

# **NIST Special Publication 500-267Br1 Revision 1**

## **USGv6 Profile**

Doug Montgomery  
Mark Carson  
Sheila Frankel  
Timothy Winters  
Michayla Newcombe  
Timothy Carlin

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

# **NIST Special Publication 500-267Br1**

## **Revision 1**

# **USGv6 Profile**

Doug Montgomery

Mark Carson

Sheila Frankel

*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>

October 2019



U.S. Department of Commerce

National Institute of Standards and Technology

### **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.

National Institute of Standards and Technology Special Publication 500-267Br1  
Nat'l. Inst. Stand. Technol. Spec. Publ. 500-267Br1, NNN pages (Month YYYY)  
CODEN: NSPUE2

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-M-17-06] 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.



## **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.

## Table of Contents

<b>1. Introduction.....</b>	<b>1</b>
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
<b>2. Profile Scope, Applicability and Conventions .....</b>	<b>3</b>
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
<b>3. Selection of IPv6 Capabilities.....</b>	<b>6</b>
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
<b>4. Technical Definition of IPv6 Capabilities .....</b>	<b>13</b>
<b>5. Profile Usage Guidance and Examples.....</b>	<b>14</b>
5.1. Example Translations of Other Profiles .....	15
<b>Acknowledgments.....</b>	<b>16</b>
<b>References .....</b>	<b>17</b>
<b>Appendix A: Listing of USGv6-r1 Capability Templates .....</b>	<b>32</b>
USGv6-r1: Host Capabilities: .....	32
USGv6-r1: Router Capabilities: .....	33
USGv6-r1: App-Serv   Switch   NPP Capabilities: .....	35

<b>Appendix B: Change Log .....</b>	<b>36</b>
Revision 1 – October 2019 .....	36



## 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-M-17-06] 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 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, October 2019,**  
<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, October 2019,**  
<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.

## 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.

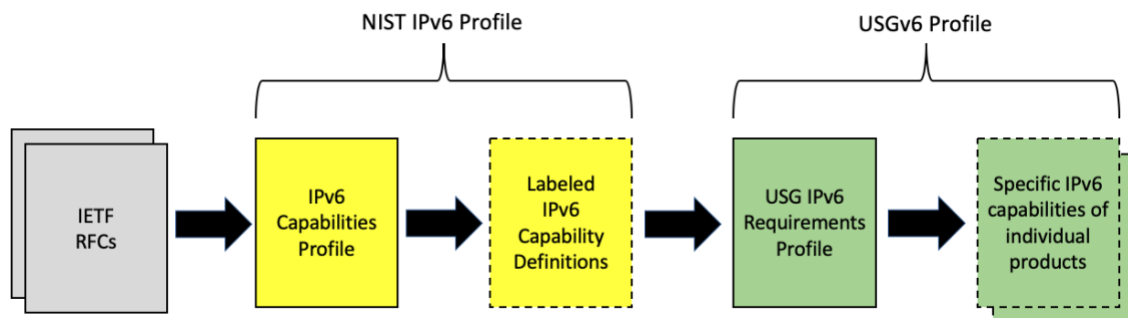


Figure 1 USGv6 usage scenario.

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.

- **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-M-17-06].

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).

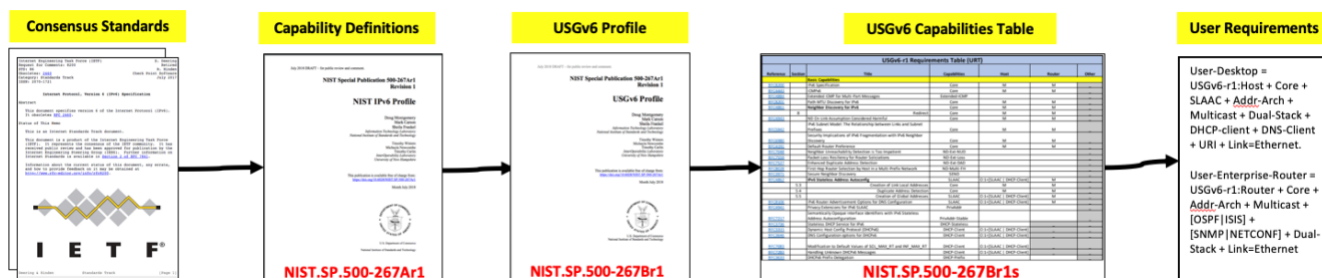


Figure 2 Traceability of USGv6 CSS Requirements.

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.

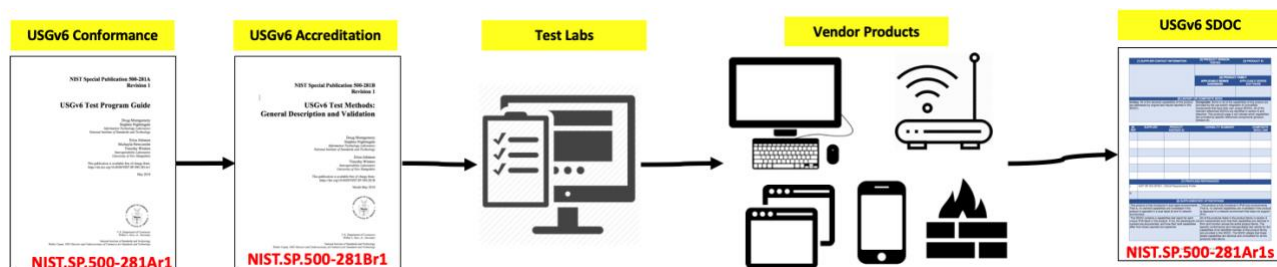


Figure 3 Traceability of USGv6 Suppliers Declarations of Conformity

The *USGv6 Test Program Guide* [SP-500-281Ar1] documents the basic components, concepts and processes necessary to claim conformance to USGv6 requirements. The *USGv6 Test Methods: General Description and Validation* [SP-500-281Br1] specification defines the processes for accreditation and quality control for USGv6 test laboratories.

### 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 **Error! Reference source not found.** for a complete listing and technical definition of these capabilities.

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

<b>USGv6-r1:Host Capabilities:</b> <ul style="list-style-type: none"> <li>• <b>IPv6-Only Capabilities</b> – see section 4.1 <ul style="list-style-type: none"> <li>○ [M] – <b>IPv6-Only</b> - support for full product functionality on an IPv6-only network</li> </ul> </li> </ul>
<b>USGv6-r1:Router Capabilities:</b> <ul style="list-style-type: none"> <li>• <b>IPv6-Only Capabilities</b> – see section 4.1 <ul style="list-style-type: none"> <li>○ [M] – <b>IPv6-Only</b> - support for full product functionality on an IPv6-only network</li> </ul> </li> </ul>
<b>USGv6-r1:NPP Capabilities:</b> <ul style="list-style-type: none"> <li>• <b>IPv6-Only Capabilities</b> – see section 4.1 <ul style="list-style-type: none"> <li>○ [M] – <b>IPv6-Only</b> - support for full product functionality on an IPv6-only network</li> </ul> </li> </ul>
<b>USGv6-r1:Switch Capabilities:</b> <ul style="list-style-type: none"> <li>• <b>IPv6-Only Capabilities</b> – see section 4.1 <ul style="list-style-type: none"> <li>○ [M] – <b>IPv6-Only</b> - support for full product functionality on an IPv6-only network</li> </ul> </li> </ul>
<b>USGv6-r1:App-Serv Capabilities:</b> <ul style="list-style-type: none"> <li>• <b>IPv6-Only Capabilities</b> – see section 4.1 <ul style="list-style-type: none"> <li>○ [M] – <b>IPv6-Only</b> - support for full product functionality on an IPv6-only network</li> </ul> </li> </ul>

##### 3.1.1. Selecting IPv6-Only Capabilities

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.

