NCOIC Lab Interoperability Project:
A Method for Connecting Distributed Labs

October 28, 2010
Version: 1.5
Abstract

Joint activities between Government and Industry or between Industry partners often require connecting distributed labs, a process that is often time consuming and costly. This paper presents a method for connecting distributed labs based on the experiences of members companies on the Net Centric Operations Industry Consortium (NCOIC) Lab Interoperability project. It discusses both policy related items such as protecting Corporate Intellectual Property (IP) and International Traffic in Arms Regulations (ITAR) concerns as well as technology practices for network security, data interoperability and network delivered services.
Abstract............................................................................................................................................2

1 Project Introduction..................................................................................................................................................5
  1.1 Challenges in Connecting Distributed Labs...........................................................................................................5

2 Project Overview ....................................................................................................................................................7
  Project Participants ..................................................................................................................................................8

3 Design Approach ..................................................................................................................................................11
  Constraints .............................................................................................................................................................11
  3.1 Technology Approach...........................................................................................................................................12
  3.2 Networking..........................................................................................................................................................12
    3.2.1 Topology Integration ........................................................................................................................................13
    3.2.2 Wide-Area Network Transport Approach .....................................................................................................13
    3.2.3 Tunneling, Security, & Routing Approach ..................................................................................................14
    3.2.4 Tunneling .......................................................................................................................................................14
    3.2.5 Network Security ...........................................................................................................................................14
    3.2.6 Routing..........................................................................................................................................................16
  3.3 Video.................................................................................................................................................................16
  3.4 Data Interoperability..........................................................................................................................................16
  3.5 Network Delivered Services – Cloud Computing..............................................................................................17
    3.5.1 Network Delivered Service Experiments ....................................................................................................18
    3.5.2 Cloud Computing Design ..........................................................................................................................20

4 Policy Approach..................................................................................................................................................23
  4.1 Export / ITAR ......................................................................................................................................................23

5 Demonstrations ..................................................................................................................................................24
1 Project Introduction

In 2007, member companies in the NCOIC expressed an interest in having a common approach for connecting industry and customer laboratory networks. The limitations of the current approach within industry are the time and cost required to develop interconnectivity that enables a demonstration, experiment, or test to take place. The resulting business need is to develop a common approach and applicable pattern that enables industry to rapidly assemble a lab infrastructure environment, thereby lowering time to market and cost and reducing technical process and ITAR risks. It is an inherent belief by all communities that the infrastructure should have a common set of assembly parameters. As a result of these requirements, an NCOIC working group, the Lab Interoperability Working Group, was formed with the goal of identifying a repeatable, scalable, process and technology for enabling lab interoperability at the infrastructure level.

The Lab Interoperability project was executed in multiple phases in order to focus on a set of activities and deliverables that can be made available to the NCOIC community. Phase-I focused on Level 1, the Network Infrastructure, and Level 2, the Visualization and Presentation capability, also described as the Audio/Video (A/V) component capabilities. Phase-II incorporated Level 3, the Middleware, and explored network-delivered services and data interoperability. The result of the project phases will provide a pattern and set of lessons learned across industry in order to create a common pattern for the interconnection of labs. It is envisioned that this pattern will be adopted into the internal policies of member companies and be recognized by their customers, thus speeding up the time required for future collaborative work.

1.1 Challenges in Connecting Distributed Labs

The Lab Interoperability project was initiated by the NCOIC to address the challenges faced in developing joint collaboration activities requiring distributed lab connectivity among government and industry. These challenges can be technical, business, and policy in nature and can often have significant impacts to cost, time to implement, and overall risk to successful event production. Recent data indicated that a common method for distributed lab interoperability did not exist and that a typical four company event could take up to six months to implement at a cost of up to US $300,000 per company. These factors, combined with the inherent risks associated with a developing a multi-company, distributed environment without a common approach, led the NCOIC to charter an effort to develop a common method for lab interoperability.

The project had to address internal company concerns about exposure and loss of intellectual property. To avoid possible exposure of proprietary data, the project scope dealt strictly with connectivity that is considered outside the firewall perimeters of participating companies. Given the international nature of potential collaborative efforts, export compliance regulations had to be accommodated in the design, due to the potential for multi-company, multi-national collaborative environments. In addition, the technical approach was designed
to utilize protocols and processes considered to be in the public domain and to incorporate commercially available hardware so as not to violate any export or ITAR-related specifications.

There are numerous technical challenges associated with developing and implementing a common approach for distributed lab interoperability. The design must be scalable, repeatable and able to accommodate short lead-time activities such as first responder environments and mobile ad-hoc networks. In addition, the common infrastructure must be secured in order to maintain data integrity, as well as to prevent the loss of Intellectual Property within the common environment. In cases where the network security policies vary among companies, these policies must be aligned in order to provide adequate data security while also meeting the internal policies of the participants.

