OASIS eGov Member Section Guidance Document

The Transition from IPv4 to IPv6

- removing the barriers

OASIS (Organization for the Advancement of Structured Information Standards) [Ref 1] is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. The consortium produces open standards for Web services, security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS was founded in 1993.

The OASIS eGovernment Member Section (eGov MS) [Ref 2] serves as a focal point for discussions of governmental and public administration requirements for e-business standardization. Bringing together representatives from global, regional, national and local government agencies, the eGov MS provides a platform for those who share a common interest in directing and understanding the impact of open standards on the public sector.

Table of Contents

Overview

This paper draws on the experiences and lessons learnt by organisations in both the public and private sectors, and in particular early Government implementers, who have made the transition from IPv4 to IPv6. It provides guidance on how to remove the barriers from making that transition. Failure to make this transition and doing so within the next few years, will almost certainly lead to significant problems in new web services development and also the maintenance of existing web services.

The paper provides a focus on the most common barriers and for each there is a discussion on the issues and possible solutions, and finally recommendations on how to remove the barrier.

The intended audience is:

- Government and other public sector officials responsible for eGovernment policy, strategy, and implementation.
- Other public or global Institutions that provide advice and guidance on implementing eGovernment Progammes.
- Providers of hardware, software and services to Governments.
- OASIS membership.

Introduction

There is now general consensus amongst leading ICT strategists over the criticality of making the transition from IPv4 to IPv6 as a result of the existing stock of IPv4 addresses running out within the next 2 or 3 years[1]. Why does this matter - well everything connected to the Internet needs an "IP address" to ensure data reaches the right person or device. The Internet is built around version four of the Internet Protocol addressing scheme (IPv4) which has space for about four billion addresses. Its successor - IPv6 - has trillions available. While four billion was enough in the 1970s when the Internet was being set up, the growth of the World Wide Web is rapidly depleting this store and the entire pool is expected to be used up in 2012.

This will mean that no new websites, devices, etc will be able to connect to the Internet and also that web services currently only available to the Internet using IPv4 will not be reachable from IPv6 only clients. It does not mean the IPv4 Internet will stop working. The problem of IPv6 only clients will be gradual and the impact may not be significant for several years and that assumes a market 'translation' solution does not arrive before the issue becomes significant. Those impacted most are the nations closest to running out of address space e.g. China. However to avoid the transition problems it is essential therefore for all users to start making the transition to IPv6 now[2].

This is probably the biggest challenge to the global ICT industry since the Year 2000 problems and similar priority and action is required now to avoid the increasingly serious potential problems arising from the depletion of IPv4 addresses.

Governments have two roles to play in this issue. Firstly as an Internet user - leading by example in transitioning their ICT systems, and secondly as a policy maker supporting the work of the appropriate organizations responsible for IPv6 address assignments and getting involved in the processes of policy formation for IPv6 deployment.

In producing this document, the editors have drawn on their own experiences as well as those of the members of the OASIS eGov Member Section plus researching the experiences of governments and other jurisdictions – see Appendix A. In addition we would acknowledge the recent room document[3] entitled the “Evolution of the Internet’s Address Distribution Function, IPv6 and the Role of Government” produced by OECD/ITAC as providing a significant contribution to this debate.

It is not the intention of this paper to provide a full “How to do” guide to making the transition to IPv6, but to focus on those issues that are holding back Governments and their suppliers from starting work on the transition now. If further guidance or help is required on any aspect addressed in this paper please contact the eGov MS Steering Committee using the Contact facility at www.oasis-egov.org/contact .

[1] http://news.bbc.co.uk/1/hi/technology/10105978.stm

[2] http://en.wikipedia.org/wiki/IPv6_deployment

[3] www.internetac.org/?p=455

Barrier 1 – Not recognising the need

Barrier: Lack of understanding or appreciation that there is a problem that needs solving.

Discussion

There is always the danger that general apathy will stifle any positive action. Politicians, government managers and suppliers may need convincing that this is not just another scare story and want to know what is different about this one. They may well point out that the Year 2000 problem was a damp squib even though significant time and effort was put into mitigating the risks of that issue. Of course as it turned out it was a non-event precisely because of the effort put into solving the problem before it proved to be a catastrophe.

There is now a lot of well documented evidence produced by leading ICT strategists to prove that there is an impending problem and that unless action is taken existing Government web services will gradually fail to be available and new services will not reach intended audiences.

Recommendation:

Those charged with producing and implementing a Government ICT Strategy must ensure that all stakeholders appreciate the seriousness of the problem and assign it the attention it necessitates. A good way of doing this is for government agencies to place IPv4 on their risk registers and regularly report remaining address space against take up from anticipated projects. This will give a 'running estimate' of when they will run out. The aggregated results could then be collated and published to show the seriousness of the problem.

