2

IDA PAPER P-2041

THE EFFECTS OF TRANSITION FROM DoD TO ISO OSI COMMUNICATION PROTOCOLS

James Baldo
David O. Levan

November 1987

Prepared for
C3 Systems, Joint Requirements Integration Manager

IDA

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION
Unclassified

1b RESTRICTIVE MARKINGS

2a SECURITY CLASSIFICATION AUTHORITY

2b DECLASSIFICATION/DOWNGRADING SCHEDULE

3 DISTRIBUTION/AVAILABILITY OF REPORT
Public release/unlimited distribution.

4 PERFORMING ORGANIZATION REPORT NUMBER(S)
IDA Paper P-2041

5 MONITORING ORGANIZATION REPORT NUMBER(S)

6a NAME OF PERFORMING ORGANIZATION
Institute for Defense Analyses

6b OFFICE SYMBOL
IDA

7a NAME OF MONITORING ORGANIZATION
OUSDA, DIMO

6c ADDRESS (City, State, and Zip Code)
1801 N. Beauregard St.
Alexandria, VA 22311

7b ADDRESS (City, State, and Zip Code)
1801 N. Beauregard St.
Alexandria, VA 22311

8a NAME OF FUNDING/SPONSORING ORGANIZATION
C3 Systems, JRIM/JCS

8b OFFICE SYMBOL (if applicable)

9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
MDA 903 84 C 0031

8c ADDRESS (City, State, and Zip Code)
IE833, The Pentagon
Washington, D.C. 20301

10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
		T-I5-444	

11 TITLE (Include Security Classification)
The Effects of Transition from DoD to ISO OSI Communication Protocols (U)

12 PERSONAL AUTHOR(S)
James Baldo, David O. Levan

13a TYPE OF REPORT
Final

13b TIME COVERED
FROM _______ TO _______

14 DATE OF REPORT (Year, Month, Day)
1987 November

15 PAGE COUNT
112

16 SUPPLEMENTARY NOTATION

17 COSATI CODES

FIELD	GROUP	SUB-GROUP

18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Communication protocols; Open System Interconnection (OSI); Government Open System Interconnection Profile (GOSIP); interoperability.

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The purpose of this IDA Paper is to analyze the results of the Federal Government's transition to the ISO OSI communication protocols as mandated by the Government Open System Interconnection Profile (GOSIP). This document analyzes the interoperability issues that will affect the communications between C2Is during the transition from DoD to ISO protocols. Information for the analysis was gathered from the open (unclassified) literature, correspondence with protocol implementors on the ARPANET, attendance at the NBS OSI Implementors workshop, and the authors' implementation experience with communications protocols.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED □ SAME AS RPT. □ DTIC USERS

21 ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a NAME OF RESPONSIBLE INDIVIDUAL
James Baldo

22b TELEPHONE (Include area code)
(703) 824-5516

22c OFFICE SYMBOL
IDA/CSED

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

IDA PAPER P-2041

THE EFFECTS OF TRANSITION FROM DoD TO ISO OSI COMMUNICATION PROTOCOLS

James Baldo
David O. Levan

November 1987

INSTITUTE FOR DEFENSE ANALYSES

MDA 903 84 C 0031
Task T-15-444

CONTENTS

LIST OF FIGURES

Preface

The purpose of IDA Paper P-2041, *The Effects of Transition from DoD to ISO OSI Communication Protocols*, is to analyze the results of the Federal Government's transition to the International Standards Organization (ISO) Open Systems Interconnection (OSI) communication protocols as mandated by the Government Open System Interconnection Profile (GOSIP). This paper analyzes the interoperability issues that will affect the communications between the C2ISs during the transition from DoD to OSI protocols.

Information for the analysis was gathered from the open (unclassified) literature, correspondence with protocol implementors on the ARPANET, attendance at the National Bureau of Standards OSI Implementors Workshop, and the authors' implementation experience with communications protocols.

This document fulfills an objective of IDA task order T-I5-444, "Command and Control Information System (C2IS) Interoperability," which was to assist the JCS/J6W office in determining that Command and Control systems used in Joint and combined operations are interoperable. P-2041 analyzes the ISO OSI protocols' effects on the interoperability of military C2IS.

The document was reviewed on 3 December 1987 by the members of the following IDA Peer Review Panel: Dr. Robert Winner, Dr. Joseph Linn, Dr. James Pennell, and Ms. Katydean Price.

EXECUTIVE SUMMARY

The sponsor, the Joint Chiefs of Staff, Command, Control and Communications Systems, Joint Requirements Manager Office (officially referred to as JCS/J6W, JRM), requested the Institute for Defense Analyses to assess the effect of the proposed transition from the Department of Defense (DoD) communication protocols to the International Standards Organization Open Systems Interconnect (ISO OSI) standards on the Command and Control Information Systems (C2IS). This document was developed under IDA task order T-I5-444, entitled "Command and Control Information System Interoperability."

This paper is not intended to be a transition plan for the DoD, since the official transition plan was released by the Defense Communications Agency (DCA) in November 1987. This IDA study did not have access to the DCA transition plan and the observations in this document were based on the status of ISO OSI protocols, NBS Implementors Workshop, discussions with principals involved with OSI implementations, and current open literature.

The motivation for transition to the ISO OSI communication protocols is interoperability, standardized hardware and software, and therefore, lower development time and costs. There is a strong desire by the DoD to obtain interoperability between current and planned military and commercial communication networks. At present, OSI communication protocols are being developed for the commercial sector, which will begin to purchase such systems as soon as mature products become available.

During times of crisis, the military should have the potential capability of using commercial networks. This relieves them from having to build and maintain large capacity

networks that will be under-utilized.

NATO has also declared [STANAG 4250] that all member countries will use ISO OSI communication protocols in their communication systems. The ability to use commercially available products that adhere to accepted international standards enables the DoD to benefit from using Commercial-Off-The-Shelf (COTS) hardware and software communication products, which will result in lower development time and costs.

Military communication systems requirements for security, performance, and survivability are difficult to realize under any network architecture. The DoD has met some of these requirements by moving toward a multi-network architecture using Transmission Control Protocol (TCP) for end-to-end services and Internet Protocol (IP) for internetwork connections. The efforts of the ARPANET and other military packet-switch networks (e.g., WWMCCS Intercomputer Network) have obtained impressive results.

However, new demands on network capabilities and capacities will require new technology. Traffic congestion resulting from increased numbers of new users, applications, and Local Area Networks needs to be addressed. There is a need for new applications programs, possibly requiring network services that were not designed into the current architectures, to be developed.

The Government's Open System Interconnection Profile (GOSIP) [GOSIP 87] provides guidelines and recommendations for federal agencies in the procurement of ISO OSI communication protocols. The document will become a Federal Information Processing Standard (FIPS) by the end of 1987. The DoD, as of 2 July 1987 through a memorandum from the Assistant Secretary of Defense for Command, Control, Communication, and

Intelligence, stated that ISO OSI communication protocols can be used as alternatives to DoD protocols. The memorandum explicitly states that the services and agencies must be aware of issues that may impact their communication operations (i.e., interoperability with other systems) by using the OSI protocols. Although it is clear that the DoD will eventually move to the OSI protocols, the transition path is unclear.

Currently, there is a testbed, OSINET, managed by the National Bureau of Standards (NBS) for the development of ISO OSI protocols. This network is used by vendors to demonstrate interoperability of their products. Discussions with vendors has indicated that OSI products are in various stages of development and testing.

It has been recognized that converging to an international communications standard will improve the current interoperability problems experienced in the military and commercial sectors. However, OSI alone is not a solution to all of the current or projected communications problems. The following list is a set of observed problems that are related to the transition to a complete OSI communication network:

a. The development of gateways that provide interoperability between OSI, TCP/IP, proprietary, and mixed OSI/TCP/IP networks must be given a high priority.

b. The transition to OSI protocols will result in a mix of OSI and TCP/IP hosts on a TCP/IP network. How interoperability among these different protocol families will be achieved is not currently clear and must be addressed.

c. Currently, the Acquisition Authorities do not have personnel that are knowledgeable about the DoD and ISO OSI models, protocols, their options, and implementation details in order to procure the appropriate OSI products to fulfill their organizational requirements.

d. At this time there are only two OSI applications available and specified by GOSIP. They are the File Transfer and Access Management (FTAM) and the Message Handling System (MHS).

e. The development state of the network management services is too immature to support any products. From discussions in the Implementation Agreements for Open Systems Interconnection Protocols, it does not appear that products will be available until 1991. This will slow the process of implementing security services into OSI protocols and other application protocols that use the management services.

f. The development of Directory Services products is not expected until 1989. Currently, primitive solutions such as static routing tables are used on hosts. As with network management, protocols relying on sophisticated services provided by the Directory will either be developed with a pseudo-directory service built-in or their introduction may be delayed until Directory Services become available. The OSI protocols were developed with an international community in mind and therefore, had to provide a much greater flexibility than the current DoD implementation. This implies more overhead (i.e., parsing) for many applications of the OSI protocols with the resulting adverse effect on performance.

g. At present, due to the lack of a Draft International Standard for an Intermediate System to Intermediate System (IS-IS) protocol, no long-haul OSI networks exist. Past experience (e.g., ARPANET) has shown that until such a prototype network is implemented, interoperability problems undetected during development may manifest themselves in the implementation.

h. Methods to achieve interoperability between networks using a mixture of connection and connectionless Network Layers need to be implemented and tested. At present, COS 265 is the only proposal that is being reviewed by ISO to address this potential problem.

i. A number of interoperability problems between the 1984 and 1988 X.400 Message Handling Systems (MHSs) must still be resolved. Since vendors have already implemented to the 1984 specification, these MHS versions will be operational wher 1988 MHS systems become operational.

1. INTRODUCTION

1.1 PURPOSE

The purpose of IDA Paper P-2041 is to provide the Joint Chiefs of Staff, Command, Control and Communications System Joint Requirements Integration (C3SJ) effort with an analysis of the effects of the transition from Department of Defense communications protocols to the International Standards Organization (ISO) Open Systems Interconnect (OSI) communications protocols.

1.2 BACKGROUND

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence issued a memorandum on 2 July, 1987, stating that ISO OSI communications protocols could be used as alternatives to the DoD protocols. The same memorandum explicitly stated that it was the responsibility of the services and agencies considering such a transition path to be aware of such issues as interoperability with other systems. A copy of the memorandum is found in Appendix C.

Although it is inevitable that the DoD will eventually adopt the OSI protocols, the transition path is unclear. The Government Open System Interconnect profile (GOSIP) provides guidelines and recommendations for federal agencies in the procurement of ISO OSI communications protocols [GOSIP 87]. GOSIP is scheduled to become a Federal Information Processing Standard by the end of 1987.

1.3 SCOPE

The organization of the document is as follows:

a. Current network status (Section 2)

b. Analysis of the OSI Network Architecture (Section 3)

c. Analysis of GOSIP (Section 4)

d. Issues affecting the transition (Section 5)

Appendix A contains an overview and a more detailed description of the ISO OSI Network Architecture and Appendix B presents an overview of GOSIP. Appendix C contains a copy of the Latham memorandum, 2 July 1987.

Information for the analysis was based on open (unclassified) literature searches and reviews, ARPANET correspondence with the protocol implementors, notes from the National Bureau of Standards (NBS) OSI Implementors Workshop [NBS 87], and the authors' own implementation experience of certain communications protocols.

1.4 STANDARDS ORGANIZATION

Standards play a key role in achieving interoperability for heterogeneous computer systems and networks. Countries and organizations are working in concert on the development of standards. Both commercial and military organizations within the participating countries are considering transition plans for adaptation to the ISO standards.

A large number of commercial vendors are already implementing the OSI suite of protocols and interoperability testing between vendors is currently being performed. IDA Paper P-1842 [Nash 85] gives a detailed list of standards and standards organizations.

1.5 REFERENCES

The following references were used in developing this document.

[Baker 86] Baker, V.C. and J. Baldo Jr. 1986. Developing communication protocols in Ada. *Defense Electronics* 18/6 (December): 90-96.

[CCITT X.25] CCITT. 1984. *X.25, Interface between data terminal equipment (DTE) and data circuit terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.* Vienna, VA: Omnicom.

[CCITT X.200-250] CCITT. 1985. *Red Book. Volume VIII - Fascicle VIII.5, Data communication networks: Open Systems Interconnection (OSI), system description techniques. Recommendations X.200-X.250.* Vienna, VA: Omnicon, Inc.

[CCITT X.400-X.430] CCITT. 1985. *Red Book. Volume VIII - Fascicle VIII.7, Data communication networks message handling systems. Recommendations X.400-X.430.* Vienna, VA: Omnicon, Inc.

[Cerf and Lyons 83] Cerf, Vinton G. and Robert E. Lyons. 1983. Military requirements for packet-switched networks and their implications for protocol standardization. *IEEE Computer Networks* 7 (July): 293-306.

[COS 265] Corporation for Open Systems. A COS proposal is being reviewed by the ISO to address the method of implmenting and testing interoperability between networks using a mixture of connection and connectionless network layers

[DoD 3405] U.S. Department of Defense. 1987. *DoD Directive 3405, Computer programming language policy.* Washington, D.C.: DoD.

[EIA-232-D] Electronics Industries Association (EIA). *EIA-232-D, Interface between data terminal equipment and data communication equipment employing serial binary data interchange.*

[FIPS 71] U.S. Department of Commerce, National Bureau of Standards. 1979. *FIPS PUB 71, Advanced data communication control procedures (ADCCP).* Springfield, VA: NTIS.

[FIPS 100] U.S. Department of Commerce, National Bureau of Standards. 1983. *FIPS 100, Interface between data terminal equipment (DTE) and data circuit terminating equipment (DCE) for operation with packet-switched data communications networks.* Springfield, VA: NTIS.

[FIPS 107] U.S. Department of Commerce, National Bureau of Standards. 1984. *FIPS PUB 107, Local area networks: Baseband carrier sense multiple access with collision detection access method and physical layer specifications and link layer protocol.* Springfield, VA: NTIS.

[GOSIP 87] U.S. Department of Commerce. National Bureau of Standards. 1987. *U.S. Government open systems interconnection profile (GOSIP).* Draft. Springfield, VA: U.S. Department of Commerce.

[HDLCP] *Information processing systems - Data communications - High-level data link control procedures - Description of the X.25 LAPB- compatible DTE data link procedures, IS*

7776.

[IEEE 802.2] IEEE, Inc. 1982. *ANSI/IEEE Std 802.2-1985, IEEE standards for local area networks: Logical link control.* New York: IEEE, Inc.

[IEEE 802.3] IEEE, Inc. 1985. *ANSI/IEEE Std 802.3-1985, IEEE standards for local area networks: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification.* New York: IEEE, Inc.

[IEEE 802.4] IEEE, Inc. 1985. *ANSI/IEEE Std 802.4-1985, IEEE standards for local area networks: Token-passing bus access method and physical layer specifications.* New York: IEEE, Inc.

[ISO 7498] International Standards Organization. 1984. *ISO information processing systems - Open system interconnection - Basic reference model.* Vienna, VA: Omnicon.

[ISO 8348] International Standards Organization. 1986. *Information processing systems - Open systems interconnection - Network service definition.* Vienna, VA: Omnicom.

[ISO 8473] International Standards Organization. 1986. *Information processing systems - Open systems interconnection - Protocol for providing the connectionless network service.* Vienna, VA: Omnicon.

[ISO 8072/DAD1] International Standards Organization. 1986. *ISO 8072/DAD1, Transport service definition for connectionless-mode transmission.* Vienna, VA: Omnicom.

[ISO DIS 8602] International Standards Organization. *ISO DIS 8602, Transport protocol for* *connectionless-mode transmission*. Vienna, VA: Omnicom.

[ISO DP 9542] International Standards Organization. 1986. *ES-IS routing with ISO IS 8473*. Vienna, VA: Omnicom.

[JCS Pub 1] U.S. Department of Defense, Joint Chiefs of Staff. 1986. *JCS Pub 1, Dictionary of military and associated terms*. Washington, D.C.: U.S. DoD.

[MIL-STD-188/144A] U.S. Department of Defense. 1985. *MIL-STD-188/144A, Electrical characteristics of digital interface circuits.* Washington, D.C.: U.S. DoD.

[MIL-STD-1777] U.S. Department of Defense. 1983. *MIL-STD-1777, Military standard internet protocol.* Washington, D.C.: U.S. DoD.

[MIL-STD-1778] U.S. Department of Defense. 1983. *MIL-STD-1778, Military standard transmission control protocol.* Washington, D.C.: U.S. DoD.

[Nash 85] Nash, S.H. and S.T. Redwine. 1985. *Information interface related standards, guidelines, and recommended practices*. Alexandria, VA: Institute for Defense Analyses. IDA Paper P-1842; NTIS AD-A170 630.

[NBS 87] U.S. Department of Commerce, National Bureau of Standards. 1987. *Implementation agreements for open systems interconnection protocols: NBS workshop for implementors of open systems interconnection.* Springfield, VA: NTIS. NBSIR 86-3385-6, Revised July 1987.

[Quarterman and Hoskins 86] Quarterman, J. and J.C. Hoskins. 1986. Notable computer networks. *Communications of the ACM* 29/10 (October): 932-971.

[RFC 983] Cass, D.E. and M.T. Rose. 1986. *ISO Transport Services on Top of the TCP.* Menlo Park, CA: SRI International.

[Schneidewind 83] Schneidewind, Norman F. 1983. Interconnecting local networks to long-distance networks. *IEEE Computer* 16/9 (September): 15-24.

