Juniper NETWORKS®

The IPv6 Best Practices World Report Series

January 2006

Guide for Federal Agencies Transitioning to IPv6

IPv6 SUMMIT INC.

Table of Contents

Table of Figures

1 Introduction

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 since 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 protocol supporting the Internet, IP version 4 (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 significant increase in complexity.

The problems surrounding IPv4 were recognized early on 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 IP version 6 (IPv6) as the basis for the next generation Internet. IPv6 not only provided a solution to the limited address space within IPv4, but 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 without transition mechanisms; 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.

1.1 Overview

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) as shown in Figure 1. 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.

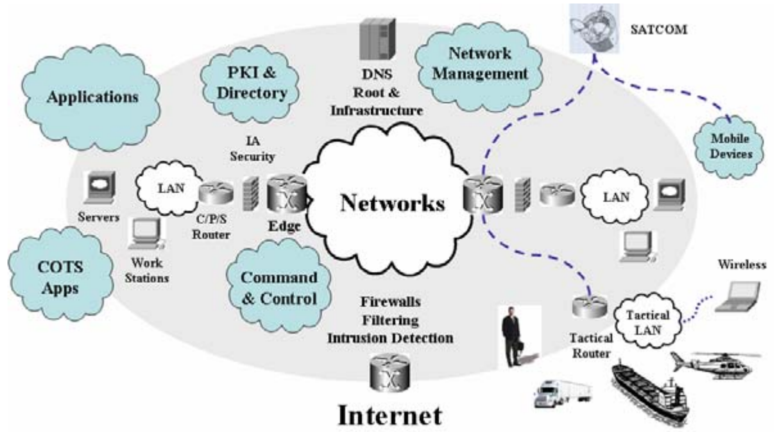


Figure 1: IPv6 Will Touch Everything[1]

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 U.S. government to IPv6. The entire transition process will most likely span over ten years and could leave the United States behind the rest of the world if an active transition is not established and managed proactively.

1.2 Scope

This report provides an understanding of industry-based best practices as they relate to the transition of a Federal agency’s enterprise to IPv6; however, the solutions addressed in this document should be considered as addressing more than the transition to IPv6. These guidelines address the integration of any new technology or set of technologies and the foundations addressed here, including governance and technological elements, should be considered for a place of permanence in the organization. The insertion of IPv6 will occur over many years and require the transition of other enabling technologies, which will require the same processes.

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”

[1] Federal CIO IPv6 Transition Planning Workshop 11 October 2005, Presented by Dr. Charles Lynch

OMB and the Department of Defense (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 likely transition to IPv6 on their own timeframes with varying approaches, which could lead to considerable interoperability issues and could significantly increase the overall cost of transition. Figure 2 shows a summary of the transitional planning activities required by OMB and the major milestones developed by the DoD.

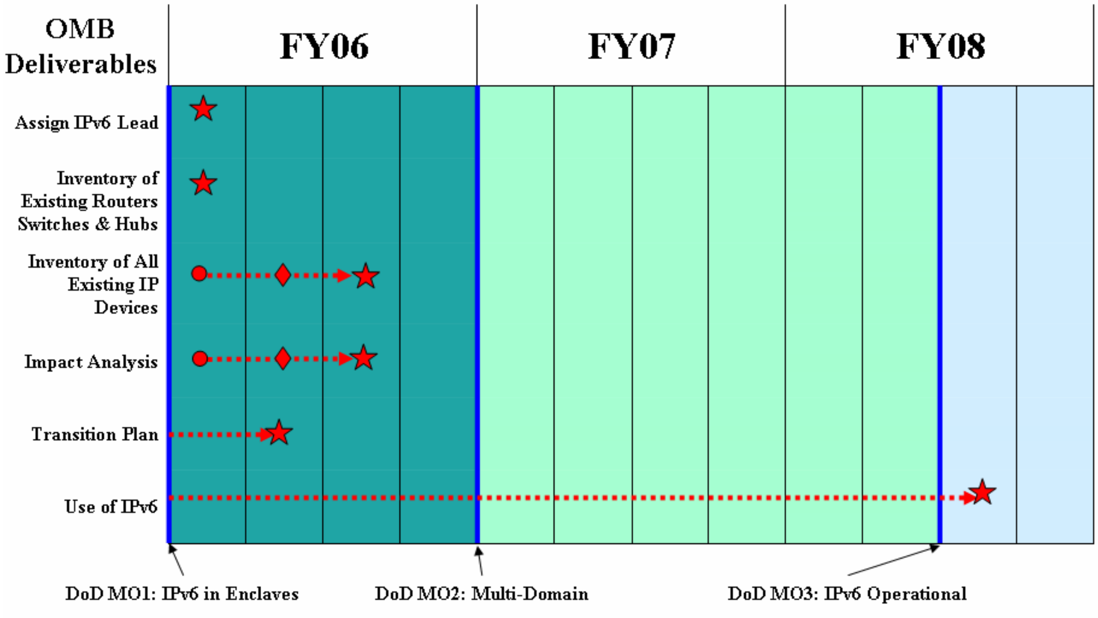


Figure 2: Federal IPv6 Transition Planning Deliverables and DoD Milestones

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 agency must develop and implement an overall vision of how IPv6 will be employed in their architectures and how the way the agency does business will evolve.

1.3 Approach

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-phased 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 requests 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 included:

- 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)
- OMB
- Sprint

The information gathered was reviewed for its relevance and ability to be applied to support Federal agencies in their IPv6 transition planning effort. The lessons learned and approaches were grouped into common categories, analyzed, and distilled into best practices based on the collective experiences. The best practices were then formed into an overall process that agencies can reference as they establish their specific transition approaches and strategy.

Key points to be aware of when planning the transition to IPv6 are identified using this format throughout the report.

2 Organizational Strategy and Architecture Best Practices

The value to be gained by IPv6 is not just a technological value and may not be calculated based on technological efficiencies using today's enterprise and network architectures. Today's architectures are based on the technology framework that currently exists, with an "old school" approach to packetized communications. IPv6 can represent a significant shift in the communications paradigm, fundamentally changing the way organizations do business. Understanding this new paradigm is important in that new organizational strategies can be developed. These new strategies can overcome existing barriers and provide capabilities that had not been considered before.

Examine IPv6 as a new communications paradigm to develop future architectures. Reliance on past concepts will prohibit the realization of new IPv6 capabilities.

To achieve this, organizational strategists need to understand what IPv6 and its related enabling technologies bring to the table. Understanding these capabilities will provide the strategist the insight to develop new organizational strategies. This will most likely require a technology advisory group to provide technical capabilities to strategists in order to provide them insights regarding IPv6 capabilities. This is not to conclude that the technology should drive the organizations implementation of IPv6. On the contrary, the organization's strategic mission, as clearly stated as the primary objective of the Federal enterprise architecture, must be the driving force.

Develop an organizational strategy that drives technical functionality, through enterprise architecture, to determine future IPv6 feature needs. This strategy should take into account the various capabilities of IPv6 and the synergistic effect these capabilities will have across all organizational functions and business lines.

Enterprise architectures, driven by the strategic mission, can only be accomplished by providing traceability from organizational activities back to the organizational strategy and ensuring that appropriate measures of success or effectiveness are in place.

Develop organizational measures of effectiveness that relate the technical features of IPv6 milestones and the business strategy.

Figure 3, Organizational Strategy Drivers, shows the relationship between the various activities associated with aligning business strategy and technological solutions. The concepts and value of enterprise architecture are addressed in this section, while systemic management and engineering are addressed in Section 3 and technology is addressed in Section 4.

Business strategy drives the IT enterprise architecture (EA), which provides the blueprint from which managerial and technological systemic processes develop organizational solutions. These solutions, in turn, rely on existing or developing technologies and standards as their building blocks. To meet the objectives of the organization, an EA and its parent business strategy must be informed and take into account the future nature of technology.

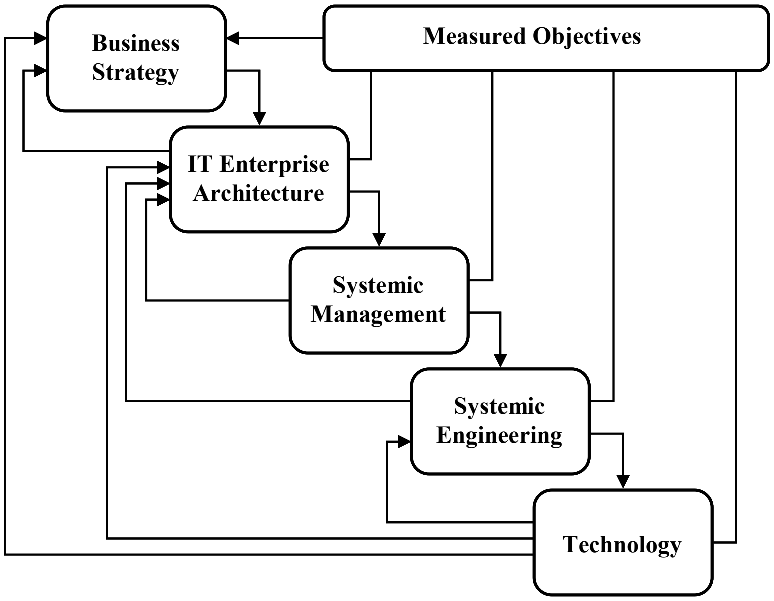


Figure 3: Organizational Strategy Drivers

In this case, the fundamental technologies available from IPv6 are summarized in Figure 4, IPv6 Features. This view of IPv6 capabilities shows that IPv6 will provide new capabilities to networks as well as networked applications. Ultimately, these capabilities will improve the users' communications capabilities.

Taken individually, some of the features are not significantly different from "perceived" IPv4 features. However, the IPv6 framework is different and will provide a significant enhancement to current network and end-to-end application capabilities.

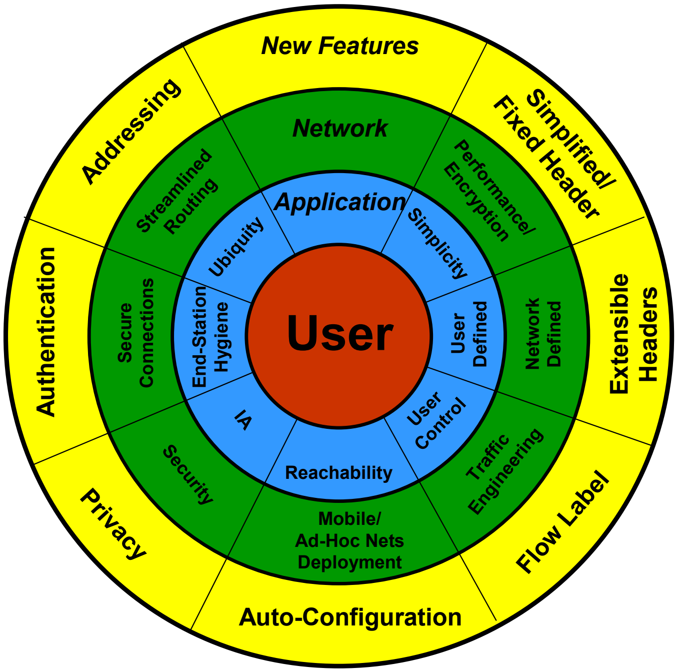


Figure 4: IPv6 Features[2]

The features of IPv6 should not be evaluated individually but rather as a whole. As an example, auto-configuration is a valuable feature, but combined with appropriate routing and addressing schemas and other emerging technologies, such as Radio Frequency Identification (RFID), near real-time tracking of mobile devices and inventory over IP may become a reality.

2.1 Enterprise Architecture

While EA has existed since the early 1980's, it has become a major organizational endeavor over the past five years. Many different views of EA exist, but all of them appear to derive from the Zachman Framework. The Zachman Framework depicts EA as having multiple "views." These views can be considered strategic, operational, systems, technology, and design. Likewise, as each view is developed, the architect should attempt to answer the questions who, what, where, when, why, and how?

This approach to EA has served its role well over the past two decades, as it is an excellent model to conceptualize an organization's IT structure. However, future technologies may require a slight modification to the EA structure. While automation is a performance enabler for many types of systems, IPv6 automated features will provide additional networking and application automations. These automations, while born in systems, can provide operational value. So, a simple modification to the Zachman EA could be an Automata layer that accounts for new IPv6, and other technology, automation features. Additionally, because success in any programmatic or technical effort requires measurement, it is necessary to consider the question of how well an architectural view will serve the intended organizational need when developing the various views of the

[2] Federal CIO IPv6 Transition Planning Workshop 4 November 2005, Presented by Dr. Chuck Lynch

architecture. Additionally, at each of the layered views of the EA, consider how its achievement will be measured.

In developing the enterprise architecture, consider the automation features of IPv6 and related technologies, such as wireless communications.

Developing measures for each view of the enterprise architecture will provide insight into which information technology solution best serves the organization's strategy.

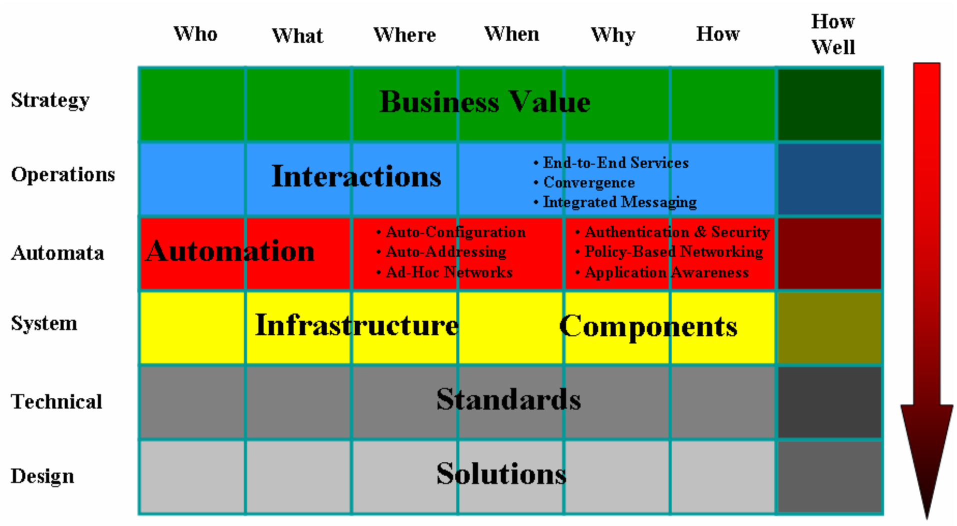


Figure 5: Modified Zachman Enterprise Architecture Framework[3]

As stated previously, the FEA process is a superior approach to aligning organizational strategy with information technology. The FEA approach is geared toward achieving organizational improvements by developing "as-is" architecture and "to-be" architectures, such that a delta between the current and future architectures can be determined. This approach provides very clear paths to measuring achievement of the "to-be" architecture.

Government agency architectures are measured on the maturity of their EA and its associated work products, as well as the investment recommendations. These investment recommendations should be accompanied by a business case showing improved performance or cost savings.

A successful IPv6 program must be tied to a business case and related investment recommendations.

[3] Federal CIO IPv6 Transition Planning Workshop 11 October 2005, Presented by Dr. Chuck Lynch

Agency EAs are also measured based on their degree of alignment with the agency's mission, direction, and plan. To be successful, IPv6 and its related enabling technologies must become part of the organization's strategic culture. The agency should develop an IPv6-capable "direction" and "plan."

Successful IPv6 transitions require organizational direction and plans that utilize IPv6.

Further guidelines for FEA assessment show that the architecture should facilitate the management of change. IPv6, as a foundation technology, can provide a significant platform for change.

Successful change requires the insight to see the potential of present and future technologies. IPv6 has tremendous potential for change.

Successful EAs demonstrate a clear path of integration, including standardization of interfaces and interoperation. Agencies should carefully review IPv6 transition mechanisms to ensure that a transition path exists for their systems, such that continued integration and interoperation is possible. Integration must be considered from all aspects of the system, including interoperations of:

- Intra-agency operations
- Extra-agency operations
- Inter-agency operations
- Agency to customer operations
- Agency to vendor/industry operations

To provide a smoother transition, agencies should utilize standard transition mechanisms and develop interface standards and specifications for intra-, extra-, and inter-agency operations as well as agency to customer and agency to vendor/industry operations.

