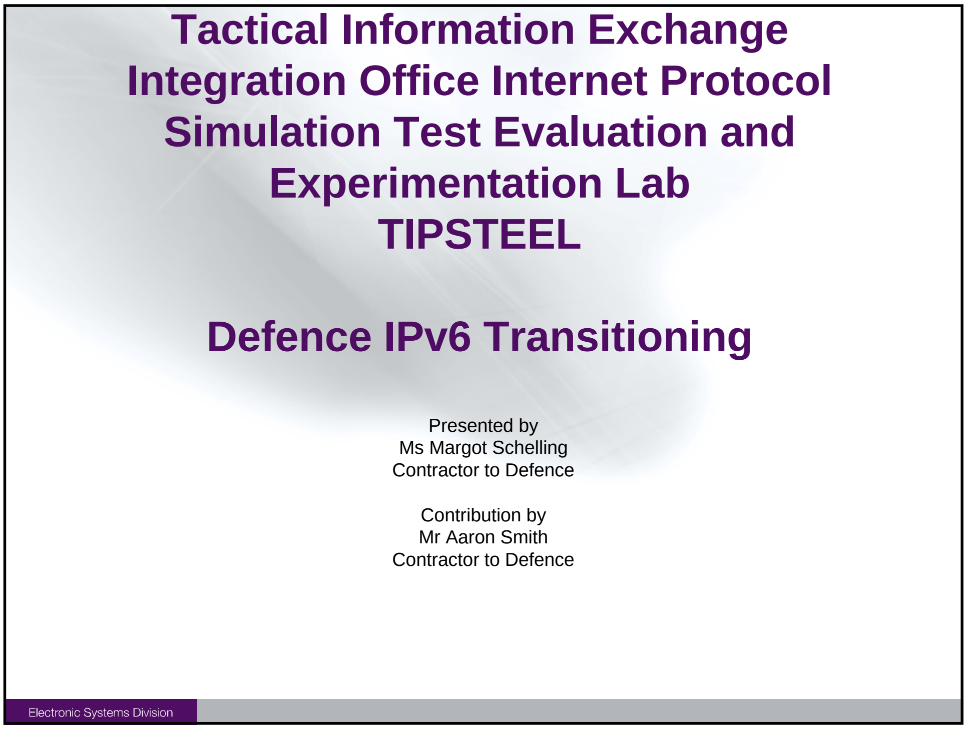
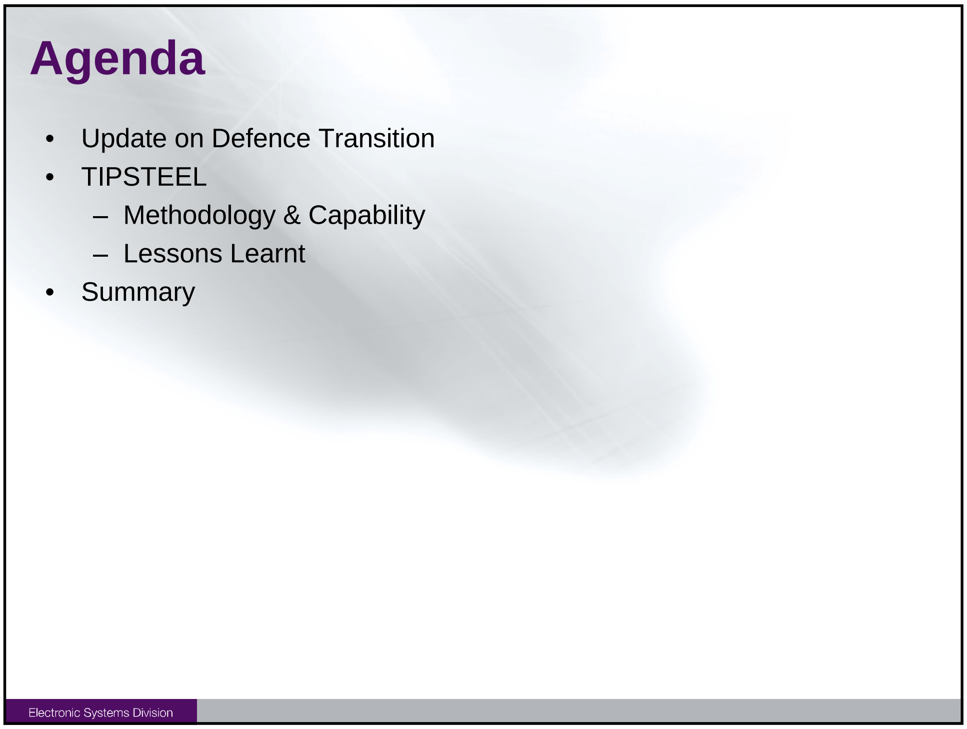


