NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

GOVERNMENT OPEN SYSTEMS
INTERCONNECTION PROFILE (GOSIP)
TRANSITION STRATEGY

by

Mark R. Laxen

September, 1993

Co-Advisor: Myung Suh
Co-Advisor: Barry Frew

UNCLASSIFIED

Security Classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification: UNCLASSIFIED			1b Restrictive Markings	
2a Security Classification Authority			3 Distribution/Availability of Report Approved for public release; distribution is unlimited.	
2b Declassification/Downgrading Schedule				
4 Performing Organization Report Number(s)			5 Monitoring Organization Report Number(s)	
6a Name of Performing Organization Naval Postgraduate School	6b Office Symbol *(if applicable)* 37		7a Name of Monitoring Organization Naval Postgraduate School	
6c Address *(city, state, and ZIP code)* Monterey CA 93943-5000			7b Address *(city, state, and ZIP code)* Monterey CA 93943-5000	
8a Name of Funding/Sponsoring Organization	6b Office Symbol *(if applicable)*		9 Procurement Instrument Identification Number	
Address *(city, state, and ZIP code)*			10 Source of Funding Numbers	
			Program Element No	Project No / Task No / Work Unit Accession No
11 Title *(include security classification)* Government Open Systems Interconnection Profile (GOSIP) Transition Strategy (Unclassified)				
12 Personal Author(s) Mark R. Laxen				
13a Type of Report Master's Thesis	13b Time Covered From To		14 Date of Report *(year, month, day)* 1993, September	15 Page Count 112
16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
17 Cosati Codes			18 Subject Terms *(continue on reverse if necessary and identify by block number)* GOSIP, OSI, Open Systems, Transition, Interoperability, Network Architectures, Standards Organizations.	
Field	Group	Subgroup		

19 Abstract *(continue on reverse if necessary and identify by block number)*

This thesis analyzes the Government Open Systems Interconnection Profile (GOSIP) and the requirements of the Federal Information Processing Standard (FIPS) Publication 146-1. It begins by examining the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) architecture and protocol suites and the distinctions between GOSIP version 1 and 2. Additionally, it explores some of the GOSIP protocol details and discusses the process by which standards organizations have developed their recommendations. Implementation considerations from both government and vendor perspectives illustrate the barriers and requirements faced by information systems managers, as well as basic transition strategies. The result of this thesis is to show a transition strategy through an extended and coordinated period of coexistence due to extensive legacy systems and GOSIP product unavailability. Recommendations for GOSIP protocol standards to include capabilities outside the OSI model are also presented.

20 Distribution/Availability of Abstract X unclassified/unlimited __ same as report __ DTIC users	21 Abstract Security Classification UNCLASSIFIED	
22a Name of Responsible Individual Myung Suh	22b Telephone *(include Area Code)* (408) 656-2637	22c Office Symbol AS/SU

DD FORM 1473,84 MAR 83 APR edition may be used until exhausted

All other editions are obsolete

security classification of this page

UNCLASSIFIED

Approved for public release; distribution is unlimited.

GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE (GOSIP) TRANSITION STRATEGY

by

Mark R. Laxen
Lieutenant, United States Navy
B.S., Northwestern University, 1987

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1993

Author: _____
Mark R. Laxen

Approved by: _____
Myung Suh, Co-Advisor

_____
Barry Frew, Co-Advisor

_____
David R. Whipple, Jr., Chairman
Department of Administrative Sciences

ABSTRACT

This thesis analyzes the Government Open Systems Interconnection Profile (GOSIP) and the requirements of the Federal Information Processing Standard (FIPS) Publication 146-1. It begins by examining the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) architecture and protocol suites and the distinctions between GOSIP version 1 and 2. Additionally, it explores some of the GOSIP protocol details and discusses the process by which standards organizations have developed their recommendations. Implementation considerations from both government and vendor perspectives illustrate the barriers and requirements faced by information systems managers, as well as basic transition strategies. The result of this thesis is to show a transition strategy through an extended and coordinated period of coexistence due to extensive legacy systems and GOSIP product unavailability. Recommendations for GOSIP protocol standards to include capabilities outside the OSI model are also presented.

TABLE OF CONTENTS

I. INTRODUCTION

The US Government Open Systems Interconnection Profile (US GOSIP) is the specification of the approach which the US Federal Government has adopted to interconnect its information systems and enable them to exchange information easily and reliably. The Open Systems Interconnection (OSI) suite is a set of internationally standardized, vendor independent protocols defined by the Stable Implementation Agreements for Open Systems Interconnection Protocols from the International Organization for Standardization (ISO), the Consultative Committee for International Telegraphy and Telephony (CCITT) and the Institute of Electrical and Electronics Engineers, Inc. (IEEE) [GOSIP Institute, 1992]. These "Workshop Agreements" provide implementation specifications for protocols cited by GOSIP, and ensure international compliance for open system interoperability [FIPS SP500-177, 1985].

Knowledge and understanding of the GOSIP requirements became a critical issue for information systems (IS) managers in August, 1990 when GOSIP version 1 became mandatory for Federal systems procurement.

> GOSIP shall be used by Federal Government agencies when acquiring computer network products and services and communications systems or services that provide equivalent functionality to the protocols defined in the GOSIP documents. Currently, GOSIP supports the Message Handling System (MHS) and File Transfer, Access and Management (FTAM) applications. GOSIP also supports interconnection of the following network technologies: CCITT

Recommendation X.25; Carrier Sense Multiple Access with Collision Detection (IEEE 802.3); Token Bus (IEEE 802.4); and Token Ring (IEEE 802.5). [FIPS 146, 1988]

GOSIP version 2 expanded the requirements to include protocols for Virtual Terminal (VT), End System to Intermediate System Routing (ES-IS), and Integrated Services Digital Networks (ISDN) and became mandatory for Federal procurement on 3 October, 1992 [FIPS 146-1, 1991].

The motivation behind adopting an open system standard was to save money by providing increased communications capabilities through effective and interoperable computer networks, to reduce development costs and expand the competitive marketplace. The stated objectives for this protocol standard are [Federal Register, 1991]:

- To achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment.
- To reduce the costs of computer network systems by increasing alternative sources of supply.
- To facilitate the use of advanced technology by the Federal Government.
- To stimulate the development of commercial products compatible with Open Systems Interconnection (OSI) standards.

The assumption was that by selecting a core subset of OSI and requiring that it be provided for all Government information systems, GOSIP would create a huge standardization market for OSI applications and network solutions, thereby bringing down the prices of OSI hardware and software [GOSIP Institute, 1992].

A. PURPOSE

While the requirements of GOSIP are quite specific and are supported by extensive technical references, there is little or no guidance on how to transition from legacy systems into the international open systems world of OSI. The Department of the Navy (DoN) is committed to the open systems concept and directs that transition from non-GOSIP systems will be accomplished where technically feasible, operationally sufficient, and affordable. [DoN, 1993]

Unfortunately, the ISO body, in developing open system standards, has intentionally produced a displacement technology in an environment of extended coexistence. The committees which produce OSI standards are very careful neither to reference nor accommodate any non-OSI technology (i.e., the installed base). Management issues purposefully left outside the scope of GOSIP are:

- coexistence between OSI and the installed base; and,
- transition from the installed base to OSI.

There are even barriers to transitioning from one generation of OSI protocols to the next, with application interoperability issues of 1984 and 1988 software versions unresolved [Rose, 1992].

The purpose of this thesis is to emphasize transition options in a period of coexistence between existing systems and GOSIP-compliant systems with the primary focus on management issues of transition as effected by regulation, the

standardization process and industry support. This plan applies to information systems requiring inter-computer connection services.

B. OBJECTIVES

The GOSIP mandate is quite specific on what it requires and when, however it is conspicuously missing any implementation or transition strategies. The objective of this study is to contribute to DoD conversion efforts. An analysis of industry support for GOSIP and current implementation efforts is presented as a tool for future transition efforts.

C. SCOPE

The analysis of requirements and mechanisms which direct and enable implementation of GOSIP will be conducted as a basis for evaluating transition strategies in order to guide management efforts in adopting GOSIP. The goal is to provide a transition strategy which is technically feasible and resource responsible while maintaining operational stability.

D. ORGANIZATION OF STUDY

1. The Standards Process

Chapter II describes the process whereby standards are developed and adopted by the ISO and how the ISO's process differs from the Internet Engineering Task Force's process.

The course of events that create standards dramatically affect how the marketplace responds with product development.

2. Open Protocol Suites

Chapter III presents the reader with a brief background on the make-up of network protocol stacks as defined by ISO and NIST. It is designed to assist the user in understanding and interpreting GOSIP technical information.

3. GOSIP Background

Chapter IV provides expanded background information on GOSIP functionality and provides amplifying information on procedures and guidelines for implementing GOSIP.

4. Product Development and Support

Chapter V examines computer industry support, commitment and product development of GOSIP compliant products and assesses the future of OSI interoperability.

5. Transition Strategies

Chapter VI provides three stages of transition focusing on an extended period of coexistence. Six generic transition approaches along with specific military considerations are presented.

6. Conclusions

The final chapter provides conclusions and recommendations from the study.

II. THE STANDARDS PROCESS

It is currently mandated that new computer networks in DoD will use a foundation of OSI protocols. Computing environments are rapidly migrating toward truly "openness" and total interoperability. However, the path of transition and the final destination is unclear and is complicated by conflicts between standards organizations and vendors. The FIPS 146-1, directing that OSI protocols be implemented, in itself is not an answer to how to manage the transition. For example, the OSI protocol Common Management Information Protocol (CMIP) has at least nine different profiles available for implementation. [Burns, 1992] Similar examples dominate the OSI stack while Internet protocols are adding improved and interoperable features. Unfortunately, the standards process does not respond to either users or industry but seeks to accommodate every possible point of view.

Conflicts in the standardization of technology is not a new dilemma brought on by advancements in computer networks. There have been successes and failures in standardization throughout history. The belief that a common international standard is critical for continued coexistence is inconsistent with working examples of standardization. Television broadcasting, the metric system and monetary exchange are working examples of how standardization is not an imperative

for international coexistence, while a strict adherence to a standard in telephone switching and international air traffic control is critical and effective. The determining factors in establishing and enforcing a technology standard are the requirements of an industry to achieve its goals and the amount of capital it is willing to invest. Users and managers want to effectively and efficiently maximize the use of tools to maximize a competitive advantage in a cost-effective manner. Technology producers desire to provide what the users want in order to maximize profit. Thus the "standard" is what is desirable and for sale at a competitive price. We live in a de facto world where we document successful innovations and procedures until they becomes the common wisdom of the day [Taylor, 1993]. If standardization and acceptance were dependent on legislation or declaration then the law requiring the metric system in the US should have been sufficient to facilitate the transition.

Critical to the eventual adoption of a standard is the process by which it is developed. A process that involves the users is more likely to reflect the de facto requirements already in place.

A. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

> ... there are about 5,000 people who are part of that committee. These guys have a hard time sorting out what day to meet, and whether or not to eat croissants or doughnuts for breakfast let alone how to define how all

these complex layers are going to be agreed upon. [Rose, 1992]

The GOSIP program is a complex and lengthy process of requirements analysis, specification development, public review, product development, testing, and procurement. The seven steps from model to deployment, shown in Figure 1, is overburdened with controversy and compromise on an international scale.

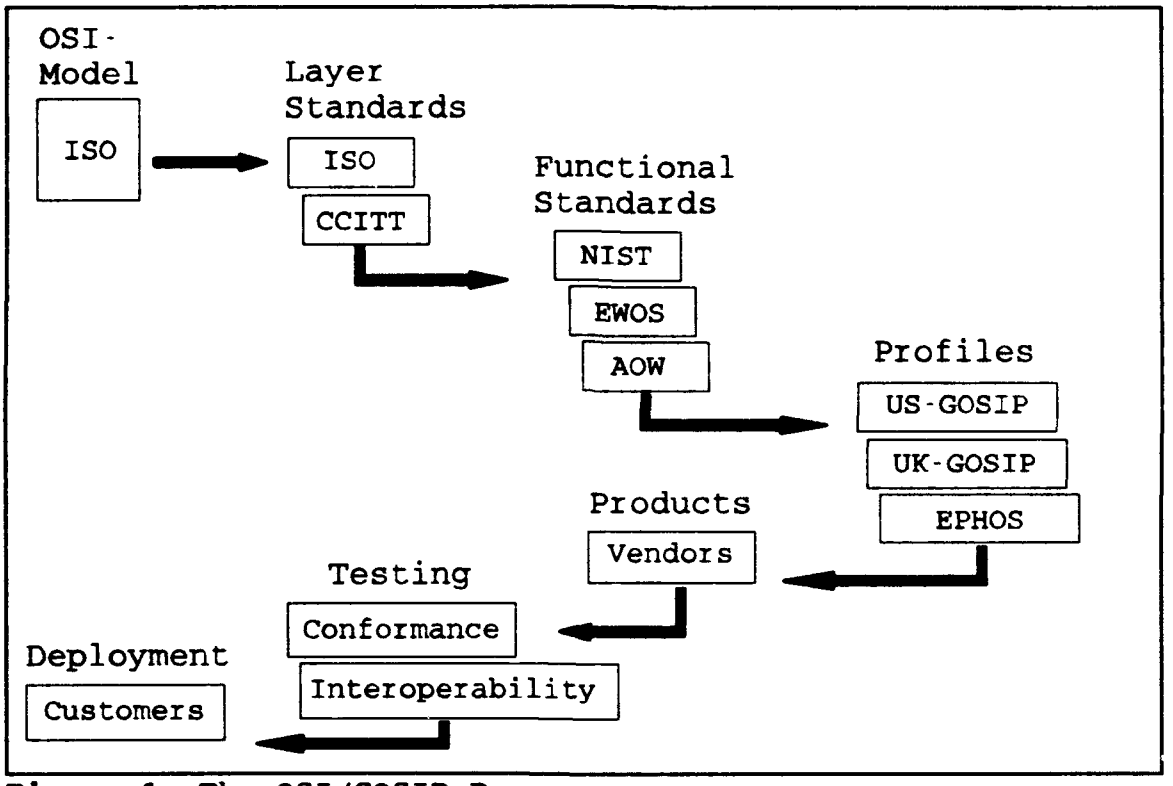

Figure 1 The OSI/GOSIP Process

1. OSI Model

The *International Organization for Standardization (ISO)* began development of the Open Systems Interconnection model in 1978. Four years later, with the cooperation of the

Consultative Committee for International Telegraphy and Telephony (CCITT) the OSI Basic Reference Model was published (ISO International Standard 7498 and CCITT X.200).

2. Layer Standards

The lower five layers of the model were published less than a year later for X.25 Wide Area Networks (WAN) and IEEE 802 Local Area Networks (LAN), as well as for Transport, Session, and the X.400 Message Handling System (MHS). The joint ISO/CCITT program expanded to include the *International Electrotechnical Commission (IEC)* in a Joint Technical Committee (JTC) to standardize overlapping activities.

3. Functional Standards

The publication of ISO/IEC/CCITT standards in the mid 1980's moved vendor product representatives and user representatives to form workshops to discuss OSI implementation. Three Functional Standards Regional Workshops discussed OSI producability, interoperability, and wide acceptability beginning in 1987.

- National Institute of Standards and Technology (NIST) OSI Implementors Workshop (OIW)
- European Workshop on Open Systems (EWOS)
- Asia and Oceania Workshop (AOW)

4. Profiles

Governmental bodies created profiles by referencing their procurement requirements to Regional Workshop Agreements. Specifications of subsets, options, and

parameters standardized requirements for vendors attempting to produce product in large quantities. Similar, but unique, profiles include US GOSIP, UK GOSIP, and European Procurement Handbook for Open Systems (EPHOS).

5. Products

Once profiles have been written into procurement specifications, development of working system prototypes and contract competition begins. Request for proposals are published with specific system requirements for contractor bids. The award of a contract will begin the product development phase.

6. Testing

Conformance to profile testing centers have been established in the three OSI world regions. Independent consortiums established by OSI vendors and major users such as *Corporation for Open Systems International (COS)* provide testing facilities for FTAM, X.400, TP4, and CLNP. Interoperability testing is also conducted by independent laboratories established by NIST and OSINET, with results submitted and verified by the Joint Interoperability Test Center (JITC).

7. Deployment

Installation and successful operation of OSI products in an "open" environment is the ultimate test of a standard. The obvious problem with this system lies not in the

progression of steps, but rather in the move from profile to product. Full system development is often costly and risky, and in today's economic environment resources are not available for independent and speculative product R&D. The federal procurement process requires vendors to have actual working products before they can enter the bidding process. This dictates what products will be developed in support of a profile. This phenomenon is unique in the government arena because the users of the developing technology are often unidentified. Private industry instantly gains valuable feedback from end-users during prototyping, alpha and beta tests and either continues product development, which is a reflection of commercial user needs, or abandons them for a more cost effective solution. Because government is not responsive to the market place, interoperability and product availability becomes a limiting factor.

B. INTERNET STANDARDIZATION PROCESS

The Internet suite of protocols is developed in a dramatically different process. The development of the DoD Open Systems Profile progressed through four stages.

1. Definition

A technological advancement is documented and supported by a constituency of vendors and/or users. Prototype implementations of a new technology undergo review and appraisal. If the document passes review as a defining

document of the technology, it is reclassified as a proposed standard.

2. Proposal

Once a proposed standard is accepted the proponents must demonstrate interoperability and usefulness. This process is given a deadline of six to nine months, during which time there must be significant experience with implementation. An openly-available, working reference implementation must be demonstrated to provide interoperability evidence. If public scrutiny of the technology shows that the criteria has been met then the document becomes a draft standard.

3. Draft

A draft standard has an additional six to nine months to demonstrate its interoperability in several independent installations. If extensive deployment of the document is successful it becomes a full standard.

4. Full Standard

The document is amended and modified as incompatibility or weaknesses are identified. The important issue in the adoption process, is that at every level there are products in place and in operation for technical review. Implementation, deployment and interoperability are developed simultaneously, providing understanding and availability for users and vendors.

III. OPEN PROTOCOL SUITES

A. OPEN SYSTEMS INTERCONNECTION (OSI) REFERENCE MODEL

The Consultive Committee on International Telephone and Telegraph (CCITT) developed a reference model which groups common protocol functions into seven layers, as shown in Figure 2. These seven layers represent groupings of major functions required to effectively send data through a network. The OSI Reference Model layers are grouped according to these major functions: application, presentation, session, transport, network, data link, and physical. Additionally, Figure 2 groups the functions into categorized services: Application Services, Networking Services, and Transmission Services.

