NIST Special Publication 500-267A
Revision 1

NIST IPv6 Profile

Doug Montgomery
Mark Carson
Timothy Winters
Michayla Newcombe
Timothy Carlin

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

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

NIST Special Publication 500-267A
Revision 1

NIST IPv6 Profile

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

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Ar1

Month February 2020

DRAFT

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

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

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 NIST's Trustworthy Networks Program. Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

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

DRAFT

National Institute of Standards and Technology Special Publication 500-267Ar1
Natl. Inst. Stand. Technol. Spec. Publ. 500-267Ar1, 81 pages (February 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Executive Summary

This document defines a profile of Internet Protocol version 6 (IPv6) capabilities for the purpose of expressing technical requirements for networked information technology (IT) products and to report the IPv6 capabilities of specific products. The original design of this profile was developed collaboratively with, and aligned to, industry led product test programs [IPv6-Ready, NIST-IPv6F] and documented in an acquisition profile for one specific user group [SP500-267].

This new document provides significant revisions to the original IPv6 profile, including:

1. Separating the definition of IPv6 capability profiles from their use in specific acquisition programs to permit other user groups to re-use the capability profiles and their aligned product testing programs.

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.

An example of one user group's use of this capability profile in an acquisition program and coordinated product testing program can be found in [SP500-267Br1] and [SP500-281Ar1]. While this capability profile has its origins in that specific user group, it has been refactored to be independent of any specific acquisition program.

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

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

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, when combined with specific acquisition and product testing programs, this profile can facilitate the efficient adoption of IPv6 technologies in many industry sectors.

Keywords

Internet Protocol version 6; IPv6; standards profile; acquisition; NISTv6; NISTv6-r1.

DRAFT

Table of Contents

1. Introduction 1

1.1. Audience 2

1.2. Profiling IPv6 Capabilities 3

1.3. Profile Structure: Functional Roles and Capability Groups 4

1.4. Profiling Products and Implementations. 5

2. Profile Scope, Applicability and Conventions 6

2.1. Scope and Applicability 6

2.2. Life Cycles and Change Management. 6

2.3. Statements of Requirements Levels 7

2.4. Profile Capabilities Table. 7

2.5. Capability Summary Strings. 8

2.6. Conformance, Testing and Reporting. 10

3. Selection of IPv6 Capabilities 12

3.1. IPv6-Only Capabilities 13

3.1.1. Selecting IPv6-Only Capabilities 13

3.2. Host Capabilities 15

3.2.1. Selecting Host Capabilities 16

3.3. Router Capabilities 19

3.3.1. Selecting Router Capabilities 21

3.4. Network Protection Product Capabilities 24

3.4.1. Selecting Network Protection Product Capabilities 24

3.5. Switch Capabilities 25

3.5.1. Selecting Switch Capabilities 25

3.6. Application and Services Capabilities 26

3.6.1. Selecting Application and Services Capabilities 26

4. Technical Definition of IPv6 Capabilities 27

4.1. IPv6-Only Capabilities 28

4.1.1. Definition of IPv6-only Capability Requirements 28

4.2. Basic Capabilities 30

4.2.1. Definition of Basic Capability Requirements 30

4.3. Routing Capabilities 33

4.3.1. Definition of Routing Capability Requirements 33

4.4. Quality of Service Capabilities 37

4.4.1. Definition of Quality of Service Capability Requirements 37

4.5. Transition Mechanism Capabilities 38

4.5.1. Definition of Transition Mechanism Capability Requirements 38

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.6. Link Specific Capabilities 40
4.6.1. Definition of Link Specific Capability Requirements 40
4.7. Addressing Capabilities 41
4.7.1. Definition of Addressing Capability Requirements 41
4.8. Security Capabilities 42
4.8.1. Definition of Security Capability Requirements 42
4.9. Network Management Capabilities 46
4.9.1. Definition of Network Management Capability Requirements 46
4.10. Multicast Capabilities 48
4.10.1. Definition of Multicast Capability Requirements 48
4.11. Network Support Capabilities 50
4.11.1. Definition of Network Support Capability Requirements 50
4.12. Application and Service Capabilities 52
4.12.1. Definition of Application and Service Capability Requirements 52
4.13. Switch Capabilities 54
4.13.1. Definition of Switch Capability Requirements 54
4.14. Network Protection Product Capabilities 55
4.14.1. Definition of Network Protection Product Capability Requirements 55
4.14.2. Source of requirements 56
4.14.3. Common requirements for network protection products 56
4.14.4. Firewall requirements (Common Requirements) 58
4.14.5. Application firewall requirements 59
4.14.6. Intrusion detection and prevention system requirements 60
4.14.7. Intrusion prevention requirements 60
5. Profile Usage Guidance and Examples 62
Acknowledgments 66
References 67
Appendix A: Change Log 81

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

1. Introduction

This document establishes a profile of Internet Protocol version 6 (IPv6) capabilities for the purpose of expressing technical requirements for networked information technology (IT) products and to report the IPv6 capabilities of specific products. The original design of this profile was developed collaboratively with, and aligned to, industry led product test programs [IPv6-Ready, NIST-IPv6F] and documented in an acquisition profile for one specific user group [SP500-267].

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

1. Separating the definition of IPv6 capability profiles from their use in specific acquisition programs to permit other user groups to re-use the capability profiles and their aligned product testing programs.

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.

An example of one user group's use of this profile in an acquisition program and coordinated product testing program can be found in [SP500-267Br1] and [SP500-281Ar1]. While this capability profile has its origins in a specific user group, it has been refactored to be independent of any specific acquisition program.

This profile is not subject to copyright and its reuse, either in its entirety, or in derivative works is encouraged. References to this specification should cite:

- **"NIST IPv6 Profile", NIST Special Publication 500-267A revision 1, National Institute of Standards and Technology, February 2020, https://doi.org/10.6028/NIST.SP.500-267Ar1**
- The abbreviation **"NISTv6-r1"** is used to identify this profile in various usages.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

1.1. Audience

This document is intended to assist several communities of interest in the planning and implementation of IPv6 acquisition programs. The range of potential uses of this profile include establishing a technical basis for broad IPv6 acquisition strategies, defining requirements for individual procurements or documenting the IPv6 capabilities of individual products.

This profile assumes that the readers have some level of familiarity with IPv6 and with its corpus of specifications (i.e. IETF RFCs). Readers are directed to the wealth of books and training materials that provide such introductions to IPv6 technologies.

The main purpose of this document is to identify and organize the vast collection of IPv6 specifications into subsets of labeled *capabilities* that may be of common utility in planning for and acquiring specific IPv6 products and services. As such, the profile is primarily targeted to users in the following groups:

- **Users and Purchasers -** Those writing procurement and contract language may use this document as a reference to develop product requirement specifications. For their purposes, this document aims to facilitate the development of precise specifications of IPv6 technical requirements that must be met by offered products. It should be noted that this profile only addresses IPv6 requirements, and thus cannot stand in isolation as a complete procurement specification. Many other technical issues (e.g., IPv4 capabilities, hardware, performance, reliability, support) and procurement policies must be typically addressed to fully define a complete procurement requirement. Those developing procurement requirements will be primarily interested in sections 1.4, 2.4 and 3 of this document.
- **Developers** – Developers of network protocols, applications and services may use this document as reference when they describe the IPv6 capabilities of their products. In addition, developers of networked IT should view the defined capabilities in this profile as a potential source of technical requirements for future acquisitions and the anticipate the need to demonstrate and document compliance with such requirements. Developers and vendors will be primarily interested in sections 1.4, 2.4, 2.6 and 4 of this document.
- **Testing and Accreditation Organizations** – Some user groups may request or require independent testing of networked IT products to demonstrate compliance with requirements defined in this profile. Often such testing programs may require accreditation of testing services. Organizations that support formal testing programs associated with this profile will be primarily interested in sections 2.6 and 4 of this document.
- **Other Profile Developers** – User groups may choose to develop derivative works based upon this profile, potentially modifying the recommendations, conformance, testing and/or reporting requirements described herein. While such efforts are encouraged when necessary, it is requested that they avoid duplication and adopt unmodified portions of this profile by reference rather than duplication.

DRAFT

All members of this audience, and others, are encouraged to carefully review this profile and provide comments so that future versions might be improved. Comments should be addressed to: ipv6-program@nist.gov.

1.2. Profiling IPv6 Capabilities

The technical specification of capabilities required by modern networking products is inherently complex. While some use the term "IPv6" as if it were a single, monolithic technology with a simple concise technical definition, the reality is quite different. The complete specification of the range of IPv6 capabilities commonly found in products requires reference to scores of individual protocol, architecture, and algorithm specifications. While this profile provides some background and rationale about the choices that are contained within it, it is well beyond the scope of this document to provide a tutorial on these technologies and specifications.

Some of the IPv6 capabilities in this profile are defined in terms of protocol and algorithm specifications that are not specific to IPv6. In fact, many such specifications may not mention IPv6 at all. Examples include various application layer and security services. Although these specifications may have been written with IPv4 in mind, when referenced in this profile, the understanding is that the requirements apply to IPv6 networking. In addition, some specifications for IPv6 capabilities may only define the required changes from the corresponding IPv4 capability. In these cases, the implied requirement is to also support the unchanged functions from the IPv4 specification.

This profile establishes a taxonomy of IPv6 capabilities that are defined primarily in terms of IETF specifications. The result is a collection of labeled IPv6 capability definitions for common network functions, applications, services and usage scenarios. The design choices for the granularity and composition of individual named IPv6 capabilities in this profile are guided by several factors including (1) a judgement of the protocol capabilities that are common to all IPv6 products, and the capabilities that differentiate individual IPv6 products, (2) an assessment of when multiple specifications are necessary to fully implement a given user visible functionality, and (3) the granularity and organization of existing industry defined conformance and interoperability tests [IPv6-Ready]. As such, some labeled capabilities in this profile map one-to-one to specific IETF protocol specifications (or parts of specifications), and some labeled capabilities map to a set of two or more distinct protocol specifications.

By default, 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. These labeled capability sets effectively form a vocabulary for expressing technical requirements for IPv6 products, and for testing, documenting and reporting IPv6 capabilities of specific products. By using the same vocabulary to express requirements and to report product capabilities, this profile facilities the efficient comparison of user requirements with vendor offerings.

This profile provides the means by which its users can develop requirement specifications for IPv6 capabilities in a wide range of networked IT products and services. Users of this

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

profile can develop IPv6 requirement statements for specific networked IT products and services directly from the NISTv6 Profile, or they might develop their own requirements profiles, derived from this specification as a base, but with the additional guidance and requirements suitable for their user group.

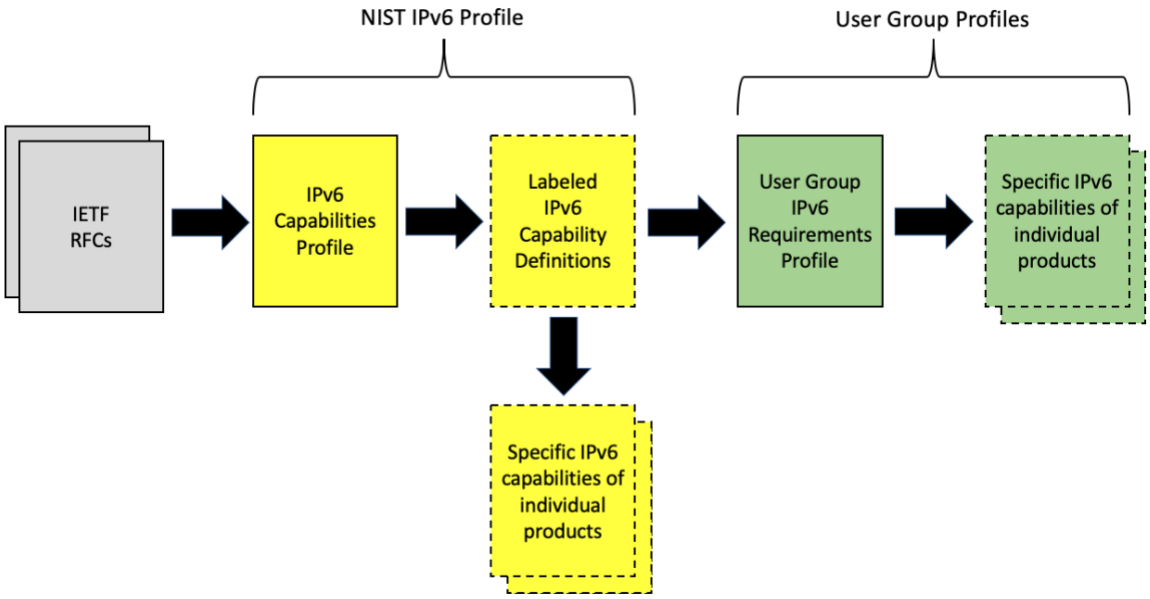

Figure 1 NIST IPv6 Profile usage scenarios.

It is expected that, when combined with specific user group requirements profiles and product testing programs, this profile can facilitate the efficient acquisition and adoption of IPv6 technologies in many industry sectors.

1.3. Profile Structure: Functional Roles and Capability Groups

Often IETF specifications are written to describe the normative behavior of multiple parties in a distributed protocol. Often the technical requirements of each party are different based upon the *functional role* they play in the protocol. The most common functional roles distinguished in IETF specifications are those of *Hosts* and *Routers*. Many protocols describe both the required behavior for Hosts and for Routers in a single specification. An individual implementation of such a protocol typically only supports the requirements for either Hosts or Routers depending up the purpose of the product. In order to carefully specify, test and report such differing capabilities, we need to distinguish between a few common functional roles in our profile.

One approach to dealing with this need is to produce separate labeled capability variants for each functional role. In some cases where the functional role differences are limited to a single protocol, we do this (e.g., "**DHCP-Client**", "**DHCP-Server**"). But in case of Hosts and Routers, the differences span many capabilities and specifications. To enable concise

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

specification of these varied requirements we partition our profile to describe Host and Router IPv6 capabilities separately.

This profile defines the following functional roles:

- **Router** – an IPv6 implementation that forwards packets not explicitly addressed to itself. A Router implementation's primary purpose is to support the control protocols necessary to enable interconnection of distinct IP sub-networks by IP layer packet forwarding.
- **Host** – an IPv6 implementation that is not a router. A Host implementation's primary purpose is to support application protocols that are the source and/or destination of IP layer communication.
- **Other** – products that implement IPv6 capabilities that are neither standard Host nor Router functions. Currently the profile identifies three additional roles for such products:
    - **Network Protection Product (NPP)** – an IPv6 product which provides network protection functions (e.g., firewalls, intrusion detection / prevention). For security reasons, such products often have only partial, or non-standard, Host and/or Router capabilities. For this reason, and because this profile only specifies the protection capabilities required for these products, we call them out using a distinct functional role.
    - **Switch** – a product which provides Layer-2 (i.e., sub IP layer) switching, but needs to support IPv6 specific functions for security and performance reasons.
    - **Application and Services** – a network enabled application or service that does not directly implement IPv6 protocols (e.g., typically these are implemented by an underlying distinct product such as an operating system) but must operate on IPv6 enabled systems and IPv6 networks.

