Australian Government
Department of Defence
Chief Information Officer Group

Paul Pappas
Director – Infrastructure Design
Chief Information Officer Group

IPv6 Summit 2007

Status of IPv6 in Department of Defence Planning

Background

- 2004
  - Initial planning
- 2005
  - Released transition policy – DIMPI 1/2005
  - Developed *"IPv6 Transition Plan"*
- 2006
  - Defence Science and Technology Organisation (DSTO) review and recommendations of "*IPv6 Transition Plan*"
  - DSTO report *"Determining an IPv6 Address Allocation"*
  - Defence Materiel Organisation approved the establishment of TIPSTEEL

Defence IPv6 Policy

- Mandated transition to IPv6 by 2013

Department of Defence
DEFENCE INFORMATION MANAGEMENT POLICY INSTRUCTION NO 1/2005
22 February 2005

DEFENCE INFORMATION ENVIRONMENT—TRANSITION TO INTERNET PROTOCOL VERSION 6 (IPv6)

Policy
1. The Defence Information Environment (DIE) will transition from the current Internet Protocol (IP) version 4 (IPv4) to IPv6 and all DIE networks are to have completed transition to IPv6 by the end of 2013. All capability management, development and acquisition staff are to address DIE IPv6 interoperability requirements when developing their architecture in accordance with the Defence Architecture Framework and when implementing associated projects.

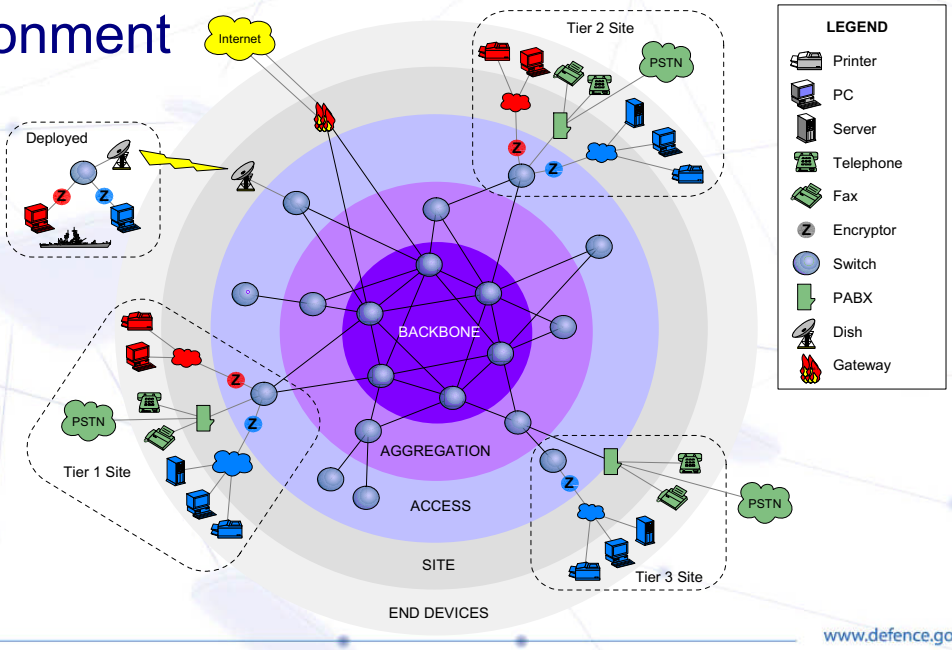
Why Does Defence need to Transition to IPv6?

- Continued interoperability with key Allies
  - US Department of Defense will transition in 2008
  - UK Ministry of Defence transitioning by 2012-14
- Network Centric Warfare
  - Proliferation of networks in the battle space
  - Rapidly increasing number of nodes over next 15 years
  - Increased need for network address space
- Pool of IPv4 address space rapidly depleting
  - Recent studies estimate 2010-2013
  - IPv6 is required to ensure the Defence Information Environment will meet the needs of its users into the future

Why 2013?