Barrier 2 – Lack of Strategy

Barrier: Lack of a strategy to making the transition.

Discussion

There are several possible ways of tackling the IPv6 transition and unless this is co-ordinated across Government there is a danger that any transition planning becomes ad-hoc and different solutions are put in place by different agencies. Whilst this may not be too serious it does raise the possibility of duplication of effort resulting in increasing costs and re-inventing wheels. A more strategic approach will help to ensure that all stakeholders are brought into the process thus leading to a better chance of success.

In making the strategic decisions, Governments need to take a business risk decision of either waiting for robust market solutions that do not yet exist or investigating solutions that will mitigate the business risk. Drawing on the experiences of others, both in the public and private sectors, will help determine the most appropriate strategy but it should be recognised that there is not a one-size-fits-all solution. Governments will have different circumstances that required different solutions.

Recommendation:

Governments should produce a strategy for making the transition. It might start with an analysis of various government approaches and then creating, publishing and maintaining a catalogue of ISPs, networks and applications that are either IPv6 capable, ready, or enabled.

Barrier 3 – Lack of Priority

Barrier: Lack of priority given to making the transition.

Discussion

Even if there is acceptance of an impending problem, there is always the issue of prioritisation. Sceptics may not accept the timescales being predicted and of course there are always the issues of "We've got more important project work to do" or "Our IT plans are already overloaded". Whilst the predicted timescales are not cast iron certainties and there are emerging transition arrangements that can delay the inevitable, it is only a matter of time before the full transition to IPv6 will need to be made.

Recommendation:

Governments must accept the advice being given about timescales and re-assess their IT programmes and project plans to give the IPv6 transition work the priority it requires. It is advisable to establish a single project for the transition within their overall IT programme with a series of small step projects rather than one big bang approach.

Barrier 4 – Lack of Funding

Barrier: Lack of necessary funding being allocated to deliver the transition strategy.

Discussion

It is likely that the IPv6 transition will not have been built into any long-term budgetary plans and hence finding the money to implement the solutions will cause a great strain on already over-stretched public finances. IPv6 hardware support will increase costs and also IPv6 software development will be expensive. It is therefore imperative to plan well in advance, spread the transition over as long a period as possible given the specific circumstances pertaining to each Government, and taking a cross-government strategic approach rather than implementing ad-hoc agency solutions.

Recommendation:

At the earliest opportunity re-assess Government ICT budgets to identify the funding required for the IPv6 transition. This will require an analysis first to establish what the funding need might be and its phasing, and particularly identifying where there is a funding gap on the critical path.

Barrier 5 – Lack of Supplier Buy-in

Barrier: Suppliers of Government systems fail to make the transition in line with Government wishes.

Discussion

Governments will be very dependent on their current, and potential new, suppliers in making a smooth transition to IPv6. However problems can occur, for example:

- the suppliers don't plan to move to IPv6 in the same timeframe
- the suppliers don't agree with the urgency
- the suppliers' plans for how to make the transition are different to the Government's

Good supplier management can help to find solutions to these sorts of problems and this topic should become a regular agenda item on supplier management meetings.

Recommendation:

It is very important to work with all suppliers to remove any bottlenecks before they arise.

Barrier 6 – Lack of Technical Ability

Barrier: Lack of required technical skills in-house to implement the transition.

Discussion

The implementation of an IPv6 transition plan will take most Governments into new territory and it is possible that they will not have sufficient skills for this in-house or the limited skills they do have are engaged on other things. It is advisable therefore to plan to buy-in or loan the expertise in the short term, and in parallel build a longer term strategy to develop in-house capabilities. Estimates of how long it will take to complete the full transition to IPv6 vary but it is likely to be several years, so it will be worth investing in a long-term skills strategy.

Recommendation:

Do not under-estimate the need for skills when introducing a transition project and decide how to fill the gaps very early on in the implementation plan.

Barrier 7 – Too Much Legacy

Barrier: Transition difficulties caused by a lot of old legacy systems.

Discussion

There are a number of specific problems caused by old legacy systems and for some Governments these can compound the overall problem. For example:

- the manufacturer no longer exists
- the manufacturer refuses to support IPv6 or makes updates prohibitively expensive
- software upgrades are impossible (software is in permanent ROM)
- a device has insufficient resources to implement the IPv6 stack
- IPv6 is supported but performance is poor

For any of these issues the solution may be extremely difficult and/or extremely expensive. It may be after full investigation that the complete replacement of the legacy system is the only real alternative but that of course can impact on resources and funding.

