IPv6

Essential Background, Business Value and Best Practices for Implementation

Lori Sheppard

Senior Systems Engineer

May 2012

I. Executive Summary

The entire Internet protocol version four (IPv4) address space provides approximately 4.3 billion unique IP addresses. With a current world population of more than 7 billion, that is not enough for even one IP address per person. Since individuals today use multiple methods, such as mobile phones, iPads and laptops, to access Internet content, the number of unique IP addresses required per person has increased significantly. Even more compelling, however, is the proliferation of IP addresses for ubiquitous use in mobile devices, household appliances, automobiles and sensors. Internet protocol version six (IPv6) is the next-generation protocol, designed to support the continued exponential growth in user devices, services and applications that require unique IP addresses to communicate on the Internet.

This white paper is intended to help readers avoid common misconceptions associated with IPv6, identify key areas that require up front monetary investment and determine key concepts that should be captured in an enterprise-wide strategic plan. Lastly, as one of the first to deploy an enterprise Internet protocol address management solution in the defense and intelligence communities, NJVC shares benefits realized from the successful deployment and provides recommendations to maximize the IPAM return on investment (ROI).

II. Document Structure

The structure of this document is as follows:

- Brief background of IPv6
- Common issues, misconceptions and obstacles to IPv6 adoption and implementation
- Crucial investments required for successful IPv6 deployment
- Best practices to prepare for enterprise IPv6 integration
- Benefits realized from a successfully planned and implemented IPAM solution

III. The Shift to IPv6

Today, the most common version of the Internet protocol is IPv4. This version has been in use for more than three decades, and is the standard by which devices on a network, such as the Internet, communicate with each other. The Internet Engineering Task Force published the first IPv4 Request for Comment 791 in September 1981. RFC 791 and hundreds of subsequent IPv4-related specifications have been used by a multitude of Internet experts for technical direction on how to implement the wide variety of options available within the IPv4 protocol suite successfully and securely.

Realizing that the 4.3 billion available IPv4 addresses would eventually be depleted, networking experts began planning well in advance for its successor, IPv6. The first specification for this next-generation protocol, IETF RFC 1883, was published in December 1995. Even though IPv6 has not been widely deployed to date, the case for integrating IPv6 into the enterprise is a solid one. For example, without IPv6, continued growth of wireless sensor networks to satisfy vital healthcare and emergency response needs would not be possible. IPv6 is a must for organizations to be competitive in the Internet business of the future, and remain at the forefront of enterprise-related technological advances.

IPv6 is a must for organizations to be competitive in the Internet business of the future, and remain at the forefront of enterprise-related technological advances.

The case for enterprise IPv6 integration became much stronger on Feb. 3, 2011: the day the Internet Assigned Numbers Authority allocated the last of its pool of free IPv4 address blocks[1]. While IPv4 address pool depletion had been predicted many years prior, the event marked a significant milestone in Internet history, and provided a reality check that reignited momentum for a global shift toward IPv6. The continued steady decline of IPv4 address availability reinforces the fact that a global-scale IPv6 adoption must occur to propel continued innovation and the future expansion of Internet services and applications.

IV. Federal Government Response

To ensure the federal government was positioned to support IPv6, the Office of Management and Budget (OMB) issued memorandum M-05-22 to chief information officers in August 2005. The memo directed "all agency infrastructures (network backbones) must be using IPv6"[2] by 30 June 2008." Federal organizations followed a plan developed by the Federal CIO Council Architecture and Infrastructure Committee to demonstrate IPv6 compliance of their network backbones. This demonstration plan[3], dated Jan. 28, 2008, identified three objectives that had to be achieved to claim success:

1. Transmit IPv6 traffic from the Internet and external peers through the network backbone (core) to the local area network (LAN).
2. Transmit IPv6 traffic from the LAN through the network backbone (core) out to the Internet and external peers.
3. Transmit IPv6 traffic from the LAN through the network backbone (core) to another LAN (or another node on the same LAN).

[1]Free Pool of IPv4 Address Space Depleted. (2012, 3 February). Retrieved April 03, 2012, from http://www.nro.net/news/ipv4-free-pool-depleted
[2]Executive Office of the President Office of Management and Budget. (2005, August 02). Transition Planning for Internet Protocol Version 6 (IPv6). Washington, DC: Karen S. Evans.
[3] Federal CIO Council (2008, January 28). Demonstration Plan to Support Agency IPv6 Compliance version 1.0. Federal CIO Council Architecture and Infrastructure Committee.

Figure 1, extracted from the Federal CIO Council's Demonstration Plan, shows one logical network configuration option to accomplish these objectives.