In the sections that follow, we organize our lists and textual descriptions of capabilities into groups of related functions (e.g. "Security Capabilities", "Routing Capabilities"). These groupings are purely for the convenience of organizing the large range of capabilities described by this profile, and to allow users to easily see related capabilities which may represent alternatives for the same basic functions. Such groupings have no technical impact on the use of this profile and could have been omitted without any normative impact.

1.4. Profiling Products and Implementations.

The purpose of this profile is to support the precise technical specification of IPv6 requirements for networked information technology, and to enable documentation of the IPv6 capabilities of individual products. There is a vast variety of networked IT products and systems in the world today, ranging from supercomputers to systems on a chip and from carrier class routers to home wireless access points. It is impossible to develop a priori a static taxonomy of products that would adequately and flexibly capture such a vast range of offerings. Instead, our approach is to provide a common vocabulary for expressing the requirements and capabilities of individual implementations, thus enabling users to developed unique detailed descriptions of nearly any product.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Even within a single product or system, it is often the case that there are multiple distinct implementations of network protocols and functions. These individual implementations, often called "protocol stacks", may have different capabilities and even different functional roles. For example, an IPv6 Router may well have one or more Host stacks to support network management and configuration functions. It is important to document the requirements and capabilities of all network functions in each product, not just those associated with its main purpose.[1]

2. Profile Scope, Applicability and Conventions

The following section provides context information for the general interpretation and use of this profile. Users of this specification that need to alter the information that follows are encouraged to do so explicitly in a separate derivative document. While derivative works are encouraged when necessary, care should be taken to avoid unnecessary duplication of specification and/or potentially conflicting guidance.

2.1. Scope and Applicability

This profile was developed to assist in the acquisition of robust, IPv6 capable networked IT products. The capabilities identified in this profile represent the union of those viewed as being necessary to enable production IPv6 deployment in a wide range of usage scenarios.

While this profile is designed to allow users to specify what IPv6 capabilities are required in products being purchased for specific deployment scenarios, it is beyond the scope of this profile to address operational concerns such as deployment plans, coexistence and transition schemes to ensure interoperability with legacy IPv4 infrastructure, or specific approaches to securing individual network environments.

Planning for IPv6 deployment in production IT systems is a complex undertaking. There is a large, and ever growing, knowledge base of industry developed specifications and guidance in this area. The IETF IPv6 Operations (v6ops) [IETF-V6OPS] and Operational Security Capabilities for IP Network Infrastructure (opsec) [IETF-OPSEC] working groups are sources of numerous operational guides addressing deployment plans for various environments (e.g., enterprise networks, Internet service providers, cellular networks), security considerations and guidance, and transition and interoperability approaches for deployment in legacy networks.

2.2. Life Cycles and Change Management.

This document is the first major structural and technical revision of an IPv6 profiling effort first published in 2008. While IPv6 technologies and product offerings have matured and stabilized significantly over that period, they continue to evolve. Future revisions of this

[1] It is not uncommon to find products that claim to support IPv6 but are not fully functional in IPv6-only environments. Typically, it is the configuration, management and maintenance interfaces / stacks that are lacking full IP6 support.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

profile are expected to maintain the structure and format of this document, while only modifying the technical definitions of IPv6 capabilities within.

When a profile revision changes or adds significant new technical capabilities, it is unreasonable to expect the product and testing industry to be able to respond immediately. As a general principle, we recommend waiting at least 24 months between the addition of a significant new capability to the profile and its citation as a procurement requirement. Profile updates that are more incremental (e.g., errata, updates to existing capabilities) may be operative in less time. The profile capabilities table, marks all changes in capability requirements as being either new, or an update to existing previous requirements (see section 2.4)

Going forward, we expect to issue updates to this profile every two years. In general, when new revisions of the profile are published, we recommend that users cite the most recent version of this profile when appropriate and always include a specific indication of the version being referenced.

2.3. Statements of Requirements Levels

In general, the terminology used to describe requirements levels in this specification include: "mandatory", "optional" (with their common meaning), and "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" which are to be interpreted as described in [RFC2119].

2.4. Profile Capabilities Table.

The NISTv6 Capabilities Table (NCT) provides a concise tabular summary of the technical requirements of this profile. For ease of reference, the NCT is maintained as supplemental information to this profile and provided in a separate document. Readers are encouraged to access and review the NCT as an adjunct to this document.

- **NISTv6-r1 Capabilities Table - https://doi.org/10.6028/NIST.SP.500-267Ar1s**

The NCT is interpreted as follows:

- The NCT is organized in rows of references to IPv6 technical specifications, or specific subsections of specifications. The *Reference*, *Section* and *Title* columns provide the full context for each cited specification. For ease of readability if the Reference column is empty, the last Reference from the rows above is understood.
- The *Flag* column indicates changes from previous versions of the profile. ***N*** indicates that an RFC wasn't in a previous revision of the profile. ***U*** indicates that the RFC has been updated since the last revision of the profile. If the Flag Column is blank it indicates there is no change from the last revision of the profile.
- The *Capabilities* column defines the capability label (or conjunction or disjunction of multiple capabilities) that indicates support of the referenced technical specification.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Capabilities column may be logically joined with "|" and "&". The "|" stands for "or" indicating that having either capability will satisfy the requirement. The "&" stands for "and" indicating that both capabilities must be met to satisfy the requirement.

  - Some capability labels contain an "=" symbol. This is just a notational convenience to allow such labels to be easily grouped by name.

- The *Host*, *Router* and *Other* columns provide profile specific guidance for products in each specific functional role (see section 1.3). The values in each column provide recommendations as to which capabilities should be considered mandatory (**M**), optional (blank), or not recommended [**X**]. Entries with the notation "**O:1**" indicate that at least one of the listed capabilities is recommended to be selected. Entries that are grayed out in any of these columns indicate that the corresponding specification is typically not applicable to products in that functional role.
  - The capability selection guidance in provided in this profile is derived from the IETF *IPv6 Node Requirements* specification [RFC8504]. That is, the capabilities marked "**M**" in the NCT correspond to those specifications that are indicated as MUST in RFC 8504.

While the NCT 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 NCT for the purpose of developing requirement statements and to consult section 4 for guidance on interpreting the NCT for the expression of the capabilities of individual products.

2.5. Capability Summary Strings.

The primary purpose of this profile is to establish a vocabulary for expressing the IPv6 requirements for networked IT and documenting the IPv6 capabilities of specific products. The named IPv6 capability sets defined in the profile form the terms for this vocabulary. We form *Capability Summary Strings (CSS)* from these terms to define a single specific requirement statement or to document the capabilities of a specific product.

Capability Summary Strings have the following syntax:

CSS_Name = Profile:Functional_Role + Capability + Capability + …

The following is an example of a specific CSS:

Example-Desktop-PC = NISTv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + [DHCP-Client | SLAAC] + Link=Ethernet

CSS definitions are used to develop both requirement statements and to document product capabilities. Use the following guidance to develop and interpret capability summary strings.

- **CSS_Name –** A shorthand name for the part of the CSS to the right of the "**=**" sign. The CSS_Name has only local significance and should be fully defined in a complete CSS before its use in isolation. If a CSS_Name is defined in a document, then one can refer to a complete specification by referring to both the source document and the

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

CSS. Two strings with the same CSS_Name are understood to be multiple parts of a single requirement or product description.

- **Profile –** The name of the specific profile and version that establishes the technical definitions of the capabilities and roles used in the CSS.
    - **NISTv6-r1** is the profile name associated with this document.
- **Functional_Role –** One of the functional roles identified in the cited profile.
    - **Host, Router, NPP, Switch,** and **App-Serv –** are the functional roles identified in this profile.
- **Capability + Capability + …** - A list of capability labels concatenated with "**+**" signs enumerating the IPv6 capabilities that comprise the CSS. When used as a requirement statement the capability list should be viewed at the minimal required set of capabilities necessary. When used to document a specific product, the list should include all the capabilities supported by the product.
    - When used as a requirement statement the capability list may indicate that any of a list of capabilities can fulfill the requirement. This is the equivalent of "O:1" notation in the NCT. In the example above, "[**DHCP-Client | SLAAC**]" indicates that at least one of these capabilities MUST be supported. Note this O:1 notation is not used when documenting the capabilities of specific products. All capabilities supported should just be listed.
    - When used to describe the capabilities of a specific products, support for multiple alternatives is expressed by simple concatenation of labels with "+". For example, a product that supported both forms of address configuration mentioned above would simply include the substring "… **+ DHCP-Client + SLAAC +** …".

As previously noted, real networked IT products often contain multiple logically or physically distinct IPv6 protocol stacks that may perform different functional roles as defined in this profile. For example, an IPv6 Router that also includes Host functions to support its configuration and management. It is not uncommon to require multiple CSS to fully describe the IPv6 capabilities of a modern IT product.

The flexibility provided by CSS specifications can represent a vast range of capabilities and features found in modern networked IT products and services. Having this flexibility avoids the artificial constraints of standardizing a priori a small set of product configurations that could not possibly capture the full variety of current or future networked IT products.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

2.6. Conformance, Testing and Reporting.

This profile establishes the means to describe the IPv6 capabilities required of and implemented by networked IT products. Users of this profile will rely on capability summary strings to document both IPv6 requirement statements and product capabilities. Those developing procurement specifications will use this profile to develop or cite specific CSS that define the IPv6 capabilities required in product offerings.

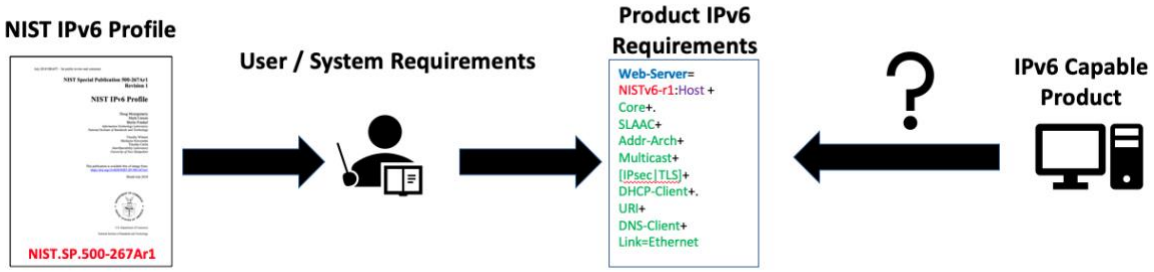

Figure 2 Development of IPv6 procurement requirements.

Vendors will use this profile to document the IPv6 capabilities of their products as well. It is meaningless to claim conformance to this profile alone. The only meaningful statement of product conformance is to a specific CSS that has been defined in terms this profile. In general, it is envisioned that vendors will document the IPv6 capabilities of their products by reporting CSS that include all of the IPv6 capabilities supported by a specific product.

In many situations users may desire additional assurances of the completeness, correctness and interoperability of the IPv6 capabilities provided by vendor products. In these situations, specific user groups may develop additional guidance on testing and reporting requirements for vendor supplied CSS. Testing guidance might require demonstrated conformance and/or interoperability testing results (potentially from independent testing sources) and/or specific additional means of documenting and reporting the results from such testing.

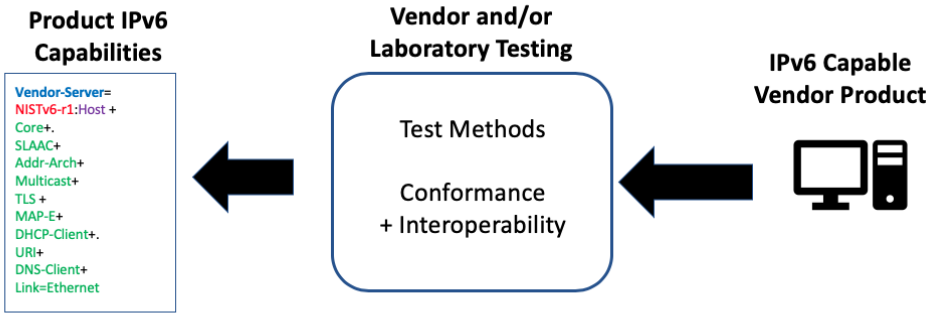

Figure 3 Documenting IPv6 product capabilities

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

User groups wishing such levels of additional assurance are encouraged to fully document the details of how such detailed testing and reporting mechanisms are to be conducted and how they will result in the derivation of one or more CSS for individual products.

When both purchasers and vendors use CSS statements based upon this profile, it should be possible to perform a simple matching function to determine if a product offering satisfies a specific requirement statement.

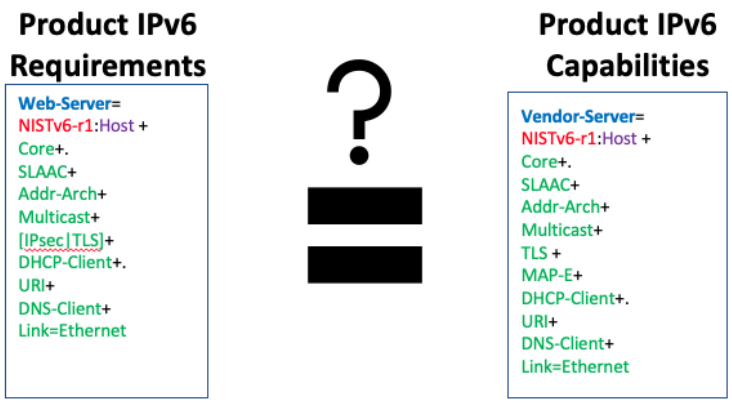

Figure 4 Matching IPv6 procurement requirements to product capabilities.

While the goal of this profile is to enable users and vendors to compare and match stated requirements to the documented capabilities of products, the profile and CSS derived from it are still valuable if only one side of this process is exercised. In particular, product capability summary strings are useful "full disclosure" statements of the IPv6 features that purchasers can expect, even if a corresponding CSS requirement statement was not provided.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

3. Selection of IPv6 Capabilities

The subsections that follow provide templates to facilitate the selection of capabilities for the purpose of developing requirement statements. The subsections are organized by the functional roles identified in this profile (i.e., Host, Router, NPP, App-Serv). Within each subsection capabilities are arranged in groups of related functions (e.g., Addressing Capabilities, Routing Capabilities).

For each capability a recommended requirement level is indicated. The notations used to indicate the requirement level of each capability include:

- **[M]** – Mandatory, it is recommended that this capability be included in all CSS for this functional role. For example, all Host CSS should include the **Core** capability.
- **[O:1]=[Capability1 | Capability2]** – Choice, it is recommended that at least one of the indicated list of capabilities be included in all CSS for this functional role.
- **[O]** – Optional, the profile user can choose to include this capability in CSS as needed. Note, in capability tables, optional is denoted by a blank cell.
- **[X]** – Not recommended for the profile uses described in the scope and applicability section. Such capabilities are included in the profile to maintain alignment with other profiles and/or to document the full range of possibilities.

Users should be conservative in the selection of optional capabilities when developing requirement statements. While there are many optional capabilities defined in this profile, they vary in their common availability in commodity network IT products. Users are recommended to survey the documented IPv6 capabilities of relevant products and/or to interact with potential vendors / system developers / integrators as part of the process of developing CSS requirement statements.

To further understand the detailed technical definition of the capabilities below, see the corresponding entries in the NISTv6-r1 Capabilities Table (section 2.4) and section 4 Technical Definition of IPv6 Capabilities. See section 5 for example CSS that incorporate these capabilities.

