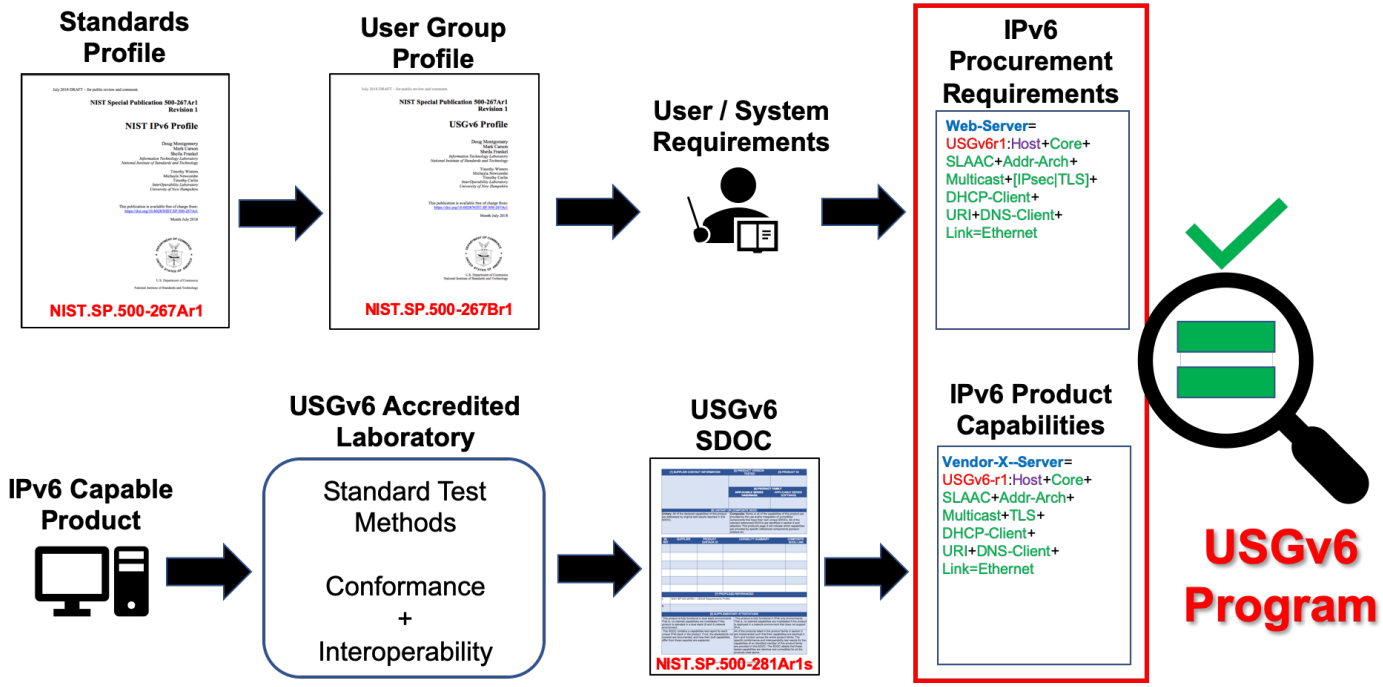
USGv6 Program

Supporting the USG Transition to IPv6-Only Networks



Doug Montgomery / NIST / USGv6 Program Manager. (dougm@nist.gov)

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

Introductions

- **Doug Montgomery**
  - https://www.nist.gov/people/doug-montgomery
  - douglas.montgomery@nist.gov

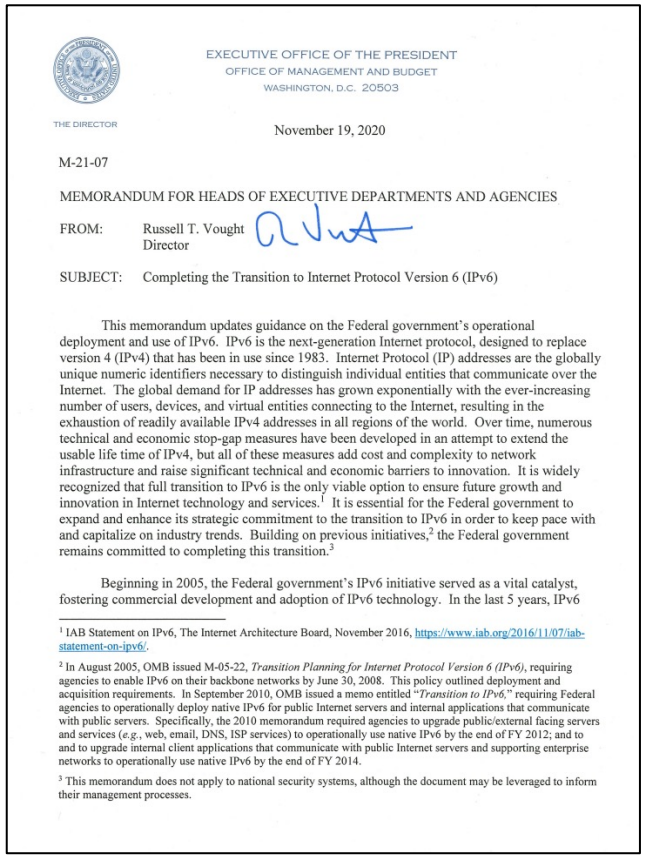
  - **Manager, Internet Technologies Research Program.**
    - https://www.nist.gov/itl/antd/internet-scalable-systems-research

  - **Program Manager – USGv6 Program**
    - https://www.nist.gov/programs-projects/usgv6-program

  - 35+ years as technical leader in NIST efforts in Internet technologies research, standardization and security.

