1-1-1994

Standard For Distributed Interactive Simulation Communication Architecture And Security: Draft

University of Central Florida Institute for Simulation and Training

INSTITUTE FOR SIMULATION AND TRAINING

MARCH 1994

STANDARD FOR DISTRIBUTED INTERACTIVE SIMULATION COMMUNICATION ARCHITECTURE AND SECURITY

IST DOCUMENTATION

IST-CR-94-15

IST

INSTITUTE FOR SIMULATION AND TRAINING

Contract Number N61339-91-C-0091
STRICOM
DMSO
March 1994

DRAFT

Standard for Distributed Interactive Simulation-- Communication Architecture and Security

IST

Institute for Simulation and Training
3280 Progress Drive
Orlando FL 32826

University of Central Florida
Division of Sponsored Research

IST-CR-94-15

DRAFT STANDARD
March 1994

COMMUNICATION ARCHITECTURE

FOR

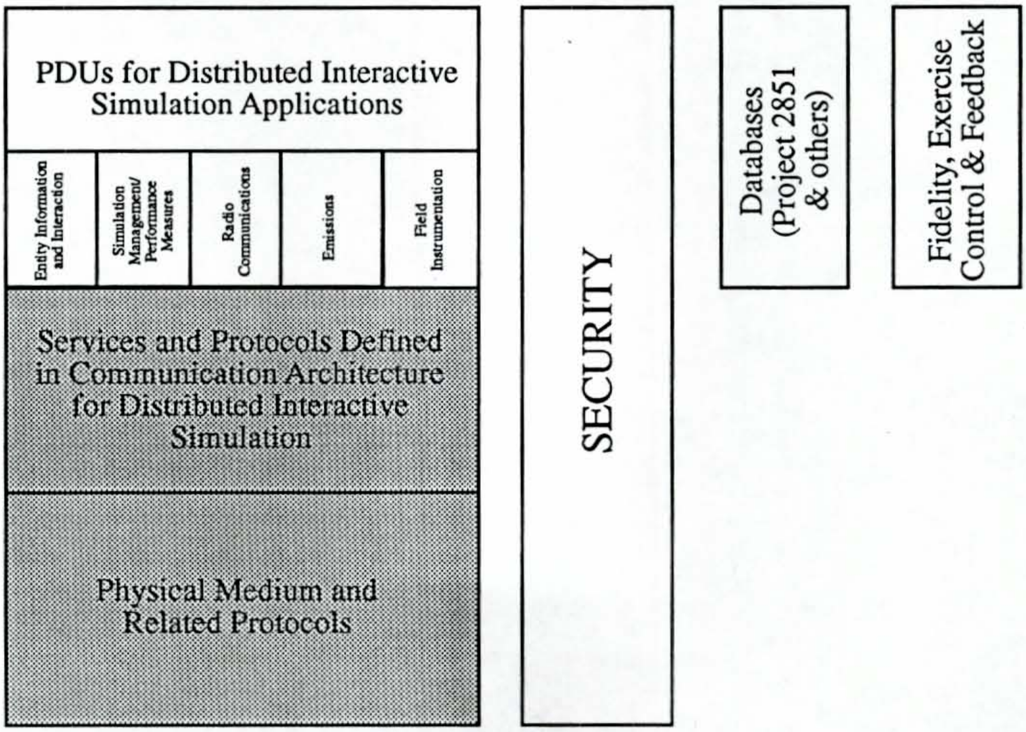
DISTRIBUTED INTERACTIVE SIMULATION

[CADIS]

"NOTE: This draft, dated March 1994, prepared by the Institute for Simulation and Training for STRICOM, has not been approved and is subject to modification. DO NOT USE PRIOR TO APPROVAL."

FOREWORD

This standard is part of a set of standards for Distributed Interactive Simulation (DIS). The relationship between this standard and other DIS standards is shown in the figure below.



0447-5159

Documentation Relationships

This set of standards deals with requirements for simulations participating in a Distributed Interactive Simulation. There are several elements that make up the DIS environments. Each element is addressed by one or more standard documents. Used together, these standards will define an interoperable simulated battle environment.

The main elements addressed by these standards are:

(1) Communications
(2) Simulation Environment
(3) Fidelity, Exercise Control, and Feedback Requirements

The scope of this document lies within the first element, Communications. Its purpose is to define the requirements for the communication architecture to be used to support distributive interactive simulation applications. This document makes recommendations concerning the communication profiles that can provide the services to meet those requirements.

A related draft standard, the "Standard for Interactive Simulation - Protocols for Distributed Interactive Simulation Applications"[1], defines the data messages that are exchanged between simulation applications. These Protocol Data Units (PDUs) provide data concerning simulated entity states and the types of entity interactions that take place in a DIS exercise.

In the second element, Simulation Environment, the government's Project 2851 is providing a military standard describing database formats for terrain, culture, and dynamic model representation. The draft military standard "Standard Simulator Data Base (SSDB) and Interchange Format (SIF) for High Detail Input/Output (SIF/HDI) and Distributed Processing (SIF/DP)" is recommended for use with the developing DIS standards.

