1-1-1992

# Communication Architecture For Distributed Interactive Simulation (CADIS): Rationale Document Draft

University of Central Florida Institute for Simulation and Training

INSTITUTE FOR SIMULATION AND TRAINING

NOVEMBER 1992

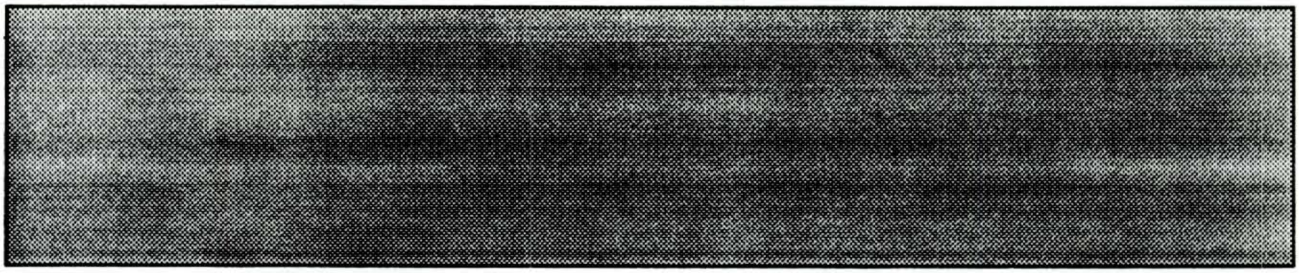
# RATIONALE DOCUMENT (DRAFT)

# COMMUNICATION ARCHITECTURE FOR DISTRIBUTED INTERACTIVE SIMULATION (CADIS)

IST-CR-92-20

iST

INSTITUTE FOR SIMULATION AND TRAINING

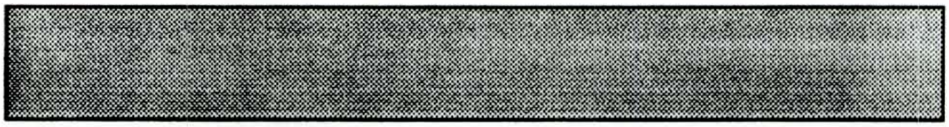


Contract Number N61339-91-C-0091
STRICOM
DMSO

November 1992

# Rationale Document Draft

## Communication Architecture for Distributed Interactive Simulation (CADIS)



iST

Institute for Simulation and Training
12424 Research Parkway, Suite 300
Orlando FL 32826

University of Central Florida
Division of Sponsored Research

IST-CR-92-20

INSTITUTE FOR SIMULATION AND TRAINING

# Rationale Document
# Draft

## Communication Architecture for Distributed Interactive Simulation (CADIS)

Contract Number N61339-91-C-0091

November 1992

IST-CR-92-20

Institute for Simulation and Training • 12424 Research Parkway, Suite 300 • Orlando, Florida 32826

**University of Central Florida • Division of Sponsored Research**

TABLE OF CONTENTS

## LIST OF TABLES

# LIST OF FIGURES

Figures

This page intentionally left blank.

# 1. INTRODUCTION

## 1.1 Forward

The purpose of the communication subsystem for Distributed Interactive Simulation (DIS) is to provide an appropriate interconnected environment for effective integration of locally and globally distributed simulation entities. There are many diverse aspects of this integration, ranging from the nature of the entities represented within the common simulated environment, to the common communication interface used for receiving packets of information from other simulators. The standard addressed by this Rationale Document is concerned only with the necessary communication system standards which must be accepted and adopted for supporting the integrated framework.

The Protocol Data Units (PDUs) defined in the DIS Standard are the "lingua franca" by which any two simulators or simulation sites can communicate. This includes simulators of different and unrelated design and architecture. No restriction is placed on what the participating simulator or site is, only on the way it communicates with the outside world.

Where the DIS PDUs define the information passed between simulators and simulation sites, this standard will define how those simulators, simulation sites, and other DIS entities can be connected in a modular fashion to facilitate the communication at the local and global levels. This will be done through the required use of communications standards which promote interoperability, such as the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) reference model and the Government OSI Profile (GOSIP).

This standard describes the communication architecture subsystem that will support DIS exercises and activities. The DIS PDU standard describes the format of the application protocol data units that contain the entity, environment, and simulation management information that will be carried on the network. This standard describes the structure and use of the network to carry that information. This document describes the rationale behind the requirements and specifications in the communication architecture standard. The guidance document describes how to use the information in the standard and rationale to create a communication subsystem to support DIS activity by providing tutorial descriptions and sample prototypes as well as discussing unresolved DIS communication architecture issues.

### 1.1.1 Background

The current work on standards began in August 1989 with the First Workshop on Standards for the Interoperability of Defense Simulations. Using the work of SIMNET as a baseline and considering recommendations made in workshop meetings and position papers, IST developed a first draft for a military standard which describes the form and types of messages to be exchanged between simulated entities in a Distributed Interactive Simulation. The workshops also provided for discussion in other areas associated with DIS such as environment, fidelity and exercise control and feedback, and communication architecture and security. Through the meetings of the workshops, based on discussions and individual input, the first draft of the COMMUNICATION ARCHITECTURE FOR DISTRIBUTED INTERACTIVE SIMULATION (CADIS) military standard has been developed. This rationale document addresses this first draft of the communication architecture/security standard.

### 1.2 Scope

This document contains extensive rationale supporting the choice of key items that have become part of the draft military standard entitled COMMUNICATION ARCHITECTURE FOR DISTRIBUTED INTERACTIVE SIMULATION . This rationale is intended to give the system designer a better understanding of why some choices were made and what impact deviation from them might have on the communication architecture system being designed. The communication architecture defined in the above mentioned draft military standard encompasses layers 1 through 5 of International Organization for Standardization's (ISO) Open Systems Interconnection (OSI) Reference Model (ISORM).

#### 1.2.1 Intended use

The intended use for this rationale document is as follows:

a. To define the service and performance requirements of a communication architecture to support DIS applications.

b. To recommend standard, non-proprietary protocols to be used in the communication architecture which will support the above requirements.

c. To recommend interim protocols to be used in the communication architecture for those requirements that cannot be met by existing standardized protocols.

#### 1.2.2 Future Goals

The standard for communication architecture for DIS has been created to meet the program needs of those programs using or scheduled to use DIS. The phased approach to the communication architecture is an attempt to progress to communication technology which does not exist today but must be developed to meet the service requirements. This section describes some of those technologies which are not currently addressed in this standard but will need to be addressed in the future.

#### 1.2.2.1 Video Conferencing

A number of DIS documents, including the DIS Operational Concept, have identified a video conferencing requirement. This is to support exercise planning, briefing, and debriefing, but specific requirements (e.g. number of sites, functionality) have not been identified. The communications industry is creating new ways to achieve such video conferencing, but mature products are not yet available. Video conferencing is very demanding of network capabilities and will have a major impact on any DIS network design. Because the requirements for video conferencing are not clearly identified and because industry offerings are not stable, video conferencing is not addressed in this document; however this requirement will be addressed in future versions as the requirements and available services become better understood.

#### 1.2.2.2 Interface to $C^3I$ systems

It is anticipated that DIS will interface to Communication, Command, Control and Intelligence ($C^3I$) systems in the future. This issue, however, will require considerable study before any actions can be taken.

#### 1.2.2.3 Interface to Field Instrumentation

DIS exercises will include participation of Field Instrumentation (FI) through the development of interfaces between DIS networks and FI equipment.

#### 1.2.2.4 Interface to High Order Models (e.g. ALSP)

DIS will be applied to wargame simulations and other high order models in the future. Eventually the goal is for next generation high order models (e.g. WARSIM 2000) to be DIS compliant and link directly to other DIS entities. An interim step is necessary to link DIS with existing high order models. This may be done by creating an application gateway between DIS and the Aggregate Level Simulation Protocol (ALSP), the mechanism that now links major wargame simulations.

#### 1.2.2.5 Emerging Technologies

DIS will be flexible enough to take advantage of emerging technologies, such as Asynchronous Transfer Mode (ATM), Synchronous Optical NETwork (SONET), Frame Relay, and emerging gigabit technologies. These technologies will be included in the standard as the need for more encompassing communication services dictate their use. These technologies will not be included in this standard unless they are standardized, but they will not be excluded from implementations if they are not standardized.

## 1.3 Assumptions

### 1.3.1 Layers 6 & 7 Usage

The DIS standard for protocol data units describes and specifies the services of layers 6 and 7, the Presentation and Application layers of the protocol stack. The standard addressed by this rationale document will therefore not address the services of these layers unless they are needed to describe services/requirements needed in the lower layers.

