

# A Guide For Federal Agencies Transitioning To IPv6

## *Executive Summary*

IPv6 is the Next Generation in IP communications technology that will drive converged voice, video and data solutions globally. In this report, discover Best Practices for transitioning to IPv6 that:

- Leverage experiences from organizations across the world that have transitioned to IPv6 and are using it today
- Are tailored to meet the specific needs of Federal agencies
- Cover the entire transition process from architecture and planning to implementation and deployment

Over the past three decades, the development and use of packet networks based on the Internet Protocol (IP) has spawned one of the greatest revolutions in communications the world has ever seen in the advent of the Internet. It is now possible to share information with anyone, anywhere in the world almost instantly.

The benefits of IP are so great, a preponderance of organizations are moving towards Convergence, also called Everything over IP (EoIP), where all voice, video and data communication would occur over IP-based networks.

Unfortunately, the existing protocols supporting the Internet, IPv4, was not designed to handle the unpredictable and overwhelming growth that has occurred with the Internet or many of the advanced capabilities required to support EoIP. Many advances have been made with IPv4 to provide the scalability needed over the past decade to keep up with growth on the Internet; however, the trade-off has been significant with the erosion of ubiquity, loss of end-to-end connectivity and substantial increase in complexity.

The problems surrounding IPv4 were recognized and in the mid-1990's the Internet Engineering Task Force (IETF), an international body which develops the majority of standards associated with the Internet, agreed upon IPv6 as the basis for the next generation or New Internet. IPv6 not only provided a solution to the limited address space within IPv4, it also provided many advanced capabilities for functionality such as Quality of Service (QoS), security, mobility, auto-configuration and extension headers. IPv6 was designed to provide greater performance with a much simpler overall configuration. IPv6 could not provide the advances that were necessary and remain directly interoperable with IPv4; therefore, transitioning to IPv6 must be accomplished through a careful planning process to prevent operational impacts during periods where IPv4 and IPv6 coexist on a network.

The transition to IPv6 is not just associated with one application or a specific network element; it is a complete technology transition that will impact every Information Technology (IT) based system within the Federal Enterprise Architecture (FEA). Every piece of hardware and any application that utilizes the network today or in the future will need to be included in the transition planning activities. IPv6 will provide the foundation necessary to deliver advanced network centric services and solutions for a wide variety of applications and provide the necessary infrastructure to support EoIP.

The Office of the Secretary of Defense (OSD) and the Office of Management and Budget (OMB) should be commended for taking the first steps necessary to begin the transition of the United States (US) government to IPv6, which will most likely span over ten years. Without the focus of a proactive and well managed transition, the US will continue to follow Asia and Europe in transitioning to the IPv6 and the New Internet and not reap the level of benefits that we have enjoyed from being the world leader in Internet technology and services today.

The purpose of this report is to provide a comprehensive set of best practices to support Federal agencies in their IPv6 transition planning efforts. In order to achieve that goal, a multi-phase approach was used to collect IPv6 transition experiences, lessons learned and recommended approaches from a variety of sources with an emphasis on organizations that have successfully transitioned to IPv6. The methods for collecting information included:

1. Interviews
2. Surveys and request for information
3. Review of transition documents, reports and analysis
4. Review of presentations and other publicly available documents and articles

When possible, multiple sources of information were used from each organization to develop a complete picture of their transition experiences to IPv6. The information contained in this report came from numerous sources and organizations including government agencies, research and development networks and private industry. They include:

- 6bone
- 6net
- Air Force IPv6 Transition Management Office
- American Registry for Internet Numbers (ARIN)
- Army IPv6 Core Team
- China Education and Research Network 2 (CERNET2)
- Defense Research and Engineering Network (DREN)
- Department of Commerce, National Telecommunications and Information Association (NTIA)
- DoD IPv6 Transition Office
- Global Crossing
- Government Accountability Office (GAO)
- Internet2
- IPv6 Promotion Council of Japan
- Juniper Networks
- Korea Research Environment Open NETwork-2 (KREONET2)
- MCI
- Microsoft Corporation
- Navy IPv6 Transition Office
- Nippon Telephone and Telegraph (NTT) Communications
- North Atlantic Treaty Organization (NATO)
- Office of Management and Budget (OMB)
- Sprint



"We have found that the toughest part of evolving to IPv6 is managing the transition. An agency's transition to IPv6 will be complex and require coordinating a wide range of political, programmatic and technical activities throughout the process."

– Dale Geesey, Vice President of Consulting, v6 Transition

The processes and best practices described in this report are the results of intensive analysis from researching a variety of IPv6 transitional approaches and interviewing organizations across the world that are recognized leaders in IPv6. This information is then synthesized into a format targeted specifically for Federal Chief Information Officers (CIOs) and their staff to provide the maximum value on supporting their transition planning efforts. Although the enterprise architecture of governmental organizations has become much closer to those of private industry through the wide spread use of commercial-off-the-shelf (COTS) products and services, Federal agencies must keep in mind unique characteristics such as:

- Federal IT law including the Clinger-Cohen Act
- Federal Enterprise Architecture
- Federal budget process
- “Operations focus” rather than “research focus”

OMB and the DoD have both set aggressive, but needed, schedules for the transition to IPv6. Without a centralized approach to transition, the Federal agencies and components within the DoD would probably transition to IPv6 on their own timeframes with varying approaches which could lead to considerable interoperability issues and significantly increase the overall cost of transition.

It is important to note that the transition guidance and activities provided to the Federal agencies and DoD to date are just the first steps in the overall IPv6 transition planning process. As transition planning occurs, each of the agencies must develop and implement an overall vision of how IPv6 will be employed in their architectures and the evolution in the way the agency does business.

## To learn more:

This Executive Summary provides an overview of the “Guide for Federal Agencies Transitioning to IPv6”. To request the complete version, please go to [www.juniper.net/federal/IPv6](http://www.juniper.net/federal/IPv6).

The “Guide for Federal Agencies Transitioning to IPv6” is the first installment in the “IPv6 Best Practices World Report” series. The second installment in this new series will be published in early 2006.

Written by IPv6 Summit, Inc. in collaboration with Juniper Networks, Inc.

© IPv6 Summit, Inc. 2005. All Rights Reserved. Reproduction in whole or in part of any content of this report in any form or medium without express written permission of the IPv6 Summit, Inc. or Juniper Networks, Inc. is prohibited.