Defence Research and Development Canada Recherche et développement pour la défense Canada

Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks

Nabil Rafei and Andrew L. Vallerand

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2006-269
November 2006

Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks

Nabil Rafei
DRDC Ottawa

Andrew L. Vallerand
DRDC Ottawa

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2006-269

November 2006

Abstract

The DRDC Ottawa Future Forces Synthetic Environments section (FFSE) is an R&D centre of excellence in the area of Science and Technology for distributed Synthetic Environments (SE), distributed Capability Management as well as Distributed Collaborative Environments (collectively they can be referred to as Distributed Environments, for simplicity).

The use of Distributed Environments for experimentation across Governments, Industry, Academia and Allies is becoming increasingly prevalent, particularly with the adoption of International Standards such as the Institute of Electrical and Electronic Engineers (IEEE) 1278 Distributed Interactive Simulation (DIS) protocol as well as the IEEE 1516 (and the HLA 1.3 Baseline) High Level Architecture (HLA) protocol for distributed simulation and IEEE 1220 and 1362 for System Engineering. In a recent Case Studies, for example, DRDC Ottawa, with the support of DRDC Corporate, used an unclassified, non-dedicated, through VPN-Protected network, to perform distributed simulation across the Government of Canada, Industry (the private sector) and Academia using a military scenario in a “JSMARRT 1” experiment in just a few weeks (Vallerand et al, 2004). This success was followed up in another Experiment using this time a National Security Scenario where DND’s Capabilities were required by Public Security Partners with the Threat of a simulated “dirty bomb” around Parliament Hill. This “JSMARRT 2” Experiment was performed in January 2006. Though, both experiments were eventually performed with some agility, the overhead in time and effort to have access to national connectivity was still way too high to be called seamless and persistent. For all partners involved.

The Maritime Air Littoral Ops (MALO) Technology Demonstration Project (TDP) led by DRDC Ottawa, in conjunction with DRDC Valcartier, DRDC Atlantic and Canadian Forces Maritime Warfare Centre (CFMWC), aims to break that paradigm and make the use of HLA-Based distributed events, not as a yearly activity, but as a seamless persistent daily/weekly activity. For that to occur it is necessary to be able to document and assess what a Code of Best Practices for such a network should be, either at the unclassified or classified level. The primary objective of this Report is to document a Code of Best Practice for selection, creation, and use of a network for distributed environments that enables a critical outcome never achieved in Canada: enabling a seamless, persistent national connectivity at the, a) unclassified level [Government (both Canadian and Allied), the private sector and Academia] b) classified (SECRET) level, to support with agility, distributed simulation, distributed Capability Management, and distributed Collaborative Environments

Résumé

La section des Environnements synthétiques pour les futures forces (ESFF) de RDDC Ottawa est le centre de R et D par excellence dans le domaine de la science et de la technologie relatif aux environnements synthétiques répartis, à la gestion répartie des capacités de même qu'aux environnements de collaboration répartis (en termes simples, on peut parler en général d'environnements répartis).

L'utilisation des environnements répartis pour réaliser des expériences dans les gouvernements, l'industrie, le monde universitaire et chez les alliés prend de plus en plus d'ampleur, en particulier avec l'adoption de normes internationales comme le protocole de la simulation interactive répartie (DIS) de l'*Institute of Electrical and Electronic Engineers* (IEEE) 1278 et le protocole à architecture de haut niveau (AHN) (avec les paramètres de base AHN 1.3) de l'IEEE 1516 pour la simulation répartie, de même que l'IEEE 1220 et l'IEEE 1362 pour l'ingénierie système. Ainsi, dans une récente étude de cas, RDDC Ottawa, avec l'aide du bureau principal de RDDC, s'est servi d'un réseau non classifié et non dédié, par le biais d'un réseau RPV protégé, pour exécuter une simulation répartie au sein du gouvernement du Canada, de l'industrie (secteur privé) et du monde universitaire à l'aide d'un scénario militaire dans une expérience « JSMARRT 1 », en quelques semaines seulement (Vallerand et al, 2004). Cette réussite s'est poursuivie dans une autre expérience à l'aide, cette fois, d'un scénario de sécurité nationale où des capacités du MDN étaient exigées de la part des partenaires du milieu de la sécurité publique, avec la menace d'une « bombe sale » simulée non loin de la Colline du Parlement, dans le cadre de l'expérience « JSMARRT 2 » réalisée en janvier 2006. Bien qu'elles aient été exécutées avec une certaine souplesse, le temps d'attente et les efforts déployés pour avoir accès à la connectivité nationale étaient encore beaucoup trop élevés pour que ces deux expériences soient considérées uniformes et constantes par tous les partenaires touchés.

Le projet de démonstration de technologies (PDT) des opérations navales et aériennes côtières (ONAC), dirigé par RDDC Ottawa de concert avec RDDC Valcartier, RDDC Atlantique et le Centre de guerre navale des Forces canadiennes (CGNFC), vise à casser ce paradigme et à utiliser les événements répartis à architecture de haut niveau (AHN), non pas comme une activité annuelle, mais comme une activité quotidienne/hebdomadaire uniforme et constante. Pour que cela se produise, il faut pouvoir documenter et évaluer ce que devrait être un code de déontologie pour ce type de réseau, que ce soit au niveau non classifié ou au niveau classifié. Le premier objectif de ce rapport est de documenter un code de déontologie pour la sélection, la création et l'utilisation d'un réseau, destiné à des environnements répartis, qui donne des résultats critiques jamais atteints au Canada, notamment assurer une connectivité uniforme et constante à l'échelle nationale a) à un niveau non classifié du gouvernement (canadien et allié), du secteur privé et du monde universitaire, b) à un niveau classifié (SECRET), afin d'appuyer avec souplesse la simulation répartie, la gestion des capacités réparties et les environnements de collaboration répartis.

Executive summary

The Final Report contained in this document presents a schedule of Findings and Recommendations to ensure the enabling of a seamless, persistent national connectivity at the Unclassified and Classified level. During the past two years, the Future Forces Synthetic Environments (FFSE) section has planned and executed several distributed simulations involving partners from the Canadian private sector and academia. Though the experiments were eventually executed with success, the time and effort needed to organize the events and to configure the required network infrastructure was excessive and cannot be qualified as the required seamless or even persistent. As such FFSE commissioned a study, through DRDC Corporate, to document a Code of Best Practice for the selection, creation and use of networks to enable seamless and persistent connectivity for the purpose of conducting distributed simulation experiments.

Four networks are available to the Department of National Defence (DND) for supporting Distributed Simulation experiments, distributed capability management/engineering analyses, and distributed collaborative environments:

1. Defence Research Establishment Network (DREnet), the connectivity that supports the exchange of R&D related experimental data in DRDC.
2. Canadian Forces Experimentation Network (CFXNet).
3. Canadian high-speed research network CA*net 4.
4. The general Internet.

The study determined that DND cannot simply choose a network. The network topology for a specific distributed simulation experiment will primarily be influenced by the participants and how each participant attains network access. Only the CFXNet can currently support classified distributed simulation experiments, whereas any combination of the other networks can be considered for unclassified distributed simulation experiments. Other key factors to consider are the experiment’s bandwidth and latency requirements, the applications in use, and the applications’ communication requirements (unicast versus multicast).

Participants require private network infrastructure to conduct distributed simulation exercises. The private networks are achieved with the use of virtual private network (VPN) technology, which also securely interconnect the segregated synthetic environment experimental networks of each participant. Unfortunately VPN solutions are difficult to configure. This study examined new dynamic VPN solutions that can dramatically reduce the time and effort needed to establish VPNs.

From a Security perspective, an agreement with private sector or academic organizations is needed that describes the use and operation of segregated synthetic environment experimental networks. This agreement takes the form of a memorandum of understanding (MOU), which must be executed between FFSE as a representative of DND and the private sector or academic organization that is interested in engaging in distributed Simulation experiments,

distributed capability management/engineering analyses, and distributed collaborative environments:

The key recommendations as Code of Best Practices contained in this report include:

1. Segregation of FFSE Synthetic Environment (SE) development network and the SE experimental network
2. Segregation of partner SE experimental networks and the need for MOUs.
3. Acquire Cisco routers in place of PIX firewalls.
4. Ensure that bandwidth requirements are included as part of future DND requirements
5. Classification of data, the need for Statements of Sensitivity (SoS) and Threat and Risk Assessments (TRAs). If the material is classified, one must allow for sufficient lead-time to arrange a CFXNet connection

Rafei, Nabil; Vallerand, Andrew, L. 2006. Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks. DRDC Ottawa TM 2006-269. Defence R&D Canada - Ottawa.

Sommaire

Le rapport final du présent document renferme un ensemble de conclusions et de recommandations visant à permettre une connectivité nationale uniforme et constante au niveau classifié et au niveau non classifié. Au cours des deux dernières années, la section des Environnements synthétiques pour les futures forces (ESFF) a planifié et réalisé plusieurs simulations réparties auxquelles ont participé des partenaires du secteur privé et du monde universitaire du Canada. Bien que les expériences aient été réalisées avec succès, le temps et les efforts consacrés à l'organisation des événements et à la configuration de l'infrastructure requise ont été excessifs. On ne peut donc pas parler d'expériences uniformes, ni même constantes. Ainsi, les ESFF ont réalisé une étude, par le biais du bureau principal de RDDC, visant à documenter un code de déontologie pour la sélection, la création et l'utilisation de réseaux qui assurent une connectivité uniforme et constante aux fins d'expériences de simulation réparties.

Le ministère de la Défense nationale (MDN) dispose de quatre réseaux pour le soutien des expériences réparties de simulation, de l'analyse technique/de la gestion des capacités répartie de même que des environnements de collaboration répartis :

1. le réseau des centres de recherches pour la défense (DREnet), la connectivité qui permet l'échange de données expérimentales liées à la R et D à RDDC.
2. le réseau d'expérimentation des Forces canadiennes (CFXNet).
3. le réseau canadien de recherches à grande vitesse « CA*net 4 ».
4. l'Internet.

L'étude a montré que le MDN ne peut pas simplement choisir un réseau. La topologie de réseau pour une expérience particulière de simulation répartie sera tout d'abord influencée par les participants et par la façon dont chaque participant a accès au réseau. Présentement, seul le CFXNet peut être utile aux expériences classifiées de simulation répartie, tandis que pour les expériences réparties non classifiées de simulation, toute combinaison des autres réseaux peut suffire. Il y a d'autres facteurs importants à considérer, notamment les exigences liées au temps d'attente et à la largeur de bande de l'expérience, les applications en service et les exigences des applications en matière de communications (unicast par rapport à multicast).

Les participants ont besoin d'une infrastructure de réseau privé pour exécuter des exercices répartis de simulation. On obtient des réseaux privés grâce à la technologie des réseaux privés virtuels (RPV), qui permettent d'interconnecter solidement des réseaux expérimentaux distincts d'environnement synthétique pour chaque participant. Malheureusement, il est difficile de configurer des solutions RPV. L'étude a porté sur de nouvelles solutions RPV dynamiques permettant de réduire considérablement le temps et les efforts requis pour établir des RPV.

Sur le plan de la sécurité, un accord avec les organismes du secteur privé ou du monde universitaire est nécessaire pour permettre l'utilisation et le fonctionnement des réseaux expérimentaux distincts d'environnement synthétique. Cet accord prend la forme d'un protocole d'entente (PE) devant être exécuté entre les ESFF, comme dans le cas d'un représentant du MDN et d'organismes du secteur privé ou du monde universitaire intéressé à entreprendre des expériences réparties de simulation, l'analyse technique/de la gestion répartie des capacités de même que des environnements de collaboration répartis.

Les principales recommandations faisant office de code de déontologie dans ce rapport sont les suivantes :

1. la distinction entre le réseau de développement de l'environnement synthétique ESFF et le réseau expérimental d'environnement synthétique;
2. la distinction entre les réseaux expérimentaux d'environnement synthétique et le besoin de protocoles d'entente;
3. l'acquisition de routeurs Cisco à la place de coupe-feu PIX;
4. s'assurer que les besoins en matière de largeur de bande sont inclus dans les besoins futurs du MDN;
5. le classement des données, le besoin d'énoncés de la nature délicate et d'évaluations de la menace et des risques. Si les documents sont classifiés, il faut prévoir du temps pour l'installation d'un raccordement CFXNet.

Rafei, Nabil; Vallerand, Andrew, L. 2006. Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks. DRDC Ottawa TM 2006-269. R & D pour la défense Canada - Ottawa.

Table of contents

List of figures

.

Acknowledgements

The authors would like to acknowledge the continuous and dedicated support of Mr Robert Strachan, DRDKIM 3-2, and his contractors at NRNS Inc, under Mr Joe Spagnolo. This dedication and support is providing DRDC connectivity that supports the exchange of experimental data across DRDC Labs, Governments labs, Industry, Academia and Allies. Such exchange of experimental data has been shown fundamental in DRDC from the point of view of Exchanging R&D Experimental data and fundamental from the point of view of allowing the linking up with the originators of such experimental data, their R&D partners. This COBP report would not have been possible without the support of DRKIM and NRNS Inc and this is gratefully acknowledged.

This page intentionally left blank.

1. Identification of Available Networks

The choices in available networks are few and their use is governed by the status of partners participating in experiments and exercises, across Government, Industry , Academia and Allies. The choices are limited to four only: Defence Research Establishment Network (DREnet), Canadian Forces Experimentation Network (CFXNet), the Canadian high-speed research network CA*net 4 as well as the general Internet.

1.1 DREnet

The Defence Research Establishment Network (DREnet) interconnects the headquarters of the Defence Research and Development Canada (DRDC) Agency with its five research centers (Ottawa, Toronto, Valcartier, Atlantic and Suffield). The DREnet provides unclassified network service for DRDC community and has been used as a support facility for R&D within DND. The DREnet has, occasionally, hosted other "guest" sites to meet specific objectives or during cooperative efforts and programs. Unlike most federal government networks, the DREnet is a dual-purpose network; it serves as a research network as well as a network for conducting the organization's business, including internet searches, Org business, web-based distributed Shared Common Collaborative Environment for S&T data, info, reports, across DRDC labs, NATO, TTCP, ABCA countries, etc.

Figure 1 illustrates the DREnet sites within Canada. They include the five previously identified research centres as well as DRDC Corporate in Ottawa, Ontario, the Centre for Operational Research and Analysis (CORA) in Ottawa, Ontario, DRDC Corporate, the new DRDC Centre for Public Security and the Pacific Dockyard Lab in Esquimalt, B.C (a detachment of DRDC Atlantic). The DREnet employs a hub and spoke topology, with all sites connecting to the DREnet Network Coordination Centre (NCC) in Ottawa, Ontario. Most DREnet links are comprised of single or dual 1.544 Mbps T1 circuits, but these circuits are heavily subscribed with Internet traffic such as web browsing and email. DREnet can be configured to support multicast services but, at the present, does not.

