Document:

Reference Architecture

Part:

Network Layer Reference Architecture

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.**

# Network Layer Reference Architecture

### References:

Open Systems Interconnection Reference Model

## Introduction

The tempo of the battlefield has increased over time and the ubiquitous presence of the media has reduced the tolerance for fratricide and other errors, placing an ever-increasing demand on the timeliness, accuracy and currency information supporting any Defence activity.

1. This information must be transported over various communication systems. The nature of Defence business requires it to operate its own communications systems that not only have to be robust but can be deployed, are transportable and often mobile. Yet at the same time inter-work with the fixed networks and support commercial and military specific applications.
2. This Reference Architecture covers the ISO OSI Networking Layer (Layer 3) and the layers below it, which in data communications are the layers that constitutes the communication network. Higher layers, the Transport Layer (Layer 4) and up, by design have the operation and topology of the network hidden from them.
3. This Reference Architecture introduces the following concepts:

Layer 3 - Services

routing boundaries.

1. addressing;
2. quality of service.
3. confidentiality, integrity, and authentication.
4. Layer 2 - Services
5. Local segment traffic.
6. Class of Service.

### Definition

OSI Layers 1, 2 and 3 establish an autonomous whole network which transfers data. Its purpose is to: ‘… establish, maintain, and terminate network-connections between open systems containing communicating application-entities and the functional and procedural means to exchange network-service-data-units between transport-entities over network-connections.’

1. In simple terms this layer is responsible for moving data effectively, deterministically at a required quality from end-to-end in a network, across physical media, but is not responsible for ensuring it gets there.

### Scope

This document specifies the Network characteristics, boundaries and capabilities required to provide the Enterprise a Network capable of delivering national and international Layer 2 and Layer 3 services. This document does not define how the higher layer application and presentation services make use of the network capability.

### Audience

This document is for solution architects and capability planners. It is intended to guide and constrain technical solutions to fit within the overall enterprise. Planners involved in the capability planning function should apply the language and concepts introduced to ensure a consistent approach.

## Network Transport

The network architecture is a tiered model that provides a trusted secure transport interconnect Service for End User devices and applications across geographical boundaries. The network provides services to the transport and application layers but abstracts the detail how connectivity is achieved.

1. The objective is for Defence to leverage its network infrastructure capability in the most efficient means possible and enable host and device communications in a manner that meets business and security needs while ensuring that capability is provided at the most relevant points within the reference model.

## 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

The figure below provides a network reference architecture that enables enterprise-wide Layer 3 connectivity.

1. Figure 1: Defence Layered Network Architecture
2. Figure 2: Defence Layered Network Architecture

### End Users/Host Devices

End Users and host devices connect to the Access Layer via fixed or mobile means to obtain communication services at Layer 2 on the local network segment. When the destination Layer 3 address is not located on the local network the host device utilises the Core/Aggregation layer to perform the required routing between the local and distant networks. For End User devices to connect to the network they must provide valid authentication credentials in the form of a X.509 certificate or other endorsed means.

### Access Layer

The Access network provides fixed and mobile End User connectivity to the greater network and enables host to host communications.

1. The Access Layer is responsible for providing reliable connectivity to devices and hosts. It is agnostic of the classification of traffic that is being presented to it and provides local host network communication through the discovery of Layer 2 adjacencies. Layer 2 discovery mechanisms are dependent upon the communication medium in use and each device is responsible for maintaining associations between the Layer 2 address and the appropriate physical communication port.
2. Support is provided for effective distribution of traffic streams that must be delivered to multiple end users at the same time through multicast distribution.
3. The access network classifies traffic and provides class of service to establish prioritisation.
4. Scalability, resiliency, and maintainability are achieved through virtualisation of the device, which enables physical element redundancy, simplification of Layer 2 protocols and greater infrastructure utilisation capacity.
5. Communication between hosts and devices that are not based upon the local network segment is achieved through routing performed at the Core/Aggregation Layer.
6. Network Access Control is implemented by the Access Layer devices utilising X.509 certificates to ensure that only endorsed approved fixed and wireless devices are provided access to the network.

### Core/Aggregation Layer

The Core/Aggregation Layer provides the Layer 3 default routing for the Access Layer domains within a Site and enables communication between different networks on Site.

1. Routing scalability is provided through a hierarchical design of which this layer provides the lowest or Site based capability. The Core/Aggregation routing peers with the high layer regional based routing domains that enables communication between Sites within the region. The routing protocols are optimised to reduce bandwidth requirements and enable fast convergence under conditions of network topology changes.
2. Prioritisation of traffic across the layer 3 network is provided through the classification and honouring of application traffic provided to this routing domain. This information is then carried seamlessly across the WAN to the destination device/hosts.
3. The Core/Aggregation Layer provides the point of distribution for traffic that must be distributed to multiple End User devices connected to the Access Layer.
4. All routing adjacencies must be authenticated to ensure that the routes are exposed only to trusted entities within the network.
5. Scalability, resiliency, and maintainability are achieved through virtualisation of the device, which enables physical element redundancy, geographical distribution, simplification of Layer 2 protocols and greater infrastructure utilisation capacity.
6. Communication between hosts and devices that are not based upon the Site is achieved through routing performed at the WAN/Edge Layers.

