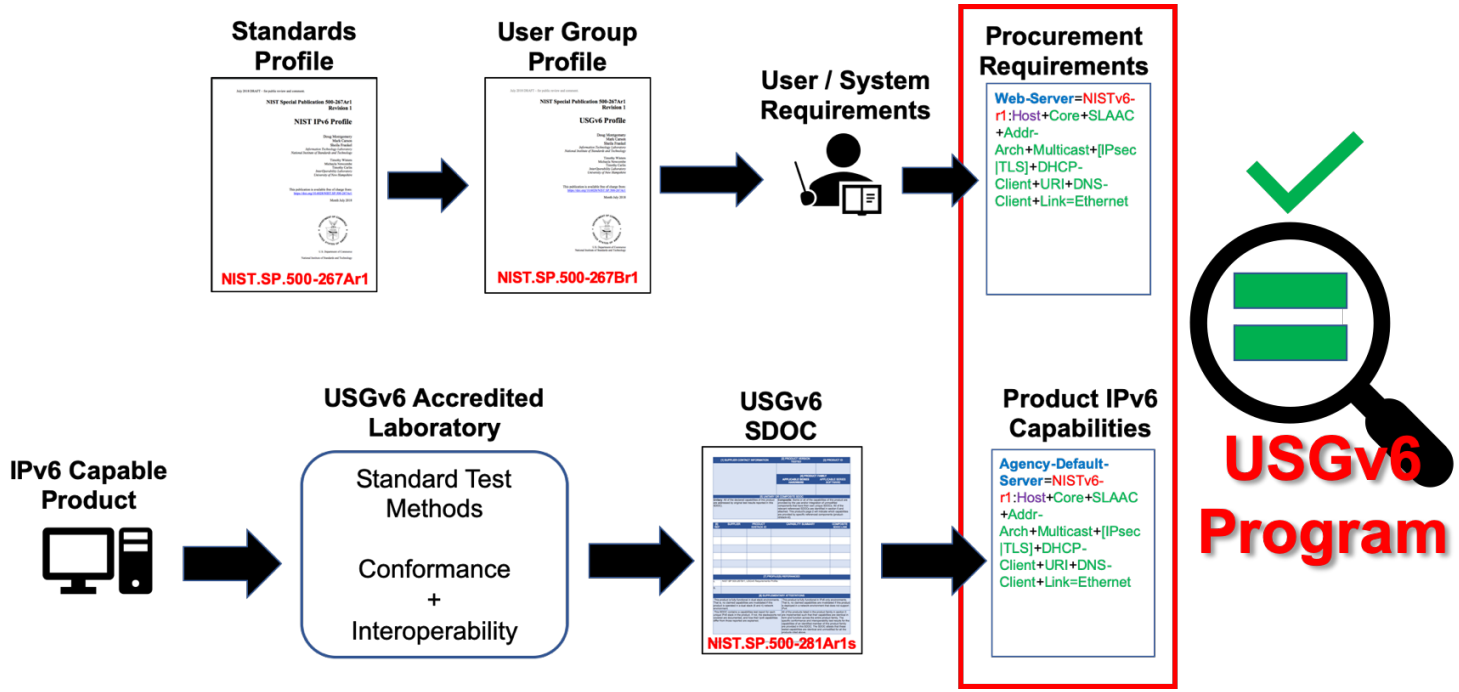
USGv6 Program

Revision 1 Update

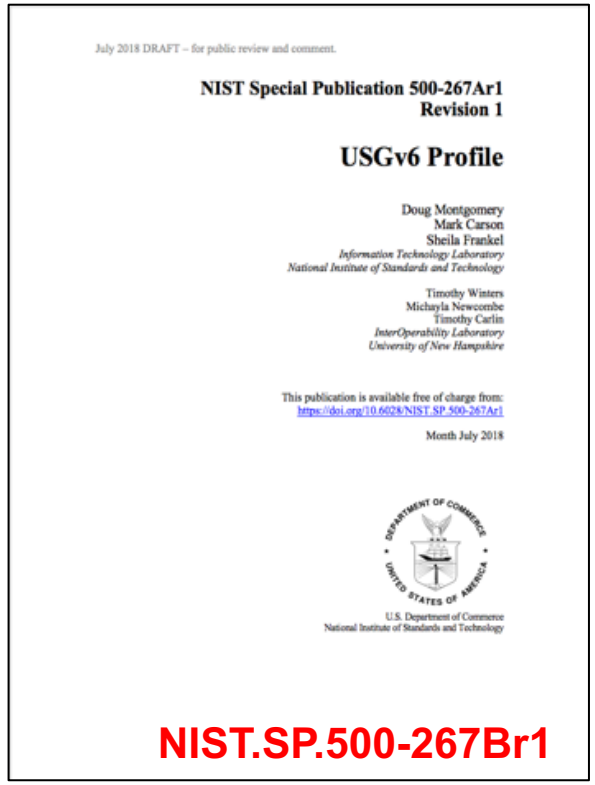


Doug Montgomery (dougm@nist.gov)

https://www.nist.gov/programs-projects/usgv6-program

USGv6 Program – Revision 1

- **What has changed?**
  - **Update** evolving standards & new IPv6 capabilities.
  - **Remove** failed technologies from ~2008.
  - **Improve** profile utility for specifying user requirements.
  - **Expand** test program scope and completeness.
    - Test V6-Only capabilities
  - **Maintain** alignment with IPv6Ready testing program.
  - **Simplify** means of specifying requirements / capability.
  - **Consolidate** and simplify program documentation.
  - **Enable** other user groups reusing profile & test program.


July 2018 DRAFT – for public review and comment.

NIST Special Publication 500-267Ar1
Revision 1

USGv6 Profile

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

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

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

Month July 2018

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

NIST.SP.500-267Br1

Please Review & Comment !

DRAFT3 of USGv6 Revision 1 Specifications: https://www.nist.gov/programs-projects/usgv6-program

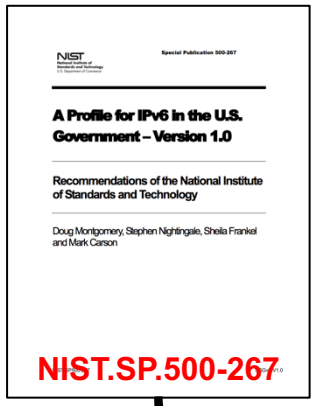
NIST and its partners in the USGv6 Program solicit public review and comment on the following revised specifications:

- ***"NIST IPv6 Profile"***, draft3-nist-sp-500-267ar1.pdf , October 2019.
- ***"NISTv6 Capabilities Table"***, draft3-nist-sp-500-267ar1s.pdf , October 2019.
- ***"USGv6 Profile"***, draft3-nist-sp-500-267br1.pdf , October 2019.
- ***"USGv6 Capabilities Table"***, draft3-nist-sp-500-267br1s.pdf , October 2019.
- ***"USGv6 Test Program Guide"***, draft3-nist-sp-500-281ar1.pdf , October 2019.
- ***"USGv6 Suppliers Declaration of Conformity"***, draft3-nist-sp-500-281ar1s.pdf , October 2019.
- ***"USGv6 Test Methods: General Description and Validation"***, draft3-nist-sp-500-281br1.pdf , October 2019.