The required fidelity correlation between simulations in a DIS exercise is addressed in the draft standard "Fidelity Correlation Requirements for Distributed Interactive Simulation". The proposed method for setup and control of a DIS exercise and providing feedback at the end is addressed in the draft standard "Exercise Control and Feedback Requirement".

The Communication Architecture/Security Subgroup that developed this standard had the following membership during the development cycle:

Kevin Boner, Christina Bouwens, Jerry Burchfiel, Danny Cohen, Claus Crassous de Medeuil, Wim DeJong, Ron Deluca, Debra Deutsch, Ken Doris, Mark Eliot, Allen Farrington, Edward Feustel, Thomas Gehl, Dave Gobuty, Victor Griswold, Dale Guhse, Amnon Katz, Al Kerecman, John Kirkpatrick, Wayne Lindo, Margaret Loper, Ben Mackey, Richard Mecklenborg, William Miller, Walter Milliken, Richard Modjeski, James Moulton, Edward Oswald, Willie Price, Ray Rhode, Mark Riecken, Robert Romalewski, William Rowan, Richard Schantz, Steve Seidensticker, James Sleeth, Amy Vanzant-Hodge, Gary Warden, and David Wood.

This draft standard has been prepared by the Institute for Simulation and Training for the Simulation, Training and Instrumentation Command (STRICOM), the Advanced Research Projects Agency (ARPA), and the Defense Modeling and Simulation Office (DMSO). This draft is based on currently available technical information but it has not been approved for promulgation. It is subject to modification. However, pending its promulgation as a coordinated standard, it may be used.

Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Danette Haworth, Institute for Simulation and Training, 3280 Progress Drive, Orlando, FL 32826. Use the self-addressed Standardization Document Improvement Proposal Form that appears at the end of this document or send comments by letter.

---

[1] This is an extension of earlier version: "Standard for Information Technology Protocols for Distributed Interactive Simulation Applications, Entity Information and Interaction" This is also referred to in this document as the PDU Standard.

TABLE OF CONTENTS

LIST OF FIGURES

Figures

1. SCOPE

1.1 Scope. This standard establishes the requirements for the communication architecture to be used in a Distributed Interactive Simulation application. This standard supports the DIS PDU standard through IEEE P1278.1 (draft version 2.0.4). This standard may be used for later versions of the PDU standard but it has not been reviewed for consistency with later versions. References in this document to the DIS PDU standard shall mean IEEE P1278.1 (draft version 2.0.4) or earlier.

1.2 Application. This document has three main purposes. The first purpose is to provide government agencies that are procuring DIS applications with the information necessary to write specifications. As such, the document establishes a series of standards for network services, protocols, and network performance. When invoked in a specification or statement of work, these requirements will apply to the communication architecture supporting simulation devices, stimulation devices, and wargame simulations intended for participation in a Distributed Interactive Simulation (DIS).

The second purpose of this document is to provide system designers with the information necessary to develop key areas of the system.

A third purpose is to provide the characteristics of communications service that will be required when interconnecting DIS applications at different locations.

The strategy for OSI compliance is based on a phased, evolutionary approach. The first step to this evolution is the recommendation of an interim protocol suite that provides the services of the above layers; this step is based on available network products and services and is capable of supporting current exercises. A transition to OSI/GOSIP standards will then occur over a period of years, as protocol standards are adopted to support DIS.

1.3 Key Assumptions For This Standard. This document makes a number of assumptions about underlying requirements of the DIS application and how they will be applied. The assumptions are explained below.

1.3.1 Long Haul Connection. Simulators at different sites will be connected via a Wide Area Network (WAN). This document defines the functional and performance characteristics which will be satisfied by the communications service, including the WAN.

1.3.2 Multiple Exercises. DIS has the ability to accommodate multiple exercises over the network by assigning each exercise a different exercise ID. Those entities participating in the exercise will be assigned exercise IDs by a mechanism outside the scope of this standard.

1.3.3 Non-PDU[2] Traffic. The communication architecture is specified to support several types of data transmission as stated earlier. This data may be directly related to DIS applications or not.

---

[2] non-PDU (Protocol Data Unit) refers to non-DIS traffic.

1.3.4 Communication Management Requirements. This standard does not recommend or preclude the use of network management protocols.

1.3.5 Security. This Standard provides intersite and intrasite interoperability between DIS participants. This Standard neither provides, nor precludes, specific security requirements. In this way, security is as an attribute of those exercises which process unclassified sensitive or classified information, and that use this Standard for interoperability. From a DIS perspective the owners of specific systems and exercises must independently assess their security threats and resulted vulnerabilities. Thereafter, they are responsible for implementing appropriate countermeasures in accordance with the system- or exercise-specific security policy in effect.

