Establishing the Technical Basis for Trustworthy Networking

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.
Establishing the Technical Basis for Trustworthy Networking

USG Transition to IPv6-Only Networks

- Completing the USG Transition to IPv6
  - “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;
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 bearer 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 IPv4 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`

NIST IPv6 Profile

USGv6 Profile

IPv6 Procurement Requirements

User / System Requirements

IPv6 Capable Product
Establishing the Technical Basis for Trustworthy Networking

USGv6 Profile – Details

Defines Capability Choices for Products

Maps Capabilities to Technical Requirements

- 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] External ICMP - support for ICMPv6 extended messages.
    - [O] PLMTPUD - support for Packetization Layer Path MTU Discovery.
    - [O] SEND - support for neighbor discovery security extensions.
    - [O] SLAAC - support for stateless global address auto-configuration.
    - [O] PrvAddr - 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 excluding prefix delegation.

- 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 Leasen.
    - [O] DHCP-Relay - support for DHCP relay capabilities.

- Security Capabilities - see section 4.8
  - [O] IPSec - support for the IP security architecture.
  - [O] TLS-3.3 - support for Transport Layer Security architecture version 1.3.

Basic Capabilities

<table>
<thead>
<tr>
<th>Flag</th>
<th>Host</th>
<th>Router</th>
<th>Other</th>
<th>Capability</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Core</td>
<td>support for IPv6 core functions.</td>
</tr>
</tbody>
</table>


RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)

RFC 8201: Path MTU Discovery for IP version 6

RFC 4861: Neighbor Discovery for IP version 6 (IPv6)

RFC 4861 Section 8 Redirect Neighbor Discovery for IP version 6 (IPv6)

RFC 6437: IPv6 Flow Label Specification

RFC 5942: IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes

RFC 6990: Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

RFC 7608: IPv6 Prefix Length Recommendation Forwarding

RFC 4191: Default Router Preferences and More-Specific Routes

RFC 4862 Section 5.3 Creation of Link Local Addresses IPv6 Stateless Address Autoconfiguration

RFC 4862 Section 5.4 Duplicate Address Detection IPv6 Stateless Address Autoconfiguration

RFC 4884: Extended ICMP to Support Multi-Part Messages

Mandates support for optional feature

Groups requirements in logical / testable sets

10/13/21

USGv6 Program - IEEE 5G World 2021

9
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
USGv6 Test Program

- USGv6 Tested Product List
  - [https://www.iol.unh.edu/registry/usgv6](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.
Establishing the Technical Basis for Trustworthy Networking

USGv6 Testing & Reporting

- 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.

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

• 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