Tactical Information Exchange Integration Office Internet Protocol Simulation Test Evaluation and Experimentation Lab
TIPSTEEL

Defence IPv6 Transitioning

Presented by
Ms Margot Schelling
Contractor to Defence

Contribution by
Mr Aaron Smith
Contractor to Defence



Agenda

- Update on Defence Transition
- TIPSTEEL
  - Methodology & Capability
  - Lessons Learnt
- Summary

IPv6 and Defence

Why?

Interoperability with coalition partners and allies.

When?

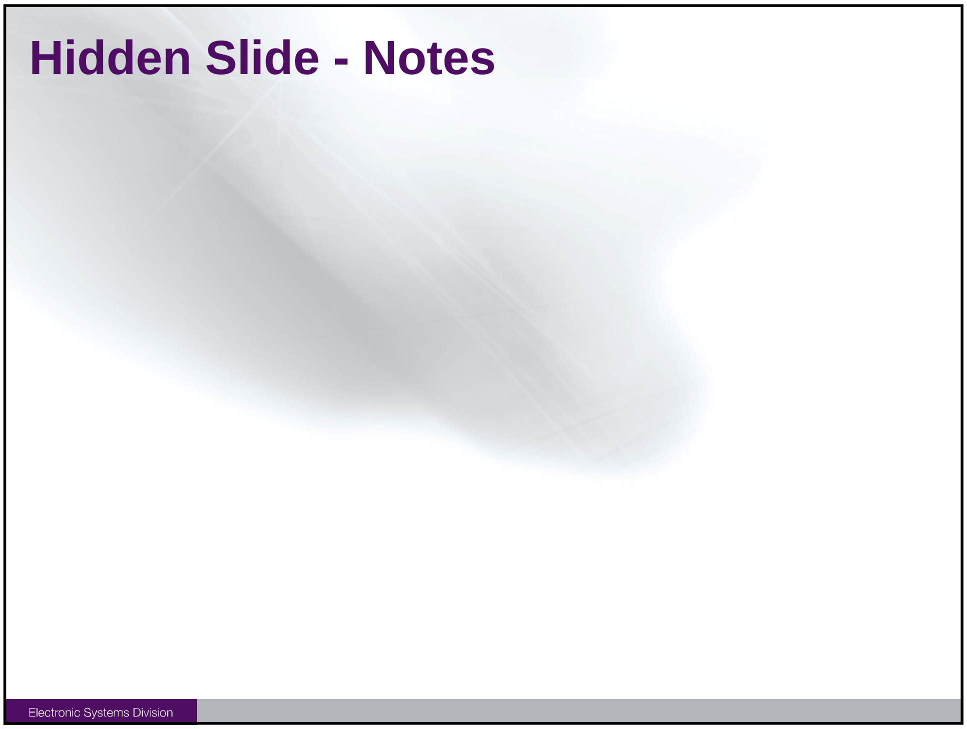
– US DoD transition (Backbone) to IPv6 - 2008