USG Transition to IPv6-Only Networks

- **Completing the USG Transition to IPv6**
  - https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf
  - *"The strategic intent is for the Federal government to deliver its information services, operate its networks, and access the services of others using only IPv6"*
  - *At least 20% IPv6-only by the end of FY 2023*
  - *At least 50% IPv6-only by the end of FY 2024*
  - *At least 80% IPv6-only by the end of FY 2025*
  - *Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;*



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 19, 2020

M-21-07

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Completing the Transition to Internet Protocol Version 6 (IPv6)

This memorandum updates guidance on the Federal government's operational deployment and use of IPv6. IPv6 is the next-generation Internet protocol, designed to replace version 4 (IPv4) that has been in use since 1983. Internet Protocol (IP) addresses are the globally unique numeric identifiers necessary to distinguish individual entities that communicate over the Internet. The global demand for IP addresses has grown exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet, resulting in the exhaustion of readily available IPv4 addresses in all regions of the world. Over time, numerous technical and economic stop-gap measures have been developed in an attempt to extend the usable life time of IPv4, but all of these measures add cost and complexity to network infrastructure and raise significant technical and economic barriers to innovation. It is widely recognized that full transition to IPv6 is the only viable option to ensure future growth and innovation in Internet technology and services.[1] It is essential for the Federal government to expand and enhance its strategic commitment to the transition to IPv6 in order to keep pace with and capitalize on industry trends. Building on previous initiatives,[2] the Federal government remains committed to completing this transition.[3]

Beginning in 2005, the Federal government's IPv6 initiative served as a vital catalyst, fostering commercial development and adoption of IPv6 technology. In the last 5 years, IPv6

[1] IAB Statement on IPv6, The Internet Architecture Board, November 2016, https://www.iab.org/2016/11/07/iab-statement-on-ipv6/.

[2] In August 2005, OMB issued M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, requiring agencies to enable IPv6 on their backbone networks by June 30, 2008. This policy outlined deployment and acquisition requirements. In September 2010, OMB issued a memo entitled "*Transition to IPv6*," requiring Federal agencies to operationally deploy native IPv6 for public Internet servers and internal applications that communicate with public servers. Specifically, the 2010 memorandum required agencies to upgrade public/external facing servers and services (*e.g.*, web, email, DNS, ISP services) to operationally use native IPv6 by the end of FY 2012; and to and to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.

[3] This memorandum does not apply to national security systems, although the document may be leveraged to inform their management processes.

Why IPv6?

- **Enable Internet growth and innovation.**
  - **Remove technical and economic barriers.**
    - IPv4 – the Internet's basis for global interoperability stopped evolving ~20 years ago.
    - IPv4 address exhaustion creates both technical and economic barriers to innovation.
  - **Provide a modern network protocol as the global barer service for interoperability.**
    - In 2016 the IAB adopted a policy that all new standards assume IPv6 and not require IPv4.
    - The result is that in many recent network advances are only designed and standardized for IPv6.

- **Ensure Internet security and stability.**
  - The use of globally unique network addresses significantly improves the effectiveness of today's network defense technologies and cyber forensics.
  - IPv6 and its vast address space enables innovation in network security technologies.

- **Reduce cost and complexity in networks.**
  - Engineering around address exhaustion has had a significant impact on protocol design and system architectures for years.
    - While NAT has successfully extended the life of IPv4, its ramifications on protocol and system design adds cost and complexity to today's networks.
    - In modern networks NATs / CGNATs have become the bottle neck resource in delivering internet scale services.

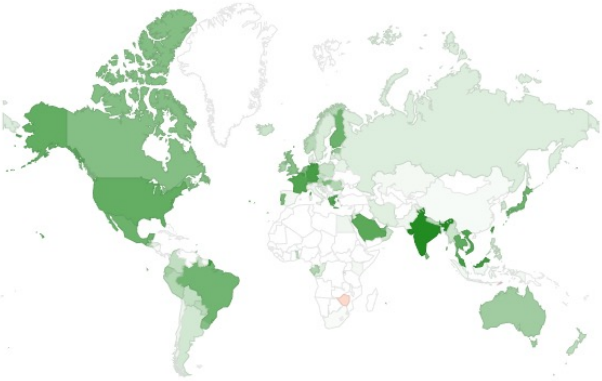
Why Now?

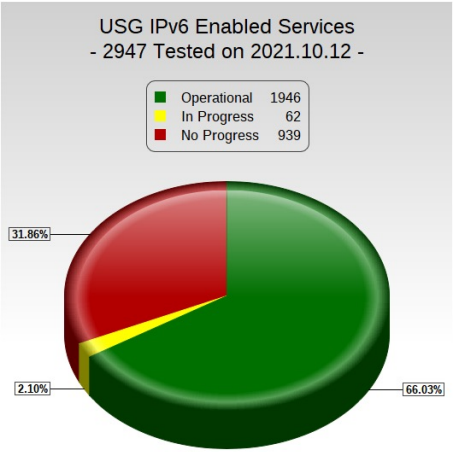
- **In short, it is doable and needs to be done.**
  - Significantly easier than in 2010.

- **Significant advances in both the state of technology and deployment of IPv6 over the last 10 years.**
  - Major operating systems include mature IPv6 implementations.
  - Major ISPs and service providers have IPv6 services.

- **IPv6 deployment and use is growing throughout the Internet.**
  - Various measurement efforts (with differing techniques) show significant growth in IPv6 adoption and use
  - USG agencies have gained operational IPv6 deployment experience over the last 10 years.

- **Industry and Governments aligned on strategic direction.**
  - Numerous large enterprises, service providers, governments / DoD have stated plans to migrate to IPv6-only environments in the next 5-10 years.
    - Some organizations are already there in data-center networks, mobile broadband networks, ISP core network functions.





Why IPv6-Only?

- **Why would you operate two protocol stacks if you did not have to?**
  - Is continued support of IPv4 a strategic goal?