2. GENERAL REFERENCES

The following documents are referenced in this Standard:

FIPS PUB 146-1 April 1991	U.S. Government Open Systems Interconnection Profile (GOSIP)Version 2.0. This is available from: U.S. Department of Commerce National Technical Information Service (NTIS) 5285 Port Royal Road Springfield, VA 22161
IST-CR-93-40 February 1994	Standard for Distributed Interactive Simulation -- Application Protocols Version 2.0.4
IEEE 802-1990	Standards for Local and Metropolitan Area Networks Overview and Architecture
ISO 7498-1984	Information Processing Systems - Open Systems Interconnection - Basic Reference Model. This is available from: ISO Central Secretariat 1 rue de Varembe Case Postale 56 CH1211 Geneva 20 Switzerland/Suisse and from: American National Standards Institute (ANSI) Sales Department 11 West 42nd Street New York, NY 10036 USA Telephone: 212-642-4900

IST-CR-93-42 November 1993	Rationale Document Draft Communication Architecture for Distributed Interactive Simulation (CADIS)
	All IST Documents can be obtained from: University of Central Florida Center for Continuing Education Orlando, Florida 32816-0177 USA Telephone: 407-249-6100
IST-CR-92-21 November 1992	Guidance Document Draft Communication Architecture for Distributed Interactive Simulation (CADIS)
RFC 1305 March 1992	Network Time Protocol (Version 3) Specification, Implementation, and Analysis.
	See Appendix A for information on how to obtain RFCs.
RFC 1123	Requirements for Internet Hosts -October 1989Application and Support.
RFC 1122 October 1989	Requirements for Internet Hosts - Communication Layer Requirements for Internet Hosts Communication Layers.
RFC 1112 August 1989	Host Extensions for IP Multicasting.
RFC 793 September 1981	Transmission Control Protocol (TCP).
RFC 791 September 1981	Internet Protocol (IP).
RFC 768 August 1980	User Datagram Protocol (UDP).

3. DEFINITIONS

3.1 Acronyms used in this standard. The acronyms used in this standard are defined as follows:

ANSI	-	American National Standards Institute
ARPA	-	Advanced Research Projects Agency
BER	-	Bit Error Rate
CCITT	-	International Telegraph and Telephone Consultative Committee
CMIP	-	Common Management Information Protocol
CMIS	-	Common Management Information Services
COTS	-	Commercial Off The Shelf
DIS	-	Distributed Interactive Simulation
DMSO	-	Defense Modeling and Simulation Office
FDDI	-	Fiber Distributed Data Interface
GOSIP	-	Government Open Systems Interconnection Profile
IEEE	-	Institute of Electrical and Electronics Engineers
IGMP	-	Internet Group Management Protocol
IP	-	Internet Protocol
ISO	-	International Organization for Standardization
LAN	-	Local Area Network
NIST	-	National Institute for Standards and Technology
OSI	-	Open Systems Interconnection
PDU	-	Protocol Data Unit
RFC	-	Request For Comment
SIMNET	-	Simulation Network: An R&D effort whichdemonstrated the ability of simulators to interact dynamically over a LAN.
STRICOM	-	U.S. Army Simulation, Training, and Instrumentation Command (formally PMTRADE)
TCP	-	Transmission Control Protocol
UCF/IST	-	University of Central Florida / Institute for Simulation and Training
UDP	-	User Datagram Protocol
WAN	-	Wide Area Network

3.2 Application interface. The programming access mechanism to the communication resources of a network.

3.3 Application layer (layer 7). The layer of the ISO reference model which provides the means for user application processes to access and use the network's communications resources.

3.4 Best effort service. A communication service in which transmitted data is not acknowledged. Such data typically arrives in order, complete, and without errors. However, if an error occurs or a packet is not delivered, nothing is done to correct it (e.g., there is no retransmission).

3.5 Broadcast mode (BC). A transmission mode in which a single message is sent to all network destinations, i.e. one-to-all. Broadcast is a special case of multicast.

3.6 Connectionless (CL). A mode of information transfer between peer entities in which each data transfer is independent of and not coordinated with previous or subsequent transfers and in which no state information has to be maintained.

3.7 Connection-oriented (CO). A mode of information transfer between peer entities in which a logical association is established prior to the exchange of data and which is maintained for the lifetime of the exchange process.

3.8 Datagram. A unit of data that is transferred as a single, non-sequenced, unacknowledged unit.

3.9 Distributed Interactive Simulation (DIS). A time and space coherent synthetic representation of world environments designed for linking the interactive, free play activities of people in operational exercises. The synthetic environment is created through real time exchange of data units between distributed, computationally autonomous nodes comprised of entities in the form of simulations, simulators and instrumented equipment interconnected through standard computer communicative services. The computational nodes may be present in one location or may be distributed geographically.

3.10 Emitter. A device that is able to discharge detectable electromagnetic or acoustic energy.

3.11 Exercise. See Simulation Exercise.

3.12 Host or Host computer. A computer that supports one or more simulation applications. All host computers participating in a simulation exercise are connected by a common network.

3.13 Interoperability. The capability, promoted but not guaranteed by joint conformance with a given set of standards, that enables heterogeneous equipment, generally built by various vendors, to work together in a network environment.

3.14 Link layer (layer 2). The layer of the ISO reference model which provides the functional and procedural means to transfer data between stations, and to detect and correct errors that may occur in the physical layer.

3.15 Local Area Network (LAN). A communications network designed for a moderate size geographic area and characterized by moderate to high data transmission rates, low delay, and low bit error rates.

3.16 Long-Haul network. See Wide Area Network.

3.17 Loosely coupled. A condition that exists when simulation entities are not involved in very close interaction such that every action of an entity does not need to be immediately accounted for by the other entities. Two tanks moving over terrain a mile apart from each other is an example of a loosely coupled situation.