FEA also concerns itself with convergence and how well the EA converges the information technology assets of an agency. This must be accomplished with respect to the Technical Reference Model (TRM). The Internet Protocol has been, if nothing else, a great integrator of technologies. Its sole purpose was to permit inter-networking among disparate networking technologies. IPv6 will provide the next step in the evolution of inter-networking and may provide the opportunity to finally achieve communications convergence in a secure and more reliable communications environment.

Consider that IPv6 is a convergence technology by definition and consider its capability to support technology convergence in the organization.

Finally, FEA must consider transition strategy. Since mature EAs must contain a "baseline" as-is architecture and to-be architecture, it follows that there should be a plan to transition from one architecture to the other. This plan should consider technology availability, funding profiles, interoperations, as well as the business strategy it is trying to realize.

Develop a comprehensive transition strategy that takes into account technology timelines, available functions, and organizational priorities.

To achieve a successful enterprise architecture, the agency should utilize existing EA resources and tools. One tool that can serve as a common sharing environment for IPv6 profiles, plans, approaches, and technologies is CORE.gov.

CORE.gov is an Inter-agency collaboration and development environment. Component Organization and Registration Environment (CORE) is a component resource repository where agencies' register processes, capabilities, case studies, best practices, documentation, and software. CORE.gov was started by the FEA Project Management Office with the goal of supporting cross-agency collaboration, transformation and government-wide improvement. The concept is to create a collaborative environment to share resources and technologies such that agencies do not have to reinvent the wheel. The CORE.gov website is located at https://www.core.gov/.

FEA resources:

FEA Web Site
http://www.whitehouse.gov/omb/egov/a-1-fea.html

A Practical Guide to Federal Enterprise Architecture:
http://www.gao.gov/bestpractices/bpeaguide.pdf

The Federal Enterprise Architecture Management System (FEAMS):
https://www.feams.gov/

Guidelines for Enterprise Architecture Assessment Framework:
http://www.feapmo.gov/resources/040427 EA Assessment Framework.pdf

2.2 Strategic IT View

In developing the strategic view for the EA, first identify the strategic documents that define the organization's mission. The organization should update these documents to take into account the potential role of IPv6 and its impact on the strategic vision:

- Who will lead the organization's IT infrastructure to change?
- What are the potential benefits of IPv6 in achieving the organizations strategic mission?
- Where might the organization be deployed to achieve its mission or expand its influence?
- When must critical new capabilities be deployed to make the strategic mission achievable?
- Why are legacy systems necessary and can they be phased out to achieve greater performance?
- How do the specific capabilities of IPv6 impact the way the organization does business?
- How well can the strategic mission be achieved in the future with IPv6 versus without it?

Can IPv6 aid in achieving the organization's strategic vision and mission? The answer is "yes" if agencies understand its potential and the new communications paradigm it creates.

2.3 Operational View

In order to accomplish the strategic vision (Strategic View), the operational view considers how, why, and when the organizational elements communicate. Organizations need to communicate internally and externally to accomplish their missions. Often, mission scenarios require the transfer of information and knowledge with systems that can be replaced over time with newer technologies. In some cases, these information transfers can be automated. The following questions need to be answered to determine how this communication might change with the implementation of IPv6 features:

- Who depends on the organization's IT infrastructure to communicate and transfer information? Include customers, other federal agencies, non-federal agencies, and international organizations.
- What types of data, information, and knowledge need to be created, transferred, or stored, and what are the security requirements?
- Where must data, information, and knowledge be transferred or stored?
- When must data, information, and knowledge be created, transferred, or stored, and what are the timing requirements for such events? What are the priorities for such transfers?
- Why must data, information, and knowledge be transferred, and are there mission critical aspects of the transmission that require special handling?

- How should data, information, and knowledge be created, processed, transmitted, and stored?
- How well must the IT infrastructure perform in order to ensure organizational mission success?
- Do the answers to these question change based on the potential capabilities of IPv6 deployment?

2.4 Systems View

In order to accomplish the operational communication requirements (Operational View), what systems are needed? What are the system architectural changes that can occur as a result of deploying IPv6 features? In order to develop an appropriate IPv6-based system architecture, the architect must understand:

- The nature of core, distribution, and edge network routing and addressing
- Networking enclaves (locations and facilities)
- Domain Name Service (DNS) resolution requirements
- Application networking requirements and the associated Application Programming Interfaces (API)
- End-to-end security and information assurance requirements and issues
- Network management solutions
- End-to-end policy-based networking requirements
- Training requirements for network design, deployment, and operations; application development; and security implementations.

The system architect must also define:

- Mission threads
- Application needs
- System functional requirements
- Security needs
- Storage needs
- Redundancy (reliability and availability)
- End devices

2.5 Technical View

In order to develop systems that are harmonized throughout the organization, a technical architecture is needed to provide a set of standards for enterprise systems development. This standards profile should reflect current “design-to” and “build-to” specifications and standards as well as maturing standards that are under consideration for future builds and buys. The standards and specifications may be gleaned from existing efforts by U.S.-based and international standards organizations, but some agency specific standards and specifications will most likely be required. The technical architect should:

- Define a set a of current IPv6-capable standards and functional specifications
    - Utilize current work of the DoD, industry, The Open Group, The IETF, and test vendors
- Define future IPv6-capable standards and functional specifications
    - Realize that "period" or milestone specifications are needed as the protocols mature over time
- Define interface specifications for system interoperability

The technical architect should utilize the FEA's TRM for software and Internet functionality. The TRM provides a component framework, which defines the technical elements used to develop, integrate, and deploy systems and service components. Example categories for components are:

- **Business Logic:** Defines the software, protocol or method in which business rules are enforced within applications

- **Data Interchange:** Data Interchange defines the methods in which data is transferred and represented in and between software applications

- **Data Management:** The management of all data/information in an organization. It includes data administration, the standards for defining data and the way in which people perceive and use it

- **Presentation / Interface:** This defines the connection between the user and the software, consisting of the presentation that is physically represented on the screen

- **Security:** Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. Biometrics, two-factor identification, encryption, and technologies based on the NIST FIPS-140 standards are evolving areas of focus

3 Program Management Best Practices

Program management of the IPv6 effort is the most critical element of a successful transition. The technology will come about due to market forces and the development, build and deployment processes. An organization's ability to deploy IPv6 capabilities is dependent upon their ability to plan for the rapid integration of new technologies like IPv6 and other enabling technologies, such as wireless, RFID, etc. This requires an understanding of the advantages to be gained as well as constant assessments of maturity and potential influence on the technology process.

Sound systemic managerial and technical processes, which are responsible for developing the IT infrastructure defined by the enterprise architecture, are well defined by systems management and systems engineering. What is often confused is the nature of both processes as they work together to achieve a stated objective. In some systems engineering documents, such as Military Standard (Mil-Std) 499B, Systems Engineering, the process is defined as a combination of systems management and engineering, as shown in Figure 6, Systems Management and Systems Engineering. The management portion of the process, known as Systems Analysis and Control, directs the technically oriented activities of the organization. The key here is not the specific nature of the processes, but the fact that they are systemic and repeatable. This is critical, because the adoption of technological functions over a period of time, much like the transition to IPv6 will be, requires a continuous, sustained, repeatable process, such that continuous progress and measurement can be elicited.

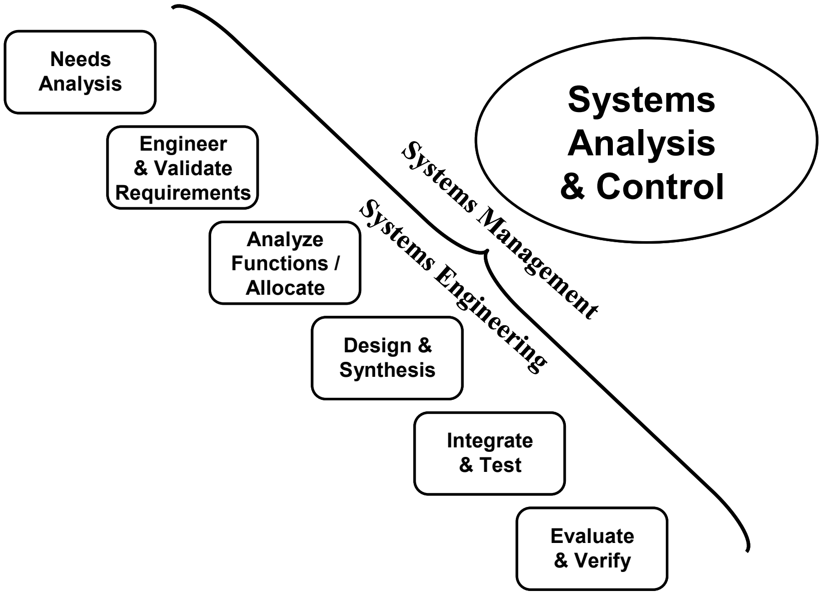


Figure 6: Systems Management and Systems Engineering

The transition to IPv6 will be a difficult task, primarily because of the managerial and technological risks associated with the ever-present uncertainty of the market and international politics. Figure 7 provides a context of the transition management activities involved. The transition itself will take years and will be a series of technology insertion efforts rather than a single programmatic effort to build or migrate a system of systems to a well-known or well-defined outcome. With IPv6, the target capability "states" will be uncertain or moving targets, with drivers that are outside the control of an agency and the Federal government at large. The Federal government mandate to move to IPv6, regardless of the specified date, will serve as a stabilizing factor and keep industry more focused on IPv6 technologies.

The transition to IPv6 will not have a clear path of execution. Anything anticipated beyond the two-year timeframe will carry additional technical risk.

3.1 Transition Management Context (Diagram)

A successful IPv6 transition program should consider the following areas. The program should start with the strategic mission of the agency and utilize the existing agency processes and infrastructure, versus developing a new effort. A new, stand-alone effort will create a core team with IPv6 knowledge but will not make that knowledge pervasive. It does make sense to create an IPv6 center for the purposes of coordinating the various agency-wide activities that must occur and in sharing lessons learned. This concept will work at an agency level and at a government-wide level.

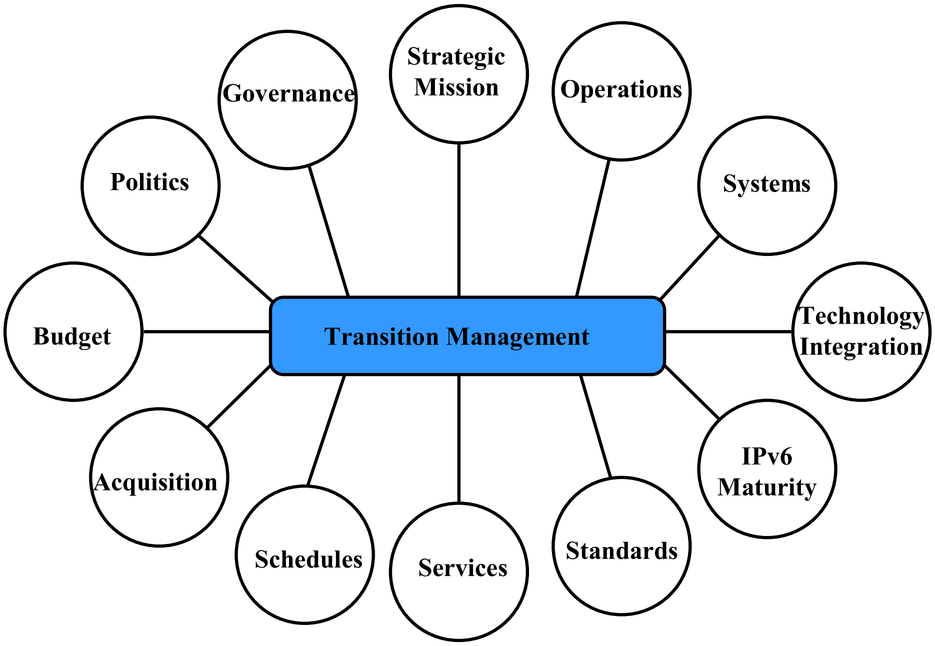


Figure 7: Transition Management Activity – Context Diagram

Another key aspect of managing the IPv6 transition effort is that the activities must be separated based on organizational capabilities. A technical organization responsible for developing transition solutions should not be left to handle the processes for governance, budget, acquisition, etc. The lead for IPv6 should not be deemed a "Program Manager" as though the transition were a discrete program.

The organization should utilize and perhaps modify existing processes when possible, rather than inventing new ones that duplicate an organizational function.

A centralized office for integration and technology can provide significant reduction of transition effort and cost due to reduction of duplication.

A "Program Office" mode of operation is inappropriate for IPv6 transition, since all aspects of the organizations IT will transition.

3.2 Concept of Operations

Functionally, the organization needs to understand the complexity of the IPv6 effort that is within its sphere of influence. As an agency effort, the transition may be viewed as an effort to simply follow the trends. This very well could be an appropriate approach. However, a proper review of business strategy and the EA should reveal future functional capabilities that IPv6 could afford the organization that are currently in a state of flux. It is advantageous for an organization to engage with the various organizations and institutions that play a part in the development of the protocol and the policies that surround it.

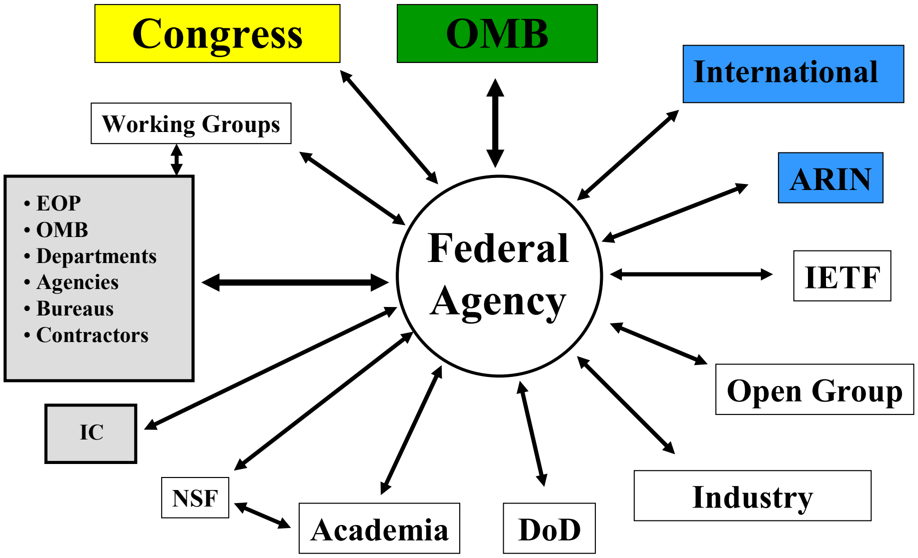


Figure 8: Concept of Operations - Context Diagram

Figure 8, Concept of Operations – Context Diagram, shows many of the potential interfaces that may exist for an organization during the IPv6 transition. Most obvious relationships are already well understood, but many new relationships and activities may be required. The following are examples of the various relationships that may need to be established:

- **Inter-agency:** Utilize existing forums for the interchange of best practices and lessons learned. Possibly create new sub-groups under existing committees. Possibly establish a federal-wide IPv6 transition office to provide common solutions to federal agencies.

- **Academia:** Interact with academic efforts to study IPv6 and develop new capabilities. Monitor the National Science Foundation's (NSF) efforts on network and application research. Most advanced technologies start with research in universities or cooperative efforts between academia and industry.

- **Department of Defense:** The DoD has progressed toward their IPv6 transition since June 2003. Request and utilize existing work that has already been accomplished.

- **Industry:** Most advanced technology implementations can be predicted by interfacing with industry leaders. Today, many hardware and software vendors are developing IPv6-capable products and have plans to roll them out within the next couple of years. Additionally, Internet Service Providers have or are implementing IPv6 in their networks. Interfacing with these organizations can reveal a great deal about how to implement IPv6 and when unique IPv6 functionality will be available.

- **IETF:** The IETF is responsible for developing the standards for the IPv6. These standards, which go through many different stages of maturity, are known as Requests for Comment (RFC). Any organization can participate in the IETF and have a voice in the RFCs or develop a proposed RFC on their own.

- **ARIN:** ARIN is the Internet registry for North America. Any organization acquiring IPv6 addresses must request the addresses from ARIN. If the organization qualifies, they can get a standard allocation without justification. If, on the other hand, the organization has a larger need for address space, they must follow ARIN guidelines and justify the address space. It is also advisable to participate as an ARIN member, since the membership helps to establish the address allocation policies for the region.