### 1.3.2 Open Architecture

The architecture defined in this standard will be open via the use of commercial standards and protocols. Nothing proprietary will be specified.

### 1.3.3 Scalability/Extensibility

The architecture will be specified such that it is scalable and extensible. This will allow DIS systems to be designed to expand to meet more encompassing needs and to take advantage of emerging technologies.

### 1.3.4 Other Uses of the Same Network

The underlying communication networks used for DIS exercises via PDU traffic will also be used for video conferencing, bulk data transfer, voice and video.

### 1.3.5 Programs (i.e. Gov't Programs)

There are three categories of DIS applications: simulations, which include both manned simulators and Computer Generated Forces (CGF); instrumentation, which brings real hardware into the loop; and wargames, which incorporates aggregate level entities. For all categories, there are both existing DIS applications, which will require retro-fitting for the new standard and new procurements, which have been called out in the DIS standard. Each application has different bandwidth, PDU, and entity requirements.

The communication architecture requirements specified in the standard addressed by this rationale document will be utilized by the following programs:

Close Combat Tactical Trainer (CCTT)
Battle Force Tactical Trainer (BFTT)
Tactical Combat Training System (TCTS)
Mobile Automated Instrumentation Suite (MAIS)
Tactical Aircrew Combat Training System (TACTS)
Joint Aircrew Combat Training System (JACTS)

### 1.3.6 Compression

This standard will not specify any means of data compression other than what is included in specified protocols.

### 1.3.7 Simulation vs Network Management

For this standard, the distinction is made between simulation management and network management. Simulation management will not be specified by this standard. Network management will be covered by the specification of network management protocols.

### 1.3.8 Long Haul Connection

Simulators at different sites shall be connected via a Wide Area Network (WAN). The standard addressed by this document defines the functional and performance characteristics which shall be satisfied by the communications service, including the WAN. It is the goal of this communications architecture that the WAN be based on standards such as frame relay, Switched Multimegabit Data Service (SMDS), Broadband Integrated Services Digital Network (BISDN), and Synchronous Optical NETwork (SONET). The provision of the WAN will depend on the evolution of these high speed communications services in the marketplace and the particular organization using the DIS applications.

Wide area networks today do not in general support multicasting. If two or three sites using DIS are to participate in a demonstration or exercise, they could be interconnected by point-to-point circuits or by a network with sufficient capacity to support repeated transmission to each site. This, however, would not be economical for a larger number of sites.

The nature and development of WANs for DIS application is taking two distinct paths. The first is the establishment of a permanent infrastructure that will connect all DIS sites. Although physically one large network, it will support multiple exercises via the creation of individual logical networks for each exercise. This approach is called the Defense Simulation Internet (DSI). The second approach is the establishment of Ad Hoc WANs as necessary to support exercises and tests. The primary mechanism for this is the bandwidth-on-demands services starting to be offered by the major communications suppliers (e.g. AT&T, MCI, Sprint). The concept is that a network connecting any set of DIS sites can be created quickly and efficiently from commercial services without the cost of maintaining a permanent infrastructure. The Advanced Distributed Simulator Technology (ADST) program is exploring this approach. This document does not assume either of these approaches and will support both of them.

## 2. COMMUNICATION FEATURES / SERVICES

### 2.1 Communication Service Requirements

Distributed simulation environment support requires various types of communication. The communication requirements encompass control and data. Data communications may be with or without real time requirements and will likely be augmented to include such things as voice, video and other forms of pictorial information. Upon the introduction of each of these forms of traffic, it is recommended that they share communications facilities instead of having disjoint facilities for each.

A summary of the communication service requirements is shown in Table I.

TABLE I. DIS Communication Service Requirements

Unicast
Multicast
Broadcast
Real Time Operating Speeds
Non-Real Time
Small Packets
Bulk Transfer
Reliable
Best Effort
Low Interpacket Dispersion for Voice/Video
Multicast Implementation
Multicast Management
Authentication/Access Control
Non-Blocking Interface
Flow Control
Low Latency Packet Delivery
Security
Flexible Entity Naming & Addressing
High Throughput

#### 2.1.1 Service Requirements of PDUs.

This section establishes DIS communication classes based on the application service characteristics for both the required and recommended interim DIS PDUs. Each DIS PDU requires certain service characteristics to make its communication practical. These characteristics are grouped into broad classes of operation for DIS.

##### 2.1.1.1 Application Requirements.

The DIS PDUs have been characterized by the communication services that their application requires. A subset of the communication service requirements include unicast, multicast, broadcast, reliable, best effort, real time, non-real time, packet size, and bulk transfer. The application service characteristics are used to define a service model necessary to support DIS communication. The service model developed from the PDU characterization shall be used to develop the interface to the application and lower layers.

### 2.1.1.2 DIS PDU Service Characterization.

DIS functional requirements are to provide: Entity Information, Entity Interaction, DIS Management, and Environment Information. Within each functional category, PDUs have been defined or recommended to satisfy specific requirements. The October 1991 version of the DIS standard defines ten required PDUs and six recommended interim PDUs.[1] The application services for required and recommended DIS PDUs are defined in Tables II and III, respectively.

Although packet size and bulk transfer are included as application requirements in 2.1.1.1, they are not presented in the summary tables for the following reason. Inter-entity communication in a distributed interactive simulation environment consists largely of packets sent between two or more of the simulation participants. These packets are usually small, less than 250 octets, and constitute the majority of PDU traffic. All PDUs listed in Table II and III fall into the "small packet" characterization. There are situations which mandate non-real time, point-to-point, reliable bulk transfer, however. Such situations arise when moving large items such as database files or video images. The bulk transfers fall into the Network and/or Simulation Management functions, but there are currently no PDUs which reflect this type of interaction. Consequently, bulk transfer is considered a special case.

[1] The October version of the DIS standard specifies three recommended PDUs for Update Threshold Control. As of this writing, those PDUs have been removed from the standard and, therefore, will not be included in this characterization.

TABLE II. Required DIS PDU Communication Services

| | Reliable | Best Effort | BC | MC | UC | Real Time |
|---|---|---|---|---|---|---|
| Entity State | | ❋ | | ❋ | | ❋ |
| Fire | future | ❋ | | ❋ | | ❋ |
| Detonation | future | ❋ | | ❋ | | ❋ |
| Service Request | | ❋ | | | ❋ | (few seconds) |
| Resupply Offer | | ❋ | | | ❋ | (few seconds) |
| Resupply Received | | ❋ | | | ❋ | (few seconds) |
| Resupply Cancel | | ❋ | | | ❋ | (few seconds) |
| Repair Complete | | ❋ | | | ❋ | (few seconds) |
| Repair Response | | ❋ | | | ❋ | (few seconds) |
| Collision | ❋ | | | | ❋ | ❋ |

TABLE III. Recommended DIS PDU Communication Services

| | Reliable | Best Effort | BC | MC | UC | Real Time |
|---|---|---|---|---|---|---|
| Emitter | *desired* | ❋ | | ❋ | | ❋ |
| Laser | *desired* | ❋ | | ❋ | | ❋ |
| Activate Request | | ❋ | | | ❋ | |
| Activate Response | | ❋ | | | ❋ | |
| Deactivate Request | | ❋ | | | ❋ | |
| Deactivate Response | | ❋ | | | ❋ | |

Legend: BC-Broadcast, MC-Multicast, UC-Unicast

DIS Management will require additional capability beyond the activation and deactivation PDUs. Although these capabilities have not yet been specified, Table IV projects additional application requirements for these areas.

TABLE IV. DIS Functional Requirements Communication Services

| | Reliable | Best Effort | BC | MC | UC | Real Time |
|---|---|---|---|---|---|---|
| Network Management | | * | | | * | |
| Simulation Management | * | | | *desired* | * | |

2.1.1.2.1 Entity Information.

The Entity State PDU (ESPDU) constitutes the bulk of network traffic for a simulation exercise. Currently, the appearance updates represented by the ESPDU are of most interest to exercise participants within a limited radius of the initiating entity. Any exercise participant who is not in the area of interest, but receives the ESPDU, will have to filter out this unwanted information. Therefore, Entity State has a strong requirement for multiple multicast interactions. Multicast interactions deliver identical packets to multiple recipients as part of a single sender operation.

In addition to their multicast requirements, ESPDUs must be delivered in real time but do not need to be transmitted reliably. Dead Reckoning (DR) algorithms are used to predict the entity's position over time in order to preserve network bandwidth by reducing the frequency at which state information is required. Reliability need only be a best effort. If an ESPDU is lost, the DR models used to reduce network traffic may also be able to compensate for the lost packet.

