IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

IPv6 state-sector adoption Phase 1: Report on status and barriers

Executive summary

This report finds that:

1. the majority of organisations interviewed have tackled, or are tackling, IPv6 for their external Internet presences.
2. 2012 should see an adoption spurt as planning turns to execution for the early adopters.
3. there is an emerging policy thrust by central government to encourage IPv6 adoption, backed by IPv6-enabled 'common capability' services purchasing.

A number of common barriers have been identified, both business and technical. Lack of clarity of business case (costs vs benefits) for pursuing IPv6 implementation remains the most common business barrier. Organisations advancing their IPv6 plans most commonly quote accessibility from developing markets, and future risk mitigation as their drivers. Lack of IPv6-ready LAN networking and firewall design skills are the most significant technical barriers.

Proposed response options centre around benchmarking, education (both business and technical) and continued engagement.

The recommended next steps (Phase 2) for this project include continued engagement with the state-sector (in particular on an agreed joint programme with Department of Internal Affairs), the execution of a Wellington-based implementation-focused one-day IPv6 event, targeted discussions with key suppliers and organisations, and the development of a New Zealand IPv6 benchmarking framework.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Status and forecast trajectories

Selection for interview

State sector organisations interviewed were selected via a prioritisation process, which ranked across four factors:

1.   popularity of public website (based on data from alexa.com, Netcraft, Nielsen)
2.   requirement for access internationally, particularly in developing countries
3.   current and near-term demand for accurate geo-location and for mobile access
4.   advanced services requirements, eg VPN, P2P, streaming, video conferencing

Table 1: Summary pivot table of engagement prioritisation analysis

	Importance of IPv6 to organisation			
Sector	**High**	**Medium**	**Low**	***Total***
Core Govt	7	5	3	*15*
Crown Entity	4			*4*
Local Govt		1		*1*
R&E		9		*9*
SoE	3			*3*
Grand Total	14	15	3	*32*

The subset of organisations assessed as being high priority, i.e. having a strong probable need for IPv6 (at least on their public facing services, including websites) has 14 members. To this high priority 14 was added a local government organisation and the major tertiary education institutions, leading to a target list of 24 organisations to interview.

Table 2: Priority organisations for engagement

Core Government	**Crown Entity**	**SOE**	**Local Government**	**Research & Education**
Immigration NZ (DOL) Land Information NZ Statistics NZ Ministry of Culture and Heritage Customs Service Ministry of Foreign Affairs + Trade NZ Trade + Enterprise	TVNZ Tourism NZ Radio NZ GeoNet (GNS Science)	MetService Kiwibank NZ Post	Auckland Council	University of Auckland University of Otago Waikato University AUT University Massey University University of Canterbury University of Canterbury Unitec Victoria University

Note that not all prioritised organisations were interviewed for this report, and that some organisations that were not initially prioritised emerged during the process as being important to speak to.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

IPv6 adoption quadrant

The information gathered through the interview process was largely unstructured. Detailed notes from these discussions have been captured but remain confidential. To present the data in a rapidly digestible form, this report uses an adapted version of the Gartner "magic quadrant".

One problem of such quadrants is that they are static in nature. To give a sense of the trajectory of the entire sector towards IPv6 adoption, a 'forecast vector' is also plotted for each organisation. (**Note** *that both the positioning of each organisation and associated forecast vector are the author's interpretation and should not be taken as a definitive statement of any organisation's actual plans or likely outcomes.*)