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

3.1. IPv6-Only Capabilities

There is no standard definition of what it means for products to capable operating in "IPv6-only" networks. This profile defines the **IPv6-Only** capability as requiring a product to support the full lifecycle of operation (i.e., product installation, configuration, operation, management, instrumentation and update) in environments with no IPv4 capabilities (e.g., either IPv4 is not implemented or is administratively disabled).

A product claiming support of the **IPv6-Only** capability must be fully functional when deployed in an IPv6-only network.

The **IPv6-Only** capability applies to a product as a whole and is applicable to each functional role defined in this profile. The technical definition of this capability is provided in section 4.1 of this profile but is the same for all product types. For the sake of clarity, we summarize these capabilities in a single location here.

NISTv6-r1:Host Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [O] – **IPv6-Only** - support for full product functionality on an IPv6-only network
NISTv6-r1:Router Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [O] – **IPv6-Only** - support for full product functionality on an IPv6-only network
NISTv6-r1:NPP Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [O] – **IPv6-Only** - support for full product functionality on an IPv6-only network
NISTv6-r1:Switch Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [O] – **IPv6-Only** - support for full product functionality on an IPv6-only network
NISTv6-r1:App-Serv Capabilities: • **IPv6-Only Capabilities** – see section 4.1   ○ [O] – **IPv6-Only** - support for full product functionality on an IPv6-only network

3.1.1. Selecting IPv6-Only Capabilities

Users of this profile may require any product to be capable of operating in IPv6-only environments.

- Common dual-stack deployments may not require **IPv6-Only** capabilities today, but there are several user group initiatives targeting migration to IPv6-only network infrastructures in the near future.
- Future revisions of the profile will likely recommend **IPv6-Only** as a mandatory requirement for all networked IT systems.
- When the **IPv6-Only** capability is indicated, it is implied that all other specified capabilities of a product, must operate in IPv6-only environments.

DRAFT

Note: At the time of publication of this document, few commercial products are fully capable of IPv6-only operation. Users of this profile should carefully consider the state of the marketplace before selecting this capability.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

3.2. Host Capabilities

A template of the various Host capabilities is given below along with references to sections of this profile that provide further discussion and interpretation of the requirements.

NISTv6-r1:Host Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [O] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section 4.2
  - [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 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] - **PrivAddr** - support for SLAAC privacy extensions.
  - [O] - **DHCP-Stateless** - support for stateless (DHCP) configuration.
  - [O] - **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 4.7
  - [M] - **Addr-Arch** - support for address architecture and selection.
  - [O] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities** - see section 4.11
  - [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 additional DHCP options and Bulk Leasequery.
  - [O] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Security Capabilities** - see section 4.8
  - [O] - **IPsec** - support for the IP security architecture.
  - [O] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [O] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [O] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.
  - [**O**] - **SSHV2** - support for SSHv2 over IPv6.
  - [O] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [O] - **TLS-1.3** - support for Transport Layer Security architecture version 1.3.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- **Transition Mechanism Capabilities** - see section 4.5
    - [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 4.9
    - [O] - **SNMP** - support for simple network management protocol.
    - [O] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities** - see section 4.10
    - [O] - **SSM** - require full support for multicast communications.
    - [M] - **Multicast** - support for link-local multicast communication.
- **Quality of Service Capabilities** - see section 4.4
    - [O] - **DiffServ** - support for Differentiated Services capabilities.
    - [O] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities** - see section 4.6
    - [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.

3.2.1. Selecting Host Capabilities

The following guidance is provided for selecting capabilities from this section.

- **Core**, **SLAAC**, **Multicast**, and **Addr-Arch** capabilities are recommended to be mandatory in all systems.

- For systems that will be deployed on potentially lossy networks with specific features, users will want to consider requiring neighbor discovery and compression extension capabilities of **ND-WL** and **6Lo**.

- IPv6 Neighbor Discovery has several optional updates that provide optimizations in some use case scenarios. Users may want to require **ND-EXT** for a more robust solution in these deployment scenarios.

- User may want to require additional methods to mitigate packet loss due to fragmentation. An alternative to Path MTU Discovery required in Core is Packetization Layer Path MTU Discovery (**PLPMTUD**) designed for use over paths where end-to-end delivery of ICMPv6 messages is not assured.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- Capabilities to secure neighbor discovery include **ND-SEND** and **CGA**. Note, to date these capabilities are not commonly implemented in commodity systems and should be required only when necessary.

- Privacy addressing features are provided by the **PrivAddr** capability. Note: Certain use cases, such as Enterprise deployments, may not want this capability enabled as it makes tracking IP addresses difficult.

- Systems that will use stateful address and configuration management (i.e., DHCPv6) should require **DHCP-Client**. **DHCP-Prefix** allows for assigning address ranges to a system that will sub-allocate addresses to other nodes and network functions. **DHCP-Stateless** should be required when **SLAAC** is the only supported address configuration protocol and additional network configuration information is necessary.

- **DHCP-Client-Ext** includes support for additional DHCPv6 options including SIP. **DHCP-Prefix-Ext** adds support for the Prefix Exclude Option.

- **Happy-Eyeballs** is an algorithm that enhances the robustness and performance of dual-stack systems by trying to contact remote systems with both IPv4 and IPv6 in parallel. Whichever protocol receives the first response is used for the remainder of the communication. Edge Dual stack networks should consider requiring this capability.

- The capability to operate DNS over IPv6 is available for both client and server. The **DNS-client** and **DNS-server** capabilities require products to support DNS resolution for IPv6 address records and for DNS queries over native IPv6.

- Users of DHCPv6 for network addressing and information will want to select **DHCP-Server** for the systems managing network address and configuration information. Additional DHCPv6 Server functions, such as Bulk Leasequery, are included in **DHCPv6-Server-Ext** that may be required for advanced DHCPv6 deployments.

- Users requiring support for the Network Time Protocol will want to require **NTP-server** and **NTP-client** capabilities where appropriate.

- Secure end-to-end communications channels can be required by selecting either **TLS, SSH** or **IPsec** capabilities. **IPsec-IoT**, **IPsec-CHACHA**, **IPsec-SHA-512** are additional algorithms and must only be selected when IPsec is selected. The **IPSec-VPN** capability is for secure data plane channels in router products. Similarly, **IPsec-IOT-VPN**, **IPsec-IOT-CHACHA-VPN**, and **IPsec-SHA-512-VPN** must only be selected when **IPsec-VPN** is selected.

- The **SSHv2** capability defines the suite of RFCs for supporting SSHv2 over IPv6.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- The **TLS** capability is currently defined in terms of the TLS1.2 specification. The **TLS-1.3** capability is available for users that need the enhanced security features of the new specification and understand the operational implications of its use.

- Users have several options for transition mechanisms when deploying IPv6. The capabilities in this profile primarily focus on transition over IPv6-only networks. Host based transition mechanisms include **Tunneling-IP**, **Tunneling-UDP** and **XLAT**. To support XLAT both **NAT64** and **DNS64** are included as additional functions that are required but often are embedded in different products.

- Systems that require remote management and configuration should elect either **NETCONF** or **SNMP** capabilities. Note: commodity Host products do not commonly support either of these remote management capabilities.

- The **Multicast** capability is specifically defined for link-local multicast necessary to support protocols such as Neighbor Discovery. The **SSM** capability allows for a host to support source specific multicast requirements.

- Systems can indicate support for IPv6 Quality of Service using the **DiffServ** or **ECN** capabilities. Note that in scenarios where QoS is required, both Hosts and Routers should support the corresponding capabilities.

- The Link Specific Capabilities indicate support for IPv6 mapping to specific layer 2 technologies. Most commodity products support **Link=Ethernet** (which includes WiFi), but other link technologies can be indicated. A CSS for a single system may include multiple Link capabilities for distinct physical interfaces.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

3.3. Router Capabilities

A template of the various Router capabilities is given below along with references to sections of this profile that provide further discussion and interpretation of the requirements.

NISTv6-r1:Router Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [O] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section 4.2
  - [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 4.7
  - [M] - **Addr-Arch** - support for address architecture and selection.
  - [O] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities** - see section 4.11
  - [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 additional options and Bulk Lease query.
  - [O] - **DHCP-Relay** - support for DHCP relay capabilities.
- **Routing Capabilities** - see section 4.3
  - [**O**] - **OSPF** - support for OSPF for intra-domain routing protocol.
  - [**O**] - **OSPF-IPsec** - support for OSPF Authentication/Confidentiality using IPSec.
  - [**O**] - **OSPF-Auth** - support for OSPF Authentication Trailer.
  - [**O**] - **OSPF-Ext** - support for additional OSPF robustness and optimization features.
  - [**O**] - **OSPF-Trans** - support for OSPF IPv4 over IPv6.
  - [**O**] - **OSPF-Graceful** - support for OSPF Graceful restart.
  - [**O**] - **IS-IS** - support for IS-IS for intra-domain routing protocol.
  - [**O**] - **IS-IS-Auth** - support for IS-IS Authentication support.
  - [**O**] - **IS-IS-Ext** - support for additional IS-IS robustness and optimization features.
  - [**O**] - **IS-IS-MT** - support for Multi Topology in IS-IS.
  - [**O**] - **BGP** - support for BGP for inter-domain routing protocols.
  - [**O**] - **BGP-Reflect** - support for BGP Route Reflection
  - [**O**] - **BGP-Graceful** - support for BGP Graceful Restart
  - [**O**] - **BGP-FlowSpec** - support for BGP FlowSpec capabilities.
  - [**O**] - **BGP-OV** - support for BGP Origin Validation capabilities.

DRAFT

- [**O**] - **BGP-VPLS** - support for BGP VPLS capabilities.
- [**O**] - **BGP-EVPN** - support for BGP EVPN capabilities.
- [**O**] - **BGP-6VPE** - support for BGP 6VPE capabilities.
- [**O**] - **BGP-MVPN** - support for BGP MVPN capabilities.
- [**O**] - **MPLS** - support for MPLS IPv6 capabilities.
- [**O**] - **CE-Router** - support for customer edge router capabilities.
- [**O**] - **VRRP** - support for VRRP Routing protocols.

- **Security Capabilities** - see section 4.8
  - [O] - **IPsec** - support for the IP security architecture.
  - [O] - **IPsec-VPN** - support for the IP security architecture gateways.
  - [O] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [O] - **IPsec-IoT-VPN** - support for IoT Cryptographic Algorithms in gateways.
  - [O] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [O] - **IPsec-CHACHA-VPN** - support for ChaCha20 Cryptographic Algorithms in gateways.
  - [O] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.
  - [O] - **IPsec-SHA-512-VPN** - support for SHA-512 Cryptographic Algorithms in gateways.
  - [O] - **SSHV2** - support for SSHv2 over IPv6.
  - [O] - **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 4.5
  - [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 4.9
  - [O] - **SNMP** - support for simple network management protocol.
  - [O] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities** - see section 4.10
  - [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-IPsec** - support for PIM-SM over IPsec.
  - [O] - **PIM-SM-BiDir** - support for Bidirectional PIM-SM routing protocol.
- **Quality of Service Capabilities** - see section 4.4
  - [O] - **DiffServ** - support for Differentiated Services capabilities.
  - [O] - **ECN** - support for Explicit Congestion Notification.
- **Link Specific Capabilities** - see section 4.6
  - [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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

3.3.1. Selecting Router Capabilities

The following guidance is provided for selecting capabilities from this section.

- **Core**, **SLAAC**, **Multicast**, and **Addr-Arch** capabilities are recommended to be mandatory in all systems.

- For systems that will be deployed on potentially lossy networks with specific features, users will want to consider requiring neighbor discovery and compression extension capabilities of **ND-WL** and **6Lo**.

- IPv6 Neighbor Discovery has several optional updates that provide optimizations in some use case scenarios. Users may want to require **ND-EXT** for a more robust solution in these deployment scenarios.

- Capabilities to secure neighbor discovery include **ND-SEND** and **CGA**. Note these capabilities are not commonly implemented on commodity systems and should be required only when necessary.

- The capability to operate DNS over IPv6 is available for both client and server. The **DNS-client** and **DNS-server** capabilities require products to support DNS resolution for IPv6 address records and for DNS queries over native IPv6.

- Users of DHCPv6 for network addressing and information will want to select **DHCP-Server** for the routers that managing network address and configuration information. Additional DHCPv6 Server functions such as Bulk Leasequery are included in **DHCPv6-Server-Ext** capability to allow for advanced DHCPv6 deployments.

- **DHCP-Prefix** allows for routers to delegate address ranges to either host or router. **DHCP-Prefix-Ext** allows for users that require the PD-Exclude Option for deployments.

- **DHCP-Relay** will commonly be selected on routers in DHCPv6 networks.

- Users requiring support for the Network Time Protocol will want to require **NTP-server** and **NTP-client** capabilities where appropriate.

- The **OSPF** capability includes the OSPF over IPv6 Routing Protocol functionality. Additional capabilities such as **OSPF-IPSec**, **OSPF-Auth**, **OSPF-Ext**, **OSPF-Trans** and **OSPF-Graceful** allow for additional feature parity with existing IPv4 features.

- The **IS-IS** capability includes IS-IS over IPv6 Routing Protocol functionality. Requirements such as **IS-IS-Auth**, **IS-IS-Ext**, and **IS-IS-MT** allow for additional feature parity with existing IPv4 features.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- The **BGP** capability includes the collection of RFCs necessary for BGP operation over IPv6. **BGP-FlowSpec** and **BGP-OV** allow for additional BGP security. BGP capabilities support additional BGP extensions including **BGP-Reflect, BGP-Graceful, BGP-VPLS**, **BGP-EVPN**, **BGP-MVPN** and **BGP-6VPE**, which may be required if a user is already deploying these features in IPv4.

- The **MPLS** capability allows for running MPLS over an IPv6 network.

- The **CE-Router** capability is for small routers often provided by a service provider and used for the home or small business networks.

- The **VRRP** capability allows for support of an IPv6 routing redundancy Protocol.

- Secure end-to-end communications channels can be required by selecting either **TLS, SSHv2** or **IPsec** capabilities. **IPsec-IoT**, **IPsec-CHACHA**, **IPsec-SHA-512** are additional algorithms and must only be selected when IPsec is selected. The **IPSec-VPN** capability is for secure data plane channels for routers products. Similarly, **IPsec-IOT-VPN**, **IPsec-IOT-CHACHA-VPN**, and **IPsec-SHA-512-VPN** must only be selected when **IPsec-VPN** is selected.

- The **SSHv2** capability defines the suite of RFCs for supporting SSHv2 over IPv6.

- The **TLS** capability is currently defined in terms of the TLS1.2 specification. The **TLS-1.3** capability is available for users that need the enhanced security features of the new specification and understand the operational implications of its use.

- Users have several options for transition mechanisms when deploying IPv6. The capabilities in this profile primarily focus on transition over IPv6-only networks. Users will need carefully select from the following Router based transition mechanisms: **Tunneling-IP**, **Tunneling-UDP**, **GRE**, **DS-Lite**, **LW4over6**, **MAP-E**, **MAP-T**, **6PE**, **XLAT**, **DNS64**, **NAT64** and **LISP**.

