Social Security

Information Resources Management Strategic Plan

Fiscal Year 2007

www.socialsecurity.gov

Table of Contents

Transition to Internet Protocol Version 6 (IPv6)

Background

All Federal government agencies have been directed by the Office of Management and Budget to make their network backbones Internet Protocol Version 6-enabled (operational) by June 30, 2008. The Internet Protocol (IP) is the logical mechanism for sending data from one computer to another across the Internet. Most networks combine IP with the higher-level Transmission Control Protocol (TCP), which establishes a virtual connection between source and destination. The current standard for IP is version 4 (IPv4) which was developed in the 1970s. It has proven remarkably robust, and interoperable with a wide range of protocols and applications. However, the explosive growth of the Internet and Internet-based services has exposed deficiencies in IPv4. Perhaps the most urgent of these is the depletion of available IPv4 address space which has long been anticipated by the Internet Engineering Task Force (IETF). The IETF began developing a successor to IPv4 in the early 1990s. A proposed standard was first submitted in 1994, and the core set of IPv6 protocols became a standard in August, 1998 with the publication of RFC 2460 – Internet Protocol Version 6 (IPv6) Specification.

IPv6, with its 128-bit address space, was designed to support continued Internet growth, both in terms of the number of users and available functionality. It is expected to overcome other IPv4 limitations through features such as end-to-end IP Security (IPSec) support, mobile communications, Quality of Service (QoS), and other features that are designed to ease system and network management burdens.

The main advances from IPv4 to IPv6 are:

- Expanded addressing capability,
- Simplification and standardization of the packet header format,
- Auto-configuration mechanisms that allow for plug-and-play capability,
- Improved support for extensions and options,
- Security extensions for authentication and privacy; and
- Flow labeling capability.

Additionally, IPv6 includes transition and interoperability mechanisms that allow users to deploy IPv6 incrementally.

IPv6 at the Social Security Administration

Over the course of several years, SSA has evolved its network architecture, its business processes and its organizational structures in ways that position it well to integrate IPv6. SSA delivers services, conducts business operations, and executes data exchanges with its partners over a shared IT environment. The Agency's private network (SSANet) has been migrated to a flat (i.e., non-hierarchical), Multi-Protocol Label Switching (MPLS) architecture that supports direct point-to-point communications and effective Quality of Service (QoS) and Class of Service (CoS) traffic management. SSA's organizational components and lines of business do not operate in discrete silos but rather share centrally managed IT platforms, networks, and application support services.

Most of the features and functionality that are built into IPv6 have been provided as extensions or enhancements to SSA's IPv4-based networks. However, it is recognized that IPv6 offers a number of key design improvements that may provide long-term strategic benefit to the Agency, including:

- Improved efficiency in routing and packet handling,
- Support for auto-configuration and plug-and-play capabilities,
- Support for embedded IP Security,
- Elimination of the need for Network Address Translation (NAT),
- Support for widely deployed routing protocols, and
- Network efficiency and bandwidth conservation.

SSA has long recognized that IPv6 was the emerging standard for IP. Through participation in the North American IPv6 Task Force (Nav6TF) and the MoonV6 project, SSA determined that it would be best to incorporate IPv6 into SSANet as part of the Agency's ongoing technology refresh cycles. SSA also determined that IPv6 integration should be accomplished in defined phases, beginning with the network core and, through technology refreshment, extend to the Extranet, and then throughout the rest of the network infrastructure.

The transition to IPv6 will affect a broad spectrum of SSA's IT and network infrastructure, including network routers, switches and other network infrastructure components, but also network services such as Domain Name Servers, network security and information assurance devices (e.g., firewalls). It will affect operating systems, directory services administration, and many applications and related IT services. However, the introduction of IPv6 capability will not significantly change the basic architecture of SSA's existing network (SSANet). Integrating IPv6 functionality and capability while continuing to support the Agency's legacy IPv4 infrastructure (including IPv4-based applications) will be a significant challenge.

IPv6 Transition Plan

Deployment of IPv6 capable devices on the network will be undertaken not to provide for immediate, enterprise-wide use of IPv6, but rather to prepare the existing network infrastructures to support IPv6-capable nodes. Even if IPv6 is not being used, dual protocol nodes will exist, allowing network managers and engineers to transition to IPv6 traffic when required.

SSA has evaluated several transition mechanisms and found that deployment of a dual-stack IPv4/IPv6 network architecture represents several distinct advantages that cannot clearly be demonstrated by other transition mechanisms. A dual-stack network architecture is one in which network hosts, e.g., routers, switches, etc., support separate and distinct layers—one for IPv4 traffic and another for IPv6 traffic. The advantages of a dual stack architecture include:

- There is no additional overhead to manage tunnels or translation boxes,
- The ability to manage IPv6 and IPv4 traffic consistently,
- The ability to protect against potential security vulnerabilities associated with other transition mechanisms (especially tunneling, and tunnel broker mechanisms), and
- The ability to support the public, business partners, and other Government agencies utilizing either native IPv4 or native IPv6 according to their individual needs and requirements.

Establishing and maintaining a dual IP stack IPv4/IPv6 network architecture presents some technical challenges that do not override the substantial advantages of the dual-stack network architecture.

SSA's IPv6 transition strategy will integrate IPv6 capability with the Agency's existing IPv4-based networks in a structured and staged manner. Utilizing SSA's existing technology refresh plans, IPv4-based routers and switches (and their associated subnets) will be made dual-stack capable; i.e., able to support either IPv4 or IPv6 communications. Alternate transition mechanisms will not be deployed. SSA has no plans to establish a pure or "native" IPv6 network for the foreseeable future, but will establish and maintain a dual-stack IPv4/IPv6 capability throughout its network system.