3.18 Multicast mode (MC). A transmission mode in which a single message is sent to multiple network destinations, i.e. one-to-many.

3.19 Network layer (layer 3). The layer of the ISO reference model which performs those routing and relaying services necessary to support data transmission over interconnected networks.

3.20 Network management. The collection of administrative structures, policies and procedures which collectively provide for the management of the organization and operation of the network as a whole.

3.21 Node. A general term denoting either a switching element in a network or a host computer attached to a network.

3.22 Non-Real time service. Any service function which does not require real time service. (see 3.30)

3.23 ISO Reference Model (ISORM). A model that organizes the data communication concept into seven layers and defines the services that each layer provides.

3.24 Peer. Elements of a distributed system that communicate with each other using a common protocol.

3.25 Physical layer (layer 1). The layer of the ISO reference model which provides the mechanical, electrical, functional, and procedural characteristics access to the transmission medium.

3.26 Presentation layer (layer 6). The layer of the ISO reference model which frees the application processes from concern with differences in data representation.

3.27 Protocol. A set of rules and formats (semantic and syntactic) which determines the communication behavior of peers in the performance of functions.

3.28 Protocol Data Unit (PDU). A unit of data specified in a protocol and consisting of protocol-information and user-data. The term is used in this standard to refer to application layer PDUs as defined in DIS PDU Standard that are passed on a network between application processes.

3.29 Protocol suite. A defined set of complementary protocols within the communication architecture profile.

3.30 Real time. An event or data transfer in which, unless accomplished within an allotted amount of time, the accomplishment of the action has either no value or diminishing value.

3.31 Real time service. A service which satisfies timing constraints imposed by the service user. The timing constraints are user specific and should be such that the user will not be adversely affected by delays within the constraints.

3.32 Reliable service. A communication service in which the received data is guaranteed to be exactly as transmitted.

3.33 Session layer (layer 5). The layer of the ISO reference model which provides the mechanisms for organizing and structuring the interaction between two entities.

3.34 Simulation Application. A computer generated representation of real world phenomena for the purpose of training or experimentation. Examples of simulation applications include vehicle simulators, computer generated forces, or a computer interface between the network and real equipment.

3.35 Simulation Entity. An element of a simulated world (such as a vehicle) that is generated and controlled by one or more host computers. An entity may also be an element of the simulated world (such as cultural features including buildings and bridges) that may be subject to changes in appearance as a result of the simulation exercise.

3.36 Simulation Exercise. A simulation exercise consists of one or more interacting simulation applications. Simulations participating in the same simulation exercise share a common identifying number called the Exercise Identifier.

3.37 Simulation Host. See Host.

3.38 Simulation Site. Location of one or more simulation hosts connected by a LAN.

3.39 Tightly Coupled. A condition that exists when simulation entities are involved in very close interaction such that every action of an entity must be immediately accounted for by the other entities. Several tanks in close formation involved rapid, complicated maneuvers over the terrain is an example of a tightly coupled situation.

3.40 Transport layer (layer 4). The layer of the ISO reference model which accomplishes the transparent transfer of data over the established link, providing an end-to-end service with high data integrity.

3.41 Wide Area Network (WAN). A communications network designed for large geographic areas. Sometimes called Long-Haul Network.

3.42 Unicast mode (UC). A transmission mode in which a single message is sent to a single network destination, i.e. one-to-one.

4. GENERAL REQUIREMENTS

This section presents the general requirements for DIS communication services and consists of three major areas; communication architecture overview, service requirements, and protocol suites. Specific requirements are stated in section 5.

4.1 Communication Architecture Overview. The purpose of the communication subsystem for 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 information from other simulators. This standard 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 PDU Standard are the common language by which simulation hosts can communicate. This includes simulators of different and unrelated design and architecture, instrumented platforms, and wargame simulations. No restriction is placed on what the participating simulator or site is, only on the way it communicates within a DIS exercise.

Where the DIS PDUs define the information passed between simulation hosts, this standard defines how those simulation hosts 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.

4.2 Service Requirements. This section describes the services required to be provided by the communication architecture for DIS applications. These services are divided into three categories: communication requirements, performance requirements, and error detection. The communication requirements are based on experience with state-of-the-art distributed simulation activities as well as projections based on anticipated use and evolution of the technology base.

4.2.1 Communication Service Requirements. DIS environment support requires control and data communications. Data communications may be with or without real time requirements and may be augmented to include voice, video and other forms of pictorial information. Upon the introduction of each of these forms of traffic, they shall be able to share communications facilities instead of having disjoint facilities for each.

4.2.1.1 Service Requirements of PDUs. Each DIS PDU requires certain services to make its communication practical. These services are grouped into broad classes of operation for DIS.

Best Effort Multicast, non-time sensitive
A mode of operation where the multicast service provider uses no added mechanisms for reliability except those inherent in the underlying service.

Best Effort Multicast, time sensitive
A mode of operation where the multicast service provider uses no added mechanisms for reliability except those inherent in the underlying service. The service provider will also ensure that the underlying service adheres to the latency requirements outlined in 5.2.2.

