1. ADF IPv6 Transition Strategy

NCW - BATTLESPACE OPERATIONS RESEARCH GROUP

Delivering An Operational Edge Through Collective Thinking, Applied Science & Systems Engineering

AUSTRALIAN DEFENCE ORGANISATION CDR-01 INTERNET PROTOCOL VERSION 6 (IPV6) TRANSITION PLAN

Issue 1 Revision 1.5 (Final)
Date: 29 July 2005

Ball Solutions Group
Level 2, John McEwen House
7 National Circuit, Barton ACT 2600
Postal: PO Box 3276 Manuka ACT 2603
Telephone: (02) 6270 7777 Facsimile: (02) 6273 8125

DOCUMENT VERSION HISTORY

Issue	Revision	Date	Authors	Reason for Change
0	0 - 7	18 May 2005 – 9 June 2005	Paul Burns and The Panel	Draft document versions.
1	1.0	30 June 2005	Paul Burns and The Panel	Creation of Issue 1 Document.
1	1.1	14 July 2005	Paul Burns and The Panel	Workshop issues, and Commonwealth comments to Draft Plan incorporated.
1	1.2	21 July 2005	Paul Burns and The Panel	Additional input following Panel review.
1	1.3	25 July 2005	Paul Burns and The Panel	Reorganisation of introduction section.
1	1.4	27 July 2005	Paul Burns and The Panel	Completed the Executive Summary and Conclusions.
1	1.5 Final	29 July 2005	Paul Burns and The Panel	Final version for Work Package 2.

Introduction

Introduction

This Australian Defence Organisation (ADO) Internet Protocol Version 6 (IPv6) Transition Plan (IPv6TP) has been developed by Ball Solutions Group "BSG" in collaboration with a Panel of UK and US subject matter experts "the Panel". The Panel has members from the IPv6 Forum, QinetiQ, the Naval Post Graduate School (NPS) and the World Wide Consortium for the Grid (W2COG). This plan was developed over the period from May through to July 2005 via virtual collaboration (email) between the Panel and three teleconferences between all parties.
A draft version of the plan was delivered to the Commonwealth in June and was the subject of a workshop on 29 June 2005 with the Commonwealth, BSG, NPS and QinetiQ Panel members. `
Section 3 of the plan provides the top-down methodology used to generate the recommended IPv6 transition strategy which is detailed in Section 4 of this IPv6TP. The plan provides an IPv6 address space recommendation and includes sections on Governance, Workforce and Risk.

Acknowledgements

BSG would like to extend its special appreciation to Mr Jim Bound (IPv6 Forum), Mr Rex Buddenberg (Naval Post Graduate School) and Mr Chris Gunderson (W2COG) who volunteered their time on behalf of their respective organisations to make crucial and major contributions to the development of this IPv6 Transition Plan for the ADO. The Panel consisted of the following individuals:

Name	Organisation	Title	Role
Paul Burns	BSG	IPv6 Transition Plan Task Manager	Overall task management and point of contact for all personnel and the Commonwealth.
Phil Ashton	BSG	Systems Engineer	Task support
John Pennington	QinetiQ	Senior Principle Consultant - Networks	Contracted to BSG to provide expert IPv6 support.
Jim Bound	IPv6 Forum	Chief Technology Officer	Voluntary provision of expert IPv6 consultancy services.
Rex Buddenberg	Naval Post Graduate School	Professor, Department of Information Science	Voluntary provision of expert IPv6 consultancy services.
Chris Gunderson	W2COG	Executive Director	Voluntary provision of supporting IPv6 consultancy services.

Scope

The scope of this IPv6TP covers the Australian Department of Defence, Defence Information Environment (DIE). Figure 1 indicates that the DIE is composed of Information Domains built upon the Information Infrastructure. Information is currently transported around the fixed and deployed infrastructure by a mix of IPv4 and other non-packetised and/or switched-circuit means. The fixed and deployed infrastructure is composed of an enterprise network and a tactical network.

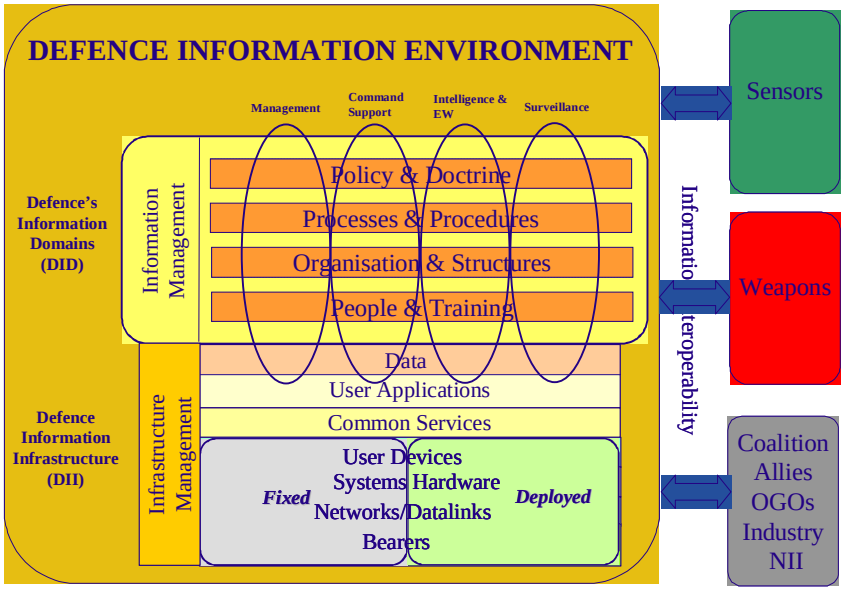


Figure 1 Defence Information Environment

ADO IPv6 Transition Policy

The ADO issued the policy "Transition To Internet Protocol Version 6" [1] in February 2005. The policy states that the transition process will have broad reach across the DIE and involve all[1] Defence computer operating systems, network operating systems, network services, information services, core and distributed networks, and many of Defence's corporate applications.

Policy Statements

The policy states;

- all DIE networks to have completed IPv6 transition by 2013;
- no IPv6 capable hardware or software shall be installed on ADO networks carrying operational traffic unless a risk assessment has been completed, the result approved by the CIOG and use is authorised by the CIOG in consultation with Headquarters Joint Operations Command (J6);
- no IPv6 capable hardware or software shall be installed on ADO networks carrying operational traffic unless a risk assessment has been completed and the result approved;
- the cost of transitioning will be reduced by leveraging information technology (IT) refreshment programs;
- DIE IP enabled hardware and software procured or upgraded that is likely to be in service after 2013 shall be acquired with an IPv6 capability or an upgrade path that will allow it to be upgraded prior to 2013;
- from 1 March 2005 all DIE IP enabled procurements should be both IPv4 and IPv6 capable provided the cost of procurement or the marginal increase in the whole of life cost is acceptable and
- current in-Service ADO equipment that has a scheduled end-of-life before 2010 is exempt from the policy.

The drivers for ADO transition to IPv6 are stated in the policy as follows;

- improved end-to-end network security over IPv4;

[1] It is assumed that "all" relates to all the mentioned systems (e.g. Defence computer operating systems etc) within the DIE.

- better support for the expected growth in the number of mobile IP enabled devices, compared with that provided by IPv4;
- the ability to improve the QoS for IP communications compared with IPv4;
- simpler network management through more efficient hierarchical addressing and routing processes compared with that provided by IPv4;
- is an enabler for the ADO's vision of NCW;
- will aid interoperability with Allies and
- will reduce the likelihood of suffering from technology obsolescence.

The policy also advises that:

- IPv6 migration planning will also develop a consolidated ADO IPv6 address space management strategy to ensure that the ADO's requirements are satisfied and to maximise Allied interoperability and
- the CIOG will manage the transition planning and provide enterprise level guidance on IPv6 transition issues.

This document covers the above "address space management strategy" point in Section 8 and this document as a whole is a part of CIOG's transition planning guidance.

Policy Limitations

The "Transition To Internet Protocol Version 6" policy [1] is aimed at and limited to components of the DIE that;

- are currently IPv4 enabled and will stay IP enabled into the future, or
- components that are not currently IP enabled but will be IP enabled in the future.

The policy does not explicitly mandate[2] the transition to IP per se of components of the DIE that;

- are currently not IP enabled and are not planned to be made IP enabled in the future[3].

Additional Steps To Realising the Policy Objectives

The IPv6 benefits stated in the policy [1] and above in 1.2.1 are not wholly dependent on migration to IPv6, nor will they be guaranteed by migration unless the following significant additional steps are taken:

- Network security
    - High grade IP network encryptors are available now for IPv4 networks. IPv6 capable high-grade products are not yet available off-the-shelf. There is work under way in the US to upgrade the HAIPIE standards to include IPv6.
    - For high grade security there is no significant improvement to be expected from IPv6.
    - The IPSec standards are applicable to both IPv4 and IPv6. Implementations of these standards are widely available, including in Windows 2000 and XP and in most routers. The advantage of IPv6 is that support for IPSec is mandatory and should therefore be provided in all IPv6 capable devices.
    - IPSec VPNs implemented in hosts or routers can be used to provide confidentiality where a lower grade of security is acceptable, for example for 'need-to-know' separation of personnel or financial data.

[2] Although the policy does not explicitly mandate this, it is recommended that some governance measures should be put in place to ensure that all the required elements of the DIE achieve a routable status in the future to enable NCW, see section 1.2.2.

[3] For completeness sake only, there is also the scenario that DIE components that are currently IP enabled could revert "back" to switched circuit (and would therefore not be covered by the policy), however this is not considered as a sensible alternative.

- A public key certificate infrastructure (PKI) is necessary to exploit IPSec. It is expected that the ADO will wish to deploy its own PKI (rather than relying on commercial certification authorities). There may already be a PKI in place to support secure messaging in the ADO, but it would most likely require enhancement to support the more extensive demands of a large IPSec implementation.

- Mobility
  - Mobility is a complicated issue involving potentially many layers of the protocol stack and not just the IP layer. However IPv6 does offer features that can contribute toward improved mobility. If the ADF expects to have increasing movement of users and platforms between networks where the impact is realised at the IP layer, then this feature will be valuable. Please see Annex G for more information on Mobile IP (MIP) and MIP version 6 (MIPv6).

- Quality of Service
  - There is no difference between IPv4 and IPv6 in their support for basic QoS. Although IPv6 packets include a field for flow labels, its use has not been standardized. The QoS field carries the same diffserv code points (DSCP) in IPv4 and IPv6.
  - Effective use of QoS in IPv4 or IPv6 requires ADO-wide agreement on traffic classes, and considerable detailed planning of capacity allocations for each traffic class. If existing service provision contracts do not provide for consistent DSCP definitions, then re-negotiation will be needed.
  - Provision of QoS for Allied networks is an open topic. Currently it is understood that some US networks place Coalition traffic in a different QoS class.

- Network management
  - It is not clear that IPv6 will offer any benefit to network management. There may be potential for some routing efficiencies because of the larger address space, but it will need considerable care in address allocation to achieve this, and the necessary administrative/management overhead may not be justified.
  - The ability of IPv6 to support auto-configuration is often cited as leading to a reduction in management effort. In military secure networks, this must be balanced against the need to have effective control over who or what may connect.

- Address space
  - Although this will be a problem for organizations requiring additional address space, it may not be an immediate problem for the ADO. Unless there are plans to significantly increase the numbers of network elements, then the current allocation should be sufficient. A decision to provide IP capability to all land tactical units would be an example where a significant increase in address space would be required. However, even in this case, a private address range could be used (as the UK MOD is doing within Bowman). A forward-looking long-term view of the potential IPv6 address space requirement is provided in Section 5.

- Interoperability
  - IPv6 everywhere is not essential for interoperability. The extent to which this is required depends on how far the ADF requires network-level interoperability with its Allies.

- Obsolescence
  - Eventually this will be the driver for IPv6 transition. All other issues can be worked around, but at some point it is anticipated that commercial support for IPv4 will be discontinued. The ADO must ensure that all its projects take appropriate action to avoid problems of obsolescence. In most cases this will be dealt with by normal technology refresh activities, although it is noted that refresh

in military systems run over much longer timescales than most commercial IT systems.

Referenced Documents

Publicly Available Documents

This section lists referenced documents including the source if the document is not available through normal Commonwealth channels.

Title	Revision	Date	Source
[1] Defence Information Management Policy Instructions NO 1/2005 : DIE Transition to IPv6		22 Feb 2005	CIOG
[2] IPv6 Essentials, Silvia Hagen, ISBN 0-596-00125-8	1st Ed.	July 2002	O'Reilly
[3] DoD's IPv6 Transition, Michael Brig, German IPv6 Summit Jun/July 2004		July 2004	http:/linda.ipv6.berkom.de/summit/03_mike.brig_DoDs_IPv6_Transition.pdf
[4] Function and Performance Specification DWACN JP2047 Phase 2A - Unclassified		31 May 2002	CIOG
[5] Transforming the Defence Information Environment through Improved Governance, AVM Julie Hammer.		5 November 2004	Australian Computer Society.
[6] Internet Protocol Version 6 (IPv6), John P. Stenbit, US DOD		9 June 2003	US DOD.
[7] NATO IPv6 Transition Planning, Rob Goode, NATO Consultation, Command and Control Agency		26 May 2005	Coalition Summit for IPv6, Reston, VA, 26/5/2005.
[8] IEEE 802.16 COTS Technologies As A Compliment To Ship To Objective Manoeuvre (STOM) Communications. R. Guice & R. Munoz.		September 2004	Naval Post Graduate School Thesis.
[9] IP Version 6 Addressing Architecture			ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-ipv6-addr-arch-v4-04.txt
[10] IETF RFC 3587			http://www.ietf.org/rfc/rfc3587.txt?number=3587
[11] IPv6 Response to National Strategy to Secure Cyberspace	Final V2.0	November 14 2002	http://www.nav6tf.org/documents/Response_NAV6TF_Secure_Cyberspace_Final_V2.pdf
[12] NAV6TF PCIPB Input Part II	Final V2.0	December 2 2002	http://www.nav6tf.org/documents/NAV6TF_PCIPB_INPUT_PART_II.pdf
[13] NAv6TF NTIA IPv6 RFC Response	Final	March 1 2004	http://www.nav6tf.org/documents/NAv6TF_Response_NTIA_IPv6_RFC_FINAL.pdf
[14] e-Nations The Internet for All, NAv6TF.		September 23 2003	http://www.nav6tf.org/documents/e-Nations-Internet-for-

Title	Revision	Date	Source
			All.pdf
[15] IPv6 A Practical Technology Maturity Investigation			Naval Post Graduate School Thesis.
[16] Good Network Citizens, Professor Rex Buddenberg.			http://web1.nps.navy.mil/~budden/lecture.notes/good_net_citizen.html
[17] Radio WAN Protocol Notes, Professor Rex Buddenberg.			http://web1.nps.navy.mil/~budden/lecture.notes/r-wan/radio_wan.html
[18] GIG Strategy, Professor Rex Buddenberg.			budden@nps.navy.mil

Government to Government Documents

The following is a list of relevant IPv6 documents that are not publicly available but are expected to be able to be source by the ADO through its Government-to-Government links.

Title	Revision	Date	Source
[19] Navy Internet Protocol Version 6 (IPv6) Technical Transition Strategy	1.0	30 June 2005	US Navy - Karen ODonoghue karen.odonoghue@navy.mil
[20] US DoD IPv6 Transition Plan		March 2004	ADO has this document.
[21] Draft DoD IPv6 Master Test Plan	Rev .13	December 23 2004	US DoD – Michael P. Brig birgm@ncr.dosa.mil
[22] Security Analysis for DoD IPv6 Transition, Report 1: IPsec; NSA report #I333-011R-2004.	Report 1 : IPsec	June 2004	USA – NSA.
[23] US DoD IPv6 Address Plan			US DoD. (This was prepared for submission to ARIN).
[24] Scoping of IPv6 Migration Strategy		July 2004	UK MOD, Integration Authority.
[25] MOD IPv6 Transition Conference, Malvern U.K.		28 February 2005	UK MOD.
[26] IPv6 Issues NC3A, TN-1053	Draft		NATO.

Acronyms and Abbreviations

ADF	Australian Defence Force
AEW&C	Airborne Early Warning and Control
AG	Application Gateway
ATM	Asynchronous Transfer Mode
BSG	Ball Solutions Group
CIDR	Classless Inter-Domain Routing
CIOG	Chief Information Officer Group
CISSO	Command & Intelligence Systems Sustainment Office
DCN	Defence Communications Network
DCP	Defence Capability Plan
DIE	Defence Information Environment
DII	Defence Information Infrastructure
DISA	Defense Information Systems Agency
DMO	Defence Materiel Organisation
DOD	Department of Defence (Australia) Department of Defense (US)
DWACN	Defence Wide Area Communications Network
FISSO	Fleet Information Systems Support Organisation
FTP	File Transfer Protocol
GIG	Global Information Grid
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPv6TP	Internet Protocol Version 6 Transition Plan
ISD	Information Systems Division (part of the CIOG)
ISSA	Information Systems Security Assurance (a sub-branch of ISD)
JWICS	Joint World-wide Intelligence Communications System
MAN	Metropolitan Area Network
MANET	Mobile Ad-hoc Network
MOD	Ministry of Defence
NAT	Network Address Translation
NAV6TF	North American IPv6 Task Force
NII	Networks and Information Integration
NIPRNET	Non-secure Internet Protocol Router Network
NTIA	National Telecommunications and Information Administration
OSD	Office of the Secretary of Defense
SIPRNET	Secret Internet Protocol Router Network
TADIL	Tactical Digital Information Links
TIEIO	Tactical Information Environment Integration Office

Executive Summary

This Internet Protocol Version 6 Transition Plan (IPv6TP) has been developed by BSG in collaboration with a Panel ("the Panel") of world-leading IPv6 subject matters experts from the IPv6 Forum, QinetiQ, the Naval Post Graduate School and the World Wide Consortium for the Grid (W2COG). The scope for this IPv6TP includes the whole of the ADO's Defence Information Environment (DIE).

This plan commences in Section 3 by using a Systems Engineering methodology to develop the "context" for Internet Protocol (IP) generally within the DIE and the transition from IPv4 to IPv6 specifically. The results of this "context" setting analysis proposes that "modularisation" is the key to achieving interoperability and "net centricity". Two crucial overall design principles were generated, Principle 1 : Unit Level LANs and Principle 2 : Routable WANs. These principles are used throughout as a basis for many section of this IPv6TP.

The Section 3 analysis also produced derived design requirements for the end-systems that connect to the DIE. The context setting analysis concluded with a definition of the boundary between the non-DIE and the DIE, this is important because the boundary often extends into the ADF's tactical environment and its platforms where many of the "legacy" issues will be encountered in the future.

Section 3 also summarises the IPv6 activities being conducted by the UK MOD, NATO and the US DOD. It was concluded by the Panel that because IPv6 has yet to progress to a sufficient state (anywhere in the world) there are currently no "off-the-shelf" strategies that could be applied to the DIE. As a result of this IPv6TP, the ADO is likely to be in advance of many organisations with regard to its IPv4 to IPv6 transition, and potentially better placed to meet its desired time-schedule if the governance mechanisms can be smoothly and successfully implemented.

The current and future DIE was also analysed with specific emphasis on the DWACN. The future DIE architecture was covered by specifying the DCP projects that will move the DIE from its current baseline to its future state.

Section 3 concluded by providing relevant challenges, opportunities and emerging technologies. The ADO can expect to find its major challenges in the areas of transitioning its non-routable networks and security.

The recommended IPv6 transition strategy is provided in Section 4 and depicted in Figure 15, this shows seven overlapping phases commencing from now until 2013. Importantly this strategy allows for a progressive roll-out of IPv6 whilst recognising that some parts of the DIE may never transition and small enclaves of IPv4 will be required past 2013. The strategy has also been designed to be cost-effective, to have no impact on defence operations and not to degrade interoperability with Allies, justification for this is provided in 4.3.

To reduce the level of risk and ensure a successful transition Section 4.4 proposed a range of information assurance and test activities The recommended strategy section concludes with some specific advice for the key DCP projects.

Section 5 provides a detailed step by step analysis method for constructing a robust IPv6 address plan, this indicates that the IPv6 address range could be anywhere between 34 bits (/30 address) and 46 bits (/18 address). Although this analysis requires further work, it is recommended that the ADO attempt to gain access to the largest contiguous block of addresses possible.

Section 6 details a recommended governance structure for the ADO to transition the entire DIE. Two new organizational offices are proposed to ensure that the governance regime is implemented in an astute and timely fashion and that the actual implementation of IPv6 is appropriately funded and scheduled.

The IPv6 Transition Office (IPv6TO) is proposed to be part of the CIOG, its prime responsibility will be as the “interoperability custodian”. The IPv6TO will become the ADO’s centre of excellence for IPv6 and will also offer technical guidance to the whole of the ADO.

The IPv6 Program Office (IPv6PO) has been proposed to act as the Program Manager for the implementation of IP across the whole DIE. Functionally the office must cover the scope of ADO projects from inception through to second pass (where they are under the control of the CDG) then on past second pass and into service (where they are under the control of the DMO). The IPv6PO is envisaged as an Integrated Product Team (IPT) with members from CDG and the DMO. Its creation, function and lines of reporting are seen as crucial to a successful transition. Section 7 details the organisational structure of the IPv6TO and IPv6PO. Each position within these offices is provided with a position description and details of the required competencies and experience.

The conclusion to the process of developing this IPv6 transition strategy was to assess all its elements (including the proposed governance structure and workforce) for risk, see Section 8.

Transition Strategy Analysis

The section applies a top-down methodology and provides several lead-in and supporting topics (Sections 3.1 to 3.5) in order to generate the “Recommended IPv6 Transition Strategy” which is presented in the following Section 4.

Setting The Context For IPv6

In dealing with narrow topics like how to implement IPv6, it's rather difficult to grapple without a clear and detailed context. Indeed, the justification for IPv6 is weak without this context.
It's not clear when or if the ADO will ever run out of IPv4 addresses, therefore the usual address exhaustion reason for justifying IPv6 work is not convincing in the light of real world usage. But placed into an industrialization and network centric context, the case for IPv6 becomes stronger, particularly as a risk mitigation activity.
In order to set an appropriate context we shall use a systems engineering approach, apply a top-down methodology and analyse the following subjects in order:

- Transitioning from artisan-based to industrial based information systems.
- Defining the GIG.
- Over all design principles (These are the principles needed to achieve net-centricity).
- Defining Radio-WAN interface and performance requirements.
- Defining the DIE boundary.

Transitioning from artisan-based to industrial based information systems

A review of the mechanical Industrial Revolution of the 1790s shows us the following:

A. Use of chemical energy to extend man's muscles (steam and internal combustion engines).

B. A transition from artisan to industrial methods of building systems. This transition requires an overall design, but then is able to take advantage of specializations of labour to ease constraints on quality and quantity.

    a. Modularisation of components is essential to the assembly line.

    b. Standards (e.g. bolt threads) are necessary to the modularisation.

    c. Technical training is required in the workforce.

C. Rise of universal public education, where the focus shifted away from Latin and towards maths, chemistry and physics.

These characteristics mirror almost perfectly into the Information Revolution chapter of the Industrial Revolution, this time from the 1990s onwards:

A. We are using the network and the computer to extend man's mind.

B. In a muddling way (because we lack historical perspective), we are shifting to a more industrial method of building information systems. This requires an overall design (see the principles below).

    a. Modularisation is critical to horizontally integrated information systems.

    b. Standards do not solve the modularisation problem (it's entirely possible to use the correct standards, mis-modularise a system and build a non-functional artisan information system), but the standards are essential to defining the modular boundaries. IP (and IPv6) is one among a handful of critical standards necessary to the modularisation problem.

    c. We need a technically trained workforce to manage our information systems. The divisions of labour show up on the job survey analyses but not yet in our skill-set definitions and training.

C. The information technology skill-sets exhibit some patterns that can be capitalised in workforce planning throughout both the commercial and military environments.

Defining The GIG

The US DoD has developed the concept of a Global Information Grid (GIG), however the PowerPoint definitions that are used to describe it are often confusing. For our purposes, the GIG can be defined as the ADO's internet and the definition can be further divided into the following components:

A. **Terrestrial WAN**. This is analogous to the backbone services provided by the DWACN.

B. **Unit level LANs**. In the US Navy[4] there is a good existing proof in the form of the LANs installed their ships. Base/campus area networks are also considered as a good fit into this category.

C. **Radio-WANs**. The purpose of the radio-WAN is to reach from the terrestrial WAN to mobile platforms (that contain the unit level LANs).

D. **End-to-end security**. Familiar link and enclave security techniques must be complemented by end-to-end (or object level, or layer 7) security measures as the GIG grows.

E. **End-to-end management**. It is no longer suitable to manage a network unto itself, the network segment inevitably routes into other network segments and we need to manage end-to-end.

F. **Upper layer protocols**. The advent of reach to mobile platforms will trigger a new generation of upper layer protocols (MANET, NORM, device-aware, IPv6 and others). This topic remains rather moot until some of the above prerequisites appear (especially the radio-WANs), but is mentioned for completeness. The shortcomings of TCP over satellite networks is a well-known example of current-generation symptoms that need to be addressed in due time.

The GIG is essentially the plumbing for the DIE. What we deliberately leave outside the GIG 'cloud' is the end-systems that attach to it. These end systems (many in mobile platforms) define specific applications. And the end systems also consume IP addresses.

The network plus end systems attached to it can represent information systems (sense, decide, act functions with the communications to connect them together).

Overall Design Principles

This section uses the “industrialisation” observations from 3.1.1 and applies a top-down method to develop a set of core “principles”. In this section we focus on how information systems should be assembled, where the aim is to describe a modularisation pattern that all of the ADO's information systems should adhere to.

A modularisation pattern is important to ensure that our systems achieve interoperability across platforms, programs and also with Allies. We can observe that as a side effect of the industrialisation process the life cycles of information systems have become more rational and the cascading maintenance[5] issues have become much better controlled.

Therefore, we need two principles of 'network centric' to apply to the design and implementation of our information systems.

[4] In the Blue Navy i.e. the part of the US Navy that sails the open ocean.

[5] Cascading maintenance: The problem caused when one component (that is tightly coupled) in a system requires maintenance (or replacement) and because of the tight coupling the requirement for maintenance cascades or flows into the other system components.

Principle 1 : Unit Level LANs

Principle 1 : Unit-Level LANs

End-systems (e.g. sensors, weapons, Allies etc) are connected to "the network" and not to each other. They are attached to unit-level LANs which are in turn connected via a router to either a radio-WAN or a terrestrial WAN.

The Unit-Level LANs principle implies that no end systems are connected to each other (e.g. by point-to-point serial links) and no end systems in a platform are connected to off-board entities, that's what the router on the unit level LAN is for, see Figure 2.

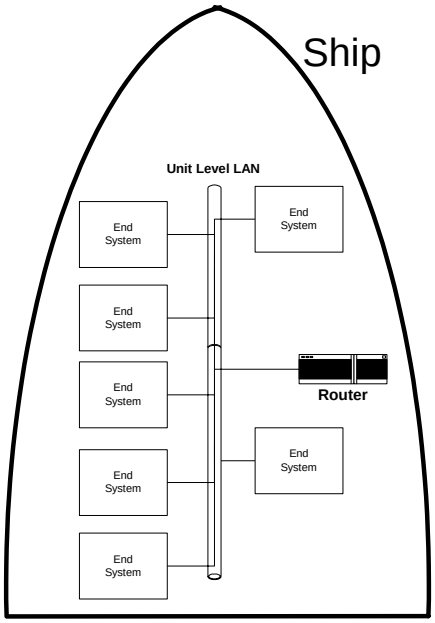


Figure 2 Example application of Principle 1

As the implementation of this principle is outside the program scope of the CIOG, it must be captured as a governance issue where the CIOG has directive authority over the ADO's Program Managers to ensure this modularisation and systems view is realised uniformly across the whole DIE (see Section 6).

The end-goal is "modularisation" and it should be kept in mind that "standards", although important, are only one of the means to that end. Part of the "modularisation" goal is creating what we term "good network citizens". To become "good network citizens" our end-systems must encompass the following:

- a LAN interface (which implies a protocol stack, which may in turn imply an IPv6 protocol stack);
- an enveloping (wrapper) definition (MIME or XML are good examples), this provides all end-systems (that need to be interoperable) with a common language;
- a means for authentication and encrypting data (e.g. S/MIME);
- setting of DSCP on exiting data-grams for QoS purposes and
- an SNMP agent that affords both local and remote manageability.

Reasonable exceptions

There are some reasonable exceptions to the Unit-Level LAN principle.
The objective is to place the mission sensors, the mission decision support systems and the mission actors (weapons) in an 'inherently interoperable' position. If the platform is, for example,

an aircraft, we should note that this category does not necessarily include the platform's avionics (the information system necessary to fly the aircraft). A mindless enforcement of the above rules on the avionics package yields no interoperability benefits and is likely to be detrimental to issues such as flight safety. How far these rules penetrate into the platform's own control systems should be a decision properly left to the program manager acquiring the platform.

Principle 2 : Routable WANs

Principle 2 : Routable WANs

Make Radio-WANs and terrestrial WANs routable.

The WAN, both radio and terrestrial, can be viewed (SV-1) as a network cloud with routers at the border, see Figure 3.

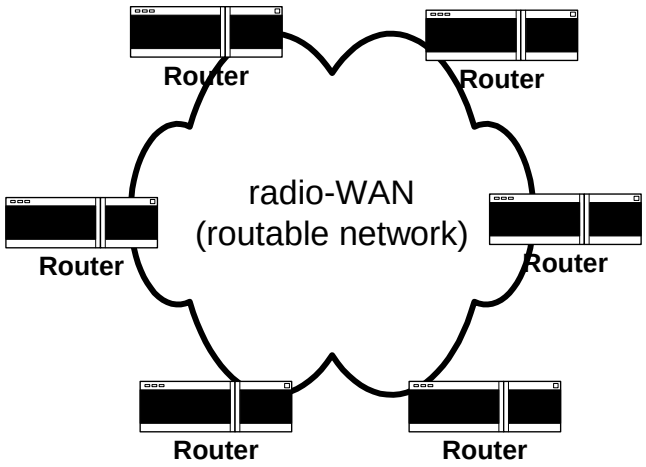


Figure 3 Routable Network

CIOG has some direct programmatic control over this segment (e.g. DWACN)(which is different to the US CIO organisation), so the issue for this principle is one of self-governance.
The next section develops the interoperability requirements for radio-WANs. There are specific requirements (such as for covertness) that are considered to be outside the scope as they are not interoperability related. However if the CIOG is also acting as the Program Manager, then these other specific requirements will also have to be considered.

Defining Radio-WAN interface and performance requirements

The next step is to develop the interoperability and performance requirements for the radio-WANs. Note that it is not necessary to know the specific uses to which these radio-WANs will be put, our approach is to make them part of the general purpose “internet plumbing”.
Placing the radio into the rest of the GIG context enormously simplifies the protocol design. By defining a radio-WAN as a network cloud with routers at the edge, we find that we only need to get the protocols in the bottom two layers of the ISO Reference Model correct. Indeed, worrying about layers 3-7 of the Model constitutes an attempt to reinvent the internet (which is clearly a retrograde step) rather than extending the internet to mobile platforms.

There are at least a two ways to analyse the protocol requirements for radio-WANs:

- **Operational views** (Use Cases). This approach is a useful place to start, but it tends to be incomplete.
- **Taxonomic approach**: e.g. look at the IEEE 802 protocols and hypothesize that if a requirement exists here, it's probably something that our military radio-WANs should consider

Operational Views (Use Cases)

Let us consider an infantry soldier as an example. Recalling “Principle 1” (all end-systems attach to a LAN) and applying this to the soldier, he now “wears” the LAN as a part of his uniform. There will be several end-systems that will attach to his LAN:

- his rifle scope (which doubles as a camera and becomes a sensor);
- other cameras (in counterinsurgency operations, it's often useful to snap a picture of a person interrogated and send it somewhere);
- his radio navigation receiver (e.g. GPS) which both tells him where he is and tells his allies where he is (blue force track, or, in USMC-ese, EPLRS);
- his voice communications system (e.g. a VoIP equipment, the microphone and headset of which are part of his helmet) and
- an instant messaging pad (a PDA or something similar that is strapped to his forearm).