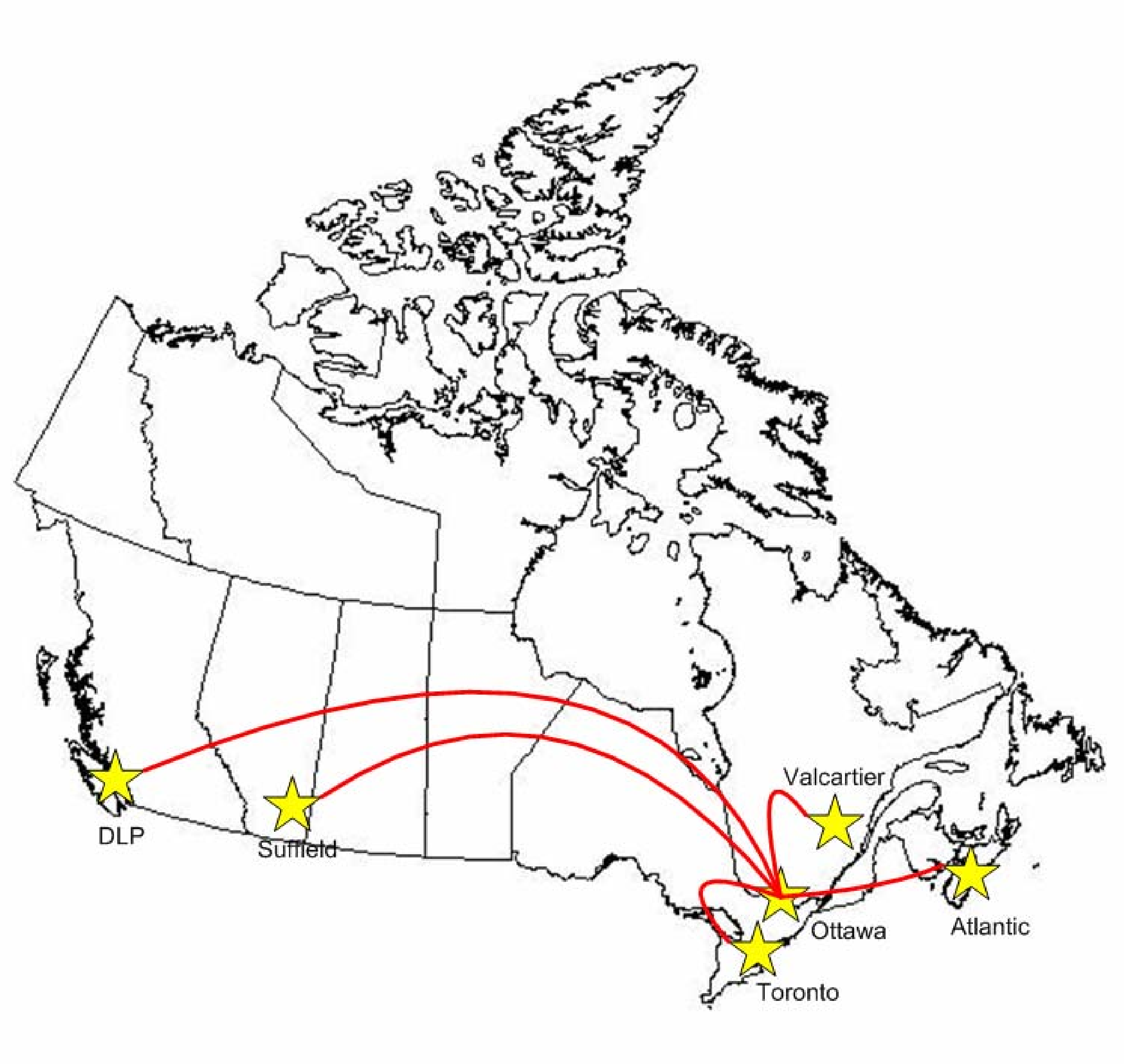


Figure 1 - The DREnet

Although FFSE and Capability Engineering would not incur any additional cost for using the DREnet in its current form, bandwidth limitations make the DREnet an unattractive option for conducting today's more complex and intense Distributed Simulation experiments. Distributed Capability Management Capability and Distributed Collaborative Environments.

DREnet includes tight controls at its perimeter (firewall and VPN) and the main firewall hides the DRDC "Intranet" from the Internet. The DRDC Intranet is shared by both, R&D systems as well as corporate servers and desktops. However, there currently exists little segregation between these systems within the DRDC Intranet. As such, the R&D systems inherit the protection posture afforded to DRDC corporate systems, which is considered too restrictive by the scientific community. The current DREnet architecture and protection posture inhibits the use of the DREnet to conduct networked experimentation such as distributed simulation.

A new architecture illustrated in Figure 2 is being implemented, by DRDC Corporate that introduces site level firewalls to segregate corporate systems from R&D systems. The site level firewalls offer the required protection to the corporate infrastructure (corporate zone) and public servers (public server zone) but do not impede R&D network traffic (R&D zone).

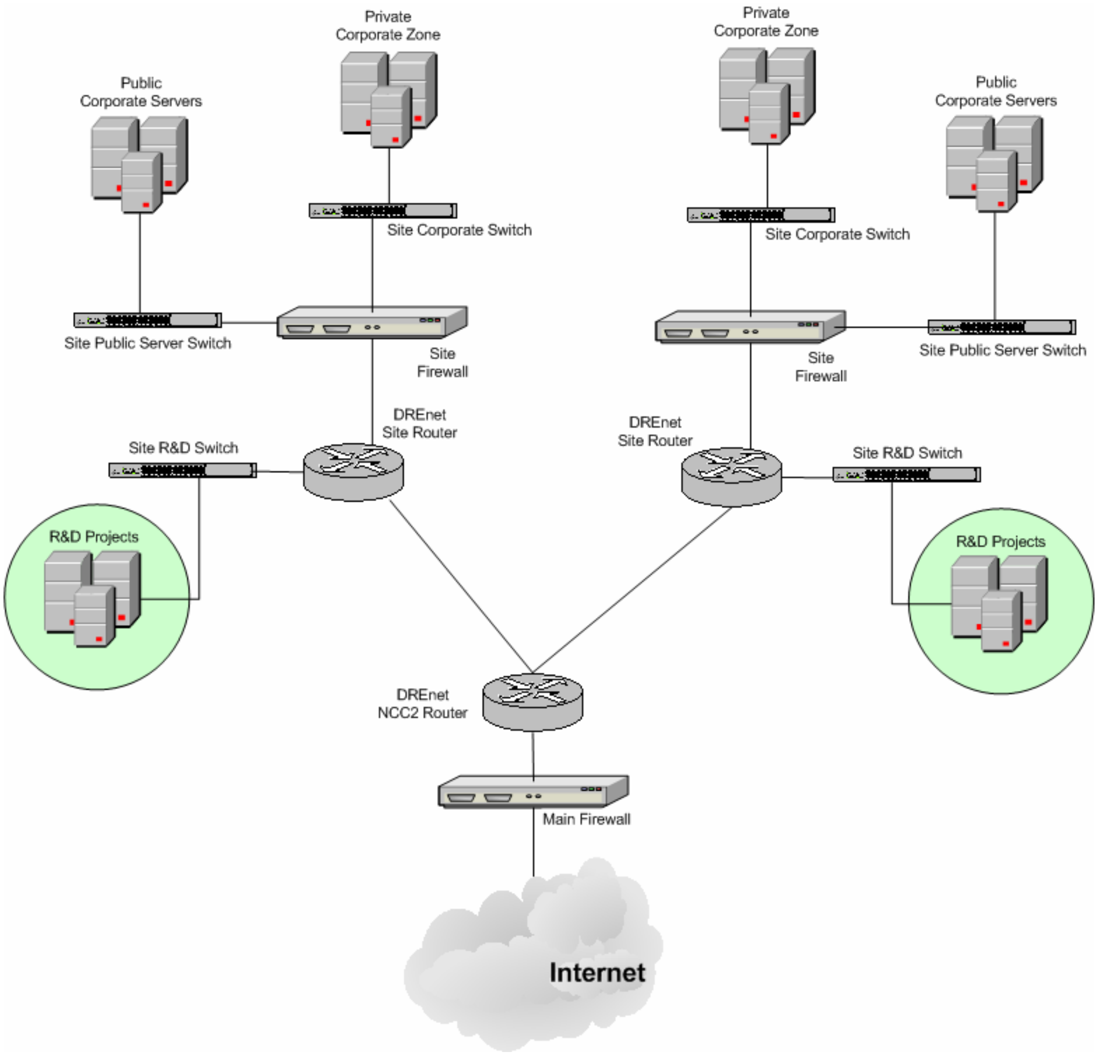


Figure 2 - New DREnet Architecture

It is estimated that the full implementation of this new architecture will take a further six months to complete. The number of request for a new architecture and the related level of commitment and engagement indicated that the most urgent priority should be given to DRDC-Ottawa, DRDC-Valcartier and DRDC-Atlantic, as a first step.

1.2 The CFXNet

The Canadian Forces Experimentation Network (CFXNet) is the Canadian segment of a much larger experimentation network, the multinational Combined Federated Battle Lab network (CFBLNet). The CFBLNet is a permanent /persistent network infrastructure used for conducting military technical demonstrations, evaluations, assessments and experimentation among member nations. The Canadian domain of the experimentation network, the CFXNet, is managed and operated by the Canadian Forces Experimentation Centre (CFEC) and is permanently connected to the CFBLNet infrastructure.

CFXNet currently provides a communications networked environment between various Canadian sites, primarily DND bases and DRDC Laboratories[1]. J2 Information Management, environmental experimentation organizations, and other establishments are connected as required. CFXNet also has the ability to connect to various development networks that are in use with allies, other government departments (OGDs), the private sector and academia[2]. These locations conduct initiatives to support pan-DND/CF activities.

CFXNet supports such continuous activities as Concept Development and Experimentation (CD&E), Modelling and Simulation (M&S), and any other activity requiring a robust and reliable non-operational network infrastructure.

Each participant in CFXNet provides, manages, supports and is responsible for its own components that are not designated as core components of the CFXNet. CFXNet participants can construct and execute initiatives between participants, at various security levels, and exchange the data needed to meet the objectives of a specific activity.

Access to the CFXNet is restricted. Any organization may propose an event; if that organization does not have a direct connection to the CFXNet, the event, if approved, must be hosted by a DND sponsoring organization. Experiments are put forward to the CFXNet Functional Network System Manager (FNSM) for approval.

Figure 3 shows the configuration of the CFXNet[3]. As with the DREnet, the CFXNet also implements a hub-and-spoke topology with all sites connecting to the CFXNet in Ottawa. CFXNet includes fairly high-speed links of at least 5 Mbps. CFXNet links are believed to be very lightly utilized in the absence of any major experimentation activities. As such, the CFXNet would be able to support distributed simulation experiments at the classified level at no additional cost to FFSE and other DRDC Lab, provided that no other large scale experiments were scheduled at that time. CFXNet does not support multicast services.

[1] DRDC Ottawa shares a connection with the Canadian Forces Experimentation Centre (CFEC).

[2] Although, to our knowledge, CFXNet has not, to date, connected to academia or private industry

[3] Figure 3 is out of date in that the two sites shown as being proposed (Shirley's Bay and Kingston) have now been approved.

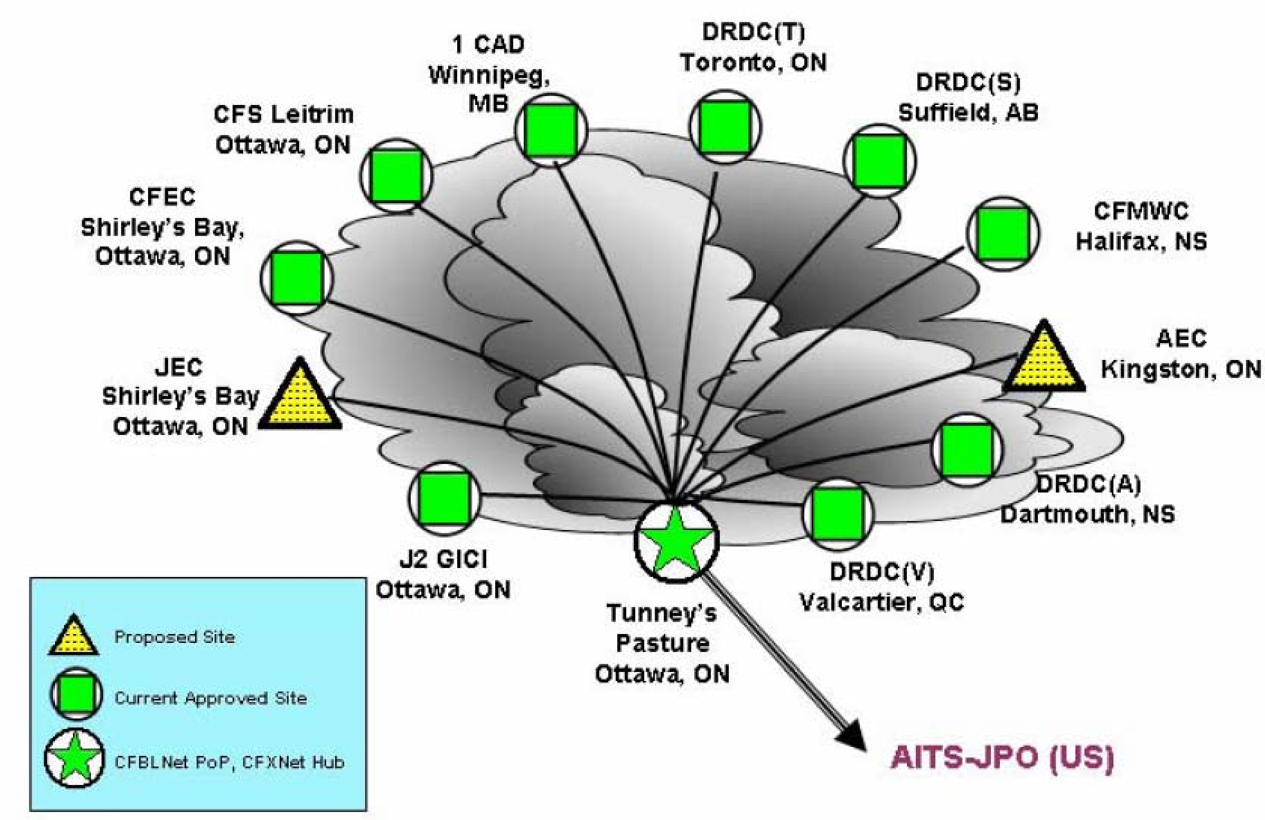


Figure 3 - The CFXNet

Figure provided by CFEC.