2.1.1.2.2 Entity Interaction.

Entity Interaction PDUs have varied characteristics. Within the Weapons Fire category, the Fire PDU (FPDU) and the Detonation PDU (DPDU) have the same service characterization. Similar to the ESPDU, both the FPDU and the DPDU have a strong multicast requirement. This requirement allows only those entities within the area of interest to receive information about weapons firing and detonation.

These PDUs are also desired to have a real-time requirement in the future, and should be as reliable as ESPDUs. Whereas ESPDUs can rely on DR to extrapolate position after packet loss, FPDUs and DPDUs are not as robust. When a weapon impacts, it is crucial that everyone in the multicast group receive that information so that "killed" targets do not continue to play in the exercise. A high degree of reliability is desired for the FPDUs and DPDUs, however current multicast protocols do not provide this service. Therefore, FPDUs and DPDUs must use a best effort real-time multicast service.

The Logistics Support PDUs (i.e., Service Request, Resupply Offer, Resupply Received, Resupply Cancel, Repair Complete, and Repair Response) represent activities which, although long in duration, do not require real time service. The resupply and repair interactions require a simple reliable transaction (request/reply) paradigm. This reliability is built into the application by pairing the acknowledgement (or reply) PDU with the request (e.g., Service Request and Resupply Offer PDUs). The Logistics Support PDUs do not require multicast, because only the entities involved in the service are interested. Therefore, the Logistics Support PDUs are characterized as requiring a best effort unicast service.

The last required category of PDUs in Entity Interaction is Collisions. Collision PDUs require a real time, unicast service. Again, only the entities involved in the collision will be interested in this information. Changes in entity appearance resulting from the collision will be communicated using ESPDUs.

The only category of PDUs not required for Entity Interaction is Electromagnetic Interaction. Electromagnetic Interaction currently consists of two recommended PDUs, Emitter and Laser. Both PDUs are desired to have a reliable real time multicast transmission but, as stated before, this is not available. Therefore, these PDUs are characterized as requiring best effort real time multicast.

2.1.1.2.3 DIS Management.

There are no PDUs specified for Network Management. Network management will be handled by a standard network management protocol (e.g., Simple Network Management Protocol or Common Management Information Protocol) and will not require DIS PDUs to accomplish the management of the physical network. Network management is accomplished with an best effort unicast service.

The Simulation Management category of PDUs is responsible for the activation and deactivation of simulation players. The request to activate or deactivate entities in a simulation exercise requires a simple reliable transaction (request/reply) paradigm. The reliability is built into the application by pairing the acknowledgement (or reply) PDU with the request. This service is characterized as non-real time unicast. Other possible functions of Simulation Management include management and control messages spanning multiple exercises. This type of service is desired to have a reliable multicast transmission, however reliable multicast is not currently available. Therefore, this type of service is characterized as reliable unicast. In addition to the packet form of interaction, there are situations which mandate non-real time, point-to-point, reliable bulk transfer. Such situations arise when moving large items such as databases or video images. Standard file transfer protocols such as File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) will be used.

There are no PDUs required or recommended for Performance Measures. If PDUs are developed for this functional area, the required services will fall into one of the established service classes.

2.1.1.2.4 Environment Information.

There are no PDUs required or recommended for Environment Information. If PDUs are developed for this functional area, the required services will fall into one of the established service classes.

2.1.2 Communication Classes.

From the previously stated rationale, three service models emerge as characterizing the DIS application.

**CLASS 1** **Best Effort Multicast**
A mode of operation where the multicast service provider uses no added mechanisms for reliability except those inherent in the underlying service.

**CLASS 2** **Best Effort Unicast**
A mode of operation where the unicast service provider uses no added mechanisms for reliability except those inherent in the underlying service.

**CLASS 3** **Reliable Unicast**
A mode of operation where the unicast service provider uses whatever mechanisms are available to ensure the data is delivered in sequence with no duplicates and no errors.

The service model is shown in Table V.

TABLE V. DIS Application Service Model

| **CLASS 1**<br>Best Effort Multicast | **CLASS 2**<br>Best Effort Unicast | **CLASS 3**<br>Reliable Unicast |
|---|---|---|
| Entity State | Service Request | Collision |
| Fire | Resupply Offer | Simulation Management |
| Detonation | Resupply Received | |
| Emitter | Resupply Cancel | |
| Laser | Repair Complete | |
| | Repair Response | |
| | Network Management | |
| | Activate Request | |
| | Activate Response | |
| | Deactivate Request | |
| | Deactivate Response | |

## 3. PERFORMANCE

### 3.1 Bandwidth

There are a number of factors which have a major influence on DIS bandwidth. At the very highest level, they include:

- Total number of entities
- Mixture of entity types.
- Type of exercise or scenario
- Choice of dead reckoning algorithm (and positional/angular thresholds)
- Security requirements

For the current set of approved DIS PDUs, the majority of network traffic will be Entity State PDUs (ESPDUs). ESPDUs are required to be sent at some minimum rate (e.g. every 5 seconds) by every entity and may be sent much more frequently depending on entity dynamics. The start-up of a session will also see high traffic but that is deterministic. The PDUs used to initialize an exercise or entity (such as the recommended Activate PDUs) represent a significant amount of data to be sent via the net, but they can be transmitted at a controlled rate. In the near term, the inclusion of Emitter PDUs may add a significant traffic load to the network, depending on the degree of electronic warfare (EW) present in a given exercise. Similarly, the future inclusion of simulated tactical communication links (both voice and data) will undoubtedly have a substantial impact on bandwidth.

There are also additional bandwidth requirements due to communications "overhead". A given PDU of "n" bits in length requires the addition of both headers and trailers in order to satisfy routing and data integrity requirements. The proposed UDP/IP protocols add 28 octets (8 for UDP and 20 for IP). The underlying media adds further overhead, such as FDDI's 20 to 28 octets of preamble, header and trailer information. A method to reduce this load is to concatenate PDUs at the application layer such that the overhead bits are applied to groups of PDUs rather than to every PDU. This approach, however, imposes an additional computational load on each host. This trade-off of processing load vs network traffic requires further study before serious recommendations can be made.

Another source of "overhead" traffic are security measures. The degree of overhead depends on at what layer (of the OSI seven layer stack) the security measures are implemented.

Refer to the Guidance Document for an explanation of one method of estimating bandwidth.

## 3.2 Latency

Some interactions between simulated entities are very tightly coupled in time. That is, the action of an individual controlling one of the entities may be a reaction to the activity of another. How tightly these interactions are coupled in time depends on the performance of the unit being controlled. High performance units, that is those units that react quickly to a human controllers input, tend to be very tightly coupled. An example of this is one simulated fighter aircraft flying in close formation with another. Units that respond to control inputs less quickly, such as ships, are only loosely coupled.

The issue of communications latency is directly related to how tightly a simulated entity is coupled to the entity to which it is reacting. The more tightly coupled two simulated entities are, the less latency is permitted in the communications that carry the state data of each to the other. Allowable latency under different circumstances is the subject of considerable debate. Little research of the quality that can serve as the basis of standards for latency has been done. The best information available is from the flight simulator industry, which for many years has been struggling with a related issue called transport delay. Flight simulator experience provides the following:

1. Humans cannot distinguish differences in time that are less than 100 milliseconds. This is due to physiological factors of the human body. This effectively provides a floor latency/transport delay value. That is, with a human in the control loop, there is no benefit to be gained from latency/transport delay less than 100 milliseconds.

2. In situations where latency/transport delay reaches 300 milliseconds, pilots start compensating for the lag in response. The result is a phenomenon known as Pilot Induced Oscillation (PIO). Such PIO can range from a minor annoyance to total loss of control.

The flight simulation community has also experimented with schemes to compensate for transport delay by predicting the behavior of the device being controlled. This approach showed promise, but the main emphasis in dealing with transport delay has been in reducing the delay by faster processing and better communications within the simulator. The DIS community has also begun to explore prediction of position as a means to compensate for latency in tightly coupled interaction. Northrop has done the most work in this area.

Studies reported to the DIS community[2] suggest that sophisticated prediction algorithms can compensate for up to 750 milliseconds of latency in the interaction of high performance aircraft carrying out radical maneuvers.

The position of simulated vehicles is not the only consideration in dealing with latency. DIS networks will also carry voice in the simulation of tactical radio nets. A speaker's voice will be converted from analog to a digital data stream that will be treated as just another series of PDUs. At the listener's position these will be converted back into analog form and will be output to speakers and/or headphones. Latency in such voice communications carries its own considerations.

In the case of an overseas phone call that was routed via a geosynchronous satellite, latency of a half second or more is inherent in such communication. In normal conversation, this is annoying but the speakers can generally adjust to it without difficulty. However, in the heat of a simulated operation such delays would render a simulated radio net unusable and would not be acceptable. Also, there is no prediction mechanism that can compensate for delays in voice traffic.