– NATO transition to IPv6 - 2011

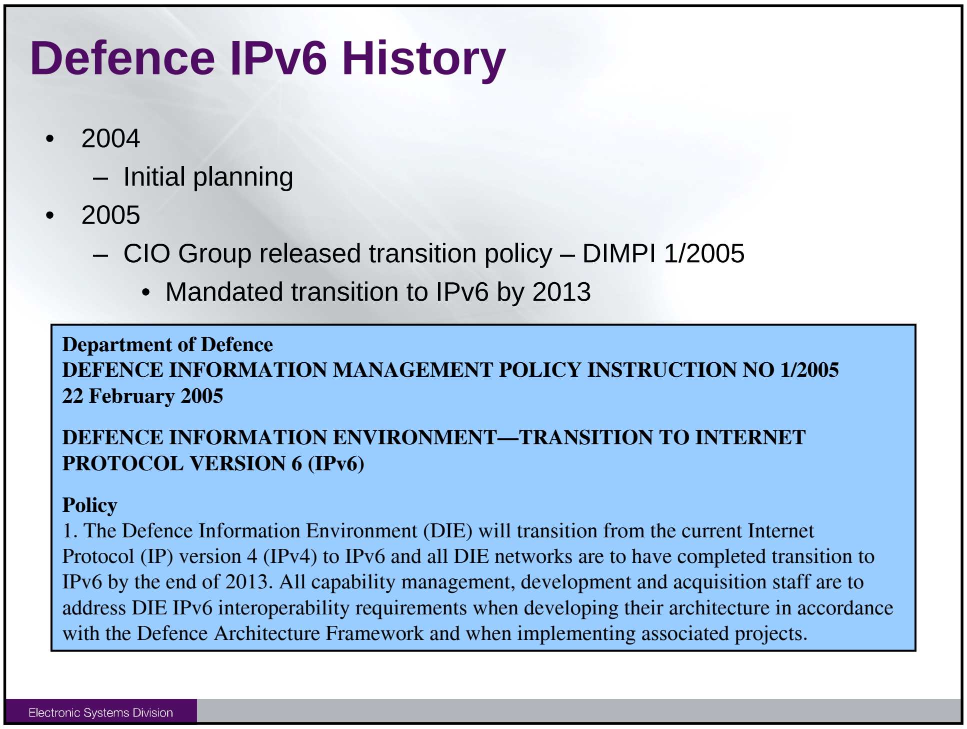
– Australian DoD to IPv6 - 2013

Defence Wide Area Network History

- **Mid 80's:** First PCs arrive in Defence.
- **Late 80's:** Small Local Area Networks.
- **Early 90's:** Large LANs only at Service Headquarters.
  - No standardisation on protocols.
- **Late 90's:** Wide area network moves to Asynchronous Transfer Mode (ATM).
  - Centrally managed WAN but still many independent domains.
- **Y2K:** Consolidation of domains and expansion of the Defence Restricted Network (DRN).
- **Early 00's:**
  - Consolidation of network management – single Defence Network Operations Centre (DNOC).
  - Implementation of common standard operating environment for DRN/DSN.
  - Major upgrade to Defence Wide Area Communications Network (DWACN).
- **Today:** Continues to manage numerous independent data environments.
  - Host numerous independent networks.