- **International:** Many international organizations are involved in IPv6 development and promotion. Additionally, many agencies have existing relationships with international entities that require interoperability of communications systems. As agencies begin to transition, it will be necessary to understand the interoperability implications of international partners.

3.3 Systemic Processes

As stated earlier, successful transition will require adherence to existing capabilities that are sometimes modified to handle technology insertion. Existing managerial and technological processes are most likely systemic. Systemic processes are repeatable and consistent and many are formalized in process documentation. Keeping in mind that IPv6 transition is equivalent to many technology insertion programs, the technical insertion effort will have to be repeated many times, from architecture updates, to planning, to execution and measurement. IPv6 transition will not be unlike the transition that has occurred over the past 15 years with growing Internet technologies. Today's Internet technologies are very complex in that they involve both hardware and software. While most functional responsibilities exist in a client/server environment, it is not a hard and fixed rule. Functional capabilities can be distributed such that application and network functionality are intertwined. Future IPv6-based systems will most likely make interactive functions seem more complex.

3.3.1 Governance Process

The organization should create a stable governance process for IPv6 transition. This process should have very clear lines of authority and communications. It is most likely that an agency already has existing governance processes, via the CIO or chief technology officer (CTO), that can be used for this purpose. However, IPv6 governance and management may create situations that have never existed before. With current Internet technologies, there are rarely high-level controls on the implementation of new technologies, except for the potential security and information assurance ramification. In many quarters, IPv6 will be handled differently, with controls on all aspects of engineering, deployment, monitoring, etc. If this is the case, then new governance efforts may be needed.

Utilize existing governance, management, and technical processes for IPv6 transition when possible.

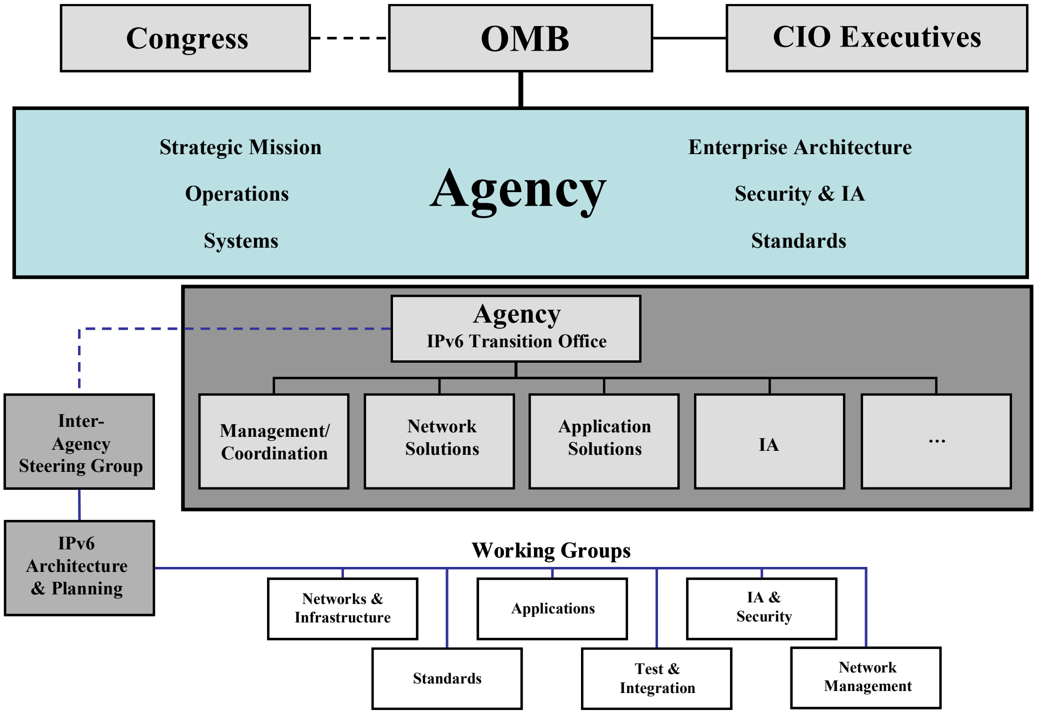


Figure 9: Governance Structure

The governance structure suggested in Figure 9, Governance Structure, provides a hierarchical notion of how an agency may organize to transition to IPv6 or any of the various enabling technologies under development. The agency should utilize existing processes when possible and create only those entities that add value or reduce duplication of effort. If the agency establishes an IPv6 transition office, it should not supplant existing roles and responsibilities. In other words, a transition office's technical effort in IPv6 security should not alleviate the agency security organization from performing the necessary work to prepare the agency for IPv6 security measures.

If an IPv6 Transition Office is established, it should not supplant existing organizational effort, but should provide technical expertise to ensure that the agency accomplishes the necessary activities for IPv6 transition and supports the integration of IPv6 efforts across the organization.

To avoid confusion, it may be necessary for the organization to establish a primary IPv6 working group that can provide guidance and prioritization to other existing or created working groups. Independent efforts working toward IPv6 solutions must be coordinated and a common solutions "knowledge center" or Knowledge Management System established such that various program offices or procurement centers are following common guidelines.

A common solutions knowledge center or Knowledge Management System should be established to ensure that all organizational elements are using the same solution base.

This is very much inline with the existing Federal enterprise architecture efforts and CORE.gov recommendations.

There should be a clear distinction between the governance of IPv6 transition and the management of the transition at a program level. An IPv6 transition office should not carry the burden of transitioning organizational assets. A transition office should be responsible for developing common solutions and coordinating the various efforts to ensure a timely and coherent transition, but program managers should be responsible for all aspects of the transition of their program.

An IPv6 transition office should be responsible for developing guidelines, common solutions, and coordinating the organization's transition effort. Individual program offices should be responsible for all aspects of their program's transition.

3.3.2 Systems Management

Systems management is the controlling function that ensures appropriate resources are utilized to accomplish the program, including people, assets, facilities, schedule, etc. The systems management element is responsible for providing input into enterprise architecture and other organizational functions with regards to systems solutions, capabilities, and timelines for implementation.

As shown in Figure 10, Systems Management, there are specific responsibilities that should be enacted by the management team for any program transition to IPv6.

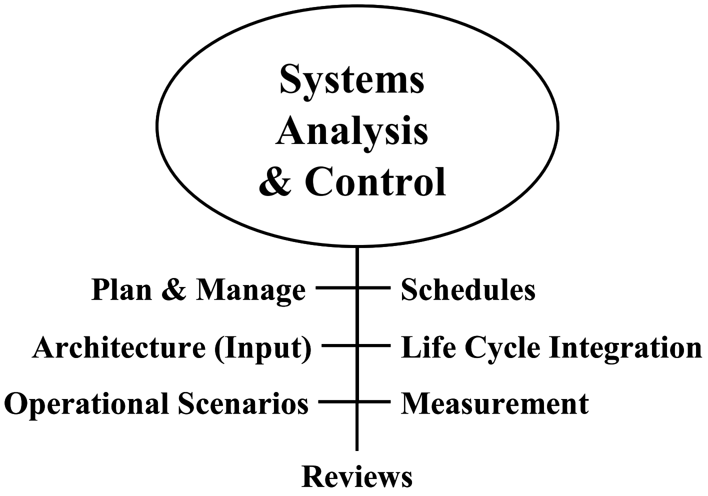


Figure 10: Systems Management

Management should be responsible for providing input to the enterprise architecture effort, planning and scheduling, and reviews and measurement. The program should seek guidance from the IPv6 transition leader to ensure they are adhering to best technical practices. The program manager must also provide planning and scheduling information to the IPv6 team so that it can be coordinated with other programs. A program manager need not develop a separate IPv6 planning document and can roll the IPv6 transition effort into existing program management documentation.

A program does not need to develop distinct IPv6 documentation, but can roll the IPv6 elements into existing, broader scope program management documentation.

3.3.3 Systems Engineering

Systems engineering is a systemic process for translating organizational and user needs into a system description, integrating the various technical and non-technical disciplines, and integrating systems and components into solution definitions. This is not the specific design of the system, but the specifications for making it achievable. This is all done with a focus on the life cycle(s) of the system(s) being defined.

Just as systems management focuses on the managerial aspects of a project or program, systems engineering focuses on the technical aspects from validation to verification. Each system requirement should be appropriately engineered and validated and every defined solution must be verified to meet the intended objective.

Validating a requirement means asking: 'Are we building the right system?' whereas verification of a system means asking: 'Did we build the system correctly?'

Figure 11 shows the fundamental elements of a standard systems engineering effort. For some, systems engineering may be the wrong term. In actuality, systems engineering is systemic engineering and simply describes a systemic solution process.

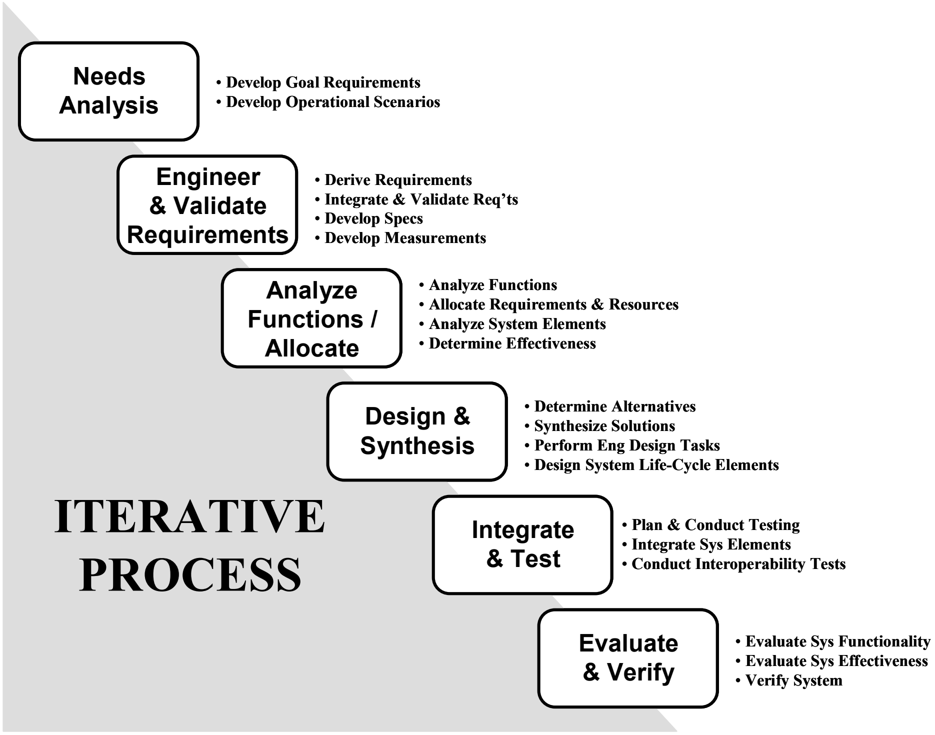

Needs Analysis
• Develop Goal Requirements
• Develop Operational Scenarios
Engineer & Validate Requirements
• Derive Requirements
• Integrate & Validate Req'ts
• Develop Specs
• Develop Measurements
Analyze Functions / Allocate
• Analyze Functions
• Allocate Requirements & Resources
• Analyze System Elements
• Determine Effectiveness
Design & Synthesis
• Determine Alternatives
• Synthesize Solutions
• Perform Eng Design Tasks
• Design System Life-Cycle Elements
ITERATIVE PROCESS
Integrate & Test
• Plan & Conduct Testing
• Integrate Sys Elements
• Conduct Interoperability Tests
Evaluate & Verify
• Evaluate Sys Functionality
• Evaluate Sys Effectiveness
• Verify System

Figure 11: Systems Engineering Process

The principles of systems engineering are clearly defined in EIA 632, Mil-Std 499B, and IEEE-1220.

- EIA/IS 632, *Interim Standard: Systems Engineering.* 1994. Electronic Industries Alliance, December 1994.

- IEEE 1220-1998. IEEE Standard for Application and Management of the Systems Engineering Process, IEEE Computer Society, Institute of Electrical and Electronics Engineers, 1998.

- MIL-STD-499B, *Draft Military Standard: Systems Engineering*. HQ/AFSC/EN, Department of Defense, "For Coordination Review" draft, May 6, 1992.

An excellent guide to systems engineering is available from the Defense Acquisition University. The guide, Systems Engineering Fundamentals, can be found at:

- http://www.dau.mil/pubs/gdbks/sys_eng_fund.asp

A systemic engineering process is necessary to ensure that common solutions are implemented in organizational information technology efforts.

3.3.4 Systems Integration

While systems engineering focuses on the system(s) being defined, systems integration focuses on the interoperability of the various systems that must work together. In this regard, systems integration will be responsible for determining the appropriate schedules for system capability deployment, transition mechanisms, system interface specifications, and customer interface specifications.

Most organizations do not have a specific systems integration effort but instead manage the integration of their various IT functions through the CIO. This is a perfectly acceptable approach. However, if a specific team is organized to support the integration of IPv6 across an agency and they are given the responsibility of developing integration solutions, it may be worthwhile to have that specific team reporting directly to the CIO's office.

> ***An IPv6 transition office or team should be responsible for developing integration solutions. If they are responsible for monitoring integration, the team should report to the CIO's office.***

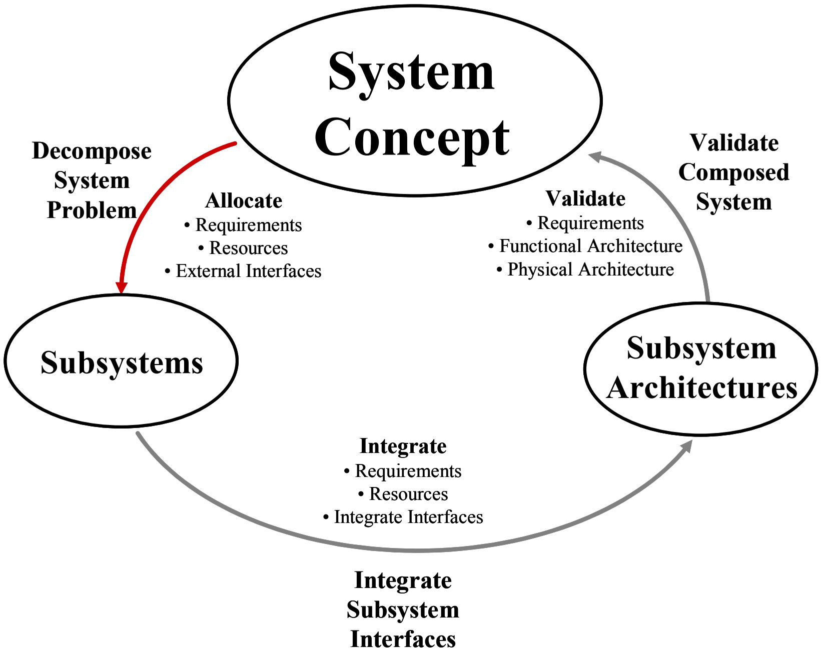


Figure 12: Complex System Integration Process

Integration within or across complex systems requires a thorough decomposition of the systems concept and an iterative process for developing appropriate interfaces and validating that those specified interfaces meet the intended purposes of the systems. As shown in Figure 12, a Complex Systems Integration Process involves:

- A system is decomposed into subsystems
    - Requirements and resources are allocated to each subsystem

  - External interfaces are defined
- Subsystems are integrated at the interface level
  - Requirements and resources are matched
  - Interfaces are integrated and matched
- A system level architecture is defined
  - System architecture requirements are complete
  - Internal and external interfaces are complete
  - Architecture is validated against the original system intent
- The process is repeated, first for a functional architecture and then for a physical architecture.

3.4 Governance

The governance process, as described in section III.C.1, Governance Process, should be responsible for the development for IPv6 policy, managerial and technical guidelines, and measurement and reporting. Various levels of the governance process will be required to handle different aspects of these critical areas.

3.4.1 Policy

Policy development is rather straight-forward; it is designed to maintain control of ongoing and future activities, but is also in response to higher-level authority and legislation. Organizational-wide policy has a procedural approach that can and should be utilized for IPv6 transition. A cautionary note, however, is that bureaucratic slowness may prevent the rapid deployment of new IPv6 features. In some cases, internal IPv6 policy should be driven down to the lowest common denominator or fully expressed in the enterprise architecture.