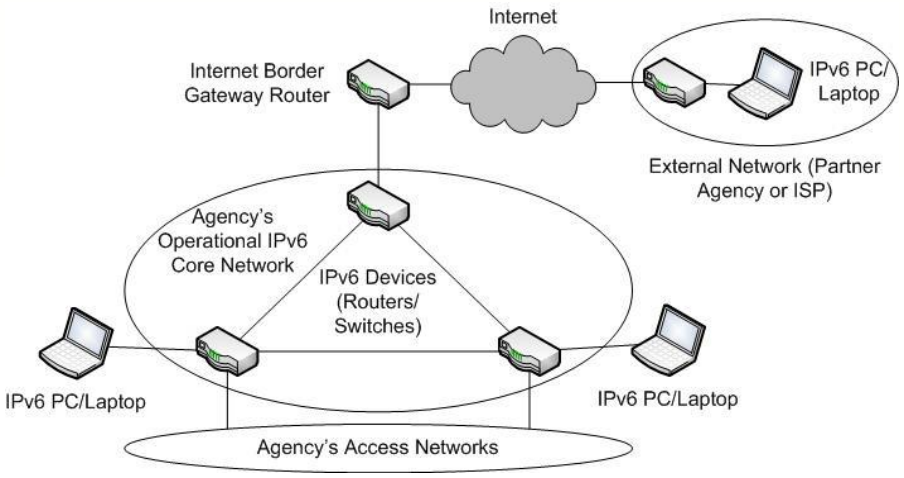

Figure 1: Sample Configuration of IPv6 PCs/Laptops Directly Connected to Agency Backbone

In September 2010, the OMB released a second memorandum to build upon the 2008 foundation of an IPv6-capable network core.The second memo directed operational IPv6 deployment within the Department of Defense (DoD) and the Intelligence Community by the end of fiscal year (FY) 2012. The two technical directives specified in the 2010 memo were:

1. Upgrade public/external facing servers and services (e.g., web, email, domain name system or DNS, Internet service provider services) to operationally use native IPv6 by the end of FY 2012.
2. 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.[4]

These activities are critical steps for the government as IPv6 deployment begins to increase in the global operational enterprise. The latest guidance, released by the Assistant Secretary of Defense in March 2011[5], provides additional direction for implementation of the OMB IPv6 FY12 and FY14 directives.

[4]Executive Office of the President Office of Management and Budget. (2010, September 28). Transition to IPv6. Washington, DC: VivekKundra.
[5] Assistant Secretary of Defense Networks and Information Integration (ASD NII). (2011, March 07). Guidance and Policy for Implementation of Office of Management and Budget (OMB) Internet Protocol Version 6 (IPv6) Fiscal Years (FYs) 2012 and 2014 Requirements. Washington, DC: Teresa M. Takai.

V. Two Common Misconceptions Regarding IPv6 Deployment

A few widespread IPv6 challenges are vendor product availability and support, prioritization of the IPv6 initiative compared to other enterprise requirements and security-related issues. However, the most common inhibitor to integrating IPv6 into the enterprise is funding availability. Two common IPv6 misconceptions related to funding are discussed below.

1. Enterprise experts are already familiar with IPv4, so on-the-job training is sufficient to understand and implement IPv6.

A common misconception is that because enterprise experts, such as network engineers and system administrators, are already familiar with IPv4, IPv6 should be learned fairly easily through outside reading and on-the-job training. However, with more than 180 IPv6 RFCs that describe how to implement different capabilities within the IPv6 protocol suite, the complexity of the protocol goes well beyond the sheer size of the IP address (128bits) and changes to the packet header. Of greater concern are the implications the address size has on the establishment of a new IP schema, changes to the way IPv6 address blocks are managed and the transparent integration of enterprise IPv6 services.

Enterprise IPv6 experts are invaluable assets who require an upfront training investment to maximize their effectiveness and minimize the risk of an enterprise outage or malicious exploitation of known vulnerabilities during solution deployment. Training requirements include, but should not be limited to, an overview of the IPv6 protocol suite and its capabilities and vulnerabilities, followed by hands-on training tailored to each enterprise functional area.

Enterprise IPv6 experts are invaluable assets who require an upfront training investment to maximize their effectiveness and minimize the risk of an enterprise outage or malicious exploitation of known vulnerabilities.