The Open System Interconnection (OSI) profile is a concept in data communications whereby computer systems are able to communicate in an open environment without knowledge of specific characteristics of remote host computers [Boland, 1991]. The network structure, established by the ISO, is a series of components or layers that work together to provide a service. Each of the seven layers performs a related subset of the functions required to communicate with another system. It relies on the next lower layer to perform more primitive functions and to conceal the details of those functions

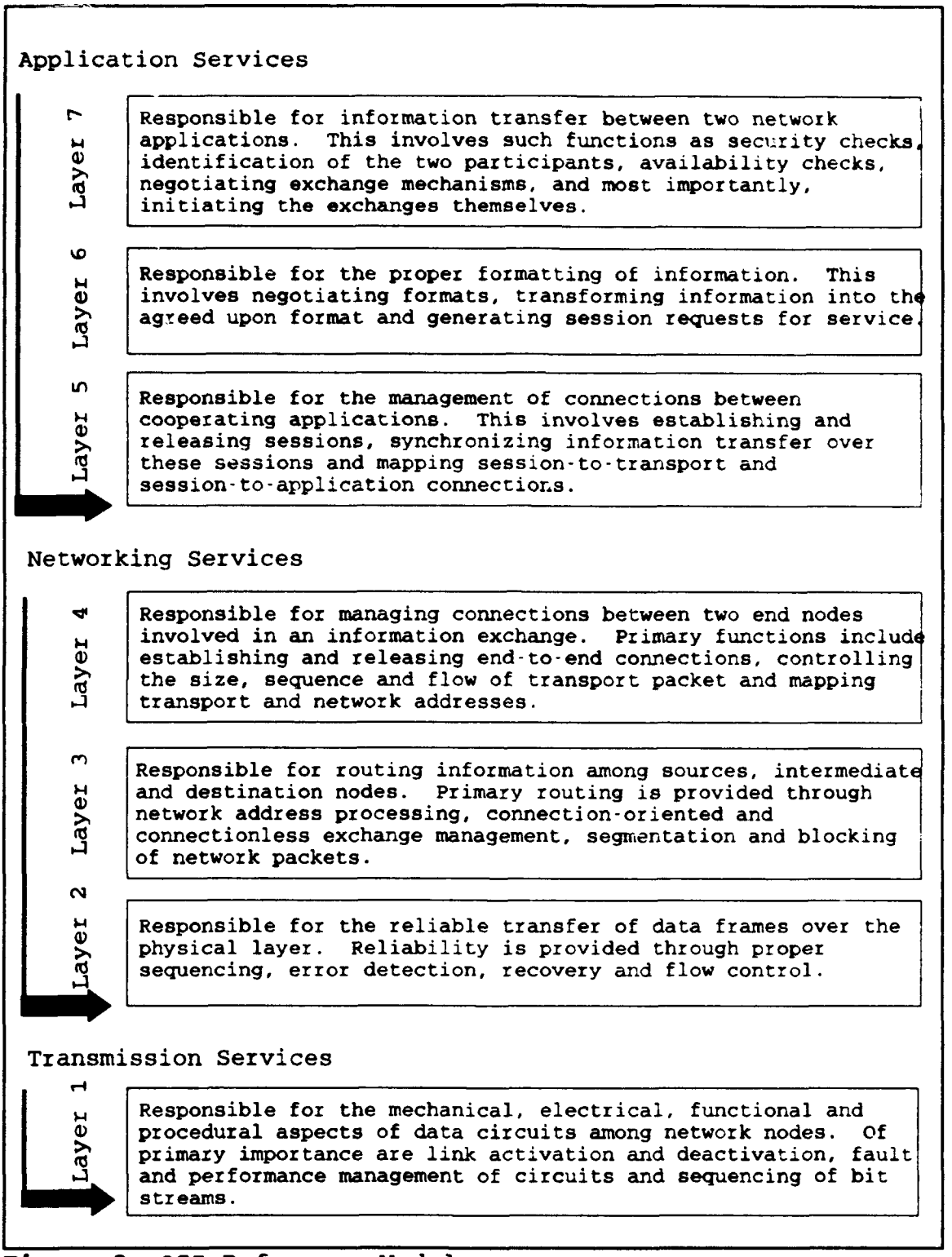

Figure 2 OSI Reference Model

[Stallings, 1991].

1. The Application Layer (Layer 7)

The Application Layer (Layer 7) provides services to application processes that lie outside the reference model. Layer 7 allows for protocols and services required by particular user-designed applications. Functions satisfying these particular user requirements are contained in this layer. Representation and transfer of information necessary to communicate between applications are the responsibility of the lower levels.

2. The Presentation Layer (Layer 6)

The Presentation Layer (Layer 6) provides for the negotiation and establishment of the transfer syntax, which represents the encoding of values for the purpose of transferring structured data types. Layer 6 negotiates the way information is represented for exchange between entities. The presentation layer provides representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. The presentation layer is concerned only with the syntax of the transferred data, with the data's meaning known only to the application entities.

3. The Session Layer (Layer 5)

The Session layer (Layer 5) is the user's interface to the network. This layer manages the connection between users.

Layer 5 allows cooperating application entities to organize and synchronize conversation and to manage data exchange. To transfer the data, session connections use transport connections. During a session, session services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection.

4. The Transport Layer (Layer 4)

The Transport Layer (Layer 4) provides a network-independent transport service to the session layer. The basic function of the transport layer is to accept data from the session layer, and ensure that the pieces all arrive correctly at the other end. Layer 4 connection-oriented service provides reliable, transparent transfer of data between cooperating session entities. The transport layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to transport layer entities. Transport protocols regulate flow, detect and correct errors, and multiplex data an end-to-end basis.

5. The Network Layer (Layer 3)

The Network Layer (Layer 3) routes information from one network computer to another. Layer 3 provides message routing and relaying between end systems on the same network

or on interconnected networks, independent of the transport protocol used. The network layer may also provide hop-by-hop network service enhancements, flow control, and load leveling. Services provided by the network level are independent of the distance separating interconnected networks.

6. The Data Link Layer (Layer 2)

The Data Link Layer (Layer 2) provides a reliable means of transmitting data across a physical link. Layer 2 provides communication between two or more adjacent systems. The data link layer performs frame formatting, error checking, addressing, and other functions necessary to ensure accurate data transmission between adjacent systems. The data link layer can operate in conjunction with several different access methods in the physical layer.

7. The Physical Layer (Layer 1)

The Physical Layer (Layer 1) provides a physical connection for the transmission of data among network systems and a means by which to activate and deactivate a physical connection. Layer 1 provides physical connection for transmission of data between link entities. Physical layer entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network.

B. GOSIP VERSION 1

GOSIP is the result of a desire to simplify and ease the process of assimilating OSI technology into Federal agencies by specifying a common generic set of requirements. GOSIP versions 1 and 2 are technical specifications which contain a core set of protocols and services. Version 2 contains additional functions while retaining all the functionality of version 1. The GOSIP protocols are described in the Federal Information Processing Standards (FIPS) Publication 146-x, with FIPS 146-1 of 3 April, 1991 the current standard. Figure 3 shows the GOSIP version 1 architecture within the OSI stack.

Because GOSIP specifies a subset of the OSI protocols many of the functions are defined by referencing the "Workshop Agreements" which give specific technical information for protocol conformance. These details are found in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Special Publication 500-177.

1. Application Layer

- *Message Handling System (MHS)*

Message transfer services and interpersonal message services are as specified by section 7 of the Workshop Agreements. Communication between two Message Transfer Agents takes place as specified by CCITT Recommendation X.410 (1984). Transport class 0 and the Connection Oriented Service (CONS)

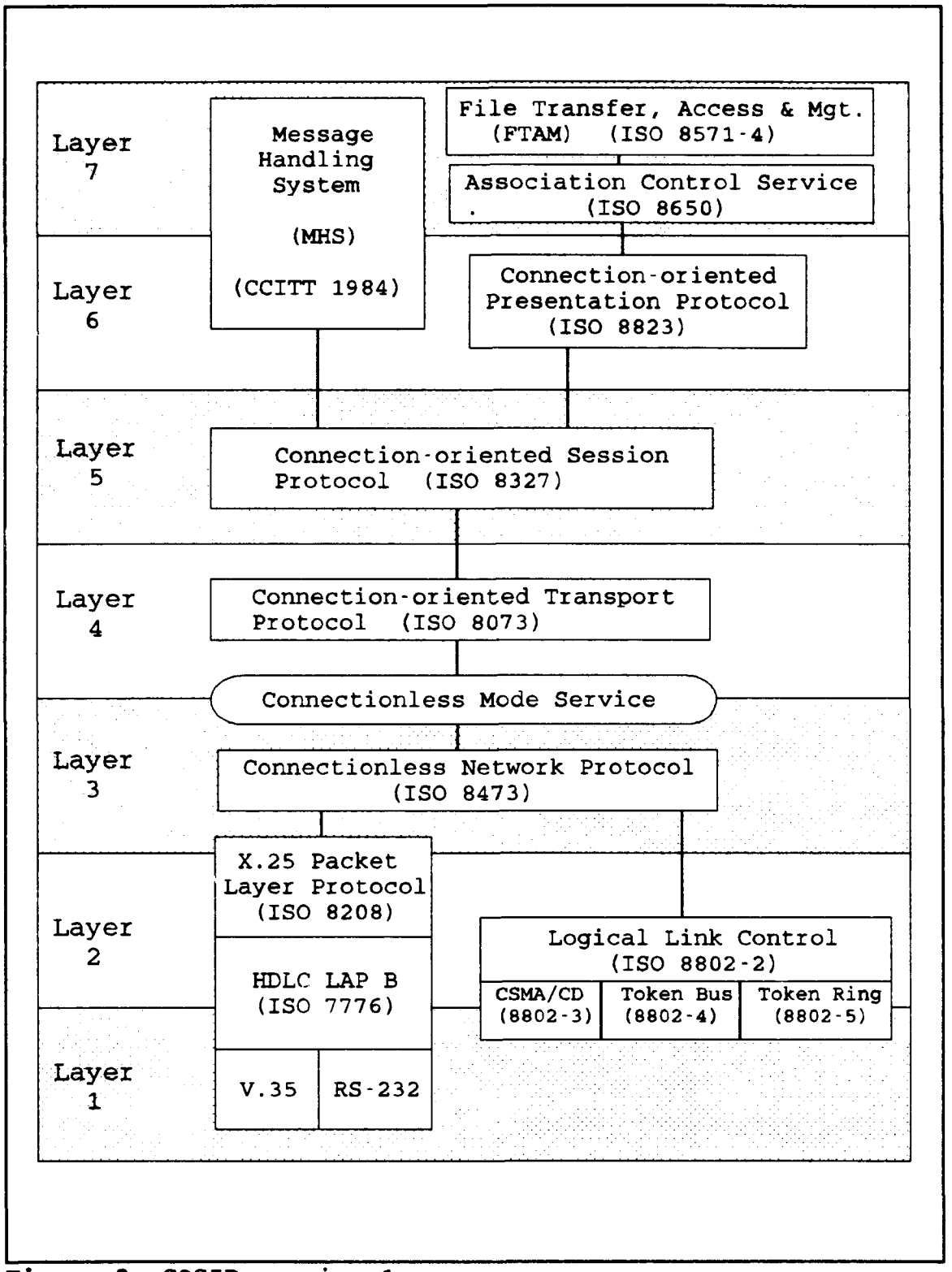

Figure 3 GOSIP version 1

will be used by end-systems when messaging over public messaging domains on public data networks. End-systems on private domains must use transport class 4. Private management domain end-systems connected to public domains conforming to X.410 must implement transport class 0 when relaying between domains.

- *File Transfer, Access and Management (FTAM)*

FTAM services are as specified by section 9 of Workshop Agreements. Limited-purpose or full-purpose file transfer services, as specified by ISO 8571-4, operate as the initiator of remote file activity, and as a responder to requests for remote file activity, or as both initiator and responder.

- *Association Control Service Element (ACSE)*

The ACSE is as specified by section 5.5 and 5.12 of the Workshop Agreements. A fixed value for the Application Entity (AE) Title, specified by ISO 8650, support FTAM requirements for exchange of AE types and logical configuration of AE types for non-GOSIP systems.

2. Presentation Layer

- *Connection-oriented Presentation Protocol*

Presentation protocols are as specified by section 5.8 and 5.12 of the Workshop Agreements and by ISO 8823.

3. Session Layer

- *Connection-oriented Session Protocol*

Session protocols are as specified by section 5.9 and 5.12 of Workshop Agreements and by ISO 8327.

4. Transport Layer

- *Connection-oriented Transport Protocol Class 4*

Connection-oriented Transport Protocol (COTS) transport class 4 are as specified by section 4.5.1 of the Workshop Agreements and are amended by ISO 8073 to support CCITT X.400 (1984).

5. Network Layer

- *Connectionless Mode Service (CLNS)*

Connectionless network service is required for Government-wide interoperability and connects logically distinct local and long-haul subnetworks. CLNS is provided by ISO Connectionless Network Protocol and is required to support 1984 CCITT X.25, HDLC LAP B (ISO 7776), ISO 8802.2 and Draft International Standard 9574 (ISDN).

- *Connectionless Network Protocol (CLNP)*

CLNPs are implemented as specified by section 3.5 of the Workshop Agreements and by ISO 8473. CLNP must be implemented and used for internetworking or concentrated subnetworks, and End System to Intermediate System (ES-IS) protocol connects end-systems to local area or point-to-point subnetworks.

6. Data Link Layer

- *X.25 Packet Layer Protocol (ISO 8208)*
- *HDLC LAP B (ISO 7776)*
- *Logical Link Control (ISO 8802-2)*

7. Physical Layer

- *V.35 (CCITT)*
- *RS-232-C (EIA)*
- *CSMA/CD (ISO 8802-3)*
- *Token Bus (ISO 8802-4)*
- *Token Ring (ISO 8802-5)*

C. GOSIP VERSION 2

GOSIP version 2 includes all protocols from version 1 with the following additions defined by FIPS Pub 146-1. Figure 4 shows GOSIP version 2 within the OSI stack.

1. Application Layer

- *Office Document Architecture (ODA)*

The ODA Standard specifies rules for describing the logical and layout structures of documents as well as rules for specifying character, raster, and geometric content of documents, thus, providing for the interchange of complex documents. Interchanged documents may be in formatted form (i.e., for presentation such as printing, displaying), in processable form (i.e., for further processing such as editing) or in formatted processable form (i.e., for both presentation and further processing). Transfer services, for

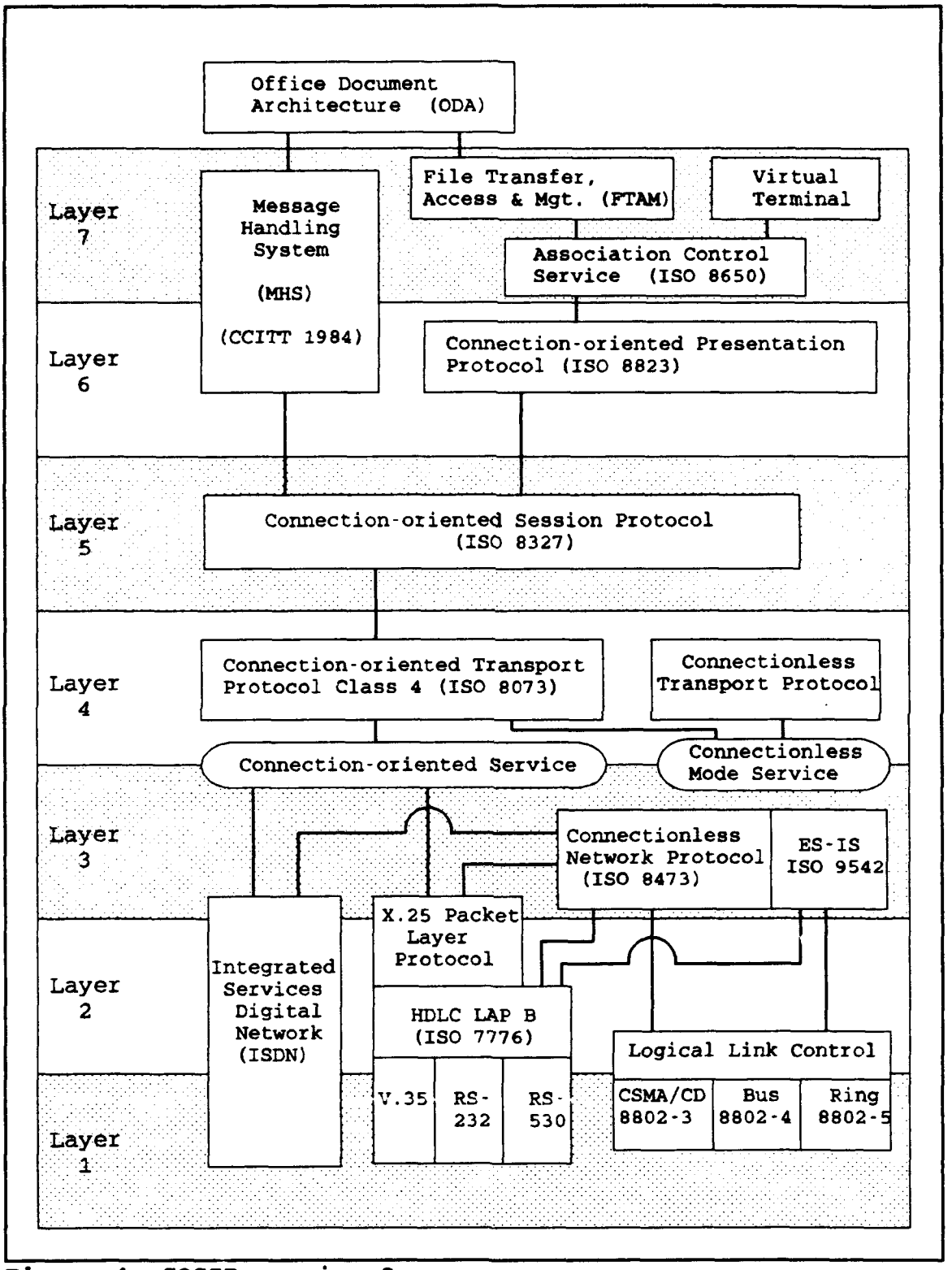

Figure 4 GOSIP version 2

ODA documents, may be provided by either MHS or FTAM. If the MHS application is used, OdaBodyParts are encoded for transmission over a CCITT X.400 (1984) service. When using FTAM to transfer an ODA file, the FTAM-3 document type should be specified; however, since files that are not ODA files can have the same document type, it is left up to the user of application programs that remotely access files using FTAM to know that a given file contains ODA information.