The role of an IPv6 transition office should be to review higher-level policy and legislation and to draft and review agency IPv6 policy. IPv6 policy must reach throughout the organization and must be administered from recognized authority. If senior leadership is not behind the policy or if the policy is not timely (i.e., gets outdated), then the transition effort will be weakened.

> ***IPv6 policy should be handled just as any other organization-wide policy is handled. It should carry the authority of agency leadership and be maintained in a timely manner.***

Policy should be directed at the following areas:

3.4.1.1 What?

IPv6 policy must provide:

- What are the stated organizations objectives for the transition?
- What must systems (network, application, etc.) be capable of performing at stated milestones?

- What advanced features of IPv6 must be ready?
- What are the specific IPv6 functional hurdles that should be targeted?
    - What is IPv6-capable?
    - How does the definition of "IPv6-capable" change over time?
- What IPv6 features and capabilities should be avoided due to risk?
- What other technologies are enablers to new, desired organizations functional capabilities?
- What must programs do to prepare and plan?
- What must programs do to perform necessary programmatic activities?

Policy must provide stated objectives for IPv6 functionality and criteria for programs to achieve the objectives.

3.4.1.2 When?

Policy must establish "believable" milestones with realistic resources behind them to make the schedule achievable. It must also recognize the simple fact that there are dependencies outside of the agency's control, i.e., product and function availability provided by vendors and service providers. Agency policy must recognize the risks involved in IPv6 deployment and the need to interact with other agencies and industry to ensure consistent IPv6 direction.

IPv6 policy must provide:

- Milestones that are believable and achievable.
- Guidelines for minimum functional capabilities by specific milestones.
- Mandated procurement and acquisition of IPv6-capable systems and components.
- Standards profiles that must be adhered to as the protocol and products mature
    - Policy must point to a technical architecture
- Guidelines for developing programmatic plans and schedules
- An agency plan and schedule

Figure 13 provides a high-level view of a five-phase schedule for IPv6 transition and the critical efforts that must be accomplished during each phase. It should be noted that there is no timeline associated with the phases, as every organization will have to develop an appropriate timeline that is achievable and ensures internal and external interoperability.

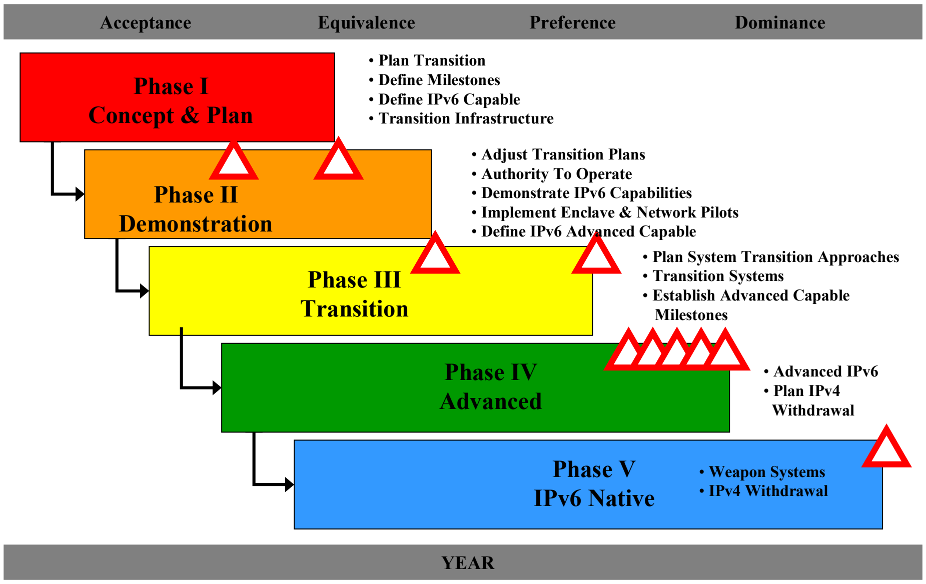


Figure 13: IPv6 Transition Phases

3.4.1.3 How?

IPv6 policy should specify constraints for IPv6 programmatic implementations. The policy should focus on what must be done in order to allow IPv6 deployment. Also, policy must account for constraints that can be implemented via restrictions, i.e. security policy, vice physical implementations. Areas of policy consideration include:

- Locations for deployment
    - Core networks
    - Edge or enclave networks
    - Isolated applications
    - End-to-end applications
    - End-sites
- Levels of security
- Utilization of IPv6
    - Minimal capability
    - Dual-Stack
    - Tunneled
    - IPv6 Native
- Functional profiles
- Prohibitions of use
    - Ports and Protocols

3.4.1.4 Procurement

IPv6 policy should address and point to standard acquisition and procurement specifications and procedures. This ensures adherence to guidelines that will be amended from time to time. Consider:

- Standard acquisition and procurement language
- Standard contractual language
- Modification of past contractual language
- An IPv6 contractual vehicle that permits all agency entities to contract for IPv6 support, thus providing some commonality

3.4.2 Managerial and Technical Guidelines

Managerial and technical guidelines should be considered distinct from IPv6 policy. If a centralized IPv6 transition office or team is established, it should be given the authority to draft managerial and technical guidelines for IPv6-related issues or to provide input to other agency documents. Managerial and technical guidelines should carry the authority appropriate for the scope of guidelines, presumably CIO-level.

> ***Managerial and technical guidelines relating to IPv6 should be drafted by an IPv6 team, versus independently throughout the organization.***

A sound approach to developing managerial and technical guidelines for IPv6 and vetting them appropriately involves using a working group process.

Working groups, if established for the IPv6 effort, should be hierarchical with clear lines of communication and authority. The highest level IPv6 working group should manage and control, or at least direct, the IPv6 efforts of lower-level IPv6 sub-working groups.

> ***IPv6 expertise will be very limited at first and there will be a need to avoid having the same "experts" on every working group.***

> ***Utilize existing working group structures when possible, especially working groups that have senior-level backing, a good reputation, and that get things accomplished.***

Possible working group levels include:

- IPv6 Architecture Working Group (WG)
    - IPv6 Network Sub Working Group (SWG)
        - Routing
        - Addressing
        - DNS
        - Network Time
    - IPv6 Applications SWG
    - IPv6 Security & IA SWG
    - IPv6 Network Management SWG

3.4.3 Measurement and Reporting

The IPv6 effort in the organization must develop sound approaches to measuring transition effectiveness. These measures must be reportable and understandable to senior level managers and higher level authority, including senior executives and Congress. These measures can include:

- Milestones achieved
- Systems transitioned
  - Capable
  - Enabled
  - Operational (with Transition Mechanisms)
  - Operational (IPv6 native)
- Applications transitioned
  - Capable
  - Enabled
- DNS servers transitioned
- IPv6 procurement opportunities
  - Achieved
  - Missed

Sound and reportable metrics must be developed and monitored to ensure the IPv6 transition effort is on track and milestones achieved.

3.4.3.1 Audits and Inventories

Audits and inventories should be conducted of hardware, software, communication systems, and services on a regular basis. The initial audits required by OMB should only be a starting point. Processes should be instated that maintain records of IPv6-capable procurements and capability. Additional audits should be accomplished of existing contracts and procurement activities that do not specify IPv6.

Potential audits and inventories include:

- Network hardware and software
- Security and Information Assurance hardware and software
- Host and server hardware and software
- Application Software
  - Back Office
  - Front Office
- Other software system
  - Embedded, real-time
  - Control
  - Avionics
  - Software under development or modification

- Procurement activities
    - IPv6-capable
    - IPv6 upgradeable
    - IPv6 incapable
- Contracts
    - IPv6 specific language
    - No IPv6 specific language

Additional audits and inventories should be accomplished to determine the future scope of IPv6 needs within an organization. In order to acquire an appropriate amount of IPv6 address space, an agency should know:

- Locations
- Facilities and buildings
- Platforms
- Vehicles
- Vessels
- Personnel
- Devices
- Current IPv4 enabled devices
- Current IPv4 address blocks utilized (/24 CIDR Blocks)

An inventory of current and potential future assets aids in the IPv6 address justification and procurement process. Specific modeling techniques relating to the organization's operational profile, estimated communications growth, global presence, and need for security and surge capability all impact the amount of IPv6 address space you can qualify for.

4 Technical and Deployment Approach Best Practices

The base protocols associated with IPv6 are stable and equipment has been available to support IPv6 implementations for a number of years. Many of the organizations surveyed for this report began testing and purchasing IPv6-capable equipment over five years ago and were able to deploy their networks with no significant operational impacts due to the emphasis placed on planning and testing for the transition.

> ***Proper planning and testing reduces the potential impacts during the deployment phase of the transition. Money spent today in planning and testing will pay off with a smoother transition.***

Although limited applications are available today for use with IPv6, the networking products are readily available from leading vendors such as Juniper Networks for routers, and most major operating systems support IPv6 today with significant enhancements planned in the near future.

> ***Vendors are eager to learn specific agency requirements to build their solutions. Meet with vendors and let them know your requirements early in their product development cycle to ensure they will meet your needs in the future.***

Among the chief concerns in the technical arena will be integration across agency systems and between governmental organizations and bodies. One key to success, besides appropriate systemic processes, will be configuration control of all baseline solutions. It will be critical to develop understanding and agreement on what "IPv6-capable" means, planned rollout schedules, and support for legacy systems as well as manage the ongoing changes to the definitions.

> ***Use working groups within and across agencies to identify, prioritize and solve technical issues, specifications and deployment timelines.***

Although the base functionality for IPv6 is stable, significant work is still underway within the IETF to standardize advanced capabilities for IPv6 such as QoS, network mobility, network management and advanced security features. The U.S. government has numerous representatives within the IETF but has not taken a very active role in recent years.

> ***If the Federal agencies and the DoD work together and put forth their requirements, a greater number of standards and commercial products will meet requirements without customization.***

4.1 Technical Integration

The sequencing of the IPv6 transition is critical based on the goals and objectives of the organization. Several transition approaches have been identified at a high level such as:

- **Core-to-edge:** Transition begins in the core backbone networks, extends out through the sites to the Local Area Network (LAN) and end workstations, and finally to the applications.

- **Edge-to-core:** Transition begins with applications and workstations and carries inward to the core backbone network.

- **Geographical:** Transition occurs based on network geography.

- **Subnet:** Transition occurs based on network subnet segments.

Several steps that have been used in the transition to IPv6 include:

- **Experimentation and early adoption:** During this step, IPv6 access is usually over an IPv4-only infrastructure; automated and manual tunneling is extensively used so that researchers can experiment with IPv6 integration. Transition working groups are established to a) develop IPv6 adoption requirements, transition plans, deployment policy, and IPv6 information assurance policy; b) determine the best integration techniques: c) determine infrastructure upgrade requirements: and d) issue acquisitions guidance. Test beds are established and experiments conducted to gather information to support the transition working groups. During this period IPv6 capability requirements should be defined and a detailed definition of IPv6-capable product standards should be developed or adopted to ensure IT products will meet the enterprise's requirements.

- **Dual Stack Infrastructure Integration:** Once a decision to integrate IPv6 has been made, infrastructure to support IPv6 must be acquired and deployed. IPv6-capable routers, L-3 switches, information assurance equipment, servers, host operating systems, and applications must be purchased or developed. Most routing infrastructure and servers purchased in the last few years will already support IPv6 or need software upgrades. For older IT equipment, a complete replacement will be necessary to upgrade to a dual-stack capability. During this period purchasing and licensing agreements for IT hardware, operating systems, and software upgrades should specify IPv6-capable equipment. Training programs for IT administrators and for application developers must include IPv6. Experimentation continues and early adopter pilots occur during this phase to obtain operational experience and data to update transition plans and deployment plans to prepare them to support IPv6 production network deployment.

- **IPv6-Production Network Activation:** Once IPv6 deployment policy, information assurance infrastructure, network transport infrastructure, and administrator training is in place, a network can transition to IPv6 operations for users. During this period the IPv6 network is activated and IPv6 applications are integrated into user platforms on edge networks. Legacy edge networks are provided IPv6 service through tunnels.

- **IPv6-Dominant Transition:** During this period, IPv4 deactivation begins as all new applications are all IPv6-capable and some are born IPv6-only to leverage IPv6 network features. Some advanced networks will be built to leverage IPv6-only services (mobility, enhanced multicasting, etc.) and new networks may be designed IPv6-only and begin operation in this phase. As some networks become IPv6-only, IPv4-in-IPv6 tunneling will provide IPv4 service to legacy users. Translation may be required to add IPv6 capabilities to some legacy IPv4-only imbedded devices and application that have no upgrade path.

- **Mission Thread Transition (Alternative):** Some planning aspects of IPv6 transition may be based on critical mission needs with limited resources. In this case, it may be appropriate to deploy IPv6 capability to support end-to-end mission threads, vice specific networks or enclaves. In such a scenario, parts of the core, distribution, and edge networks would be transitioned to support end applications that have been transitioned to IPv6.

Plan for IPv4 deactivation. Once IPv6 has become dominant in the agency's enterprise, continuing to support IPv4 will increase operational costs and could limit widespread access to new features and capabilities.

Agency transition approaches will be a combination of the above. Experience to date has focused on transitioning from the core out, but considerations based on early adopters, mission critical systems, funding and other factors will most likely cause the approach to become convoluted. Another consideration in the transition approach is the use of transition mechanisms. Tunneling and translation should be used to support the overall roll-out approach and to maintain interoperability in the transitional environment. Other factors will impact the timing of the overall agency transition. Figure 14 shows potential drivers and constraints to the transition schedule.

It is important that each agency gain a thorough understanding of the drivers and constraints associated with their transition schedule and the overall impact each may have.

Use transition mechanisms such as tunneling and translation to support early adopters.

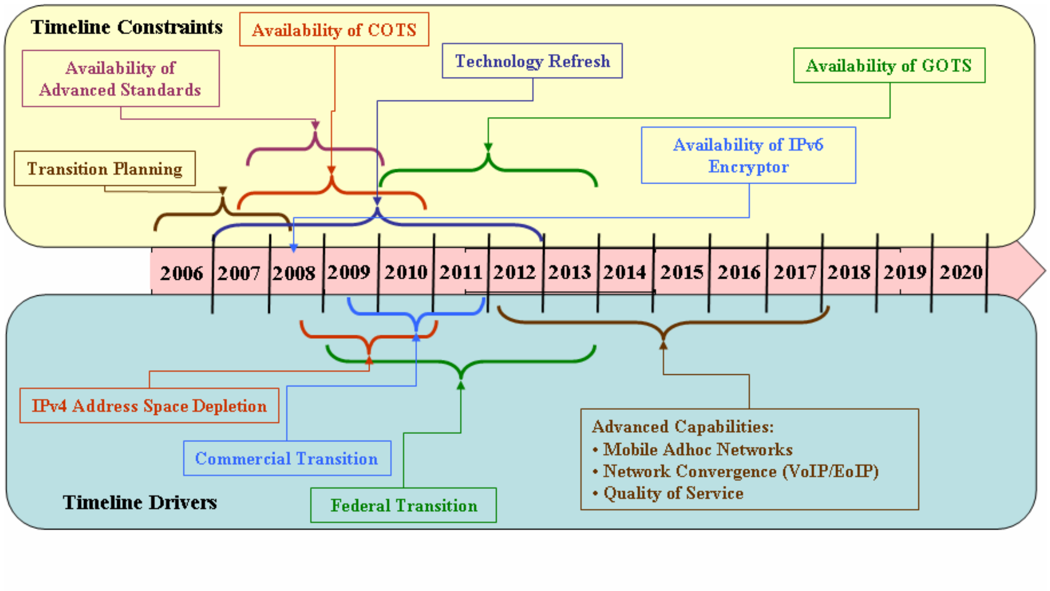


Figure 14: Transition Schedule Drivers and Constraints

No matter what approach is taken, certain aspects of the transition must occur early in the activation of IPv6.

DNS, network management, and security services must be taken into account from the beginning for proper and safe network operation. DNS should be one of the first elements of the transition.