The dispersion of the arrival times of voice PDUs is also important. In the process of converting analog voice to a digital data stream, the analog signal is sampled at regular intervals and each sample is converted to a digital message. For the reconstruction of the voice back to analog, these messages should ideally arrive at the same regular interval. However, due to a variety of factors, there will some dispersion of arrival times. If the dispersion is too great, voice quality will suffer and may be unintelligible. The mechanism of converting voice from digital to analog form can handle some dispersion in arrival times. It is also possible to deliberately hold incoming voice PDUs in an accumulating FIFO buffer and then meter them to the voice reconstruction mechanism at a same rate at which the voice was sampled. This technique would eliminate the effects of delay dispersion, but would do so at the cost of additional overall latency.

### 3.2.1 Allocation of Latency Values.

In designing systems that meet the total latency standards defined in the CADIS standard, it is important to allocate these latencies in a reasonable manner. For example, if one designs a simulator in a LAN with a latency of 45 milliseconds between the application

[2] Position paper "Techniques for Extrapolation, Delay Compensation, and Smoothing with Preliminary Results and an Evaluation Tool," S. Goel, K. Morris, IST-CR-91-13, Summary Report: The Fifth Workshop on Standards for the Interoperability of Defense Simulations.

layer and the media (layer 1), it will still meet the standard of 100 milliseconds for total latency with similar simulators on the same LAN. However, if this same simulator becomes part of an exercise that includes simulators from other geographic sites, the total latency will likely exceed 100 milliseconds due to the latency consumed by the WAN connecting the sites.

### 3.3 Error Control

Section 2.1 identifies PDUs which shall be delivered reliably. This means that each of those PDUs shall be delivered to its destination without error. Implied in this definition is that the receipt of each PDU shall be acknowledged and retransmitted if necessary. Such acknowledgement and retransmission will be handled by the error detection/correction mechanism of the protocols used at level 4 and below. That is, there is no action required at the application level other than to indicate that a particular PDU is to be sent reliably. The receiving application can assume that all PDUs sent reliably are in order and intact.

PDUs not requiring reliable delivery shall be given best effort delivery. These PDUs make up the bulk of network traffic and include those PDUs that are multicast to all simulators in a DIS exercise. Acknowledgement and retransmission, associated with reliable delivery, is not feasible due to the additional latency and network bandwidth that would be required.

A PDU with corrupted data may be received. The processing of such corrupted data may create unacceptable behavior in the receiving simulator. For this reason, a checksum is required to be implemented in the communication architecture.

## 4. INTEROPERABILITY REQUIREMENTS

Much progress has been made over the past decade on standardizing approaches to interconnecting computer systems. Three aspects of distributed interactive simulation distinguish DIS from the more general computer/communication interconnection. These are: 1) real time delivery requirements for interactive, man-in-the loop behavior 2) multicast delivery options for convenient updating of shared data items and 3) military security considerations.

Any approach taken toward communication interoperability must apply to as wide a variety of existing simulators as possible, preferably all. This interoperability integration shall be possible with minimal disruption of existing simulators, even at the expense of optimality and efficiency. To accomplish this for the widest class of existing simulators (including those already interconnected and those running stand-alone) only the minimum properties should be standardized. This allows as many pre-existing configurations as possible to remain compliant with the minimum change, as well as accommodating the maximum flexibility for future innovation with minimum disruption to working systems.

## 5. ARCHITECTURE

### 5.1 Protocol Suites

### 5.1.1 Role of the Communication Architecture.

The ISO Reference Model is probably the most widely referenced model for communication architecture, and we adopt its use here. Under this model, the communication interconnection problem is broken down into seven layers, each with specific responsibility in carrying out part of the overall communication integration. The development of this reference model was in large measure motivated by and patterned after the success of the DARPA Internet program, which was the pioneer of the general machine interconnection technology base. Along with the development of the reference model, ISO has developed a series of protocols which in some cases mirror comparable entities in the Internet, and in other cases extend and formalize concepts only primitively developed by the Internet program. Currently, there are two dominant suites of protocols (Internet and ISO) which fit within the Reference Model communication architecture and are instantiations of a solution to the general communication interoperability problem. These protocol suites differ in details, maturity, number of options, flexibility, performance, number of currently available commercial products, number of fielded systems, and organizational support, among other factors.

Functionality lies within level 3 of this reference model and is the key to a generalized interconnection model. This network level provides for packets of information to be transparently delivered from system to system across almost arbitrary interconnections of local and wide area networks. By adopting the low cost conventions of providing for remote delivery even when delivery is actually local, and through the provision of gateway processors linking the local and wide area networks, a single approach (from the application perspective) can handle both the local and global cases, as well as transparently handle any needed change from one to the other. Under this approach, any reasonable selection for the layers below will be perfectly acceptable and work. These decisions can be handled locally on a case by case basis or by policy over some administrative domain if deemed appropriate. Building to the level three interface admits a mixing and matching approach to all of the levels below without sacrificing interoperability. Levels above do need to be matched. However, in our immediate case, handling interoperability for these functional elements has already been subsumed into the current DIS PDU standard. This approach ensures the maximum interoperability with the minimum of specification and new development.

### 5.1.2 Generalized Functional Architecture.

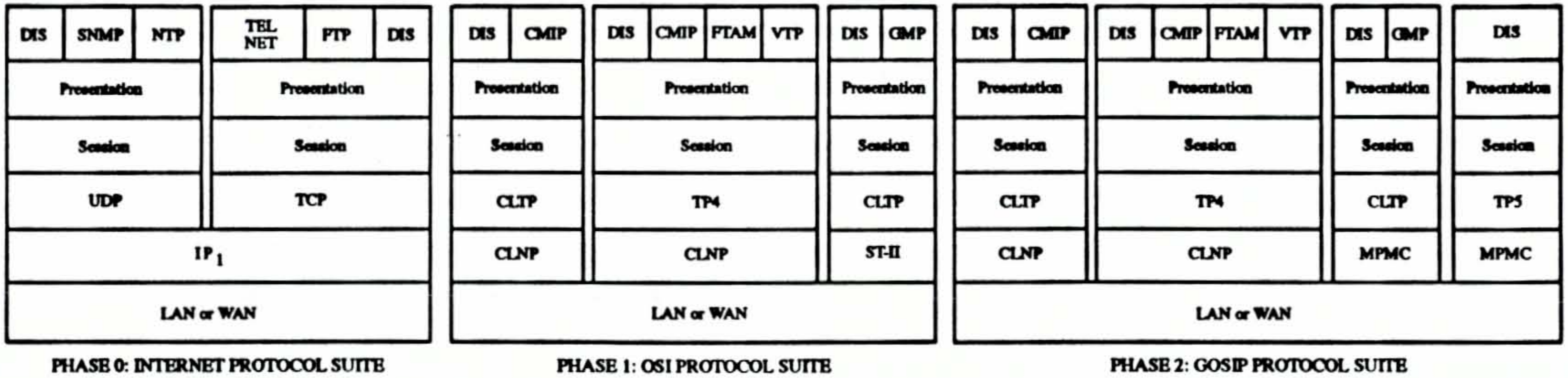
The Communications community thinks in terms of a vertical layering of communications functions. The accepted nomenclature (adopted by the International Standards Organization) refers to seven layers. Table VI identifies the levels and illustrates their meaning in the context of the networking of simulators.

TABLE VI: Seven Layer OSI Model Applied to Simulation

| Number | Name | Content |
|---|---|---|
| 7 | Application | Kind of data exchanged (position, orientation,...)<br>Dead reckoning rules.<br>Rules on determining hit or miss and damage. |
| 6 | Presentation | Representation of position (local vs geocentric coordinates), orientation (Euler angles, Quaternions, SPV), units (English, metric, degrees, BAMs..), and encoding (integer vs float, big vs little endian). |
| 5 | Session | Procedure for starting and ending an exercise.<br>Rules for joining and leaving an exercise.<br>Freeze. |
| 4 | Transport | Addressing from end user to end user. Assuring communications reliability, if required. |
| 3 | Network | Addressing information from node to node. |
| 2 | Link | Framing of information on a physical link. Flags, zero bit insertion. Conflict resolution. |
| 1 | Physical | Wire, optical fiber, radio transmission. Voltage levels, impedance values, clock rates. |

The DIS PDU document addresses levels 5 through 7. It does so without separating the levels. Levels 4 and below are defined in the remainder of this section.