Additional challenges in the area of data interoperability are also prevalent in international, multi-company environments. It is not uncommon for companies to utilize different data protocols, hardware and software components, and product solutions to solve similar problem statements. For example, in a distributed modeling and simulation environment, one company may incorporate the Distributed Interactive Simulation (DIS) protocol, while another may use the Cursor on Target (CoT) protocol to provide the same simulation entities. In such a case, data interoperability methods would need to be incorporated in order to ensure application layer compatibility within the common environment. Similarly, environmental setup issues such as in-the-field locations, time zone variances, and language barriers must be accommodated to facilitate a successful interoperability approach.
2 Project Overview

The lab Interoperability Project was conducted in two Phases. Phase-I focused on the technologies and processes at the infrastructure level, i.e. Levels 1 and 2, as shown in the Interoperability Matrix in Figure 1 below. In Phase-I, these levels dealt primarily with the implementation of the global network infrastructure and the integration of selected A/V component capabilities.

![Interoperability Matrix](image)

**Figure 1. NCOIC Interoperability Matrix**

The Interoperability Matrix shown above is a consolidation of the Open System Interconnection (OSI) model which depicts the relationship of conceptually similar communications functions that provide services to the layer above it and receives services from the layer below it. The comparison of the Interoperability Matrix and the OSI reference model is shown in Figure 2 below.

![Interoperability Matrix compared with the OSI model](image)

**Figure 2. Interoperability Matrix compared with the OSI model**
Phase-II of the Lab Interoperability Project focused on products and processes defined at Level 3, the Core Middleware, and included areas of data interoperability and network delivered services. Level 4, the application layer, is where most member company proprietary assets or IP would exist and was therefore categorized as out of scope for this project working group.

Project Participants

The following NCOIC Member Companies participated in one or more phases of the project:

- Raytheon
- Lockheed Martin
- IBM
- Thales
- Selex-SI, a Finmeccanica company
- Boeing
- EADS
- Cisco

With the exception of Cisco, each member company provided network connectivity to and from the global laboratory locations. Figure 3 depicts the participants and locations from Phase I. Phase II participants and locations are given in Figure 4.
Figure 3. Phase I Participants and Locations
Figure 4. Phase II Participants and Locations
3 Design Approach

Constraints

In establishing the charter for the Lab Interoperability Project, the NCOIC Executive Operations committee defined the request for an infrastructure capability that is not competitive but is required in order to test concepts and capabilities between disparate organizations. To this end, the basic premise of the Phase-I approach is that the design be scalable, easily repeatable, and would result in a set of processes and lessons learned that could be used to reduce time, cost and risk for future collaborative efforts. As a result of this approach, numerous design guidelines and technical constraints had to be accommodated in order to meet the intended scope of the project.

The following technical guidelines and constraints were followed:

- The project design must be scalable and easily repeatable
- The infrastructure design must not expose the Intellectual Property of any member company
- The network infrastructure design must be simple in order avoid technical, logistical, and export issues associated with overly-complex designs
- The Wide Area Network (WAN) transport solution must reside in the public domain, be low cost, and available and/or readily accessible in a short time frame to participating companies
- The infrastructure design must only deal with the connectivity that is considered outside of the security perimeter (i.e., firewall) of the participating member companies
- The technical design must utilize protocols and processes considered to be in the public domain
- The technical hardware solutions must utilize Commercial Off The Shelf (COTS) equipment. No military or defense articles or solutions can be included.

The following logistical guidelines and constraints were also accommodated:

- The project design must accommodate the participation of global companies. All required Export and ITAR guidelines must be followed in establishing the design and implementation criteria
- The infrastructure design must allow all participating member companies to adhere to their own company policies pertaining to the management of Intellectual Property, export compliance, and maintaining the integrity of their technical data
3.1 Technology Approach

The technology approach for Levels 1 and 2 covers the design criteria for the network infrastructure, connectivity of member company laboratories, and the pattern for audio/video component capabilities.

At the infrastructure level, the lab integration efforts of this project dealt primarily with connectivity that is outside the security perimeter (i.e., firewalls) of each member company. The inter-company connectivity was established using COTS hardware and industry-standard encrypted tunneling technology. The network infrastructure relied on a Public Internet access presence established and maintained by each member company. Member companies participating in the Phase-I activities were responsible for the costs and management associated with the hardware and Internet access presence to be used for establishing connectivity to/from the required locations.

3.2 Networking

As part of the Phase I design, the network transport infrastructure was logically comprised of a geographic “hub-and-spoke” Virtual Private Network (VPN) topology, as shown in Figure 5 below. One U.S.-based hub site was defined as the common aggregation point for all U.S.-based member company connectivity. Likewise, one European-based hub site was defined as the common aggregation point for all European-based member connectivity. The two hub sites were then connected to each other in order to provide the required global transport path linking all member company labs together.
3.2.1 Topology Integration

The technical approach for Phase-I focused on the use of COTS hardware and open standards-based tunneling, encryption and routing technologies. At the network infrastructure level, the integration activity was complex, given the multi-company participation and international footprint of the network environment. The design approach developed by the project team was therefore intended to minimize complexity to the extent possible, to reduce integration time for future collaborative efforts, and to ease troubleshooting and management of the network topology going forward.