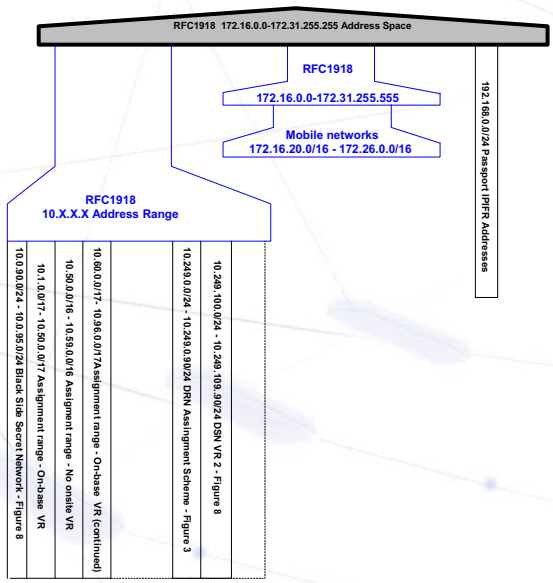
- There is no absolute reason to complete the transition earlier
- 2013 is a target date derived by balancing transition risks
  - Leverage the experience of our Allies
  - Technology and standards still evolving
  - Industry support
  - Defence's acknowledged immaturity in IPv6
- Refresh and replacement cycles

