Federal IPv6 Transition Best Practices

Ralph Wallace
Program Director, IPv6 Lead
Aptive Resources
Ralph.Wallace@aptiveresources.com

First presented to the Federal IPv6 Task Force on 2/26/2021

Context

The following is a combination of lessons learned and best practices developed, practiced and validated by a dedicated team of professionals operating within a very large Federal agency with financial responsibilities. During the course of this initiative, we underwent an Inspector General's audit in the third year of the nine year effort. The corrective actions requested after the audit were effectively to establish more governance and executive oversight. The apparatus needed to support this action was already in place, and the only item lacking was the people to actively engage (the audit report is open source and available on request).

This presentation has been given to an extended audience of the Federal IPv6 Task Force and the DoD IPv6 Working Group, affording each organization a risk mitigation opportunity for benchmarking and adaptation to the specific agencies' mission, environment and capabilities.

Table of Contents

Introduction

US Government Impact -

- This transition touches EVERY component on the USG enterprises including
  - All websites
  - All email
  - All Switches & Routers
  - All Platform Operating Systems
  - All devices that connect to the network (e.g. printers, IoT)
  - All Applications need to be tested and some may require updates
- Current USG customers using IPv4 will continue to access the USG web services and communicate via email (or until USG support for IPv4 is removed).
- Future Access of USG customers to the USG Internet Access Points must be provided for USG customers who only have IPv6 access
- We will need to support a “dual stack” (IPv4 & IPv6 host connectivity) for many years as the “world” makes the transition to IPv6 (or until USG support for IPv4 is removed).
- Internal client applications such as Web Browsers on workstations must be able to access both the IPv4 and IPv6 Internets

Internet traffic accessing key Federal Websites is now 50% using IPv6 exclusively, increasing annually by ~5%

Introduction

Originating Direction -

In October 2003, the President's National Strategy to Secure Cyberspace (National Strategy) directed the Secretary of Commerce to form a task force to examine the most recent iteration of the Internet Protocol version 6 (IPv6). The President charged the task force with considering a variety of IPv6-related issues, "including the appropriate role of government, international interoperability, security in transition, and costs and benefits."

GAO-05-471 May 2005 INTERNET PROTOCOL VERSION 6
Federal Agencies Need to Plan for Transition and Manage Security Risks

OMB M-05-22 August 2, 2005
MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS
FROM: Karen S. Evans, Administrator, Office of E-Government and Information Technology
SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government Version 1.0, May 2009
Issued by Federal CIO Council Architecture and Infrastructure Committee

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES, September 28, 2010
FROM: Vivek Kundra , Federal Chief Information Officer
SUBJECT: Transition to IPv6

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government Version 2.0, July 2012
Issued by Federal CIO Council Strategy and Planning Committee

OMB M-21-07 November 19, 2020
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
SUBJECT: Completing the Transition to Internet Protocol Version 6 (1Pv6)

Background

OMB M-05-22, August 2, 2005

Attachment C: Transition Activities (Notional Summary of CIO Council Guidance)
The CIO Council will develop additional transition guidance as necessary covering the following actions. To the extent agencies can address these actions now, they should do so.

Beginning February 2006, agencies' transition activity will be evaluated using OMB's Enterprise Architecture Assessment Framework:

- Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
- Develop a sequencing plan for IPv6 implementation, integrated with your agency Enterprise Architecture.
- Develop IPv6-related policies and enforcement mechanisms.
- Develop training material for stakeholders.
- Develop and implement a test plan for IPv6 compatibility/interoperability.
- Deploy IPv6 using a phased approach.
- Maintain and monitor networks.
- Update IPv6 requirements and target architecture on an ongoing basis.

Agencies following the above planning guidance have been the most successful

Background

OMB M-21-07, November 19, 2020

1. 45 Days from issuance - *Designate an integrated agency-wide IPv6 integrated project team* (including acquisition, policy, and technical members), or other governance structure, within 45 days of issuance of this policy to effectively govern and enforce IPv6 efforts;

2. 180 days from issuance - *Issue and make available on the agency's publicly accessible website*, an agency-wide IPv6 policy, within 180 days of issuance of this memorandum. The agency-wide IPv6 policy must require that, no later than FY 2023, all new networked Federal information systems are IPv6-enabled at the time of deployment, and outline a strategy to phase out the use of IPv4 for all systems;

3. NLT the end of FY2021 - Identify opportunities for IPv6 pilots and *complete at least one pilot of an IPv6-only operational system* by the end of FY 2021 and report the results of the pilot to OMB upon request;

4. NLT the end of FY2021 - *Develop an IPv6 implementation plan* by the end of FY 2021, and *update the Information Resources Management (IRM) Strategic Plan* as appropriate, to update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation. The plan shall describe your transition process and include the following milestones and actions:
   a. At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023;
   b. At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024;
   c. At least 80% of IP-enabled assets on Federal networks are operating IPv6-only environments by the end of FY 2025; and
   d. Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;

5. Continuance from previous mandated efforts - Work with external partners to identify systems that interface with networked Federal information systems to migrate all network interfaces to the use of IPv6; and

6. Continuance from previous mandated efforts - *Complete the upgrade of public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) and internal client applications that communicate with public Internet services and supporting enterprise networks to operationally use native IPv6.*

M-21-07 is intended to be the final guidance established to complete the Federal transition