- Systems that require remote management and configuration should select either **NETCONF** or **SNMP** capabilities.

- The **Multicast** capability is specifically defined for link-local multicast necessary to support protocols such as Neighbor Discovery. The **SSM** capability allows for both a router to support source specific multicast requirements.

- The **PIM-SM** capability allows for support of routing multicast groups. **PIM-SM-IPsec** allows for security of **PIM-SM**. **PIM-SM-BiDir** allows for a user to require that a router support Bidirectional PIM-SM.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- Systems can indicate support for IPv6 Quality of Service using the **DiffServ** or **ECN** capabilities. Note that in scenarios where QoS is required, both Hosts and Routers should support the corresponding capabilities.

- The Link Specific Capabilities indicate support for IPv6 mapping to specific layer 2 technologies. Most commodity products support **Link=Ethernet** (which includes WiFi), but other link technologies can be indicated. A CSS for a single system may include multiple Link capabilities for distinct physical interfaces.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

3.4. Network Protection Product Capabilities

A template of the various Network Protection Product capabilities is given below along with references to sections of this profile that provide further discussion and interpretation of the requirements.

NISTv6-r1:NPP (Network Protection Product) Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [O] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Network Protection Capabilities** - see section 4.14
  - [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.

3.4.1. Selecting Network Protection Product Capabilities

The following guidance is provided for selecting capabilities from this section.

- For Network Protection Products the profile identifies four basic capabilities for common usage scenarios. A CSS for an NPP should include one or more of these capabilities. Note that all NPP capabilities include a common base set of technical requirements (see section 4.12.3).
- Products in this space often have highly specialized, sometimes non-standard (for security purposes) implementations of many other Host and Router IPv6 capabilities. Where these additional required capabilities follow the standards for their use in other functional roles, they can be included as an additional CSS string for that role.
  - For example, a firewall that provides full support of OSPF and operates over Ethernet could add those capabilities.
    - **FW = NISTv6-r1:NPP + FW**
    - **FW-Router = NISTv6-r1:Router + OSPF + Link=Ethernet**
  - Care must be taken in selecting standard Host or Router capabilities for NPPs because often such security products have non-standard implementations of core protocols (often in the areas of error reporting, etc.).

DRAFT

3.5. Switch Capabilities

A template of the various IPv6 Switch capabilities is given below along with references to sections of this profile that provide further discussion and interpretation of the requirements.

NISTv6-r1:Switch Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [O] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Switch Capabilities** - see section 4.13
  - [O] - **DHCPv6-Guard** - support for DHCPv6 Guard at Layer 2.
  - [O] - **RA-Guard** - support for RA Guard at Layer 2.
  - [O] - **MLD-Snooping** - support for MLD Snooping at Layer 2.

3.5.1. Selecting Switch Capabilities

The following guidance is provided for selecting capabilities from this section.

- A user is deploying DHCPv6 should consider requiring switches to support **DHCPv6-Guard** to protect against rogue DHCPv6 Servers which can be a security risk.
- A user is deploying SLAAC for host addressing they should consider requiring switches to support **RA-Guard** for protecting against rogue Router Advertisements which can be a security risk.
- **MLD-Snooping** should be required in use cases deploying multicast applications as it allows switches to only forward IPv6 multicast traffic to the listening ports.
- Products in this space often have additional IP stacks that are distinct from the layer 2 switching and provide functionality such as switch management and configuration. Where these additional required capabilities follow common standards, they can be specified as an additional CSS string for that role.
  - For example, a switch that provides full Host support for management purposes.
    - **Switch = NISTv6-r1:Switch + DHCPv6-Guard + RA-Guard + MLD-Snooping.**
    - **Switch-Host = NISTv6-r1:Host + IPv6-Only + Core + [SLAAC|DHCP-Client] + Addr-Arch + Multicast + Link=Ethernet.**

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

3.6. Application and Services Capabilities

A template of the various Application and Service capabilities is given below along with references to sections of this profile that provide further discussion and interpretation of the requirements.

NISTv6-r1:App-Serv (Application and Services) Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.1
  - [O] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Application and Services Capabilities** - see section 4.12
  - [O] - **App-Serv=[TBD]** - support for application/service specific functions (to be individually specified) over IPv6.

3.6.1. Selecting Application and Services Capabilities

The following guidance is provided for selecting capabilities from this section.

- The number of unique networked applications is vast, making it impossible to develop a priori detailed capability definitions for specific products. The general framework above allows users to develop specifications for generic application / service IPv6 requirements and then to enumerate additions requirements specific to the applications. Note when developing such requirements, it is recommended to use one CSS per application. An example of a simple network attached storage might be:
  - **NAS-Host = NISTv6-r1:Host + IPv6-Only + Core + Multicast + Addr-Arch**
  - **NAS-Apps = NISTv6-r1:App-Server + IPv6-Only + App-Serv=[NFS & SMB & AFS]**
- The phrase "over IPv6" is understood to mean that the application or service capability is fully functional, with feature parity to its operation over IPv4, when operating over native IPv6.
- When combined with the **IPv6-Only** capability requirement, the application must be fully functional on a network without IPv4 services.

DRAFT

4. Technical Definition of IPv6 Capabilities

The subsections that follow provide the full technical definition of the IPv6 capabilities defined in this profile. In general, the technical definitions are expressed as a mapping a NISTv6-r1 named capability to RFC specifications. A given capability might map to a one or more RFC specifications, or a specific subsection of a specification. In areas in which IETF specifications are lacking (e.g., network protection products), this profile defines the technical requirements associated with the relevant capabilities.

By default, when a profile capability is defined in terms of an IETF specification, it means that all the mandatory (e.g., MUST and MUST NOT) requirements of the specification must be met. In some rare cases this profile might specifically call out an optional feature of an IETF specification as being required for the capability.

Note that some technical specifications are indicated by either the conjunction or disjunction of labeled capabilities (e.g., **SNMP & DiffServ**, **FW or IDS or IPS or APFW**). For those specifications that are indicated by a disjunction of multiple capabilities, we list them under each capability individually. That is, the referenced specification(s) will appear multiple times. When a specification is only required with the conjunction of capabilities (e.g., **SNMP & DiffServ**), we will list the combination as its own capability definition.

For each named capability and corresponding technical requirement, the capability definition tables indicate (by check marks) the functional roles (e.g., Host, Router, Other) for which the definition is applicable. The flag column also indicates if the requirements are new (**N**), updated (**U**), or unchanged (blank) from the previous version of this profile.

To further understand the detailed technical definition of the capabilities below, see the corresponding entries in the NISTv6-r1 Capabilities Table (section 2.4). See section 5 for example CSS that incorporate these capabilities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.1. IPv6-Only Capabilities

There is no standard definition of what it means for products to capable operating in "IPv6-only" networks. This profile defines the **IPv6-Only** capability as requiring a product to support the full lifecycle of operation (i.e., product installation, configuration, operation, management, instrumentation and update) in environments with no IPv4 capabilities (e.g., either IPv4 is not implemented in the product or is administratively disabled, or IPv4 is not provided on the network).

A product claiming support of the **IPv6-Only** capability must be fully functional when deployed in an IPv6-only network and provide no less functionality than is currently available in IPv4 environments.

The **IPv6-Only** capability applies to a product as a whole and is applicable to each functional role defined in this profile. The technical definition of this capability is provided in the section below.

4.1.1. Definition of IPv6-only Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

IPv6-Only Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓	✓	**IPv6-Only**	**support for full product functionality on an IPv6-only network.**
N	✓	✓	✓		SP500-267Ar1 Section: 4.1 Install product over IPv6-only network *NIST IPv6 Profile*
N	✓	✓	✓		SP500-267Ar1 Section: 4.1 Product user Interface fully supports IPv6 *NIST IPv6 Profile*
N	✓	✓	✓		SP500-267Ar1 Section: 4.1 Manage product over IPv6-only network *NIST IPv6 Profile*
N	✓	✓	✓		SP500-267Ar1 Section: 4.1 Update product over IPv6-only network *NIST IPv6 Profile*

The detailed implications of the **IPv6-Only** capability will vary with product implementation environments (e.g., operating systems, management and control software, applications, etc.) but the functional requirements are the same. The functional requirements of this capability include:

- The product is fully functional in IPv6 network environments in which no IPv4 services are provisioned.

DRAFT

- A product that conforms to the **IPv6-Only** capability must support operation of all its other claimed capabilities in IPv6-only networks.

- The product must support full product lifecycle functions (defined below) in an IPv6-only context. Note that often the product support functions below are often provided by additional applications or functions distinct from the main function of the product (e.g., installer applications, update applications, management applications for an OS).
  - Installation – the product or service must be able to be instantiated and installed on nodes and in network environments that do not provide IPv4 services. Initial configuration of the product to a state where other remote services are operational, are part of the installation functions.
  - User Interface – all forms of interactive access to the product (e.g., web-based interfaces or APIs) must fully support the use of IPv6 and IPv6 addresses of all forms.
    - If the product displays IP addresses, then IPv6 addresses must be displayed according to [RFC5952].
  - Management – all forms of remote management and monitoring functions must be fully functional in IPv6-only environments.
  - Update – all forms of product update functions (e.g., software, BIOS updates), both automated and user initiated, must be fully functional in IPv6-only environments.

It is expected that the definition of the **IPv6-Only** capability may evolve over time. While **IPv6-Only** is currently defined as a separate optional capability in this version of the profile, over time, this requirement may become an implicit part of all capability definitions. That is, in the future we would expect all products to be fully capable of IPv6-only operation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.2. Basic Capabilities

The Basic capabilities group consists of the fundamental protocols necessary for basic IPv6 operations. This includes capabilities for the base IPv6 and ICMPv6 protocols, neighbor discovery protocol (plus numerous ND enhancements), and auto configuration protocols (DHCP and SLAAC). Note that this version of the profiles does require support for non EUI-64 addresses in SLAAC.

4.2.1. Definition of Basic Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Basic Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**Core**	**support for IPv6 core functions.**
U	✓	✓			RFC8200 *Internet Protocol, Version 6 (IPv6) Specification*
	✓	✓			RFC4443 *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
U	✓	✓			RFC8201 *Path MTU Discovery for IP version 6*
	✓	✓			RFC4861 *Neighbor Discovery for IP version 6 (IPv6)*
	✓	✓			RFC4861 Section: 8 Redirect *Neighbor Discovery for IP version 6 (IPv6)*
N	✓	✓			RFC6437 *IPv6 Flow Label Specification*
N	✓	✓			RFC5942 *IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*
N	✓	✓			RFC6980 *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*
N		✓			RFC7608 *IPv6 Prefix Length Recommendation for Forwarding*
N	✓	✓			RFC4191 *Default Router Preferences and More-Specific Routes*
	✓	✓			RFC4862 Section: 5.3 Creation of Link Local Addresses *IPv6 Stateless Address Autoconfiguration*
	✓	✓			RFC4862 Section: 5.4 Duplicate Address Detection *IPv6 Stateless Address Autoconfiguration*
	✓	✓		**Extended-ICMP**	**support for ICMPv6 extended messages.**
	✓	✓			RFC4884 *Extended ICMP to Support Multi-Part Messages*

DRAFT

Basic Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**PLPMTUD**	**support for Packetization Layer Path MTU Discovery.**
N	✓	✓			RFC4821 *Packetization Layer Path MTU Discovery*
	✓	✓		**ND-Ext**	**support for Neighbor Discovery features of enhanced DAD and First-Hop Selection.**
N	✓	✓			RFC4429 *Optimistic Duplicate Address Detection (DAD) for IPv6*
N	✓	✓			RFC7527 *Enhanced Duplicate Address Detection*
N	✓	✓			RFC8028 *First-Hop Router Selection by Hosts in a Multi-Prefix Network*
	✓	✓		**ND-WL**	**support for packet-loss for router solicitations.**
N	✓	✓			RFC7048 *Neighbor Unreachability Detection Is Too Impatient*
N	✓	✓			RFC7559 *Packet-Loss Resiliency for Router Solicitations*
N	✓	✓			RFC8319 *Support for Adjustable Maximum Router Lifetimes per Link*
	✓	✓		**SEND**	**support for neighbor discovery security extensions.**
	✓	✓			RFC3971 *SEcure Neighbor Discovery (SEND)*
	✓	✓			RFC6494 *Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)*
	✓	✓			RFC6495 *Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields*
	✓	✓		**SLAAC**	**support for stateless global address auto-configuration.**
	✓	✓			RFC4862 *IPv6 Stateless Address Autoconfiguration*
	✓	✓			RFC4862 Section: 5.5 Creation of Global Addresses *IPv6 Stateless Address Autoconfiguration*
N	✓	✓			RFC8106 *IPv6 Router Advertisement Options for DNS Configuration*
N	✓				RFC7217 *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*
	✓			**PrivAddr**	**support for SLAAC privacy extensions.**
	✓				RFC4941 *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*
	✓			**DHCP-Stateless**	**support for stateless (DHCP) configuration.**
U	✓				RFC8415 *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Basic Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓			**DHCP-Client**	**support for stateful (DHCP) address auto-configuration.**
U	✓				RFC8415 *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
	✓				RFC3646 *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
	✓			**DHCP-Client-Ext**	**support for additional DHCP options including SIP.**
N	✓				RFC3319 *Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers*
	✓	✓		**DHCP-Prefix**	**support for stateful (DHCP) prefix delegation.**
U	✓	✓			RFC8415 *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
	✓	✓		**DHCP-Prefix-Ext**	**support for additional DHCP options for prefix exclude using prefix delegation.**
N	✓	✓			RFC6603 *Prefix Exclude Option for DHCPv6-based Prefix Delegation*
	✓	✓		**6Lo**	**support for IPv6 over low power networks.**
N	✓	✓			RFC6282 *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*
N	✓	✓			RFC6775 *Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*
	✓			**Happy-Eyeballs**	**support for Happy Eyeballs algorithm for dual stack environments.**
N	✓				RFC8305 *Happy Eyeballs Version 2: Better Connectivity Using Concurrency*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.3. Routing Capabilities

The Routing capabilities group consists of capabilities for IPv6 routing protocols for enterprise and wide-area network usage scenarios and the CE-Router capability for typical home or small office routers. Both OSPFv3 and IS-IS contain routing mechanisms that are unchanged when using IPv4 or IPv6. As stated in OSPFv3 RFC these mechanisms are documented RFC 2328. IS-IS routing mechanisms are documented in RFC 1195.

This revision of the profile contains more OSPF, IS-IS and BGP extensions with the intention of keeping parity between IPv4 and IPv6.