Best Effort Unicast, non-time sensitive
A mode of operation where the unicast service provider uses no added mechanisms for reliability except those inherent in the underlying service.

Best Effort Unicast, time sensitive
A mode of operation where the unicast service provider uses no added mechanisms for reliability except those inherent in the underlying service. The service provider will also ensure that the underlying service adheres to the latency requirements outlined in 5.2.2.

Reliable Unicast
A mode of operation where the unicast service provider uses whatever mechanisms are available to ensure that the data is delivered in sequence with no duplicates and no detected errors. Reliable Unicast service is not required to adhere to the latency requirements outlined in 5.2.2.

4.2.1.2 Multicasting. Multicast addressing shall be supported. The capability of a single simulation to send PDUs to a group of other simulation hosts is a fundamental requirement of a network supporting DIS exercises.

4.2.2 Performance Requirements

4.2.2.1 Network Bandwidth. Network bandwidth requirements are subject to estimation procedures based on the latest available data on networked simulations. See the Guidance Document for a detailed explanation of bandwidth estimation procedures.

4.2.2.2 Latency. Proper operation of many DIS systems require strictly bounded network latency. The DIS communications architecture shall specify latency requirements for time sensitive information.

4.2.3 Error Detection. The DIS communications architecture shall include mechanism(s) to detect corrupted PDUs.

4.2.4 Synchronization. If the DIS communication architecture is supporting a DIS simulation application using absolute time, the DIS communication architecture shall include a mechanism(s) to synchronize simulation applications.

4.3 Approach to Communication Architecture. The communications architecture for DIS employs a layered model which is based on the seven layer OSI Reference Model (ISORM) (see ISO 7498). The ISO 7498 standard defines the communication functions of the network by dividing them into a hierarchical set of layers. Each layer performs an integral subset of special functions required to communicate with another layer of similar type. There are seven layers in the ISORM: Application, Presentation, Session, Transport, Network, Link, and Physical (Layers 7-1, respectively).

The DIS functions provided by each layer are summarized below:

Number	Name	Example Content
7	Application	Kind of data exchanged (position, orientation,...) Dead reckoning rules. 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. Rules for joining and leaving an exercise, and freezing an exercise.
4	Transport	Addressing from end user to end user. Assuring communications reliability, if required.
3	Network	Addressing information from host to host.
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.

4.3.1 Communication Architecture Protocol Suites for DIS. The DIS communication architecture shall evolve in three phases. Each phase of evolution uses a different suite of communication protocols.

Phase 1 is based upon products and services currently available and widely used. Phase 2 is based upon OSI protocols, and Phase 3 is based upon full GOSIP compliance. Phase 2 and Phase 3 are not included in this standard because they contain protocols that have not yet been standardized. When needed protocols are defined and accepted by a recognized standards body, these protocol suites shall be included in this Standard. The proposed protocol suites for Phase 2 and Phase 3 are currently included in the Rationale Document.

5. DETAILED REQUIREMENTS

This section contains specific requirements for DIS. These requirements are *Mandatory* for DIS compliance. In addition, several requirements which are identified as *Recommended* which include those requirements that should be met in order to support large-scale DIS applications.

5.1 Communication Architecture Overview. The communication architecture requirements consist of a set of specific service requirements, and a protocol suite that supports those requirements.

5.2 Service Requirements.

5.2.1 Communication Service Requirements

5.2.1.1 Service Requirements of PDUs. Five classes of communications service are available for use with the DIS PDU Standard: CLASS 1, Best Effort Multicast, non-time sensitive; CLASS 2, Best Effort Multicast, time sensitive; CLASS 3, Best Effort Unicast, non-time sensitive; CLASS 4, Best Effort Unicast, time sensitive; and CLASS 5, Reliable Unicast. These service classes are defined in 4.2.1.

5.2.1.2 Multicasting. The multicast addressing capability of a DIS-compliant network has the characteristics defined in the following sections.

5.2.1.2.1 Broadcast. The minimal form of Best Effort Multicast services to support DIS shall consist of transmitting to a group consisting of all hosts on a LAN simultaneously.

5.2.1.2.2 Multicast Services. For networks employing multicast service beyond the minimal form, these services shall be required to support DIS.

a. A multicast group shall be able to include members anywhere on the network.

b. The maximum number of members in a single multicast group shall be large enough to encompass all hosts within the DIS system supported by the multicast network.

c. The simulation application need know nothing about a group except the address of the multicast group to which it is sending PDUs.

d. The multicast service shall have the capability to support multiple, independent exercises sharing the same networks.

5.2.1.2.3 Recommended Multicast Services. These services are not required but are recommended for compatibility with future phases.

a. A simulation application should be able to belong to more than one multicast group at the same time. The maximum number of groups to which a simulation application may belong at any one time is not defined.

b. A simulation application should be able to drop its membership from a group and/or join another at will. The time required to drop or join membership should be the minimum possible.

c. Change in membership of a multicast group should be entirely initiated by the simulation application.

d. The number of multicast groups should be exercise dependent and is envisioned to be on the order of several hundred.

e. IGMP (RFC 1112) should be used for group membership.