1.3 The CA*net 4

CA*net 4 is the Canadian national optical Internet research and education network and is funded by Industry Canada through CANARIE. CA*net 4 interconnects provincial research networks, and through them universities, research centres, government research laboratories, schools, and other qualified sites. Such sites connect with each other and also with international peer networks. CA*net 4, via a series of point-to-point optical wavelengths, most of which run at a speed of 10 Gbps, is capable of high communications speeds.

CA*net 4, which places dynamic allocation of network resources in the hands of end users allows a much greater ability for users to innovate in the development of network-based applications. Such applications, considering the ever increasing use of computers and networks as platforms for research in many and disparate fields, are essential for national and international collaboration, data access and analysis, distributed computing, and remote control of instrumentation required by researchers.

Future funding of CANARIE for CA*net 4 beyond March 2007 is not currently in place. Discussions are being held regarding continuance of CANARIE funding and a consensus of opinion is that CA*net 4 may be funded for a further five years but that CANARIE funds for research grants would be curtailed. Obviously, this is speculative, but it does indicate that FFSE and academia may not be able to rely upon continued use of CA*net 4 beyond March 2007.

CA*net 4 does not charge organizations for use of their network, however, the cost of connection to the nearest CA*net 4 point-of-presence (POP) is the responsibility of the user organization. The DREnet connects to CA*net 4 through a local 100 Mbps connection through the Communications Research Centre (CRC), which shares the Shirley Bay complex with DRDC Ottawa. Figure 4 shows coverage of CA*net 4 serviced areas. CA*net 4 does support multicast services.

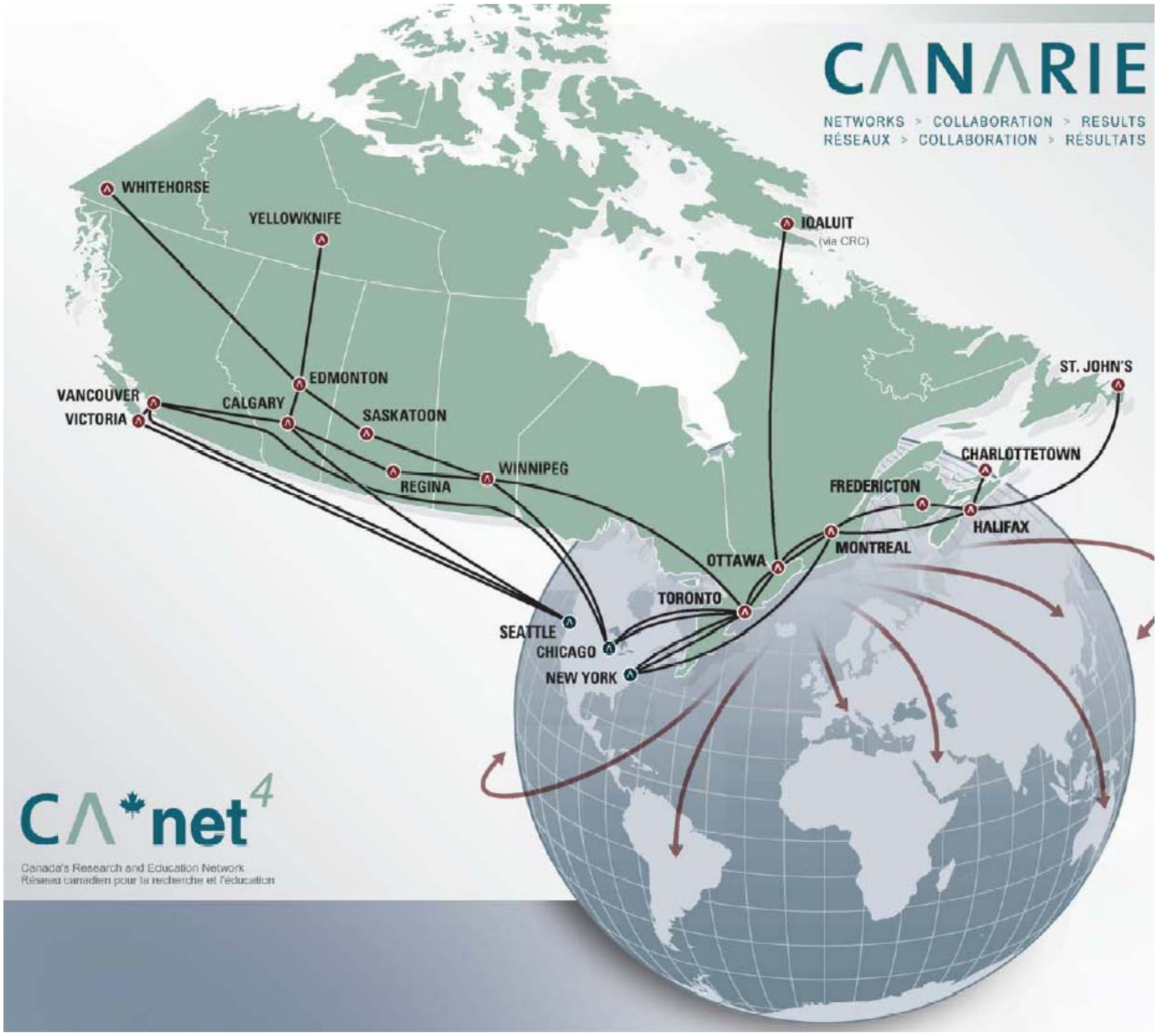


Figure 4 - CA*net 4

Fiigure from CANARIE Annual Report 2004/2005

1.4 The Internet

In many cases, DRDC partners and in particular FFSE will already have an existing connection to the Internet that can serve as a conduit for participating in distributed simulation exercises. It is common place today for academic institutions and corporations, both large and small, to possess multi megabit broadband access to the Internet. Relatively inexpensive digital subscriber line (DSL) connections provide sufficient bandwidth to support distributed simulation exercises. Unfortunately, FFSE and its partners do not control the intermediate network links and therefore can not guarantee or control the quality of service provided to simulation traffic as it traverses those intermediate Internet links. The Internet does not does generally support multicast services.

1.5 Dedicated Telecommunication Services

There may be cases where none of the identified networks are considered suitable for interconnecting a DND organization that needs to participate in distributed simulation exercises. Instead a DND organization could potentially establish a connection to the nearest DREnet site using DND supplied communication facilities such as a 1.544 Mbps T1 link. The new segregated DREnet architecture more easily accommodates this requirement since the DRDC site firewall protects the site corporate infrastructure from both the R&D network as well as the Internet.

2. JSimNet : FFSE's example of a Local Capability to support Distributed Environments

The Joint Simulation Network (JSimNet) is an unclassified network enclave located at DRDC Ottawa and administered by the FFSE section. JSimNet is comprised of a Synthetic Environments Battle Lab (SEB), a Distributed Capability Engineering Lab and a Distributed Collaborative Environment Lab in order to conduct/support Concept development and experimentation (CDE) work in particular. The JSimNet is an unclassified sub-network.

The main purpose of the JSimNet is to carry out both R&D and simulation environment experiments and exercises, by performing high-end computational processing and running unclassified simulations with advanced 3D graphics for CDE using exercise and visualization management tools. The JSimNet is used to run and experiment with simulation execution environments, models, simulations, tools, utilities, data interchange standards, Simulation Object Models (SOM), Federation Object Models (FOM), and related functionalities using database records, video streams, graphics using terrain and visual databases, data files, and selected e-mail messages. This simulation environment enables the development and testing of new concepts and ideas: the experimentation, checking, and testing of content transfers and real time simulations, network and system latencies: and the storing and retrieving of a pool of M&S datasets and simulation-related content.

Further, the JSimNet is a strategic element of the DRDC M&S/SE Strategic Plan in the development of a DRDC Federation capability for conducting large scale distributed and integrated synthetic environments scenarios generations using simulation models and tools across Govt, Industry and Academia and Allies. Furthermore, this network grid is used for concept development, experiments and demonstrations at the unclassified level and which can then, if required, be extended to the classified Canadian Forces Experimentation Network (CFXNet) to carry out classified experiments and exercises, as fit for the purpose.

Figure 5 illustrates how the JSimNet connects to the DREnet through a firewall device administered by the DREnet Management Team. The JSimNet firewall connects the JSimNet to both the DRDC Intranet and directly to the Internet. The connection to the DRDC Intranet permits limited access to DRDC network services such as file shares and email. The connection to the DRDC Intranet allows provides connectivity to the other DRDC research centres for the purpose of conducting simulation experiments. The connection to the Internet permits the establishment of virtual private network (VPN) channels to external academic and private sector partners for the purpose of conducting simulation experiments.

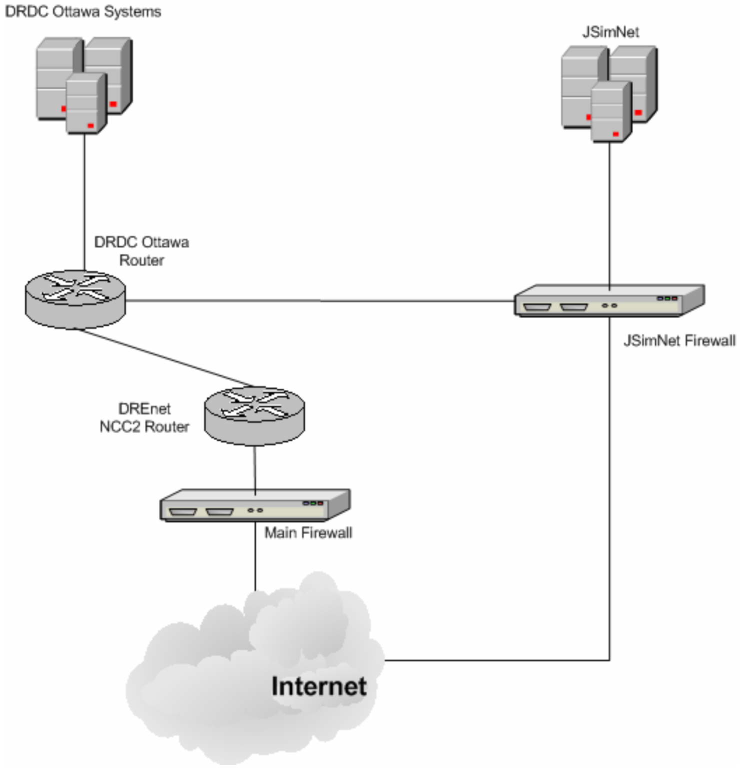


Figure 5 - The JSimNet

Findings and Recommendations

2.1 Connectivity

Currently FFSE is supplying preconfigured Cisco PIX firewalls to partners for each experiment. The firewalls create an encrypted Internet Security Protocol (IPSec) based VPN between each pair of participants.

The High Level Architecture (HLA) uses random ports, determined at run-time, for communication. This means that it is extremely difficult to 'firewall' HLA as all ports must be made available for HLA communications. To allow HLA communication, firewall rules have, of necessity, been minimized to the point that there is little control and very abbreviated security.

Various firewall hardware and firewall software versions and configurations have caused problems in configuration and have added considerably to the time taken to set up an experiment. Furthermore, it is almost impossible to recreate an experiment that has been previously run. Particularly PIX firewalls have been acquired on a "use what is available" basis and a considerable time and effort has been spent in getting them to work.

Currently when direct communications between two external partners is required (spoke to spoke), each firewall must be separately configured to recognize all of the other firewalls. Furthermore, as stated previously, each firewall must be manually configured. This, obviously, does not lend itself to rapid deployment nor to adding a new partner during the course of an exercise, particularly as FFSE require a minimum time and effort to set up an exercise. Not found here are agility and persistence, two key elements of transformation.

We have also noted that in-depth technical discussions with non-DND partners do not occur at an early stage of the experiment but, on occasion, only when technical connectivity problems arise.

Firewall/router configuration details are shown in Annex C.

2.1.1 DMVPN

Cisco Dynamic Multipoint VPN (DMVPN) allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and the Next Hop Routing Protocol (NHRP). DMVPN creates a hub and spoke topology, but allows direct spoke-to-spoke communication through dynamically created VPN tunnels between spoke locations. Hub-to-spoke configurations require that all traffic must first traverse the hub router, while spoke-to-spoke configurations deliver traffic addressed to another spoke directly to the destination spoke router. DMVPN currently supports multicast routing using hub-to-spoke delivery. Direct spoke-to-spoke multicast routing is not supported.

DMVPN can establish and maintain large VPN environments without the need to configure exhaustive information within a large number of devices. DMVPN spoke routers need only be configured with the identity of the DMVPN central hub router. Spokes connect to the central hub, register with the hub router using NHRP, and use NHRP to dynamically ‘learn’ about other spokes as and when required to communicate with other spokes. This method minimizes the configuration necessary, prior to connectivity and makes it extremely simple to add new partners (spokes) during the course of an experiment.

Since NHRP alleviates the need to configure the identity of spoke routers within the hub router, spoke routers can employ dynamically assigned addresses (i.e. dial-up and Digital Subscriber Line (DSL)) in addition to statically defined addresses.

Figure 6 illustrates how DMVPN can be leveraged to support a simulation exercise consisting of three internal DND locations (spokes) and two external locations from academia or the private sector. The green lines interconnecting the routers represent the VPN tunnel that each spoke router maintains to the hub router at all times. It is through this VPN tunnel that the spoke router learns of other spokes via NHRP. The blue lines interconnecting the spoke routers represent the VPN tunnels for direct spoke-to-spoke delivery of traffic. The spoke-to-spoke VPN tunnels are dynamic and created only as required to deliver traffic to another spoke. The spoke-to-spoke VPN tunnels are aged and removed when they expire, but are only recreated as required to deliver direct spoke-to-spoke traffic. If the simulation exercise includes multicast traffic, all multicast packets must be delivered to the hub router, which takes care of sending a copy of multicast packets to all spoke routers where there are interested recipients.

To expand the simulation exercise shown in Figure 6, only the new spoke router and possibly the hub router need to be configured. All existing spoke routers learn of the new spoke router from the hub router via NHRP.