3.2.2 Wide-Area Network Transport Approach

Use of the Public Internet as the Phase-I network transport was chosen based on the following criteria:

(1) The Internet is, by definition, considered a public domain environment and is not subject to specific export regulations or approval requirements

(2) Support of open standards-based protocols is inherent
(3) Each member company would be able to utilize an existing Internet presence, thereby preventing a time-consuming and costly acquisition of additional circuit capacity.

(4) Given the common availability of Internet capabilities for most organizations, integration time for future collaborative work could be reduced.

In addition to defining use of the Public Internet as the communication path for connectivity between VPN endpoints, the COTS hardware implemented as part of the overall topology was required to support a combination of open standards-based tunneling and encryption protocols. Specifically, the Generic Route Encapsulation (GRE) protocol for tunneling and the Internet Protocol Security (IPSec) protocol for encryption were chosen based on their availability within most, if not all, network-based COTS hardware and software platforms. Further, use of common GRE and IPSec configuration standards, such as tunnel mode characteristics and encryption and authentication algorithms were defined in order to ensure site-to-site interoperability between member company endpoints.

### 3.2.3 Tunneling, Security, & Routing Approach

Each member company was independently responsible for maintaining and administering a tunnel endpoint device (i.e. “tunnel router” or “tunnel firewall”) and for adhering to the technical, security and export compliance parameters as defined for the overall project framework. Each tunnel endpoint device had to support a combination of the Generic Routing Encapsulation (GRE) tunneling protocol and the IPSec encryption protocols in order to establish the required tunnel connectivity paths between member company endpoint devices. In addition, a minimum of static routing capability had to be supported in order to exchange network routing information between the tunnel endpoint devices.

### 3.2.4 Tunneling

For the site-to-site tunnel infrastructure, the GRE protocol was chosen as the primary implementation method due to its definition as a public domain protocol and its widespread availability in most, if not all, of the COTS network routing hardware solutions sold today. GRE is an extensively used tunneling protocol that can encapsulate a wide variety of network-layer protocol types, such as the Internet Protocol, inside of an IP tunnel. The resultant IP tunnel effectively creates a virtual point-to-point link between the local and remote tunnel endpoint devices of the participating member companies.

### 3.2.5 Network Security

Use of the Public Internet as the Wide Area Network (WAN) transport required that a secure method of encryption and authentication be utilized in order to provide the secure and reliable transfer of data between tunnel endpoint devices. For this, the IPSec protocol suite was employed based on its widespread use and definition as a public domain protocol. IPSec uses common authentication and encryption protocols to encapsulate data that needs
to be secured; thereby protecting the inter-site data flows as they traverse over the Public Internet. IPSec secures the communication stream by first authenticating, and then encrypting each IP packet of the data stream between GRE endpoints. Effectively, this dual IP-Sec/GRE approach creates multiple layers of data encapsulation - that is, the original data stream is encapsulated within a GRE tunnel to provide the virtual point-to-point communications link, and the resulting GRE tunnel is, in turn, encapsulated in an IPSec tunnel to provide a secure and reliable transfer of data.

As a secondary method to IPSec/GRE encapsulation, some of the Phase-I tunnel implementations utilized a newer method called IPSec Virtual Tunnel Interfaces (VTIs) to secure the inter-site communications path. IPSec VTIs do not require the use of GRE for first-level encapsulation, and as a result, simplify the configuration needed for IPSec to protect data between sites. However, since not all implementations currently support the use of IPSec VTIs, use of the IPSec/GRE solution was defined as the primary method for data protection, with the IPSec VTI method being allowed if desired and if both tunnel endpoint devices could support this mechanism.

In order to determine the necessary authentication and encryption protocols to be used for each connection, a pre-determined list of supported protocols was defined by members of the project team. The goal was to first document any known incompatibilities between vendor products used by participating companies and then to develop a capability matrix that could be used to track the workable solutions used for each tunnel connection.

The following list of supported authentication and encryption protocols were defined for use during Phase-I:

- **Internet Key Exchange (IKE) Phase 1**
  - Encryption: AES-128, AES-256, or 3DES
  - Hash: MD5 or SHA-1
  - Diffie Hellman: Group 2 (1024-bit)
  - Authentication: Pre-shared key
  - Phase 1 Lifetime: 28800 to 86400 seconds (negotiated per-link)

- **IKE Phase 2**
  - Encryption: ESP-AES-128, ESP-AES-256, or ESP-3DES
  - Hash: ESP-SHA-1
  - Perfect Forward Secrecy (PFS): No
  - Phase 2 lifetime: 3600 seconds
3.2.6 Routing

Static routing was used to facilitate route reachability within the infrastructure topology. Given the singular design of a single U.S. and European hub site, the use of a dynamic routing protocol such as the Open Shortest Path First (OSPF) protocol was not required. Future topology enhancements could incorporate the use of a dynamic routing protocol as needed to ensure routing scalability and ease of configuration.

3.3 Video

To provide distributed video teleconference capability for all participants, a centralized Multipoint Control Unit (MCU) was utilized to join multiple audio and video participants into a single conference. The MCU was deployed within the VPN topology at the U.S. hub site and was accessible to all participants connected via the GRE/IPSec infrastructure. Remote site participants were connected to the centralized MCU via hardware video teleconference (VTC) equipment of their choosing, or via desktop video software and supporting web camera and microphone components in cases where VTC hardware was not available. A mixture of VTC hardware and desktop software configurations were used during both Phase I and II demonstrations.