- *Virtual Terminal (VT)*

VT Systems are specified to support both 1) simple systems, and 2) forms capable systems, by section 14 of the Workshop Agreements.

A simple system provides the functions of a teletype (TTY) compatible device that supports a dialogue of a simple line or character at a time. Such a system uses control character (single) functions from the ASCII character set, such as "carriage return", "form feed", "horizontal tab", and "back space". A simple system supports the TELNET profile specified in section 14.8.1 of the Workshop Agreements. The TELNET profile requires Asynchronous mode (A-mode) of operation (i.e., no token handling protocols are needed) and specifies simple delivery control.

A forms capable system is intended to support forms-based applications with local entry and validation of data by the terminal system. A forms capable system supports functions such as "cursor movement", "erase screen", and

"field protection". A forms-capable system supports the forms profile specified in section 14.8.3 of the Workshop Agreements. The forms profile requires the Synchronous mode (S-mode) of operation and specifies simple delivery controls.

The Basic Class VT International Standard specifies three negotiation option protocols: No Negotiation, Switch Profile, and Multiple Interaction Negotiation which are all independent of VT profiles. Multiple Interaction Negotiation is not addressed by the Workshop Agreements, but any system claiming support of this negotiation option must also support the Switch Profile Negotiation and the No Negotiation options. Any system supporting Switch Negotiation Profile must also support the No Negotiation option. Seven bit USASCII, as well as the International Reference Version (IRV) of ISO-646 graphic repertoires, must be supported by both simple and forms capable systems.

2. Presentation Layer

There are no additions to the presentation layer protocols in GOSIP version 2. It remains defined by FIPS Pub 146 (GOSIP version 1).

3. Session Layer

There are no additions to the session layer protocols in GOSIP version 2. It remains defined by FIPS Pub 146 (GOSIP version 1).

4. Transport Layer

- *Connectionless Mode Transport Service (CLTS)*

Optional connectionless mode transport service for GOSIP end-systems may be specified only as an addition to the required connection-oriented transport service. Although no GOSIP mandated protocols require CLTS, a number of non-GOSIP protocols widely available in industry can use CLTS as an efficient means of communicating across local area networks. The CLTS option shall be implemented using ISO 8602 according to section 4.6 of the Workshop Agreements.

5. Network Layer

- *End System to Intermediate System (ES-IS) Routing*

For end-systems connected to local area and Point to Point subnetworks, the end system to intermediate system (CLNP ES-IS) routing service shall be provided by the ES-IS protocol ISO-9542 implemented as specified in the Workshop Agreements section 3.8.1. For end-systems connected to wide area networks, provision for an end system to intermediate system routing service is network specific.

- *Connection-oriented Network Service (CONS)*

The CONS is an additional, optional service that may be specified for end-systems that is directly connected to X.25 wide area networks and ISDNs. Use of this service can, under certain circumstances, avoid the overhead associated with CLNP and may permit interoperation with end-systems that

do not comply with GOSIP (i.e., do not implement CLNP). CONS shall be provided by the X.25 Packet Level Protocol (PLP). The mapping of the elements of the CONS to the elements of the X.25 PLP is according to ISO-8878 and as specified in section 3.6.1 (except section 3.6.1.3) of the Workshop Agreements.

- *Integrated Services Digital Network*

Integrated Services Digital Network (ISDN) enables X.25 PLP data to be sent across the D channel, sharing the channel with signaling data, and across a B channel. When operation of X.25 over a B channel is selected, the B channel can be provided as a switched service or a permanent service. ISDN physical and data link layer access as specified by section 2.7.2 of the Workshop Agreements.

6. Data Link Layer

There are no additions to the data link layer protocols in GOSIP version 2. It remains defined by FIPS Pub 146 (GOSIP version 1).

7. Physical Layer

- *RS-530 (EIA)*

GOSIP version 2 requires one additional physical interface protocol.

IV. GOSIP BACKGROUND

This chapter provides expanded background information on GOSIP and provides amplifying information for procedures and guidelines in implementing GOSIP. Additional GOSIP implementation specifics are found in Appendix A.

A. GOSIP APPLICABILITY

Since August, 1990, the procurement of new computer networks and major upgrades to existing systems have required GOSIP-conformant products. Because GOSIP deals with communications functionality it does not specify specific hardware, software or operating systems. This means that GOSIP requirements may apply to all types of systems, in all types of environments regardless of size or communication medium used [Boland, 1991]. There are three general criteria for GOSIP applicability:

- there must be computer-to-computer communications;
- using an autonomous communication system;
- and communications functionality must be contained in GOSIP.

GOSIP applies to communications between computer systems providing standard applications over a network and reliable end-to-end transfer services. Thus, GOSIP is designed to provide a set of flexible functions to be used on any system with the ability to interconnect to create a larger network.

B. OPEN SYSTEMS ENVIRONMENT (OSE)

Figure 5 shows a generally accepted representation of the OSE Reference Model. This model consists of three major components (Application Software, Application Platforms and Platform External Environment) with intervening interfaces (Application Program Interface (API) and External Environment Interface (EEI)).

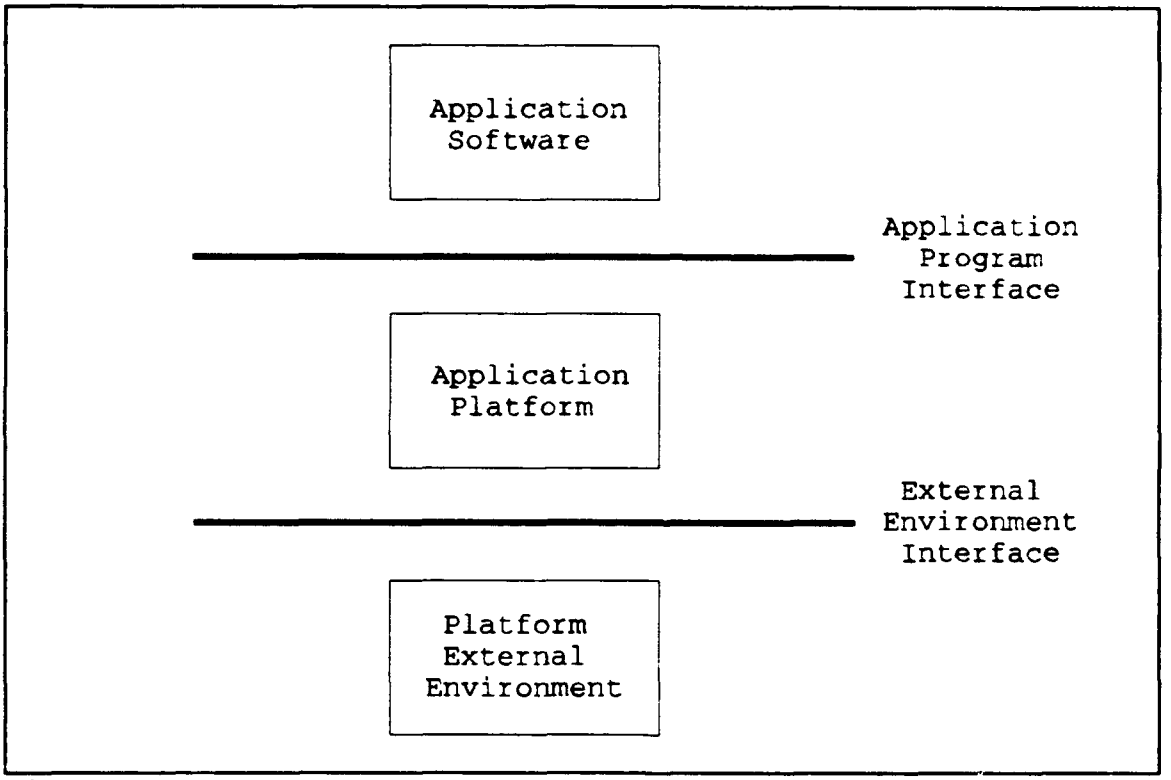

Figure 5 OSE Reference Model

1. Application Software

The application software is the computing element supporting particular operational needs (word processing, databases, spreadsheets, graphical drawing) and includes data, documentation and training, as well as programs.

2. Application Platform

The application platform is composed of the collection of hardware and software components that provide the services used by application programs. Application platforms facilitate portable application programs through services accessed by Application Program Interfaces (APIs) that make the specific characteristics of the platform transparent to the application (i.e., printer and I/O interrupts).

3. Platform External Environment

The platform external environment consists of those system elements which are external to the application program and the application platform (i.e., remote gateways, LANs and WANs).

4. Application Program Interface (API)

The API is the interface, or set of functions between the application software and the application platform. APIs support software portability by providing a common interface as an intermediary function. An API is categorized according to the services accessible through it: User interface, information interchange, communications or internal systems.

5. External Environment Interface (EEI)

The EEI is the interface which supports information transfer between the application platform and the external environment. An EEI is categorized to the type of information

transfer services provided: Human users, external data stores and other application platforms.

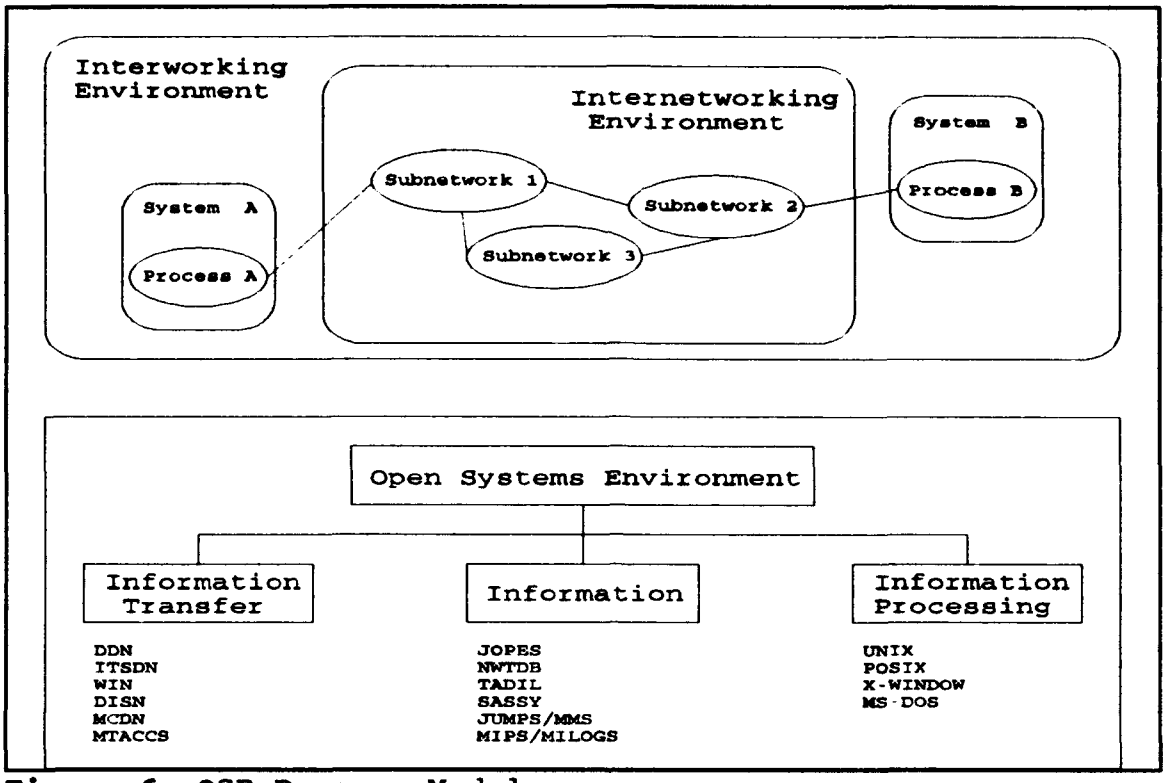

Figure 6 OSE Process Model

The GOSIP protocol stack and OSI philosophy are a fundamental component of the OSE concept. Functionally, an OSE has three components: Information Transfer, Information and Information Processing as shown in Figure 6. GOSIP protocols are concerned with the Information Transfer function of an OSE. The GOSIP transition must also be consistent with other OSE components, i.e., information and information processing. In addition, the transition to GOSIP must be consistent with the concurrent effort established in the Defense Message

System Target Architecture and Implementation Strategy (TAIS) as part of OSE.

6. CIM Standards Profile

The Corporate Information management (CIM) Technical Reference Model is based on a consensus-based standards approach. The standards profile supports this reference model and directly addresses the OSE perspective of end-to-end interoperability. Figure 7 shows the CIM Standards Profile and the relationship of GOSIP to CIM. The following set of open systems interconnection services apply.

- Program (Ada, C)
- User Interface (X-Windows, VT)
- Data Management (RDA, SQL, IRDS)
- Data Interchange (ODA, RJE, EDI, FTAM, X.400)
- Graphics (NITF, GKS, PHIGS)
- Network (X.25, IEEE 802.3, Banyan VINES, ArcNet, SNA)
- Operating System (MS-DOS, UNIX)

7. User Operating Environment

Figure 8 shows a set of open systems interconnection inter-computer services for the DoN automated enterprise.

a. User Interface

The user interface uses a Graphical User Interface (GUI) such as Microsoft Windows or textual such as MS-DOS command line interaction. This interface is supported by the application software. This software consists of generic

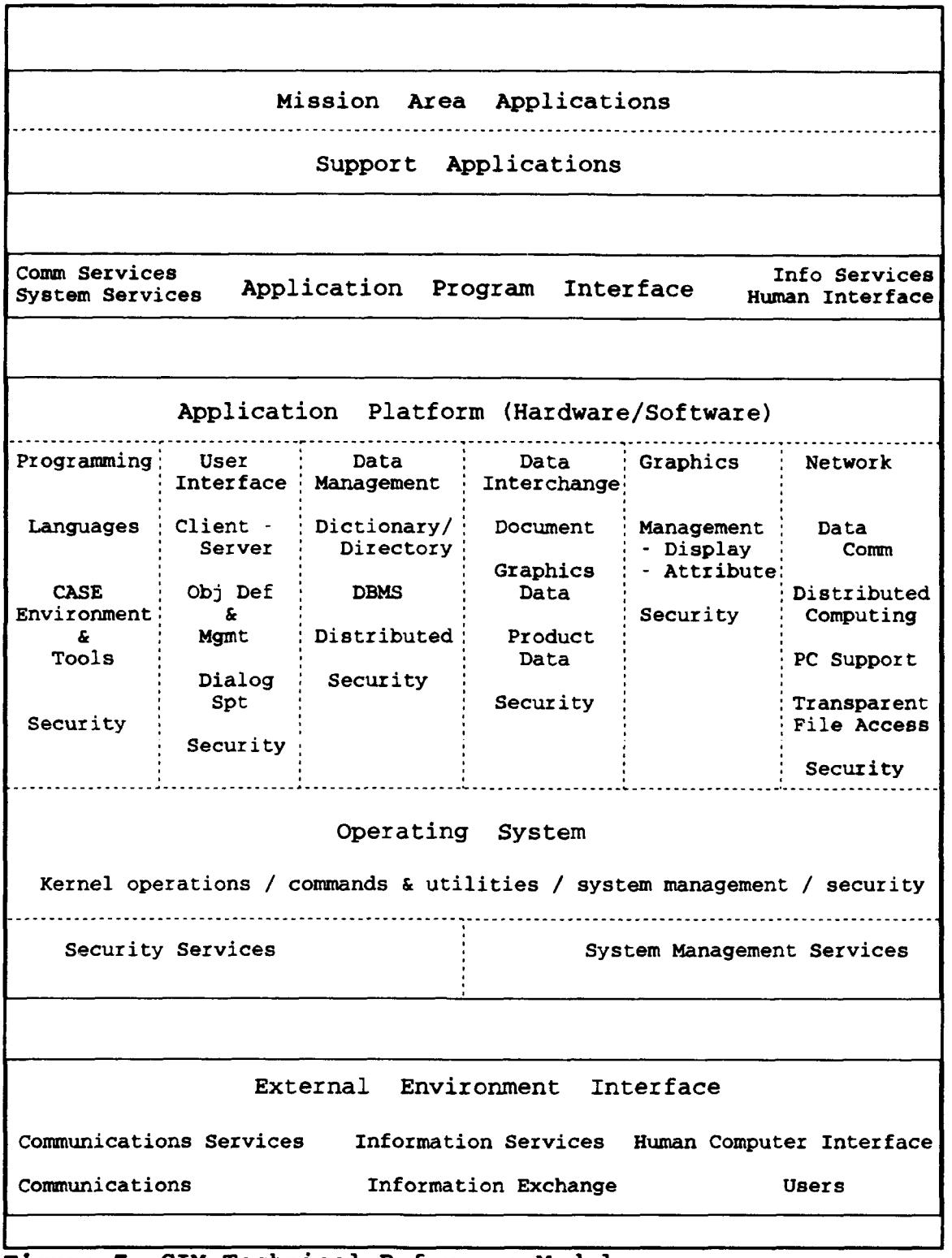

Figure 7 CIM Technical Reference Model

applications (i.e., E-Mail, word processing, database)

b. Program Services

These services include programming languages (Ada, C, etc.) and language bindings, Computer Aided Software Engineering (CASE) environment and tools, and security (access to programming objects).

c. User Interface Services

These services define how users interact with the application. Presentation determines the user interface appearance. The tool kit defines objects such as menus, scroll bars, etc. used to build an interface. The data stream interface specifies a function call interface to build messages defined in the encoding layer. The application dialogue coordinates the interaction between user and systems. The subroutine foundation builds components of window interfaces such as scroll bars. Security defines the types of user access to objects and functions used for interface management.

d. Data Management Services

These services manage the creation or use of data. Directory/dictionary services, facilitate access to metadata, allow access to modify data rules, provide a set of security rules for location of data in a distributed system. Database management System (DBMS) services provide controlled access and management of structured data. Distributed data provides