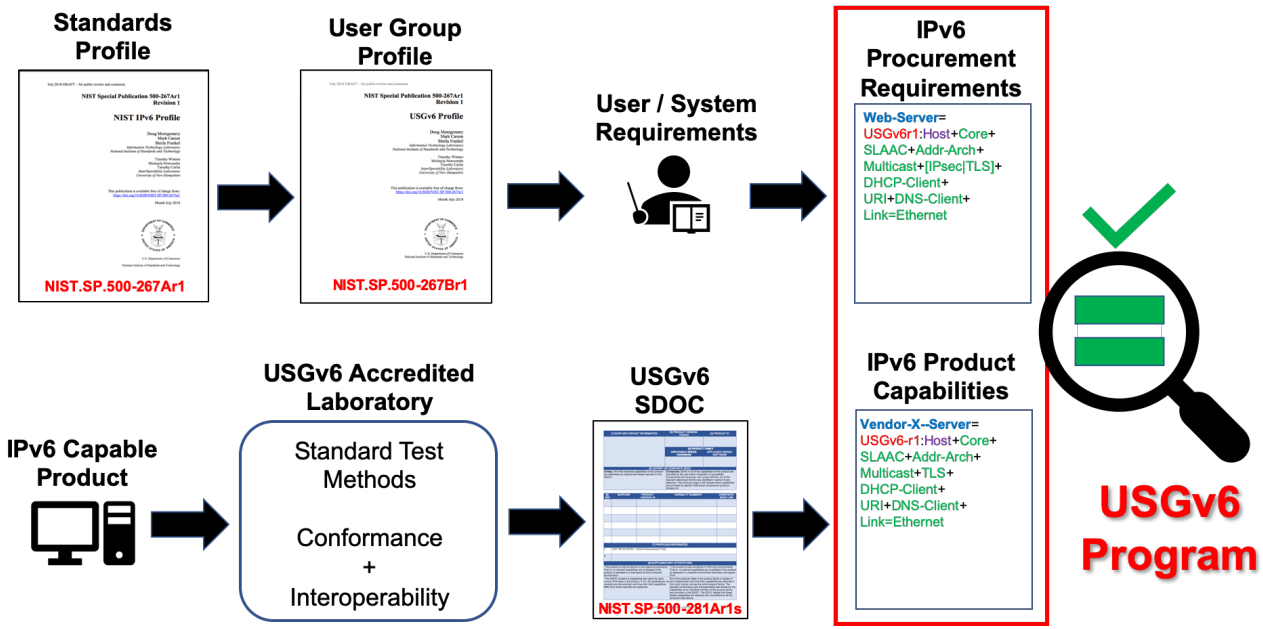
- **Ubiquitous dual-stack networking is a necessary transition phase in IPv6 deployment …**
  - … but it is not designed nor desired to be a final state.
  - Operating the control and data plane for two IP protocols does add some complexity to network operations.
  - Increased attack surface to secure – although few attacks are IP centric.
  - Monitoring and debugging dual-stacked hosts is complicated by simultaneous use of two protocols.

- **Commercial implementations of scalable transition mechanisms are readily available.**
  - To allow IPv6-only systems to communicate with IP4 only systems.

- **Getting to IPv6-only will require work in some areas**
  - Application space is near infinite – legacy applications that are not IPv6 capable must be addressed.
  - Some environments – such as network internals of cloud service providers will require longer to migrate.
  - IPv6 support of full range of networked functions (install, configure, update, etc) on some platforms are still under development.

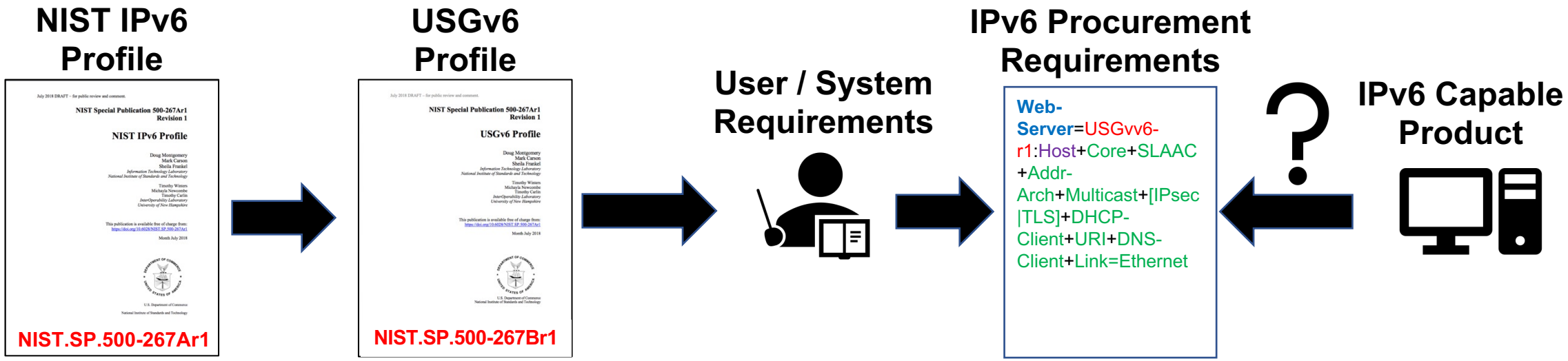
USGv6 Profile and Test Program

- **How to evolve IT infrastructure?**
  - Establish policies to always buy IPv6-capable networked IT.
    - Long term tech refresh cycles.
- **How to define IPv6-capable?**
  - Establish means for specifying detailed IPv6 capability requirements in individual procurements.
- **How to protect IPv6 investments?**
  - Establish means to test vendor products against requirements statements.
    - Conformance, Interoperability, and Functional tests to insure completeness, correctness and interoperability.



USGv6 Profile: IPv6 Capability Vocabulary

- **<Label>=Profile:<Host|Router|NPP>+<Capabilities>**
  - Capability Summary String (CSS) – Named set of IPv6 requirements for a specific system.
  - Can specify capability choice. e.g. [DHCP-Client|SLAAC]
  - A single product might have multiple capability strings for different stacks / management.
- **Agency-Web-Server**=USGv6-r1:Host+Core+SLAAC+Addr-Arch+Multicast+[IPsec|TLS]+DHCP-Client+URI+DNS-Client+Link=Ethernet



USGv6 Profile – Details

Defines Capability Choices for Products

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.