[SPAG 85] Standards Promotion and Application Group. 1985. *Guide to the use of standards.*

[STANAG 4250] STANAG. 1983. *STANAG-4250 - NATO reference model for open systems interconnection - Overview.* Brussels: STANAG.

[Zhang 87] Zhang, Lixia. 1987. Some thoughts on the packet network architecture. *ACM Computer Communications Review* 17/1 & 2 (January/April): 3-17.

1.6 TERMS AND ABBREVIATIONS

The following terms and abbreviations are used in this document.

ACM	Association for Computing Machinery
ACSE	Association Control Service Element
AD	Addendum
ADCCP	Advanced Data Communication Control Procedure
ADP	Automated Data Processing

ANSI	American National Standards Institute
AT&T	American Telephone & Telegraph
C2IS	Command and Control Information Systems
C3I	Command, Control, Communications, and Intelligence
C3SJ	Command, Control and Communications System Joint Requirements Integration
CCITT	International Telegraph and Telephone Consultative Committee
CL	Connectionless
CLNP	Connectionless Network Protocol
CMSA/CD	Carrier Sense Multiple Access with Collision Detection
CO	Connection Oriented
COS	Corporation for Open Systems
DCA	Defense Communication Agency
DCE	Data Circuit Terminal Equipment
DDN	Defense Data Network
DIS	*Draft International Standard*

DoD	Department of Defense
DTE	Data Terminal Equipment
ECMA	European Computer Manufacturers Association
ES-IS	End System to Intermediate System
FIPS	Federal Information Processing Standard
FTAM	File Transfer and Access Management
FTP	File Transfer Protocol
GOSIP	Government Open Systems Interconnection Profile
GW	Gateway
IDA	Institute for Defense Analyses
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISO	International Standards Organization
ISODE	International Standards Organization Development Environment
JCS	Joint Chiefs of Staff

LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
MHS	Message Handling System
MIL-STD	Military standard
NBS	National Bureau of Standards
NIC	Network Information Center
NSAP	Network Service Access Point
NTIS	National Technical Information Service
NVLAP	National Voluntary Laboratory Accreditation Program
OSI	Open Systems Interconnection
OSINET	Open Systems Interconnection Network
PDU	Protocol Data Unit
RFC	Request for Comments
SAP	Service Access Point
SMTP	Simple Mail Transfer Protocol
SPAG	Standards Promotion and Application Group

TCP	Transmission Control Protocol
TP	Transport Protocol
VT	Vitual Terminal
WAN	Wide Area Network

2. CURRENT NETWORK STATUS

2.1 U.S. - MILITARY NETWORK REQUIREMENTS

2.1.1 Introduction

The DoD is depending more upon communications for successful operations of their mission critical systems. This dependence requires a communications model that is flexible enough for a myriad of DoD environments. The model must be easily extendable to future systems and accommodate performance requirements. This section discusses DoD military network requirements and the motivation for the transition to the OSI model and concludes with an analysis of future functionality that networks will need to support.

2.1.2 Requirements

The communication requirements of the DoD continue to increase with new requirements for new military systems. These systems not only require increased functionality and capabilities, but need to be interoperable[1] with present systems and future systems. Any transition that the U.S. or its Allies undergo with respect to the architecture of their communications systems must be closely scrutinized for interoperability and requirements of the military.

Military network requirements have been summarized in the following list [Cerf and Lyons 83]:

[1] Interoperability is the ability of systems, units, or forces to provide information or services to and accept information or services from other systems, units or forces and to use the information or services so exchanged to enable them to operate effectively together [JCS Pub 1].

a. Immunity to electronic countermeasures and spoofing.

b. Reliable and timely message delivery when network traffic exceeds normal operations.

c. For some military networks, survivabili'y under a variety of conditions and environments. Redundant and self-healing systems should be considered for military netwurks.

d. Security requirements are much more demanding than for public networks.

e. Interoperability with other military and public packet-switched networks.

In response to requirement (e), the current Internet is based on the Transmission Control Protocol [MIL-STD-1778] and Internet Protocol [MIL-STD-1777]. With the ISO OSI networks coming into existence during the next ten-year period, the DoD will be faced with interoperating within a collection of heterogeneous networks (Figure 1). The key to handling this problem is using gateways to interconnect the various networks. *Gateways* are entities (hardware or software) that convert from one protocol family to another, such as DoD to OSI. They usually reside in an *Intermediate System* (a system connected to two or more *networks) and often can perform relaying and routing operations* in addition to the translation function[2].

An example of the above interoperability problem is shown in Figure 2. It should be noted that gateways between proprietary LANs are usually a major design and

[2] A variation on this is the Translating Application Gateway, discussed in Chapter 4.

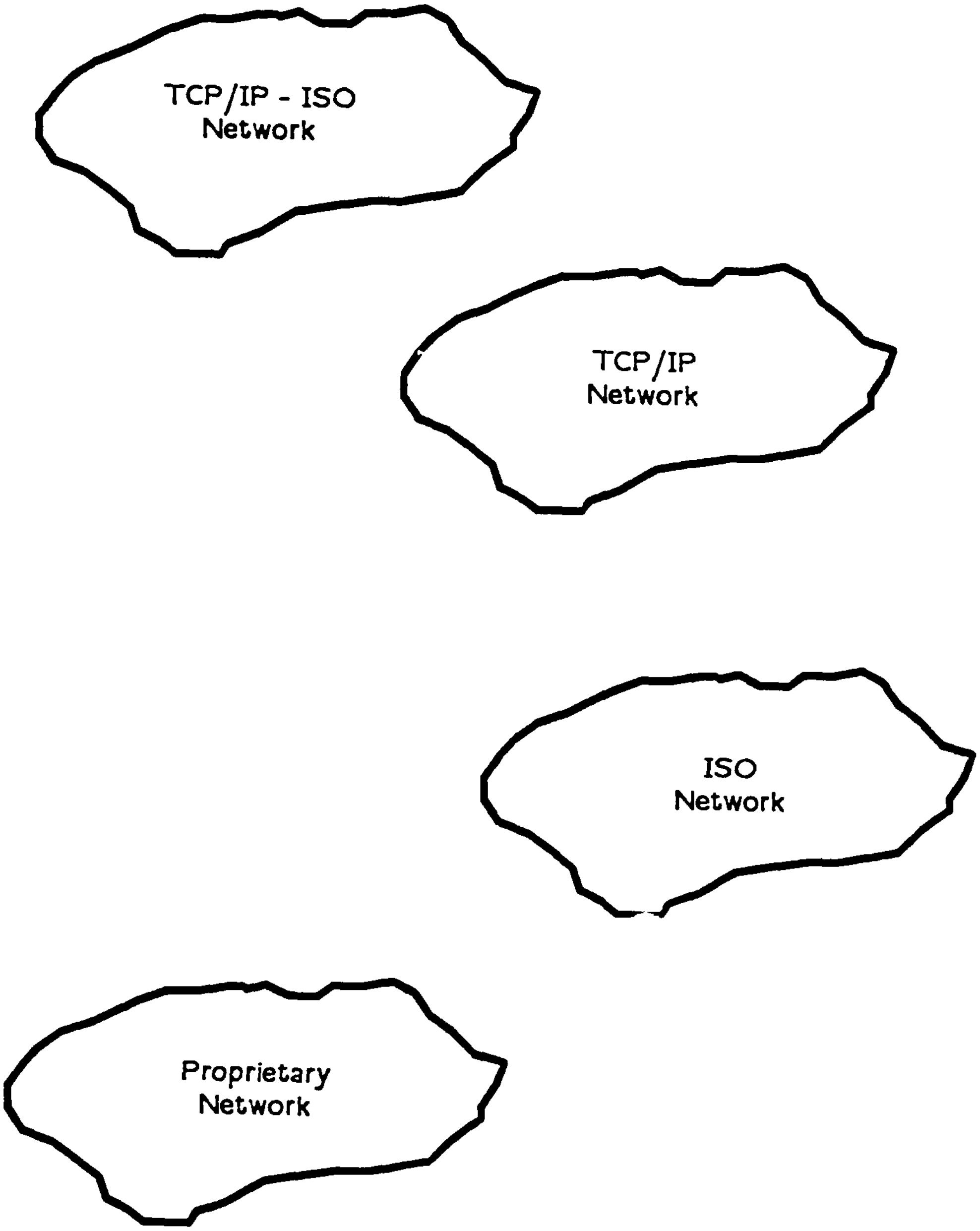

Figure 1. Possible Aggregate of DoD Networks

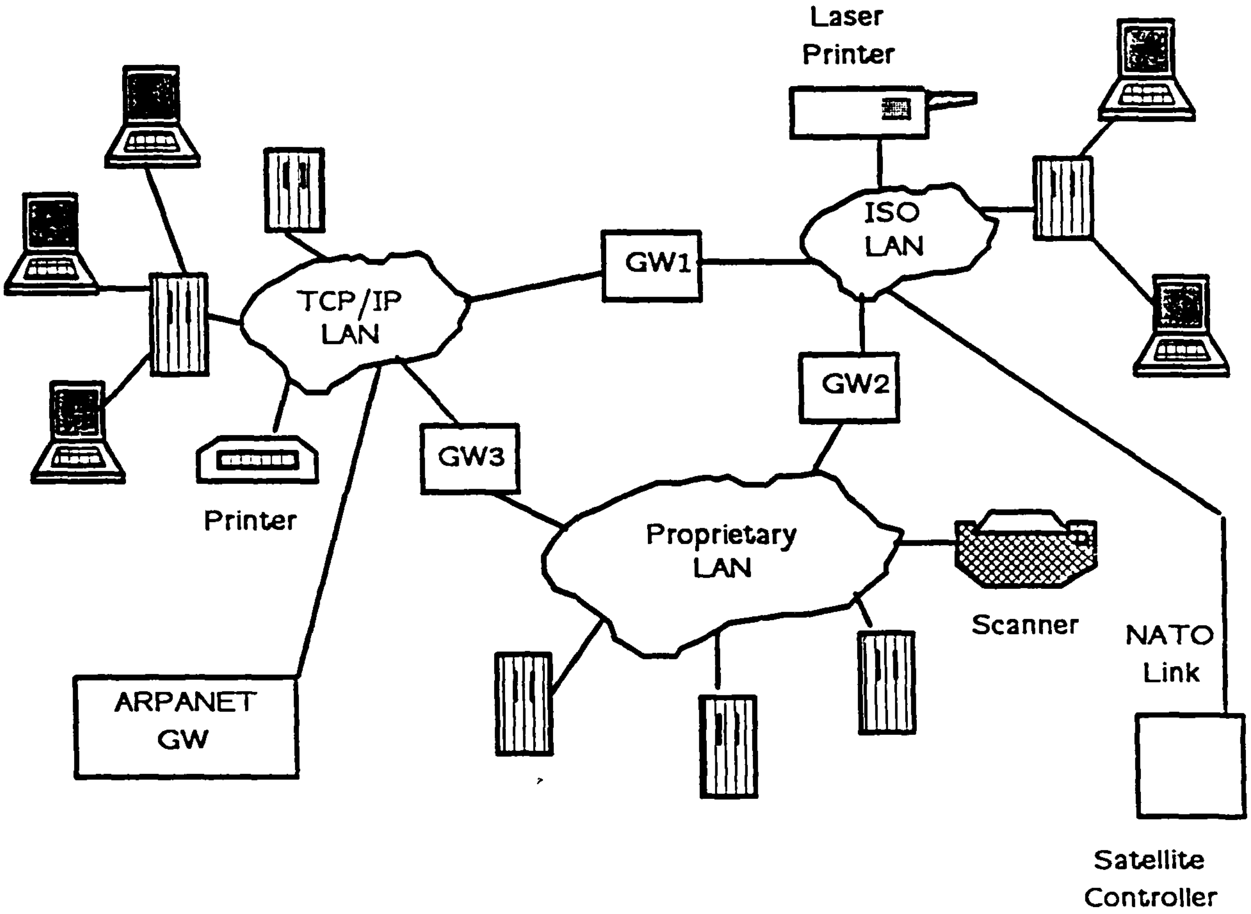

Figure 2. Possible DoD Scenario

implementation effort. This is due to the confidentiality of proprietary protocols and the difficulty of protocol-to-protocol translation.

2.1.3 DoD Motivation to Transition to OSI Protocols

The primary advantages of the DoD adhering to the ISO OSI communication standards are threefold:

a. *Economy.* Commercial products developed in the commercial arena will lower the costs of DoD procurement of systems.

b. *Availability.* Procuring systems that are composed of commercially-available-off-the-shelf (COTS) hardware and software components will reduce system delays due to development and implementation problems.

c. *Existing Services.* The DoD will be able to use existing commercial network services for a portion of their applications.

Therefore, if it is feasible to use commercial ISO OSI implementations and services in a large enough portion of the DoD's present and future applications, then transitioning to the ISO OSI protocols will be beneficial to the DoD in the long term.

2.1.4 Future Growth and Impediments

Network proliferation will continue in both the DoD and commercial sectors. User demands will increase for greater functionality in areas such as:

a. Graphics

b. Database

c. Real-time voice

d. Image data

e. Teleconferencing

f. Multimedia

As these applications become more widespread throughout networks, demands for network resources will surpass the DoD's current capacities.

2.1.5 DoD Reference Model Introduction

The DoD Communication Reference Model organizes protocols into groups, such that all protocols within a group have certain features in common. Within each group, one or more protocol levels have been identified for the purpose of defining more specific protocol functionality [Baker 86].

Figure 3 shows each protocol group and examples of current protocols. The groups are separated by interfaces to adjacent protocols. Each protocol defines a set of response and request primitives that adjacent protocols have access to from the interface. Request for Comments (RFCs) and Military Standards (MIL-STDs) are used as specifications from which the protocols are designed and implemented.

2.1.6 Current Status - DoD

At present, the current Internet (communication based on Internet Protocol (IP)) is composed of networks such as the ARPANET, NSFnet, military networks, university and research institutions, and a number of commercial institutions (Figure 4).