For reality check reasons, note that there are voice applications here, but there are also several “data” applications. In order to not burden this soldier with multiple communications systems, the “converged bandwidth” (also known as “all-IP”) solutions are absolutely required.
The infantryman's equipment includes, a router and subscriber station of at least one radio-WAN which plugs into that and becomes the edge of the radio-WAN cloud. Because routers can have multiple ports, this is not mutually exclusive.

Taxonomic[6] Approach

In applying a taxonomic approach it is useful to dissect the IEEE 802.x protocol architecture. In doing this we are hypothesizing requirements by finding their presence in existing network standards.

Working down from the top of the stack (see Figure 4), all IEEE 802.x protocols (Ethernet, WiFi, WiMAX, etc.) use the IEEE 802.2 Logical Link Control (LLC). This interface definition (known as a SAP – service access point) provides an interface to the “higher layers” in the protocol stack. It is the LLC's presence that makes an 802.x network, a routable one.

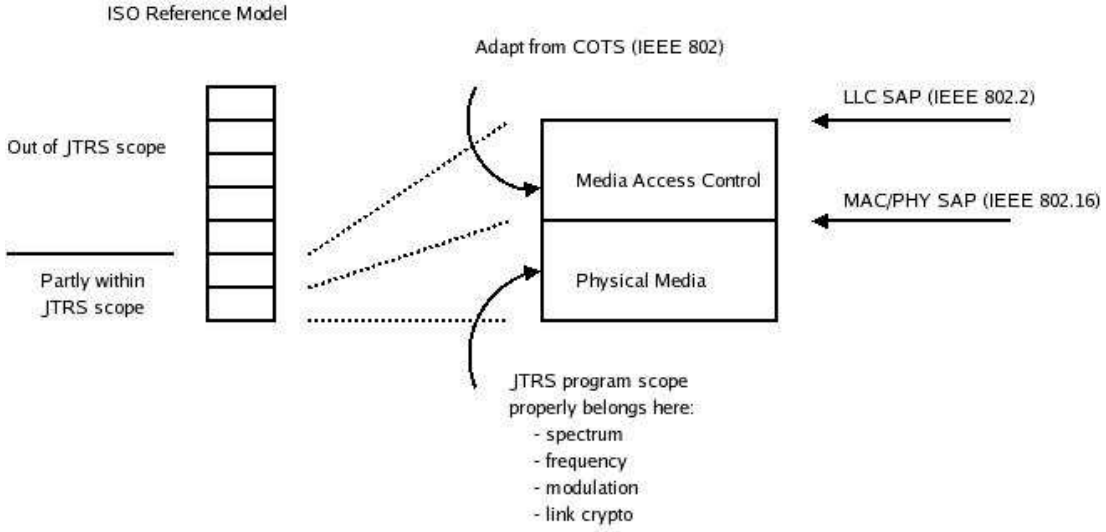


Figure 4 Protocol Architecture

Below the LLC interface is the MAC (Media Access Control) function. The MAC defines how multiple subscriber stations on an 802.x network segment take turns transmitting. There are two kinds of access methods in IEEE 802.x:

- **contention** based access (Ethernet and WiFi both use carrier sense multiple access) or

[6] Taxonomy : “The science, laws, or principles of classification; systematics.”

- **non-contention** based access (Token systems (including FDDI) and WiMAX (802.16) use this method, these are necessarily more complex, but are more efficient in bandwidth usage and are stable under overload). Non-contention queues also offer ability to control QoS, something that contention based access does not do.

Below the MAC functionality is a security sub-layer. This is a new appearance in IEEE 802.16 and is a reaction to the poorly designed, band-aid approach to security in WiFi (802.11) that turned out to be easily exploitable. The purpose of the 802.16 security sub-layer is to protect the MAC layer messages that pass between subscriber and base stations to control the MAC state machine[7]. The presence of this security sub-layer in 802.16 is an area for further design when considering the additional security measures that should be built into a militarised version of the protocol.

At the bottom of the MAC layer is an interface definition (another SAP) that provides a modular interface to the physical layer (Layer 1) beneath it. This is reflected in some COTS chipsets, particularly for 802.16. Some chip-set vendors have a MAC device and a Physical layer device so the interface has a real-world rendering. This interface is important to us when considering two things:

- adapting COTS technology to military purposes (we want to minimize the parts we have to change) and
- adapting to new technology over life cycles and controlling cascading maintenance (e.g. Ethernet has gone through a half dozen generations in the past 30 years by keeping the MAC stable and changing the Physical layer specification. Even here, the Physical Media Independent (PMI) part of the Physical layer specification has remained stable).

IEEE 802.x splits Layer 1 into two parts:

- **PMI layer**. This is the upper half of the physical layer and contains the frame structures. Essentially all COTS LAN protocols actively used today (e.g. cable modems and DSL) use the Ethernet framing standard. Aside from the COTS reuse aspects, use of Ethernet frames, and the necessary Ethernet addressing scheme, supports multicast. The frame structure is also “protocol independent” meaning that the frame cares not whether the data grams inside the frame are IPv4 or IPv6 or something else.
- **The Physical layer**. This is the lower half of the physical layer and is Physical Medium Dependent. Potential media include wire, glass or the aether. For radio systems (i.e. via the aether), the Physical layer specification includes RF characteristics such as frequency, spectrum, modulation and, if existing, link crypto. Of these, the first three are covered in the IEEE 802.x specifications, usually in exhausting detail.

Management interface

Management interfaces do not map cleanly onto the tightly specified layered protocol stack design despite the fact that IEEE 802.x networks do have management interfaces. In earlier networks (e.g. FDDI) the management interface was captured as a modular specification. In 802.16, the management interface is expressed as a MIB (Management Information Base) within the Simple Network Management Protocol (SNMP) context.

Mapping to radio-WAN programs

There are two major points to consider when mapping to the radio-WAN programs:

1. All of these programs should yield routable networks. This is supported by the GIG context definition, it matches the use case (assuming voice = VoIP) and the presences of the 802.2 LLC in all IEEE 802 networks indicates that this is a solid requirement. We have therefore, necessarily expanded the scope of ‘transitioning to IPv6’ to include the requirement to transition radio-WANs to ones that yield routable networks.

[7] For readers familiar with current and older generation military satcom systems, these are analogous to orderwire messages.

2. Within the radio-WAN cloud we need to meet four requirements:

    a. A stable MAC that allows for QoS control. All radio networks can look forward to being saturated, so MAC stability (and consequent bandwidth efficiency) are important. Military networks clearly need to support QoS privileges to some users in some situations (e.g. official business over morale traffic, contact reports over logistics requests, everything else over PowerPoint).

    b. Multicast. For the “Supply-side”, Multicast is the only offset to the limited bandwidth that radio-WANs will have compared to the wired networks they route into. For the “Demand-side”, a lot of military data (e.g. the blue force track in the use case) is multicast in nature.

    c. Layer 2 and 1 security. Clearly we have LPI/LPD (Low Probability of Intercept and Detection), TA/TFA (Traffic Analysis and Traffic Flow Analysis) and jam resistance requirements.

    d. Management. The ability to manage the components in a radio-WAN is critical, both within the radio-WAN itself and for end-to-end across an internet in which the radio-WAN is a network segment. In the early design stages, its not necessary to derive management requirements via operational concepts, what's important is that all radio-WAN components have SNMP agents embedded in them so that their management interfaces (controls, dials, knobs) can be “read from”/”written to” both locally and remotely in a secure manner.

COTS Re-use

Of the protocols surveyed, IEEE 802.16 offers the best place to start adapting from:

1. Like all other IEEE 802 protocols, it uses the 802.2 LLC so we have a routable network.
2. And most of the objective criteria above is met within the network:

    a. 802.16 uses a scheduling MAC layer that is highly bandwidth efficient, stable under overload and allows QoS control.

    b. 802.16 reuses the Ethernet framing protocol and addressing so multicast is easily accommodated.

    c. The layer 2 security measures in 802.16 are far superior to anything in previous commercial network protocols. 802.16 does not provide layer 1 security – this is one of the adaptations we need to make (neither does any other commercial network spec).

    d. 802.16 specifies an SNMP MIB.

There are several adaptations required to make 802.16 suitable for use in military information systems, the obvious ones reside in the Physical layer:

- Military users routinely use different spectrum allocations and modulation methods than those used by commercial users. Commercial 802.16 uses higher frequencies and OFDM (Orthogonal Frequency Division Multiplex) modulation. But these changes are confined below the MAC/Physical Layer SAP and do not affect anything above that in the protocol stack (Note: the 802.16 structure could not be used with a HF Physical layer implementation because of the bandwidth requirements).

- Security needs to be added at Layer 1. This can take the form of spread spectrum (which affords covertness in addition to TA/TFA protection). Or it can take the form of link encryption (providing TA). If these protections are provided, we can re-examine whether the incompleteness in the layer 2 (802.16 security sub layer) require further design effort.

Other than the Physical layer there is also one MAC layer problem that needs to be dealt with in adapting 802.16 to a military context. Some of the MAC messages (including some critical ones like the upload map) are transmitted in one frame and are required to be acted upon in the next frame. The existing protocol works (and has been tested by developers to show adequate headroom) as long as frame length exceeds propagation time. In geo-synchronous Satellite Communications situations, the COTS 802.16 protocol would see many frames 'in flight' at any point in time which will cause the timing constraints to be broken. This issue is being studied in

the United States where there is a proposal to solve the problem by simply stretching the MAC frame in time (from the current 0.5 – 2 msec spec in the standard) to whatever the maximum propagation time is.

Use of radio-WANs based on IEEE 802 protocols places the addressing issue beneath layer 3, so the IPv4/v6 questions do not apply.

Managing Legacy

For the purposes of this discussion we put non-routable but current technology (e.g. Link 11 and Link 16) in the same class as legacy technology (i.e. non-routable out-dated technology). TADILs are classed here as legacy because the same methods are used to make them routable as would be used for a pure-legacy system (e.g. Raven CNR). There are two proven methods for handling legacy:

- **Cocooning**. This method uses an 'IP wrapper' around a non-internet communications system. The US Navy's ADNS system employs this method to put IP cocoons around non-IP communications channels such as MILSTAR EHF and SHF channels. There may be cases where the ADO could use this technique, but in the main it is judged to be of limited use.
- **Layer 7 gateways**. These gateways (see Figure 5) provide a means of “entire-protocol-stack” translation from one domain to another. For instance, we can use a layer 7 gateway to translate from the 'pure IP' illustrated above and a platform that has, perhaps, a Link 11 terminal as it's interface to the outside world.

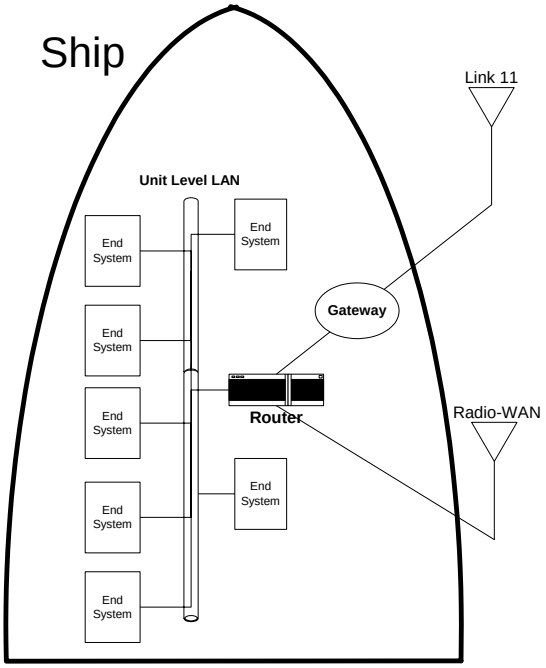


Figure 5 Layer 7 Gateway

The objective is to keep in tact Principle 1 and the “Good Network Citizenship” rules. If either of these is corrupted, all the modularisation benefits will be lost. The means is to add a Layer 7 gateway outside the router, as illustrated. This gateway receives IP data grams with XML-tagged track data from the router. It translates that data into, for example, a Link 11 track transaction and encloses it in a Link 11 frame per all the Link 11 standards. This makes the Link 11 side of the gateway wholly interoperable with a Link 11-equipped platform.

Gateways are not new, nor are they new in this kind of application. But the familiar form may not be immediately recognizable as a gateway. There are a large collection of 'connectors' in Global

Command & Control System (GCCS), including a connector for Link 11. It's a computer-centric implementation of the same tool where this is a network-centric implementation.

Good Network Citizen Data Wrapper

Our definition of a “Good Network Citizen” included the need for an enveloping data wrapper. The list of end-systems must now be expanded to include any layer 7 gateways as well. There is however a severe scalability problem to be avoided. This is because the number of gateways can increase with the square of the number of end-systems to be integrated, e.g. one gateway is required to integrate two end-systems but three gateways are required to integrate (add) a third end-system

The increasingly accepted approach (in the US) seems to be to use XML tagging as the wrapper, if a common wrapper language (e.g. XML) is used, then the exponential effect can be avoided and the number of gateways only expands linearly with the number of end-systems.

DIE Boundary

The DIE does not include the ADF’s sensors or weapons but does include the interfaces to allow information to flow between them and the rest of the DIE. Figure 6 illustrates the DIE boundary using the example of a Wedgetail AEW&C aircraft. This shows that the DIE includes the ground to air link and the Link-11 terminal in the aircraft.

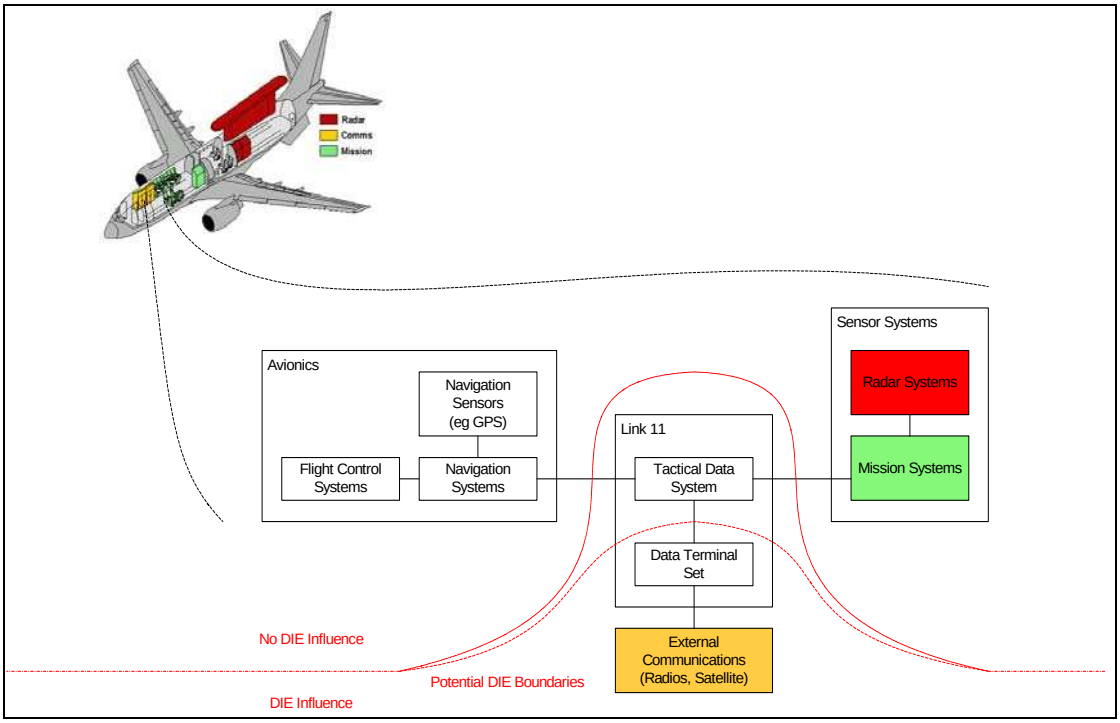


Figure 6 DIE Boundary Example

Figure 7 expands upon the Defence Information Infrastructure (DII) and details examples of both the user applications and the communications systems that make up the static and deployed bearers. The DIE bearers include HF, VHF, UHF and satellite communications systems.

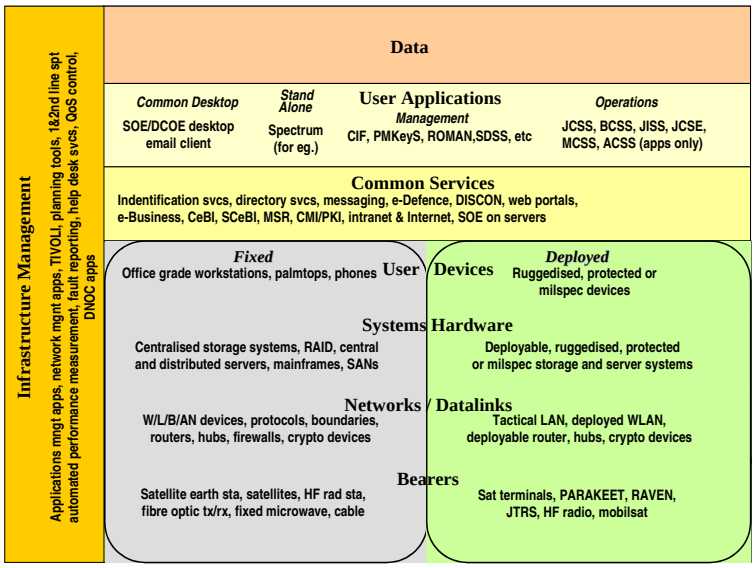


Figure 7 DII (Defence Information Infrastructure) Detailed

Figure 8 shows (an example of) the full extent of the boundary between DIE and non-DIE components of the ADF where Principles 1 and 2 have been followed. In this figure we can see the “mission-thread” from another platform (implementing the decide function) through the radio-WAN to the aircraft.

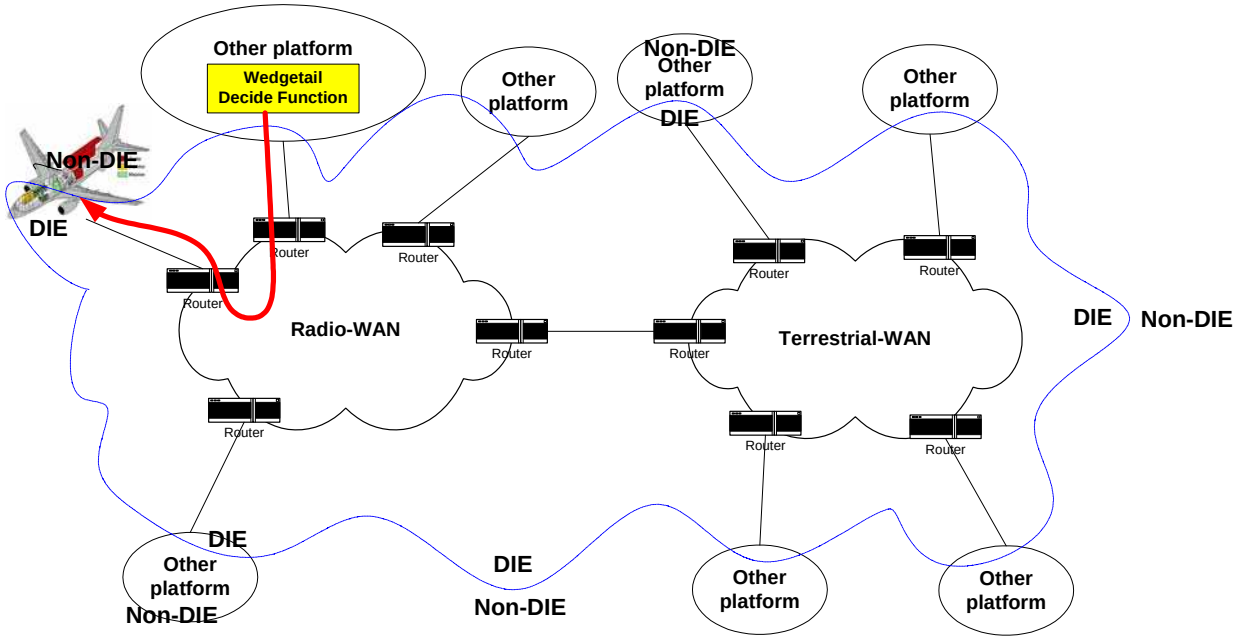


Figure 8 Radio and Terrestrial WANs

Context Conclusion

The above two Principles (3.1.3.1 & 3.1.3.2) will be referred to throughout this IPv6TP.

Execution of these principles modularly separates end-systems and the network infrastructure. This increases modularity, reduces cascading maintenance problems and allows technology insertion[8] in both the network infrastructure and in the end-systems independent of each other. Implementing these principles does not automatically achieve interoperability, but it does lay the enabling foundation. Conversely, avoiding these principles may lead to interoperability problems within the ADF and between the ADF and it's Allies.

IPv6 Background

Current or Previous IPv6 Transitions

The world-wide experience with transitioning to IPv6 from IPv4 is such that the Panel is of the opinion that fully-completed/previous transition strategies do not exist because no organisation has yet completed a transition. The UK, NATO and US defence organisations are in the process of planning their transitions, however the Panel is not able to provide substantial details (beyond what is available in the public domain) of these current transitions strategies because this information either cannot be shared under the existing arrangements and or is classified (See 1.3.2 for a list of Government-to-Government documents).

The Panel has a range of views concerning the actual state of completeness of the MOD and DOD plans. Details of these transition plans can me made available to the ADO by direct liaison between the ADO and the relevant members of these organisations. The Panel will be able to assist the ADO to make the necessary contacts.

The following paragraphs summarise what can be advised concerning the progress with current IPv6 planning within the UK, NATO and US defence organisations.

UK MOD IPv6 Transition

The UK MOD is in the process of developing an IPv6 transition strategy that will be followed by a detailed IPv6 plan[9]. A study undertaken in 2004[10] explored the key drivers for transition and highlighted critical issues. In summary the report concluded that:

- the primary driver for MOD transition is UK – US interoperability;
- there is no pressing UK national need for IPv6 migration;
- the primary UK national driver is to avoid obsolescence;
- the UK MOD has ample address space;
- the features of IPv6 (when compared with IPv4) do not lead to obvious enhancements to military capability and
- security is a critical issue which has yet to be fully explored.

About eighteen (18) months ago the UK MOD set about to quickly determine a strategy for IPv6 transition, and initially settled on a preference to use the Dual-Stack[11] approach. That early decision is now being re-appraised and questions have been raised.

In 2004 the MOD Defence Interoperable Network Services Authority (DINSA) was tasked to acquire IPv6 address space. It is our understanding that DINSA do not see this acquisition as a high priority and consequently they have not made significant progress. They are however looking at the request generated by the US DOD with the intention of using it as a template and initially requesting a small allocation with the view to expanding this at a later stage.
To our knowledge there have been no studies to ascertain the address space size or address hierarchy required by the UK MOD. The MOD's current fixed IPv4 network infrastructure is

[8] IPv6 is one such technology that can be inserted.
[9] It is understood that the UK MOD and US DOD are considering demonstrating IPv6 at CWID 60/07.
[10] This study was undertaken by a team of two consultants within the Integration Authority from within the MOD's Procurement Agency. One of the consultants was replaced by John Pennington in August 2004.
[11] See Annex A for a description of the Dual-Stack approach, it's advantages and disadvantages.

provided by British Telecom (BT) who are responsible for technical management of the network including addressing structure.

The UK MOD has yet to allocate funding to conduct an IPv6 study (similar to the one that has generated this Plan/Strategy) and therefore the ADO is likely to be more advanced than the UK MOD in its planning by the time this report is complete.

NATO IPv6 Transition

The NATO Consultation, Command and Control Agency (NC3A) has been tasked to develop an IPv6 transition plan by early 2006. This is aimed at transition for the NATO command chain, which largely operates at the strategic level (between NATO and national defence headquarters). The scope is NATO funded communications and information systems and interfaces to national systems, including national systems deployed in support of NATO operations. NATO is developing a definition of IPv6 conformance and related procurement guidance and a STANAG for IPv6 interoperability may be produced in the future. Initial studies have reached the following conclusions:

- there is no overarching technical reason for NATO to transition to IPv6;
- the drivers are national transition plans and the pace of commercial developments;
- current NATO policy is to prepare for IPv6;
- maintaining operation and interoperability within the complex NATO infrastructure are crucial issues;
- systems will be fully functional and tested prior to cut-over from IPv4;
- a strategy being considered is to cut-over each distributed information system separately and selecting the transition mechanism from a range of options in order to fit the characteristics of the subject system being transitioned;
- the NATO strategy implies that IPV4 and IPv6 networks will be supported in parallel for some considerable time and
- the parallel support of IPv4 and IPv6 will result in increased cost and the chosen transition profile may significantly affect the overall cost, however a detailed cost analysis must be conducted to quantify the cost implications.

This NATO view was reinforced by a presentation at the recent Coalition Summit for IPv6 conference in Reston USA [7].

US DOD IPv6 Transition

The US DOD issued the memorandum “Internet Protocol Version 6 (IPv6)” [6] in 2003. This document provides policy for enterprise-wide deployment of IPv6. IPv6 is specified as the next generation network layer protocol of the Internet as well as the Global Information Grid(GIG)[12], including current networks such as the Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Joint World-wide Intelligence Communications System (JWICS), as well as emerging DOD space and tactical communications. The DOD has the goal of completing the transition by the end of the 2008 US financial year. A summary of some of the major elements of the policy include:

- from 1/10/2003 all GIG assets being developed, procured or acquired shall be IPv6 capable;
- transition of the GIG will occur between 2005 and 2007 (US financial years);

[12] US definition: The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to war fighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority.

- IPv6 was not permitted on networks carrying operational traffic from 2003, subject to further review;
- DISA to acquire IPv6 address space to meet five years of requirement;
- DISA specified as agency to manage DOD IP addresses and
- DOD Chief Information Officer to develop an IPv6 transition plan.

As stated in 3.2.1 the ADO will require direct liaison with the US DOD to share the full extent of its IPv6 planning. The Panel is also aware that the company Electronic Data Systems (EDS) is working on IPv6 for the Navy/Marine Corps Intranet (NMCI) and that the state of this IPv6 planning could be obtained through the appropriate government-to-government links.

The international organisation the IPv6 Forum (www.ipv6forum.org) and the North American IPv6 Task Force (www.nav6tf.org) have provided input to the US DOD to help with their IPv6 transition planning. These two organisations are a significant source of publicly available documentation and work supporting the benefits of transitioning to IPv6.

The paper "IPv6 Response to National Strategy to Secure Cyberspace Final V2.0" [11] highlights many of the problems with today's Internet architecture (IPv4 and NAT) and is supportive of transitioning from this architecture to IPv6.

The paper "NAv6TF PCIPB Input Part II" [12] agrees with the benefits (put forward in the DIMPI [1]) of adopting IPv6, e.g.

- larger address space for end-to-end global reach ability and internet scaleability;
- simplified IPv6 data packet header;
- support for routing and route aggregation, making Internet backbone routing more streamlined and efficient;
- server less ("stateless") IP auto-configuration, easier network renumbering, and much improved plug and play support[13];
- security with mandatory implementation of IP Security (IPSec) and
- improved support for IP mobility inherent in IPv6.

The paper also puts forward a (US) business case for the transition to IPv6 and makes a series of recommendations for US Government and US Industry, some of those recommendations included:

- application providers to support Dual IPv4/IPv6 stack (see Annex A for more detail) to begin delivery of IPv6 services coexistent with IPv4;
- take early steps to obtain adequate IPv6 address allocations and
- consider in their (industry) manufacturing plans that the majority of mobile devices, and a growing number of household and consumer-electronic devices will require some form of IP connectivity.

The paper "NAv6TF NTIA IPv6 RFC Response" [13] also supports the previously cited benefits for the transition to IPv6. This paper was generated in response to the NTIA's request for comment (RFC) on IPv6 and provides a view on the costs of transitioning to IPv6 including "Hardware Costs, Software Costs, Training Costs and Other Costs".

Although the US DOD IPv6 transition is mandated by [6] to be completed by 2008, it is the Panels view that the actual transition of all IP based systems will take some years longer than 2008. The emphasis for the US is to transition selected IP networks and entities to be IPv6 capable by 2008.

[13] [12] specifies that, "This is the most important future benefit for the Department of Defense and Home Land Defense communications."

The Defense Information Systems Agency's (DISA) IPV6 transition strategy is summarised in Figure 9 [3].

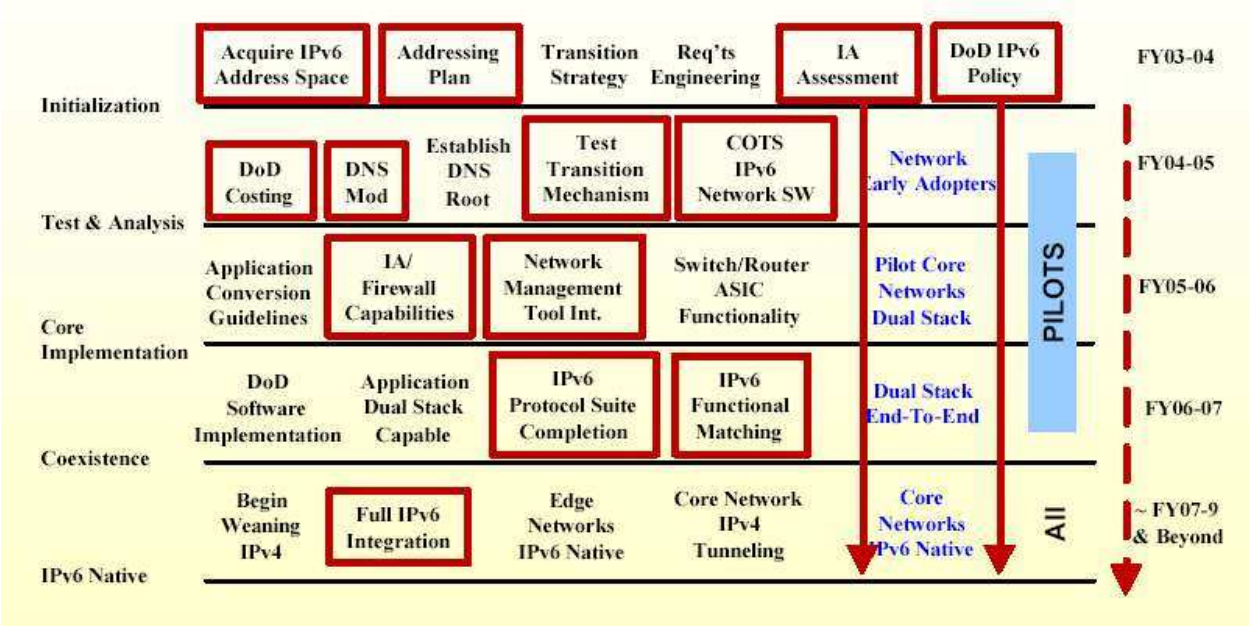


Figure 9 DISA's IPv6 Strategy

DISA does not own any sensors or weapons or decision support nodes (other than their own network operations sites) and therefore the scope of this strategy cannot be considered as a complete US DOD IPv6 strategy. Even if it were completely and successfully executed it would not address the issue of the many artisan[14] data links (e.g. tactical data-links) that are closely coupled to sensors within platforms (Refer to "Principle 1").

Potential Transition Strategies

It is the Panel's view that there are no "off-the-shelf" strategies that could be applied to the DIE, however some elements of the MOD, NATO and US experiences may have potential for incorporation into an effective strategy for the ADO and the DIE. More importantly however the strategy should draw on the principles suggested in 3.1 and work within the timetable and constraints of the DCP programs that will shape the DIE into the future.
The remainder of this transition plan therefore calls upon the collective expertise of the Panel and an analysis of the DIE to provide strategic options and a recommended strategy in Section 4.

Defence Information Environment (DIE)

As an input to forming a suitable transition strategy, it is first necessary to understand the current baseline DIE and then explore where it is likely to progress over the period to 2013. Another view of the DIE (compared with Figure 1) and its interfaces is the view that shows the command support environment, see Figure 10.

[14] Artisan view – Sensors connected directly to decision support, connected directly to actors. Also known as "Stove-Pipes".