Comments should be submitted to usgv6-program@nist.gov using the attached template: draft-usgv6-r1-comment-template.xlsx .

REVISED DRAFT DOCUMENTS AVAILABLE FOR A 3RD ROUND OF PUBLIC COMMENTS. COMMENTS DUE BY NOVEMBER 8, 2019.

Refactoring Program Documentation


Special Publication 500-267

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

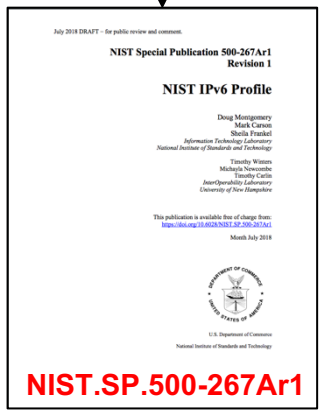
Recommendations of the National Institute of Standards and Technology

Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson

NIST.SP.500-267

NISTv6
Capability Definitions

NISTv6-r1
Capabilities Table


July 2018 DRAFT – for public review and comment.

NIST Special Publication 500-267Ar1
Revision 1

NIST IPv6 Profile

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

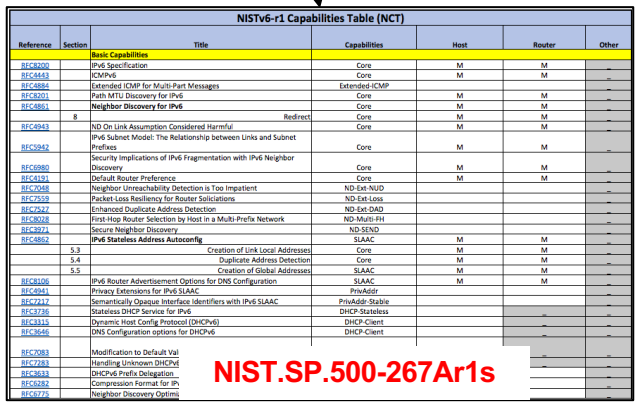
Timothy Winters
Michayla Newcombe
Timothy Carlin
InterOperability Laboratory
University of New Hampshire

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

Month July 2018

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

NIST.SP.500-267Ar1


NISTv6-r1 Capabilities Table (NCT)

Reference	Section	Title	Capabilities	Host	Router	Other
		Basic Capabilities				
RFC8200		IPv6 Specification	Core	M	M	_
RFC4443		ICMPv6	Core	M	M	_
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_
	8	Redirect	Core	M	M	_
RFC4943		ND On Link Assumption Considered Harmful	Core	M	M	_
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	Core	M	M	_
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery	Core	M	M	_
RFC4191		Default Router Preference	Core	M	M	_
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-Ext-NUD			_
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-Ext-Loss			_
RFC7527		Enhanced Duplicate Address Detection	ND-Ext-DAD			_
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Multi-FH			_
RFC3971		Secure Neighbor Discovery	ND-SEND			_
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	M	M	_
	5.3	Creation of Link Local Addresses	Core	M	M	_
	5.4	Duplicate Address Detection	Core	M	M	_
	5.5	Creation of Global Addresses	SLAAC	M	M	_
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	M	M	_
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr			_
RFC7217		Semantically Opaque Interface Identifiers with IPv6 SLAAC	PrivAddr-Stable			_
RFC3736		Stateless DHCP Service for IPv6	DHCP-Stateless			_
RFC3315		Dynamic Host Config Protocol (DHCPv6)	DHCP-Client			_
RFC3646		DNS Configuration options for DHCPv6	DHCP-Client			_
RFC7083		Modification to Default Val				_
RFC7283		Handling Unknown DHCPv6				_
RFC3633		DHCPv6 Prefix Delegation				_
RFC6282		Compression Format for IPv				_
RFC6775		Neighbor Discovery Optimiz				_

NIST.SP.500-267Ar1s

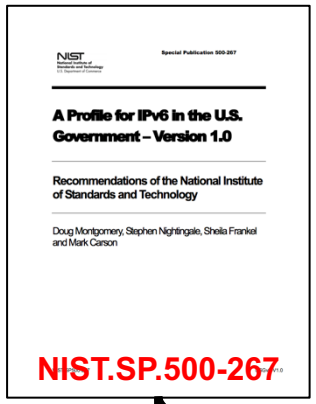
Generic IPv6 Capabilities Profile

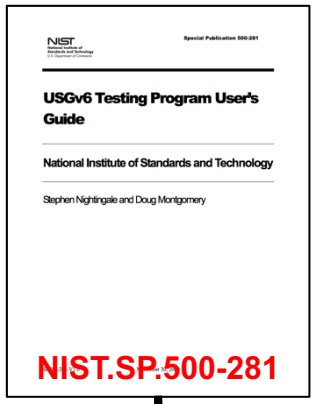
Requirements match new ETF Node Requirements

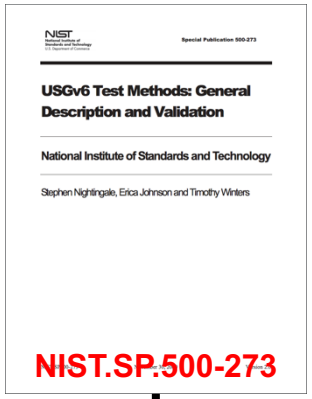
No mention or coupling to USG

Generic conformance guidance

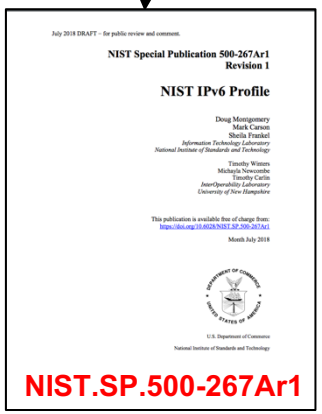
Revised USGv6 Program Documentation.