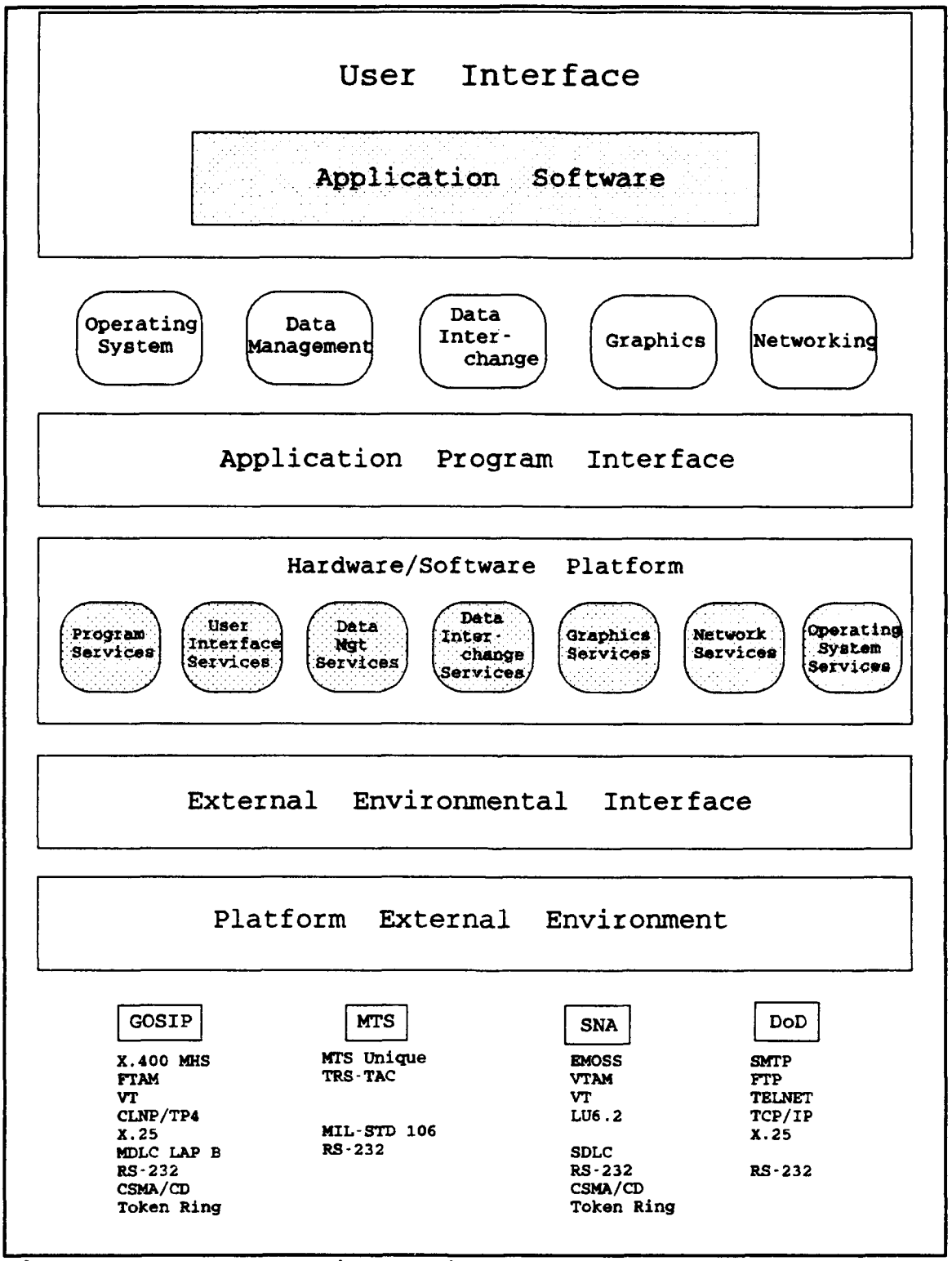

Figure 8 User Operating Environment

access to and modification of data in a remote database. Security includes control of access to and integrity of stored data.

e. Data Interchange Services

These services provide specialized support for the interchange of data between applications. Document interchange include specifications for encoding the data. Graphics data services include device independent descriptions of picture elements. Product data encompasses data necessary to describe technical drawings, and documentation. Security is used to verify and validate interchanges such as nonrepudiation, encryption and labeling.

f. Graphics Services

Graphics services provide functions required for creating and manipulating pictures. Graphics management includes display element definition and object attribute definition. Security restricts access to functions that support the development of graphics software and data.

g. Network Services

These services are provided to support required data access and interoperability across networked environments. Data communications includes protocols for reliable, transparent end-to-end transmission across networks. Distributed computing include specifications for extending local procedure calls across a network. Personal Computer

(PC) support provides interoperability with systems in a variety of operating systems. Transparent file access to local and remote files provides ease of use to users. Security includes access control, authentication both for network users and network management.

h. Operating System Services

These services operate and administer the application platform. Also they provide an interface between application software and the platform. Kernel operations provide services to manage processes and execute programs. Command and utilities provide printing and displaying file content. System management defines and manages user access, and devices. Security ensures data confidentiality, integrity, access control and availability.

i. External Environment Interface

Security services and system management overlap among certain types of individual system management functions (i.e., KG-84, STU-3, Kerberos).

j. Hardware/Software/External Environment

This environment is composed of the collection of hardware and software components that provide the services used by application programs (i.e., CD-ROM, remote sensors).

C. WAIVERS

Exemption from GOSIP procurement requirements, is available if it can be clearly demonstrated that there are

significant performance or cost advantages to be gained and is in the best interests of the government. Waivers may also be requested when functionality critical to an agency mission is not included in GOSIP-compliant products. Additional considerations include special purpose networks and systems supporting network research [Boland, 1991]. Waivers should include:

- a description of the existing or planned ADP system;
- a description of the system configuration, identifying the items for which the waiver is being requested and planned expansion of the system over its life cycle;
- and a justification explaining the disadvantage caused through conformance to the standard as compared to the proposed alternative.

Federal department heads and agency heads (SECDEF, SECNAV) may approve waivers to FIPS when: 1) compliance with the standard would adversely affect the accomplishment of the mission of an operator of a computer system, or 2) cause a major adverse financial impact on the operator which is not offset by government-wide savings. Waivers must be sent to NIST, House of Representatives and Senate Committees on Government Operations, and must be published in the Federal Register and Commerce Business Daily [Boland, 1991].

V. GOSIP PRODUCT DEVELOPMENT AND SUPPORT

The transition to OSI is an evolutionary process and dependent on GOSIP product development and availability. Unfortunately, this situation requires extended periods of heterogenous protocol coexistence, a condition not well supported by OSI.

> OSI is designed as a displacement technology. In fact, the committees which produce OSI standards are very careful neither to reference nor accommodate any non-OSI technology. [Rose, 1992]

GOSIP product acquisition in support of mission requirements and within the arena of Program Objective Memorandum (POM) cycles, while mandated, is extremely difficult. Wholesale replacement of existing systems is both impractical and unrealistic given current fiscal restraints and a "right-sizing" environment [Cooney, 1993]. Technological upgrades are important life cycle considerations for current systems, and while it seems to allow a window for OSI introduction, the availability and inter-operability stumbling blocks exist. A careful and purposeful transition plan must be devised for each activity, with unique requirements and missions addressed with respect to effectiveness and efficiency. It is suggested in much of the transition literature that a single, comprehensive plan is necessary for adoption of GOSIP. The truth is that the non-OSI base is growing at a faster rate, and in many cases non-OSI systems have superior capabilities

than those in the OSI market [Cline, 1993]. Established computer vendors are increasingly abandoning support of OSI protocols altogether.

> IBM is pulling back on development of OSI products because of a loss of customer interest in OSI. [Nelson-Rowe, 1993]

Nevertheless, if a DoN information system requires inter-computer connection outside of a host device, then GOSIP is necessitated. The ability to comply with FIPS 146-1 while maintaining functional computing capability is a challenge for DoD IS Managers due to the extensive investment in non-GOSIP compliant systems and the problems associated with GOSIP product availability.

A. INSTALLED BASE

Federal agencies have a huge investment in installed proprietary networks. IBM's System Network Architecture (SNA), DECnet, Novell's IPX/SPX and AppleTalk make up eighty-five percent of the currently installed architectures, with 1 in 4 government computer networks based on SNA. The Internet "open" protocol TCP/IP is making strong gains at the expense of older asynchronous and bisynchronous communications and is gaining popularity as the open standard of choice. Estimates expect TCP/IP to hold twenty-one percent of the base by 1994 [Masud, 1993].

Complicating the networking picture is that eighty-two percent of networks worldwide have three or more protocols.

Legacy systems often provide critical functions and are not abandoned when new systems are introduced. This reality provides the greatest stumbling block for open systems and GOSIP transition. Manufacturers are not about to abandon their loyal customers to embrace open systems. These companies have a large investment in their proprietary architecture and are unlikely to offer competition to their own sales as well as dead-end their systems.

> The software vendors won't want to adopt OSI as their native protocol. IBM won't. They will continue to put the good stuff on SNA. Knowing this, why would a customer want to migrate to OSI? [Becker, 1992]

OSI protocols also suffer from the standards process. Companies are embracing TCP/IP protocols because they are developed on-line, they are open, and available for free. The ISO process is strictly controlled and excluded from the public domain, and stringent certification requirements cause development costs and schedules to skyrocket [Masud, 1993]. The situation has become a self-fulfilling prophecy, GOSIP migration is stymied by lack of product availability and thus organizations become further entrenched in their old architecture and contractors resist developing GOSIP products because they are not being bought. Because OSI products are often more expensive and incompatible with the installed base (thus making them mission degrading) contracting officers have the flexibility to specify a second protocol and the cycle repeats itself.

B. PRODUCTS

GOSIP transition ultimately depends on products being available to meet the demand and fulfill operational and legislative requirements. The issues surrounding GOSIP products are compliance, conformance and interoperability [Cline, 1992].

1. GOSIP Compliance

Compliance means that a vendor has, to the best of its ability, faithfully implemented the specification for the OSI standard. Companies become skillful and effective at implementing the required protocols by implementation experience, and participation in the standards process by being members of an ISO product committee. However, compliance is subjective and not subject to independent verification. Ultimately, a vendor's history and committed resources determine the degree of protocol compliance.

2. GOSIP Conformance

Conformance is considerably different than compliance, it requires that a product is tested and shown to faithfully implement required specifications. This type of product assurance is overseen by the National Institute of Standards and Technology (NIST), which is responsible for GOSIP conformance tests. NIST accredits GOSIP conformance testing laboratories through the National Volunteer Laboratory Accreditation Program (NVLAP) and other standards bodies

(i.e., Corporation for Open Systems International and NIU-Form). Results of product tests are certified by the Joint Interoperability Test Center (JITC).

JITC is under the Defense Information Systems Agency (DISA) and the exclusive agent for GOSIP conformance certification. JITC reviews test suite results and certifies tools used in testing but does not itself conduct conformance testing. Vendors desiring their products to be listed on the GOSIP Conformance Test Register are required to pay for both the independent testing and the JITC certification [Wilson, 1992].

3. GOSIP Interoperability

The third, and potentially the most important consideration is product interoperability. GOSIP-conformant products must demonstrate that they work well with other conformant products. This additional testing is certified by OSINET of the Corporation for Open Systems, with products listed in the "Interoperability Acceptance" database and beginning in the Summer of 1993, JITC will test for interoperability in corporation with the Standards Promotion and Application Group (SPAG).

OSINET is an organization dedicated to OSI interoperability testing and is a member of an international consortium of OSI interoperability test organizations. Until recently, OSINET was the only accredited US test center and

operated GOSIP test suites for X.400, FTAM, X.500 and VTP. The OSINET certification is the most tangible and practical measure of GOSIP products because it shows multi-vendor products will work in concert.

SPAG will provide additional product testing with it's Process to Support Interoperability (PSI) mark. IBM, Digital Equipment Corporation and Hewlett-Packard Company have teamed to give vendors a formal mechanism for certifying the interoperability of their GOSIP products. PSI testing for X.400 (1984) and FTAM will be available in late 1993 with planned expansion for X.500 and 1988-version X.400. This increased opportunity for interoperability testing is hoped to improve the availability of GOSIP products, however OSINET and the PSI mark are not mandatory for GOSIP products [Masud, 1993].

4. GOSIP Problem

Adoption of the GOSIP standard would seem to facilitate the production of conformant and interoperable products in large numbers. Unfortunately, vendors find it more convenient to proclaim compliance, skip the expensive and difficult conformance testing and go straight to interoperability testing [Cline, 1992]. The problem faced in obtaining these products is that GOSIP procurement is bound by FIPS 146-1, Federal Acquisition Regulations (FAR), and Federal Information Resource Management Regulations (FIRMR), which

combine to specify GOSIP "conformance". Adding to the problem is the fact that government conformance certification is not yet available for some OSI components, including VT, 1988 X.25, 1988 X.400, CIMP/CMIS, and GNMP [Cline, 1993]. Also, NIST does not require interoperability testing, even though conformance to the standard does not ensure interoperability. While many vendors claim compliancy with GOSIP, about fifty percent fail the tests [Messmer, 1992]

Procurement and introduction of GOSIP products as directed by the FIPS become quite difficult when there are no certified products available. There is hope for the future of OSI products however. GOSIP has narrowed the OSI definitions to clarify the interoperability requirements. This improvement in the standard and the emergence of organizations committed to GOSIP implementation has dramatically improved the situation facing IS managers. The Corporation for Open Systems (COS) has certified many products which have passed conformance tests and has reduced the risk of obtaining non-interoperable products. The list of GOSIP products available has quadrupled in the last year, however still numbering fewer than twenty [Becker, 1992]. Additionally, OSINET, an organization made up of users, vendors, and regulatory groups involved in open systems standards testing, keeps a listing of all vendors and products that have passed interoperability testing. The register currently lists 165 entries from seventeen companies using sixty-two products [Becker, 1992].

Help can also be elicited from an open systems integration laboratory in Annapolis Junction, Maryland. Van Dyke and Associates has demonstrated interoperation of OSI products from more than thirty vendors. The lab will conduct performance and functional analysis, develop OSI solutions for specific needs, and demonstrate the interworking of OSI and TCP/IP suites [Masud, 1993].

Vendors faced with a declining government economic base and an open resistance to OSI in the commercial market place have resisted development of GOSIP conformant products. In 1992 there was only one JITC-certified conformant 1984 X.400 product and no 1988 X.400 versions available [Cline, 1993]. OSI protocols have seemed increasingly irrelevant, being overshadowed by de facto standards and proprietary dominance. However, OSI can become a dominant protocol for the 21st century if its advocates continue to developing viable and coherent migration strategies which embrace coexistence with the installed base [Hall, 1993].

C. THE GOSIP INSTITUTE

There are many supporting organizations which have aligned themselves with both the Internet and the OSI communities. The future of networking however, while still unclear, would rationally be a combination of the Internet installed base and the proposed improvements offered by OSI. A promising future

for standardization is the single convergency solution proposed by The GOSIP Institute.

The INTERNET 2000 : A Protocol Framework to Achieve a Single Worldwide TCP/IP/OSI/CLNP Internet by Year 2000 proposal advocates, "anything over anything" and calls for the respective communities to,

> ... put the divisions of the past behind them and join together to achieve a single Worldwide Internet. [GOSIP Institute, 1993]

The approach advocated by The GOSIP Institute is based on converging IP and CLNP to provide an easy to understand, easy to implement, win-win environment.

1. Approach

The GOSIP Institute White Paper, version 3.0 recommends building "Internet 2000" on the basis of the TCP/IP Internet de facto four-layer architecture and US GOSIP. The belief is that Application services over Transport services over Internetwork over Subnetworks will provide for the "anything over anything" internetworking future.

2. Subnetworks Layer

The existing TCP/IP Internet does not specify subnetwork technologies. The TCP/IP Internet approach allows organizations to decide their own subnetwork based on their own criteria. GOSIP currently recommends a specific set of subnetwork technologies: IEEE 802.3 CSMA/CD, IEEE 802.5 token ring, X.25 packet switched network, HDLC point-to-point links,

ISDN digital telephone network; with future GOSIP versions adding FDDI fiber optic LAN, frame relay fast packet switched network, and PPP (point-to-point protocol).

GOSIP requires agencies to select a subset of the subnetwork technologies specified in order to promote internetworking. Current practices with the TCP/IP Internet and OSI communities are compatible at the subnetwork layer as subnetwork technologies are permitted to be selected based on individual criteria [GOSIP Institute, 1993].

3. Internetwork Layer

TCP/IP Internet requires IP as the internetwork protocol. IP is being reworked to provide more addresses to help solve the large flat routing table problem. Currently available improvements are TCP and UDP with Bigger Addresses (TUBA) and Classless Interdomain Routing (CIDR). These two methods are not mutually incompatible but provide two evolutionary ways of dealing with IP address depletion while still providing traditional IP and CLNP routing. CIDR provides many more addresses immediately, delaying the addressing crisis until at least the end of the century, and TUBA provides a means for the OSI/GOSIP community to interoperate immediately with the IP community through dual stacks.

The importance of achieving a single Worldwide Internet based on a single "convergence" internet protocol and

supported by a single suite of routing is recognized by both communities. The availability of CIDR and TUBA will allow timely deliberation to occur, so that all internet protocol features and routing protocol features required by the next generation IP are included in the protocol which is selected. If a new IP "next generation" protocol with significant new functionality does in fact emerge from the current process, then the new protocol should become both "IPng" and "CLNPv.2", and that both the Internet and OSI communities should adopt the new protocol as the single internetwork protocol for the worldwide community.

GOSIP requires CLNP, however functionally CLNP is just IP with lots of addresses. CLNP solves the large flat routing table problem by having lots of addresses available, so that end-systems may be assigned two (or more) addresses, at least one of which is hierarchical. The CLNP is attractive in the medium term when teamed with CIDR and TUBA because IP addresses from the new CIDR distribution can interoperate with older IP hosts. The CIDR and TUBA recommendations would produce a Worldwide Internet that provides both CLNP and IP routing.

New TCP/IP Internet hosts should implement TCP over CLNP in addition to IP, while older hosts should automatically be assigned a new Internet NSAP address to use whenever they decide to add CLNP capability. Legacy systems could continue to use traditional IP routing into the medium term, but the

long-term view would be to phase it out after everyone has converted to the new convergence protocol. Achieving worldwide "dialtone" (i.e., routing) is the important part of this approach, because it is the expensive part due to the large infrastructure investment that it represents. Once worldwide routing is in place, everyone new who joins the Internet will be able to support two (or more) Transport stacks economically.