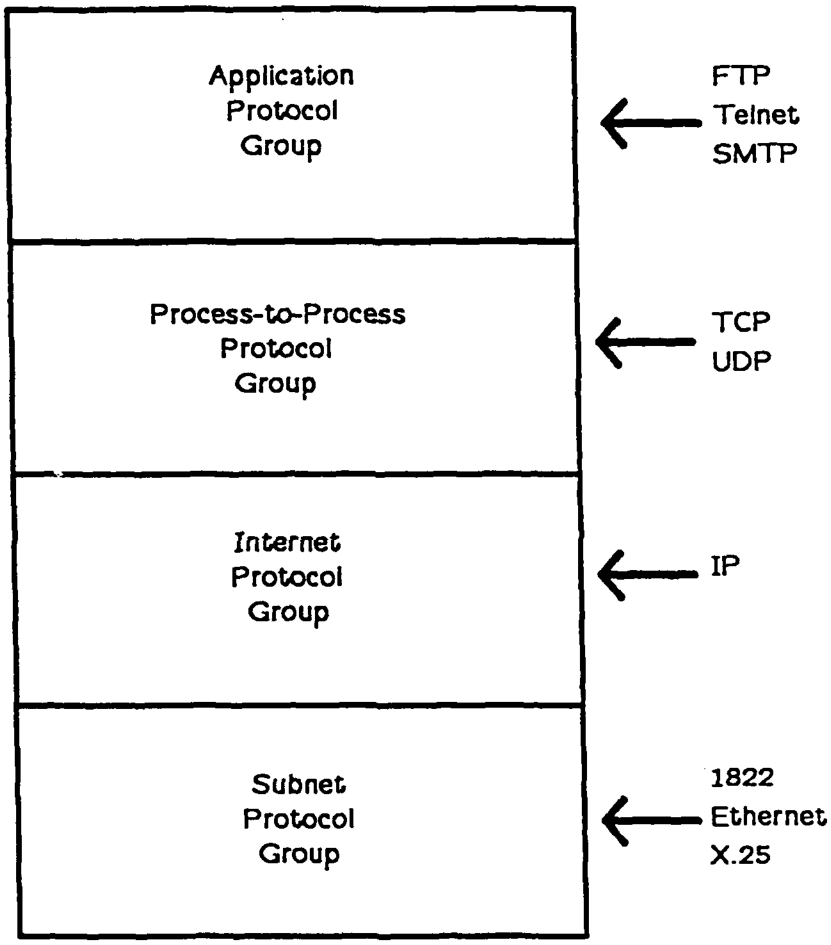

Figure 3. DoD Reference Model

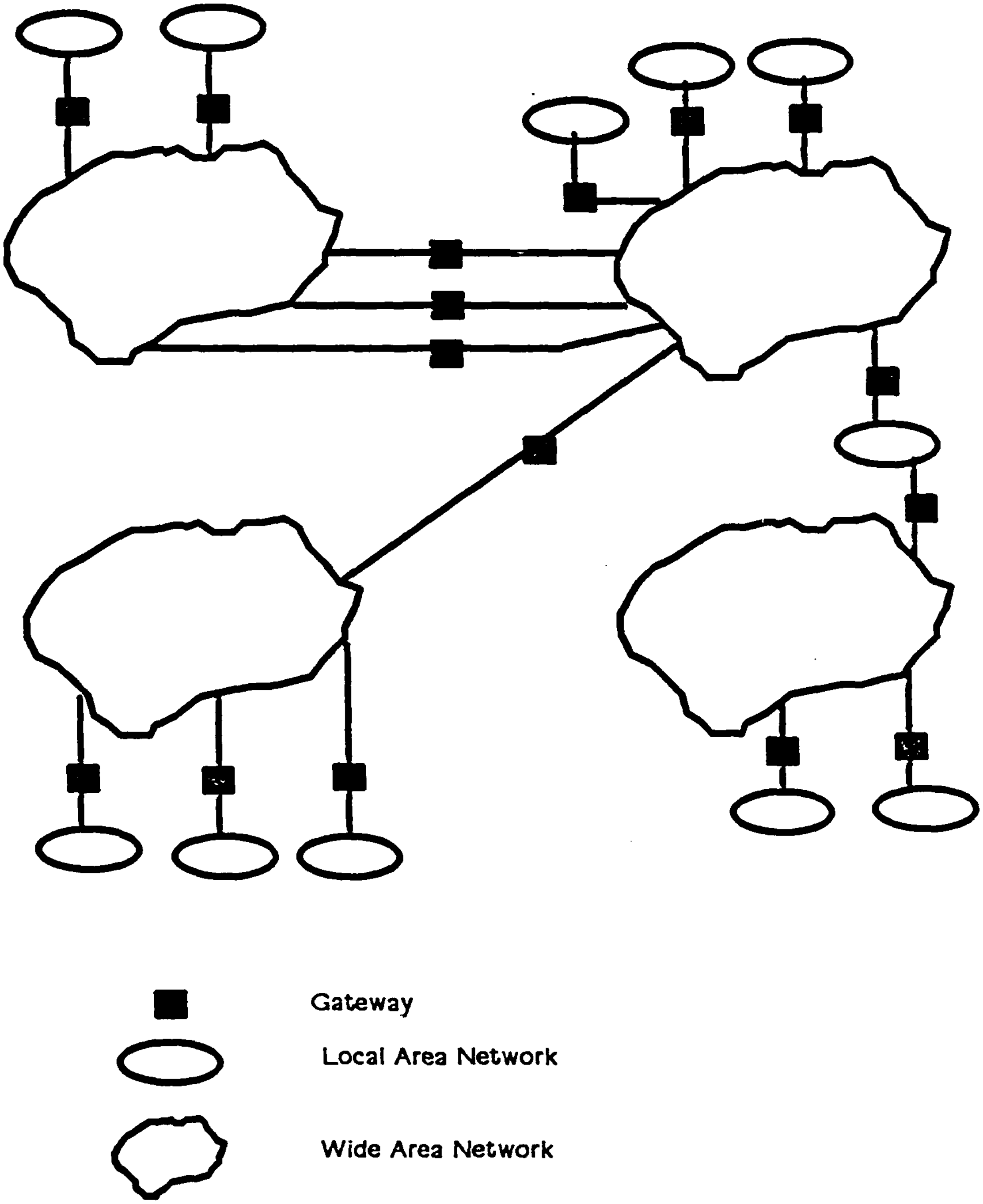

Figure 4. Overview of Present Internet

Networks presently exist as two types: Local Area Network (LAN) and Wide Area Network (WAN). A LAN is defined as a network internal to a university system, corporation, government agency, military base, etc. A WAN generally provides connectivity between LANs.

Networks classified as "connected" are attached to the Internet and must be registered with the Network Information Center (NIC) located at SRI. "Independent" networks are those registered with NIC but are not authorized to connect to the Internet. "Unregistered" networks are networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) but are using random network numbers[3] (possibly in conflict with each other and the registered networks). The following is a count of networks by NIC classification:

a. Connected - 300

b. Independent - 5,397

c. Unregistered - 10,000

A subset of the Internet funded by the DoD called the Defense Data Network (DDN), includes research networks, like ARPANET, and military networks, like MILNET. The ARPANET and MILNET form the backbone of the current Internet.

The MILNET is the result of splitting the ARPANET in October 1983. ARPANET gateways interconnect the two networks; this enables the MILNET to restrict traffic.

[3] Network numbers are part of the network address that represents the network. The NIC is the authority that issues network numbers.

The current number of hosts connected to the ARPANET and MILNET has been estimated at about 2,000 with anywhere between 10,000 and 100,000 users [Quartermain and Hoskins 86]. The ARPANET is currently run by the Defense Communications Agency (DCA).

2.2 OSI MODEL

The ISO OSI Communications Reference Model is based on an ordered set of layers. Within each layer, communication occurs between *peer-protocol entities* through peer-to-peer protocols. *Peer-protocol entities* are defined to be entities that reside at the same layer.

The model provides for two basic types of communication services: connection or connectionless service. Connection service essentially establishes a connection between protocol entities before passing data. Connectionless service sends data between protocol entities without establishing a connection. This distinction turns out to be important in that there is a difference between European and U.S. judgements on the appropriate choice. This, in turn, may lead to interoperability problems in NATO C2ISs.

A technical description of the OSI model is presented in Appendix A.

2.3 CURRENT R&D EFFORTS AND TECHNICAL GROUPS FOR ISO OSI

The DoD memorandum dated 2 July 1987 from Donald Latham, Assistant Secretary of Defense, stated that OSI protocols in accordance with GOSIP may be used as an optional alternative to DoD protocols (Appendix C). The OSI protocols are still regarded as experimental due to their current limited usage and implementations.

The Latham memorandum, however, clearly indicates that the transition to OSI protocols is definite. Currently, a number of efforts in the U.S. and internationally are going on to design and implement OSI protocols. Most of these efforts are just starting and many have not progressed far enough for any useful feedback. This section will describe the work of several prominent groups that are involved with actual implementation, developing protocol testing criteria, or OSI protocol profiles. OSI protocols support a large number of options and as a result may lead to a number of interoperability problems. An OSI profile provides implementation information to maintain interoperability among heterogeneous implementations.

2.3.1 SPAG and ECMA

Two major influences within the commercial European community for ISO OSI communication protocols are the European Computer Manufacturers Association (ECMA) and Standards Promotion and Application Group (SPAG). ECMA, despite its name, allows any computer manufacturer with any kind of base in Europe to be a member; so most of the US based multi-nationals are members of ECMA. In terms of role, ECMA tends to establish protocol standards for input to ISO. In 1981, ECMA started a new task group on local area networks (TG LAN) within the ECMA Technical Committee 24 that was responsible for the layers 1 - 4 of the OSI model. The work performed in this area by ECMA is concerned with the technical issues of standards and agreements made between the participating companies for endorsing the standard.

In 1983 SPAG was formed, comprising 12 major European computer and telecommunications companies. SPAG only allows European companies to join. This was the result of a number of European countries developing procurement policies that would affect the selection of communications protocols. These independent national procurement policies had the potential of causing interoperability problems at country borders, presumably due to product differences. This problem had already been encountered with X.25 [CCITT X.25] and telematic services.[4] SPAG produced a *Guide to the Use of Standards* [SPAG 85]. This guide contains information concerning profiles for LANS and choice of technology, protocols, and options within protocol layers 1 - 4. Eight of the 12 original SPAG members have set up a company called SPAG Services to work in the area of OSI testing, primarily interoperability testing rather than conformance testing.

2.3.2 Corporation for Open Systems

The Corporation for Open Systems (COS) is a U.S. non-profit consortium located in McLean, Virginia. It comprises both vendors and users and has taken on the task to establish conformance tests for emerging OSI network products. The COS has a large membership and includes the DCA and the NBS.

2.3.3 OSINET

The Open Systems Interconnection Network (OSINET) is a research and development network used to demonstrate the feasibility of ISO OSI communication protocol implementations. This effort provides a testbed for implementors to demonstrate the interoperability of their products among the participating members of OSINET. At present, the implementations are being developed by members who are communications vendors and who will be selling ISO OSI products in the marketplace.

[4] Telematic services is defined in this document as user-oriented information transmission services.

OSINET is geographically dispersed throughout the world. Two means of connection to the OSINET exist: ACCUNET[5] and WANGPAC[6]. ACCUNET is an X.25 network that is owned and maintained by American Telephone and Telegraph (AT&T). WANGPAC is an X.25 network that is owned and maintained by the Wang Information Service Corporation (wholly owned subsidiary of Wang Laboratories). Both networks supply X.25 networks that are compatible with the CCITT Recommendation [CCITT X.25].

Members connecting to OSINET need to select either ACCUNET or WANGPAC and supply the necessary Data Terminal Equipment (DTE) for the interface. The rest of the OSI protocols[7] recommended for communications on the network are:

a. ISO connectionless internetwork protocol

b. ISO Transport Class 4 protocol

c. ISO Session protocol (basic combined subset with full duplex)

Figure 5 illustrates two different connections to the OSINET. It should be mentioned that, for example, an Ethernet LAN may be used with end systems running OSI protocols. A link to ACCUNET and WANGPAC provides the interconnectivity with the rest of OSINET.

The implementation of a long haul interconnected (gateway - gateway) working version of an ISO OSI network does not currently exist today (Intermediate System to Intermediate System (IS-IS) standard is scheduled to be released by ISO in 1988). Unfortunately, since

[5] ACCUNET is a trademark of AT&T.

[6] WANGPAC is a trademark of WANG.

[7] Appendices A and B contain discriptions of these protocols.

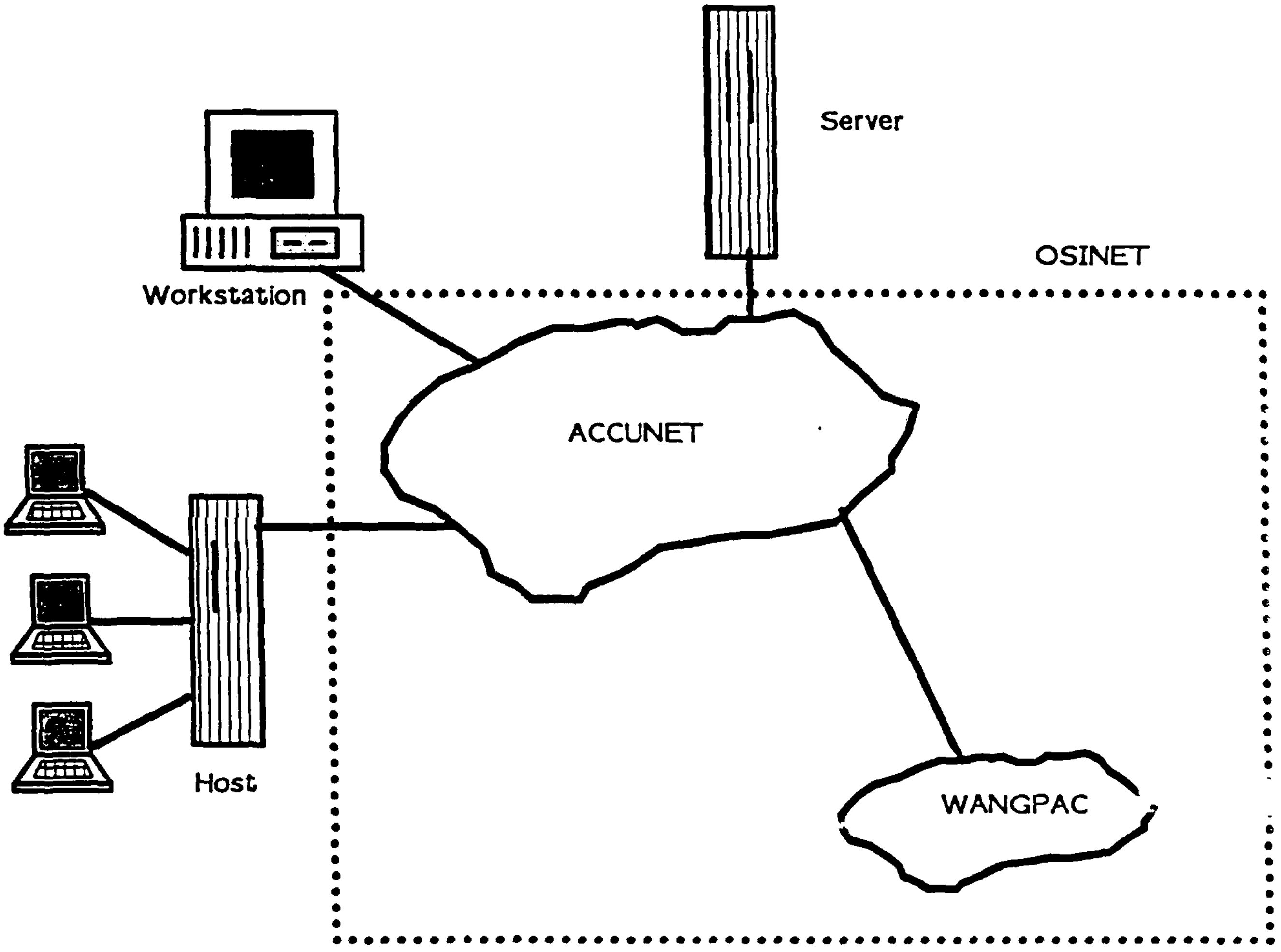

Figure 5. Example of OSINET

there are no internetwork standards available for the ISO OSI communication suite, the demonstration of this capability will be delayed.

2.3.4 University Efforts

The only university effort observed during this study was a group of implementors at the University of Wisconsin at Madison. This effort consisted of ISO OSI communication protocols being developed on an IBM PC/RT[8]. The following ISO OSI communication protocols are being implemented: Session, Connectionless Network, TP4, and X.400. There has been discussion about this group connecting to the OSINET for testing of their implementations for interoperability with other products.

2.3.5 ISO Development Environment

A major obstacle in obtaining experience with OSI protocols is lack of a fully operational OSI network. Although OSINET is operational, it is still evolving and does not support a fully operational OSI network. It is currently possible to gain experience with upper layer OSI protocols (layers 5 - 7) on top of an existing mature network (Figure 6).

The ISO Development Environment (ISODE) [RFC 983] allows OSI application protocols to use the existing services of a TCP/IP base network. The advantages of using a TCP/IP network currently are listed below:

a. Working Intermediate-to-Intermediate (IS-IS) protocol

b. Mature network

[8] IBM PC/RT is a trademark of IBM.

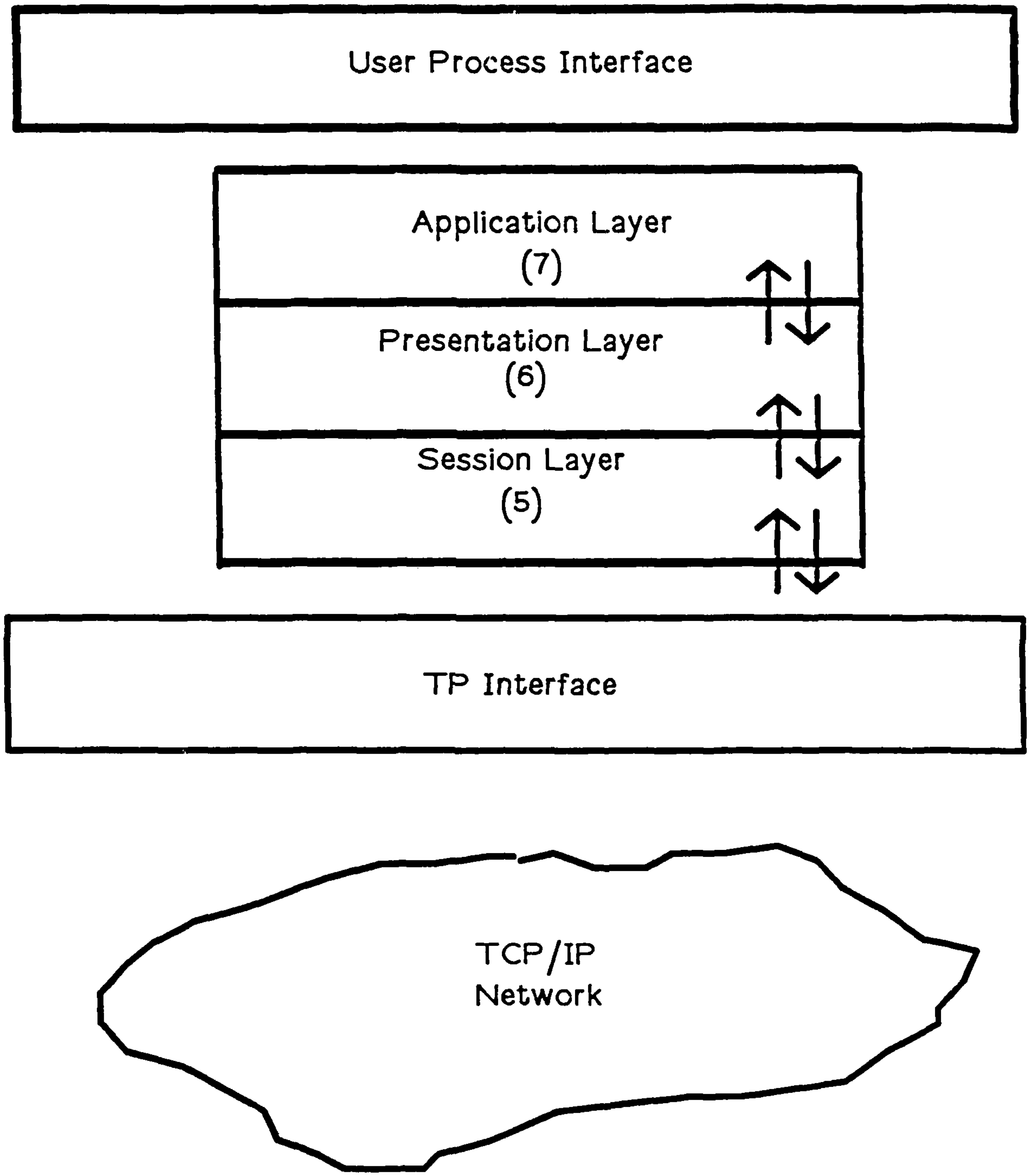

Figure 6. ISODE

c. Over 150 vendor supported versions

d. Large body of expertise

Since a fully operational OSI network may take some time, ISODE can provide a mechanism for developing, testing, and a method of gaining experience with application protocols on a fully operational network.

