6-r1"** is used to identify the general capability profile in various usages.

All uses of this USGv6 Profile should cite:

- **"USGv6 Profile", NIST Special Publication 500-267B revision 1, National Institute of Standards and Technology, February 2020, https://doi.org/10.6028/NIST.SP.500-267Br1**

- The abbreviation **"USGv6-r1"** is used to identify this profile in various usages.

This USGv6 Profile is not subject to copyright and its reuse, either in its entirety, or in derivative works is encouraged.

All questions and comments about this profile should be addressed to: usgv6-program@nist.gov.

1.1. Audience

See section 1.1 of the NISTv6-r1 profile.

1.2. Profiling IPv6 Capabilities

See section 1.2 of the NISTv6-r1 profile.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

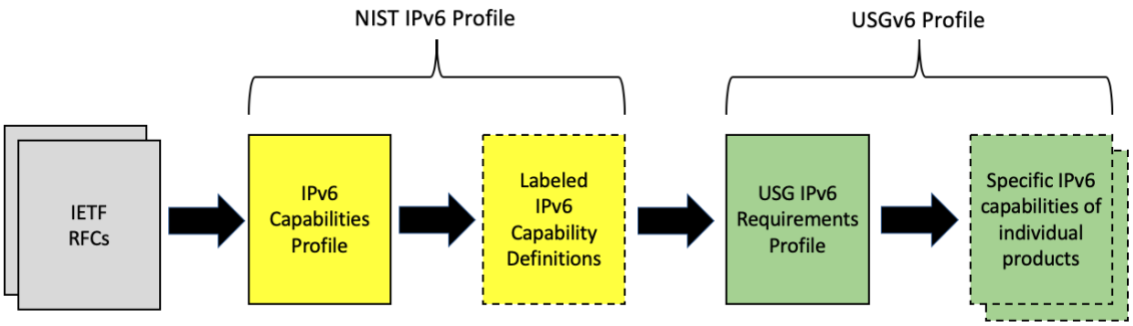

Figure 1 USGv6 usage scenario.

This USGv6 Profile is an instance of a specific user group profile defined in terms of the general NIST IPv6 capabilities profile. For USG use, requirements specifications and product testing requirements MUST reference this USGv6-r1 profile.

1.3. Profile Structure: Functional Roles and Capability Groups

See section 1.3 of the NISTv6-r1 profile.

1.4. Profiling Products and Implementations.

See section 1.4 of the NISTv6-r1 profile.

2. Profile Scope, Applicability and Conventions

See section 2 of the NISTv6-r1 profile.

2.1. Scope and Applicability

See section 2.1 of the NISTv6-r1 profile.

2.2. Life Cycles and Change Management.

See section 2.2 of the NISTv6-r1 profile.

2.3. Statements of Requirements Levels

See section 2.3 of the NISTv6-r1 profile.

2.4. Profile Capabilities Table.

The USGv6 Capabilities Table (UCT) provides a concise tabular summary of the technical requirements of this profile. For ease of reference, the UCT is maintained as supplemental information to this profile and provided in a separate document. Readers are encouraged to access and review the UCT as an adjunct to this document.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

- **USGv6-r1 Capabilities Table - https://doi.org/10.6028/NIST.SP.500-267Br1s**

See section 2.4 of the NISTv6-r1 profile for an explanation of the basic syntax and semantics used in the UCT.

The capability selection guidance in this profile is primarily derived from two sources.

- The NISTv6-r1 profile which follows the IETF *IPv6 Node Requirements* specification [RFC8504]. All specifications that are indicated as MUST in RFC 8504 are marked "**M**" in the UCT.
- This profile augments the capability selection guidance provided in the NISTv6-r1 profile with specific recommendations for USG acquisitions. Sections 3 and 4 of this profile only document these differences.

While the UCT is a complete tabular summary of the normative content of this profile, readers are encouraged to consult section 3 for guidance on how to interpret the UCT for the purpose of developing requirement statements and to consult section 4 for guidance on interpreting the UCT for the expression of the capabilities of individual products.

2.5. Capability Summary Strings.

See section 2.3 of the NISTv6-r1 profile for the specification of the syntax and semantics of *Capability Summary Strings (CSS)* used in this profile.

CCS derived from this specification with use **USGv6-r1** for the profile name. The following is an example of a specific CSS based upon this profile:

> **Example-Desktop-PC = USGv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + [DHCP-Client | SLAAC] + Link=Ethernet**

See section 5 for numerous example CSS specifications based upon this profile.

2.6. Conformance, Testing and Reporting.

Section 2.6 of the NISTv6-r1 profile describes the general topic of conformance to profile requirements, testing and reporting of product capabilities.

The USGv6 Program was explicitly developed to provide the technical basis for government wide IPv6 acquisition initiatives. The USGv6 Profile and USGv6 Test Program are referenced in several USG IT policies [OMB-IPv6, FAR-2005-041, OMB-M17-06].