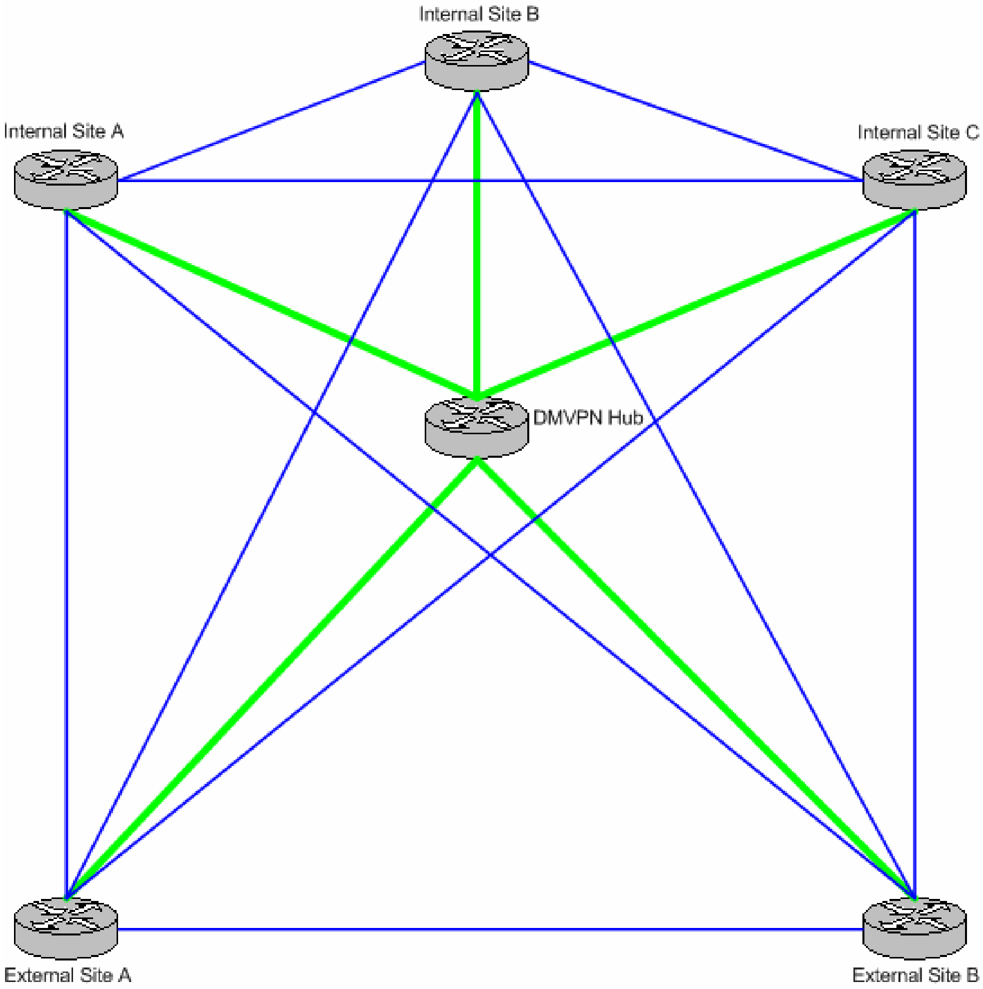


Figure 6 - DMVPN Spoke-to-Spoke Configuration

2.1.2 Segregation of JSimNet

Currently, the JSimNet firewall segregates the JSimNet from the remainder of the DREnet. This firewall has introduced delays and connectivity problems between JSimNet and other DRDC sites when conducting distributed simulation exercises as well as video conferences. DREnet policy requires that FFSE compile a firewall change request form each time a firewall configuration change is needed. This process is somewhat error prone and time consuming. Moreover, the JSimNet firewall has been known to interfere with application level data such as video conferencing. Lastly, the HLA communication requirements mandate a liberal firewall policy, which renders the firewall somewhat ineffective.

The JSimNet consists of a development network component where models are developed and experimental data stored. The JSimNet also includes an SE experimental network component, where the developed models are executed and resulting data is gathered. The development network component requires access to corporate email, files transfer as well as other generally available network services on an on-going basis. Only the SE experimental network component needs to be exposed to partners when conducting SE experiments.

2.2 Connectivity Recommendations

There are several recommendations to alleviate the current connectivity problems.

2.2.1 DMVPN

We recommend the acquisition of DMVPN capable Cisco routers with embedded firewall. The routers would be used as IPSec gateways as is currently the case with the PIX devices. These routers provide all the capability of existing PIX firewalls and would interoperate with existing PIX firewalls until the PIX firewalls can be phased out.

We also recommend that FFSE acquire a pool of identical DMVPN capable Cisco hardware and software and that FFSE compile detailed instructions for the required configuration changes when deploying a DMVPN spoke router. Moreover, we recommend that a maintenance contract be entered into to ensure access to software patches and updates.

2.2.2 Segregated SE Experimental Networks

Due to the impossibility of suitably “firewalling” HLA traffic caused by the continuous run-time allocation of ports, we recommend that University/Private Sector partners use a segregated network for SE traffic and experiments. Such a segregated network must be completely isolated from all other University/Private Sector partner networks and network activity.

This requirement should form part of a Memorandum of Understanding (MOU) with the University/Private Sector partner. Figure 7 shows how such segregation could be accomplished.

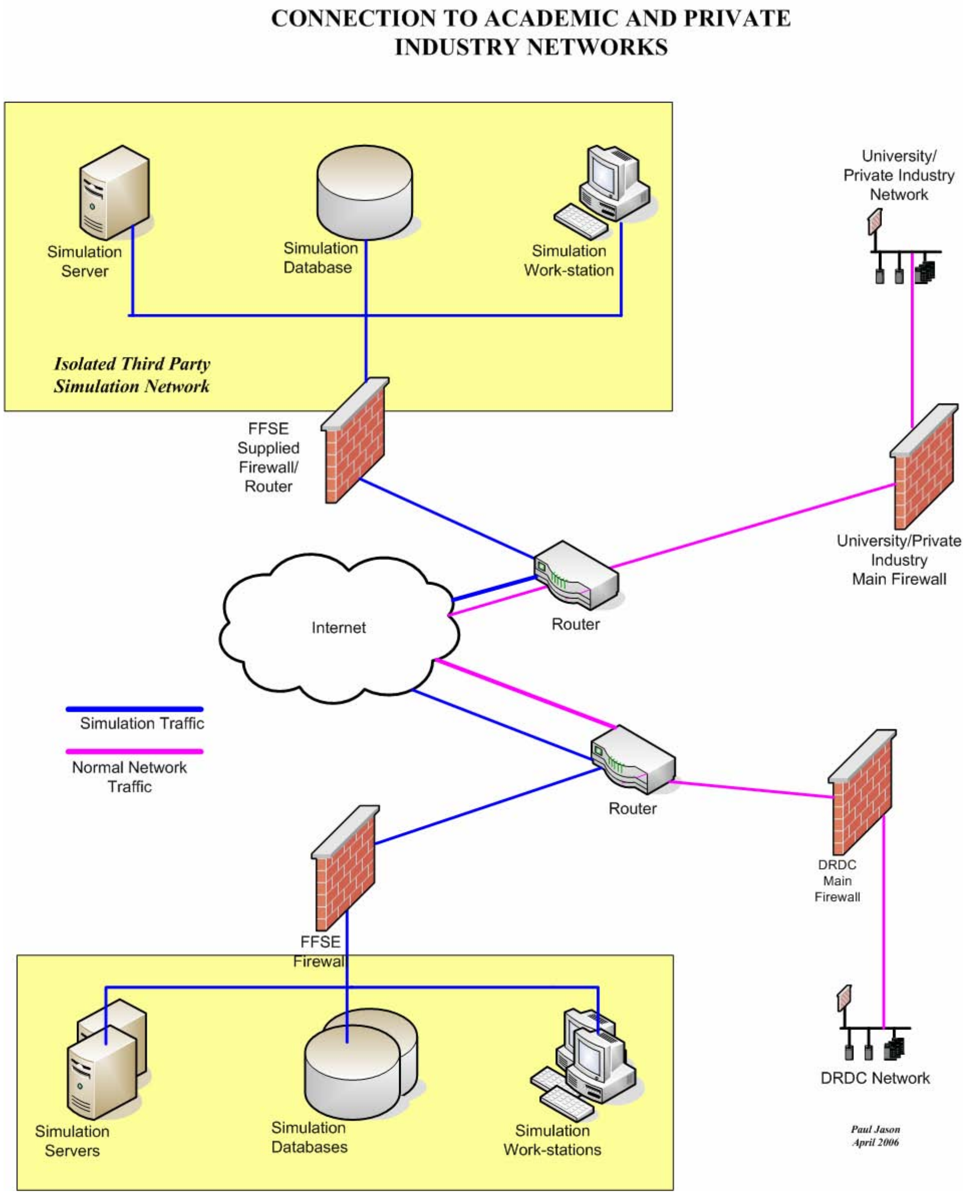


Figure 7 - Segregated Experimental SE Network

2.2.3 JSimNet Segregation or Segragation of Local Capability

The JSimNet development network component should be segregated from the JSimNet SE experimental network component and afforded some level of network security. Information should enter or leave the development network only at the discretion of FFSE.

The new DREnet architecture described in section 1.1 provides an opportunity to extend JSimNet to other DRDC sites. We recommend that FFSE segregate the JSimNet development network from the JSimNet SE experimental network. FFSE can transfer systems between the development network and the experimental network as required to conduct experimentation with its partners provided it adheres to the guidelines outlined in section 1.28.9.

Although the JSimNet development network could benefit from the protection afforded by the DRDC site firewall if it resides within the DRDC corporate zone, DRDC policy does not permit the transfer of systems between the DREnet R&D zone and the DRDC corporate zone. As such, we recommend that both the JSimNet development network and experimental network reside within the DREnet R&D zone. FFSE must assume the responsibility for providing security for the development network since DRDC Corporate is not responsible for the security of the DREnet R&D zone. It is important that FFSE not underestimate the effort and cost associated with securing network infrastructure.

FFSE researchers stated that certain experiments may require participation from the majority of the development systems, making the relocation of systems between the development network and the experimental network impractical. As such, we define a third JSimNet network called the JSimNet infrastructure network that houses infrastructure services.

Figure 8 illustrates the three JSimNet network components within the DREnet R&D zone. Figure 9 provides a more detailed view of the split JSimNet environment. The infrastructure network houses systems such as domain controllers, Dynamic Host Configuration Protocol (DHCP) servers, Domain Name System (DNS) servers, file/print servers, software update servers as well as anti-virus update servers. The development network houses developer workstations and the software license server. Finally, the experimental network houses only developer workstations and possibly an instance of the software license server.

The JSimNet firewall provides protection and segregation to the JSimNet infrastructure and development networks. The JSimNet firewall permits workstations in the development network to access services within the infrastructure network servers and possibly services provided by DRDC Corporate servers such as email using DREnet approved access methods. The JSimNet firewall permits workstations in the development network to also access select Internet services such as the World Wide Web (WWW) and File Transfer Protocol (FTP).

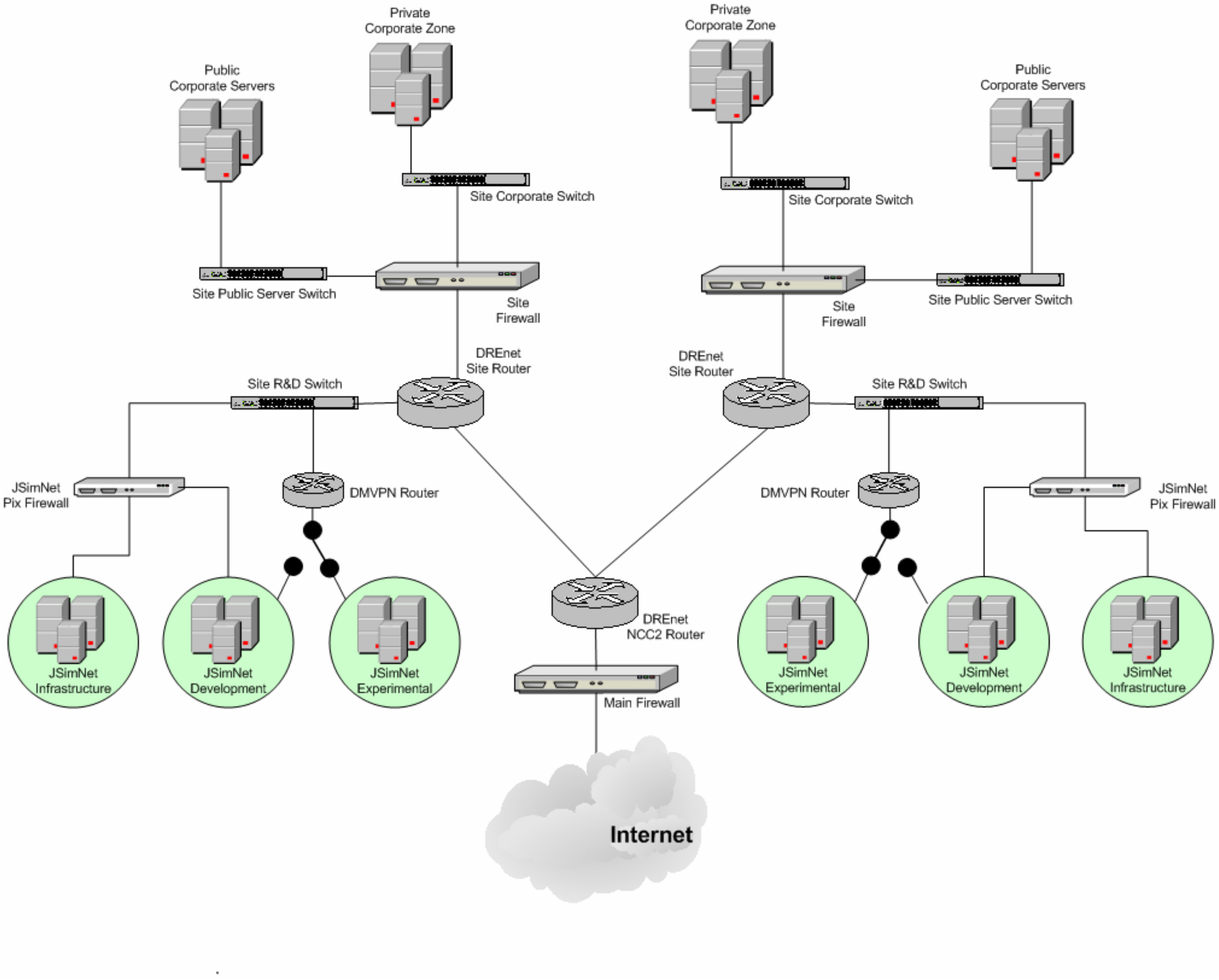


Figure 8 – Overview of JSimNet Spilt Environment

The DMVPN router provides private connectivity to the JSimNet experimental or development networks. FFSE researchers can undertake experiments involving a small number of workstations by connecting the participating workstations to the experimental network. For larger experiments that require participation from the majority of the development network systems, FFSE can instead connect the experimental network to the private network interface on the DMVPN router provided that FFSE first disconnects the development network from the JSimNet firewall.