A high level of interdependency exists between enterprise elements, but in many cases the use of transition mechanisms properly placed in the network can allow for the orderly and timely transition of the various attributes. The interdependency between network elements such as the backbone routers, site LANs, servers and hosts primarily focus on the ability for IPv6 packets to flow between and through these elements (although hosts and servers also have interdependencies with applications). The use of dual-stack, tunnels and/or translation mechanisms may be used to create interoperability or at least the ability to pass traffic through to another destination. Agencies should leverage a “distributed execution” approach where programs are responsible for planning and executing the transition of their systems.

Develop a detailed project plan for the entire transition through roll-out with linked interdependencies using automated tools. It is critical to keep the plan up-to-date and run project analysis reports often. The scope of the overall project is complex and utilizing automated tools will help identify issues prior to becoming critical path items. Figure 15 shows an example of a high-level timeline for the planning and testing elements associated with an agency’s transition approach. The steps included in the timeline are notional and will need to be tailored for each agency.

Utilize project planning tools with associated interdependencies to establish a realistic schedule and automatically identify impacts based on changes to the schedule.

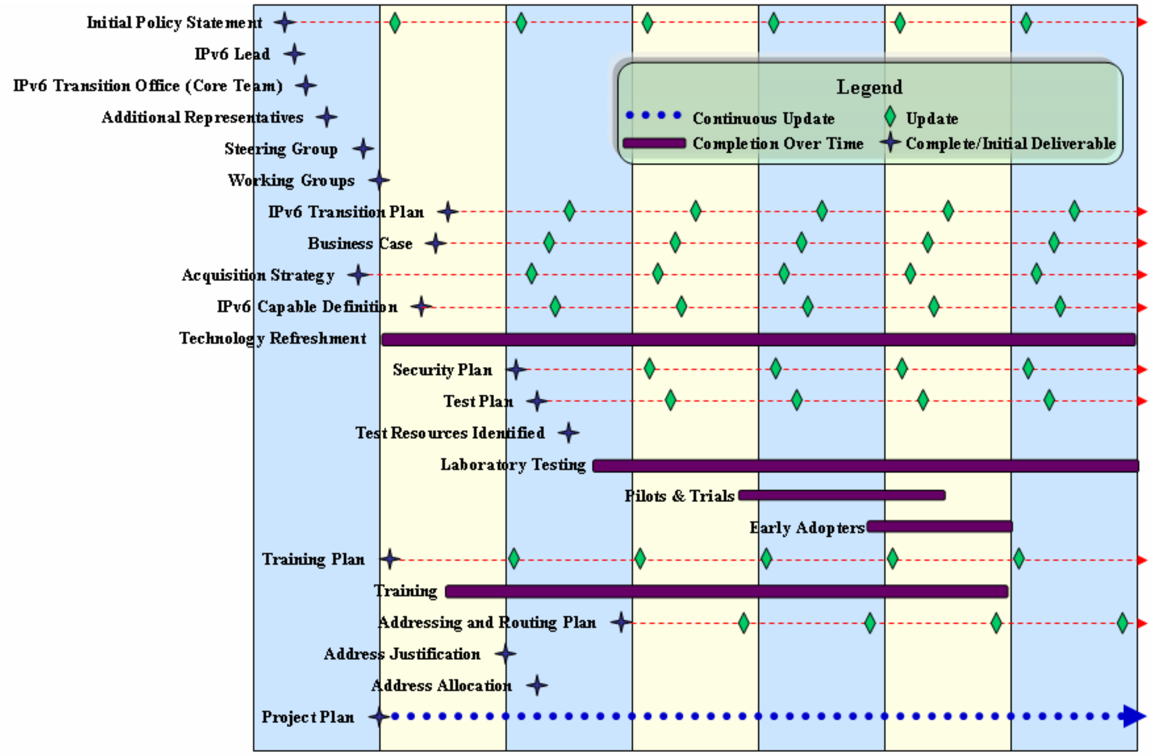


Figure 15: Notional Planning and Testing Timeline

Figure 16 shows a notional timeline for the deployment of IPv6 into the agency's enterprise. The sequencing plan used in this example is based on a core-out approach and utilizes a phased deployment of enterprise elements.

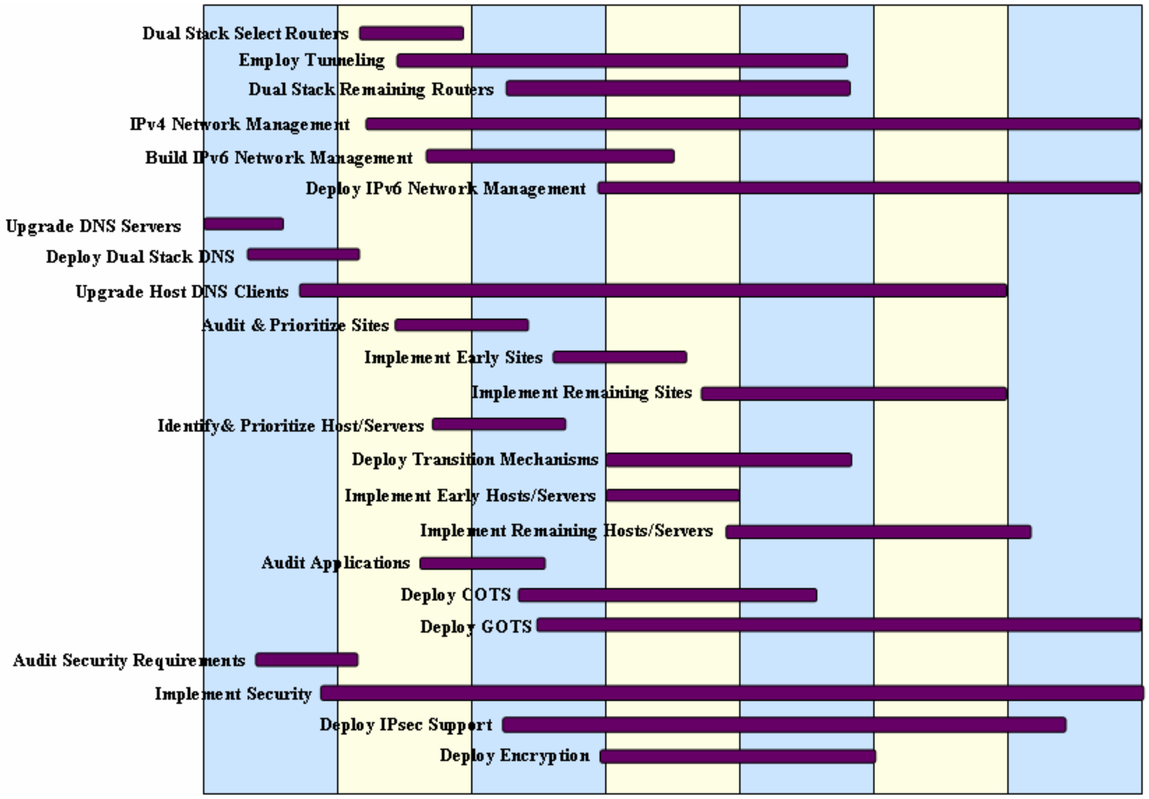


Figure 16: Notional Enterprise Deployment Approach

4.2 Testing

Testing is a critical activity when introducing any new components or software into the enterprise and is even more important when implementing a technology insertion of the size and scope of IPv6. The majority of organizations that have transitioned to IPv6 have been able to avert potentially significant operational issues through a solid test program. Many early IPv6 adopters view themselves in a positive light with helping the overall industry transition as they have identified and helped correct several problems in various vendor products.

> ***Test everything. Leverage significant testing for each phase of the deployment prior to implementing in operational environments. Most potential impacts can be identified and avoided with proper testing.***

Several test methodologies exist and should be utilized by the agency prior to fully deploying IPv6 including:

- **Conformance:** Testing of an element in isolation based on a set of standard specifications for protocols, hardware and software.

- **Interoperability:** Testing to determine if the hardware and software interact properly with other elements within the enterprise and interconnected networks.

- **Performance:** Testing the hardware and software performance based on a set of stress criteria.

- **Functional:** Testing the functionality of the hardware and software in an operational-like environment based on a set of system requirements.

- **Operational testing:** Testing the hardware and software in limited operational settings such as pilots and field trials.

> ***Utilize the definition your agency employs for "IPv6-capable" to define conformance test suites. Work with other agencies and commercial industry to develop industry accepted testing based on government requirements.***

Interoperability is not automatic in any situation (IPv4⇔IPv4, IPv6⇔IPv6 or IPv4⇔IPv6). Standards help but do not guarantee interoperability. Most standards have options that may or may not be widely implemented and many vendors insert proprietary add-ons to try and differentiate themselves. It is important to know that IPv4 and IPv6 are not directly interoperable. Overall enterprise interoperability must be accomplished through various means during the transition process such as transition mechanisms, but careful planning and execution should allow for desired interoperability during the transitional timeframe.

> ***Work closely with vendors to identify bugs even before they get into your test lab. Many vendors have identified issues and may have fixes ready if they speak to their development teams. Keep your vendor close throughout the testing process to make sure any problems are reported and patched quickly.***

Agencies should have access to one or more IPv6 test beds. Initially, a simple laboratory environment will be sufficient to begin individual product testing, but a test network should be planned in the future to provide a better simulated environment.

> ***Leverage IPv6 test bed support from other agencies, vendors and contractors. Budget can be saved by sharing test resources. Connect multiple IPv6 test labs together to create an IPv6 test network.***

Each agency should develop a test plan that includes all planning and execution associated with testing. At a minimum the test plan should include:

- Test strategy
  - What will (or will not) be tested and why
  - Internal versus external usage
  - Industry-based or agency-based

    - Overall testing timeframes
- Testing methods
    - Conformance, interoperability, performance, other
- Types of testing
    - Analysis, modeling & simulation, lab, pilots, proof of concept, early adopters
- Test Prioritization and synchronization
    - Which testing is the highest priority
    - Does testing have to occur in certain order
    - Linking testing with availability of products and capabilities
- Testing schedule
    - Detailed schedule of when tests will be performed and results expected
- Test reporting requirements
    - What type of reporting will be required
    - Mandatory or voluntary

Each agency should also develop an IPv6 Transition Testing Matrix as part of the overall test effort. The testing matrix will help identify the overall scope of the testing required, the methods and environments for the testing and who will perform the tests. Figure 17 shows a small snapshot of a notional test matrix at a high level. In the example, high level test requirements are shown for the rows and test types/environment are shown for the columns. Test requirements should be agency-specific and broken into specific detail. Test environments show what type of testing is required and may use one or more of the test methodologies discussed above. The next step is indicated in each of the cells and includes the resources that will be utilized to perform the testing. Do not limit resource identification to those within the agency; instead, utilize results from other agencies, the DoD and industry to help complete the matrix.

		Test Environments						
		Analysis (paper)	Modeling and Simulation	Laboratory Testing	Formal Test Facilities	Field Trial	Pilots	Early Adopters
IPv6 Test Requirements	**IPv6 Base**							
	Header							
	Extension Headers							
	Packet Size (MTU)							
	Unicast IP address							
	Special Unicast Addresses							
	Prefix							
	Multicast Addresses							
	Multicast Listener Discovery (MLD)							
	Anycast Address							
	Stateless Auto Configuration							
	Neighbor Discovery							
	Neighbor Discovery Messages							
	Path MTU Discovery							
	UDP							
	Default Selection for IPv6							
	Link Layer-Ethernet							
	Link Layer-PPP							
	Link Layer-Frame Relay							
	Link efficiency							
	Transition Mechanisms							
	Applications and Services							
	Operations							
	Network Management							
	Control Plane							
	Mobility							
	Information Assurance (IA)							

Figure 17: Test Matrix Example

Once the test matrix has been developed, utilize testing from outside resources to complete it. If another agency or vendor has already performed the tests you identified, and they meet your requirements, leverage their results. This will save significant time and resources than can be utilized elsewhere.

Partner with other agencies and have each concentrate on different aspects of the test matrix. There is likely to be a large degree of overlap, and sharing resources and results will be advantageous.

4.3 Address and Routing

Over the past decade, significant work and diligence from the stewards of the IP address space have prevented IPv4 address depletion through various policy and enforcement mechanisms. However, during a recent workshop, a representative from ARIN presented the "Internet Number Resource Status Report As of 30 June 2005". The report was prepared by the regional Internet registries including African Network Information Center (AFRINIC), Asia Pacific Network Information Centre (APNIC), ARIN, Latin American and Caribbean Internet Address Registry (LACNIC) and RIPE Network

Coordination Centre (RIPE NCC). Figure 18 shows the current allocation of IPv4 address space.

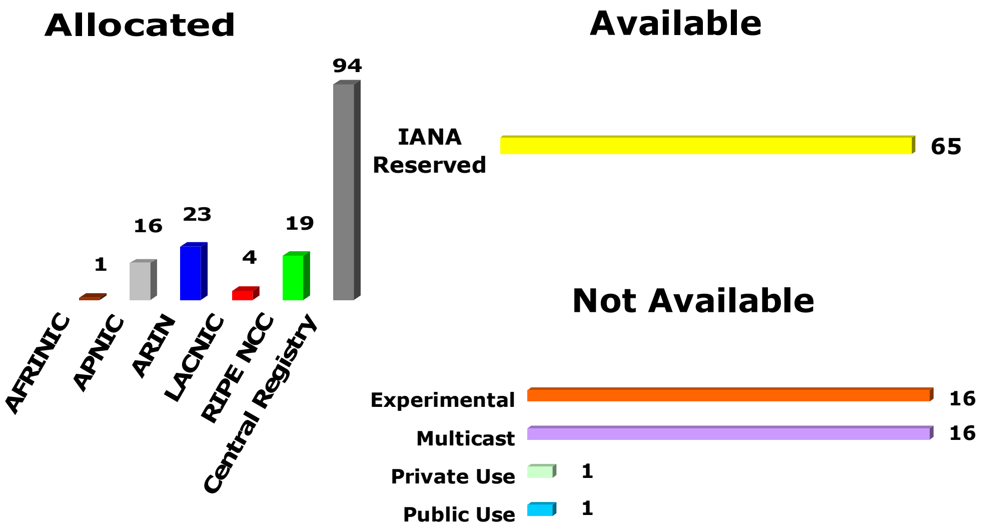


Figure 18: Current IPv4 Address Space Allocation[4]

Figure 19 shows the allocation trends since 1999 of Classless Inter-Domain Routing (CIDR) /8s by regional registry; note that the 2005 data was only for the six months ending in June, 2005. The number of /8s allocated shown are new allocations each year and are not cumulative.

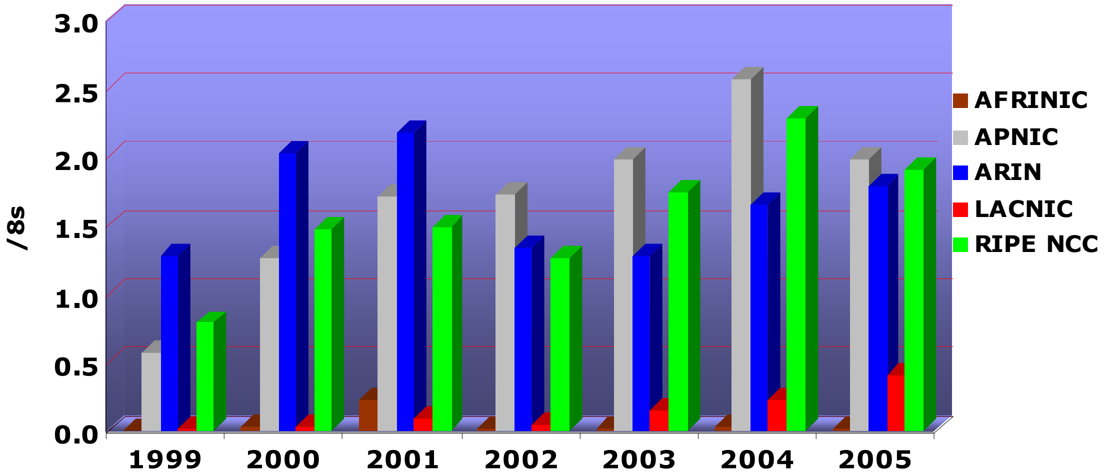


Figure 19: IPv4 CIDR /8 Allocations per Year[5]

[4] Federal CIO IPv6 Transition Planning Workshop 11 October 2005, ARIN Registry Update, IPv6 Addresses and Present IPv4 Allocation, Presentation by Richard Jimmerson, Director of External Relations for ARIN

[5] Federal CIO IPv6 Transition Planning Workshop 11 October 2005, ARIN Registry Update, IPv6 Addresses and Present IPv4 Allocation, Presentation by Richard Jimmerson, Director of External Relations for ARIN

Using the information in the allocation table, Figure 20 was created to show potential IPv4 address space exhaustion dates based on steady-state allocations of IPv4 address space and continued growth of address allocation based on the past four year growth rates. During the workshop, ARIN noted that there is concern regarding the amount of remaining IPv4 address space and believe additional actions would be required immediately.