When used to support the acquisition of USG networked information technology and services, technical requirements for the IPv6 capabilities of product offerings should be made in terms traceable to this USGv6 Profile. Such requirements shall be expressed as USGv6 Capability Summary Strings (CSS).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

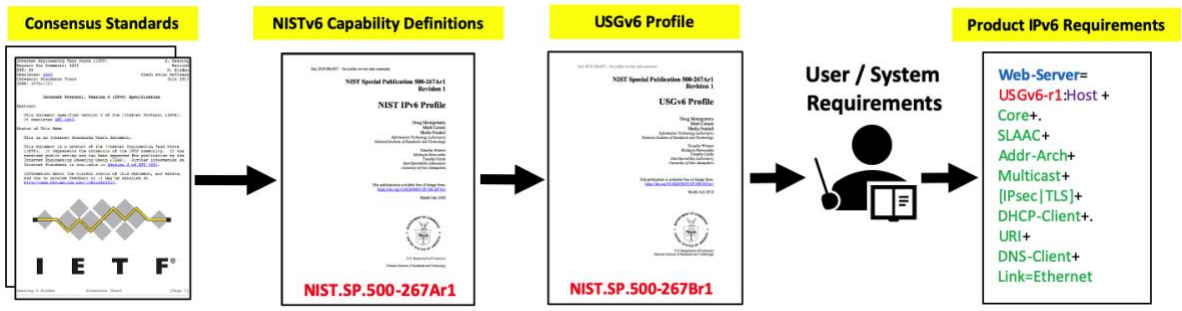

Figure 2 Traceability of USGv6 CSS Requirements.

When used in conjunction with USG acquisitions, vendor claims of conformance to specified requirements and / or general documentation of product IPv6 technical capabilities shall be made through the USGv6 Test Program. This program establishes a system of accredited test laboratories that execute standardized open test suites for testing conformance to the capabilities and underlying base standards defined in the USGv6 Profile. All such statements of the USGv6 capabilities supported by a given product shall be documented through the USGv6 Suppliers Declaration of Conformity (SDOC). USGv6 SDOCs provide a standardized format to document the USGv6 capabilities supported by a specific product or set of products and provides traceability back to the accredited laboratory that conducted the tests. The SDOC also summaries test results in one or more Capability Summary Strings.

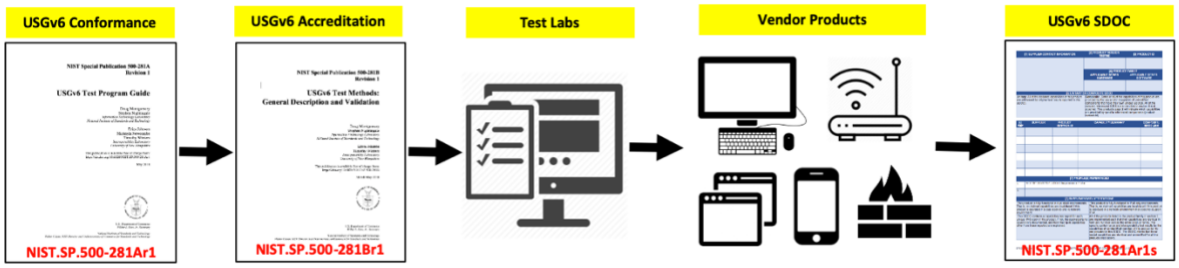

Figure 3 Traceability of USGv6 Suppliers Declarations of Conformity

The *USGv6 Test Program Guide* [SP500-281Ar1] documents the basic components, concepts and processes necessary to claim conformance to USGv6 requirements. The *USGv6 Test Methods: General Description and Validation* [SP500-281Br1] specification defines the processes for accreditation and quality control for USGv6 test laboratories.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

3. Selection of IPv6 Capabilities

Note that this section only specifies the differences in selection guidance between the USGv6 Profile and the general NIST IPv6 Profile. To fully understand the detailed technical definition of the capabilities below, see the corresponding entries the NISTv6 Profile, the USGv6-r1 Capabilities Table (section 2.4) and section 4 Technical Definition of IPv6 Capabilities. See section 5 for example CSS that incorporate these capabilities.

3.1. IPv6-Only Capabilities

See section 3.1 of the NISTv6-r1 profile. In order to support broad USG IPv6 initiatives, it is recommended that all requirement specifications based upon this profile include the **IPv6-Only** capability. See the UCT and section 4.1 for a complete listing and technical definition of these capabilities.

See section 3.1 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:Host Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [M] – **IPv6-Only** - support for full product functionality on an IPv6-only network
USGv6-r1:Router Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [M] – **IPv6-Only** - support for full product functionality on an IPv6-only network
USGv6-r1:NPP Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [M] – **IPv6-Only** - support for full product functionality on an IPv6-only network
USGv6-r1:Switch Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [M] – **IPv6-Only** - support for full product functionality on an IPv6-only network
USGv6-r1:App-Serv Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [M] – **IPv6-Only** - support for full product functionality on an IPv6-only network

3.1.1. Selecting IPv6-Only Capabilities

See section 3.1.1 of the NISTv6-r1 profile. Users of this profile are recommended to require all products to be capable of operating in IPv6-only environments.

- When the **IPv6-Only** capability is indicated, it is implied that all other specified capabilities of a product, must operate in IPv6-only environments.