3. ANALYSIS OF THE OSI NETWORK ARCHITECTURE

This section discusses some of the more subtle but important aspects of the OSI Network Architecture. The analysis requires knowledge of the OSI model which is described in further detail in Appendix A.

It is important to realize that ISO did not intend the OSI Network Architecture as the solution to *all* network problems. Instead, it attempted to define a set of standard protocols by which computer systems could communicate in a manner hopefully superior to what the current standard methods allow. Issues related to the OSI Architecture itself as well as to implementation efforts and concerns are examined with the goal of presenting the reader with a picture of what the status of OSI is today.

3.1 APPLICABILITY OF THE OSI ARCHITECTURE TO REAL SYSTEMS

In order to be implementation independent, the ISO definitions for OSI are stated at an abstract level. These abstract definitions can be ambiguous. ISO defines how computer systems should communicate with each other via OSI and real systems that use OSI are referred to as open systems. Real systems are defined by ISO to be:

> A set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer. [CCITT X.200-X.250]

OSI is not concerned with the internal functioning of each individual real open system, only the exchange of information between open systems. In other words, OSI is concerned only with the interconnection of systems:

> All other aspects of the systems which are not related with interconnection are outside the scope of OSI. [CCITT X.200-X.250]

For example, a VAX[9] cluster of three machines would be considered an autonomous whole in that the way VAXs communicated with each other through the cluster controller was of no concern to the OSI standard. Hcwever, if now the cluster were to try to communicate with another system over a network, then the OSI standards would apply. In the same manner, the multiple computer systems on board a jet fighter could use any appropriate means to communicate with each other and the OSI standard would not apply since only when taken together would they be considered an autonomous whole. However, when the fighter communicated with its base, then the OSI standards could be brought to bear since the fighter could be considered a real open system.

3.2 STANDARDS ADOPTED FOR THE OSI LAYERS

The OSI Reference Model states what features each layer will support and the protocols to be used when accessing these features. The reference model does not itself restrict the implementation of these standards, thus allowing vendors the freedom to develop products addressing the needs of user's particular systems. The following sections present some of the currently accepted standards and any restrictions that may apply to them.

The protocols for use in the OSI Network Architecture are set by the ISO OSI standard, thus allowing systems by different vendors to communicate freely with each other regardless of their differences in hardware and operating systems. It is through this standardization that interconnection and interoperability are enhanced.

[9] VAX is a trademark of the Digital Equipment Corp.

3.2.1 The Physical Layer

Among many standards usable for this layer, two classes, IEEE and CCITT, will be discussed. Which of these two should be used depends upon the choice of the Data Link Layer's and the Network Layer's features.

If the IEEE standard [IEEE 802.2] is chosen for the Data Link Layer, then to date, the following three IEEE standards have been adopted by the commercial segment for use in the Physical layer:

a. [IEEE 802.3]. Carrier sense multiple access with collision detection (CSMA/CD), for example, Ethernet and StarLAN.

b. [IEEE 802.4]. Token-passing bus; for example, MAP 802.4.

c. [IEEE 802.5]. Token-passing ring; for example, IBM Token-Ring Network.

If the CCITT X.25 standard is chosen for part of the Network Layer, then the physical layer is composed of:

a. Interim MIL-STD-188-114-A or

b. EIA RS-232D

3.2.2 Data Link Layer

The standards for this layer fall into two groups, depending whether the CCITT X.25 is used or not. If X.25 is present, then layer is the High-Level Data Link Control (HDLC) Link Access Procedure B (LAP B) [HDLCP]. If not, then this layer is composed classes of operation.

3.2.3 Network Layer

The OSI model defines two modes of network operation, connectionless (Internetwork Protocol (IP)) [ISO 8473] and connection-oriented [ISO 8348].

3.2.4 Transport, Session, and Presentation Layers

The OSI Reference Model [ISO 7498] dictates what the capabilities of these layers are. See Appendix A for a more detailed discussion.

3.2.5 Application Layer

Currently, there are three standard applications: the Message Handling System (MHS), File Transfer and Access Management (FTAM), and the Virtual Terminal (VT), the last one still under development. Their capabilities and the manner in which they communicate with the lower layers have been set; however, the manner of human interface is left up to the implementors.

3.3 ROUTING AND PROTOCOL TRANSLATING SYSTEMS

This section presents a discussion of what gateways are, what functions they perform, and where they might be implemented in the OSI Network Architecture.

3.3.1 Introduction

The definition of a Gateway is not a standard, therefore often leading to confusion during discussions. A definition to be used throughout this paper is as follows. Gateways are systems connected to two or more networks to perform routing, relaying, and translating [Schneidewind 83]. A gateway may take many basic forms. One form connects two networks that have different communication media, such as Token Ring and Ethernet. The conversion is done at the first three OSI layers and is transparent to the applications using the networks. This assumes the same types of applications are available on both networks. A second form connects two networks that use different protocols at all levels, especially the upper levels where they deviate the most. These are protocol converters and might not achieve 100 per cent compatibility between the two dissimilar networks.

When the protocol converter runs at the Application Layer and performs translations for specific applications, the converter is known as a Translating Applications Gateway (see Section 4).

An End System is the ultimate source and/or destination of user-oriented data in a network while an Intermediate System is responsible for the proper relaying and routing of data. An Intermediate system might connect two dissimilar networks and must perform the functions of a gateway in routing messages across the boundary between the two networks.

3.3.2 End System to Intermediate System (ES-IS)

The ES-IS protocol is well defined although not yet a standard, existing as an ISO Working Paper. It is used in passing data from an End System to an Intermediate System for routing and relaying. This may also be used by an Intermediate System to deliver data to the target End System. In the process of performing routing and relaying, the IS may perform the translating functions of a gateway.

3.3.3 Intermediate System to Intermediate System (IS-IS)

The IS-IS protocol, used by ISs to communicate routing and relaying information among themselves without the needed intervention of End Systems, is still evolving in ISO without any standards yet released.

4. ANALYSIS OF GOSIP

The Government Open Systems Interconnection Profile Specification [GOSIP 87] sets forth the requirements for ADP equipment concerning their networking capabilities, and therefore, their ability to interconnect. This section presents an analysis of the state of the OSI Network Architecture in regards to GOSIP and how that state could affect the planned transition to the OSI protocols. The immediate needs of the OSI Architecture in order for it to be used in pursuit of the GOSIP goal are first examined, followed by a look at significant issues to be faced during the transition

A detailed overview of GOSIP is presented in Appendix B for the readers who need a review of its scope and applicability.

4.1 IMMEDIATE NEEDS FOR IMPLEMENTING GOSIP

The OSI Network Architecture is still evolving and all the necessary ISO Standards and CCITT Recommendations are not yet in place. An effort is underway at the NBS/OSI Implementors Workshop to produce standards that commercial vendors can agree to and produce products that conform to them. There are several distinct components of the OSI Architecture that are needed in order for the GOSIP transition to succeed fully and satisfactorily.

4.1.1 Gateways

No standards exist for an Intermediate to Intermediate Systems communication protocol (IS-IS), although the protocol for End Systems to Intermediate Systems (ES-IS) has been well developed by the NBS/OSI Implementors Workshops and exists as an ISO Draft Proposal (DP) [ISO DP 9542].

Translating Applications Gateways[10] (Figure 7) will be used to convert one application protocol to another. This will be done at the messaging level; in other words, the Translating Gateways will convert the TCP/IP Simple Mail Transfer Protocol (SMTP) to the OSI Message Handling System (MHS) [RFC 983] for use in OSI networks and the OSI File Transfer, Access, and Management (FTAM) application will be translated to the TCP/IP File Transfer Protocol (FTP). These Translating Gateways will, of course, work in both directions between TCP/IP and TP4/IP.

4.1.2 Virtual Terminals

There is a need for remote terminal log-in capability for the ISO Virtual Terminal Protocol (VTP). This may be implemented by the TELNET mode of the VTP. These standards are still evolving in the NBS/OSI Workshops.

4.1.3 Directory Services

Directories will be used in an on-line manner to provide humans with rapid and easy retrieval of information useful for determining what network services are available and how to address their correspondents.

In another instance, the Directory Services will be used as a service by computer applications without direct human interaction. One important service is to provide Presentation Address (PSAP) translation for named objects, on behalf of network management. At present, no Directory Services standards exist.

[10] Translating Application Gateways are the product of NBS for use during the transition from the TCP/IP protocols to the OSI protocols mandated by GOSIP.

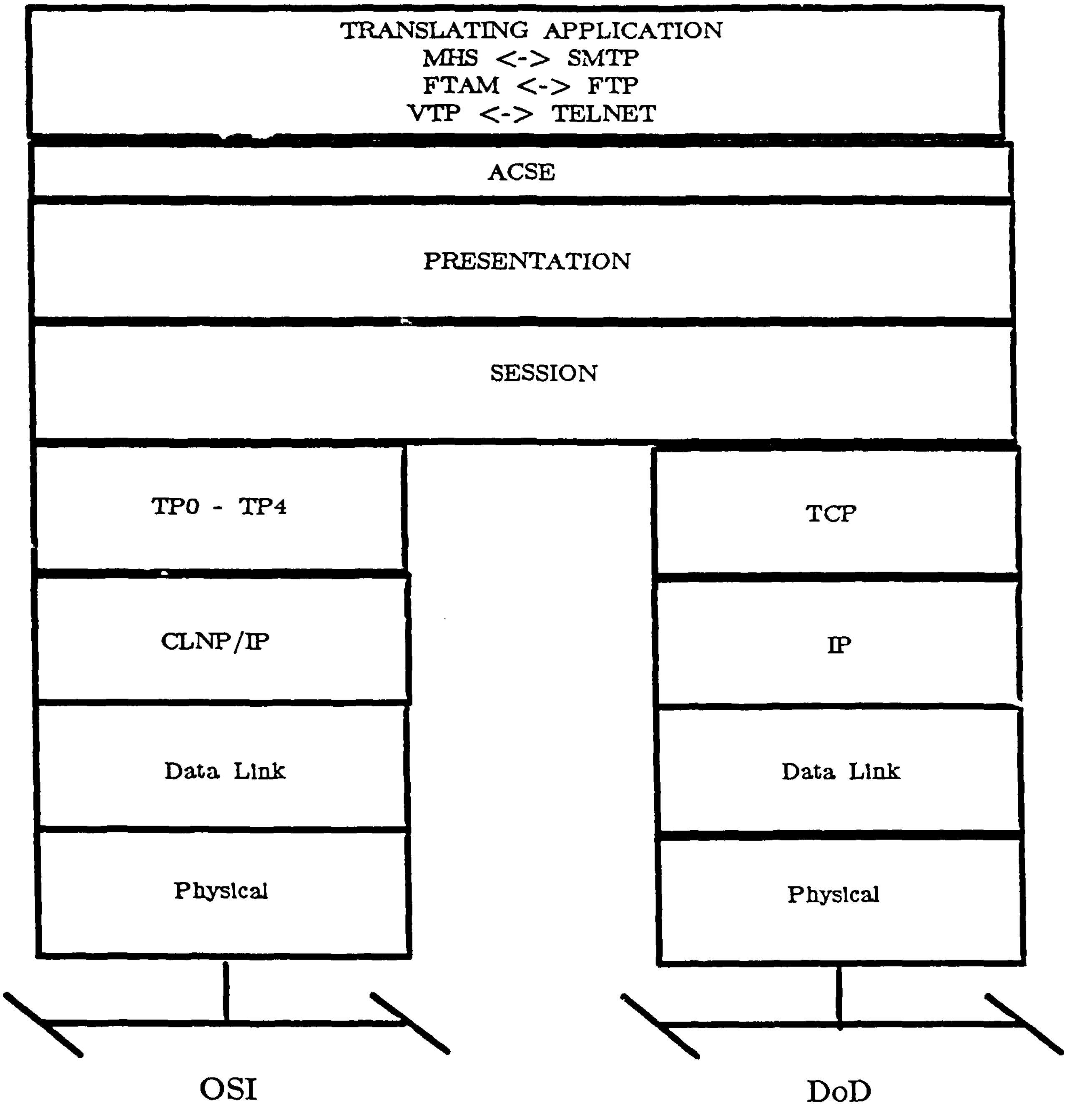

Figure 7. Translating Gateway

4.1.4 Network Management

Network Management is concerned with the management of network resources with the goal to plan, control, and account for interconnection services. It is also concerned with providing facilities to ensure predictable communication, protect information, and to respond to changing requirements. At present, the network management protocols are evolving due to the efforts of the participants of the NBS/OSI Workshops.

4.2 SIGNIFICANT ISSUES RAISED BY GOSIP

A discussion follows presenting an overview of the significant issues raised due to the planned transition to OSI protocols as mandated by GOSIP. These issues revolve around the aspects of the GOSIP document where it is vague as to the method needed to achieve the desired goal, and the important points that someone (such as an Acquisition Authority) using GOSIP to procure a computer system must address. A detailed analysis of these and other issues is presented in Chapter 5.

4.2.1 Implementation Considerations

The reader should keep in mind that the GOSIP protocol implementation agreements and basic capabilities are the result of a collaboration between the National Bureau of Standards (NBS) and the commercial vendor community. Therefore, the GOSIP document concentrates upon what is or will soon be commercially available. This may affect special DoD applications (i.e., mission critical [DoD 3405]) where commercial products cannot be directly used. This is significant since no known vendor is presently using Ada to implement OSI protocols. Therefore, the system would require an Ada implementation of the OSI protocols or a waiver to use an existing non-Ada version.

To reduce software development time and costs, the DoD has been actively pursuing methods to develop reuseable software through the Software Technology for Adaptable and Reliable Systems (STARS) program and the Software Engineering Institute (SEI). That is, if a number of systems are going to require the use of ISO OSI protocols, then designing systems from a library of reuseable ISO OSI components would be advantageous.

It is important to note that the DoD is in a position to force their contractors to utilize software components that they have procured in the past from different or the same contractors. From a practical point of view, starting a large system with an existing foundation of tools is much better than starting from scratch.

GOSIP provides for the possibility that the OSI protocols are not sufficient for all applications and describes the waiver criteria and mechanism.

4.2.2 Conformance

The GOSIP specification states that OSI implementations must meet the standards as stated in the GOSIP document and that conformance testing will be used to do this. However, there are no companies or agencies yet certified to generate the test suites.

4.2.3 Enhancements

The GOSIP document encourages "enhancements" to the standards it stipulates. Enhancements can take the form of additional functionality at the different layers, greater selection of Physical Layers, and/or a greater variety of applications. Since the basic functions needed for interoperability are specified by GOSIP, if two systems wishing to interoperate do not share the same enhancements, they can fall back to the fundamental functions. If this is not sufficient for the intended use then the two systems cannot interoperate. This danger is more obvious at the application and physical layer where the user knows or can easily find out if the same version of the application is in use on both End Systems or if two physical media standards are compatible. What enhancements might be present on any particular system would only be known by the system manager.

Additional functions and services at the layer level would cause a reversion to the fundamental functions in the event ihat one of the systems did not support the enhancements. Applications designed to exploit these enhancements might then not operate as desired.

4.2.4 Layer Access Requirements

The capability for user access to each OSI layer's protocol through Service Access Points (SAPs) can be specified by the Acquisition Authority. Then access points may be used as "hooks" for future enhancements. Participant vendors of the NBS/OSI Implementors Workshop recommend the use of the layer pass-through mode instead of direct access to SAPs.

4.2.5 Security

Security capability is not currently implemented; however, the GOSIP document discusses data fields in the protocols for use by security implementations. If these security options are desired, then they must be specified during the procurement phase. A Special Interest Group at the NBS Implementors Workshop for OSI is currently working on implementation guidelines.

4.2.6 Data Integrity

The integrity of received data is determined via the use of checksums. GOSIP requires that checksums be implemented but that they may be turned on (used) or not turned on for source End Systems at the discretion of the End System manager.

Checksums have been used in DoD networks for data integrity and the algorithms used have been optimized for performance. The OSI algorithm for computing checksums is computationally more demanding than the DoD checksum. The performance penalty may be too great a cost for some OSI implementations. The use or non-use of checksums can become a fundamental interoperability issue when mixing the systems.

4.2.7 Performance Measurement

There is no standard method suggested to evaluate the performance of existing systems, much less methods to assess the performance of systems utilizing the OSI protocols. The GOSIP specification states:

> The principal thrust of OSI is to provide interworking of distributed applications using heterogeneous, multi-vendor systems. Modern implementations of OSI products may perform adequately for most government applications. Or they may not. GOSIP does not cite performance criteria. [GOSIP 87]

It is up to the Acquisition Authority to stipulate any performance issues at the time the equipment is requested. This area is being addressed by a Special Interest Group for Performance at the NBS/OSI Implementors Workshop. GOSIP provides for the possibility that OSI protocols will not properly work in certain circumstances and recommends that a waiver should be sought in these situations.

4.2.8 Time Out Values

Time out values are used to control the amount of time a piece of data will be allowed to exist on the network as it travels from node to node, in addition to other goals. Time out values help reduce congestion by preventing processes from waiting indefinitely for some event to occur. Suggested values are given by CCITT and the GOSIP document. The most difficult values are the ones involved with Time to Live and message retransmission since the size and topology of the network have a great impact on the magnitude of these times. Care must be taken by the system manager when choosing these values. However, the GOSIP document mandates some formulas for computing these values in order to produce a standard.

4.2.9 Addressing

Addressing encompasses many areas of the OSI network. Several of particular importance are discussed below.