4.3.1. Definition of Routing Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Routing Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
		✓		**OSPF**	**support for OSPF for intra-domain routing protocol.**
U		✓			RFC5340 *OSPF for IPv6*
N		✓			RFC5613 *OSPF Link-Local Signaling*
		✓		**OSPF-IPsec**	**support for OSPF Authentication/Confidentiality using IPSec.**
		✓			RFC4552 *Authentication/Confidentiality for OSPFv3*
		✓		**OSPF-Auth**	**support for OSPF Authentication Trailer.**
N		✓			RFC7166 *Supporting Authentication Trailer for OSPFv3*
		✓		**OSPF-Ext**	**support for additional OSPF robustness and optimization features.**
N		✓			RFC5838 *Support of Address Families in OSPFv3*
N		✓			RFC6845 *OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type*
N		✓			RFC6860 *Hiding Transit-Only Networks in OSPF*
N		✓			RFC8362 *OSPFv3 Link State Advertisement (LSA) Extensibility*
N		✓			RFC5185 *OSPF Multi-Area Adjacency*
		✓		**OSPF-Trans**	**support for OSPF IPv4 over IPv6.**
N		✓			RFC7949 *OSPFv3 over IPv4 for IPv6 Transition*
		✓		**OSPF-Graceful**	**support for OSPF Graceful restart.**

Routing Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N		✓			RFC5187 *OSPFv3 Graceful Restart*
N		✓			RFC8379 *OSPF Graceful Link Shutdown*
		✓		**IS-IS**	**support for IS-IS for intra-domain routing protocol.**
N		✓			RFC5308 *Routing IPv6 with IS-IS*
		✓		**IS-IS-Auth**	**support for IS-IS Authentication support.**
N		✓			RFC5304 *IS-IS Cryptographic Authentication*
N		✓			RFC5310 *IS-IS Generic Cryptographic Authentication*
		✓		**IS-IS-Ext**	**support for additional IS-IS robustness and optimization features.**
N		✓			RFC7775 *IS-IS Route Preference for Extended IP and IPv6 Reachability*
N		✓			RFC6232 *Purge Originator Identification TLV for IS-IS*
N		✓			RFC6233 *IS-IS Registry Extension for Purges*
N		✓			RFC5301 *Dynamic Hostname Exchange Mechanism for IS-IS*
		✓		**IS-IS-MT**	**support for Multi Topology in IS-IS.**
N		✓			RFC5120 *M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*
		✓		**BGP**	**support for BGP for inter-domain routing protocols.**
		✓			RFC4271 *A Border Gateway Protocol 4 (BGP-4)*
		✓			RFC4760 *Multiprotocol Extensions for BGP-4*
		✓			RFC2545 *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
N		✓			RFC5492 *Capabilities Advertisement with BGP-4*
N		✓			RFC6286 *Autonomous-System-Wide Unique BGP Identifier for BGP-4*
N		✓			RFC6608 *Subcodes for BGP Finite State Machine Error*
N		✓			RFC6793 *BGP Support for Four-Octet Autonomous System (AS) Number Space*
N		✓			RFC7606 *Revised Error Handling for BGP UPDATE Messages*
N		✓			RFC7607 *Codification of AS 0 Processing*
N		✓			RFC7705 *Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Routing Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N		✓			RFC8212 *Default External BGP (EBGP) Route Propagation Behavior without Policies*
		✓		**BGP-Reflect**	**support for BGP Route Reflection**
N		✓			RFC4456 *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
		✓		**BGP-Graceful**	**support for BGP Graceful Restart**
N		✓			RFC4724 *Graceful Restart Mechanism for BGP*
		✓		**BGP-FlowSpec**	**support for BGP FlowSpec capabilities.**
N		✓			RFC5575 *Dissemination of Flow Specification Rules*
N		✓			RFC7674 *Clarification of the Flowspec Redirect Extended Community*
		✓		**BGP-OV**	**support for BGP Origin Validation capabilities.**
N		✓			RFC6811 *BGP Prefix Origin Validation*
N		✓			RFC8481 *Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)*
N		✓			RFC8097 *BGP Prefix Origin Validation State Extended Community*
N		✓			RFC8210 *The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1*
		✓		**BGP-VPLS**	**support for BGP VPLS capabilities.**
N		✓			RFC4761 *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
		✓		**BGP-EVPN**	**support for BGP EVPN capabilities.**
N		✓			RFC7432 *BGP MPLS-Based Ethernet VPN*
		✓		**BGP-6VPE**	**support for BGP 6VPE capabilities.**
N		✓			RFC4659 *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
N		✓			RFC6565 *OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*
		✓		**BGP-MVPN**	**support for BGP MVPN capabilities.**
N		✓			RFC6515 *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Routing Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
		✓		**MPLS**	**support for MPLS IPv6 capabilities.**
N		✓			RFC7506 *IPv6 Router Alert Option for MPLS Operations, Administration, and Maintenance (OAM)*
N		✓			RFC7552 *Updates to LDP for IPv6*
		✓		**CE-Router**	**support for customer edge router capabilities.**
N		✓			RFC7084 *Basic Requirements for IPv6 Customer Edge Routers*
N		✓			RFC7084 Section: 4.5 Ingress Filtering (BCP38) *Basic Requirements for IPv6 Customer Edge Routers*
N		✓			RFC6092 *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*
		✓		**VRRP**	**support for VRRP Routing protocols.**
N		✓			RFC5798 *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.4. Quality of Service Capabilities

The Quality of Service capabilities group consists of the support for Differentiated Services QoS signaling and forwarding and support for Explicit Congestion Notification capabilities for congestion avoidance.

4.4.1. Definition of Quality of Service Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Quality of Service Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**DiffServ**	**support for Differentiated Services capabilities.**
	✓	✓			RFC2474 *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
	✓	✓			RFC3140 *Per Hop Behavior Identification Codes*
	✓	✓			RFC2597 *Assured Forwarding PHB Group*
	✓	✓			RFC3246 *An Expedited Forwarding PHB (Per-Hop Behavior)*
	✓	✓			RFC3247 *Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)*
	✓	✓		**ECN**	**support for Explicit Congestion Notification.**
	✓	✓			RFC3168 *The Addition of Explicit Congestion Notification (ECN) to IP*

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.5. Transition Mechanism Capabilities

The Transition Mechanisms capabilities group consists of multiple approaches to tunneling and interworking between IPv6 and IPv4 networks and Hosts. While the first technologies in this area focused on supporting tunneling IPv6 over IPv4, recent trends are for the reverse. It should be noted that IPv6 GRE (RFC 7676) requires support for RFC 2784 to make GRE functional.

4.5.1. Definition of Transition Mechanism Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Transition Mechanism Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**Tunneling-IP**	**support for generic packet encapsulation tunnels using IPv6.**
	✓	✓			RFC2473 *Generic Packet Tunneling in IPv6 Specification*
	✓	✓		**Tunneling-UDP**	**support for generic packet encapsulation tunnels using UDP.**
N	✓	✓			RFC6936 *Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums*
		✓		**GRE**	**support for generic router encapsulation tunnels.**
N		✓			RFC7676 *IPv6 Support for Generic Routing Encapsulation (GRE)*
		✓		**DS-Lite**	**support for transition mechanism DS-Lite.**
N		✓			RFC6333 *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*
		✓		**LW4over6**	**support for transition mechanism Lightweight 4over6.**
N		✓			RFC7596 *Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture*
		✓		**MAP-E**	**support for transition mechanism MAP-E.**
N		✓			RFC7597 *Mapping of Address and Port with Encapsulation (MAP-E)*
		✓		**MAP-T**	**support for transition mechanism MAP-T.**
N		✓			RFC7599 *Mapping of Address and Port using Translation (MAP-T)*
	✓	✓		**XLAT**	**support for transition mechanism 464XLAT.**
N	✓	✓			RFC6877 *464XLAT: Combination of Stateful and Stateless Translation*
N	✓	✓			RFC7915 *IP/ICMP Translation Algorithm*

Transition Mechanism Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**NAT64**	**support for transition mechanism NAT64.**
N	✓	✓			RFC6146 *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*
	✓	✓		**DNS64**	**support for transition mechanism DNS64.**
N	✓	✓			RFC6147 *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*
		✓		**6PE**	**support for 6PE.**
		✓			RFC4798 *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*
		✓		**LISP**	**support for LISP protocol.**
N		✓			RFC6830 *The Locator/ID Separation Protocol (LISP)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.6. Link Specific Capabilities

The Link Specific capabilities group consists of the specifications for mapping and encapsulating IPv6 over various layer 2 technologies. Systems with a diversity of interface types will have multiple Link capability specifications.

4.6.1. Definition of Link Specific Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Link Specific Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**Link=Ethernet**	**support for IPv6 over Ethernet.**
	✓	✓			RFC2464 *Transmission of IPv6 Packets over Ethernet Networks*
	✓	✓		**Link=PPP**	**support for IPv6 over PPP links.**
	✓	✓			RFC5072 *IP Version 6 over PPP*
	✓	✓		**Link=G.9959**	**support for IPv6 over Z-Wave.**
N	✓	✓			RFC7428 *Transmission of IPv6 Packets over ITU-T G.9959 Networks*
	✓	✓		**Link=Bluetooth**	**support for IPv6 over Bluetooth.**
N	✓	✓			RFC7668 *IPv6 over BLUETOOTH(R) Low Energy*
	✓	✓		**Link=BACnet**	**support for IPv6 over BACnet.**
N	✓	✓			RFC8163 *Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks*
	✓	✓		**Link=6LoWPAN**	**support for IPv6 over 802.15.4.**
N	✓	✓			RFC4944 *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.7. Addressing Capabilities

The Addressing capabilities group consists of the requirements for supporting the common IPv6 addressing architecture and some enhancements for cryptographically generated addresses. Note, the capabilities associated with Privacy Addressing are in the Basic Capabilities section along with other extensions that affect Neighbor Discovery protocol.

4.7.1. Definition of Addressing Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Addressing Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**Addr-Arch**	**support for address architecture and selection.**
	✓	✓			RFC4291 *IP Version 6 Addressing Architecture*
	✓	✓			RFC4007 *IPv6 Scoped Address Architecture*
	✓	✓			RFC4193 *Unique Local IPv6 Unicast Addresses*
	✓	✓			RFC3879 *Deprecating Site Local Addresses*
	✓	✓			RFC2526 *Reserved IPv6 Subnet Anycast Addresses*
U	✓	✓			RFC6724 *Default Address Selection for Internet Protocol Version 6 (IPv6)*
N	✓	✓			RFC5952 *A Recommendation for IPv6 Address Text Representation*
N	✓	✓			RFC7136 *Significance of IPv6 Interface Identifiers*
N		✓			RFC6164 *Using 127-Bit IPv6 Prefixes on Inter-Router Links*
N	✓	✓			RFC7346 *IPv6 Multicast Address Scopes*
	✓	✓		**Addr-Arch & DHCP-Client**	**applicable when both capabilities are selected.**
U	✓	✓			RFC7078 *Distributing Address Selection Policy Using DHCPv6*
	✓	✓		**CGA**	**support for cryptographically generated addresses.**
	✓	✓			RFC3972 *Cryptographically Generated Addresses (CGA)*
	✓	✓			RFC4581 *Cryptographically Generated Addresses (CGA) Extension Field Format*
	✓	✓			RFC4982 *Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.8. Security Capabilities

The security capabilities group consists of the specifications related to both IP (IPsec) and Transport (TLS) secure channels. This includes capabilities for key management and underlying cryptographic algorithms.

4.8.1. Definition of Security Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Security Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**IPsec**	**support for the IP security architecture.**
	✓	✓			RFC4301 *Security Architecture for the Internet Protocol*
	✓	✓			RFC4303 *IP Encapsulating Security Payload (ESP)*
U	✓	✓			RFC7296 *Internet Key Exchange Protocol Version 2 (IKEv2)*
U	✓	✓			RFC8221 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
U	✓	✓			RFC8247 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
		✓		**IPsec-VPN**	**support for the IP security architecture gateways.**
		✓			RFC4301 *Security Architecture for the Internet Protocol*
		✓			RFC4303 *IP Encapsulating Security Payload (ESP)*
U		✓			RFC7296 *Internet Key Exchange Protocol Version 2 (IKEv2)*
U		✓			RFC8221 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
U		✓			RFC8247 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
	✓	✓		**IPsec-IoT**	**support for IoT Cryptographic Algorithms.**
N	✓	✓			RFC8221 Section: 5 AES-CCM with a 8 octet ICV *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

DRAFT

Security Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N	✓	✓			RFC8247 Section: 2.1 AES-CCM with a 8 octet ICV *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N	✓	✓			RFC8247 Section: 2.2 PRF_AES128_XCBC *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N	✓	✓			RFC8247 Section: 2.3 AUTH_AES_XCBC_96 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
		✓		**IPsec-IoT-VPN**	**support for IoT Cryptographic Algorithms in gateways.**
N		✓			RFC8221 Section: 5 AES-CCM with a 8 octet ICV *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
N		✓			RFC8247 Section: 2.1 AES-CCM with a 8 octet ICV *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N		✓			RFC8247 Section: 2.2 PRF_AES128_XCBC *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N		✓			RFC8247 Section: 2.3 AUTH_AES_XCBC_96 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
	✓	✓		**IPsec-CHACHA**	**support for ChaCha20 Cryptographic Algorithms.**
N	✓	✓			RFC8221 Section: 5 CHACHA20_POLY1305 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
N	✓	✓			RFC8247 Section: 2.1 CHACHA20_POLY1305 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
		✓		**IPsec-CHACHA-VPN**	**support for ChaCha20 Cryptographic Algorithms in gateways.**
N		✓			RFC8221 Section: 5 CHACHA20_POLY1305 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Security Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N		✓			RFC8247 Section: 2.1 CHACHA20_POLY1305 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
	✓	✓		**IPsec-SHA-512**	**support for SHA-512 Cryptographic Algorithms.**
N	✓	✓			RFC8221 Section: 6 AUTH_HMAC_SHA2_512_256 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
N	✓	✓			RFC8247 Section: 2.2 PRF_HMAC_SHA2_512 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N	✓	✓			RFC8247 Section: 2.3 AUTH_HMAC_SHA2_512_256 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
		✓		**IPsec-SHA-512-VPN**	**support for SHA-512 Cryptographic Algorithms in gateways.**
N		✓			RFC8221 Section: 6 AUTH_HMAC_SHA2_512_256 *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
N		✓			RFC8247 Section: 2.2 PRF_HMAC_SHA2_512 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
N		✓			RFC8247 Section: 2.3 AUTH_HMAC_SHA2_512_256 *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*
	✓	✓		**SSHV2**	**support for SSHv2 over IPv6.**
N	✓	✓			RFC4250 *The Secure Shell (SSH) Protocol Assigned Numbers*
N	✓	✓			RFC4251 *The Secure Shell (SSH) Protocol Architecture*
N	✓	✓			RFC4252 *The Secure Shell (SSH) Authentication Protocol*
N	✓	✓			RFC4253 *The Secure Shell (SSH) Transport Layer Protocol*
N	✓	✓			RFC4254 *The Secure Shell (SSH) Connection Protocol*
	✓	✓		**TLS**	**support for Transport Layer Security architecture version 1.2.**
N	✓	✓			RFC5246 *The Transport Layer Security (TLS) Protocol Version 1.2*
N	✓	✓			RFC6176 *Prohibiting Secure Sockets Layer (SSL) Version 2.0*
N	✓	✓			RFC7465 *Prohibiting RC4 Cipher Suites*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Security Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N	✓	✓			RFC7568 *Deprecating Secure Sockets Layer Version 3.0*
N	✓	✓			RFC5746 *Transport Layer Security (TLS) Renegotiation Indication Extension*
	✓	✓		**TLS-1.3**	**support for Transport Layer Security architecture version 1.3.**
N	✓	✓			RFC8446 *The Transport Layer Security (TLS) Protocol Version 1.3*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.9. Network Management Capabilities

The Network Management capabilities group consists of the specifications related to management of networked devices. This includes capabilities for both SNMP and NETCONF based configuration, monitoring and management.