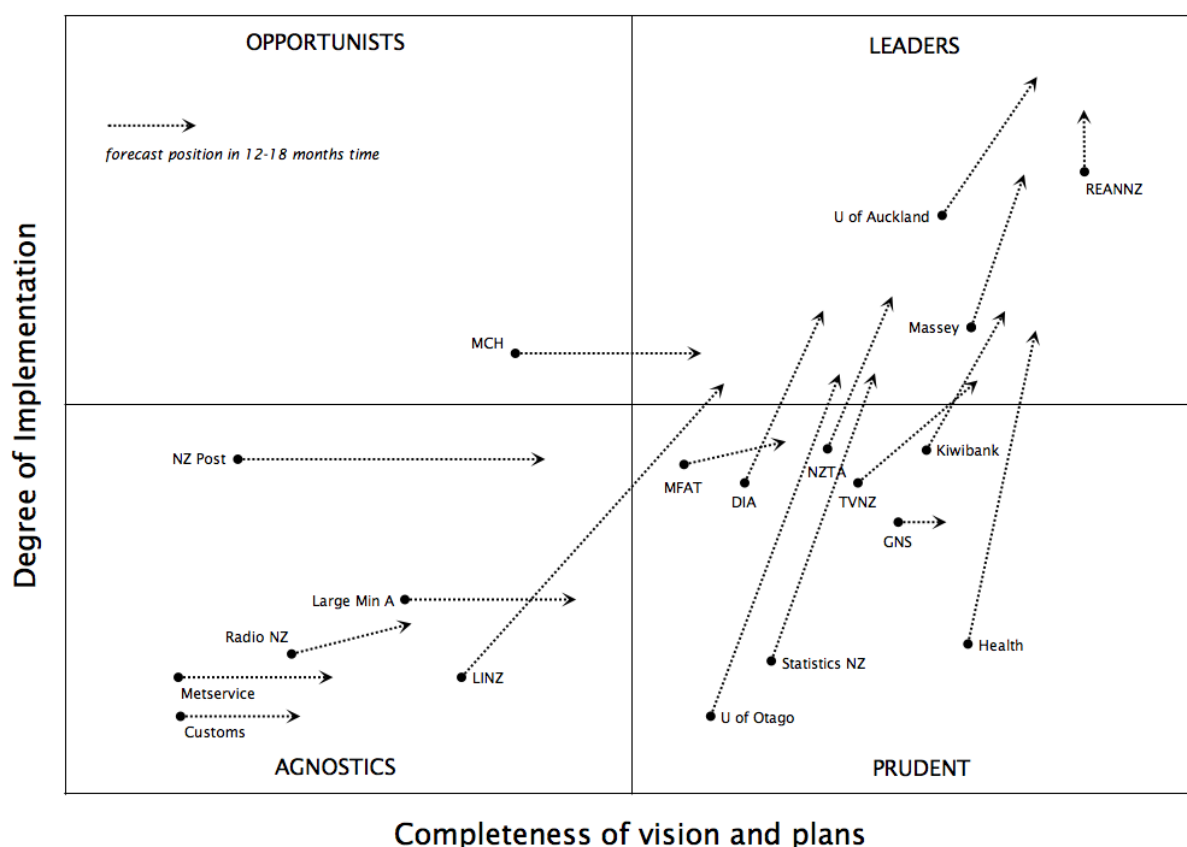Summary comments on each organisation are presented below the quadrant.

Figure 1: IPv6 Adoption Quadrant

Quadrant descriptions

- **opportunistic** - see the value, and seize chances to implement when presented to them, but usually lack a firm view and plan / timetable across the whole organisation.
- **leaders** - irrespective of route taken to be here, have been doing IPv6 for some time and it is an integrated requirement in all of their operational thinking.
- **agnostics** - are not convinced that IPv6 will impact their business (and have made a conscious choice not to plan to implement), or are very early on the IPv6 journey.
- **prudent** - are on the journey to IPv6 implementation, usually as a result of making it a future 'BAU requirement'; may be waiting for resources or the compelling "reason to implement".

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Summary analysis

Awareness of IPv6 and of IPv4 exhaustion is high in the government and wider state sector, as Task Force surveys have demonstrated. The good news is that almost everyone is specifying IPv6 readiness in hardware they are buying, or in their hosting / ISP services. This means that general IPv6 "readiness" is steadily encroaching across the sector.

There is a lot of real **planning** for IPv6 going on - some of it stimulated and accelerated by the engagement process supporting this report. Those 'planning and/or doing' are clearly the majority. It appears that 2012 will be watershed year where many organisations anticipate making at least some of their public services available natively on IPv6 - or having the capabilities in place to do so if they wish.

When it comes to **implementation**, the situation bifurcates reasonably clearly into those actually doing some implementation (or at least with solid near-term plans and intentions) to those with no plans. At the risk of some gross generalisation and simplification:

Those organisations planning and/or doing....
> … tend to be driven by IT specialists making it a part of BAU (sometimes with sanction and encouragement of executives), more than "top-down" near-term business drivers from senior management. These IT specialists see IPv6 readiness as good practice, having little incremental impact on costs and good risk management for the future.