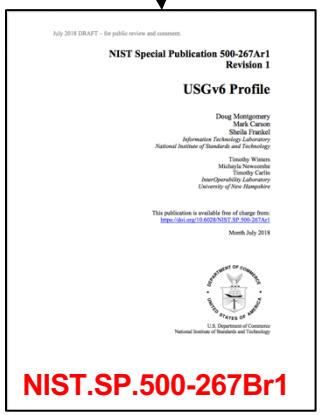




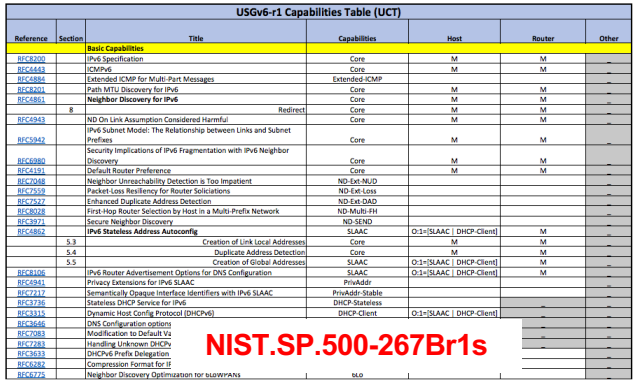
NISTv6-r1 Profile



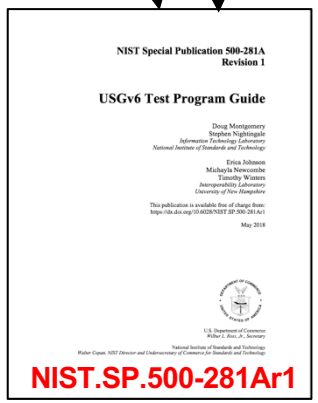
USGv6-r1 Profile



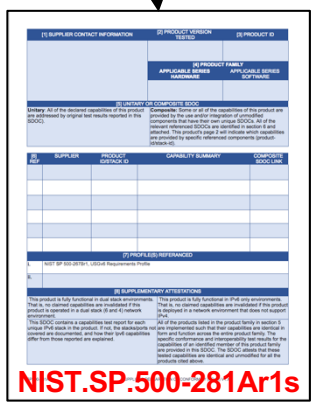
USGv6-r1 Capabilities Table



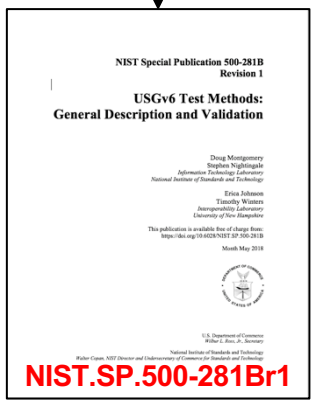
USGv6 Conformance



USGv6 SDOC



USGv6 Accreditation



USGv6-r1 Capabilities Table

USGv6-r1 Capabilities Table (UCT) - June 2019							
Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					
RFC8200		IPv6 Specification	Core	M	M	_	U
RFC4443		ICMPv6	Core	M	M	_	
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_	U
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_	
	8	Redirect	Core	M	M	_	
RFC6437		IPv6 Flow Label Specification	Core	M	M	_	N
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet	Core	M	M	_	N
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor	Core	M	M	_	N
RFC7608		IPv6 Prefix Length Recommendation for Forwarding	Core	_	M	_	N
RFC4191		Default Router Preference	Core	M	M	_	N
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_	
RFC4821		Packetization Layer Path MTU Discovery	PLPMTUD			_	N
RFC4429		Optimistic Duplicate Address Detection (DAD) for IPv6	ND-Ext			_	N
RFC7527		Enhanced Duplicate Address Detection	ND-Ext			_	N
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Ext			_	N
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-WL			_	N
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-WL			_	N
RFC8319		Support for Adjustable Maximum Router Lifetimes per Link	ND-WL			_	N
RFC3971		Secure Neighbor Discovery	SEND			_	
RFC6494		Certificate Profile and Certificate Management for SEcure Neighbor	SEND			_	
RFC6495		Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name	SEND			_	
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
	5.3	Creation of Link Local Addresses	Core	M	M	_	
	5.4	Duplicate Address Detection	Core	M	M	_	
	5.5	Creation of Global Addresses	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	N
RFC7217		Generating Semantically Opaque Interface Identifiers with SLAAC	SLAAC	O:1=[SLAAC | DHCP-Client]	_	_	N
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr		_	_	
RFC8415		DHCPv6 Stateless (Two Message Exchange)	DHCP-Stateless		_	_	U
RFC8415		Dynamic Host Config Protocol for IPv6	DHCP-Client	O:1=[SLAAC | DHCP-Client]	_	_	U

UCT Concepts and Notation

- IPv6 Specifications mapped into labeled ***Capabilities***
  - Grouped by logic and function.
  - Testable units.
  - Aligned to industry testing programs.

USGv6-r1 Capabilities Table (UCT) - June 2019

Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					
RFC8200		IPv6 Specification	Core	M	M	_	U
RFC4443		ICMPv6	Core	M	M	_	
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_	U
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_	
	8	Redirect	Core	M	M	_	
RFC6437		IPv6 Flow Label Specification	Core	M	M	_	N
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet	Core	M	M	_	N
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor	Core	M	M	_	N
RFC7608		IPv6 Prefix Length Recommendation for Forwarding	Core	_	M	_	N
RFC4191		Default Router Preference	Core	M	M	_	N
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_	
RFC4821		Packetization Layer Path MTU Discovery	PLPMTUD			_	N
RFC4429		Optimistic Duplicate Address Detection (DAD) for IPv6	ND-Ext			_	N
RFC7527		Enhanced Duplicate Address Detection	ND-Ext			_	N
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Ext			_	N
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-WL			_	N
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-WL			_	N
RFC8319		Support for Adjustable Maximum Router Lifetimes per Link	ND-WL			_	N
RFC3971		Secure Neighbor Discovery	SEND			_	
RFC6494		Certificate Profile and Certificate Management for SEcure Neighbor	SEND			_	
RFC6495		Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name	SEND			_	
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
	5.3	Creation of Link Local Addresses	Core	M	M	_	
	5.4	Duplicate Address Detection	Core	M	M	_	
	5.5	Creation of Global Addresses	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	N
RFC7217		Generating Semantically Opaque Interface Identifiers with SLAAC	SLAAC	O:1=[SLAAC | DHCP-Client]	_	_	N
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr		_	_	
RFC8415		DHCPv6 Stateless (Two Message Exchange)	DHCP-Stateless		_	_	U
RFC8415		Dynamic Host Config Protocol for IPv6	DHCP-Client	O:1=[SLAAC | DHCP-Client]	_	_	U

UCT Concepts and Notation

- **Selection Criteria**
  - Defined in terms of functional roles.
    - Host / Router
    - Client / Server
- **Not Product Classes**
  - Functional roles just identify different behavior / requirement classes in RFCs