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

3.2. Host Capabilities

This section provides a template for the specification of Host IPv6 requirements. The USGv6-r1 Host capabilities are the same as those of the NISTv6-r1 profile with the following modifications. See the UCT and section 4 for a complete listing and technical definition of these capabilities.

See section 3.2 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:Host Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section 4.2
  - [O:1=[SLAAC | DHCP-Client]] - **SLAAC** - support for stateless global address auto-configuration.
  - [O:1=[SLAAC | DHCP-Client]] - **DHCP-Client** - support for stateful (DHCP) address auto-configuration.
- **Security Capabilities** - see section 4.8
  - [O:1=[IPsec | TLS]] - **IPsec** - support for the IP security architecture.
  - [O:1=[IPsec | TLS]] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [X] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [X] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [X] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.

3.2.1. Selecting Host Capabilities

See section 3.2.1 of the NISTv6-r1 profile. The following additional guidance is provided for selecting capabilities from this section.

- **IPv6-Only** capabilities are recommended to be mandatory in all Host implementations.
- It is recommended that all Host implementations support one form of automated address configuration. Either **SLAAC** or **DHCP-Client** capabilities are recommended for all Host implementations.
- It is recommended that all Host implementations support the capability for secure communication. Either **IPsec** or **TLS** capabilities are recommended for all Host implementations.
- The IPsec algorithms defined in the **IPsec-IoT**, **IPsec-CHACHA**, **IPsec-SHA-512** are not recommended for use in USG systems.
- For supporting the most common transition mechanism it's recommended that DNS servers support **DNS64**.

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

3.3. Router Capabilities

This section provides a template for the specification of Router IPv6 requirements. The USGv6-r1 Router capabilities are the same as those of the NISTv6-r1 profile with the following modifications. See the UCT and section 4 for a complete listing and technical definition of these capabilities.

See section 3.3 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:Router Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Security Capabilities** - see section 4.8
  - [O:1=[IPsec | TLS]] - **IPsec** - support for the IP security architecture.
  - [O:1=[IPsec | TLS]] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [X] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [X] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [X] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.
  - [X] - **IPsec-IoT-VPN** - support for IoT Cryptographic Algorithms in gateways.
  - [X] - **IPsec-CHACHA-VPN** - support for ChaCha20 Cryptographic Algorithms in gateways.
  - [X] - **IPsec-SHA-512-VPN** - support for SHA-512 Cryptographic Algorithms in gateways.
- **Network Management Capabilities** - see section 4.9
  - [O:1=[SNMP | NETCONF]] - **SNMP** - support for simple network management protocol.
  - [O:1=[SNMP | NETCONF]] - **NETCONF** - support for network configuration functions.
- **Quality of Service Capabilities** - see section 4.4
  - [M] - **DiffServ** - support for Differentiated Services capabilities.

3.3.1. Selecting Router Capabilities

See section 3.3.1 of the NISTv6-r1 profile. The following additional guidance is provided for selecting capabilities from this section.

- **IPv6-Only** capabilities are recommended to be mandatory in all Router implementations.
- It is recommended that all Router implementations support the capability for secure communication. Either **IPsec** or **TLS** capabilities are recommended for all Router implementations.
- The IPsec algorithms defined in the **IPsec-IoT**, **IPsec-IoT-VPN**, **IPsec-CHACHA**, **IPsec-CHACHA-VPN, IPsec-SHA-512, IPsec-SHA-512-VPN** are not recommended for use in USG systems.
- It is recommended that all Router implementations support some capability for remote management. Either **SNMP** or **NETCONF** capabilities are recommended for all Router implementations.
- Support of basic **DiffServ** QoS capabilities is recommended for all Router implementations.

DRAFT

- For supporting the most common transition mechanism it's recommended that DNS servers support NAT64.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

3.4. Network Protection Product Capabilities

This section provides a template for the specification of IPv6 requirements for Network Protection Products. The USGv6-r1 NPP capabilities are the same as those of the NISTv6-r1 profile with the following modifications. See the UCT and section 4 for a complete listing and technical definition of these capabilities.

See section 3.4 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:NPP (Network Protection Product) Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.

3.4.1. Selecting Network Protection Product Capabilities

See section 3.4.1 of the NISTv6-r1 profile. The following additional guidance is provided for selecting capabilities from this section.

- **IPv6-Only** capabilities are recommended to be mandatory in all Network Protection Product implementations.

DRAFT

3.5. Switch Capabilities

This section provides a template for the specification of IPv6 requirements for Switch Products. The USGv6-r1 Switch capabilities are the same as those of the NISTv6-r1 profile with the following modifications. See the UCT and section 4 for a complete listing and technical definition of these capabilities.

See section 3.5 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:Switch Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [M]- **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Switch Capabilities** - see section 4.13
  - [**M**] - **RA-Guard** - support for RA Guard at Layer 2.

3.5.1. Selecting Switch Capabilities

See section 3.5.1 of the NISTv6-r1 profile. The following additional guidance is provided for selecting capabilities from this section.