4.9.1. Definition of Network Management Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Network Management Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**SNMP**	**support for simple network management protocol.**
	✓	✓			RFC3411 *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
	✓	✓			RFC3412 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
	✓	✓			RFC3413 *Simple Network Management Protocol (SNMP) Applications*
	✓	✓			RFC3414 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
	✓	✓			RFC4293 *Management Information Base for the Internet Protocol (IP)*
	✓	✓			RFC4292 *IP Forwarding Table MIB*
	✓	✓			RFC4022 *Management Information Base for the Transmission Control Protocol (TCP)*
	✓	✓			RFC4113 *Management Information Base for the User Datagram Protocol (UDP)*
	✓	✓		**SNMP & Tunneling**	**applicable when both capabilities are selected.**
	✓	✓			RFC4087 *IP Tunnel MIB*
	✓	✓		**SNMP & IPsec**	**applicable when both capabilities are selected.**
	✓	✓			RFC4807 *IPsec Security Policy Database Configuration MIB*
	✓	✓		**SNMP & DiffServ**	**applicable when both capabilities are selected.**
	✓	✓			RFC3289 *Management Information Base for the Differentiated Services Architecture*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Network Management Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**NETCONF**	**support for network configuration functions.**
N	✓	✓			RFC6241 *Network Configuration Protocol (NETCONF)*
N	✓	✓			RFC8344 *A YANG Data Model for IP Management*
N	✓	✓			RFC8343 *A YANG Data Model for Interface Management*
N	✓	✓			RFC8348 *A YANG Data Model for Hardware Management*
N	✓	✓			RFC8349 *A YANG Data Model for Routing Management (NMDA Version)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.10. Multicast Capabilities

The Multicast capabilities group consists of the specifications for both link local and routed multicast communications. Since MLDv2 requires the Router Alert Option (RFC 2711) as specified in RFC 3810 its support is included in the Multicast and SSM Capabilities. PIM-SM and its extended features provides multicast routing.

4.10.1. Definition of Multicast Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Multicast Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**SSM**	**require full support for multicast communications.**
	✓	✓			RFC3810 *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
	✓	✓			RFC4607 *Source-Specific Multicast for IP*
	✓	✓			RFC4604 *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*
	✓	✓		**Multicast**	**support for link-local multicast communication.**
	✓	✓			RFC3810 *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
	✓	✓			RFC3306 *Unicast-Prefix-based IPv6 Multicast Addresses*
	✓	✓			RFC3307 *Allocation Guidelines for IPv6 Multicast Addresses*
N	✓	✓			RFC7371 *Updates to the IPv6 Multicast Addressing Architecture*
		✓		**PIM-SM**	**support for PIM-SM Routing protocols.**
U		✓			RFC7761 *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*
N		✓			RFC5059 *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
		✓		**PIM-SM-IPsec**	**support for PIM-SM over IPsec.**
N		✓			RFC5796 *Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages*
		✓		**PIM-SM-BiDir**	**support for Bidrectional PIM-SM routing protocol.**
N		✓			RFC5015 *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.11. Network Support Capabilities

The Network Support capabilities group consists of the specifications for protocols for DHCPv6 Server, DNS resolution of IPv6 names and the use of IPv6 addresses in URIs.

4.11.1. Definition of Network Support Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Network Support Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**DNS-Client**	**support for DNS client/resolver functions.**
	✓	✓			RFC3596 *DNS Extensions to Support IP Version 6*
	✓	✓			RFC2671 *Extension Mechanisms for DNS (EDNS0)*
	✓	✓			RFC3226 *DNSSEC and IPv6 A6 aware server/resolver message size requirements*
	✓	✓		**URI**	**support for IPv6 uniform resource identifiers.**
	✓	✓			RFC3986 *Uniform Resource Identifier (URI): Generic Syntax*
	✓	✓			RFC6874 *Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers*
	✓	✓		**NTP-Client**	**support for NTP client capabilities.**
N	✓	✓			RFC5905 *Network Time Protocol Version 4: Protocol and Algorithms Specification*
	✓	✓		**NTP-Server**	**support for NTP server capabilities.**
N	✓	✓			RFC5905 *Network Time Protocol Version 4: Protocol and Algorithms Specification*
	✓	✓		**DNS-Server**	**support for DNS server capabilities.**
	✓	✓			RFC3596 *DNS Extensions to Support IP Version 6*
	✓	✓		**DHCP-Server**	**support for DHCP server capabilities.**
U	✓	✓			RFC8415 *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
U	✓	✓			RFC3646 *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
	✓	✓		**DHCP-Server-Ext**	**support for DHCP server for additional DHCP options and Bulk Leasequery.**
N	✓	✓			RFC5460 *DHCPv6 Bulk Leasequery*

Network Support Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
N	✓	✓			RFC3319 *Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers*
	✓	✓		**DHCP-Relay**	**support for DHCP relay capabilities.**
N	✓	✓			RFC8415 *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.12. Application and Service Capabilities

The Application and Service capabilities group consists of a framework to define the IPv6 capabilities of a broad range of general applications. User defined capabilities allow the specification of application specific functions and protocols that may not have consensus standard specifications.

4.12.1. Definition of Application and Service Capability Requirements

The technical requirements of the capabilities in this group are defined by the users based on the application types:

Application and Services Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
			✓	**App-Serv=[TBD]**	**support for application/service specific functions.**
			✓		SP500-267Ar1 Section: 4.12 Application/Service Specific Functions over IPv6-only network. *NIST IPv6 Profile*

Beyond the application environment requirements explained above, users of this profile should require any application to demonstrate working in an IPv6-only environment as documented in Section 4.1. The following general guidance may be useful in the formulation of such additional validation of application requirements.

The practical implications of the above guidance will vary with applications and specific implementation. The following lists some of the common issues that will require code modifications to support IPv6 at the application level.

- If the application or service parses text that may contain an IP address (e.g., as part of URI processing), such code must also support IPv6 addresses.
- If the application or service stores any information in files (e.g., in a cache), and that information can include IP addresses, it must be possible to store IPv6 addresses as well.
- If the application or service stores IP addresses in binary format, then it should make use of protocol agnostic structures (e.g., sockaddrs), rather than, say 4-byte integers, so that it will automatically be able to handle IPv6's longer addresses.
- If the application or service uses DNS names that application support use IPv6 AAAA resource records and the operation of DNS natively over IPv6. It should also support receiving A resource records in conjunction with AAAA and be able to connect over IPv6.

- The application or service must be fully functional when operating over IPv6. That is no claimed functionality of the product can be missing when operating over a native-IPv6 network.

Users of this profile may supply any additional requirements that must be met by specific applications.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.13. Switch Capabilities

The Switch capabilities group consists of capabilities for Layer 2 switches improve network performance and security of IPv6.

4.13.1. Definition of Switch Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Switch Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
			✓	**DHCPv6-Guard**	**support for DHCPv6 Guard at Layer 2.**
N			✓		RFC7610 *DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers*
			✓	**RA-Guard**	**support for RA Guard at Layer 2.**
N			✓		RFC6105 *IPv6 Router Advertisement Guard*
N			✓		RFC7113 *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*
			✓	**MLD-Snooping**	**support for MLD Snooping at Layer 2.**
N			✓		RFC4541 *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.14. Network Protection Product Capabilities

The Network Protection Product capabilities group consists of the requirements defined in this document to specify the requirements of common network security devices. This includes capabilities for firewalls, intrusions detection and protection applications, as well as application specific firewalls.

4.14.1. Definition of Network Protection Product Capability Requirements

The technical requirements of the capabilities in this group are defined by the following mappings:

Network Protection Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
			✓	**FW**	**support for basic firewall capabilities.**
U			✓		SP500-267Ar1 Section: 4.14.4 Firewall Requirements *NIST IPv6 Profile*
			✓	**IDS**	**support for intrusion detection capabilities.**
U			✓		SP500-267Ar1 Section: 4.14.5.1 Intrusion Detection System *NIST IPv6 Profile*
			✓	**IPS**	**support for intrusion protection capabilities.**
U			✓		SP500-267Ar1 Section: 4.14.5.2 Intrusion Prevention *NIST IPv6 Profile*
			✓	**APFW**	**support for application firewall capabilities.**
U			✓		SP500-267Ar1 Section: 4.14.4.2 Application Firewall *NIST IPv6 Profile*

Given the lack of public consensus standards in this area, this section serves as the primary source of Network Protection Product (NPP) requirements. Thus, this section provides both the definition of the capabilities in this area and the definition of their technical requirements.

Network protection products (firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and the like) are currently essential for securing external network connections in the Internet. As IPv6 is deployed in production networks, it is essential that IPv6 network protection products be just as capable as their IPv4 counterparts. Ensuring this capability exists is the goal of these requirements.

The requirements listed here concentrate on the IPv6-specific features required for network protection products. Any other features an agency requires for its network function (e.g.,

support for a particular administrative model or a special authentication method) are to be addressed through the user's usual specification and validation methods.

IPv4-only features are not addressed here. While it is to be expected that IPv4 traffic will continue for the foreseeable future, and hence IPv4 network protection products will be required, a user can choose to use separate network protection products for IPv4 and IPv6 traffic. Hence, even for network functions which offer both IPv4 and IPv6 network protection features, this profile only addresses their IPv6 functionality.

In general, these requirements seek merely to establish the minimal threshold of functionality required for IPv6 network protection products. For firewalls, this means basic port-blocking and (for application firewalls) application data filtering, while for intrusion detection and prevention systems, this means the ability to detect (and, in the case of IPSs, to prevent or disrupt) known attack patterns, including IPv6 version of known IPv4 attacks. In both cases, network protection products will typically offer other more sophisticated features, such as statistical anomaly detection, but given the minimal nature of these requirements, they will not be addressed here.

4.14.2. Source of requirements

The sort of functionality provided by network protection products is not well-covered by protocol or interoperability specifications such as Internet RFCs. Hence, we cannot create the same sort of profiles as for Host systems or Routers, where we can specify desired functionality by listing relevant RFCs and options. Instead, we must list all requirements explicitly.

4.14.3. Common requirements for network protection products

The common requirements are applied to all the network protection products unless otherwise specified for in the product types definitions.

4.14.3.1. Basic host or router IPv6 connectivity requirements

While network protection products are technically, in terms of their connection characteristics, either hosts or routers, they are not typically expected to provide the same level of functionality, unless they are part of some combined capabilities (such as a firewall-router).

More commonly, network protection products only implement basic protocol capabilities to the extent necessary to perform their security functions while not interfering with the interoperability of desirable traffic passing through them. This typically includes basic protocol parsing, address recognition, link encapsulation, etc. Often many other basic protocol functions (e.g., error reporting, auto configuration) are implemented in non-standard ways on such functions or omitted.

Given the variance of capability and behavior of these basic IPv6 connectivity requirements in NPPs, we do not attempt to specify them in detail here. Instead we focus on the specification of their network security capabilities. Certainly, for combined capabilities,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

users of this profile can specify that a network protection device comply with the requirements of both a Router and a firewall (for example).

4.14.3.2. Dual stack

While it is expected that most network protection products will provide protection functionality for both IPv4 and IPv6 traffic, only IPv6 protection functionality is addressed here.

4.14.3.3. Administrative functionality

A network protection device must offer sufficient administrative controls to allow effective use of the facilities it offers. This includes controls over the configuration of its protective functionality, its logging and alert facilities, and access to the administrative facilities themselves. Such administrative functionality MUST be available either directly on the network protection device console or equivalent, or through remote communications using openly defined means.

4.14.3.4. Authentication and authorization

All administrative access to a network protection device MUST be controlled through appropriate authentication mechanisms and restricted to appropriately authorized users. In the case of network protection products which do not separate administrative roles, authentication as an administrator can be viewed as sufficient authorization.

4.14.3.5. Security of control and communications

All administrative controls MUST be secure from non-authorized access, and all administrative communications with a network protection device must be secure from outside observation. This can be done through local console-type access; through FIPS-approved encrypted network communication; or through network communications which are secured through other means from outside access (such as VLAN separation or firewall blocking).

4.14.3.6. Persistence

All network protection products settings MUST persist through loss and restoration of electrical power.

4.14.3.7. Logging and alerts

Network protection products MUST provide sufficient administrative capability to allow inspection of all administratively controlled settings and give assurance of their proper functioning. Such capability MUST be controllable by, and accessible to, properly authorized administrators.

Intrusion detection systems have additional logging requirements, as described below.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

4.14.3.8. Fragmented packet handling

Network protection products MUST be able to handle fragmented packets by provisionally reassembling and applying appropriate controls based on the reassembled packet.

4.14.3.9. Tunneled traffic handling

Network protection products MUST be able to handle all IPv4/IPv6 tunneling schemes, no matter how embedded, either by analyzing and applying the appropriate controls based on the encapsulated packet header, or (in the case of firewalls) by simply blocking all unanalyzed tunneled packets.

4.14.4. Firewall requirements (Common Requirements)

Firewalls MUST support all the Common Requirements listed in 4.13.3.

4.14.4.1. Port/protocol/address blocking

Firewalls MUST allow selective blocking/admission of traffic by protocol, and, for IPv6 packets, by source and/or destination subnet and/or address, by extension header type and, for higher-level protocols, by the appropriate per-protocol subfields - ports for UDP and TCP, and type and code for ICMP. Such blocking/admission MUST be equally effective for both normal and IPsec traffic; the latter to the extent such fields are visible in the packet.

Port blocking/admission functionality MUST be sufficiently rich to allow discrete controls in both directions down to the individual port level, for all UDP/TCP ports available. While it is desirable to be able to block/admit any possible combination of ports, at a minimum the port-blocking functionality MUST have sufficient capacity to selectively include or exclude all commonly used services.

Address blocking functionality MUST be sufficiently rich to allow blocking of all traffic with source or destination addresses which ought not to be present in traffic sent between external and internal networks, such as local addresses (including loopback, link local, site local, and RFC4193-style unique local addresses), or source multicast addresses.

Firewalls MUST allow blocking of all traffic which has not been explicitly authorized.

4.14.4.2. Asymmetrical blocking

Firewalls MUST, either through software or hardware configuration, distinguish between external and internal connected networks, and allow imposing asymmetrical controls on traffic between these networks. In particular, for connection-oriented protocols such as TCP, firewalls MUST have the ability to allow bidirectional traffic flow over connections initiated from hosts on the internal network to hosts on the external network, while blocking connection initiation from the external network. A firewall MUST properly enforce the TCP state.

DRAFT

For request/response protocols without explicit connection setup (e.g., ICMP echo request and reply), firewalls MUST be able to selectively block unsolicited (vs. solicited) replies coming from the external network.

4.14.4.3. IPv6 Traffic Filtering

Firewalls MUST discard all traffic from and to reserved IPv6 address space. Firewalls should also filter packets with illegal IPv6 Header chains. The firewall shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

4.14.4.4. IPsec traffic handling

Firewalls MUST either be capable of terminating IPsec connections (security gateways) or be capable of selectively blocking IPsec traffic.

4.14.4.5. Performance under load, fail-safe

When firewalls suffer operational degradation or failure due to high network loads or other factors, they MUST fail in such a manner as not to allow unauthorized access.