2. Enterprise stakeholders are trained, and the hardware is IPv6 capable, so the next step is deployment, not planning.

A second mistaken belief is that once enterprise stakeholders have participated in IPv6 training, and a network inventory confirms that hardware is IPv6 capable, the next step is to operationally deploy IPv6. Training and upgrading equipment are crucial steps, but when viewed individually, they are simply two pieces of a much bigger picture—the enterprise strategic plan—that need to be funded, developed, disseminated and executed using a phased approach. Enterprise stakeholder expertise is the foundation upon which an effective and realistic IPv6 strategic plan and schedule are built.

Enterprise stakeholder expertise is the foundation upon which an effective and realistic IPv6 strategic plan and schedule are built.

VI. Best Practices for IPv6 Implementation

There is a multitude of recommended best practices for IPv6 integration. Rather than provide an exhaustive list, we will touch on two best practices that proved vital to NJVC successful IPv6 installations: strategic planning and testing.

1. Strategic Planning

With a group of functional experts prepared to enable IPv6 in the enterprise, it is tempting to jump right into implementation. Without a meticulous implementation plan, chances are that all of the hard work invested will fail to achieve the desired end state. Time must be set aside at the forefront to perform a thorough requirements analysis and use stakeholder expertise to build a realistic implementation plan and schedule.

The strategic plan should contain, at a minimum, six core elements:

- **Background.** Explain the purpose of the project, the known drivers and the objectives. Stakeholders must have a common understanding of the requirements and a clear vision of the planned outcome.
- **Stakeholder Identification.** Specify roles and responsibilities for completing the project objective(s), and align those roles and responsibilities with enterprise subject matter experts.
- **AS IS Architecture.** Develop logical and physical network diagrams that depict the impacted areas of the enterprise (e.g., external-facing servers and services).
- **TO BE Architecture.** Create logical and physical network diagrams that illustrate the enterprise architecture upon completion of the objective(s).
- **Plan of Action and Milestones (POA&M).** Detail the steps required to move from the AS IS architecture to the TO BE architecture.
- **Schedule.** Establish dates for each of the milestones specified in the POA&M.

Keep the strategic plan current and relevant by continually evaluating it against new enterprise initiatives, incorporating lessons learned and making necessary plan modifications to align with the organizational strategic vision and mission.

2. Testing

The AS IS and TO BE network diagrams form the blueprint for constructing a valuable test environment that provides the capability to perform end-to-end IPv6 testing. The test environment should be built to mirror the AS IS infrastructure as closely as possible, and incorporate any new hardware and software required to achieve the TO BE architecture. A test environment that closely mirrors the operational environment enables the development of more accurate IPv6 configurations, and decreases the risk of unforeseen configuration issues when IPv6 is deployed in the operational environment. An added benefit is that laboratory hardware becomes, in essence, cold spares that can be quickly moved into operation should a hardware failure occur.

Three protocol-specific tests should be included for each test case:

- IPv6 only
- IPv4 only
- IPv4/IPv6 (dual stack)

Testing the protocols independently and simultaneously facilitates the identification of specific functional, performance and interoperability issues that might otherwise never be discovered.

VII. The Case for IPAM

IPv6 offers the opportunity for a fresh start—providing new, contiguous IP address blocks and an opportunity to redesign existing IP address and management plans. For the majority of organizations, IPAM is accomplished using spreadsheets or homegrown databases to allocate and manage addresses from assigned IPv4 address blocks. Such manual methods of IP address management are adequate for IPv4, but will no longer be feasible with IPv6.

The magnitude of IPv6 address blocks requires the use of automated methods, such as an IPAM solution, for subdividing, assigning, managing and reporting usage of IP space. In addition, an enterprise IPAM solution promotes the centralization of IP and other closely-related enterprise functions, such as DNS and dynamic host configuration protocol. Four benefits that administrators observed after successful IPAM deployment are outlined below.

1. Centralization of Roles and Responsibilities

One benefit that was immediately apparent to IP and DNS administrators was a centralization of roles and responsibilities. IPAM allowed central control of DNS servers, alleviating the need for network DNS servers to be controlled by different groups of administrators. Central control of enterprise DNS servers changed the way enterprise DNS was managed, and fostered the development of a single, more agile enterprise DNS team postured to support all networks.

2. Faster Parsing of Subnets

The IP team reported much faster parsing of subnets. In one case, manually parsing a single /24 network into 64/30 subnets took an administrator between one and two minutes per subnet, or approximately two hours of work. After IPAM deployment, three /24 networks could each be parsed into 64/30 subnets, resulting in a total of 192 subnets parsed in less than three minutes! The team can now manage and assign more addresses and capture more metadata, such as site, segment and virtual LAN name in a shorter period of time with no increase in manpower.