- **IPv6-Only** capabilities are recommended to be mandatory in all Switch Product implementations.
- It is recommended that all switches support **RA-Guard** for security of the network.
- If a user is deploying DHCPv6, **DHCPv6-Guard** is recommended for security.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

3.6. Application and Services Capabilities

This section provides a template for the specification of IPv6 requirements for Application and Network Service Products. The USGv6-r1 App-Serv capabilities are the same as those of the NISTv6-r1 profile with the following modifications. See the UCT and section 4.12 for a complete listing and technical definition of these capabilities.

See section 3.6 of the NISTv6-r1 profile with the following modifications.

USGv6-r1:App-Serv (Application and Services) Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.

3.6.1. Selecting Application and Services Capabilities

See section 3.6 of the NISTv6-r1 profile. The following additional guidance is provided for selecting capabilities from this section.

- **IPv6-Only** capabilities are recommended to be mandatory in all Switch Product implementations.
- When combined with the **IPv6-Only** capability requirement, the application or service must be fully functional on a network without IPv4 services.

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

4. Technical Definition of IPv6 Capabilities

This profile makes no changes to the technical definitions of capabilities as defined in the NIST IPv6 profile. See section 4 of the NISTv6-r1 profile for a discussion of capabilities definitions organized by functional groups.

4.1. IPv6-Only Capabilities

See section 4.1 of the NISTv6-r1 profile.

4.2. Basic Capabilities

See section 4.2 of the NISTv6-r1 profile.

4.3. Routing Capabilities

See section 4.3 of the NISTv6-r1 profile.

4.4. Quality of Service Capabilities

See section 4.4 of the NISTv6-r1 profile.

4.5. Transition Mechanism Capabilities

See section 4.5 of the NISTv6-r1 profile.

4.6. Link Specific Capabilities

See section 4.6 of the NISTv6-r1 profile.

4.7. Addressing Capabilities

See section 4.7 of the NISTv6-r1 profile.

4.8. Security Capabilities

See section 4.8 of the NISTv6-r1 profile.

4.9. Network Management Capabilities

See section 4.9 of the NISTv6-r1 profile.

4.10. Multicast Capabilities

See section 4.10 of the NISTv6-r1 profile.

DRAFT

4.11. Network Support Capabilities

See section 4.11 of the NISTv6-r1 profile.

4.12. Application and Service Capabilities

See section 4.12 of the NISTv6-r1 profile.

4.13. Switch Capabilities

See section 4.13 of the NISTv6-r1 profile.

4.14. Network Protection Product Capabilities

See section 4.14 of the NISTv6-r1 profile.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

5. Profile Usage Guidance and Examples

This appendix provides guidance and examples to illustrate the expected usage of this profile. This profile is intended to be a strategic document for USG IT planning and acquisition officials that provides a technical basis for conveying technical requirements to IPv6 product vendors. Likewise, vendors can use the profile to unambiguously convey detailed information about the IPv6 capabilities of their product offerings.

The primary means to facilitate this exchange of information between users and vendors is through Capability Summary Strings (CSS) (see section 2.5). As noted, CSS can be used both as statements of IPv6 requirements from purchasers and statements of product IPv6 capabilities from vendors.

Section 5 of the NISTv6-r1 profile provides numerous examples of CSS specifications for various classes of products. All of those examples are applicable to the USGv6 profile simply by changing the profile reference in each CSS to **USGv6-r1.**

Typically, CSS strings are used to as requirements statements for specific purchases or product capability reports of specific products. CSS can also be used to express more general acquisition policies such as establishing the minimal requirements for products of certain classes. In such uses, the CSS can serve a template from which more explicit requirement statements can be derived. Some examples of such CSS uses are below.

- **USGv6-Capable-Host = USGv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + [SLAAC|DHCP-Client] + [IPsec|TLS] + Link=Ethernet**
- **USGv6-Capable-Router = USGv6-r1:Router + IPv6-Only + Core + Addr-Arch + Multicast + SLAAC + [IPsec|TLS] + [SNMP|NETCONF] + [CE-Router|OSPF|IS-IS|BGP] + DiffServ + [Tunneling-IP|Tunneling-UDP] + Link=Ethernet**
- **USGv6-Capable-Switch = USGv6-r1:Switch + IPv6-Only + DHCPv6-Guard + RA-Guard + MLD-Snooping + Link=Ethernet**
- **USGv6-Capable-Application = USGv6-r1:App-Serv + IPv6-Only + App-Serv=[TBD]**

By providing a convenient way to select and articulate sets of requirements, the profile facilitates the description of a vast array of distinct product requirements and configurations. While we suspect that there will be a few bundled sets of requirements that will be used quite commonly, we also believe that there is tremendous variance in the packaging of feature sets in commercial products and attempts to overly “standardize” such configurations may not afford the flexibility needed.

DRAFT

Acknowledgments

The original profile from which this specification has been adapted had considerable input from Stephen Nightingale and Sheila Frankel who have since retired from NIST. Numerous others from industry and large user groups had inputs that contributed to the original effort.