## 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 **Error! Reference source not found.** f or 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 **Error! Reference source not found.**
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section **Error! Reference source not found.**
  - [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 **Error! Reference source not found.**
  - [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 **TLSA** 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.

### 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 **Error! Reference source not found.** f or 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 **Error! Reference source not found.**
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Security Capabilities** - see section **Error! Reference source not found.**
  - [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 **Error! Reference source not found.**
  - [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 **Error! Reference source not found.**
  - [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.



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

### 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 **Error! Reference source not found.** 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 **Error! Reference source not found.**
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.

#### 3.4.1. Selecting Network Protection Product Capabilities

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.

### 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 **Error! Reference source not found.** 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 **Error! Reference source not found.**
  - [M]- **IPv6-Only** - support for full product functionality on an IPv6-only network.

#### 3.5.1. Selecting Switch Capabilities

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.

### 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 **Error! Reference source not found.** 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 **Error! Reference source not found.**
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.

#### 3.6.1. Selecting Application and Services Capabilities

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.

#### **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.

## 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|ISIS|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.

## 5.1. Example Translations of Other Profiles

A primary objective of the USGv6 Program is to establish a vocabulary for the expression of IPv6 requirements and/or product capabilities that can be used by many diverse user groups. It is hoped that by providing such a vocabulary and aligning the definition of capabilities to widely adopted testing program, we will encourage other profiling activities to adopt these conventions. The goal of establishing a common standardized means of expressing requirements and

Section 5 of the NISTv6-r1 profile contains example CSS that express the requirements of the IETF Node Requirements specification [RFC8504]. Below is another example of the ability to express the requirements of other profiles using the USGv6-r1 CSS notation. In this case we develop USGv6-r1 CSS to express the requirements of the product classes defined in *DoD IPv6 Standard Profiles for IPv6 Capable Products Version 6.0* [DOD-IPv6].

Note, these are only examples to demonstrate the ability to express the capability requirements of from other user group profiling efforts in the vocabular of the USGv6 profile. This does not represent any agreement from that user group to do so in their official documents.

- **Example-DOD-Host** = USGv6-r1:Host + Core + [SLAAC|DHCP-Client] + Addr-Arch + DNS-Client + Multicast + IPsec + [Dual-Stack|Tunneling] + Link=Ethernet
- **Example-DOD-Simple-Server** = USGv6-r1:Host + Core + [SLAAC|DHCP-Client] + Addr-Arch + Link=Ethernet
- **Example-DOD-Advanced-Server** = USGv6-r1:Host + Core + Addr-Arch + DNS-Client + Multicast + IPsec + [Dual-Stack|Tunneling] + Link=Ethernet
- **Example-DOD-Router** = USGv6-r1:Router + Core + SLAAC + Addr-Arch + Multicast + IPsec + DS + SNMP + [Dual-Stack|Tunneling] + Link=Ethernet
- **Example-DOD-L3-Switch** = USGv6-r1:Router + Core + Addr-Arch + Multicast + [Dual-Stack|Tunneling] + DS + Link=Ethernet
- **Example-DOD-IAD** = Core + Addr-Arch + Multicast + Link=Ethernet

NIST and the USGv6 Program partners encourage other user groups to adopt the capability definitions and CSS notation from this profile and would welcome collaborative efforts to accommodate such broader use.

## **Acknowledgments**

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

This new revised and restructured profile benefited from substantive review and input from the following: TBD.



## References

- [1] [[DODv6](#)] "DoD IPv6 Standard Profiles For IPv6 Capable Products Version 5.0", DISR IPv6 Standards Technical Working Group, July 2010. Online at: [http://jitc.fhu.disa.mil/apl/ipv6/pdf/distr\\_ipv6\\_50.pdf](http://jitc.fhu.disa.mil/apl/ipv6/pdf/distr_ipv6_50.pdf)
- [2] [[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>
- [3] [[IAB-IPv6](#)] "IAB Statement on IPv6", Internet Architecture Board, November 2016. Online at: <https://www.iab.org/2016/11/07/iab-statement-on-ipv6/>
- [4] [[IETF-OPSEC](#)] "IETF Operational Security Capabilities for IP Network Infrastructure (opsec) Working Group", Internet Engineering Task Force, on going. Online at: <https://datatracker.ietf.org/wg/opsec/about/>
- [5] [[IETF-V6OPS](#)] "IETF IPv6 Operations (v6ops) Working Group", Internet Engineering Task Force, Online at: <https://datatracker.ietf.org/wg/v6ops/about/>
- [6] [[IPv6-Ready](#)] "IPv6 Ready Logo Program", The IPv6 Forum, on going. Online at: <https://www.ipv6ready.org/>
- [7] [[IPv6-Forum](#)] "The IPv6 Forum", on going. Online at: <http://www.ipv6forum.com/>
- [8] [[ISO/IEC 17011-2:2017](#)] "Conformity Assessment - General Requirements for accreditation bodies accrediting conformity assessment bodies" November 2017. Online at: <http://www.iso.org/>
- [9] [[ISO/IEC 17025:2017](#)] "General requirements for the competence of testing and calibration laboratories." November 2017. Online at: <http://www.iso.org/>
- [10] [[ISO/IEC 17050-1:2004](#)] "ISO/IEC 17050-1:2004 Conformity Assessment - Supplier's Declaration of Conformity - Part 1: General requirements" October 2004. Online at: <http://www.iso.org/>
- [11] [[ISO/IEC 17050-2:2004](#)] "ISO/IEC 17050-1:2004 Conformity Assessment - Supplier's Declaration of Conformity - Part 2: General requirements" October 2004. Online at: <http://www.iso.org/>
- [12] [[ISO/IEC 9646-2:1994](#)] "Information technology - Open Systems Interconnection - Conformance testing methodology amd framework - Part 2: Abstract Test Suite specification." December 1994. Online at: <http://www.iso.org/>
- [13] [[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>
- [14] [[Note-1297](#)] B. Taylor, C. Kuyatt, "Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results", U.S. Department of Commerce, National Institute of Standards and Technology, NIST Technical Note 1297, 1994. Online at: <http://physics.nist.gov/Pubs/guidelines/TN1297/tn1297s.pdf>
- [15] [[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](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/transition-to-ipv6.pdf)
- [16] [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>
- [17] [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>
- [18] [RFC2119] Bradner, S., "*Key words for use in RFCs to Indicate Requirement Levels*", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997. Online at: <https://www.rfc-editor.org/info/rfc2119>
- [19] [RFC2410] Glenn, R. and S. Kent, "*The NULL Encryption Algorithm and Its Use With IPsec*", RFC 2410, DOI 10.17487/RFC2410, November 1998. Online at: <https://www.rfc-editor.org/info/rfc2410>
- [20] [RFC2464] Crawford, M., "*Transmission of IPv6 Packets over Ethernet Networks*", RFC 2464, DOI 10.17487/RFC2464, December 1998. Online at: <https://www.rfc-editor.org/info/rfc2464>
- [21] [RFC2473] Conta, A. and S. Deering, "*Generic Packet Tunneling in IPv6 Specification*", RFC 2473, DOI 10.17487/RFC2473, December 1998. Online at: <https://www.rfc-editor.org/info/rfc2473>
- [22] [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*", RFC 2474, DOI 10.17487/RFC2474, December 1998. Online at: <https://www.rfc-editor.org/info/rfc2474>
- [23] [RFC2526] Johnson, D. and S. Deering, "*Reserved IPv6 Subnet Anycast Addresses*", RFC 2526, DOI 10.17487/RFC2526, March 1999. Online at: <https://www.rfc-editor.org/info/rfc2526>
- [24] [RFC2545] Marques, P. and F. Dupont, "*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*", RFC 2545, DOI 10.17487/RFC2545, March 1999. Online at: <https://www.rfc-editor.org/info/rfc2545>
- [25] [RFC2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "*Assured Forwarding PHB Group*", RFC 2597, DOI 10.17487/RFC2597, June 1999. Online at: <https://www.rfc-editor.org/info/rfc2597>
- [26] [RFC2671] Vixie, P., "*Extension Mechanisms for DNS (EDNS0)*", RFC 2671, DOI 10.17487/RFC2671, August 1999. Online at: <https://www.rfc-editor.org/info/rfc2671>
- [27] [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "*Generic Routing Encapsulation (GRE)*", RFC 2784, DOI 10.17487/RFC2784, March 2000. Online at: <https://www.rfc-editor.org/info/rfc2784>
- [28] [RFC3140] Black, D., Brim, S., Carpenter, B., and F. Le Faucheur, "*Per Hop Behavior Identification Codes*", RFC 3140, DOI 10.17487/RFC3140, June 2001. Online at: <https://www.rfc-editor.org/info/rfc3140>
- [29] [RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "*The Addition of Explicit Congestion Notification (ECN) to IP*", RFC 3168, DOI 10.17487/RFC3168, September 2001. Online at: <https://www.rfc-editor.org/info/rfc3168>