The Internetwork Layer proposal is implemented within the existing Internet. CLNP and its associated routing protocols are based on and improve upon IP experience and lessons learned, in that they support autoconfiguration (i.e., dynamic network address learning). The CLNP and associated routing protocols have already been implemented by the major vendors, and are currently being deployed in the major Worldwide Internet provider networks. Everyone already knows how to do global longest-prefix routing, which is the basis of IP and CLNP routing protocols. Addresses would be recognized within GOSIP and the other worldwide OSI bodies, but would be assigned by Internet. The worldwide backbone and regional networks would define a routing hierarchy and addressing structure to solve the routing table problem by assigning administrative authority identifiers and routing domain addresses to regional networks, and routing domain and area addresses to organizational networks [GOSIP Institute, 1993].

4. Transport Services Layer

TCP/IP Internet currently requires that Transport Services be provided by TCP and UDP, however there are no formal service specifications. The Sockets and TLI interfaces are de facto standard program interfaces to the Transport service. GOSIP requires that TP4 be used to provide the Connection-oriented Transport Service, and allows the use of CLTP (Connectionless Transport Protocol, equivalent to UDP) to provide the Connectionless Transport Service as an option (ISO 8072 and CCITT X.214). The X/Open XTI interface is the de facto standard program interface.

The Internet 2000 proposal for the Transport Services Layer is a three-part recommendation. First, TCP/IP Internet should continue to provide TCP and UDP services at Sockets and TLI interfaces, and GOSIP should continue to provide the OSI connection-oriented and connectionless Transport services at XTI interfaces using TP4 and CLTP. This first part of the recommendation simply means that both TCP/UDP and TP4/CLTP Transport protocol suites should be allowed in the near term. The type of Transport protocol entity bound to each NSAP address should be identified in the address. Transport addresses are already structurally equivalent between the two communities.

Second, the GOSIP community should adopt the Internet RFC 1006 OSI/TCP Coexistence Stack (i.e., TP0 over TCP) as well as the TUBA stack as legitimate options to the TP4/CLNP

mandatory stack, and should carry the concept a step further by defining all the legitimate ways that Application Services from either suite may call upon Transport Services from the other suite. A Transport entity that wants to reach an NSAP address bound to a different type of Transport stack may still be able to interoperate if it knows the NSAP address of an appropriate Transport switch (called a "Transport bridge" within Internet and a "Transport interworking unit" within ISO). The IETF, in collaboration with ANSI, IEEE and ISO, should develop and specify the legitimate ways of calling upon and interoperating among these Transport stack combinations in the near term. IEEE POSIX is currently developing a Detailed Network Interface (DNI) that supports both Sockets and XTI (i.e., an application can run directly over one or the other Transport interface) as well as a Simple Network Interface (SNI) that hides the details of the Transport interface. This work should be accelerated and brought to completion, and its use should be recommended by both communities.

Third, for the long term, both communities should work together to develop the next-generation Transport protocol, and define the ways that it can run over CONS, CLNS, IP service, and subnetwork services directly (i.e., Transport directly over LANs, MANs, and connection-oriented WANs). Note that TCP and TP4 are both based on the same generation of technology, i.e., the 1970s. TP4 is more efficient and faster than TCP with checksum turned off, but may run slower in

actual operation due to the choice of a heavy duty mandatory checksum and due to improved operational procedures defined for TCP. By the year 2000, rate-based and selective retransmission Transport technology will be needed to provide isochronous service over high-speed, mostly-reliable networks such as LANs, frame relay/ISDN, SMDS, and ATM/BISDN.

There is no reason, with available technology, to perpetuate the "two-community" divisiveness into the next century. The two groups should join together, with either one taking the lead or both working together over the Internet, to define a single protocol. This problem should be used as an opportunity to develop a pilot project to find out how the IETF, X3S3, and SC6 should work together in the future. The proposal for doing a combined IETF/ANSI/ISO future transport standard really is a perfect test case for the two communities working together. IETF should just say how they would like to work on the project, and see if the ANSI/ISO process won't accommodate the best way of working. Proprietary transport services are also provided in this layer via support of Sockets and XTI program interface specifications, as well as through transport interworking schemes specified by those vendors. Each vendor would specify its own "three-legged" (or more-legged) architecture under the common Sockets and/or XTI program interfaces. This Transport Services Layer component of the Internet 2000 Framework proposal is a win-win situation because both communities would continue to support their

defined Transport services, so both would be happy in that respect. Application services written to a standard Sockets or XTI specification would run over both stacks, and both communities would converge to a common next-generation Transport protocol running over the next-generation convergence stack or directly over LANs, MANs, or ATM/BISDN service by Year 2000. Then there will be a common, single Worldwide Internet/Networking community up through the Transport layer [GOSIP Institute, 1993].

5. Application Services Layer

TCP/IP Internet currently plugs its Application services such as FTP and TELNET directly into Transport services. The virtue of this approach is simplicity. OSI/GOSIP uses a three-upper-layer stack to provide its Application services. Session Layer is used to provide dialogue control (primarily, graceful close). Presentation Layer is used to identify alternative encodings. Application Layer is built up in standard ways called "application contexts" using building blocks called "application service elements (ASEs)" (e.g., Association Control Service Element (ACSE) to do call control, Directory User Agent (DUA) Service Element to look up information in the X.500 Directory). The virtue of this approach is interworking flexibility, but at a cost of complexity. The future OSI Upper Layer Architecture now under development may become fully recursive above the

Transport Service, i.e., basically one layer with a specified three-layer internal organization, like the OSI Network Layer is now.

The Internet 2000 proposal for Application Services Layer recommends that both communities keep their current methods of providing Application services. This means specifically that OSI would continue to look into how to streamline its upper layers. To interwork with each other, both communities should use Application gateways (i.e., dual Application service implementations with mapping between them), and both communities should provide their Application services over dual Transport stacks. OSI Presentation addresses of the form (NULL, NULL, T-selector, NSAP-address) may be used by both sides to address applications seen through gateways. The advantage of using this form is that it is already an X.500 Directory attribute type.

Both communities should continue to roll out new Application protocols such as SNMP2, PEM, MIME, X.400-1988, X.435-1992 (PEDI), X.500-1993, ODA, SGML, Distributed Transaction Processing, Knowledge Discovery (Gopher), World Wide Web (WWW), Wide Area Information Server (WAIS). Additionally, development of an "open RPC" (remote procedure call) standard between IETF and ISO SC21 is crucial. The ISO/CCITT standardization process should increasingly take account of the principles and methods of the Internet standardization process, principally:

- electronic "groupware" distribution, discussion, and development of draft standards, together with the principle of "implement first, standardize second" (this process is known in the Internet community as "rough consensus and running code");

- providing specifications and software implementations on-line and at low or no cost. The Internet should continue to take on the task of discussing, developing and deploying the infrastructure needed to support new networking standards. Ultimately, the marketplace will decide what works.

To promote application portability and interworking, both communities should continue to support the development and use of consortia-defined or IEEE POSIX open systems environments, APIs and protocols. Continued support for standards running TCP/IP Internet applications over OSI/CLNP Internet stacks, such as X Window over the OSI skinny stack, SNMP over CLNP, and NFS over CLTP or over a connectionless ACSE skinny stack is necessary for uninterrupted functionality.

Proprietary schemes found in legacy systems really begin to proliferate in this Application Services layer, raising important issues for users. It is important to find a way for users to benefit from the competition for best applications features and functionality while still achieving a maximum of applications interoperability and portability. The consortia-defined and IEEE API standards are key to the solution. All operating systems environments, (including Windows NT, OS/2, SunOS, Solaris, SCO, Univel, OSF/1, Macintosh) should support the open systems environment (OSE)

functional standards agreed by the three regional workshops: NIST OSE Implementors Workshop (OIW), European Workshop for Open Systems (EWOS), and Asia and Oceania Workshop (AOW). Procurement profiles such as GOSIP should not even consider adopting anything other than International Standardized Profiles, harmonized workshop agreements, or convergence standards worked out between ISOC, ISO, and CCITT, except as a consensus approach to promoting convergence that has been coordinated with all interested parties [GOSIP Institute, 1993].

VI. TRANSITION STRATEGIES

The Brooks Act (Public Law 89-306) established the Federal Information Processing Standards (FIPS) under the direction of the Secretary of Commerce and NIST. The GOSIP requirements (FIPS 146) have been mandatory for use in solicitations and contracts since 15 August, 1990 and GOSIP version 2 (FIPS 146-1) as of 3 October 1992.

The Navy currently maintains requirements in support of DoN GOSIP transition goals [DoN, 1993]:

- Implement GOSIP standards which are technically feasible;
- Insure that GOSIP standards are operationally sufficient;
- Implement solutions that are affordable within budget cycles;
- Maintain consistency with ongoing DoD programs such as other Services GOSIP plans, C4I for the Warrior, Corporate Information Management (CIM) efforts, Defense Information Systems Network (DISN), Defense-wide Information System Security Program (DISSP), Integrated Tactical-Strategic Data Network (ITSDN), Defense Information Infrastructure (DII), and Defense Message System (DMS);
- Support both tactical and non-tactical communities;
- Provide near-term capability with minimal disruption to current operations;
- Provide information transfer service transparent to the operator over common user networks.

Transition from the installed base to GOSIP standards must progress through three distinct phases: non-GOSIP dominance, coexistence, and GOSIP dominance. Currently, proprietary standards make-up the majority of government systems.

Initially, GOSIP pilot subnetworks need to be established where the mixing of standards will create an environment of coexistence. The length of the coexistence period will be determined by the availability and maturity of GOSIP products. The move to a fully GOSIP compliant system will occur if and when the functionality of the GOSIP products exceeds the proprietary functionality to such a degree as to make it cost effective to replace existing systems. The limiting factor in the GOSIP development is thus inherent in the management of the coexistence and the methods available to create the partnership between standards [DoN, 1993].

A. NON-GOSIP DOMINANCE

In spite of the GOSIP requirements, the DoD is in a position of proprietary networking dominance. Communications are accomplished through disjointed and non-interoperable networks. Currently messaging needs are satisfied by NTS, AUTODIN of the DCS, and DDN. Secret general service end-systems achieve interoperability through the DDN's Defense Secure Network 1 (DSNET 1), Top Secret Worldwide Military Command and Control (WWMCCS) end-systems use DSNET 2, and Top Secret Sensitive Compartmented Information (TS/SCI) end-systems communicate through DSNET 3. Tactical computers provide a pathway to connect these systems by interfacing with the DDN [DoN, 1993].

The Defense Integrated Secure Network (DISNET) will interconnect the three DSNET systems and allow subscribers to access any network with a single connection. Application layer gateways currently provide interoperability bridges between legacy systems and new protocols. Use of these gateways offers a path to a single operating environment and coexistence among heterogenous systems.

B. COEXISTENCE

There is a strategic imperative to provide application infrastructure solutions to allow the coexistence of: JANAP 128 (DoD AUTODIN message format), ACP 127 (NATO AUTODIN message format), DDN SMTP/RFC-822 (DDN message protocol), 1984 and 1988 X.400, Defense Message System MSP/X.400, and ACP 123 (DoD common message format) systems. The installed base of entrenched users must transition gradually to the modern architecture, with the new infrastructure flexible enough to absorb new products and technological advances. Coexistence must be built into DoN application infrastructure, not a wholesale reaction to implement GOSIP as a replacement technology [DoN, 1993].

The cornerstone of coexistence is the widespread implementation of the Defense Message System (DMS). DMS will employ GOSIP protocols, which will provide the base for eventual GOSIP transition. Legacy systems can then be tailored to meet operational requirements via gateways and

routers so that all or part of the architecture is absorbed into the system. Older systems will be able to interoperate with GOSIP systems with OSI and proprietary stacks coexisting in the network. Because of the costly overlap of existing systems and GOSIP systems, only the latest and proposed protocols should be implemented (i.e., 1988 X.400).

Multiple protocol connection gateways are the tools by which coexistence will be achieved. This approach allows backward interoperability with legacy systems, while allowing GOSIP transition to progress with minimum disruption of operations. This modular evolution also allows for flexibility as technology and standards evolve [DoN, 1993].

1. Evolutionary Transition

The move into and through network protocol coexistence can be accomplished using one of six transition strategies using GOSIP compliant products. Information systems planners must assess individual needs of their organizations in order to merge current proprietary networks into larger GOSIP based networks.

a. Parallel Networks

- Parallel networks involve concurrent support of multiple autonomous computer networks.
- This unconnected system works well where isolated groups do not need to interoperate and where a single user does not access multiple network.

- Interoperability is not enhanced in this strategy and duplicate network functions and staffing makes this approach very costly.

- Multiple systems of this type are likely to occur when unrelated commands are collocated.

b. Bottom-up Integration

- Bottom-up integration involves substituting GOSIP lower layer protocols (layers 1-3) for proprietary protocols.

- This physically connected system allows for resource sharing (i.e., printers) and is relatively inexpensive.

- Interoperability of data and applications is not achieved in this approach with each node remaining isolated.

- Simple LANs of this type are useful when there are very few nodes in close proximity and there is no requirement to communicate outside the command.

c. Multiple Protocol Routing and Bridging

- Multiple Protocol Routing and Bridging consists of a single computing system concurrently supporting multiple, coexisting protocols.

- This approach offers a solution for networks where it is impractical or impossible to standardize on a single protocol. An example includes LAN routers which simultaneously support GOSIP, TCP/IP and SNA communication

protocols or LAN bridges tying two or more physically different LANs into one logical LAN.

- The multiple protocol stacks support a gradual integration of GOSIP protocols into an existing environment. However, this approach only provides interoperability to like protocols, and does not provide any conversion function between different protocols.

- For organization with extensive investment in hardware and software and require connection to external networks but do not share applications, this approach offers the connectivity but does not enhance interoperability.

d. Top-down Transition

- Top-down transition implements GOSIP applications over an existing network. Applications such as FTAM and X.400 would be used over the existing network by using a common transport layer interface.

- Implementing GOSIP applications allows for international interoperability and communication with any OSI system via gateways.

- Drawbacks to this proposal are that a mixed protocol environment of this type may not be interoperable with a purely GOSIP environment due to the differing transport layers and the number of GOSIP systems available to "talk to" are limited.

- Organizations anticipating the replacement or upgrading of hardware may want to take advantage of the improved functionality of GOSIP applications in advance of total interoperability.

e. Application Gateways

- Application gateways operate at the Application Layer and typically use application level software to translate proprietary applications.

- Gateways utilize a "mapping" process that requires significant processing time and resources. This strategy is good in those situations where response time is not critical. Proprietary applications remain in place and the phased approach minimizes communications disruptions.

- This approach is not suitable for bulk transfers and interactive sessions due to the excessive processing time required for translation.

- Organizations that have unique applications may find this approach useful if rewriting the code would be impracticable and they do not require real time interoperability.

f. Hybrid Networks

- Hybrid networks consist of the implementation of a combination of transition strategies. This approach may be appropriate for networks that may require linking previously isolated islands of proprietary computing.

- This combination allows for the "best" solution to be used on a case by case basis.

- While hybrid networks are extremely flexible they have limited interoperability and without careful planning can exacerbate the problem of proprietary disconnect.

- Commands that have many highly specialized networks but require common word processing and E-Mail services may interconnect portions of their networks using this strategy.

2. DoD Transition

The Department of Defense (DoD) has taken a leading role in the evolution of networking. The Defense Advanced Research Projects Agency (DARPA) has been instrumental in network research. The DoD issued a GOSIP policy statement in July 1987, announcing plans to adopt FIPS 146 and begin transitioning to GOSIP protocols. In June 1988 the DoD issued a plan for implementing the policy. OSI transition, interoperability issues, and proposed approaches were intentionally left generic. Accordingly, any DoD approach to transition may be used, particularly when there is functional equivalence between existing architectures and the OSI architecture. For DoD, the OSI protocols are the sole mandatory interoperable protocol suite for new DoD acquisitions; however, a capability for interoperation with

existing DoD protocols needs to provide for the expected life of installed systems.

The DoD transition to the OSI architecture is concerned with both implementing OSI and providing interim DoD/OSI interoperability until OSI implementation is complete. Implementation deals specifically with deploying GOSIP protocols in existing or future DoD networks. Interoperability provides a capability for the military standard protocols on existing networks to coexist and communicate with OSI protocols being introduced. The approach to transition is multi-faceted, including: 1) developing a stack of OSI protocols on top of DoD's TCP/IP using the ISO Development Environment (ISODE), 2) having both protocols co-exist on a particular host (dual protocol hosts) and converting from one Application Layer protocol to another (Application Layer gateway), 3) supporting both DoD IP and CLNP at the network layer (multi-protocol router) [Boland, 1991].

a. ISODE

The DoD protocol stack and the OSI protocol stack are functionally similar; therefore, it is possible to build protocol implementations with a mixture of DoD and OSI protocols in the stack (mixed stack).

The ISODE (ISO Development Environment) is a UNIX based public domain software package that includes the OSI

Application, Presentation and Session layers. The ISODE runs over the Transmission Control Protocol (TCP). Using ISODE, OSI applications can run in a DoD networking environment using DoD hosts. The disadvantage of this approach is that an end-system can communicate only with an end-system that has the same mixed protocol stack. This alternative may be useful as a research or education tool during the transition period. The ISODE software includes the MHS, FTAM, Directory Services, and VT applications.

POSIX (Portable Operating System for Computer Environments) is a standard specification for UNIX-like operating systems. Efforts are underway by University of Pennsylvania to put additional functionality into ISODE and to make ISODE POSIX-compliant [Boland, 1991].

b. DoD-OSI Multiprotocol Routers

In order for DoD-OSI internetworking to occur, it is necessary to provide OSI hosts, on a local area or wide area network. Since the DoD IP and OSI CLNP are similar in functionality and protocol structure, multiprotocol routers are a viable alternative. The availability of multiprotocol routers would reduce the number of components, and therefore presumably reduce the cost and complexity for DoD LANs that are composed of a mixture of DoD and OSI protocol hosts, allowing the use of DoD protocols in areas where OSI protocols are not yet mature.