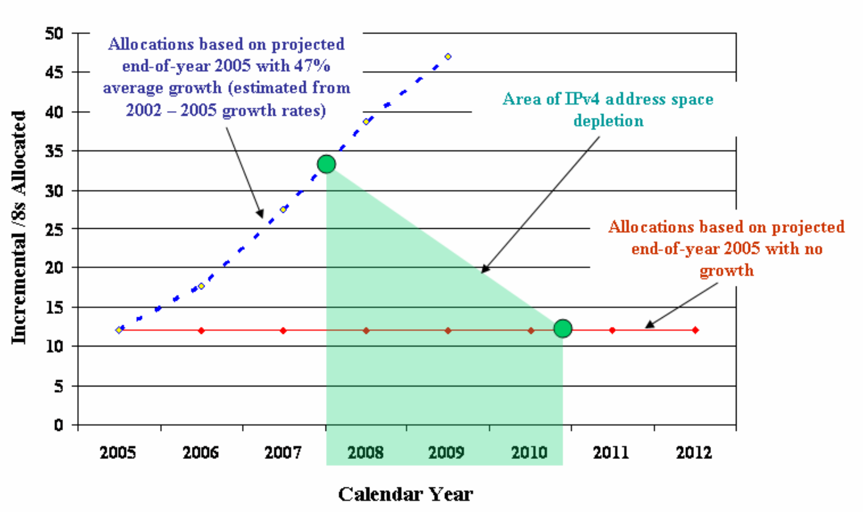


Figure 20: Estimated Timeframe for Address Depletion

Although Federal agencies may not have a short term concern based on their current IPv4 address allocation pool, given the continued exponential growth of IP-enabled devices, lack of available IPv4 address space will continue to drive solutions such as the quickened migration to IPv6.

One significant impact on Federal agencies is the continued expansion of e-government and the continued growth of Internet communications to interface with public and private entities, including citizens. Future electronic communications requirements may be impacted if IP address resources are depleted. While most American households are still dial-up users, the continued move toward broadband will consume many IP addresses as fixed addresses are needed.

Understand and plan for IPv4 address depletion. It will occur in the near future and may negatively impact agencies in one form or another. With more peer-to-peer applications beginning to appear, globally routed addresses will become an increasing requirement.

The development of an IPv6 addressing and routing plan is critical to achieve the agency's overall vision for IPv6. IPv6 addressing is intended to be very hierarchical in nature and focus on maximizing the performance of the core networks.

Agencies may develop multiple IPv6 addressing plans over time and may have more than one implemented simultaneously.

The addressing and routing plan should cover at a minimum:

- Agency requirements that drive addressing and routing decisions
- Addressing and routing requirements
- Addressing and routing policies
- Addressing and routing architectures
- IPv6 address space requirements and justification
- IPv6 address distribution
- Address management and reporting
  - Address and routing architectures and structures

Typical initial allocations from the ARIN is a /32 with each site (sub-netable entity) typically being allocated a /48.

The definition of a site is open to interpretation and the agency should make the broadest interpretation possible to ensure maximum address allocation. It is not unreasonable to assume that each Federal employee, vehicle, building, etc. be included as a site.

During the process to identify and apply for the agency's IPv6 address allocation requirements, it is recommended that a 50-year view be taken and that a request to reserve a much larger address space than the initial allocation is included in the ARIN submission, based on specific agency requirements.

This will allow the agency to grow over time without having to change its network prefix. It is important to note that a significant difference in IPv6 from IPv4 is that network interfaces may have multiple IP addresses in IPv6. It is conceivable that each interface could require multiple addresses based on factors such as classification level, redundancy, community of interest, geospatial coding, etc. Another important factor to consider is how the lower /64 bits of address space will be identified if using auto-configuration. As a general rule, the high order 64 bits will identify the network (where am I?) bits and the low-order 64 bits will identify the host (who am I?) bits. Several techniques exist or are in development to utilize the 128 bits of an IPv6 address. For interoperability and policy purposes, it is important the agency understands and develops a methodology for IPv6 address use.

4.4 Network Solutions

The transition of the enterprise to IPv6 is more than simply taking the current IPv4 architecture and inserting IPv6. In order to take advantage of the benefits associated with

IPv6, each Federal agency will need to determine its visionary architecture that it will move to over the longer term and then plan the transition in steps over a 10-20 year period to reach it. In order to support advanced mobility, multicasting and end-to-end services the agency's architecture may radically change, but this will not occur immediately. During the transition process, each portion of the network must transition in a coordinated manner to ensure proper operation and continuing support for the user base. In addition to the network elements that must transition such as the backbone, hosts, servers and security devices, other elements such as DNS, routing and addressing must evolve to meet the new requirements. Federal agencies should develop a Network Transition Plan that at a minimum includes:

- Target architecture
  - IPv6 architecture being targeted once transition is complete
- What needs to be transitioned
  - Detailed description of the network elements and systems that need to transition
- Transition requirements
  - Critical requirements during the transition (performance, interoperability, timeframes, etc.)
  - Milestone and date targets
- Transition mechanisms
  - Which will be used and where
- Network transition strategy
  - Edge-core, core-edge, by subnet, by geography, combination
- Network element impacts
  - Equipment used in the network
  - Upgrade requirements for equipment (upgrade/replace)
  - Will equipment/functions remain or be phased out
  - Network management capabilities (could become a plan on its own)

One of the most critical lessons learned from many organizations during their transition process was to have configuration control of the operating systems and applications on their networks. Organizations that had numerous release versions of operating systems and applications in use had a much greater challenge in testing and implementing IPv6 than those with tight configuration control policies and quick release cycles. The general rule of thumb is that the newer the system or application, the better the support for IPv6.

Plan the activation of IPv6 for network elements in conjunction with new releases.

A perfect example of this is with Microsoft's pending release of Vista™. Vista has significant IPv6 capabilities bundled into it that will make the transition of workstations, servers and Microsoft based applications much simpler. This approach can also be taken with upgrading the operating systems on routers or the version of the database that is in use within the agency.

For systems and software that are in or will soon be in procurement, specify the agency's criteria for upgrading those systems and applications as IPv6 capabilities become available.

Plan to upgrade systems to the latest releases to obtain maximum IPv6 functionality and reduce potential impact.

Core network infrastructure upgrades must be planned and deployed with new routing protocols and addressing plans. Networking equipment should be upgraded through technology refreshment cycles. Selected routers should be implemented with dual stack IPv6 and IPv4 capabilities initially. Tunneling IPv6 over the remaining IPv4 core network can be utilized to provide IPv6 capabilities to the remainder of the enterprise networks. Eventually all routers should be transitioned to dual stack capabilities, but this can occur over a longer period of time based on testing and equipment availability. When available, utilize Multi Protocol Label Switching (MPLS) over an IPv4 core to reduce the initial complexity in the transition and allow for the gradual introduction of IPv6.

Deploy IPv6 on a limited number of routers to start. This provides a manageable test scenario in an operational environment to gain experience.

Use tunneling to extend the reach of IPv6 across the enterprise and allow for a measured approach to upgrading the remainder of the routing core.

The general approach advocated within the DoD is to deploy dual-stack systems to help perpetuate interoperability and allow for an extended coexistence period if necessary. Several groups are reviewing the approach, particularly in mobile tactical environments where size, weight and power are critical. There is a question whether the additional requirements to support dual-stack on small handheld equipment will be an issue. Federal agencies with requirements for small, highly portable devices may face the same challenges.

Utilize a phased approach to implementing IPv6 at agency sites. Sites should be audited and prioritized for rollout based on technical capability, available funding, existing planned upgrades and backbone connectivity. It is important to identify "friendly" early adopter sites to test and refine the deployment processes. Providing ample training to sites prior to the activation of IPv6 will help reduce negative impacts. It is also important to upgrade host and server operating systems to the latest version to ensure maximum support for IPv6. Transition mechanisms (tunneling/translation) can be used for a site or select users at the site to support native IPv6 environments until the remainder of the enterprise can transition. Firewalls are a natural point to implement translation or tunneling in the architecture as shown in Figure 21. Host administration tools need to be upgraded for IPv6. DNS, Network Time Protocol (NTP), and other key network enterprise servers must be upgraded to IPv6 versions. Servers for new IPv6-only mobility and other advanced services may be deployed.

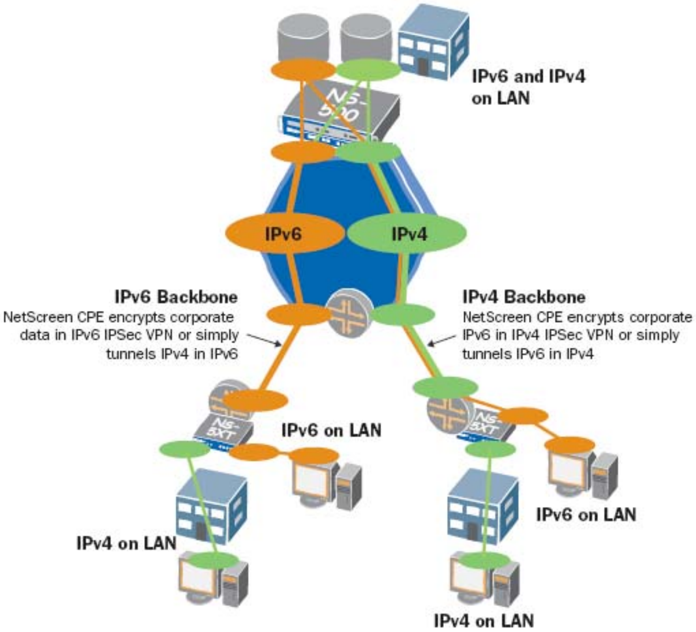

IPv6 and IPv4
on LAN
NS-500
IPv6
IPv4
IPv6 Backbone
NetScreen CPE encrypts corporate data in IPv6 IPSec VPN or simply tunnels IPv4 in IPv6
IPv4 Backbone
NetScreen CPE encrypts corporate IPv6 in IPv4 IPSec VPN or simply tunnels IPv6 in IPv4
NS-5XT
IPv6 on LAN
NS-5XT
IPv6 on LAN
IPv4 on LAN
IPv4 on LAN

Figure 21: Example of Using a Firewall to Tunnel[6]

> ***Identify and use "friendly" early adopters throughout the transition process. This will allow for the maximum cooperation in testing and honing the deployment processes and limit headaches.***

DNS is a critical service for name/number resolution and reverse lookups and is a requirement for many networks. It will also be critical to support certain testing, particularly pilots and early adopters.

> ***The deployment of IPv6-capable DNS services should be one of the first infrastructure elements that transitions in the overall deployment plan.***

DNS should be upgraded to Berkeley Internet Name Domain (BIND) version 9 or higher to support IPv6 AAAA records, DNS Security (DNSsec), Secret Key Transaction Authentication for DNS, and other new features. Agencies will need to audit the types and versions of DNS resolvers used by hosts and test their ability to support IPv6. Early local IPv6 deployment can use a local, IPv6-capable DNS server, but inter-domain routing within an agency will require the hierarchical DNS infrastructure to be transitioned. In order to perform inter-domain routing between agencies, the .GOV domain will require IPv6-capable DNS.

[6] Juniper Networks Enables a Secure and Assured Transition to Internet Protocol Version 6 (IPv6) in the Federal government. Solutions Brief, Juniper Networks, Inc.

Dual stack DNS services (one system for both IPv4 and IPv6) should be utilized if enterprise DNS clients support IPv6. The use of a DNS that supports both IPv4 and IPv6 clients will be much easier to manage and maintain.

Consider a dual DNS approach (separate DNS for IPv4 and IPv6) to reduce operational impacts if a large number of older DNS clients exists that do not support IPv6. This will be much more difficult to manage, but could reduce operational impact in the short term.

4.5 Application Solutions

Organizations have not implemented a large number of IPv6-capable applications. The general rule has been that commercial IPv6 equipment is generally available to support the routing infrastructure and the operating system on hosts and servers; however, most implementations have occurred in dual-stack environments and the majority of applications and network management capabilities are still leveraging the IPv4 solutions that were in use prior to the deployment of IPv6. Microsoft has already released a Beta version of Vista, which will default to IPv6, and plans commercial release for the end-user operating system in 2006 with releases of server operating systems and applications from 2006 – 2008. Oracle and other major software providers have announced their IPv6 support strategies in order to remain compliant with the increasing number of nations requiring IPv6 compatibility in their COTS purchases. During the application transition process, agencies need to include the potential movement to end-to-end and peer-to-peer applications and functionality. Future applications will need additional control and will perform multiple functions beyond simple client/server functionality. Applications will also provide control signals for network services, such as QoS, priority and preemption, and policy-based networking.

Applications must be made IPv6-capable and should be optimized to take advantage of IPv6-only network features like enhanced multicasting, anycast, and embedded IP security (IPsec). Application development environments need new IPv6 libraries and APIs so developers can access IPv6 networking features. Applications need to be audited to determine the level of existing support for IPv6 and the scope of work required for the transition. COTS applications will most likely transition first with government Off the Shelf (GOTS) application following over a longer period of time.

Agencies should work closely with application vendors to leverage testing and fixes they have already developed and request vendors to test based on agency requirements.

The availability of government developed equipment and applications will probably be one of the most complex and expensive obstacles in the transition to IPv6.

> ***Depending on where GOTS products are in a technology life cycle, consider phasing out existing GOTS platforms in favor of new ones during an IPv6 transition period as a part of a normal technology refreshment cycle.***

In these cases, separate budgeting for the legacy system to transition to IPv6 need not be identified as they would be phased out. Whenever possible, applications should be upgraded to provide dual-stack support and utilize standard API calls if available.

> ***Significant time and effort can be saved through the use of code scanning tools to identify potential lines of code that must be modified.***

Each agency should develop an Application Transition Plan that, at a minimum, should include:

- Application requirements
    - Application functionality requirements
    - Use of standardized APIs
    - IPv6 capability requirements
    - Dual use (IPv4 & IPv6) or single use (IPv4 or IPv6)
    - IPv6-capable transition requirements
- Transition approach
    - One set of applications that support both IPv4 & IPv6
    - Separate applications running in native IPv4 or IPv6 mode
    - Timing of application transition with network transition
- Application audit & analysis
    - Identify all applications in use within the agency today
    - Determine if they are impacted
    - Identify method of transition
- Application Transition Resources
    - Who will modify the application
        - COTS product (vendor responsibility)
        - Contractor
        - Internal
    - Budget considerations
    - Prioritization versus other upgrades and patches
    - Rolling in new versions of software
- Support for legacy applications
    - Length of time they will be supported
    - Transition mechanisms to be used to extend life

4.6 Security Solutions

The general view today is that users on the corporate intranet are considered trustworthy while users on the Internet are not, as shown in Figure 21. Most network and security administrators know this philosophy is not true, but given the complexity of their networks and a lack of widely deployed network security protocols and tools, security architectures reflect this simplified philosophy. Boundaries are deployed around the enterprise network creating an enclave with a firewall acting as the gate through which all traffic must pass. Unfortunately, this leaves the majority of the enterprise's internal resources vulnerable as it is not always possible to close off all "back doors" into the network and from attacks originating within the network.

