IRS

Information Technology | **Federal IPv6 Task Force**

IPv6 Task Force
Frequently Asked Questions

June 7th, 2016

Ralph Wallace
IRS IPv6 Transition Manager
Ralph.L.Wallace@irs.gov

Agenda

- Introduction
- Background
- Purpose
- Scope Questions
- Implementation Questions
- Acquisition Questions
- Standards And Test Program Questions
- Security Questions
- General Questions
- References

Introduction

All agency infrastructures must be using IPv6 and agency networks must interface with this infrastructure, meaning the network backbone is either operating a dual stack network core or it is operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic by June 30, 2008

M-05-22 “Transition Planning for Internet Protocol Version 6 (IPv6),” August 2, 2005

Background

In September 2010, OMB issued a memorandum requiring federal agencies to operationally deploy **native** Internet Protocol Version 6 (IPv6) for public Internet servers and internal applications that communicate with public servers. This directive builds upon an August 2005 memorandum, M-05-22 titled “Transition Planning for Internet Protocol Version 6 (IPv6)”, which established the goal of deploying IPv6 in all Federal government agency network backbones by June 30, 2008

Purpose

The purpose of this Frequently Asked Questions (FAQ) is to provide United States Federal Government agency teams with practical and actionable guidance on how to successfully complete the requirements and goals contained in the September 2010 OMB IPv6 memorandum.

In accordance with the September 2010 memorandum issued by OMB, agencies are to:

- Upgrade public external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;

- 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;

- Designate an IPv6 Transition Manager to serve as the person responsible for leading the agency's IPv6 transition activities, and liaise with the wider Federal IPv6 effort as necessary; and,

- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program to control the completeness and quality of IPv6 capabilities during acquisition.

Scope

Whom does the September 2010 OMB directive apply?

The directive applies to unclassified information systems within the Federal Executive Branch Departments and Agencies and builds upon the Federal government's previous work in the area of IPv6. A copy of the September 2010 memorandum can be located at http://www.cio.gov/Documents/Transition-to-IPv6.pdf.

What is the specific scope of the FY2012 goal?

The first deployment milestone is to upgrade external Internet facing servers and services that are accessible to the general public to operationally use native IPv6. The FY2012 requirement makes sure that Federal information systems are accessible to IPv6-enabled end systems on the public Internet. The 2012 requirement will ensure that Federal information systems (and their supporting network infrastructure) keep pace with these developments and remain accessible to the emerging base of IPv6-connected users. This technical objective requires all Domain Name System (DNS), public websites and email are available on both the IPv4 and IPv6 Internets. Successful completion of the FY2012 goal means that all Federal services that are intended for the general public are available to all members of the public regardless of whether they are using IPv4, IPv6-only or dual-stack.

Scope

What is the specific scope of the FY2014 goal?

The second deployment milestone is to upgrade agency internal client applications that communicate with public Internet servers and supporting enterprise networks to support native IPv6 by the end of FY 2014. The 2014 milestone addresses how Federal client systems and their applications can natively communicate with the IPv6 Internet. The 2014 requirement will ensure that Federal client systems and their Internet applications, along with the supporting network infrastructure, will all be able to access the emerging base of IPv6-connected Internet services. Successful completion of the FY2014 goal means that all Federal client systems are able to access IPv6 enabled public services and systems.

Scope

How do you define what is a USG provided "public/externally facing server or service"?

The intent of the FY 2012 requirement is to ensure that any and all networked services that agencies provide to the general public over the Internet are seamlessly accessible via both IPv6 and IPv4. Therefore, a public/externally facing server or service are accessible external to the agency (i.e., over the Internet) and intended for use by the general public users.

Internal services (i.e., accessible only within an agency enterprise or intra-net) and external services that are only accessible to sites/users employing virtual private network (VPN) technologies, or to closed user groups (e.g., requiring an out-of-band establishment of a login account) are not in scope of the FY 2012 requirement.

What sites, domains and services are in scope for FY2012?

Typical examples of public external facing services that are within the scope of the memorandum include external web (HTTP/HTTPS), email (SMTP) and domain name system (DNS) services; but the scope extends to any and all such public services provided or contracted by an USG agency. This includes USG network services both named under the .gov top level domain (TLD), and in other TLDs, and includes services that are entirely outsourced to commercial providers.