Background

IPv6 Transition Guidance, February 2006 (37 pages) Federal CIO Council

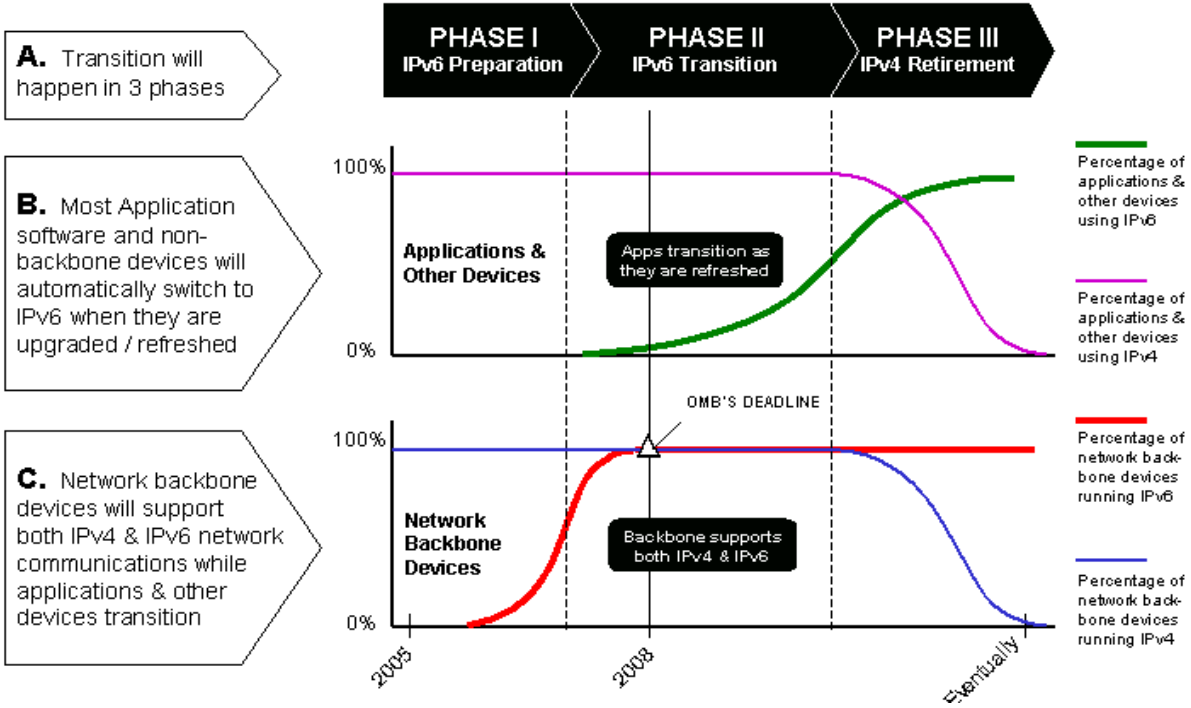
4.2 Components of an IPv6 Transition Plan

The following is a list of components that could be used as the basis for an IPv6 transition plan. Although agencies are not required to include all of these components in their transition plan, it is recommended that agencies cross-check their own plan against this list to ensure no critical transition elements have been overlooked.

1. Identification of strategic business objectives
2. Identification of transition priorities
3. Identification of transition activities
4. Transition milestones
5. Transition criteria for legacy, upgraded, and new capabilities
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability
8. Management and assignment of resources for transition
9. Maintenance of interoperability and security during transition
10. Use of IPv6 standards and products
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment
12. Application migration (if required to support backbone transition)
13. Costs not covered by technology refresh
14. Transition governance
    a. Policy
    b. Roles and responsibilities
    c. Management structure
    d. Performance measurement
    e. Reporting
15. Acquisition and procurement
16. Training
17. Testing

Background

The below graphic accurately represents the phases of a transition (milestone dates refer back to M-05-22 guidance)



Graphic from "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government ", Version 1.0, May 2009

Background

Department of Education's approach for their transition plan (Released 2011)

Table of Contents

Background

IRS approach to their transition plan (Released 2012, updated 2015)

TABLE OF CONTENTS

Transition Planning

Establish Objectives (Objectives include still valid 2010 mandate objectives)

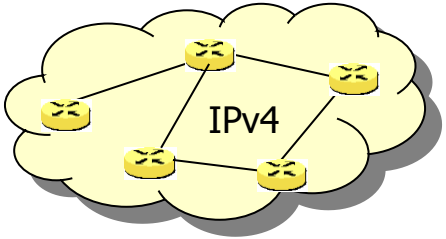
2012 Technical Objective: Websites, Email and External DNS
2014 Technical Objective: Internal client applications that require the Internet to accomplish their business function (e.g. FTP servers, Internet browsers)
2021 Objectives: Form IPT, Create Strategic Policy, Create Implementation Plan
2021 Technical Objective: Conduct a Pilot by the end of FY21
2023 Technical Objective: 20% of Enterprise IPv6 Only
2024 Technical Objective: 50% of Enterprise IPv6 Only
2025 Technical Objective: 80% of Enterprise IPv6 Only
Strategic Initiative: Remove reliance on IPv4 enterprise-wide as soon as it is reasonable and prudent

Establish Approach

Agency-wide Transition Manager with assigned authority to conduct efforts between IT and Business Unit organizations.
Central Transition Management PMO with corresponding IPT
Establish functional areas to establish and sustain focus
Establish functional objectives in each area supporting the overarching objectives

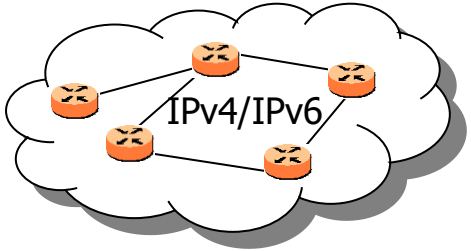
Objectives

Pre-2012



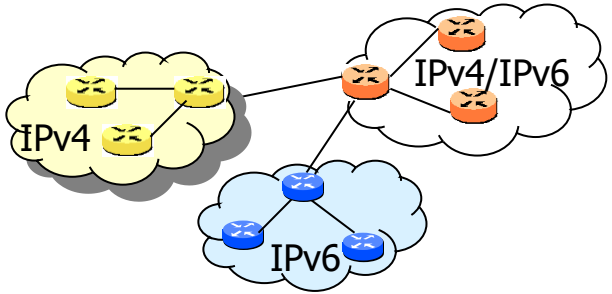
IPv4-only Network

Post-2014 Internet Facing



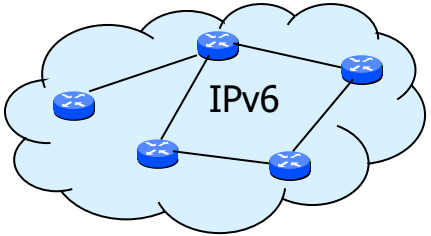
Dual Stack Network

M-21-07 20/50/80 Objective



Heterogeneous Network

Strategic Initiative



IPv6-only Network

Create virtual enclaves containing IPv4 and IPv6 entities (network, platform, cybersecurity, applications) to monitor their transition state