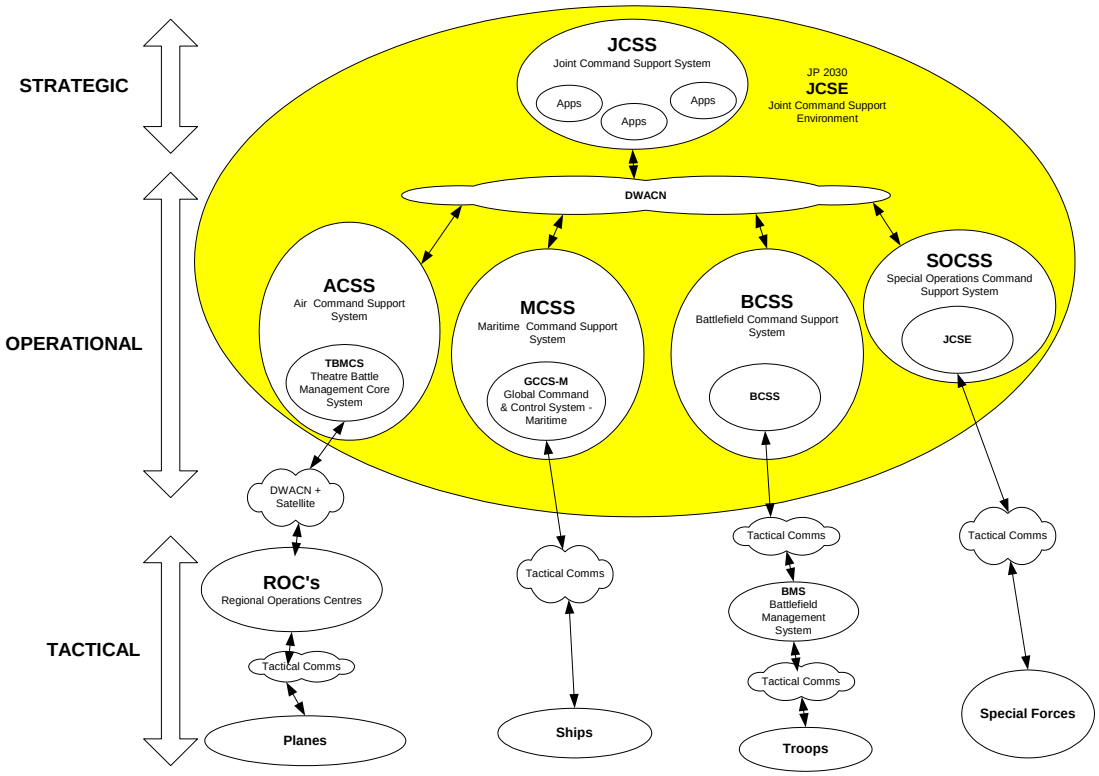


Figure 10 DIE Command Support System Environment

This view indicates that the command support systems are divided along service (Army, Navy, Airforce & Special Operations) lines and each of these systems contains a unique set of legacy DIE infrastructure.

The rest of this section focuses on the current and future configurations of the infrastructure components (DII) of the DIE.

DII Baseline Configuration in 2005

The current (in 2005) DII configuration and architecture description is divided into “fixed” and “tactical” components as follows.

DII Fixed Infrastructure Configuration

A generic view of the Defence Communications Network (DCN) is depicted in Figure 11 and consists of:

- Defence Wide Area Communications Network (DWACN) and
- tactical networks.

The DWACN component of the DCN consists of:

- Defence owned wide area communications equipment/services,
- Telstra owned wide area communications equipment/services,
- Singtel/Optus owned wide area communications equipment/services,
- satellite provider owned wide area communications equipment/services,
- Defence owned local area networks and
- Other Government Organisation local area networks.

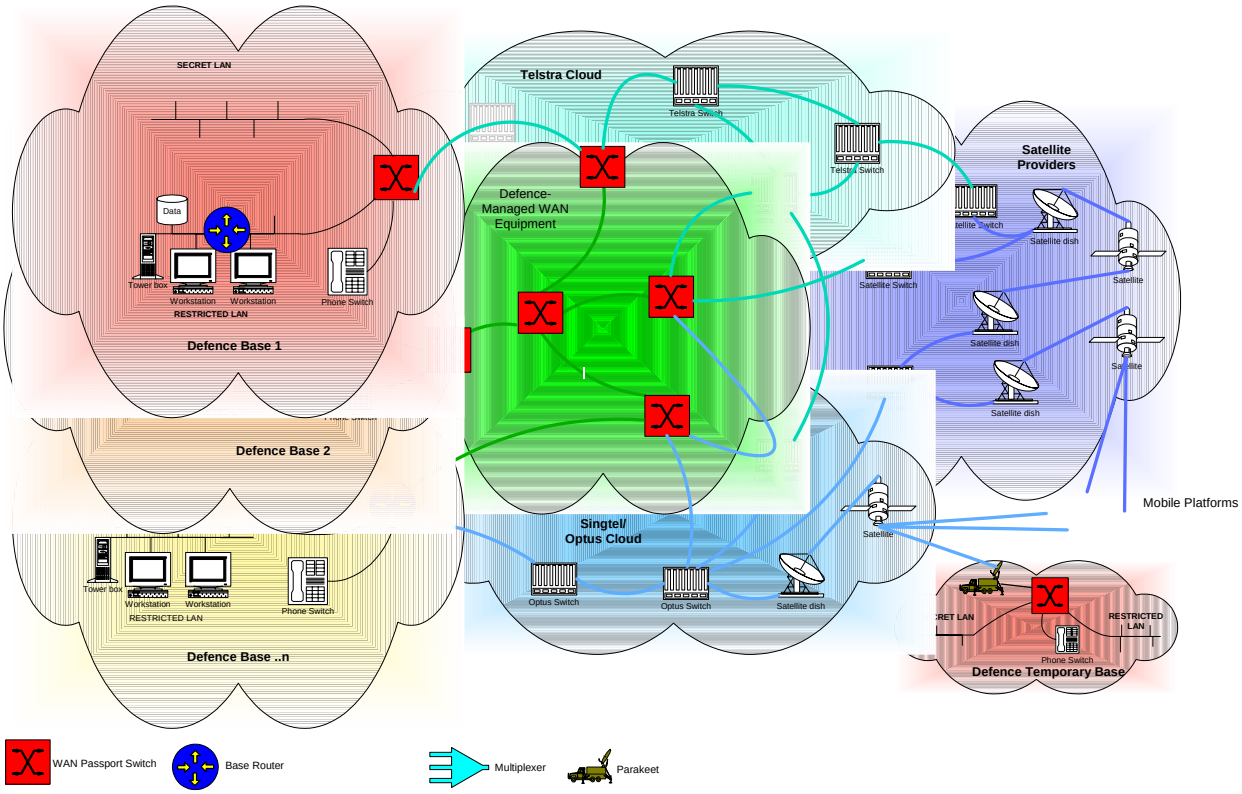


Figure 11 Generic DCN

Defence Wide Area Communications Network (DWACN)

The high level relationships for the DWACN are illustrated in Figure 12. The DWACN provides voice, video and data services via:

- the Defence Restricted Network (DRN),
- the Defence Secret Network (DSN),
- the Defence Voice Network (DVN) and
- other networks.

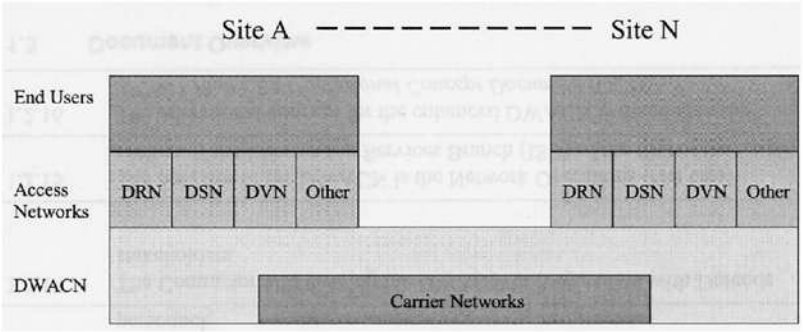


Figure 12 High-level Overview of the existing DWACN Relationships[15]

The DWACN interfaces to Carrier Networks (Telstra & Singtel/Optus) and to Defence owned carrier-grade infrastructure. The DWACN provides connectivity between approximately three hundred (300) sites[16], most of which are located within Australia, see Figure 13.

[15] Source = [4] DWACN FPS
[16] Source = [4] 1.2.4 DWACN FPS

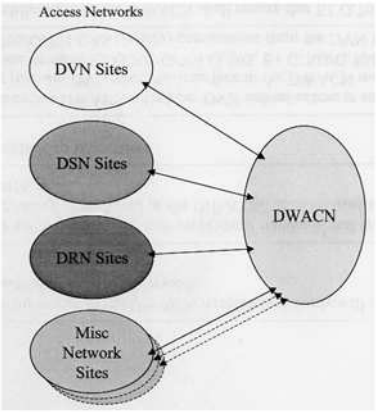


Figure 13 High-level External Interfaces[17]

DWACN sites include nearly all DOD establishments (bases, barracks, headquarters, offices etc) that are regularly staffed and a small number of Other Government Organisations (OGOs). There are also approximately twenty (20) overseas sites within the DWACN.

The DWACN has a hierarchical structure and is managed centrally. ATM is used extensively to aggregate different types of traffic and traffic from different sources. Commercial telecommunications carrier services (Telstra & Singtel/Optus) are utilised for most of the inter-site transmission.

The core of the DWACN (see Figure 14) consists of fourteen (14) large switches and these in-turn are connected around the core by approximately 150 smaller (Nortel Passport) switches. There is just “one network” and all the DRN, DSN and DVN traffic is handled over this network, all routing and network separation is done virtually by software routers implemented in the switches.

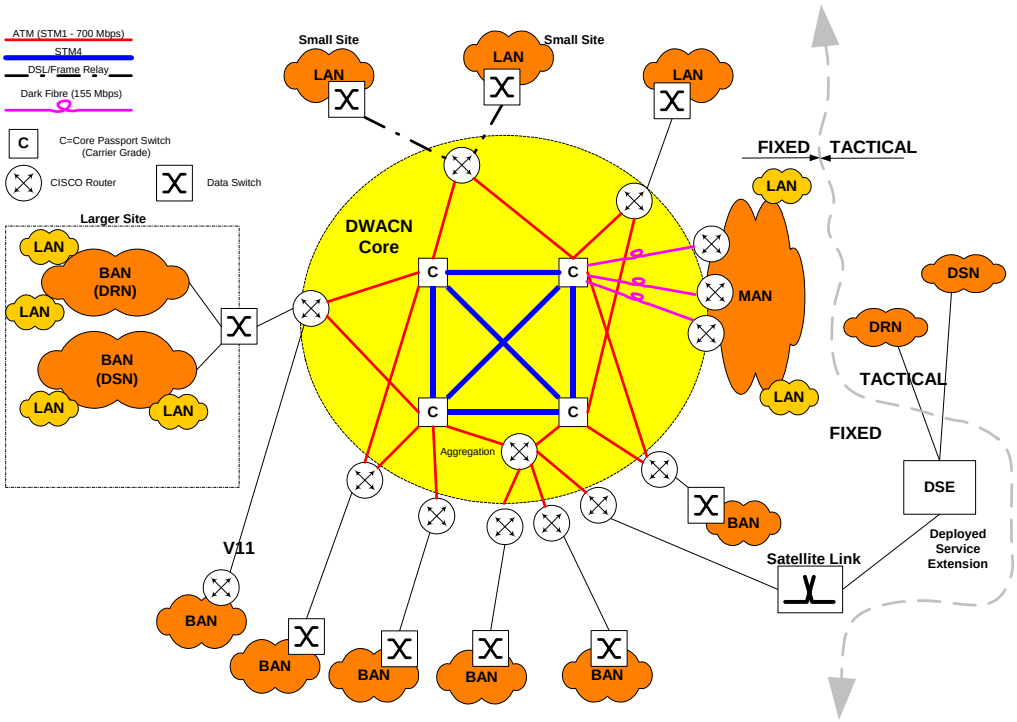


Figure 14 DWACN Core

[17] Source = [4] DWACN FPS

The DRN consists of the following environment[18]:

- Users: 79,000,
- Platforms: 55,500,
- Servers: 1300,
- LANs: 500 and
- Applications: 50 Corporate 600 Others.

The DSN consists of the following environment[19]:

- Users: 13,000,
- Platforms : 10,500,
- Servers: 395,
- LANs: 70 and
- Applications: 50 Corporate 600 Others.

DII Tactical/ Deployable Infrastructure Configuration

The tactical infrastructure consists of:

Airforce Infrastructure

Operational Link 11 in aircraft. Installed but not operational LINK 4A in some aircraft (FA-18) and ROCs.

Army Infrastructure

Raven - Combat Net Radio (CNR) + Parakeet + VHF/UHF/Satellite Trunks.

Navy Infrastructure

Link 11 in some ships (FFGs + FFHs). Extant HF and UHF.

Common Infrastructure

JP2043 HF Modernisation Project. The purpose of the High Frequency (HF) Modernisation Project (JP 2043) is to provide the ADF with a secure, cost-effective information exchange capability for the command and control of deployed forces as a primary survivable system and as a parallel system to satellite communications. The Modernised High Frequency Communications System (MHFCS) comprises a nation-wide network of distributed HF radio stations (the Fixed Network) with a central network management system in Canberra. The Project includes upgrading of HF radio systems in selected mobile platforms and transportable HF communication shelters (the Mobiles). The MHFCS is replacing some of the existing single Service HF fixed-mobile tactical HF gateways.

DII Future Configuration

The future DIE will be shaped by a number of current, ongoing and future projects[20].

DII Fixed Configuration

The future configuration of the fixed component of the DII will be formed by the extant components and will be most influenced by the changes implemented by the following DCP projects:

- DEF 7013 Joint Intelligence Support System (JISS),
- JP 2008 Military Satellite Communications ,
- JP 2030 Joint Command Support Environment,

[18] Source = [5] plus information provided by DOD Information Systems Division
[19] Source = [5] plus information provided by DOD Information Systems Division
[20] See Annex D for a detailed list of the DCP projects

- JP 2047 Defence Wide-Area Communications Network (DWACN),
- JP 2068 DNOC,
- JP 2069 High Grade Cryptographic Equipment (HGCE) and
- JP 2090 Combined Information Environment.

DII Tactical/ Deployable Configuration

The future configuration of the tactical component of the DII will be formed by the extant components and will be most influenced by the changes implemented by the following DCP projects:

Airforce Infrastructure

- AIR 5276 Ph 6 Data links for AP3-C Orion aircraft,
- AIR 6000 Joint Strike Fighter (JSF),
- AIR 7000 Multi-mission Maritime Aircraft (MMA). AP3-C replacement and
- AIR 9000 Helicopters.

Army Infrastructure

- JP 2072 Battlespace Communications System (Land),
- LAND 75 Battlefield Communications Support System (BCSS) and
- LAND 125 Soldier Combat System.

Navy Infrastructure

- SEA 1442 Maritime Communications Modernisation and
- SEA 4000 Airwarfare Destroyer.

Common Infrastructure

- JP 2089 Tactical Information Exchange Domain (TIED) (Data Links).

Challenges

This section identifies the major challenges faced by the ADO in transitioning the entire DIE to a network that will support the concepts of Network Centric Operations. The scope of this section extends beyond simply considering the transition of IPv4 networks to IPv6 ones, but also considers to transition of the entire DIE to IP.

Transitioning Non-Routable Networks

Outside of the DWACN the extant DIE is featured by many non-routable networks[21]. Presuming that there is an aspirational goal (past 2013) to provide routable connections from the network all the way out to the very edge (i.e. to the sensor/shooter), the largest concentration of non-routable entities within the ADF is likely to be in the Army.

Potentially the most significant challenge will be, not only transitioning the extant DIE IPv4 networks to IPv6, but also transitioning the entire DIE toward an all-IP network. Specific challenges are likely to be realised in DIE related DCP programs where:

- they have been in progress for an extended period prior to generation of the ADO's IPv6 policy and a non-routable design has already been chosen;
- there is a DIE component, but the DCP program is ostensibly a platform purchase (Foreign Military Sales (FMS)) where the solution (non-routable) is part of the FMS design or

[21] Non-routable networks are those networks that do not use IP.

- where the program has sufficient time but insufficient budget to implement a more-costly routable solution. Note that if the design decision is made early enough, the routable solution can be cost-neutral.

For the above cases it is expected that these networks will be very slow to transition to IP and IPv6 with some networks remaining non-routable well past 2013.

The implementation of IP and routable networks is an enabler for interoperability, but does not guarantee it, this leads us to the next challenges.

Interoperability

IP occupies just one layer (layer 3)[22] of the seven layer ISO communications model and interoperability between nodes across a network requires all layers at either end of the circuit to be compatible and interoperable.

The transition process will involve the rolling out of hardware and software from various vendors by various organisations at varying points of time. Simply stating that a network component is IPv6 capable will not ensure interoperability with other "IPv6 enabled" components and mechanisms will need to be in-place to test components prior to their insertion into the DIE. However the biggest interoperability challenge will most likely come from differing security implementations cross-ally.

Security

The security mechanisms in place today within the DIE and Allied networks use a mix of physical separation and encryption at the Data Link layer (2) or Network layer (3). Layer 2 solutions have to do with covert communications and link security. The scope of these solutions is limited to single links or network segments where the applied security must be reversed at the nearest router. Layer 3 solutions are those yielded by Virtual Private Network (VPN) equipment as well as firewalls, intrusion detection devices, passwords and physical security measures. Everything within an enclave must run up to the same security level (e.g. Secret). Layer 3 solutions can be vulnerable to insider attacks.

Continuing to solely rely upon these security methods may lead to a future where there is insufficient interoperability within the ADF and between the ADF and Allies to achieve the degree of network centric operations desired. It is not recommended that current security tools be discarded. Link security measures are necessary for covertness and traffic analysis immunity in at least some situations and enclaving (provided by layer 3 security tools) is necessary for infrastructure protection/separation.

It may be possible to improve the flexibility, power and interoperability of the DIE by transitioning to an end-to-end network model with security implemented at the Application layer (7), or "object-based". This is offered as an "opportunity" and is discussed in 3.5.

Taking this approach and modifying the security architecture would present major challenges (for the ADO and Allies) as it is a fundamentally different approach with potentially large ramifications across the entire DIE. It would need to be very carefully planned by experts and would need to consider both the technical impacts of implementation and the requirements for the development of new policies, practices and training.

Although the concept of object-based security can be recommended for its advantages, it is not placed within scope or on the timeline for the purposes of this IPv6TP. Considering this, the only requirement identified by this plan for IPv6 transition will be to ensure that any cryptographic equipment (implemented at the IP layer) within the security architecture is IPv6 enabled, equipment which only implements security at layer 1 or 2 is not affected.

[22] There are other protocols (e.g. MANET ones) that can also occupy layer 3.

Opportunities

This section discusses the lessons learnt and emerging technologies that may influence the transition to IPv6.

Lessons Learnt

Transitioning to IPv6 is yet to have sufficiently progressed anywhere in the world to be in a position to provide any substantial "lessons learnt". However the Panel has other experience that is worthwhile relating to this IPv6TP:

- Mandating the transition to a new, complicated and competing protocol (e.g. GOSIP) over a short time frame is likely to lead to significant cost with a high probability of failure.
    - Therefore it is recommended that the IPv4 to IPv6 transition is long and over-lapping and made as easy as possible.
- The initial "wired" IEEE 80x.x LAN standards (802.3, 803.4 & 802.5) all use a common Layer 2 Logical Link Control (LLC) interface (802.2). As well as all these standards being routable, the use of a common LLC allows all these LAN standards to interoperate and be bridged together. This is also true of the subsequent wireless 802.x standards. The LLC framing standard includes a "payload" field which in the context of this IPv6TP means that any Layer 3 can be interfaced to the Layer 2 and 1 that sits below, in other words these IEEE standards are IPv6 ready. Some of the LAN standards (e.g. 803.4 and 802.5) have faded from popularity but Ethernet (802.3) has continued to evolve with the underlying Layer 1 (PHY) being improved whilst leaving the upper specification virtually unchanged. This success has meant that other standards (e.g. FDDI[23] & DOCSIS[24]) have reused large amounts of the 802.x standards. Therefore:
    - the features of the 802.x protocol architecture forms a significant basis for the requirements of military wireless networks, with some components being directly applied whilst others will require modification and
    - the 802.x networks are "IP agnostic" and therefore largely immune to the success/failure of narrowly scoped IPv6 transition initiatives.
- The Defence Message System (DMS)[25]. DMS was conceived in 1988 as a secure messaging system where confidentiality was provided by encrypting parts of the email body. This was designed to provide confidentiality, authenticity, integrity and non-repudiation on an end-to-end, media independent basis. The system took fourteen years (2002) to begin fielding despite the fact that it is essentially a software system. Therefore:
    - there are significant risks in diverging too far from the general trends being followed and developed by the rest of the information technology community and
    - re-inventing an essentially COTS product (email) to provide just one feature (security) has major acceptance risks, on the other hand, adapting essentially COTS products to the same end tends to leverage existing technology and eases user acceptance.
- There are millions of IPv4 nodes in existence today with a very large investment in IPv4 applications, the consequences of this will be that:
    - some IPv4 nodes will never upgrade to IPv6,

[23] FDDI Fibre Distributed Data Interface.
[24] DOCSIS Data Over Cable Service Interface.
[25] DISA's description of the DMS. "The Defense Message System (DMS) is the designated messaging system created by the Defense Information Systems Agency (DISA) for the Department of Defense (DOD) and supporting agencies. It is a flexible, commercial-off-the-shelf (COTS) based application providing multimedia messaging and directory services using the underlying Defense Information Infrastructure (DII) network and security services."

- IPv4 and IPv6 will coexist for an extended period (beyond 2013) that will be heavily dependent on commercial interests and the pace of technological change,
- transition should prevent the isolation of IPv4 nodes and
- it is very unlikely that there will be a "flag day"[26].

Emerging Technologies

The following emerging technologies are taking hold within the general Internet and may have some application and advantages for the DIE.

Public Key Infrastructure (PKI)

Public Key technology is used in a variety of places and is becoming extremely important within the Internet. The uses are far more than just securing email and include:

- email security is an excellent example of object level security and as already stated, object-level security is possibly one of the most important enablers for cross-Allied interoperability;
- PKI is used within SNMPv3 (Simple Network Management Protocol). Remote management of a network with any protocol involves exposing data to risks from interceptors and spoofers. PKI enables get, set and trap messages to be authenticated and confidentiality-protected in an end-end, media-independent fashion. This will be increasingly important as networks become more integrated;
- IEEE 802.16 added a security sub-layer in its specification (as a result of the exploits that emerged once IEEE 802.11 WiFi became popular). This layer secures certain MAC-layer messages that pass between the terminal and the base station. The purpose of this security is to increase resistance to man-in-middle attacks which result in theft or denial or service. In the case of 802.16, the PKI is to be managed very similar to the MAC addresses in Ethernet, the X.509 certificates will be factory-installed just like a MAC address and
- various technologies under the general heading of "over-the-air", such as re-keying cryptographic devices, are using some form of PKI.

IP-over-DWDM

IP over DWDM applies only to the terrestrial WAN part of the large infrastructure. It is not part of the "end-systems", LANs or radio-WANs which are all on the other side of at least one router. Dense Wavelength Division Multiplexing involves an array of laser diodes at one end of a piece of optic fibre. Each laser is tuned to a different wavelength of light, at the other end of the fibre is found a matching set of photoreceptors, tuned to the same respective wavelength/frequency. This enables very large data-rates to be transmitted down the fibre, 2.4 Gbps and greater.

The great advantage with this technology is that the optic interface can reside inside a core IP router without any intervening technology (other than optic repeaters every ~30 km) between routers, just the fibre optic cable. Switching (frame relay, ATM etc) and ISDN structures (e.g. SONET) are not needed. This leads to a greatly simplified architecture.

Most backbone US ISPs as well as the GIG Bandwidth Expansion (GIG-BE) programs within DISA are using IP-over-DWDM.

Ethernet as a WAN protocol

As IP-over-DWDM was evolving from telephone technology, a parallel development was evolving from the Ethernet community. Particularly with the advent of gigabit Ethernet, the idea of using Ethernet as a long-haul mechanism developed. The basic fibre optic characteristics of Ethernet (e.g. usable distance) are the same as DWDM and the capacities are similar (the industry today

[26] A nominated date when IPv4 is turned-off.

has gigabit Ethernet and 10-gigabit Ethernet products that compare well with OC-48 and OC-192 capacities common in IP-over-DWDM implementations.[27]

Object Based Security

Although it is assumed that the current DIE security architecture will not be radically altered within the period up to 2013, object based security is offered here as an "emerging technology" that may find application in the DIE over the longer term.

By moving the security/encryption function up the protocol stack (from layer 2/3 up to layer 7) to the application layer, it may be possible to improve interoperability between applications. There may also be a performance improvement due a distribution of the encryption function to many terminals.

However a major disadvantage of the "big-cloud" architecture is that the cloud lacks the same type of diversity that exists within the DWACN which currently has several degrees of segmentation that provide diversity and isolate problems. Another issue is that object based security is still immature when applied to austere (radio-WAN) links (<64 kbit/sec) as the issue of validating large certificates has the potential to significantly impact data throughput performance.

IEEE 802.x Based COTS Infrastructure

The IEEE[28] has been successful at developing a range of networking standards for wired and wireless physical layer communications. These standards have been turned into successful products (productised) and broadly taken up by the commercial networking community. Successful 802.x standards include 802.3 Ethernet, 802.11x Wireless LAN (WiFi) and 802.16 Wireless MAN (WiMax)[29].

One of the keys to their adoption by the networking community has been in their design where the layered communications model[30] has been adopted and successful components from earlier standards have been reused in the newer standards, e.g. the 802.2 LLC[31]. This means that the Layer 1 and 2 parts of these standards are payload and Layer 3 agnostic, i.e. IPv6 ready. Some appealing features of these standards include:

- WiMax (802.16) enables routable wireless networks (seamless interconnection to the internet) by virtue of the use of the 802.2 LLC;
- WiFi and more so WiMax, offer wireless broadband at data rates far in excess of those typically in use by the military today[32] and
- Large-scale manufacturing, technology advances and commercial adoption have lead to very low cost devices, when compared to military equivalents.

In applying these COTS standards to the military domain the following issues need to be considered:

- range (distance) capability, WiFi's range is purposely limited, WiMax is a better standard here;

[27] www.neptune.washington.edu illustrates one program that plans to use gigabit Ethernet as it's (ocean bottom) WAN protocol.
[28] IEEE The Institute of Electrical and Electronic Engineers
[29] 802.16 is just starting to gain popularity.
[30] Ideally each layer (ISO 7 layer model) should only interface one layer up and one layer down, this enables portability between different application at the top and physical transmission mediums at the bottom.
[31] 802.2 Logical Link Control (LLC) is a Layer 2 protocol (used in 802.3 Ethernet) and can therefore interface to IP (Layer 3).
[32] 802.16 has been investigated for use in broadband wireless maritime communications [8].

- WiFi uses a contention based access Media Access Control (MAC) as does Ethernet which becomes unstable under overload and oversubscription and does not allow for QoS mechanisms;
- the requirement is then for a stable MAC that supports QoS[33]. WiMax uses a scheduling MAC which provides stability and positive QoS control;
- protocol layer security. WiFi used poor security that was easily broken. WiMax added a security sub-layer (PKI) which provides security for the MAC messages and prevents denial or service and theft of service type attacks and
- physical layer security. None of the commercial wireless standard provide this type of security which is a definite requirement for the military domain (e.g. WiFi uses spread-spectrum which is good for jam-resistance but has a high probability of interception). Requirements such as Low Probability of Intercept/Detection (LPI/D) and techniques including link crypto could be "bolted onto" these standards by replacing/modifying the applicable layer. This is possible because of the adherence to the layered protocol model.
- Timing. Only applies to satellite systems where the (Physical) frame length is exceeded by the return trip propagation time.[34]
- Multi-cast support.

Recommended IPv6 Transition strategy

This section is the core of the IPv6TP and provides a recommended strategy for the ADO to transition the DIE from IPv4 to IPv6 before 2013.

Strategic Options

Potential options (4.1.1 to 4.1.3) are considered and analysed in the following sections prior to making a final recommendation in 4.2.

Big Bang Transition Option

A big-bag transition would involve the entire DIE being switched from IPv4 to IPv6 almost instantly at some point prior to 2013. This approach would not include a period where IPv4 and IPv6 were run side-by-side. Such an approach is considered to be not only far too risky but it would lead to significantly higher cost than other approaches and is not consistent with the IPv6 DIMPI [1].

Incremental/ Phased Transition With Hard Milestones Option

A less risky approach would allow a significant period where IPv4 and IPv6 were allowed to co-exist side-by-side using some or all of the transition/interoperability technologies/mechanisms introduced in Annex A (e.g. Dual-stack, Tunnelling etc).

Implementation of the selected interoperability mechanisms could be mandated "hard milestones" to ensure that the transition is tightly managed and tracked using standard project management techniques. However this approach also does not comply with the DIMPI [1], which specifies that the transition process should leverage technology refresh programs and take advantage of the "natural" progress of "commercial" technology.

Forcing the transition follow a specific timetable could lead to increased cost, interoperability gaps and potentially retard the role-out of IPv6 if commercial technology outpaces any ADO specified milestones. The specified timetable may also limit the ADO's capability to respond to rapidly changing operational requirements.

[33] 802.16 uses scheduling protocols that meet this requirement.
[34] Because some MAC messages are sent in frame x and must be acted upon in frame x+1, otherwise the link is broken and fails.

Incremental/ Phased Transition With Soft Milestones Option

The recommended approach is to phase in IPv6 over a long period (between now and 2013) and operate it side-by-side with IPv4. Broad windows “soft-milestones” should be provided to indicate when the various components of the DIE should introduce IPv6 and phase out IPv4, this should be done in accordance with the provisions of the DIMPI [1].

These windows must leverage from technology refresh programs and the planning must be flexible enough to cope with the progress of commercial technology. Currently the core infrastructure within the DWACN (including the Cryptographic equipment) is averaging a five to six year refresh period. With the DWACN being upgraded (JP2047) in the near future it can be expected that there will be up to two hardware refreshes between now and 2013 (see Figure 15). It will also be important to recognise that some IPv4 components will never transition to IPv6 and allowances must be made to continue to support them past 2013.

Recommended Strategy

The recommended strategy is divided into seven phases, these are illustrated in Figure 15 and detailed in the following paragraphs. It is expected that (for DWACN equipment) there will be up to two technology refresh cycles over the period between 2005 and 2013.