Those organisations with no plans...
> ...tend to be where IT departments do not consider IPv6 to be a relevant problem; believe that someone else will solve it for them (cloud translation services); consider that there is no business reason to be doing anything; believe that it is going to be expensive and difficult to tackle; or simply just have no spare resources to devote to thinking about it.

Outsourced services are providing a scale and expertise advantage that is allowing some organisations to get IPv6-ready more quickly, and with less cost and risk, e.g. those using content delivery networks and hosting providers. This trend is likely to continue as organisations seek cost reductions and the government's 'common capability' procurement initiatives expand.

Summary observations by organisation

Not all target organisations were available to be interviewed. Equally, some organisations not on the priority list were discovered during the process to be important, including Xero and the Department of Internal Affairs.

State sector / organisation	Observation
SOE	
Metservice	Has been specifying IPv6 capable hardware for 18+ months. No current plans to implement. May or may not be a specification for internal services development.
Kiwibank	In a start of advanced preparedness: all equipment and services being bought with IPv6 as requirement. Has internal testing lab. Probable roll-out in 2012.
NZ Post	Participated in IPv6 Day with nzpost.co.nz [2404:130:80:10::18:12] - taken down as proof-of-concept. No wider strategy in place, but considering an audit and standard approach. Plan to add IPv6 requirement to current market discussions.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

TVNZ	Clear driver to make content available to all and see IPv6 as a future accessibility issue, so want to get ready. Have /48 from APNIC, staff trained. Aiming for some external deployment happening early in 2012. Upstream ISP v6 ready;, been buying v6 ready hardware. CDN (Akamai) and tunnelling - potential geo-fencing problem
Crown Entity / Company	
Radio NZ	Runs Linux which is IPv6 capable. Issues with IPv6 tunneling will prevent moving streaming services to IPv6 for foreseeable future. May move static web elements - but no current driver. (Web Operations only)
REANNZ	Has been running IPv6 internally and on KAREN since 2006/07. All services dual-stacked as strong driver being KAREN. Website still not accessible via IPv6 due to hosting partner firewall issues.
Core agency	
Ministry of Culture and Heritage	Websites IPv6 enabled, by virtue of hosting provider (Modica). Organisation building IPv6 into future internal network upgrade plans (including email) but has no current timing for this work.
NZ Transport Agency	Key websites likely to be live late this year and early 2012. Implementing as part of contract changes to ISP and hosting. All sector standards being renewed have IPv6 capability specified.
Department of Internal Affairs (inc Passports)	Has plans to make all web properties IPv6 enabled in coming 12 or so months. Has experimented with internally hosted site. Internal procurement policy in place requiring IPv6 capable services and kit.
Large Ministry A	No plans, or plans to plan. Is a one.govt customer. Likely to wait to see outcome of common capability IaaS deal - IPv6 would be part of any large upgrade.
Land Information NZ	In the middle of major migration. After discussion, will plan on IPv6 enabling into website and open data service (both on Ubuntu and w/ one.govt so IPv6 ready). No impetus for internal network transition.
Statistics NZ	Trying to get something done by mid 2012 - starting on a smaller web property. Project underway.
Customs Service	Aware, but no current plans around IPv6. ISP planning to offer IPv6 services during 2012.
Ministry of Foreign Affairs + Trade	Is largely capable in terms of hardware and services, having specified IPv6 capability in its recent WAN upgrade and kit. However, no plans to turn it on until told, or a clear requirement is demonstrated.
Ministry of Health	In process of new ICT plan, involving movement of web properties to an IPv6 capable provider. IPv6 specified in these plans.
Tertiary and Research	
GNS Science	Is largely IPv6 ready on LAN/WAN; waiting for proven need to turn on. Has recently refreshed L3 kit and that is all IPv6 capable.. Websites run on v6 capable OS and ISP is IPv6 ready.
University of Auckland	Computer Science dept has been IPv6 enabled and on the web for some years. Solid plans in place should see main website live on IPv6 late 2011/ early 2012, with internal roll-out starting later in 2012.
University of Otago	Major LAN/WLAN upgrade being planned. Includes spec for IPv6 capability. Planning to start with main website and key apps. Likely progress during 2012.
Massey University	Has been running IPv6 services (email, web) for several years due to clear need (China relations). Internal networks still to be fully dual-stacked, but planned. Some problems with firewall upgrades and security policies.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

In context with the private sector

To gain some context on where state sector agencies sat with respect to private sector organisations regarding IPv6 adoption, Xero was interviewed. Xero was selected as an example of an organisation that is technically advanced and operating across multiple economies. If placed on the above quadrant, Xero would be in a similar location to TVNZ, NZTA and Kiwibank. Although ready and capable to turn on IPv6 for external services thanks mainly to its outsourced suppliers being ready, Xero sees no near-term drivers to flip the switch yet and bear the additional operating burden as it does not operate significantly in countries that are leaders in IPv6 implementation.