This revised profile benefited from substantive review and input from several reviewers during three rounds of public comments. This published version reflects numerous changes made in response to the over 200 technical comments submitted during these review periods.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

Reference

Citation	Reference
[FAR-2005-041]	"*Federal Acquisition Regulation: FAR Case 2005-041, Internet Protocol Version 6 (IPv6)*", December 2009. Online at: https://www.federalregister.gov/documents/2009/12/10/E9-28931/federal-acquisition-regulation-far-case-2005-041-internet-protocol-version-6-ipv6
[IPv6-Ready]	"*IPv6 Ready Logo Program*", The IPv6 Forum, ongoing. Online at: https://www.ipv6ready.org/
[NIST-IPv6F]	"*Grant of Use Rights: IPv6 Test Specifications*", MOU between NIST and the IPv6 Forum, April 2008. Online at: https://www.nist.gov/document/ipv6forumnistmoupdf
[OMB-IPv6]	V. Kundra, "*Transition to IPv6: Memorandum for Chief Information Officers of Executive Departments and Agencies*", September 2010. Online at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/transition-to-ipv6.pdf
[OMB-M05-22]	K. Evans, "*Transition Planning for Internet Protocol Version 6 (IPv6): Memorandum for The Chief Information Officers*", August 2005. Online at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf
[OMB-M17-06]	S. Donovan, H. Shelanski, T. Scott, "*Policies for Federal Agency Public Websites and Digital Services: Memorandum for The Heads of Executive Departments and Agencies*", November 2016. Online at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf
[RFC8504]	Chown, T., Loughney, J., and T. Winters, "*IPv6 Node Requirements*", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019. Online at: https://tools.ietf.org/html/rfc8504
[SP500-267]	D. Montgomery, S. Nightingale, S. Frankel, M. Carson, "*A Profile for IPv6 in the U.S. Government - Version 1.0*", NIST SP-500-267, July 2008. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267
[SP500-267Ar1]	D. Montgomery, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*NIST IPv6 Profile*", NIST Special Publication 500-267A revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267Ar1
[SP500-281]	S. Nightingale, D. Montgomery, "*USGv6 Testing Program User's Guide*", November 2009. Online at: https://doi.org/10.6028/NIST.SP.500-281-v1.0

DRAFT

Citation	Reference
[SP500-281Ar1]	D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Test Program Guide*", NIST Special Publication 500-281A revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-281Ar1
[SP500-281Br1]	D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Test Methods: General Description and Validation*", NIST Special Publication 500-281B revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-281Br1
[USGv6-Web]	"*NIST USGv6 Program*", website, ongoing Online at: https://www.nist.gov/programs-projects/usgv6-program

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

Appendix A: Listing of USGv6-r1 Capability Templates

USGv6-r1: Host Capabilities:

- **IPv6-Only Capabilities**
  - [**M**] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities**
  - [**M**] - **Core** - support for IPv6 core functions.
  - [**O**] - **Extended-ICMP** - support for ICMPv6 extended messages.
  - [**O**] - **PLPMTUD** - support for Packetization Layer Path MTU Discovery.
  - [**O**] - **ND-Ext** - support for Neighbor Discovery features of enhanced DAD and First-Hop Selection.
  - [**O**] - **ND-WL** - support for packet-loss for router solicitations.
  - [**O**] - **SEND** - support for neighbor discovery security extensions.
  - [**O:1=[SLAAC | DHCP-Client]**] - **SLAAC** - support for stateless global address auto-configuration.
  - [**O**] - **PrivAddr** - support for SLAAC privacy extensions.
  - [**O**] - **DHCP-Stateless** - support for stateless (DHCP) configuration.
  - [**O:1=[SLAAC | DHCP-Client]**] - **DHCP-Client** - support for stateful (DHCP) address auto-configuration.
  - [**O**] - **DHCP-Client-Ext** - support for additional DHCP options including SIP.
  - [**O**] - **DHCP-Prefix** - support for stateful (DHCP) prefix delegation.
  - [**O**] - **DHCP-Prefix-Ext** - support for additional DHCP options for prefix exclude using prefix delegation.
  - [**O**] - **6Lo** - support for IPv6 over low power networks.
  - [**O**] - **Happy-Eyeballs** - support for Happy Eyeballs algorithm for dual stack environments.
- **Addressing Capabilities**
  - [**M**] - **Addr-Arch** - support for address architecture and selection.
  - [**O**] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities**
  - [**O**] - **DNS-Client** - support for DNS client/resolver functions.
  - [**O**] - **URI** - support for IPv6 uniform resource identifiers.
  - [**O**] - **NTP-Client** - support for NTP client capabilities.
  - [**O**] - **NTP-Server** - support for NTP server capabilities.
  - [**O**] - **DNS-Server** - support for DNS server capabilities.
  - [**O**] - **DHCP-Server** - support for DHCP server capabilities.
  - [**O**] - **DHCP-Server-Ext** - support for DHCP server for additional DHCP options and Bulk Lease-query.
  - [**O**] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Security Capabilities**
  - [**O:1=[IPsec | TLS]**] - **IPsec** - support for the IP security architecture.
  - [**X**] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [**X**] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [**O**] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.
  - [**O**] - **SSHV2** - support for SSHv2 over IPv6.
  - [**O:1=[IPsec | TLS]**] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [**O**] - **TLS-1.3** - support for Transport Layer Security architecture version 1.3.
- **Transition Mechanism Capabilities**
  - [**O**] - **Tunneling-IP** - support for generic packet encapsulation tunnels using IPv6.
  - [**O**] - **Tunneling-UDP** - support for generic packet encapsulation tunnels using UDP.
  - [**O**] - **XLAT** - support for transition mechanism 464XLAT.