3.4 Data Interoperability

The participants in the exercise were utilizing a variety of simulations and display technologies. The various technologies involved the use of different protocols to move the data, including DIS, CoT, Java Messaging Service (JMS), and High-level Architecture (HLA). In order to allow interoperability, the participants agreed to use DIS over IP multicast as the standard protocol for communication between participants. Thus, each participant had to convert the various source data types to and from DIS as necessary for their specific applications in order for the data to be display in a Common Operating Picture (COP). For example, one participant’s entity simulation was based on a proprietary CoT via JMS data format. In order to achieve interoperability, a middleware component was required to convert this CoT/JMS simulation data to the required DIS format so that the entity data could be used and viewed on the COP by other participants.

For the Brussels demonstration, a second COP that displayed the CoT data format was utilized to show an extra layer or middleware functionality and data interoperability among participants. In a similar way that the data was converted to DIS for display in the first COP, the incoming source DIS entity data from other participants had to be converted back to the CoT format to be displayed on the second COP used during the Brussels demonstration. In this way, the team demonstrated the ability of the middleware components to provide interoperability between multiple source data formats being displayed on multiple common operating pictures. See Figure 6.
3.5 Network Delivered Services – Cloud Computing

With the introduction of the data interoperability middleware in Phase II, the team was required to install and configure middleware servers running at different node locations. This process, though repeatable, was labor intensive and generally required several days to identify physical hardware sever, install the appropriate operating system and patch levels, and configure the necessary middleware software. Expanding the project beyond a handful of nodes resulted in an intensive labor investment for node IT enablement. To address these challenges the project investigated Cloud Computing, a disruptive approach for consuming and delivering IT based services. Cloud purported to provide anytime, anywhere access to IT resources delivered dynamically as a service in a Net-centric fashion. The project was specifically interested in the following Cloud characteristics:

- On-demand self-service catalog – lab participants can request IT assets from a catalog of capabilities (pre-configured middleware in our case)
- Automated Provisioning – User requests from middleware are automatically provisioned as virtual machines and deployed onto resources running in the cloud
- Ubiquitous network access – assets can be accessed ubiquitously from an machine connected on the VPN
• Rapid elasticity - provisioned assets can expand and contract based on the requirements of the underlying workload and the usage characteristics

An important consideration in any cloud delivery is the type of service that is made available for consumption. These services range from simple compute and storage to more elaborate mission services involving human interaction. Typically, such services (referred to “as a service”) are thought to fall into three main categories:

• **Infrastructure as a Service (IaaS)** relates to providing the basic elements of computing, such as servers, storage, networking, and operating systems, enabling users to construct computing environments without building or owning the infrastructure themselves

• **Platform as a Service (PaaS)** adds to the infrastructure a richer software environment with a variety of built-in capabilities and tools such as database, transaction management, middleware platforms and development tools

• **Software as a Service (SaaS)** provides applications and business processes, such as customer relationship management or enterprise resource management

The lab project was specifically interested in a PaaS capability where the various messaging middleware could be rapidly deployed on-demand for any node to access.

### 3.5.1 Network Delivered Service Experiments

To investigate Cloud Computing’s applicability to the Lab project, a new node was added to the shared VPN, acting in the role of a Cloud Service Provider. IBM’s Cloud Lab in Dublin, Ireland instantiated a Private Cloud instance for the project and was connected as a node using the method optimized in Phase I.

Two Cloud Computing experiments were conducted to investigate how the Cloud could deliver services over the network. In Experiment #1 the servers running the Data Interoperability Middleware were migrated from physical machines running at member labs, to virtual machines running in the Cloud. These virtual machines were then transformed into templates and made available via the Cloud’s catalog of services. A team member on the shared VPN could go to the Cloud node’s portal, browse a catalog of services and select one to be provisioned. On average the provisioning time for a new middleware server took less than 30 minutes. In comparison, the project team’s industry average to install and configure physical machines was approximately 3 days as seen in Figure 7.
For Experiment #2, the project considered other types of services that could be delivered over the cloud. A major consideration of the project from its inception was security. Although the team developed documented steps for connectivity and necessary security configuration, there was no automated way to verify node-by-node compliance. This area seemed a very tractable problem for a cloud delivered service – essentially creating a virtual network discovery appliance each time a node was added and using it to verify the security posture of the network.

Using COTS Network Discovery software, the team created a virtual appliance that could be requested from the service catalog, automatically provisioned, and deployed into the cloud. This appliance could then run a network discovery across the VPN. Appropriately secured nodes should provide little information beyond their firewall. An unsecured node would report information beyond its firewall indicating a mis-configured node.