5.2.2 Performance Requirements.

5.2.2.1 Network Bandwidth Requirements. Network bandwidth requirements are exercise specific and should be determined on a per exercise basis. See the Guidance Document for recommended estimation procedures.

5.2.2.2 Latency Requirements. The following latency requirements shall not be exceeded for CLASS 2 and CLASS 4 services:

100 milliseconds	Total latency permitted between the output of a PDU at the application level of a simulator and input of that PDU at the application level of any other simulator when that exercise contains simulated units whose interactions may be tightly coupled.
300 milliseconds	Total latency permitted between the output of a PDU at the application level of a simulator and input of that PDU at the application level of any other simulator when that exercise contains only simulated units whose interactions are not tightly coupled (i.e., loosely coupled).
50 milliseconds	Maximum dispersion of arrival times of the PDUs carrying voice information at the application level of the device converting digital voice to analog.
10 milliseconds	Maximum latency between the application and physical layers of any DIS simulator.

Figure 1 summarizes the latency standards.

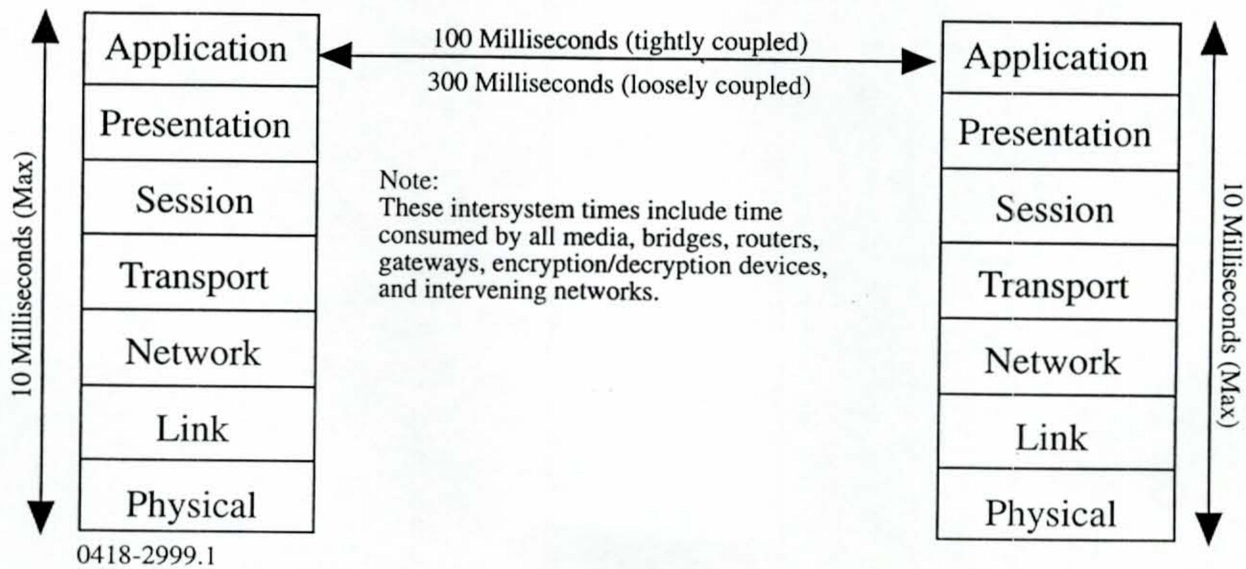


Figure 1. Standard Latency Values

5.2.3 Error Detection. In Phase 1, error detection shall be handled by the UDP and TCP checksums.

5.2.4 Synchronization. If the DIS communication architecture is supporting a DIS simulation application using absolute time, the following functions shall be required to support the DIS simulation application:

a. Each DIS exercise shall provide a time server to provide master time for the exercise.

b. The time server time shall be UTC within a tolerance to be defined by the exercise (the recommended value is 50 ms).

5.3 The Communication Architecture Protocol Suite for DIS. This section lists the specific requirements for the protocol suites.

5.3.1 Phase 1 - Initial Internet Protocol Suite. The Phase 1 protocol suite is based on current Internet network products and communications service. Under Phase 1, Best Effort Multicast (both CLASS 1 and CLASS 2 service) shall be implemented with directed broadcast

addresses; where services beyond broadcast are required, UDP / IP Multicast shall be used. Best Effort Unicast (both CLASS 3 and CLASS 4) shall be implemented using UDP / IP. Reliable Unicast shall be implemented using TCP over IP. This service can be used to support current exercises and early implementations of DIS applications. At each site there shall be a Local Area Network (LAN) with a local broadcast capability. For testing, demonstrations, and exercises involving multiple sites, the LANs shall be interconnected using a Wide Area Network (WAN) that can provide the required communications services at those locations. The Phase 1 protocol suite is as shown below.

Layer	Name	Content
7	Application	- DIS (DIS PDU Standard) - NTP (RFC 1119) provides global clock synchronization
6	Presentation	- DIS (DIS PDU Standard)
5	Session	- DIS (DIS PDU Standard)
4	Transport	- UDP (RFC 768) provides best-effort transport - TCP (RFC 793) provides reliable unicast transport
3	Network	- IP (RFC 791) - IP/MC (RFC 1112)
2	Link	- any LAN protocol(s) that supports the level 3 protocol in use
1	Physical	- any LAN protocol(s) that supports the level 2 protocol in use

Each simulator shall support IP with UDP and TCP. TCP provides reliable unicast service while UDP provides the best effort multicast service.