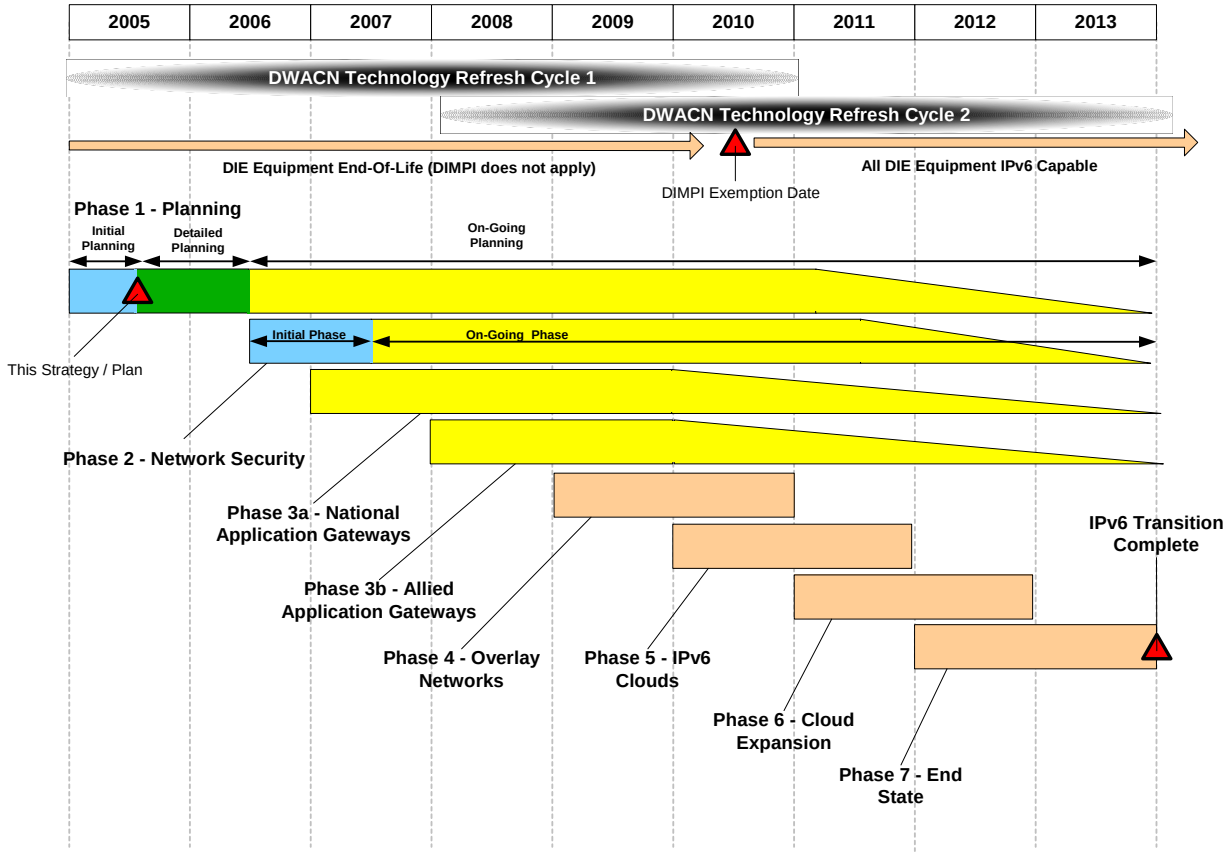


Figure 15 Recommended Strategy Phases for ADO Transition to IPv6

Phase 1 Planning

The planning phase consists of i) initial planning and ii) detailed planning. The ADO IPv6 Transition Plan (this document) forms the foundation of the initial planning phase and provides the big picture view of the whole IPv6 transition process from now until 2013.

A period of detailed planning should then follow the initial phase and this work will seek to answer more detailed questions, see Annex B.

Once information from the detailed planning phase is gathered and understood it will be possible to select the actual IPv6 transition mechanisms and assure network interoperability. This work is likely to be conducted by individual projects but will need high-level coordination by the CIOG (IPv6TO and IPv6PO, see Section 6).

The planning phase will be periodically revisited over the life of the transition to ensure that technology changes are carefully monitored and the state of IPv6 transitions external to the ADO are also considered.

Phase 2 Network - Security

Once the level of detailed planning is sufficiently mature, the Network Security phase will commence. Security will be addressed using two phases:

During the initial phase, security will be enhanced across the DIE to protect against potential threats from the introduction of IPv6. Security will be enhanced by;

- Initial IPv6 threats assessments,
- initially blocking all IPv6 traffic to prevent unauthorised use of IPv6 until protection is adequate) and
- deploying and configuring firewalls, cryptos and intrusion detection systems to provide adequate control of both IPv4 and IPv6 traffic.

This phase is very important to the success of this strategy and should be initiated as soon as possible.

The second phase of Network Security is on going and continues for the life of the DIE. The baseline DIE is continually analysed for vulnerabilities and any threats are treated with counter measures. New network capabilities are thoroughly analysed from a security perspective and only released for use (creating a new DIE baseline) once they are “trusted”.

Phase 3a National Application Gateways

Phase 3a and 3b are not contingent on the previous phase and can commence as soon as enough detailed planning has been completed. National Application-level Gateways are intended to be used intra-DIE, i.e. between disparate DIE networks that need to exchange information. This phase ensures that the various branches of the ADO (see Figure 10) can interoperate at the application level with each other by implementing Application Gateways (AGs) at the network edges. These gateways also decouple the networks, so in principle they also protect against network level threats.

These AG’s will allow IPv4 applications (e.g. Email, FTP etc) and IPv4 DIE infrastructure to inter-change application level information with like applications on the other side of the AG, independent of the version of IP (4 or 6) being used on the other side of the AG.

These AGs will need to support the range of applications to be used jointly and there will need to be a process of negotiation to determine where the gateways will be hosted and who will be responsible for providing and maintaining them, see 6.3.1.

The AGs could potentially be hosted in any of the ADF support systems e.g. ACSS, MCSS, JCSS (see Figure 10) etc.

Prior to the commencement of this phase of the transition the DIE is completely IPv4. Any infrastructure (routers, switches, servers, hosts etc) that contains an IPv6 capability (e.g. a dual IPv4/IPv6 stack) will have that capability disabled. As AGs are added the matching parts of the DIE can start to transition to IPv6, but as for the Security phase, this phase may need to be run in parallel with the other phases for many years and potentially for-ever if some parts of the DIE or Allied environments (for Phase 3b) never transition to IPv6.

Phase 3b Allied Application Gateways

Allied Application gateways are intended to function in the same way as the National Application Gateways described in Phase 3a, except that they provide a gateway between the DIE and Allied information environments at the application level.

The commencement of Allied Application Gateways is expected to be dependent upon a period of interaction/negotiation with the required Allied IPv6 Transitioning bodies. Because of this, it is recommended that Phase 3a is commenced first followed by an independent Phase 3b that is allowed to run in parallel with the other phases. In this way if the international negotiations take longer than expected, the progress of IPv6 transition within the DIE will suffer no significant impact.

Phase 4 Overlay Networks

The Overlay Networks[35] phase can commence in parallel with Phase 3 and begins with the small-scale use of IPv6 applications/systems[36] in parallel with a mostly IPv4 DIE, i.e. this phase can commence well prior to 2010. The systems elected to switch to IPv6 are chosen because they need to (or will benefit from) interoperating with other DIE or Allied/Coalition IPv6 systems. Because of the associated coordination issues, it is recommended that the ADO commence with Overlay Networks within the DIE only and then progress to interoperating outside of the DIE with Allies.

For the chosen IPv6 systems, IPv6 data is tunnelled across the DIE's IPv4 infrastructure, through Tunnel-End Points[37] and on to the IPv6 end-system, see Figure 17.

There may be some benefit in using "IPv4 compatible IPv6 addresses"[38], however this is unlikely to be an effective long-term solution as it may reduce flexibility.

---

[35] These Overlay Networks are intended to be created by tunnelling, which is one way of creating a Virtual Private Network (VPN). VPNs can however be created by other means (e.g. Multi-Protocol Label Switching (MPLS) and this is why we have not used the term VPN. Also, VPNs are sometimes associated with a security function ("private networks") and the Overlay Networks here do not propose any security, just the use of IP tunnels.

[36] A small scale IPv6 application/system could consist of anything between one up to several hosts interconnected by a WAN.

[37] Functionally either a 4 –over-6 or a 6-over-4 tunnel-end point. Note that physically the function usually resides on a router but could also reside on the same machine as a security gateway for instance.

[38] "IPv4 compatible IPv6 address is described as "This type of address is used to tunnel IPv6 packets dynamically over an IPv4 routing infrastructure. IPV6 nodes that use this technique are assigned a special IPv6 uni-cast address that carries an IPv4 address in the low-order 32 bits." [2] pg 37.

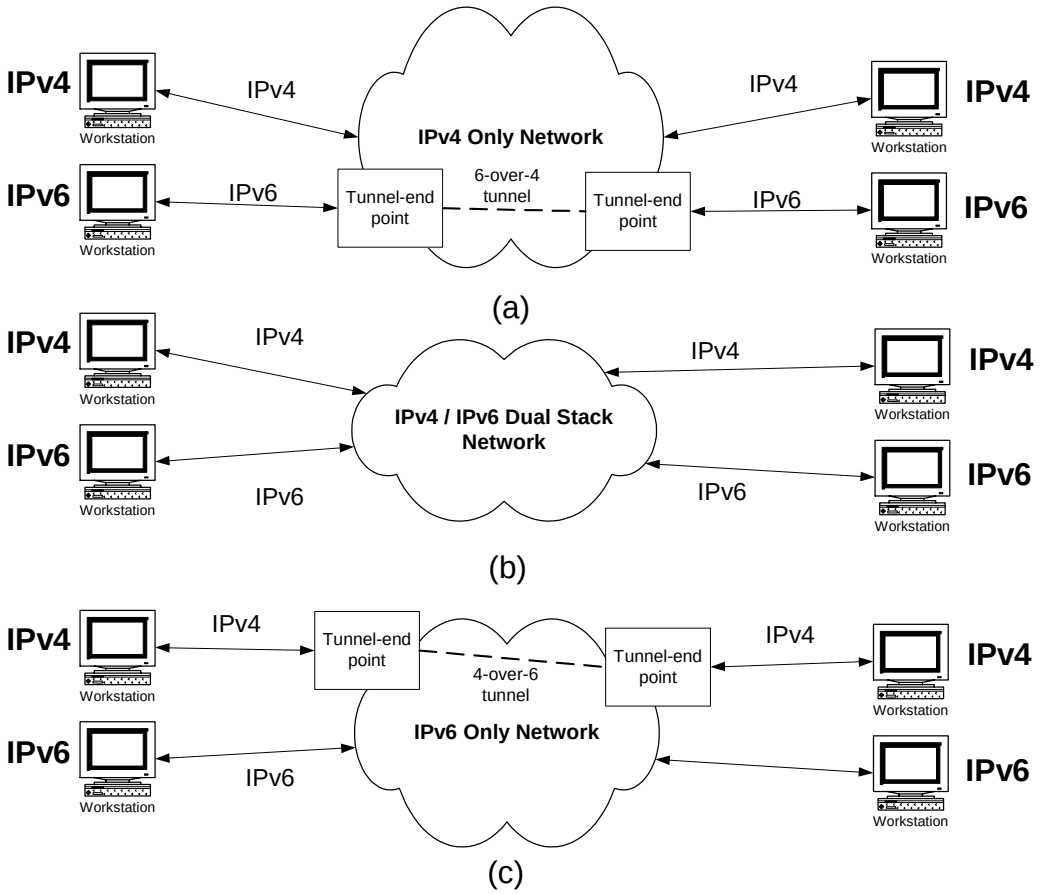


Figure 16 Tunnelling Options

Phase 5 IPv6 Clouds

This phase can overlap with the previous phase and can start whilst the DIE is still migrating to IPv6. This next stage concentrates on migrating larger portions of the DIE to IPv6 along logical boundaries, e.g. complete communication systems, these become the "IPv6 Clouds". Additional AGs and network translation servers are added within the DIE to allow the new IPv6 clouds to inter-work with the rest of the DIE which is still substantially IPv4.

Networks are connected to other networks by using "4 over 6 tunnels"[39] and IPv6 clouds are interconnected by using "6 over 4 tunnels"[40].

Alternatively there may be benefit in taking a dual stack approach[41] (see Figure 16 option (b)) within the IPv6 clouds rather than using tunnelling, especially if bandwidth is an issue or there are security and or fragmentation problems with the tunnelling implementation. The dual stack approach however needs to be analysed for cost (of managing dual stacks) before being considered.

Phase 6 Expanding The Clouds Towards IPv4 Phase Out

The next stage expands the reach of the IPv6 networks within the DIE whilst at the same time shrinking the IPv4 segments, this phase can overlap with the previous phase. This could be achieved by joining together suitable IPv6 systems (implemented in Phase 4) and reducing the number of gateways and tunnels.

[39] "4 over 6 tunnels" This assumes that IPv6 only networks are in place and IPv4 packets are required to be sent via the IPv6 infrastructure (See Figure 16 option c).
[40] "6 over 4 tunnels" (See Figure 16 option a).
[41] Dual-stack is the favoured approach in the UK but may not be necessary or desirable for the DIE.

The expansion process continues until most of the DIE has migrated to IPv6.

Phase 7 2013 End State

This is the 2013 state where ideally all IPv4 systems within the DIE have transitioned to IPv6, however there is likely to be some legacy systems that either cannot be migrated or need to be kept in place because an external party (e.g. Other Government Organisation) is very slow to migrate to IPv6. For this case the required AGs and network overlays will be kept in place as long as required.

Strategy Justification

Cost Effectiveness

The proposed strategy is considered cost-effective as it leverages the natural commercial (COTS infrastructure) refresh cycles that are likely to occur between now and 2013. The strategy does not force any hard-requirements for transition and uses an overlapped phasing plan that will allow for flexibility and co-existence between IPv4 and IPv6 networks and systems.

Impact on Defence Operations

The proposed IPv6 transition strategy is designed to have almost no impact to the ADO at the operational and tactical level. The gradual and phased strategy that allows the co-existence of IPv4 and IPv6 networks should not require any lost capability or “down-time” that is typically associated with large-scale “big-bang” hardware and or software upgrades.

Impact on Interoperability With Allies

An essential feature of the transition strategy is that Allied interoperability will not be degraded during migration, and where possible it should be enhanced. The migration plans of the US DOD will have a major impact in this area, although the ADO will need to co-ordinate with the plans of its Asia-Pacific partners. At present, it is understood that there are few Allied networks. Much of the inter-working is conducted at the application level through appropriate gateways.

For example, the Griffin network currently exchanges information using e-mail with attachments. It would be possible for part of the network to migrate to IPv6, whilst the rest remained on IPv4, with a mail server acting as the interface gateway. This would introduce some additional management cost, and a potential single point of failure. Migration would be simpler if all the Griffin participants agree to transition the network at the same; it should be noted that eventually the e-mail application will need to be transitioned as well as the network.

Other networks in which the ADF participates are CENTRIX and COWAN. These are managed and provided by the US DOD, which will presumably make its plans for transition in consultation with its Allies. If the ADO has application gateways available, it will be possible to maintain interoperability even if the migration timescales are not exactly aligned.

In the future, as the concepts of network-centric warfare are increasingly adopted, there will be increasing requirements for network-to-network interoperability with Allies at the operational and tactical levels. The Allied maritime tactical WAN described in ACP 200 is an example. Migration plans will need to be closely co-ordinated in the appropriate forum. In the maritime case this would be the AUSCANNZUKUS C3I organisation.

Information Assurance and Test Activities

Information Assurance (IA)

It is essential that migration to IPv6 shall not prejudice the security of ADO systems. In this context security includes confidentiality, integrity and availability. It is noted that the US DOD does not yet approve the use of IPv6 networks for operational traffic.
Continuing efforts are required to explore and understand any vulnerabilities which may be introduced by the new or improved features of IPv6. It is recommended that the ADO exploit its close links with appropriate organisations in the US (NSA) and other Allied nations to leverage its national expertise.

IA devices, such as firewalls and intrusion detection systems, must be provided with the capability to handle IPv6 traffic. It is expected that on initial migration to IPv6, including to dual-stack capability, end systems and networks will have some IPv6 features locked down (e.g. neighbour discovery, mobility support). These will only be enabled once appropriate IA protection mechanisms are in place.

Systems migrating to IPv6 (applications, LANs and WANs) will need to be appropriately accredited. It is likely that some systems will only be accredited for IPv6 operation in a stand-alone mode, or only for interconnection over IPv4 networks using secure tunnels.
Initially, it is expected that the built-in IPSec features in all IPv6 compliant devices will be used to provide “need to know” separation between communities, rather than military grade security separation. A PKI (public key infrastructure) certificate authority and distribution system will be required to support this.

Military grade IPv6-capable network encryption devices will be required. The ADO may wish to consider taking part in the US-led High Assurance IP Interoperability Specification (HAIPIS) programme.

Test Activities

The ADO will need to gain experience on the behaviour of IPv6 before relying on its use for operational military systems.

It is recommended that the ADO consider taking part in multinational experimental programmes. The CFBLNet (see Figure 17) initiative on IPv6, led by Germany, may be a candidate[42]. This work should focus on IPv4 – IPv6 inter-working mechanisms. The ADO should also initiate a programme to investigate the availability of IPv6 capable network elements and, more importantly, applications.

Initial migration of ADO systems should preferably on a pilot, supporting non-operational information systems, in order to gain confidence.

As systems (applications as well as networks) are migrated to IPv6, they will need to be tested to confirm that the operational requirements are met for performance and inter-working with IPv4. The IPv6 Transition Office (see Section 6.3.1) will oversee this testing, and should be able to reduce the testing requirements as confidence is gained and best practice is shared between projects.

[42] There are CFBLNet connections at Campbell Park, Russell Offices and DSTL sites in Canberra and Adelaide.

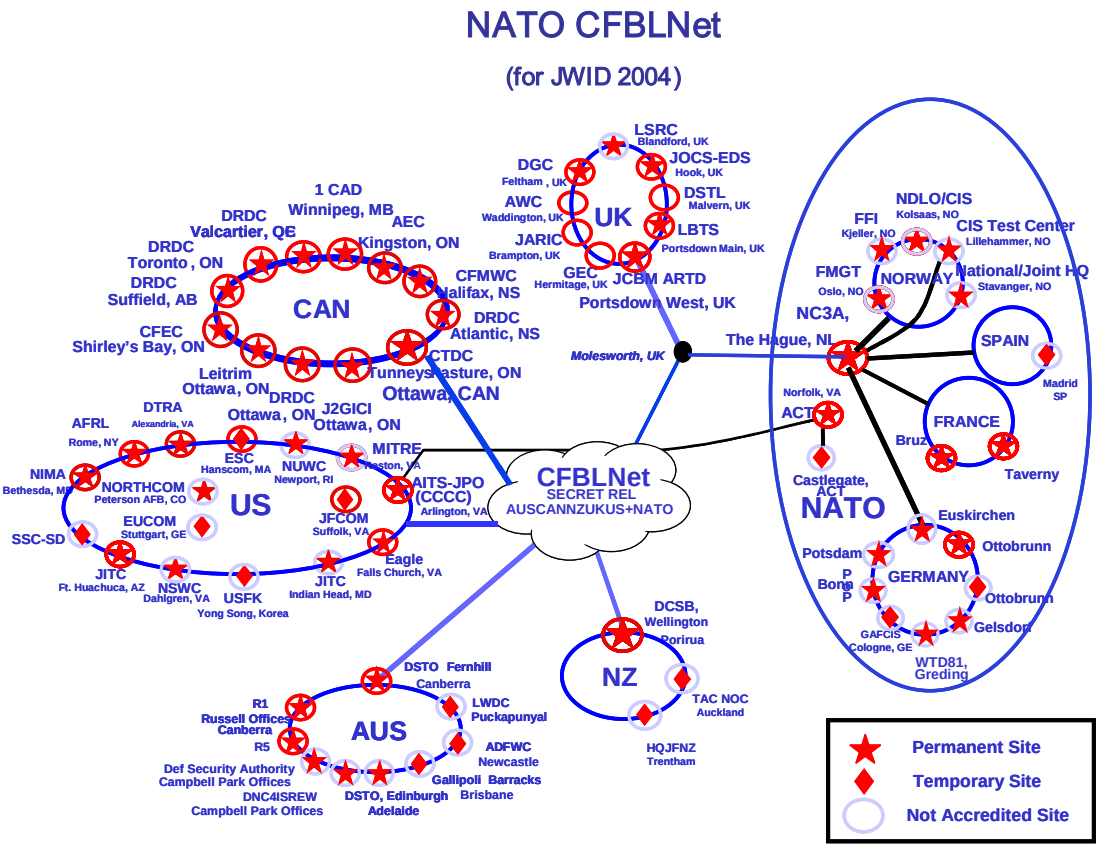


Figure 17 CBFLNet

Key Projects For Transition

A number of current ADO projects will have a key role in implementing the IPv6 transition. This section highlights the actions that these projects should be taking.

- **JP 2047** Defence Wide Area Communications Network

  This will be the core programme for transition at the network level. It should develop a strategy and plan for transition including support for IPv6 and IPv4 over an extended period. It is expected that the DWACN plans will drive the planning timelines of other network and application projects. Initial studies should also consider how QoS will be delivered and supported in ADO networks – it is anticipated that “diffserv” will be the underlying technology. This project should also consider how VPN services will be provided, and whether the IPSec features in IPv6 can be effectively exploited. It may well be appropriate for this project to study the provision of mobility services in a general sense across the DWACN area of interest.

  The DWACN IPv6 Plan should aim to provide a staged process, where confidence in the reliability and security of the IPv6 service can be gained in a limited environment before extending the scope of the service.

  The DWACN currently employs a core ATM switching fabric, based on Nortel passport switches, with Cisco routers at the WAN boundaries. This architecture lends itself well to migration to IPv6, as the underlying connections between core switches use ATM permanent virtual circuits (PVCs). The PVCs are agnostic to the flavour of IP carried over them.

  For initial experimentation with IPv6, it is suggested that a small number of dual-stack LANs would be deployed, with edge routers carrying the IPv6 traffic in manually

configured 6 over 4 tunnels. The existing DWACN could provide interconnection between these LANs, using its current IPv4 service.

The second step would be to configure a few DWACN edge routers to provide the 6 over 4 tunnels. Once initial testing is complete, the DWACN could offer a limited IPv6 service to 'early adopter' IPv6 applications. This may also be a useful option for interconnection to allied IPv6 systems.

Step three would be to configure a number of the core Passport switches to support IPv6 as well as IPv4. It might be appropriate to allocate separate PVCs for the IPv6 traffic; this would provide a degree of separation and avoid any inadvertent denial of service to the critical IPv4 traffic.

Once sufficient operational experience has been obtained to provide adequate confidence in the IPv6 service, the fourth step would be to configure all the core switches to support dual stack operation.

A final stage, likely very much later, would be to withdraw IPv4 service and require any legacy IPv4 systems to provide their own tunnels over the DWACN IPv6 service.

- **JP 2008** Military Satellite Communications

  If this project includes the provision of services at the network level, then it should develop plans to support IPv6 as well as IPv4. It should be left to this project to determine whether the solution is to be dual stack or tunnelling. The project must also consider QoS support, following the architecture developed in JP 2047. On the other hand, if this project deals with bearer services only, then transition is not an issue.

- **JP 2068** Defence Network Management System and Computer Network Defence (CND)

  It is critical that this project can put in place a CND capability for IPv6. It will be necessary to conduct studies on network management during migration. Desirably, a single system should manage both IPv4 and IPv6 network services. Management of tunnels and gateways will also need to be considered.

- **JP 2069** High Grade Cryptographic Equipment

  This project will need to ensure that IPv6 capable network cryptos are provided. The capability to pass IPv6 header fields from "red" to "black" is highly desirable, but the security implications will need to be considered.

- **JP 2072** Battlespace Communications System (Land)

  For the tactical trunk component of this project, plans should be developed for migration to IPv6. It is probable that these will include support for IPv4 and IPv6, for some period of time, depending on application transition and interoperability issues. The project should be given freedom to determine the preferred approach. QoS must also be provided. The combat net radio (CNR) part of this project will need to give close attention to the IP data capability. IPv6 capable CNR equipment may not be available off-the shelf within the procurement timescale of this project, in which case it will be important to develop plans for migration during a mid-life upgrade.

- **SEA 1442** Maritime Communication and Information Management Architecture Modernisation

  It is understood that the maritime tactical WAN will be required to support inter-networking with Allies (ACP 200). Studies on IPv6 migration should take account of the USN's plans for ADNS transition. QoS issues and application transition will need to be addressed.

- **JP 2030** Joint Command Support Environment

  It is important to recognise that IPv6 transition impacts applications as much as networks. This project should develop plans for transitioning applications. It should also study how to make use of the QoS capabilities being offered by the networks.

- **LAND 75** Battlefield Command Support System

  The same considerations apply to this project as for JP 2030.

Ipv6 address space requirements

Introduction

The aim of this section is to provide the ADO with an analysis method for the DIE in order to make a recommendation for the total IPV6 address space required. The analysis method is designed to ensure that the results enable the expected benefits provided by IPv6.[43]
The analysis method is demonstrated by providing a worked example (see 5.4), however the results can only be considered as preliminary. It is recommended that the analysis method is revisited as part of the detailed planning phase[44] (see 4.2.1) and becomes the subject of a specific workshop.

A Case For More Addresses

In direct response to the position that IPv4 address space will meet the world's IP address needs for decades to come, the NAv6TF[45] has produced the work titled “e-Nations, The Internet for All” [14] (Annex E also provides a view on IPv4 address space exhaustion). This work uses data available from the Regional Internet Registries (RIR) and takes into account the growing adoption of the Internet and networking technologies on a global basis. The NAv6TF view this as a strong and accurate argument for the adoption of IPv6 as the only viable way to sustain the growth of the Internet for all the world's inhabitants.

IPv6 Address Space Analysis Outline

To arrive at an address space plan that meets the long-term need of the ADO, it will be necessary to have a long-term vision for every conceivable network device, node, sensor, and person that may have a requirement for an IPv6 address. It will then be necessary to determine the structure of the network topology that all these addresses will operate from and then interoperate with at other network attachment points. This will determine the prefix size required for the entire ADO IPv6 address space. It is highly recommended that the ADO select an IPv6 prefix large enough to encompass all future addressable network points of attachment.

The IETF IPv6 address architecture document [9] provides the following guidance:

IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. There are three types of addresses:

- Uni-cast: An identifier for a single interface. A packet sent to a uni-cast address is delivered to the interface identified by that address.
- Any-cast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an any-cast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).
- Multicast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

There are no broadcast addresses in IPv6, their function being superseded by multicast addresses. IPv6 addresses of all types are assigned to interfaces, not nodes. An IPv6 unicast address refers to a single interface. Since each interface belongs to a single node, any of that node's interfaces' unicast addresses may be used as an identifier for the node.
All interfaces are required to have at least one link-local unicast address (see Section 2.8 [9] for additional required addresses). A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope. Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6

[43] The ADO could also seek a copy of the US DoD IPv6 Address Plan [23], through Government to Government channels.
[44] To the Panel’s knowledge there are currently no publicly available IPv6 address space plans.

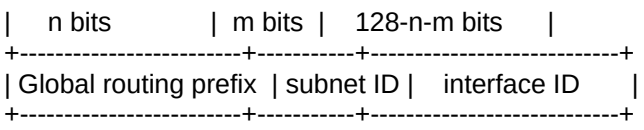
[45] http://www.nav6tf.org/html/rir_enations.html

packets to or from non-neighbours. This is sometimes convenient for point-to-point interfaces. There is one exception to this addressing model. A unicast address or a set of unicast addresses may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the Internet layer. This is useful for load sharing over multiple physical interfaces.

Currently IPv6 continues the IPv4 model that a subnet prefix is associated with one link. Multiple subnet prefixes may be assigned to the same link.

The available and current IPv6 Global Unicast Address Format is defined in IETF RFC 3587 [10], and is being used by the Regional Internet Registries (RIRs).

The general format for IPv6 global unicast addresses as defined in "IP Version 6 Addressing Architecture" [10] is as follows:



Where the global routing prefix is a (typically hierarchically-structured) value assigned to a site (a cluster of subnets/links), the subnet ID is an identifier of a subnet within the site, and the interface ID is as defined in Section 2.5.1 of [9]. The global routing prefix is designed to be structured hierarchically by the RIRs and ISPs. The subnet field is designed to be structured hierarchically by site administrators.

After the ADO has determined its IPv6 address requirements and Global routing prefix, it will then need to work with the Asia Pacific RIR (APNIC www.apnic.net). The current work from the IETF regarding Network Address Protection (NAP) [NAP] should also be reviewed. This provides a view of how to define IPv6 networks for privacy and maintain the tenets of end-to-end.

Requirements For Address Space Determination

The important requirements to be met by the address space analysis method include:

- The address space shall be sufficient to permit efficient allocation of addresses to users, equipments and interfaces.
- The allocation process, including registration of names to addresses (populating the DNS) must be fast and easy to manage.
- The address space should be distributed in a hierarchical manner, in accordance with the network topology. This is necessary to facilitate aggregation of routing information, so that the size of the routing advertisements can be minimised. Where networks use limited bandwidth bearers (e.g. long haul links to deployed forces, or tactical nets) this is critically important.
- The address space should be contiguous and therefore the complete allocation will need to be applied for as soon as IPv6 is brought into service.

The requirement to use hierarchical addressing implies that the total address space requirement may be significantly greater (by orders of magnitude) than the total number of addressable interfaces actually used. However, the savings which result from efficient administration and route aggregation will far outweigh the additional cost of address ownership[46].

[46] /32 $2,500 per year (2nd and subsequent years) /20 $40,000 (2nd and subsequent years)

Analysis Method

Analysis Method Steps

The following is a sequential list of analysis steps that can be followed to design a generic IP network addressing scheme:

i) Specify the lifetime for the network topology. This is an important step as it will drive the size of the address range required. To ensure that routing efficiency is maximised it is recommended that a single contiguous address space is sought and utilised. It is assumed that the size of the network will only continue to expand from the present day through its lifetime.

ii) Design a hierarchical network topology to meet the specified lifetime. Start with the network core (parent/top level of hierarchy), then add child/lower level sub-nets in accordance with the operational, security, physical and legacy systems requirements and constraints. Continue adding subnets in a hierarchical manner until the lowest "IP" addressable entity is reached at the end of each of the network's branches.

iii) At each level in the hierarchy specify the maximum number of interfaces. This is achieved by analysing each branch on the subject level and using the branch that yields the largest number of interfaces. The final result is achieving by rounding up this number to the nearest power of two. This will determine the number of address bits required (e.g. 2 bits = maximum of 4 interfaces, 4 bits = maximum of 16 interfaces etc). In general it is expected that the number of interfaces will increase as one moves down each level of the hierarchy (i.e. Level 2 may have more interfaces than Level 1 and Level 3 may have more than Level 2 and so on).

iv) Review the address prefix structure and size. If the size is too large then re-visit the levels of the hierarchy where the allocated binary address size is just larger than a binary increment (e.g. 17 is just beyond 16) and review the assumptions to see if one or more bits can be saved by slightly reducing the allocated size to below the previous binary increment.

Worked Examples

In each example, we have followed the usual practice of allocating 64 bits to the interface ID. Typically the interface unique MAC address is used, which allows stateless auto-configuration[47] to be used, if permitted by the security policy.

Using the analysis steps provided in 5.4.1 we provide the following worked examples for reference.

A Large Network Example

i) Lifetime is specified as 15 years, this assumes that the design meets the 2020 needs of the ADO.

ii) The DWACN is assumed to be at the core (Level 1) in the highest level of the hierarchy (see Figure 18). The subsequent levels are populated as follows:

a. The next level (Level 2) is occupied by the virtual (uses the same core infrastructure) and other physical security domains. The virtual domains include the DRN, DSN and DVN[48], the other security domains could include multiple coalition domains, other Australian government domains and the Internet etc.

b. The next level (Level 3) is occupied by a number of Base Area Networks (BANs) and a number of Long-haul sub-nets to meet operational requirements. The number of Long-haul subnets will be determined by assessing the number of geographic areas required to be covered and the actual coverage of the available

[47] RFC2462

[48] It is recommended that the use of addresses to provide security separation be expressed differently when making the application to APNIC.

Long-haul service options. The Long-haul subnets could be IP transit services provided by ADO, allied or commercial networks.

c. The next level (Level 4) is occupied by a number of LANs connected to their parent BANs and a number of Tactical area sub-nets connected to the parent Long-haul subnet. The Tactical area sub-nets represent IP service provided over a system such as Parakeet (JP2072 in the future). These sub-nets provide service to a number of deployed headquarters (HQs) as well as transit service to mobile sub-nets.

d. The next level (Level 5) is only utilised on the Long-haul branches and is populated by a number of mobile sub-nets. The mobile sub-nets could comprise a number of routers installed in land vehicles (Australian Light Armoured Vehicles (ASLAVs), Command vehicles, Jeeps etc). In the future a group of aircraft, or a swarm of Unmanned Combat Air Vehicles (UCAVs) might also form a mobile sub-net.

e. The last level (Level 6) is also only utilised on the Long-haul branches and is populated by a number of LANs within each vehicle.