Maps Capabilities to Technical Requirements

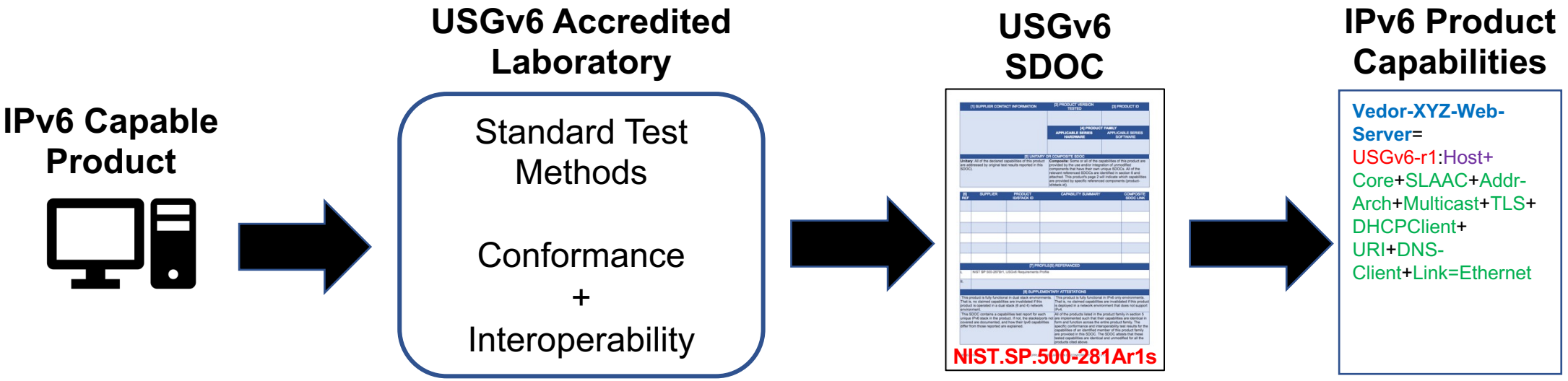
Basic Capabilities					
Flag	**Host**	**Router**	**Other**	**Capability**	**Definition**
	✓	✓		**Core**	**support for IPv6 core functions.**
U	✓	✓			RFC8200 *Internet Protocol, Version 6 (IPv6) Specification*
	✓	✓			RFC4443 *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 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*

Mandates support for optional feature

Groups requirements in logical / testable sets

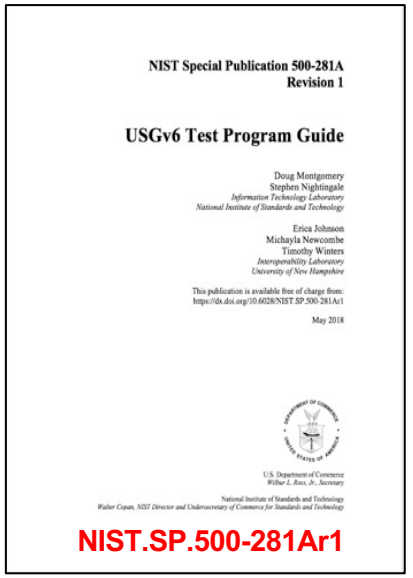
USGv6 Test Program

- **USG defined and managed - operated by independent test laboratories.**
- **USGv6 Test Program committed to converge / harmonize**
  - IPv6 Ready Logo Test Specifications
    - NIST and IPv6 Forum sign MOU
- Claims of compliance documented using Supplier's Declaration of Conformity (SDoC)

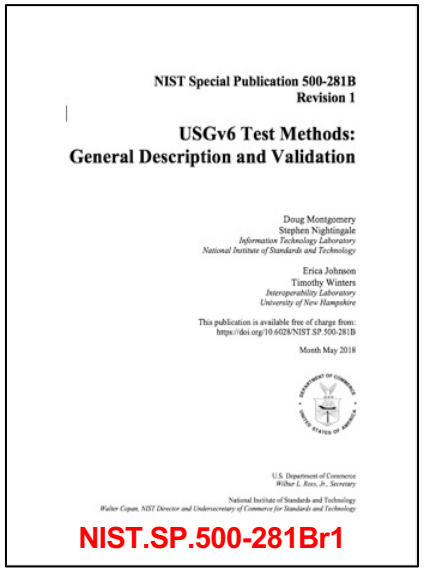


USGv6 Testing Program Definitions

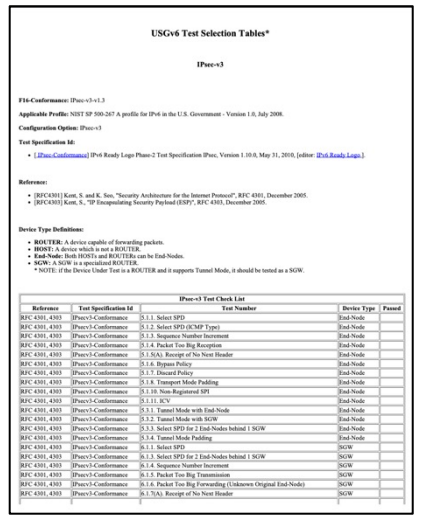
- **Quality Program for Test Labs.**
  - Allows for 1st, 2nd, 3rd party labs.
  - Requires laboratory accreditation.
    - Defines requirements for accreditation for specific test methods.
    - Defines methods for inter-laboratory comparisons and quality control.
- **Defines Detailed Issues of Testing**
  - Product life cycles
  - Product families
  - Composite and OEM products
  - Suppliers Declaration of Conformity (SDOC)
- **Standardized Test Suites**
  - Test selection tables
    - https://www.nist.gov/programs-projects/usgv6-program


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

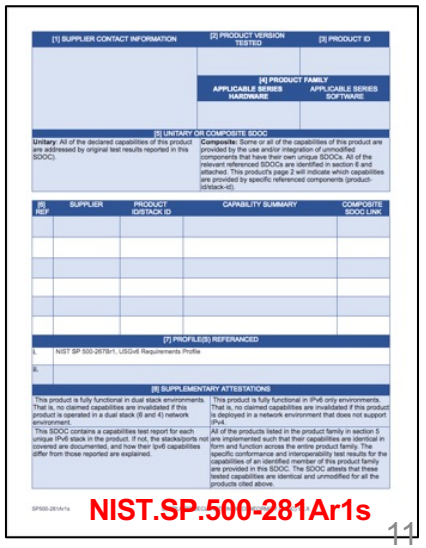
NIST.SP.500-281Ar1


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

NIST.SP.500-281Br1


USGv6 Test Selection Tables*
IPsec-v3
F16-Conformance: IPsec-v3-v1.3
Applicable Profile: NIST SP 500-267 A profile for IPv6 in the U.S. Government - Version 1.0, July 2008.
Configuration Option: IPsec-v3
Test Specification Id:
• [IPsec-Conformance] IPv6 Ready Logo Phase-2 Test Specification IPsec, Version 1.10.0, May 31, 2010, [editor: IPv6 Ready Logo.]
Reference:
• [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
• [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
Device Type Definitions:
• ROUTER: A device capable of forwarding packets.
• HOST: A device which is not a ROUTER.
• End-Node: Both HOSTs and ROUTERs can be End-Nodes.
• SGW: A SGW is a specialized ROUTER.
* NOTE: if the Device Under Test is a ROUTER and it supports Tunnel Mode, it should be tested as a SGW.
IPsec-v3 Test Check List