In either the DoD or OSI protocol architectures, Internet Protocol (IP) or CLNP performs routing functions to connect nodes on different networks. A DoD/OSI multiprotocol router is a device that is able to distinguish between the DoD and OSI internetwork protocol data units. When a packet arrives at an intermediate system, a network layer protocol identification field is checked and then the packet is passed to the appropriate module (either DoD IP or OSI CLNP) [Boland, 1991].

c. Dual Protocol Hosts and Application Gateways

A dual protocol host has the complete OSI and DoD protocol suites available as part of its networking capabilities. A user of such a host would have the option of invoking DoD protocols or the analogous OSI application protocols. A dual protocol host can be used directly by users with accounts to communicate to any OSI or DoD destination. It can also be used as a staging point for manual interoperation between a host that has only DoD protocols and a host that has only OSI protocols.

An Application Layer gateway is a dual protocol host which contains a conversion module residing at the Application Layer of each protocol stack. The module performs the semantic, syntax, and service transformation required for the protocol conversion.

The OSI FTAM and MHS protocols are candidates for

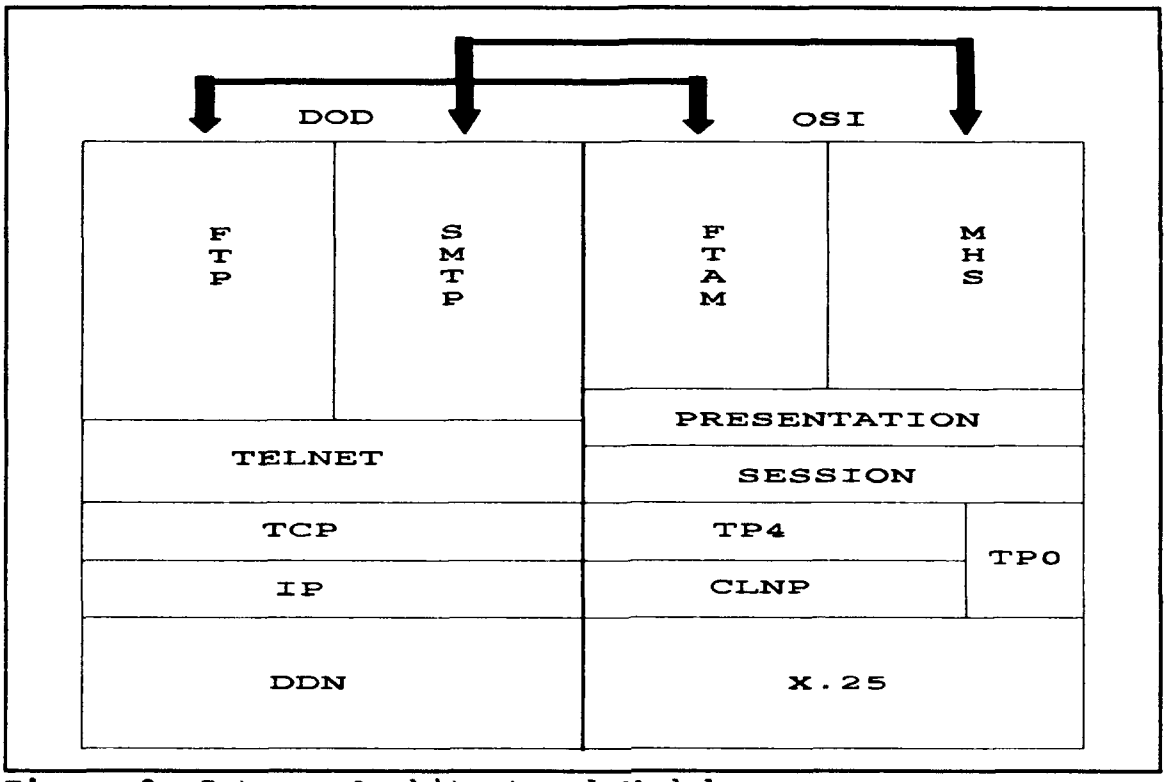

Figure 9 Gateway Architectural Model

such a gateway. The NIST has developed and tested prototypes of a gateway connecting the DoD SMTP and the OSI MHS protocols, and a gateway connecting the DoD FTP and OSI FTAM protocols. NIST also plans to provide an MHS-SMTP gateway as an FTS-2000 service. These efforts demonstrate the viability of a relatively efficient means of interoperation between systems based on TCP and OSI based systems. Gateways are designed so that users are required to have minimal knowledge of a remote protocol. Figure 9 illustrates how the SMTP-MHS and the FTP-FTAM gateways match protocols [Boland, 1991].

3. Military Considerations

The DoD transition to GOSIP must also consider the functional capabilities necessary for tactical operations because currently available OSI standards lack necessary military considerations. Military enhancements to GOSIP at each OSI layer must be considered in implementing a transition strategy and choosing products during the coexistence period.

a. Application Layer

The Message Handling System should be specified with the optional smart duplicating/splitting procedure to provide some multicast capability. Granularity should be provided through the Secure Data Network System Message Security Protocol combined with the Key Management Protocol as specified by the security profile. Additionally, the File Transfer and Access Management and Virtual Terminal protocol need to have additional security mechanisms added to protect passwords and systems access [DoN, 1993].

b. Presentation Layer

No additional considerations.

c. Session Layer

Session layer protocols should use the unlimited data size option specified in version 2 of the ISO specification. Negotiation capabilities of the Session layer can be expanded to provide Quality of Service negotiation [DoN, 1993].

d. Transport Layer

This layer should be augmented with additional technologies developed within DoD Internet to give improved performance, a reliable multicast protocol at the network layer, and security mechanisms [DoN, 1993].

e. Network Layer

This layer should be augmented with additional protocols to support a best effort multicast protocol and security mechanisms [DoN, 1993].

f. Data Link Layer

Products should be expanded through additional protocols to support tactical needs for security and forward error detection/correction to be used with spread spectrum techniques. Protocol augmentation such as the 32 bit checksum field can significantly improve the data integrity for tactical systems. Additionally, it should include the existing tactical multicasting systems as subnets within the link layer [DoN, 1993].

g. Physical Layer

No additional considerations.

C. GOSIP DOMINANCE

Implementation of GOSIP protocols to the Defense Information System Network (DISN) will mark the final transition to a truly GOSIP-compliant internetworking system. Product maturity and availability will allow for widespread

replacement of legacy systems with gateways, routers and bridges remaining in place until all systems can be transformed to GOSIP protocols. However, the expectation that all government computers will be interconnected via a single standard is remote. There will always be systems which will not interconnect with other systems. Ultimately, a management decision based on a strategic plan for the individual organization will determine the necessary level of connectivity. A move to GOSIP protocols must not overshadow the operational requirements of a system. As functional deficiencies within GOSIP are identified and corrected in follow-on standards the occurrence of waivers to GOSIP will be reduced. However, exceptions to standards will not be eliminated as long as DoN transition goals contain vague language such as: "affordable"; "operationally sufficient"; and "minimal disruption".

VII. CONCLUSIONS

A. SUMMARY

The key to achieving information transfer transparency in a multi-vendor environment lies in implementing information technology products based on standard protocols. Implementation of standards enables inter-operability by using a common basis for information transfer. The failure of OSI and thus GOSIP to effectively transition into the mainstream is that there are few OSI commercial off-the-shelf (COTS) products available. Those products come from only a few vendors. Questions arise as to fair and open competition in DoD procurement. In addition, future availability and support questions are relevant.

The DoD to GOSIP transition may include an extended period of coexistence. In order for internetworking to occur, it may be necessary to provide OSI hosts with the ability to communicate with other OSI hosts on a DoD-based network. Multiple protocol stack gateways and routers provide a transitional path between legacy systems and a complete OSI environment. Current capabilities are maintained through the implementation of Application Layer Gateways and the ISO Development Environment (ISODE).

The TCP/IP Internet and the OSI/CLNP Internet communities are moving together to develop standards recommendations that all sides can agree on. By creating an "anything over anything" environment, applications will run over APIs and multiple application services implementations for effective interoperability. Through application gateways, application services will run over multiple transport service protocol stacks identified by internetwork addresses and define a new type of standard that incorporates the best functions from both legacy and proposed environments [GOSIP Institute, 1993].

B. CONCLUSIONS

Commercial off the shelf application software vendors, hardware manufacturers, and operating systems vendors race headlong towards global interconnectivity, in a truly "open system" while the Government and standards bodies (justifying their own existence) promote some aberration of "openness". Open systems hardware and software (TCP/IP, OSI and GOSIP) are desirable for the flexibility they offer, but are acquired by DoD in an environment of ultimate rigidity and inflexibility. GOSIP migration, as directed by NIST, is achieving compliance but not interoperability and complexity rather than flexibility. A major "problem" with GOSIP transition is solvable quite simply, sink enough money into transition and products will flood the marketplace. Questions to be addressed are whether or not a wholesale replacement of the

infrastructure is the most cost effective way to move into the next century, and is transition to OSI protocols really the problem. I believe that the installed base is too entrenched, too important and too fragile to be abandoned. Legacy systems must evolve into the next generation of computing not replaced. The second question speaks to the mission of the Navy. Our mission is not to develop the worlds perfect network, it is to use the computer resources necessary to defend the Nation. The efficient and effective accomplishment of this task, with respect to computers, can not be defined simply by a standard set of protocols. When OSI protocols are the best choice to solve a problem (communication with NATO) or accomplish a task, then they should be used. If the situation requires a different set of protocols (TCP/IP, SNA, Mac) then that should be used. Interconnection can be used as an option if interoperability is necessitated.

This thesis addresses the mechanics of GOSIP and requirements of FIPS 146-1. My conclusion points away from transition. I believe that the requirements of GOSIP have missed the mark. Global interconnectivity should be a goal in developing technology, but Naval Officers are problem solvers who use technology as tools and our problem is not transition. The problems we face are dynamic and can not be captured in a single set of protocols. The simple truth is that every computer in the DoD does not need to interconnect and interoperate with every other computer in the world. In

today's environment of fiscal restraint we can afford to get the job done but nothing more.

The goals of GOSIP are, however, important and have merit, but the solution is not found in FIPS 146-1. The computer industry is creating an environment where interoperability will be built into systems as a matter of course. In the last five years commercial software has gone from proprietary stand alone programs to almost complete openness. The computing engines and kernels of programs are shared between vendors allowing transparent conversion (Lotus, Excel, Word, Word Perfect). Off the shelf "Gator boxes" are connecting heterogenous networks for pennies. Hardware developments such as the PowerPC 601 processor from IBM, Apple and Motorola will bridge the gap between RISC, Mac and DOS. Before this thesis is printed the concepts of networking and distributed computing will be significantly altered by this processor alone. Technology is advancing at rapidly increasing speed towards complete interoperability and standards while dictate procurement can not hope to keep pace. The marketplace is offering global interconnectivity with cost effective solutions. The government can not afford to be a unique outlet for OSI and support an entire industry. Neither can DoD afford to abandon legacy systems.

C. SOLUTIONS

A major problem facing government IS managers is how to improve and expand computer resources to support a command's mission within the constraints of budgets and the GOSIP requirements. At issue is whether or not GOSIP systems will efficiently and cost effectively deliver the support needed. The lament of the computer professional has become:

> "Do you want GOSIP compliance, or do you want it to work?" [Breidenbach, 1992]

Unfortunately for those in DoD, the answer is "yes". For the IS manager constrained by GOSIP procurement regulations there are four basic approaches to transition [Becker, 1992]:

- Do nothing and wait for a full set of standards to emerge;
- Have custom interfaces developed;
- Gradually implement the available OSI or other standards-based products as they come to the market; or
- Purchase coexistence products that enable dissimilar systems to talk whether or not these products are standards-based.

The answer supported by this thesis is the latter, however each organization must asses it's own needs and find products that support the individual mission. Industry leaders in the standards process are moving in a new direction that will facilitate open systems and reduce conflict.

> The focus is being taken off of OSI. The issue is not "Is OSI good, and will it win out?" but rather "How can [we] provide the technical means to manufacture products that users want to buy to achieve interoperable, manageable open communications systems?" [Becker, 1993]

Computer companies, networking companies and standards organizations eschew open systems orthodoxy but users don't buy protocols, they buy applications. Multiprotocol networking, protocol coexistence to support migration is the only responsible course of action, and the only one users will support [Metcalfe, 1993].

D. AREAS RECOMMENDED FOR FURTHER RESEARCH

1. Industry and Government Open Systems Specification

Industry and Government Open Systems Specification (IGOSS) is being developed as a follow-on protocol specification to GOSIP. A number of manufacturing companies and federal agencies are working to develop the standard to improve GOSIP by adding Remote Database Access, improvements to X.400 and transaction processing. IGOSS covers a wider range of functionality than GOSIP and it is expected to expand the standard by adding seventeen new function areas [NIST, 1993].

2. INTERNET 2000

The GOSIP Institute and the Networking Institute are private educational organizations devoted to explaining and demonstrating open systems networking, applications, software, and data technologies. The proposed INTERNET 2000 is quickly becoming a driving force in shaping the future of open systems. If the efforts of the GOSIP Institute are successful

there may be a wholesale reevaluation of current standards in an attempt to create a single convergence standard.

3. SAFENET

The Survivable Adaptable Fiber Optic Embedded Network (SAFENET) is the application of open systems in Navy Mission Critical Systems. The adoption of an industry network standard is intended to provide innovative technology, better service and improved products for the Navy. The objective of the SAFENET standard program is to develop computer network standards that support the needs of shipboard mission-critical computer resources. These needs include increased connectivity, survivability, performance, and capacity for future system growth. The SAFENET standard, originally based solely on GOSIP, is evolving to including non-OSI protocols and legacy capabilities.

APPENDIX A. GOSIP PRINCIPLES

A. DOMAIN ORGANIZATION

The topology of an internetwork has a significant effect in administering the network, allocating addresses, and network management. This section discusses the basic ISO model of internetwork domains. Figure A-1 shows the ISO routing architecture used during this discussion.

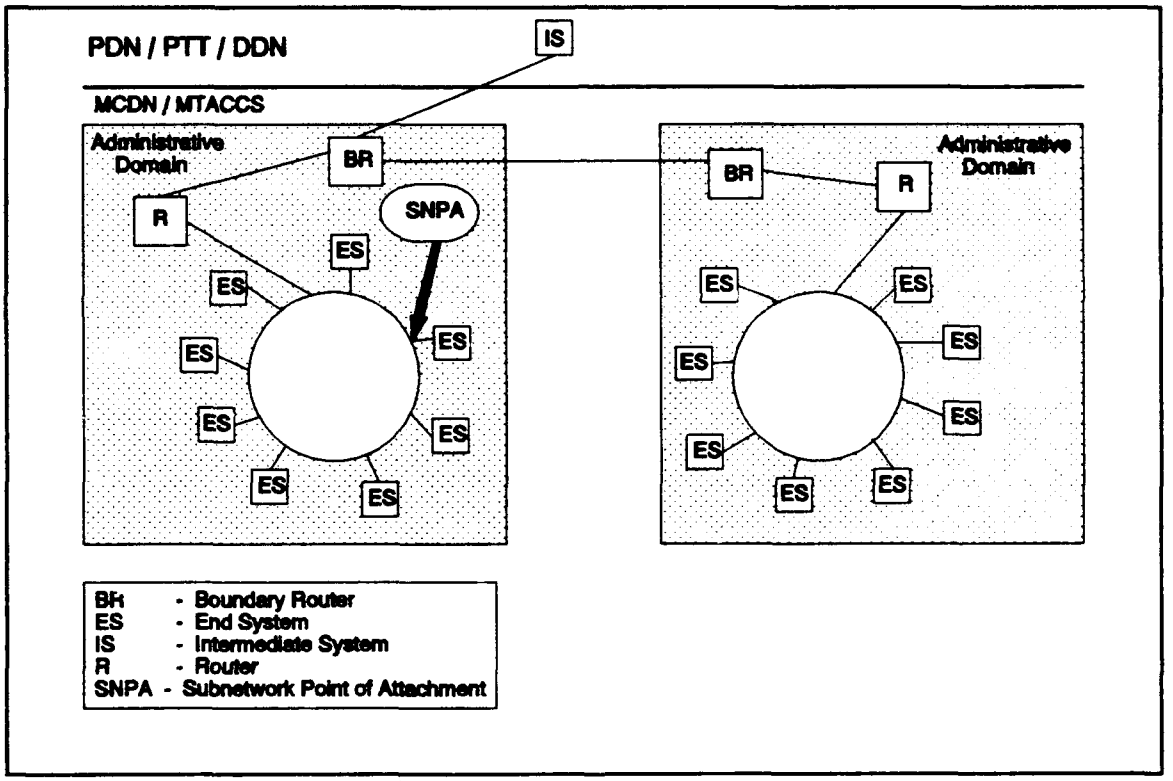

Figure A-1 ISO Routing Model

1. Routing Domains (RDs)

A routing domain is a group of routers using a common routing information distribution protocol, common metrics to

express cost, speed, delay, or other link attributes, and a common method of computing a path using performance based calculations (ISO Technical Report (TR) 9575).

2. Administrative Domain (AD)

Collecting one or more routing domains may constitute an AD. ADs control the organization of RDs, the assignment of addresses, and other policies. Different protocols may be used between routers in separate ADs.