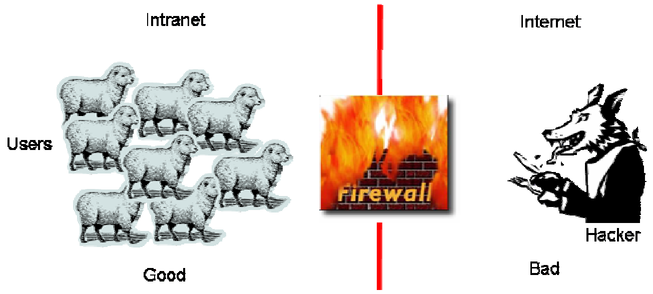


Figure 22: Current View of Security

A more realistic view of network security, shown in Figure 22, includes the need to worry about the vulnerability of resources within the enterprise's enclave due to internal malicious users as well as from outside network connections. In many cases, robust security capabilities are not implemented on enterprise networks due to excessive complexity, cost and management requirements. In the mix, it is sometimes forgotten that the Internet not only contains hackers but also customers and remote employees that need to connect to corporate resources. Generally thought of as a "corporate" responsibility, users view security as someone else's concern and a necessary evil and has grown into an "us-versus-them" mentality. Security is seen as a way to stop something from occurring – even advances in technology or work the company needs to accomplish, which may lead users to attempt to circumvent security policy to complete their work. This is not necessarily done with malicious intent, but rather from a lack of understanding or a disconnect in the way security policy is developed.

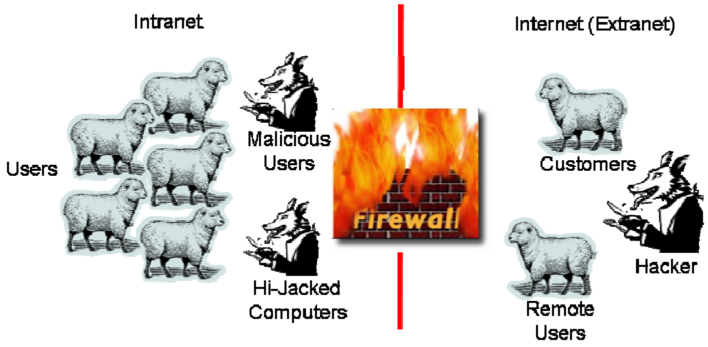


Figure 23: Realistic View of Security

Transmission Control Protocol (TCP)/IP was originally developed to operate over protected networks where physical and link layer security techniques were used. Eventually, the needs for higher layer security services were identified, primarily at the

IP layer and the application layer. Many work-a-rounds have been developed to deliver the desired security functionality such as virtual private networks (VPNs), firewalls, gateways, etc. Unfortunately, these devices typically break the end-to-end connectivity model, making the networks more complex, harder to manage, more expensive and more difficult to roll out new applications upon. Security has traditionally been an afterthought in the network development and deployment cycle and has been implemented from an enclave-to-enclave point-of-view.

As the New Internet continues to unfold with the rapid deployment of IPv6, security must be in the forefront to support the advanced capabilities that will quickly follow. Next generation networks will offer significant increases in capabilities over the functionality of the current Internet, and applications will evolve and become more complex. Security for next generation networks:

- Must be built-in from the start
- Cannot be redesigned based on every new application
- Should provide a foundation to develop security applications and service offerings

Plan for security at the beginning of the transition. Don't make it an add-on or afterthought. Not incorporating security considerations in the early part of the process will impact cost and functionality.

Some of the advanced capabilities that must be considered when developing security for the New Internet include:

- End-to-end connectivity
- Multi-level security (MLS)
- Mobility
- Convergence

New security architectures are required to support end-to-end communications. End-to-end connectivity is a significant requirement for the New Internet to handle the large number of peer-to-peer applications and services that will become prevalent over the next decade. Nodes will need to connect directly to each other without breaks from devices such as Network Address Translators (NATs). Current security devices such as firewalls, VPNs and intrusion detection systems (IDS) will continue to be used, but in ways that do not break end-to-end connectivity.

IPv6 can provide better functionality than NATs under IPv4 for security and hiding network users and topology.

NATs increase the cost to operate and maintain networks. They also utilize additional resources when building applications that must account for them in the network. Removing NATs can save resources.

MLS is a core requirement within the U.S. Federal government, particularly the DoD. Traditionally, networks which run at different levels of classification are physically separated and operated independently from each other. This leads to greatly increased costs and complexity to operate numerous networks and at times requires three or more workstations on a single individual's desk. One major initiative in the DoD is to develop a "black core" in which all data will be encrypted and put onto one unclassified network. Although this is only the first step to true MLS, it will significantly reduce the required costs and resources and provide for the foundation to move to a true MLS capability.

Mobility, shown in Figure 23, is of significant importance in the New Internet and security plays a vital role. The ability to not drop connection while moving at high speeds through heterogeneous networks is necessary. Mobile voice over IP (VoIP) will increasingly become more popular not only with end users but also with carriers for delivering traditional and advanced wireless capabilities. In addition to node-based mobility, network mobility is also playing a key role in the New Internet. Many Federal agencies require the ability to move entire networks and remain operational. This type of capability is critical in responding to disasters such as the destruction caused by Hurricane Katrina and terrorist incidents such as 9-11. Security will play a critical role in not only protecting the communications but also providing network level authentication to support users accessing the networks and associated assets.

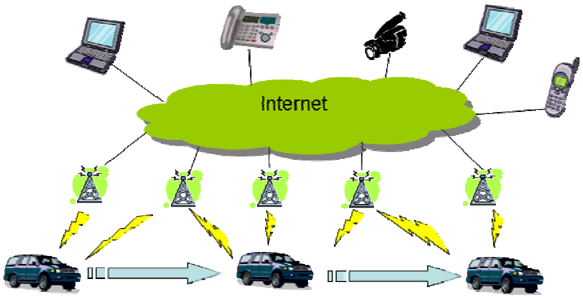


Figure 24: IPv6 Host Mobility

Convergence, also known as EoIP and shown in Figure 24, is the combination of voice, video and data onto a single IP network and is one of the primary drivers of the New Internet. Given the extensive use of NATs, lack of available IP addresses and inability to support sophisticated QoS requirements, the existing Internet cannot provide for true IP convergence. Developing efficient and effective security is essential. Security will play a significant role by taking policy from three distinct areas and merging them onto a single delivery platform.

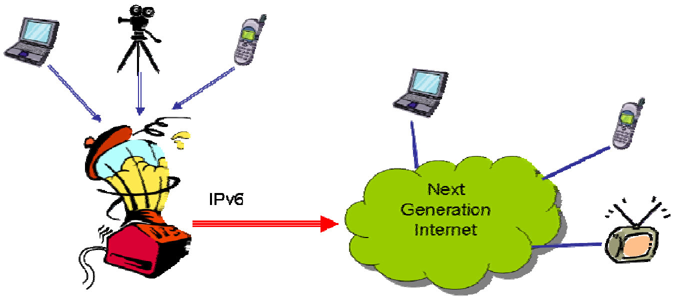


Figure 25: Convergence or EoIP

Security has been thought of and built-into IPv6 from the very beginning, and although it is not perfect, it is better than what we have today and it is still evolving. IP-based security provides the foundation from which to build enterprise security solutions; however, everything cannot be done at the IP layer. Security must be based on overall policy, requirements and involve all aspects of the enterprise.

IPv6 is here today and is included in most routers, operating systems and in some applications. Many enterprises are not aware to what extent IPv6 is included in their existing equipment and fail to plan for it. This could become a security risk if not understood by network administrators and can associate IPv6 with higher levels of risk due to lack of knowledge.

The transition to IPv6 will occur over a number of years where both IPv4 and IPv6 will be present in most enterprises. Given that the security architecture that enables many of the new capabilities in IPv6 to support the New Internet will differ from the existing security architecture, developing a security model during the period of overlap will take careful planning and testing. Today, enterprise security is primarily Enclave based and centrally administrated. Tomorrow, security will need to be moved toward the hosts and be integrated with policy-based networking.

Security during the period of co-existence of IPv4 and IPv6 may look very different from future IPv6 security architectures. Agencies should plan to evolve the security architecture throughout the transition process.

Key management has been a challenge associated with almost every form of encryption deployed. In many instances, encryption keys are provided via out-of-band techniques. This means that they are not automatically established through the network, but through another means that is typically not automated. One of the visions for the New Internet is to be able to support large numbers of remote devices, such as sensors, which will require automated key management techniques.

Although a version of IP security exists for the New Internet, several efforts have been established to modify the protocols based on a particular national view. One national view is that users should be completely anonymous and all traces associated with IP usage should be untraceable. Another national view is that all actions by users should be monitored and traced to conform to national Internet usage policy. Over the next few years, the nations and organizations that focus on developing and deploying the New Internet and the associated security protocols will be in a position to lead and decide how security is performed.

One of the major constraints identified in the transition to IPv6 today has been the security architecture and availability of approved security products from industry. Many of the capabilities and functionalities desired in IPv6 move networks away from a domain-to-domain based model and towards an end-to-end model. The difficulty that is transpiring within certain organizations is how to support this changing model and still provide enclave level protection through devices such as firewalls that traditionally break the end-to-end model. Security planners are also grappling with the transition to not just one other security architecture, but two, as there will most likely be a significant difference in the architecture supported during the transition period and when IPv6 is the dominant protocol. Security devices, particularly firewalls and IDS, have not been available until recently. A number of vendors have announced support for IPv6, but testing and verification of the devices are still under way in most organizations.

Work closely with security vendors to understand proper formatting of IPv6 rules and filters for routers and firewalls from both a security and performance perspective.

A significant challenge will arise in the development and availability of IPv6-capable encryption devices. In addition to commercial encryption considerations, various Federal agencies may need to consider stronger, military-grade encryption systems that may not always interoperate with IPv6.

Government-developed and -approved encryptors may not be IPv6 compatible. Look into these requirements early as these systems generally take a long period of time to update.

Offload encryption processing to a separate hardware card/device to prevent performance impact.

The challenges associated with planning and developing the security architectures will be complex. An IPv6 security policy and architecture should be developed and deployed prior to the adoption of IPv6 in any enterprise. Audit existing equipment and applications to determine what level of IPv6 capability exists currently within the enterprise and develop a security policy/plan to deal with vulnerabilities prior to transition. Firewalls, IDS, security auditing tools, network encryptors, and VPNs may need to be upgraded or replaced to secure IPv6 networks. IPv6 requirements for mandatory IPsec offer an opportunity create a more secure end-to-end environment for users if proper IPsec support is deployed. Enterprise networks need a Public Key Infrastructure (PKI) to distribute and manage IPsec keys used for authentication and encryption. This infrastructure may be deployed internally or enterprises may rely on third party PKI service providers.

Utilize IPsec authentication and integrity features in the short term to provide additional security, but do not break IPv4-based security architectures need for deep packet inspection and virus scanning from gateway firewalls.

A security transition plan should be developed and at a minimum include:

- Threats, Vulnerabilities and Risks
    - Covers threats to IP based network
        - Primarily same as IPv4
        - New threats may be identified as IPv6 deployed in new areas (wireless, etc.)
    - Identify vulnerabilities associated with IPv6 (existing in IPv6 and unique to IPv6)
        - Associate vulnerabilities to specific environments and capabilities where appropriate
    - Risks
        - Likelihood of attacks succeeding and potential impact
- Mitigation and management techniques
    - How can risks be mitigated (technical, procedural, other)
- Recommended approaches
    - Recommended course of action to enhance the security posture
- Policy
    - Recommended security policies relating to IPv6 within the agency
- Security Tools
    - What tools are available and should be used
- Certification & Accreditation (C&A)
    - What C&A procedures are required, when and where

4.7 Network Management Solutions

Network management has been one of the weakest areas identified in the deployment of IPv6; however, the deployment of IPv6 has primarily occurred on existing network infrastructures through the use of dual-stack techniques or tunneling. Thus, the demand for IPv6-only network management solutions has been very negligible. It is very unlikely that multiple network management systems will be utilized for managing IPv4 and IPv6; it is much more likely that existing network management tools will evolve to include support for IPv6. The network management solution for IPv6 will need to be included in the current management approach. Implementations will include Simple Network Management Protocol (SNMP) with the appropriate Management Information Bases (MIBs) deployed in hardware and instrumentation.

> ***Utilize IPv4 network management tools and supplement with IPv6 specific requirements until the industry provides more robust IPv6 network management capabilities.***

Network management systems should be upgraded for IPv6 over Internet Control Message Protocol version 6 (ICMPv6) and be loaded with new IPv6 ICMP MIBs. Tools for designing networks and analyzing network performance need to be updated for IPv6. Normal administrative tools such as Syslog and Telnet/Secure Shell (SSH) should be supported over IPv6. IPv6 based management should be phased in over time as existing network management tools are upgraded to support IPv6 and IPv6 MIBs are better defined. As the deployment of advanced IPv6 capabilities begin, network management systems will play a greater role in policy based networking and QoS.

> ***Plan to build customized scripts to support the IPv6 management in the near-term.***

4.8 Training

Training and education has been identified as a significant element of the planning and deployment process for IPv6. The development of a training plan should be included as a part of every agency's transition planning efforts. Many of the transition teams take on the role of training to provide supplemental expertise to existing training methods. One of the most significant challenges faced in the roll-out of IPv6 at many organizations was the lack of understanding and experience deploying IPv6. To help alleviate this problem, many organizations formed training and education working groups that utilized several techniques such as workshops and seminars to train the technical staff and also published deployment guides and papers on IPv6. Training should not be limited to only technical staff but should include everybody in the transition process, especially decision makers.

> ***Brown bag sessions and other informal training events are a great way to provide education and training to a wide number of staff members. Training on cutting edge technology, important programs and changes to the organization always peak interests and generate great turn-outs. The training topics should be varied and come from a variety of sources, including vendors working in the IPv6 industry, IPv6 efforts from programs within the agency, IPv6 efforts from other agencies, experts willing to spend an hour talking about IPv6.***

During the initial planning stages of the transition, the agency's IPv6 transition team should reach out to its community and hold kick-off sessions to set the tone for the transition. This could occur through a centralized kick-off meeting where program managers, network owners and other impacted group representatives are brought to a central location to understand what will be happening, the planned process and their overall involvement. Another method that has been effective is the use of "road shows" where the agency's IPv6 transition team travels to a limited number of locations and supports a distributed set of kick-off meetings. Throughout the transition process, the agency's IPv6 Transition Team should be called on to support a wide variety of events and training, and education should be built in where possible, including the use of:

- Centralized training sessions
- Internal or external training workshops
- Informal training such as "brown bag" seminars
- Industry conferences
- Vendor sponsored training
- Outside classroom training
- In-house training provide by experts

Two resources that have been established to help train Federal personnel are the IPv6 Summits (www.usipv6.com) held twice each year and the Federal CIO IPv6 Transition Workshops (www.v6training.com) held monthly.

Everyone within the agency will not become an expert on IPv6, but everyone should have access to someone who is very knowledgeable on IPv6 and the agency's transition plans.

Identify and develop expertise in specific individuals throughout the organization who can be the local IPv6 "evangelist" to help with the transition effort, answer questions for their colleagues and demystify the entire transition process.

IPv6 "evangelists" do not have to be technical experts but should understand IPv6 from a high level, including specific benefits, and be comfortable helping the rest of their organization understand what is happening.

Get the maximum impact out of all training material (classes, presentations, guides, white papers, etc.) by incorporating it onto a web site or portal targeted at the IPv6 transition community within your agency.

Develop training tracks targeted at the different user communities within your organizations and make them easily accessible. Make sure to capture all vendor presentations and pull in outside resources to include for reference material. Consider using streaming media tools to reach a wider base of students and make the most efficient use of instructor's time during live training events.

The development of a training plan provides the basis to identify the entire scope of the organization that needs to be trained and at a minimum should include:

- Target audience
    - Who needs to be trained?
    - Engineers, programmers, policy makers, managers, acquisition, program managers, finance, etc.

- Training material
    - What type material is required?
    - Guides, courses, certification programs, briefings
    - Technical, programmatic, other
- Delivery mechanisms
    - Existing training distribution techniques
    - External classes and training
    - Instructor led, web-based, seminar/conference based
- Training schedule
    - What training is required when?
    - Who needs to be trained when?
    - When does training material and mechanisms need to be in place?
- Training resources
    - Who will provide training?

5 Examples of IPv6 Enabled Networks

The deployment of IPv6 has not been limited to laboratory-only environments. Numerous enterprise, carrier and research networks have either launched IPv6 as a core part of their capability or are in the advanced planning stages of incorporating IPv6 into their network. IPv6 has become more than a future goal; it is being utilized today in operational networks to support customer demand. MCI is offering a free IPv6 overlay service and may begin offering native IPv6 services to customers as early as the end of 2005. Sprint supports an IPv6 offering which is an overlay (utilizing tunneling) over its IPv4 backbone. The following examples include commercial carriers that have launched IPv6 as a standard part of their service offering and an R&D networks that utilize IPv6 in their networks to support their research activities.