3. Enforcement of Enterprise Naming Policies

The ability to capture metadata allowed the enforcement of a standard enterprise naming policy. This function was critical to ensuring that devices were named appropriately, and relevant comments could be added for DNS transactions and IP tracking.

4. Automatic Implementation of Security Technical Implementation Guides (STIGs)

When supporting the DoD, one valuable feature identified in some IPAM solutions was the automatic implementation of Defense Information Systems Agency STIGs, a "methodology for standardized, secure installation and maintenance of computer software and hardware."[6] While it may not apply to all organizations, the time-saving benefits this feature provides for DoD installations were worth noting.

Other Benefits Reported

When IPAM solutions were successfully planned and deployed, functional experts noted many other automated improvements, such as local and offsite daily backups, geographic redundancy, system health monitoring and full auditing of user activities.

IPAM Administrator Recommendations

To maximize the ROI of an enterprise IPAM solution, there must be continual coordination and communication between the IP and DNS administrators and other internal enterprise functional experts, as well as externally with the IPAM vendor toprovide the latest software releases and support. The top three IPAM administrator recommendations are:

1. **Invest in user training.** An IPAM solution is only as good as the data that go into it and the capability of the administrators managing it.
2. **If available, request technical/engineering support.** Vendors can assist with identified issues and concerns, and answer questions that arise during installation and maintenance.
3. **Procure cold spares.** Spares can be used in a laboratory environment to test preplanned product improvements and moved to the operational network should an emergency occur.

[6]Security Technical Implementation Guide. Retrieved April 03, 2012, from http://en.wikipedia.org/wiki/Security_Technical_Implementation_Guide

VI. Conclusion

The proliferation of IP addresses for individuals and commonplace objects and thesteadily declining number of available IPv4 addresses are some of the reasons driving IPv6 adoption on a global scale. Both federal and commercial organizations must strategically plan to integrate IPv6 into their enterprises to foster continued innovation and future expansion of Internet services and solutions.

The underlying business value in moving to IPv6 for organizations is the continuity in reaching customers, upkeep of the competitive position and fortification of the corporate image. To prepare for the future, organizations must invest time and funding up front to support functional training and development of an IPv6 strategic plan. The plan must be based on enterprise stakeholder expertise, and include an agreed-upon end state, realistic milestones and associated timelines for completion.

To facilitate achievement of the desired end state, establishment of an IPv6 test environment is highly encouraged. The infrastructure in the test environment should be as close as possible to the operational environment, and incorporate separate tests for IPv4 only, IPv6 only and dual stack configurations for each test case.

The case study highlighted a few of the valuable IPAM features and the resulting improvements in enterprise IP and DNS functionality experienced by NJVC administrators. Two benefits included development of a single, more agile enterprise DNS team and an IP team that can accomplish more work in less time with existing resources.

About the Author

Lori Sheppard is an NJVC Senior Systems Engineer specializing in the management, engineering and integration of IT solutions for the intelligence and defense communities. She has served as an IPv6 Transition Manager for more than five years and brings that practical knowledge, experience and lessons learned to the IPv6 arena. Ms. Sheppard can be contacted at lori.sheppard@njvc.com.

About NJVC®

With a focus on information technology automation, NJVC® specializes in supporting highly secure, complex IT enterprises in business-critical environments. We offer a wide breadth of IT solutions to our customers, ranging from strategic consulting to flexible managed services in five business areas: Cloud Services, Cyber Security, Data Center Services, IT Services and Print Solutions. Our global workforce includes dedicated and talented employees, with 94 percent holding security clearances, located at more than 160 customer sites. We partner with our customers to support their missions. To learn more, visit www.njvc.com.

About NJVC IPv6 Expertise

NJVC has played an active role in the federal IPv6 arena for more than five years. We have worked alongside many organizations, both government and commercial, and had the opportunity to identify and solve IPv6 deployment challenges. The experience and knowledge gained during these deployments formed a cohesive team of talented engineers whose IPv6 expertise spans the enterprise from networks to applications.

The NJVC IPv6 team brings a proven systems engineering methodology that can be tailored to meet specific client needs, such as the FY12 IPv6 OMB mandate. This phased approach includes the development of a customized IPv6 implementation plan, work breakdown structure and schedule. NJVC offers large-scale Internet solution provider IPv6 expertise with the agility and flexibility of a smaller firm. Our IPv6 solution offerings range from enterprise assessments to solution engineering and implementation.

NJVC
8614 Westwood Center Dr
Suite 300
Vienna, VA 22182
703.556.0110

www.njvc.com