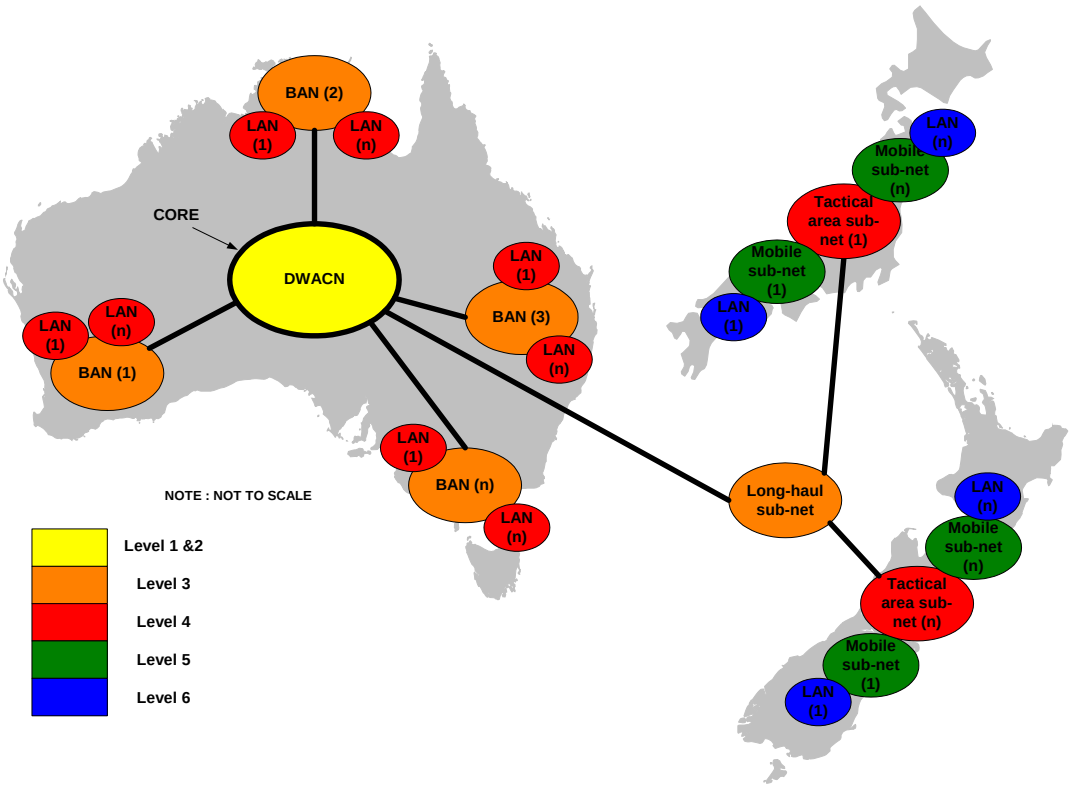


Figure 18 Example[49] Network Topology

[49] Except for Australia, these countries are only an example.

iii) The number of interfaces at each level of the hierarchy is depicted in Figure 19 and detailed as follows:

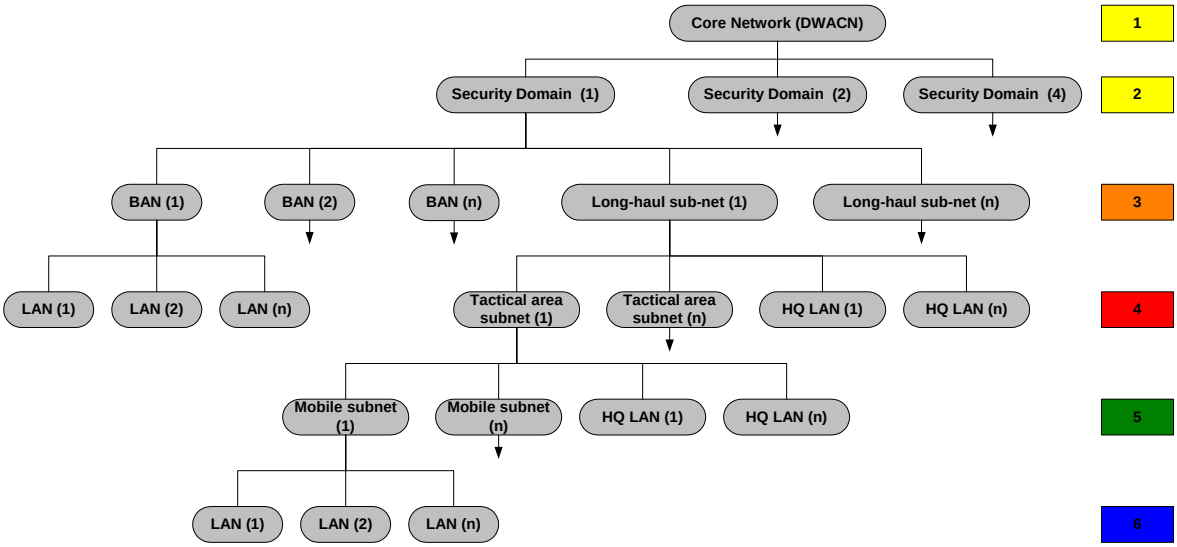


Figure 19 Example Network Hierarchy

a. Level 1 interfaces. Assuming that there are up to 4 ADO security domains (including DSN, DRN and DVN), 3 coalition domains, 2 other government domains and 2 miscellaneous domains, this equals 11 interfaces, rounding up to nearest power of two equates to 16 interfaces (4 bits).

b. Level 2 interfaces. Assuming that there are 300 BANs[50] and 4 Long-haul sub-nets and 600 internal routers, this equals 904 interfaces, rounding up this equates to 1024 interfaces (10 bits).

c. Level 3 interfaces. For the BAN branches, it is assumed there would be a maximum of 4 LANs and 10 internal routers, for the Tactical sub-net branches, it is assumed that there would be a maximum of 4 Tactical sub-nets, 4 attached Headquarters and 20 internal routers. Therefore the Tactical sub-net branch has the largest number of interfaces (28), rounding up this equates to 32 interfaces (5 bits).

d. Level 4 interfaces. As both the (BAN/LAN) and the (Long-haul sub-net/HQ LAN) branches have terminated we only need consider the attachments to the Tactical area sub-net branches. For these branches we assume that there will be a maximum of 4 mobile sub-nets, 40 HQ LANs and 50 trunk routers, therefore 94 interfaces and rounding up this equates to 128 interfaces (7 bits).

e. Level 5 interfaces. As the (Tactical area sub-net/HQ LAN) branches have terminated we only need consider the attachments to the Mobile sub-net branches. For these branches we assume that there will be a maximum of 100 vehicle LANs, therefore 100[51] interfaces and rounding up this equates to 128 interfaces (7 bits).

f. Level 6 interfaces. At each vehicle LAN we assume that the maximum number of interfaces is 100 and rounding up this equates to 128 interfaces (7 bits).

[50] Source = [4] 1.2.4 DWACN FPS

[51] The figure of 100, could well be argued and is very much a forward looking number assuming that in 15 to 20 years time there could be many entities requiring and IP address.

iv) The address structure uses 40 bits (a /24 address) as follows:

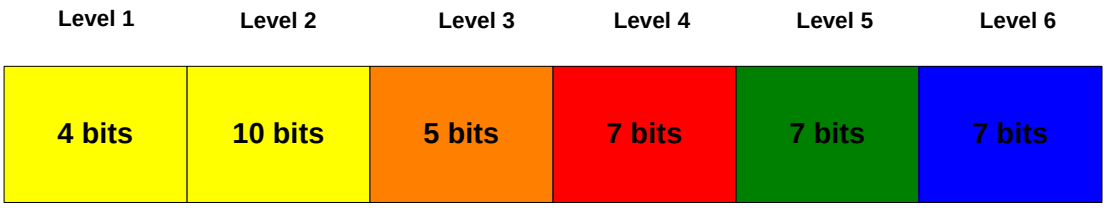


Figure 20 Address Size

A Future Large Network

We now consider expanding the previous example by considering potential areas of growth.

i) Lifetime is also specified as 15 years.

ii) The same topology and hierarchy is assumed.

iii) The same number of interfaces at each level is assumed except for those at Level 6. It is likely that major increases in demand from address space will only arise from significant changes in technology. One potential for the additional of an address-hungry sub-network could come from the addition of unattended sensors. These sensors (small low-power seismic, acoustic, RF sensing etc) could be scattered from the air in their thousands across a tactical area. This could lead to a sub-net at Level 6 with say 5000 nodes/interfaces. Assuming that the sensor control station branches from a mobile sub-net this would be rounded up to a maximum of 9182 interfaces (13 bits).

iv) The address structure uses 46 bits (a /18 address) as follows:

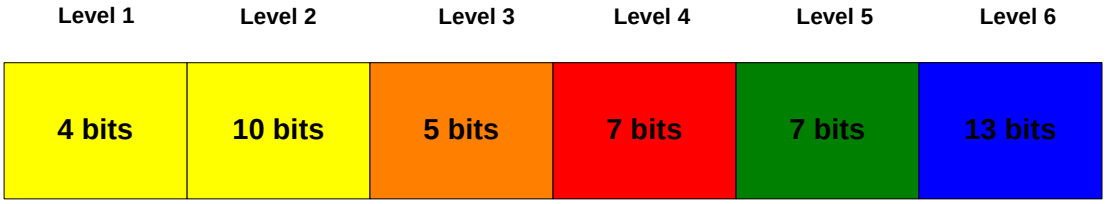


Figure 21 Address Size

A Modest Network

We now consider the previous “Large Network” and revisit each level in the hierarchy to investigate how the network could be reduced in size to a network with a more modest address space requirement.

i) Lifetime is also specified as 15 years, this is viewed as the minimum requirement.

ii) The number of interfaces at each level of the hierarchy is as follows:

a. Level 1 interfaces. Assuming that there are just 3 ADO security domains (the DSN, DRN and DVN), 2 coalition domains (Restricted and Secret), 1 other government domain and 2 miscellaneous domains, this equals 8 interfaces, rounding up to nearest power of two equates to 8 interfaces (3 bits).

b. Level 2 interfaces. Assuming that there are still 300 BANs[52] and just 2 Long-haul sub-nets and 200 internal routers, this equals 502 interfaces, rounding up this equates to 512 interfaces (9 bits).

[52] Source = [4] 1.2.4 DWACN FPS

c. Level 3 interfaces. For the BAN branches, it is assumed there would be a maximum of 4 LANs and 10 internal routers, for the Tactical sub-net branches, it is assumed that there would be a maximum of 2 Tactical sub-nets, 2 attached Headquarters and 12 internal routers. Therefore the Tactical sub-net branch has the largest number of interfaces (16), rounding up this equates to 16 interfaces (4 bits).

d. Level 4 interfaces. As both the (BAN/LAN) and the (Long-haul sub-net/HQ LAN) branches have terminated we only need consider the attachments to the Tactical area sub-net branches. For these branches we assume that there will be a maximum of 2 mobile sub-nets, 20 HQ LANs and 30 trunk routers, therefore 52 interfaces and rounding up this equates to 64 interfaces (6 bits).

e. Level 5 interfaces. As the (Tactical area sub-net/HQ LAN) branches have terminated we only need consider the attachments to the Mobile sub-net branches. For these branches we assume that there will be a maximum of just 64 vehicle LANs, therefore 64 interfaces and rounding up this equates to 64 interfaces (6 bits).

f. Level 6 interfaces. At each vehicle LAN we assume that the maximum number of interfaces is just 64 and rounding up this equates to 64 interfaces (6 bits).

v) The address structure uses 34 bits (a /30 address) as follows:

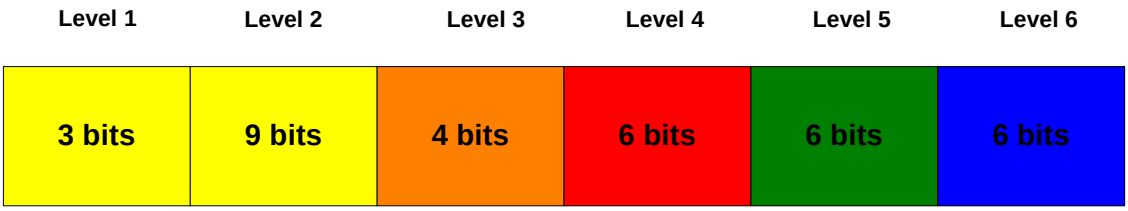


Figure 22 Address Size

Regional IPv6 Addressing

IPv6 address allocation is managed on a regional basis (by ARIN, RIPE, APNIC). It is the aim that global routing will be more efficient by allocating address blocks in relation to the location of the organisations requesting the allocation.

The ADO has a fixed infrastructure, but also expects to be engaged in operations with a regional or occasionally global reach. Will this create a problem?

The short answer is no. The ADO will use addresses for deployed networks which are sub-netted from those allocated to the fixed network. The connectivity to deployed networks will be over long-haul networks (or bearers), so that the routing path will be from Australia, even if the deployed forces are in a different region.

If a deployed ADF network needs to connect to a network belonging to a coalition partner, which could have addresses from a completely different range, this is not a problem. It is likely that an exterior gateway routing protocol (e.g. BGP) will be used at the boundary. This will need to be configured appropriately, it will normally be necessary to avoid a situation where, for example, traffic from the deployed ADF unit to a destination in Australia is routed over the ally's networks to their home nation and thence to Australia. Similar issues apply today with routing in IPv4, and will be solved in the same way in IPv6, by careful and intelligent router configuration.

If a deployed ADF network uses IP transit services from a coalition partner, or commercial ISP, then it is most probable that tunnelling will be used. This separates the routing domain of the ADO from that of the service provider, so again no addressing problem should arise.

Address Space Conclusion

The three worked examples of the previous section suggest that a wide-range of network sizes could be realised using a 6 level hierarchy. The example analysis shows that the network size can vary quite dramatically between 34 bits (/30 address) and 46 bits (a /18 address).
Because we have specified a lifetime of 15 years and we assume that we are more likely (at this point in time) to have under-estimated the potential for growth over that period, it is recommended that the ADO apply for a minimum allocation of a /18 address.

Ipv6 Transition Governance

This section details the recommended ADO IPv6 transition governance structure that should be used to manage and coordinate all the ADO's IPv6 transition activities.

Introduction

This section is introduced by revisiting our important high-level network centric principles and by providing some background to the potential difficulties that have been experienced as the result of other organisations approaches to their information environment governance structures.

As a starting point, the ADO's DIE governance structure must support the ability of the various ADO organisations to work together to achieve network-enabled operations by following our two (previously espoused) crucially important principles (see section 3.1.3 for further explanation of the principles):

Principle 1 : Unit-Level LANs

End-systems (e.g. sensors, weapons, Allies etc) are connected to "the network" and not to each other. They are attached to unit-level LANs which are in turn connected via a router to either a radio-WAN or a terrestrial WAN.

Principle 2 : Routable WANs

Make Radio-WANs and terrestrial WANs routable.

In general other organisations have tended to cast their CIOs into one of two roles, or in some cases the job description is a mix of these two roles, i.e.:

a) as the program manager for the implementation of various information infrastructure projects, with responsibility for their budget and schedule, or

b) as the interoperability custodian across a diverse range of projects and programs, some information environment related and some not (i.e. end-systems and platforms).

Both roles introduce major challenges, especially if the role encompasses responsibilities as both a program manager in the information environment space and as the interoperability custodian across the whole defence environment, including for the end-systems and platforms.

If a CIO is cast with only program manager responsibilities (e.g. hypothetically, DWACN, JP2072 and others) it is likely that:

a) The CIO will have the potential to be successful at achieving **Principle 2**, but because their responsibility does not extend to the end-systems, it will be difficult to achieve **Principle 1**. Whilst the result may be a highly capable information network (the plumbing, routers, servers, cable etc), it is highly likely that the desired capability of network centric operations will not be realised to the extent required by the ADO. In this context the fact that the network is IPv6 capable largely becomes irrelevant.

The OSD CIO in the US DoD has gone down this path and has attempted to solve the resultant problem by splitting its organisation into a CIO's office, who looks after standards compliance, and the Networks and Information Integration (NII) office who is the networking advocate. This has however resulted in the CIO becoming the advocate for the very programs that he's supposed to have oversight for. There is every possibility that this could create many conflicts of interests with the result being less than fully successful.

We recommend that the optimum situation will be formed by instituting a governance structure (for IPV6 transition) that focuses on the CIO being the "interoperability custodian" where:

b) The CIO has measures in place to ensure that **Principle 2** is applied by the "information infrastructure[53]" projects managers and **Principle 1** is applied by all other project managers. These other project managers will be delivering projects that connect to the DIE in some way, they will be the end-systems and will include the platform projects (e.g. JSF, AWD etc). As long as the existing projects/programs are suitably structured and of a manageable size, then it is recommended that their program structures be left intact. The important concept is to put measures in place that allow the interfaces between projects to be become compatible and interoperable.

Ideally the sequence of events in the process that should be adopted to achieve the optimum result is: interoperability, followed by modularity and modularisation followed by standardisation.

Management and Organisational Structures

Figure 23 illustrates the stakeholder organisations from an ADO IPv6 transition perspective.

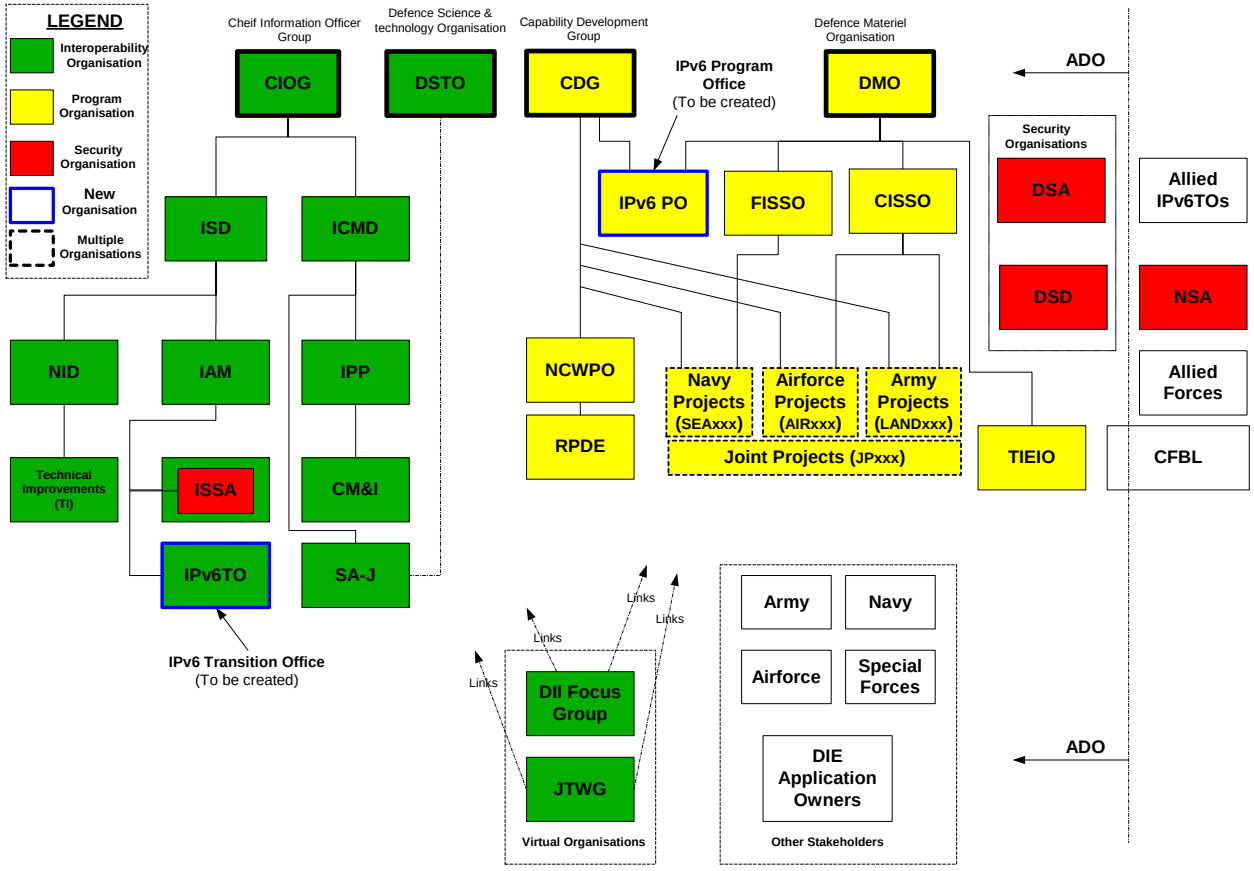


Figure 23 ADO Stakeholder Organisations From an IPv6 Perspective

The roles of the existing lead organisations and their existing subordinate organisations are described as follows.

Chief Information Officer Group (CIOG)

The CIOG is divided into the Information Systems Division (ISD) and the Information Capability Management Division (ICMD), for a complete CIOG organisational structure please see Annex F. Within these two divisions the following branches will have an IPv6 role as follows.

[53] e.g. DWACN, JP2072 etc.

Network Infrastructure Development (NID) Branch

As part of ISD, NID is an important organisation from an IPv6 perspective as responsibility for all the ADO's software applications have recently been centralised within the branch.

Technical Improvements (TI)

As part of NID, TI is expected to play a role in the development of an ADO pilot/test-bed[54] capable of implementing IPv6 for the purposes of evaluating the technology and the strategies for transition.

Information Architecture & Management (IAM) Branch

As part of ISD, IAM Branch is responsible for developing and maintaining the enterprise architecture and governance processes and tools that support the Defence Information Environment. Using its specialist staff and innovative support arrangements, IAM Branch assists Defence's Groups and Services in establishing and supporting their individual architecture offices and practices within the federated approach mandated by the Defence Architecture Framework.

Information Systems Security Assurance Branch

As part of IAM, ISSA will have responsibilities for the accreditation of applications and systems to the ADO IPv6 standard.

Information Policy and Plans (IPP) Branch

As part of ICMD, IPP branch executes the CIO's principal responsibilities as Coordinating Capability Manager of the Defence Information Environment (DIE). The Branch is responsible for the management and coordination of the DIE capability on a short-to-mid term basis (typically 0-5 years). The Branch is responsible for the short-to-mid term prioritisation of the information capability investment program (including minors) and oversight of portfolio DIE expenditure.

Scientific Advisor - Joint (SA-J) Branch

As part of ICMD, The Scientific Adviser - Joint (SA-J), represents the Defence Science and Technology Organisation (DSTO). SA-J advises the Australian Defence Joint Warfare, Information, Intelligence and Strategic communities on science and technology (S&T) issues and trends relevant to the development of capability and conduct/support of operations.

Defence Science and Technology Organisation (DSTO)

DSTO provides the ADO with scientific advice and supports the CDG and DMO through providing specialist scientific reports and conducting risk-analysis work and experiments in the support of these organisations.

Capability Development Group (CDG)

CDG is the ADO's capability manager and is responsible during the start-up phase of projects through to the completion of second-pass where the projects are handed over to the DMO. In Figure 23 we are showing this relationship for the Navy, Airforce, Army and Joint projects where there are links back to both CDG and DMO.

Network Centric Warfare Program Office (NCWPO)

The NCWPO has been established within the Integrated Capability Branch of CDG where it has authority to integrate projects into the force in being and the future force. The NCWPO is expected to be closely involved with ensuring that Principles 1 and 2 are followed.

Rapid Prototyping Development Environment (RPDE)

The Mission of the RPDE Program is "To enhance ADF war fighting capacity through accelerated capability change in the Network Centric Warfare (NCW) environment". The RPDE concept aims

[54] This was suggested by the Commonwealth at the IPv6 workshop. The hardware for this test-bed may already be in existence.

to create a collaborative, non-competitive environment where Defence and industry can seek opportunities where rapid enhancement to capability can be achieved, principally by incremental enhancement of existing capability.

Defence Materiel Organisation

Fleet Information Systems Support Organisation (FISSO)

The FISSO takes responsibility for Navy projects.
Command & Intelligence Systems Sustainment Office (CISSO)

The CISSO takes responsibility for Airforce and Army projects.
Tactical Information Environment Integration Office (TIEIO)

The TIEIO provides a support service to the DMO where it performs integration services for the ADO's tactical information environment including Tactical Digital Information Links (TADILs), e.g. Link-11, Link-16 and Link-22 etc.

Other ADO Stakeholders

DII Focus Group

This group currently does not exist. It should be formed as a virtual/matrix organisation of existing O6/EL2 level ADO members who will be responsible for leading the detailed planning phase, for making the required executive decisions in support of this IPV6 Transition Plan and tasking the JTWG (see 6.2.5.2). The DII Focus Group will have wider DII responsibilities than just IPv6. It should be noted that there is currently a Tactical Gateway Focus Group and it is recommended that this group is subsumed into the DII Focus Group[55].

Joint Technical Working Group (JTWG)

This group currently exists and should be expanded to receive IPv6 related tasking by the DII Focus Group. The JTWG will undertake further IPv6 related analysis and technical work to determine solutions and make more detailed proposals. It should be noted that at the time of writing this plan, the CIOG/IAM organisation will soon assume sponsorship and chair of the JTWG[56].

Security Organisations

The ADO's Defence Security Authority (DSA) is the ADO's internal security authority with oversight over security for the whole of the ADO.

The ADO's Defence Signal Directorate's (DSD) purpose is to support Australian Government decision-makers and the ADO with high-quality foreign signals intelligence products and services. DSD also directly contributes to the military effectiveness of the ADF, and provides a range of information security services to ensure that their sensitive electronic information systems are not susceptible to unauthorised access, compromise or disruption.

The ADO's IPv6 transition organisations (see section 6.3) will need to closely interact with both DSA and DSD on the security aspects of the transition from IPv4 to IPv6.

Others

The remaining stakeholders within the ADO fall into the category of users of the DIE and DII and the owners of applications that reside within the DIE. These users will be the subject of IPv6 communications (see section 6.3) and training programs.

[55] These recommendations are in accordance with Commonwealth comments to the draft IPv6TP.
[56] This was advised by Commonwealth comments to the draft IPv6TP.

Other Stakeholders

Stakeholders external to the ADO include:

- the Allied IPv6 organisational elements (e.g. US IPv6TO),
- the US National Security Authority who the ADO will need to interact with to achieve interoperability and
- other government organisations.

IPv6 Transitioning OrganisationS

To support the goal of providing a governance structure which:

i) champions interoperability through policy measures and ensures that **Principles 1 and 2** are implemented and

ii) avoids an organisational structure (from an IPv6 transition view) like the US DoD CIO and NII offices,

We recommend that two new organisations are created as indicated in Figure 23.
The first organisation, the IPv6 Transition Office (IPv6TO), will sit within the CIOG and will provide the CIO with the governance measures to ensure that the CIOG becomes the "interoperability custodian" for the transition of the ADO's DIE and its end-systems from IPv4 to IPv6 i.e. to support **Principles 1 and 2** being implemented by CDG and DMO.

The second organisation, the IPv6 Program Office, will be functionally responsible to the CDG for projects during the start up phase and to the DMO for projects post second pass. It is enabled (by way of budget and schedule responsibility) to actually implement **Principles 1 and 2**. It is recognised that such an arrangement may be difficult to achieve and the resolution may be to create one program office within CDG and a second within DMO.

The roles and responsibilities of these two organisations are provided in more detail in the following sections.

IPv6 Transition Office (IPv6TO)

The prime function of the ADO's IPv6TO is to operate as the "interoperability custodian" for IPv6 transitioning activities (please see section 7 for the recommended office organisational structure and position descriptions).

The ADO IPv6 Transition Office will be established to carefully plan and manage, at the enterprise level, Defence's transition to IPv6 and will document this planning in the ADO IPv6 Transition Plan. This plan will be developed through broad consultation with key stakeholders. The ADO IPv6 Transition Office will be responsible for co-ordinating transition planning, analysis, testing and implementation efforts across Defence, promoting knowledge sharing, ensuring needed infrastructure is provided, and implementing a systematic program of outreach within Defence. The office will ensure that critical enterprise transition issues are prioritised and addressed.

The Transition Office will be responsible for providing policy and technical guidance to services, groups and projects/IPTs, and for defining procedures for approval and testing of migration/transition implementations.

The Transition Office should be structured to provide direction and guidance in the following technical areas:

- **Security**: this is a critical area; procedures must be in place to ensure that policy is enforced. System accreditors must be engaged to ensure that IPv6 issues are understood. There should be close co-ordination with ADO defence security organisations.

- **Networks**: this will cover both WANs and LANs. The provision of IPv6 service by individual component networks within the DIE will need to be co-ordinated. Issues relating to the provision and management of 6 over 4 and 4 over 6 tunnels and/or dual stack operation will need to be resolved. It will be important to reach agreement on where the responsibility for inter-working lies at network boundaries. This will probably need to be determined on a case-by-case basis.
- **Address allocation**: the Transition Office will be responsible for the management of IPv6 address allocation and the naming and addressing policy. It will also be responsible for the establishment of a root IPv6 Domain Name service (DNS). In performing these tasks the Transition Office will liase with the Network Architecture Office.
- **Applications**: initially this area will be concerned with the provision of application layer gateways between IPv4 systems and IPv6 systems. Subsequently it will be important to address migration of applications to IPv6. This will apply to common services (e.g. e-mail) as well as specific applications. Over the long term, this may become the major effort in the transition process.
- **Allied interoperability**: the Transition Office should provide a central focus for discussions with Allies (principally the US DOD) on the co-ordination of IPv6 migration where necessary for interoperability.
- **Scheduling**: the overall schedule for IPv6 migration will be maintained by the transition Office, which will need to co-ordinate the schedules of DIE component networks and information systems.
- **Standards**: IPv6 is currently a general term used to describe a wide range of technical standards. The IPv6TO will be responsible for defining the IPv6 standards baseline for the ADO.
- **Testing**: it will be necessary to set technical specifications and standards to ensure inter-working of DIE components as they migrate to IPv6. The Transition Office will produce high-level test plans and have oversight of the testing process, this will include interoperability testing and IPv6 certification. The IPv6TO will also set criteria for the assessment of performance and inter-working.
- **Test-bed**: it is recommended that the ADO commence migration with a pilot implementation, in order to gain understanding and confidence before going forward to migration on operationally critical systems. The ADO IPv6 Transition Office should have close oversight of this pilot project. This pilot test-bed could either be newly constructed specifically for the purpose or hosted on one of the existing ADO test-beds[57].

IPv6 Program Office (IPv6PO)

The IPv6PO's prime function is to act as the Program Manager for the implementation of IP and the implementation of the transition of IPv4 to IPv6, ensuring **Principle 2** is implemented. This program level responsibility will extend to end-systems and platforms (outside the scope of the DIE), where the role is to ensure that **Principle 1** is implemented. As such the IPv6PO will have allocated budget to carry out its duties and will have schedule responsibility.

As the IPv6PO is expected to have minimal staff, individual projects/IPTs (Navy, Army, Airforce and Joint) will be required to contribute staffing resources to help the development of the Transition Plans, particularly in the area of cost and schedule estimates. The IPv6PO will work with the IPv6TO who will provide guidance and consultancy to assist the projects/ IPTs and to ensure reasonable consistency in the estimating process. The IPv6PO will have the following responsibilities:

- Program level responsibility (budget and schedule) for the implementation of IPv6 across all the ADO's projects.

[57] This issue was discussed at the IPv6 workshop. There are many test-beds within the ADO, 28 in ISD alone, there are J-series message test beds in the TIEIO and another 6 test-beds in the RPDE. There is also the ADO's involvement in the CFBL test-environment.

- High-level participant on the IPv6 Detailed Planning Phase in collaboration with the IPv6TO.
- Development, management and maintenance of the ADO's IPv6 Implementation Project Plan including cost and schedule.
- Responsibility for complying with the IPv6 governance measures and technical standards as set by the IPv6TO.
- Take direction for IPv6 related implementation tasks from various CDG and DMO managers.
- Overall management responsibility for the IPv6PO at an organisational and program/technical level. Will monitor progress against schedule and budget.
- IPv6 implementation interface with all CDG and DMO projects. This duty will require the incumbent to liase with all impacted projects and programs (DWACN, JP2072, SEA1442 etc) to construct and maintain an overall ADO IPv6 schedule with inter-program/project dependencies. This schedule will also extend to Allied and other government programs.

Relationships with other IPv6 Transitioning Bodies

The ADO IPv6TO should establish and maintain close links with transition management organisations in Allied national defence departments. The prime link should be to the US DOD and DISA. The CCEB can facilitate this linkage and links to similar bodies in UK and Canada. It is expected that the US will wish to deal with Allies in multilateral bodies, rather than through many bilateral arrangements. The IPv6TO should also establish and maintain links with other Australian organisations (including industry) to achieve a whole of Government approach to the transition of IPv6.