Scope

<u>How do you define what USG “internal client applications that communicate with public Internet servers and supporting enterprise networks” for FY2014?</u>

Internal client systems (e.g. laptops, desktops, etc.) and their applications that communicate with the public Internet must be IPv6 enabled. Therefore, the all Internet capable internal client systems must be IPv6 enabled. Further, each of the applications that reside on the client systems (e.g. web browsers, email (SMTP), etc.) must be IPv6 enabled as well. Successful implementation of the FY2014 goal will ensure that all Internet capable internal client systems and their applications are capable of communicating with all IPv6 enabled public services, particularly those that are accessible via IPv4.

Implementation Questions

What does it mean to “upgrade … to operationally use native IPv6” ?

The intent of the FY 2012 requirement is to upgrade public external services to support native IPv6 transport end-to-end to IPv6-enabled clients on the public Internet. The support of this service should be transparent to the end user, meaning that it should be provided with the same service name (Uniform Resource Identifier - URI) as the existing IPv4 enabled service. That is, www.agency.gov should be IPv6 enabled, not some specially named variant of the well know service (e.g., www-v6.agency.gov).

Implementation Questions

How can progress toward these goals be tracked across all Federal networks?

OMB, in coordination with the IPv6 Task Force, has defined the official processes for agencies to report progress with respect to these policies. Additionally, there are several test and measurement tools that have proven useful in characterizing overall progress and the status of individual agencies and networks. Such tools include:

- NIST IPv6 Deployment Monitor (http://fedv6-deployment.antd.nist.gov/) - a tool that measures the status of IPv6 enabled public websites (NOTE: The NIST Deployment Monitor provides IPv6 status (web, email and DNS) for the list of secondary domains that is maintained by GSA via data.gov). Further explanation of the NIST Deployment Monitor measurements is contained within their website.
- NIST IPv6 Client Tester (https://www-x.antd.nist.gov/ipv6/usgv6-2014-targets.html) - a test site that can be used to validate clients and their applications have been successfully IPv6 enabled.
- Other Tools - Several other tools exist to test the IPv6 capabilities of websites and client systems. Some examples include:
    - http://test-ipv6.com/
    - http://netalyzr.icsi.berkeley.edu/

Implementation Questions

Must the IPv6-enabled service be provided on the same physical resources as their IPv4 equivalents?

While the service must logically appear to be dual stacked to the public, this does not require that the IPv6 enabled service must share the same physical resources as the IPv4 accessible equivalent. How agencies map (e.g., load balance) external service requests to internal physical resources is beyond the scope of this requirement.

Can the IPv6 services be provided by placing protocol translators in front of existing services?

For the servers and clients that are providing IPv6 access, it is required that the native operating systems/platforms be upgraded to directly support IPv6. In particular, providing this capability with IP protocol translators operating in conjunction with IPv4-only servers is not consistent with the intent of this requirement.

As noted above the intent of the requirements is for native, end-to-end / client-to-server support of IPv6. As such, agencies are strongly encouraged to make the in-scope services IPv6 accessible as soon as possible, using any suitable technique that is transparent to the end user and that provides a user experience (e.g., in terms of content, performance, reliability) comparable to IPv4 services. Note in particular, that agencies might use protocol translation techniques (e.g., protocol translating load balancers, etc) as an interim step to achieve intermediate milestones.

Acquisition

Is there an IPv6 Federal Acquisition Regulation (FAR)?

What are the practical implications of the FAR changes?

Is there a template that agencies should use in following the new FAR language?

How does the FAR change impact the definition of requirements?

How do the acquisition regulations relate to these goals?

No changes or updates required

Standards and Test Program

What standards are agencies required to follow?

How can an agency determine if an IT product complies with USGv6 requirements?

What is the difference between lab accreditors and test labs?

How can I learn more about the testing program?

Will the Federal government IPv6 standards profile divide the IPv6 marketplace? Hasn’t an industry-wide profile already been developed (e.g. IPv6 Ready Logo)?

How can vendors test their products against the profile?

Where can I see the list of already tested products?

No changes or updates required

Standards and Test Program

What other forms of testing might be required?

The USGv6 Testing Program will provide the basis for product conformance and interoperability testing. The goal of the testing program is to allow agencies to have reasonable assurance of the completeness, correctness and demonstrated multi-vendor interoperability of IPv6 products. While the testing program addresses a large portion of the problems space, especially for relatively new implementations, there are other forms of testing that agencies might find necessary before operational deployment.