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

  - [**O**] - **NAT64** - support for transition mechanism NAT64.
  - [**O**] - **DNS64** - support for transition mechanism DNS64.
- **Network Management Capabilities**
  - [**O**] - **SNMP** - support for simple network management protocol.
  - [**O**] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities**
  - [**O**] - **SSM** - require full support for multicast communications.
  - [**M**] - **Multicast** - support for link-local multicast communication.
- **Quality of Service Capabilities**
  - [**O**] - **DiffServ** - support for Differentiated Services capabilities.
  - [**O**] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities**
  - [**O**] - **Link=Ethernet** - support for IPv6 over Ethernet.
  - [**O**] - **Link=PPP** - support for IPv6 over PPP links.
  - [**O**] - **Link=G.9959** - support for IPv6 over Z-Wave.
  - [**O**] - **Link=Bluetooth** - support for IPv6 over Bluetooth.
  - [**O**] - **Link=BACnet** - support for IPv6 over BACnet.
  - [**O**] - **Link=6LoWPAN** - support for IPv6 over 802.15.4.

USGv6-r1: Router Capabilities:

- **IPv6-Only Capabilities**
  - [**M**] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities**
  - [**M**] - **Core** - support for IPv6 core functions.
  - [**O**] - **Extended-ICMP** - support for ICMPv6 extended messages.
  - [**O**] - **PLPMTUD** - support for Packetization Layer Path MTU Discovery.
  - [**O**] - **ND-Ext** - support for Neighbor Discovery features of enhanced DAD and First-Hop Selection.
  - [**O**] - **ND-WL** - support for packet-loss for router solicitations.
  - [**O**] - **SEND** - support for neighbor discovery security extensions.
  - [**M**] - **SLAAC** - support for stateless global address auto-configuration.
  - [**O**] - **DHCP-Prefix** - support for stateful (DHCP) prefix delegation.
  - [**O**] - **DHCP-Prefix-Ext** - support for additional DHCP options for prefix exclude using prefix delegation.
  - [**O**] - **6Lo** - support for IPv6 over low power networks.
- **Addressing Capabilities**
  - [**M**] - **Addr-Arch** - support for address architecture and selection.
  - [**O**] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities**
  - [**O**] - **DNS-Client** - support for DNS client/resolver functions.
  - [**O**] - **URI** - support for IPv6 uniform resource identifiers.
  - [**O**] - **NTP-Client** - support for NTP client capabilities.
  - [**O**] - **NTP-Server** - support for NTP server capabilities.
  - [**O**] - **DNS-Server** - support for DNS server capabilities.
  - [**O**] - **DHCP-Server** - support for DHCP server capabilities.
  - [**O**] - **DHCP-Server-Ext** - support for DHCP server for additional DHCP options and Bulk Lease-query.
  - [**O**] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Routing Capabilities**
  - [**O**] - **OSPF** - support for OSPF for intra-domain routing protocol.

- [**O**] - **OSPF-IPsec** - support for OSPF Authentication/Confidentiality using IPSec.
- [**O**] - **OSPF-Auth** - support for OSPF Authentication Trailer.
- [**O**] - **OSPF-Ext** - support for additional OSPF robustness and optimization features.
- [**O**] - **OSPF-Trans** - support for OSPF IPv4 over IPv6.
- [**O**] - **OSPF-Graceful** - support for OSPF Graceful restart.
- [**O**] - **IS-IS** - support for IS-IS for intra-domain routing protocol.
- [**O**] - **IS-IS-Auth** - support for IS-IS Authentication support.
- [**O**] - **IS-IS-Ext** - support for additional IS-IS robustness and optimization features.
- [**O**] - **IS-IS-MT** - support for Multi Topology in IS-IS.
- [**O**] - **BGP** - support for BGP for inter-domain routing protocols.
- [**O**] - **BGP-Reflect** - support for BGP Route Reflection
- [**O**] - **BGP-Graceful** - support for BGP Graceful Restart
- [**O**] - **BGP-FlowSpec** - support for BGP FlowSpec capabilities.
- [**O**] - **BGP-OV** - support for BGP Origin Validation capabilities.
- [**O**] - **BGP-VPLS** - support for BGP VPLS capabilities.
- [**O**] - **BGP-EVPN** - support for BGP EVPN capabilities.
- [**O**] - **BGP-6VPE** - support for BGP 6VPE capabilities.
- [**O**] - **BGP-MVPN** - support for BGP MVPN capabilities.
- [**O**] - **MPLS** - support for MPLS IPv6 capabilities.
- [**O**] - **CE-Router** - support for customer edge router capabilities.
- [**O**] - **VRRP** - support for VRRP Routing protocols.