The JSimNet experimental network and the JSimNet development network, when participating in experiments, must be isolated from the services provided by the JSimNet infrastructure network. This isolation presents numerous challenges that need to be further studied before practical solutions can be identified. They include host configuration, Windows domain logon and authentication, file access, software and anti-virus updates, and software license dissemination.

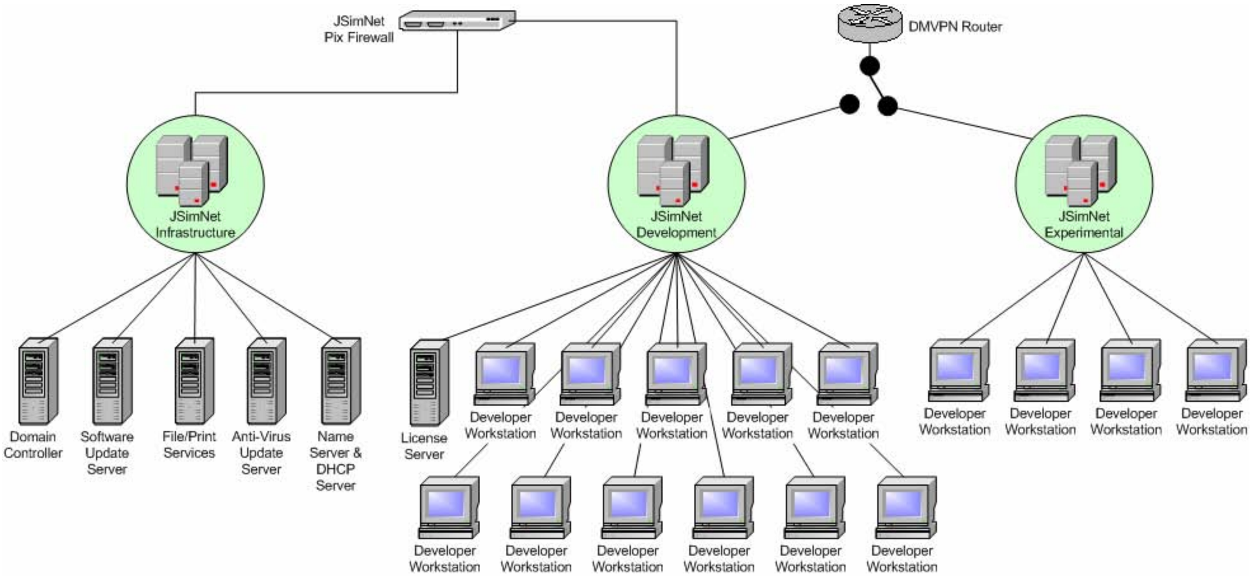


Figure 9 – Detailed View of JSimNet Spilt Environment

2.2.3.1 Movement of JSimNet Systems

The movement of systems between the development network and the experimental network must be achieved with care. We recommend that all systems must be fully patched and possess the latest anti-virus updates[4] prior to being connected to the segregated experimental network. This also applies to the development network when it is connected as a whole to the DMVPN router. These updates can be easily acquired from the software and anti-virus update servers within the JSimNet infrastructure network.

We also recommend that a system must obtain the latest software patches and anti-virus updates before the system can be moved from the experimental network to the development network. This also applies to all systems within the development network before the development network as a whole is disconnected from the DMVPN router and re-connected to the JSimNet firewall.

Unfortunately, the segregated experimental network does not include a source for software and anti-virus updates. We propose that an additional network interface be configured on the JSimNet firewall. This JSimNet firewall policy must only permit access to the software and anti-virus update servers from this additional firewall interface. Each development workstation must first connect to this additional JSimNet firewall interface and acquire its necessary updates[4]. Likewise, the development network must first be connected to this additional JSimNet firewall interface and each system must acquire its necessary updates

[4] Systems must be fully scanned after the anti-virus updates are applied.

before the development network can be re-connected to its primary JSimNet firewall interface.

We recommend that a Threat and Risk Assessment (TRA) be carried out to further consider the ramifications of moving systems between networks. We also recommend the compilation of detailed procedures to undertake the movement of these systems.

2.3 Video Conferencing

Problems have been encountered with enabling video conferencing between JSimNet and DRDC sites as well as other Internet sites. Video conferencing has worked erratically and, on some occasions, not at all. This is in the process of review and is most probably caused by the QoS configuration of new routers deployed in the past eight months. The DREnet Management Team has corrected the QoS configuration but FFSE have not yet tested video conferencing since the corrected QoS configuration was applied.

2.4 Video Conferencing Recommendations

We recommend that the FFSE work with the DREnet Management Team to re-test video conferencing in order to determine if the recent change to the QoS configuration has rectified the problem.

2.5 Development Tools

Problems have been encountered with enabling the CORE Enterprise development tool from JSimNet to the Valcartier site where the CORE Enterprise server resides. The DREnet Management Team has updated the QoS configuration and has determined that the lack of performance is no longer attributed to abnormal network latency. The CORE application appears to be a very network intensive application requiring a large number of interactions between the client and the server.

2.6 Development Tools Recommendations

We recommend that the FFSE engage the CORE Enterprise vendor, Vitech Corporation, to assist the FFSE and the DREnet Management Team in resolving the performance problems associated with the CORE Enterprise application.

2.7 Bandwidth

The DREnet does not possess sufficient bandwidth to support SE experimentation. This lack of bandwidth will be further felt in the future as FFSE conducts larger more complex experiments on a more frequent basis. DRDC Corporate examined the possibility of increasing bandwidth for the DREnet over a year ago. At that time the Telecom Services Renewal Project (TSRP) contractor expressed an informal opinion that multi-megabit extended LAN service could be acquired to interconnect DRDC sites.

DRDC Corporate is planning to increase bandwidth as part of the national DND telecom procurement project – Global Defence Network Services (GDNS). However, the Letter of Intent for the project was issued in Q4 2005 and the RFP will likely only be issued in 2Q 2006. We therefore consider it unlikely, for any DREnet bandwidth improvement via GDNS to happen in the near future and probably not until the next fiscal year (2007/2008).

Currently, the DREnet employs T1 time division multiplexed links to interconnect DREnet sites. These links offer a maximum bandwidth of 1.544 Mbps. If additional bandwidth is required, an additional physical T1 link must be acquired, installed and configured into the network. This process requires a minimum of 30 days to complete and requires a visit to the site by telecom provider technicians. Modern telecom service offerings such as Asynchronous Transfer Mode (ATM) or its derivatives such as extended LAN service include a high-speed access into the telecom provider's cloud, but provide a reduced utilization rate within the cloud based on customer requirements and the fees charged to the customer. If the customer needs to increase the utilization rate, the telecom provider simply adjusts configuration parameters within the cloud. There is no need to install additional physical hardware at the customer premises or to have telecom provider technicians visit the customer premises.

CFXNet appears to have sufficient bandwidth when no large scale experiments are scheduled. The CFXNet network infrastructure is based on modern ATM technology and as such additional bandwidth can be easily acquired if needed by FFSE to conduct SE experimentation.

FFSE has no control over bandwidth allocations within CA*net 4 or Internet. Partner organizations that connect to those networks will need to ensure that their network access possesses sufficient bandwidth for distributed simulation.

2.8 Bandwidth Recommendations

It is important that DREnet acquire modern telecom services at each DRDC research centre in order to facilitate increased bandwidth requirements driven by SE experiments.

We recommend that FFSE make their bandwidth requirements known to DRDC Corporate. Furthermore, it must be ensured that FFSE requirements are included as part of the GDNS requirements.

We further recommend that TDP's such as MALO pool their funds and attempt to undertake a modernization of DREnet telecom services as soon as possible to those DREnet sites that will participate in these TDP's.

2.9 Classified Domain

The DREnet is an unclassified DND network and is not accredited to process, transmit or store classified data. As such, the DREnet cannot be considered when dealing with SE experiments that require classified data. The only DND experimentation network capable of accommodating classified data is the CFXNet.

In the unclassified domain, we are proposing to establish closed network environments using commercial VPN technology. CFXNet achieves its caveat separation using military grade cryptographic devices. These devices are considered controlled goods and can only be obtained though well defined acquisition channels.

Typically the large-scale exercises that use CFXNet take three to four years to set up. This is acceptable for large international experiments/exercises but inconsistent with FFSE's need to quickly and effectively establish SE experiments in a relatively ad-hoc manner. Classified SE experiments must be planned long in advance.

CFXNet requires strict adherence to Government Security Policy (GSP) involving the completion of detailed request forms and their approval well in advance of any connection being allowed. This means a minimum of six to twelve months to set up use of CFXNet for a new project or new partner. Addition of a new node requires the full Certification and Accreditation process.

CFXNet Administration allows non-DND access, but requires DND sponsorship (FFSE/DRDC could be a sponsor). CFXNet does not have a direct Internet connection and is unlikely to for the next several months and probably not until the next fiscal year (2007/2008) due to staffing shortages.

We discussed the possibility of a cross-connection of CFXNet to DREnet but were informed that it will require full security restrictions as noted above.

2.10 Classified Domain Recommendations

CFXNet provides the only viable option to FFSE for conducting classified SE experiments. FFSE must approach CFXNet at least one year in advance of conducting its first classified SE experiment. FFSE must establish a classified "Distributed Environment" caveat within CFXNet at each participating DRDC or DND site. If non-DND organizations will participate in the classified SE experiment, FFSE must secure CFXNet sponsorship for those organizations. These classified JSimNet caveats must be certified and accredited to process classified data before FFSE can undertake classified SE experiments.

2.11 Classification of Data

The sensitivity of Synthetic Environment data must to be reviewed to take into account the following scenarios:

- When conducting, for instance, a major counter terrorism/emergency management exercise, what emergency management and security force elements are used and their tactical deployment would be of a considerable intelligence value to a terrorist organization.

Of further intelligence interest would be tactical and operational failures and successes as would the test or exercise scenarios themselves.

- Synthetic Environment testing of a weapons system shows its faults and tactical deployment which, once again, would be of considerable intelligence interest to a potential enemy and would enable them to develop measures to defeat the weapon system.

- Data held within the Modeling & Simulation Resources Repository could include weapon, weapon system and vehicle characteristics and, particularly, for new weapons and vehicles, could be of considerable intelligence value.

This type of data, particularly in aggregate, may be of more importance and at greater risk than is currently assumed.

2.12 Classification of Data Recommendations

We recommend that Statements of Sensitivity (SoS) and Threat and Risk Assessments (TRAs) be developed for the aggregate data for each individual project, including those that have already commenced. SoS and TRAs for existing projects should be developed as a matter of urgency.

We further recommend that if a new experiment differs substantially from those originally planned (i.e. when the original TRA was completed), that an updated TRA be required.

2.13 Monitoring

As FFSE relies, predominantly, on the security of its external partners (Universities and private enterprise) and the fact that protective firewalls must be configured to allow most traffic through to enable HLA communications, we have concerns regarding the possibility of compromise of the SE experimental network from partners SE systems or by FFSE SE systems.

Although the applications and databases within the FFSE segregated environment should be capable of being easily and rapidly reconstructed, we have concerns regarding the aggregate information and data accumulated during an experiment. Compromise of the segregated SE experimental network environment could cause the loss of this data and thus a total waste of the experiment.

2.14 Monitoring Recommendations

We recommend that FFSE should obtain and use, on a regular basis, Intrusion Detection (IDS) to detect attacks or compromises within the SE experimental network. The IDS is to be used to detect viruses, malware and worms within the segregated SE environment.

We recommend that Data Back-up and Recovery Procedures for FFSE be developed and that back-up be carried out on a regular and timely basis. It is important that all data generated and collected as part of an SE experiment be moved from the segregated SE experimental environment to the development or corporate environment as soon as an experiment is completed or more frequently in cases when experiments run for extended periods of time (days).

2.15 Patches and Virus Software

As we are recommending segregated networks for FFSE and for University and Private Sector partners, we have concerns regarding patches and upgrading virus protection software. Obviously, if the networks are segregated, upgrading patches and virus protection designation files could prove difficult to undertake. Nevertheless, such upgrades must be carried out in a timely fashion.

2.16 Patches and Virus Software Recommendations

As stated earlier, segregated SE experimental networks may only be connected to one network at a time –the segregated SE experimental network or the development or corporate network. We recommend that partners be permitted to disconnect from the SE segregated experimental network and connect to their respective corporate network to undertake patch updates and anti-virus updates. Each time a partner needs to connect or reconnect a system to the experimental segregated network, the system must first be subjected to software patch updates and anti-virus updates.

Although FFSE has no control over when these patch and virus protection updates are done, FFSE may notify its partners that, due to specific risks, such updates must be done at a given time.

2.17 Problem Handling

We have noted that problems that have occurred in the past were not well documented or relayed in a timely fashion. We have further noted that FFSE has no Problem Resolution Procedures in place.

2.18 Problem Handling Recommendations

We recommend that FFSE develop a Problem Resolution Procedure including, but not limited to:

- Documentation of all problems as they arise;

- Who to report to;
- Depending on the problem, what action to take;
- Documentation of solutions attempted;
- Final solution.
- Each step to show the person responsible, what they have done and the date of their action.

It must be ensured that problems that are not immediately resolved be followed up on a timely basis.

2.19 Memorandum of Understanding

Agreements with University/Private Sector and OGDs appear to be entered in to on an ad-hoc basis. We have noted, earlier, that in some cases, technical and network issues were only brought up when technical problems occurred. We therefore conclude that there is no governing framework for partnership agreements. It should be noted that FFSE can stipulate the level of security to be afforded to the information.

Agreements with other DND groups and OGDs are bound by GSP requirements and we can assume that they are providing adequate security for the level of data held and/or processed. Nonetheless, an agreement itemizing the conditions of the partnership and the respective involvements, technical and otherwise, would be indicated.

Agreements with Allied Nations are bound by Agreements for the protection of data between Canada and the Allied Country. Furthermore, we can assume that the Allied Nation provides adequate security for the information and data that it holds and/or processes. Nonetheless, an agreement itemizing the conditions of the partnership and the respective involvements, technical and otherwise, would be indicated, particularly as foreign nations will have different law structures.

These measures are for the protection of FFSE.

2.20 Memorandum of Understanding Recommendations

As there are differences in the relationships and security posture of FFSE’s different partners we are making three separate recommendations to cover each of the partner types.