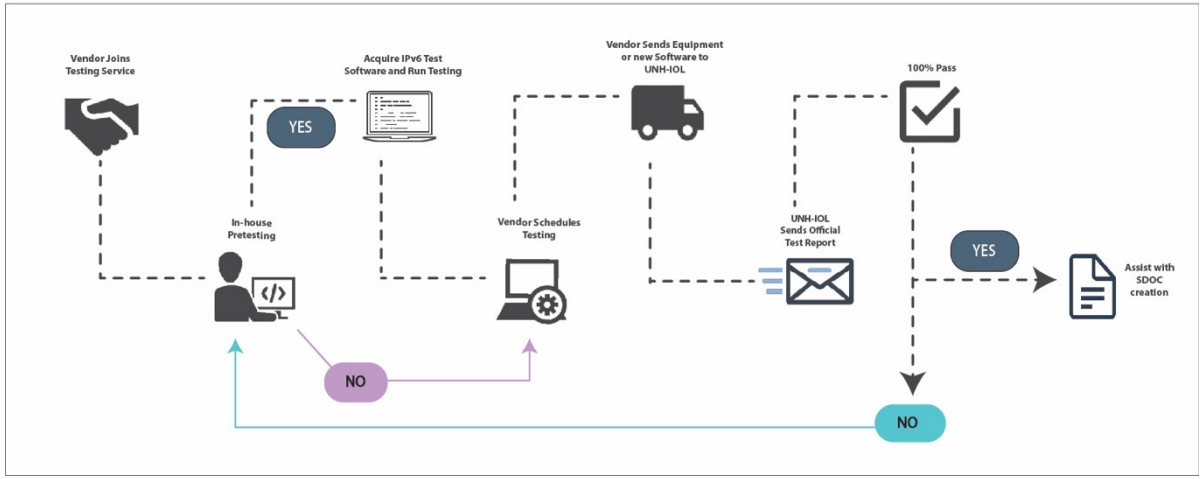
Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4301, 4303	IPsecv3-Conformance	5.1.1. Select SPD	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.2. Select SPD (ICMP Type)	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.3. Sequence Number Increment	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.4. Packet Too Big Reception	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.5(A). Receipt of No Next Header	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.6. Bypass Policy	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.7. Discard Policy	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.8. Transport Mode Padding	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.10. Non-Registered SPI	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.1.11. ICV	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.2.1. Tunnel Mode with End-Node	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.3.2. Tunnel Mode with SGW	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.3.3. Select SPD for 2 End-Nodes behind 1 SGW	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	5.3.4. Tunnel Mode Padding	End-Node	
RFC 4301, 4303	IPsecv3-Conformance	6.1.1. Select SPD	SGW	
RFC 4301, 4303	IPsecv3-Conformance	6.1.3. Select SPD for 2 End-Nodes behind 1 SGW	SGW	
RFC 4301, 4303	IPsecv3-Conformance	6.1.4. Sequence Number Increment	SGW	
RFC 4301, 4303	IPsecv3-Conformance	6.1.5. Packet Too Big Transmission	SGW	
RFC 4301, 4303	IPsecv3-Conformance	6.1.6. Packet Too Big Forwarding (Unknown Original End-Node)	SGW	
RFC 4301, 4303	IPsecv3-Conformance	6.1.7(A). Receipt of No Next Header	SGW	


[1] SUPPLIER CONTACT INFORMATION
[2] PRODUCT VERSION TESTED
[3] PRODUCT ID
[4] PRODUCT FAMILY
APPLICABLE SERIES HARDWARE
APPLICABLE SERIES SOFTWARE
[5] UNITARY OR COMPOSITE SDOC
Unitary: All of the declared capabilities of this product are addressed by original test results reported in this SDOC).
Composite: Some or all of the capabilities of this product are provided by the use and/or integration of unmodified components that have their own unique SDOCs. All of the relevant referenced SDOCs are identified in section 6 and attached. This product's page 2 will indicate which capabilities are provided by specific referenced components (product-id/stack-id).
[6] REF
SUPPLIER
PRODUCT ID/STACK ID
CAPABILITY SUMMARY
COMPOSITE SDOC LINK
[7] PROFILE(S) REFERENCED
a. NIST SP 500-267Br1, USGv6 Requirements Profile
b.
[8] SUPPLEMENTARY ATTESTATIONS
This product is fully functional in dual stack environments. That is, no claimed capabilities are invalidated if this product is operated in a dual stack (6 and 4) network environment.
This product is fully functional in IPv6 only environments. That is, no claimed capabilities are invalidated if this product is deployed in a network environment that does not support IPv4.
This SDOC contains a capabilities test report for each unique IPv6 stack in the product. If not, the stacks/ports not covered are documented, and how their Ipv6 capabilities differ from those reported are explained.
All of the products listed in the product family in section 5 are implemented such that their capabilities are identical in form and function across the entire product family. The specific conformance and interoperability test results for the capabilities of an identified member of this product family are provided in this SDOC. The SDOC attests that these tested capabilities are identical and unmodified for all the products cited above.