The assignment of addresses to systems, applications, and Network Service Access Points (NSAPs) is the responsibility of certain Address Registration Authorities. NBS lists those authorities to be considered and these authorities ensure that duplicate addresses are not assigned. When procuring systems the Acquisition Authority must consider this assignment of addresses and how those assigned addresses may be set on the particular implementation of the OSI layers.

There is a slight difference in the way in which source routing is specified between the DoD and OSI models. This difference raises some concerns in the operation of OSI networks.

Source routing is where the sender of data specifies the gateways that the packet must pass through. Normally, however, the gateways determine the path a packet will traverse to its destination. There are occasions, though, when an explicit, source routed, path is warranted:

a. A specified path for a datagram to traverse in which the current gateways would not route. Some paths across networks are not listed (known to the gateway) due to security or lack of routing information at the gateway.

b. Multiple paths between many originator/destination pairs sometimes need explicit path selection due to factors such as cost, traffic congestion, and administrative reasons.

c. A specified path for testing network connectivity is a primary use of source routing at present.

Source routing as specified within the DoD IP specification [MIL-STD-1777] is an option. The OSI IP [ISO 8473] also defines source routing as an option. However, the method used in the DoD IP is more robust in that all gateways need not implement source routing for this service to operate. For source routing to correctly operate with the OSI IP *all* gateways must use the option or reliable source routing will not occur.

The current OSI Implementation Agreements [NBS 87] state that source routing "will not" be implemented and, therefore, it is unlikely that all gateway vendors will actually support it.

In the DoD IP, an echo packet is available to determine reachability in the network. With the echo packet, source routing is an option when the availability of a particular path to a desired destination must be tested.

ISO IP does not have this feature since connection establishment in the layers above the Network Layer will return a confirmation if the destination system is reachable. This ISO technique will not work if the destination system is not known to any of the routing gateways and therefore, source routing must be used instead. However, as indicated above, since source routing is not a mandated feature, this may not always be possible.

It is not clear how the lack of source routing will affect the development and maintenance of OSI networks. Problems with testing certainly seem to be an area that may show up initially.

The addresses of higher level service access points (Session, Presentation, and Application) are recommended by the GOSIP document. These recommendations must be considered when procuring network systems, if conformance is desired.

The Acquisition Authority must be very familiar with the capability and needs of the computer system upon which network services are to be implemented. As the preceding sections show, there are many fine details that have choices associated with them.

4.2.10 Requirements of X.25 Protocols

The Acquisition Authority should note that GOSIP states the Connectionless Network Service (CLNS) must be provided with interfaces to the 1984 CCITT Recommendation of X.25, if X.25 is to be used Care must be taken when mixing X.25 and the OSI model to ensure compatibility with the standards. GOSIP references only the 1984 version of X.25 since the 1980 version lacks some features needed by the OSI protocols.

4.2.11 Upgrading of Existing Equipment

No requirements are stated in the GOSIP document for the upgrading of existing equipment to the OSI standard. This means that present End and Intermediate Systems may and probably will remain with their current network protocol until they must be replaced by new computer systems. After the two-year co-standard period, only OSI-compatible equipment will be procured. How can a node on a proprietary network be upgraded to a newer computer system when the new system will be incompatible with the rest of the network? Two possible solutions are a protocol translating gateway or a Translating Applications Gateway, to allow the new machine to interconnect with the rest of the network.

This process could continue with the eventual replacement of all old, non-OSI equipment with the GOSIP-mandated systems. At that time the entire network would convert to OSI protocols. However, there is no guarantee that old equipment will be replaced.

This upgrading process must be studied in greater detail since the conversion of an existing network with many nodes to an OSI only network could be a lengthy and expensive process.

4.2.12 Commercial Products

The GOSIP specification requires that Automated Data Processing (ADP) equipment must support the OSI protocols. However, there are no commercial products available at this time that implement the entire suite of OSI protocols plus the FTAM, MHS, and Virtual Terminal applications.

Add-in network products do exist for the IBM PC/AT compatible line of microcomputers that implement the bottom two layers according to the GOSIP standard [IEEE 802.2; IEEE 802.3; IEEE 802.4; or IEEE 802.5]. The upward layers are still vendor specific.

5. ISSUES AFFECTING THE TRANSITION

This section presents observations made regarding the OSI Network Architecture and the transition to OSI from DoD systems. Analysis is provided on the implications of some of the requirements of the GOSIP document although comprehensive coverage could not be provided due to the limited timetable.

A report on the transition strategy to be used by the DoD is in the process of being prepared by the DCA. This IDA paper is a totally independent report.

5.1 CRITERIA FOR SYSTEM INTEROPERABILITY

The ability for computer systems to work together to achieve a common goal is one way to interpret interoperability. GOSIP is an attempt to establish the foundation upon which interoperability will grow. This section analyses GOSIP's applicability, the reason for interoperation, and some of the expected costs.

5.1.1 What GOSIP Applies To

GOSIP is to be used by Federal government agencies when acquiring computer network products and services that provide equivalent functionality to the OSI protocols as defined in the GOSIP document [GOSIP 87]. If the computer system has special requirements that preclude OSI protocols or has no need ever to interoperate with other open systems, then a waiver can be obtained according to the process outlined in the GOSIP document.

5.1.2 Motivation for Interoperability

The primary goal of interoperability is to enable heterogeneous systems to interconnect and interoperate through the use of a standardized network facility. This standardization should reduce the costs of computer network systems by encouraging vendors to provide alternate sources for OSI communication products. This will have the likely effect of reducing the number of vendor specific and propriety network systems.

The use of standardized OSI applications will allow personnel to move easily from one system to another. The human interface might differ, but this would be due to implementation goals of the vendor. If standardized human interfaces are desirable, then the Aqcuisition Authority should communicate this to the vendors involved.

5.1.3 Costs of Achieving Interoperability

There are various kinds of costs associated with transitioning to the OSI network architecture. They include performance of the protocols, necessary machine capacity to implement them, limited availability of OSI applications, and dealing with a sizable present investment in proprietary protocol based communication equipment.

5.1.3.1 Performance Related Costs

Interoperation for a wide variety of applications operating in a diverse collection of computer systems requires a very powerful and comprehensive mechanism for communication between peer-protocol entities. OSI provides this capability in a manner that is transparent at the Application Layer. A layer attempting to form a connection will establish communication with the same layer in the destination machine and "negotiate" a protocol to use when performing all further communication. The manner that the two peer-layers pass information back and forth to perform this negotiation is the protocol process. This peer-layer negotiation can occur for virtually all layers. This provides an automatic adjustment mechanism whereby the more sophisticated systems (possessing a greater array of protocols) can be negotiated downwards (towards a simpler protocol) to a point that a common data exchange method can be agreed upon. The success of this negotiation depends primarily upon two points. Both systems must have a common protocol to negotiate down to and the application processes must have allowed the negotiation.

This could place an intolerable amount of overhead into the communication process for some small special-purpose LANs. Such a special purpose LAN might be used in a process control environment where real-time response is necessary and the ability to connect to systems on other LANs is not required OSI can require large message sizes with multiple headers plus complicated, and in small systems, perhaps unnecessary acknowledgement procedures. In addition, the amount of software needed to implement the OSI suite could be prohibitive on small machines. This would affect the overall performance of the network and possibly degrade it to undesirable levels.

The layered approach and the possibility of access to lower layer SAPs suggests that special applications could be used that simply bypass the upper layers to achieve the needed performance. Another possibility is that the upper layers use protocol options that cause the intermediate layers to be set to a flow-through mode whereby information is passed on to lower layers without interpretation. This effectively removes the undesired intermediate layers in a more standard manner as recommended by participants of the NBS/OSI Implementors Workshop. These techniques could be used and the result may then have the needed performance. However, if a large portion of the OSI layered system must be bypassed and special applications required in order to achieve the desired goal, then it is necessary to reassess the original decision to use the OSI protocols. Perhaps the OSI protocols must be used for the sake of standardization or in the light of other requirements.

5.1.3.2 Availability of OSI Applications

Presently, there are two applications discussed in the GOSIP document and these are the extent of applications currently available. They are File Transfer, Access, and Management (FTAM) plus the 1984 Message Handling System (MHS) [CCITT X.400-X.430]. A Virtual Terminal Protocol (VTP) is being developed for possible future inclusion in GOSIP. There is a new 1988 version of the MHS [CCITT X.400-X.430] currently under development by participant vendors of the NBS/OSI implementors Workshop. However, there is some concern surrounding its compatibility with the 1984 version of the MHS.

If some other application is needed, then either vendors must be trusted to bring it to the market place or the application must be specially developed. However, one of the benefits of a widespread standard is that it encourages vendors to create competitive products that will be compatible. This has been observed many times in the past in both the hardware field (e.g., VT100 standard) and the software area (e.g., the MS-DOS[11] operating system).

5.1.3.3 Present Investment in Alternate Protocols

Another cost is that of transitioning to the GOSIP-mandated standards when there exists a sizable present investment in alternate protocol network services. The problems are not unlike those encountered whenever a move to a new product line in made. Before the move is started, however, careful thought must be given to the benefits to be gained. This comment assumes that there is a choice about the conversion process.

[11] MS-DOS is a trademark of Microsoft Corp.

5.1.4 Security

The GOSIP standard does discuss security and some of the data fields and code values that will be used. These reflect the DoD mandatory access classifications of Unclassified, Confidential, Secret, and Top Secret. These code fields appear in the Internetwork headers and are used to control routing of classified and unclassified user data. An Extended Security Option exists which allows additional security-related data to appear in the OSI IP header. These security options must be specified by the Acquisition Authority if desired. No statement is made in the GOSIP document concerning what the contents of a classified user data unit should look like, other than at the OSI IP header level. There is a general suggestion that user accessible service points to the lower layers might be used in the security process. However, the present state of security is still evolving with the NBS/OSI Implementors Workshop's Security SIG very much aware of the need for security and working to establish a comprehensive plan for it within OSI implementations. This SIG's work is especially important since the Implementation Agreements [NBS 87] specify that the Security parameter *will not* be used. Further, should an OSI implementation receive a PDU containing the Security parameter, the PDU should be ***discarded.*** Whether the resulting work of the Security SIG addresses the special needs of the DoD will not be immediately known.

5.2 WHAT THE ACQUISITION AUTHORITY MUST CONSIDER

The OSI protocols have a great variety of options and those desired must be known before the transition to OSI can be completed. This section collects together many of the issues facing the Acquisition Authority during the transition period. Some of these issues were briefly discussed in Section 4.3 and are brought up again in this section for further analysis. The analysis presented here covers some of the less obvious points of the OSI Architecture and GOSIP. It is strongly indicated by the analysis that the Acquisition Authority must be fully familiarized with the OSI Architecture before attempting to procure network components or services of the OSI protocols.

5.2.1 Introduction

It is the responsibility of the Acquisition Authority to evaluate the needs of its realm of computer systems and their need to interoperate. GOSIP lays a foundation for those features of the OSI standards needed for basic interconnection and interoperation. Features in addition to these may be, and perhaps should be, specified to add additional functionality for present and future applications.

5.2.2 Applications and Their Requirements

Applications are the ultimate source and destination of user data in a network environment. Therefore, networks exist to support the applications and their requirements whether these applications are being operated manually or are operating in an unattended ADP environment. The capabilities of the network are dictated by the needs of the applications. In the same manner, the OSI layers and the functions these layers must support are dictated by the functionality of the applications to be used.

End Systems support applications which source or sink user oriented data. All seven OSI layers are required to support general applications. The one present exception to this rule is the 1984 Message Handling System [CCITT X.400-X.430] which includes the Presentation and Application Layers such that it communicates directly with the Session Layer. The functions and services the layers must support are also dictated by the applications intended to be utilized. The Acquisition Authority must carefully ascertain the present and future needs of the applications desired.

This applies to both presently available applications and future. With a standard protocol defined at the Application Layer, vendors are encouraged to work towards new products/applications that might require protocols not currently included. The cost and difficulty of adding protocols at a later time after the initial procurement must be considered by the Acquisition Authority. Those systems which will be used for development of new applications must be procured with an eye towards the addition of protocols not needed originally. The ability to incrementally add protocols to layers would then be a desirable feature.

5.2.3 Source of Conformance Test Requirements

Conformance is shown by the vendor when the product successfully implements the functional units specified in the GOSIP document. The Acquisition Authority must supply documentation which identifies specific testing requirements on the protocols required in a network system.

Conformance tests and test systems are currently being developed. When these are complete, the National Bureau of Standards will specify the test, test systems and testing organizations certified by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform the conformance testing of the GOSIP protocols. At the present time, the Corporation for Open Systems (COS) is attempting to become one of these accredited organizations.

The Acquisition Authority will determine which of the test systems and test cases are required for certification of the target system and set the minimum acceptable test results for the purposes of procuring the network system.

5.2.4 Performance Requirements

It is up to the Acquisition Authority to specify any and all performance requirements when procuring computer network systems or services. GOSIP itself does not stipulate any standards for performance.

Checksums have been used in DoD networks to greatly increase data integrity and the algorithms used have been optimized for performance. The OSI algorithm for computing checksums is far more complex thus making a larger demand upon the computational resources in the systems. The performance penalty may be too great a cost for some OSI implementations. The use or non-use of checksums can become a fundamental interoperability issue when mixing the systems.

5.2.5 Desired Vendor Provided Enhancements

Enhancements can take the form of additional functionality at the different layers, greater selection of Physical Layers, and a greater variety of applications. Since the basic functions needed for interoperability are specified by GOSIP, if two systems wishing to interoperate do not share the same enhancements, they can fall back to the fundamental functions. If this is not sufficient for the intended use then the two systems cannot interoperate. This danger is particularly obvious at the application level and the physical layer. Additional functions and services at any layer would cause a reversion to the fundamental functions in the event that one of the systems did not support the enhancements. Applications designed to exploit these enhancements might then not operate as desired.

The support of additional protocols added to the layers might be desirable at some future time. The classes TP0 and TP4 are the two transport types discussed by GOSIP; however, it might become useful to support the other intermediate types, TP1-TP3. The addition of a connectionless transport protocol [ISO 8072/DAD1; ISO 8602] might be used in the future to support a datagram service at the Transport Layer. The Acquisition Authority has the responsibility to specify these additional protocols and their features.

5.2.6 User-Accessible Layer Interfaces

The Acquisition Authority must specify the desired characteristics of user-accessible interfaces at the appropriate layers. These requirements would then be included in the conformance tests. If these service interface access profiles are not specified, a vendor could provide no interface and still be conformant. The stated characteristics should concentrate on the desired features rather than implementation specifics unless they are of particular importance to the access interface. Such user-accessible interfaces might be used by new application programs (user developed) as a language interface.

5.3 METHODOLOGY FOR ANALYSIS OF SYSTEMS

The application of OSI protocols in any network is not a trivial matter especially since they may co-exist with other protocols such as TCP/IP. This section examines network topologies and analyzes how the OSI Architecture and its applications (FTAM, MHS, etc.) could be integrated.

5.3.1 The Autonomous Whole

The ISO OSI standards were developed primarily to establish an International Standard for interoperability. Due to the intended audience being the international community and ISO not desiring to mandate computer system or network designs, the wording of the International Standards is sometimes difficult to follow. The applicability of the OSI standard that ISO intended is shown by the wording used to define the use of OSI protocols. The OSI protocols are to be used for communication between open systems. Here the term "open system" refers to those aspects of a real open system that are pertinent to OSI and a real open system is a real system which complies with the OSI standards in its communication with other real systems. Finally, a real system is:

> A set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer. [CCITT X.200-X.250]

This states that the intent of the OSI architecture is for standardized communication protocols between complete systems, not necessarily each computer component contained within the system.

5.3.2 Where Should OSI Be Implemented?

In examining a computer network a question to ask is whether each computer system on the network will need to communicate in an open systems environment with each other and connected networks. If this is the case then OSI protocols probably should be implemented on all. If however, the network as a whole, or a distributed application on the net, needs to communicate with other open systems, perhaps only one node on the network with the ability to use OSI protocols when communicating with other open systems will suffice. There would be no need for each system to support the OSI protocols since this one system, acting as a gateway, would translate from the local protocol to the OSI protocols. This is a compromise measure that allows the network as a whole to communicate but imposes limitations for members of the network. Space and performance constraints might dictate such an approach.

5.3.3 Maturity of Network

The methods used to implement OSI in networks will depend somewhat upon how well developed the network is to start. A new network can be built entirely using the OSI protocols; a small network utilizing TCP or some other protocol can probably be converted to OSI when a new OSI-only machine is added. The most difficult situation is with a large, physically dispersed network. All nodes on a network usually cannot be allowed to be impacted by the addition of one more, even if this new node is OSI. Therefore, a transition method for these particular types of existing networks must be developed. The following subsections address these possibilities in turn.

5.3.3.1 New Implementation

With new network implementations, the Acquisition Authority has many options. The two major considerations are (1) with what other systems will communications have to be conducted and (2) is true interoperability desired now or at any time in the future?

If the OSI protocols as specified in GOSIP will perform the same functions as some other (meaning vendor specific) protocoi, then GOSIP must be used. For a new network this is not a problem in general. If the systems on this net must interconnect with other networks then care must be given to the protocols chosen and the manner the two networks will be connected. If the other net is OSI based, there is no problem. However, if the other net is a TCP/IP-based net, then a gateway will be required.

5.3.3.2 Existing OSI Network

This is the simple case due to the fact that GOSIP-based products must be procured if they provide comparable functionality to the requirements of the new computer system. However, when interconnecting OSI-based networks with different options selected for the layers as well as different types chosen for the layers (e.g., connection-oriented versus connectionless) interoperability problems may arise. The following discussion illustrates this point.