Hidden Slide - Notes



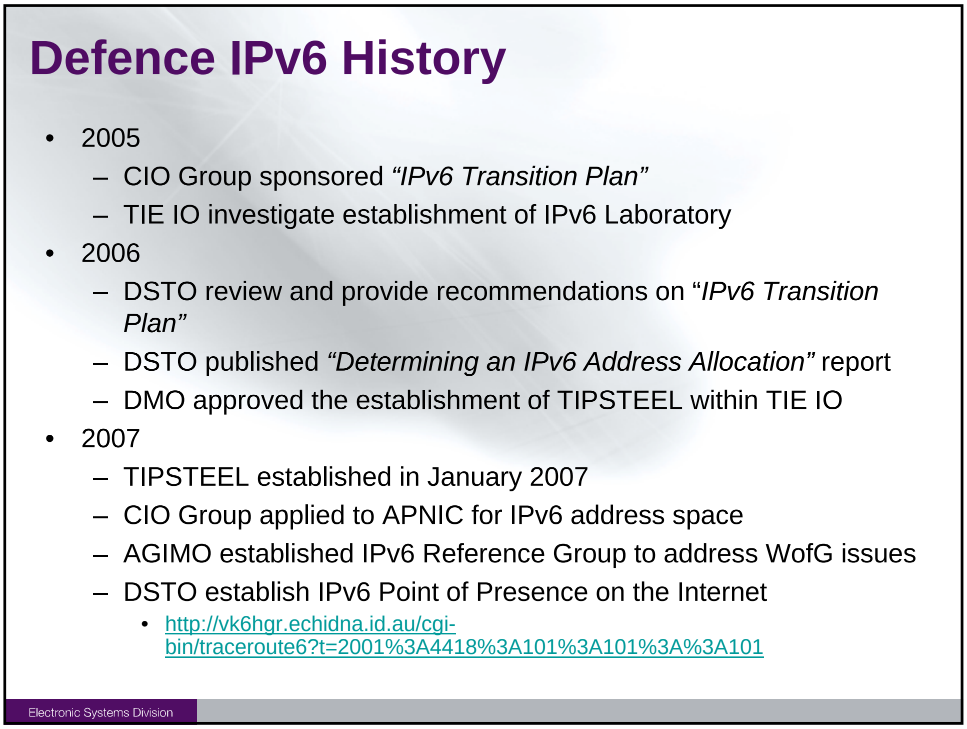
Defence IPv6 History

- 2004
  - Initial planning
- 2005
  - CIO Group released transition policy – DIMPI 1/2005
    - 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)

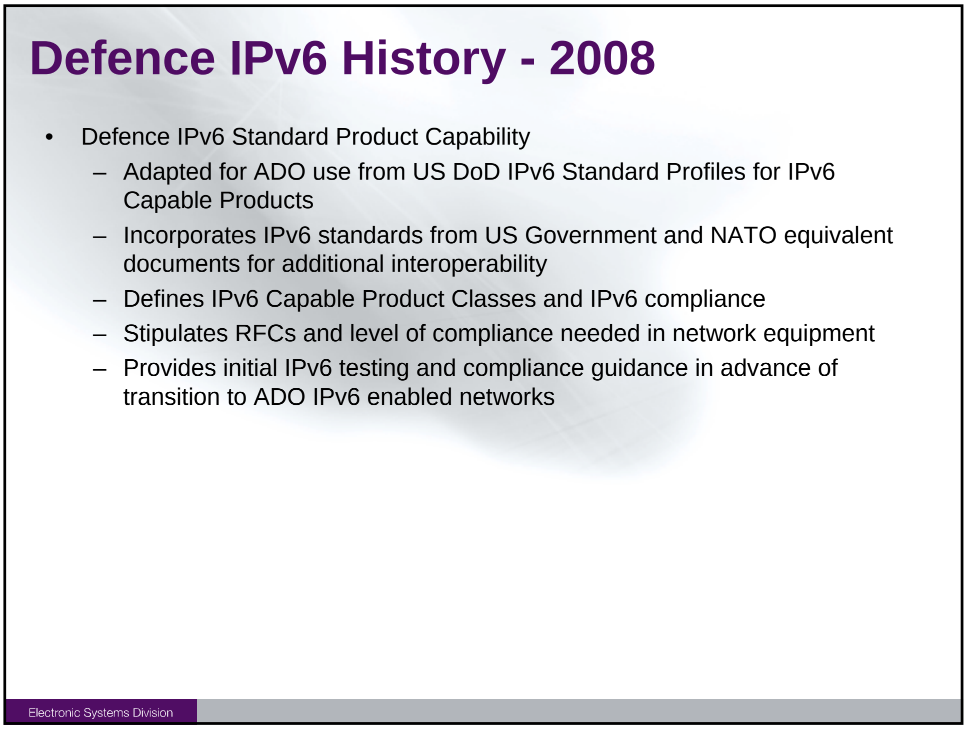
Policy
1. The Defence Information Environment (DIE) will transition from the current Internet Protocol (IP) version 4 (IPv4) to IPv6 and all DIE networks are to have completed transition to IPv6 by the end of 2013. All capability management, development and acquisition staff are to address DIE IPv6 interoperability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