- [30] [RFC3226] Gudmundsson, O., "DNSSEC and IPv6 A6 aware server/resolver message size requirements", RFC 3226, DOI 10.17487/RFC3226, December 2001. Online at: <https://www.rfc-editor.org/info/rfc3226>
- [31] [RFC3246] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, DOI 10.17487/RFC3246, March 2002. Online at: <https://www.rfc-editor.org/info/rfc3246>
- [32] [RFC3247] Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, "Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)", RFC 3247, DOI 10.17487/RFC3247, March 2002. Online at: <https://www.rfc-editor.org/info/rfc3247>
- [33] [RFC3289] Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, DOI 10.17487/RFC3289, May 2002. Online at: <https://www.rfc-editor.org/info/rfc3289>
- [34] [RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, DOI 10.17487/RFC3306, August 2002. Online at: <https://www.rfc-editor.org/info/rfc3306>
- [35] [RFC3307] Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", RFC 3307, DOI 10.17487/RFC3307, August 2002. Online at: <https://www.rfc-editor.org/info/rfc3307>
- [36] [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003. Online at: <https://www.rfc-editor.org/info/rfc3315>
- [37] [RFC3319] Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, DOI 10.17487/RFC3319, July 2003. Online at: <https://www.rfc-editor.org/info/rfc3319>
- [38] [RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002. Online at: <https://www.rfc-editor.org/info/rfc3411>
- [39] [RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, DOI 10.17487/RFC3412, December 2002. Online at: <https://www.rfc-editor.org/info/rfc3412>
- [40] [RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, DOI 10.17487/RFC3413, December 2002. Online at: <https://www.rfc-editor.org/info/rfc3413>
- [41] [RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, DOI 10.17487/RFC3414, December 2002. Online at: <https://www.rfc-editor.org/info/rfc3414>
- [42] [RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, DOI 10.17487/RFC3526, May 2003. Online at: <https://www.rfc-editor.org/info/rfc3526>
- [43] [RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, DOI 10.17487/RFC3566, September 2003. Online at: <https://www.rfc-editor.org/info/rfc3566>
- [44] [RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003. Online at: <https://www.rfc-editor.org/info/rfc3596>

- [45] [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "*The AES-CBC Cipher Algorithm and Its Use with IPsec*", RFC 3602, DOI 10.17487/RFC3602, September 2003. Online at: <https://www.rfc-editor.org/info/rfc3602>
- [46] [RFC3633] Troan, O. and R. Droms, "*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*", RFC 3633, DOI 10.17487/RFC3633, December 2003. Online at: <https://www.rfc-editor.org/info/rfc3633>
- [47] [RFC3646] Droms, R., Ed., "*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*", RFC 3646, DOI 10.17487/RFC3646, December 2003. Online at: <https://www.rfc-editor.org/info/rfc3646>
- [48] [RFC3736] Droms, R., "*Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*", RFC 3736, DOI 10.17487/RFC3736, April 2004. Online at: <https://www.rfc-editor.org/info/rfc3736>
- [49] [RFC3810] Vida, R., Ed., and L. Costa, Ed., "*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*", RFC 3810, DOI 10.17487/RFC3810, June 2004. Online at: <https://www.rfc-editor.org/info/rfc3810>
- [50] [RFC3879] Huitema, C. and B. Carpenter, "*Deprecating Site Local Addresses*", RFC 3879, DOI 10.17487/RFC3879, September 2004. Online at: <https://www.rfc-editor.org/info/rfc3879>
- [51] [RFC3956] Savola, P. and B. Haberman, "*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*", RFC 3956, DOI 10.17487/RFC3956, November 2004. Online at: <https://www.rfc-editor.org/info/rfc3956>
- [52] [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "*SEcure Neighbor Discovery (SEND)*", RFC 3971, DOI 10.17487/RFC3971, March 2005. Online at: <https://www.rfc-editor.org/info/rfc3971>
- [53] [RFC3972] Aura, T., "*Cryptographically Generated Addresses (CGA)*", RFC 3972, DOI 10.17487/RFC3972, March 2005. Online at: <https://www.rfc-editor.org/info/rfc3972>
- [54] [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "*Uniform Resource Identifier (URI): Generic Syntax*", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005. Online at: <https://www.rfc-editor.org/info/rfc3986>
- [55] [RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "*IPv6 Scoped Address Architecture*", RFC 4007, DOI 10.17487/RFC4007, March 2005. Online at: <https://www.rfc-editor.org/info/rfc4007>
- [56] [RFC4022] Raghunathan, R., Ed., "*Management Information Base for the Transmission Control Protocol (TCP)*", RFC 4022, DOI 10.17487/RFC4022, March 2005. Online at: <https://www.rfc-editor.org/info/rfc4022>
- [57] [RFC4038] Shin, M-K., Ed., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "*Application Aspects of IPv6 Transition*", RFC 4038, DOI 10.17487/RFC4038, March 2005. Online at: <https://www.rfc-editor.org/info/rfc4038>
- [58] [RFC4087] Thaler, D., "*IP Tunnel MIB*", RFC 4087, DOI 10.17487/RFC4087, June 2005. Online at: <https://www.rfc-editor.org/info/rfc4087>
- [59] [RFC4106] Viega, J. and D. McGrew, "*The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*", RFC 4106, DOI 10.17487/RFC4106, June 2005. Online at: <https://www.rfc-editor.org/info/rfc4106>
- [60] [RFC4113] Fenner, B. and J. Flick, "*Management Information Base for the User Datagram Protocol (UDP)*", RFC 4113, DOI 10.17487/RFC4113, June 2005. Online at: <https://www.rfc-editor.org/info/rfc4113>



- [61] [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005. Online at: <https://www.rfc-editor.org/info/rfc4191>
- [62] [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005. Online at: <https://www.rfc-editor.org/info/rfc4193>
- [63] [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, DOI 10.17487/RFC4213, October 2005. Online at: <https://www.rfc-editor.org/info/rfc4213>
- [64] [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006. Online at: <https://www.rfc-editor.org/info/rfc4271>
- [65] [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006. Online at: <https://www.rfc-editor.org/info/rfc4291>
- [66] [RFC4292] Haberman, B., "IP Forwarding Table MIB", RFC 4292, DOI 10.17487/RFC4292, April 2006. Online at: <https://www.rfc-editor.org/info/rfc4292>
- [67] [RFC4293] Routhier, S., Ed., "Management Information Base for the Internet Protocol (IP)", RFC 4293, DOI 10.17487/RFC4293, April 2006. Online at: <https://www.rfc-editor.org/info/rfc4293>
- [68] [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005. Online at: <https://www.rfc-editor.org/info/rfc4301>
- [69] [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005. Online at: <https://www.rfc-editor.org/info/rfc4303>
- [70] [RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, DOI 10.17487/RFC4307, December 2005. Online at: <https://www.rfc-editor.org/info/rfc4307>
- [71] [RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, DOI 10.17487/RFC4309, December 2005. Online at: <https://www.rfc-editor.org/info/rfc4309>
- [72] [RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006. Online at: <https://www.rfc-editor.org/info/rfc4429>
- [73] [RFC4434] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, DOI 10.17487/RFC4434, February 2006. Online at: <https://www.rfc-editor.org/info/rfc4434>
- [74] [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006. Online at: <https://www.rfc-editor.org/info/rfc4443>
- [75] [RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006. Online at: <https://www.rfc-editor.org/info/rfc4541>
- [76] [RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, DOI 10.17487/RFC4552, June 2006. Online at: <https://www.rfc-editor.org/info/rfc4552>
- [77] [RFC4581] Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format", RFC 4581, DOI 10.17487/RFC4581, October 2006. Online at: <https://www.rfc-editor.org/info/rfc4581>

- [78] [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*", RFC 4601, DOI 10.17487/RFC4601, August 2006. Online at: <https://www.rfc-editor.org/info/rfc4601>
- [79] [RFC4604] Holbrook, H., Cain, B., and B. Haberman, "*Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*", RFC 4604, DOI 10.17487/RFC4604, August 2006. Online at: <https://www.rfc-editor.org/info/rfc4604>
- [80] [RFC4607] Holbrook, H. and B. Cain, "*Source-Specific Multicast for IP*", RFC 4607, DOI 10.17487/RFC4607, August 2006. Online at: <https://www.rfc-editor.org/info/rfc4607>
- [81] [RFC4609] Savola, P., Lehtonen, R., and D. Meyer, "*Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements*", RFC 4609, DOI 10.17487/RFC4609, October 2006. Online at: <https://www.rfc-editor.org/info/rfc4609>
- [82] [RFC4610] Farinacci, D. and Y. Cai, "*Anycast-RP Using Protocol Independent Multicast (PIM)*", RFC 4610, DOI 10.17487/RFC4610, August 2006. Online at: <https://www.rfc-editor.org/info/rfc4610>
- [83] [RFC4659] De Clercq, J., Ooms, D., Carugi, M., and F. Le Faucheur, "*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*", RFC 4659, DOI 10.17487/RFC4659, September 2006. Online at: <https://www.rfc-editor.org/info/rfc4659>
- [84] [RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "*Multiprotocol Extensions for BGP-4*", RFC 4760, DOI 10.17487/RFC4760, January 2007. Online at: <https://www.rfc-editor.org/info/rfc4760>
- [85] [RFC4761] Kompella, K., Ed., and Y. Rekhter, Ed., "*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*", RFC 4761, DOI 10.17487/RFC4761, January 2007. Online at: <https://www.rfc-editor.org/info/rfc4761>
- [86] [RFC4798] De Clercq, J., Ooms, D., Prevost, S., and F. Le Faucheur, "*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*", RFC 4798, DOI 10.17487/RFC4798, February 2007. Online at: <https://www.rfc-editor.org/info/rfc4798>
- [87] [RFC4807] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "*IPsec Security Policy Database Configuration MIB*", RFC 4807, DOI 10.17487/RFC4807, March 2007. Online at: <https://www.rfc-editor.org/info/rfc4807>
- [88] [RFC4821] Mathis, M. and J. Heffner, "*Packetization Layer Path MTU Discovery*", RFC 4821, DOI 10.17487/RFC4821, March 2007. Online at: <https://www.rfc-editor.org/info/rfc4821>
- [89] [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "*Neighbor Discovery for IP version 6 (IPv6)*", RFC 4861, DOI 10.17487/RFC4861, September 2007. Online at: <https://www.rfc-editor.org/info/rfc4861>
- [90] [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "*IPv6 Stateless Address Autoconfiguration*", RFC 4862, DOI 10.17487/RFC4862, September 2007. Online at: <https://www.rfc-editor.org/info/rfc4862>
- [91] [RFC4868] Kelly, S. and S. Frankel, "*Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*", RFC 4868, DOI 10.17487/RFC4868, May 2007. Online at: <https://www.rfc-editor.org/info/rfc4868>
- [92] [RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "*Extended ICMP to Support Multi-Part Messages*", RFC 4884, DOI 10.17487/RFC4884, April 2007. Online at: <https://www.rfc-editor.org/info/rfc4884>
- [93] [RFC4891] Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "*Using IPsec to Secure IPv6-in-IPv4 Tunnels*", RFC 4891, DOI 10.17487/RFC4891, May 2007. Online at: <https://www.rfc-editor.org/info/rfc4891>

- [94] [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007. Online at: <https://www.rfc-editor.org/info/rfc4941>
- [95] [RFC4943] Roy, S., Durand, A., and J. Paugh, "IPv6 Neighbor Discovery On-Link Assumption Considered Harmful", RFC 4943, DOI 10.17487/RFC4943, September 2007. Online at: <https://www.rfc-editor.org/info/rfc4943>
- [96] [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007. Online at: <https://www.rfc-editor.org/info/rfc4944>
- [97] [RFC4982] Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, DOI 10.17487/RFC4982, July 2007. Online at: <https://www.rfc-editor.org/info/rfc4982>
- [98] [RFC5015] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, DOI 10.17487/RFC5015, October 2007. Online at: <https://www.rfc-editor.org/info/rfc5015>
- [99] [RFC5059] Bhaskar, N., Gall, A., Lingard, J., and S. Venaas, "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)", RFC 5059, DOI 10.17487/RFC5059, January 2008. Online at: <https://www.rfc-editor.org/info/rfc5059>
- [100] [RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007. Online at: <https://www.rfc-editor.org/info/rfc5072>
- [101] [RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-IS)", RFC 5120, DOI 10.17487/RFC5120, February 2008. Online at: <https://www.rfc-editor.org/info/rfc5120>
- [102] [RFC5185] Mirtorabi, S., Psenak, P., Lindem, A., Ed., and A. Oswal, "OSPF Multi-Area Adjacency", RFC 5185, DOI 10.17487/RFC5185, May 2008. Online at: <https://www.rfc-editor.org/info/rfc5185>
- [103] [RFC5187] Pillay-Esnault, P. and A. Lindem, "OSPFv3 Graceful Restart", RFC 5187, DOI 10.17487/RFC5187, June 2008. Online at: <https://www.rfc-editor.org/info/rfc5187>
- [104] [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008. Online at: <https://www.rfc-editor.org/info/rfc5246>
- [105] [RFC5301] McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS", RFC 5301, DOI 10.17487/RFC5301, October 2008. Online at: <https://www.rfc-editor.org/info/rfc5301>
- [106] [RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008. Online at: <https://www.rfc-editor.org/info/rfc5304>
- [107] [RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/RFC5308, October 2008. Online at: <https://www.rfc-editor.org/info/rfc5308>
- [108] [RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009. Online at: <https://www.rfc-editor.org/info/rfc5310>
- [109] [RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008. Online at: <https://www.rfc-editor.org/info/rfc5340>
- [110] [RFC5460] Stapp, M., "DHCPv6 Bulk Leasequery", RFC 5460, DOI 10.17487/RFC5460, February 2009. Online at: <https://www.rfc-editor.org/info/rfc5460>