The results of this experiment are depicted in Figure 8 and show how a typical network discovery visualization would result from security scan. As in the first experiment, this capability could be requested automatically from the cloud and made available in less than 30 minutes. When the capability was no longer needed it was removed, and the used compute capacity returned to the Cloud’s resource pool for other requests.
3.5.2 Cloud Computing Design

The basic workflow associated with this experiment’s scenario is shown in Figure 9. The lab user requests a service from the catalog and provides pertinent information for the request including configuration choices (if available), account information (if needed) and reservation timeframes (to facilitate scheduling of the resources and reclaim them at the end of the reservation.) The service automation manager is the key component responsible for provisioning the service (by allocating the appropriate resources, installing the needed middleware and applications, and configuring it according to the service template definition) and activating it for use.

As is evident, the key technology needed from the architecture is the service automation manager. The service automation manager provides the service delivery catalog and service request manager components to handle the requests from the lab users. It orchestrates the image lifecycle management, asset management, provisioning, and virtualization management components to activate the service and support its use.

- Network Management service delivered On-Demand from the Cloud
- Verified the security posture of the network. All Virtual Private Network security features operated as designed.

Figure 8. Cloud Computing Experiment #2 Results
Figure 9. Requesting a Cloud Service

The lab interoperability Private Cloud implementation shown in Figure 10 depicts the key cloud architectural components: service request portal, service automation manager, service request manager, provisioning, monitoring & event management, security & resiliency, and the virtualization management (to interface with the managed environment.) For the project there were two small server farms in the cloud: a development server farm in which the team could develop and test the services, and a "production" server farm to host the services to be used for the live demonstrations to the NCOIC, NATO, etc.

The management environment contained the management servers that were needed to make the Cloud resources functional. In our case this included Windows virtual machines running the messaging middleware (virtualized with the VMware hypervisor) and Red Hat Linux machines running the network discovery COTS (virtualized with the Xen hypervisor). The management environment included the core components of a Service Request Manager, an Automation Manager, a workflow-based provisioning manager and a Configuration Management Data Base (CMDB) which is used to store the data in an Information Technology Infrastructure Library (ITIL) compliant service management best practice format. The Service Request Manager advertised the Cloud Services by means of a Service Catalog, and provided the interfaces that allowed the Service Portal to fully specify and submit a Service Request. It supported the workflows for approval of the request before invoking the Automation Manager to fulfill it. The Automation Manager interpreted the Service Requests, and used predefined workflows to fulfill the requested service. The Provisioning Manager was then triggered by the Automation Manager to provision or de-provision virtual servers, to install or uninstall software packages, or to invoke configuration actions on virtual servers.

Lastly, the Provisioning Manager was responsible for discovering resources in the Managed Environment, in order that they could be populated into the Configuration Management da-
tabase (CCMDB) and therefore be referenced by the Automation Manager. The Directory Server provided the authentication service for all of the elements in the Cloud.

Figure 10. Lab Interoperability Project Private Cloud
4 Policy Approach

4.1 Export / ITAR

As shown in Figure 3, the Phase-I infrastructure topology incorporated member companies located in both U.S. and European locations. In addition, provisions were made in the infrastructure design to incorporate member participation from other global locations as needed. In order for industry to move forward on establishing a global infrastructure that would provide for lab interoperability, ITAR and Export compliance regulations had to be identified and addressed.

Once the member companies were identified, the NCOIC Export Compliance Director provided training to the team to not include any ITAR-controlled information and to not provide comments or information pertaining to specific military systems or hardware. All aspects of the Phase-I design were intended to be drawn from, and currently in use in, the public domain. To that end, member company participants worked to identify, discuss and utilize open standards capabilities and use cases to ensure network centricity in the Phase-I infrastructure design.

In addition to the use of open standards protocols and processes defined for use in phase-I, the project team determined that all hardware used in design and testing of Phase-I would be COTS equipment. As a result, the Lab Interoperability Project is considered a COTS-level technology infrastructure used for testing of Levels 1 through 3 data between disparate global organizations, using COTS hardware and public domain information.

In order to ensure compliance with the above stated export considerations, the NCOIC Export Compliance Director submitted a Commodity Jurisdiction (CJ) request to the U.S. State Department in January 2010. The purpose of the CJ request was to receive U.S. State Department agreement that the Lab Interoperability Project was considered a Public Domain activity and did not meet the 120.9(a)(1) U.S. ITAR definition of a Defense Service. The CJ ruling from the State Department confirmed that this project as described was a public domain activity, and confirmed that same ruling from the US Commerce Department. During the time the CJ request was under review, the Lab Interoperability Project was conducted outside the auspices of the NCOIC.

CJ approval and NCOIC sponsorship does not relieve member companies of complying with internal company policies and U.S. Government export regulations. Member companies must still ensure that they are not involving ITAR controlled information or defense services in their activities with NCOIC.
5 Demonstrations

5.1 NNEC (NATO Network Enabled Capability) Capabilities Conference

To demonstrate the Phase-I approach, a capability demonstration was given to conference attendees of the NATO NNEC Capabilities Conference in Rome, Italy on March 24, 2010. The purpose of this presentation was to demonstrate the current Level 1 and Level 2 capabilities of the infrastructure, to solicit feedback from industry participants on the current Phase-I technical approach and progress to date, and to gather input on recommendations for the Phase-II approach going forward.