- **Security Capabilities**
  - [**O:1=[IPsec | TLS]**] - **IPsec** - support for the IP security architecture.
  - [**O**] - **IPsec-VPN** - support for the IP security architecture gateways.
  - [**X**] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [**X**] - **IPsec-IoT-VPN** - support for IoT Cryptographic Algorithms in gateways.
  - [**X**] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [**X**] - **IPsec-CHACHA-VPN** - support for ChaCha20 Cryptographic Algorithms in gateways.
  - [**O**] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.
  - [**O**] - **IPsec-SHA-512-VPN** - support for SHA-512 Cryptographic Algorithms in gateways.
  - [**O**] - **SSHV2** - support for SSHv2 over IPv6.
  - [**O:1=[IPsec | TLS]**] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [**O**] - **TLS-1.3** - support for Transport Layer Security architecture version 1.3.
- **Transition Mechanism Capabilities**
  - [**O**] - **Tunneling-IP** - support for generic packet encapsulation tunnels using IPv6.
  - [**O**] - **Tunneling-UDP** - support for generic packet encapsulation tunnels using UDP.
  - [**O**] - **GRE** - support for generic router encapsulation tunnels.
  - [**O**] - **DS-Lite** - support for transition mechanism DS-Lite.
  - [**O**] - **LW4over6** - support for transition mechanism Lightweight 4over6.
  - [**O**] - **MAP-E** - support for transition mechanism MAP-E.
  - [**O**] - **MAP-T** - support for transition mechanism MAP-T.
  - [**O**] - **XLAT** - support for transition mechanism 464XLAT.
  - [**O**] - **NAT64** - support for transition mechanism NAT64.
  - [**O**] - **DNS64** - support for transition mechanism DNS64.
  - [**O**] - **6PE** - support for 6PE.
  - [**O**] - **LISP** - support for LISP protocol.
- **Network Management Capabilities**
  - [**O:1=[SNMP | NETCONF]**] - **SNMP** - support for simple network management protocol.
  - [**O:1=[SNMP | NETCONF]**] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities**
  - [**O**] - **SSM** - require full support for multicast communications.
  - [**M**] - **Multicast** - support for link-local multicast communication.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

- [**O**] - **PIM-SM** - support for PIM-SM Routing protocols.
- [**O**] - **PIM-SM-IPsec** - support for PIM-SM over IPsec.
- [**O**] - **PIM-SM-BiDir** - support for Bidrectional PIM-SM routing protocol.

- **Quality of Service Capabilities**
  - [**M**] - **DiffServ** - support for Differentiated Services capabilities.
  - [**O**] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities**
  - [**O**] - **Link=Ethernet** - support for IPv6 over Ethernet.
  - [**O**] - **Link=PPP** - support for IPv6 over PPP links.
  - [**O**] - **Link=G.9959** - support for IPv6 over Z-Wave.
  - [**O**] - **Link=Bluetooth** - support for IPv6 over Bluetooth.
  - [**O**] - **Link=BACnet** - support for IPv6 over BACnet.
  - [**O**] - **Link=6LoWPAN** - support for IPv6 over 802.15.4.

USGv6-r1: App-Serv | Switch | NPP Capabilities:

- **IPv6-Only Capabilities**
  - [**M**] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Application and Services Capabilities**
  - [**O**] - **App-Serv=[TBD]** - support for application/service specific functions.
- **Switch Capabilities**
  - [**O**] - **DHCPv6-Guard** - support for DHCPv6 Guard at Layer 2.
  - [**M**] - **RA-Guard** - support for RA Guard at Layer 2.
  - [**O**] - **MLD-Snooping** - support for MLD Snooping at Layer 2.
- **Network Protection Capabilities**
  - [**O**] - **FW** - support for basic firewall capabilities.
  - [**O**] - **IDS** - support for intrusion detection capabilities.
  - [**O**] - **IPS** - support for intrusion protection capabilities.
  - [**O**] - **APFW** - support for application firewall capabilities

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

Appendix B: Change Log

Revision 1 – February 2020

Revision 1 of the USGv6 Profile and Test Program specifications includes significant refactoring of the original documents. The most significant such change was to capture the generic definition of labeled IPv6 capability definitions in a generic NIST IPv6 Profile [SP-500-267Ar1]. This general profile has no specific mention of USG acquisition processes or procedures. The objective of this profile is to support its use by multiple user groups.