- [111] [RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "*Dissemination of Flow Specification Rules*", RFC 5575, DOI 10.17487/RFC5575, August 2009. Online at: <https://www.rfc-editor.org/info/rfc5575>
- [112] [RFC5613] Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "*OSPF Link-Local Signaling*", RFC 5613, DOI 10.17487/RFC5613, August 2009. Online at: <https://www.rfc-editor.org/info/rfc5613>
- [113] [RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "*Transport Layer Security (TLS) Renegotiation Indication Extension*", RFC 5746, DOI 10.17487/RFC5746, February 2010. Online at: <https://www.rfc-editor.org/info/rfc5746>
- [114] [RFC5796] Atwood, W., Islam, S., and M. Siami, "*Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages*", RFC 5796, DOI 10.17487/RFC5796, March 2010. Online at: <https://www.rfc-editor.org/info/rfc5796>
- [115] [RFC5798] Nadas, S., Ed., "*Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*", RFC 5798, DOI 10.17487/RFC5798, March 2010. Online at: <https://www.rfc-editor.org/info/rfc5798>
- [116] [RFC5838] Lindem, A., Ed., Mirtorabi, S., Roy, A., Barnes, M., and R. Aggarwal, "*Support of Address Families in OSPFv3*", RFC 5838, DOI 10.17487/RFC5838, April 2010. Online at: <https://www.rfc-editor.org/info/rfc5838>
- [117] [RFC5903] Fu, D. and J. Solinas, "*Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*", RFC 5903, DOI 10.17487/RFC5903, June 2010. Online at: <https://www.rfc-editor.org/info/rfc5903>
- [118] [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "*Network Time Protocol Version 4: Protocol and Algorithms Specification*", RFC 5905, DOI 10.17487/RFC5905, June 2010. Online at: <https://www.rfc-editor.org/info/rfc5905>
- [119] [RFC5942] Singh, H., Beebe, W., and E. Nordmark, "*IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*", RFC 5942, DOI 10.17487/RFC5942, July 2010. Online at: <https://www.rfc-editor.org/info/rfc5942>
- [120] [RFC5952] Kawamura, S. and M. Kawashima, "*A Recommendation for IPv6 Address Text Representation*", RFC 5952, DOI 10.17487/RFC5952, August 2010. Online at: <https://www.rfc-editor.org/info/rfc5952>
- [121] [RFC6092] Woodyatt, J., Ed., "*Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*", RFC 6092, DOI 10.17487/RFC6092, January 2011. Online at: <https://www.rfc-editor.org/info/rfc6092>
- [122] [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "*IPv6 Router Advertisement Guard*", RFC 6105, DOI 10.17487/RFC6105, February 2011. Online at: <https://www.rfc-editor.org/info/rfc6105>
- [123] [RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "*Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*", RFC 6146, DOI 10.17487/RFC6146, April 2011. Online at: <https://www.rfc-editor.org/info/rfc6146>
- [124] [RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "*DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*", RFC 6147, DOI 10.17487/RFC6147, April 2011. Online at: <https://www.rfc-editor.org/info/rfc6147>
- [125] [RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "*Using 127-Bit IPv6 Prefixes on Inter-Router Links*", RFC 6164, DOI 10.17487/RFC6164, April 2011. Online at: <https://www.rfc-editor.org/info/rfc6164>



- [126] [RFC6176] Turner, S. and T. Polk, "*Prohibiting Secure Sockets Layer (SSL) Version 2.0*", RFC 6176, DOI 10.17487/RFC6176, March 2011. Online at: <https://www.rfc-editor.org/info/rfc6176>
- [127] [RFC6232] Wei, F., Qin, Y., Li, Z., Li, T., and J. Dong, "*Purge Originator Identification TLV for IS-IS*", RFC 6232, DOI 10.17487/RFC6232, May 2011. Online at: <https://www.rfc-editor.org/info/rfc6232>
- [128] [RFC6233] Li, T. and L. Ginsberg, "*IS-IS Registry Extension for Purges*", RFC 6233, DOI 10.17487/RFC6233, May 2011. Online at: <https://www.rfc-editor.org/info/rfc6233>
- [129] [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "*Network Configuration Protocol (NETCONF)*", RFC 6241, DOI 10.17487/RFC6241, June 2011. Online at: <https://www.rfc-editor.org/info/rfc6241>
- [130] [RFC6282] Hui, J., Ed., and P. Thubert, "*Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*", RFC 6282, DOI 10.17487/RFC6282, September 2011. Online at: <https://www.rfc-editor.org/info/rfc6282>
- [131] [RFC6286] Chen, E. and J. Yuan, "*Autonomous-System-Wide Unique BGP Identifier for BGP-4*", RFC 6286, DOI 10.17487/RFC6286, June 2011. Online at: <https://www.rfc-editor.org/info/rfc6286>
- [132] [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "*Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*", RFC 6333, DOI 10.17487/RFC6333, August 2011. Online at: <https://www.rfc-editor.org/info/rfc6333>
- [133] [RFC6379] Law, L. and J. Solinas, "*Suite B Cryptographic Suites for IPsec*", RFC 6379, DOI 10.17487/RFC6379, October 2011. Online at: <https://www.rfc-editor.org/info/rfc6379>
- [134] [RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "*IPv6 Node Requirements*", RFC 6434, DOI 10.17487/RFC6434, December 2011. Online at: <https://www.rfc-editor.org/info/rfc6434>
- [135] [RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "*IPv6 Flow Label Specification*", RFC 6437, DOI 10.17487/RFC6437, November 2011. Online at: <https://www.rfc-editor.org/info/rfc6437>
- [136] [RFC6485] Huston, G., "*The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)*", RFC 6485, DOI 10.17487/RFC6485, February 2012. Online at: <https://www.rfc-editor.org/info/rfc6485>
- [137] [RFC6494] Gagliano, R., Krishnan, S., and A. Kuec, "*Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)*", RFC 6494, DOI 10.17487/RFC6494, February 2012. Online at: <https://www.rfc-editor.org/info/rfc6494>
- [138] [RFC6495] Gagliano, R., Krishnan, S., and A. Kuec, "*Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields*", RFC 6495, DOI 10.17487/RFC6495, February 2012. Online at: <https://www.rfc-editor.org/info/rfc6495>
- [139] [RFC6565] Pillay-Esnault, P., Moyer, P., Doyle, J., Ertekin, E., and M. Lundberg, "*OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*", RFC 6565, DOI 10.17487/RFC6565, June 2012. Online at: <https://www.rfc-editor.org/info/rfc6565>
- [140] [RFC6603] Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O. Troan, "*Prefix Exclude Option for DHCPv6-based Prefix Delegation*", RFC 6603, DOI 10.17487/RFC6603, May 2012. Online at: <https://www.rfc-editor.org/info/rfc6603>
- [141] [RFC6608] Dong, J., Chen, M., and A. Suryanarayana, "*Subcodes for BGP Finite State Machine Error*", RFC 6608, DOI 10.17487/RFC6608, May 2012. Online at: <https://www.rfc-editor.org/info/rfc6608>