Hierarchy of Documents

This section proposes a hierarchy of documents to be used by the ADO to manage and coordinate the IPv6 transition activities. This IPv6TP is the top-level parent document. The IPv6TO will maintain this document with changes and additions as required. Other IPv6 transition planning documents (including project budgets and schedules) will be subservient to this plan as depicted in Figure 24.

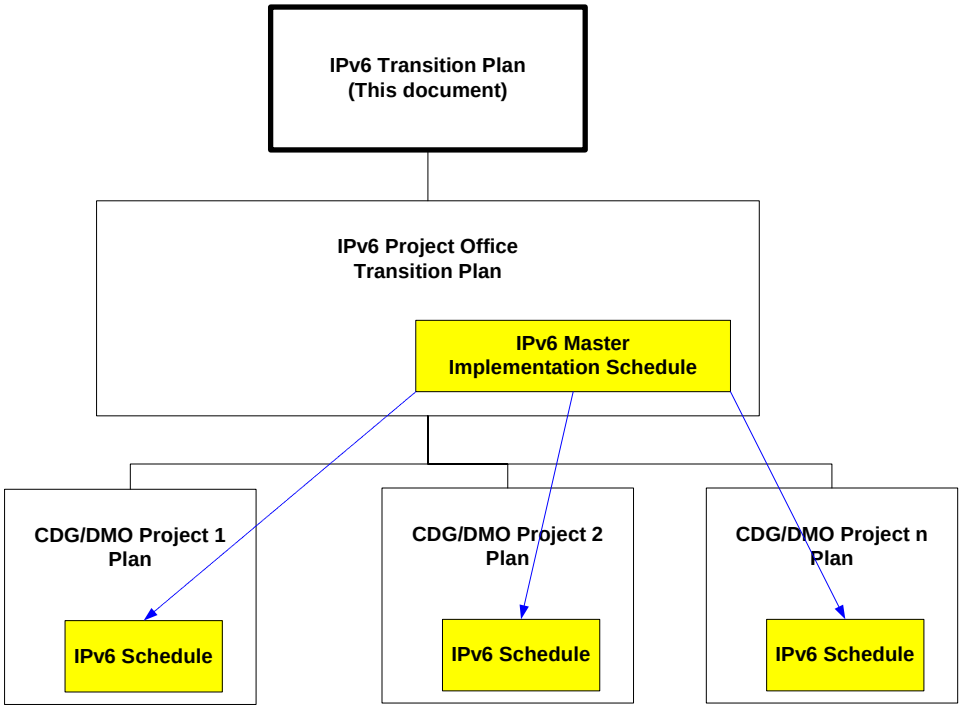


Figure 24 IPv6 Document Hierarchy

Lower Level IPv6 Transition Plans

The IPv6PO is assigned to coordinate the management of the implementation of IPv6 within the individual Defence Services, groups and projects. The IPv6PO will work closely with the IPv6TO and the projects being run by CDG and the DMO to develop an IPv6PO Transition Plan. A key function of the IPv6PO Transition Plan is to capture an integrated (whole of ADO) budget and schedule for the implementation of IPv6. The development of the top level integrated schedule (and budget) and the derived lower level (per project) schedules will require significant coordination and iteration between the IPv6PO and the individual projects. Also, because the transition strategy is leveraging off normal technology refresh cycles, these plans will require continual maintenance into the future.

These lower-level plans will be consistent with the overarching ADO IPv6 Transition Plan but will be focused on the planned transition within the Service/Group/Project, and will identify Service/Group/Project-specific issues and how they will be addressed. Critical dependencies and disconnects will be identified and worked through the DII Focus Group and the JTWG as appropriate. Individual Service/Group/Project plans would be endorsed by the ADO IPv6 Transition Office and approved within the individual Service/Group/Project.

These lower-level Transition Plans will include schedule and cost information. As they are produced it will become possible to refine the overarching ADO IPv6 Transition Plan, and the co-ordination process will lead to revision of these plans as necessary.

Ado ipv6 workforce requirements

To effect the ADO's transition to IPv6 over the period from now until 2013 will require effort to be applied in three major areas:

i) Level of effort undertaken by staff within the IPv6TO,

ii) Level of effort undertaken by staff within the IPv6PO and

iii) Results/milestone based effort undertaken by other ADO staff (or contractors) to transition the DII's applications (software) and hardware.

The following sections propose a suitable workforce to cover the above areas of effort.

ADO IPv6 Workforce

The IPv6TO and IPv6PO will need to perform a number of functions that can be allocated to one or more of the respective office's staff members.

IPv6TO Functions

The functions to be performed by the IPv6TO include:

i) Management and update of the ADO IPv6 Transition Policy [1].

ii) Planning, management and implementation of IPv6 governance measures and processes.

iii) Management of the transition of all DII applications and hardware from IPV4 to IPv6.

iv) Management of the IPv6 Test Program, this includes management and oversight of an IPv6 Test-bed.

v) Management of the IPv6 Security Program.

vi) Management of the IPv6 Allied Interoperability Program.

vii) Management of the IPv6 Communications Plan.

viii) Definition and management of the ADO's IPv6 standard.

ix) Provision of IPv6 technical specialist services.

IPv6TO Organisational Structure

The above functions of the IPv6TO could be fulfilled by an organisation with between three and four full time positions. The IPv6TO Lead may be a part-time (50%) position.

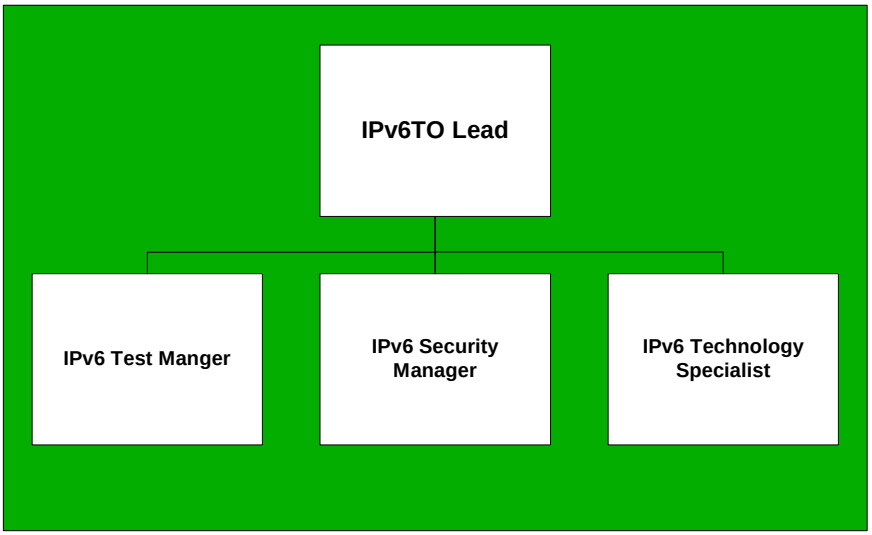


Figure 25 Suggested IPv6TO Organisational Structure

Lead Position

Position Duties

The IPv6TO Lead will perform the following duties:

i) Take direction for IPv6 related tasks from various CIOG managers and the DII Focus Group.

ii) Overall management responsibility for the IPv6TO at an organisational and program/technical level. Will monitor progress against schedule and budget.

iii) Planning and management of the IPv6 governance measures and processes. This will include involvement in First and Second Pass project review processes from an IPv6 perspective.

iv) Management of the IPv6 Communications Program. This duty will involve planning and performing IPv6 related education and information dissemination initiatives throughout the ADO, Allied organisations and other government organisations. The aim of the Communications Program is to ensure that the level of awareness within the ADO is sufficiently high across all the impacted ADO organisations to ensure an astute and timely transition from IPv4 to IPv6.

v) IPv6 Coordination. This duty will require the incumbent to liase with all impacted projects and programs (DWACN, JP2072, SEA1442 etc) to construct and maintain an overall ADO IPv6 schedule with inter-program/project dependencies. This schedule will also extend to Allied and other government programs.

vi) Management of the IPv6 Allied Interoperability Program. This duty will involve planning and performing the various initiatives required to support Allied interoperability from an IPv6 perspective. The incumbent will be responsible for liasing with Allied IPv6 transition offices and ensuring that Allied related information is past onto ADO projects as well as putting the case for ADO IPv6 requirements to Allies.

Owning Organisation

Each IPv6TO position is part of the CIOG organisation.

Competencies and Qualifications

The incumbent will need to be a competent manager of technology in a defence environment and is expected to hold a minimum of a diploma or degree qualification in engineering and preferably with a specialty in communications and network engineering. They will be capable of understanding the technical issues of transitioning the DIE to IPv6 and directing the technical effort within the IPv6TO.

Experience Required

The incumbent will need to have several years experience managing related projects within the DIE. A broad range of experience will be required in area of the terrestrial (DWACN) and deployed/tactical networks.

Tenure

This position will be required for the life-time of the IPv6 transition.

Test Manager Position

Position Duties

The IPv6TO Test Manager will perform the following duties:

i) Take direction for IPv6 related testing and related tasks from the IPv6TO Lead and from various CIOG managers and the DII Focus Group in consultation with the IPv6TO Lead.

vii) Overall management responsibility for the ADO's IPv6 test program at the program and technical level. The incumbent will be responsible for ensuring that the required

"IPv6 test-bed" assets are in place within the ADO. It is expected[58] that the Combined Forces Battle Lab Network (CFBLNet, see Figure 17) will have a major role in the IPv6 test program.

ii) Overall responsibility for the program to assess all the DII's applications and hardware for transition to IPv6. This includes managing and undertaking all the recommended assessment activities listed in section 7.2.

Owning Organisation

Each IPv6TO position is part of the CIOG organisation.

Competencies and Qualifications

The incumbent will need to be a competent manager of technology in a defence environment and is expected to hold a minimum of a diploma or degree qualification in engineering and preferably with a specialty in communications and network engineering. They will be very capable of understanding the technical issues of transitioning software applications and hardware within the DIE to IPv6.

Experience Required

The incumbent will have experience in the acquisition, test and acceptance of complicated hardware and software systems in the areas of communications and networking. It is preferable that they also have experience in the development and implementation of integrated hardware and software systems. It is also preferred that this experience extends across both the terrestrial (DWACN) and deployed/tactical environments.

Tenure

This position will be required for the life-time of the IPv6 transition.

Security Manager

Position Duties

The IPv6TO Security Manager will perform the following duties:

i) Take direction for IPv6 related security tasks from the IPv6TO Lead and from various CIOG managers and the DII Focus Group in consultation with the IPv6TO Lead.

ii) This position will be responsible for coordinating and liasing with the ADO's security organisation including the Defence Security Authority (DSA), the Defence Signals Directorate (DSD) and the Information Systems Security Assurance (ISSA) branch of the CIOG.

iii) The position will also be responsible for liasing with other security authorities and administrations, most importantly the US and UK authorities.

Owning Organisation

Each IPv6TO position is part of the CIOG organisation.

Competencies and Qualifications

The incumbent will need to be a competent manager of technology in a defence environment and is expected to hold a minimum of a diploma or degree qualification in engineering and preferably with a specialty in communications and network engineering. They will be very capable of understanding the security issues with the transitioning of software applications and hardware within the DIE to IPv6.

Experience Required

The incumbent will have experience in assessing software and hardware systems from a security perspective in a defence environment. They will need to have prior experience working with

[58] As advised by the Commonwealth during the IPv6 Working Group meeting on 29 June 2005.

similar issues with the ADO's security organisations and it is preferable that they have experience working with at least one other external security organisation e.g. the USA's NSA. It is also preferred that this experience extends across both the terrestrial (DWACN) and deployed/tactical environments.

Tenure

This position will be required for the life-time of the IPv6 transition.

Technology Specialist

Position Duties

The IPv6TO Technology Specialist will perform the following duties:

i) Take direction for solving IPv6 technical issues from the IPv6TO Lead and from various CIOG managers and the DII Focus Group in consultation with the IPv6TO Lead.

ii) Provide IP specialist technical support to the IPv6TO and to the ADO as a whole.

iii) IPv6 is currently a general term used to describe a wide range of technical standards. The incumbent will be responsible for defining the IPv6 standards baseline for the ADO.

iv) Be actively involved in designing and performing IP related tests (general areas and security related) and assessment activities on the IPv6 Test Bed and the DII.

v) Liase with software engineers to evaluate application code for compliance with IPv6 and assessment of the level of effort required to move an IPV4 application to IPv6. Perform the same function with the relevant hardware engineers for the transition of hardware to IPv6.

Owning Organisation

Each IPv6TO position is part of the CIOG organisation.

Competencies and Qualifications

The incumbent will be the prime technical point of contact for IPv6 within the ADO and as such they must in the first instance have a very good overall technical competency in the areas of communications and networking technology. They will have general knowledge of IPv6 and will over a short period of time become the ADO's subject matter expert in IPv6.
They are expected to hold a minimum of a degree qualification in engineering with a specialty in communications and network engineering.

Experience Required

The incumbent will have experience with the design and implementation of IP systems within the DII.

Tenure

This position will be required for the life-time of the IPv6 transition.

IPv6PO Functions

The functions to be performed by the IPv6PO include:

i) Program level responsibility (budget and schedule) for the implementation of IPv6 across all the ADO's projects, within the realms of the Capability Development Group and the Defence Materiel Organisation.

ii) High level participant on the IPv6 Detailed Planning Phase in collaboration with the IPv6TO.

iii) Development, management and maintenance of the ADO's IPv6 Implementation Project Plan including cost and schedule.

iv) Responsibility for complying with the IPv6 governance measures and technical standards as set by the IPv6TO.

IPv6PO Organisational Structure

The IPv6PO is conceived as an Integrated Product Team (IPT) with lines of reporting back through to CDG and DMO as required by the stage of the project (with an IPv6 requirement) being managed. The IPT would be staffed by members of both CDG and DMO and is estimated to be equivalent to one full-time position.

Although only consisting of nominally one new full-time position, the IPv6PO IPT will be supported by individual projects who will allocate resources to support the responsibilities of the IPv6PO (see IPv6 Project Managers below).

IPv6 Program Manager

Position Duties

The IPv6PO Program Manager will perform the following duties:

i) Program level responsibility (budget and schedule) for the implementation of IPv6 across all the ADO's projects.

ii) High level participant on the IPv6 Detailed Planning Phase in collaboration with the IPv6TO.

iii) Development, management and maintenance of the ADO's IPv6 Implementation Project Plan including cost and schedule.

iv) Responsibility for complying with the IPv6 governance measures and technical standards as set by the IPv6TO.

v) Take direction for IPv6 related implementation tasks from various CDG and DMO managers.

vi) Overall management responsibility for the IPv6PO at an organisational and program/technical level. Will monitor progress against schedule and budget.

vii) IPv6 implementation interface with all CDG and DMO projects. This duty will require the incumbent to liase with all impacted projects and programs (DWACN, JP2072, SEA1442 etc) to construct and maintain an overall ADO IPv6 schedule with inter-program/project dependencies. This schedule will also extend to Allied and other government programs.

Owning Organisation

Each IPv6PO position nominally reports back through to either the CDG or the DMO depending upon the stage of the subject project. As stated above, because of the difficulties with creating such a dual reporting structure it may be necessary to have two separate IPv6POs.

Competencies and Qualifications

The incumbent will need to be a competent manager of technology in a defence environment and is expected to hold a minimum of a diploma or degree qualification in engineering and preferably with a specialty in communications and network engineering. They will be capable of understanding the technical issues of transitioning the DIE to IPv6 and directing the technical effort within the IPv6PO.

Experience Required

The incumbent will need to have several years experience managing related projects within the DIE. A broad range of experience will be required in area of the terrestrial (DWACN) and deployed/tactical networks.

Tenure

This position will be required for the life-time of the IPv6 transition.

IPv6 Project Manager

There will be many IPv6 Project Managers spread across the range of Army, Navy, Airforce and Joint projects. The level of effort required to support each position within a project will vary between a small part-time role to a larger part-time role depending upon the scale of the IP implementation.

Each IPv6 Project Manager will be responsible to the IPv6 Program Manager and will have responsibility for either:

- the implementation of IP within their project, if they are DIE related, or
- the implementation of Principle 1 for end-system/platform projects.

Workforce to Transition Applications and Hardware

The depth of DIE analysis conducted in support of this IPv6TP has been insufficient to allow an accurate estimate of the total effort in man-years to transition the DIE's thousands of applications and hundreds of thousands of hardware items. What is provided here is a sequence of steps that needs to be followed during the detailed planning phase to formulate a quantifiable measure of the effort required. Management of this work will be the responsibility of the IPv6TO.

DII Applications

Each DII application needs to be assessed using the following steps:

i) The first step is to define the set of applications that will need to connect to the IP network either now or into the future.

ii) Applications are then categorised as either COTS or in-house/specialist developed. For those that are COTS, the vendor should be queried as to the IPv4/IPv6 roadmap. If the application is scheduled for IPv6 transition as part of the normal product development cycle then the additional level of effort (over that expended for any other product upgrade) is limited to that required to meet the conformance standards which verify that the application meets the ADOs IPv6 standard.

iii) For COTS applications where IPv6 is not on the applications developmental roadmap or the date for delivery of IPv6 is too far in the future, the vendor should be requested to provide a price and schedule for inclusion of IPv6 specifically for the ADO. If the cost and schedule is acceptable to the ADO then the upgrade would proceed with the normal conformance testing process being applied.

iv) For in-house or specialist applications where the ADO has ownership of the source-code and design documentation for the application, it should be possible for qualified software engineers to inspect the quality of the software design and implementation for transition to IPv6. This process will determine the level of effort required to perform that software upgrade including documentation and testing. The outcome of this process will determine the cost effectiveness of upgrading the application. If it is cost effective to upgrade the application then the upgrade should be undertaken and the software put through the same acceptance into service processes as any other IPv6 enabled application. If it turns out to not be cost effective then there are two options, the first is to continue to use the application (and therefore continue to provide IPv4 support) or to seek an alternative application that is IPv6 capable.

v) Should the above steps not lead to an acceptable solution, the alternatives include maintaining IPv4 support for the application or potentially seeking an alternative application that is IP agnostic i.e. a web-based application where the IP requirement falls to the browser application.

DII Hardware.

The DII hardware will have many of the same issues as software applications, except that some hardware items (usually peripheral devices) will possess an embedded IP stack where the stack cannot be upgraded via software (e.g. printers). The steps and solutions are the same for software except that it is most unlikely that it will ever be cost effective to upgrade lower cost peripheral hardware devices. In these situations where the hardware item cannot be replaced, the

only solution is to continue using the device and provide IPv4 support. This then becomes an obsolescence issue.

Risk management

Risk Log

The completed risk log is included in Annex C. The remainder of this section summarises the results of the risk log.

Risk Mitigation Strategies

Risk mitigation strategies are included in the "Treatment Strategies" column of the risk log in Annex C.

Risk Summary

With cognisance of the ADO IPv6 Transition context (see 3.1), the risk analysis process generated a risk log containing twenty six (26) risks, the log includes contributions from stakeholders who attended the IPv6 Workshop and others generated by the IPv6 Panel. The risks were rated for "Likelihood" and "Consequence" using the process from the ADO's Project Risk Management Manual, a summary of the outcome of the rating process for these risks is provided in the matrix in Figure 26.

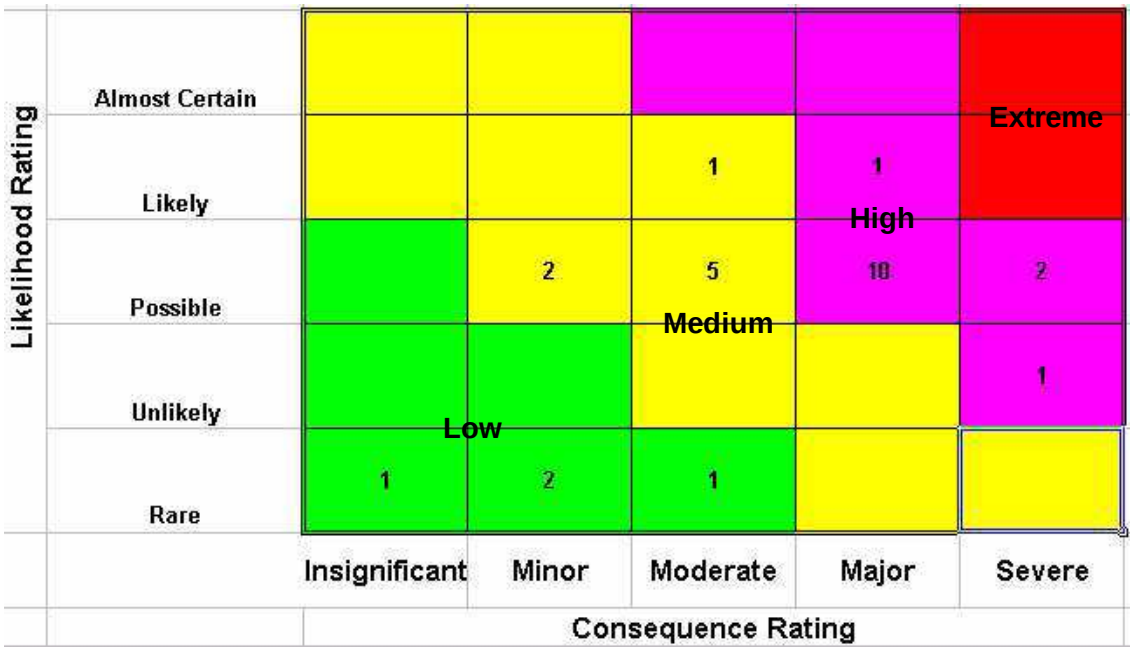


Figure 26 Risk Ratings Summary Matrix

As Figure 26 indicates, there were no "Extreme" level risks identified, fourteen (14) "High" level risks, eight (8) "Medium" level risks and four (4) "Low" level risks. The most common "Likelihood" rating was in the "Possible" category where 19 of the risks were classed. The most common "Consequence" rating was in the "Major" category where 11 of the risks were classed, although there was almost a 50/50 split between risks classed from "Insignificant" to "Moderate" and those in the "Major" to "Severe" category.

Each risk was also classified for the "Sources of Risk"[59] using the standard list of sources from the ADO's Project Risk Management Manual. As this IPv6TP is the very first step of a transition activity that is currently scheduled to run over the next eight years until 2013, the results for the most common sources of risk highlight the critical importance of the governance structure and

[59] See Annex C for the complete list of Risk Sources.

controls employed by the ADO to effect the transition from IPv4 to IPv6. The most common sources of risk (in order of frequency) were:

- “Management activities and controls” followed by,
- “Technology and technical issues” followed by,
- ”ADO project offices”.

Whilst much of the risk is sourced internally within the ADO, the reliance on COTS to effect the implementation of the transition and the need to interface with external bodies that lie outside the governance structure (e.g. Allied IPV6 transitions) means that there is also a large body of risk that lies outside the direct control of the ADO. The reliance on COTS is reflected by the next two most common sources of risk being in the classified areas of “Defence contractors” and “Maturity of technology required”.

Therefore the most sensible (and likely best value for money) mitigation/treatment strategies will concentrate on maintaining flexible governance structures, plans and technical architectures to allow the ADO implementation to cope with COTS IPv6 and Allied transitions that fail to meet the expected (and planned) timelines and budgets. A large part of this flexibility will be achieved by the wide-spread (across the ADO) adoption of Principles 1 and 2 (see Section 6.1).

Therefore a large part of the risk mitigation activity will be effected by the ADO (IPv6TO) periodically and continually revisiting this plan and maintaining a flexible stance to ensure that it can compensate for the effects of any realised risks during the transition from IPv4 to IPv6.

Dependencies and Key Assumptions

Key Assumptions

The key assumptions used to compile this document are as follows:

- **Ubiquitous IP** : Although it appears that it is not yet specific ADO policy to include in the architectural baseline requirements specifying that all Networks / Data-links / Bearers within the DII become routable by implementing IP, it is a key assumption that the requirements for NCW and the general push toward maximising the usage of COTS will mean that system designers will consider IP as a candidate technology wherever possible. Further to this it is also assumed that IP will be the first "Layer 3" technology considered by system designers and if it is not chosen for DIE system past 2013, it will be because of other reasons e.g. cost, interoperability or performance.
- **IPv6 Program Synchronisation** : Although the ADO will liase and coordinate with Allies and their programs to transition from IPv4 to IPv6, the coupling between these programs will be loose and not necessarily synchronised. This implies that the ADO must be prepared to inter-operate with Allies using both IPv4 and IPv6 for an extended period, probably well past 2013 and potentially up until any IPv4 flag day[60], should one be pronounced.
- **Security** : The security mechanisms in place today within the DIE and Allied networks use a mix of physical separation and encryption at the Data Link layer (2) or Network layer (3). Despite this there are techniques in place that allow a certain degree of interoperability between the ADF and its Allies. Ideally though, the most flexible, powerful and interoperable networks would be achieved if the DIE and Allied networks completely progressed to implementing the end-to-end network model with all security implemented at the Application layer (7), or "object-based". As object-based security is yet to be mandated for the DIE and there is significant momentum in the DCP toward expanding the current security mechanisms (e.g. $50 mil JP 2069[61]), it is assumed that there will be no fundamental change to the DIEs security architecture up until 2013.

[60] It is the Panel's view that an IPv4 Flag Day is almost certain to never occur.
[61] High Grade Cryptographic Equipment.

Conclusions

The ADO issued the policy "Transition To Internet Protocol Version 6" [1] in February 2005, this policy requires the DIE to transition to IPv6 by 2013 and importantly the policy states that IPv6 is an enabler for the ADO's vision of NCW.

This IPv6TP has been developed by BSG in collaboration with a Panel ("the Panel") of IPv6 subject matters experts from the IPv6 Forum, QinetiQ, the Naval Post Graduate School and the W2COG over the period from May through to July 2005. A draft of this plan was discussed at a workshop on 29 June 2005 and was attended by members of the Panel and various Commonwealth members. This Plan is considered to be a living document that will require revision and maintenance in order to keep pace with the rapid changes in networking technology. The scope for this IPv6TP includes the whole of the ADO's DII and DIE.

Although the ADO's IPv6 Policy was in place at the start of this task, the "context" for Internet Protocol (IP) (and the transition from IPv4 to IPv6 specifically) within the DIE was not apparent. Therefore the Panel's first response was to use a top-down system engineering methodology and develop the "context", this is the focus for Section 3.

The methodology in Section 3 analysed transitioning from artisan-based to industrial based information systems and then developed a definition for the GIG. The key observation from this analysis is that "modularisation" is the key to achieving interoperability (Note: Standards are also important but not key). To achieve modularisation (and then "net centricity") the following crucial overall design principles were generated:

Principle 1 : Unit-Level LANs

End-systems (e.g. sensors, weapons, Allies etc) are connected to "the network" and not to each other. They are attached to unit-level LANs which are in turn connected via a router to either a radio-WAN or a terrestrial WAN.

Principle 2 : Routable WANs

Make Radio-WANs and terrestrial WANs routable.

The analysis also produced derived design requirements for the end-systems (these connect to the DIE) and classified end-systems that comply with these requirements as "Good Network Citizens". The analysis also defined performance requirements for radio-WANs and proposed potential candidates for COTS re-use, i.e. IEEE 802.x standards are recommended as prime-candidates for consideration, even though some of the standards (e.g. WiMAX) will require modification to suit military systems. Two methods of dealing with legacy technology (during the IPv6 transition) were also considered, Cocooning and Layer 7 gateways, of the two Layer 7 gateways are viewed as more useful.

The context setting analysis concluded with a definition of the boundary between the non-DIE and the DIE, this is important because the boundary often extends into the ADF's platforms where many of the "legacy" issues will be encountered in the future. The use of the developed DIE IP context extended beyond just the technical (implementation) domain and was pivotal to the generation of the governance structure and workforce plan to support the transition from IPv4 to IPv6.

Section 3 also summarised the history and plans of the IPv6 activities being conducted by the UK MOD, NATO and the US DOD. Much of the detailed information concerning these plans was not available to BSG but should be available to the ADO through its Government-to-Government links. A list of known IPv6 documents is provided in 1.3.2 and the Panel is pleased to offer its assistance to the ADO with obtaining access to this material. It was concluded by the Panel that because IPv6 has yet to progress to a sufficient state (anywhere in the world) there are currently

no “off-the-shelf” strategies that could be applied to the DIE. In fact the implementation of the US DOD’s IP governance structure is viewed as containing a few lessons learnt and attributes that should be avoided by the ADO. As a result of this IPv6TP, the ADO is likely to be in advance of many organisations with regard to its IPv4 to IPv6 transition, and potentially better placed to meet its desired time-schedule if the governance mechanisms can be smoothly and successfully implemented.

The next input to the development of the IPv6 transition strategy was to analyse the current and future Defence Information Environment (DIE), see 3.3. The 2005 architecture and network magnitude was detailed with a specific emphasis on the DWACN, the DWACN is seen as a core element of the transition activity. This information was used an input to the development of an IPv6 numbering plan in Section 5. The future DIE architecture was covered by specifying the DCP projects that will move the DIE from its current baseline to its future state.

Section 3 concluded by providing relevant challenges, opportunities and emerging technologies. The ADO can expect to find its major challenges in the areas of transitioning its non-routable networks and security. To ensure that the ADO can rise to these challenges, the IPv6TO is proposed to be staffed with positions (Technology Specialist & Security Manager) that specifically address these areas of challenge.

The recommended IPv6 transition strategy commenced in Section 4 by considering three options. A “big bang” strategy was deemed too risky and costly, an incremental approach with hard-milestones did not comply with the approach of leveraging off the natural technology refresh cycles and so this led to recommending an incremental transition with soft milestones. The recommended strategy is depicted in Figure 15, this shows seven overlapping (soft milestone) phases:

- Phase 1 Planning,
- Phase 2 Network Security,
- Phase 3 National Application Gateways & Allied Application Gateways,
- Phase 4 Overlay Networks,
- Phase 5 IPv6 Clouds,
- Phase 6 Cloud Expansion and
- Phase 7 End State.

Importantly this strategy allows for a progressive roll-out of IPv6 whilst recognising that some parts of the DIE may never transition and small enclaves of IPv4 and links to external IPv4 networks will be required past 2013. The Planning phase extends for the life-time of the transition and it will be the IPv6TO and IPv6PO who will be responsible for conducting this planning effort and maintaining the over-arching IPv6 documentation. Also, the Network Security, National Application Gateways and Allied Application Gateway phases will also span the entire transition period (although having staggered starts) due to their importance and need to iterate with changing conditions both within the DIE and those of influence external to it.

The strategy has also been designed to be cost-effective, to have no impact on defence operations and not to degrade interoperability with Allies, justification is provided in 4.3.
To reduce the level of risk and ensure a successful transition Section 4.4 proposed a range of information assurance and test activities that will need to be conducted. These are designed to help ensure that ADO security is not prejudiced and experienced can be gained by the ADO with IPv6 before rolling the capability out into the DIE and operational environment. The recommended strategy section concludes with some specific advice for the DCP projects that are seen to be key to the IPv4 to IPv6 transition. Included in the list of key projects is JP2047, JP2008, JP2072, SEA1442 and JP2030.

At this early stage of the planning process it has not been possible to develop an IPv6 address space plan that can withstand the test of time i.e. from now until 2020 and beyond. However Section 5 provides a detailed step by step analysis method that can be used during the detailed

planning phase to construct a robust IPv6 address plan for the ADO. The method is illustrated using several examples, these are related to the ADOs current DIE architecture and consider future technologies that may be taken up by the ADO and consume addresses. These examples suggest that the ADO's IPv6 address range could be anywhere between 34 bits (/30 address) and 46 bits (/18 address). However the ADO should attempt to gain access to the largest contiguous block of addresses (e.g. /18) it can as the cost of using these addresses is likely to outweigh the costs of modifying the network in the future to suit a smaller (and or fragmented) address range.