NIST.SP.500-281Ar1s

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

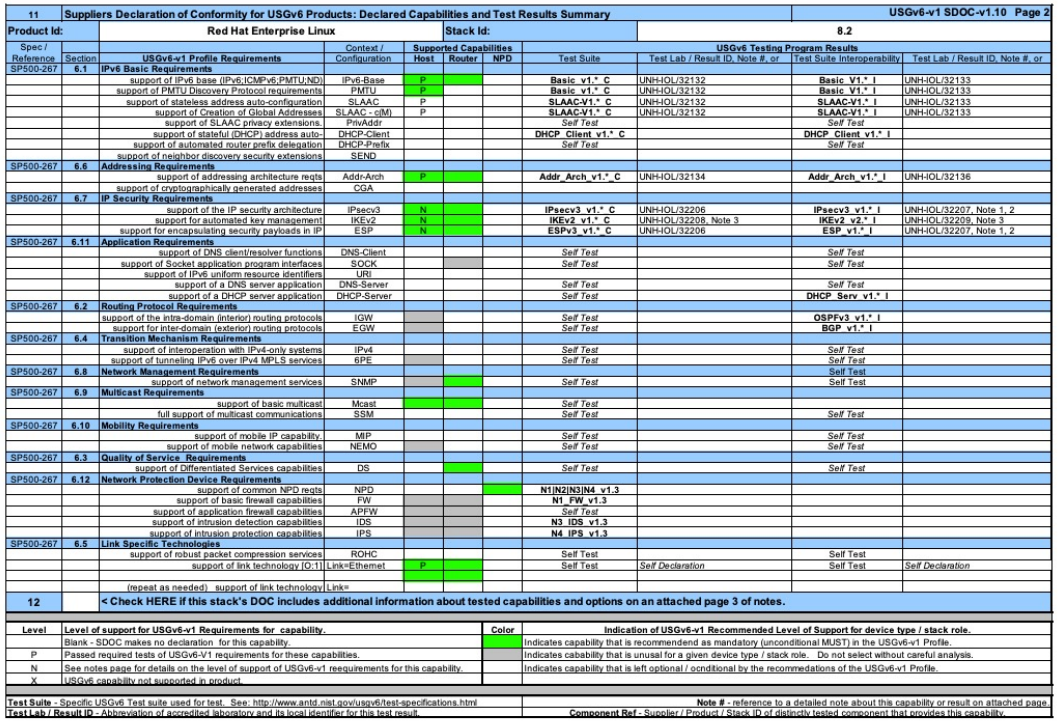
Company	Product Name	Type	Version Tested	Hardware	Software	Test Suites	SDoc
Cisco Systems	Cisco ATA 191 Analog Telephone Adapter	Host	12.0(1)SR1	• ATA 191 Analog Telephone Adapter	12.0(1)SR1	• Basic Interoperability v1.1 (29915) • Basic Conformance v1.2 (29913) • SLAAC Interoperability v1.2 (29915) • 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

USGv6 Testing & Reporting

https://www.iol.unh.edu/registry/usgv6

- **Detailed Conformance and Interop Results**
  - Standardized test suites, standardized reporting format.
- **Goal - Full Disclosure of IPv6 capabilities**
  - Report of capabilities that pass all conformance and Interop Tests
    - Red Hat REL 8.2 = USGv6-v1-Host: IPv6-Base+Addr-Arch+SLAAC+Link = Ethernet
- **Pragmatic Test Reports**
  - Some ”near miss” capabilities are reported with notes as to what was missing / failed.
    - See IPsec notes on REL 8.2 IPsec deficiencies.

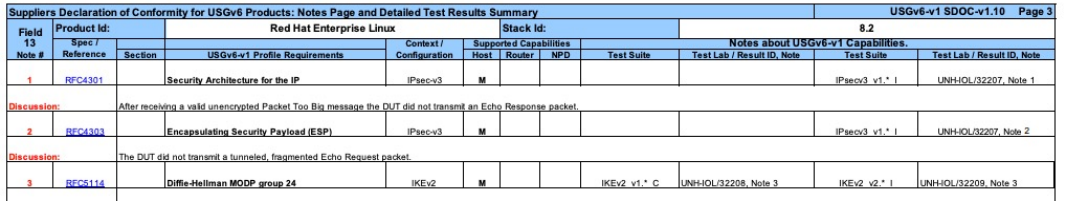
Company	Product Name	Type	Version Tested	Hardware	Software	Test Suites	SDoc
Red Hat	Red Hat Enterprise Linux	Host	8.2		8.2	• Basic Interoperability v1.2 (32133) • Basic Conformance v1.3 (32132) • SLAAC Interoperability v1.3 (32133) • SLAAC Conformance v1.2 (32132) • Addr Arch Interoperability v1.2 (32136) • Addr Arch Conformance v1.3 (32134) • ESP Interoperability v1.1 (32207) * Notes • ESP Conformance v1.1 (32206) • IKEv2 Interoperability v2.0 (32209) * Notes • IKEv2 Conformance v1.1 (32209) * Notes • IPsecv3 Interoperability v1.2 (32207) * Notes • IPsecv3 Conformance v1.3 (32206)	View