- [142] [RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012. Online at: <https://www.rfc-editor.org/info/rfc6724>
- [143] [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012. Online at: <https://www.rfc-editor.org/info/rfc6775>
- [144] [RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012. Online at: <https://www.rfc-editor.org/info/rfc6793>
- [145] [RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013. Online at: <https://www.rfc-editor.org/info/rfc6811>
- [146] [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013. Online at: <https://www.rfc-editor.org/info/rfc6830>
- [147] [RFC6845] Sheth, N., Wang, L., and J. Zhang, "OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type", RFC 6845, DOI 10.17487/RFC6845, January 2013. Online at: <https://www.rfc-editor.org/info/rfc6845>
- [148] [RFC6860] Yang, Y., Retana, A., and A. Roy, "Hiding Transit-Only Networks in OSPF", RFC 6860, DOI 10.17487/RFC6860, January 2013. Online at: <https://www.rfc-editor.org/info/rfc6860>
- [149] [RFC6874] Carpenter, B., Cheshire, S., and R. Hinden, "Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers", RFC 6874, DOI 10.17487/RFC6874, February 2013. Online at: <https://www.rfc-editor.org/info/rfc6874>
- [150] [RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013. Online at: <https://www.rfc-editor.org/info/rfc6877>
- [151] [RFC6936] Fairhurst, G. and M. Westerlund, "Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums", RFC 6936, DOI 10.17487/RFC6936, April 2013. Online at: <https://www.rfc-editor.org/info/rfc6936>
- [152] [RFC6980] Gont, F., "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, DOI 10.17487/RFC6980, August 2013. Online at: <https://www.rfc-editor.org/info/rfc6980>
- [153] [RFC7048] Nordmark, E. and I. Gashinsky, "Neighbor Unreachability Detection Is Too Impatient", RFC 7048, DOI 10.17487/RFC7048, January 2014. Online at: <https://www.rfc-editor.org/info/rfc7048>
- [154] [RFC7078] Matsumoto, A., Fujisaki, T., and T. Chown, "Distributing Address Selection Policy Using DHCPv6", RFC 7078, DOI 10.17487/RFC7078, January 2014. Online at: <https://www.rfc-editor.org/info/rfc7078>
- [155] [RFC7083] Droms, R., "Modification to Default Values of SOL\_MAX\_RT and INF\_MAX\_RT", RFC 7083, DOI 10.17487/RFC7083, November 2013. Online at: <https://www.rfc-editor.org/info/rfc7083>
- [156] [RFC7084] Singh, H., Beebe, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013. Online at: <https://www.rfc-editor.org/info/rfc7084>

- [157] [RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014. Online at: <https://www.rfc-editor.org/info/rfc7113>
- [158] [RFC7133] Kashima, S., Kobayashi, A., Ed., and P. Aitken, "Information Elements for Data Link Layer Traffic Measurement", RFC 7133, DOI 10.17487/RFC7133, May 2014. Online at: <https://www.rfc-editor.org/info/rfc7133>
- [159] [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014. Online at: <https://www.rfc-editor.org/info/rfc7136>
- [160] [RFC7166] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", RFC 7166, DOI 10.17487/RFC7166, March 2014. Online at: <https://www.rfc-editor.org/info/rfc7166>
- [161] [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014. Online at: <https://www.rfc-editor.org/info/rfc7217>
- [162] [RFC7223] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014. Online at: <https://www.rfc-editor.org/info/rfc7223>
- [163] [RFC7277] Bjorklund, M., "A YANG Data Model for IP Management", RFC 7277, DOI 10.17487/RFC7277, June 2014. Online at: <https://www.rfc-editor.org/info/rfc7277>
- [164] [RFC7283] Cui, Y., Sun, Q., and T. Lemon, "Handling Unknown DHCPv6 Messages", RFC 7283, DOI 10.17487/RFC7283, July 2014. Online at: <https://www.rfc-editor.org/info/rfc7283>
- [165] [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014. Online at: <https://www.rfc-editor.org/info/rfc7296>
- [166] [RFC7321] McGrew, D. and P. Hoffman, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 7321, DOI 10.17487/RFC7321, August 2014. Online at: <https://www.rfc-editor.org/info/rfc7321>
- [167] [RFC7346] Droms, R., "IPv6 Multicast Address Scopes", RFC 7346, DOI 10.17487/RFC7346, August 2014. Online at: <https://www.rfc-editor.org/info/rfc7346>
- [168] [RFC7371] Boucadair, M. and S. Venaas, "Updates to the IPv6 Multicast Addressing Architecture", RFC 7371, DOI 10.17487/RFC7371, September 2014. Online at: <https://www.rfc-editor.org/info/rfc7371>
- [169] [RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015. Online at: <https://www.rfc-editor.org/info/rfc7428>
- [170] [RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015. Online at: <https://www.rfc-editor.org/info/rfc7432>
- [171] [RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015. Online at: <https://www.rfc-editor.org/info/rfc7465>
- [172] [RFC7527] Asati, R., Singh, H., Beebee, W., Pignataro, C., Dart, E., and W. George, "Enhanced Duplicate Address Detection", RFC 7527, DOI 10.17487/RFC7527, April 2015. Online at: <https://www.rfc-editor.org/info/rfc7527>
- [173] [RFC7559] Krishnan, S., Anipko, D., and D. Thaler, "Packet-Loss Resiliency for Router Solicitations", RFC 7559, DOI 10.17487/RFC7559, May 2015. Online at: <https://www.rfc-editor.org/info/rfc7559>

- [174] [RFC7568] Barnes, R., Thomson, M., Pironti, A., and A. Langley, "*Deprecating Secure Sockets Layer Version 3.0*", RFC 7568, DOI 10.17487/RFC7568, June 2015. Online at: <https://www.rfc-editor.org/info/rfc7568>
- [175] [RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "*Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture*", RFC 7596, DOI 10.17487/RFC7596, July 2015. Online at: <https://www.rfc-editor.org/info/rfc7596>
- [176] [RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "*Mapping of Address and Port with Encapsulation (MAP-E)*", RFC 7597, DOI 10.17487/RFC7597, July 2015. Online at: <https://www.rfc-editor.org/info/rfc7597>
- [177] [RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S., and T. Murakami, "*Mapping of Address and Port using Translation (MAP-T)*", RFC 7599, DOI 10.17487/RFC7599, July 2015. Online at: <https://www.rfc-editor.org/info/rfc7599>
- [178] [RFC7605] Touch, J., "*Recommendations on Using Assigned Transport Port Numbers*", BCP 165, RFC 7605, DOI 10.17487/RFC7605, August 2015. Online at: <https://www.rfc-editor.org/info/rfc7605>
- [179] [RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "*Revised Error Handling for BGP UPDATE Messages*", RFC 7606, DOI 10.17487/RFC7606, August 2015. Online at: <https://www.rfc-editor.org/info/rfc7606>
- [180] [RFC7607] Kumari, W., Bush, R., Schiller, H., and K. Patel, "*Codification of AS 0 Processing*", RFC 7607, DOI 10.17487/RFC7607, August 2015. Online at: <https://www.rfc-editor.org/info/rfc7607>
- [181] [RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "*IPv6 Prefix Length Recommendation for Forwarding*", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015. Online at: <https://www.rfc-editor.org/info/rfc7608>
- [182] [RFC7610] Gont, F., Liu, W., and G. Van de Velde, "*DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers*", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015. Online at: <https://www.rfc-editor.org/info/rfc7610>
- [183] [RFC7634] Nir, Y., "*ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec*", RFC 7634, DOI 10.17487/RFC7634, August 2015. Online at: <https://www.rfc-editor.org/info/rfc7634>
- [184] [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "*IPv6 over BLUETOOTH(R) Low Energy*", RFC 7668, DOI 10.17487/RFC7668, October 2015. Online at: <https://www.rfc-editor.org/info/rfc7668>
- [185] [RFC7674] Haas, J., Ed., "*Clarification of the Flowspec Redirect Extended Community*", RFC 7674, DOI 10.17487/RFC7674, October 2015. Online at: <https://www.rfc-editor.org/info/rfc7674>
- [186] [RFC7676] Pignataro, C., Bonica, R., and S. Krishnan, "*IPv6 Support for Generic Routing Encapsulation (GRE)*", RFC 7676, DOI 10.17487/RFC7676, October 2015. Online at: <https://www.rfc-editor.org/info/rfc7676>
- [187] [RFC7705] George, W. and S. Amante, "*Autonomous System Migration Mechanisms and Their Effects on the BGP AS\_PATH Attribute*", RFC 7705, DOI 10.17487/RFC7705, November 2015. Online at: <https://www.rfc-editor.org/info/rfc7705>
- [188] [RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016. Online at: <https://www.rfc-editor.org/info/rfc7761>