The logical demo topology used for the NNEC Rome demonstration is shown in Figure 11 below. The topology followed the overall hub-and-spoke network topology defined for Phase-I, with Boeing acting as the U.S. hub site and Finmeccanica acting as the European hub site. Encrypted Internet tunnels were established from each of the hub sites to the other member laboratory locations in that region, as well as to each other. The event site, the Ergife Palace Hotel in Rome, Italy, was connected to the U.S. hub site to provide connectivity for the remote lab participants.

The NNEC demonstration focused on existing project capabilities at Level 1 and Level 2, the Network, and Audio/Video components, respectively. The demonstration content consisted of a combination of video conference streams showing remote laboratory participants and the exchange and display of DIS data used to present a civilian scenario showing real-time interoperability of a collaborative network environment. The scenario chosen for this
event represented a humanitarian relief effort based upon the recent earthquake disaster in Haiti. The remote lab participants and collaborative view presented during the demonstration are shown in Figure 12.

![Figure 12. NNEC Rome Demonstration Remote Lab Participants](image)

To present a real-time, fictional scenario showing a collection of non-military relief vehicles and platforms supporting a relief effort in Haiti, member companies utilized the Level 1 network topology to send real-time, interactive DIS entity-state data to a central DIS collector device. The entity-state data received from each member lab was then presented in a joint common operating picture (COP) display that was streamed to the event site and displayed in real-time for onsite viewing by the demonstration audience in Rome.

5.2 NCOIC Plenary

Phase II of the project was demonstrated at the NCOIC Plenary in Brussels, Belgium on June 22 – 24, 2010. As discussed above, Phase-I of the Lab Interoperability project focused primarily on Levels 1 and 2, the infrastructure and audio-video capabilities, respectively. Phase-II incorporated the products and processes defined at Level 3, specifically the messaging middleware software and Cloud Computing components.

Figure 13 represents a conceptual view of the integrated middleware components used for the Phase-II demonstration:
Figure 13. Phase II Conceptual Model
6 Lessons Learned

The purpose of the NCOIC Lab Interoperability project team was to provide a set of processes and lessons learned from across industry in order to create a common approach for interconnection of member company labs. It is envisioned that this approach would be adopted into the internal policies of the NCOIC and its member companies and be recognized by their customers, thereby reducing cost and speeding up the time required for future collaborative work.

Throughout the project, a set of lessons learned was identified during the design, integration, and demonstration stages of the project. These lessons learned can be categorized into the areas of Technical Approach & Integration, Export / ITAR, and Live Demonstration activities.

6.1 Technical Approach & Integration

Despite the use of COTS hardware and open standards-based protocols during implementation of the Phase-I topology, numerous incompatibilities were discovered during setup and integration of the site-to-site Internet tunnels and exchange of Level-2 data. On average, 2 to 3 days were required to establish connectivity from the regional hub site to each remote site. In all, approximately two weeks were required to establish connectivity to all companies based on the topology shown in Figure 4. It should be noted that use of a full-mesh (one-to-one) topology would have increased time to implement significantly.

In some cases, it was difficult to determine whether a given incompatibility was the result of hardware, software, human error, or a combination of all of these factors. In addition, based on the fact that each member company was independently responsible for maintaining and administering their own tunnel endpoint device, internal company processes and implementation standards also may have contributed to integration incompatibilities being introduced into the tunnel topology.

At levels 1 and 2, the technical integration lessons learned can be categorized into three main areas, as follows:

- Vendor Implementation
- Multicast Support
- Video Teleconference Capabilities

In certain cases, there were known incompatibilities between types of network hardware and required software configurations. Given that participating companies typically maintain processes for utilizing a standard type of hardware and software code associated with that hardware, these incompatibilities can easily be introduced into a multi-organizational environment despite the definition of a set of standards-based protocols. Furthermore, some vendors may implement a given software feature or capability differently across different
platforms or across different code revisions within the same platform. And in some cases, different vendor products may implement a given feature or capability using a newer mechanism, or syntax, which may not be backwards compatible.

The project team discovered one such instance where a newer implementation of the encrypted tunnel technology in one vendor product was not compatible with the “traditional” implementation of the same feature within the second vendor product. In this case, a software upgrade in the second product was required, as was a change to the implementation policy for the member company using the second vendor product, in order to establish the required connectivity.

To enable IP multicast support, the project team discovered that certain network products being used in the VPN topology did not support the use of the Protocol Independent Multicast (PIM) protocol within a GRE tunnel configuration, or GRE-PIM. This protocol is used to send multicast control messages through an establish GRE tunnel path to the remote tunnel endpoint. If not supported, an alternate method such as application layer multicast would be needed to facilitate end-to-end multicast data transfer. At the time of implementation, as many as a one-third of the tunnel endpoint devices used did not support the GRE-PIM feature. As a result, inconsistent multicast support led to a mixture of desired multicast implementation schemes and an increased time for integration across the topology.

For purposes of the Phase-I NNEC Rome demonstration activity, a mixture of native multicast (GRE-PIM) within the U.S-based VPN connections and an application-layer solution called mTunnel within the European VPN connections was used to accomplish the required multicast functionality. The mTunnel application was also used for the connection between the U.S. and European hub site. For this event, multicast functionality performed well, however, utilizing a common solution would be recommended going forward in order to speed integration, reduce potential issues associated with different solutions, and ease troubleshooting of multicast issues.