Identified barriers

Where issues and challenges were raised multiple times by interviewees, this report considers them *common barriers to IPv6 adoption*. These common barriers are highlighted below under two categories: business and technical.

Business barriers

Absence of a business driver

Times are tight financially, especially around Wellington's core government sector. Many organisations who lack a clear specification from their business users are not actively planning to deploy IPv6. Most are specifying IPv6 capability in their hardware, and have been for some time. Often, executive's do not appear to have made the connection between IPv6 as an apparent 'future technical matter' and their ability to provide / sell services in developing markets.

Potential response: *Exposure to stories of, and interactions with, peers who have gone IPv6 already with a focus on it being good risk management. The Wellington IPv6 Govt-centric event should cater for this audience. More case studies could help at the executive level. Create a business driver simply by allowing them to benchmarking their organisation to the rest of New Zealand and the APAC region. On-going engagement to continue the debate.*

Lack of an internal champion

Organisations that have made the most implementation progress have usually had a strong internal champion; often just the one person. Whilst this has sometimes been the CIO (or relevant senior IT / Operations role), more often than not it is someone reporting to them.

Potential responses: *Target organisations in the "agnostics" quadrant and encourage members of the IT team to get some training and/or attend the Wellington IPv6 event. Possibly provide an IPv6 "buddy" scheme, where a practitioner from the "leaders" quadrant is joined with an emerging practitioner on an informal, peer-to-peer basis.*

Uncertainty of costs and approach

As a relatively new implementation issue, there is not a good understanding of the costs and "best common practice" that might be involved for an organisation implementing IPv6. Equally, organisations may be unaware of their current state / readiness of their services and infrastructure.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

For some, this provides a valid reason to delay, and exposes business cases to higher uncertainty for those proceeding.

Potential responses: *Produce some 'hard' case studies with estimates of incremental costs for those that have already done some IPv6. Provide real hands-on configuration workshops at training / exposure events. Encourage IPv6 Audits and Consultancy by the supplier community. Expand / implement a section on the website ipv6.org.nz with links to tools, other case studies (culled to some extent from blogs, but extending beyond this).*

Unclear business model for service providers

Integrators, service providers, ISPs, hosting providers and hardware vendors do not see a clear upside sales opportunity in IPv6. Some have done IPv6 as it's the "right thing to do". (There are hints that things are changing, in that suppliers who are not IPv6 ready are starting to lose out given the level of IPv6 requirements in recent tenders.)

Potential responses: *Work with a few most-used service providers in government to ensure they have a good understanding of the importance of IPv6 and help them to identify IPv6-related opportunities. Benchmarking also has a role here as it can provide confidence of the need to tackle IPv6 and encourage suppliers to dedicate time and resources to developing offerings.*

Technical

Design for large, complex internal networks

For small, well understood, networks, simply enabling IPv6 autoconfig on a compliant edge device is an easy and simple process. However, for larger organisations many issues are not well enough understood: how to address and manage multiple VLANs, DHVCPv6 vs autoconfig decisions, varied server and hosting environments, VPNs, LDAP and other networks services, DNS promulgation in IPv6. Very often different paradigms / thinking to IPv4 is required.

Potential responses: *Encourage a range of education - both top-down and peer-to-peer, e.g. hands on sessions, lectures, courses, case studies. The supplier community in particular can have a role to play here by allowing some of the problems to be uncovered, quantified and outsourced in Audits.*

Security (firewalling) underdone and not well understood

This point accompanies that on internal network design. Firewall / organisation security is a very important IPv6 issue as it applies even if an organisation is not actively deploying IPv6. There are issues around firewall settings (ICMP, NAT is gone, multicast non-optional, multiple addresses per interface) that mean skills from IPv4 are not directly translatable. It is critical to get security skills and approaches up to speed so as to not slow down the forecast 2012 adoption spurt.