11	Suppliers Declaration of Conformity for USGv6 Products: Declared Capabilities and Test Results Summary									USGv6-v1 SDOC-v1.10 Page 2
Product Id:	Red Hat Enterprise Linux				Stack Id:			8.2		
Spec / Reference	Section	USGv6-v1 Profile Requirements	Context / Configuration	Supported Capabilities: Host	Router	NPD	USGv6 Testing Program Results: Test Suite	Test Lab / Result ID, Note #, or	Test Suite Interoperability	Test Lab / Result ID, Note #, or
SP500-267	6.1	**IPv6 Basic Requirements**								
		support of IPv6 base (IPv6;ICMPv6;PMTU;ND)	IPv6-Base	P			Basic_v1.*_C	UNH-IOL/32132	Basic_V1.*_I	UNH-IOL/32133
		support of PMTU Discovery Protocol requirements	PMTU	P			Basic_v1.*_C	UNH-IOL/32132	Basic_V1.*_I	UNH-IOL/32133
		support of stateless address auto-configuration	SLAAC	P			SLAAC-V1.*_C	UNH-IOL/32132	SLAAC-V1.*_I	UNH-IOL/32133
		support of Creation of Global Addresses	SLAAC - (GM)	P			SLAAC-V1.*_C	UNH-IOL/32132	SLAAC-V1.*_I	UNH-IOL/32133
		support of SLAAC privacy extensions.	PrivAddr				*Self Test*		*Self Test*	
		support of stateful (DHCP) address auto-	DHCP-Client				DHCP_Client_v1.*_C		DHCP_Client_v1.*_I	
		support of automated router prefix delegation	DHCP-Prefix				*Self Test*		*Self Test*	
		support of neighbor discovery security extensions	SEND							
SP500-267	6.6	**Addressing Requirements**								
		support of addressing architecture reqts	Addr-Arch	P			Addr_Arch_v1.*_C	UNH-IOL/32134	Addr_Arch_v1.*_I	UNH-IOL/32136
		support of cryptographically generated addresses	CGA							
SP500-267	6.7	**IP Security Requirements**								
		support of the IP security architecture	IPsecv3	N			IPsecv3_v1.*_C	UNH-IOL/32206	IPsecv3_v1.*_I	UNH-IOL/32207, Note 1, 2
		support for automated key management	IKEv2	N			IKEv2_v1.*_C	UNH-IOL/32208, Note 3	IKEv2_v2.*_I	UNH-IOL/32209, Note 3
		support for encapsulating security payloads in IP	ESP	N			ESPv3_v1.*_C	UNH-IOL/32206	ESP_v1.*_I	UNH-IOL/32207, Note 1, 2
SP500-267	6.11	**Application Requirements**								
		support of DNS client/resolver functions	DNS-Client				*Self Test*		*Self Test*	
		support of Socket application program interfaces	SOCK				*Self Test*		*Self Test*	
		support of IPv6 uniform resource identifiers	URI							
		support of a DNS server application	DNS-Server				*Self Test*		*Self Test*	
		support of a DHCP server application	DHCP-Server				*Self Test*		DHCP_Serv_v1.*_I	
SP500-267	6.2	**Routing Protocol Requirements**								
		support of the intra-domain (interior) routing protocols	IGW				*Self Test*		OSPFv3_v1.*_I	
		support for inter-domain (exterior) routing protocols	EGW				*Self Test*		BGP_v1.*_I	
SP500-267	6.4	**Transition Mechanism Requirements**								
		support of interoperation with IPv4-only systems	IPv4				*Self Test*		*Self Test*	
		support of tunneling IPv6 over IPv4 MPLS services	6PE				*Self Test*		*Self Test*	
SP500-267	6.8	**Network Management Requirements**							Self Test	
		support of network management services	SNMP				*Self Test*		Self Test	
SP500-267	6.9	**Multicast Requirements**								
		support of basic multicast	Mcast				*Self Test*			
		full support of multicast communications	SSM				*Self Test*		*Self Test*	
SP500-267	6.10	**Mobility Requirements**								
		support of mobile IP capability.	MIP				*Self Test*		*Self Test*	
		support of mobile network capabilities	NEMO				*Self Test*		*Self Test*	
SP500-267	6.3	**Quality of Service Requirements**								
		support of Differentiated Services capabilities	DS				*Self Test*		*Self Test*	
SP500-267	6.12	**Network Protection Device Requirements**								
		support of common NPD reqts	NPD				N1|N2|N3|N4_v1.3			
		support of basic firewall capabilities	FW				N1_FW_v1.3			
		support of application firewall capabilities	APFW				*Self Test*			
		support of intrusion detection capabilities	IDS				N3_IDS_v1.3			
		support of intrusion protection capabilities	IPS				N4_IPS_v1.3			
SP500-267	6.5	**Link Specific Technologies**								
		support of robust packet compression services	ROHC				Self Test		Self Test	
		support of link technology [O:1]	Link=Ethernet	P			Self Test	*Self Declaration*	Self Test	*Self Declaration*
		(repeat as needed) support of link technology	Link=							
12		**< Check HERE if this stack's DOC includes additional information about tested capabilities and options on an attached page 3 of notes.**								

Level	Level of support for USGv6-v1 Requirements for capability.	Color	Indication of USGv6-v1 Recommended Level of Support for device type / stack role.
	Blank - SDOC makes no declaration for this capability.		Indicates capability that is recommended as mandatory (unconditional MUST) in the USGv6-v1 Profile.
P	Passed required tests of USGv6-V1 requirements for these capabilities.		Indicates cabability that is unusal for a given device type / stack role. Do not select without careful analysis.
N	See notes page for details on the level of support of USGv6-v1 requirements for this capability.		Indicates capability that is left optional / conditional by the recommendations of the USGv6-v1 Profile.
X	USGv6 capability not supported in product.		

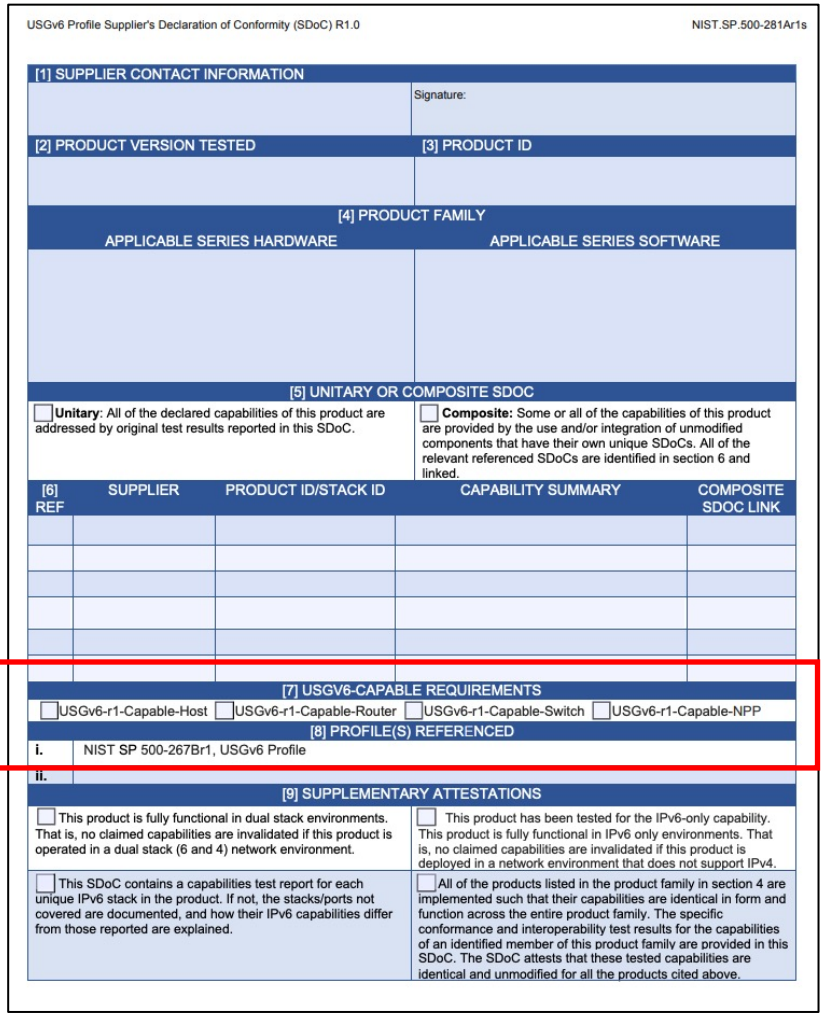
Test Suite - Specific USGv6 Test suite used for test. See: http://www.antd.nist.gov/usgv6/test-specifications.html
Test Lab / Result ID - Abbreviation of accredited laboratory and its local identifier for this test result.
Note # - reference to a detailed note about this capability or result on attached page.
Component Ref - Supplier / Product / Stack ID of distinctly tested component that provides this capability.