At present the ISO OSI protocol suite provides for both the connection-oriented (CO) and connectionless (CL) protocols at the network level. Internetworking between CO and CL protocoi based networks having possibly different transport classes existing on top of the network layers complicates the construction of gateways.

To solve this probiem would require a Transport Layer Gateway. This is in direct violation of the OSI model. A proposal to interconnect a CL and CO network is being discussed in the ANSI X3S3.3 working group. The proposal calls for a converter, called a COS 265 box [COS 265], based on work done at the Corporation for Open Systems (COS), to be placed between the two networks as shown below:

CL subnetwork <-- COS 265 --> CO subnetwork

For packets going from a CL to CO network, the CL header is stripped off and a channel is opened to the destination on the CO subnetwork. In the opposite direction, a CO connection is accepted at the converter (COS 265), and the data unit is transformed into a CL packet for transmission into the CL subnetwork.

Although a number of other proposals (not mentioned in this report) are being actively discussed, none have been adopted. It may require a Transport Layer Gateway to solve some of interconnect incompatibilities. Gateways of this type, however, tend to be complicated due to the state information that must be maintained for both sides of each subnetwork.

5.3.3.3 Existing Non-OSI Network

This is the most complicated case and probably a common one. An OSI machine directly connected to a TCP-based LAN could communicate with any other OSI machine on the LAN but not to any of the TCP-based machines (Figure 8). The addressing scheme of the LAN hardware itself would keep the two types of systems from interfering with each other, assuming that an OSI host did not try to send to a TCP-based host. This is due to the fact that to the LAN hardware all data packets to be placed on the physical media are treated the same. They are delivered to the destination stated in the header of the packet and no interpretation of the data contained within is performed. Protocols used by OSI and TCP/IP are important only above this level. Therefore, this method would allow the addition of new computer systems to an existing network but would provide no interoperability. In general, this observation is true of networks using protocols other than TCP/IP as well.

If the proper protocol gateway (Figure 9) were to be inserted between the OSI host and the TCP-based network, it would then be possible for all hosts to communicate if compatible applications were present on them. At this time, OSI Applications are not yet implemented for any other network protocol; therefore, the OSI Applications would have to be used on top of the ISO Development Environment (ISODE) or the equivalent. Again, all OSI machines connected this way could communicate with each other and their standard applications (MHS or FTAM) could interoperate. This assumes that the gateway would not lose any of the functionality provided by the protocols and needed by the applications.

The one clear benefit that a protocol gateway might provide is the use of interconnected sub-networks via TCP/IP. Thus, remote OSI based machines could be accessed easily and the

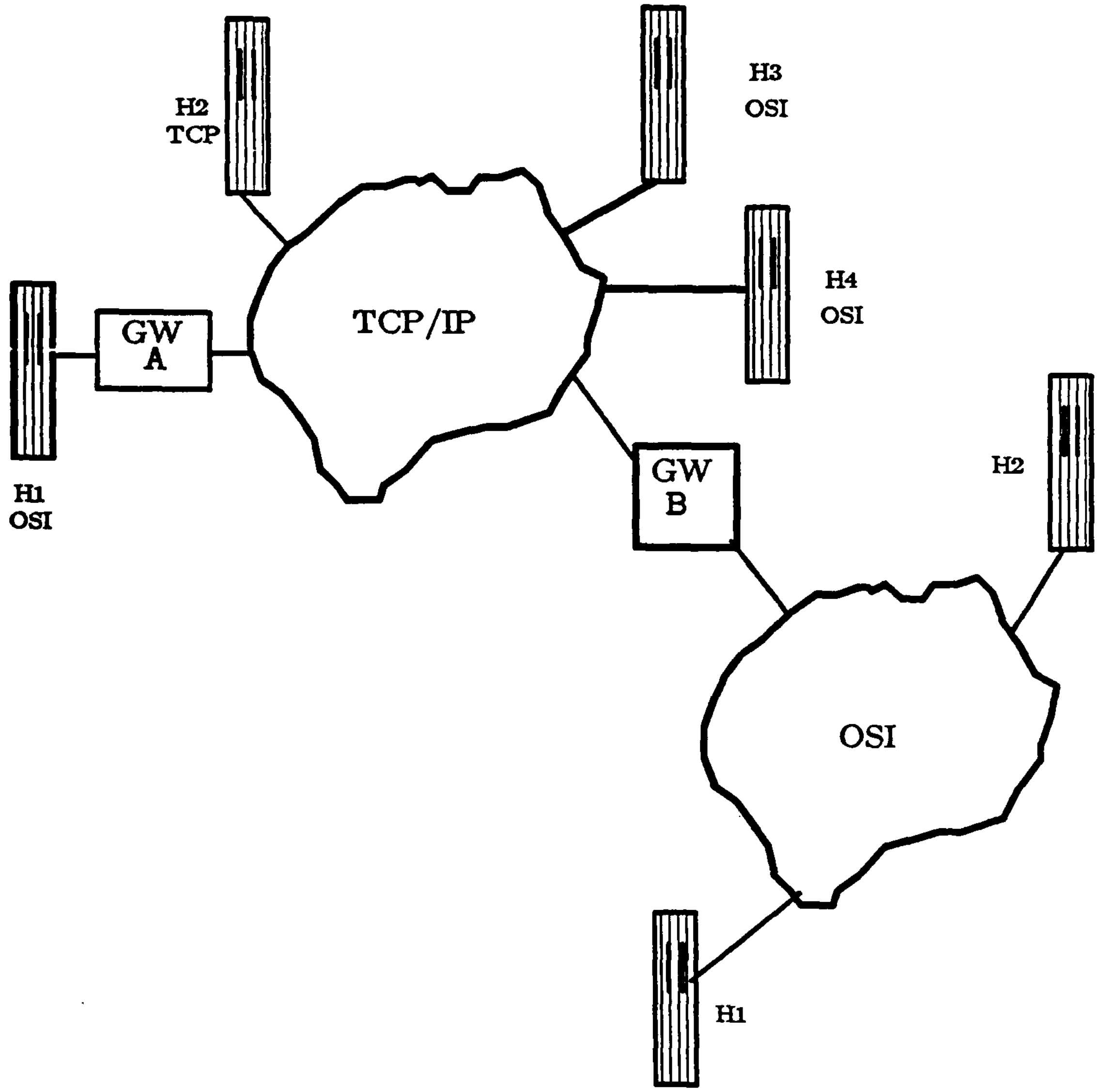

Figure 8. DoD to OSI Networks

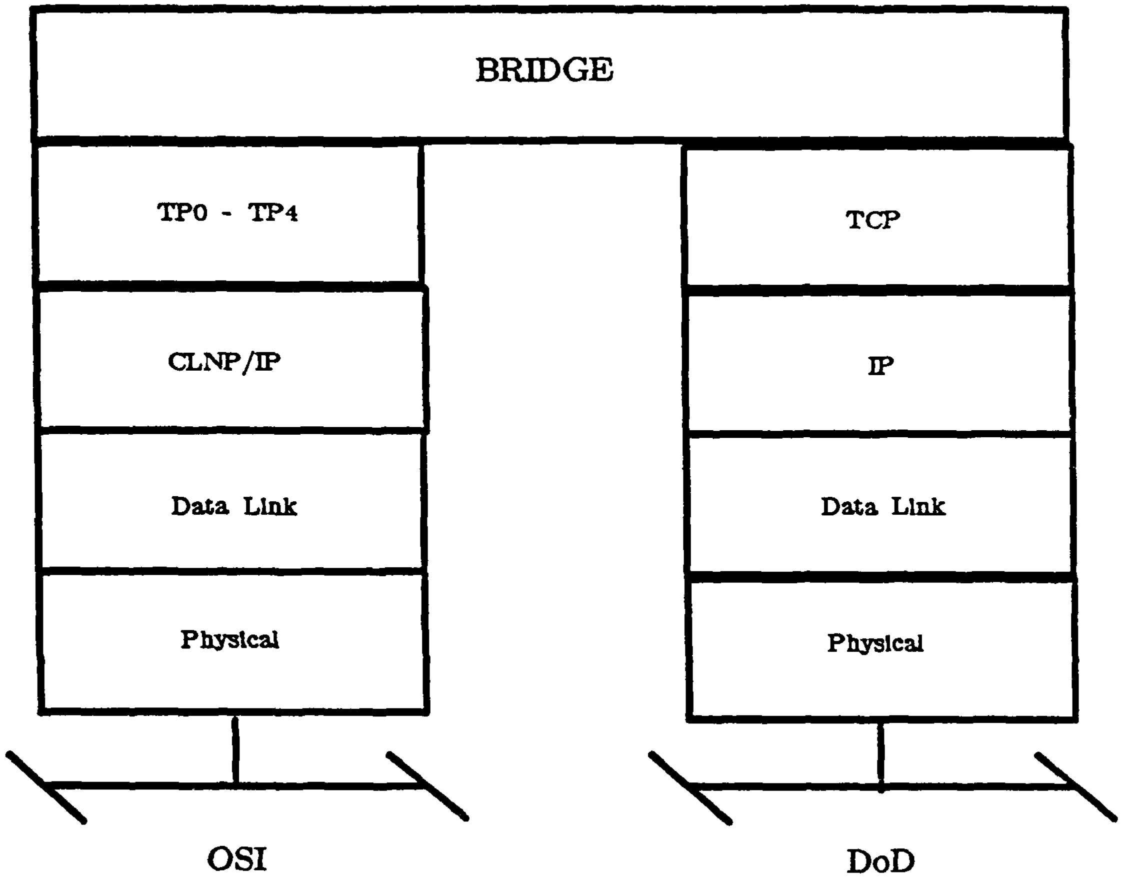

Figure 9. Protocol Gateway

applications interoperate. This still only allows the OSI based systems to interconnect while leaving the TCP systems on their own.

If Translating Application Gateways (Figure 7) were used to convert from the OSI domain to the TCP domain at the application level, then OSI applications could interoperate with TCP applications. In Figure 8, GW A (Gateway A) could be a Translating Application Gateway thus allowing OSI applications (FTAM, MHS, VTP) to interoperate with TCP/IP applications (FTP, SMTP, TELNET). What form GW B might take to allow the two dissimiliar networks to interoperate properly is not clear at this time. This must be further defined.

A heterogeneous network can be seen in the example of three sub-networks, or LANS, connected in the order of OSI, TCP, and then OSI again (Figure 10). If an OSI system needs to interoperate with an application on a TCP-based machine, then the Translating Applications Gateway is needed. However, if a system on one OSI network wished to communicate with an OSI machine on the other, then no translation would be desired. The TCP-based LAN would be used as a communications media for the two OSI machines. The actual manner to manage this interoperability problem must be clarified.

This suggests that both a protocol converter and a translating gateway would be required for maximum interoperability.

5.3.4 Alternate Vendor Software Compatibility

GOSIP is intended to encourage alternate vendors for both hardware and software, among other things. Nowhere does either the ISO OSI specifications or the NBS Implementor's Workshop specify the manner in which the OSI protocols will be actually made a reality in any particular computer system environment. The way that the protocols are implemented will

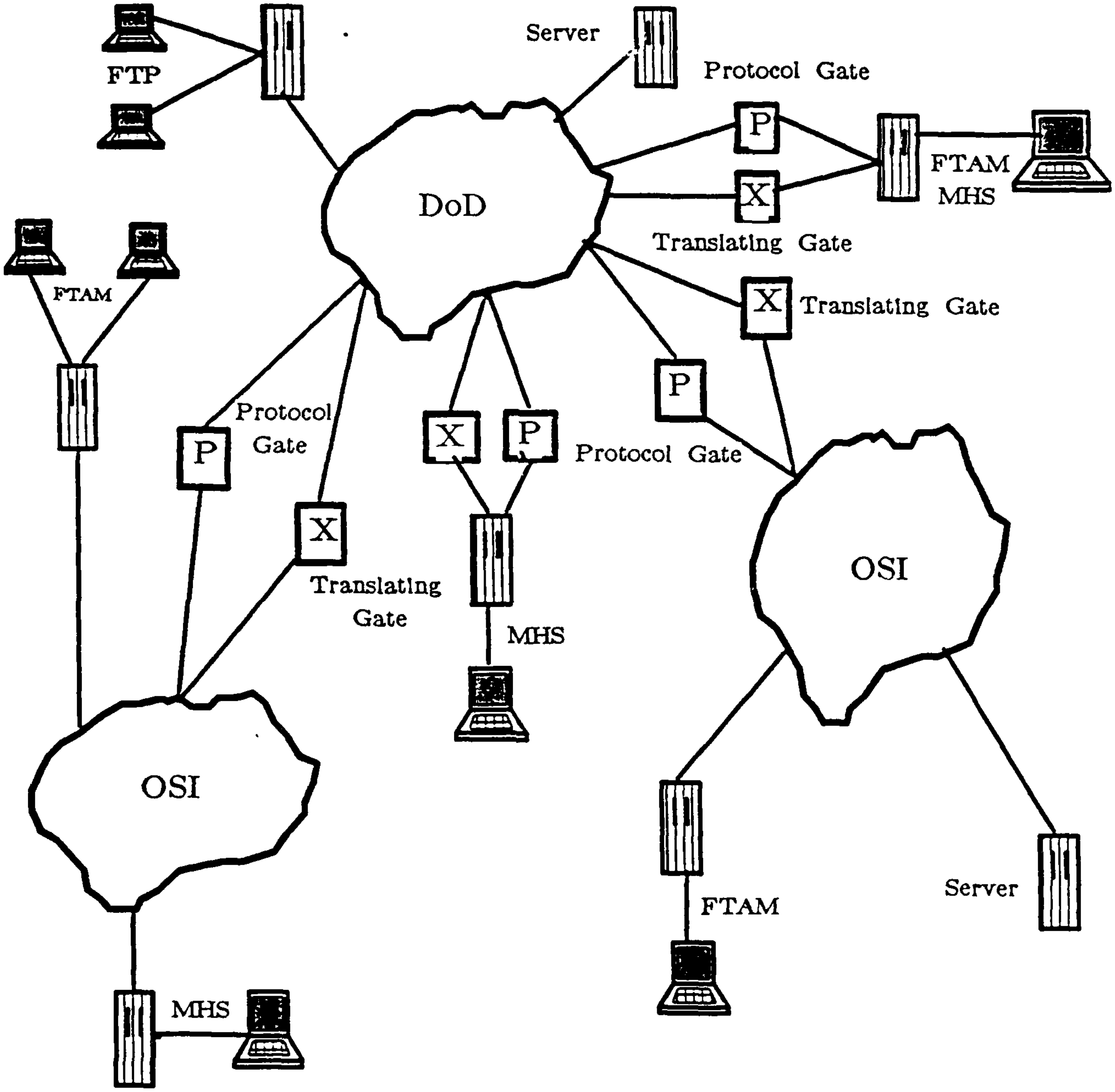

Figure 10. Heterogeneous Network

depend upon the target machine, operating system, and OSI network implementation. Thus, a standard FTAM from one vendor may not work on another machine from a different manufacturer solely due to implementation methods. This is a common problem today with products meant to be utilized on a variety of computer systems. Each system has its own version of the product. The Acquisition Authority must keep these details in mind when procuring products from alternate vendors. An international standard does not guarantee machine independence of software but it does guarantee machine interoperability.

5.3.5 Waivers

In the event that equivalent functionality is not provided by GOSIP either by reason of lack of protocol features or cost or performance, then a waiver should be sought. The GOSIP document is very detailed in the procedure to be used. The head of the agency involved must be the one to issue the waiver.

6. SUMMARY

The motivation for transition to the ISO OSI communication protocols is interoperability, standardized hardware and software, and therefore, lower development time and costs. There is a strong desire by the DoD to obtain interoperability between current and planned military and commercial communication networks. At present, OSI communication protocols are being developed for the commercial sector, which will begin to purchase such systems as soon as mature products become available.

During times of crisis, the military should have the potential capability of using commercial networks. This relieves them from having to build and maintain large capacity networks that will be under-utilized.

NATO has also declared [STANAG 4250] that all member countries will use ISO OSI communication protocols in their communication systems. The ability to use commercially available products that adhere to accepted international standards enables the DoD to benefit from using Commercial-Off-The-Shelf (COTS) hardware and software communication products, which will result in lower development time and costs.

Military communication systems requirements for security, performance, and survivability are difficult to realize under any network architecture. The DoD has met some of these requirements by moving toward a multi-network architecture using Transmission Control Protocol (TCP) for end-to-end services and Internet Protocol (IP) for internetwork connections. The efforts of the ARPANET and other military packet-switch networks (e.g., WWMCCS Intercomputer Network) have obtained impressive results.

However, new demands on network capabilities and capacities will require new technology. Traffic congestion resulting from increased numbers of new users, applications, and Local Area Networks needs to be addressed. There is a need for new applications programs, possibiy requiring network services that were not designed into the current architectures, to be developed.

The Government's Open System Interconnection Profile (GOSIP) [GOSIP 87] provides guidelines and recommendations for federal agencies in the procurement of ISO OSI communication protocols. The document will become a Federal Information Processing Standard (FIPS) by the end of 1987. The DoD, as of 2 July 1987 through a memorandum from the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence, stated that ISO OSI communication protocols can be used as alternatives to DoD protocols. The memorandum explicitly states that the services and agencies must be aware of issues that may impact their communication operations (i.e., interoperability with other systems) by using the OSI protocols. Although it is clear that the DoD will eventually move to the OSI protocols, the transition path is unclear.