We recommend that a Memorandum of Understanding (MOU), be developed for partnerships with Academia/private sector organizations. An MOU is a legal document and should be signed by both parties as a prelude to any connectivity activity. We have developed an MOU for Academic/Private Sector organizations and it is shown in Annex A.

We recommend that FFSE develop an MOU for partnerships with other DND groups and OGDs.

We recommend that FFSE develop MOU for partnerships with Allied Nations, particularly as they may not be bound by Canadian law without such an agreement.

3. Code of Best Practices: Recommendation & Timing of their Implementations

The recommendation shown in this section has all been made in the body of the previous section, Findings and Recommendation.

3.1 Recommendation Explanation

The following time ranges have been utilized in the production of this report:

- As soon as Possible - Within the next two weeks
- Immediate - within the next three months.
- Soon - within six months.
- Future - within one year, and
- When further developments make them appropriate.

3.2 As Soon As Possible Implementation

We recommend that a Threat and Risk Assessment (TRA) be carried out to further consider the ramifications of moving systems between the JSimNet experimental and development networks.

We also recommend the compilation of detailed procedures to undertake the movement of these systems.

3.3 Immediate Implementation

3.3.1 DMVPN

We recommend the acquisition of DMVPN capable Cisco routers with embedded firewall. The routers would be used as IPSec gateways as is currently the case with the PIX devices. These routers provide all the capability of existing PIX firewalls and would interoperate with existing PIX firewalls until the PIX firewalls can be phased out.

We also recommend that FFSE acquire a pool of identical DMVPN capable Cisco hardware and software and that FFSE compile detailed instructions for the required configuration changes when deploying a DMVPN spoke router. Moreover, we recommend that a maintenance contract be entered into to ensure access to software patches and updates.

3.3.2 Segregated SE Experimental Networks

Due to the impossibility of suitably firewalling HLA traffic caused by the continuous run-time allocation of ports, we recommend that University/Private Sector partners use a segregated network for SE traffic and experiments. Such a segregated network must be completely isolated from all other University/Private Sector partner networks and network activity.

This requirement should form part of a Memorandum of Understanding with the University/Private Sector partner. Figure 7 shows how such segregation could be accomplished.

3.3.3 Video Conferencing

We recommend that the FFSE work with the DREnet Management Team to re-test video conferencing in order to determine if the recent change to the QoS configuration has rectified the problem.

3.3.4 Development Tools

We recommend that the FFSE engage the CORE Enterprise vendor, Vitech Corporation, to assist the FFSE and the DREnet Management Team in resolving the performance problems associated with the CORE Enterprise application.

3.3.5 Bandwidth

It is important that DREnet acquire modern telecom services at each DRDC research centre in order to facilitate increased bandwidth requirements driven by SE experiments.

We recommend that FFSE make their bandwidth requirements known to DRDC Corporate. Furthermore, it must be ensured that FFSE requirements are included as part of the GDNS requirements.

3.3.6 Classification of Data

We recommend that Statements of Sensitivity (SoS) and Threat and Risk Assessments (TRAs) be developed for the aggregate data for each individual project, including those that have already commenced. SoS and TRAs for existing projects should be developed as a matter of urgency.

We further recommend that if a new experiment differs substantially from those originally planned (i.e. when the original TRA was completed), that an updated TRA be required.

3.3.7 Monitoring

We recommend that FFSE should obtain and use, on a regular basis, Intrusion Detection (IDS) to detect attacks or compromises within the SE experimental network. The IDS is to be used to detect viruses, malware and worms within the segregated SE experimental network environment.

We recommend that Data Back-up and Recovery Procedures for FFSE be developed and that back-up be carried out on a regular and timely basis. It is important that all data generated and collected as part of an SE experiment be moved from the segregated SE experimental environment to the development or corporate environment as soon as an experiment is completed or more frequently in cases when experiments run for extended periods of time (days).

3.3.8 Problem Handling

We recommend that FFSE develop a Problem Resolution Procedure including, but not limited to:

- Documentation of all problems as they arise;
- Who to report to;
- Depending on the problem, what action to take;
- Documentation of solutions attempted;
- Final solution.
- Each step to show the person responsible, what they have done and the date of their action.

It must be ensured that problems that are not immediately resolved be followed up on a timely basis.

3.3.9 Memorandum of Understanding

We recommend that a Memorandum of Understanding (MOU), be developed for partnerships with academia/private sector organizations. An MOU is a legal document and should be signed by both parties as a prelude to any connectivity activity. We have developed an MOU for Academic/Private Sector organizations and it is shown in Appendix C.

3.4 Soon Implementation

3.4.1 DMVPN

We recommend that FFSE experiment with DMVPN hub-to-spoke and spoke-to-spoke configurations and only migrate to DMVPN if DMVPN is found to be effective. If DMVPN is not found to be effective, continue using the routers for manually configured IPSec based VPN as is currently being done with the PIX firewalls.

3.4.2 JSimNet/Local Capability Segregation

We recommend that the JSimNet development network component be segregated from the JSimNet SE experimental network component and afforded some level of network security.

3.4.3 Bandwidth

We recommend that TDP’s such as MALO pool their funds and attempt to undertake a modernization of DREnet telecom services as soon as possible to those DREnet sites that will participate in these TDP’s.

3.4.4 Classified Domain

CFXNet provides the only viable option to FFSE for conducting classified SE experiments. FFSE must approach CFXNet at least one year in advance of conducting its first classified SE experiment. FFSE must establish a classified JSimNet caveat within CFXNet at each participating DRDC or DND site. If non-DND organizations will participate in the classified SE experiment, FFSE must secure CFXNet sponsorship for those organizations. These classified JSimNet caveats must be certified and accredited to process classified data before FFSE can undertake classified SE experiments.

3.4.5 Memorandum of Understanding

We recommend that FFSE develop an MOU for partnerships with other DND groups and OGDs.

3.5 Future Implementation

3.5.1 Memorandum of Understanding

We recommend that FFSE develop MOU for partnerships with Allied Nations, particularly as they may not be bound by Canadian law without such an agreement.

4. Assessment Methodology

When planning an SE experiment or exercise, there are key criteria to take into consideration.

4.1 Type of Experiment

Is it a full-scale exercise with multiple participants or a small scale test with few participants? Other considerations are the number of participants, their locations, the length of the experiment, etc.

4.2 Classification of Exercise

Whether the exercise is classified or unclassified will determine what networks are available. If the experiment is classified, the time to set up partners (assuming that they are approved) could take in excess of a year.

4.3 Type of Partner

There are several different types of partner and each has its own characteristics and any combination of them could be participants in an experiment.

1. Other DRDC locations
2. Other DND locations
3. OGDs
4. Universities
5. Private enterprise
6. Allied Governments

Has the partner signed an MOU with FFSE? This would ensure that the MOU conditions are met.

Is it necessary to negotiate an agreement with the partner? This may affect the way that the experiment is conducted and give connectivity problems if there is no agreement.

4.4 Connectivity

How does each partner connect to the SE environment? What network type will they use? This is out of FFSE’s control and is affected by what the partner is (DND, OGD, academia, etc.) and what networks are available to them.

Ease of connectivity is the critical factor. Our recommendations regarding the use of DMVPN and a pool of the same firewall/routers and software will make connectivity as seamless as possible. The recommendation for the segregation of a partner's networks will also ease this situation.

Problems will be encountered if a partner's network is protected by firewalls with robust rule sets since HLA allocates random ports at run-time. A robust rule set will block all ports that are not specifically allowed to be open. This must be taken into account when negotiating a new partnership. Our recommendation that each partner should establish an SE experimental network segregated from its corporate infrastructure will mitigate these concerns.

The requirement for delivery will influence the architecture of the SE experimental network. Although the CA*net supports multicast delivery and the DREnet could easily be configured to do so, the Internet generally does not provide a multicast delivery service. DMVPN does include multicast support in hub-to-spoke environments, but not in spoke-to-spoke environments.

The SE exercise partners must understand the flow of data associated with their applications. If each partner's SE systems communicate directly with most or all of the other partner SE systems, a DMVPN spoke-to-spoke environment may serve the SE exercise best. If the SE partner's SE systems primarily communicate with SE systems at the hub location, a DMVPN hub-to-spoke environment may serve the SE exercise best. The need for multicast will dictate a DMVPN hub-to-spoke environment, but all SE traffic will need to be relayed to the hub.

4.5 Bandwidth and Latency

FFSE needs to determine the maximum bandwidth and minimum network latency required for each experiment or exercise. Account must be taken of the bandwidth requirements of SE applications such as:

- Simulation
- Audio
- Video

Bandwidth depletion is a serious impediment to conducting successful SE exercises. We have made several recommendations regarding bandwidth and the use of other networks. Bandwidth associated with external partners that connect via the Internet or CA*net 4 is not under FFSE's control. FFSE, using project funds, may be able to augment bandwidth at DREnet and CFXNet locations. FFSE must drive the modernization of DREnet telecom services at each DRDC research centre in order to facilitate increased bandwidth requirements for SE experiments.

4.6 Security

Security is always a major consideration and care must be taken to ensure the proper separation and handling of classified and unclassified material. FFSE can impose its security requirements on partners but, conversely, OGDs and allied Governments can also, as a condition of sharing data, impose their security requirements on FFSE. These issues should form part of the project MOU.

Security within segregated SE experimental networks will rely on strong manual and administrative controls to ensure that patches and updates are done regularly and intrusion detection technology is used to monitor the SE experimental network.

4.7 Technical Characteristics of Simulation Software

There are several different simulation software packages being used. As long as the same packages and versions are used, FFSE should not encounter any difficulties.

However, Allied Nations, particularly, have strong preferences and in a multi-player situation, where partners are using different simulation software, we would expect communications and hand-shaking problems to occur.

For example, the MNE 4 exercise to be run on CFXNet in Ottawa has German, French and U.S participation (there is no direct Canadian participation) has each of the three participants using their own simulation software. As a result it has taken in excess of three years to set up this exercise.

4.8 Classification of Data

Care must be taken to correctly classify projects and then consider whether a prospective partner has a sufficient site security clearance to participate. Consideration must also be given to whether the employees/staff of the prospective partner are sufficiently security cleared and whether sufficient security protection (physical and technological) can be given, by the partner, to the aggregate data that they hold and/or process.

FFSE cannot assume that the aggregate data from a project is unclassified, simply because nobody has said that it should be classified. An SoS should be completed for each projects aggregate data and, if necessary, a TRA completed and, obviously, sufficient time for this must be allowed.

Taking this into account, FFSE will dictate the security requirements in an MOU for unclassified data. Classified data handling will be dictated by GSP and Unit Orders and must be subject to the C&A process.

4.9 Available Networks

Effectively there are only three networks available to FFSE for unclassified SE experimentation: DREnet, CA*net 4 and the Internet. We have not included CFXNet due to its restrictive policy. CFXNet however is the only option currently available to FFSE for conducting classified SE experimentation.

FFSE cannot simply choose a single network for a project. Reality is that partners will use whatever they can to connect and there is not a single network that can accommodate them all. There may be cases where none of the identified networks are considered suitable for interconnecting a DND organization that needs to participate in distributed simulation exercises. Instead a DND organization could potentially establish a connection to the nearest DREnet site using DND supplied communication facilities.

4.10 New Technology

Currently Canada, the United Kingdom, the United States of America and Australia are using HLA technology for simulation exercises and experiments. Some other NATO nations are still using the older DIS technology for their simulations.

We do not know what further advances in technology and standards will come in the future. FFSE must make itself aware of new technology and take it into consideration when planning projects and partnerships.

References

1. *Daniel Claude, Antoine Laydier, Jean-Eric Bohdanowicz* - Supervision Toolkit for distributed simulation and training infrastructures [01E-SIW-043]
2. *Richard Reading, Magnus Örnfelt, Dr. John M. Duncan, Ernst-Wichard Budde*- Results and Lessons Learned from a Multi-National HLA Federation Development Supporting Simulation Based Acquisition [02E-SIW—952] (2001)
3. *Science Applications International Corporation (SAIC) and Lockheed martin information Systems Company* – Advanced Distributed Simulation Technology II (ADST II) - High Level Architecture (HLA) Implementation for the MC-130E and MC-130H Combat Talons Final Report and Implementation Results [ADST-II-CDRL-MC130-2000071] (18th April 2000)
4. *Science Applications International Corporation (SAIC) and Lockheed martin information Systems Company* – Advanced Distributed Simulation Technology II (ADST II) - Synthetic Theater of War Architecture (Stow-A) Final Report [ADST-II-CDRL-HLAAPPS-2000085] (3rd April 2000)
5. *Douglas R. Hardy and Elaine C. Allen, Kevin P. Adams, Charles B. Peters, and Larry J. Peterson, Michael A. Cannon, Jeffrey S. Steinman, Bruce W. Walter* - Advanced Distributed Simulation: Decade in Review and Future Challenges [ADST-II-CDRL-STOWA99-9900318A] (18th January 2000)
6. *David A. Greschke, Dr. Stefano Cerutti* - Aircrew Mission Training via Distributed Simulation (MTDS) – Development of the Multi-Country Complex Synthetic Environment [RTO-MP-HFM-101] (October 2003)
7. *Peng Leong Seah, Wai Kong Chung* Architectures for device aware – Thesis [NSN 7540-01-280-5500] (March 2005)
8. *John Blacklock, Lucien Zalcman* - The Royal Australian Airforce, Virtual Air Environment, Interim Training Capability [DSTO-CR-0279] (April 2003)
9. *Luiz Felipe Perrone, Yougu Yuan, David M. Nicol* – Modeling and simulation best practices for wireless Ad Hoc networks (Winter Simulation Conference 2003)
10. Brainstorm - Informal meeting on Network infrastructure options for: 1) CFEC 2) DND SECO and 3) DREO FFSE [DND SECO] (6th February 2002)
11. *Kathryn Roose, Greg Tackett, James Van Bebber* – The calibration experiment network architecture [Technical report RD-SS-03-17] (July 2003)
12. *Gary Geling, Craig Williams, Myriam Guirguis*- D-SAFIRE: A Distributed Simulation DREO TM 2001-151, Defence Research Establishment Ottawa (December 2001)
13. *Dr. Harold W. Carter* - Development, Exploitation and Transition of Computer Aided Engineering (CAE) Tools [AFRL-IF-WP-TM-2004-1535] (June 2003)
14. *Gary Blank – CACI* – Distributed information enterprise modeling and simulation (DIEMS) [AFRL-IF-RS-TR-2004-299 Final Technical Report] (October 2004)
15. *Dhavy Gantsou* - Targeting Ada95/DSA for Distributed Simulation of Multiprotocol Communication Networks