Current State of the Defence Information Environment



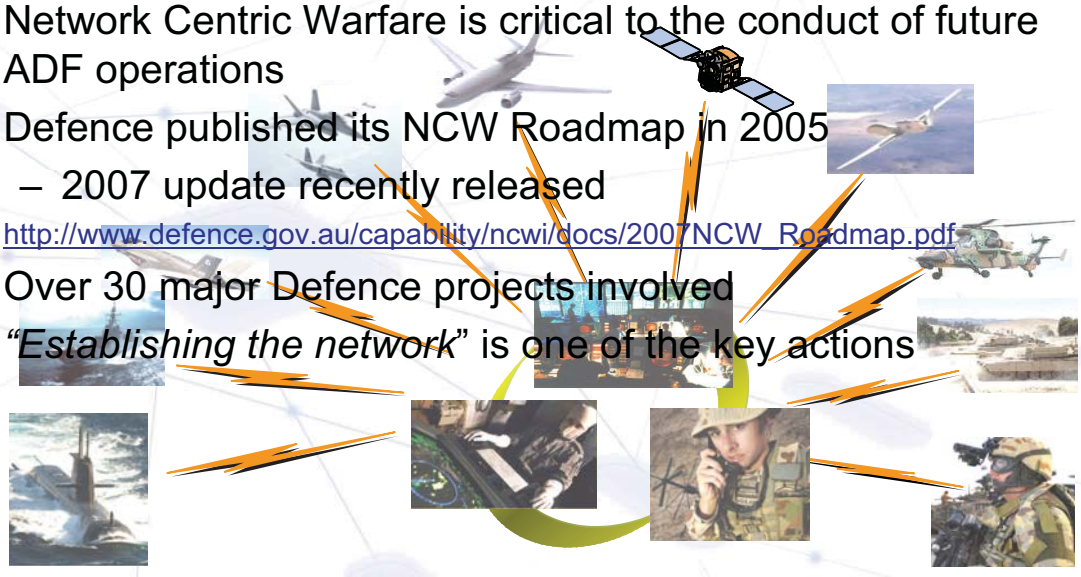
Defence IPv4 Address Architecture

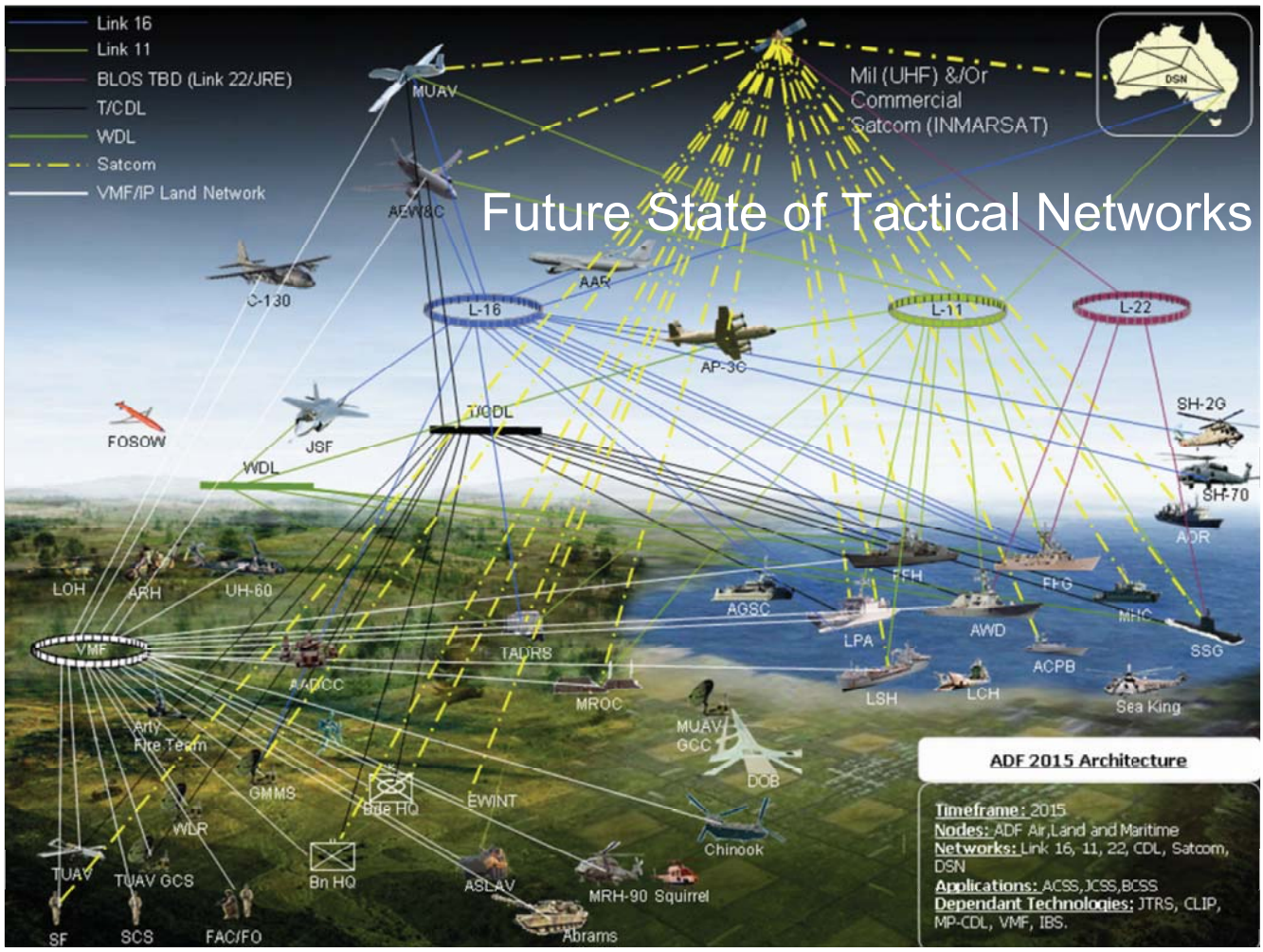
- Hierarchical structure
  - Backbone
  - Aggregation nodes
  - Access nodes
  - Sites
- Separate address range for deployed networks
- Uses private address range
  - Based on RFC1918
- Only publicly visible addresses are at Defence gateways