Potential responses: *As above.*

6to4 Tunnelling issues

Billed as, and commonly used as, a way to bridge IPv4 islands, 6to4 tunnelling is built into most modern operating systems. However, several organisations have raised it as a serious potential barrier to IPv6 adoption. Where organisations are serving content form multiple global locations, e.g.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

via a content delivery partner of themselves, then 6to4 tunnelling can impact the latency and reliability of service as it masks the geo-location of the user.

Some organisations raised questions relating to the geo-fencing of content - the need to control access to content based on location (and usually achieved via IP addressing).

Auckland University's Brian Carpenter has a draft advisory RFC out that covers the issues:
http://tools.ietf.org/html/draft-ietf-v6ops-6to4-advisory-02

Potential responses: *As above. (Note that IPv6 tunnelling is on the decline over the last year, and may be declining as an issue).*

Vendor readiness vs promises

Some, indeed most, of those interviewed that have implemented IPv6 on their public websites or internal networks have reported a relatively painless and quick process. Where problems have existed they have principally been around firewall and DNS hosting issues.

However, one Leader, Massey University, had to temporarily roll-back bits of its IPv6 deployment due to vendors over-promising on equipment and service readiness. It is also the case that in some areas, IPv6 functionality is not yet on par with IPv4 and many organisations are waiting for full feature parity to reduce operational cost.

Potential responses: *As above, including direct engagement with an identified sub-set of principal suppliers and systems integrators.*

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Summary matrix of barriers and response options

Plotting barrier vs. response in a sparse matrix shows that the best approach to addressing business barriers are likely to be benchmarking, one-on-one engagement and great, detailed, case studies. Technical barriers are more likely to be addressed through case studies, encouraging audits, providing training and continuing to engage in on-going discussions (via website, through follow-up meetings).

The Wellington-based government-centric IPv6 one-day event could provide an opportunity to tackle several of these response options.

Table 3: barriers and response options matrix

	Benchmarks - NZ	Benchmarks - Global	1-on-1 engagement	Great case studies	Encourage audits	Encourage / provide training	Continued dialogue
Business							
Absence of business driver	X	X	X	X			X
No internal champion			X			X	X
Uncertainty of cost & approach				X	X	X	
Unclear business model for service providers	X	X	(X*)	X			X
Technical							
Design for large, complex internal networks					X	X	X
Security underdone and not well understood				X		X	X
6to4 tunnelling issues					X	X	X
Vendor readiness vs promises			(X**)			X	

* - whilst the Task Force is a neutral body, there is a case for discrete engagement with the largest suppliers to government
** - if a sub-section of the supplier or equipment market was deemed to be of particular importance (in either magnitude and/or commonality), there may be case for discrete engagement with those suppliers.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Positive themes

As included in the summary analysis above, the engagement process uncovered findings that were relatively positive in relation to IPv6 adoption.

Having the conversation is important

As IPv6 represents a future business risk for most organisations, it can easily be forgotten, even by experienced and knowledgeable network staff. Indeed, the engagement process behind this report itself has prompted several organisations to accelerate their IPv6 planning. By simply maintaining a dialogue - on a one-to-one or event-driven basis - the Task Force is ensuring that IPv6 capability gets embedded as a 'check box' on plans.

"It's not a huge project, it's a business-as-usual specification"

The foundations are (being) laid

As above, laying the foundations so that everything is IPv6 capable, appears to be going well. Whether that is MetService's or DIA's procurement specifications, or all the one.govt and IaaS 'common capability' offerings being IPv6 compliant. Only a very few organisations were not specifying IPv6 capability under current procurement.

This is a particularly strong story emerging theme that is inline with the TF's recommended approach and should make for a much easier transition to 'turning on' IPv6 for organisations.

Outsourcing the problem to solve it

Organisations of all size increasingly have elements of their infrastructure hosted and managed by a specialist provider (primary servers, DNS, content delivery network). The scale and specialisation of outsources is generally resulting in greater levels of IPv6 readiness and implementation sooner than self-managing organisations.

This has a double benefit: the organisation gets a lower risk, (probably) lower cost and earlier IPv6 implementation; suppliers can differentiate their services.

Government 'common capability' deals will be vital

The DIA procured one.govt and IaaS deals are very important enablers. One.govt is already IPv6 enabled (for WAN and Internet) and DIA has confirmed that the upcoming one.govt mail, firewall and voice.video gateway products are also going to be IPv6 ready from the outset. The recently completed procurement process for hosted and virtual servers (Infrastructure as a service - IaaS) also has a requirement that these are v6 ready from the outset.