USGv6-r1 Capabilities Table (UCT) - June 2019

Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					
RFC8200		IPv6 Specification	Core	M	M	_	U
RFC4443		ICMPv6	Core	M	M	_	
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_	U
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_	
	8	Redirect	Core	M	M	_	
RFC6437		IPv6 Flow Label Specification	Core	M	M	_	N
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet	Core	M	M	_	N
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor	Core	M	M	_	N
RFC7608		IPv6 Prefix Length Recommendation for Forwarding	Core	_	M	_	N
RFC4191		Default Router Preference	Core	M	M	_	N
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_	
RFC4821		Packetization Layer Path MTU Discovery	PLPMTUD			_	N
RFC4429		Optimistic Duplicate Address Detection (DAD) for IPv6	ND-Ext			_	N
RFC7527		Enhanced Duplicate Address Detection	ND-Ext			_	N
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Ext			_	N
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-WL			_	N
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-WL			_	N
RFC8319		Support for Adjustable Maximum Router Lifetimes per Link	ND-WL			_	N
RFC3971		Secure Neighbor Discovery	SEND			_	
RFC6494		Certificate Profile and Certificate Management for SEcure Neighbor	SEND			_	
RFC6495		Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name	SEND			_	
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
	5.3	Creation of Link Local Addresses	Core	M	M	_	
	5.4	Duplicate Address Detection	Core	M	M	_	
	5.5	Creation of Global Addresses	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	N
RFC7217		Generating Semantically Opaque Interface Identifiers with SLAAC	SLAAC	O:1=[SLAAC | DHCP-Client]	_	_	N
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr		_	_	
RFC8415		DHCPv6 Stateless (Two Message Exchange)	DHCP-Stateless		_	_	U
RFC8415		Dynamic Host Config Protocol for IPv6	DHCP-Client	O:1=[SLAAC | DHCP-Client]	_	_	U

UCT Concepts and Notation

- **Why not just cite RFCs?**
  - Organization of RFCs often contains both mandatory and optional behavior.
  - Behavior for multiple functional roles.
  - Organization often based upon packet formats.

USGv6-r1 Capabilities Table (UCT) - June 2019

Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					
RFC8200		IPv6 Specification	Core	M	M	_	U
RFC4443		ICMPv6	Core	M	M	_	
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_	U
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_	
	8	Redirect	Core	M	M	_	
RFC6437		IPv6 Flow Label Specification	Core	M	M	_	N
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet	Core	M	M	_	N
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor	Core	M	M	_	N
RFC7608		IPv6 Prefix Length Recommendation for Forwarding	Core	_	M	_	N
RFC4191		Default Router Preference	Core	M	M	_	N
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_	
RFC4821		Packetization Layer Path MTU Discovery	PLPMTUD			_	N
RFC4429		Optimistic Duplicate Address Detection (DAD) for IPv6	ND-Ext			_	N
RFC7527		Enhanced Duplicate Address Detection	ND-Ext			_	N
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Ext			_	N
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-WL			_	N
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-WL			_	N
RFC8319		Support for Adjustable Maximum Router Lifetimes per Link	ND-WL			_	N
RFC3971		Secure Neighbor Discovery	SEND			_	
RFC6494		Certificate Profile and Certificate Management for SEcure Neighbor	SEND			_	
RFC6495		Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name	SEND			_	
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
	5.3	Creation of Link Local Addresses	Core	M	M	_	
	5.4	Duplicate Address Detection	Core	M	M	_	
	5.5	Creation of Global Addresses	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	N
RFC7217		Generating Semantically Opaque Interface Identifiers with SLAAC	SLAAC	O:1=[SLAAC | DHCP-Client]	_	_	N
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr		_	_	
RFC8415		DHCPv6 Stateless (Two Message Exchange)	DHCP-Stateless		_	_	U
RFC8415		Dynamic Host Config Protocol for IPv6	DHCP-Client	O:1=[SLAAC | DHCP-Client]	_	_	U

UCT Concepts and Notation

- **Profile evolution**
  - Flags indicate capability changes since last revision
  - __ - no change
  - U – updated requirements
  - N – new requirements

USGv6-r1 Capabilities Table (UCT) - June 2019

Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					
RFC8200		IPv6 Specification	Core	M	M	_	U
RFC4443		ICMPv6	Core	M	M	_	
RFC8201		Path MTU Discovery for IPv6	Core	M	M	_	U
RFC4861		**Neighbor Discovery for IPv6**	Core	M	M	_	
	8	Redirect	Core	M	M	_	
RFC6437		IPv6 Flow Label Specification	Core	M	M	_	N
RFC5942		IPv6 Subnet Model: The Relationship between Links and Subnet	Core	M	M	_	N
RFC6980		Security Implications of IPv6 Fragmentation with IPv6 Neighbor	Core	M	M	_	N
RFC7608		IPv6 Prefix Length Recommendation for Forwarding	Core	_	M	_	N
RFC4191		Default Router Preference	Core	M	M	_	N
RFC4884		Extended ICMP for Multi-Part Messages	Extended-ICMP			_	
RFC4821		Packetization Layer Path MTU Discovery	PLPMTUD			_	N
RFC4429		Optimistic Duplicate Address Detection (DAD) for IPv6	ND-Ext			_	N
RFC7527		Enhanced Duplicate Address Detection	ND-Ext			_	N
RFC8028		First-Hop Router Selection by Host in a Multi-Prefix Network	ND-Ext			_	N
RFC7048		Neighbor Unreachability Detection is Too Impatient	ND-WL			_	N
RFC7559		Packet-Loss Resiliency for Router Solicitations	ND-WL			_	N
RFC8319		Support for Adjustable Maximum Router Lifetimes per Link	ND-WL			_	N
RFC3971		Secure Neighbor Discovery	SEND			_	
RFC6494		Certificate Profile and Certificate Management for SEcure Neighbor	SEND			_	
RFC6495		Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name	SEND			_	
RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
	5.3	Creation of Link Local Addresses	Core	M	M	_	
	5.4	Duplicate Address Detection	Core	M	M	_	
	5.5	Creation of Global Addresses	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	
RFC8106		IPv6 Router Advertisement Options for DNS Configuration	SLAAC	O:1=[SLAAC | DHCP-Client]	M	_	N
RFC7217		Generating Semantically Opaque Interface Identifiers with SLAAC	SLAAC	O:1=[SLAAC | DHCP-Client]	_	_	N
RFC4941		Privacy Extensions for IPv6 SLAAC	PrivAddr		_	_	
RFC8415		DHCPv6 Stateless (Two Message Exchange)	DHCP-Stateless		_	_	U
RFC8415		Dynamic Host Config Protocol for IPv6	DHCP-Client	O:1=[SLAAC | DHCP-Client]	_	_	U

Key Technical Changes

- **Testing in IPv6 Only Networks**
  - New IPv6-Only Capability
    - Users can require and vendors can declare support for IPv6-Only operation.
  - Requires Full Life Cycle of product to be fully functional in absence of IPv4.
    - Install, Manage, Update, UI
  - Requires other claimed capabilities to be tested in IPv6-Only environment.
    - Should we test other capabilities in IPv6-Only by default going forward?