There are a variety of existing protocols and interfaces which populate the functional areas for levels 1-4. The two most prominent suites of protocols which are collectively put forth as solutions to the interoperability problem are the DoD (Internet) suite and the OSI (GOSIP) suite. At this stage of evolution, the two are conceptually similar, but vary considerably in the details and in maturity. Both suites emphasize the network transparency from level 3 and above, as discussed previously. This means that one simulator is completely isolated from the selections made at levels 1 and 2 for every other simulator or collection of simulators, by adopting one of the "internetwork" layer standards as the base level for interoperability. This provides the freedom to delegate to local decision making the protocols used for the lower levels (assuming the selections conform with overall, real time performance objectives). The current real work of this document focuses essentially on levels 3 and 4. A plan which starts from the more mature Internet suite and evolves as appropriate over time toward the GOSIP suite is the most prudent path at this time. The three phased approach adopted by the standards effort is shown in detail in Figure 1.



PHASE 0: INTERNET PROTOCOL SUITE

PHASE 1: OSI PROTOCOL SUITE

PHASE 2: GOSIP PROTOCOL SUITE

1. WAN multicast protocols are not specified for phase 0 and are left open to the implementation.

Figure 1: DIS Three Phase Protocol Suite

0330-2540.1a

**Phase 0** is a proof-of-concept for DIS communication applications. The Phase 0 communication architecture protocol suite shall be composed of the following Internet standards:

| | | |
|---|---|---|
| DIS | - | Distributed Interactive Simulation PDUs |
| SNMP | - | Simple Network Management Protocol (RFC 1157) |
| Telnet | - | (Terminal Protocol) (RFC 854) |
| FTP | - | File Transfer Protocol (RFC 959) |
| NTP | - | Network Time Protocol (RFC 1305) |
| UDP | - | User Datagram Protocol (RFC 768) |
| TCP | - | Transmission Control Protocol (MIL STD 1778) |
| IP | - | Internet Protocol (MIL STD 1777) |
| ICMP | - | Internet Control Message Protocol (RFC 792) |
| ARP | - | Address Resolution Protocol (RFC 826) |
| RARP | - | A Reverse Address resolution Protocol (RFC 903) |
| Open | - | STream-II (RFC 1190), XTP (by PEI), or others |

Note: All phases of the protocol suites shall require a group manager function to specify the group membership management, group initiation, and group communication termination.

**Phase 1** is proof-of-concept of the DIS OSI communication infrastructure and hybrid implementation of the multicast protocol. The Phase 1 communication architecture protocol suite shall be composed of the following ISO and Internet standards:

| | | |
|---|---|---|
| DIS | - | Distributed Interactive Simulation PDUs |
| CMIP | - | Common Management Information Protocol (ISO 9596) |
| VTP | - | Virtual Terminal Protocol (ISO 9041) |
| FTAM | - | File Transfer Access and Management (ISO 8571) |
| NTP | - | modified Network Time Protocol (RFC 1305) |
| CLTP | - | ConnectionLess Transport Protocol (ISO 8602) |
| TP4 | - | Transport Protocol Class 4 (ISO 8073) |
| CLNP | - | ConnectionLess Network Protocol (ISO 8473) |
| Open | - | STream-II (RFC 1190) or XTP (by PEI) |

**Phase 2** is an enhanced OSI architecture based upon lessons learned in Phase 1, added functionality, and final versions of OSI/GOSIP multicast protocols. The Phase 2 communication architecture protocol suite shall be composed of the following ISO standards:

| | | |
|---|---|---|
| DIS | - | Distributed Interactive Simulation PDUs |
| CMIP | - | Common Management Information Protocol (ISO 9596) with possible extensions for multicast group management |
| VTP | - | Virtual Terminal Protocol (ISO 9041) |
| FTAM | - | File Transfer Access and Management (ISO 8571) |
| OSITP | - | OSI Time Protocol (undefined) |
| CLTP | - | ConnectionLess Transport Protocol (ISO 8602) |
| TP4 | - | Transport Protocol Class 4 (ISO 8073) |

TP5 - Transport Protocol Class 5 to provide a reliable multicast service (undefined)
CLNP - ConnectionLess Network Protocol (ISO 8473)
MPMC - Multipeer / Multicast Protocol to provide bandwidth reservation (undefined)

Phase 0 is currently the only phase which consists completly of protocols accepted by a recognized standards body. The detailed description of Phase 0 is contained in the Draft Standard Document. The following section describe the details of Phases 1 and 2 and the proposed transitions from phase to phase.

### 5.1.3 Phase One - OSI Protocol Suite.

The Phase 1 protocol suite is based on OSI network products which are available today. Interim wide area network facilities are used as in Phase 0. The Phase 1 protocol suite is shown in Figure 2. Phase 1 represents a possible interim transition step for DIS applications that start with Phase 0 and are migrating to Phase 2. In addition, systems that are under development using DIS may start with Phase 1, depending on the timing of their program schedule.

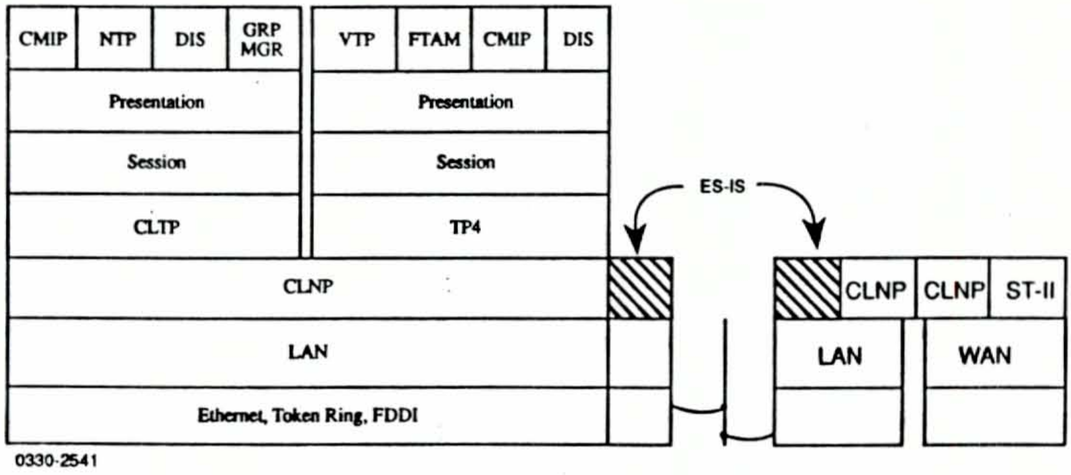


Figure 2. Phase 1: OSI Protocol Suite

The OSI protocol suite will successfully operate over any type of communication subnetwork environment that meets minimum performance requirements.

At the Network Layer, the protocol suite specifies the CLNP, as modified for multicast, for basic routing and connectivity. Routing will be based upon End System (ES)-Intermediate System (IS) and IS-IS. However, in the early implementation, static routing will be used. On top of CLNP is the Internet ST-II protocol, which will provide the needed resource reservation and delay bounding characteristics.

At the Transport Layer, the protocol suite is based on CLTP for datagram service and TP4 for reliable data transfer. At the Session and Presentation Layers, the protocol suite specifies the null layer functionality. This requires the padding of the Application Layer headers with two octets of zero.

At the Application Layer, the protocol suite specifies the DIS application protocol and a group management function. The DIS application protocol will handle the DIS specific protocol interactions. The multicast group manager function will specify the group membership management, group initiation, and group communication termination.

The following items are considered developmental based on product availability: multicast (ST-II and XTP), group management, and CLTP.

5.1.3.1 Migration Path to Phase One.

The transition from Phase 0 to Phase 1 will require protocols at all levels to change. The protocol migration is shown in Table VII.

TABLE VII. Transition From Phase 0 to Phase 1

| Phase 0 | | Phase 1 |
|---|---|---|
| Internet Standards | | OSI |
| SNMP | --> | CMIP |
| NTP | --> | NTP |
| TELNET | --> | VTP |
| FTP | --> | FTAM |
| TCP | --> | TP4 |
| UDP | --> | CLTP |
| IP | --> | CLNP |
| Open | --> | ST-II |
| | | XTP |

5.1.3.2 Migration Process to Phase One.

Two types of milestones can be used to determine when the transition from Phase 0 to Phase 1 should occur. The first set of milestones is the "maturity criteria." This set includes: protocol maturity, product availability, product maturity, product cost, and implementations. The second set of milestones, the "risk criteria", includes: required development and development cost.

### 5.1.4 Phase Two - Full GOSIP Protocol Suite.

The proposed Phase 2 protocol suite incorporates the future OSI multicast protocols into the GOSIP compliant network. The Phase 2 protocol suite is shown in Figure 3.