Over the coming 12-36 months, as an increasing number of organisations take advantage of these 'common capability' services, IPv6-readiness will increase steadily. Turning readiness into implementation (turning it on) may require some specific / targeted work to identify a clear driver for a some leading agencies, from which case-studies showing how easy it is can be developed.

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Phase 2: proposed next steps

Phase 2 of this project will need to tackle the outstanding contracted deliverables (see Annex 1), i.e.:
- Development of options to accelerate [induce] adoption and test these with at least one organisation.
- Working with the Task Force members to help ALGIM to develop a white paper and other mutually agreed collateral to assist their members in the adoption of IPv6.

Recommended next steps that are in-line with the contracted objectives for this work and the findings of this report are:
1. Ongoing work with the DIA to engage and communicate with core agencies (set and communicate the "expectation").
2. Support planning and implementation of a Wellington government-focused IPv6 event, focused on implementation.
3. Work with a subset of the top providers of IT services to government to enhance their IPv6 offerings (leverage industry sales force).
4. Survey hosting providers and ISPs for IPv6 readiness and plans and update directory on IPv6.org.nz.
5. IPv6 Benchmarking: support nascent work on IPv6 benchmarking and deliver a practical set of measures for NZ, available publicly.

Disclaimer and Copyright

IPv6 state-sector adoption
Phase 1: Report on status and barriers
Donald Clark
Version: Final

Annex 1: Phase 1 Method

Scope (from contract)

Encourage and support government agencies (central and local) to implement IPv6 on their internal and external networks in coordination with the work of the IPv6 Task Force.

Deliverables (from contract)

- Engagement with key influencers to encourage adoption of IPv6 in central and local government, including science and research institutions.
- Summary of barriers to adoption of IPv6 within central and local government.
- Development of options to accelerate [induce] adoption and test these with at least one organisation.
- Working with the Task Force members to help ALGIM to develop a white paper and other mutually agreed collateral to assist their members in the adoption of IPv6.

Hypothesis

The public sector (specifically central and local government) is lagging the NZ private sector and comparable international government sectors in its adoption of IPv6.
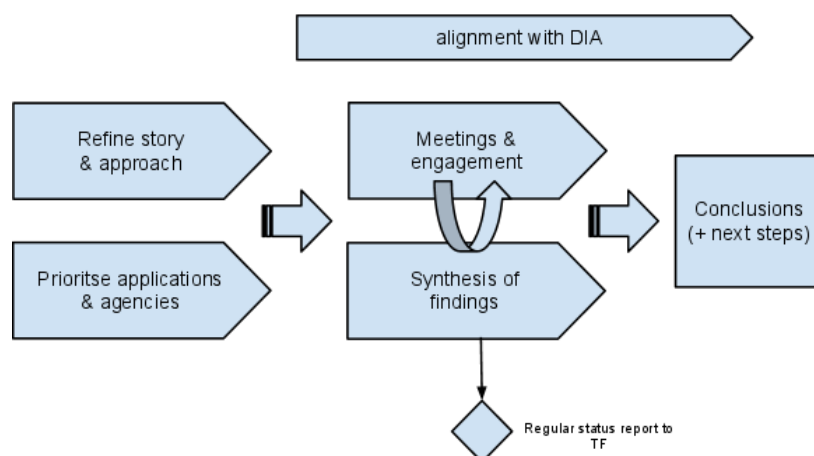
Supporting observations

- low[ish] / declining response in IPv6 surveys
- very low numbers of government websites / services already IPv6 capable
- lack of enforced standards and procurement guidelines regarding IPv6

Method

As per the Deliverables (above), more specifically as set out in the diagram below.

1. leverage work to date, including the upcoming 'state of the nation' deck to create an agreed 'story' deck, including various options.
2. at the same time, develop a working list of prioritised agencies to engage with (see Annexes).
3. As engagement progresses, insights will emerge that will become increasingly solid over time - these will be reported regularly to the TF.

Critical success factors

1. Alignment between TF and DIA on the process and scope of this workstream.
2. Access to the right CIOs / CEOs and specialist network and applications staff in each agency.
3. A gentle approach that induces open and positive behaviours -> cajole, network, share, expose vs name + shame.