USGv6-r1 Capabilities Table (UCT) - June 2019							
Reference	Section	Title	Capabilities	Host	Router	Other	Flag
		IPv6-only Capabilities					
SP500-267Ar1	4.1	Install product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Product user Interface fully supports IPv6	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Manage product over IPv6-only network	IPv6-Only	M	M	M	N
SP500-267Ar1	4.1	Update product over IPv6-only network	IPv6-Only	M	M	M	N
		Basic Capabilities					

NIST IPv6 Profile

- **Capabilities Templates**
  - Defines broad ***capabilities groups***
    - E.g. Security Capabilities
  - Identifies ***functional roles***
    - Host, Router, NPP, Application.
  - Defines individual named ***capabilities***
    - E.g., IPsec – support for the IP security architecture.
    - Defines recommended requirement level
      - M → Mandatory
      - O → Optional
      - O:I → Optional, must choose 1
      - X → Not recommended
    - M = mandatory in IETF Node Requirements specification.
  - Provides **guidance**
    - Text provides additional explanation of capability

NISTv6-r1:Host Capabilities Template:

- **Basic Capabilities** - see section 4.1
  - [M] - **Core** - support for IPv6 core functions.
  - [O] - **Extended-ICMP** - support for ICMPv6 extended messages.
  - [O] - **ND-Ext-NUD** - support for extended for neighbor unreachable detection.
  - [O] - **ND-Ext-Loss** - support for packet-loss for router solicitations.
  - [O] - **ND-Ext-DAD** - support for enhanced duplicate address detection.
  - [O] - **ND-Multi-FH** - support for neighbor discovery in multi-prefix network.
  - [O] - **ND-SEND** - support for neighbor discovery security extensions.
  - [M] - **SLAAC** - support for stateless global address auto-configuration.
  - [O] - **PrivAddr** - support for SLAAC privacy extensions.
  - [O] - **PrivAddr-Stable** - support for SLAAC stable privacy extensions.
  - [O] - **DHCP-Stateless** - support for stateless (DHCP) configuration.
  - [O] - **DHCP-Client** - support for stateful (DHCP) address auto-configuration.
  - [O] - **DHCP-Prefix** - support for stateful (DHCP) prefix delegation
  - [O] - **6Lo** - support for IPv6 over low power networks.
- **Addressing Capabilities** - see section 4.6
  - [M] - **Addr-Arch** - support for address architecture and selection.
  - [O] - **CGA** - support for cryptographically generated addresses.
- **Network Support Capabilities** - see section 4.8
  - [O] - **DNS-Client** - support for DNS client/resolver functions.
  - [O] - **URI** - support for IPv6 uniform resource identifiers.
  - [O] - **DNS-Server** - support for a DNS server capabilities.
  - [O] - **DHCP-Server** - support for a DHCP server capabilities.
  - [O] - **DHCP-Relay** - support for a DHCP relay capabilities.
- **Security Capabilities** - see section 4.7
  - [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] - **TLS** - support for the Transport Layer Security architecture.
- **Transition Mechanism Capabilities** - see section 4.4
  - [O] - **Dual-Stack** - support for dual-stack functions
  - [O] - **Tunneling** - support for encapsulation tunnels of IPv6 over IPv4
  - [O] - **XLAT** - support for transition mechanism 464XLAT.
- **Network Management Capabilities** - see section 4.8
  - [O] - **SNMP** - support for simple network management protocol.
  - [O] - **NETCONF** - support for network configuration functions.
- **Multicast Capabilities** - see section 4.9
  - [O] - **SSM** - require full support for multicast communications.
  - [M] - **Multicast** - support for link-local multicast communication.
- **Quality of Service Capabilities** - see section 4.3
  - [O] - **DiffServ** - support for Differentiated Services capabilities.
  - [O] - **ECN** - support for Explicit Congestion Notification.

NIST IPv6 Profile

- **Capabilities Requirements Definition**
  - Maps named capabilities to IETF specifications
    - By default, implies support of all the MUST requirements in RFC.
    - Where necessary, requirements of IETF specifications may be enhanced, with specific section references.
  - Capability Combinations
    - Cap1 – requirements apply with capability selected.
    - Cap2 & Cap3 – requirements only apply when both capabilities are selected.
    - Cap4 | Cap5 – requirements apply when either capability is selected.

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)*

User Requirements & Product Capabilities

- **Capability Summary Strings**
  - CSS_NAME = Profile: Functional_Role + Capability + Capability + …
  - Can express choice [IPsec|TLS]
- **Only form of requirements specification going forward.**
  - Profile provides capability taxonomy and selection guidance.
  - User develops named capability strings to describe requirements.
- **Product Capabilities**
  - Products don't conform to the USGv6 profile, they conform to specific capability strings.
  - SDoCs express product capabilities in terms of the same strings.
  - A single "product" may support multiple capability configurations.

Default-Desktop = USGv6-r1:Host + Core + SLAAC + Addr-Arch + Multicast + Dual-Stack + DHCP-client + DNS-Client + URI + Link=Ethernet.

Default-App-Server = USGv6-r1:Host + Core + Addr-Arch + Multicast + Dual-Stack + [IPSec|TLS] + URI + DNS-Client + Link=Ethernet.

Default-Embedded = USGv6-r1:Host + Core + Addr-Arch + Multicast + SLAAC + Link=Ethernet

Default-IOT = USGv6-r1:Host + 6LoWPAN + Link=802.15.4

Default-Enterprise-Router = USGv6-r1:Router + Core + Addr-Arch + Multicast + [OSPF|ISIS] + [SNMP|NETCONF] + Dual-Stack + Link=Ethernet

Default-Intranet-Router = USGv6-r1:Router + Core + Addr-Arch + Multicast + OSPF + [SNMP|NETCONF] + [IPsec|TLS] + [Dual-Stack|Tunneling] + Multicast-Routing + Link=Ethernet

Default-CE-Router = USGv6-r1:Router + CE-Router + Link=Ethernet

Default-MAP-E = USGv6-r1:Router + CE-Router + MAP-E + Link=Ethernet

Default-Border-Router = USGv6-r1:Router + Core + Addr-Arch + Multicast + BGP + TLS + [OSPF|ISIS] + [SNMP|NETCONF] + Dual-Stack + Tunneling + Link=Ethernet

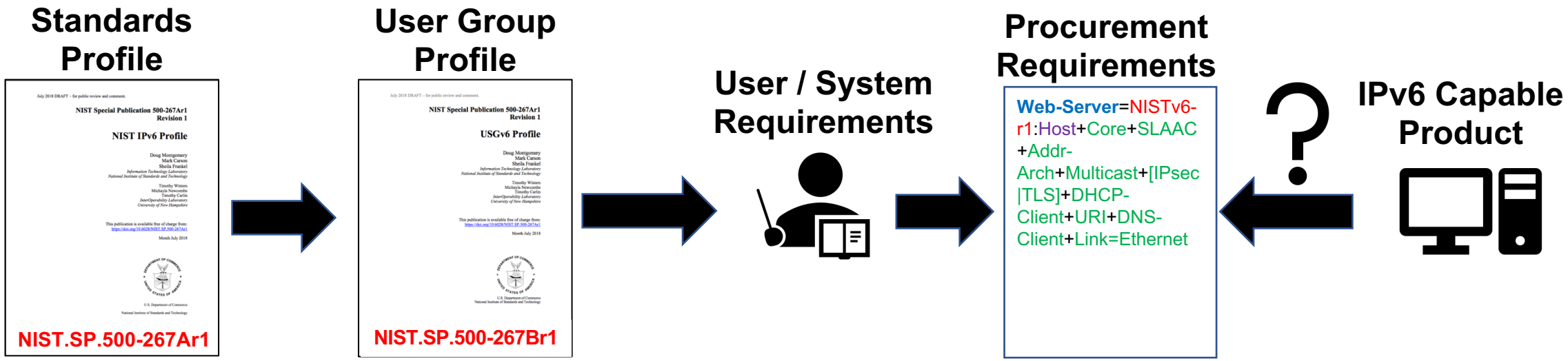
Default-SGW = USGv6-r1:Router + Core + TLS + IPsec-VPN + Link=Ethernet