3. Routing Protocols

It is widely accepted within the internetworking industry that the most dynamic and robust solutions lie within distributed adaptive routing where end-systems (ESs) and intermediate systems (ISs) learn from one another's location and attributes by communication directly. Figure A-2 shows these protocols defined by ISO, scheduled for usage in GOSIP.

a. ES-IS Protocol (ISO 9542)

This routing standard is used for mutual discovery by ESs and ISs. It supports broadcasting on LAN subnetworks, and allows an IS to redirect an ES toward another IS. Finally, it allows ISs to exchange static routing information with other ISs when they do not wish to use the more dynamic ISO protocols.

b. IS-IS Protocol (ISO 10589)

This standard is used to exchange reachability information with other ISs. It is designed to operate within

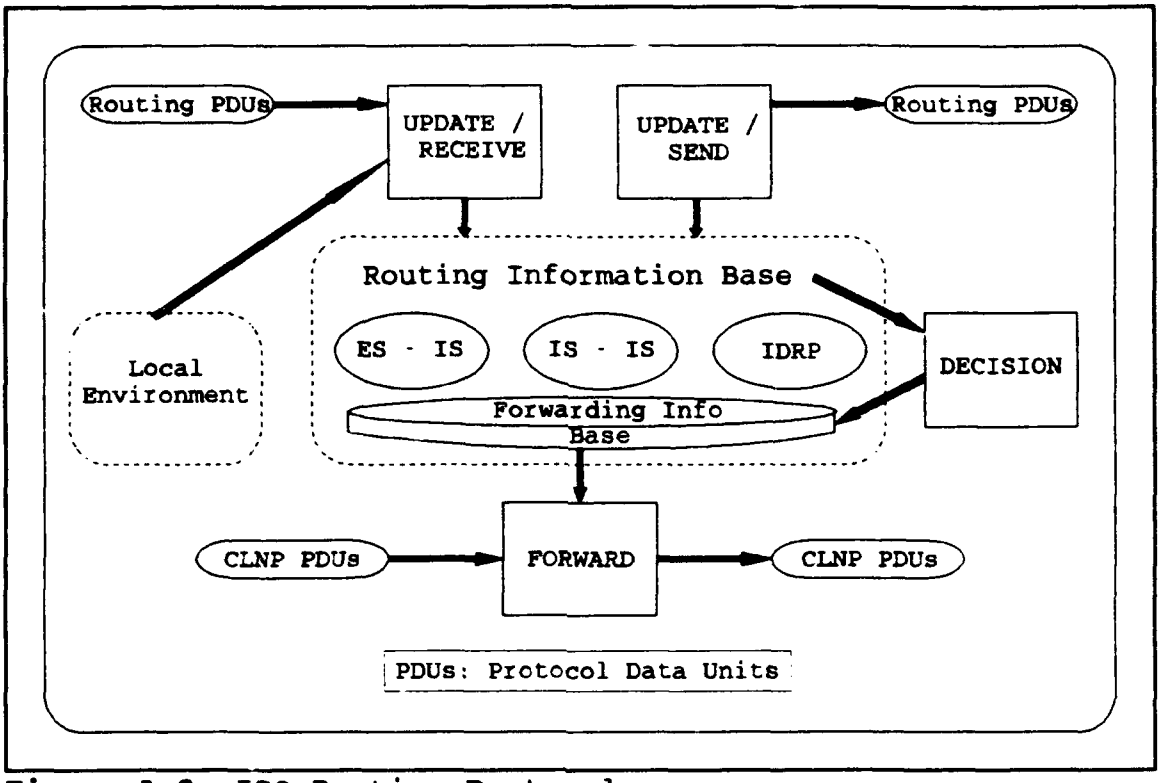

Figure A-2 ISO Routing Protocols

a routing domain.

c. Inter-Domain Routing Protocol (IDRP)

This standard is used to exchange dynamic routing information across routing domain boundaries. IDRP also supports exchange of path information, which could be used for policy-based routing decisions. Such decisions could be used to select low cost routes, to restrict domains used, or to enforce other policies.

4. Distributed Backbone Topology

This topology contains a small number of transit routing domains and a larger number of site routing domains.

Figure A-3 provides a diagram of this topology. These are the characteristics of this topology:

- Interconnections between site RDs are made through backbone routers in the Transit Routing Domains (TRDs).
- Arbitrary levels of hierarchy may be introduced within the site domains.
- All local traffic is handled in the site RDs.
- ESs and routers would derive their addressing authority from the local RD within their site RD.
- TRDs are centrally administered by groups responsible for coordinating all aspects of interconnection.
- Site routers comply with an interface specification governing routing protocols, network management, security and other operational aspects.

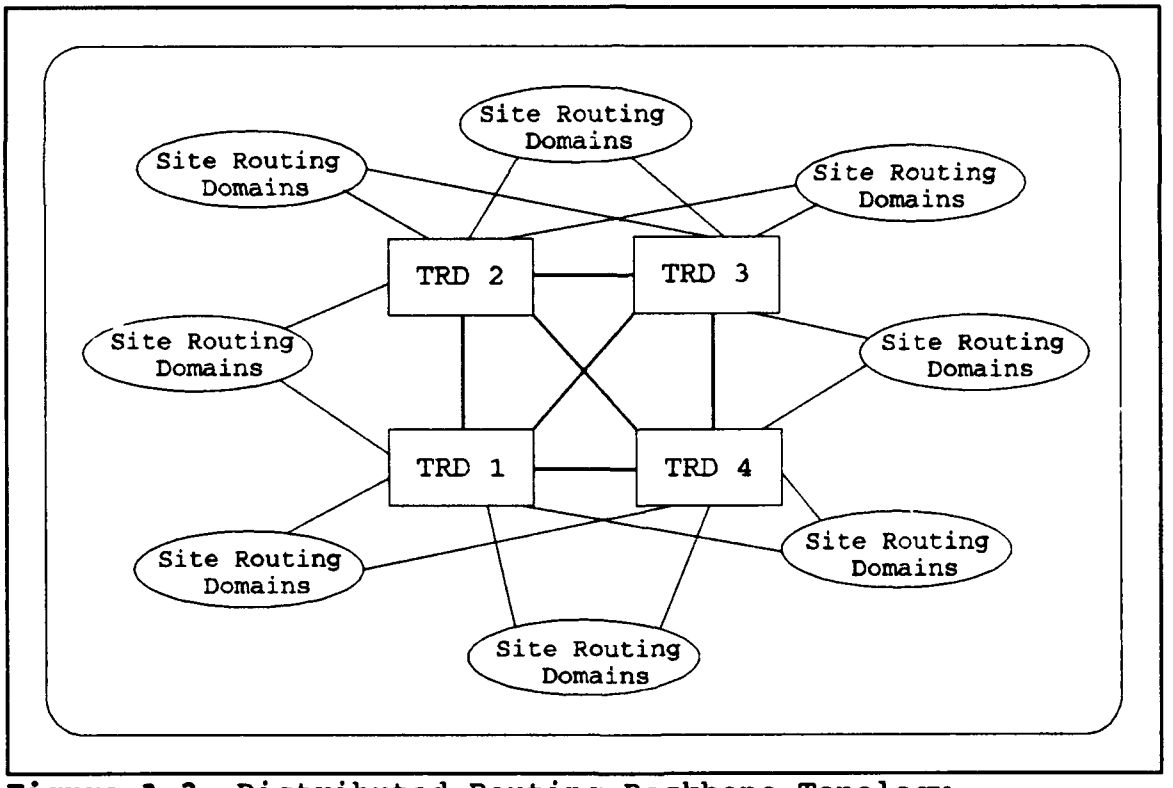

Figure A-3 Distributed Routing Backbone Topology

5. Routing Domain Size

Large routing domains degrade router performance due to the size of link states being maintained for IS-IS communications. Small-to-medium RDs should be administered from aggregated facilities for the network.

6. OSI Communication Principles

In transferring information, certain actions are expected before, and after, the message passes a specific OSI layer. Each information transfer function is uniquely identified through the transfer of service primitives (protocol parameters) at OSI layer access points. In Figure A-4, an arbitrary protocol layer is identified as the nth layer. The layer above is identified as the (n + 1), and the protocol layer below is identified as the (n - 1) layer. The (n - 1) protocol layer is the service provider and the (n + 1) protocol layer is the service user as shown in Figure A-4. These OSI layer access points are identified within the protocol header using a particular layer's access point selector. This allows developers to write Application Program Interfaces (APIs) which efficiently interface the application program in a standard way to an operating system. This allows for more efficient portability of software.

As a GOSIP transition tool, this is an effective point to place a "translator" or gateway to non-GOSIP software or protocols. Existing application software which does not

comply with OSI protocol standards passes information to the API which translates the information to a form which conforms to OSI protocol specifications.

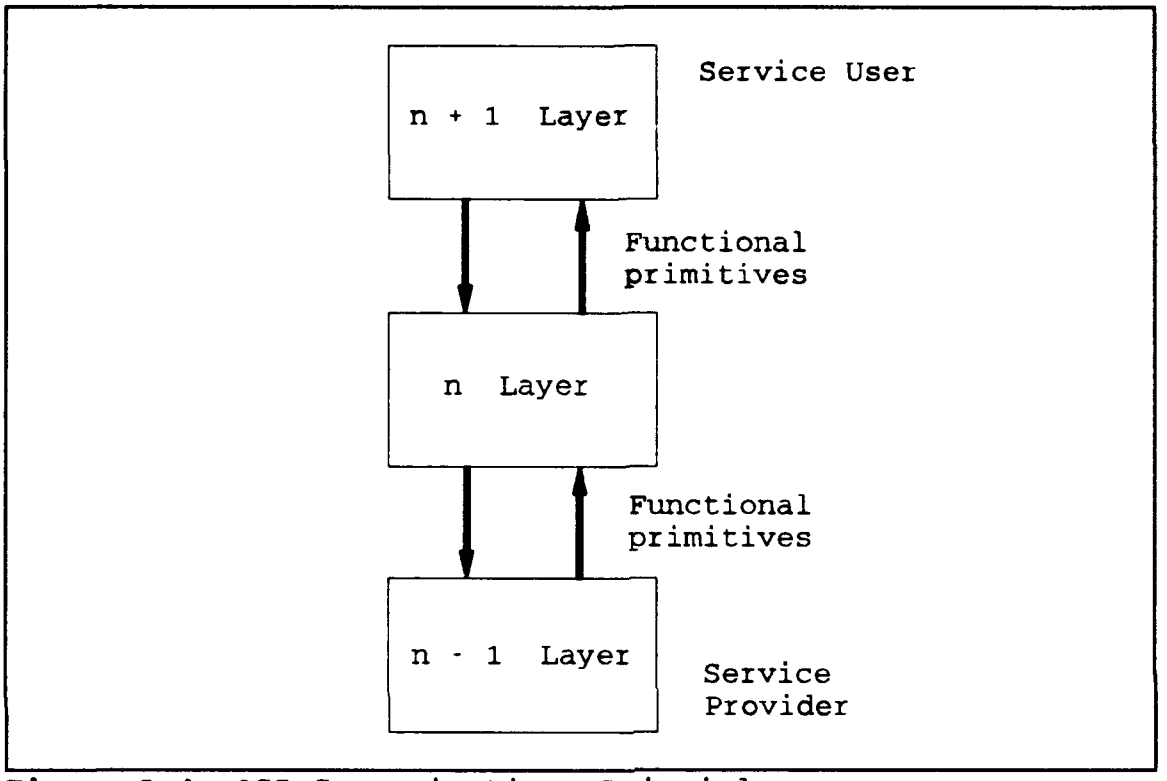

Figure A-4 OSI Communications Principles

a. Service Access Points

The protocol layers communicate required services between layers through Service Access Points (SAPs). These access points are identified as the Presentation Service Access Point (PSAP), Session Service Access Point (SSAP), Transport Service Access Point (TSAP), and Network Service Access Point (NSAP). Figure A-5 shows this model of OSI layer service access points. The NSEL field of the NSAP address structure determines the type of access point.

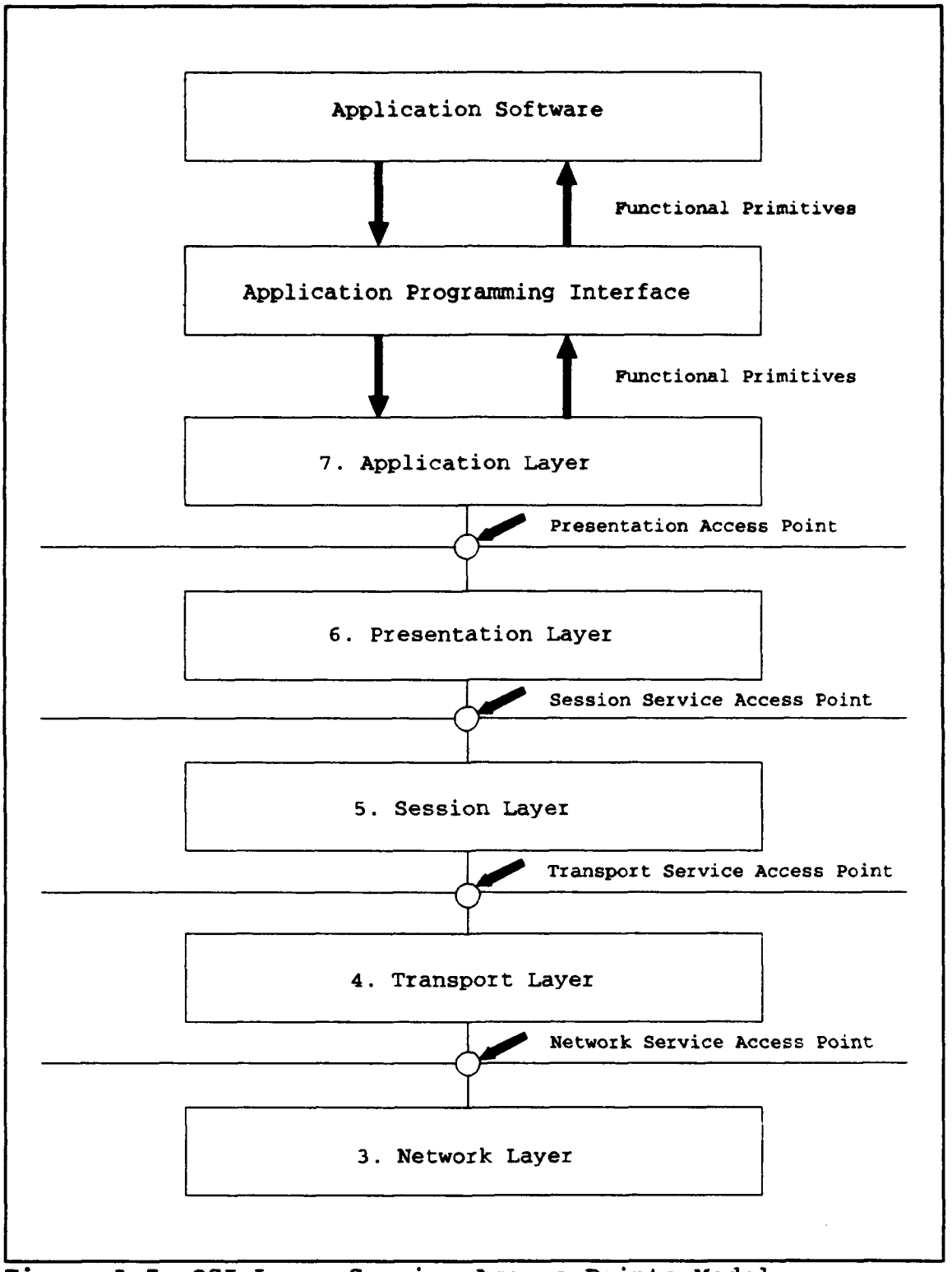

Figure A-5 OSI Layer Service Access Points Model

b. Network Service Access Point (NSAP)

The Network layer provides for end-to-end transmission. This means that higher layers need not be concerned with the physical topology of the network. This independence from concerns of the network topology is accomplished by providing logical network address mechanisms to higher layers. This logical address is called NSAP. The NSAP address is used to identify a user of the network service on a remote system, as opposed to the remote system network layer itself. This identifier uniquely distinguishes one ES from another in a network of systems.

A directory mapping function may be required to relate a NSAP address to its associated Sub-Network Point of Attachment (SNPA) address to permit the network service provider to determine the routing. The SNPA is the address that identifies a real open system on a particular subnetwork and is in the format of whatever addressing scheme is used on the particular subnetwork. An example of a SNPA address are the physical layer addresses of IEEE 802 style LANs. Figure A-6 shows routing domains and an ES's SNPA is shown in the figure. An NSAP address does not, in theory, have to include any information relevant to subnetwork routing but it is recognized that, in practice, NSAP addresses (in particular the Domain Service Part (DSP)) should be constructed in such

a way that routing through interconnected subnetworks is facilitated.

ISO 8348 describes NSAP addresses. The principle idea behind NSAP addresses is that they are assumed to be essentially stable, globally unique identifiers of NSAPs. The global identification of NSAPs does not imply the universal availability of the directory functions required to enable communication among all NSAPs to which NSAP addresses have been assigned.

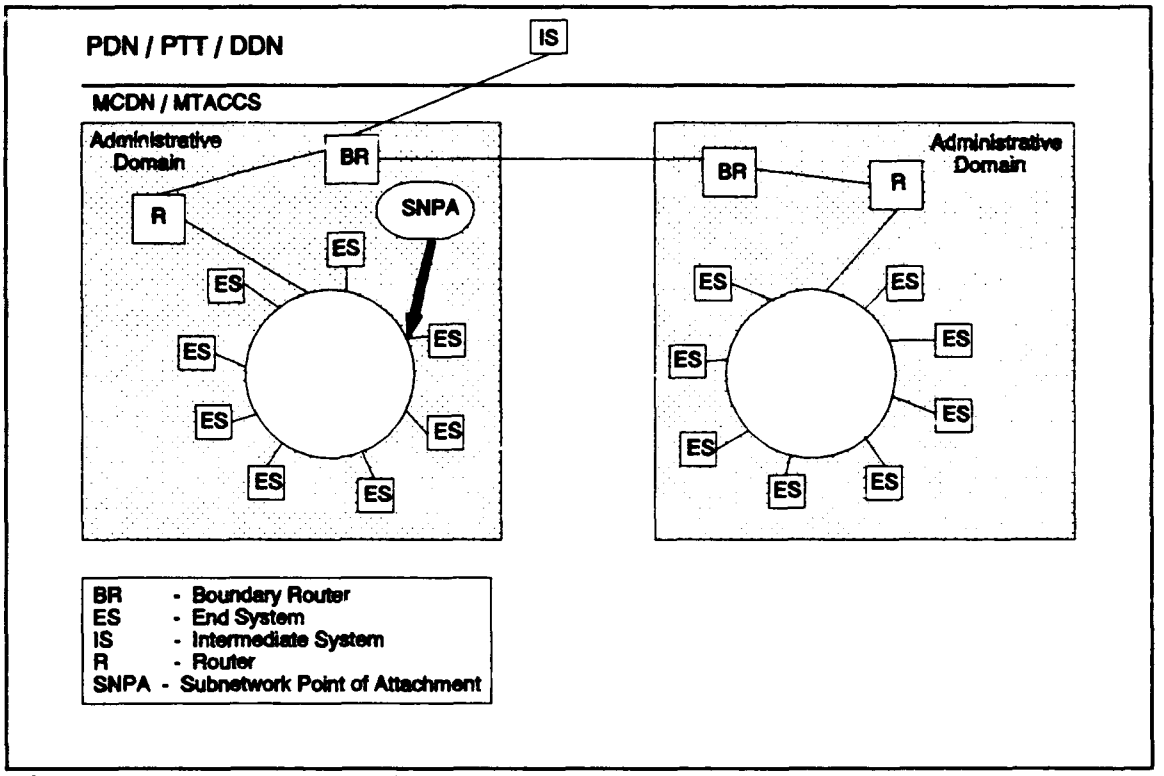

Figure A-6 OSI Routing Topology

(1) NSAP Structure

NSAP addresses have a structure that is composed of two main parts: Initial Domain Part (IDP) and

Domain Specific Part (DSP). The DoN will use the GOSIP 2.0 NSAP address format. Figure 18 provides the generic NSAP address structure from GOSIP Version 2.0 to be used for NSAP address registration.