Within the latest Roadmap document of June 2012 is a section which specifically details how an agency may establish an appropriate IPv6 test program that will be complementary with the UNH-IOL and other NIST accredited laboratories. The testing detailed below falls under the respective agency's purview to ensure what has been procured meets or exceeds the requirements specified for IPv6 capability above the basic minimum standards achieved by the NIST testing.

Performance / Scaling Testing

Systems Integration Testing

Deployment Testing

Security Questions

What is being done to address security concerns related to implementing IPv6?

How do I find out what security solutions are available for IPv6 systems?

How does the Federal government Trusted Internet Connections (TIC) effort (OMB Memorandum M-08-05) affect agencies' ability to meet the new deadlines for IPv6?

Do agency TIC Access Providers (TICAPS) support IPv6?

Does Managed Trusted Internet Protocol Services (MTIPS) support IPv6?

No changes or updates required (except grouping the security info together)

General Questions

Why has the Federal government mandated adoption of IPv6?

The exhaustion of the global IPv4 address space has stopped the growth of the IPv4 Internet use, the innovation of new services aligned with an Internet Protocol, the robustness of existing services, and the cost and complexity of network operations based upon IPv4. While many near term engineering fixes were developed to prolong the inevitable (e.g. NAT, CIDR), over the long-term the wide-scale adoption and deployment of IPv6 is necessary to maintain the business-continuity of the Internet, and enhance the effectiveness and security of our internal enterprises.

The Federal government has requested all agencies adopt IPv6 in order to:

- Maintain continuity of operations as the IPv4 Internet gradually diminishes and the IPv6 Internet continues to grow, and to reach and be reached by our customers over the Internets.
- Continue the USG initiative to move forward to an enhanced network environment, significantly increasing performance, reducing administrative costs and increasing the security posture of our enterprises.

General Questions

What is the rationale for this specific set of deployment, acquisition and management requirements?

The September 2010 OMB directive defines a set of deployment, acquisition and management requirements aimed to ensure the timely adoption of IPv6 in the Federal Government. While previous directives (e.g., OMB-05-22) required agencies to plan for the general adoption of IPv6, the 2010 directive defines new requirements meant to bring these plans into implementation with specific milestones.

In addition to IPv4 address depletion, the directives identify two specific deployment milestones (2012 and 2014) that have been identified as critical steps to (a) ensure that Federal agencies are reacting to the accelerating IPv6 roll out through-out the Internet; (b) demonstrate that Federal IPv6 planning and acquisition processes can be put into action; and, (c) to establish a base-line of Federal IPv6 capability that should become a “tipping point” for fostering agency-directed broad IPv6 use in scopes beyond those of the directive.

General Questions

What is the broader intent of these requirements?

The broad adoption of IPv6 in Federal information systems, with the ultimate goal of removing IPv4 when considered reasonable and prudent. From this point forward, IPv6 technologies should be addressed in all system design, acquisition, and deployment plans. The requirement to designate IPv6 Transition Managers to lead and report on agency's plans and process and the establishment of the Federal IPv6 Task Force is meant to provide the sustaining coordination necessary to efficiently achieve the ultimate goal.

What is the role of the Federal IPv6 Task Force?

The Federal IPv6 Task Force was established by the Federal CIO Council as part of the Architecture and Infrastructure Committee (AIC). The role of the Task Force is to assist and coordinate agency activities in response to OMB's IPv6 policies. The Task Force's extensive technical and policy experience with IPv6 enables continuity of knowledge to help integrate USG IPv6 activities with the worldwide Internet community.

General Questions

What is expected of Agency IPv6 Transition Managers?

Agency Transition Managers represent their agency IPv6 efforts to OMB and other federal agencies. Moreover, the Transition Manager should be capable of communicating across the technical and executive perspectives necessary to manage a successful adoption.

Transition Managers should educate themselves on the importance of IPv6 to A Strategy For American Innovation (National Economic Council and Office of Science and Technology Policy; October 2015) and so the global Internet community. In addition, Transition Managers are expected to build the necessary organizational structures within their respective organizations to champion and manage a successful adoption of IPv6 enabled services. Finally, Transition Managers are encouraged to communicate the impact of IPv6 efforts within agency architectures to the Federal IPv6 Task Force and OMB.