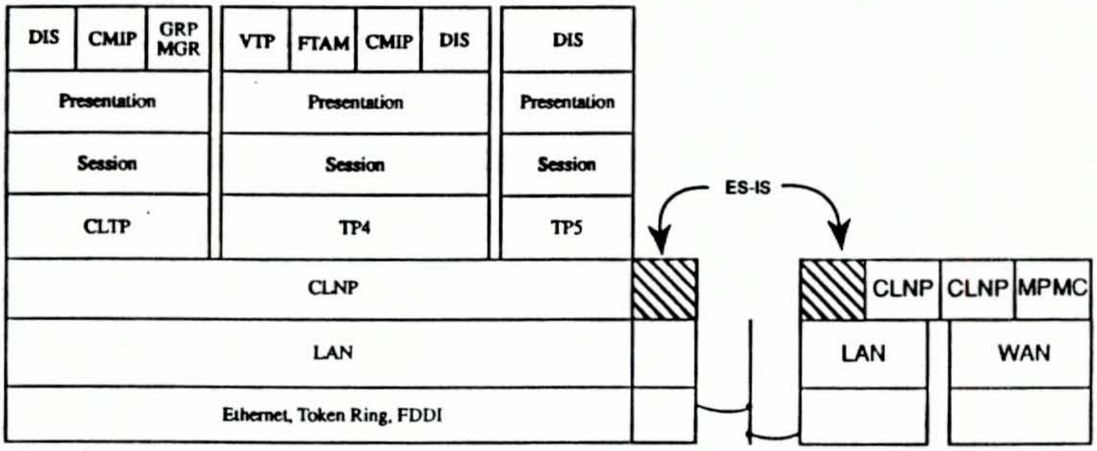


Figure 3. Phase 2: GOSIP Protocol Suite

The time protocol and multicast protocols have to transition from Phase 1 to Phase 2. Although DIS does not currently require a reliable multicast protocol, this requirement is desired for the long-term architecture. This reliability will be provided by a Transport Layer protocol called TP5. DIS will also need a Network Layer multicast protocol to provide bandwidth reservation for real-time communication. This protocol is tentatively called MPMC. DIS may also want to take advantage of multicast extensions to the network management protocol, CMIP. When DIS simulation management is defined, it will be possible to anticipate a desired use.

#### 5.1.4.1 Migration Path to Phase Two.

The transition from Phase 1 to Phase 2 will require the multicast protocols and the network time protocol to change. The protocol migration is shown in Table VIII.

TABLE VIII. Transition From Phase 1 to Phase 2

| Phase 1 |  | Phase 2 |
|---|---|---|
| OSI |  | GOSIP Standards |
| CMIS/CMIP | --> | CMIP w/multicast extensions |
| NTP | --> | OSI Time Protocol |
| VTP |  |  |
| FTAM |  |  |
| TP4 |  |  |
|  | --> | TP5 |
| CLTP |  |  |
| CLNP |  |  |
| ST-II or XTP | --> | MPMC |

#### 5.1.4.2 Migration Process to Phase Two.

The transition from Phase 1 to Phase 2 should be based on the multicast protocols being standardized by ISO. After adoption, the functionality of the new protocols should be demonstrated and tested in prototype implementations. Once testing is completed and the protocols have been validated, the new architecture should be assessed by the maturity criteria established for the Phase 0 to Phase 1 transition.

### 5.2 OSI Compatibility.

The ISORM was developed in 1977 by the International Organization for Standardization in response to the need to interconnect heterogeneous computers. OSI defines a framework for the interaction of users and applications in a distributed environment.

The Government Open Systems Interconnection Profile is the U.S. Government program for adoption of OSI across all Federal agencies. The purpose of GOSIP is to provide: networking connectivity, through GOSIP network architecture; interoperability, through standard "profiles" of OSI protocols; and competition, through focus on small number of subnetwork technologies and interoperable applications.

#### 5.2.1 Benefits of DIS Compliance to the OSI/GOSIP Architecture.

DIS compliance with the OSI/GOSIP architecture provides the following benefits: reduced cost, increased interoperability, and increased application-level functionality. Efforts to ensure conformance to OSI/GOSIP standards and ensure interoperability between products of different vendors means that computer networking can be done as an integration of multi-vendor, commercial-off-the-shelf (COTS) components. Easy access to vendor interoperable COTS OSI/GOSIP products gives wider availability to networking capabilities at a reduced cost.

Not only will OSI/GOSIP standards provide interoperability between products, but international interoperability will also be increased. The OSI standards are international in scope and will be used by North Atlantic Treaty Organization (NATO) allies, among others. Using OSI standards opens the possibility that interoperation with our NATO allies will be accomplished within the framework of international standards.

5.2.2 Desired Extensions & Additions to OSI.

The DIS multicast requirement is not presently found in OSI, however, work is underway to develop these standards. Currently, there are six American National Standards Institute (ANSI) working groups participating in the development of multicast standards: X3T5.1 (OSI Architecture), X3T5.4 (OSI Management), X3T5.5 (OSI Upper Layers), X3T5.7 (OSI Security), X3S3.3 (Network and Transport Layers), and X3S3.7 (Public Data Networks). The goal of the Multipeer/Multicast (MPMC) effort is to develop a complete set of standards which will provide DIS with a full range of multicast functions and capabilities.

To include multipeer/multicast in the ISORM, the following extensions and additions to current ISO standards are required:

> **ISO Reference Model**, including Part 1: Multipeer Addendum to the Basic Reference Model, Part 2: Security, Part 3: Naming and Addressing, and Part 4: Management Framework;
>
> **Application Layer**, including the Application Layer Structure and Extended Application Layer Structure;
>
> **Transport Layer**, including Connectionless Transport Protocol and Connection Oriented Transport Protocol;
>
> **Network Layer**, including Connectionless Network Protocol,
>
> **Routing**, including End System to Intermediate System Protocol (ES-IS), Intermediate System to Intermediate System Protocol (IS-IS), and Intra-Domain Routing Protocol (IDRP);
>
> **Network Management**, including Common Management Information Service (CMIS), Common Management Information Protocol (CMIP), Systems Management Overview, OSI System Management, and Structure of Management Information

Other extensions to the OSI architecture include a time protocol. This is being developed within the OSI program of work in the OSI Management Working Group.

### 5.3 PDU Encapsulation for Phase 0.

For the 1992 Interservice/Industry Training Systems Conference (I/ITSC), a demonstration of the use of DIS will occur. This demo will use the UDP/IP protocols for the communication architecture. The encapsulation of PDU in the UDP header was defined for the demonstration as shown below.

|  |  |  |
|---|---|---|
| IP | UDP | Data |

The UDP fields are defined as:

|  |  |  |  |
|---|---|---|---|
| 1 - | source port | (2 octets) | An optional field, when meaningful, indicates the port of the sending process. |
| 2 - | destination port | (2 octets) | [DIS = 3000][3] |
| 3 - | length | (2 octets) | Length of the datagram including the header and data. |
| 4 - | checksum | (2 octets) | Verifies part of the IP header, the entire UDP header and data |
| 5 - | data |  | DIS PDU data |

Commonly used source and destination port numbers are available in RFC 1340 "Assigned Numbers".

[3] The port number(s) for DIS are currently being requested and will be put into this document as soon as they are assigned.

## 6. SECURITY

### 6.1 DIS Security Requirements.

A comprehensive list of DIS security requirements is not available, nor is there one in preparation. Yet certain specific security needs are already discernible. It is the responsibility of the network sponsor to describe the overall network security policy enforced by the Network Trusted Computing Base (NTCB). At a minimum, this policy shall include the discretionary and mandatory integrity, or both. The policy may require data secrecy, or data integrity, or both. It is essential that development of the discretionary and mandatory secrecy policy be addressed as an integral part of network design. Some of the elements that support the security policy are described briefly in the remainder of this section. The elements are merely examples. Development of a security policy and security appliques for specific DIS application requires support from information security specialist within a given organization or command and may also require support from INFOSEC specialist from the National Security Agency's (NSA) Information Systems Security Organization.

The example security profile in Appendix A has been driving the security decisions made by the CASS.

## 7. REFERENCES

Listed below are some of the documents referenced in this rationale document.

### 7.1 Standards Referenced

The following standards have been referenced in this document:

a. ISO 7498 and CCITT X.200 (ISO Reference Model).

b. Mil Std. Final Draft Protocol Data Units for Entity Information and Entity Interaction in a Distributed Interactive Simulation, October 1991.

### 7.2 Other Documents Referenced

The following non-standard documents have been referenced in this document:

a. Tannenbaum, Computer Networks. Prentice Hall, 1988.

# APPENDICES

# APPENDIX A:

## Security Architecture Profile for Phase 0

## 10. Security Architecture Profile for Phase 0

The following example of a profile requiring security has been driving the security decisions made by the CASS.