The project team also discovered numerous hardware and software inconsistencies during setup of the distributed VTC environment used during Phase-I. VTC was used as the primary Level-2, audio-video application capability during the NNEC Rome demonstration activity. In some cases, member companies were able to provide a dedicated VTC hardware unit that was available during setup, testing and demonstration. In other cases, while a hardware resource was available, it was not always accessible at times when needed to accommodate the project schedule and demonstration preparations, due to conflicts with other internal company activities. And in still other cases, member companies did not have available VTC hardware and instead had to rely on a web browser-based VTC connection in order to participate in the Phase-I VTC environment.

For the NNEC Rome demonstration, an MCU was used to bridge the remote lab locations with the event site to present an integrated, or “split-screen”, video display of all participants. Inconsistent VTC hardware availability for some of the participating companies led to the
inability to control these remote VTC sessions from the MCU. This led to inconsistencies in
the ability to control video and audio parameters and to make real-time changes to individ-
ual connections as needed to maintain demonstration quality and performance.

For remote participants using a browser-based VTC client with attached web camera to
connect to the MCU, it was noted that overall video and audio quality was lower than that
observed by companies using a VTC hardware system. For these connections, integration
and testing time was increased due to the need to customize the video and audio settings to
a level needed to achieve demonstration-level quality and performance.

As a result of lessons learned during Phase-I in the area of Technical Integration, the follow-
ing considerations are in place for future project activities:

• Document a set of hardware, software and configuration parameters that eliminate
known technical incompatibilities

• Ensure that critical sites (i.e., hub sites) support and adhere to the known set of com-
patible products and configuration parameters

• Allow maximum lead time for multi-company international integration efforts

• Utilize common implementation criteria to reduce integration time and potential for
critical issues

6.2 Export / ITAR

The stated export requirements outlined by the NCOIC, the U.S. State Department and by
the internal policies of each participating member company led to numerous lessons
learned as part of the Phase-I project activities. As stated previously, a Commodity Jurisdic-
tion request, submitted to the U.S. State Department, was required in order to receive certi-
fication that all project activities were being worked in the Public Domain and did not meet
the ITAR definition of a defense service or activity. As a result of this requirement, the
NCOIC Export Director required that this project be worked under the auspices of the indi-
vidual member companies, and not the NCOIC, until such time that the Commodity Jurisdic-
tion certification was received.1

1 Formal Commodity Jurisdiction approval was received from the U.S. State Department on April 13, 2010. It
certified that results of this project are in the public domain and are not subject to the licensing jurisdiction of
the U.S. Department of State or U.S. Department of Commerce.
The fact that the Lab Interoperability project dealt only with information considered to be in the Public Domain and did not include any reference to Intellectual Property or otherwise sensitive, military, or classified data meant that process lead time required to facilitate design, integration and demonstration discussions and activities was reduced. However, based on the fact that the Commodity Jurisdiction certification was not in place for a majority of the Phase-I activities, provisions had to be made to minimize impact to project schedule.

In order to comply with the stated export requirements, any exchange of technical information between U.S. and non-U.S. member companies and the actual network integration (i.e. Internet tunnel establishment) between U.S. and non-U.S. companies was subject to export controls as defined by the internal policies of each member company. In an effort to reduce project schedule impact, portions of the design phase that focused on technical data exchange, as well as the actual network integration, were worked as two separate, but parallel efforts. In this manner, U.S. member companies, including IBM, Lockheed Martin, Boeing and Raytheon, were allowed to facilitate design discussions with each other and to proceed with establishing required Internet tunnels as needed to meet project schedule. In the same manner, the European companies, including Finmeccanica, Thales and EADS, worked in parallel to accomplish the same stated list of deliverables and milestones. As the required export approvals were received to allow information sharing across all domains, the U.S. and European efforts were aligned and validated to ensure technical and process compliance with each other.

6.3 Export / ITAR Lessons Learned

Despite a clear understanding of the stated ITAR and export requirements and a project model for working the initial design and integration activities as two parallel efforts, numerous lessons learned were gathered during Phase-I.

First, the lead time needed to receive internal company export clearance for technical planning materials and network integration took longer than expected due to the global footprint of the member companies. Member companies’ internal export clearance policies required that materials shared with international companies be cleared internally prior to each meeting/conference call. As a guideline, five (5) business days were needed to receive these proper export clearances and marking. The project team found that a weekly meeting schedule was limited by the time required to prepare materials and receive company export clearance in time to maintain a weekly recurring schedule. Meeting materials would need to be prepared and submitted for approvals and marking on the same day and time as the previous week’s meeting. Due to the design complexity of this activity and the technical integration involved, working “one week ahead” was not feasible. As a result, bi-weekly meetings were established in order to allow adequate lead time for the necessary internal clearances.

Second, since the Lab Interoperability Project activity of interconnecting international industry labs had not been previously undertaken by the NCOIC and its member companies, the
required U.S. State Department Commodity Jurisdiction (CJ) was not in place at the outset of the Project. As previously described, this led to additional time and effort associated with submission of the Commodity Jurisdiction request and the additional lead time needed to work the activity in parallel efforts.