### WAN Layer

The Wide Area Network (WAN) Layer is responsible for providing access to secure transportation services between Defence Sites on a domestic and international basis.

1. The WAN encrypts all traffic that is required to be transported across commercial networks and provides confidentiality, integrity, and authentication services to ensure secure communications. Traffic requiring higher grades of encryption may be steered to appropriate devices before being placed upon the commercial network. Secure network tunnels should be able to be dynamically created across the commercial networks based upon the destination Sites.
2. The WAN commercial network utilisation will be capable of being directed by policy such that multiple commercial networks can be utilised at the same time based upon quality of service and service level requirements needing to be supported by Defence. Commercial network capacity and performance is rivalling the dedicated network performance and can be more effective in costs reduction for non-critical applications.
3. The WAN provides the top layer of the routing hierarchy and forms the backbone of the routing domain across the regional Sites. The routing also peers with the Site Core/Aggregation Layers and all routing adjacencies are authenticated.
4. Route peering with commercial carrier network is performed with an external routing protocol and enables a security control point for route distribution.
5. The WAN provides access to logically separate Layer 2/3 services provided by the commercial carrier networks.

### Edge Layer

The Edge Layer is responsible for providing access to secure transportation services between Defence Sites on a domestic and international basis.

1. The Edge Layer encrypts all traffic that is required to be transported across commercial networks and provides confidentiality, integrity, and authentication services to ensure secure communications. Traffic requiring higher grades of encryption may be steered to appropriate devices before being placed upon the commercial network. Secure network tunnels should be able to be dynamically created across the commercial networks based upon the destination Sites.
2. The Edge network will peer with commercial providers through an external routing protocol to provide international carriage to remote Defence Sites while maintaining internal route peer relationships with the remainder of the network.
3. The Edge networks will honour and potentially provide the ability to reclassify the traffic based upon business need as and provides bandwidth management across multiple deployed Sites.

### Services

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

1. Security.
2. Data management.
3. Prioritisation of traffic.
4. Network.
5. Availability.

## Decision Framework

The above architecture represented provides a generic pattern for an enterprise communication network and provides the basis for Layer 2 and Layer 3 services being provided for local and remote sites.

1. The decision framework now examines the usage patterns associated with the reference architecture to determine the applicability to Defence taking into consideration the information classification.

## Patterns

There are several usage patterns that can be applied with the reference architecture. The primary question that needs to be addressed is how classified information segregation is handled to meet the Information Security Manual requirements and if this should be implemented via the network.

1. The most basic pattern that meets all requirements is as indicated below:
2. Figure 3: Information Security transportation through network segregation
3. The above diagram represents the network transport solution required when the application and devices are agnostic of the level of their security information as well as the network. At a basic level, all security classification domains are treated as independent, and air gapped from each other. Cross domain solutions from lower to higher security domains are used to provide situational awareness.
4. The WAN layer is common to all security domains because all traffic that traverses any commercial network external to Defence is encrypted. The resulting model of the pattern where both network and applications/devices are agnostic of the information classification that is created by the devices is below.
5. Figure 4: Information Security transportation through network segregation with common WAN
6. As each information security domain is encrypted prior to external transmission a common black WAN service can be utilised.
7. These models result in network and application duplication consequentially increasing the complexity and cost of maintenance and support of the network.
8. Examination of the options of where information segregation is performed is provided below:

Table 1: Network Options for implementation of information security classification segregation

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** **#** | **Implementation within Network** | **Implementation within Application / Host / Devices** | **Comments** |
| 1 | No | No | Invalid capability as will not meet the security requirements. |
| 2 | Yes | No | Multiple duplicated network domains based upon the classification of data provided to the network. Refer Figure 4. |
| 3 | No | Yes | Application domain manages the information classification and treats the payload prior to presentation to the network.  Provides the potential of a single network domain and implementation reducing cost and complexity in the network.  Increases the complexity in the application domains requiring implementation of treatment of information to meet the required security classification potentially increasing costs for Application/End User devices. Refer Figure 5. |
| 4 | Yes | Yes | Represents duplication in information handling for no ultimate gain. |

1. The following diagram represents Option 3 above where the Application layer manages the treatment of the information prior to presentation to the network for transportation.
2. Figure 5: Application architecture performing classification of its information prior to network transport
3. The treatment of the application data and understanding of the classification of the data has been viewed above as being a function of the application. It has been considered that the ability of the network to implement dynamic multilayer security treatment at a packet layer based upon the application End User identity, and function being performed on the application, is not a function that can be reliably performed by the network. This pattern has been excluded from the above consideration.
4. The elected architecture pattern needs to consider the total cost of ownership and consideration of the future strategy of Defence in determining a direction. If the architectural direction is that identified in Figure 5 then Option #4 may be a migration step towards the final target architecture.
5. This paper will be underpinned by a few separate Solution Architecture papers that will provide the deep dive information required to guide projects performing implementation.