5.1 Global Crossing[7]

Global Crossing provides telecommunications solutions over an integrated global IP-based network. Its core network connects over 300 cities in 30 countries worldwide, and services in excess of 500 cities in 50 countries over six continents. The company offers a full range of managed data and voice products including an IP-based VPN Service and a converged IP Service that support voice, video and data. Figure 25 shows the high-level connectivity associated with Global Crossing's IP network, which is IPv6 enabled.

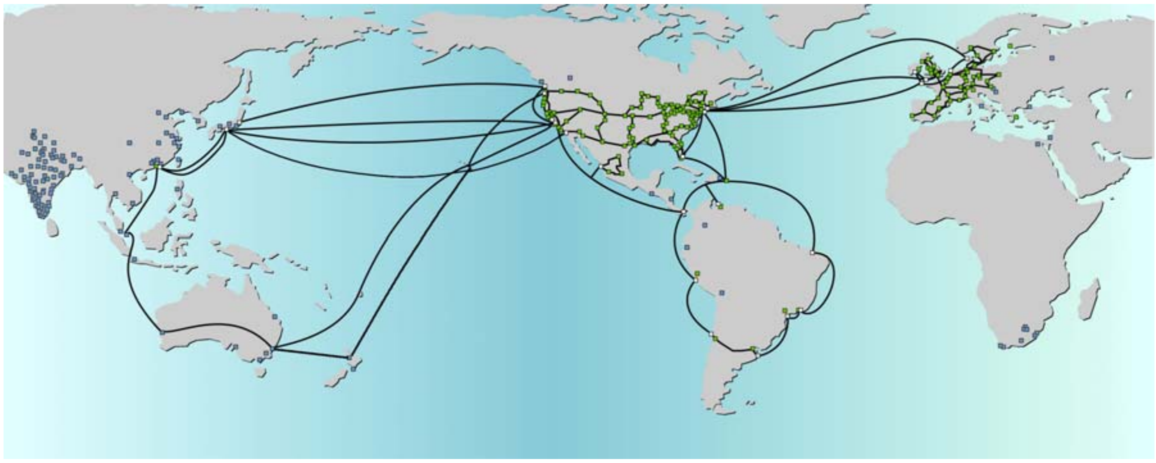


Figure 26: Global Crossing's Network Map

Global Crossing provisioned their first trial customer in 2002. Beta trials on their production network were completed in May 2005 and IPv6 has been generally available for Internet access customers since July 2005. The current DNS servers will be utilized to support both IPv4 and IPv6 name resolution. Global Crossing provides IPv6 as a basic capability of their network and does not charge a premium for IPv6 and offers the same service level agreements (SLA) on IPv6 as they do on IPv4. IPv6 features include:

[7] http://www.globalcrossing.com/xml/index.xml

- Dual-stack edge routers
- Native IPv4/IPv6 over MPLS
- IPv4/IPv6 on the same port and within the same VPN
- IPv6 addresses provided (or customers may use their own IPv6 addresses)
- IPv6 DNS delegation
- IPv6 caching servers

5.2 NTT Communications[8]

NTT is one of the largest communications companies in the world. Figure 26 shows a high-level view of NTT's network with native support for IPv6 and primary IPv6 exchange points. NTT's goal and philosophy is to offer all features and services in IPv4 and IPv6.

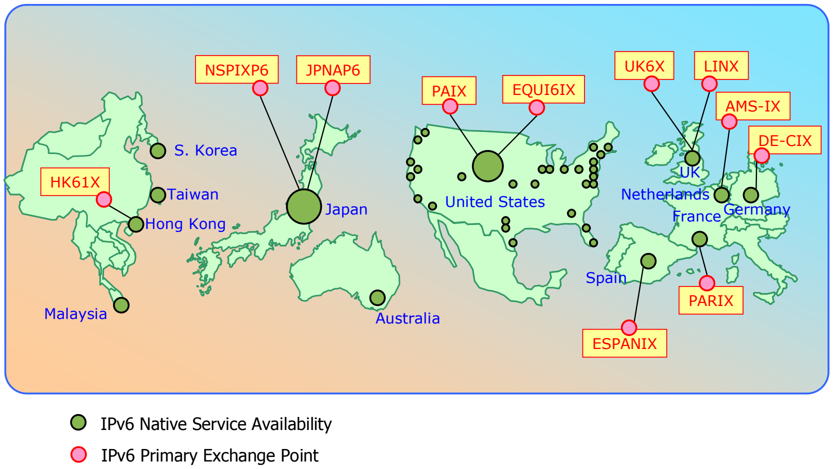


Figure 27: NTT IPv6 Network

In the fourth quarter of 2003 NTT's global backbone was upgraded to dual stack, and in December, 2003 three types of IPv6 service were offered on a commercial basis:

- Native IPv6 (available at every point of presence)
- Manually configured IPv6 over IPv4 tunneling
- Dual stack IPv4/IPv6

In June, 2004 NTT provided additional service offerings with a "Phase II" release which added IPv6 support for:

- N x T1 connections
- Frame relay
- Managed router service
- Shadow support for TDM and ethernet
- Advanced DNS support

[8] http://www.ntt.net/

5.3 Internet2[9]

Internet2 is a consortium of over 240 university, government, and industry partners developing and deploying a leading-edge national research network and developing revolutionary Internet applications with the goal of accelerating the creation of a next-generation Internet. Internet2 is a test bed for advanced network applications and services, including IPv6, differentiated QoS, multicast, measurement, and security, which are not available on the production Internet. Internet2 runs the Abilene OC-192 (10 Gbps) optical transport backbone shown in Figure 27 that links Internet2's 220 university, corporate, and affiliate members in all 50 states, the District of Columbia, and Puerto Rico. The Abilene backbone connects regional network aggregation points, called GigaPoPs, to provide service to Internet2 universities and partners as they develop advanced Internet applications.

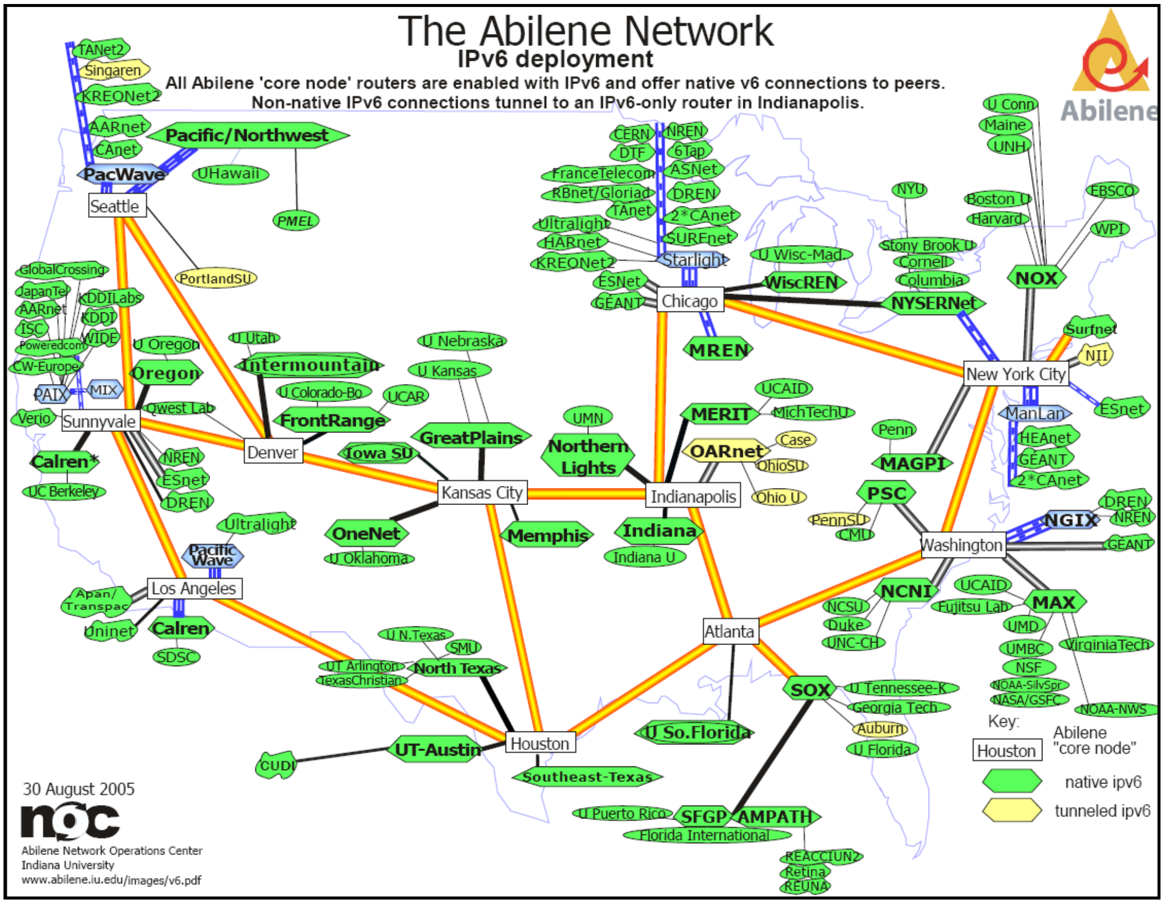
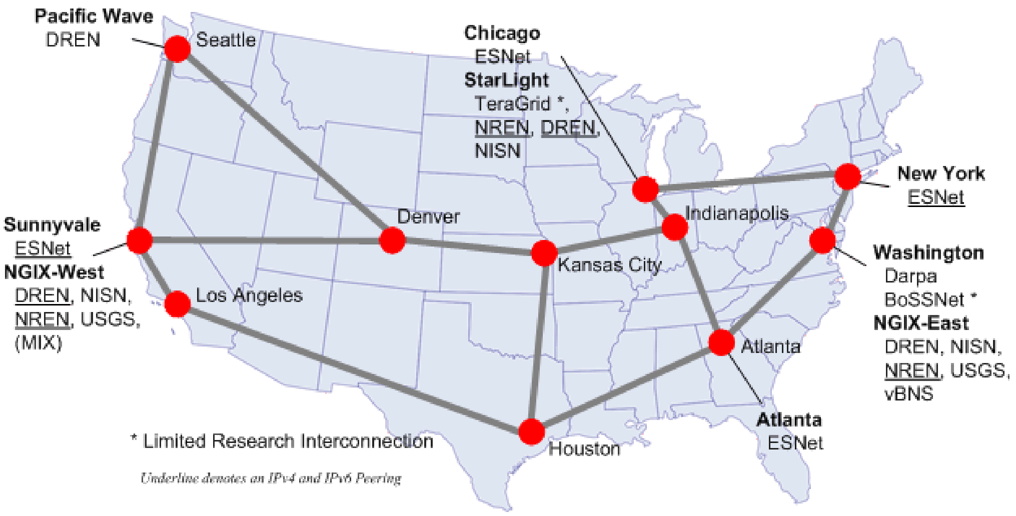


Figure 28: Abilene IPv6 Backbone Deployment[10]

Abilene peers with other high-performance research and education networks as shown in Figure 28.

[9] http://www.internet2.edu/

[10] http://www.abilene.iu.edu/images/v6.pdf

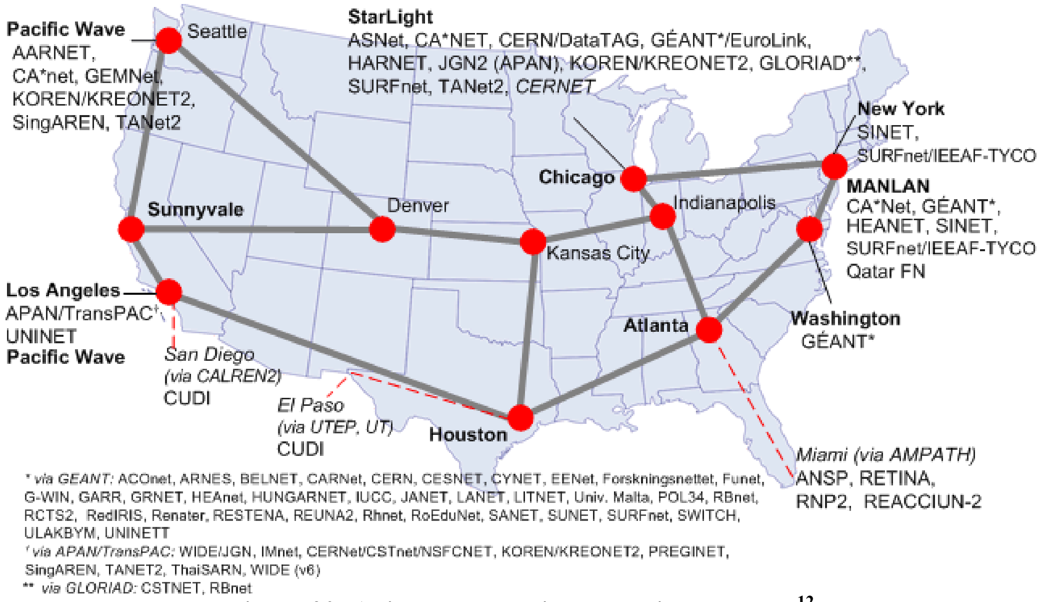


* Limited Research Interconnection

Underline denotes an IPv4 and IPv6 Peering

Figure 29: Peering with Federal/Research Networks[11]

Abilene is peered with over 30 international networks as indicated if Figure 29.



* *via GEANT:* ACOnet, ARNES, BELNET, CARNet, CERN, CESNET, CYNET, EENet, Forskningsnettet, Funet, G-WIN, GARR, GRNET, HEAnet, HUNGARNET, IUCC, JANET, LANET, LITNET, Univ. Malta, POL34, RBnet, RCTS2, RedIRIS, Renater, RESTENA, REUNA2, Rhnet, RoEduNet, SANET, SUNET, SURFnet, SWITCH, ULAKBYM, UNINETT

† *via APAN/TransPAC:* WIDE/JGN, IMnet, CERNet/CSTnet/NSFCNET, KOREN/KREONET2, PREGINET, SingAREN, TANET2, ThaiSARN, WIDE (v6)

** *via GLORIAD:* CSTNET, RBnet

Figure 30: Abilene International Peering Partners[12]

In addition to standard Internet applications, Internet2's Abilene network provides high speed service for leading-edge applications and services including:

[11] http://abilene.internet2.edu/images/abilene-fed-res-peers-title.gif

[12] http://international.internet2.edu/intl_connect/Intlpeering_Abilene.gif

- Remote Instrumentation – Twin 8.1-meter astronomical telescopes in Hawaii and Chile can be accessed via Abilene and operated remotely in real time.
- NanoManipulation – The nanoManipulator is an interface to Scanning Probe Microscopes (SPM) that, via Abilene, allows remote users to see, feel, and manipulate samples ranging in size from DNA to single atoms.
- Streaming Video – High-speed video service over Abilene enabled a musical performance and master class discussion streamed live from the Manhattan School of Music to University of Oklahoma students and faculty.
- Mobile Cluster Computing – Abilene's IPv6 backbone provides superior mobility services, network load balancing, geographically distributed clusters, and cluster security to create a clustered environment where mobile devices/agents (cellular phone, PDA 's, etc.) can submit computation requests to be performed on cluster computers.
- Virtual Reality – Developed by the University of Missouri, Columbia and Central Missouri State University to supplement African-American literature courses, a virtual portal "transports" students to the 1925-35 Harlem renaissance where they navigate city streets and interact with key figures.
- Cyber Security – The Internet Tsunami Warning System project at Carnegie Mellon University aims to distribute a high-speed network monitoring system to automatically detect and react early to Internet attacks.
- PlanetLab Grid Computing **–** This overlay network serves as a test bed for the deployment and evaluation of planetary-scale network services which could be potentially disruptive on the underlying network. PlanetLab is used to experiment with distributed storage, network mapping, peer-to-peer systems, distributed hash tables, distributed query processing, and other emerging technologies. PlanetLab is co-located in eleven Abilene routers for network experimentation.

Internet2 aims to make IPv6 an effective tool for creating next-generation networks by exercising, proliferating, and improving IPv6 infrastructure and software in the Internet2 context and to prepare it for deployment in the broader Internet community.

The “Guide to 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.

Author:

Dale Geesey
Vice President of Consulting
v6 Transition
dale@usipv6.com

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