Governance

Oversight
Business Processes
Risk Management
Collaboration across organizations
Assigned responsibility, authority and accountability
Appropriate delegation
Phased approach
Agreed on expected outcomes

Governance

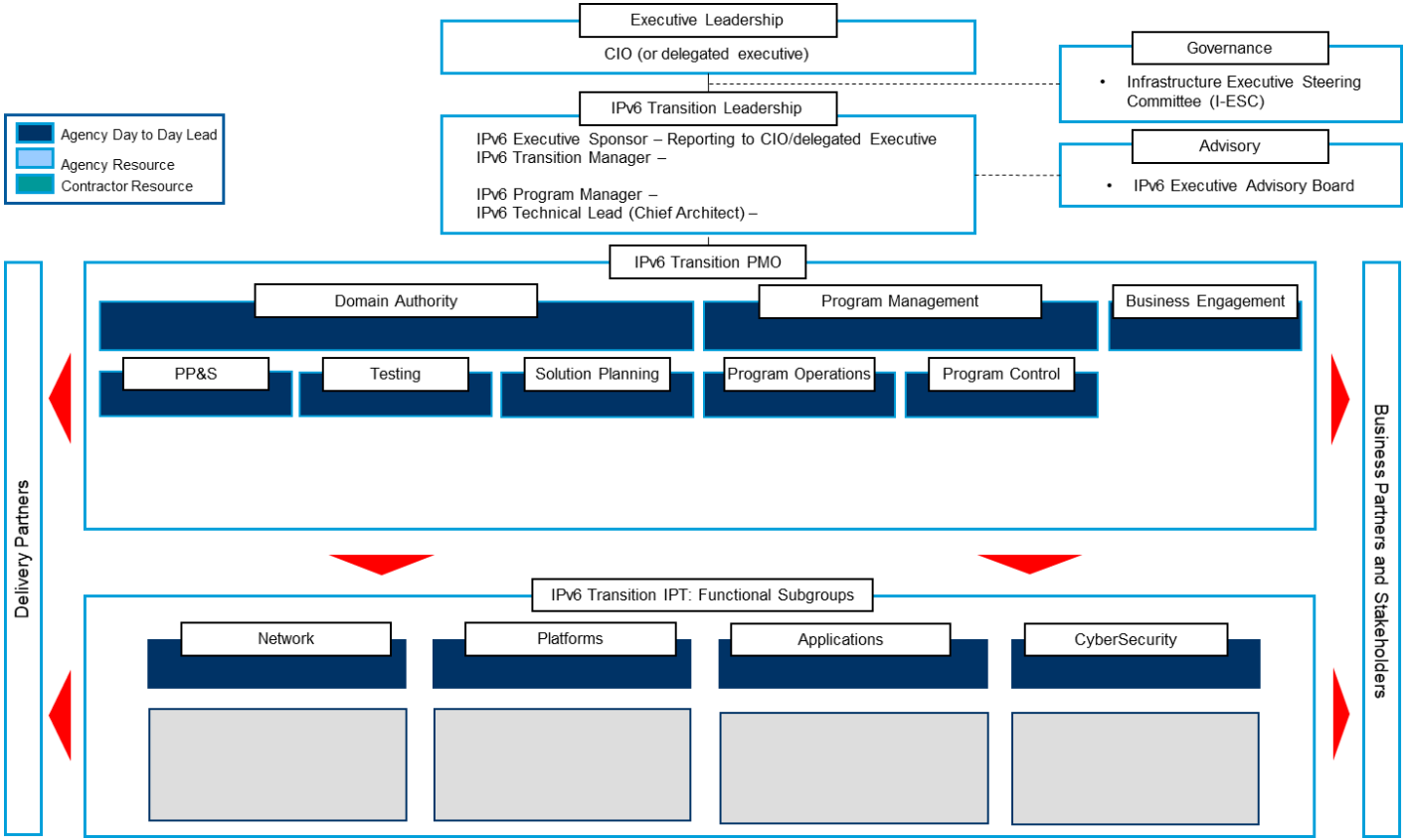
Establish PMO/IPT (within 45 Days of memo issuance)

- Agency IT Organization Objectives
  - Establish Program Management Office (PMO) capabilities for the Agency's IPv6 Transition effort
  - Establish Integrated Project Team (IPT) per respective agencies' process to ensure stakeholders' engagement
  - To effectively manage the overall OMB mandated IPv6 Transition effort to meet M-21-07 objectives
- Principles
  - The primary purpose of this effort is to design Core Team programmatic and technical functions
  - Each functional group of the PMO and IPT should be supported by an Agency lead, a PMO support resource, and additional Agency resources as needed. In smaller agencies, multiple functions may be assigned to individuals
  - Responsibility for execution of program activities should be assigned to the lowest level feasible within an organizational component
  - Staffing estimates are built based on resources required to support FY activities extrapolated from the implementation plan
  - Each activity performed by a Core Team or IPT member also requires effort for primary and secondary oversight (e.g. inclusion within risk and issue management plans)

PMO/IPT Roles

Functional Group		Functional Area	Activities
Domain Authority		Solution Planning	▪ Develop the IPv6 Transition Plan for the All Objective ▪ Establish and support the IPT functional subgroups (network, platforms, applications and cybersecurity) ▪ Oversee projects to ensure that the Program delivers the desired capabilities and will meet Program objectives ▪ Integrate IPv6 with internal and external enterprise Programs
		Policies, Procedures, and Standards	▪ Incorporate the adoption of IPv6 into specific policies, procedures and standards within the Agency
		Testing	▪ Establish and operate IPv6 Test Lab
Program Management	Program Operations	Scope Mgmt.	▪ Develop and maintain Project Charter, Project Management Plan, and LC Tailoring Plan ▪ Manage change requests to project and program scope
		Schedule Mgmt.	▪ Develop and maintain the Integrated Master Schedule (IMS) for the IPv6 program ▪ Review schedule trends and forecasts and perform continuous critical path analysis
		Resource Mgmt.	▪ Manage Agency and contractor staffing for IPv6 Transition PMO
		Budget Mgmt.	▪ Develop IPv6 Transition Spend Plan and risk reserve budget ▪ Monitor the program's overall budget and financial status
		Procurement Mgmt.	▪ Plan, conduct, and administer procurement and requisition management support
		Program Reporting	▪ Collect, monitor, and report program-related data
	Program Control	Risk & Issue Mgmt.	▪ Identify, analyze, evaluate, prioritize, and control risks ▪ Identify, validate, prioritize, and resolve issues
		Quality Mgmt.	▪ Review processes, deliverables, and work products for quality
		LC and Governance Mgmt.	▪ Develop required LC artifacts ▪ Coordinate the consensus of required approval authorities based on LC guidelines
		Performance Mgmt.	▪ Complete monthly Health Assessment Survey
Organizational Readiness		Stakeholder Engagement	▪ Coordinate with Business Partners and external stakeholders, e.g. Federal IPv6 Task Force ▪ Support Business Units in managing their transition efforts, e.g. preparation of materials
		Outreach & Communications Mgmt.	▪ Coordinate daily tactical communications; disseminate information to key stakeholders ▪ Produce written and other communications as needed to support the IPv6 transition
		Training	▪ Establish and maintain a training "continuum" for key personnel across the enterprise working in their respective functional areas who must know IPv6 at an apprentice, journeyman, and master level

PMO/IPT Structure



Governance

Functional Group	Functional Area	Activities
Domain Authority	Solution Planning	▪ Develop the IPv6 Transition Plan for the All Objective ▪ Establish and support the IPT functional subgroups (network, platforms, applications and cybersecurity) ▪ Oversee projects to ensure that the Program delivers the desired capabilities and will meet Program objectives ▪ Integrate IPv6 with internal and external enterprise Programs
	Policies, Procedures, and Standards	▪ Incorporate the adoption of IPv6 into specific policies, procedures and standards within the Agency
	Testing	▪ Establish and operate IPv6 Test Lab

Define IPv6 Requirements for the agency

Table of Contents:

Page 4 of 93

Governance

IPT Network Subgroup Responsibility

Create and Implement IPv6 Address Management Plan
Define Transition Mechanism(s)
Create Standards
Conduct device/system/application gap analysis
Establish plan constrained by contracts and funding

Device Responsibility (Analysis, Standard Development, Testing, and Deployment)
Routers
Switches
DHCPv6
DNS
Load Balancer
WAN, MAN, LAN, PAN, IoT and Cloud architecture
NOC devices and applications

Governance

IPT Platform Subgroup Responsibility

Platform (Workstation/Server- Physical/Virtual)

- MS
- Apple
- Linux
- Unix
- Mainframe
- IoT
- Cloud

Conduct gap analysis
Establish plan constrained by contracts and funding

Governance

IPT Application Subgroup Responsibility

- Define software specification for GOTS developed applications
- Define software specification for COTS procured applications
- Establish testing criteria in collaboration with software developers
- Conduct gap analysis to specification
- Create transition schedule per contract and funding constraints

Applications ability to operate in an IPv6 only environment is the single most important critical path item in any agency transition

Applications Data Call (Required for gap analysis)

Technical POC (Name/Phone/Org):
Developer Organization or Business Unit Owning Application

Does any portion of the application connect to or accept connections from any system outside the Agency network? (Yes/No)

Are there any hardcoded IP addresses present in the code, connection strings, configuration, etc. (Yes/No) - Provide specific information in Component Tab

Does application pass IP addresses to another application (Yes/No) - Provide specific information in Component Tab.

Does your application have application variables for IPv4 addresses or database fields for IPv4 addresses.(Yes/No) - Provide specific information in Component Tab.

Have you performed a complete review of application for IPv6 compatibility? (Yes/No)

Is the application already fully IPv6 capable or protocol independent? (Yes/No) **

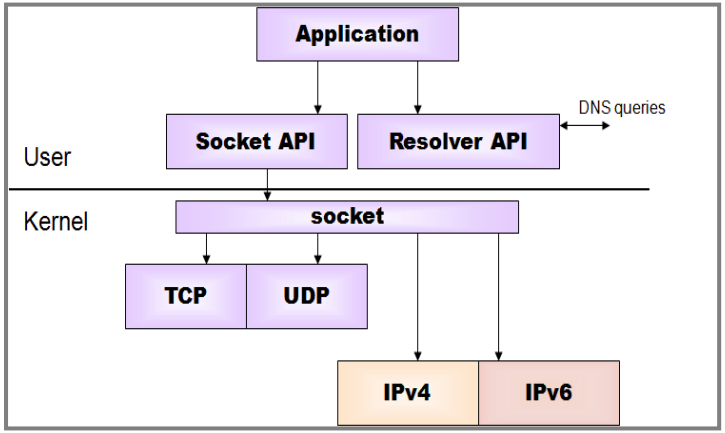
**** The scope of this question covers all in house or contractor developed application code, third party libraries, COTS/GOTS software on which the application depends, operating system(s) used, and any hardware used by the application. If the answer to this question is yes, then the assessment is complete and the rest of the data call can be left blank. Otherwise on the next tab capture all project components that are not IPv6 capable and estimate the level of effort required to make them IPv6 capable or protocol independent.**

Component Name	Component Type & Description (Code/Configuration/Library/COTS/OS /Hardware/ DB Field/Conn string)	Platform/ Language	Strategy (Upgrade/Replace/ Rewrite)	Resources Required (Estimate in FTE days, include integration)	Non-FTE Costs

Governance

IPT Applications Subgroup Responsibilities

Industry experience has identified the prevalence of hard coded IPv4 addresses used to establish host to host network connections. These addresses are often neither documented in the application documentation nor annotated in the code base.



Industry best practices and IETF guidance advise the use of DNS and DHCPv6 to effectively manage the deployment and distribution of IPv6 addresses due to the 128 bit address nomenclature, size and scope.

Industry and Federal IPv6 Transition best practices advise to remove reliance on any hard coded IP addresses, and transition to use of Fully Qualified Domain Names (FQDN) to resolve hosts.

The End Goal is to facilitate the transition of any application from an IPv4 connection to an IPv6 environment employing DNS, in keeping with M-21-07 20/50/80 direction. This will result in reduced manual effort, decreased risk, and a higher percentage of success.

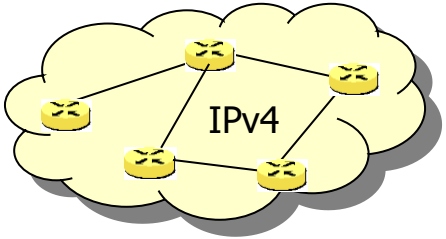
Governance

Application IPv6 Best Practices

Table of Contents

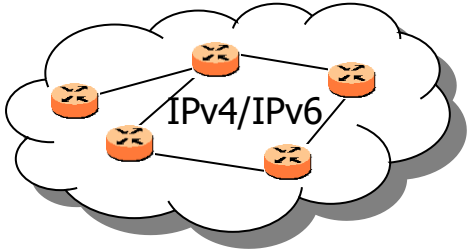
Objectives

Pre-2012



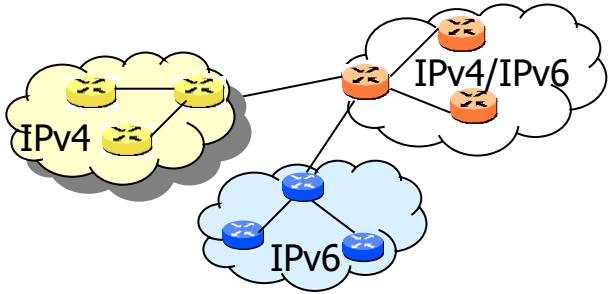
IPv4-only Network

Post-2014 Internet Facing



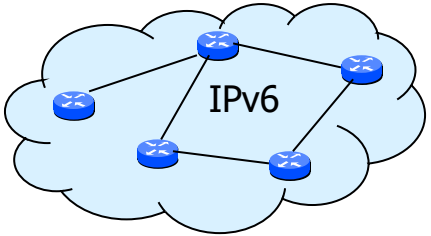
Dual Stack Network

M-21-07 20/50/80 Objective



Heterogeneous Network

Strategic Initiative



IPv6-only Network

Create virtual enclaves containing IPv4 and IPv6 entities (network, platform, cybersecurity, applications) to monitor their transition state

Governance

IPT Cybersecurity Subgroup Responsibility (Defense in Depth Architecture)

- **Architecture Design**
  - Perimeter, Infrastructure, Host
- **Perimeter**
  - Firewalls
  - Proxies
  - Edge Access Control Lists (ACLs)
  - Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
  - Deep Packet Inspection (DPI)
- **Infrastructure**
  - Address Planning
  - Internal Router ACLS
  - Router Advertisement (RA) Guard
  - DHCPv6 Guard
- **Host**
  - Workstation firewalls
  - Host configuration (workstation, servers, mainframes, IoT and Cloud)

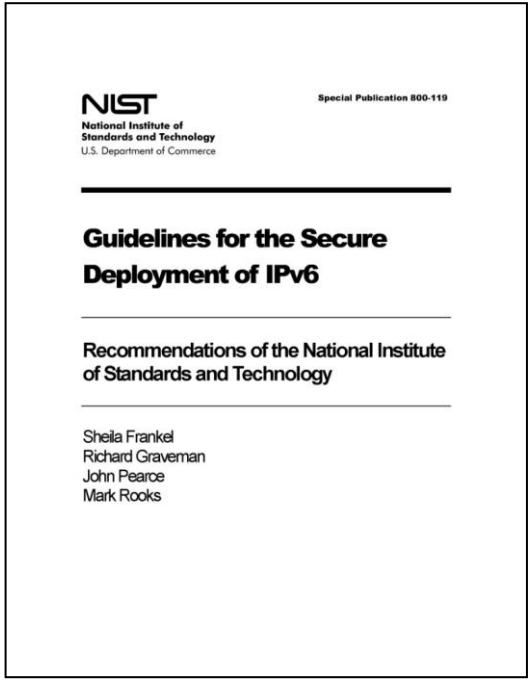
- **Policies and Procedures**
  - Agency Cybersecurity policies regarding deployment and enablement of IPv6

Governance

Guidelines for Secure Deployment of IPv6

(NIST Special Publication 800-119)

- Addresses operational issues of IPv6 secure deployment.
- IPv6 Technology
- Security Risks
- Addressing Issues
- Transition Mechanisms
- Deployment Planning Process



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-119

Guidelines for the Secure Deployment of IPv6

Recommendations of the National Institute of Standards and Technology

Sheila Frankel
Richard Graveman
John Pearce
Mark Rooks

Transition Planning

Define requirements

Determine the current state

- Assess Enterprise state of readiness (Data Calls) in the following areas in support of M-21-07 objectives:
  - Network Infrastructure (including DHCP, DNS and platforms)
  - Cybersecurity (perimeter, infrastructure, and host)
  - Applications (external facing and internal)
  - Policy, Procedures and Standards (including FISMA Compliance)

Conduct Gap Analysis

Establish requirements, design, test, pilot and deployment workflow for each objective

Establish respective WBS per fiscal year

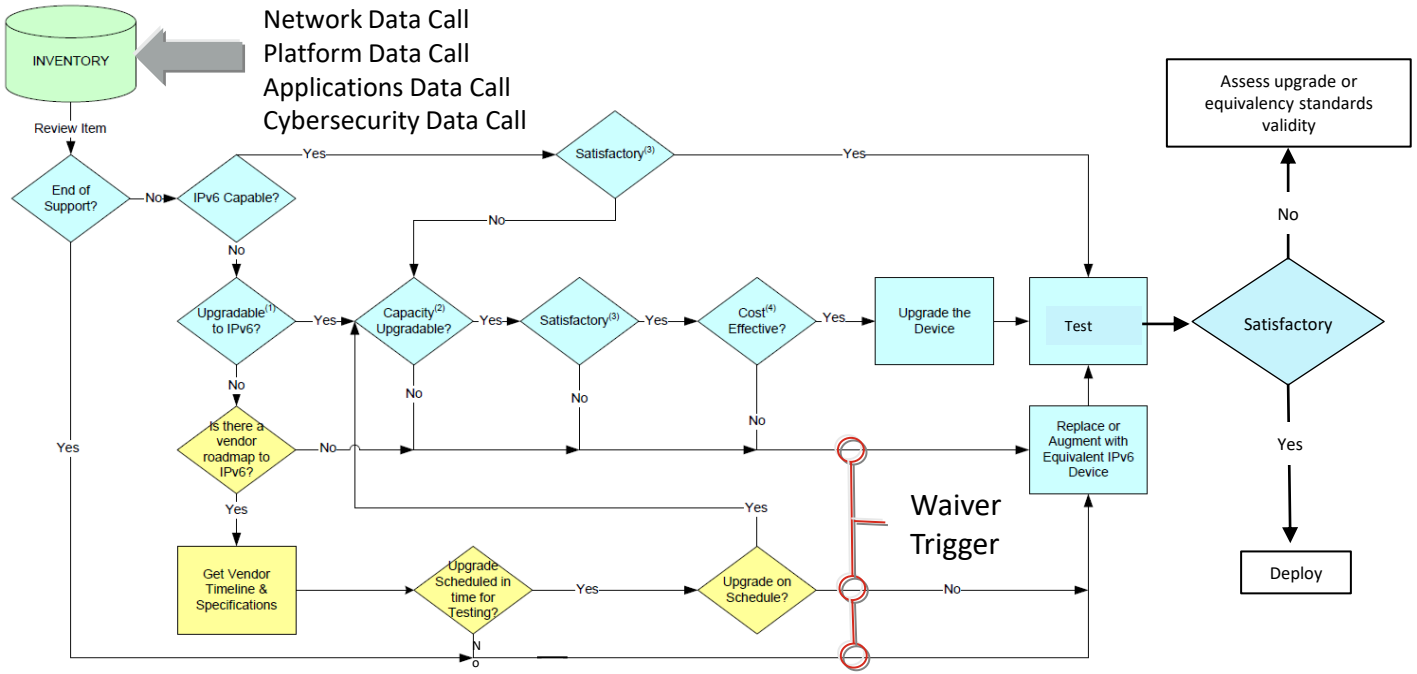
- **Schedule, Resources, Risks**

Determine Costs per fiscal year

- **Hardware, Software, Labor (including training), Risk Mitigation**

Establish budget per fiscal year

Gap Analysis Workflow to IPv6 Capable



1. **Upgradable to IPv6** – The possibility of modifying a product so that it is IPv6 capable. An assumption is that after the product is upgraded it will continue to be IPv4 capable as well as IPv6.
2. **Capacity Upgradable** – The possibility of modifying an IPv6 product so that it is capable of performing in a specific use, e.g., by increasing memory capacity or processor speed.
3. **Satisfactory** – The capability of an IPv6 product to perform in a specific manner. and on schedule.
4. **Cost Effective** – The economic advisability of upgrading an IPv4 product so that it is IPv6 capable.

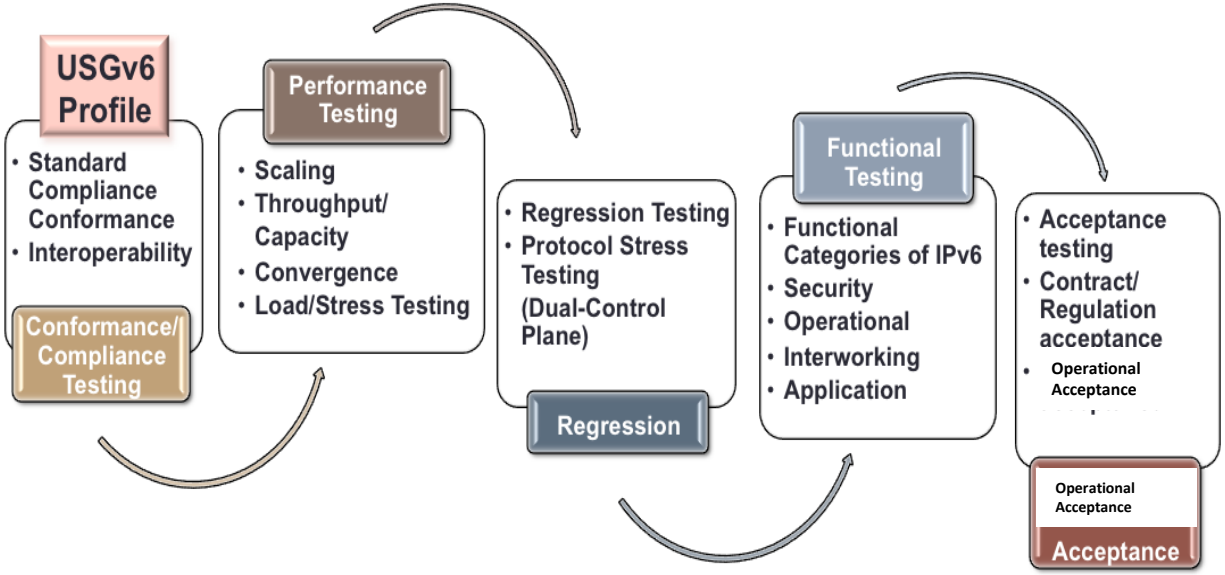
Transition Planning

- Establishing the Path (practical examples)
  - Develop Addressing and Routing Plan
  - Acquire IPv6 Address from ARIN, and revisit ARIN if the original ask was inappropriate
  - Establish Address Management and Allocation Procedures
  - Create Domain Name Service (DNS)/ DHCPv6 enterprise architecture
  - Map with MS Active Directory architecture, if appropriate
  - Set standard for both internal and external platform web services
  - Test and deploy web proxies
  - Test and deploy load balancers
  - Set application standard and once tested, deploy capable applications
  - Establish workstation access via dual stack
  - Establish means for workstation Telework/VPN over IPv6 Internet
  - Security
    - Engineering the defense in depth architecture
    - Complying with FISMA criteria
  - Governance documentation
    - Acquisition
  - Training
  - Testing

Transition Planning

- Establishing the Path (additional considerations)
  - Establish IPv4 and IPv6 enclaves
  - Assign and label legacy IPv4 entities to the enclave
  - Maintain dual stack to the workstation until all applications are IPv6 only
  - On designated subnets were safe and secure to do so, turn off IPv4
  - Monitor IPv6 traffic
  - Security
    - Ensure CDM monitoring concept of operations includes IPv6 nuances

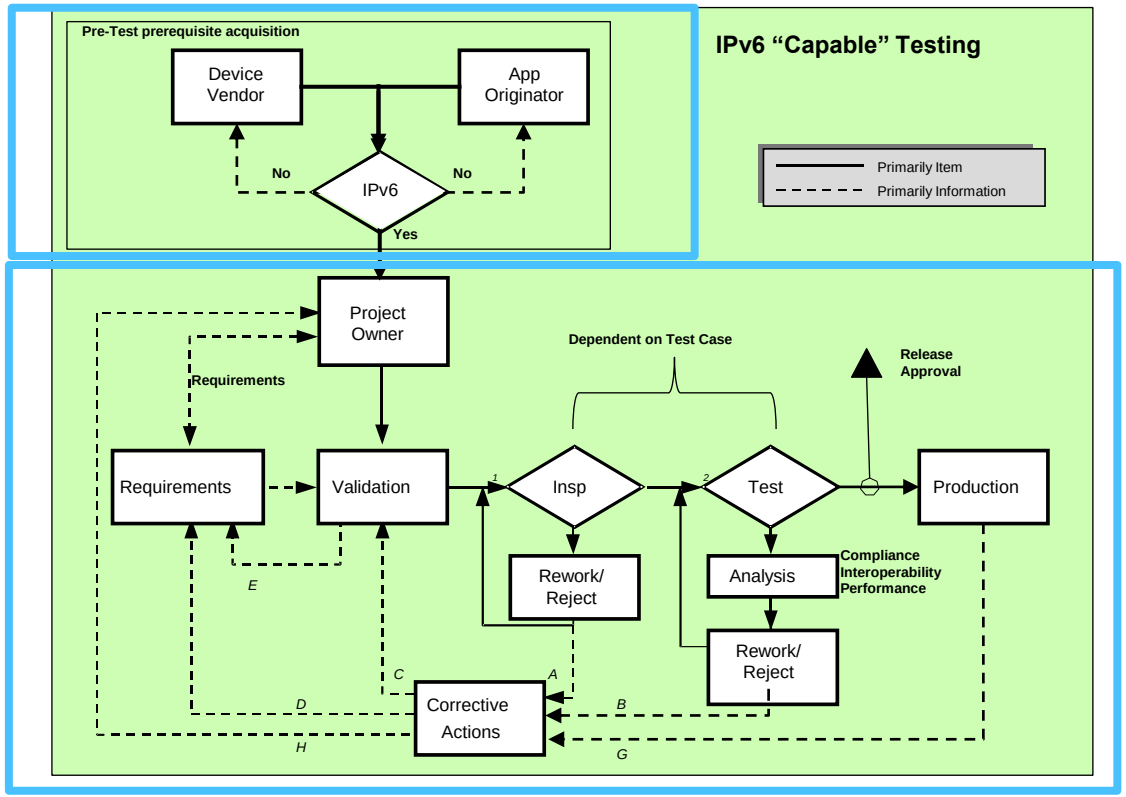
Transition Implementation (Testing)



Transition Implementation (Testing)

Agency acquisition guidelines per USGv6 profile and SDOCs submittal/Contractual Letter of Compliance from vendor based on agency requirements

Agency required testing of capability, performance and interoperability over IPv6 “only” to ensure mission effectiveness prior to deploying into production



Acquisition

September 28, 2010

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Vivek Kundra

Federal Chief Information Officer

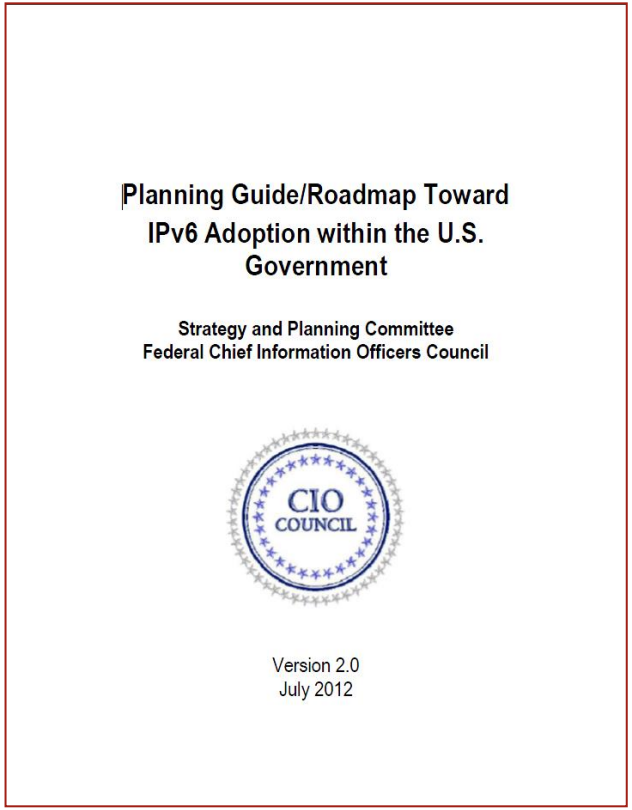
SUBJECT: Transition to IPv6

In order to facilitate timely and effective IPv6 adoption, agencies shall:

1. Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;
2. Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
3. Designate an IPv6 Transition Manager and submit their name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
4. ***Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.***

Acquisition

2.2 IPv6 Federal Acquisition Regulations (FAR)
DoD, GSA, and NASA published a proposed rule in the Federal Register at 71 FR 50011, August 24, 2006, to amend the FAR to ensure that all new IT acquisitions using Internet Protocol are IPv6 compliant. The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule amending the FAR to require that IPv6-compliant products be included in all new IT acquisitions using Internet Protocol effective December 10, 2009.


Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

Strategy and Planning Committee
Federal Chief Information Officers Council

CIO COUNCIL

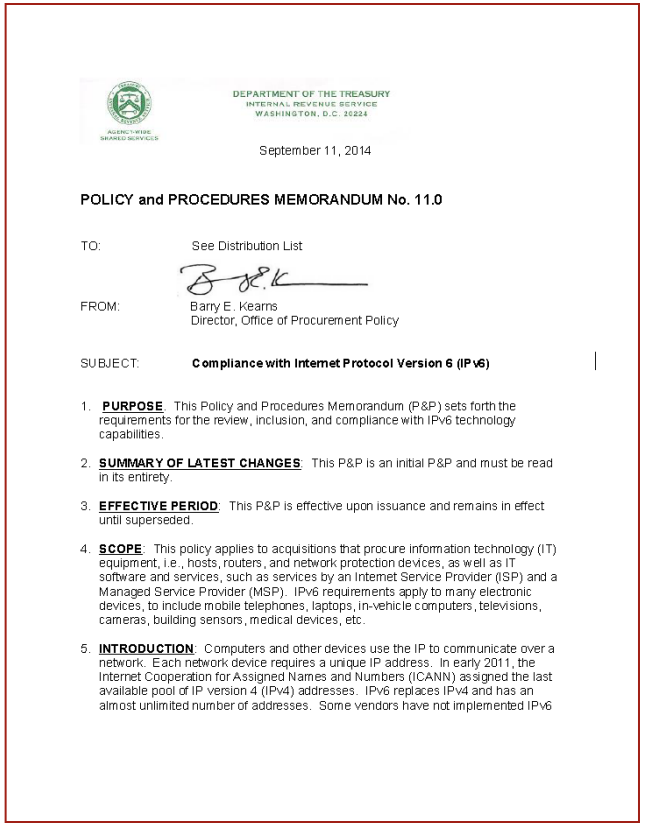
Version 2.0
July 2012

Acquisition

7. POLICY.
All offices and officials involved in the acquisition of IT equipment, devices, and services will follow and adhere to the policies and procedures set forth herein, regardless of the dollar value of the acquisition.

9. PROCEDURES:
A. Business Units (BUs) will:
1. Identify relevant acquisitions that require IP technical capabilities and address these capabilities within acquisition plans, statements of work or performance work statements, source selection plans, and technical evaluation plans, as deemed necessary.
2. Obtain a waiver, if the IP technical capability within the requisition documentation does not reference or include IPv6.

B. Contracting Officers (CO) will:
1. Verify that the statement of work (SOW)/performance work statement (PWS) for an IT acquisition contain an appropriate IP statement of requirements and/or specifications.
2. If the requirements are for other than IPv6 technical capabilities, the CO will direct the customer to the CTO Office identified herein for the purposes of including the requirements or assisting the customer in obtaining a waiver from them.



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

AGENCY-WIDE SHARED SERVICES

September 11, 2014

POLICY and PROCEDURES MEMORANDUM No. 11.0

TO: See Distribution List

FROM: Barry E. Kearns
Director, Office of Procurement Policy

SUBJECT: **Compliance with Internet Protocol Version 6 (IPv6)**

1. **PURPOSE**: This Policy and Procedures Memorandum (P&P) sets forth the requirements for the review, inclusion, and compliance with IPv6 technology capabilities.

2. **SUMMARY OF LATEST CHANGES**: This P&P is an initial P&P and must be read in its entirety.

3. **EFFECTIVE PERIOD**: This P&P is effective upon issuance and remains in effect until superseded.

4. **SCOPE**: This policy applies to acquisitions that procure information technology (IT) equipment, i.e., hosts, routers, and network protection devices, as well as IT software and services, such as services by an Internet Service Provider (ISP) and a Managed Service Provider (MSP). IPv6 requirements apply to many electronic devices, to include mobile telephones, laptops, in-vehicle computers, televisions, cameras, building sensors, medical devices, etc.

5. **INTRODUCTION**: Computers and other devices use the IP to communicate over a network. Each network device requires a unique IP address. In early 2011, the Internet Cooperation for Assigned Names and Numbers (ICANN) assigned the last available pool of IP version 4 (IPv4) addresses. IPv6 replaces IPv4 and has an almost unlimited number of addresses. Some vendors have not implemented IPv6

Training

A training “continuum” must be established for those personnel across the enterprise working in their respective functional areas who must know IPv6 at an apprentice, journeyman, and master level of engagement. The comparison is software engineering.

	Levels of Engagement				
Topic	1	2	3	Focus	Audience
Overview	x			Awareness	Executive, Master
Fundamentals, Design, and Deployment		x		Engineering	Master, Journeyman
Security Engineering			x	Engineering	Master, Journeyman
Application Developer			x	Engineering	Master, Journeyman
IT Acquisition		x		Operational	Master, Journeyman
Enterprise Architecture		x		Operational	Master, Journeyman
Service Desk (ITSM)		x	x	Operational	Journeyman, Apprentice
Change Management (ITSM)		x	x	Operational	Journeyman, Apprentice
Security Operations		x		Operational	Journeyman, Apprentice

Closing

1. Identification of strategic business objectives
2. Identification of transition priorities
3. Identification of transition activities
4. Transition milestones
5. Transition criteria for legacy, upgraded, and new capabilities
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability
8. Management and assignment of resources for transition
9. Maintenance of interoperability and security during transition
10. Use of IPv6 standards and products
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment
12. Application migration (if required to support backbone transition)
13. Costs not covered by technology refresh
14. Transition governance
    a. Policy
    b. Roles and responsibilities
    c. Management structure
    d. Performance measurement
    e. Reporting
15. Acquisition and procurement
16. Training
17. Testing