This Standard does not specify the physical layer media and data link layer protocols to be used since these choices are to be implementation dependent.

5.3.1.1 Host Requirements. Each host shall comply with the Hosts Requirements RFC (currently RFC 1122 and RFC 1123). In addition, each host shall support:

a. IP reassembly of datagrams, with MMS-R equal to at least 8192 octets and preferably indefinite (see RFC 1122, section 3.3.2).

b. IP limited and directed broadcast address (RFC 1122, section 3.3.6).

c. IP multicast address (where services beyond broadcast are provided) and IGMP (RFC 1122, section 3.3.7).

d. Checksum (RFC 1122, section 4.1.3.4).

5.3.1.2 Receipt of PDUs.

5.3.1.2.1 PDU Encapsulation. Every host shall be able to receive multiple DIS PDUs concatenated inside a single UDP datagram.

5.3.1.2.2 PDU Size. Each host shall be capable of receiving DIS PDUs as defined in 5.3.1.1 (a) and 5.3.1.3.

5.3.1.3 Transmission of PDUs. The simulation application shall support a configuration parameter for maximum DIS PDU size and maximum concatenated PDU size (if the application concatenates PUDs). It is recommended that the maximum size of DIS PDUs or concatenated DIS PDUs be no larger than 1400 octets.

Appendix A

How To Obtain Internet Request For Comment (RFC) Documents

A1. Introduction

RFCs may be obtained via EMAIL, FTP, UUCP, or US Mail from many RFC Repositories.

There is no charge for RFCs retrieved via EMAIL and/or FTP.

The Primary Repositories will have the RFC available when it is first announced, as will many Secondary Repositories. Some Secondary Repositories may take a few days to make available the most recent RFCs.

A2. RFCs Via EMAIL

A2.1. RFC-INFO@ISI.EDU

Address the request to "rfc-info@isi.edu" with a message body of:

```
Retrieve: RFC
Doc-ID: RFCnnnn
```

Where "nnnn" refers to the number of the RFC (always use 4 digits - the DOC-ID of RFC-822 is "RFC0822").

The RFC-INFO@ISI.EDU server provides other ways of selecting RFCs based on keywords and such; for more information send a message to "rfc-info@isi.edu" with the message body "help: help".

contact: RFC-Manager@ISI.EDU

A2.2. MAIL-SERVER@NISC.SRI.COM

Address the request to MAIL-SERVER@NISC.SRI.COM and in the body of the message indicate the RFC to be sent: "send rfcNNNN" or "send rfcNNNN.ps" where NNNN is the RFC number. Multiple requests may be included in the same message by listing the "send" commands on separate lines. To request the RFC Index, the command should read: send rfc-index.

contact: rfc-update@nisc.sri.com

A2.3. NIS-INFO@NIS.NSF.NET

Address the request to NIS-INFO@NIS.NSF.NET and leave the subject field of the message blank. The first text line of the message must be "send rfcnnnn.txt" with nnnn the RFC number.

contact: rfc-mgr@merit.edu

A2.4. SENDRFC@JVNC.NET

Address the request to SENDRFC@JVNC.NET and in the subject field of the message indicate the RFC number, as in "Subject: RFCnnnn" where nnnn is the RFC number. Please note that RFCs whose number are less than 1000 need not place a "0". (For example, RFC932 is fine.) No text in the body of the message is needed.

contact: Becker@NISC.JVNC.NET

A2.5. INFO-SERVER@DOC.IC.AC.UK

Address the request to info-server@doc.ic.ac.uk with a Subject: line of "wanted" and a message body of:

```
request sources
topic path rfc/rfcnnnn.txt.Z
request end
```

(Where "nnnn" refers to the number of the RFC.) Multiple requests may be included in the same message by giving multiple "topic path"
commands on separate lines. To request the RFC Index, the command should read: topic path rfc/rfc-index.txt.Z

contact: ukuug-soft@doc.ic.ac.uk

A3. RFCs Via FTP

Primary Repositories:

RFCs can be obtained via FTP from NIC.DDN.MIL, FTP.NISC.SRI.COM, NIS.NSF.NET, NISC.JVNC.NET, VENERA.ISI.EDU, WUARCHIVE.WUSTL.EDU, SRC.DOC.IC.AC.UK, or FTP.CONCERT.NET.