The Phase 0 Distributed Interactive Simulation scenario consists of multiple IP-based simulators located in several sites, participating in a real-time exercise. Each site uses a LAN (such as an Ethernet or FDDI) which could be interconnected securely via a black WAN to the other sites. Some of the simulators will participate in a given exercise at a system-high level using a red LAN, i.e., all the subscribers to that LAN will have access to all the traffic associated with the exercise. The system-high operation may interfere with the ability of a site to participate in several independently secure exercises simultaneously.

At each site there will be a Local Exercise Manager (LEM). The LEM is a software process that will participate in the set-up of that exercise and would know which other sites participate. It would also distribute specific parameter values for each exercise (such as the bandwidth allocated to the site, update frequency, the choice of coordinate system, and the version of the geographic database in use). It is anticipated that some manual set-up will be required initially for each exercise; this manual set-up would be either of a new type, or with a new set of participants.

The LEM will use TCP to communicate with each of the simulators, with LEMs at other sites, and with the GEM, the Global Exercise Manager. The individual simulators will use TCP (with FTP) for reliable loading of critical files, such as programs and geographic databases. The real-time communication among the simulators during the exercise will use UDP.

For security considerations, the LEM is divided into separate black and red components.

The WANs may or may not support bandwidth reservation and multicast, such as the TWBnet. For generality, the assumption is made that the WANs support neither. The example addressed here represents the worst case scenario. Two-by-two approaches have to be considered:

(H) System-high operation
(C) Controlled access to exercises

and

(2) Network security at Level-2
(3) Network security at Level-3

For the total of four approaches:

(H.2): System-high operation based on network security at Level-2

(H.3): System-high operation based on network security at Level-3

(C.2): Controlled access based on network security at Level-2

(C.3): Controlled access based on network security at Level-3

We assume that initially (H.X), system-high operation at Level-2 or at Level-3, would be used with encryption devices per site, regardless of the number of simulators there. This is done because of the understanding that eventually the system will migrate to (C.X), controlled local access to exercises, with individual encryption devices for all the simulators participating in the exercise, and for the red LEM.

The migration from (H.X) to (C.X) will require some development costs with no significant implications for the architecture, the software, or the hardware. This will require the addition of another network encryption device and a red LEM per local physically separated community of interest (i.e., using a separate encryption key when leaving their system high LAN).

For maximal flexibility, there may be a dedicated encryption device for each host. However, the budget may not be able to support a large number of such security devices since the cost of NSA-approved encryption devices does not follow the trend of consumer electronics (commercial computers, included) and does not decrease dramatically annually.

In principle, approaches (H.2) and (H.3) are similar, even though they differ in many details. For brevity we describe here only (H.2). This is not a recommendation to prefer (H.2) over (H.3), (C.2), or (C.3).

The actual choice among (H.2) and (H.3) and among the various devices available on the market (through the Commercial COMSEC Endorsement Program (CCEP), of National Security Agency (NSA)) could be made only after objective engineering tradeoffs are taken into account. Considerations of interest include:

- Performance (both in bps and pps)
- Keying
- Security management
- Multicast (and crypto synchronization),
- Real-time behavior (and packet loss)
- Security doctrine (modes/policy)
- Configuration
- Error response
- Error characteristics

- Scalability
- Network management
- Interaction with other protocols and services (e.g., Redirect, ARP, and SQ)
- Cost.

### 10.1 Approach-(H.2): System-High at Level-2.

Figure 3 shows the configuration. The local system-high LAN supports the simulators. The encryption is performed at the Ethernet level, by Xerox's XEU.

The LEM job is divided among two units, the Black-LEM (B-LEM) and the Red-LEM (R-LEM). The configuration information that is entered into the B-LEM is then distributed over airgaps to the R-LEM, the Ethernet bridge, and the KML (for the XEU). It is also distributed to the Reno (a.k.a. XET, the front end for the gateway) over a black-LAN. The R-LEM is on the red system-high LAN. The B-LEM cannot be on the red LAN because it has to provide information to the black Reno. Neither part of the LEM requires a dedicated hardware unit. Both are software modules that can be run at a user level, the B-LEM on the black side (e.g., in a Reno) and the R-LEM on the red side (e.g., on any simulator). R-LEMs communicate with other R-LEMs, only in a secure mode over the WAN once the appropriate keying arrangements are made. B-LEMs can always talk with each other over the WAN in an unsecured mode.

Each exercise has its own IP MultiCast Address (IPMCA) (and Ethernet MultiCast Address (EMCA)) used for all the communication with the other simulators, at the other sites. The transmission scenario, after the initial set up is as follows. Consult the diagram of (H.2), below.

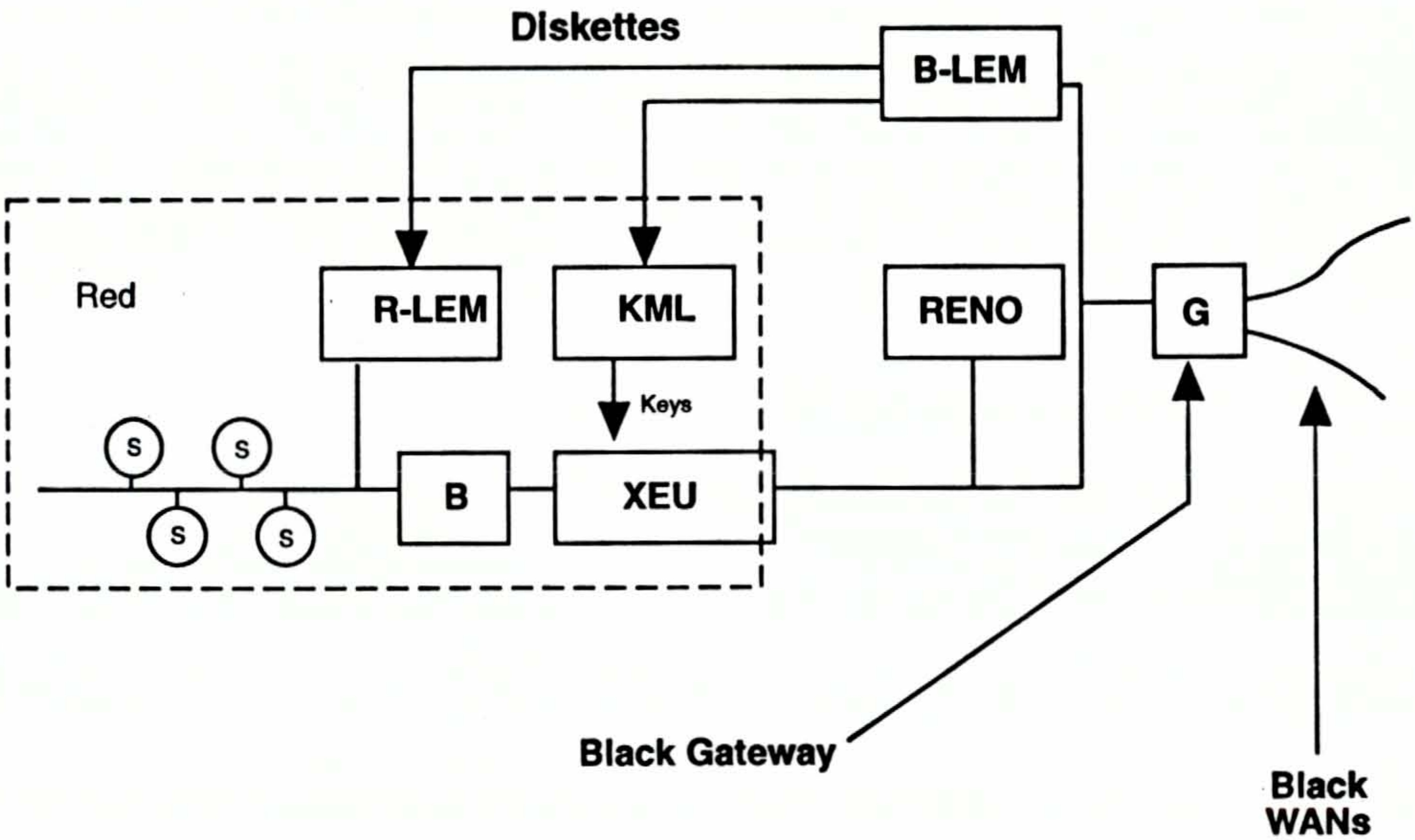


Figure 3. Diagram of (H.2): Net-Security at Level-2, System-High

## 10.2 Example Scenarios.

Each simulator prepares data for transmission, in red UDP/IP packets addressed to the IPMCA assigned to the exercise. These red packets leave the simulator and enter the red LAN using the EMCA[4]. (The IPMCA was provided earlier by the R-LEM to the simulators (using TCP).)