Suppliers Declaration of Conformity for USGv6 Products: Notes Page and Detailed Test Results Summary										USGv6-v1 SDOC-v1.10 Page 3
Field 13 Note #	Product Id:		Red Hat Enterprise Linux		Stack Id:			8.2		
	Spec / Reference	Section	USGv6-v1 Profile Requirements	Context / Configuration	Supported Capabilities: Host	Router	NPD	Notes about USGv6-v1 Capabilities: Test Suite	Test Lab / Result ID, Note	Test Suite	Test Lab / Result ID, Note
1	RFC4301		**Security Architecture for the IP**	IPsec-v3	M					IPsecv3_v1.*_I	UNH-IOL/32207, Note 1
Discussion:	After receiving a valid unencrypted Packet Too Big message the DUT did not transmit an Echo Response packet.										
2	RFC4303		**Encapsulating Security Payload (ESP)**	IPsec-v3	M					IPsecv3_v1.*_I	UNH-IOL/32207, Note 2
Discussion:	The DUT did not transmit a tunneled, fragmented Echo Request packet.										
3	RFC5114		**Diffie-Hellman MODP group 24**	IKEv2	M			IKEv2_v1.*_C	UNH-IOL/32208, Note 3	IKEv2_v2.*_I	UNH-IOL/32209, Note 3

Increasing the Usability and Utility of USGv6

- **Example requirement statements**
  - See USGv6 Profile section 5 – Profile Usage Guidance and Examples.
- **Default requirement statements**
  - USGv6 Profile now specifies default definition of "IPv6 Capable" for several product types
    - USGv6-Capable-Host
    - USGv6-Capable-Router
    - USGv6-Capable-Switch
    - USGv6-Capable-NPP
    - USGv6-Capable-Application
  - SDoC now clearly identifies if products meet the above requirements.



USGv6 Profile Supplier's Declaration of Conformity (SDoC) R1.0 — NIST.SP.500-281Ar1s

[1] SUPPLIER CONTACT INFORMATION — Signature:

[2] PRODUCT VERSION TESTED | [3] PRODUCT ID

[4] PRODUCT FAMILY

APPLICABLE SERIES HARDWARE | APPLICABLE SERIES SOFTWARE

[5] UNITARY OR COMPOSITE SDOC

☐ **Unitary**: All of the declared capabilities of this product are addressed by original test results reported in this SDoC.

☐ **Composite:** Some or all of the capabilities of this product are provided by the use and/or integration of unmodified components that have their own unique SDoCs. All of the relevant referenced SDoCs are identified in section 6 and linked.

[6] REF	SUPPLIER	PRODUCT ID/STACK ID	CAPABILITY SUMMARY	COMPOSITE SDOC LINK

[7] USGV6-CAPABLE REQUIREMENTS

☐ USGv6-r1-Capable-Host ☐ USGv6-r1-Capable-Router ☐ USGv6-r1-Capable-Switch ☐ USGv6-r1-Capable-NPP

[8] PROFILE(S) REFERENCED

i. NIST SP 500-267Br1, USGv6 Profile

ii.

[9] SUPPLEMENTARY ATTESTATIONS

☐ This product is fully functional in dual stack environments. That is, no claimed capabilities are invalidated if this product is operated in a dual stack (6 and 4) network environment.

☐ This product has been tested for the IPv6-only capability. This product is fully functional in IPv6 only environments. That is, no claimed capabilities are invalidated if this product is deployed in a network environment that does not support IPv4.

☐ This SDoC contains a capabilities test report for each unique IPv6 stack in the product. If not, the stacks/ports not covered are documented, and how their IPv6 capabilities differ from those reported are explained.

☐ All of the products listed in the product family in section 4 are implemented such that their capabilities are identical in form and function across the entire product family. The specific conformance and interoperability test results for the capabilities of an identified member of this product family are provided in this SDoC. The SDoC attests that these tested capabilities are identical and unmodified for all the products cited above.

USGv6 Revision 1 – Published!

- **Revision of the USGv6 Program**
  - Split profile into generic and USG specific profiles.
  - Update specifications to latest versions.
  - Add new capabilities, including IPv6-Only.
  - Simply the notation and use of the profiles.
  - Simply the definitions of the testing program.
- **Extensive public review**
  - 3 rounds of public comments (USG, DoD, industry).
- **Published November 2020.**
  - https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1

- **Specifications**
  - ***"NIST IPv6 Profile"***, NIST Special Publication (NIST SP) - 500-267Ar1, November 2020.
  - ***"NISTv6 Capabilities Table"***, NIST Special Publication (NIST SP) - 500-267Ar1s, November 2020.
  - ***"USGv6 Profile"***, NIST Special Publication (NIST SP) - 500-267Br1, November 2020.
  - ***"USGv6 Capabilities Table"***, NIST Special Publication (NIST SP) - 500-267Br1s, November 2020.
  - ***"USGv6 Test Program Guide"***, NIST Special Publication (NIST SP) - 500-281Ar1, November 2020.
  - ***"USGv6 Suppliers Declaration of Conformity"***, NIST Special Publication (NIST SP) - 500-281Ar1s, November 2020.
  - ***"USGv6 Test Methods: General Description and Validation"***, NIST Special Publication (NIST SP) - 500-281Br1, November 2020.

"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

Questions and Discussion

- **For more information:**
  - **USGv6 Program**
    - https://www.nist.gov/programs-projects/usgv6-program
  - **Internet Technologies Research**
    - https://www.nist.gov/itl/antd/internet-scalable-systems-research
  - **Trustworthy Networks Program**
    - https://www.nist.gov/programs-projects/trustworthy-networks-program
  - **Communications Technology Laboratory**
    - https://www.nist.gov/ctl
  - **Information Technology Laboratory**
    - https://www.nist.gov/itl