Recommendation:

When formulating transition plans, identify very early on those legacy systems that are most likely to cause problems and decide how to deal with them. At the same time review all procurement contracts for specific assurance that they are delivering IPv6 ready solutions.

Summary

The increasing problem of a diminishing stock of IPv4 addresses is not going to go away and therefore immediate action is required to start putting in place the necessary transition arrangements to IPv6. Experiences of avoiding chaos in the Year 2000 crisis showed that solutions cannot be put in place overnight. Detailed planning, funding, resources and prioritisation need to be allocated to the issue and all of that takes time to put in place. With the current stock of IPv4 addresses likely to run out in the next 2 or 3 years action has to be taken ***now***.

We support the recommendations made in the OECD's report[4] "Internet Address Space: Economic Considerations in the Management of IPv4 and in the Deployment of IPv6, Ministerial Background Report" that Governments should create a policy environment conducive to the timely deployment of IPv6 by:

1) Working with the private sector and other stakeholders to increase education and awareness and reduce bottlenecks;
2) Demonstrating government commitment to adoption of IPv6;
3) Pursuing international co-operation and monitoring IPv6 deployment.

There are plenty of guidance websites[5] and use cases[6] to refer to about the technical challenges involved in making the transition but there is less written about the political and strategic issues. This paper seeks to help with those aspects and sets out the recommendations of the OASIS eGov Member Section on how to remove the barriers that are and can impede Governments in starting the transition process. The views expressed and recommendations made in this paper are not those any particular individual or government body, they are an agreed consensus of views made by the Member Section.

Contacts and Additional Information

This Document and other documents can be obtained through the OASIS website [Ref 1].

For more information on how to participate in eGov Member Section activities, please contact the eGov Member Section [Ref 2]

[4] www.oecd.org/dataoecd/7/1/40605942.pdf

[5] www.ipv6forum.com/

[6] www.ipv6.org/

Appendix A – Case Studies

1. Canada

The Government of Canada (GC) is currently establishing a high-level GC IPv6 Transition Strategy. They have established a working group with the mandate to recommend a GC IPv6 Transition Strategy.

The WG is currently conducting an IPv6 Transition Assessment which includes the following activities:

a. Establish a clear statement of the problem and key issues associated with not transitioning to IPv6 in a timely manner;
b. Research the IPv6 status of the telecommunication industry (i.e. private sector) and its capacity/capability to support the IPv6 in GC initiative;
c. Establish the IPv6 high-level requirements (i.e. time pressured requirements) to be used to recommend the IPv6 Transition road map;
d. Research similar initiatives and identify best practices, lessons learned, and achieved benefits (e.g. USG 2008 transition, Australian Gov. transition);
e. Recommend an IPv6 Transition roadmap (i.e. short-term, medium-term, long-term strategies) along with perceived challenges and how it will ensure continuous support for the achievement of the GC strategic goals;
f. Establish an estimate of the activities (i.e. WBS), cost, and resources required to implement the recommended roadmap;
g. Develop and nurture the GC Community Of Expertise (CoE) for IPv6; and
h. Promote the need to transition to IPv6 to ensure that all stakeholders become aware of the potential impact IPv6 may impose on their business operations and provide to them the opportunity to plan accordingly (e.g. requirements, budgets).

This group should be finishing its work by September 2010 and then the transition projects will start in earnest.

2. New Zealand

The New Zealand Government is using one agency (Department of Internal Affairs) as a pilot for transition and then will reverse those learnings into a transition strategy group.

3. USA

The Department of Defense is leading the U.S. Federal sector on the IPv6 transition.

4. Australia

The Australian Government has developed ‘‘A Strategy for the Implementation of IPv6 in Australian Government Agencies”[7]. The strategy sees Agencies having their IPv6 ready hardware and software in place by end 2011 and having all systems IPv6-enabled by end of 2012. This means that:

• Government services will remain accessible to all citizens, regardless of whether they are using IPv4 or IPv6;

• Agencies are able to access web based services, regardless of whether they are provided over IPv4 or IPv6.

[7] www.finance.gov.au/e-government/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdfgovernment/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf

Appendix B – References

The following references are either used directly in this paper or the material within them has been used to help formulate the advice and recommendations.

1. OASIS

   see www.oasis-open.org

2. eGov Member Section

   see www.oasis-egov.org

3. Wikipedia - IPv6 Deployment

   see http://en.wikipedia.org/wiki/IPv6_deployment

4. BBC News article on criticality of making the transition

   see http://news.bbc.co.uk/1/hi/technology/10105978.stm

5. OECD/ITAC ICCP room document on the “Evolution of the Internet’s Address Distribution Function, IPv6 and the Role of Government”

   see www.internetac.org/?p=455