An Ethernet-bridge, B, on the LAN transfers only the red packets with the EMCA to the XEU. The EMCA was provided earlier to the bridge by the B-LEM[5].

The XEU verifies that the originating host (identified by its individual Ethernet address) is indeed authorized to send red packets to this EMCA. The EMCA and the list of the Ethernet addresses of all the authorized simulators should have been provided earlier by the B-LEM via the Key Manager/ Loader (KLM) to the XEU. The XEU generates the black version of these red packets by encrypting them in their entirety, adding headers (for crypto synchronization, etc.), and also adding black Ethernet headers with the original EMCA in the black.

The KML is physically located at one site (per exercise). It generates physical keys that have to be distributed to the sites. New keys have to be distributed to all sites from the KML at least once a year unless security compromises occur. Whenever a site adds devices with new Ethernet addresses (e.g., new simulators), a new key is required to be generated for that site only for the exercises in which these new devices are to participate. The packets are then given by the XEU, over the black Ethernet, to the Reno, that operates totally in the black[6]. The Reno recognizes the exercise packets by their EMCA and encapsulates them in IP (or ST) packets, as required by the gateway to the WAN. These packets are IP-addressed (or ST-addressed) to Renos at the other participating sites. Being a general purpose computer, the Reno can easily be programmed to set the priority field, or to open a connection with bandwidth reservation as required. The black Reno packets are sent

[4] The EMCA is derived from the IPMCA according to the standard IP operation procedures as defined in RFC1112, "Host extensions for IP Multicasting", by S.E. Deering, Aug-01-1989.

[5] The exact way for doing that depends on the particular bridge in use.

[6] The Reno (a.k.a. XET is a software package developed by Xerox that can run on any general purpose computer (e.g. any 386 system or a SPARC). The function of the Reno is to serve as a front-end for the gateway by encapsulating the black Ethernet packets (produced by the XEU) inside black packets suitable for handling by the WAN, and by performing the inverse task at the receiver end. If needed, the Reno may perform the gateway front-end tasks described in the Architecture-Profile section above.

over the black LAN to the black gateway for transmission over black WANs. That gateway should be a COTS unit, optimized for the WAN in use.

It is possible for a sending Reno to strip off the black Ethernet headers for the transmission over the WAN. Those headers will then be re-inserted by the receiving Reno. This saves some WAN bandwidth at a cost of additional processing (a typical engineering tradeoff). If an IP-WAN does not support IP-multicast, the Reno can replicate the black packets to achieve the desired multicast. The IP-addresses to which the packets should be forwarded were provided earlier by the B-LEM to the Reno, over the black LAN.

All the knowledge about the WAN is in the Reno, because the WAN connects (practically) only the Renos. Hence, issues such as the choice of IP vs. ST for the long haul are separated by the Renos from the rest of the system that uses IP for end-to-end communication. Note that because of the security, there is no direct interaction between the end-to-end IP and the IP that is used over the WAN. These two IPs do not have to share even their address space. Therefore, changing the WAN (for example, from a general IP-network, to a TWBnet, to its future successors, and then to a gigabit speed IP-network) could be handled by changes only to the Reno.

As advances in technology (and especially in DoD procurement) make better networks available, only the gateway selection and some Reno software may have to be modified, isolating the local site, the simulators, the LEMs, and the encryption gear from the need to adapt to the upgrading of the WANs.

The reception scenario, after the initial set-up is as follows. Consult the diagram of (H.2), (Figure 4) below.

The black WAN deliver black packets to the Reno over the black Ethernet. The Reno recognizes them, by their IPMCAs (or by their ST addresses) as belonging to a particular exercise, de-encapsulates them from the IP (or ST) packets, and gets the black Ethernet packets with the appropriate headers as expected by the XEU. These packets are delivered over the black Ethernet to the XEU, that decrypts them and recovers the original red Ethernet packets, with the original EMCA.

The XEU transmits these red packets on the red system-high Ethernet, through the bridge, and makes them available to all the local simulators, where the Ethernet headers are discarded, and the original red UDP/IP packets are received and processed.

Notes for the (H.2) diagram:

- Diskettes are used to carry information from the B-LEM to the R-LEM and to the KML, if it is at that site. The setting of the bridge depends on the particular bridge in use.

- The KML exists only in a few locations. Only one KML is in charge of any exercise. It generates the keys for all the participants in that exercise, and from it they have to be securely distributed to the various sites.

- If needed for performance, the Reno may use two Ethernet interfaces to allow splitting the black Ethernet, with one segment between the XEU and the Reno, and another for the WAN gateway(s), the B-LEM, and the Reno. This makes the LAN, the bridge, the XEU, the Reno, and the Gateway to be "in-series", as shown in the following diagram.

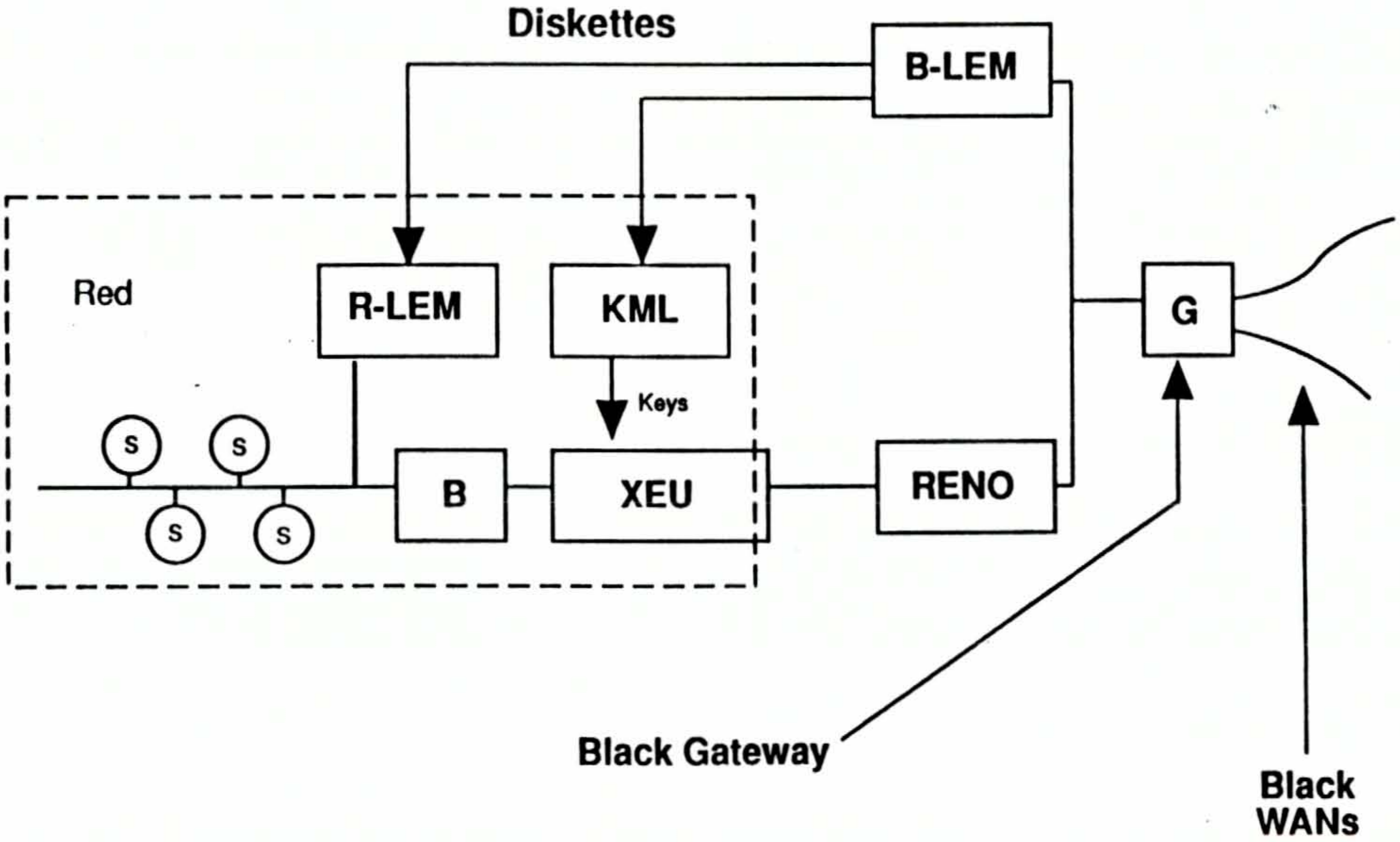


Figure 4. (H.2): Net-Security at Level-2, System-High with Reno in-series