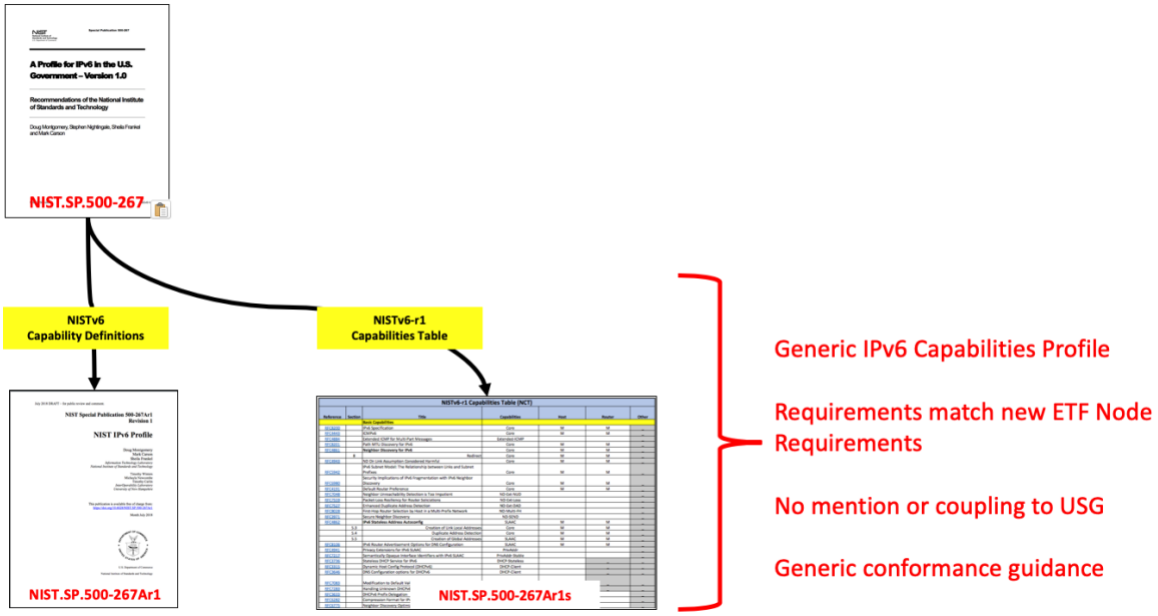

Figure 4 NIST IPv6 Profile

Other structural revisions to the USGv6 specifications include consolidation of the discussion of conformance testing and reporting into the USGv6 Test Program Guide. The NISTv6 and USGv6 Capabilities tables are now maintained as separate documents for easy of reference, as is the Suppliers Declaration of Conformity.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Br1

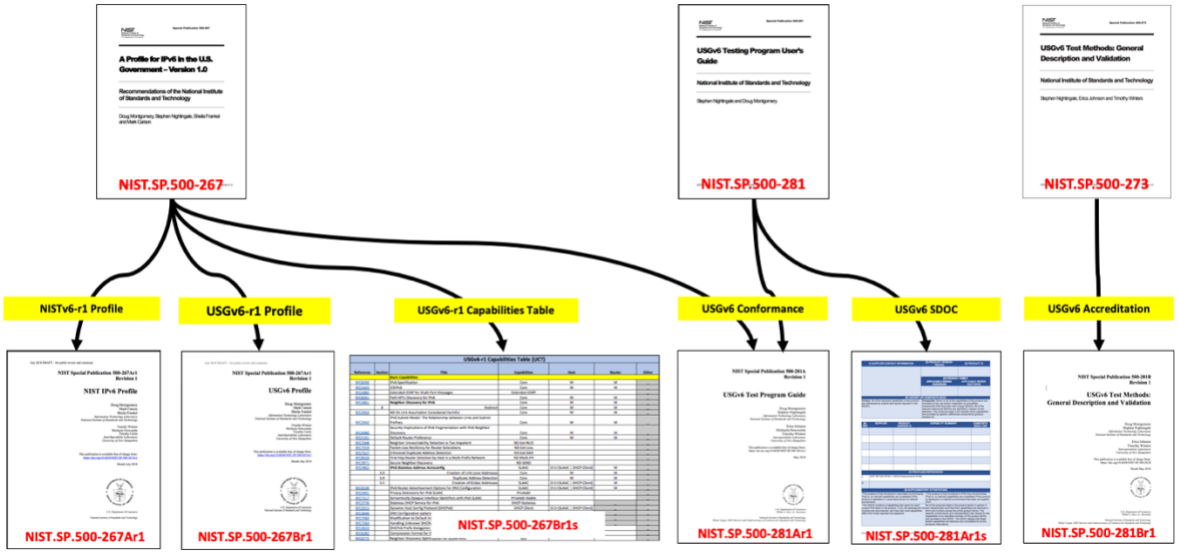

Figure 5 Structure of USGv6 revision 1 specifications

Technical changes to the profiles in revision 1 include: To update the set of Internet Engineering Task Force (IETF) specifications that form the basis for the USGv6 profile to their latest published version.

- To add new specifications for important IPv6 capabilities that have been developed since the publication of the first profile.
    - Highlights of these additions include technologies to support emerging use cases such as the Internet of Things, new forms of IPv6 transition technologies, support for "IPv6 Only" environments, and better support for specification of IPv6 enabled applications.
- To remove specifications for IPv6 capabilities included in the first version of the profile but that has since failed to achieve significant support in commercial products and network deployments.
- To update and consolidate the description of the USGv6 Test Program to reflect the lessons learned in the operation of that program to date.
    - Highlights of these changes include a more concise and consistent notation for documenting IPv6 capabilities, better support for testing in IPv6-Only environments, and an improved and streamlined Supplier's Declaration of Conformity (SDOC) for documenting test results.
- To separate the definition of IPv6 Capability Profiles from their specific use in USG acquisition programs so as to permit other user groups to re-use the capability profiles and their aligned product testing programs.