Network Centric Warfare

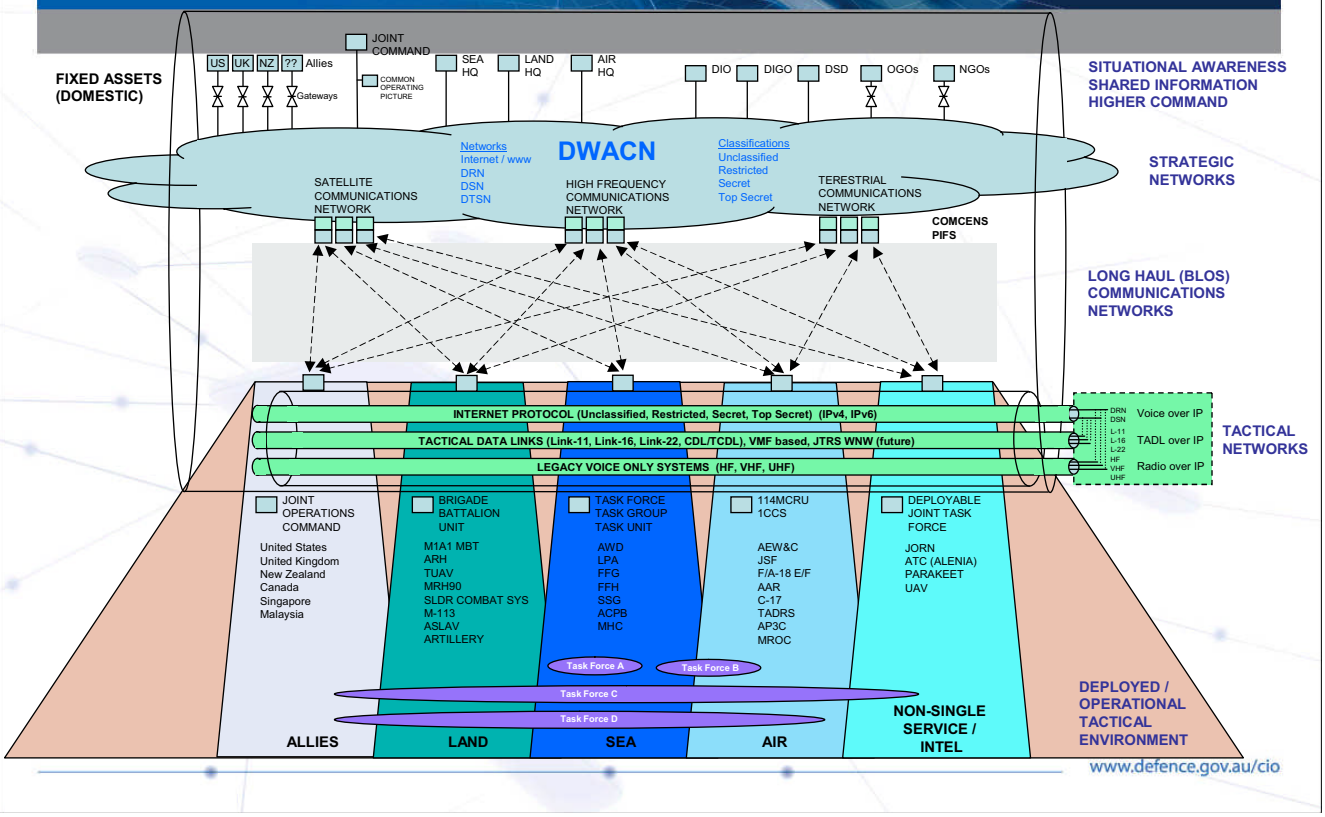
- Network Centric Warfare is critical to the conduct of future ADF operations
- Defence published its NCW Roadmap in 2005
  - 2007 update recently released
- http://www.defence.gov.au/capability/ncwi/docs/2007NCW_Roadmap.pdf
- Over 30 major Defence projects involved
- "*Establishing the network*" is one of the key actions





Australian Government
Department of Defence
Chief Information Officer Group

Future State of the DIE



Challenges for Network Designers in Defence

- Proliferation of wireless non-IP networks
- Proliferation of tactical terrestrial IP networks
- Proliferation of wireless IP networks
- All need to be seamlessly integrated
- Will require major architectural redesign of the DIE

Progress on IPv6 to date

- IPv6 address space
- Defence Science and Technology Organisation
- Other Government agencies
- TIPSTEEL

Defence's IPv6 Address Space

- *"IPv6 Transition Plan"* estimated Defence would require between /24 and /18 address space over the next 15 years
- DSTO report *"Determining an IPv6 Address Allocation"* refined this to /20 address space
  - Tactical networks require hierarchical addressing
  - Very different address allocation to conventional networks
  - Host Density ratio not applicable for determining routing space
- Defence applied to APNIC for /20 contiguous address block
- In July 2007, APNIC approved Defence's application and assigned the IPv6 address allocation of 2401:60000::/20

Defence IPv6 Activities

- Defence Science and Technology Organisation (DSTO)
  - IPv6 Point of Presence on the Internet backbone
- http://vk6hgr.echidna.id.au/cgi-bin/traceroute6?t=2001%3A4418%3A101%3A101%3A%3A101
  - Research and Development testing of IPv6 capable hosts
  - IPv6 Mobility support
  - Annex Ensemble – mobile IPv6 edge devices using 802.11i