4.14.4.6 Logging
When configured to do so, the firewall MUST log matches to filter rules that drop, deny, reject, or log packets.

4.14.5. Application firewall requirements

The Application Firewalls MUST support all the Common Requirements listed in 4.13.3.

4.14.5.1. No violation of trust barriers

Application firewall mediation of data transversal (session, file, etc.) through the firewall MUST NOT violate trust barriers, either by improperly rewriting incoming untrusted data to appear trusted, or by improperly exposing information (such as internal network structures) to external untrusted networks.

4.14.5.2. Session traffic authorization

Application firewalls MUST have means of controlled authorization for the establishment of sessions initiated from the external network to internal hosts.

4.14.5.3. Email, file filtering

Application firewalls MUST have configurable means for examining files (such as email attachments) that are transferred from the external network to internal hosts for the presence of undesired elements, and, when such elements are found, selectively blocking or stripping

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

them. The means of detection used varies with the firewall, ranging from pattern (signature)-matching or other heuristics for virus detection, to the simple blocking of, for example, all executable file content. In any case, the means MUST be sufficient to block typical threat traffic.

4.14.6. Intrusion detection and prevention system requirements

Intrusion detection systems MUST support all the Common Requirements listed in 4.13.3.

4.14.6.1. Known attack detection

Intrusion detection systems MUST provide a configurable capability to detect suspicious traffic based on known attack patterns, including those embedded in HTTP and SMTP traffic.

4.14.6.2. Port-scanning detection

Intrusion detection systems MUST detect typical port scanning (multiple ports of a single host) and host scanning (single port across multiple hosts) techniques, including "stealth" scans. (Note that while "blind" host scanning across a subnet is not considered feasible for IPv6, other techniques such as scanning based on DNS data are still a concern.)

4.14.6.3. Tunneled traffic detection

Intrusion detection systems MUST be able to detect threat patterns even for tunneled traffic, when packet data contents may be embedded with multiple IP (v6/v4) headers. For tunneling methods for which content examination is not supported, it is sufficient merely to block all such tunneled packets.

4.14.6.4. Logging and alerts

Intrusion detection systems MUST provide means to log all suspicious traffic and send notification to the appropriate administrators. The Intrusion detection systems MUST generate an audit record of fragmented packet attacks.

4.14.6.5. Performance under load, fail-safe

When intrusion detection systems suffer operational degradation or failure due to high network loads or other factors, they MUST provide notification of such failure. In cases of overload, intrusion detection systems SHOULD prioritize their processing to preferentially examine the highest-risk traffic.

4.14.7. Intrusion prevention requirements

Intrusion prevention systems MUST support all the Common Requirements listed in 4.13.3.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

4.14.7.1. Intrusion prevention

Intrusion prevention products MUST implement the intrusion detection capabilities listed in the previous section. In addition, intrusion prevention products MUST provide means to stop or attenuate detected attacks, either (when inline) directly or through manipulation of other network functions (e.g., updating a router ACL or firewall rule set). Such prevention means include dropping or rejecting suspect packets, throttling bandwidth usage from suspect sources, or rewriting or removing malicious content.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

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 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.

Some example capability summary definitions are given below. These CSS strings could be either requirements statements or product capability reports depending upon the usage scenario. These examples are provided both to illustrate the use of the profile and to provide templates that can be modified and used by others.

- **Minimal-Host = NISTv6-r1:Host + Core + SLAAC + Addr-Arch + Multicast**
    - This CSS describes the minimal mandatory Host requirements from the IETF Node Requirements specification [RFC8504]. Note this example can be used as a stub from which to build other, more complete CSS.
- **Minimal-Router = NISTv6-r1:Router + Core + SLAAC + Addr-Arch + Multicast**
    - This CSS describes the minimal mandatory Router requirements from the IETF Node Requirements specification [RFC8504]. Note this example can be used as a stub from which to build other, more complete CSS.
- **IPv6-only-Laptop = NISTv6-r1:Host + IPv6-Only + Core + SLAAC + Addr-Arch + Multicast + DNS-Client + TLS + Link=Ethernet.**
    - This CSS describes a typical configuration for a laptop to be used on an IPv6-only Wireless link. When using the IPv6-Only capability it indicates that all the capabilities work in an IPv6-only environment.
- **Default-Desktop = NISTv6-r1:Host + Core + SLAAC + Addr-Arch + Multicast + DHCP-client + DNS-Client + TLS + URI + Link=Ethernet.**
    - This CSS describes a typical configuration for a desktop PC that relies DHCP for network configuration and a dual stack transition mechanism.
- **Default-App-Server = NISTv6-r1:Host + Core + Addr-Arch + Multicast + [IPSec|TLS] + URI + DNS-Client + Link=Ethernet.**
    - This CSS describes a requirement statement for a typical application server that uses manually configured addresses, dual stack transition mechanisms, and a choice of IPsec or TLS for secure communication. If there is a specific

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

application being supported, it would be an additional capability string for that function.

- **Default-IOT = NISTv6-r1:Host + IPv6-Only + 6Lo + Link=6LoWPAN**
    - This CSS describes a requirement statement for a typical IoT device operating on a low powered wireless network with only support for IPv6. Notice the lack of support for many of the recommended mandatory capabilities. IoT devices sometimes have very minimal, or non-standard implementations of core protocols. Note this example can be used as a stub from which to build other, more complete CSS.
- **Default-DC-Router = NISTv6-r1:Router + Core + Addr-Arch + Multicast + BGP + BGP-EVPN + BGP-VPLS + [SNMP|NETCONF] + IPv6-Only + Link=Ethernet**
    - This CSS describes a requirement statement for a typical data center router supporting BGP as the IPv6 routing protocol and either NETCONF or SNMP for configuration and management. IPv6-only requires that this data center router works properly in an IPv6-only environment.
- **Example.com-DC-Router = NISTv6-r1:Router + Core + Addr-Arch + Multicast + OSPF + ISIS + NETCONF + IPv6-Only + GRE + Link=Ethernet**
    - This CSS describes a product capability statement for Example.com's data center router that meets the requirement statement above. This product supports both OSPF and ISIS as the IPv6 routing protocol but only NETCONF for configuration and management. Note that the product documents some additional capabilities (GRE) not mentioned in the requirements statement above. A requirements statement is understood to document the minimal required set of IPv6 capabilities.
- **Default-Enterprise-Router = NISTv6-r1:Router + Core + Addr-Arch + Multicast + [OSPF|ISIS] + [SNMP|NETCONF] + [IPsec|TLS] + [Tunneling-IP|Tunneling-UDP] + PIM-SM + Link=Ethernet**
    - This CSS describes a requirement statement for a typical enterprise router, that expands on the previous data center definition to add capabilities for secure channels and simple transition mechanisms.
- **Advanced-Enterprise-OSPF-Router = NISTv6-r1:Router + Core + Addr-Arch + Multicast + OSPF + OSPF-Auth + OSPF-Ext + OSPF-Graceful + [SNMP|NETCONF] + [IPsec|TLS] + [Tunneling-IP|Tunneling-UDP] + PIM-SM + Link=Ethernet**
    - This CSS describes a requirement statement for a typical enterprise router, that expands on the previous data center definition to add capabilities for secure channels and simple transition mechanisms.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

- **Default-Border-Router = NISTv6-r1:Router + Core + Addr-Arch + Multicast + BGP + BGP-OV + BGP-Flowspec + TLS + [OSPF|ISIS] + [SNMP|NETCONF] + Tunneling-IP + Link=Ethernet**
    - This CSS describes a requirement statement for a typical border router supporting either OSPF or ISIS as the IPv6 routing protocol and either NETCONF or SNMP for configuration and management. An IP Tunneling transition mechanisms is required. BGP security specifications are also included for protecting the router. Note that the choice of IPv6 routing protocols would have to be coordinated with enterprise router specifications.
- **Default-SGW = NISTv6-r1:Router + Core + OSPF + TLS + IPsec-VPN + Link=Ethernet**
    - This CSS describes a requirement statement for a Security Gateway running OSPF.
- **Default-CE-Router = NISTv6-r1:Router + CE-Router + Link=Ethernet**
    - This CSS describes a requirement statement for a typical SOHO router.
- **Default-MAP-E = NISTv6-r1:Router + CE-Router + MAP-E + Link=Ethernet**
    - This CSS describes a requirement statement for a typical Small-Office or Home router that provides the MAP-E transition mechanisms for IPv6-only wide area networking.
- **Default-Firewall = NISTv6-r1:NPP + Firewall**
    - This CSS describes a requirement statement for a typical simple firewall.
- **Default-IDS-IPS = NISTv6-r1:NPP + IPS + IDS**
    - This CSS describes a requirement statement for a typical intrusion detection / prevention system.
- **Default-Switch = NISTv6-r1:Switch + IPv6-Only + DHCPv6-Guard + RA-Guard + MLD-Snooping**
    - This CSS describes a requirement statement for a Layer 2 switch that functions on IPv6-only network supporting all the necessary functions for deploying IPv6 network. In many cases switches will also have a capability string for host for management purposes.

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

in commercial products and attempts to overly “standardize” such configurations may not afford the flexibility needed.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Acknowledgments

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

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

References

Citation	Reference
[IETF-OPSEC]	"*IETF Operational Security Capabilities for IP Network Infrastructure (opsec) Working Group*", Internet Engineering Task Force, ongoing. Online at: https://datatracker.ietf.org/wg/opsec/documents/
[IETF-V6OPS]	"*IETF IPv6 Operations (v6ops) Working Group*", Internet Engineering Task Force, Online at: https://datatracker.ietf.org/wg/v6ops/documents/
[IPv6-Ready]	"*IPv6 Ready Logo Program*", The IPv6 Forum, ongoing. Online at: https://www.ipv6ready.org/
[NIST-IPv6F]	"*Grant of Use Rights: IPv6 Test Specifications*", MOU between NIST and the IPv6 Forum, April 2008. Online at: https://www.nist.gov/document/ipv6forumnistmoupdf
[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://tools.ietf.org/html/rfc2119
[RFC2464]	Crawford, M., "*Transmission of IPv6 Packets over Ethernet Networks*", RFC 2464, DOI 10.17487/RFC2464, December 1998. Online at: https://tools.ietf.org/html/rfc2464
[RFC2473]	Conta, A. and S. Deering, "*Generic Packet Tunneling in IPv6 Specification*", RFC 2473, DOI 10.17487/RFC2473, December 1998. Online at: https://tools.ietf.org/html/rfc2473
[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://tools.ietf.org/html/rfc2474
[RFC2526]	Johnson, D. and S. Deering, "*Reserved IPv6 Subnet Anycast Addresses*", RFC 2526, DOI 10.17487/RFC2526, March 1999. Online at: https://tools.ietf.org/html/rfc2526
[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://tools.ietf.org/html/rfc2545
[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://tools.ietf.org/html/rfc2597
[RFC2671]	Vixie, P., "*Extension Mechanisms for DNS (EDNS0)*", RFC 2671, DOI 10.17487/RFC2671, August 1999. Online at: https://tools.ietf.org/html/rfc2671
[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://tools.ietf.org/html/rfc3140

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Citation	Reference
[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://tools.ietf.org/html/rfc3168
[RFC3226]	Gudmundsson, O., "*DNSSEC and IPv6 A6 aware server/resolver message size requirements*", RFC 3226, DOI 10.17487/RFC3226, December 2001. Online at: https://tools.ietf.org/html/rfc3226
[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://tools.ietf.org/html/rfc3246
[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://tools.ietf.org/html/rfc3247
[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://tools.ietf.org/html/rfc3289
[RFC3306]	Haberman, B. and D. Thaler, "*Unicast-Prefix-based IPv6 Multicast Addresses*", RFC 3306, DOI 10.17487/RFC3306, August 2002. Online at: https://tools.ietf.org/html/rfc3306
[RFC3307]	Haberman, B., "*Allocation Guidelines for IPv6 Multicast Addresses*", RFC 3307, DOI 10.17487/RFC3307, August 2002. Online at: https://tools.ietf.org/html/rfc3307
[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://tools.ietf.org/html/rfc3319
[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://tools.ietf.org/html/rfc3411
[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://tools.ietf.org/html/rfc3412
[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://tools.ietf.org/html/rfc3413
[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://tools.ietf.org/html/rfc3414

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc3596
[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://tools.ietf.org/html/rfc3646
[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://tools.ietf.org/html/rfc3810
[RFC3879]	Huitema, C. and B. Carpenter, "*Deprecating Site Local Addresses*", RFC 3879, DOI 10.17487/RFC3879, September 2004. Online at: https://tools.ietf.org/html/rfc3879
[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://tools.ietf.org/html/rfc3971
[RFC3972]	Aura, T., "*Cryptographically Generated Addresses (CGA)*", RFC 3972, DOI 10.17487/RFC3972, March 2005. Online at: https://tools.ietf.org/html/rfc3972
[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://tools.ietf.org/html/rfc3986
[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://tools.ietf.org/html/rfc4007
[RFC4022]	Raghunarayan, R., Ed., "*Management Information Base for the Transmission Control Protocol (TCP)*", RFC 4022, DOI 10.17487/RFC4022, March 2005. Online at: https://tools.ietf.org/html/rfc4022
[RFC4087]	Thaler, D., "*IP Tunnel MIB*", RFC 4087, DOI 10.17487/RFC4087, June 2005. Online at: https://tools.ietf.org/html/rfc4087
[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://tools.ietf.org/html/rfc4113
[RFC4191]	Draves, R. and D. Thaler, "*Default Router Preferences and More-Specific Routes*", RFC 4191, DOI 10.17487/RFC4191, November 2005. Online at: https://tools.ietf.org/html/rfc4191
[RFC4193]	Hinden, R. and B. Haberman, "*Unique Local IPv6 Unicast Addresses*", RFC 4193, DOI 10.17487/RFC4193, October 2005. Online at: https://tools.ietf.org/html/rfc4193
[RFC4250]	Lehtinen, S. and C. Lonvick, Ed., "*The Secure Shell (SSH) Protocol Assigned Numbers*", RFC 4250, DOI 10.17487/RFC4250, January 2006. Online at: https://tools.ietf.org/html/rfc4250

