

AUSTRALIAN GOVERNMENT
Department of Finance and Deregulation

**A Strategy for the Transition to IPv6 for Australian
Government agencies**

‘Building Capacity for Future Innovation’

Paper prepared for General Distribution
AGIMO, October 2007

For General Distribution

TABLE OF CONTENTS

A STRATEGY FOR THE TRANSITION TO IPV6 FOR AUSTRALIAN GOVERNMENT AGENCIES	1
1. Background	3
2. Why Plan for the Transition to IPv6 Now?	3
IPV6 TRANSITION TIMING	4
3 Preparation Stage	5
4 Transition Stage	6
5 Implementation Stage	6
6 Timetable And Stage Deliverables	7
7 Governance	8
8 Whole-of-Government Issues	8
9 The Market place	8

For General Distribution

1. Background

In December 2006, the Australian Government's Chief Information Officer Committee (CIOC) tasked the Australian Government Information Management Office (AGIMO) with the development of a whole-of-government strategy for a transition to Internet Protocol version 6 (IPv6).

To inform the development of the strategy, AGIMO formed an IPv6 Reference Group, consisting of representatives of the Australian Government's Chief Information Officer Committee (CIOC). The IPv6 Reference Group has subsequently met monthly to discuss transition issues and finalise this report.

The strategy was endorsed by the CIOC in December 2007 and the IPv6 Reference Group was replaced by a Community of Expertise (CoE). The CoE acts as a central point for policy advice and information regarding whole-of-government issues in the transition to an IPv6 environment. In particular, it considers issues around the whole-of-government IPv6 address space, security of networks and systems, skills, and training.

The CoE will meet regularly to ensure that transition activities are undertaken in a timely manner.

2. Why Plan for the transition to IPv6 Now?

While there are no critical business drivers that are forcing the Australian Government to move to IPv6 immediately, the development of ubiquitous IP networks (allowing for the rapid uptake of IP telephony and digital wireless networks), the shift to IP-based communications and the adoption of e-business strategies across numerous other technologies are all putting pressure on the available IPv4 address space. Organisations use Network Address Translation (NAT) and other interim measures to overcome IPv4 address space limitations, but over time these organisations will be limited in their ability to respond to address space pressures and to take advantage of capabilities offered by IPv6.

IPv6 was developed to increase the amount of available IP address space. By managing the IPv6 transition process early and collectively, Australian Government agencies will be able to better align and synchronise transition programmes, optimise procurement, manage programme and technical risks and manage vulnerabilities more deliberately. By ensuring that agencies have a target date for transition and have properly planned, organised and resourced their transition programmes, the Australian Government can promote a more disciplined and economical transition across the whole-of-government environment.

IPv6 has several well-known and understood benefits besides the increased address space. These include increased end-to-end security of systems and automated address allocation for internet connected devices.

There are several reasons for starting the planning process now and thereby not leaving it until industry and other external pressures build and introduce additional risks and costs.

In an Australian Government context, some of these reasons are:

- 1) The risk that unplanned and uncontrolled implementation of IPv6 equipment into government networks could result in failures and loss of service delivery capability.
- 2) The risk that the skills shortage in the ICT arena and in particular, the IPv6 field becomes so great that the government will not be able to compete with the private sector for IPv6 skilled technical and administrative staff.
- 3) The opportunities for increased service delivery, particularly in the health, environment and transport industries, that IPv6 will allow with its ability to have multiple sensor/tracking devices in a variety of fields.
- 4) The fact that many of our neighbours, including the US, Japan, Korea and many European nations are all moving down this path (at various speeds). The US has mandated the transition, and both Japan and Korea see the implementation of IPv6 as a way of relieving staffing and skills shortages by using robotics and remote sensors to achieve results that previously would have required manual procedures.
- 5) The risk that the cost of moving to IPv6 when industry and suppliers are driving the market will be significantly greater than if the planning and transition stages are undertaken in an environment of controlled progress.

IPv6 Transition Timing

The transition from the present IPv4 environment to a dual capability IPv4/IPv6 environment, and ultimately to a wholly IPv6 environment, is expected to take at least five-eight years. The transition to IPv6 will involve three stages:

- Preparation;
- Transition; and
- Implementation.

Ultimately, IPv6 capability will be available in all new equipment and once an agency's network backbone equipment is wholly IPv6 capable, the agency can decide when it will turn on the IPv6 capability.

Industry intends to supply dual capable IPv4/IPv6 equipment for the foreseeable future, while the IPv6 set of standards will become dominant within the next three-five years. It is anticipated that agencies will need to manage IPv4 network traffic for at least the next 15-20 years.

3 Preparation Stage

Agencies will need to plan, conduct and manage the following activities when they are transitioning to IPv6. The activities that need to be undertaken are:

- **Stocktake of equipment**
AGIMO recommends that agencies aim to complete the process by December 2009.
- **Training**
Agencies' technical and ICT administrative staff will need to be trained in IPv6. The training will need to be ongoing, systematic, and scalable for each agency's requirements.
- **Threat and Risk Assessment (TRA)**
Each agency will need to undertake an agency-specific TRA. Agencies need to assess the threat-related updates and other security related guidance that will need to be factored into any TRA and/or security planning.
- **Procurement Policy**
Agencies will need to ensure that individual agency procurement policies are updated to require that all ICT procurements consider whether any hardware or software solution should be IPv6 capable.
- **Dual Capability Networks (Dual-Stacking)**
Due to the requirement for agencies to cater for both IPv4 and IPv6 traffic into the foreseeable future, it is anticipated that agencies will need to manage dual-capable networks for at least the next 15-20 years.
- **Applications**
Agencies will need to undertake a stocktake of their software and applications (commercially and internally developed) to ascertain which will need to be upgraded to be IPv6 capable, those that will be replaced with IPv6 capable tools and those that will remain as legacy IPv4 software or applications.
- **Whole-of-Government Address Space Allocation**
AGIMO is investigating the advantages of the Australian Government seeking a whole-of-government allocation of a contiguous IPv6 address space.
- **Promoting Awareness of the Transition Strategy**
The IPv6 CoE will support AGIMO in building IPv6 awareness across government and industry, and promoting the government's transition strategy and its schedule.