- [189] [RFC7775] Ginsberg, L., Litkowski, S., and S. Previdi, "*IS-IS Route Preference for Extended IP and IPv6 Reachability*", RFC 7775, DOI 10.17487/RFC7775, February 2016. Online at: <https://www.rfc-editor.org/info/rfc7775>
- [190] [RFC7915] Bao, C., Li, X., Baker, F., Anderson, T., and F. Gont, "*IP/ICMP Translation Algorithm*", RFC 7915, DOI 10.17487/RFC7915, June 2016. Online at: <https://www.rfc-editor.org/info/rfc7915>
- [191] [RFC7949] Chen, I., Lindem, A., and R. Atkinson, "*OSPFv3 over IPv4 for IPv6 Transition*", RFC 7949, DOI 10.17487/RFC7949, August 2016. Online at: <https://www.rfc-editor.org/info/rfc7949>
- [192] [RFC8028] Baker, F. and B. Carpenter, "*First-Hop Router Selection by Hosts in a Multi-Prefix Network*", RFC 8028, DOI 10.17487/RFC8028, November 2016. Online at: <https://www.rfc-editor.org/info/rfc8028>
- [193] [RFC8097] Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "*BGP Prefix Origin Validation State Extended Community*", RFC 8097, DOI 10.17487/RFC8097, March 2017. Online at: <https://www.rfc-editor.org/info/rfc8097>
- [194] [RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "*IPv6 Router Advertisement Options for DNS Configuration*", RFC 8106, DOI 10.17487/RFC8106, March 2017. Online at: <https://www.rfc-editor.org/info/rfc8106>
- [195] [RFC8163] Lynn, K., Ed., Martocci, J., Neilson, C., and S. Donaldson, "*Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks*", RFC 8163, DOI 10.17487/RFC8163, May 2017. Online at: <https://www.rfc-editor.org/info/rfc8163>
- [196] [RFC8200] Deering, S. and R. Hinden, "*Internet Protocol, Version 6 (IPv6) Specification*", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017. Online at: <https://www.rfc-editor.org/info/rfc8200>
- [197] [RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "*Path MTU Discovery for IP version 6*", STD 87, RFC 8201, DOI 10.17487/RFC8201, July 2017. Online at: <https://www.rfc-editor.org/info/rfc8201>
- [198] [RFC8210] Bush, R. and R. Austein, "*The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1*", RFC 8210, DOI 10.17487/RFC8210, September 2017. Online at: <https://www.rfc-editor.org/info/rfc8210>
- [199] [RFC8212] Mauch, J., Snijders, J., and G. Hankins, "*Default External BGP (EBGP) Route Propagation Behavior without Policies*", RFC 8212, DOI 10.17487/RFC8212, July 2017. Online at: <https://www.rfc-editor.org/info/rfc8212>
- [200] [RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "*Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*", RFC 8221, DOI 10.17487/RFC8221, October 2017. Online at: <https://www.rfc-editor.org/info/rfc8221>
- [201] [RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "*Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*", RFC 8247, DOI 10.17487/RFC8247, September 2017. Online at: <https://www.rfc-editor.org/info/rfc8247>
- [202] [RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "*Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model*", RFC 8281, DOI 10.17487/RFC8281, December 2017. Online at: <https://www.rfc-editor.org/info/rfc8281>

- [203] [\[RFC8305\]](#) Schinazi, D. and T. Pauly, "*Happy Eyeballs Version 2: Better Connectivity Using Concurrency*", RFC 8305, DOI 10.17487/RFC8305, December 2017. Online at: <https://www.rfc-editor.org/info/rfc8305>
- [204] [\[RFC8319\]](#) Krishnan, S., Korhonen, J., Chakrabarti, S., Nordmark, E., and A. Yourtchenko, "*Support for Adjustable Maximum Router Lifetimes per Link*", RFC 8319, DOI 10.17487/RFC8319, February 2018. Online at: <https://www.rfc-editor.org/info/rfc8319>
- [205] [\[RFC8343\]](#) Bjorklund, M., "*A YANG Data Model for Interface Management*", RFC 8343, DOI 10.17487/RFC8343, March 2018. Online at: <https://www.rfc-editor.org/info/rfc8343>
- [206] [\[RFC8344\]](#) Bjorklund, M., "*A YANG Data Model for IP Management*", RFC 8344, DOI 10.17487/RFC8344, March 2018. Online at: <https://www.rfc-editor.org/info/rfc8344>
- [207] [\[RFC8348\]](#) Bierman, A., Bjorklund, M., Dong, J., and D. Romascanu, "*A YANG Data Model for Hardware Management*", RFC 8348, DOI 10.17487/RFC8348, March 2018. Online at: <https://www.rfc-editor.org/info/rfc8348>
- [208] [\[RFC8349\]](#) Lhotka, L., Lindem, A., and Y. Qu, "*A YANG Data Model for Routing Management (NMDA Version)*", RFC 8349, DOI 10.17487/RFC8349, March 2018. Online at: <https://www.rfc-editor.org/info/rfc8349>
- [209] [\[RFC8362\]](#) Lindem, A., Roy, A., Goethals, D., Reddy Vallem, V., and F. Baker, "*OSPFv3 Link State Advertisement (LSA) Extensibility*", RFC 8362, DOI 10.17487/RFC8362, April 2018. Online at: <https://www.rfc-editor.org/info/rfc8362>
- [210] [\[RFC8379\]](#) Hegde, S., Sarkar, P., Gredler, H., Nanduri, M., and L. Jalil, "*OSPF Graceful Link Shutdown*", RFC 8379, DOI 10.17487/RFC8379, May 2018. Online at: <https://www.rfc-editor.org/info/rfc8379>
- [211] [\[RFC8415\]](#) Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*", RFC 8415, DOI 10.17487/RFC8415, November 2018. Online at: <https://www.rfc-editor.org/info/rfc8415>
- [212] [\[RFC8446\]](#) Rescorla, E., "*The Transport Layer Security (TLS) Protocol Version 1.3*", RFC 8446, DOI 10.17487/RFC8446, August 2018. Online at: <https://www.rfc-editor.org/info/rfc8446>
- [213] [\[RFC8481\]](#) Bush, R., "*Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)*", RFC 8481, DOI 10.17487/RFC8481, September 2018. Online at: <https://www.rfc-editor.org/info/rfc8481>
- [214] [\[RFC8504\]](#) Chown, T., Loughney, J., and T. Winters, "*IPv6 Node Requirements*", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019. Online at: <https://www.rfc-editor.org/info/rfc8504>
- [215] [\[SP500-267\]](#) 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>
- [216] [\[SP500-267Ar1\]](#) D. Montgomery, S. Frankel, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*NIST IPv6 Capabilities Profile*", NIST SP-500-267Ar1, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-267Ar1>
- [217] [\[SP500-267Ar1s\]](#) D. Montgomery, S. Frankel, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*NISTv6 Capabilities Table*", NIST SP-500-267Ar1s, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-267Ar1s>
- [218] [\[SP500-267Br1\]](#) D. Montgomery, S. Frankel, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*USGv6 Requirements Profile*", NIST SP-500-267Br1, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-267Br1>

- [219] [\[SP500-267Br1s\]](#) D. Montgomery, S. Frankel, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*USGv6 Requirements Table*", NIST SP-500-267Br1s, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-267Br1s>
- [220] [\[SP500-273\]](#) S. Nightingale, "*IPv6 Test Methods: General Description and Validation*", NIST SP-500-273, November 2009. Online at: <https://dx.doi.org/10.6028/nist.sp.500-273v2>
- [221] [\[SP500-281\]](#) 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>
- [222] [\[SP500-281Ar1\]](#) D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Test Program Guide*", NIST SP-500-281Ar1, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-281Ar1>
- [223] [\[SP500-281Ar1s\]](#) D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Suppliers Declaration of Conformity*", NIST SP-500-281Ar1s, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-281Ar1s>
- [224] [\[SP500-281Br1\]](#) D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Test Methods: General Description and Validation*", NIST SP-500-281Br1, July 2018. Online at: <https://dx.doi.org/10.6028/NIST.SP.500-281Br1>
- [225] [\[USGv6-Tested\]](#) "USGv6 Tested Products Registry" Online at: <https://www.iol.unh.edu/registry/usgv6>
- [226] [\[USGv6-Web\]](#) "NIST USGv6 Program" Online at: <https://www.nist.gov/programs-projects/usgv6-program>