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[RFC4251]	Ylonen, T. and C. Lonvick, Ed., "*The Secure Shell (SSH) Protocol Architecture*", RFC 4251, DOI 10.17487/RFC4251, January 2006. Online at: https://tools.ietf.org/html/rfc4251
[RFC4252]	Ylonen, T. and C. Lonvick, Ed., "*The Secure Shell (SSH) Authentication Protocol*", RFC 4252, DOI 10.17487/RFC4252, January 2006. Online at: https://tools.ietf.org/html/rfc4252
[RFC4253]	Ylonen, T. and C. Lonvick, Ed., "*The Secure Shell (SSH) Transport Layer Protocol*", RFC 4253, DOI 10.17487/RFC4253, January 2006. Online at: https://tools.ietf.org/html/rfc4253
[RFC4254]	Ylonen, T. and C. Lonvick, Ed., "*The Secure Shell (SSH) Connection Protocol*", RFC 4254, DOI 10.17487/RFC4254, January 2006. Online at: https://tools.ietf.org/html/rfc4254
[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://tools.ietf.org/html/rfc4271
[RFC4291]	Hinden, R. and S. Deering, "*IP Version 6 Addressing Architecture*", RFC 4291, DOI 10.17487/RFC4291, February 2006. Online at: https://tools.ietf.org/html/rfc4291
[RFC4292]	Haberman, B., "*IP Forwarding Table MIB*", RFC 4292, DOI 10.17487/RFC4292, April 2006. Online at: https://tools.ietf.org/html/rfc4292
[RFC4293]	Routhier, S., Ed., "*Management Information Base for the Internet Protocol (IP)*", RFC 4293, DOI 10.17487/RFC4293, April 2006. Online at: https://tools.ietf.org/html/rfc4293
[RFC4301]	Kent, S. and K. Seo, "*Security Architecture for the Internet Protocol*", RFC 4301, DOI 10.17487/RFC4301, December 2005. Online at: https://tools.ietf.org/html/rfc4301
[RFC4303]	Kent, S., "*IP Encapsulating Security Payload (ESP)*", RFC 4303, DOI 10.17487/RFC4303, December 2005. Online at: https://tools.ietf.org/html/rfc4303
[RFC4429]	Moore, N., "*Optimistic Duplicate Address Detection (DAD) for IPv6*", RFC 4429, DOI 10.17487/RFC4429, April 2006. Online at: https://tools.ietf.org/html/rfc4429
[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://tools.ietf.org/html/rfc4443
[RFC4456]	Bates, T., Chen, E., and R. Chandra, "*BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*", RFC 4456, DOI 10.17487/RFC4456, April 2006. Online at: https://tools.ietf.org/html/rfc4456
[RFC4541]	Christensen, M., Kimball, K., and F. Solensky, "*Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*",

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Citation	Reference
	RFC 4541, DOI 10.17487/RFC4541, May 2006. Online at: https://tools.ietf.org/html/rfc4541
[RFC4552]	Gupta, M. and N. Melam, "*Authentication/Confidentiality for OSPFv3*", RFC 4552, DOI 10.17487/RFC4552, June 2006. Online at: https://tools.ietf.org/html/rfc4552
[RFC4581]	Bagnulo, M. and J. Arkko, "*Cryptographically Generated Addresses (CGA) Extension Field Format*", RFC 4581, DOI 10.17487/RFC4581, October 2006. Online at: https://tools.ietf.org/html/rfc4581
[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://tools.ietf.org/html/rfc4604
[RFC4607]	Holbrook, H. and B. Cain, "*Source-Specific Multicast for IP*", RFC 4607, DOI 10.17487/RFC4607, August 2006. Online at: https://tools.ietf.org/html/rfc4607
[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://tools.ietf.org/html/rfc4659
[RFC4724]	Sangli, S., Chen, E., Fernando, R., Scudder, J., and Y. Rekhter, "*Graceful Restart Mechanism for BGP*", RFC 4724, DOI 10.17487/RFC4724, January 2007. Online at: https://tools.ietf.org/html/rfc4724
[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://tools.ietf.org/html/rfc4760
[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://tools.ietf.org/html/rfc4761
[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://tools.ietf.org/html/rfc4798
[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://tools.ietf.org/html/rfc4807
[RFC4821]	Mathis, M. and J. Heffner, "*Packetization Layer Path MTU Discovery*", RFC 4821, DOI 10.17487/RFC4821, March 2007. Online at: https://tools.ietf.org/html/rfc4821
[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://tools.ietf.org/html/rfc4861

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[RFC4862]	Thomson, S., Narten, T., and T. Jinmei, "*IPv6 Stateless Address Autoconfiguration*", RFC 4862, DOI 10.17487/RFC4862, September 2007. Online at: https://tools.ietf.org/html/rfc4862
[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://tools.ietf.org/html/rfc4884
[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://tools.ietf.org/html/rfc4941
[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://tools.ietf.org/html/rfc4944
[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://tools.ietf.org/html/rfc4982
[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://tools.ietf.org/html/rfc5015
[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://tools.ietf.org/html/rfc5059
[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://tools.ietf.org/html/rfc5072
[RFC5120]	Przygienda, T., Shen, N., and N. Sheth, "*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*", RFC 5120, DOI 10.17487/RFC5120, February 2008. Online at: https://tools.ietf.org/html/rfc5120
[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://tools.ietf.org/html/rfc5185
[RFC5187]	Pillay-Esnault, P. and A. Lindem, "*OSPFv3 Graceful Restart*", RFC 5187, DOI 10.17487/RFC5187, June 2008. Online at: https://tools.ietf.org/html/rfc5187
[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://tools.ietf.org/html/rfc5246
[RFC5301]	McPherson, D. and N. Shen, "*Dynamic Hostname Exchange Mechanism for IS-IS*", RFC 5301, DOI 10.17487/RFC5301, October 2008. Online at: https://tools.ietf.org/html/rfc5301
[RFC5304]	Li, T. and R. Atkinson, "*IS-IS Cryptographic Authentication*", RFC 5304, DOI 10.17487/RFC5304, October 2008. Online at: https://tools.ietf.org/html/rfc5304

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[RFC5308]	Hopps, C., "*Routing IPv6 with IS-IS*", RFC 5308, DOI 10.17487/RFC5308, October 2008. Online at: https://tools.ietf.org/html/rfc5308
[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://tools.ietf.org/html/rfc5310
[RFC5340]	Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "*OSPF for IPv6*", RFC 5340, DOI 10.17487/RFC5340, July 2008. Online at: https://tools.ietf.org/html/rfc5340
[RFC5460]	Stapp, M., "*DHCPv6 Bulk Leasequery*", RFC 5460, DOI 10.17487/RFC5460, February 2009. Online at: https://tools.ietf.org/html/rfc5460
[RFC5492]	Scudder, J. and R. Chandra, "*Capabilities Advertisement with BGP-4*", RFC 5492, DOI 10.17487/RFC5492, February 2009. Online at: https://tools.ietf.org/html/rfc5492
[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://tools.ietf.org/html/rfc5575
[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://tools.ietf.org/html/rfc5613
[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://tools.ietf.org/html/rfc5746
[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://tools.ietf.org/html/rfc5796
[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://tools.ietf.org/html/rfc5798
[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://tools.ietf.org/html/rfc5838
[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://tools.ietf.org/html/rfc5905
[RFC5942]	Singh, H., Beebee, 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://tools.ietf.org/html/rfc5942
[RFC5952]	Kawamura, S. and M. Kawashima, "*A Recommendation for IPv6 Address Text Representation*", RFC 5952, DOI 10.17487/RFC5952, August 2010. Online at: https://tools.ietf.org/html/rfc5952

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc6092
[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://tools.ietf.org/html/rfc6105
[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://tools.ietf.org/html/rfc6146
[RFC6147]	Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "*DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*", RFC 6147, DOI 10.17487/RFC6147, April 2011. Online at: https://tools.ietf.org/html/rfc6147
[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://tools.ietf.org/html/rfc6164
[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://tools.ietf.org/html/rfc6176
[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://tools.ietf.org/html/rfc6232
[RFC6233]	Li, T. and L. Ginsberg, "*IS-IS Registry Extension for Purges*", RFC 6233, DOI 10.17487/RFC6233, May 2011. Online at: https://tools.ietf.org/html/rfc6233
[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://tools.ietf.org/html/rfc6241
[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://tools.ietf.org/html/rfc6282
[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://tools.ietf.org/html/rfc6286
[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://tools.ietf.org/html/rfc6333
[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://tools.ietf.org/html/rfc6437

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[RFC6494]	Gagliano, R., Krishnan, S., and A. Kukec, "*Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)*", RFC 6494, DOI 10.17487/RFC6494, February 2012. Online at: https://tools.ietf.org/html/rfc6494
[RFC6495]	Gagliano, R., Krishnan, S., and A. Kukec, "*Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields*", RFC 6495, DOI 10.17487/RFC6495, February 2012. Online at: https://tools.ietf.org/html/rfc6495
[RFC6515]	Aggarwal, R. and E. Rosen, "*IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN*", RFC 6515, DOI 10.17487/RFC6515, February 2012. Online at: https://tools.ietf.org/html/rfc6515
[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://tools.ietf.org/html/rfc6565
[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://tools.ietf.org/html/rfc6603
[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://tools.ietf.org/html/rfc6608
[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://tools.ietf.org/html/rfc6724
[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://tools.ietf.org/html/rfc6775
[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://tools.ietf.org/html/rfc6793
[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://tools.ietf.org/html/rfc6811
[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://tools.ietf.org/html/rfc6830
[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://tools.ietf.org/html/rfc6845
[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://tools.ietf.org/html/rfc6860

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT

Citation	Reference
[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://tools.ietf.org/html/rfc6874
[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://tools.ietf.org/html/rfc6877
[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://tools.ietf.org/html/rfc6936
[RFC6980]	Gont, F., "*Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*", RFC 6980, DOI 10.17487/RFC6980, August 2013. Online at: https://tools.ietf.org/html/rfc6980
[RFC7048]	Nordmark, E. and I. Gashinsky, "*Neighbor Unreachability Detection Is Too Impatient*", RFC 7048, DOI 10.17487/RFC7048, January 2014. Online at: https://tools.ietf.org/html/rfc7048
[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://tools.ietf.org/html/rfc7078
[RFC7084]	Singh, H., Beebee, W., Donley, C., and B. Stark, "*Basic Requirements for IPv6 Customer Edge Routers*", RFC 7084, DOI 10.17487/RFC7084, November 2013. Online at: https://tools.ietf.org/html/rfc7084
[RFC7113]	Gont, F., "*Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*", RFC 7113, DOI 10.17487/RFC7113, February 2014. Online at: https://tools.ietf.org/html/rfc7113
[RFC7136]	Carpenter, B. and S. Jiang, "*Significance of IPv6 Interface Identifiers*", RFC 7136, DOI 10.17487/RFC7136, February 2014. Online at: https://tools.ietf.org/html/rfc7136
[RFC7166]	Bhatia, M., Manral, V., and A. Lindem, "*Supporting Authentication Trailer for OSPFv3*", RFC 7166, DOI 10.17487/RFC7166, March 2014. Online at: https://tools.ietf.org/html/rfc7166
[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://tools.ietf.org/html/rfc7217
[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://tools.ietf.org/html/rfc7296
[RFC7346]	Droms, R., "*IPv6 Multicast Address Scopes*", RFC 7346, DOI 10.17487/RFC7346, August 2014. Online at: https://tools.ietf.org/html/rfc7346
[RFC7371]	Boucadair, M. and S. Venaas, "*Updates to the IPv6 Multicast Addressing Architecture*", RFC 7371, DOI 10.17487/RFC7371, September 2014. Online at: https://tools.ietf.org/html/rfc7371

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc7428
[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://tools.ietf.org/html/rfc7432
[RFC7465]	Popov, A., "*Prohibiting RC4 Cipher Suites*", RFC 7465, DOI 10.17487/RFC7465, February 2015. Online at: https://tools.ietf.org/html/rfc7465
[RFC7506]	Raza, K., Akiya, N., and C. Pignataro, "*IPv6 Router Alert Option for MPLS Operations, Administration, and Maintenance (OAM)*", RFC 7506, DOI 10.17487/RFC7506, April 2015. Online at: https://tools.ietf.org/html/rfc7506
[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://tools.ietf.org/html/rfc7527
[RFC7552]	Asati, R., Pignataro, C., Raza, K., Manral, V., and R. Papneja, "*Updates to LDP for IPv6*", RFC 7552, DOI 10.17487/RFC7552, June 2015. Online at: https://tools.ietf.org/html/rfc7552
[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://tools.ietf.org/html/rfc7559
[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://tools.ietf.org/html/rfc7568
[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://tools.ietf.org/html/rfc7596
[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://tools.ietf.org/html/rfc7597
[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://tools.ietf.org/html/rfc7599
[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://tools.ietf.org/html/rfc7606
[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://tools.ietf.org/html/rfc7607

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc7608
[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://tools.ietf.org/html/rfc7610
[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://tools.ietf.org/html/rfc7668
[RFC7674]	Haas, J., Ed., "*Clarification of the Flowspec Redirect Extended Community*", RFC 7674, DOI 10.17487/RFC7674, October 2015. Online at: https://tools.ietf.org/html/rfc7674
[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://tools.ietf.org/html/rfc7676
[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://tools.ietf.org/html/rfc7705
[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://tools.ietf.org/html/rfc7761
[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://tools.ietf.org/html/rfc7775
[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://tools.ietf.org/html/rfc7915
[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://tools.ietf.org/html/rfc7949
[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://tools.ietf.org/html/rfc8028
[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://tools.ietf.org/html/rfc8097
[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://tools.ietf.org/html/rfc8106

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc8163
[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://tools.ietf.org/html/rfc8200
[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://tools.ietf.org/html/rfc8201
[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://tools.ietf.org/html/rfc8210
[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://tools.ietf.org/html/rfc8212
[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://tools.ietf.org/html/rfc8221
[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://tools.ietf.org/html/rfc8247
[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://tools.ietf.org/html/rfc8305
[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://tools.ietf.org/html/rfc8319
[RFC8343]	Bjorklund, M., "*A YANG Data Model for Interface Management*", RFC 8343, DOI 10.17487/RFC8343, March 2018. Online at: https://tools.ietf.org/html/rfc8343
[RFC8344]	Bjorklund, M., "*A YANG Data Model for IP Management*", RFC 8344, DOI 10.17487/RFC8344, March 2018. Online at: https://tools.ietf.org/html/rfc8344
[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://tools.ietf.org/html/rfc8348
[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://tools.ietf.org/html/rfc8349

DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

Citation	Reference
[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://tools.ietf.org/html/rfc8362
[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://tools.ietf.org/html/rfc8379
[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://tools.ietf.org/html/rfc8415
[RFC8446]	Rescorla, E., "*The Transport Layer Security (TLS) Protocol Version 1.3*", RFC 8446, DOI 10.17487/RFC8446, August 2018. Online at: https://tools.ietf.org/html/rfc8446
[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://tools.ietf.org/html/rfc8481
[RFC8504]	Chown, T., Loughney, J., and T. Winters, "*IPv6 Node Requirements*", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019. Online at: https://tools.ietf.org/html/rfc8504
[SP500-267]	D. Montgomery, S. Nightingale, S. Frankel, M. Carson, "*A Profile for IPv6 in the U.S. Government - Version 1.0*", NIST SP-500-267, July 2008. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267
[SP500-267Ar1]	D. Montgomery, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*NIST IPv6 Profile*", NIST Special Publication 500-267A revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267Ar1
[SP500-267Ar1s]	D. Montgomery, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*NISTv6 Capabilities Table*", supplemental information for NIST Special Publication 500-267A revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267Ar1s
[SP500-267Br1]	D. Montgomery, M. Carson, T. Winters, M. Newcombe, T. Carlin, "*USGv6 Profile*", NIST Special Publication 500-267B revision 1, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-267Br1
[SP500-281Ar1]	D. Montgomery, S. Nightingale, E. Johnson, M. Newcombe, T. Winters, "*USGv6 Test Program Guide*", NIST Special Publication 500-281A revision 1, National Institute of Standards and Technology, February 2020. Online at: https://dx.doi.org/10.6028/NIST.SP.500-281Ar1

DRAFT

Appendix A: Change Log

Future revisions of this document will list major changes in this appendix.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-267Ar1

DRAFT