Default-Firewall = USGv6-r1:NPP + Firewall

Default-IDS/IPS = USGv6-r1:NPP + IPS + IDS

Capability Summary Strings

- **<Label>=Profile:<Host|Router|NPD>+<Capabilities>**
  - Labels are groups of the requirements a procurement might want to specify.
  - Can specify capability choice. e.g. [DHCP-Client|SLAAC]
  - A single product might have multiple capability strings for different stacks / management.
- **Agency-Default-Server**=USGv6-r1:Host+Core+SLAAC+Addr-Arch+Multicast+[IPsec|TLS]+DHCP-Client+URI+DNS-Client+Link=Ethernet



USGv6 Test Program

- **USGv6 Test Program committed to converge / harmonize**
  - IPv6 Ready Logo Test Specifications
    - NIST and IPv6 Forum sign MOU
  - DoD Generic Test Plan test cases
- Claims of compliance documented using Supplier's Declaration of Conformity (SDoC)

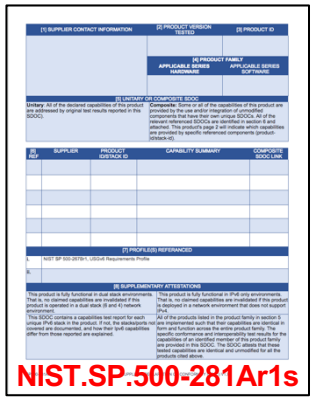
IPv6 Capable Product

USGv6 Accredited Laboratory

Standard Test Methods

Conformance + Interoperability

USGv6 SDOC



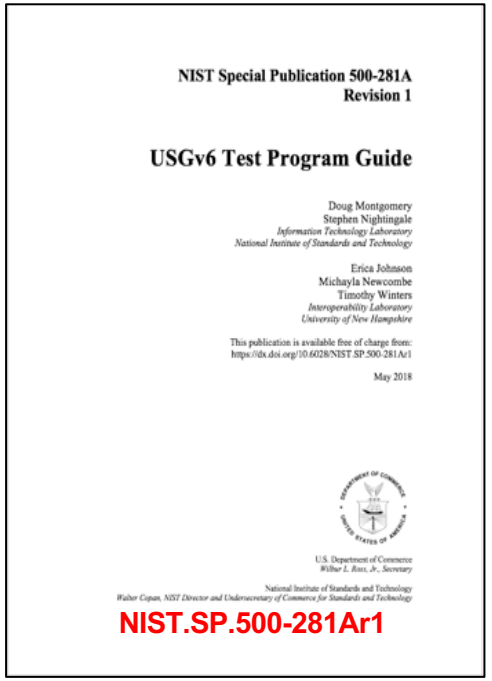
NIST.SP.500-281Ar1s

Product IPv6 Capabilities

Agency-Default-Server=NISTv6-r1:Host+Core+SLAAC+Addr-Arch+Multicast+[IPsec|TLS]+DHCP-Client+URI+DNS-Client+Link=Ethernet

USGv6 Testing Program Definitions

- **Quality Program for Test Labs.**
  - Allows for 1st, 2nd, 3rd party labs.
  - Requires 3rd party accreditation.
  - Defines requirements for accreditation for specific test methods.
  - Defines methods for inter-laboratory comparisons and quality control.
- **Defines Detailed Issues of Testing**
  - Product life cycles
  - Composite and OEM products
  - Suppliers Declaration of Conformity (SDOC) reporting.


NIST Special Publication 500-281A
Revision 1

USGv6 Test Program Guide

Doug Montgomery
Stephen Nightingale
Information Technology Laboratory
National Institute of Standards and Technology

Erica Johnson
Michayla Newcombe
Timothy Winters
Interoperability Laboratory
University of New Hampshire

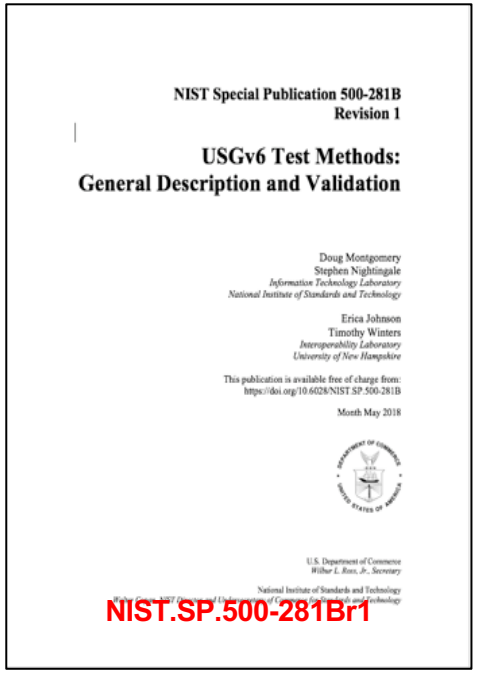
This publication is available free of charge from:
https://dx.doi.org/10.6028/NIST.SP.500-281Ar1

May 2018

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

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

NIST.SP.500-281Ar1


NIST Special Publication 500-281B
Revision 1

USGv6 Test Methods:
General Description and Validation

Doug Montgomery
Stephen Nightingale
Information Technology Laboratory
National Institute of Standards and Technology

Erica Johnson
Timothy Winters
Interoperability Laboratory
University of New Hampshire

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-281B

Month May 2018

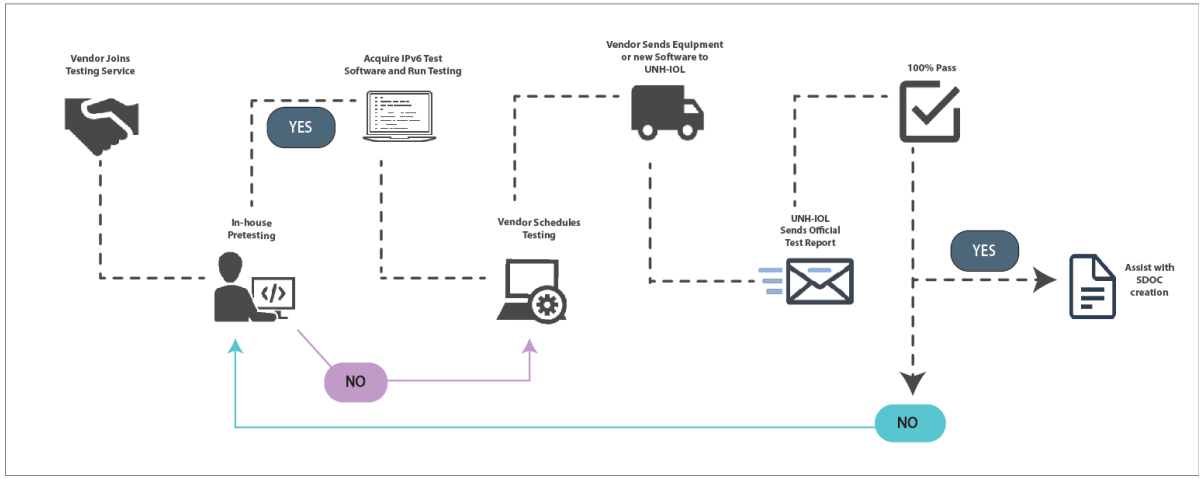
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology

NIST.SP.500-281Br1

USGv6 Test Program

- **USGv6 Tested Product List**
  - https://www.iol.unh.edu/registry/usgv6
  - Hosts Tested (298)
  - Routers Tested (142)
  - NPDs Tested (34)
  - ~1400 products tested for USGv6
    - Over 10,000 products listed.



University of New Hampshire InterOperability Laboratory

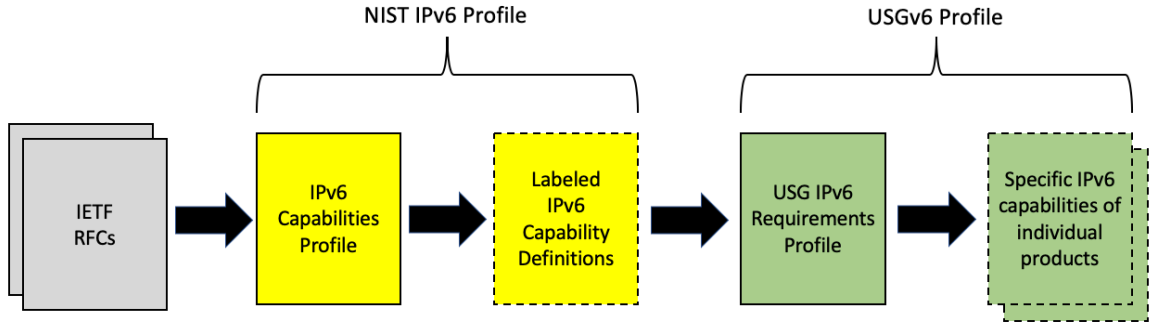
Company	Product Name	Type	Version Tested	Hardware	Software	Test Suites	SDoc
Cisco Systems	Cisco ATA 191 Analog Telephone Adapter	Host	12.0(1)SR1	• ATA 191 Analog Telephone Adapter	12.0(1)SR1	• Basic Interoperability v1.1 (29915) • Basic Conformance v1.2 (29913) • SLAAC Interoperability v1.2 (29915) • SLAAC Conformance v1.1 (29913) • Addr Arch Interoperability v1.1 (29914) • Addr Arch Conformance v1.2 (29912)	View
Riverbed Technology, Inc.	Riverbed SteelFusion	Host	6.0.0	• SteelFusion Core: SteelFusion Core 3500 • SteelFusion Edge: SteelFusion Edge 2100, SteelFusion Edge 2200, SteelFusion Edge 3100, SteelFusion Edge 3200, SteelFusion Edge 5100	Virtual SteelFusion Core 6.0 Virtual SteelFusion Edge 6.0	• Basic Interoperability v1.1 (29579) • Basic Conformance v1.2 (29577) • SLAAC Interoperability v1.2 (29579) • SLAAC Conformance v1.1 (29577) • Addr Arch Interoperability v1.1 (29580) • Addr Arch Conformance v1.2 (29578)	View
Microsoft Corporation	Windows Server	Host	Windows 2016 Server		Windows 2016 Server and all versions of Windows based on the Windows Server stack without any significant changes that would affect the performance of the IPv6 stack.	• Basic Interoperability v1.1 (29787) • Basic Conformance v1.2 (29786) • SLAAC Interoperability v1.2 (29787) • SLAAC Conformance v1.1 (29786) • Addr Arch Interoperability v1.1 (29789) • Addr Arch Conformance v1.2 (29788)	View

Coordination and Consolidation of Efforts!

- **Avoid Duplication of Efforts!**
  - Primary impact is creating undue burden on industry!
    - Divergent product requirements.
    - Repetitive, non-standard testing requirements.
    - Non portability of test results
    - Possible rejection of all profile / test efforts.
  - Already many profile / test activities
    - IPv6 Ready, USGv6, DoD/UCR, Broadband Forum, ETSI, etc.
    - Country specific profiles / test programs beginning to emerge
      - Malaysia, etc.
- **Profile / Testing Convergence**
  - Conformance / interop testing of commodity products should converge to the maximum extent possible.
    - Open, standardized test suites.
    - Maximum leverage of industry driven test programs.
    - Common test reporting mechanism.
- **Use Case Specific Testing**
  - Free resources to focus more important testing issues such as: information assurance, system integration, performance, scaling, etc.

USGv6 Profile – Derived from NISTv6

- **Specified as delta to NISTv6r1**
  - Changes to capability selection recommendations.
  - Changes to conformance requirements.
  - New example CSS strings.
    - **USGv6-Capable-Host** = USGv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + [SLAAC|DHCP-Client] + [IPsec|TLS] + Link=Ethernet
    - **USGv6-Capable-Router** = USGv6-r1:Router + IPv6-Only + Core + Addr-Arch + Multicast + SLAAC + [IPsec|TLS] + [SNMP|NETCONF] + [CE-Router|OSPF|IS-IS|BGP] + DiffServ + [Tunneling-IP|Tunneling-UDP] + Link=Ethernet
    - **USGv6-Capable-Switch** = USGv6-r1:Switch + IPv6-Only + DHCPv6-Guard + RA-Guard + MLD-Snooping + Link=Ethernet
    - **USGv6-Capable-Application** = USGv6-r1:App-Serv + IPv6-Only + App-Serv=[TBD]



USGv6-r1:Host Capabilities Template:

- **IPv6-Only Capabilities** - see section 4.2
  - [M] - **IPv6-Only** - support for full product functionality on an IPv6-only network.
- **Basic Capabilities** - see section 4.3
  - [O:1=[SLAAC | DHCP-Client]] - **SLAAC** - support for stateless global address auto-configuration.
  - [O:1=[SLAAC | DHCP-Client]] - **DHCP-Client** - support for stateful (DHCP) address auto-configuration.
- **Security Capabilities** - see section **Error! Reference source not found.**
  - [O:1=[IPsec | TLS]] - **IPsec** - support for the IP security architecture.
  - [O:1=[IPsec | TLS]] - **TLS** - support for Transport Layer Security architecture version 1.2.
  - [X] - **IPsec-IoT** - support for IoT Cryptographic Algorithms.
  - [X] - **IPsec-CHACHA** - support for ChaCha20 Cryptographic Algorithms.
  - [X] - **IPsec-SHA-512** - support for SHA-512 Cryptographic Algorithms.