Section 6 details a recommended governance structure for the ADO to transition the entire DIE and to ensure that the end-systems that attach to the DIE also conform to this IPv6TP. The "Unit-Level LANs" and "Routable WANs" principles (see above) are used again as the basis for the development of the governance structure. The CIOG organisation has recently undergone some significant changes and these are captured in the plan, the recent transition of the DMO to a prescribed agency may also have some impact on implementing these governance measures. Two new organizational offices are proposed to ensure that the governance regime is implemented in a astute and timely fashion and that the actual implementation of IPv6 is appropriately funded and scheduled.

The IPv6 Transition Office (IPv6TO) will be part of the CIOG, its prime responsibility will be as the "interoperability custodian" where it will complete the detailed planning of IPv6, promote information sharing across the ADO and ensure that the critical enterprise transition issues are prioritised and addressed. The IPv6TO will become the ADO's centre of excellence for IPv6 and will also offer technical guidance to the whole of the ADO. The IPv6TO will be staffed with up to four full-time positions.

The IPv6 Program Office (IPv6PO) has been proposed to act as the Program Manager for the implementation of IP in general and the transition of IPv4 to IPv6 across the whole DIE. Functionally the office must cover the scope of ADO projects from inception through to first pass (where they are under the control of the CDG) then on through second pass and into service (where they are under the control of the DMO). It is recognised that this may be a difficult proposition and if a single (one-person) office cannot be created, then the solution may be to have one office within the CDG and the other within the DMO. The IPv6PO will also require each project to allocate budget and schedule to the implementation of IPv6 as required. Although the office is small, its creation, function and lines of reporting are seen as crucial to a successful transition.

Section 7 details the organisational structure of the IPv6TO and IPv6PO. Each position within these offices is provided with a position description and description of the required competencies and experienced required to fulfil the role.

Although some quantification of the magnitude of the elements (hardware and software) of the current baseline DIE are provided in 3.3.1, it has not been possible within this IPv6TP to provide any detailed estimates for the level of effort required to transition software applications and hardware. Section 7.2 does however provide a detailed step by step procedure for assessing the hundreds of applications within the DIE with the aim of determining the effort/cost of making the IPv4 to IPv6 transition. It is also recognised that some applications may not be cost effective to transition and will be maintained as is in IPv4 enclaves within the DIE.

The conclusion to the process of developing this IPv6 transition strategy was to assess all its elements (including the proposed governance structure and workforce) for risk, see Section 8. A risk log capturing 26 risks was developed, each risk was assessed for likelihood and consequence and mitigation strategies were proposed. As the IPv6 transition will be heavily dependent upon COTS, there is a large degree of risk that will be beyond the direct control of the ADO. The responsibility for managing this risk will rest with the IPv6TO who will need to continually revisit this plan.

Recommendations

This IPv6TP is the first major step in an eight-year project to transition the entire DIE to IPv6 by 2013. As such the ADO will be required to complete many inter-linked activities and work with a variety of external organisations during the lifetime of the project.

The following is a list of recommendations for the immediate term:

- the ADO endorse this IPv6TP,
- the ADO endorse the governance and organisational components of this IPv6TP and commence resourcing the IPv6TO and IPv6PO,
- continue to engage the community of IPv6 subject matter experts to ensure that the progress with other organisations is tracked and lessons learnt are continually captured,
- sponsorship of combined Defence/Industry IPv6 forums to expand Defence's engagement with industry and whole of government,
- commence the Detailed Planning Phase including an initial IPv6 threat assessment and
- review the ADO's DWACN as-is and future architectures descriptions for the impact of this IPv6TP.

The following is a list of recommendations for the medium term:

- maintain and update this IPv6TP and its associated policies,
- undertake a detailed review each of the "Key Projects For Transition" (see 4.5),
- conduct a more detailed study and workshop in support of extending the work in this IPv6TP and developing a future looking IPv6 address plan and
- undertake specialist IPv6 and Network Centric focussed (See principles 1 and 2) training to raise the level of expertise within the ADO.

ANNEX A Interoperability Options

[62]IPv6 and IPV4 will coexist for many years. A wide range of techniques has therefore been defined that make the coexistence possible and provide a path toward transition. These techniques fall into three main categories:

- Dual-stack,
- Tunnelling and
- Translation.

Dual stack techniques allows IPV4 and IPv6 to coexist in the same devices and networks. Tunnelling techniques allow the transport of IPV6 traffic over the existing IPv4 infrastructure. Translation techniques allow IPv6-only nodes to communicate with IPv4-only nodes.

Dual-stack Techniques

Using the dual-stack nodes throughout a network provides complete support for both IPv4 and IPv6 protocol versions.

In communication with an IPv6 node, such a node behaves like an IPv6-only-node, and in communications with an IPv4 node, it behaves like an IPv4-only node. Implementations probably have a configuration switch to enable or disable one of the stacks. Therefore dual stack nodes can have three modes of operation:

- IPv4 enabled and IPv6 disabled – Behaves like an IPv4 only node
- IPv4 disabled and IPv6 enabled – Behaves like an IPv6 only node
- IPV4 enabled and IPv6 enabled (IPv4/IPv6) – Node can use both protocols

An IPv4/IPv6 (both stacks enabled) node has at least one address for each protocol version. For IPv4 it will configure by using either static configuration of Dynamic Host Configuration Protocol (DHCP) and for IPv6 it will use either static configuration or auto-configuration.

Domain Name System (DNS) is used with both protocol versions to resolve names and IP addresses. An IPv4/IPv6 node needs a DNS resolver that is capable of resolving both types of DNS addresses records. In some cases, DNS returns only an IPv4 or an IPv6 address. If the host that is to be resolved is a dual-stack host, DNS might return both types of addresses. Generally, applications that are written to run on dual-stack nodes need a mechanism to determine whether it is communicating with an IPv6 peer or an IPv4 peer.

A dual-stack network is an infrastructure in which both IPv4 and IPv6 forwarding is enabled on all routers. The disadvantage of this technique is that a full network software upgrade is required to run the two separate protocol stacks. This means all tables (e.g. routing tables) are kept simultaneously, routing protocols being configured for both protocols. For network management, there are separate commands (e.g. Windows OS - ping.exe for IPv4 and ping6.exe for IPv6). Other problems include higher memory and power consumption.

Dual-Stack Advantages

- Easy and flexible to use.
- Hosts can communicate with IPv4 hosts using IPv4 or with IPv6 hosts using IPv6.
- When the IPv6 upgrade is complete the IPv4 stacks can simply be disabled or removed.

[62] Most of this Annex has been sourced from [2] and the IPv6 Forum

Dual-Stack Disadvantages

- Two stacks require more CPU power and memory than one stack (not such a big issue).
- Requires two tables, one for each protocol, increased management effort.
- Requires two sets of commands, one for each protocol, increased management effort.
- A DNS resolver running on a dual-stack host must be capable of resolving both IPV 4 and IPv6 address types.
- Applications on a dual-stack host must be capable of determining whether this host is communicating with an IPv4 or IPv6 peer.
- Should use a firewall to protect the IPv4 network and the IPv6 network.

Tunnelling

Tunnelling is used to carry IPv6 traffic be encapsulating it in IPv4 packets and tunnelling it over the IPV4 routing infrastructure.

Tunnelling

There are two types of tunnelling[63]:

- Manually configured tunnels. IPv6 packets are encapsulated in IPv4 packets to be carried over IPv4 routing infrastructure. These are point-to-point tunnels that need to be configured manually.
- Automatically configured tunnels. IPv6 nodes can use different types of addresses (e.g. IPv4-compatible-IPv6 addresses, 6to4 or Intra-Site Automatic Tunnel Address Protocol (ISTAP)) to automatically tunnel packets over the IPv4 routing infrastructure. These special IPv6 uni-cast addresses carry an IPv4 address in some of the IPv6 address fields.

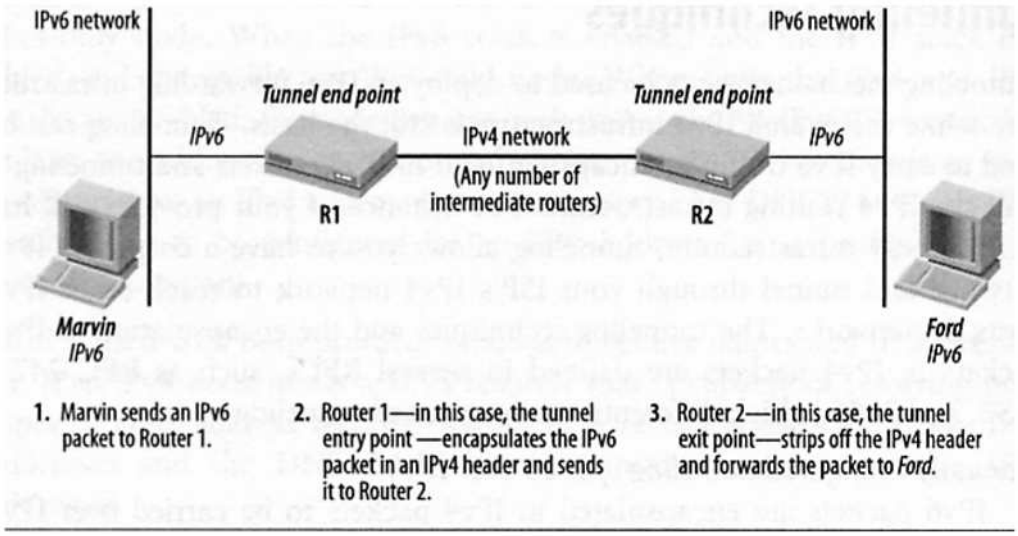


Figure 27 Tunnelling (6-over-4) Example

Tunnelling Advantages

- Flexibility, there is no specific upgrade order that needs to be followed.
- Single hosts or single sub-nets within a corporate network can be upgraded to IPv6.
- Continue to use IPv4 core network (Telstra & Singtel/Optus), core doesn't need to support IPv6.

[63] For more info see IETF RFC2893

Tunnelling Disadvantages

- Additional load placed on the router (a vendor design problem only).
- Tunnel entry and exit points need time and CPU power for encapsulating and de-capsulating packets (a vendor design problem only).
- Single point of failure (can be overcome by better network design).
- More complex trouble-shooting as may develop “hop count”, MTU size or fragmentation issues.
- Less flexibility when using IPv4 compatible IPv6 address, as the limitations of the IPv4 address space remain in place.
- Potential for the number of tunnels to become very large and unmanageable.

Manually Configured Tunnels[64]

A manually configured tunnel is an IPv4 or IPv6 tunnel configured between two end-points to carry IPv4 or IPv6 traffic. This allows for example two IPv6 networks to be connected even when the infrastructure between those two networks is not IPv6 capable, or later in the transition two IPv4 networks to be connected that are separated by an IPv6 network.

Advantages

- Simple to deploy inside a network
- Allows transport of IPv6 packets over an IPv4 network
- Available on most platforms
- Also supports IPv4 traffic over IPv6
- Permits end-to-end interoperability
- Permits end-to-end secure trust model
- IETF Standard and specified solution

Disadvantages

- Must be manually configured
- Due to management overhead does not easily scale to be used in end-hosts
- May not scale without automation for many users across routing fabric

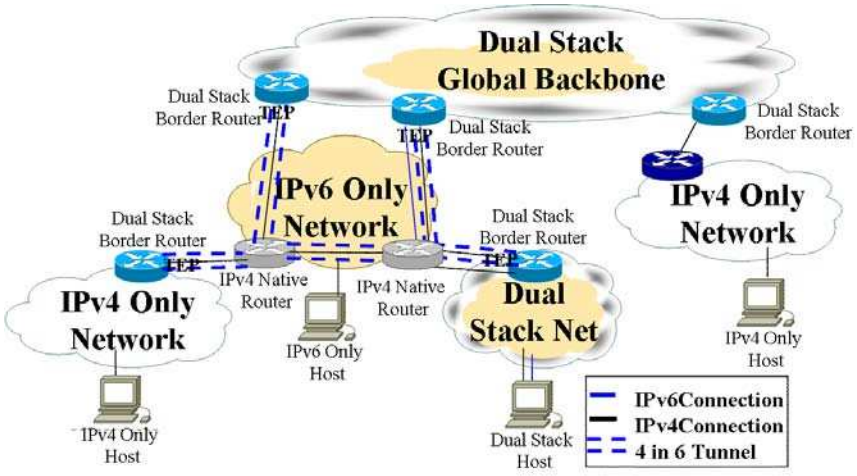


Figure 28 Manually Configured Tunnelling Example

[64] ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-v6ops-mech-v2-07.txt This document obsoletes RFC 2893.

Automatically Configured Tunnels

The following automatic techniques, 6to4, ISATAP and Teredo are expected to be more applicable for the commercial domain where more flexibility is required, mostly because it is common for the other end of the tunnel to be beyond the control of the network administrator. For defence applications it is expected that manual tunnelling methods will be more appropriate because increased control is provided and defence will have “mostly” complete control over its infrastructure.

6to4[65]

This is a mechanism that requires a single, globally unique IPv4 address. By embedding this 32 bit IPv4 address into a reserved IPv6 prefix, a router can create a globally unique /48 IPv6 prefix. The IPv6 packets are encapsulated in IPv4 packets without using explicit tunnels but automatic tunnelling mechanisms. Thus, making this low configuration overhead mechanism especially useful in IPv6 capable end-hosts. The usage of the special 6to4 address format, however, prevents the usage of an operator’s own address space. Thus, 6to4 is impractical in roll-outs beyond single host configurations or very small networks.

Advantages

- Relatively easy to deploy.
- Supported on numerous platforms.
- Provides an address block for an AS without dealing with any registry.
- An existing standard (RFC 3056).
- Permits end-to-end interoperability.
- Permits end-to-end secure trust model.
- Public 6to4 relays exist today.

Disadvantages

- Operator’s allocated IPv6 address space cannot be used.
- Impractical in network based roll-outs when entity has their own IPv6 prefix.

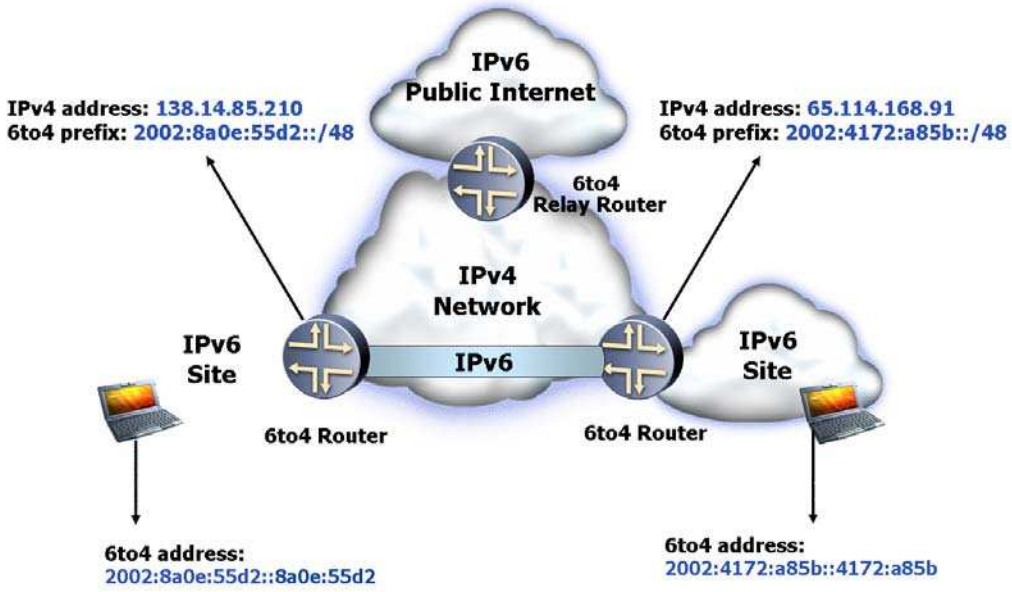


Figure 29 6to4 Example

[65] For more information see IETF RFC3056

ISATAP[66]

ISATAP is a solution to provide IPv6 connectivity to sparsely located hosts in an IPv4 network. In this solution, the IPv6 capable hosts use automatic IPv4 tunnels to connect to an ISATAP router, which is connected to further IPV6 networks.

The ISATAP addresses are created by using a special ISATAP interface identifier derived from the host's IPv4 address. Once the ISATAP router is reached, standard IPv6 stateless

Autoconfiguration is used over the automatic tunnel to create the IPv6 address. This mechanism allows the usage of operator allocated IPv6 address space in the prefix. In addition, the hosts can be in private address space as long as there is not Network Address Translation (NAT) between the hosts and the ISATAP router. Intra-site communication can be done directly between hosts using the IPv4 address in the interface identifier.

Advantages

- Provides for easy incremental deployment of IPv6 to disparate nodes in a site.
- Supported on many platforms.
- Works in sites that use private addresses when NAT is not present.
- Permits end-to-end interoperability.
- Permits end-to-end secure trust model.
- IETF work in progress, but unknown if it will be standardised by any entity.
- Supported by some platforms
- ISATAP will self-deprecate (i.e. turn itself off) when IPv6 is dominant and in use without the network operators having to dismantle the ISATAP mechanisms.

Disadvantages

- Caution has to be used when deploying the ISATAP routers to make sure they are not used to hide a Denial of Service (DoS) attack.
- ISATAP does not provide for multi-cast support

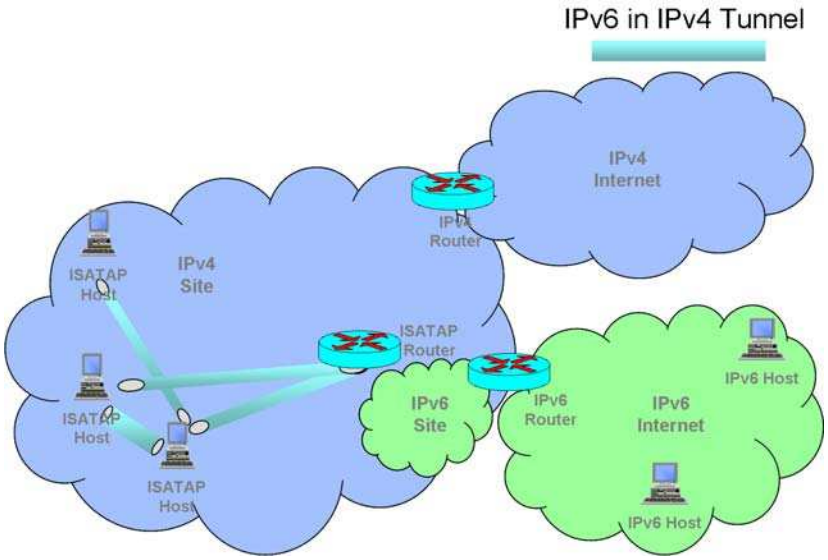


Figure 30 ISATAP Example

[66] ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-ngtrans-isatap-24.txt.

Teredo[67]

Teredo provides IPv6 connectivity to hosts that are located behind NAT-devices in networks without IPv6 support. Teredo uses a special address format where the IPv6 prefix is created using special Teredo prefix, IPv4 address and a UDP port number. The IPv6 packets are encapsulated in UDP allowing NAT traversal. The IPv6 address is automatically configured to the Teredo host by a Teredo server in the Internet. Two Teredo hosts can also use direct tunnelling between themselves.

Advantages

- Easy to implement on a "one-off" basis.
- Provides a solution that works through NATs.
- Provides a solution for networks with no IPv6 support.
- IETF standardized solution in process

Disadvantages

- Uses a special IPv6 address format. Thus, operator's own allocated address space cannot be used.
- Uses UDP to force hole in the client firewall.

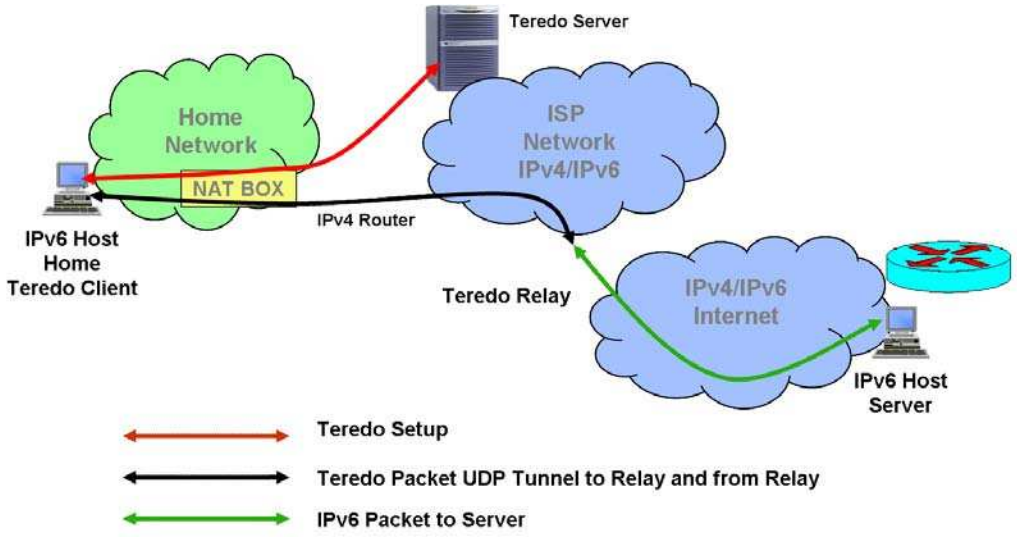


Figure 31 Teredo Example

Tunnel Broker Overview[68]

Tunnel Setup Protocol (TSP) is a tunnel broker based solution where the TSP client connects to a TSP broker that sends the client configuration information for setting up the tunnel between the TSP client and a tunnel server. TSP works both for a single host and a router. In addition, of providing IPv6 connectivity TSP supports authentication of the user and supports tunnelling of IPv4 over IPv6.

TSP is a good solution for connecting IPv6 networks as it supports IPv6 prefix delegation. In addition, TSP supports UDP encapsulation of the packets enabling NAT traversal of the tunnel. TSP can use operator's own address range for the terminals.

[67] ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-huitema-v6ops-teredo-05.txt.
[68] ftp://ftp.rfc-editor.org/in-notes/rfc3053.txt & ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-blanchet-v6ops-tunnelbroker-tsp-02.txt

TSP has not been standardized in any standardization body, yet. However, there are activities on-going to bring TSP to the IETF.

TSP is an instance of the Tunnel Broker model (RFC 3053). The TSP allows authentication of the user at tunnel setup.

Advantages

- Smaller configuration overhead than manually configured tunnels.
- Works also in dynamic environments.
- Supports NAT traversal.
- Support tunnelling of IPv4 over IPv6.
- Supports DSTM (below).
- Referenced as method to review by U.S. DoD.
- Strong industry support for deployment

Disadvantages

- Large signalling overhead.
- Heavy solution.
- Not standardized yet, but in process.

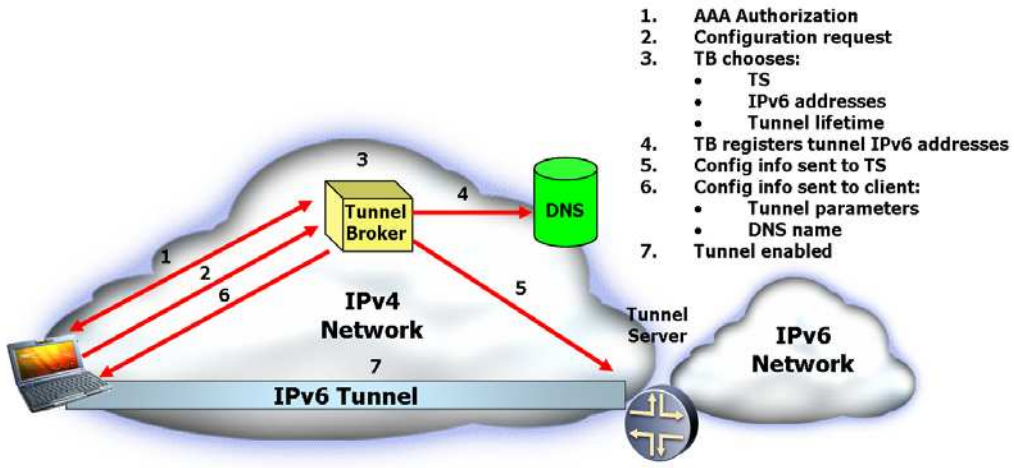


Figure 32 Tunnel Broker Example

Dual Stack Transition Mechanism (DSTM)[69]

DSTM has a different assumption to transition than the other mechanisms. DSTM assumes an IPv6 dominant deployment where most of the hosts are IPv6 capable and the network is mostly IPv6 only. In DSTM, IPv4 is transported over IPv6 tunnel to an IPv4 network.

IPv6 deployment in some operational networks will use an IPv6-dominant network deployment strategy. What IPv6-dominant means is that the network will transition to IPv6 using only IPv6 routing to transfer both IPv4 and IPv6 packets.

Advantages

- Provides IPv4 connectivity in IPv6 networks without explicitly configured tunnels.

[69] http://www.rfc-editor.org/cgi-bin/iddoctype.pl?letsgo=draft-bound-dstm-exp-03

- Maintains end-to-end security for IPv6 connectivity and for IPv4, when enough IPv4 global address space is available.
- Has had industry implementation and some testing.
- Referenced as method to review by U.S. DoD.
- Strong Industry support for this method.

Disadvantages

- Not standardized, yet, but in process.

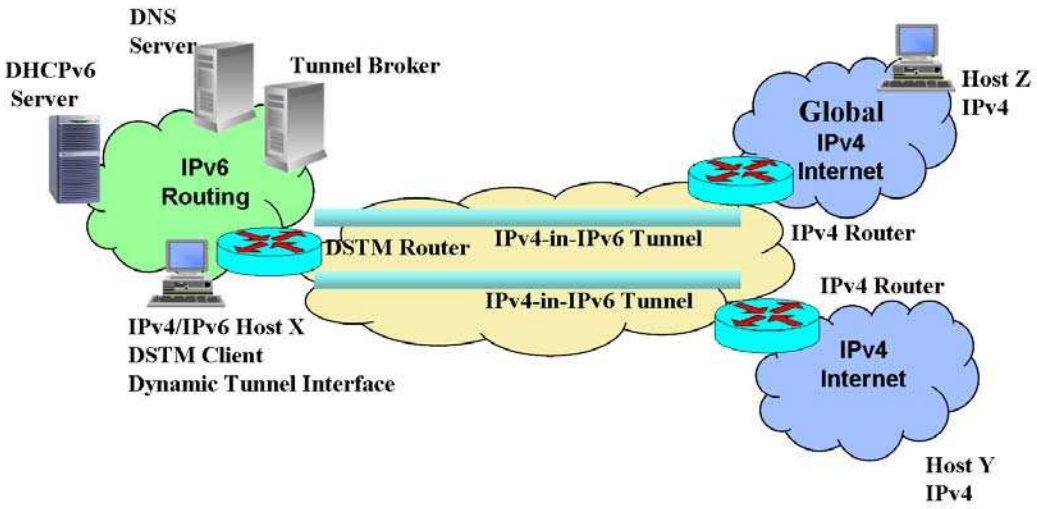


Figure 33 DSTM Example

Translation[70]

Network Address Translation – Protocol Translation (NAT-PT) uses address translation. Basically NAT-PT translates IPv6 packets to IPv4 packets and visa versa. The NAT-PT device has to keep state information of the flows passing the device to perform the protocol translation. The mechanism relies on a DNS Application Level Gateway (ALG) to translate IPv6 address queries to IPv4 queries and to build up the state in the NAT-PT device. The usage of the DNS-ALG is seen problematic due to various reasons. Thus, the IETF is in the process of moving the NAT-PT standard to experimental RFC.

The NAT-PT solution allows IPv6 only nodes in an IPv6 network to communicate with IPv4 nodes without being directly connected to the IPv4 network. However, it does have the same short-comings and restrictions than regular IPv4 NAT has. Thus, applications that do not work well with NATs do not work with NAT-PT either.

Translation Advantages

- Transparent to end nodes. Easily provide IPv4/IPv6 interoperability.
- Mechanism that allows the continued use of mission critical application or services that may be undesirable to have ported for use with IPv6.

Translation Disadvantages

- Single point of failure/bottleneck.
- Added administration.
- Has the same shortcomings of a traditional NAT.

[70] ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-v6ops-natpt-to-exprmntl-01.txt

- DNS-ALG is seen problematic.
- Does not permit the end-to-end network model

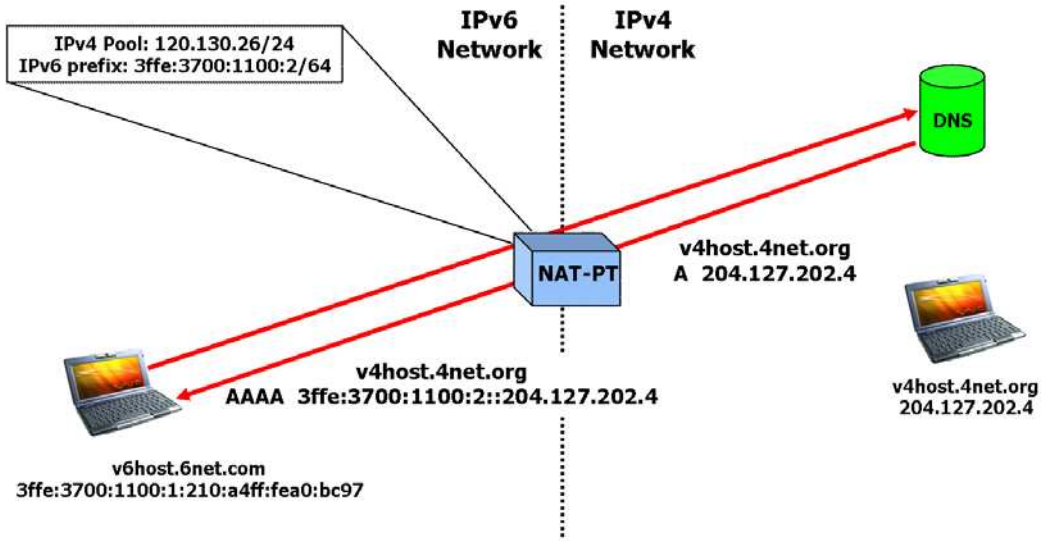


Figure 34 Translation Example

Annex B Phase 1 Detailed Planning

IPv6 Address Planning

Using the framework provided in Section 5 “IPv6 Address Space Requirements”, an address plan will be developed for the whole of the DIE.

Non-routable network Planning

Detailed planning for the DIE’s non-routable networks will consist of the following tasks:

- Determine ingress and egress points to the Non-Routable networks within the ADF DIE.
- Determine if interfaces can be specified with IP from those ingress and egress interfaces.
- Determine the data structures for those interfaces, and then a network proxy or gateway will have to be developed to support those input and output interfaces.
- Determine what semantics relative to the network are contained within those interfaces.
- If IPv4 is assumed in those interface semantics, then IPv4 should be used to input to this network.
- For an IPv6 Transition when a packet flows into or through a Non-Routable network the Transition should assume it should be presented an IPv4 packet, this implies potentially translating IPv6 to IPv4. This could have great cost and affect end-to-end interoperability for any IPv6 context and assumptions for security end-to-end.
- It would be best if possible to redefine the Non-Routable network interfaces to support IPv6 from the beginning if at all possible for the IPv6 Transition.

Interoperability Planning

Detailed planning to achieve the required interoperability will mostly be conducted by individual projects where they will need to perform a range of tasks including:

- Determine set of network applications[71] that must be ported / invented.
- Determine the geography the network applications must span.
- Identify Network components that must support IPv6.
- Identify Network components that require IPv6 Transition Mechanisms.
- Identify Network components that can be initiated with IPv6 using IPv4 as scarce resources only.

Determine the packets required over the DIE within the scope of the IPv6TP:

- Packets over a local link, a site, an intranet, an Internet and over a mobile IPv6 network.
- Packets from IPv6 Network thru IPv4 Cloud to IPv6 Network.
- Packets from IPv4 Network thru IPv6 Cloud to IPv4 Network.

Determine the points of network communications for the IPv6TP Node Types:

- Clients, Servers, Routers, Switches, Printers, Gateways, Firewalls, Proxies, and any network device or applications platform.
- Management Nodes (e.g. Network, Security, Mobility, QoS).
- Any Node supporting Transition Mechanisms.
- Public Key Infrastructure Nodes for Security.

Determine the points of network communications for the IPv6TP Software Components:

[71] In general it is expected that most applications within the DIE will need to migrate to IPv6, except for those completely stand-alone applications including those which do not connect to a LAN.

- Network Management and Utilities.
- Network Internet Infrastructure Applications.
- Network Systems Applications.
- Network End User Applications.
- Network High Availability Software.
- Network Security Software.

Costing

Once the above detailed planning is completed, each individual project should have a sufficient information and implementation level detail to complete the costing exercise for transitioning to IPv6.

ANNEX C Risk Log

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
1	IPv6 Work-shop (Grant Ranard)	DWACN	DWACN	The DIE ends-up without an overall end-to-end security architecture (there currently is no such end-to-end architecture)	6	7		Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Major: Because security is a key requirement for the DIE.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Provide budget for architectural work, undertake the work and manage the effort via governance and management structures.
2	IPv6 Worksh op (Group)	HAIPE	HAIPE	There may be insufficient quantities of HAIPE IPv4 IPv6 (combinations) encryptors made available to the ADO.	1	5	7	Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Major: Because security is a key requirement for the DIE.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Raise the level of importance of the issue by appropriate use of government to government channels.
3	IPv6 Worksh op (David Holmes)	All IPv6 affected	Accreditat ion	ISSA/DSD/DS A delay/deny IPv6 accreditation.	7	19		Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Major: Because security is a key requirement for the DIE.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Ensure that these security organisations are suitably staffed.
4	IPv6 Worksh op (Grant Ranard)	DIE	DIE	IPv6 policy implementation fails	7	19	3	Unknown/ TBD	Likelihood will be a function of either failing to provide sufficient penalties (sticks) and rewards (carrots)	Severe: Because it is possible that the ADO incurs an obsolescenc e problem and or an interoperabil ity (with allies) problem.	3	Possible	5	Severe	High	Risk must be treated as this risk has such wide-ranging impact.	Determine set of metrics to monitor during course of implementation . Use results to apply changes to policy to avoid failure.
5	IPv6 Worksh op (Group)	Major systems within the DIE	Major systems within the DIE	IPv4/6 products fail to match the need of the developed architecture.	6	9	7	Unknown/ TBD	Possible: Because the expectation if that most of the hardware and software will be COTS and the ADO does not have complete control over the commercial suppliers.	Severe: Because parts of the DIE cannot be implemente d at the required time causing loss of functionality and interoperabil ity.	3	Possible	5	Severe	High	Risk must be treated as this risk has such wide-ranging impact.	Ensure that architecture developers fully understand the COTS roadmaps and the probability of suppliers meetings those roadmaps. Develop flexible architectures that can cope with varying implementation s. Develop fall-back plans and investigate in-house solutions/patch es using software solutions.
6	IPv6 Worksh op (Group)	DIE	DIE	Schedule driven project delivery causes breakaway from the	7	19	20	Unknown/ TBD	Possible: Because the schedules of the CDG and DMO	Major: Because this may result in a loss of	3	Possible	4	Major	High	Risk must be treated as this risk has	Determine set of metrics to monitor during course of implementation

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
				planned IPv6 implementation					are subject to external forces that the ADO does not have complete control over.	functionality and or interoperabil ity within the DIE and between Allies.						such wide-ranging impact.	. Use results to apply changes to projects schedules to avoid breakaway.
7	IPv6 Worksh op (Group)	DIE	DIE	Failure to manage schedules of the interdependent IP systems	7	19	20	Unknown/ TBD	Possible: Because the schedules of the CDG and DMO are subject to external forces that the ADO does not have complete control over.	Major: Because this may result in a loss of functionality and or interoperabil ity within the DIE and between Allies.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Governance mechanisms (IPv6PO) are designed to ensure that inter-dependant projects schedules can be managed. Metrics should be put in place to determine the extent of failure as soon as possible, treatment strategies could include strengthening the Governance measures, increasing budget and man-power.
8	IPv6 Worksh op (Group)	DIE	DIE	Failure to manage technical standards between interdependent IP systems	7	19		Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Major: Because this may result in a loss of functionality and or interoperabil ity within the DIE and between Allies.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Governance mechanisms (IPv6TO) are designed to ensure that technical standards between interdependent projects can be managed. A technical audit process should be put in place to determine the extent of non-compliance (standards failure) as soon as possible. Treatment strategies could include strengthening the Governance measures, increasing budget and man-power or determining the lowest cost method of re-aligning the standards.
9	IPv6 Worksh op (Group)	DIE	DIE	Don't capture future IPv6 address space	9	6	7	Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Moderate: Because the result may mean the ADO ends up with a non-	3	Possible	3	Moderate	Medium	Risk must be treated as this risk has such wide-	The IPv6 address plan should be regularly revisited to determine trends well

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
										contiguous address space and this affect routing performance.						ranging impact.	ahead of time, so that solutions can be trailed on the IPv6 test-bed.
10	IPv6 Worksh op (Group)	DIE	DIE	Don't have skills/competen cies to manage IPv6 transition	7	19	20	Unknown/ TBD	Possible: Many of these skills will need to be supplied by organisation s external to the ADO.	Major: Because this may result in a loss of functionality and or interoperabil ity within the DIE and between Allies.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Fund training of individuals to gain these skills. Co-operate with Allied (and other) agencies and embark upon a secondment program. Slow down the transition schedule to meet the reduced resourcing/skill level.
11	IPv6 Worksh op (Group)	DIE	DIE	IPv6 Transition Office not adequately resourced	7	19	20	Unknown/ TBD	Possible: Because of funding restrictions or the inability to find these skills external to the ADO.	Major: Because this may result in a loss of functionality and or interoperabil ity within the DIE and between Allies.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	Increase funding and increase resourcing. Slow down the transition schedule to meet the reduced resourcing level.
12	IPv6 Worksh op (Group)	DIE	DIE	Fractured / poorly co-ord engineering processes and environments, e.g. test beds	7	19	20	Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Moderate: Because the test beds may not produce desired results for the planning process.	3	Possible	3	Moderate	Medium	Risk must be treated as this risk has such wide-ranging impact.	Governance mechanisms (IPv6TO) are designed to ensure that adequate engineering processes (inc test-bed environment) are created. A technical audit process (and evaluation process) should be put in place to determine the effectiveness of the developed processes. Treatment strategies could include strengthening the Governance measures, changing the processes, increasing budget and man-power.
13	IPv6 Worksh op (Group)	Affected DIE Applicatio ns	Affected DIE Applicatio ns	Cost of migrating the applications is significantly greater than planned.	7	6	13	Unknown/ TBD	Possible: Because there are many applications within the DIE (not all	Major: Because may cause loss of funding for other parts of the	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-	Increase funding. Delay migration of some non-critical applications (those not

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
									COTS) and the estimation process necessarily will have a degree of error.	transition.						ranging impact.	affecting interoperability) that can be isolated in enclaves of IPv4 for longer than planned. This delay could be permanent for the most expensive (to transition) applications.
14	IPv6 Worksh op (Group)	DIE	DIE	Independent (esp wrt to funding) stakeholder organisations don't comply with IPv6 policy/plan	7	19		Unknown/ TBD	Possible: If the treatment strategies are not followed or fail.	Major: Because this may result in a loss of functionality and or interoperabil ity within the DIE and between Allies.	3	Possible	4	Major	High	Risk must be treated as this risk has such wide-ranging impact.	It is assumed that all required ADO organisations will follow the IPv6 plan and the governance measures have been designed to achieve this goal. The governance measures will be weakest however for external organisations (e.g. Allies). The ADO should therefore extend its Communication s/Education program as far as possible to bring those stake-holders into the fold. Alternatively, measures (and fall-back plans) may need to be considered to alter the ADO plan.
15	IPv6 Worksh op (Group)	External DIE interfaces	External DIE interfaces	IP services into external orgs may need to be maintained at IPv4	6	11		Unknown/ TBD	Likely: Because we know that there are subject organisation s who have not progressed very far down the IPv6 transition path.	Moderate: Because this will increase costs for the ADO and extend the transition period.	4	Likely	3	Moderate	Medium	Risk must be treated as this risk has such wide-ranging impact.	Although it is fully expected that some IP services will remain IPv4 for a long time into the future, there may be some which it is very desirable/nece ssary to switch to IPv6. The ADO could assist these organisations to make the transition more quickly by providing technical/mana gerial support, training and even funds.

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
16	IPv6 Worksh op (Group)	DIE	DIE	IPv6 plan not responsive to speed of development of COTS	7	6	19	Unknown/ TBD	Possible: Because commercial pace of change is significantly faster than the non-commercial pace, this is just a plan and it cannot be perfect.	Moderate: Because this may create a lost opportunity for the ADO.	3	Possible	3	Moderate	Medium	Treat: Because it is better not to incur a lost opportuni ty.	Alter the plan as required to meet the actual pace of COTS development, this would be verified by testing products on the IPv6 test-bed.
17	IPv6 Worksh op (Group)	DIE	DIE	Having an adequate range of IPv6 products on the approved products list (APL)	7	6	19	Unknown/ TBD	Rare: Because we know there are already IPv6 products in the market place, the only restriction is to go through the ADO processes to get them on the APL.	Minor: Because it is assumed that there will be other products on the APL that can do the job, the only impact is that you may not end up with the optimum implementati on.	1	Rare	2	Minor	Low	Accept: This is a nice to have only.	None required.
18	IPv6 Worksh op (Group)	DIE	DIE	Risk management context not defined.	7	19		Unknown/ TBD	Rare: Because this is easily solved and largely an ADO managemen t issue.	Minor: Because the effect should only generate less finely tuned or out-of-scope risks.	1	Rare	2	Minor	Low	Treat: Because effort (cost/sch edule) could be wasted treating non-risks.	Undertake during the early part of the detailed-planning phase, a study to determine this context in detail.
19	IPv6 Worksh op (Group)	DIE	DIE	ISB don't have a rigorous enough process to detect IPv6 enabled equipment that is connected to the network and may cause problems.	7	6	19	Unknown/ TBD	Rare: Because we know this is technically possible and solvable so this is largely a managemen t issue.	Moderate: Because the effect could compromise security or cause network performance problems	1	Rare	3	Moderate	Low	Treat: Because this should be straight forward to achieve.	Using the resources of the IPv6TO to trial a better process on the IPv6 test bed and work with ISB to improve the situation.
20	IPv6 Panel (John Penning ton)	Affected DIE Application s	Affected DIE Applicatio ns	Application transition turns out to be more difficult than expected	7	6	18	Unknown/ TBD	Possible: Because the work to evaluate applications for transition is TBC and we know that there are non COTS applications that could be expensive to transition.	Moderate: Would increase costs and may affect budget for other areas of the transition.	3	Possible	3	Moderate	Medium	Treat: Because cost and schedule may be involved.	Assuming that the budget and schedule is soaked up in transitioning less applications, the solution may be to accept that more applications live on in IPv4 for longer. Alternatively more budget is sought to transition the remaining applications and or a more rigorous process is undertaken to either finds ways that the applications

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
																	can be removed from service or replaced by other processes or applications.
21	IPv6 Panel (John Penning ton)	DIE	DIE	Tactical comms equipment is not available to support IPv6 in target timescale	14	6	20	Unknown/ TBD	Likely: Because we know that JP2072 is still in the early stages of developmen t and the JTRS program is in delay.	Major: Because will need to maintain IPv4 for operational systems and will lose advantages of IPv6.	4	Likely	4	Major	High	Treat: Because the tactical space is crucial to the ADO ability to carry out operation s.	Either increase funding to pull-forward tactical equipment availability, or find an interim capability that can be delivered earlier, or support legacy systems for longer.
22	IPv6 Panel (John Penning ton)	DIE	DIE	Network design needs nested tunnels (e.g. for cryptos, routing encapsulation) but MTU limits are breached	6	18	11	Unknown/ TBD	Possible: Because this is a technical issue and the solution is TBD.	Minor: Because some network connections fail, or expensive work-arounds needed.	3	Possible	2	Minor	Medium	Accept: Because work-around is acceptabl e.	Redesign the network to avoid this situation. There may be some network equipment where the IP layer is implemented in software and the manufacturer "may" be able to provide a work-around, however this is not recommended.
23	IPv6 Panel (John Penning ton)	DIE	DIE	Evaluated firewall, CND and crypto products for IPv6 not available in time	6	14	18	Unknown/ TBD	Possible: Because security products tend to take longer to be made available than general purpose commercial COTS infrastructur e.	Moderate: Because target dates not met, cost to reschedule projects	3	Possible	3	Moderate	Medium	Treat: Because of cost and schedule impacts.	Apply more resources to the accreditation process if this is the bottleneck. Otherwise if this is a COTS availability problem then either delay the role out or consider finding ways to assist with the suppliers meeting the ADO's need.
24	IPv6 Panel (John Penning ton)	DIE	DIE	PKI solution not available to support IPsec, either in ADO, or to allies	6	14		Unknown/ TBD	Possible: Because commercial security products not under complete control of ADO.	Minor: Because greater security capability not available.	3	Possible	2	Minor	Medium	Accept: Because security products are already in place.	None required.

#	Risk Author	Affected Compon-ents or Systems	Compon-ent or System Descrip-tion	Description of Risk	Sources of Risk		Evaluation of Existing Controls		Likelihood of Risk	Conseq-uences of the Risk	#	Likelihood Rating Value	#	Conse-quence Rating Value	Overall Rating (from DoD matrix)	Accept or Treat Risk? (with reasons why)	Treatment Strategies
25	IPv6 Panel (John Penning ton)	DIE	DIE	Windows Active directory does not migrate to IPv6 in time	1	6	14	Unknown/ TBD	Possible: Because commercial products not under complete control of ADO.	Severe: Because the DIE transition must be delayed	2	Unlikely	5	Severe	High	Treat.	If the ADO uses Microsoft Active Directory (AD) widely then a delayed IPv6 transition will have to be accepted, except for specific systems where it is essential (Allies) however the application gateway approach may be a less cost lower risk solution. If the use of AD is not widespread then these systems could be enclaved and maintained as IPv4 until Microsoft delivers support.
26	IPv6 Panel	Affected DIE hardware	Affected DIE hardware	Cost of migrating the hardware is significantly greater than planned.	14	13	6	Unknown/ TBD	Rare: Because it is expected that only general purpose (e.g. printers etc) peripherals will be affected.	Insignificant: Because the solution is to continue to support IPv4 in the DIE and this is planned for some time.	1	Rare	1	Insignific ant	Low	Accept: Because the work-around has already been identified in the plan.	None required.

Source of Risk		
0		
1	Commercial and legal relationships	Between the organization and other organizations, e.g. suppliers, subcontractors, lessees.
2	Economic circumstances	Of the organization, country, internationally, as well as factors contributing to those circumstances e.g. exchange rates.
3	Human behaviour	Of both those involved and those not involved in the organization.
4	Natural events	
5	Political circumstances	Including legislative changes and factors which may influence other sources of risk.
6	Technology and technical issues	Both internal and external to the organization.
7	Management activities and controls	
8	Individual activities	
9	Materiel System requirements	Materiel System requirements, as defined in the OCD and FPS (noting that inadequate requirements are identified as the No 1 cause for project failure);
10	Operating environment	Operating environment (i.e. how similar is the operating environment for which equipment was designed with the envisaged operating environment?);
11	Interfaces	
12	Software development and management	Software development and management, including software support;
13	Degree of development required for the system	
14	Maturity of technology required	
15	Specialty engineering areas	Specialty engineering areas, such as growth and obsolescence, safety, security, electromagnetic environmental effects, human factors, and radio-frequency spectrum management;
16	Government Furnished Material	Government Furnished Material (GFM), which includes Government Furnished Equipment (GFE), Government Furnished Data (GFD) (i.e. warranted data), and Government Furnished Information (GFI);
17	Integrated Logistic Support	Integrated Logistic Support (ILS) issues, including: Support System requirements, support contract requirements, linkages between the acquisition and support contracts, and costing and resourcing the envisaged support arrangements;
18	Transition from an existing Materiel System	Transition, particularly the transition from an existing Materiel System (or part thereof) to a new Materiel System (while maintaining capability);
19	ADO project offices	ADO project offices, particularly with respect to the right balance of personnel numbers, skills and experience; and
20	Defence contractors	Defence contractors, particularly with respect to capability to undertake the required work (i.e. process maturity and the right balance of personnel numbers, skills and experience).

ANNEX D DCP Project Summary

Project Number	Title	Relevance
DEF 7013	Joint Intelligence Support System (JISS)	Further development of the JISS for support of the Australian Defence intelligence community.
AIR 5276 Ph 6	Data links for AP3-C Orion aircraft.	Upgrade aircraft communications suite and data links. Note: Currently use Link-11.
AIR 6000	Joint Strike Fighter (JSF).	Comms/Radios will come as part of this platform acquisition
AIR 7000	Multi-mission Maritime Aircraft (MMA). AP3-C replacement.	Comms/Radios will come as part of this platform acquisition
AIR 9000	Helicopters.	Comms/Radios will come as part of this platform acquisition.
JP 2008	Military Satellite Communications	Expanded capability including use of Optus/Singtel C1 satellite.
JP 2030	Joint Command Support Environment	Consolidating existing Command Support Systems into a single environment.
JP 2047	Defence Wide-Area Communications Network	Multi-phase project with ISDs between 2005 and 2014. Providing enhanced encryption services, enhanced protocols transmission and switching equipment and providing guidance of on-going development.
JP 2068[72]	DNOC –Defence Network Management System and Computer Network Defence	Improving management, monitoring, security and visibility of the DIE.
JP 2069	High Grade Cryptographic Equipment (HGCE).	Replacement HGCE.
JP 2072	Battlespace Communications System (Land)	Replacing the Army's CNR and Tactical Trunk Communications with an advanced communications system.
JP 2089	Tactical Information Exchange Domain (TIED) (Data Links)	Delivering Link-16 and VMF on Ships and Planes/Helicopters and associated land-based platforms.
JP 2090	Combined Information Environment	Establish permanent "information" connectivity between ADF and key Allied Command and Control networks and systems to support future Coalition operations.
LAND 75	Battlefield Communications Support System (BCSS)	Role out of BCSS below Brigade level.
LAND 125	Soldier Combat System	Acquire advanced capabilities for the combat soldier.

[72] It was advised during the IPv6 Workshop that Phase 2A of JP2068 has been cancelled and that JP2047 will provide NMS functionality enhancements.

SEA 1442	Maritime Communications and Information Management Architecture Modernisation	Introduction of Maritime Tactical Wide Area Network and IP Networking to a range of RAN vessels.
SEA 4000	Airwarfare Destroyer	Comms/Radios will come as part of this platform acquisition

ANNEX E IPv4

IPv4 Address Space Exhaustion

One of the potential consequences of failing to transition from IPv4 to IPv6 may be the exhaustion of IPv4 addresses. Figure 15 plots the allocation of IPv4 addresses against time and shows that prior to 1995 addresses were being allocated at a steep linear rate, these were mostly Class B[73] allocations. Since 1995 a CIDR methodology has been used to allocate addresses and Figure 27 also plots a prediction (green line out to 2015) of address allocation using an exponential model starting in 1995.
Using this exponential model the pool of un-allocated IPv4 address will be exhausted by February 2014[74].

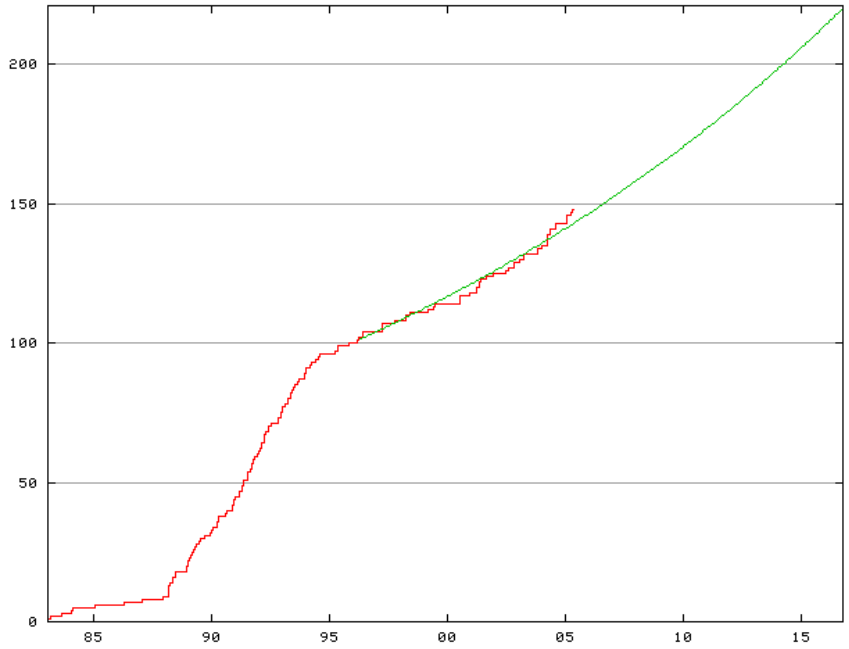


Figure 35 IPv4 IANA Allocations - Projection using Exponential Growth Model[75]

It should be noted that the above does not necessarily relate to the IPv4 address usage within the ADO.

[73] A Class B address range will support up to 65,534 Hosts.
[74] Source http://bgp.potaroo.net/ipv4/ , this chart is automatically updated each day.
[75] Source http://bgp.potaroo.net/ipv4/ , this chart is automatically updated each day.

ANNEX F CIOG Organsational Chart

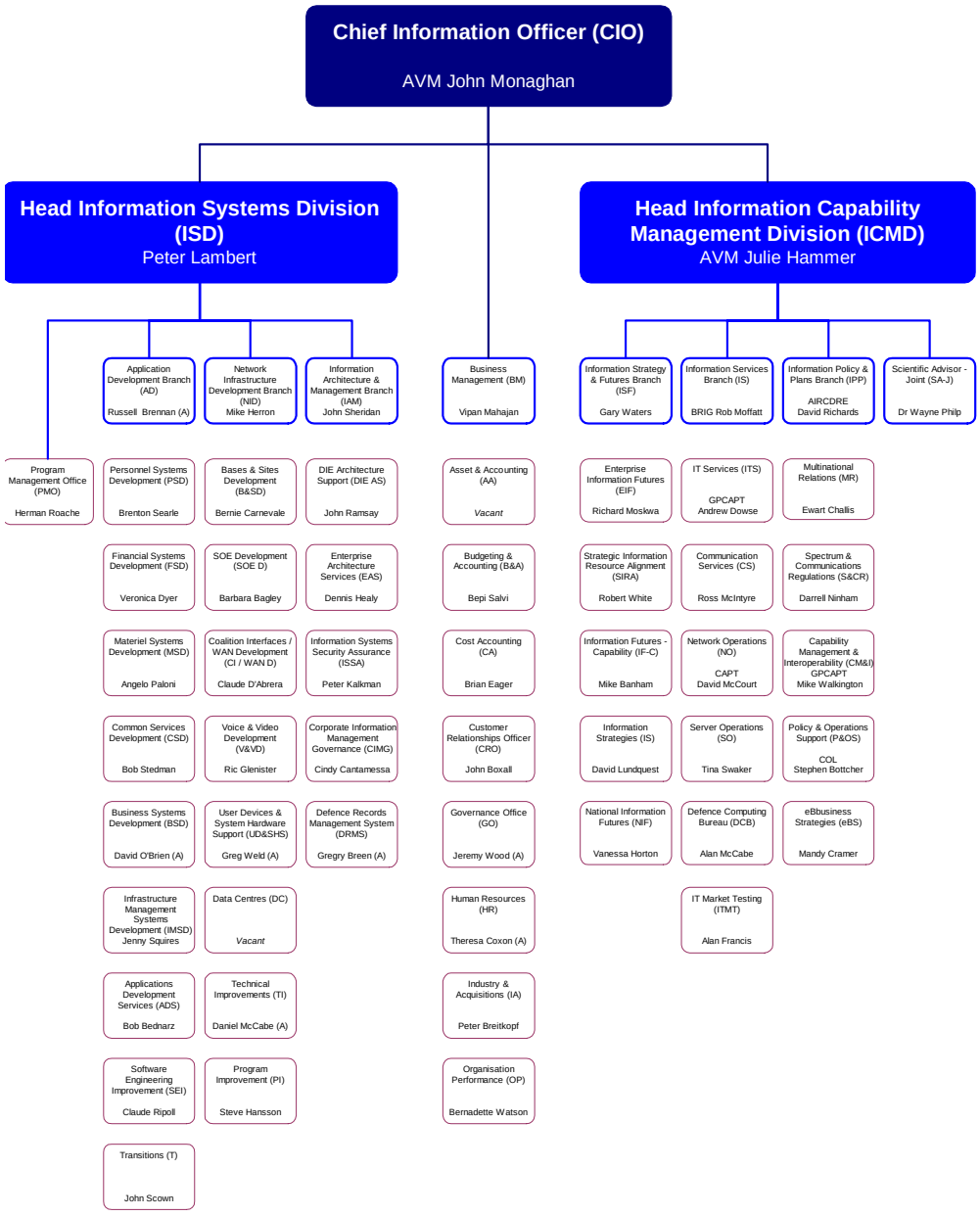


Figure 36 CIOG Organisational Structure

ANNEX G Mobile IP

Mobility in IPv6

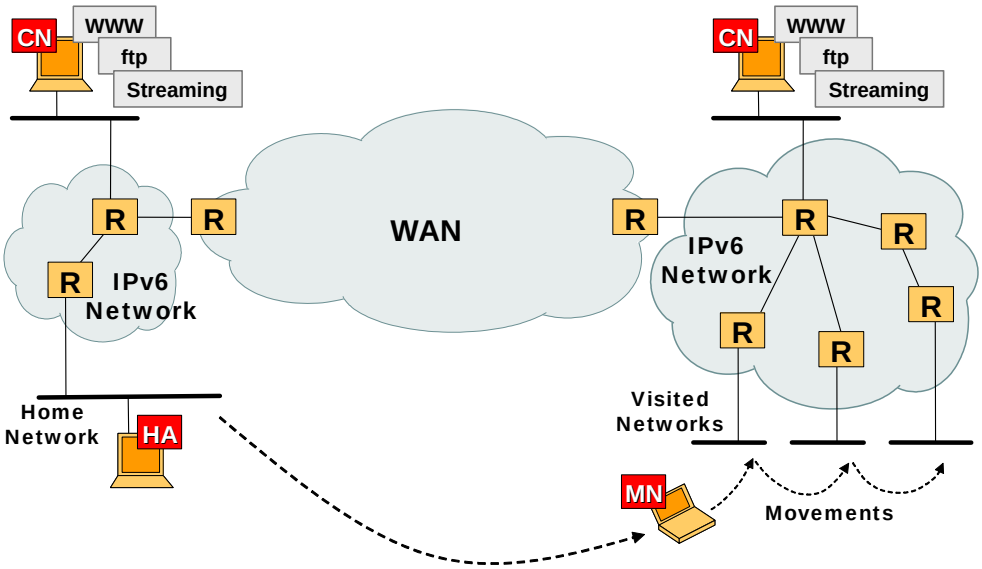


Figure 37 Edge Mobility

Mobile IPv6 is designed to support individual roaming mobile hosts. The aim of MIPv6 is to maintain reach-ability to a node as it moves to various points in a network. The mobile node can be reached via a constant “home address” when it is on a different network. Active sessions can be maintained as the node moves from one network to another.

Mobile IPv6 has three main components: the mobile node (MN), the home agent (HA), and the correspondent node (CN). The way Mobile IPv6 works is as follows. The mobile node registers with a specific home agent. When the MN moves to a new network (presumably by connecting to some sort of access point), it must detect that it has moved to a new network, and obtain a new IP address. While a new address can be obtained via DHCPv6 after being triggered by some sort of movement detection process, the more common method uses router advertisements (RADV) to detect movement and automatically assign a new address using stateless auto-configuration. Once this new address is obtained, the mobile node sends a binding update (BU) to the HA and any correspondent nodes it is currently communicating with, notifying them of its new care-of address (CoA).

There are two possible modes of communication between the mobile node and a correspondent node. The first mode, bi-directional tunnelling, does not require MIPv6 support at the correspondent node. In this mode, the home agent intercepts all packets destined for the MN using proxy neighbour discovery, and tunnels them to the MN. Packets that the MN sends to the CN are also tunnelled back through the home agent. The second mode of communication, route optimisation, requires the correspondent node to have Mobile IPv6 functionality. This process starts out the same as the bi-directional tunnelling mode, with the HA intercepting packets destined for the MN, and tunnelling them to the MN’s Care-of Address (CoA). With route optimisation, the MN then informs the CN about its CoA, and the CN and MN can then communicate directly, without the aid of the HA. As long as a session is active, the MN needs to send a binding update (BU) to the CN when it moves to a new network, so that they may continue direct communications.

General MIPv6 Benefits

Here are the primary similarities and differences between MIPv6 and MIPv4:

- ***Foreign agent.*** Both standards rely on a home agent and a mobile node, but MIPv6 does not define a foreign agent to issue a care-of address (CoA), since routable address constraints are not an issue in IPv6 networks. Instead, MIPv6 derives the CoA directly from auto-configuration schemes. This approach enables the mobile node to operate in any location without requiring special support from the local router.
- ***Route optimisation.*** MIPv6 enables direct-packet routing between the mobile node and corresponding nodes located on an IPv6 network. When the mobile node moves into a foreign network, it obtains a new CoA and reports this to its home agent. The home agent intercepts all packets destined for the mobile node and tunnels them to its registered CoA. In a MIPv4 scenario, a corresponding node's traffic must pass through the home agent, but MIPv6 route optimisation allows the mobile node to send binding updates to an IPv6-based corresponding node. The corresponding node caches the current CoA and then sends packets directly to the mobile node. This is an optional procedure for MIPv4 that requires special options to be enabled on each corresponding node, and is rarely implemented or used.
- ***Security.*** MIPv4 and MIPv6 will often be used with a VPN (virtual private network) solution for data security when the user is roaming into networks outside the corporate firewall. Both protocols will in theory allow the use of a v4 IPsec (Internet protocol security) VPN solution, providing in the case of the MIPv6 client that the IPv6 protocol stack includes a 6-to-4 function. In addition, the MIPv6 client allows the use of a v6 IPsec VPN solution.
- ***Home agent address discovery.*** Using the IPv6 anycast feature, the mobile node can send a binding update to the home agent anycast address. The mobile node will get only one response from one home agent even if several are present on the network. This is an efficient way of keeping track of multiple home agents, which may be required in many networks for redundancy or scalability.

MIPv6 status

MIPv6 has mature IETF standards-track specifications for its core functionality, as well as for the added ability to use IP Security (IPSec) to encrypt signalling between the MN and the HA. There are a few reasonably mature MIPv6 implementations available covering the Linux, BSD, CISCO IOS, and Windows operating systems, as well as simulation environments.
There is still significant evolving research being done in the area of MIPv6. Emerging enhancements and modifications, such as Hierarchical MIPv6 (HMIPv6) may help improve the performance and scalability of the protocol.

General MIPv6 Issues

MIPv6 is only necessary for mobile end systems which require a stable IP address for identification or to maintain in-progress sessions while roaming between networks. If these conditions need not be met, and it is acceptable to obtain a new address and restart current sessions, then the combination of DHCP and dynamic DNS, as one possible example, may be sufficient to meet mobility criteria, and MIPv6 maybe unnecessary.

The main MIPv6 specification includes a mechanism for Dynamic Home Agent Address Discovery (DHAAD), which can be used for avoiding a manual configuration of the Mobile Node with the Home Agent's address. However, the current mechanism that allows a Mobile Node to detect the prefix of its home network when attached to a visited network, requires additional operational administration. This must currently be done manually, though there is work underway to address this aspect in an automatic way using the Authentication, Authorization, and Accounting (AAA) infrastructure, and new methods to identify new link prefixes from work on Detecting Network Attachment (DNA) which is work in progress.

If tunnelling is used between the MIPv6 Home Agent and Correspondent the standard tunnelling overhead for any protocol will exist, but this can be avoided using the MIPv6 route optimisation. Additionally, fast handoff of a mobile node has significant limitations due to the required local interface protocol standards.

Network Mobility

Network Mobility (NEMO) is essentially an extension to Mobile IPv6. NEMO is designed to apply to entire networks in motion, rather than just individual nodes in motion. It is still an area of work in progress within the IETF.