A3.1. NIC.DDN.MIL (aka DIIS.DDN.MIL)

RFCs can be obtained via FTP from NIC.DDN.MIL, with the pathname rfc/rfcnnnn.txt (where "nnnn" refers to the number of the RFC). Login with FTP username "anonymous" and password "guest".

contact: ScottW@NIC.DDN.MIL

A3.2. FTP.NISC.SRI.COM

RFCs can be obtained via FTP from FTP.NISC.SRI.COM, with the pathname rfc/rfcnnnn.txt or rfc/rfcnnnn.ps (where "nnnn" refers to the number of the RFC). Login with FTP username "anonymous" and password "guest". To obtain the RFC Index, use the pathname rfc/rfc-index.txt.

contact: rfc-update@nisc.sri.com

A3.3. NIS.NSF.NET

To obtain RFCs from NIS.NSF.NET via FTP, login with username "anonymous" and password "guest"; then connect to the directory of RFCs with cd /internet/documents/rfc. The file name is of the form rfcnnnn.txt (where "nnnn" refers to the RFC number).

contact: rfc-mgr@merit.edu

A3.4. NISC.JVNC.NET

RFCs can also be obtained via FTP from NISC.JVNC.NET, with the pathname rfc/RFCnnnn.TXT.v (where "nnnn" refers to the number of the RFC and "v" refers to the version number of the RFC).

contact: Becker@NISC.JVNC.NET

A3.5. VENERA.ISI.EDU

RFCs can be obtained via FTP from VENERA.ISI.EDU, with the pathname in-notes/rfcnnnn.txt (where "nnnn" refers to the number of the RFC). Login with FTP username "anonymous" and password "guest".

contact: RFC-Manager@ISI.EDU

A3.6. WUARCHIVE.WUSTL.EDU

RFCs can also be obtained via FTP from WUARCHIVE.WUSTL.EDU, with the pathname info/rfc/rfcnnnn.txt.Z (where "nnnn" refers to the number of the RFC and "Z" indicates that the document is in compressed form).

At WUARCHIVE.WUSTL.EDU the RFCs are in an "archive" file system and various archives can be mounted as part of an NFS file system. Please contact Chris Myers (chris@wugate.wustl.edu) if you want to mount this file system in your NFS.

contact: chris@wugate.wustl.edu

A3.7. SRC.DOC.IC.AC.UK

RFCs can be obtained via FTP from SRC.DOC.IC.AC.UK with the pathname rfc/rfcnnnn.txt.Z or rfc/rfcnnnn.ps.Z (where "nnnn" refers to the number of the RFC). Login with FTP username "anonymous" and password "your-email-address". To obtain the RFC Index, use the pathname rfc/rfc-index.txt.Z. (The trailing .Z indicates that the document is in compressed form.)

The archive is also available using NIFTP and the ISO FTAM system.

contact: ukuug-soft@doc.ic.ac.uk

A3.8. FTP.CONCERT.NET

To obtain RFCs from FTP.CONCERT.NET via FTP, login with username "anonymous" and your internet e-mail address as password. The RFCs can be found in the directory /rfc, with file names of the form: rfcNNNN.txt or rfcNNNN.ps where NNNN refers to the RFC number.

This repository is also accessible via WAIS and the Internet Gopher.

contact: rfc-mgr@concert.net

A3.9 Secondary Repositories

Sweden

Host:	sunic.sunet.se
Directory:	rfc
Host:	chalmers.se
Directory:	rfc

Germany

Site:	University of Dortmund
Host:	walhalla.informatik.uni-dortmund.de
Directory:	pub/documentation/rfc
Notes:	RFCs in compressed format

France

Site:	Institut National de la Recherche en Informatique et Automatique (INRIA)
Address:	info-server@inria.fr
Notes:	RFCs are available via email to the above address. Info Server manager is Mireille Yamajako (yamajako@inria.fr).

Netherlands

Site:	EUnet
Host:	mcsun.eu.net
Directory:	rfc
Notes:	RFCs in compressed format.

Finland

Site:	FUNET
Host:	funet.fi
Directory:	rfc
Notes:	RFCs in compressed format. Also provides email access by sending mail to archive-server@funet.fi.

Norway

Host:	ugle.unit.no
Directory:	pub/rfc

Denmark

Site:	University of Copenhagen
Host:	ftp.diku.dk (freja.diku.dk)
Directory:	rfc

Australia and Pacific Rim

Site:	munnari
Contact:	Robert Elz <kre@cs.mu.OZ.AU>
Host:	munnari.oz.au
Directory:	rfc
	rfc's in compressed format rfcNNNN.Z postscript rfc's rfcNNNN.ps.Z

United States

Site:	cerfnet
Contact:	help@cerf.net
Host:	nic.cerf.net
Directory:	netinfo/rfc

Site:	uunet
Contact:	James Revell <revell@uunet.uu.net>
Host:	ftp.uu.net
Directory:	inet/rfc

United States / Mexico

Site:	SESQUINET
Contact:	rfc-mgr@sesqui.net
Host:	nic.sesqui.net
Directory:	pub/rfc

UUNET Archive

UUNET archive, which includes the RFC's, various IETF documents, and other information regarding the internet, is available to the public via anonymous ftp (to ftp.uu.net) and anonymous uucp, and will be available via an anonymous kermit server soon. Get the file /archive/inet/ls-IR.Z for a listing of these documents.

A4. RFCs Via UUCP

Any site in the US running UUCP may call +1 900 GOT SRCS and use the login "uucp". There is no password. The phone company will bill you at $0.50 per minute for the call. The 900 number only works from within the US.

A5. RFCs Via US Mail

Address requests for hard copies (and/or CD-ROM) to:

NISC
SRI International
333 Ravenswood Ave
Menlo Park ca 94025

or call 415-859-6387/3695, or fax to 415-859-6028,
or send email to nisc@nisc.sri.com