Currently, there is a testbed, OSINET, managed by the National Bureau of Standards (NBS) for the development of ISO OSI protocols. This network is used by vendors to demonstrate interoperability of their products. Discussions with vendors has indicated that OSI products are in various stages of development and testing.

It has been recognized that converging to an international communications standard will improve the current interoperability problems experienced in the military and commercial sectors. However, OSI alone is not a solution to all of the current or projected communications problems. The following list is a set of observed problems that are related to the transition to a complete OSI communication network:

a. The development of gateways that provide interoperability between OSI, TCP/IP, proprietary, and mixed OSI/TCP/IP networks must be given a high priority.

b. The transition to OSI protocols will result in a mix of OSI and TCP/IP hosts on a TCP/IP network. How interoperability among these different protocol families will be achieved is not currently clear and must be addressed.

c. Currently, the Acquisition Authorities do not have personnel that are knowledgeable about the DoD and ISO OSI models, protocols, their options, and implementation details in order to procure the appropriate OSI products to fulfill their organizational requirements.

d. At this time there are only two OSI applications available and specified by GOSIP. They are the File Transfer and Access Management (FTAM) and the Message Handling System (MHS).

e. The development state of the network management services is too immature to support any products. From discussions in the Implementation Agreements for Open Systems Interconnection Protocols, it does not appear that products will be available until 1991. This will slow the process of implementing security services into OSI protocols and other application protocols that use the management services.

f. The development of Directory Services products is not expected until 1989. Currently, primitive solutions such as static routing tables are used on hosts. As with network management, protocols relying on sophisticated services provided by the Directory will either be developed with a pseudo-directory service built-in or their introduction may be delayed until Directory Services become available.

g. The OSI protocols were developed with an international community in mind and therefore, had to provide a much greater flexibility than the current DoD implementation. This implies more overhead (i.e., parsing) for many applications of the OSI protocols with the resulting adverse effect on performance.

h. At present, due to the lack of a Draft International Standard for an Intermediate System to Intermediate System (IS-IS) protocol, no long-haul OSI networks exist. Past experience (e.g., ARPANET) has shown that until such a prototype network is implemented, interoperability problems undetected during development may manifest themselves in the implementation.

i. Methods to achieve interoperability between networks using a mixture of connection and connectionless Network Layers need to be implemented and tested. At present, COS 265 is the only proposal that is being reviewed by ISO to address this potential problem.

j. A number of interoperability problems between the 1984 and 1938 X.400 Message Handling Systems (MHSs) must still be resolved. Since vendors have already implemented to the 1984 specification, these MHS versions will be operational when 1988 MHS systems become operational.

A. APPENDIX A - ISO OSI NETWORK ARCHITECTURE

A.1 OVERVIEW OF MODEL

Appendix A presents an overview of the Open Systems Interconnection (OSI) Basic Reference Model [ISO 7498] as defined by the International Standard Organization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT). The CCITT work is contained in their Open Systems Interconnection (OSI) System Description Techniques, recommendations X.200-X.250 [CCITT X.200-X.250].

A.1.1 Introduction

The purpose of the OSI standard is to provide a common ground for the coordination of system development for the purpose of systems interconnection. This standard establishes a set of protocols to be used to communicate or interoperate between systems of dissimilar design. The manner of physical interconnections is via established standards while the protocols discussed are implemented through software techniques.

In order to be implementation independent, the ISO definitions for OSI are stated at an abstract level. These abstract definitions can be ambiguous. ISO defines how computer systems should communicate with each other via OSI. Real systems that use OSI to communicate are referred to as open systems and real systems are defined by ISO as:

> A set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer. [CCITT X.200-X.250]

OSI is not concerned with the internal functioning of each individual real open system, only the exchange of information between open systems. In other words, OSI is concerned only with the interconnection of systems.

> All other aspects of the systems which are not related with interconnection are outside the scope of OSI. [CCITT X.200-X.250]

For example, a VAX cluster of three machines would be considered an autonomous whole in that the way VAXs communicated with each other through the cluster controller was of no concern to the OSI standard. However, if the cluster was to try to communicate with another system over a network, then the OSI standards would apply. In the same manner, the multiple computer systems on board a jet fighter could use any appropriate means to communicate with each other and the OSI standard would not apply since only when taken together would they be considered an autonomous whole. However, when the fighter communicated with its base, then the OSI standards could be involved since the fighter could be considered a real open system.

A.1.2 OSI Model's Structure

The model is organized as seven layers (Figure A-1) with each one containing highly related functions and capabilities. They communicate with each other in a hierarchical manner with an upper layer dealing only with the layer below it and a lower layer with the layer directly above it. Presently, layers are implemented in software with the exception of the bottom most layer which is the physical connection.

Each layer on one system is capable of communicating with its peer-layer, or entity, on another machine by use of the appropriate protocols (Figure A-2). The lower layers and the

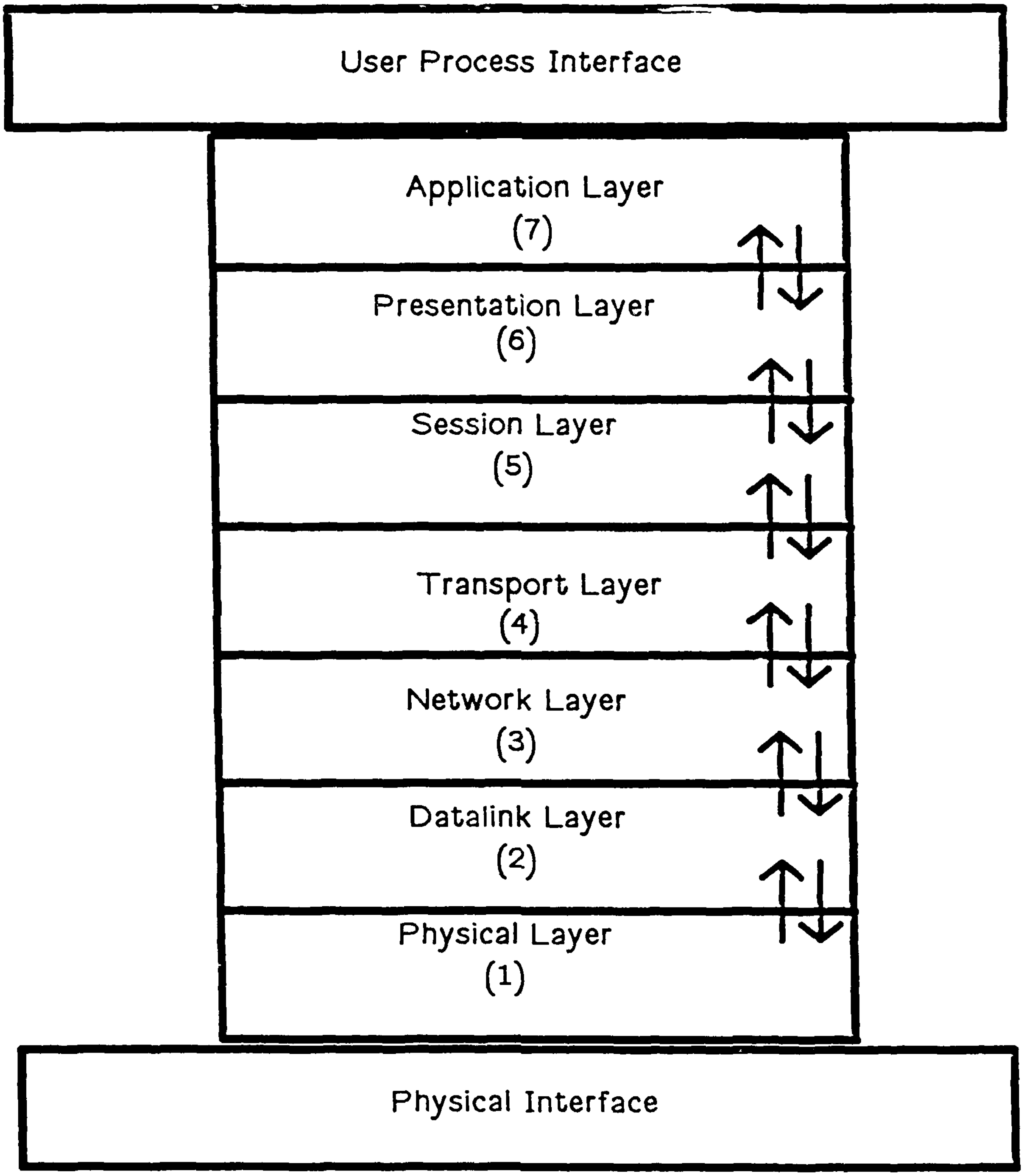

Figure A-1. OSI Reference Model

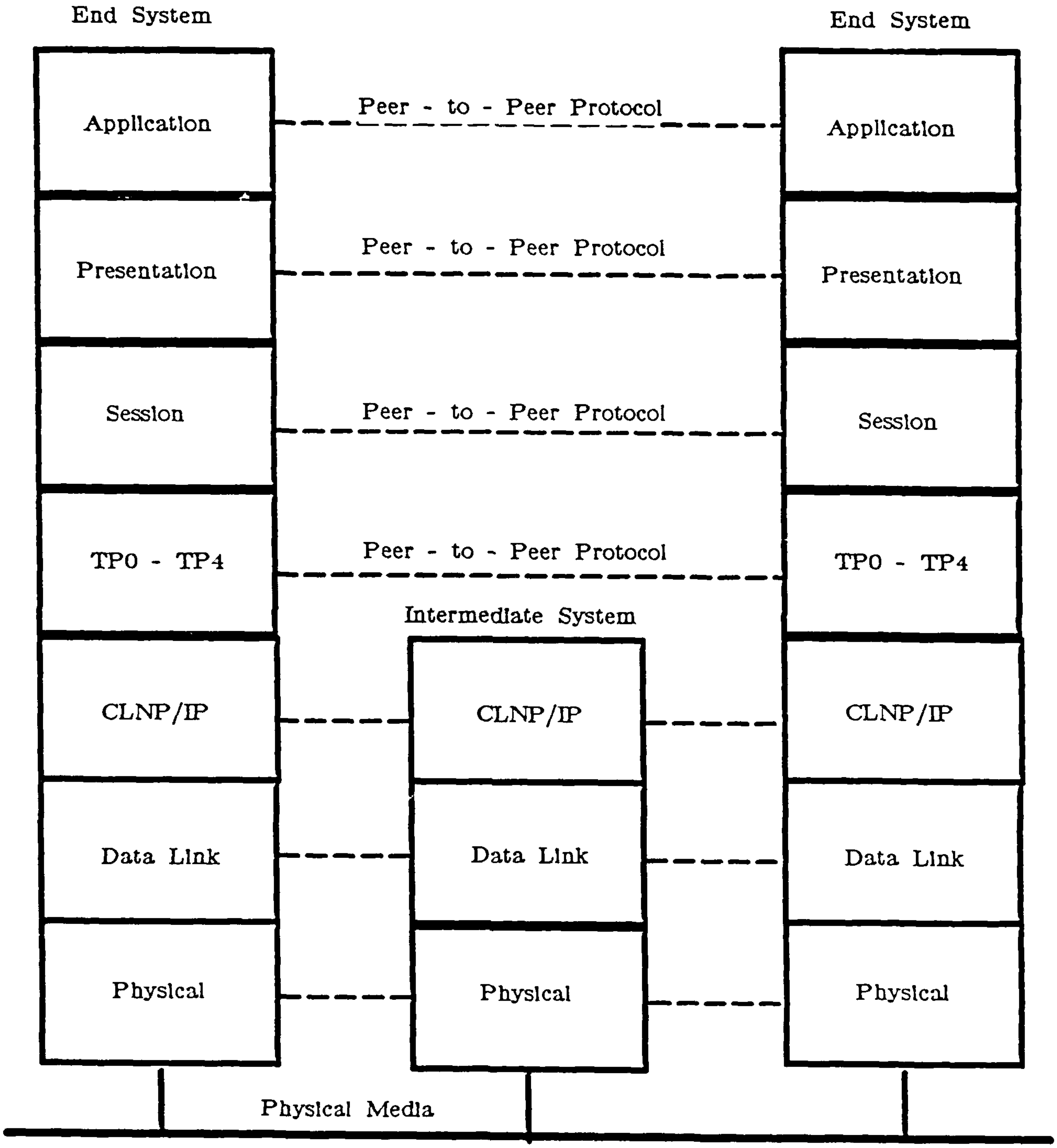

Figure A-2. Peer Entity Communication network physical medium provide the path for this communication which encompasses both the data to be transferred plus control information.

These protocols are set by the OSI standard, thus allowing systems by different vendors to freely communicate with each other regardless of their differences in hardware and operating systems. It is through this standardization that interconnection and the ability to interoperate is enhanced.

Two particular types of open systems are described in the OSI standard, End Systems and Intermediate Systems. The only real difference is that an End System is the ultimate source or destination for user-oriented data while an Intermediate System merely provides internetwork connections, relaying, and routing. For this reason, End Systems must provide the full seven layers while Intermediate Systems need only those layers that provide relaying and routing which are the lowest three (Layers 1 through 3). Computer systems may provide both the services of an End System and an Intermediate System.

A.1.3 Description of Each Layer

Layers 1 through 7 provide a step-by-step enhancement of communication services. The layers communicate with each other via protocols defined by the OSI standard although this standard does not set the manner in which these protocols are implemented. This frees the vendors to implement these protocols in the most efficient manner for their particular computer systems. As long as all use the same data format when actually transmitting data on the physical media, all systems will be able to communicate with each other.

A.1.3.1 Layer 7 - Application

The Application Layer provides a means for application-processes to access the OSI environment. An application-process is an element within an open system which performs the information processing for a particular application. Some examples of application-processes are:

a. *Manual application process.* A person using an automated teller machine.

b. *Computerized application process.* An Ada program executing in a computer system and accessing remotely located files or databases.

c. *Physical application process.* A process control program executing in a factory-based computer linked to a plant control system.

To perform completely these applications may require parts (or entities) of the overall process to be resident on different computer systems and to interact through the resources of the network utilizing the application layer protocols to do so. Through the services provided by the lower layers these entities may act as though they were co-resident on the same computer system. Thus, OSI allows open systems to cooperate in order to achieve the desired goal.

Since Layer 7 is the top-most layer, it does not interface with a higher layer. This application layer is intended to be the interface for application processes to access the OSI environment.

Some of the services provided by this layer or are intended to be included later are as follows:

a. Identification of intended communication partners (for example by name, by address, by definite description, or by generic description).

b. Determination of the current availability of the intended communication partners.

c. Establishment of authority to communicate (to be added later).

d. Agreement of privacy mechanisms (to be added later).

A.1.3.2 Layer 6 - Presentation

It provides for the representation of information that the application-entities either communicate or refer to in their communication. In some implementations it would be used to control terminal data representation in order to provide service that was not terminal specific.

The Presentation Layer is concerned only with the syntax, i.e., the representation of the data and not with its "meaning", which is known only to the application-entities. The Presentation Layer provides primarily the transformation of syntax and the selection of syntax for application-entities.

> Transformation of syntax is concerned with code and character set conversions, with the modification of the layout of the data and the adaptation of actions on the data structures. Selection of syntax provides the means of initially selecting a syntax and subsequently modifying the selection. [ISO 7498]

A.1.3.3 Layer 5 - Session

The Session Layer's chief purpose is to provide the means for peer-presentation entities to co-operate. It does this by organizing and synchronizing their dialogue and managing their data exchange.

Some of the services supplied by the Session Layer are:

a. Session-connection establishment and release

b. Normal data exchange

c. Expedited data exchange

d. Graceful close (not provided by Transport)

A.1.3.4 Layer 4 - Transport

All protocols defined for the Transport Layer have end-to-end significance, where the end-entities are defined to be correspondent transport-entities. They provide transparent and reliable transfer of data between Session-Entities. The protocols have meaning only for the ultimate source and destination of the data being passed over the network. The Transport Layer is relieved of any concern with routing and relaying since the network-service provides network-connections from any transport-entity to any other.

The services provided by the Transport Layer are as follows:

a. Transport-connection establishment (connection oriented)

b. Data transfer

c. Transport-connection release

The above descriptions are primarily for connection-oriented transport protocols. Connectionless or datagram-type of transport protocols are currently under development [ISO 8072/DAD1; ISO DIS 8602].

A.1.3.5 Layer 3 - Network

The Network Layer enables users to transfer data across subnetworks. This layer also provides routing and relaying of data plus flow control within and at the entry point to subnetworks.

In intermediate systems this forms the highest layer needed since the Network Layer is the only layer responsible for routing and relaying of data. Interactions with higher layers are not needed.

Some of the functions provided by the Network Layer are as follows:

a. Routing and relaying

b. Network-connections and their multiplexing

c. Segmenting and blocking (breaking long data streams up into smaller sets and then reassembling them)

d. Error detection and recovery

e. Flow control

f. Network layer management

A.1.3.6 Layer 2 - Data Link (Logical Link Control)

The Data Link provides the means to manage data-link connections over their lifetime. This includes the establishment, maintenance, and termination of connections. Errors may occur in the Physical Layer and the Data Link Layer detects these with possible error correction. In addition, this layer allows the Network Layer to control the interconnection of data circuits within the Physical Layer.

Some of the services provided by the Data Link Layer are the following:

a. Data link connection

b. Transceiving of data units

c. Sequencing

d. Flow control

A.1.3.7 Layer 1 - Physical

This is the lowest layer and it provides the electrical, mechanical, and functional means for the upper layers to connect to and control the physical media. The higher layers are provided primarily through software or firmware while the Physical Layer is primarily hardware, as the name implies.