The group of agency appointed Transition Managers can be contacted through the email list fedv6-deploy@nist.gov ***once you have subscribed to the list.***

General Questions

What guidance available to Federal agencies?

Transition Planning: The original guidance provided under the August 2005 memorandum, M-05-22 titled “Transition Planning for Internet Protocol Version 6 (IPv6)” provides the essential transition planning outline and action elements required to effectively conduct a transition.

Overarching Guidance: The Strategy and Planning Committee of the Federal Chief Information Officers Council has published the revised “Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government” (AKA “The Roadmap”), version 2.0, dated June 2012, which is available at http://www.cio.gov. Search on IPv6. The original and revised Roadmaps were created through collaboration between public and private partnerships and the latest revision is intended to aid Federal IPv6 deployment and management efforts. The Roadmap outlines a vision for network modernization and provides specific guidance for agencies on how to integrate this effort within each agency’s IT management environment. The “Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government” should be the basis of an agency’s IPv6 efforts and help provide a strong foundation to energize and guide agencies to transition to and ultimately adopt IPv6.

Additional Support: The Federal IPv6 Task Force will also regularly distribute guidance materials to the IPv6 Interagency Working Group members, and facilitate IPv6 implementation discussions at its meetings.

General Questions

Where can Federal government personnel working on the IPv6 effort go to share information?

In addition to attending the IPv6 Interagency Working Group meetings and other government sponsored sessions, agency staff can share information via the IPv6 wiki page at https://max.omb.gov/community/x/EhPVI.

For access to the collaborative area on the MAX Federal Community for the Federal IPv6 Interagency Working Group, Federal employees or contractors of Federal agencies must have a MAX user-id, which can be requested at the main MAX Portal: https://max.omb.gov/maxportal/

The IPv6 wiki page is visible on the E-Gov Community home page, where it’s listed by its title: “Federal Pv6 Interagency Working Group.”

In addition to the wiki, an email distribution list has been established for all Transition Managers: fedv6-deploy@nist.gov. Transition Managers should feel free to use that list to discuss issues that may be of interest to other Transition Managers and support staff.

General Questions

How can those outside of the Federal government (e.g. private industry, academia, state/local government) contribute to the IPv6 effort?

Open dialogue and information sharing between the Federal government and those in private industry, academia, etc. is encouraged and necessary in order to facilitate the successful adoption of IPv6. Clearly, the Federal IPv6 deployment initiative will require the direct involvement and close collaboration with Internet equipment and service vendors. Individuals and organizations outside of the Federal government are encouraged to contact the IPv6 Task Force to determine how their input can be appropriately leveraged.

A formal industry IPv6 working group has been established by the American Council for Technology, Industry Advisory Council (ACT-IAC). For more information please contact ACT representative, Ralph Wallace, at ralph.l.wallace@irs.gov, and IAC representative John Lee, at johnl@infoblox.com .

References

Document Name	Originator/Version/Date
Federal Government Adoption of Internet Protocol Version 6 (IPv6) - Frequently Asked Questions (FAQs)	Federal IPv6 Task Force; June 7, 2016
Guidelines for the Secure Deployment of IPv6	NIST SP 800-119; December 2010
Transition to IPv6	OMB; September 28, 2010
FAR Clauses	Federal Acquisition Regulation (FAR); December 10, 2009
USGv6 Test Methods: General Description and Validation	NIST SP 500-273; November 30, 2009 (Original; updated versions available on-line)
Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government	Federal CIO Council; Version 1.0; May 2009, Version 2.0; July 2012
A Profile for IPv6 in the U.S. Government	NIST SP 500-267; Ver 1.0; July 2008 (Original; updated versions available on-line)
IPv6 Transition Guidance	Federal CIO Council Architecture and Infrastructure Committee; February 2006
Transition Planning for Internet Protocol Version 6 (IPv6)	OMB; M-05-22; August 2, 2005
Demonstration Plan to Support Agency IPv6 Compliance	Federal CIO Council Architecture and Infrastructure Committee; January 2008
The DoD IPv6 Standard Profiles for IPv6 Capable Devices	DoD, Version 6.0, July 2011

Questions?

IRS

Federal IPv6 Task Force
Outreach Subgroup
And
ACT-IAC team