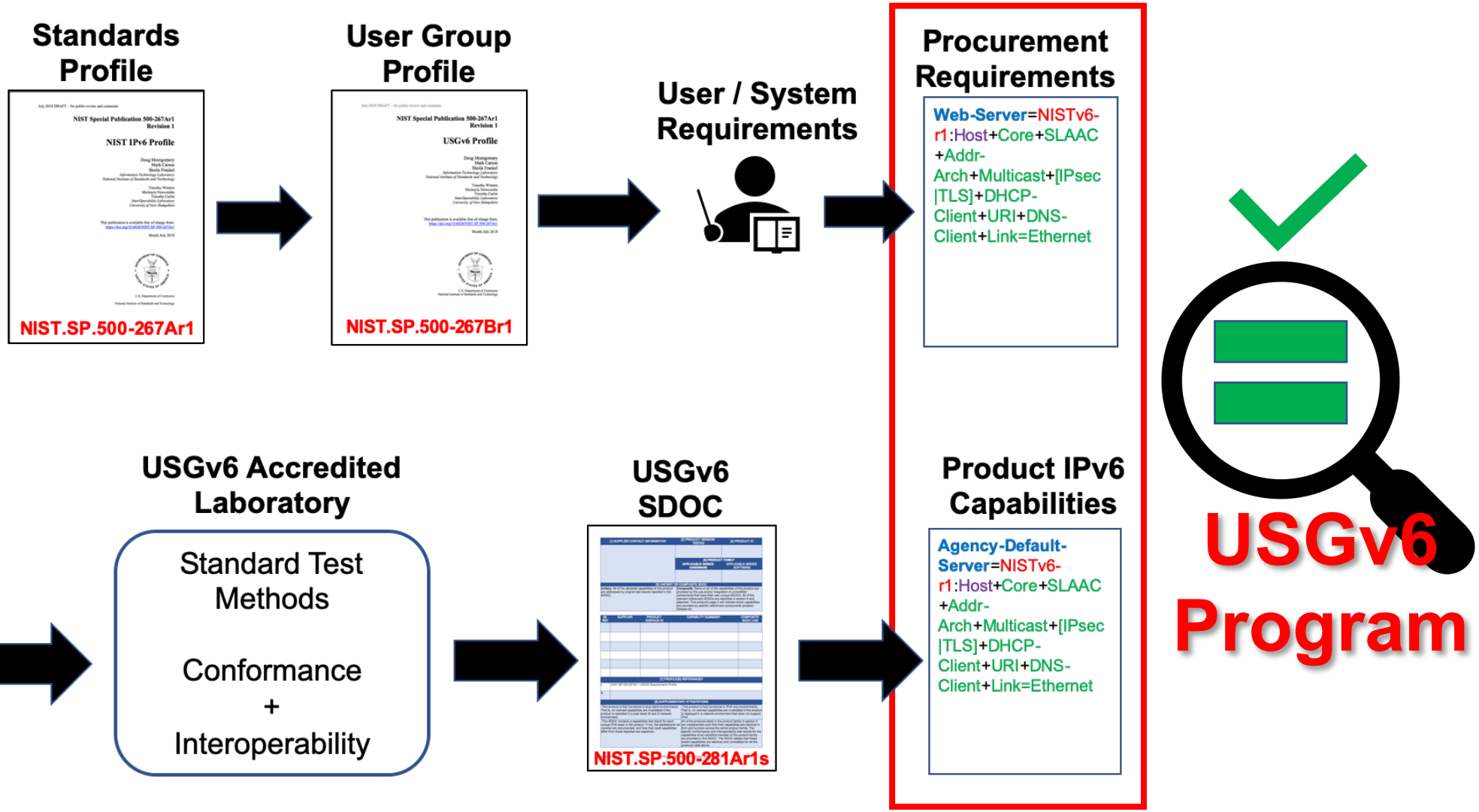
USGv6 Profile Establishes a Vocabulary

- **Example: Use of NISTv6 Profile to Express DoD requirements:**
  - Requirements from: “DoD IPv6 Standard Profiles For IPv6 Capable Products Version 6.0", DISR IPv6 Standards Technical Working Group, July 2011. Online at: https://www.hpc.mil/images/hpcdocs/ipv6/disr_ipv6_profile_version_6_july_2011.pdf
  - **DOD-Host** = USGv6-r1:Host + Core + [SLAAC|DHCP-Client] + Addr-Arch + DNS-Client + Multicast + IPSec + [Dual-Stack|Tunneling] + Link=Ethernet
  - **DOD-Simple-Server** = USGv6-r1:Host + Core + [SLAAC|DHCP-Client] + Addr-Arch + Link=Ethernet
  - **DOD-Advanced-Server** = USGv6-r1:Host + Core + Addr-Arch + DNS-Client + Multicast + IPSec + [Dual-Stack|Tunneling] + Link=Ethernet
  - **DOD-Router** = USGv6-r1:Router + Core + SLAAC + Addr-Arch + Multicast + IPSec + DS + SNMP + [Dual-Stack|Tunneling] + Link=Ethernet
  - **DOD-L3-Switch** = USGv6-r1:Router + Core + Addr-Arch + Multicast + [Dual-Stack|Tunneling] + DS + Link=Ethernet
  - **DOD-IAD** = Core + Addr-Arch + Multicast + Link=Ethernet

"USGv6 Conformance" - Misconceptions

- **Products can't "conform to USGv6 Profile".**
  - They can conform to a requirement defined in terms of the profile.
    - **USGv6-Capable-Host** = USGv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + [SLAAC|DHCP-Client] + [IPsec|TLS] + Link=Ethernet
- **Tested vs Approved Products?**
  - USGv6 Test Program results in a report of claimed and tested IPv6 product capabilities.
    - Having a USGv6 SDoC does not mean it is a USGv6 approved product!
  - It is up to users to examine the results and to see if they meet their acquisition requirements requirements.
- **FAR requirements**
  - "Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program."
- **Defining Acquisition Requirements**
  - Appendix A of the NIST IPv6 profile and USGv6 Profile contain numerous examples of Capability Summary Strings.
    - Specifying a CSS for a specific type of product effectively defines an approved product list.
    - Adapt examples to your needs.
      - **NIST-Laptop** = USGv6-r1:Host + IPv6-Only + Core + Addr-Arch + Multicast + SLAAC + DHCP-Client + TLS + Link=WiFi

USGv6 Program: The Big Picture



Questions and Discussion

- **For more information:**
  - USGv6 Program
    - https://www.nist.gov/programs-projects/usgv6-program
    - usgv6-program@nist.gov
  - Advanced Network Technologies Division.
    - https://www.nist.gov/itl/antd
  - Information Technology Laboratory
    - https://www.nist.gov/itl