Some of the services provided by this layer are as follows:

a. Physical connections

b. Data-circuit identification

c. Fault-condition notification

d. Transceiving of data via the format specified by the hardware and transmission media

APPENDIX B

AN OVERVIEW OF GOSIP

The Government Open Systems Interconnection Profile Specification [GOSIP 87] sets forth the requirements for ADP equipment concerning their networking capabilities, and therefore, their ability to interconnect. What follows in this section is an overview of the GOSIP specification.

The reader should keep in mind that the protocol definitions and basic capabilities are the result of a collaboration between the National Bureau of Standards (NBS) and the commercial vendor community. Therefore, the GOSIP document concentrates upon what is or will soon be commercially available. GOSIP provides for the possibility that the OSI protocols are not sufficient for all applications.

B.1 OVERVIEW OF THE SPECIFICATIONS

B.1.1 What is GOSIP?

GOSIP addresses the need of the Federal Government to move immediately to multi-vendor interconnectivity without sacrificing essential functionality already implemented in critical networking systems.

In other words, GOSIP is a set of rules for the specification of the interoperable capabilities of new ADP equipment.

B.1.2 Motivation for the GOSIP requirements.

GOSIP's use of the OSI standards is an attempt to prevent further proliferation of different network protocols within the government. Since all new systems must support the OSI standard, the goal is to move to only one network standard, the OSI.

The ISO standard for Open System Interconnection will provide a common meeting ground for many different vendor's equipment thus reducing the proliferation of private data network domains with each using their own, mutually incompatible, standards. Standardized hardware will also reduce the cost of data networks as well as make the upkeep process easier, since staff will have fewer different network "standards" to master.

B.1.3 What is Mandated?

GOSIP is to be used by all Federal Government agencies when procuring computer network products and services and communication systems or services that provide equivalent functionality to the protocols defined in the GOSIP documents. It is mandatory for all new network implementations.

Existing equipment of all classes is not required to be converted to the OSI standard, although this action is urged.

> Although GOSIP mandates OSI implementation in products, it does not preclude the acquisition of additional (perhaps vendor-specific) networking capabilities in that same equipment. [GOSIP 87]
>
> For a period of eighteen months after the effective date of the GOSIP documents agencies are permitted to acquire alternative protocols which provide equivalent functionality to the GOSIP protocols. [GOSIP 87]
>
> After the eighteen-month period, the new protocols (GOSIP) should be cited in solicitation proposals when systems to be acquired provide equivalent functionality to the protocols defined in the GOSIP documents. [GOSIP 87]

For an indefinite time, agencies may buy additional, perhaps vendor specific, network products in addition to GOSIP-mandated OSI products.

B.1.4 Timetable

The DoD implementation schedule for GOSIP is expected to be as follows.

GOSIP will form an "Experimental" co-standard to the DoD protocol suite in the third quarter of FY-87 with prototype implementations of the Translating Applications Gateways for both SMTP-X.400 (Simple Mail Transfer Protocol - Message Handling System, X.400) and FTP-FTAM (File Transfer Protocol - File Transfer and Access Management), to be completed in early FY-88.

GOSIP will become fully co-standard approximately one year from the time it achieves experimental status, which should be around the third quarter of FY-88. Approximately two years from full co-standard status, only GOSIP-based products will be procured and by the five- to seven-year point from co-standard, the transition from DoD protocols to OSI protocols is expected to be completed.

B.1.5 The Specified OSI Subset

The OSI standard specifies a seven-layer architecture: Application, Presentation, Session, Transport, Network, Data Link, and Physical. Some of the OSI standard layers can have many options that tailor a layer's performance, capability, and/or reliability. The GOSIP specification (Figure B-1) requires certain options while allowing the remainder to be implemented as "enhancements".

Achieving widespread use of OSI within the government can be accomplished by using standard protocol profiles at each OSI layer. A protocol profile is a collection of protocols that

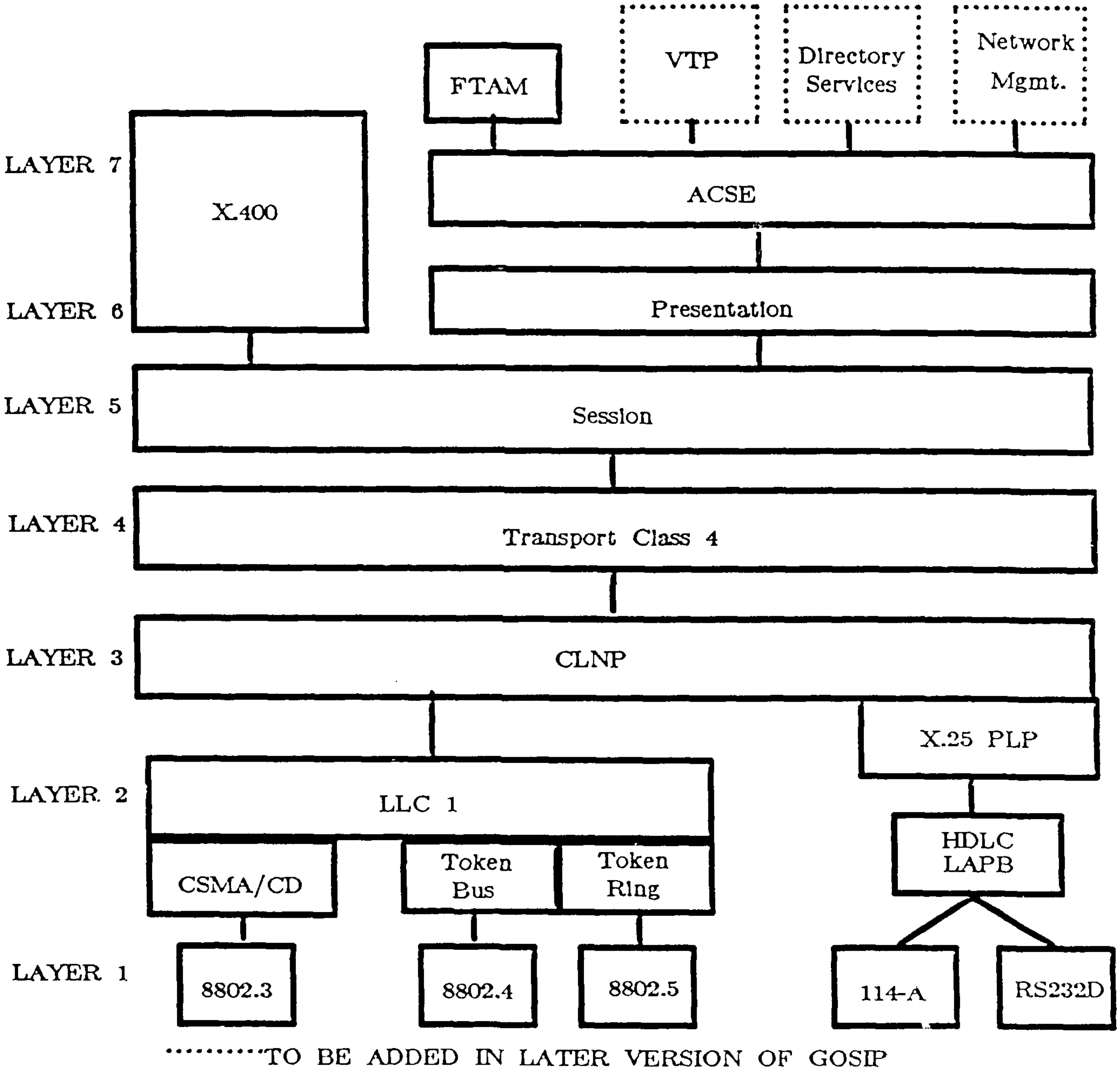

Figure B-1. Government OSI Architecture collectively perform a function (e.g., TP0, TP4, or MHS). However, when dealing with the lower layers, GOSIP specifies a selection from among a small set of network technologies for local and wide area networking. A selection is allowed since these technologies offer different cost/performance tradeoffs that makes one technology more appropriate than another in any given situation. More than one of these technologies may be selected as needed. At the upper layers only two applications are currently included. These are the file transfer (FTAM) and message handling (MHS or X.400). Each application may require a different selected set of services from the application control service elements and the presentation and session control layers.

In almost every case where there are choices to be made concerning options, enhancements, or the desired subset of all possible features, the Acquisition Authority has the responsibility to make the decisions. It is imperative therefore, that the Acquisition Authority be very familiar with the immediate needs and the long term needs of the installation so that the proper selections can be made.

B.1.5.1 Physical Layer

This layer shall be selected from among the following. In systems utilizing X.25, choose from among [MIL-STD-188/144A] and [EIA-232-D]. In conjunction with the use of IEEE 802.2 (Logical Link Control), choose from [IEEE 802.3; IEEE 802.4; and IEEE 802.5].

B.1.5.2 Data Link

In accordance with [CCITT X.25], High Level Data Link Control (HDLC) Link Access Procedure B (LAP B) shall be used and IEEE 802.2 shall be used in conjunction with [IEEE 802.3; IEEE 802.4; or IEEE 802.5].

B.1.5.3 Network

This layer shall provide network service for internetworking by the ISO connectionless

(CLNS) internet protocol (IP) [NBS 87, ISO 8072/DAD1; ISO 8473]. For interworking of concatenated networks IP must be implemented. On a single subnetwork, although IP must be implemented, it may or may not be used at the discretion of the source end system.

GOSIP specifies some modifications to the maximum lifetime of a message, the use of security parameters, what checksums will be turned on and used, and that only one switched virtual circuit per different priority requested shall be initiated. One addition is that the CLNS shall be provided with interfaces to the 1984 CCITT Recommendation X.25 and the IEEE 802.2, as selected by the Acquisition Authority. The Acquisition Authority may also require a particular mapping of Connectionless Network service (CLNS) Protocol Data Unit (PDU) priorities onto switched virtual circuits (SVCs) when CLNS is used over X.25.

B.1.5.4 Transport

The vendor shall provide transport class 4. Transport class 0 must only be used with public data network messaging systems. Therefore:

- *Class 0.* Class 0 is the simplest type of transport connection and is compatible with the CCITT recommendation S.70 for teletex terminals.
- *Class 4.* Class 4 of transport connection provides several enhancements over class 0. Multiplexing several transport connections onto a single network connection, the ability to recover from network disconnects or resets, plus the capability to detect and recover from errors which occur as the result of low grade service provided by the network layer.

B.1.5.5 Session

The vendor shall supply the Session protocol as specified by the NBS/OSI Workshop agreements [NBS 87]. Application Layer protocols determine the session functional units needed for support.

B.1.5.6 Presentation

The abstract syntax NBS-AS3 facilitates implementing a file system directory inquiry when the International Standard for FTAM includes those service primitives. This syntax is optional in the ISO specifications of the OSI model but is mandatory in the GOSIP specification.

B.1.5.7 Application Layer

Within this layer the Association Control Service Elements (ACSE) are required to support all applications except messaging. The File Transfer and Access Management Protocol (FTAM) must support many Document Types (NBS-2, NBS-3, NBS-4, NBS-5, AND NBS-9)[1] in addition to NBS-1 since GOSIP includes binary, textual, and directory file types.

The Messaging Handling System (X.400) shall support all Message Transfer Services and Interpersonal Messaging services. End systems directly connected to a public data network must use transport class 0 when messaging over the public data network. Transport class 4 is required for messaging within private management domains.

In addition, the MHS includes the Application Control Service Element and the Presentation Layers so that it operates directly with the Session Layer. Therefore, if a system is to include only this application, then the Presentation and ACSE Layers need not be specified.

B.1.6 End Systems versus Intermediate Systems

An End system contains the application processes that are the ultimate sources and destinations of user oriented data flows. The functions of an end system can be distributed

[1] These are discussed in detail in Appendix 6A of [NBS 87].

among more than one processor/computer.

An Intermediate system interconnects two or more subnetworks performing both routing and relaying of traffic. A system can implement the functions of both an End system and an Intermediate system.

End systems must support all seven layers plus their special requirements as detailed above.

Intermediate systems must support the first three layers (Application, Presentation, and Session) and operate in Connectionless mode (connectionless internetwork protocol) regardless of whether the underlying technology uses connectionless (CSMA/CD) or connection-oriented (X.25) mode.

APPENDIX C

DoD MEMORANDUM

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

2 JUL 1987

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
DIRECTORS, DEFENSE AGENCIES

SUBJECT: Open Systems Interconnection Protocols

There has been recent rapid progress in the specification and implementation of computer protocols based on the International Organization for Standardization model for Open Systems Interconnection (OSI). The Government OSI Profile (GOSIP), dated 22 April 1987, contains sufficient information to specify adequately and acquire interoperable vendor implementations of OSI message handling and file transfer capabilities. Therefore, the policy on standardization of host-to-host protocols for data communications, promulgated by USDR&E memo of 23 March 1982, is modified as follows. The OSI message handling and file transfer protocols, together with their underlying protocols as defined in GOSIP, are adopted as experimental co-standards to the DoD protocols which provide similar services (MIL-STDs 1777, 1778, 1780, and 1781). These OSI protocols may be specified in addition to, in lieu of, or as an optional alternative to DoD protocols, in cases where the current DoD protocol applicability statements apply. They are designated as experimental because of the limited operational experience currently available with the OSI protocols and the limited operational, testing, and security environment currently defined in GOSIP. Services and agencies choosing to implement OSI protocols at this time should carefully evaluate these factors and be prepared to deal with the complications which may accompany the introduction of new technology.

It is intended to adopt the OSI protocols as a full co-standard with the DoD protocols when GOSIP is formally approved as a Federal Information Processing Standard. Two years thereafter, the OSI protocols would become the sole mandatory interoperable protocol suite; however, a capability for interoperation with DoD protocols would be provided for the expected life of systems supporting the DoD protocols.

In order to extend the OSI protocol capabilities and provide interoperability between the DoD and OSI protocols as rapidly as possible, the following actions are requested:

a. The Director, Defense Communications Agency, as the DoD Executive Agent for Data Communications Protocol Standards, should:

o Publish by November 1987 the DoD-OSI Interoperability and Transition Plan. The plan should provide for interoperation of the DoD and OSI protocols at the application level. A capability for experimental interoperability of DoD and OSI message handling and file transfer capabilities should be provided by March 1988, and a limited operational capability by January 1989.

o Join the Corporation for Open Systems (COS) as the Department of Defense representative. COS is a non-profit consortium formed to deal with testing and other operational issues relating to OSI protocols. At the request of the Office of Management and Budget, the Services and other defense agencies should not join COS directly, but may participate as the agents of DCA on appropriate COS committees.

o Coordinate Service and agency participation, in accordance with existing directives, in groups developing OSI standards, specifications, and operating and management procedures. These groups include the Government OSI User's Group, the National Bureau of Standards OSI Implementor's Workshops, the Corporation for Open Systems, the Manufacturing and Automation Protocol (MAP) and Technical and Office Protocol (TOP) user's groups, the American National Standards Institute X3S3 and X3T5 committees, and the NATO Tri-Service Group on Communications and Electronic Equipment, Sub-Group 9 (Data Processing and Distribution).

b. The Director, National Security Agency should assure that the efforts of the ongoing Secure Data Network Systems program can be used to provide the security extensions defined as future work items in GOSIP.

c. The Services and defense agencies should share the results and experience of early implementations under the experimental coexistence policy by actively participating in the groups indicated above, under DCA coordination. This experience should be particularly valuable in assuring that military requirements can be satisfied by the developing OSI standards, specifications, and procedures.

This guidance provides for the interim steps necessary to continue progress toward implementation of OSI standards. As the technology matures and DoD gains additional experience, the final implementation details will be provided in a DoD Directive.

Donald C. Latham

Donald C. Latham

Distribution List for IDA Paper P-2041

NAME AND ADDRESS	NUMBER OF COPIES
Sponsor	
Lt Col Frank Graves C3 Systems, JRIM, JCS Room IE833 The Pentagon Washington, D.C. 20301	3 copies
Other	
Defense Technical Information Center Cameron Station Alexandria, VA 22314	2 copies
CSED Review Panel	
Dr. Dan Alpert, Director Center for Advanced Study University of Illinois 912 W. Illinois Street Urbana, Illinois 61801	1 copy
Dr. Barry W. Boehm TRW Defense Systems Group MS 2-2304 One Space Park Redondo Beach, CA 90278	1 copy
Dr. Ruth Davis The Pymatuning Group, Inc. 2000 N. 15th Street, Suite 707 Arlington, VA 22201	1 copy
Dr. Larry E. Druffel Software Engineering Institute Carnegie-Mellon University Pittsburgh, PA 15213-3890	1 copy
Dr. C.E. Hutchinson, Dean Thayer School of Engineering Dartmouth College Hanover, NH 03755	1 copy

NAME AND ADDRESS	NUMBER OF COPIES
Mr. A.J. Jordano Manager, Systems & Software Engineering Headquarters Federal Systems Division 6600 Rockledge Dr. Bethesda, MD 20817	1 copy
Mr. Robert K. Lehto Mainstay 302 Mill St. Occoquan, VA 22125	1 copy
Mr. Oliver Selfridge 45 Percy Road Lexington, MA 02173	1 copy
IDA	
General W.Y. Smith, HQ	1 copy
Mr. Philip Major, HQ	1 copy
Dr. Jack Kramer, CSED	1 copy
Dr. Robert I. Winner, CSED	1 copy
Dr. John Salasin, CSED	1 copy
Ms. Anne Douville, CSED	1 copy
Mr. Terry Mayfield, CSED	1 copy
Mr. James Baldo, CSED	2 copies
Dr. David O. Levan, CSED	2 copies
Ms. Katydean Price, CSED	2 copies
IDA Control & Distribution Vault	3 copies