(2) Initial Domain Part

The IDP associates a particular registration authority for that class of NSAP addresses, as well as the format for the rest of the NSAP address. The IDP is subdivided into two parts: the Authority Format Identifier (AFI) and Initial Domain Identifier (IDI).

(3) Authority Format Identifier

The first part, AFI, identifies the format being used for the IDI, identifies the authority responsible for assigning the NSAP address values and gives the abstract syntax of the DSP. GOSIP uses an AFI value of 47.

(4) Initial Domain Identifier

The second part, IDI, specifies the domain to which the address belongs. The IDI value 0005 represents the routing domain which has been assigned to the U.S. Government (non-tactical). The IDI value of 0006 has been reserved for tactical use by DoD.

(5) Domain Specific Part

The format for the DSP is not defined by the standard but must be established by the Reservation Authority for the 0005 domain. The standard allows a maximum length of

20 octets for the NSAP and this has been allocated as shown in figure A-7. The AFI of 47 occupies one octet, and the IDI of 0005 occupies two octets. These two values are encoded as decimal digits. The DSP is allocated into the following parts: DSP Format Identifier (DFI) one octet, Administrative Authority (AA) identifier three octets, Routing Domain (RD) two octets, Area two octets, ES identifier six octets and NSAP Selector (NSEL) one octet. Reserved (RSVD) has two octets for expansion.

(6) DSP Format Identifier

The DFI identifies the version of the DSP structure and associated semantics encoded within an NSAP address. GOSIP Version 2.0 has assigned the DPI value 80H to the NSAP structure.

(7) Administrative Authority

The AA identifier specifies the central authority within a GOSIP Administrative Domain for addressing.

(8) Routing Domain

A RD is a set of ESs and ISs which operate according to the same routing procedures is controlled by a single administrative authority and which is wholly contained within a single administrative domain. An administrative domain could be all the network entities under the control of a government agency. Administrative domains can have multiple routing domains. The administrative domain in this context is

not synonymous with the Message Handling System (MHS) Administrative Management Domain (ADMD). MHS Originator/Recipient (O/R) addresses exist in a separate hierarchy from NSAP addresses. The SRA will maintain a list of all assigned routing domains consistent with the established naming conventions already existing. End System naming will be under the control of the routing domain authorities. A RD identifier corresponds to the organization field in DoN naming conventions.

(9) Area

An Area field uniquely identifies a subdomain of the routing domain. An Area identifier corresponds to the Group field in Marine Corps naming conventions.

(10) End System Identifier

The ES identifier field identifies a unique system within an area. The value of the ES identifier field may be a physical address, i.e., SNPA address, or a logical address. A locally administered table is used to map the logical address to a corresponding physical address. An ES identifier corresponds to the User field in marine Corps naming conventions.

(11) NSAP Selector

The NSEL field allows the system to find the appropriate user of the network layer service within that ES. This is done by examining the value of the NSEL. The

first bit of the NSEL field identifies whether the network service is connectionless (0) or connection-oriented (1).

IDP		DSP						
AFI	IDI	DFI	AAI	RSVD	RD	A	ES	NSEL
47	0005 0006	80	005E00 000700	0000	RA	SRA	SA	SA
1	2	1	3	2	2	2	6	1

Legend			
A	Area	NSAP	Network Svc. Access Point
AAI	Admin Authority Identifier	NSEL	NSAP Selector
AFI	Authority & Format Identifier	RA	Registration Authority
DFI	DSP Format Identifier	RD	Routing Domain
DSP	Domain Specific Part	RSVD	Reserved
ES	End System	SA	System Administrator
IDI	Initial Domain Identifier	SRA	Sub-Registration Authority
IDP	Initial Domain Part		

GOSIP 2.0 NSAP Semantic

Figure A-7 OSI Network Service Access Point Structure

B. GOSIP ADDRESS REGISTRATION PROCEDURE

GOSIP addresses are registered into the GOSIP Directory using ISO 3166, Codes for the Representation of Names of Countries. The United States has been assigned a code of US and USA with a numerical code of 840. Under US, the American National Standards Institute (ANSI) has assigned the Federal Government the code of GOV with a numerical code of 101. General Services Administration (GSA) has been delegated the authority for assigning codes under code 101. The objects

used for inter-computer communications must be registered with the DoD registration authority to assure interoperability among the network users. This assurance is gained from unique, unambiguous identifiers. Objects included in the protocol standard need no be registered by users. Registration only becomes necessary when objects are not included in protocol standard specifications.

Objects are registered in a hierarchical structure as shown in figure A-8. ISO 6523, Structure for the Identification of Organizations, is used to identify organizational names. The national Institute of Standards and Technology has been assigned as the network Registration Authority for the United States. The GSA has been named the Executive Agent for Government Agencies. The DoD Executive Agent is assigned to DISA. The Navy Sub-Registration Authority (SRA) is NCTS, Washington, D.C. and the Marine Corps SRA for registering user information for OSI objects with the DoN RA is vested in Director MCCTA, Quantico for tactical and tactical support users. GOSIP registration falls within three broad categories: NSAP, Names (Message Handling System (X.400), directory (X.500)) and Application-specific (FTAM, VT, Private Message Body Parts, Document Application Profiles, i.e., Object Identifiers (OID)).

1. Names Registration

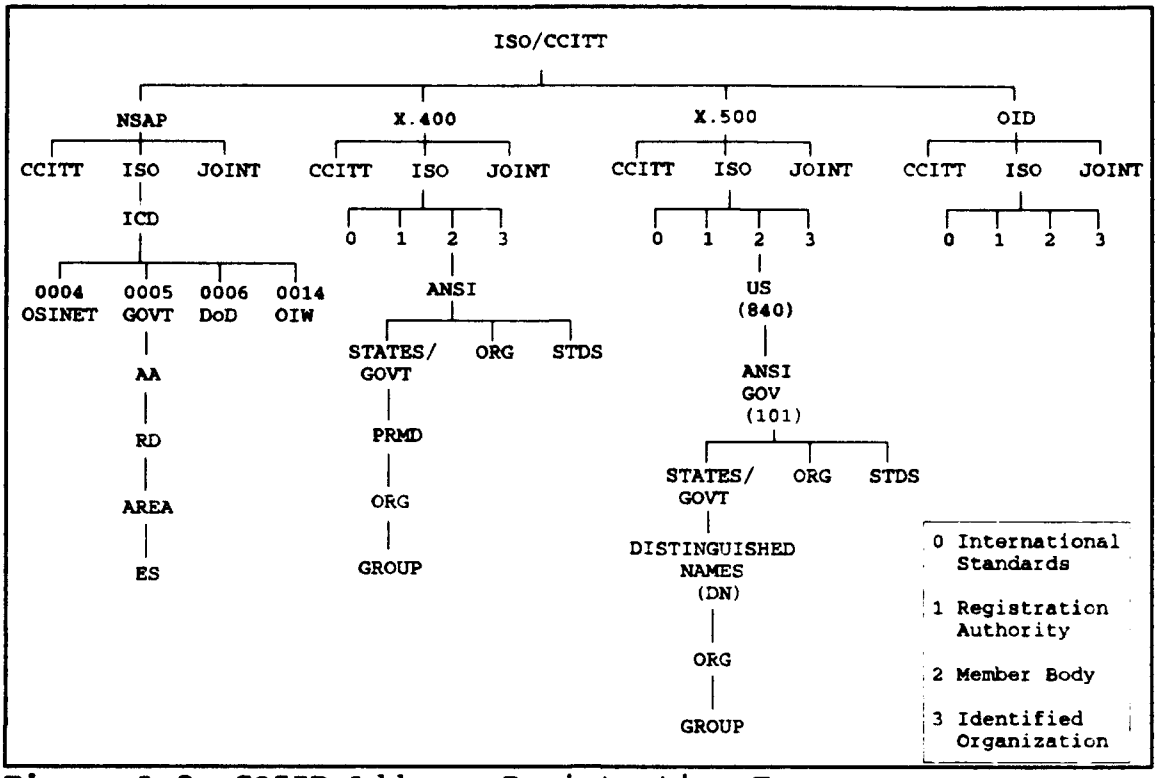

Figure A-8 GOSIP Address Registration Tree

Originator/recipient (O/R) names are assigned by a Registration Authority for use in X.400 MHSs. These names consist of alphabetic and numeric characters. O/R names are organizationally structured, analogous to Plain Language Address Designators (PLADs). An assigned name may have the following attributes:

- PrivateDomainName (16 characters max)
- OrganizationName (64 characters max)
- OrganizationalUnit (32 characters max)

2. Application-specific Registration

This group of objects requires specific registration of their profile as this situation differs from address

registration. The format of each profile specifies data field construction to assure interoperability. These objects include File Transfer, Access and Management (FTAM), document type names, MHS Private Body Parts, Virtual Terminal (VT) Profiles and Control Objects and Document Application Profiles (DAP). Registration of FTAM Document Types, MHS Private Body parts, VT Profiles and Control Objects and Document Application Profiles is optional and should be requested only under special circumstances.

LIST OF REFERENCES

Boland, T., *Government Open Systems Interconnection Profile Users' Guide, Version 2*, U.S. Government Printing Office, 1991.

Burns, N., and Radicati, S., "Anatomy of an Evolving Standard," *Corporate Computing*, v.1, n.1, pp. 179-182, June/July 1992.

Becker, P., "A Ghost of an OSI Chance," *LAN Magazine*, v.7 n.12, December 1992.

Breidenbach, S., "GOSIP Gossip: Just Lip Service?," *LAN Times*, v.9 n.7, 20 April, 1992.

Cline, G., "Real GOSIP Products: Where the Rubber Meets the Road," *Information Strategies Group of IDC Government*, No. W1591, January 1993.

Cline, G., "GOSIP: Determining Who Really Delivers the Goods," *Information Strategies Group of IDC Government*, No. W1539, August 1992.

Department of the Navy (DoN), *Government Open Systems Interconnection Profile (GOSIP) Implementation and Transition Plan (Draft)*, 1993.

Electronic Mail conversation between Robert Cooney, NARDAC Washington D.C., and author, March 1993.

Federal Information Processing Standards (FIPS) Publication 146, *Government Open Systems Interconnection Profile (GOSIP)*, National Institute of Standards and Technology, U.S. Government Printing Office, 1988.

Federal Information Processing Standards (FIPS) Publication 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, National Institute of Standards and Technology, U.S. Government Printing Office, 1991.

Federal Information Processing Standards (FIPS) Special Publication 500-177, *Stable Implementation Agreements for Open Systems Interconnection Protocols*, National Institute of Standards and Technology, U.S. Government Printing Office, 1985.

Federal Register, "Announcing the Standard for Government Open Systems Interconnection Profile (GOSIP)," v.56 n.64, April, 1991.

GOSIP Institute, *INTERNET 2000: A Protocol Framework to Achieve a Single Worldwide TCP/IP/OSI/CLNP Internet by Year 2000*, 1993.

GOSIP Institute, *One-Day GOSIP*, 1992.

Hall, M., "Hello. I Must be Going," *LAN Technology*, v.9 n.4, April 1993.

Masud, S.A., "GOSIP Barley Makes a Dent in Real-World Fed Networks," *Government Computer News*, v.12 n.6, 15 March 1993.

Masud, S.A., "Lab Will Help Agencies Implement GOSIP on Multivendor Systems," *Government Computer News*, v.12 n.7, 29 March, 1993.

Masud, S.A., "Defense's One-Stop GOSIP Shop," *Government Computer News*, v.12 n.10, 10 May 1993.

Messmer, E., "NIST Explains GOSIP Procurement Rules," *Network World*, v.9 n.50, 14 December, 1992.

Metcalfe, R.M., "Truth or Dare: Who Favors Open Systems?," *INFOWORLD*, v.14, n.50, 14 December 1992.

National Institute of Standards and Technology, *Industry/Government Open Systems Specification (Draft)*, 1993.

Nelson-Rowe, L., "IBM's Networking Head Sketches Out Unit's Near-Term Strategies," *Open Systems Today*, p. 82, v.122, 26 April, 1993.

Rose, M.T., "The Future of OSI: A Modest Prediction," *Upper Layer Protocols, Architectures and Applications*, pp. 356-365, Proceedings of the IFIP, 1992.

Stallings, W., *Data and Computer Communications*, Macmillan, Inc., 1991.

Telephone conversation between Ed Taylor, and author, July 1993.

Telephone conversation between MAJ Mike Wilson, Joint Interoperability Test Center, and author, February 1993.

BIBLIOGRAPHY

Baker, S., "The Network Lament: Routing and Addressing Problems on the Internet," *UNIX Review*, v.10 n.11, November 1992.

Bass, B., "NIST, Industry Collaborate on OSI Specs," *Federal Computer Week*, v.6 n.13, 1 June 1992.

Cline, G., "OSI Integration Strategies: Shooting the Rapids," *Information Strategies Group of IDC Government*, No. W1250, October 1990.

Cline, G., "Electronic Massaging: The Tie That Binds," *Information Strategies Group of IDC Government*, No. W1494, June 1992.

Connelly, J., "NIST's Boland Guides Feds Towards GOSIP," *Federal Computer Week*, v.6 n.26, 31 August 1992.

Dostert, M., "GOSIP: A Brave New World or a Networking Nuisance?," *LAN Times*, v.9 n.8, 11 May 1992.

Eckerson, W. and Messmer, E., "Is OSI Dead?," *Network World*, v.9 n.24, 15 June 1992.

Electronic Mail conversation between Dan Greene, Naval Surface Warfare Center Dahlgren Division, Code B35, and author, February 1993.

Electronic Mail conversation between Elle Gardner, MITRE, and author, March 1993.

Electronic Mail conversation between Ole Jacobson, INTEROP, and author, January 1993.

Electronic Mail conversation between Frank Deckelman, SPAWAR, Code 32, and author, February 1993.

Electronic Mail conversation between Marshall Rose, Dover Beach Consulting, and author, January 1993.

Electronic Mail conversation between Dennis Warne, Naval Surface Warfare Center White Oak, and author, February 1993.

Electronic Mail conversation between Richard desJardins, GOSIP Institute, and author, February 1993.

Electronic Mail conversation between Nancy Pierce, OSINET Corporation for Open Systems, and author, February 1993.

Electronic Mail conversation between Cyndi Jung, 3Com Corporation, and author, February 1993.

Electronic Mail conversation between Jerry Mulvenna, NIST, and author, February 1993.

Electronic Mail conversation between Darrel Beach, USAF DDN Program Office, and author, March 1993.

Electronic Mail conversation between Kevin Oberman, Lawrence Livermore National Laboratory, and author, March 1993.

Electronic Mail conversation between Joel Snyder, University of Arizona, and author, March 1993.

Electronic Mail conversation between CDR Greg Sawyer, SPAWAR, and author, January 1993.

Harrison, B.T., "Toward Global E-Mail," *DEC Professional*, v.11 n.8, August 1992.

Herman, E., "Federal Users Have Cold Feet About GOSIP," *Federal Computer Week*, v.6 n.8, 13 April 1992.

Holms, E., "Interoperability: A Survey of the Market," *Federal Computer Week*, v.6 n.11, 11 May 1992.

Houser, W.R., "GOSIP Meets Resistance from Wary Agencies," *Government Computer News*, v.11 n.6, 16 March 1992.

IDG Research Services, *Federal Computer Week/Interop Internetworking Study*, April 1992.

Information Strategies Group, *Federal Microcomputer Study: Technology for the '90s*, 5 August 1992.

Institute for Defense Analyses Paper P-2041, *The Effects of Transition from DoD to ISO OSI Communication Protocols*, 3 December 1987.

Martin, W.R., *C3 Interoperability Issues: An Overview of GOSIP Network Conformance Testing in the Evolution of the Defense Information System Network (DISN)*, Master's Thesis, Naval Postgraduate School, Monterey, California, June 1992.

Masud, S.A., "Livermore Official Voices Concern Over Government OSI Requirements," *Government Computer News*, v.11 n.16, 3 August 1992.

Messmer, E., "OSI Spec to Spur Product Development," *Network World*, v.9 n.37 14 September 1992.

Messmer, E., "Getting Users to Buy GOSIP Products Like Pulling Teeth," *Network World*, v.9 n.32, 10 August 1992.

Rogers, B., "Shy of Risks, Government Crawls Toward Standard," *Government Computer News*, v.11 n.2, 20 January 1992.

Silver, J., "Army Interconnection Project brings GOSIP to Life," *Government Computer News*, v.11 n.2, 20 January 1992.

Smalley, E., "SNMP Revision to Move Protocol into Prime Time," *Digital Review*, v.9 n.15, 10 August 1992.

Telephone conversation between Robert Ziff, Ziff-Davis Publishing, and author, March 1993.

Telephone conversation between John Hooder, SECNAV, and author, March 1993.

Telephone conversation between CAPT John Weggan, USMC, Defense University, and author, March 1993.

Telephone conversation between A.J. Cobbon, IBM Corporation, and author, March 1993.

Thompson, T., "PowerPC Performs for Less," *Byte*, v.18 n.9, August, 1993.

Ziff, R., "The Power of Standards," *Corporate Computing*, v.1 n.6, December, 1992.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria VA 22304-6145	2
2.	Library, Code 052 Naval Postgraduate School Monterey CA 93943-5002	2
3.	Professor Myung Suh Department of Administrative Sciences Code AS/SU Naval Postgraduate School Monterey, CA 93943	1
4.	Professor Barry Frew Department of Administrative Sciences Code AS/FW Naval Postgraduate School Monterey, CA 93943	1
5.	Lieutenant Mark R. Laxen 1800 Stoney Brook, #202 Houston, TX 77063	2