Defence IPv6 History

- 2005
  - CIO Group sponsored *“IPv6 Transition Plan”*
  - TIE IO investigate establishment of IPv6 Laboratory
- 2006
  - DSTO review and provide recommendations on “*IPv6 Transition Plan”*
  - DSTO published *“Determining an IPv6 Address Allocation”* report
  - DMO approved the establishment of TIPSTEEL within TIE IO
- 2007
  - TIPSTEEL established in January 2007
  - CIO Group applied to APNIC for IPv6 address space
  - AGIMO established IPv6 Reference Group to address WofG issues
  - DSTO establish IPv6 Point of Presence on the Internet
    - http://vk6hgr.echidna.id.au/cgi-bin/traceroute6?t=2001%3A4418%3A101%3A101%3A%3A101

Electronic Systems Division



Defence IPv6 History - 2008

- Defence IPv6 Standard Product Capability
  - Adapted for ADO use from US DoD IPv6 Standard Profiles for IPv6 Capable Products
  - Incorporates IPv6 standards from US Government and NATO equivalent documents for additional interoperability
  - Defines IPv6 Capable Product Classes and IPv6 compliance
  - Stipulates RFCs and level of compliance needed in network equipment
  - Provides initial IPv6 testing and compliance guidance in advance of transition to ADO IPv6 enabled networks

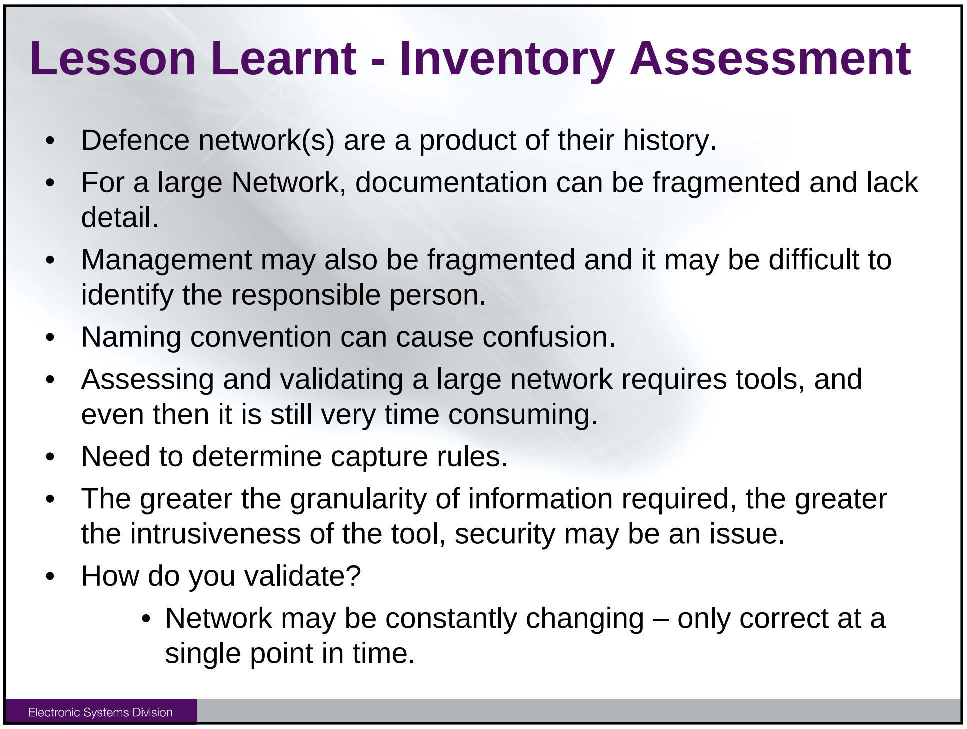
Electronic Systems Division

Defence IPv6 History - 2008

- Defence IPv6 Standard Product Capability
  - Adapted for ADO use from US DoD IPv6 Standard Profiles for IPv6 Capable Products
  - Incorporates IPv6 standards from US Government and NATO equivalent documents for additional interoperability
  - Defines IPv6 Capable Product Classes and IPv6 compliance
  - Stipulates RFCs and level of compliance needed in network equipment
  - Provides initial IPv6 testing and compliance guidance in advance of transition to ADO IPv6 enabled networks
- ACSI 33
  - Adding IPv6 guidance for September 2008 update
  - Key IPv6 points:
    - Disable IPv6 functionality until further notice
    - Recommends purchasing network equipment which is IPv6 capable
    - http://www.dsd.gov.au/_lib/pdf_doc/ism/ISM_Sep08_unclass.pdf

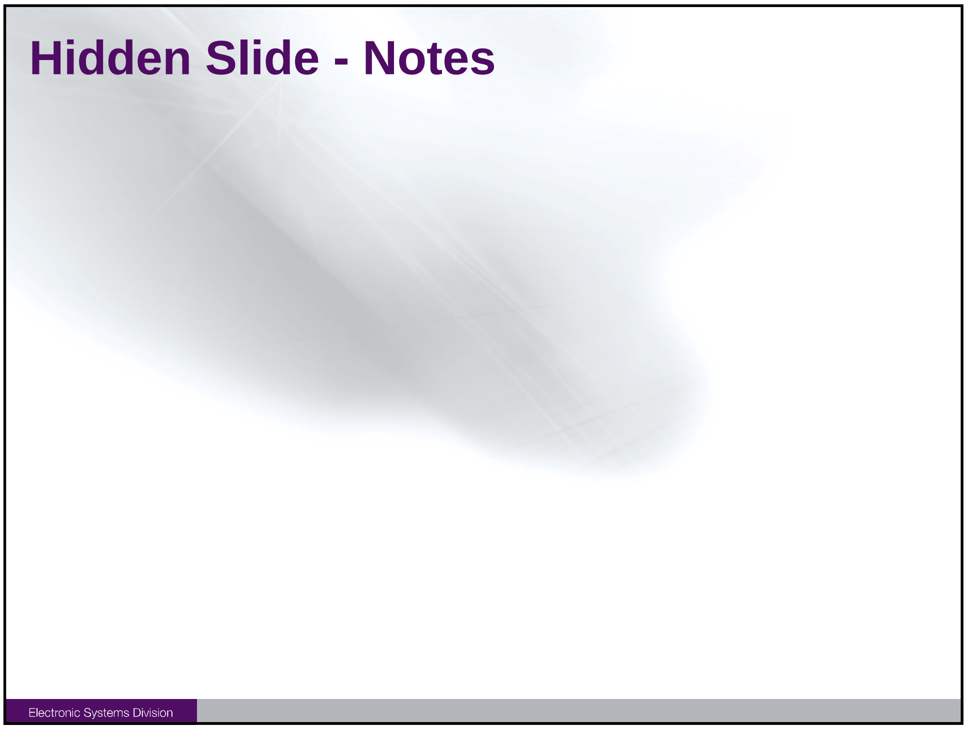
Transition Progress

Assign an official lead to coordinate IPv6 Transition Planning	CIO Group but no designated area
Determine what Defence wants to be IPv6	IAW DIMPI IPv6 covers all areas Strategic and tactical: though not yet prioritised
Define what IPv6 Means	IPv6 Standard Product Capability Draft released Aug 08
Baseline/inventory of networks	DRN / DSN captured using OPNET Sentinel and converted to OPNET Models. • Inventory Report: Vendor, Model and Operating System version • Configuration Report: Routing protocol by device / interface • Function Specific Report – tunnels
Conduct IPv6 "capable" assessment	• IPv6 Standard Product Capability as guidance • OPNET Model
Conduct Architecture Review	Models now available, but not allocated



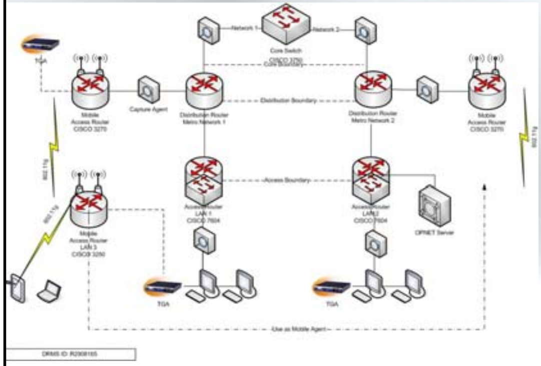
Lesson Learnt - Inventory Assessment

- Defence network(s) are a product of their history.
- For a large Network, documentation can be fragmented and lack detail.
- Management may also be fragmented and it may be difficult to identify the responsible person.
- Naming convention can cause confusion.
- Assessing and validating a large network requires tools, and even then it is still very time consuming.
- Need to determine capture rules.
- The greater the granularity of information required, the greater the intrusiveness of the tool, security may be an issue.
- How do you validate?
    - Network may be constantly changing – only correct at a single point in time.

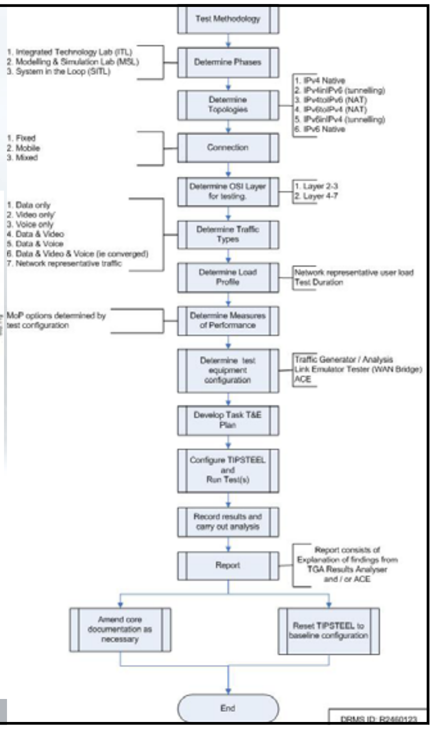


Hidden Slide - Notes

TIPSTEEL
Test Methodology & Capability



Conformance,
Interoperability &
Performance
Testing


Test Methodology
1. Integrated Technology Lab (ITL)
2. Modelling & Simulation Lab (MSL)
3. System in the Loop (SITL)
Determine Phases
Determine Topologies
1. IPv4 Native
2. IPv4inIPv6 (tunnelling)
3. IPv4toIPv6 (NAT)
4. IPv6toIPv4 (NAT)
5. IPv6inIPv4 (tunnelling)
6. IPv6 Native
1. Fixed
2. Mobile
3. Mixed
Connection
Determine OSI Layer for testing.
1. Layer 2-3
2. Layer 4-7
1. Data only
2. Video only
3. Voice only
4. Data & Video
5. Data & Voice
6. Data & Video & Voice (ie converged)
7. Network representative traffic
Determine Traffic Types
Determine Load Profile
Network representative user load
Test Duration
MoP options determined by test configuration
Determine Measures of Performance
Determine test equipment configuration
Traffic Generator / Analysis
Link Emulator Tester (WAN Bridge)
ACE
Develop Task T&E Plan
Configure TIPSTEEL and Run Test(s)
Record results and carry out analysis
Report
Report consists of Explanation of findings from TGA Results Analyser and / or ACE
Amend core documentation as necessary
Reset TIPSTEEL to baseline configuration
End
DRMS ID: R2460123