Internal company policies for export clearance of project materials often differ and can lead to additional schedule impact or the need to modify material content prior to release. In some cases, the proper export support organizations within each internal company were not identified or engaged during the initial phases of the project to help speed cycle time and minimize risks associated in operating within a global company environment.

Lastly, export requirements for hardware and software shipped to/from the U.S. for an international demonstration event can vary significantly depending on the type of equipment and actual device type. Specifically, hardware or software containing common encryption capabilities, such as IPSec, will likely require additional lead time to receive proper export and shipping approval. The project team also discovered that some devices matching these criteria could not be shipped without significant lead time and impact to schedule. It could, however, be hand-carried as a temporary export item that was not subject to the same licensing requirements as a device being shipped. And finally, in some cases, the cost to prepare appropriate export documents for a given device was greater than the cost of the device being sent and was therefore considered cost prohibitive. In these instances, the project team attempted to acquire equipment “in-country” as much as possible in order to eliminate the need for export and shipping approvals.

As a result of lessons learned during Phase-I in the area of Export & ITAR, the following considerations are in place for future project activities:

- Keep all future design planning & capabilities in the Public Domain and do not include Intellectual Property or discussion of military or classified materials
- Allow for maximum lead time to receive all required export and shipping approvals
- Export support organizations should be engaged during the initial and all subsequent phases of future project activities
- Develop and pre-approve a set of generic templates to be used for information gathering and export approval of Public Domain capabilities
- Develop and pre-approve a list of equipment to be used as part of the technical integration and/or international demonstration activities

### 6.4 Live Demonstration

As stated previously, inconsistent VTC hardware availability for some of the participating companies led to an inability to control VTC sessions from the central MCU. Initially, minimal available bandwidth at the European hub site limited ability for >256 kbps call rate sessions.
This affected the demonstration by limiting overall control of the VTC connections with the MCU and thus impacting:

- Ability to mute individual sites with the MCU
- Ability to properly label Individual VTC sites
- VTC Stability: Increased probability of VTC drop out

Limited control of the VTC session is difficult as the number of participants increases in the session. Things that need to be considered are:

- Available Bandwidth
- Language barriers
- Increased chances of malfunctions, open microphones, software/hardware incompatibilities
- Availability to rehearse and schedule conflicts

The observations regarding the MCU were not greatly noticeable to the audience due to implementation of the most common method of communication control: communication discipline. Communication discipline rehearsed prior to the demonstration minimized noticeable VTC audio problems, incompatibilities, or control for the demonstration. However, the fact that adequate bandwidth was not available at the venue required the rental of a third-party temporary circuit.

6.5 Demonstration Lessons Learned

Although there was minimal impact, some minor observations for improvements were identified during the Phase I:

- Less than desired microphone quality for one or more of the lab presenters
- Less than desired video quality for one or more of the lab presenters due to the Video interfaces being utilized
- Need for a confidence monitor for remote sites not tied into the MCU (main VTC session), preventing the onsite audience from seeing themselves on the VTC screen - this can be distracting to the audience

As a result of lessons learned during Phase-I related to the live demonstration events, the following considerations are in place for future project activities:

- Look at correcting the microphone problem, and explore possible alternatives to web interfaces that were noticeably less quality
- Look into alternate methods to give the remote labs participating in the demonstration a confidence monitor to view the audience
7 Future Considerations

While the intended infrastructure design of the Phase-I and II architectures was designed to avoid issues associated over-complexity, a number of possible enhancements have been discussed for inclusion in future phases of the project. For example, future collaborative efforts may require the development of a redundant Level-1 topology to ensure high-availability for critical network and application components. Additional network services support, such as support for IP version 6, Quality of Service, and a real-time network management view of the infrastructure may be desired. It is envisioned that review of the Capability Description and follow-on discussions with the global NCOIC community will drive requirements that will define the desired enhancements for future phases of the project.

7.1 Next Steps

Following the Phase-II demonstration at the NCOIC Plenary meeting in Brussels, the Lab Interoperability group will develop the following set of technical deliverables to document the lessons learned and processes for incorporation of the Level-3 middleware components into the overall infrastructure:

- A Capability Description Whitepaper, describing the lessons learned and a method for connecting distributed labs
- A Project Compatibility Matrix, describing the technical configurations used by participating companies to achieve data interoperability

7.2 Middleware Compatibility Matrix

The compatibility matrix defines a set of supported middleware products and associated Level-3 dependencies with the Levels 1-2 supporting infrastructure. This matrix will be periodically updated to include new middleware solutions as they are verified to be compliant with the published Technical Framework policy.

8 Summary

The complexity of integrating hardware and software domestically and internationally re-
quired significant analysis to determine if any communication problems were due to hard-
ware or software incompatibilities, as well as human error. The networking aspect of Phase I
was complex as it was multi-company, multi-national and involved heterogeneous hard-
ware. However, as a result, the working group was able to gather information that will be
used to develop a pattern for future projects. It is hoped that this pattern will become the
foundation for NCOIC member companies to collaborate in future connectivity trials.