4 Transition Stage

The Transition stage begins when an agency commences the replacement of older IPv4-only systems with dual capable IPv4/IPv6 hardware and/or software. It will end when agencies have replaced all of the IPv4 only capable equipment (bar the legacy equipment that has been consciously retained) with dual-capable equipment.

Each agency will be responsible for its individual transition plan. The CoE will be available to assist with technical or logistical matters under the auspices of the CIOC.

The transitioning stage to IPv6 will present several challenges to Australian Government agencies. These will include:

- **Updated Stocktake**
The installation of IPv6 capable equipment into their networks (as older IPv4 only equipment is replaced with IPv4/IPv6 capable equipment) will require agencies to update their initial stocktake.
- **Training**
Ongoing training of technical and ICT administrative personnel in the new protocol will be required to enable agencies to maintain dual IPv4 and IPv6 environments for an extended period of time.
- **Security**
Agencies will need to take into account any security-related guidance and/or updates provided. Agency TRAs should be managed to accommodate this advice and any resultant threats from new infrastructure added to the network.
- **Applications**
Agencies will need to incorporate IPv6 features into business cases for applications to identify new and better ways of meeting outcomes and porting existing applications to IPv6 capability, or ensuring applications are protocol neutral.
- **Internet Service Providers (ISPs)**
Agencies will need to discuss with their ISP the effect of the transition to IPv6 and ascertain how their ISP is going to cope with the on-going requirement to have both IPv4 and IPv6 capable equipment on the network.
- **Standards**
Implementing agreed standards required by the use of IPv6.

5 Implementation Stage

At the conclusion of this stage, agencies will be completely IPv6 capable (even though their systems may be dual capable).

6 Timetable and Stage Deliverables

In order to complete a whole-of-government IPv6 implementation and have the transition in line with the expected timeframes of other governments and industry, AGIMO suggests the following target periods for each phase:

IPv6 Transition - Proposed Timetable:

Stage	Deliverables
Preparation Jan 2008-Dec 2009	Stocktake of equipment (hardware)
	Investigate and recommend whole-of-government approach to IPv6 address space
	CoE to undertake Transition awareness programme.
	Stocktake of equipment (software & applications)
	Training needs analysis
	Threat & risk assessment
	Dual capable equipment to be considered with solely IPv4 equipment starting to be replaced
	Procurement policy updated
Transition Jan 2010-Dec 2012	Ongoing stocktake of equipment (hardware)
	Ongoing stocktake of equipment (software & applications)
	Relevant Training courses implemented
	Review of Infosec Registered Assessor Program (I-RAP) assessments. (if required)
Implementation Jan 2013-Dec 2015	IPv6 networks in place (dual capable)
	IPv6 capable hardware in place
	IPv6 applications in use
	ICT technical/admin staff continuing to train on IPv4/IPv6 systems

Achieving the 2015 target is more important than meeting the interim steps, though the interim steps are designed to allow agencies to control the transition with minimum disruption to ongoing business streams. The timeframes are indicative and reflect a risk managed approach. Agencies may move to Transition or Implementation before the identified dates.

7 Governance

AGIMO proposes that to enable an effective transition to IPv6, it will build on the work performed by the whole-of-government working/implementation group (the IPv6 Reference Group) to help ensure interoperability of applications and operating systems, efficient planning for the introduction of IPv6, and to ensure that agencies can tap into a bank of expertise. The IPv6 Reference Group will become the core of a CoE that will be facilitated by AGIMO. It will report to the CIOC on an annual basis, or more frequently should the need arise.

8 Whole-of-Government Issues

Where issues are common across agencies and/or jurisdictions, AGIMO will act as the central reporting agency so that all agencies and the CIOC is kept up-to-date on agency progress towards all government agencies being IPv6 capable in the recommended timeframes.

9 The Market place

To inform the availability of its products and services, industry is looking for some lead from government in regard to the likely timing of IPv6 transition. Advice from the major ICT industry companies is that they are ready to support government agencies with the supply of IPv6 capable equipment shortly after agencies identify a need for it.

AGIMO will communicate the Transition strategy through relevant forums to inform industry and other interested parties of the government's approach.

The implementation issues addressed in this paper have been informed by the *IPv6 Transition Guidance* issued by the US Federal CIO Council Architecture and Infrastructure Committee in February 2006. Other sources used include *IPv6 Essentials*, second edition, by Sylvia Hagen, and the Juniper Networks 'The IPv6 World Report Series' volumes 1, 2 and 3; *Guide for Federal Agencies Transitioning to IPv6*, issued in January 2006; *IPv6 Capable A Guide for Federal Agencies* issued in May 2006 and *An essential U.S. Government Agency Transition Guide to IPv6 Routing and Addressing* issued in June 2007.