16. *Ms Ebb Smith, BSc, Ms Heather McIntyre, MSc* Distributed Mission Training – How Distributed Should It Be? [NATO RTO-MP-HFM-101] (October 2003)
17. *Peter Clark, Peter Ryan, Lucien Zalcman* - Advanced Distributed Simulation for the Australian Defence Force [DSTO-GD-0255] (October 2000)
18. *Kai Harth* - Research on an Enabling Infrastructure for Distributed Simulation [Thesis – AFRL-SR-BL-TR-01-0386] (March 2001)
19. *W. H. (Dell) Lunceford* - FA 57_course_9June03_final Presentation (9th June 2003)
20. *Dr. Richard E. Hayes* - The Future of Military Modeling and Simulation As Seen Through the Eyes of the Military Operations Research Society Membership
21. *Richard Fujimoto, PhD, Peter Hoare, PhD, CEng* - HLA RTI Performance in High Speed LAN Environments [U.K.]
22. *Evidence Based Research, Inc.*- A human-centric architecture for net-centric operations - Final Report [CDRL 0001AC] (February 2005)
23. *Dennis M. Moen, J. Mark Pullen* - Enabling Real-Time Distributed Virtual Simulation over the Internet Using Host-based Overlay Multicast [Proceedings of the IEEE/ACM Distributed Simulation-Real Time Applications Symposium 2003]
24. *Shane A. Canney* - Constructing an Infrastructure to Facilitate Electronic Support Modelling in the Virtual Ship [DSTO-TR-1159] (May 2001)
25. *M. Pullen, M. Myjak, C. Bouwens* - Limitations of Internet Protocol Suite for Distributed Simulation in the Large Multicast Environment – Request for Comments [RFC 2502] (February 1999)
26. *David A. Greschke, Herbert H. Bell* – Training for dynamic aerospace control: an experiment in distributed training [AFRL-HE-AZ-TP-2003-0001] (February 2003)
27. *Maj. Darrell L. Wright, Jerry Black* - JADS Special Report on High Level Architecture [JADS JT&E-TR-00-024] (January 2000)
28. Joint Synthetic BattleSpace – Presentation (June 2001)
29. Joint interoperability and certification process (February 2004)
30. Joint Interoperability Test Command (October 2005)
31. *Kevin C. Trott - Northrop Grumman Mission Systems* - Joint synthetic battlespace for research and development [AFRL-IF-RS-TR-2005-177 Final Technical Report] (May 2005)
32. Joint synthetic battlespace: applying simulation to acquisition, mission effectiveness and course of action analysis - Presentation
33. *B. Kim, B. Johnson, R. Youssef, A.L. Vallerand, C. Herdman, M. Gamble, R. Lavoie, D. Kurts, K. Gladstone* - JSMARTS Initiative: Advanced Distributed Simulation across the Government of Canada, Academia and Industry, - Technical Description [DRDC Ottawa TM 2005-101] Defence R&D Canada – Ottawa (July 2005)
34. *Dr. Jack P. Landoit, John R. Evans* – R&D initiatives in modeling and simulation for capability modernization of the Canadian Air Force (Spring 2001 – Canadian Military Journal)
35. *Max Lorenzo* - MATREX Approach to Scaling – Presentation (8th September 2003)
36. *J. Mark Pullen* - Final Technical Report – Multicasting Networks for Distributed Simulation [ARO 34631.1-RT-AAS] (April 2001)
37. *Paul Labbé (P. Engineer), Zakaria Maamar (Ph. D.), Elkadhi Abdelhamid (MSc.), Bernard Moulin (Ph. D.), René Proulx (Senior Analyst), David Demers (Scientist*) - Recommendations for Network- and Internet-based Synchronized E-activities for Location- and Time-dependent Information

38. *Doug Perrault* - Review of Architectures for Simulation of Virtual Naval Platforms [DRDC Atlantic TM 2003-193] Defence R&D Canada - Atlantic (September 2003)

39. *Shunra Software Ltd.* – Recreate any production network environment - Presentation

40. *Bruno R. Preiss, Wayne M. Loucks* - Prediction and Lookahead in Distributed Simulation (1989)

41. *Gregory B. Tackett, Timothy McKelvy* - RDE Command First Application Simulation Experiment For Future Combat Systems (FCS) Networked Fires [Technical Report AMR-SS-04-14] (June 2004)

42. *Robert C. Cooper* – Remote application support in a multi level environment [Thesis NSN-7540-01-280-5500] (March 2005)

43. *Capt. Sandra J. Smith, Capt, Roman Nation, Maj. Darrrell L. Wright* - Statistical Techniques for Determining the Repeatability of Man-In-The-Loop System performance Data [AOI00-09-2797]

44. *Blane T. Shearon* – The cost effectiveness of West Coast distributed simulation training for the Pacific fleet [Thesis] (December 2001)

45. *Dolphin Technology, Incorporated* – Security enhanced multi-domain network management for Joint Warrior Interoperability Demonstration (JWID) [AFRL-IF-RS-TR-2005-86 Final Technical Report] (March 2005)

46. *R.J. Allan and M. Ashworth* - A Survey of Distributed Computing, Computational Grid, Meta-computing and Network Information Tools

47. *Dave Rowe, CAE Ltd* - NATO Research & Technology Organisation - Test Federate Handbook v 3.0 [SAS-034/MSG-001] (October 2004)

48. *Mark A. Thomas* - The U. S. Army Research Laboratory Dynamic Terrain Server [ARL-TR-962] (April 2003)

49. Phase I Verification and Validation Report for the End-To-End Test [AOI00-11-3732]

50. *LT Joseph Cohn, PhD, LCDR Dylan Schmorrow, PhD, Dr. Denise Lyons, Dr. James Templeman, Peter Muller* - Virtual Technologies and Environments for Expeditionary Warfare Training [RTO-MP-HFM-101: Paper 2] (April 2004)

51. *Katherine L. Morse, Ph.D., David L. Drake, Ryan P.Z. Brunton* - Web Enabling HLA Compliant Simulations to Support Network Centric Applications

52. CAS - Modeling and Simulation – Portion of Document

53. *Maj. Don Messier* - Classified Network Systems Overview – Presentation

54. *Jean-Baptiste Guillerit, Marco Fabbri, Curzio Batini* - EUCLID RTP 11.13 - Realising the Potential of Networked Simulations in Europe – Method for Characterising Repository Assets [RTP11.13-TT&S SA-WE3.1-TN3.1c] (2nd May 2002)

55. *Mark D. Nelson* – Integrated network application management (INAM) [Thesis] (December 2004)

56. Information Brief War-In-A-Box

57. Draft – WIB Maritime Scenario Specification (22nd September 2003)

58. *Maj. H. G. Wiegand* - Canadian Forces Experimentation Network (CFXNET) “Future Strategy” Presentation (2005)

59. *D. Skinner, A.L. Vallerand* - Connections to the JSimNet: Connecting From Non-DRDC Sites [DRDC Ottawa TN 2005-127] Defence R&D Canada – Ottawa. (April 2005) Internal publication

60. *David Skinner, Andrew L. Vallerand* - SIMNET Security Plan: Connections to the JSimNet From DRDC Sites Version 1.0 (29th March 2004)

61. *Dr. Andrew Vallerand* - Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks - STATEMENT OF WORK (March 2006)

62. Fragment of a Document – Infrastructure

63. *Marcel J.A. Thompson, CD, MBA, PEng* - Joint Simulation Network (JSimNet) and Modeling & Simulation Resources Repository Network (MSRRNet) Descriptions and Roles, and their Interactions [JSimNet/MSRRNet] (1st October 2002)

64. JSIMNET status report

65. *Dr. Andrew L. Vallerand* - JSMARTS Exercise Phase II Distributed SE Experiment – Presentation

66. *Dr. A. L. Vallerand, Dr. F. Hassaine, Dr. P. Hubbard* - Maritime Air Littoral Operation – Presentation (September 2005)

67. *D. Skinner and A.L. Vallerand* - Way ahead for FFSE network enabled capabilities: Collaborative Synthetic Environment and Collaborative Capability Engineering Environments [DRDC Ottawa TN 2005-059] Defence R&D Canada – Ottawa (April 2005) Internal publication

68. *David Skinner, Andrew L. Vallerand* - JSIMNET Security Plan: Connections to the JSimNet From non-DRDC Sites Version 2.0 (April 2005)

69. *Dr. Paul Hubbard* - RAVEN Project (January 2005)

70. *Murray G. Gamble* - Cookbook to Adapting Simulations for the High Level Architecture [CFEC 2002-101] (25th March 2002)

71. *Richard G. Brown, M. Fujimoto, and Fawzi Hassaïne* - A Vision for M&S Processes, Tools, and Standards for CapDEM An Update by the Integrated Synthetic Environment Work Stream of CapDEM [DRDC Ottawa TM 2004-133] Defence R&D Canada - Ottawa (April 2004)

72. *A.L. Vallerand and M. Thompson* - Network-Centric Synthetic Environments: A Modular Modeling & Simulation/Synthetic Environment (M&S/SE) Framework [DRDC Ottawa TM 2004-221] Defence R&D Canada – Ottawa (November 2004)

73. *B. Kim, B. Johnson, R. Youssef, A.L. Vallerand, C. Herdman, M. Gamble, R. Lavoie, D. Kurts, K. Gladstone* - JSMARTS Initiative: Advanced Distributed Simulation across the Government of Canada, Academia and Industry – Technical Description [DRDC Ottawa TM 2005-101] Defence R&D Canada – Ottawa (July 2005)

74. *Arnold Buss, Leroy Jackson* – Distributed simulation modeling: a comparison of HLA, CORBA, AND RMI [Proceedings of the 1998 Winter Simulation Conference]

75. *Alion Science and Technology, AEgis Technologies Group, Inc., Carnegie Mellon University Software Engineering Institute, Johns Hopkins University Applied Physics Laboratory, Science Applications International Corporation*`- Transition of the DoD High Level Architecture TO IEEE STANDARD 1516 (21st October 2005)

76. *Judith S. Dahmann, Richard M. Fujimoto, Richard M. Weatherley* - The DoD High Level Architecture: An Update [Proceedings of the 1998 Winter Simulation Conference]

77. IEEE P1516/D1 - Draft Standard [for] Modeling and Simulation (M&S) - High Level Architecture (HLA) – Framework and Rules

78. *José Sepúlveda, Luis Rabelo, Jaebok Park, Frank Riddick* – Implementing the high level architecture in the virtual test bed [Proceedings of the 2004 Winter Simulation Conference]

79. The High Level Architecture - Presentation

80. Martin Adelantado, Stephane Bonnet, Pierre Siron - Multiresolution Modeling and Simulation with the High Level Architecture

81. *Michael R. Reid* - An Evaluation of The High Level Architecture (HLA) as a Framework for NASA Modeling and Simulation [Presented at the 25th NASA Software Engineering Workshop, Goddard Space Flight Center, Greenbelt, Maryland, November 30, 2000.]

82. *Ulrich Klein, Thomas Schulze, Steffen Straßburger, Hans-Peter Menzler* – Traffic simulation based on the high level architecture [Proceedings of the 1998 Winter Simulation Conference]

83. *Ernest H. Page, Roger Smith* - Introduction to military training simulation: a gide for discrete event simulationists [Proceeding of the 1998 Winter Simulation Conference]

84. *Katia Sycara, Gita Sukthankar, Anupriya Ankolekar* - Agent-based Composition of Behavior Models –Presentation (2nd October 2002)

85. *Nacer Adbellaoui, Paul Hubbard, Oliver Schoenborn* - Evolution of the Synthetic Environment in the FFSE Section - Survey of Current Usage of Synthetic Environment within FFSE and Recommendations for the Future [DRDC Ottawa TM 2005-141] Defence R&D Canada - Ottawa (November 2005)

86. *Krzysztof Walczak, Wojciech Wiza* - Meta-VR: A Dynamic Approach to Building Interactive - 3D Web Applications

87. *Cisco Systems Inc.* − DMVPN and Easy VPN Server with ISAKMP Profiles Configuration Example

88. *Cisco Systems Inc.* − Dynamic Multipoint VPN (DMVPN)

89. *Cisco Systems Inc.* − Dynamic Multipoint VPN HUB and SPOKE introduction– Presentation (November 2004)

90. *Cisco Systems Inc.* − Dynamic Multipoint VPN SPOKE TO SPOKE direct tunneling – Presentation (November 2004)

91. *Cisco Systems Inc.* − Introduction to Dynamic Multipoint VPN Presentation (November 2004)

92. *Stewart Robinson* – Modes of simulation practice in business and the military [Proceedings of the 2001 Winter Simulation Conference)

93. Department of Defense – Modeling and Simulation (M&S) master plan [DoD 5000 59-P] (October 1995)

94. DoD - High Level Architecture Federation Development and Execution Process (FEDEP) Checklists (December 1999)

95. DoD - High Level Architecture Federation Development and Execution Process (FEDEP) Model (8th December 1999)

96. DoD - High Level Architecture Federation Security Process Version 1.2 (16th February 2001)

97. DoD Interpretations of the High Level Architecture Interface Specification, Version 1.3: Release 3

98. DoD Interpretations of the IEEE 1516-2000 series of standards, IEEE Std 1516-2000, IEEE Std 1516.1-2000, and IEEE Std 1516.2-2000: Release 1 (7th March 2003)

99. DoD Interpretations of the IEEE 1516-2000 series of standards, IEEE Std 1516-2000, IEEE Std 1516.1-2000, and IEEE Std 1516.2-2000: Release 2 (1st July 2003)

100. DoD – Code of best practice experimentation (July 2002)

101. *Nathalie Harrison, Bruno Gilbert, Marc Lauzon, Alfred Jeffrey, Claire Lalancette, Dr Richard Lestage, André Morin* - A M&S Process to Achieve Reusability and Interoperability [RTO-MP-094] (November 2003)

102. Student Guide – Introduction to HLA: Hands-On Tutorial (July 2004)

103. *Michael Imbrogno, Wayne Robbins and Gerard Pieris* - Selecting a HLA Run-Time Infrastructure: Overview of Critical Issues Affecting the Decision Process for War-in-a-Box [DRDC Ottawa TM 2004-111] Defence R&D Canada – Ottawa (July 2004)

ANNEX A : MEMORANDUM OF UNDERSTANDING

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FUTURE FORCES SYNTHETIC ENVIRONMENT SECTION
(HEREINAFTER REFERED TO AS “FFSE)

OF

DEFENCE RESEARCH AND DEVELOPMENT, CANADA
(HEREINAFTER REFERED TO AS “DRDC)

OF

THE DEPARTMENT OF NATIONAL DEFENCE (OF CANADA)
(HEREINAFTER REFERED TO AS “DND”)

AND

XXXX UNIVERSITY or YYYYY COMPANY
(HEREINAFTER REFERED TO AS “THE UNIVERSITY’ OR “THE COMPANY”

1. INTRODUCTION

The Department of National Defence (DND) has adopted the strategy of a Capability-based Canadian Forces; "To have a capability means to have the ability to act in a specific way in a specific situation." This strategy is extended to include a Joint Capability requirement, where the Canadian Forces must ensure interoperability with other allied forces with respect to operations and doctrine.