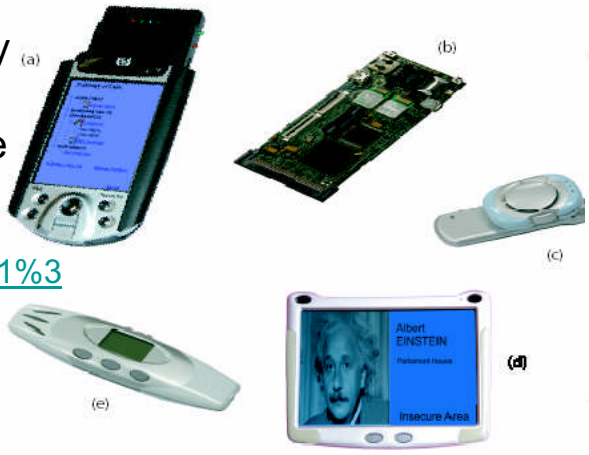


Figure 2. The first generation Annex Ensemble devices are: (a) MiniSec, which incorporates a (b) Secure Multi-function Card; (c) Button; (d) Badge; and (e) Codestick.

Defence IPv6 Activities (Cont)

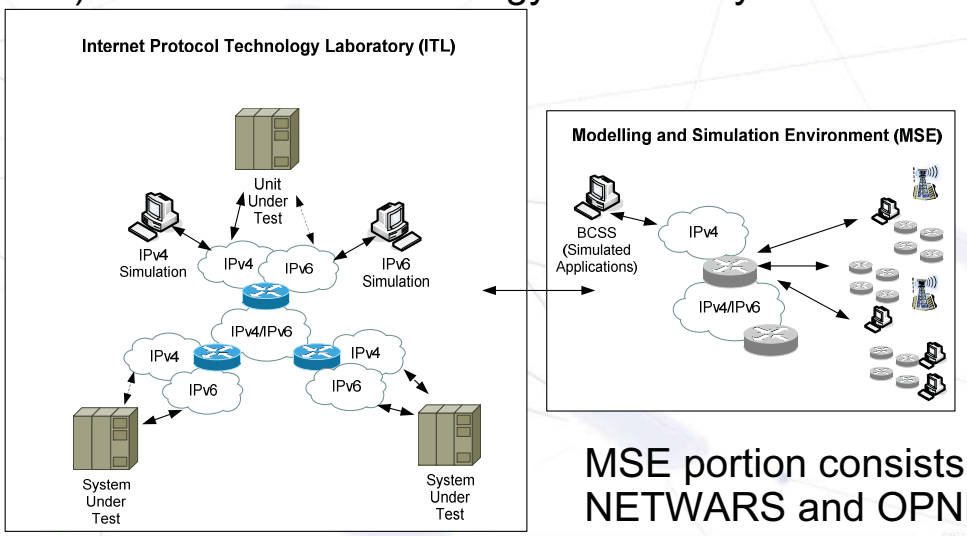
- Australian Government Information Management Office (AGIMO)
  - Considering Australia's whole-of-government transition to IPv6
  - Defence is a member of AGIMO's IPv6 Reference Group

TIPSTEEL

- *T*IEIO *IP S*imulation *T*est *E*xperimentation and *E*valuation *L*aboratory
- Established in 2006 within Tactical Information Exchange Integration Office (TIEIO) of Electronic and Weapon Systems Division in the Defence Materiel Organisation
  - Became operational in January 2007
- Purpose:
  - Support Defence's transition from IPv4 to IPv6
  - IPv6 compliance and interoperability testing platform
  - Support to major Defence projects
  - Open house testing for Industry and Defence

TIPSTEEL Logical Architecture

- ITL based on the US DoD Joint Interoperability Test Command (JITC) Advanced IP Technology Laboratory



MSE portion consists of NETWARS and OPNET modelling and simulation tools

TIPSTEEL Network Hardware

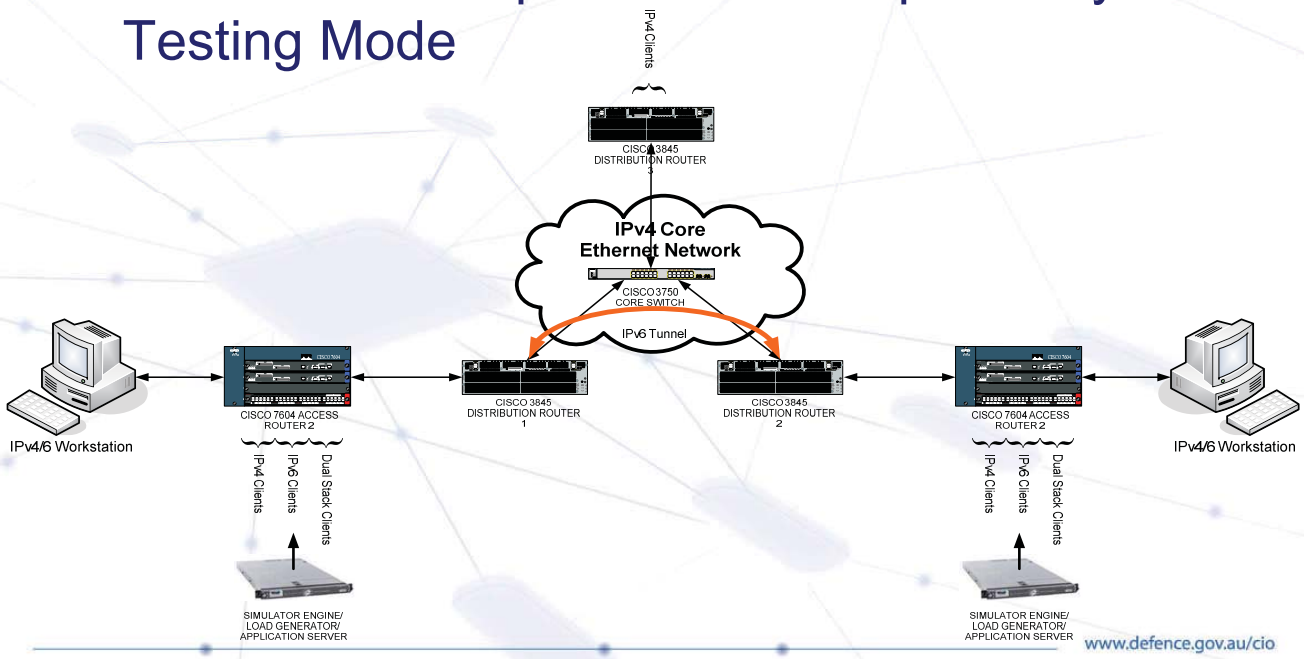
- Cisco 7604 Router
  - Provider router focus
  - 320Gbps switch fabric
  - 10/100, Gigabit Ethernet and 10 Gigabit Ethernet interfaces
- Cisco 3845 Integrated Services Router
  - Intelligent edge router
  - On board GigE plus 4 10/100 FE switch plus 4 Serial
- Cisco 3750G-24PS
  - Stackable Layer 3 switch
  - 24 x 10/100/1000 with POE and Layer 3 feature set

TIPSTEEL Case Study

- Network topologies:

Number	Source	TIPSTEEL	Destination	Comment
1	IPv4	IPv4	IPv4	Baseline IPv4 Native
2	IPv4	IPv6	IPv4	IPv4 tunnelled through IPv6
3	IPv4	IPv6	IPv6	IPv4 to IPv6 conversion
4	IPv6	IPv4	IPv6	IPv6 tunnelled through IPv4
5	IPv6	IPv6	IPv4	IPv6 to IPv4 conversion
6	IPv6	IPv6	IPv6	Future end state: Native IPv6 network

TIPSTEEL Compliance & Interoperability Testing Mode



Test and Evaluation Approach

- Phase 1 - Compliance and Interoperability testing:
  - Data; Voice; Video;
  - Data+voice; Data+voice+video
- Mobile node transfer of data, voice and video mixed traffic
- Measures of performance:

	Throughput	Latency	Jitter	Packet loss	Packet reordering	Transfer rate	Roundtrip delay
Data	✓					✓	✓
Voice	✓	✓	✓	✓	✓	✓	
Video	✓	✓	✓	✓	✓	✓	

IPv6 Challenges

- The migration from IPv4 to IPv6 is a significant undertaking
  - Will extend across the entire DIE
  - Standards and products still evolving
  - The DIE will have both v4 and v6 for many years
  - Software migration potentially more challenging than network migration
    - Legacy systems may be difficult to upgrade
- Security threats and vulnerabilities will change
- Also need to maintain interoperability with Australian Government agencies and industry

Conclusion

- IPv6 will be a key enabler for the Australian Defence Forces' Network Centric Warfare aspirations
- Defence is progressing towards IPv6 transition
- Ongoing research and testing is increasing Defence's knowledge of IPv6
- Many challenges still to be faced

Questions?