## Appendix A: Listing of USGv6-r1 Capability Templates

### USGv6-r1: Host Capabilities:

- **IPv6-Only Capabilities** - see section XXX
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section XXX
  - [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** - see section XXX
  - [M] - **Addr-Arch** - support for address architecture and selection.
  - [O] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities** - see section XXX
  - [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 Leasequery.
  - [O] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Security Capabilities** - see section XXX
  - [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: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** - see section XXX
  - [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.
  - [O] - **NAT64** - support for transition mechanism NAT64.
  - [O] - **DNS64** - support for transition mechanism DNS64.
- **Network Management Capabilities** - see section XXX
  - [O] - **SNMP** - support for simple network management protocol.
  - [O] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities** - see section XXX
  - [O] - **SSM** - require full support for multicast communications.
  - [M] - **Multicast** - support for link-local multicast communication.
- **Quality of Service Capabilities** - see section XXX
  - [O] - **DiffServ** - support for Differentiated Services capabilities.
  - [O] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities** - see section XXX
  - [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** - see section XXX
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section XXX
  - [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** - see section XXX
  - [M] - **Addr-Arch** - support for address architecture and selection.
  - [O] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities** - see section XXX
  - [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 Leasequery.
- [O] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Routing Capabilities** - see section XXX
  - [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-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] - **CE-Router** - support for customer edge router capabilities.
  - [O] - **VRRP** - support for VRRP Routing protocols.
- **Security Capabilities** - see section XXX
  - [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: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** - see section XXX
  - [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** - see section XXX
  - [O:1=[SNMP | NETCONF]] - **SNMP** - support for simple network management protocol.
  - [O:1=[SNMP | NETCONF]] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities** - see section XXX
  - [O] - **SSM** - require full support for multicast communications.
  - [M] - **Multicast** - support for link-local multicast communication.
  - [O] - **PIM-SM** - support for PIM-SM Routing protocols.
  - [O] - **PIM-SM-RP** - support for PIM-SM RP Discovery mechanisms.
  - [O] - **PIM-SM-IPsec** - support for PIM-SM over IPsec.
  - [O] - **PIM-SM-BiDir** - support for Bidirectional PIM-SM routing protocol.
- **Quality of Service Capabilities** - see section XXX
  - [M] - **DiffServ** - support for Differentiated Services capabilities.
  - [O] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities** - see section XXX
  - [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** - see section XXX
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Application and Services Capabilities** - see section XXX
  - [O] - **App-Serv=[TBD]** - support for application/service specific functions.
- **Switch Capabilities** - see section XXX
  - [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** - see section XXX
  - [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.

## Appendix B: Change Log

### Revision 1 – October 2019

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 IPv6 labeled 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.

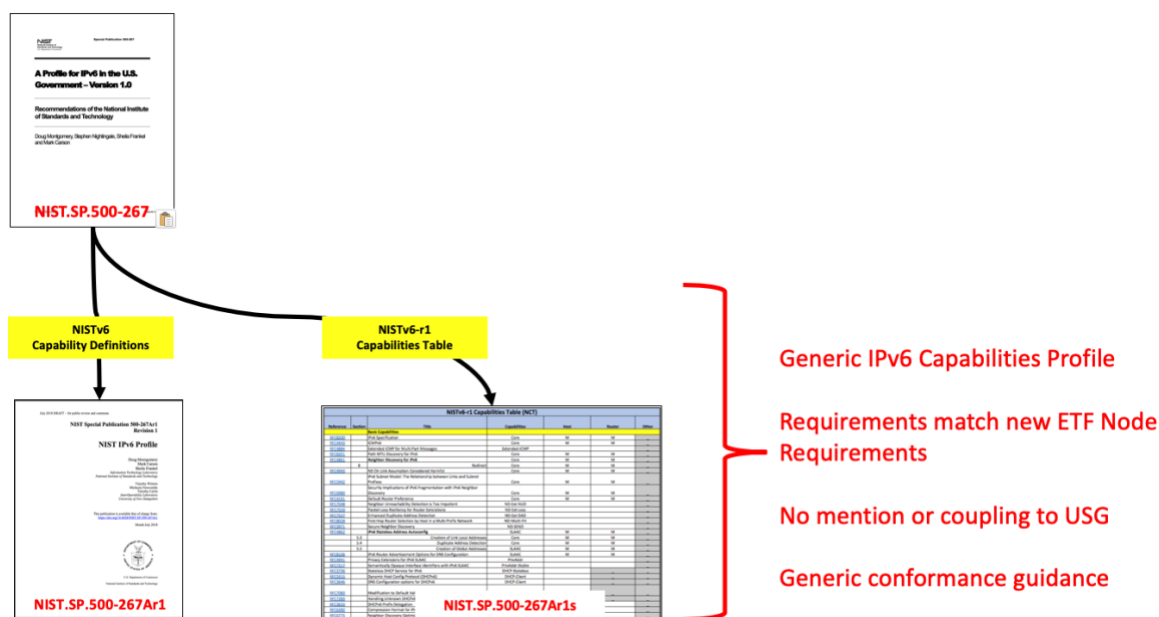


Figure 4 NIST IPv6 Profile

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.

Technical change 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.

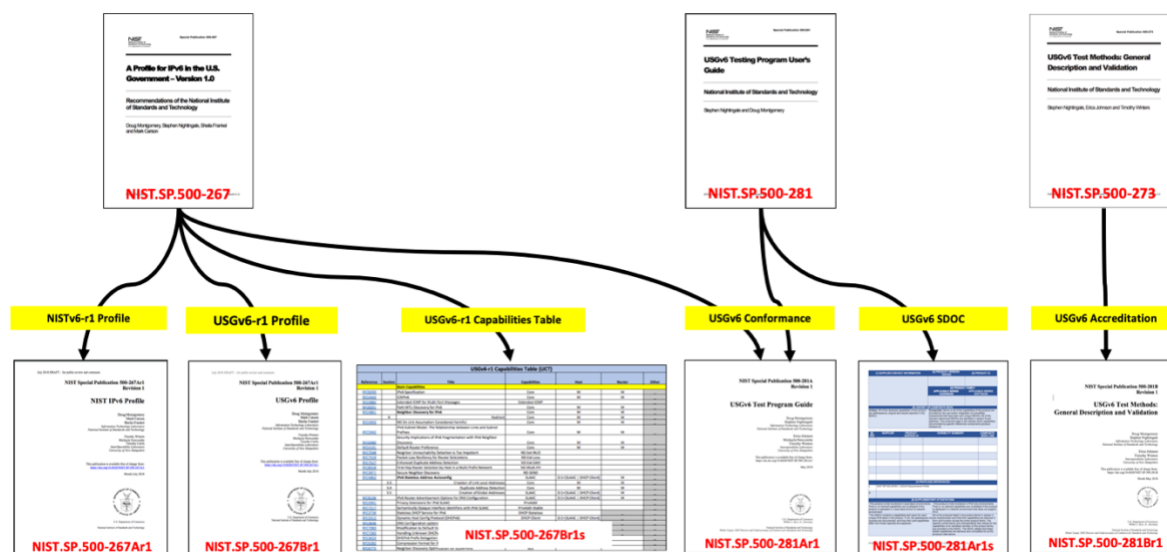


Figure 5 Structure of USGv6 revision 1 specifications