To fulfill this new direction, the Future Forces Synthetic Environments (FFSE) Section was officially created in June 2001. FFSE's mandate is to carry out experimentation, analysis and demonstration of Modeling and Simulation enablers for the development of future concepts and capabilities.

2. PURPOSE

This Memorandum of Understanding (MOU) between FFSE and (University/Company name) is for the purpose of establishing a secure link between FFSE, (University/Company name) and any other third party participants for the electronic transfer of Synthetic Environment Experimental information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU summarizes the information system (IS) security requirements for approval purposes and supplements the (University/Company Name) approved system security policies and procedures.

3. LEGAL

3.1 The Participants concur that they will fully respect the scope, intent and meaning of all sections of this MOU.

3.2 The Participants acknowledge that notwithstanding any wording used in this MOU, neither the MOU as a whole nor any of its parts taken separately are, or ever have been, intended to be a contract or be contractual in nature.

3.3 For purposes of this MOU, any reference to FFSE, DRDC or DND is a reference to the Crown.

3.4 This MOU in no way restricts either of the parties from participating in any activity with other public or private agencies, organizations, or individuals.

4. AGREEMENT INFORMATION

This MOU describes the restricted network arrangement between FFSE and (University/Company name) in support of the selected Synthetic Environment Experiments sponsored by FFSE.

The following (University/Company name) key points of contact are identified:

TITLE	NAME	TELEPHONE NUMBER
Security Officer		
IT/Network Manager		
Experiment Contact Person		
Technical Contact Person		
Other Contact Person (show title)		

At FFSE direction, (University/Company Name) is establishing a remote access capability to the JSIMNet with a remote access network located at (University/Company). This capability will allow selected (University/Company name) personnel to access the JSIMNet for the purpose of participating in Synthetic Environment Experiments as remote users.

5. TERM OF AGREEMENT

This Agreement shall remain in force for a period of (days/months/years) from the date of signature.

The Agreement is only valid during the period that experiments are being prepared for or carried out and the connection with JSIMNet will be terminated on completion of the experiment.

FFSE reserves the right to remove the firewall/router supplied to (University/Company name) at any time.

Furthermore, FFSE reserves the right to terminate this Agreement at any time.

Prior to connecting to the JSIMNet, (University/Company name) will ensure that all systems in the (University/Company name) segregated Synthetic Environment network:

1. must be fully patched using up-to-date patches;
2. must be protected by up-to-date antivirus protection;
3. will not be used for any purpose not associated with the simulation activity;

4. must include access controls: username/password;
5. will only be accessed by authorized users;
6. systems will only connect to a single network at any given time.

The network (firewall/router), supplied by FFSE, will only be connected to the Internet when needed, at the direction of FFSE. This allows FFSE to leave an installation in place for protracted periods, but only allow the network to be enabled when required.

Both FFSE and its partners, prior to implementing patches or upgrading virus protection software, change the network setting so that they are disconnected from the rest of the SE network and connected to their respective corporate networks to make the necessary upgrades. The network settings will be changed back to the SE once the upgrades are completed.

FFSE reserve the right to carry out au audit of the connection between JSIMNet and (University/Company name) as well as the segregated Simulated Environment network at (University/Company name) location.

6. DESCRIPTION

(University/Company Name) operates a segregated Synthetic Environment Experiment network which is UNCLASSIFIED, whereby all users have the required clearance and need to know for all information on the system. All personnel with access to the segregated Synthetic Environment Experiment network will read the MOU and agree to the terms and conditions of the MOU.

The (University/Company Name) IS will be connected to the JSIMNet at FFSE by an Internet based Virtual Private Network (VPN) communications channel for the transfer of data. The VPN will be protected at each end by a firewall and or router, supplied and configured by FFSE.

7. NETWORK REQUIREMENTS

The (University/Company name) will ensure that the Synthetic Environment Experiment network that is to be connected to FFSE’s JSIMNet will be separate and segregated from their other networks. See APPENDIX A, for a network diagram.

(University/Company name) will not make any changes to the configuration of any firewalls or routers supplied to them by FFSE unless directed to do so by FFSE.

8. APPROVAL

The communication link between FFSE and (University/Company Name) shall not be initialized until approval of these procedures is indicated by signature below.

(University/Company Name) FFSE)

____

____

Name of Management Official) Name of Security Official

____

____

Title Title

________________ ________________

Date of Signature Date of Signature

(University/Company Name)

____

Name of Security Officer

____

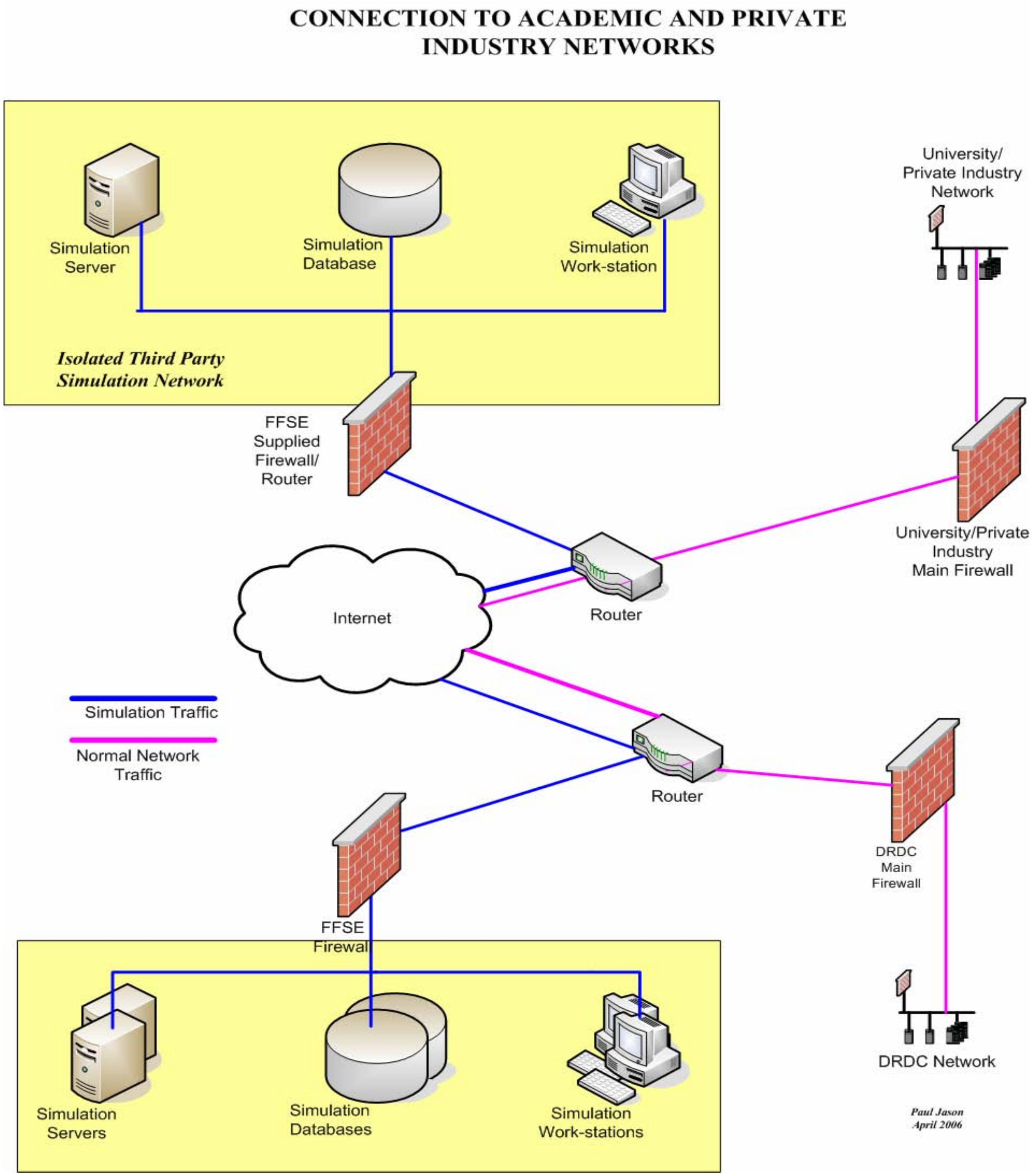
____

Title Title

________________ ________________

Date of Signature Date of Signature

ANNEX B: EXAMPLE OF NETWORK DIAGRAM



ANNEX C: FIREWALL/ROUTER CONFIGURATION DETAILS

Firewall/Router Configuration

When configuring a VPN, both parties require the same information that describes the other partner's network environments. A summarized version of this information follows:

1) The tunnel endpoint (the public IP address) of the VPN device.
2) Private Network(s) participating in the distributed communication
3) Protocol requirements for the distributed simulation communication. It is assumed that all IP traffic (TCP, UDP and ICMP) would be allowed between the hosts/networks involved.
4) Phase 1 Encryption Algorithm
5) Phase 1 Hash Algorithm
6) Phase 1 Diffie-Hellman Group Identifier
7) Phase 1 Security Association Lifetime
8) Phase 1 Identity
9) Phase 1 Shared Secret Key
10) Phase 2 Transform Set which includes the encryption and hash algorithms for subsequent data exchange.

If FFSE assumes the responsibility for configuring a partner's firewall/VPN device, the partner must provide additional information to FFSE as follows:

1) Public IP address and network mask of the firewall/VPN device.
2) Public default route for the firewall/VPN device.
3) Private IP address and network mask of the firewall/VPN device.
4) One Spare IP address from the private network to allow remote management of the partner firewall/VPN device.

List of symbols/abbreviations/acronyms/initialisms

CA*net4	Current CANARIE Network
CANARIE	Canadian Network for the Advancement of Research, Industry and Education
CapDem	Collaborative Capability Definition, Engineering and Management
CASE	Canadian Advanced Synthetic Environment
CDE	concept development and experimentation
CFBLNet	Combined Federated Battle Lab Network
CFEC	Canadian Forces Experimentation Centre
CFMWC	Canadian Forces Maritime Warfare Centre
CFXNet	Canadian Forces Experimentation Network
CIFS	Common Internet File System
CRC	Communications Research Centre
DHCP	Dynamic Host Configuration Protocol
DIS	Distributed Interactive Simulation
DMVPN	Dynamic Multipoint Virtual Private Network
DND	Department of National Defence
DND/SECO	DND Synthetic Environments Coordination Office
DNS	Domain Name System
DRDC	Defence Research and Development Canada
DREnet	Defence Research Establishment Network
DS	Defence Scientific Synthetic
DSL	Digital Subscriber Line
DWAN	Defence Wide Area Network
FFSE	Future Forces Synthetic Environment
FNSM	Functional Network System Manager
FOM	Federation Object Models
FTP	File Transfer Protocol
gbps	gigabytes per second
GDNS	Global Defence Network Services
GRE	Generic Routing Encapsulation
GoC	Government of Canada
GSP	Government Security Policy
HLA	High Level Architecture
IEEE	Institute of Electrical and Electronics Engineers
IDS	Intrusion Detection Software

IPsec	Internet Protocol Security
ISP	Internet Service Provider
JSimNet	Joint Simulation Network
JSMARTS	Joint Simulation Modelling for Materiel Acquisition Requirements, Training and Support
JSMARRT	Joint Simulation and Modelling for Acquisition, Requirements, Rehearsal and Training
MALO	Maritime Air Littoral Ops
MOU	Memorandum of Understanding
M&S/SE	Modeling and Simulation/Synthetic Environments
MSSRNet	Modeling & Simulation Resources Repository Network
NHRP	Next Hop Resolution Protocol
NFS	Network File System
NOS	Network Operating System
OGDs	Other Government Departments
POP	Point-of-Presence
RFP	Request for Proposal
SE	Synthetic Environment
SEB	Synthetic Environments Battlelab
SOM	Simulation Object Models
SoS	Statement of Sensitivity
TDP	Technology Demonstration Project
TSRP	Telecom Services Renewal Project
TRA	Threat and Risk Assessment
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WWW	World Wide Web

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario
K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Seamless Persistent National Connectivity: Code of Best Practice for Distributed Simulation Networks (U)

4. AUTHORS (Last name, first name, middle initial)

Rafei, Nabil and Vallerand, Andrew L.

5. DATE OF PUBLICATION (month and year of publication of document)

November 2006

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

64

6b. NO. OF REFS (total cited in document)

103

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

DRDC Ottawa

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

13DJ01

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC Ottawa TM 2006-269

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
(   ) Distribution limited to defence departments and defence contractors; further distribution only as approved
(   ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
(   ) Distribution limited to government departments and agencies; further distribution only as approved
(   ) Distribution limited to defence departments; further distribution only as approved
(   ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unlimited

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

The DRDC Ottawa Future Forces Synthetic Environments section (FFSE) is an R&D centre of excellence in the area of Science and Technology for distributed Synthetic Environments (SE), distributed Capability Management as well as Distributed Collaborative Environments (collectively they can be referred to as Distributed Environments, for simplicity).

The use of Distributed Environments for experimentation across Governments, Industry, Academia and Allies is becoming increasingly prevalent, particularly with the adoption of International Standards such as the Institute of Electrical and Electronic Engineers (IEEE) 1278 Distributed Interactive Simulation (DIS) protocol as well as the IEEE 1516 (and the HLA 1.3 Baseline) High Level Architecture (HLA) protocol for distributed simulation and IEEE 1220 and 1362 for System Engineering. In a recent Case Studies, for example, DRDC Ottawa, with the support of DRDC Corporate, used an unclassified, non-dedicated, through VPN-Protected network, to perform distributed simulation across the Government of Canada, Industry (the private sector) and Academia using a military scenario in a "JSMARRT 1" experiment in just a few weeks (Vallerand et al, 2004). This success was followed up in another Experiment using this time a National Security Scenario where DND's Capabilities were required by Public Security Partners with the Threat of a simulated "dirty bomb" around Parliament Hill. This "JSMARRT 2" Experiment was performed in January 2006. Though, both experiments were eventually performed with some agility, the overhead in time and effort to have access to national connectivity was still way too high to be called seamless and persistent. For all partners involved.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Distributed Simulation
Synthetic Environment
Collaborative Environment
Capability Engineering
Modelling and Simulation
Seamless networking
Persistent connection
Experimentation
VPN
Multicast
DMVPN
Public network

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca