Document:

Reference Architecture

Part:

Title

Dated:

April 2022

Company contact:

Chief Technology Officer

cto@downerdefence.com.au

Contents

**No table of contents entries found.**

Figures

**No table of figures entries found.**

Tables

**No table of figures entries found.**

# Networking Reference Architecture

References:

1. [X.200 Open Systems Interconnection - Basic Reference Model](https://www.itu.int/rec/T-REC-X.200-199407-I/en) of 1 Jul 1994
2. [RFC791](https://tools.ietf.org/html/rfc791), Internet Protocol of Sep 1981
3. Information Security Manual of 30 May 2016
4. Solution Reference Architecture of dated 24 May 16 ()
5. Deployed Reference Architecture (draft)

## Introduction

Defence runs a geographically diverse IT and communications network made up of fixed and deployable components. The network has to operate in physically and logically hostile environments that utilises all known transmission mediums across a wide range of spectrum.

1. Additionally, and uniquely to a military force, Defence has to extend its network from the fixed environment to transportable and mobile elements, operating in deployed Areas of Operation (AO). Within these AOs, the need exists to operate both connected to, and independently from, the fixed environment.
2. There is an ever increasing need to consume services from any location and make information more widely available across the enterprise. In the military context this needs to be achievable with more agility and flexibility than typically seen in the civilian sector as the actual infrastructure needs to be mobile and adaptable to the fluid nature of warfare.
3. The network, indeed the entire ICT environment, should not constrain operations it should enable them. To this end it is necessary to ensure that the network is as homogeneous as possible and that artificial constraints do not limit its function, which is of cause to enable IT systems to communicate so that information can be distributed to end users.
4. With in the Defence the term *network* has been generically used and could refer to many different aspects of the whole ICT environment. This imprecise use of the term leads to confusion and inconsistency about what the network actually is; which results in solutions being implemented at inappropriate levels/locations in the enterprise that constrain agility and; therefore, constrain operations.
5. This Reference Architecture introduces the high level taxonomies to be used to describe the network and use these to guide solutions by defining patterns for use in the various circumstances.

### Definition

In relation to ICT a *Network* is: an interconnected set of communication nodes that enables information to be carried across them to facilitate end-to-end communications. The Network Layer in Reference A is the highest layer that is aware of the physical topology of the nodes. Reference A goes on to state:

It [the Network Layer] provides to the transport-entities [ICT Devices] independence from routing and relay consideration associated with the establishment and operation of a given network-connection. This includes the case where several sub-networks are used in tandem or in parallel. It makes invisible to transport-entities how underlying resources such as data-link connections are used to provide network-connections.

Any relay functions and hop-by-hop service enhancement protocols used to support the network-service between the [Open Systems Interconnection] OSI end systems are operating below the Transport Layer [the end-to-end layer], i.e. within the Network Layer or below.

The networking layer is also referred to as Layer 3.

1. By definition a group of interconnected nodes that can communicate at Layer 3 form a network. Therefore, separate groups of nodes, where the groups do not connect at Layer 3 are independent networks.
2. Reference B defines predominate networking layer protocol in Defence, which is the *Internet Protocol* (IP), this is the protocol defined as a part of the TCP/IP stack initially developed by the Defense Advanced Research Projects Agency in the early 1970s, which although does not directly align with the OSI Reference Model, aligns well at Layer 3. Figure 1 shows the alignment of the layers.
3. 
4. Figure 1: The two Reference Models

### Scope

Where does this specific Reference Architecture apply?

### Audience

Who is this Reference Architecture aimed at?

## Discussion

The point of a network is to facilitate communications. However, in the Defence context where ICT users have different clearances and different needs to know, breaking up a network into separate segments can also facilitate information security by constraining access to information systems utilising the networks. The issue with using network segmentation as an information security solution is that the problem that is being address is actually at the application level (in ISO this is Layer 7). This is where the information has meaning, can be labelled accordingly and therefore can be released to different users based on logical business rules. Additionally, segmentation at lower layers requires duplication of all the systems above the segmented level which is costly and constrains flexibility as it is hard to change.

1. To support moving the information security problem to higher Layers, this Reference Architecture will formally introduce the concept that within Defence there should only be one network – this one network’s role is to enable communications.
2. The following will be discussed:
3. The ‘Defence Network’ – what is it and how should it be modelled.
4. The role of network segmentation for as it relates to Security Domains defined in the ISM.
5. The segmentation use cases and technologies.
6. Deriving from this discussion will be a:
7. Network Layer/Location Taxonomy
8. A Segmentation Model

## Defence Network Model

Defence does not operate a typical corporate ICT system. It is a microcosm of a whole country, operating information systems to support providing services normally considered state offerings (health, education, welfare… all the civilian functions) and on top of this conducts war fighting.

1. Reference E introduces the fact that Defence delivers and consumes IT services (therefore, exchanges information) in a variety of locations (nodes) that suffer from constrained and potentially contended communications. Defence does not deliver IT services from a single logical location. Therefore, there is no concept of a core IT system, there are multiple IT system nodes interconnected by a network. Figure 2 shows the concept. In the figure the circles with a ‘C’ represent IT service consumers, the other circles are IT service delivery locations.
2. 
3. Figure 2: Core IT model vs a meshed IT model.
4. This leads to the concept that Defence’s IT operates more like a private Internet than a typical corporate Intranet (centralised core). Each service delivery node is akin to different organisations on the Internet providing services that can be consumed from anywhere by individuals and other organisations also on the Internet. This means that the various nodes need to be inter-connected via a mesh of links rather than just hub-spoke. However, in reality the mesh will contain network nodes that the traffic flows through and is routed rather that a series of point-to-point links. This leads the routed network shown in Figure 3 (left), where the mesh is replaced with routing nodes that form the network. This is the actual Layer 3, topology aware Networking Layer, that the Internet Protocol deals with. From Layer 4 (the Transport Layer, which is end-to-end) and up the actual topology of the network is not visible, this leads to the typical cloud representation of a network as shown in Figure 3 (right).
5. 
6. Figure 3: Networked Internet model.
7. Summarising this model: Defence maintains a private Internet of multiple service and consumer nodes, which are not connected point-to-point, but are interconnected with a mesh of routing nodes that from the network, for which the detail is hidden from the higher IT system layers that only wish to know how to communicate end-to-end.

### Layered Model

Across Defence the links that connect the network and the routing equipment that makes the network is provided by different technologies and different providers. In the fixed environment fibre optic links and commercial routing equipment is used by commercial providers, while operationally, Defence utilises a range of satellite links, point-to-point microwave, fibre and tactical data links. For communications systems these links all form Layers 1 and 2 of the OSI Model. Interconnecting them with routers using the Internet Protocol forms a Layer 3 – Internet Network over them.

1. This reference architecture will introduce:
2. A Network Locations taxonomy, and
3. A Network Segmentation model.

### 

, other, higher Layer, mechanisms should constrain them. However, there are circumstances where this is impractical and/or the requirements to satisfy controls in Information Security Manual (Reference C) will require segmentation. Therefore, a model that defines the segmentation to be used and when it is appropriate will be introduced.

1. Encryption is used to achieve confidentiality. Across Defence, encryption is applied in different locations both physically, and at different X.200 Layers, to achieve different outcomes and support different technologies. To increase clarity, and support the appropriate use of encryption as a part of the segmentation model, this Reference Architecture will introduce terms that define the relevant sections of the network.

### 

### Supporting Principles

### Network Locations

The point of a network is to facilitate communications between IT systems. The systems are geographically dispersed and have to exist some there has been no discussion of where those system are.

1. The discussion is to introduce the subject area and bring to the fore the principles and Reference Model taxonomies. It should not be a surprise to the reader when the principles that are defined later nor the Taxonomies in the Reference Model.
2. Figure 3: A demo figure

### Group heading in the discussion

From the previous discussion the following types of infrastructure services are defined:

1. Security.
2. Data management.
3. Network.
4. Availability.

## Principles

The following principles are introduced to support this reference architecture:

1. Defence operates as a *private Internet*.
2. Resilience and security are paramount.

## Reference Models

From the discussion above it is evident that…

## Decision Framework

This section introduces the ‘so what’. Now that we have introduced concepts, terminology and any relationships, how do we apply the patterns and standards?

1. …

## Patterns

The following questions need to be answered:

1. How do services get discovered…
2. …
3. The following
4. Annex:
5. An example annex

Enclosure:

1. There isn’t an enclosure

* to  
  Internet Protocol Network  
  Dated 31 Mar 2022

# An example annex

This is an example Annex.

1. Appendix:

* An example appendix
  + to  
    Annex A TO  
    Internet Protocol Network  
    Dated 31 Mar 2022

# An example appendix

This is an example annex.