Summary

Transition Assessment:

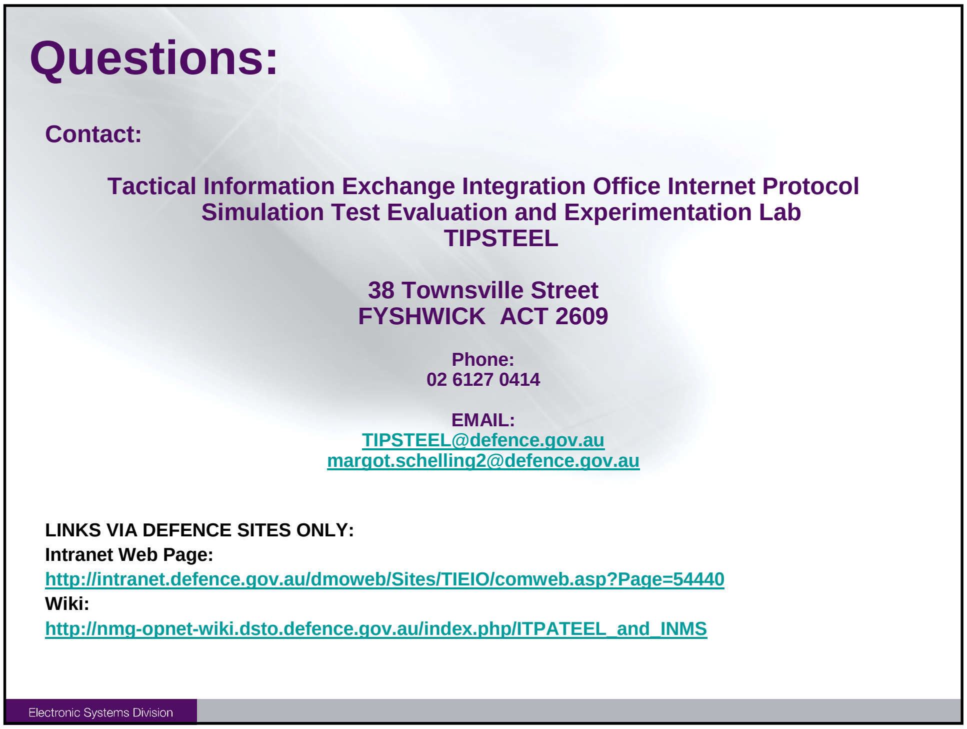
- Network(s) are a product of their history.
- Consider the state of your management, configuration and documentation – it impacts on the amount of work to be done.
- The greater the granularity of information required, the greater the intrusiveness of the tool, security may be an issue.
- How do you validate?

Setting up a Lab:

- If possible don't attempt setting up without a requirements definition.
- Suitable test equipment is essential.
- Accept that when testing a new technology there will be a high level of unknowns.
- Modelling and simulating even the smallest network will probably be underestimated.

Mobility Task:

- IOS Version – the latest is not necessarily the greatest.
- Integration – commercial off the shelf and military have issues.
- Protocols can drive design in military applications, with a need to understand all protocol options.



Questions:

Contact:

**Tactical Information Exchange Integration Office Internet Protocol
Simulation Test Evaluation and Experimentation Lab
TIPSTEEL**

**38 Townsville Street
FYSHWICK ACT 2609**

**Phone:
02 6127 0414**

**EMAIL:
TIPSTEEL@defence.gov.au
margot.schelling2@defence.gov.au**

LINKS VIA DEFENCE SITES ONLY:
Intranet Web Page:
http://intranet.defence.gov.au/dmoweb/Sites/TIEIO/comweb.asp?Page=54440
Wiki:
http://nmg-opnet-wiki.dsto.defence.gov.au/index.php/ITPATEEL_and_INMS

Electronic Systems Division